StorageGRID 11.5-Dokumentation

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-115/index.html on October 03, 2025. Always check docs.netapp.com for the latest.

Inhalt

StorageGRID 11.5-Dokumentation . . . 1
Versionshinweise . . . 2
Los geht’s . . . 3
Gittergrundierung . . . 3
Informationen zu StorageGRID . . . 3
StorageGRID Architektur und Netzwerktopologie . . . 7
Managen von Daten mit StorageGRID . . . 16
Wie Grid Manager zu sehen ist . . . 26
Entdecken Sie den Tenant Manager . . . 34
Verwenden von StorageGRID . . . 37
Netzwerkrichtlinien . . . 72
Überblick über das StorageGRID Networking . . . 72
Netzwerkanforderungen . . . 83
Netzwerkspezifische Anforderungen . . . 84
Implementierungs-spezifische Netzwerküberlegungen . . . 86
Netzwerkinstallation und -Bereitstellung . . . 89
Richtlinien nach der Installation . . . 90
Referenz für Netzwerk-Ports . . . 91
Installation und Upgrade von Software . . . 105
Installieren Sie Red hat Enterprise Linux oder CentOS . . . 105
Übersicht über die Installation . . . 105
Planung und Vorbereitung . . . 106
Implementierung virtueller Grid-Nodes . . . 129
Grid wird konfiguriert und die Installation abgeschlossen . . . 155
Automatisierung der Installation . . . 171
Überblick über DIE REST API zur Installation . . . 173
Weitere Schritte . . . 174
Fehlerbehebung bei Installationsproblemen . . . 175
Beispiel /etc/sysconfig/Network-scripts . . . 176
Installieren Sie Ubuntu oder Debian . . . 178
Übersicht über die Installation . . . 179
Planung und Vorbereitung . . . 180
Implementierung virtueller Grid-Nodes . . . 205
Grid wird konfiguriert und die Installation abgeschlossen . . . 231
Automatisierung der Installation . . . 247
Überblick über DIE REST API zur Installation . . . 249
Weitere Schritte . . . 250
Fehlerbehebung bei Installationsproblemen . . . 252
Beispiel /etc/Netzwerk/Schnittstellen . . . 252
VMware installieren . . . 254
Übersicht über die Installation . . . 254
Planung und Vorbereitung . . . 255
Grid-Nodes von Virtual Machines in VMware vSphere Web Client werden implementiert . . . 264

Grid wird konfiguriert und die Installation abgeschlossen . . . 273
Automatisierung der Installation . . . 289
Überblick über DIE REST API zur Installation . . . 303
Weitere Schritte . . . 303
Fehlerbehebung bei Installationsproblemen . . . 305
Software-Upgrade . . . 306
Informationen zu StorageGRID 11.5 . . . 306
Planung und Vorbereitung von Upgrades . . . 320
Durchführen des Upgrades . . . 332
Fehlerbehebung bei Upgrade-Problemen . . . 345
Installation und Wartung von Hardware . . . 348
SG6000 Storage-Appliances . . . 348
SG6000 Appliances – Übersicht . . . 348
Übersicht über Installation und Implementierung . . . 359
Installation wird vorbereitet . . . 361
Installieren der Hardware . . . 377
Konfigurieren der Hardware . . . 395
Implementieren eines Appliance-Storage-Node . . . 438
Monitoring der Installation der Speicher-Appliance . . . 442
Automatisierung der Installation und Konfiguration von Appliances . . . 444
Überblick über die Installations-REST-APIs . . . 452
Fehlerbehebung bei der Hardwareinstallation . . . 453
Warten des SG6000-Geräts . . . 462
SG5700 Storage-Appliances . . . 529
Übersicht über die StorageGRID Appliance . . . 529
Übersicht über Installation und Implementierung . . . 534
Installation wird vorbereitet . . . 535
Installieren der Hardware . . . 549
Konfigurieren der Hardware . . . 560
Implementieren eines Appliance-Storage-Node . . . 595
Monitoring der Installation der Speicher-Appliance . . . 599
Automatisierung der Installation und Konfiguration von Appliances . . . 601
Überblick über die Installations-REST-APIs . . . 609
Fehlerbehebung bei der Hardwareinstallation . . . 610
Warten der SG5700 Appliance . . . 614
SG5600 Storage Appliances . . . 657
Übersicht über die StorageGRID Appliance . . . 657
Übersicht über Installation und Implementierung . . . 662
Installation wird vorbereitet . . . 663
Installieren der Hardware . . . 678
Konfigurieren der Hardware . . . 690
Implementieren eines Appliance-Storage-Node . . . 723
Monitoring der Installation der Speicher-Appliance . . . 727
Automatisierung der Installation und Konfiguration von Appliances . . . 729
Überblick über die Installations-REST-APIs . . . 737

Fehlerbehebung bei der Hardwareinstallation . . . 738
Warten der SG5600 Appliance . . . 742
SG100- und SG1000-Services-Appliances . . . 780
SG100- und SG1000-Geräte im Überblick . . . 780
SG100- und SG1000-Applikationen . . . 783
Übersicht über Installation und Implementierung . . . 784
Installation wird vorbereitet . . . 786
Installieren der Hardware . . . 799
Konfigurieren von StorageGRID-Verbindungen . . . 807
Konfigurieren der BMC-Schnittstelle . . . 832
Optional: Aktivieren der Node-Verschlüsselung . . . 839
Implementieren eines Service-Appliance-Nodes . . . 841
Fehlerbehebung bei der Hardwareinstallation . . . 861
Warten des Geräts . . . 868
Konfiguration und Management . . . 897
StorageGRID verwalten . . . 897
Verwalten eines StorageGRID-Systems . . . 897
Kontrolle des Administratorzugriffs auf StorageGRID . . . 928
Konfigurieren von Verschlüsselungsmanagement-Servern . . . 971
Management von Mandanten . . . 1001
Konfigurieren von S3- und Swift-Client-Verbindungen . . . 1024
Verwalten von StorageGRID-Netzwerken und -Verbindungen . . . 1057
AutoSupport wird konfiguriert . . . 1087
Verwalten Von Storage-Nodes . . . 1103
Verwalten Von Admin-Nodes . . . 1128
Verwalten Von Archivierungs-Knoten . . . 1152
Datenmigration zu StorageGRID . . . 1176
Objektmanagement mit ILM . . . 1179
Verwalten von Objekten mit Information Lifecycle Management . . . 1180
Verwalten von Objekten mit S3 Object Lock . . . 1311
Beispiele für ILM-Regeln und -Richtlinien . . . 1323
Systemhärtung . . . 1351
Sicherung eines StorageGRID Systems . . . 1351
Hardening-Richtlinien für Software Upgrades . . . 1352
Hardening Guidelines for StorageGRID Networks . . . 1353
Hardening-Richtlinien für StorageGRID-Knoten . . . 1354
Härtungsrichtlinien für Serverzertifikate . . . 1357
Andere Hinweise zur Verhärtung . . . 1358
Konfigurieren Sie StorageGRID für FabricPool . . . 1359
StorageGRID für FabricPool wird konfiguriert . . . 1359
Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier . . . 1362
Informationslebenszyklus-Management von StorageGRID bei FabricPool-Daten ein . . . 1372
Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool . . . 1375
Weitere Best Practices für StorageGRID und FabricPool . . . 1378
Verwenden Sie StorageGRID . . . 1379

Verwenden Sie ein Mandantenkonto . . . 1379
Verwenden des Mandanten-Manager . . . 1379
Managen des Systemzugriffs für Mandantenbenutzer . . . 1394
Verwalten von S3-Mandantenkonten . . . 1416
Verwalten von S3-Plattformservices . . . 1446
S3 verwenden . . . 1488
Unterstützung für die S3-REST-API . . . 1488
Mandantenkonten und -Verbindungen werden konfiguriert . . . 1492
So implementiert StorageGRID die S3-REST-API . . . 1498
Unterstützte Vorgänge und Einschränkungen durch S3-REST-API . . . 1505
StorageGRID S3 REST-API-Operationen . . . 1559
Bucket- und Gruppenzugriffsrichtlinien . . . 1582
Sicherheit wird für DIE REST API konfiguriert . . . 1609
Monitoring und Auditing von Vorgängen . . . 1612
Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen . . . 1615
Verwenden Sie Swift . . . 1618
Unterstützung für OpenStack Swift API in StorageGRID . . . 1618
Mandantenkonten und -Verbindungen werden konfiguriert . . . 1622
Von Swift UNTERSTÜTZTE REST-API-Operationen . . . 1627
StorageGRID Swift REST-API-Operationen . . . 1639
Sicherheit wird für DIE REST API konfiguriert . . . 1644
Monitoring und Auditing von Vorgängen . . . 1647
Monitoring und Fehlerbehebung . . . 1651
Überwachen Sie ein StorageGRID System . . . 1651
Verwenden des Grid Managers zur Überwachung . . . 1651
Informationen, die Sie regelmäßig überwachen sollten . . . 1692
Verwalten von Meldungen und Alarmen . . . 1735
Verwendung von SNMP-Überwachung . . . 1786
Erfassung weiterer StorageGRID-Daten . . . 1801
Alerts Referenz . . . 1837
Alarmreferenz (Altsystem) . . . 1884
Referenz für Protokolldateien . . . 1945
Fehler in einem StorageGRID System beheben . . . 1964
Überblick über die Problembestimmung . . . 1964
Fehlerbehebung bei Objekt- und Storage-Problemen . . . 1973
Behebung von Metadatenproblemen . . . 2005
Fehlerbehebung bei Zertifikatfehlern . . . 2012
Fehlerbehebung bei Problemen mit Admin-Knoten und Benutzeroberfläche . . . 2014
Fehlerbehebung bei Netzwerk-, Hardware- und Plattformproblemen . . . 2018
Prüfung von Audit-Protokollen . . . 2027
Übersicht über Überwachungsnachrichten . . . 2027
Audit-Log-Datei und Nachrichtenformate . . . 2033
Überwachungsmeldungen und der Lebenszyklus von Objekten . . . 2052
Audit-Meldungen . . . 2060
Wartung . . . 2124

Erweitern Sie Ihr Raster . . . 2124
StorageGRID-Erweiterung geplant . . . 2124
Vorbereitung auf eine Erweiterung . . . 2139
Überblick über das Expansionsverfahren . . . 2145
Hinzufügen von Storage-Volumes zu Storage-Nodes . . . 2147
Einem vorhandenen Standort Grid-Nodes hinzufügen oder einen neuen Standort hinzufügen . . . 2154
Konfiguration des erweiterten StorageGRID-Systems . . . 2170
Kontakt mit dem technischen Support . . . 2181
Halten Sie Recoverys ein . . . 2182
Einführung in StorageGRID Recovery und Wartung . . . 2182
StorageGRID Hotfix Verfahren . . . 2184
Verfahren zur Recovery von Grid-Nodes . . . 2194
Durchführen der Standortwiederherstellung durch den technischen Support . . . 2303
Verfahren zur Deaktivierung . . . 2305
Netzwerkwartungsverfahren . . . 2359
Verfahren auf Host-Ebene und Middleware . . . 2382
Verfahren für den Grid-Node . . . 2390
Klonen von Appliance-Nodes . . . 2415
Rechtliche Hinweise . . . 2425
Urheberrecht . . . 2425
Marken . . . 2425
Patente . . . 2425
Datenschutzrichtlinie . . . 2425
Open Source . . . 2425

StorageGRID 11.5-Dokumentation

Versionshinweise

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

Versionshinweise sind außerhalb dieser Dokumentwebsite erhältlich. Sie werden aufgefordert, sich mit Ihren Anmeldedaten für die NetApp Support Site anzumelden.

- "HTML"
- "PDF"

Los geht’s

Gittergrundierung

Lernen Sie die Grundlagen eines NetApp StorageGRID Systems kennen.

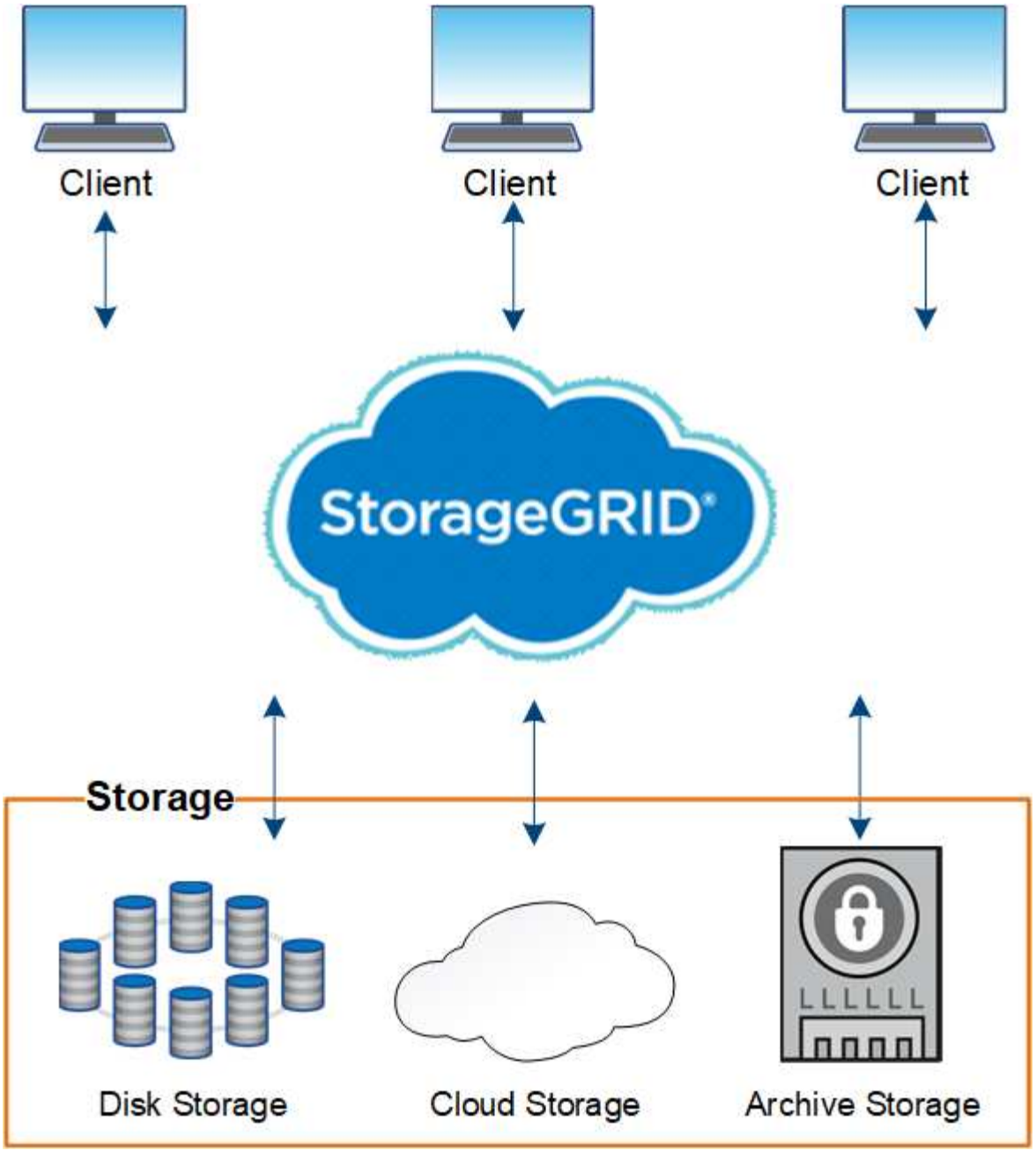
- "Informationen zu StorageGRID"
- "StorageGRID Architektur und Netzwerktopologie"
- "Managen von Daten mit StorageGRID"
- "Wie Grid Manager zu sehen ist"
- "Entdecken Sie den Tenant Manager"
- "Verwenden von StorageGRID"

Informationen zu StorageGRID

NetApp StorageGRID ist eine softwaredefinierte, objektbasierte Storage-Lösung, die dem Branchenstandard entsprechende Objekt-APIs, einschließlich der S3-API (Amazon Simple Storage Service) und der OpenStack Swift-API unterstützt.

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.



Das StorageGRID System bietet unter anderem folgende Vorteile:

- Extrem skalierbar und leicht zu verwendende Daten-Repositorys mit geografisch verteilten Standorten für unstrukturierte Daten
- Standard-Objekt-Storage-Protokolle:
  - Amazon Web Services Simple Storage Service (S3)
  - OpenStack Swift
- 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 Content-Replizierung, Ereignisbenachrichtigung und Metadatensuche in Public Clouds.
- 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. Das Band wird als integrierte Archivebene angeboten.
- 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.
  - Docker Container 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).

Verwandte Informationen

"Hybrid Clouds mit StorageGRID"

"StorageGRID Architektur und Netzwerktopologie"

"Kontrolle des StorageGRID-Zugriffs"

"Management von Mandanten und Client-Verbindungen"

"Mit Information Lifecycle Management"

"Monitoring der StorageGRID Vorgänge"

"Netzwerkeinstellungen werden konfiguriert"

"Durchführung von Wartungsverfahren"

Hybrid Clouds mit StorageGRID

Sie können StorageGRID in einer Hybrid-Cloud-Konfiguration einsetzen, indem Sie richtlinienbasiertes Datenmanagement implementieren, um Objekte in Cloud-Storage-Pools zu speichern, indem Sie StorageGRID Plattform-Services nutzen und Daten mit NetApp FabricPool auf StorageGRID verschieben.

Cloud-Storage-Pools

Mit Cloud-Storage-Pools können Sie Objekte außerhalb des StorageGRID Systems speichern. Beispielsweise möchten Sie selten genutzte Objekte in kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive oder die Archive Access 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.

> 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 SNS-Ereignisse (Receiving 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 StorageGRID

Sie können die Kosten von ONTAP Storage reduzieren, indem Sie Daten mithilfe von FabricPool auf StorageGRID verschieben. FabricPool ist eine Data-Fabric-Technologie von NetApp. Sie ermöglicht automatisiertes Tiering von Daten auf kostengünstige Objekt-Storage-Tiers – lokal oder extern.

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

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"Objektmanagement mit ILM"

"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 in den Netzwerkrichtlinien.

Verwandte Informationen

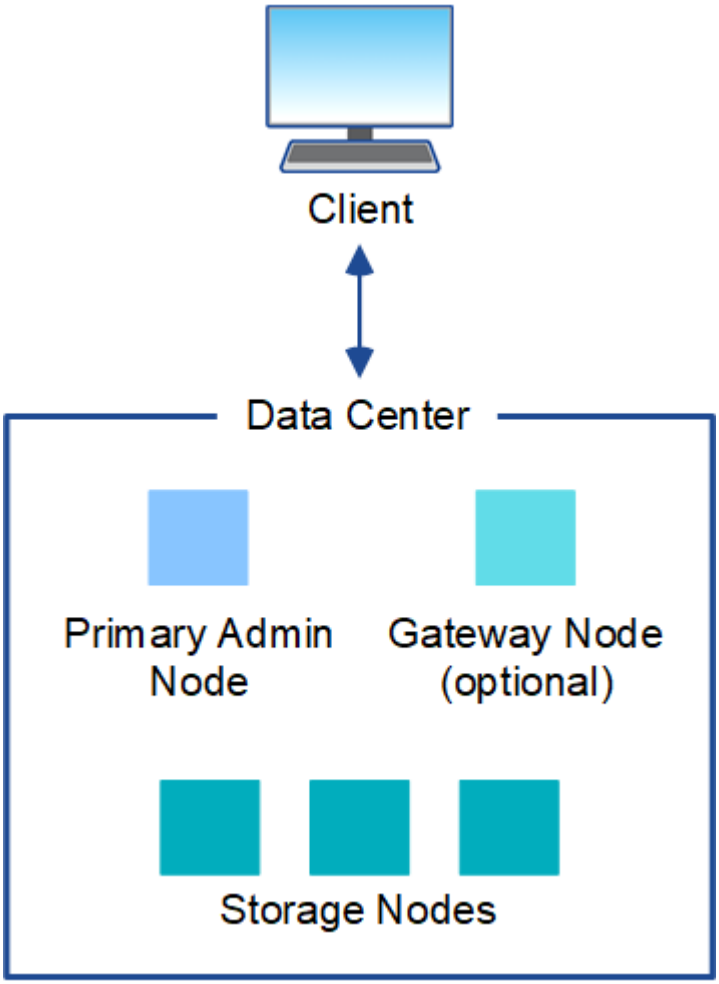
"Netzwerkrichtlinien"

Implementierungstopologien

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

Ein Standort

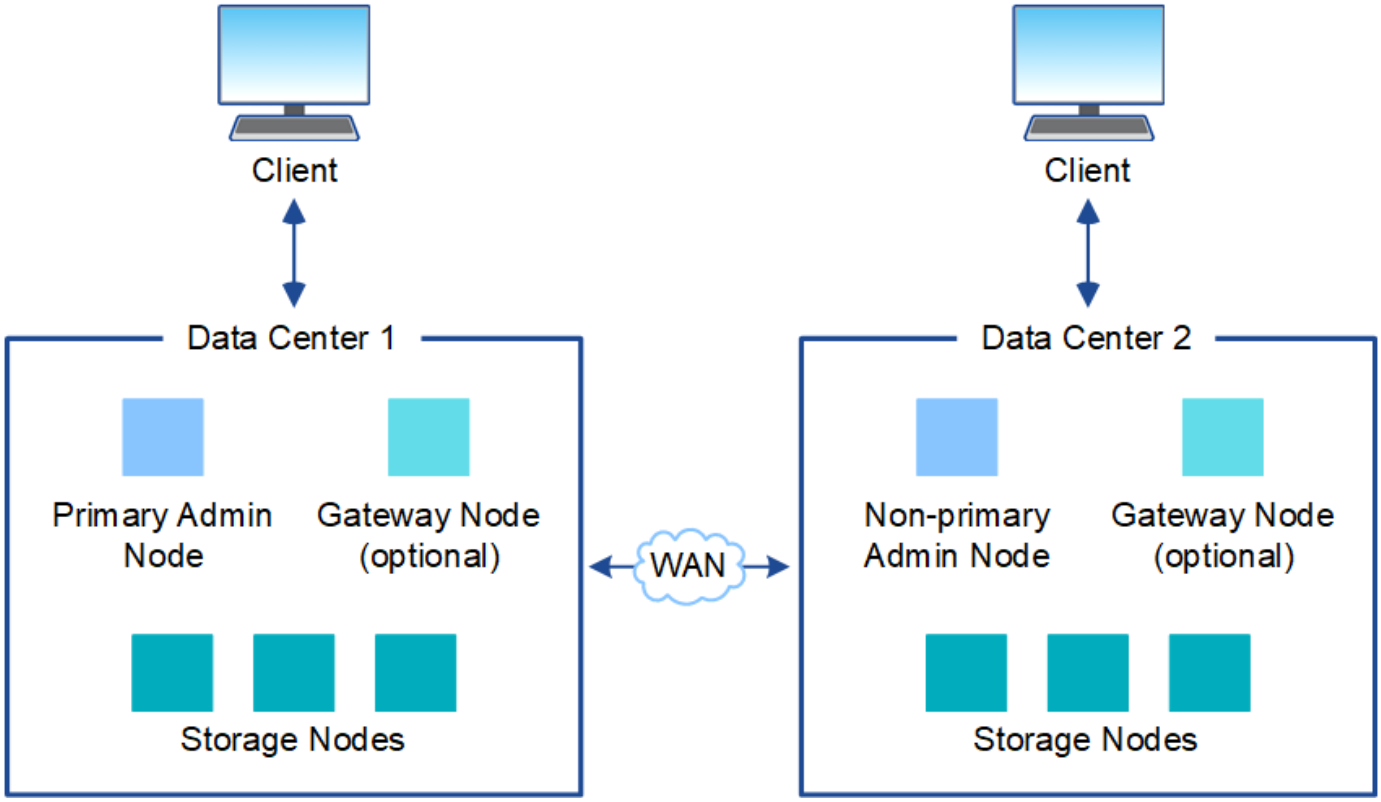
Bei einer Implementierung über einen einzigen Standort werden die Infrastruktur und der Betrieb des StorageGRID Systems zentralisiert.



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.



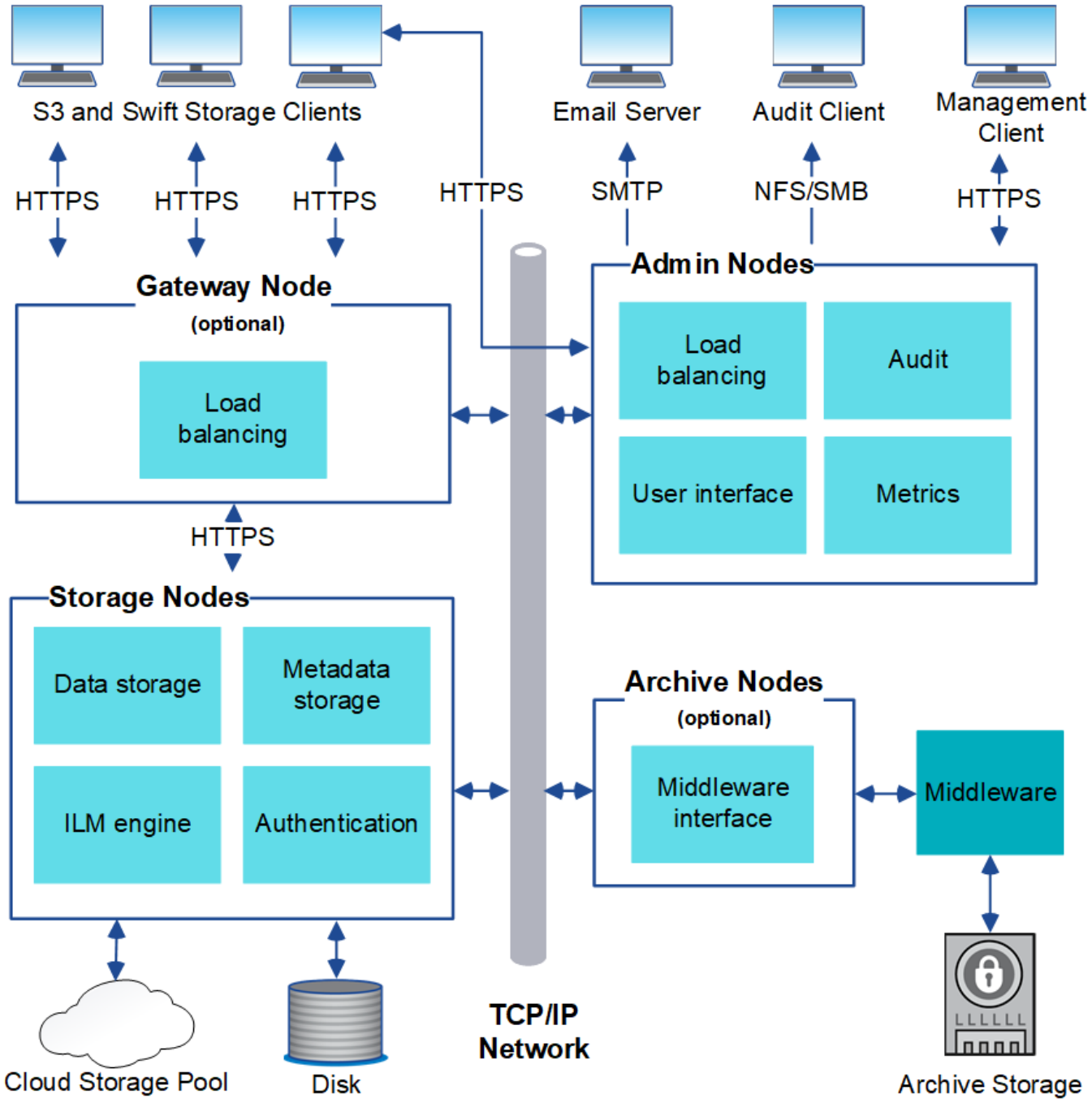
Darüber hinaus können mehrere logische Standorte innerhalb eines einzigen Datacenters eingesetzt werden, um die Verfügbarkeit und Ausfallsicherheit durch verteilte Replizierung und Erasure Coding zu verbessern.

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 Hardware-basierten Storage-Nodes, auf externen Archivierungsmedien wie Tapes oder in Cloud Storage Pools, die aus externen S3 Buckets oder Azure Blob Storage-Containern bestehen, gespeichert werden.

Verwandte Informationen

"StorageGRID verwalten"

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 (optional)** bieten eine Schnittstelle, über die Objektdaten auf Band archiviert werden können.

Softwarebasierte Nodes

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

- Als Virtual Machines (VMs) im VMware vSphere Web Client
- Innerhalb von Docker Containern auf Linux Hosts. Folgende Betriebssysteme werden unterstützt:
  - Red Hat Enterprise Linux
  - CentOS
  - Ubuntu
  - Debian

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

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.

Es sind vier Typen von StorageGRID Appliances verfügbar:

- 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.
- Die **SG5600 Storage Appliance** ist eine integrierte Storage- und Computing-Plattform, die als Storage Node ausgeführt wird. Die SG5600 ist in zwei Modellen erhältlich:
  - **SG5612**: Ein 2-HE-Gehäuse mit 12 NL-SAS-Laufwerken sowie integrierten Storage- und Computing-Controllern
  - **SG5660**: Ein 4-HE-Gehäuse mit 60 NL-SAS-Laufwerken und integrierten Storage- und Computing-Controllern.

Sämtliche Spezifikationen finden Sie im NetApp Hardware Universe.

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 die Systemaktivität.
Configuration Management Node (CMN)	Verwaltet die systemweite Konfiguration. Nur primärer Admin-Node.
Management-Applikations-Programmierschnittstelle (Management-API)	Verarbeitet Anforderungen aus der Grid-Management-API und der Mandantenmanagement-API.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. **Hinweis:** dieser Service befindet sich auch auf Gateway Nodes.

Service	Tastenfunktion
Lastausgleich	Sorgt für einen Lastenausgleich des S3- und Swift-Datenverkehrs von Clients zu Storage Nodes. **Hinweis:** dieser Service befindet sich auch auf Gateway Nodes.
Netzwerk-Management-System (NMS)	Bietet Funktionen für den Grid Manager.
Prometheus	Sammelt und speichert Kennzahlen.
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
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)	Sorgt dafür, dass Service-Anfragen der S3-Plattform an ihre jeweiligen Endpunkte gesendet werden.

Service	Tastenfunktion
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
Verbindungslastverteiler (CLB)	Bietet Layer 3- und 4-Lastausgleich für S3- und Swift-Datenverkehr von Clients zu Storage-Nodes. Mechanismen zum Lastausgleich bei älteren Systemen. **Hinweis:** der CLB-Service ist veraltet.
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 Archiv-Nodes. Diese Tabelle enthält jedoch nicht alle Node-Services.

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

- **CLB-Service (Verbindungslastenabwucher)**

  Veralteter Service, der ein Gateway in StorageGRID für Client-Applikationen bietet, die über HTTP verbunden werden. Der CLB-Dienst ist auf Gateway-Knoten vorhanden. Der CLB-Dienst ist veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

- **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.

- **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.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"NetApp Hardware Universe"

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"StorageGRID verwalten"

Managen von Daten mit StorageGRID

Bei der Arbeit mit dem StorageGRID System ist es hilfreich, zu verstehen, wie das StorageGRID System die Daten managt.

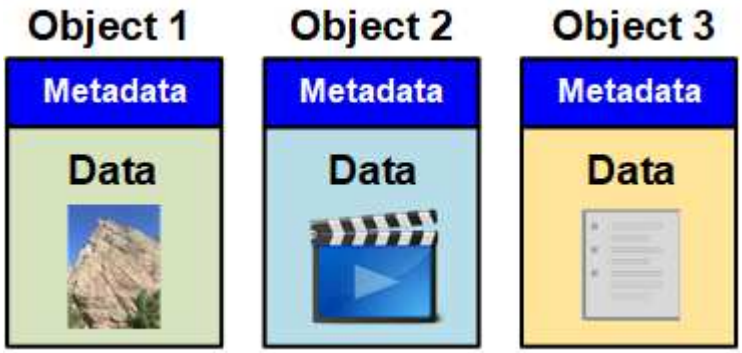
- "Was ist ein Objekt"
- "Schutz von Objektdaten"
- "Das Leben eines Objekts"

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.



Objektdaten

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

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".

Schutz von Objektdaten

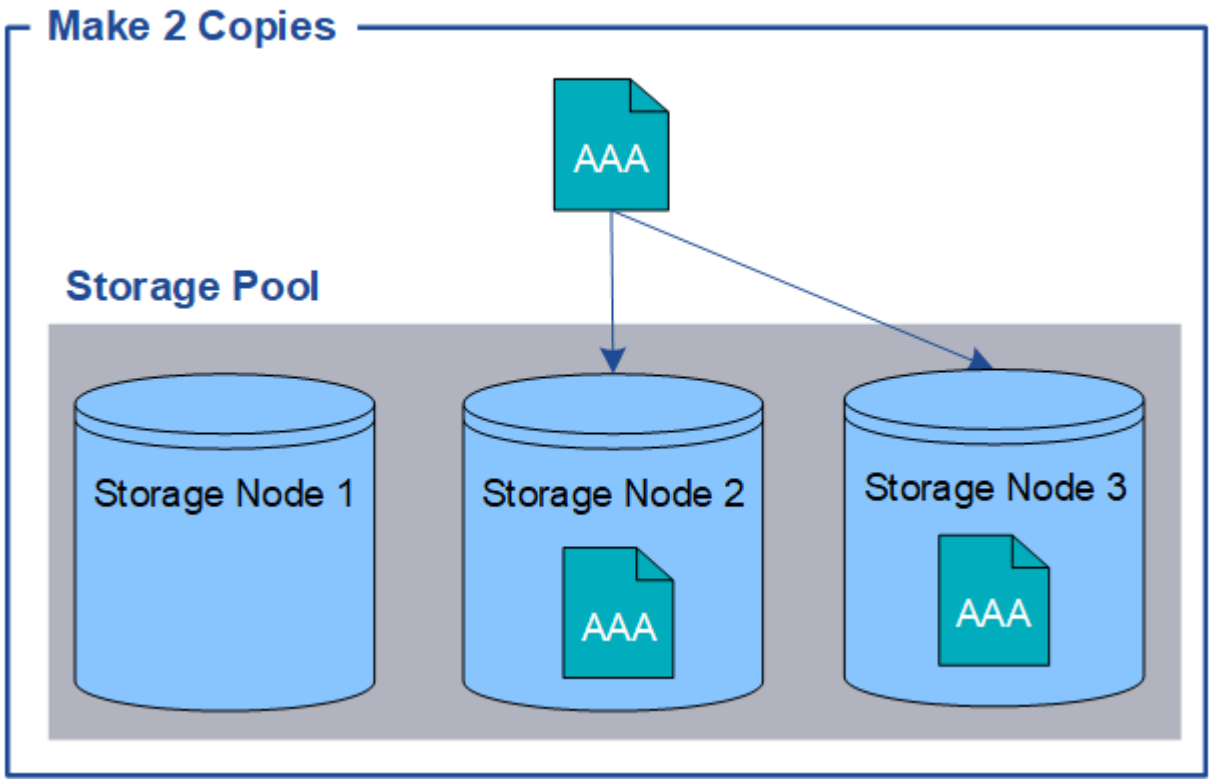
Das StorageGRID System bietet zwei Mechanismen zum Schutz von Objektdaten vor Verlust: Replizierung und Erasure Coding.

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.

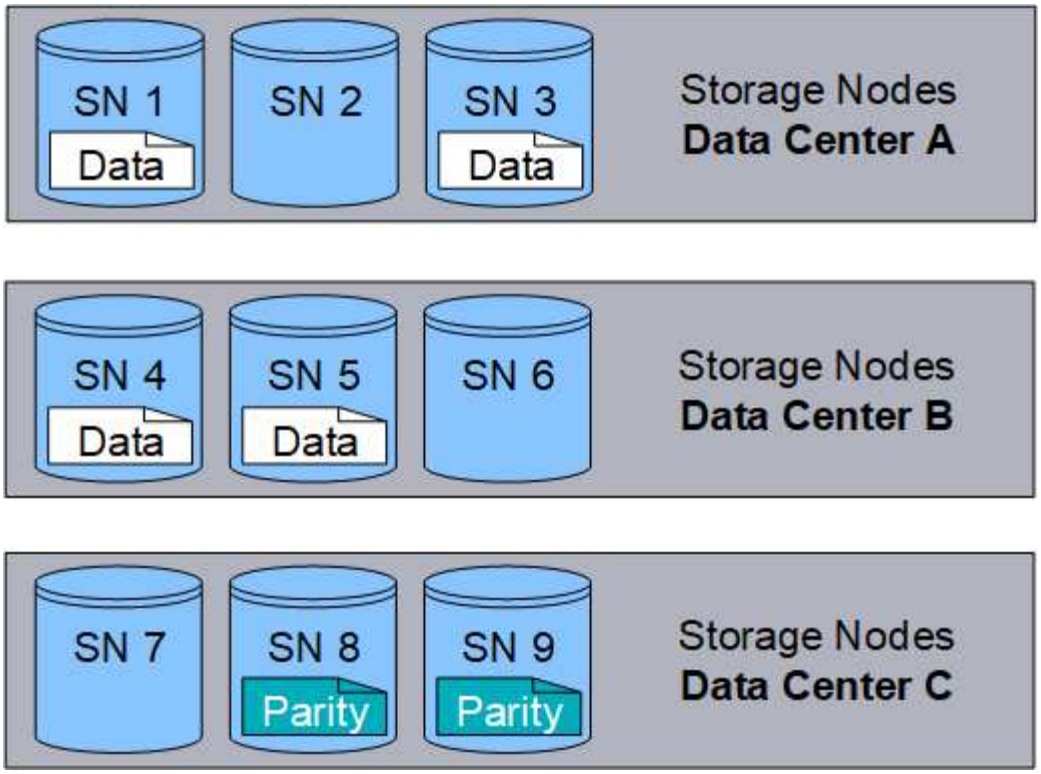
Im folgenden Beispiel gibt die Regel „2 Kopien erstellen“ an, dass zwei replizierte Kopien jedes Objekts in einem Speicherpool platziert werden, der drei Storage-Nodes enthält.



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-Profile 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"

"Mit 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"

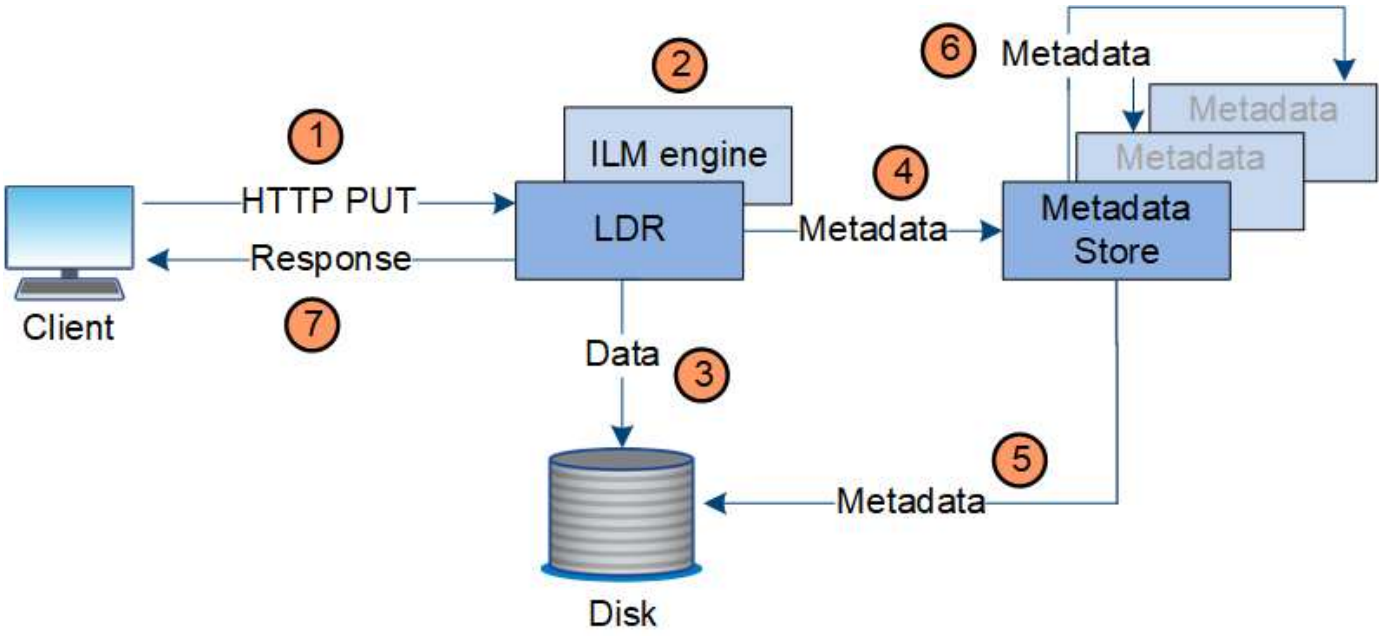
"Mit Information Lifecycle Management"

Datenfluss aufnehmen

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

Datenfluss

Wenn ein Client ein Objekt im StorageGRID-System speichert, 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 Metadatenspeicher.
5. Der Metadaten-Speicher speichert die Objekt-Metadaten auf der Festplatte.
6. Der Metadatenspeicher 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.

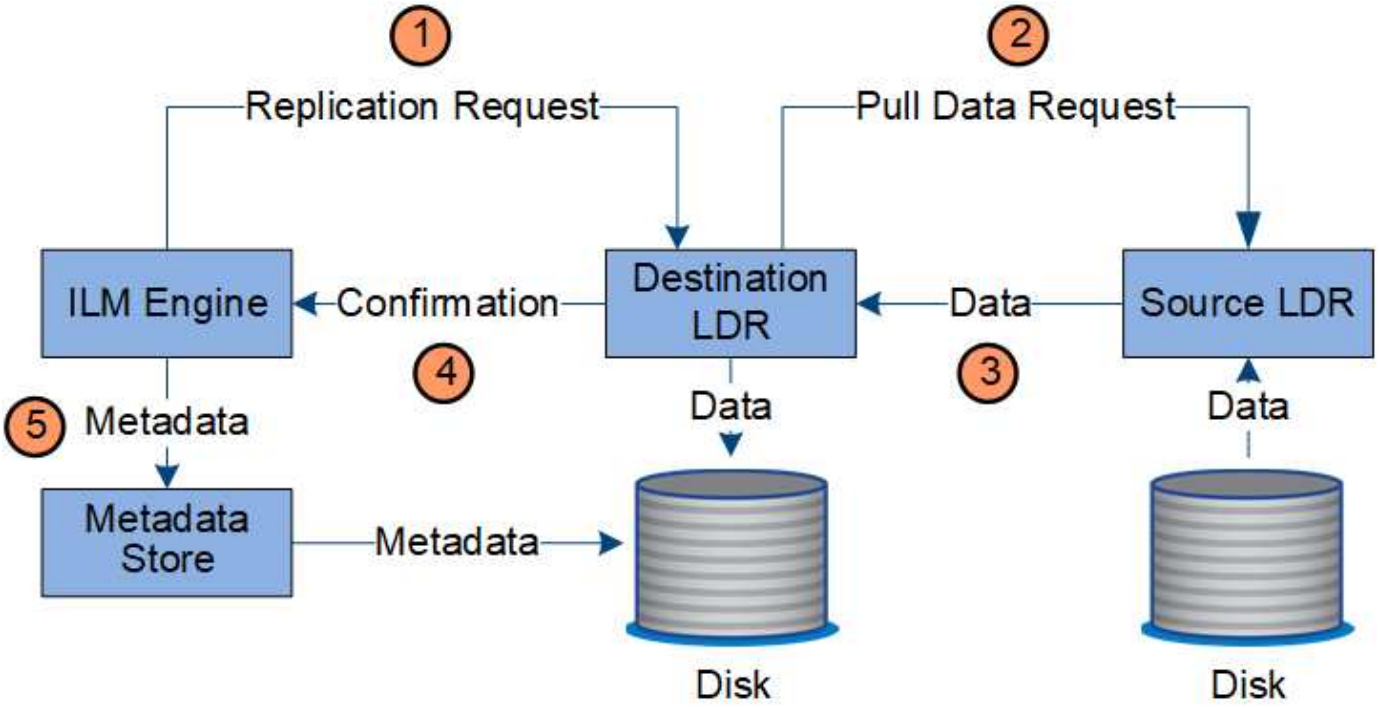
Objektdaten werden vom LDR-Service gemanagt.

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.

Datenfluss

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.



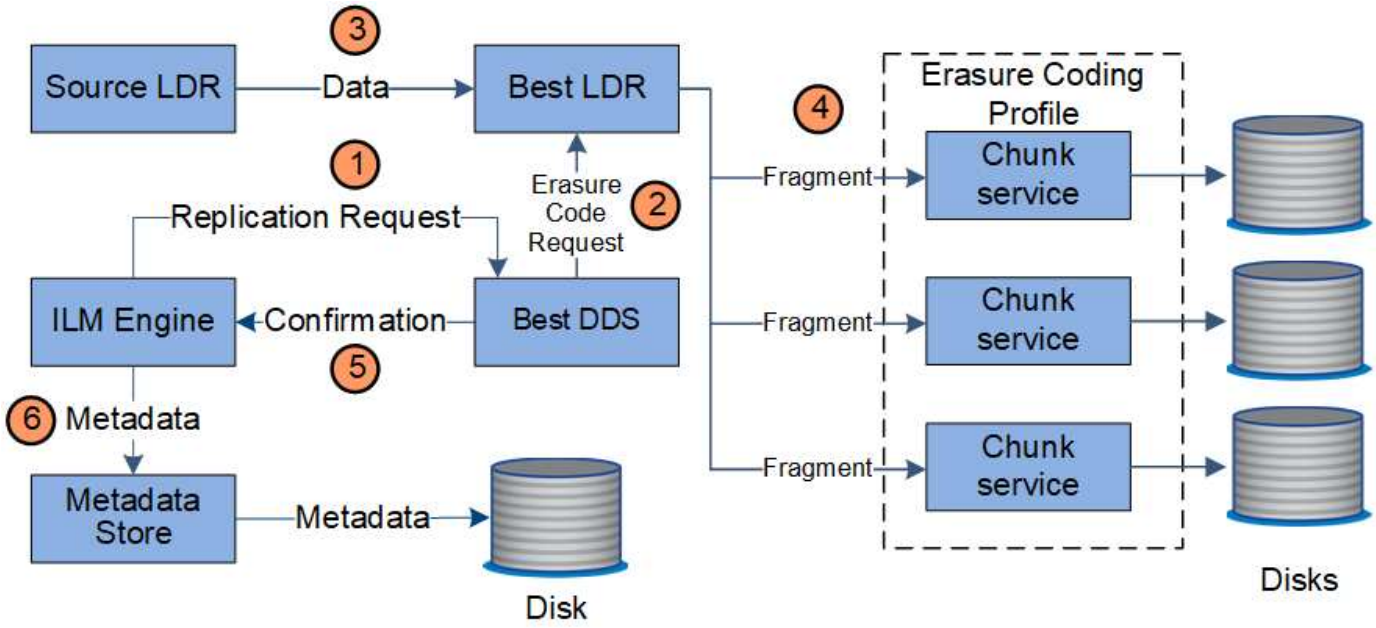
1. Die ILM-Engine fragt den ADC-Service ab, um den besten Ziel-LDR-Service innerhalb des durch die ILM-Regel festgelegten Storage-Pools zu ermitteln. Er sendet dann diesen LDR-Service einen Befehl, um die Replikation zu initiieren.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellspeicherort 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 Metadatenspeicher mit Objektspeichermetadaten.

Content Protection: Erasure Coding

Wenn eine ILM-Regel Anweisungen zur Erstellung von Erasure-codierten Kopien von Objektdaten enthält, werden Objektdaten im Rahmen des entsprechenden Erasure Coding-Schemas in Daten- und Paritätsfragmente unterteilt und diese Fragmente über die im Erasure Coding-Profil konfigurierten Storage-Nodes verteilt.

Datenfluss

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



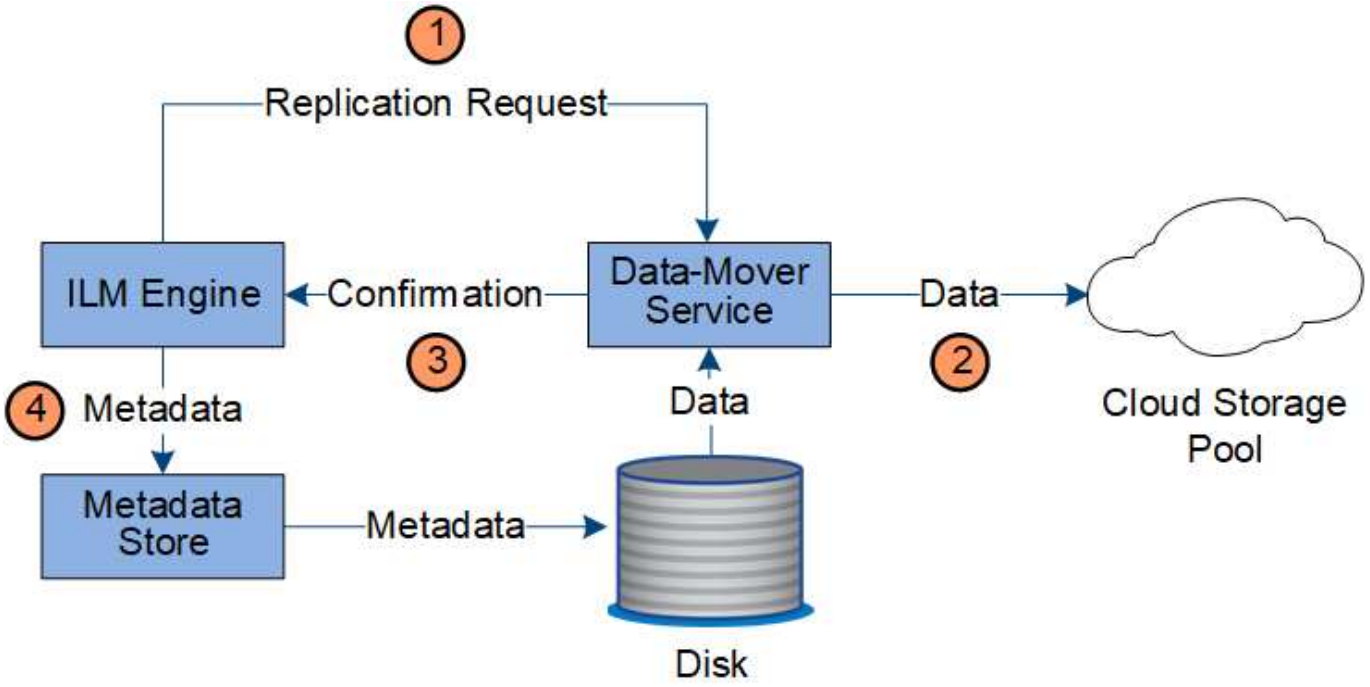
1. Die ILM-Engine fragt den ADC-Service ab, um zu bestimmen, welcher DDS-Service den Erasure Coding-Vorgang am besten ausführen kann. Sobald die ILM-Engine ermittelt wurde, sendet sie eine „Initiierung"-Anforderung an den Service.
2. Der DDS-Dienst weist ein LDR an, den Code der Objektdaten zu löschen.
3. Der Quell-LDR-Service sendet eine Kopie an den für das Erasure Coding ausgewählten LDR-Service.
4. Nach der entsprechenden Anzahl von Paritäts- und Datenfragmenten verteilt der LDR-Service diese Fragmente auf die Storage-Nodes (Chunk-Services), aus denen sich der Speicherpool des Erasure Coding-Profils besteht.
5. Der LDR-Service benachrichtigt die ILM-Engine und bestätigt, dass Objektdaten erfolgreich verteilt werden.
6. Die ILM-Engine aktualisiert den Metadatenspeicher 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 werden muss, werden Objektdaten in den externen S3-Bucket oder Azure Blob-Storage-Container verschoben, der für den Cloud Storage Pool angegeben wurde.

Datenfluss

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

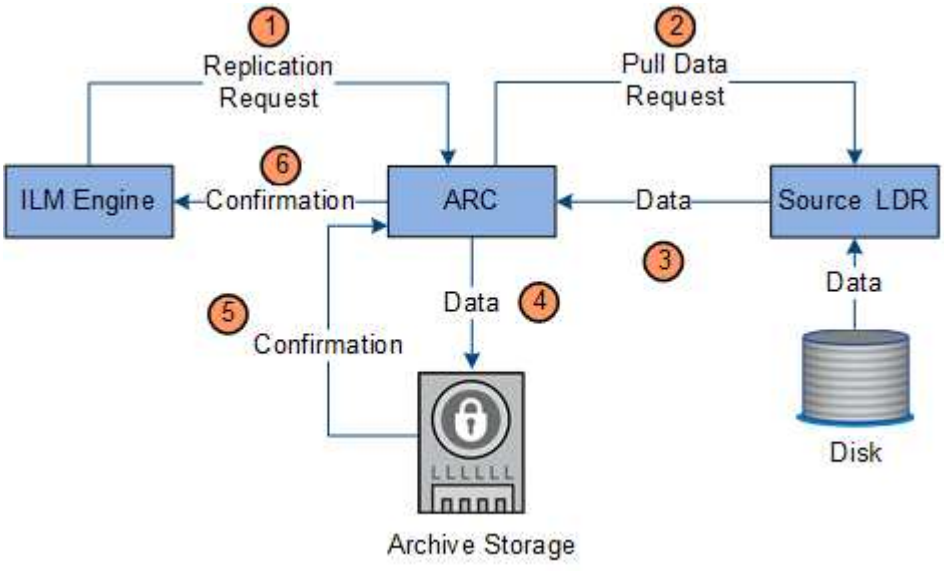


1. Die ILM-Engine wählt einen Data Mover-Service zur Replizierung in den Cloud-Storage-Pool aus.
2. Der Data Mover-Service sendet die Objektdaten an den Cloud-Speicherpool.
3. Der Data Mover-Service benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM-Engine aktualisiert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

Content-Schutz: Archivierung

Ein Archivierungsvorgang besteht aus einem definierten Datenfluss zwischen dem StorageGRID System und dem Client.

Wenn die ILM-Richtlinie erfordert, dass eine Kopie der Objektdaten archiviert wird, sendet die ILM-Engine, die eine Komponente des LDR-Service ist, eine Anforderung an den Archiv-Node, der wiederum eine Kopie der Objektdaten an das Ziel-Archiv-Storage-System sendet.



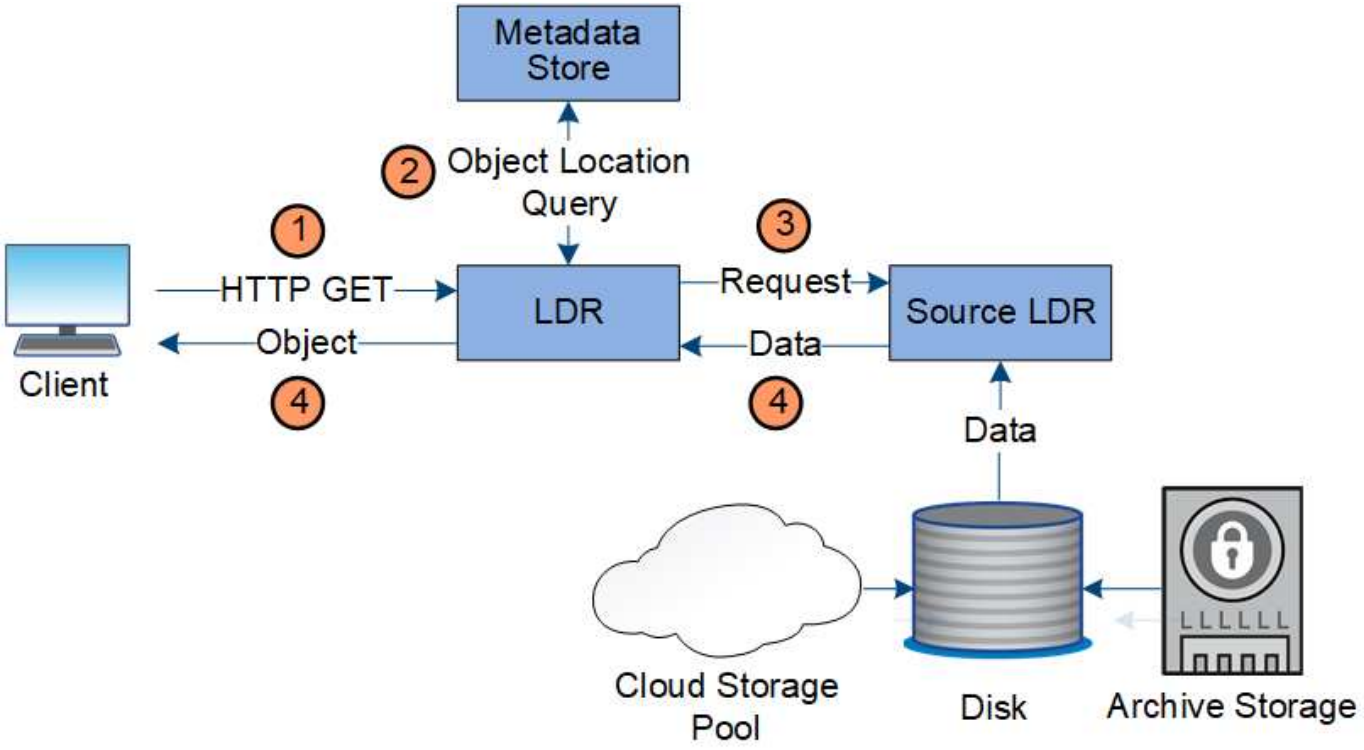
1. Die ILM-Engine sendet eine Anforderung an den ARC-Service, eine Kopie auf Archivmedien zu speichern.
2. Der ARC-Dienst fragt den ADC-Service nach dem besten Quellspeicherort ab und sendet eine Anfrage an den Quell-LDR-Dienst.
3. Der ARC-Dienst ruft Objektdaten aus dem LDR-Dienst ab.
4. Der ARC-Dienst sendet die Objektdaten an das Archivmedienziel.
5. Das Archivmedium benachrichtigt den ARC-Dienst, dass die Objektdaten gespeichert wurden.
6. Der ARC-Dienst benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.

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 Metadatenspeicher 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 Archivebene 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 Metadatenspeicher 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.

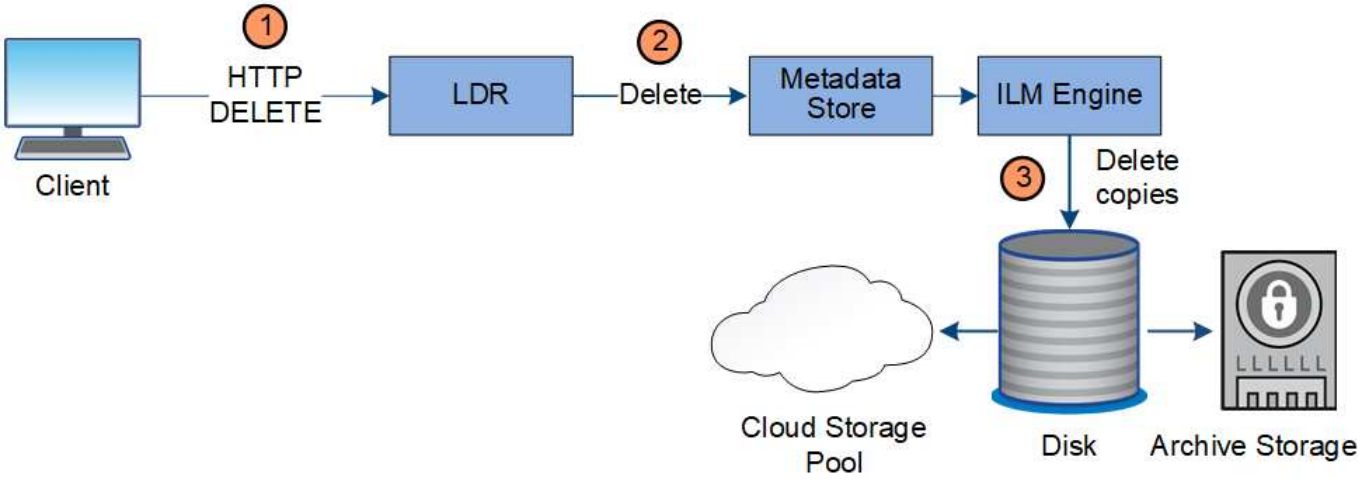
Löschhierarchie

StorageGRID bietet verschiedene Methoden zur Steuerung der Aufbewahrung oder Löschung von Objekten. Objekte können nach Client-Anforderungen 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 einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht mit irgendeiner 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.
- **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.
- **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.

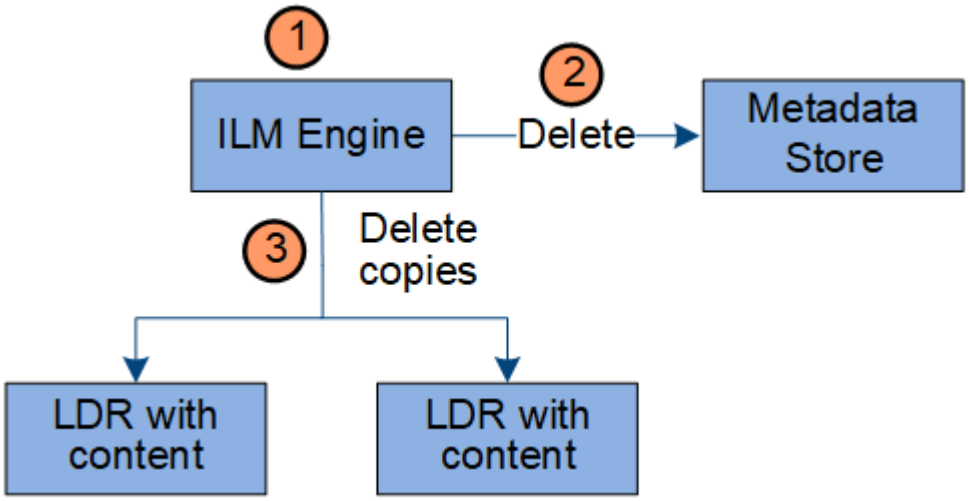
> ⓘ Die Aktion „Ablaufdatum“ in einem S3-Bucket-Lebenszyklus überschreibt immer die ILM-Einstellungen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflegen des Objekts verfallen sind.

Datenfluss für Clientlöschungen



1. Der LDR-Dienst erhält eine Löschanforderung von der Client-Anwendung.
2. Der LDR-Service aktualisiert den Metadatenspeicher, 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 Metadatenspeicher 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 Metadatenspeicher. Der Metadatenspeicher aktualisiert Objektmetadaten, sodass das Objekt auf Client-Anforderungen gelöscht aussieht.
3. Die ILM-Engine entfernt alle Kopien des Objekts. Der Metadatenspeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Wie Grid Manager zu sehen ist

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 einen unterstützten Webbrowser auf den Grid Manager zugreifen.

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

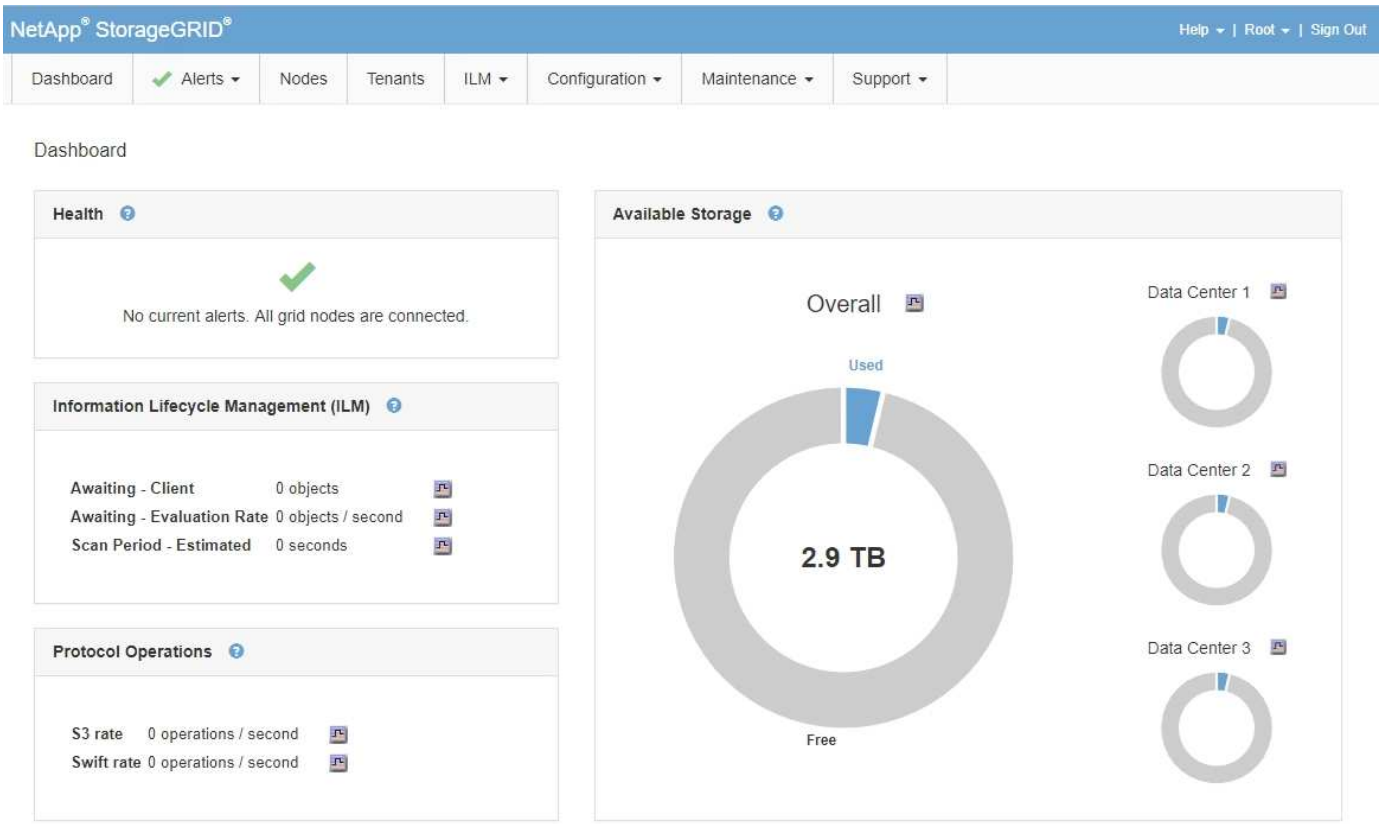
Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Grid Manager Dashboard

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

Das Dashboard bietet zusammenfassende Informationen zum Systemzustand, zur Storage-Verwendung, ILM-Prozesse sowie S3 und Swift Operationen.



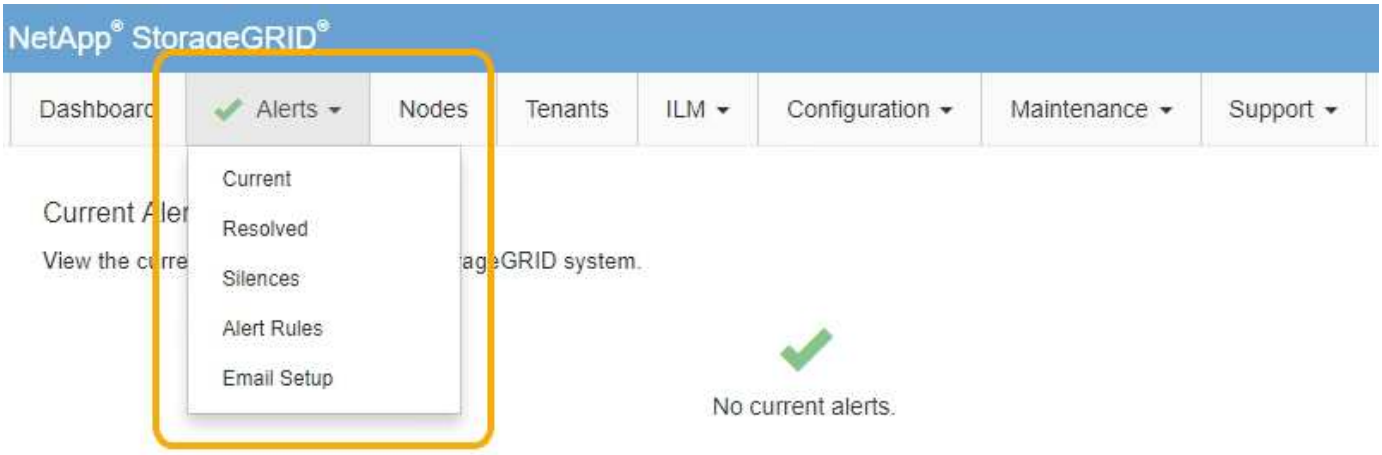
Um die Informationen in den einzelnen Bedienfelds zu erläutern, klicken Sie auf das Hilfesymbol Für dieses Panel.

Verwandte Informationen

"Monitor Fehlerbehebung"

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

Verwandte Informationen

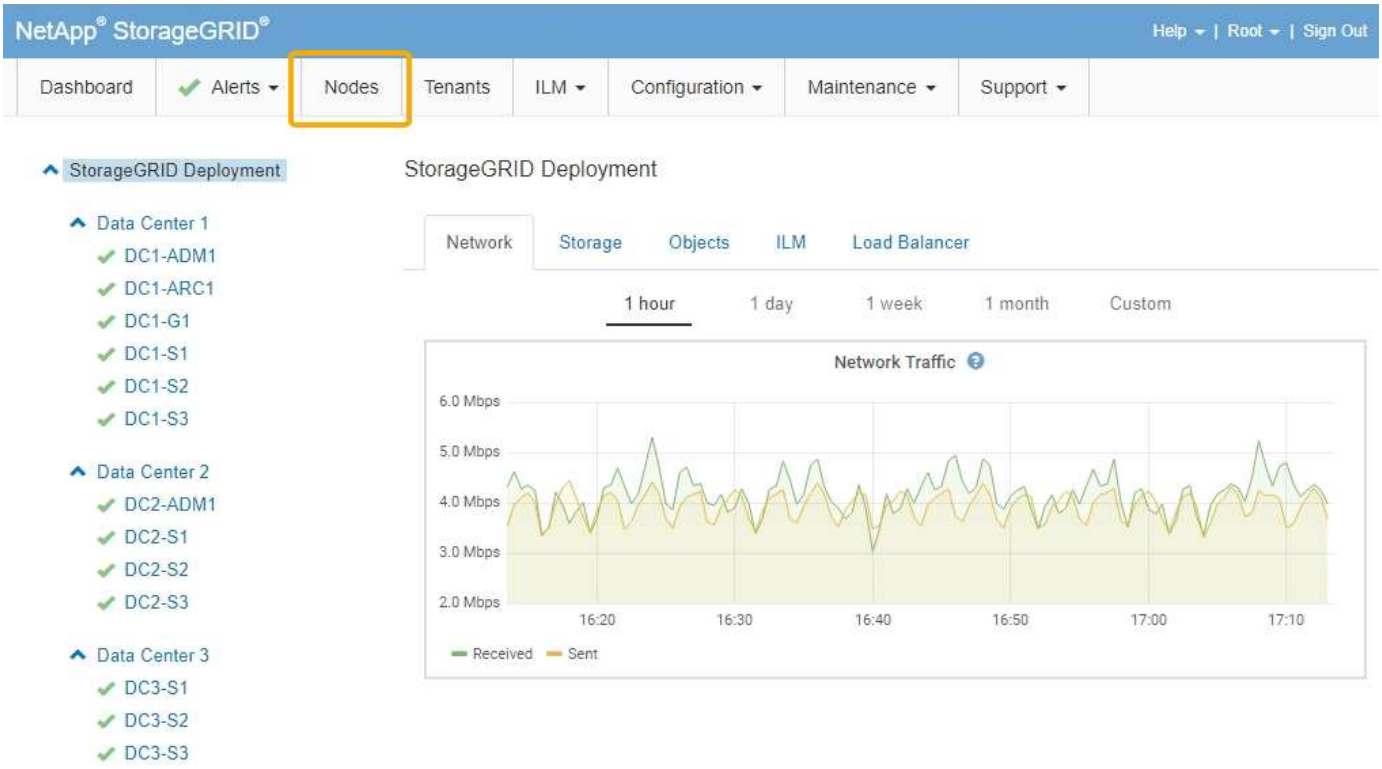
"Monitoring und Management von Warnmeldungen"

"Monitor Fehlerbehebung"

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 Knoten anzuzeigen, klicken Sie links auf den entsprechenden Link.



Verwandte Informationen

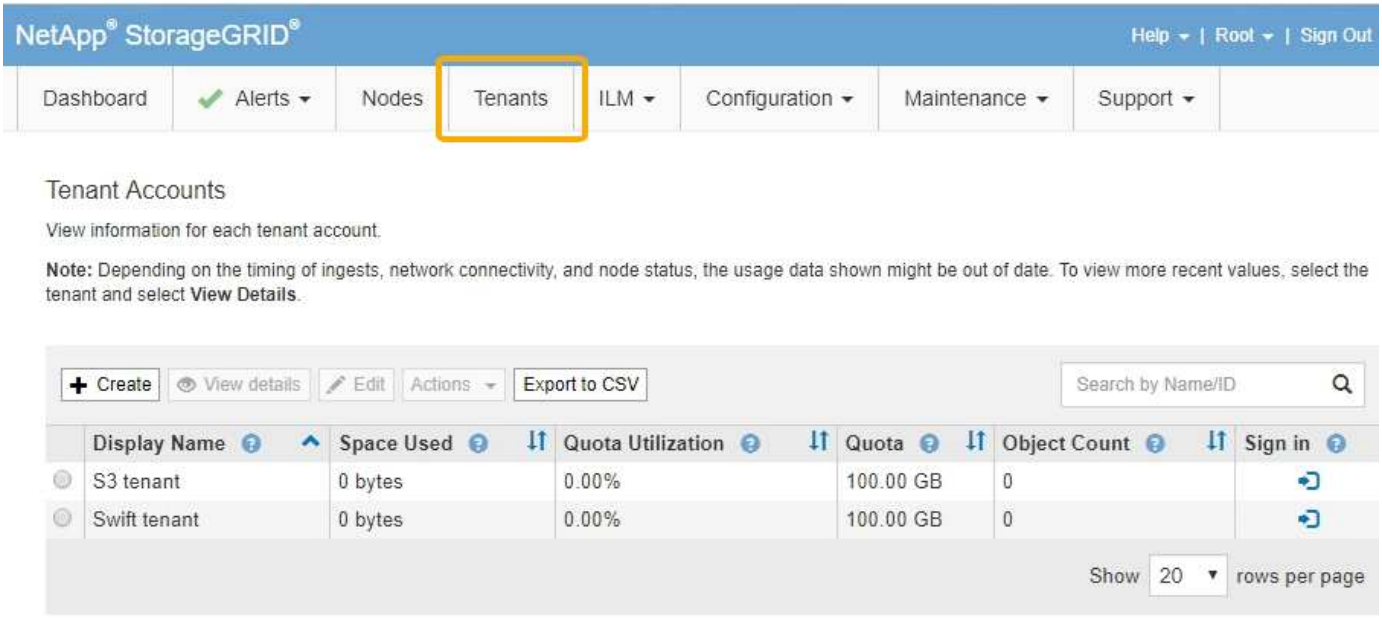
"Anzeigen der Seite Knoten"

"Monitor Fehlerbehebung"

Seite „Mandantenkonten“

Auf der Seite „Mandantenkonten“ 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 „Mandantenkonten“ bietet außerdem Einzelheiten zur Nutzung für jeden Mandanten, einschließlich der Anzahl der verwendeten Storage und der Anzahl der Objekte. Wenn Sie beim Erstellen des Mandanten eine Quote festlegen, sehen Sie, wie viel von dieser Quote verwendet wurde.



Verwandte Informationen

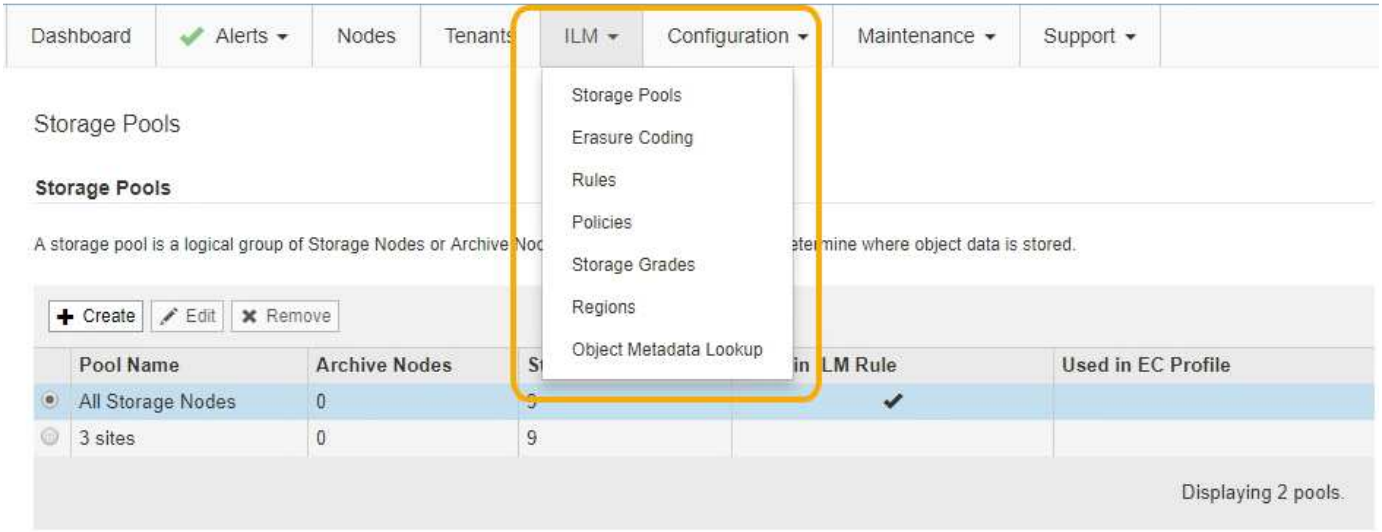
"Management von Mandanten und Client-Verbindungen"

"StorageGRID verwalten"

"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.



Verwandte Informationen

"Mit Information Lifecycle Management"

"Objektmanagement mit ILM"

Konfigurationsmenü

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

Verwandte Informationen

"Netzwerkeinstellungen werden konfiguriert"

"Management von Mandanten und Client-Verbindungen"

"Überprüfen von Audit-Meldungen"

"Kontrolle des StorageGRID-Zugriffs"

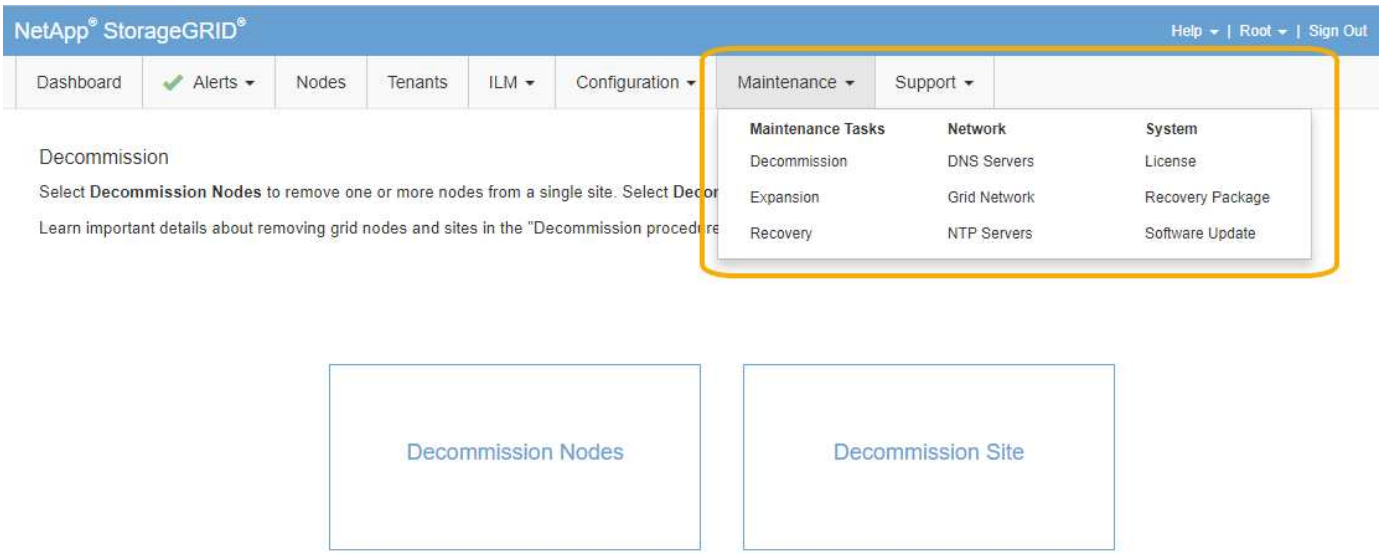
"StorageGRID verwalten"

"Monitor Fehlerbehebung"

"Prüfung von Audit-Protokollen"

Menü Wartung

Im Menü Wartung können Sie Wartungsarbeiten, Netzwerkaufgaben und Systemaufgaben durchführen.



Wartungsaufgaben

Zu den Wartungsarbeiten gehören:

- Deaktivierung von Vorgängen zur Entfernung nicht verwendeter Grid Nodes und Standorte
- Erweiterungsvorgänge ermöglichen das Hinzufügen neuer Grid-Nodes und -Standorte.
- Recovery-Vorgänge zum Austausch eines ausgefallenen Nodes und zur Wiederherstellung von Daten.

Netzwerk

Im Menü Wartung können Sie folgende Netzwerkaufgaben ausführen:

- Bearbeiten von Informationen zu DNS-Servern
- Konfigurieren der Subnetze, die im Grid-Netzwerk verwendet werden.
- Bearbeiten von Informationen zu NTP-Servern

System

Im Menü Wartung können Sie folgende Systemaufgaben ausführen:

- Überprüfen der Details für die aktuelle StorageGRID-Lizenz oder Hochladen einer neuen Lizenz.
- Erstellen eines Wiederherstellungspakets.
- Durchführung von StorageGRID Software-Updates, einschließlich Software-Upgrades, Hotfixes und Updates für die SANtricity OS Software auf ausgewählten Appliances.

Verwandte Informationen

"Durchführung von Wartungsverfahren"

"Herunterladen des Wiederherstellungspakets"

"Erweitern Sie Ihr Raster"

"Software-Upgrade"

"Verwalten Sie erholen"

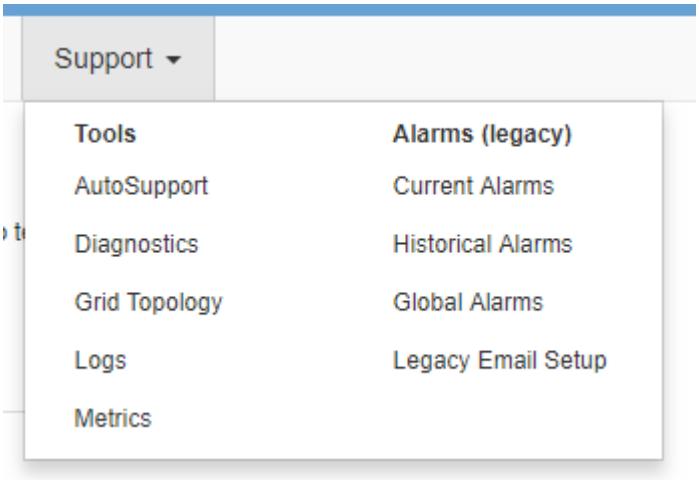
"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Menü „Support“

Das Menü Support enthält Optionen, die dem technischen Support bei der Analyse und Fehlerbehebung Ihres Systems helfen. Das Menü „Support“ enthält zwei Teile: Werkzeuge und Alarme (alt).



Tools

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

- Aktivieren Sie AutoSupport.
- Führen Sie eine Reihe von diagnostischen Prüfungen zum aktuellen Status des Rasters durch.
- Greifen Sie auf die Struktur der Grid Topology zu, um detaillierte Informationen zu Grid-Nodes, Services und Attributen anzuzeigen.
- Abrufen von Protokolldateien und Systemdaten
- Detaillierte Metriken und Diagramme prüfen

> 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 (alt)“ des Menüs „Support“ können Sie aktuelle, historische und globale Alarme überprüfen und E-Mail-Benachrichtigungen für ältere Alarme und AutoSupport einrichten.

Verwandte Informationen

"StorageGRID Architektur und Netzwerktopologie"

"StorageGRID Attribute"

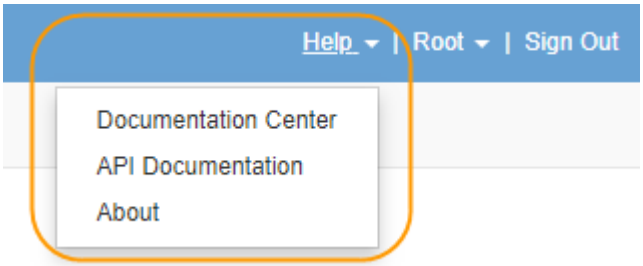
"Verwenden von StorageGRID Support-Optionen"

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

Hilfe-Menü

Die Hilfsoption bietet Zugriff auf das StorageGRID Documentation Center für die aktuelle Version und die API-Dokumentation. Sie bestimmen auch, welche Version von StorageGRID derzeit installiert ist.



Verwandte Informationen

"StorageGRID verwalten"

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.

Verwandte Informationen

"Wie Grid Manager zu sehen ist"

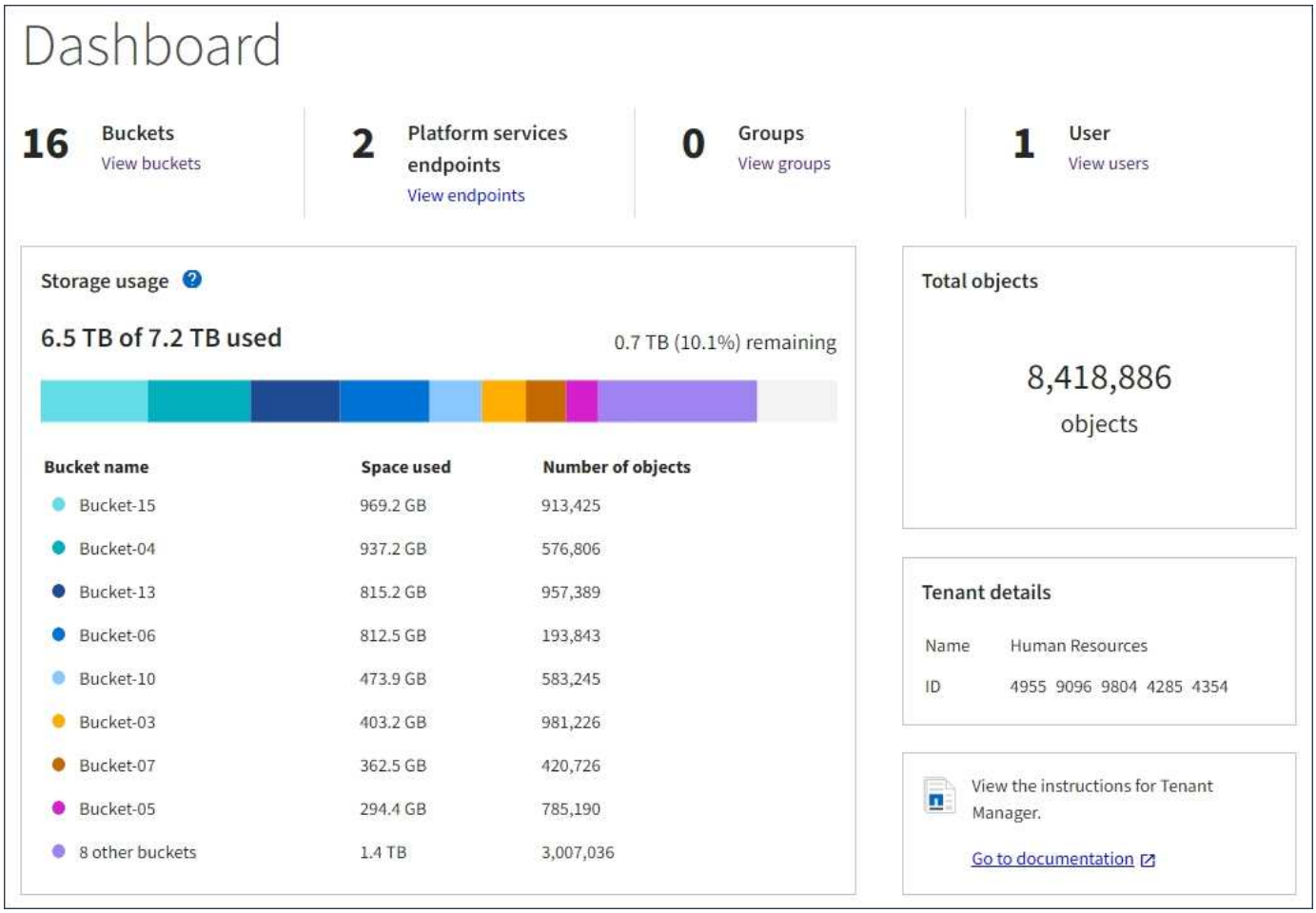
"Verwenden Sie ein Mandantenkonto"

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.

Mit dem Mandanten-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.



Storage-Menü (nur S3-Mandanten)

Das Menü Storage wird nur für S3-Mandantenkonten angezeigt. Über dieses Menü können S3-Benutzer Zugriffsschlüssel managen, Buckets erstellen und löschen und Plattform-Service-Endpunkte managen.

Meine Zugriffsschlüssel

S3-Mandantenbenutzer können die Zugriffschlüssel wie folgt managen:

- Benutzer mit der Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten 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 die folgenden Aufgaben für Buckets 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
- Konfiguration der Cross-Origin Resource Sharing (CORS)
- Aktivieren und deaktivieren Sie Einstellungen für das Update der letzten Zugriffszeit für die Buckets, die zum Mandanten gehören
- Leere Buckets löschen

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:

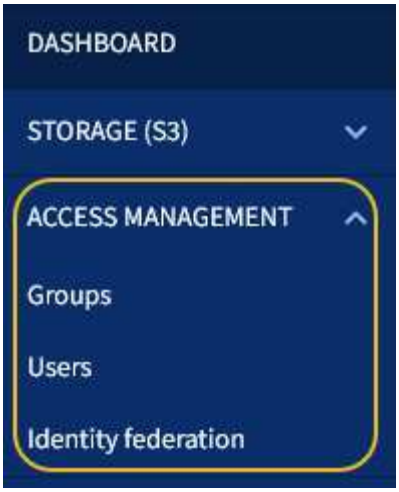
- Konfigurieren Sie S3-Ereignisbenachrichtigungen, die an einen Ziel-Service gesendet werden können, der den AWS Simple Notification Service™ (SNS) unterstützt.
- Konfigurieren Sie die CloudMirror-Replizierung, mit der Mandanten Objekte automatisch in einen externen S3-Bucket replizieren können.
- Die 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 Plattform-Services für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit der Berechtigung Endpunkte managen einen Zielendpunkt für jeden Plattform-Service konfigurieren.

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.



Verwenden von StorageGRID

Nach der Installation der Grid-Nodes und StorageGRID-Netzwerke können Sie mit der Konfiguration und Verwendung von StorageGRID beginnen. Zu den Aufgaben, die Sie durchführen werden, gehören die Kontrolle des Benutzerzugriffs auf Systemverwaltungsfunktionen, die Einrichtung von Mandantenkonten, das Verwalten von Client-Verbindungen, das Festlegen von Konfigurationsoptionen, das Managen von Objektstandorten mit ILM, die Überwachung des Systemzustands und der täglichen Aktivitäten des StorageGRID-Systems sowie die Durchführung von routinemäßigen und nicht-routinemäßigen Wartungsaktivitäten.

- "Kontrolle des StorageGRID-Zugriffs"
- "Management von Mandanten und Client-Verbindungen"
- "Netzwerkeinstellungen werden konfiguriert"
- "Systemeinstellungen werden konfiguriert"
- "Mit Information Lifecycle Management"
- "Monitoring der StorageGRID Vorgänge"
- "Durchführung von Wartungsverfahren"
- "Verwenden von StorageGRID Support-Optionen"

Kontrolle des StorageGRID-Zugriffs

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.

Steuern des Zugriffs auf den Grid Manager

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.

Durch die Verwendung von Identity Federation lassen sich Gruppen und Benutzer schneller einrichten, und Benutzer können sich mithilfe vertrauter Anmeldedaten 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 ausführen kann, indem Sie jeder Gruppe unterschiedliche Berechtigungen zuweisen. 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 vornehmen oder Vorgänge im Grid Manager oder der Grid Management API ausführen.

Aktivieren 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. Wenn SSO aktiviert ist, müssen alle Benutzer von einem externen Identitäts-Provider authentifiziert werden, bevor sie auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

Wenn SSO aktiviert ist und Benutzer sich bei StorageGRID anmelden, werden sie zur SSO-Seite Ihres Unternehmens weitergeleitet, um ihre Anmeldedaten zu validieren. Wenn sich Benutzer von einem Admin-Node abmelden, werden sie automatisch von allen Admin-Nodes abgemeldet.

Clientzertifikate werden verwendet

Sie können Clientzertifikate verwenden, um autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank zu ermöglichen. Clientzertifikate bieten eine sichere Möglichkeit zur Verwendung externer Tools zur Überwachung von StorageGRID. Sie können Ihr eigenes Clientzertifikat bereitstellen oder mit dem Grid Manager ein Zertifikat erstellen.

Grid-Passwörter werden geändert

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. Sie können diese Passphrase nach Bedarf ändern.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

Management von Mandanten und Client-Verbindungen

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift Clients zum Speichern und Abrufen von Objekten verwenden, und managen die Konfigurationsoptionen, die steuern, wie Clients sich mit Ihrem StorageGRID System

verbinden.

Mandantenkonten

Ein Mandantenkonto ermöglicht es Ihnen, festzulegen, wer mit Ihrem StorageGRID System Objekte speichern und abrufen kann und welche Funktionen ihnen zur Verfügung stehen. Mandantenkonten ermöglichen Client-Applikationen, die die S3-REST-API oder die Swift-REST-API unterstützen, um Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verwendet entweder das S3-Client-Protokoll oder das Swift-Client-Protokoll.

Sie müssen für jedes Client-Protokoll mindestens ein Mandantenkonto erstellen, das zum Speichern von Objekten auf Ihrem StorageGRID System verwendet wird. Optional können Sie zusätzliche Mandantenkonten erstellen, wenn Sie die auf Ihrem System gespeicherten Objekte durch verschiedene Einheiten trennen möchten. Jedes Mandantenkonto verfügt über eigene föderierte bzw. lokale Gruppen und Benutzer sowie eigene Buckets (Container für Swift) und Objekte.

Sie können mithilfe des Grid Manager oder der Grid-Management-API Mandantenkonten erstellen. Beim Erstellen eines Mandantenkontos geben Sie die folgenden Informationen an:

- Anzeigename für den Mandanten (die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden).
- Gibt an, ob das Mandantenkonto das S3 oder Swift verwenden wird
- Bei S3-Mandantenkonten: Unabhängig davon, ob das Mandantenkonto Plattform-Services nutzen darf. Wenn die Nutzung von Plattformdiensten zulässig ist, muss das Grid so konfiguriert werden, dass es seine Verwendung unterstützt.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte verfügbar sind. Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.
- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.
- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Wenn S3-Mandantenkonten die gesetzlichen Anforderungen erfüllen müssen, können Grid-Administratoren die globale S3-Objektsperreneinstellung für das StorageGRID System aktivieren. Wenn S3 Object Lock für das System aktiviert ist, können alle S3-Mandantenkonten Buckets erstellen, wobei S3 Object Lock aktiviert ist. Anschließend können für die Objektversionen in diesem Bucket die Einstellungen für Aufbewahrung und Aufbewahrung nach rechts angegeben werden.

Nach dem Erstellen eines Mandantenkontos können sich Mandantenbenutzer bei Tenant Manager anmelden.

Client-Verbindungen zu StorageGRID-Nodes

Bevor Mandantenbenutzer S3 oder Swift Clients verwenden können, um Daten in StorageGRID zu speichern und abzurufen, müssen Sie entscheiden, wie diese Clients eine Verbindung zu StorageGRID Nodes herstellen.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes. Dies ist die empfohlene Verbindung.
- Der CLB-Service auf Gateway-Knoten.

Der CLB-Service ist veraltet.

- Storage-Nodes mit oder ohne externen Load Balancer.

Bei der Konfiguration von StorageGRID, damit Clients den Lastverteilungsservice verwenden können, führen Sie die folgenden Schritte aus:

1. Konfigurieren von Endpunkten für den Load Balancer Service. Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage-Nodes. Beim Erstellen eines Load Balancer-Endpunkts geben Sie eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das Zertifikat, das für HTTPS-Verbindungen verwendet werden soll (falls zutreffend).
2. Geben Sie optional an, dass das Client-Netzwerk eines Node nicht vertrauenswürdig ist, um sicherzustellen, dass alle Verbindungen zum Client-Netzwerk des Nodes auf den Load Balancer-Endpunkten ausgeführt werden.
3. Konfiguration von Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) Wenn Sie eine HA-Gruppe erstellen, werden die Schnittstellen mehrerer Admin-Nodes und Gateway-Nodes in einer aktiv-Backup-Konfiguration platziert. Client-Verbindungen werden mithilfe der virtuellen IP-Adresse der HA-Gruppe hergestellt.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"S3 verwenden"

"Verwenden Sie Swift"

"Entdecken Sie den Tenant Manager"

"Netzwerkeinstellungen werden konfiguriert"

Netzwerkeinstellungen werden konfiguriert

Sie können verschiedene Netzwerkeinstellungen vom Grid Manager konfigurieren, um den Betrieb Ihres StorageGRID Systems zu optimieren.

Domain-Namen

Falls Sie beabsichtigen, virtuelle S3-Hosted-Style-Anforderungen zu unterstützen, müssen Sie die Liste der Endpunkt-Domain-Namen, mit denen S3-Clients verbunden werden, konfigurieren. Beispiele hierfür sind s3.example.com, s3.example.co.uk und s3-east.example.com.

Die konfigurierten Serverzertifikate müssen mit den Domänennamen des Endpunkts übereinstimmen.

Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen verwenden virtuelle IP-Adressen (VIPs), um aktiv-Backup-Zugriff auf Gateway Node- oder Admin-Node-Services bereitzustellen. Eine HA-Gruppe besteht aus mindestens einer Netzwerkschnittstellen an Admin-Nodes und Gateway-Nodes. Beim Erstellen einer HA-Gruppe wählen Sie

Netzwerkschnittstellen aus, die zum Grid Network (eth0) oder dem Client-Netzwerk (eth2) gehören.

Das Admin-Netzwerk unterstützt keine HA-VIPs.

Eine HA-Gruppe behält eine oder mehrere virtuelle IP-Adressen bei, die der aktiven Schnittstelle in der Gruppe hinzugefügt werden. Wenn die aktive Schnittstelle nicht mehr verfügbar ist, werden die virtuellen IP-Adressen in eine andere Schnittstelle verschoben. Dieser 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.

Es empfiehlt sich, aus mehreren Gründen Gruppen für Hochverfügbarkeit (HA) zu verwenden.

- 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.

Verbindungskosten

Sie können die Verbindungskosten entsprechend der Latenz zwischen Standorten anpassen. Wenn zwei oder mehr Datacenter-Standorte vorhanden sind, priorisieren die Verbindungskosten, welcher Datacenter-Standort einen angeforderten Service bereitstellen soll.

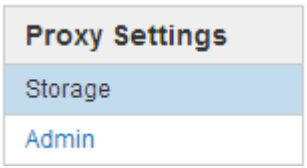
Load Balancer-Endpunkte

Mithilfe eines Load Balancer können Sie Aufnahme- und Abruf-Workloads von S3 und Swift Clients verarbeiten. Durch Verteilung der Workloads und Verbindungen auf mehrere Storage-Nodes maximiert der Lastausgleich die Geschwindigkeit und die Kapazität der Verbindungen.

Wenn Sie den StorageGRID-Load-Balancer-Dienst verwenden möchten, der in Admin-Nodes und Gateway-Nodes enthalten ist, müssen Sie einen oder mehrere Load-Balancer-Endpunkte konfigurieren. Jeder Endpunkt definiert einen Gateway-Node- oder Admin-Node-Port für S3- und Swift-Anforderungen zu Storage-Nodes.

Proxy-Einstellungen

Wenn Sie S3-Plattform-Services oder Cloud Storage-Pools verwenden, können Sie einen nicht transparenten Proxy-Server zwischen Storage Nodes und den externen S3-Endpunkten konfigurieren. Wenn Sie AutoSupport-Meldungen über HTTPS oder HTTP senden, können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und dem technischen Support konfigurieren.



Serverzertifikate

Sie können zwei Arten von Serverzertifikaten hochladen:

- Management Interface Server Certificate – dies ist das Zertifikat, das für den Zugriff auf die Managementoberfläche verwendet wird.

- Objekt-Storage-API-Service-Endpunktserverzertifikat, das die S3- und Swift-Endpunkte für direkte Verbindungen zu Storage-Nodes oder bei Verwendung des CLB-Dienstes auf einem Gateway-Node sichert.

  Der CLB-Service ist veraltet.

Die Load Balancer-Zertifikate werden auf der Seite Load Balancer Endpoints konfiguriert. Die KMS-Zertifikate (Key Management Server) werden auf der Seite Key Management Server konfiguriert.

Richtlinien für die Verkehrsklassifizierung

Mithilfe von Richtlinien für die Traffic-Klassifizierung können Sie Regeln zur Identifizierung und Handhabung verschiedener Arten von Netzwerk-Traffic erstellen, einschließlich Traffic im Zusammenhang mit bestimmten Buckets, Mandanten, Client-Subnetzen oder Endpunkten für den Load Balancer. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Nicht Vertrauenswürdige Client-Netzwerke

Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten nicht vertrauenswürdig ist. Wenn das Client-Netzwerk eines Node nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

Beispielsweise könnte ein Gateway-Node den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anforderungen ablehnen. Sie können auch den Datenverkehr des Outbound-S3-Plattformdienstes von einem Speicherknoten aktivieren, während eingehende Verbindungen zu diesem Speicherknoten im Client-Netzwerk verhindert werden.

Verwandte Informationen

"StorageGRID verwalten"

"Management von Mandanten und Client-Verbindungen"

Systemeinstellungen werden konfiguriert

Sie können verschiedene Systemeinstellungen über den Grid Manager konfigurieren, um den Betrieb Ihres StorageGRID Systems zu optimieren.

Anzeigeoptionen

Mit den Anzeigeoptionen können Sie den Zeitraum für das Timeout für Benutzersitzungen festlegen und E-Mail-Benachrichtigungen für ältere Alarme und AutoSupport-Meldungen mit Ereignisauslösung unterdrücken.

Grid-Optionen

Mit den Grid-Optionen können Sie die Einstellungen für alle Objekte konfigurieren, die in Ihrem StorageGRID-System gespeichert sind, einschließlich gespeicherter Objektkomprimierung und gespeicherter Objektverschlüsselung. Und gespeichertes Objekt-Hashing.

Mit diesen Optionen können Sie auch globale Einstellungen für S3- und Swift-Client-Vorgänge festlegen.

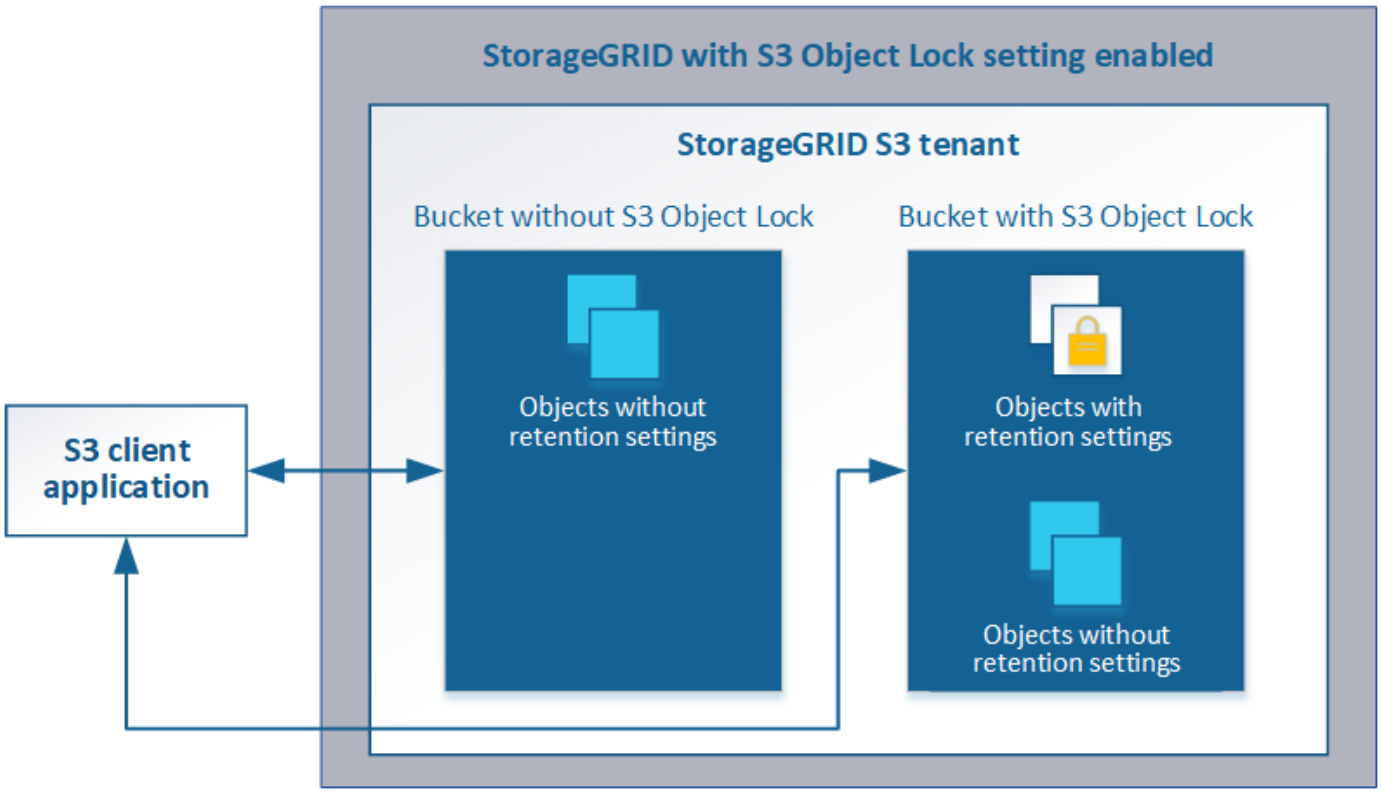
Für Schlüsselmanagement-Server

Ein oder mehrere externe Verschlüsselungsmanagement-Server (KMS) lassen sich konfigurieren, um StorageGRID Services und Storage Appliances Verschlüsselungen bereitzustellen. Jeder KMS- oder KMS-Cluster verwendet das KMIP (Key Management Interoperability Protocol), um einen Verschlüsselungsschlüssel für die Appliance-Nodes am zugehörigen StorageGRID-Standort bereitzustellen. Mithilfe von Verschlüsselungsmanagement-Servern können Sie StorageGRID-Daten schützen, selbst wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt sind, können Sie erst auf sämtliche 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.

S3-Objektsperre

Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht. Sie können die globale S3-Objektsperre für ein StorageGRID-System aktivieren, damit S3-Mandantenkonten Buckets erstellen können, wobei S3-Objektsperre aktiviert ist. Der Mandant kann dann mithilfe einer S3-Client-Applikation optional Aufbewahrungseinstellungen (Aufbewahrung bis Datum, gesetzliche Aufbewahrungspflichten oder beides) für die Objekte in diesen Buckets festlegen.



Storage-Optionen

Mithilfe von Storage-Optionen können Sie die Objektsegmentierung steuern und Storage-Wasserzeichen definieren, um den nutzbaren Storage-Speicherplatz eines Storage Node zu managen.

Mit Information Lifecycle Management

Mithilfe von Information Lifecycle Management (ILM) können Kunden die Platzierung, Dauer und Datensicherung 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.

ILM-Regeln definieren:

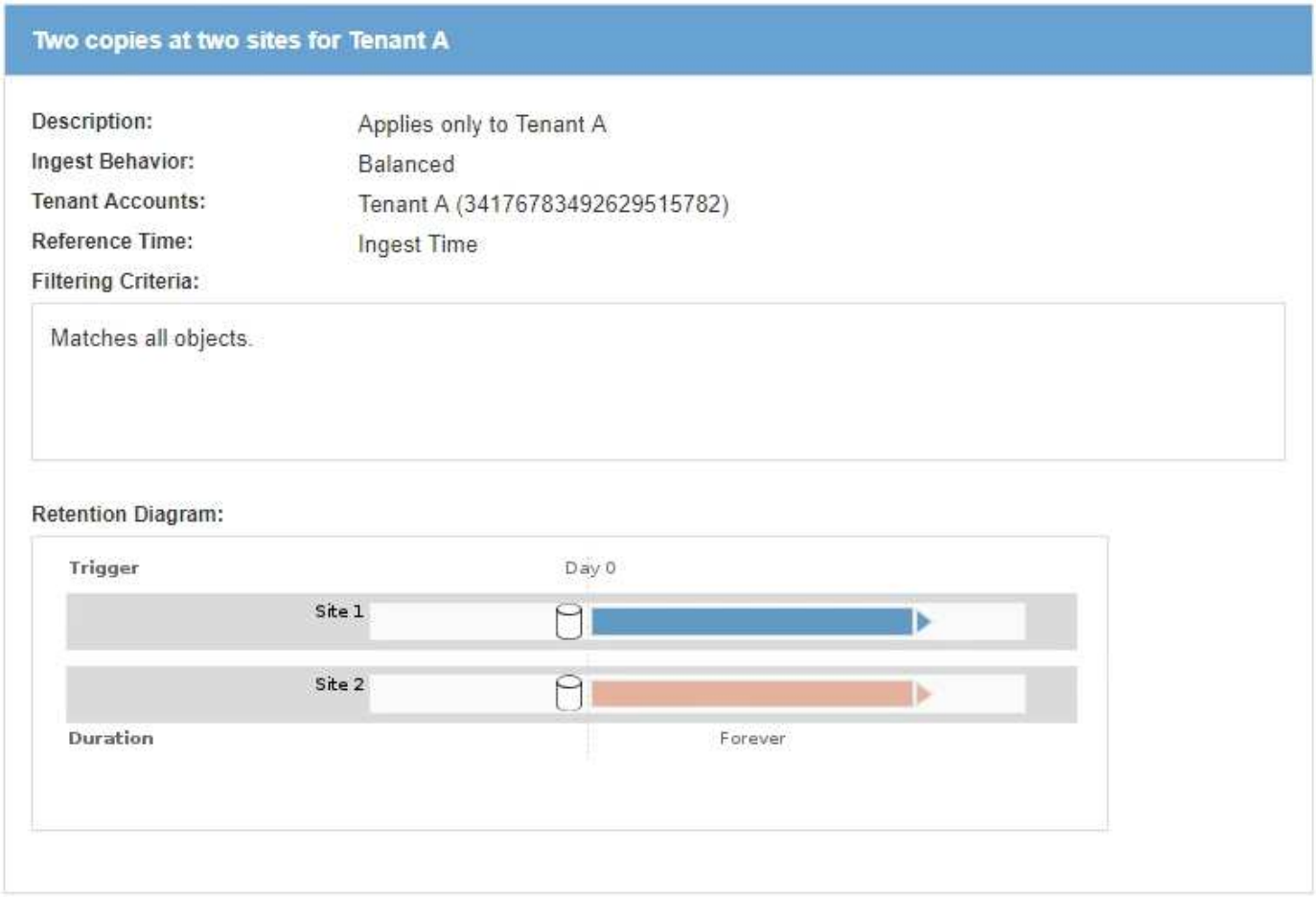
- Welche Objekte sollten gespeichert werden. Eine Regel kann auf alle Objekte angewendet werden, oder Sie können Filter angeben, um zu identifizieren, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder 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 Koprottypen 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. Die Kopien werden gleichmäßig auf alle Storage Nodes verteilt.

Beispiel für eine ILM-Regel

Diese Beispiel-ILM-Regel gilt für die Objekte, die zu Mandant A gehören Es erstellt zwei replizierte Kopien dieser Objekte und speichert jede Kopie an einem anderen Standort. Die beiden Kopien werden „`forever,`“ aufbewahrt. Das 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.

Diese Regel verwendet die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung an zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, 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

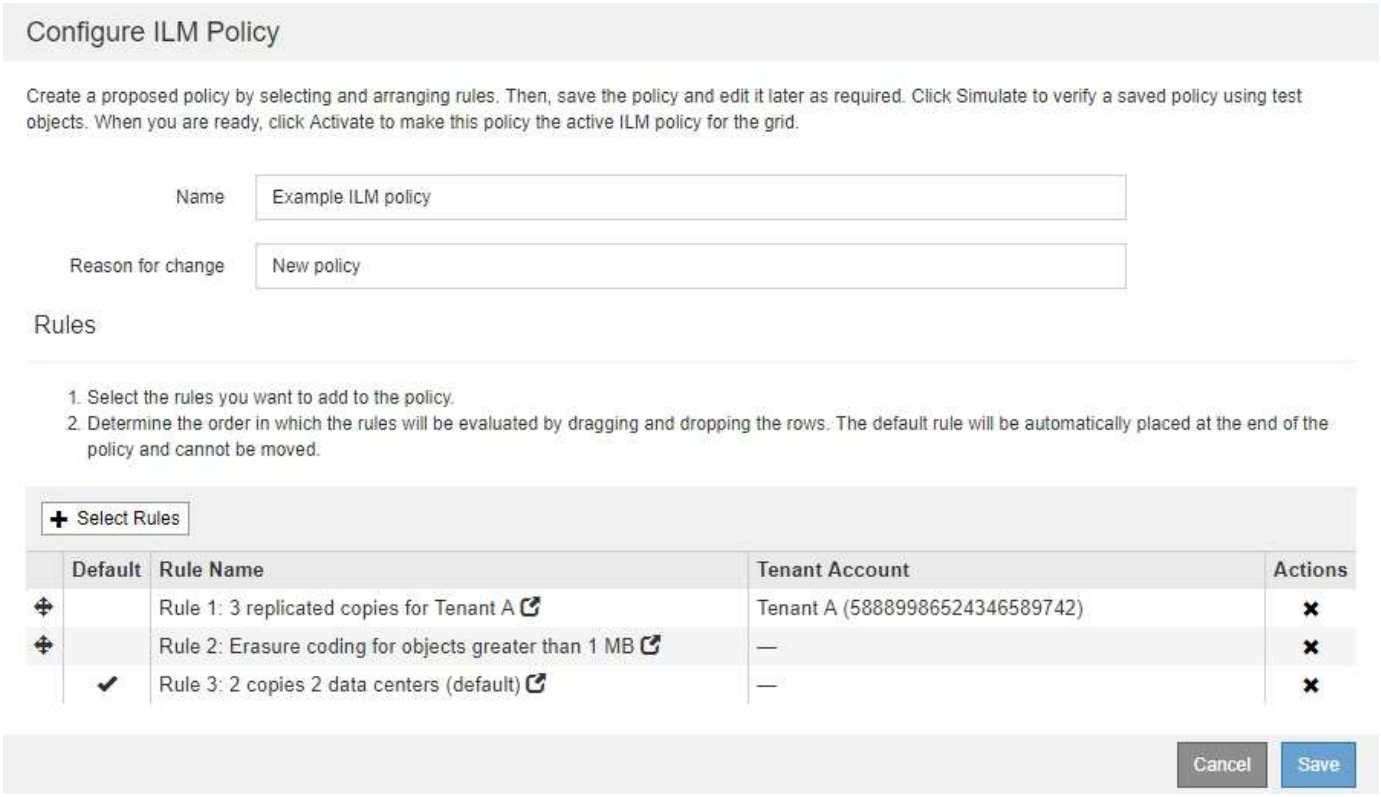
Die aktive ILM-Richtlinie für Ihr StorageGRID System steuert die Platzierung, Dauer und Datensicherung aller Objekte.

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 ausgewertet, bis eine Übereinstimmung erfolgt.
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.

Beispiel für eine ILM-Richtlinie

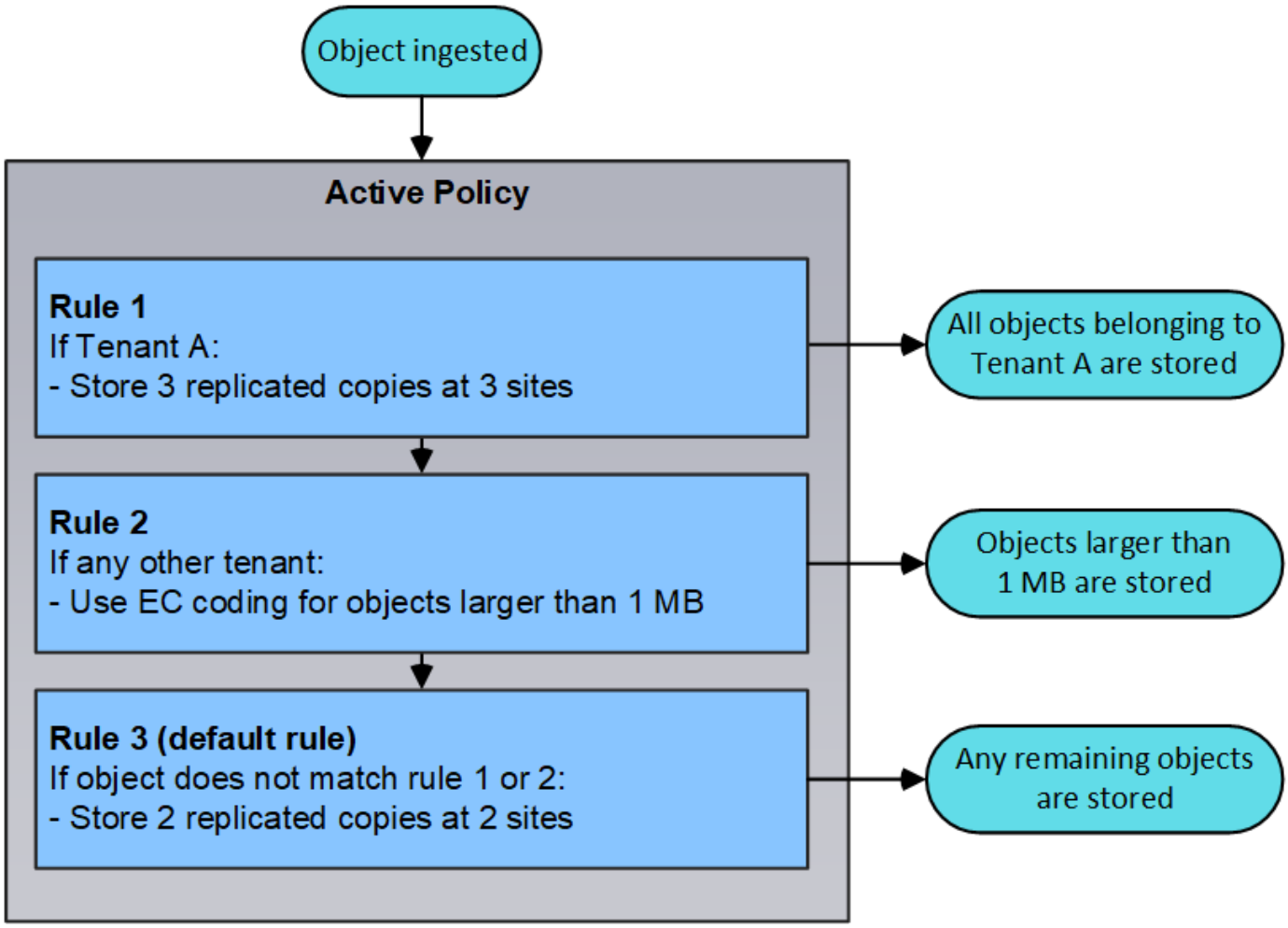
In diesem Beispiel verwendet die ILM-Richtlinie drei ILM-Regeln.



In diesem Beispiel stimmt Regel 1 mit allen Objekten überein, die zu Mandant A gehören Diese Objekte werden als drei replizierte Kopien an drei Standorten gespeichert. Objekte, die zu anderen Mietern gehören, werden von Regel 1 nicht abgeglichen, so dass sie gegen Regel 2 ausgewertet werden.

Regel 2 entspricht allen Objekten anderer Mandanten, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert. Regel 2 stimmt nicht mit Objekten 1 MB oder kleiner überein, daher werden diese Objekte gegen Regel 3 ausgewertet.

Regel 3 ist die letzte und Standardregel in der Richtlinie und verwendet keine Filter. Regel 3 erstellt zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmt (Objekte, die nicht zu Mandant A gehören, die 1 MB oder kleiner sind).



Verwandte Informationen

"Objektmanagement mit ILM"

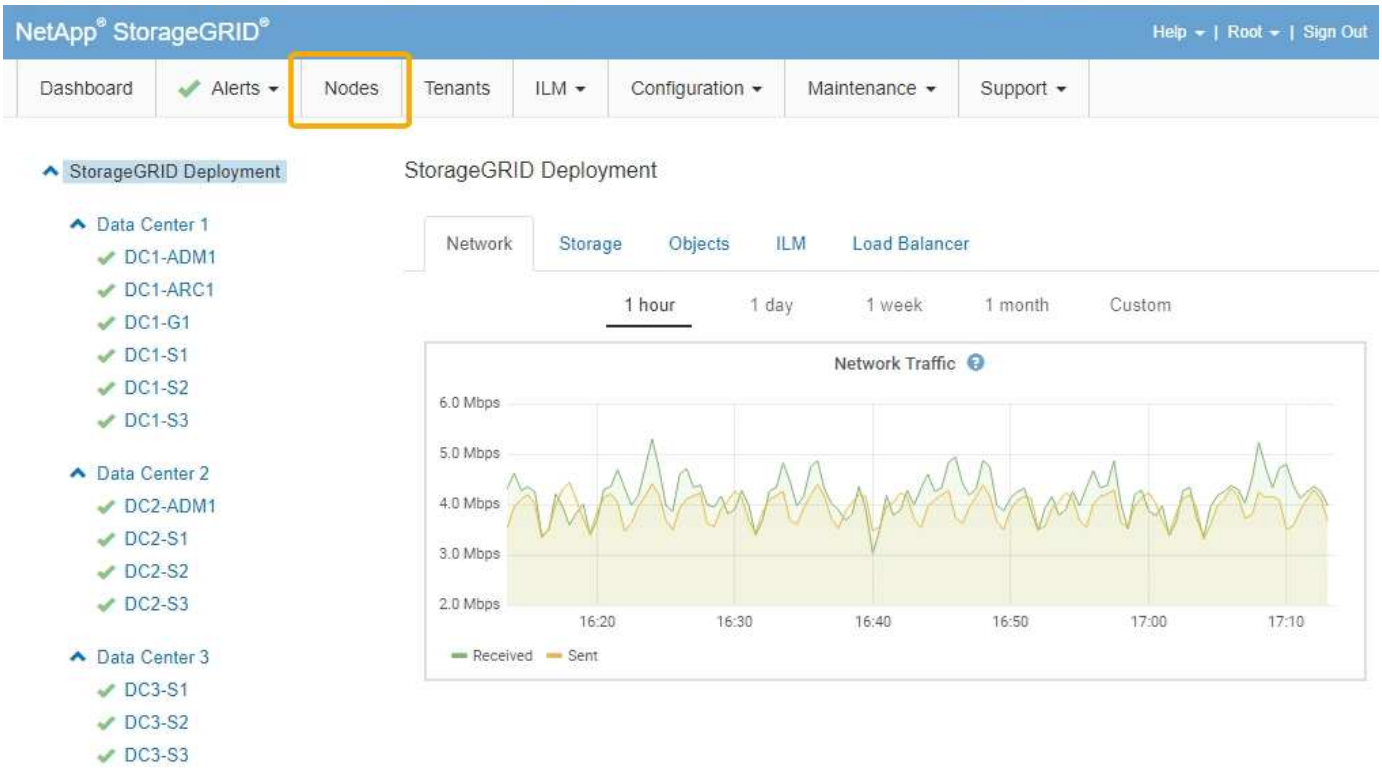
Monitoring der StorageGRID Vorgänge

Der Grid Manager liefert Informationen zur Überwachung der täglichen Aktivitäten Ihres StorageGRID Systems einschließlich des Systemzustands.

- "Anzeigen der Seite Knoten"
- "Monitoring und Management von Warnmeldungen"
- "Verwendung von SNMP-Überwachung"
- "Überprüfen von Audit-Meldungen"

Anzeigen der Seite Knoten

Wenn Sie detailliertere Informationen über Ihr StorageGRID-System als das Dashboard erhalten, können Sie auf der Seite Nodes Metriken für das gesamte Grid, jeden Standort im Raster und jeden Node an einem Standort anzeigen.



In der Baumansicht links sehen Sie alle Standorte und alle Knoten in Ihrem StorageGRID-System. Das Symbol für jeden Knoten gibt an, ob der Knoten verbunden ist oder ob aktive Warnmeldungen vorliegen.

Symbole für Verbindungsstatus

Wenn ein Knoten von der Tabelle getrennt wird, zeigt die Strukturansicht ein blaues oder graues Verbindungssymbol an, nicht das Symbol für die zugrunde liegenden Warnungen.

- **Nicht verbunden - Unbekannt**: Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom 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.

- **Nicht verbunden - Administrativ 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.

Warnungssymbole

Wenn ein Knoten mit dem Raster verbunden ist, wird in der Strukturansicht eines der folgenden Symbole angezeigt, je nachdem, ob aktuelle Warnmeldungen für den Knoten vorhanden sind.

- * 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 sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
- **Normal** ✔: Es sind keine Alarme aktiv, und der Knoten ist mit dem Raster verbunden.

Anzeigen von Details zu einem System, Standort oder Node

Um die verfügbaren Informationen anzuzeigen, klicken Sie auf die entsprechenden Links auf der linken Seite, wie folgt:

- Wählen Sie den Grid-Namen aus, um eine Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen. (Der Screenshot zeigt ein System mit dem Namen „StorageGRID Deployment“.)
- 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.

Verwandte Informationen

"Monitor Fehlerbehebung"

Registerkarten für die Seite Knoten

Die Registerkarten oben auf der Seite Knoten basieren auf dem, was Sie im Baum links auswählen.

Registerkartenname	Beschreibung	Enthalten für
Überblick	• Enthält grundlegende Informationen zu den einzelnen Nodes. • Zeigt alle aktuellen, nicht quittierten Alarme an, die den Knoten betreffen.	Alle Nodes
Trennt	• Zeigt die CPU-Auslastung und die Arbeitsspeicherauslastung für jeden Node an • Bei Appliance-Nodes werden zusätzliche Hardwareinformationen bereitgestellt.	Alle Nodes
Netzwerk	Zeigt ein Diagramm an, in dem der empfangene und über die Netzwerkschnittstellen gesendete Netzwerkverkehr angezeigt wird.	Alle Nodes, jeden Standort und das gesamte Grid

Registerkartenname	Beschreibung	Enthalten für
Storage	• Enthält Details zu den Festplattengeräten und Volumes auf jedem Knoten. • Enthält Diagramme für Storage-Nodes, die den Objekt-Storage und den über die Zeit verwendeten Metadaten-Storage zeigen.	Alle Nodes, jeden Standort und das gesamte Grid
Veranstaltungen	Zeigt die Anzahl aller Systemfehler oder Fehlerereignisse an, einschließlich Fehler wie Netzwerkfehler.	Alle Nodes
Objekte	• Bietet Informationen zu Aufnahme- und Abrufraten für S3 und Swift. • Für Storage-Nodes werden Objektanzahl und Informationen zu Metadatenspeicherabfragen und zur Hintergrundüberprüfung bereitgestellt.	Storage-Nodes, jeden Standort und das gesamte Grid
ILM	Stellt Informationen zu ILM-Vorgängen (Information Lifecycle Management) bereit. • Für Storage-Nodes enthält Details zur ILM-Bewertung und zur Hintergrund-Verifizierung zum Löschen codierter Objekte. • Zeigt für jeden Standort und das gesamte Grid ein Diagramm der ILM-Warteschlange im Laufe der Zeit an. • Stellt im gesamten Grid die geschätzte Zeit zum Abschluss eines vollständigen ILM-Scans aller Objekte zur Verfügung.	Storage-Nodes, jeden Standort und das gesamte Grid
Lastausgleich	Enthält Performance- und Diagnosediagramme zum Load Balancer-Service. • Bietet für jeden Standort eine Zusammenfassung der Statistiken für alle Nodes an diesem Standort. • Das gesamte Raster bietet eine aggregierte Zusammenfassung der Statistiken für alle Standorte.	Admin-Nodes und Gateway-Nodes, jeden Standort und das gesamte Grid
Plattform-Services	Dieser Service bietet Informationen zu S3-Plattform-Servicevorgängen an einem Standort.	Jeder Standort

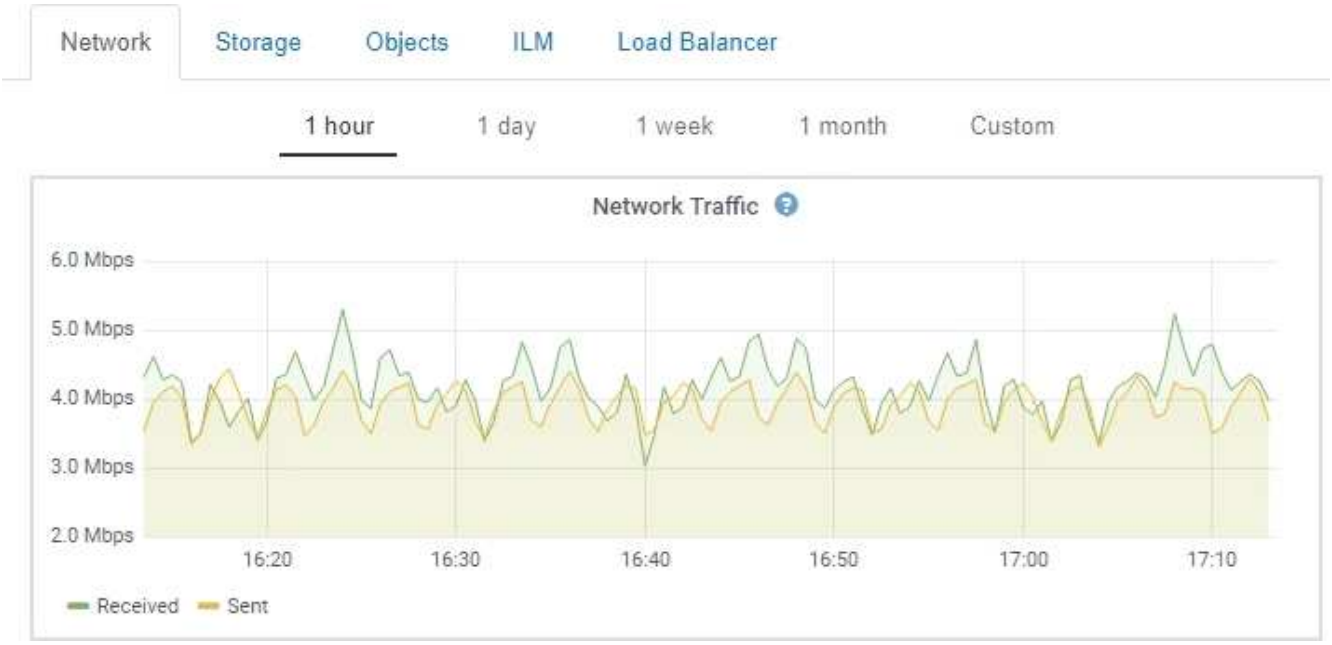
Registerkartenname	Beschreibung	Enthalten für
SANtricity System Manager	Zugriff auf SANtricity System Manager Vom SANtricity System Manager können Sie die Hardware-Diagnose und Umgebungsinformationen für den Storage Controller sowie Probleme im Zusammenhang mit den Laufwerken überprüfen.	Nodes von Storage-Appliances **Hinweis:** die Registerkarte SANtricity System Manager wird nicht angezeigt, wenn die Controller-Firmware auf dem Speichergerät weniger als 8.70 ist.

Kennzahlen von Prometheus

Der Prometheus-Service auf Admin-Knoten sammelt Zeitreihungskennzahlen aus den Diensten auf allen Knoten.

Die von Prometheus erfassten Kennzahlen werden an verschiedenen 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 (**Hilfe API-Dokumentation Metrics**). Während mehr als tausend Kennzahlen zur Verfügung stehen, ist nur eine relativ kleine Zahl zur Überwachung der kritischsten 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 Diagnose** und die **Support Tools Metriken** Seite: Diese Seiten, die hauptsächlich für den technischen Support bestimmt sind, bieten eine Reihe von Werkzeugen und Diagrammen, die die Werte der Prometheus-Kennzahlen nutzen.

  Einige Funktionen und Menüelemente auf der Seite Metriken sind absichtlich nicht funktionsfähig und können sich ändern.

Verwandte Informationen

"Monitoring und Management von Warnmeldungen"

"Verwenden von StorageGRID Support-Optionen"

"Monitor Fehlerbehebung"

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 verschiedenen 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.)
- **Alarme**: Wenn Attribute definierte Schwellenwerte erreichen, werden StorageGRID-Alarme (Altsystem) auf bestimmten Schweregraden ausgelöst.
- **Grid Topology Tree**: Attributwerte werden im Grid Topology Tree (**Support 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.

Verwandte Informationen

"Monitor Fehlerbehebung"

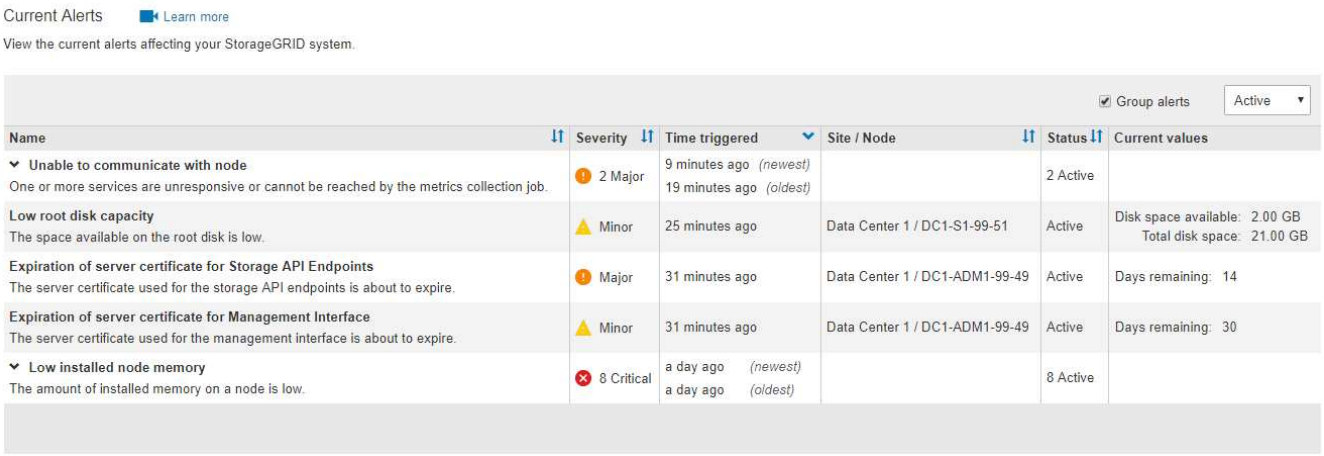
Monitoring und Management von Warnmeldungen

Das Warnsystem bietet eine benutzerfreundliche Oberfläche zum Erkennen, Bewerten

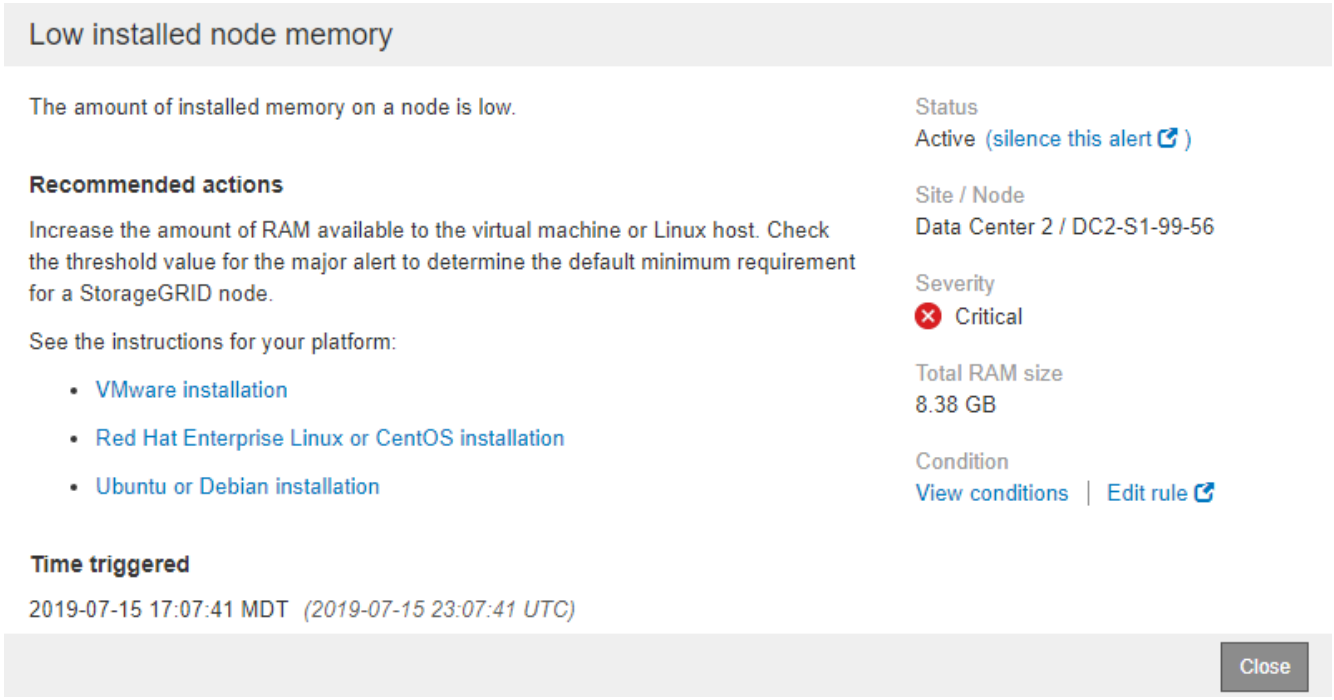
und Beheben von Problemen, die während des StorageGRID-Betriebs auftreten können.

Das Alarmsystem wurde als Ihr vorrangiges Tool entwickelt, mit dem Sie alle eventuell auftretenden Probleme in Ihrem StorageGRID System überwachen können.

- Das Warnsystem konzentriert sich auf umsetzbare Probleme im System. Bei Ereignissen, die eine sofortige Aktion erfordern, werden Warnmeldungen ausgelöst und nicht bei Ereignissen, die sicher ignoriert werden können.
- Die Seiten „Current Alerts“ und „Resolved Alerts“ bieten eine benutzerfreundliche Oberfläche zum Anzeigen aktueller und historischer Probleme. Sie können die Liste nach einzelnen Warnungen und Alarmgruppen sortieren. Beispielsweise können Sie alle Meldungen nach Node/Standort sortieren, um zu sehen, welche Meldungen sich auf einen bestimmten Node auswirken. Oder Sie möchten die Meldungen in einer Gruppe nach der Zeit sortieren, die ausgelöst wird, um die letzte Instanz einer bestimmten Warnmeldung zu finden.
- Mehrere Warnmeldungen desselben Typs werden in einer E-Mail gruppiert, um die Anzahl der Benachrichtigungen zu reduzieren. Darüber hinaus werden auf den Seiten „Current Alerts and Resolved Alerts“ mehrere Warnmeldungen desselben Typs als Gruppe angezeigt. Sie können Warnungsgruppen erweitern oder ausblenden, um die einzelnen Warnmeldungen ein- oder auszublenden. Wenn z. B. mehrere Knoten die Warnung **nicht mit Knoten** kommunizieren können, wird nur eine E-Mail gesendet und die Warnung wird als Gruppe auf der Seite Aktuelle Meldungen angezeigt.



- Benachrichtigungen verwenden intuitive Namen und Beschreibungen, damit Sie das Problem schneller verstehen können. Meldungsbenachrichtigungen umfassen Details zum betroffenen Node und Standort, den Schweregrad der Warnmeldung, den Zeitpunkt, zu dem die Meldungsregel ausgelöst wurde, und den aktuellen Wert der Metriken in Bezug auf die Meldung.
- Alert-E-Mail-Benachrichtigungen und die auf den Seiten „Current Alerts and Resolved Alerts“ angezeigten Warnmeldungen enthalten empfohlene Aktionen zum Beheben von Warnmeldungen. Dazu gehören häufig direkte Links zur StorageGRID Dokumentation, sodass detailliertere Informationen zur Fehlerbehebung leichter finden und abrufen können.



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

Verwalten von Meldungen

Alle StorageGRID-Benutzer können Warnmeldungen anzeigen. Wenn Sie über die Berechtigung Root Access oder Manage Alerts verfügen, können Sie auch Warnmeldungen wie folgt verwalten:

- Wenn Sie die Benachrichtigungen für eine Warnung vorübergehend auf einem oder mehreren Schweregraden unterdrücken müssen, können Sie ganz einfach eine bestimmte Alarmregel für eine bestimmte Dauer stummschalten. Sie können eine Alarmregel für das gesamte Raster, eine einzelne Site oder einen einzelnen Knoten stummschalten.
- Sie können die standardmäßigen Alarmregeln nach Bedarf bearbeiten. Sie können eine Meldungsregel vollständig deaktivieren oder deren Triggerbedingungen und -Dauer ändern.
- Sie können benutzerdefinierte Alarmregeln erstellen, um auf die für Ihre Situation relevanten spezifischen Bedingungen abzielen und eigene Empfehlungen auszuarbeiten. Um die Bedingungen für eine benutzerdefinierte Warnung zu definieren, erstellen Sie Ausdrücke mithilfe der Prometheus-Metriken, die im Abschnitt Kennzahlen der Grid Management API verfügbar sind.

  Dieser Ausdruck bewirkt beispielsweise, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Node weniger als 24,000,000,000 Byte (24 GB) beträgt.

```
node_memory_MemTotal < 24000000000
```

Verwandte Informationen

"Monitor Fehlerbehebung"

Verwendung von SNMP-Überwachung

Wenn Sie StorageGRID mit dem Simple Network Management Protocol (SNMP) überwachen möchten, können Sie den SNMP-Agent mithilfe des Grid-Managers konfigurieren.

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine Management Information Base (MIB) bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Alarme und Alarme. Jeder StorageGRID-Knoten unterstützt auch eine Untergruppe von MIB-II-Objekten.

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. Der Agent bietet schreibgeschützten MIB-Zugriff für Abfragen, und es kann zwei Arten von ereignisgesteuerten Benachrichtigungen an ein Verwaltungssystem senden:

- **Traps** sind Benachrichtigungen, die vom SNMP-Agent gesendet werden, die keine Bestätigung durch das Verwaltungssystem 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. Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde.
- Bestimmte Alarme (Altsystem) werden mit einem bestimmten Schweregrad oder höher ausgelöst.

> SNMP-Benachrichtigungen werden nicht für jeden Alarm oder jeden Schweregrad gesendet.

Verwandte Informationen

"Monitor Fehlerbehebung"

Überprüfen von Audit-Meldungen

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.

Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf die Audit-Share sowohl für NFS als auch für CIFS (veraltet) konfigurieren. Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Details zur Audit-Protokolldatei, zum Format von Audit-Meldungen, zu den Typen von Audit-Meldungen und zu den verfügbaren Tools zur Analyse von Audit-Meldungen finden Sie in den Anweisungen für Audit-Meldungen. Weitere Informationen zum Konfigurieren des Zugriffs auf Audit-Clients finden Sie in den Anweisungen für die Administration von StorageGRID.

Verwandte Informationen

"Prüfung von Audit-Protokollen"

"StorageGRID verwalten"

Durchführung von Wartungsverfahren

Sie führen verschiedene Wartungsverfahren durch, um Ihr StorageGRID System auf dem neuesten Stand zu halten und eine effiziente Performance zu gewährleisten. Der Grid Manager bietet Tools und Optionen, die den Prozess der Durchführung von Wartungsaufgaben vereinfachen.

Software-Updates

Sie können drei Arten von Softwareupdates auf der Seite Software-Aktualisierung im Grid Manager ausführen:

- StorageGRID-Software-Upgrade
- StorageGRID-Hotfix
- Upgrade von SANtricity OS

StorageGRID Software-Upgrades

Sobald eine neue StorageGRID-Funktionsversion verfügbar ist, führt Sie die Seite Software-Upgrade durch das Hochladen der erforderlichen Datei und das Upgrade Ihres StorageGRID-Systems. Sie müssen alle Grid-Nodes für alle Datacenter-Standorte vom primären Admin-Node aus aktualisieren.

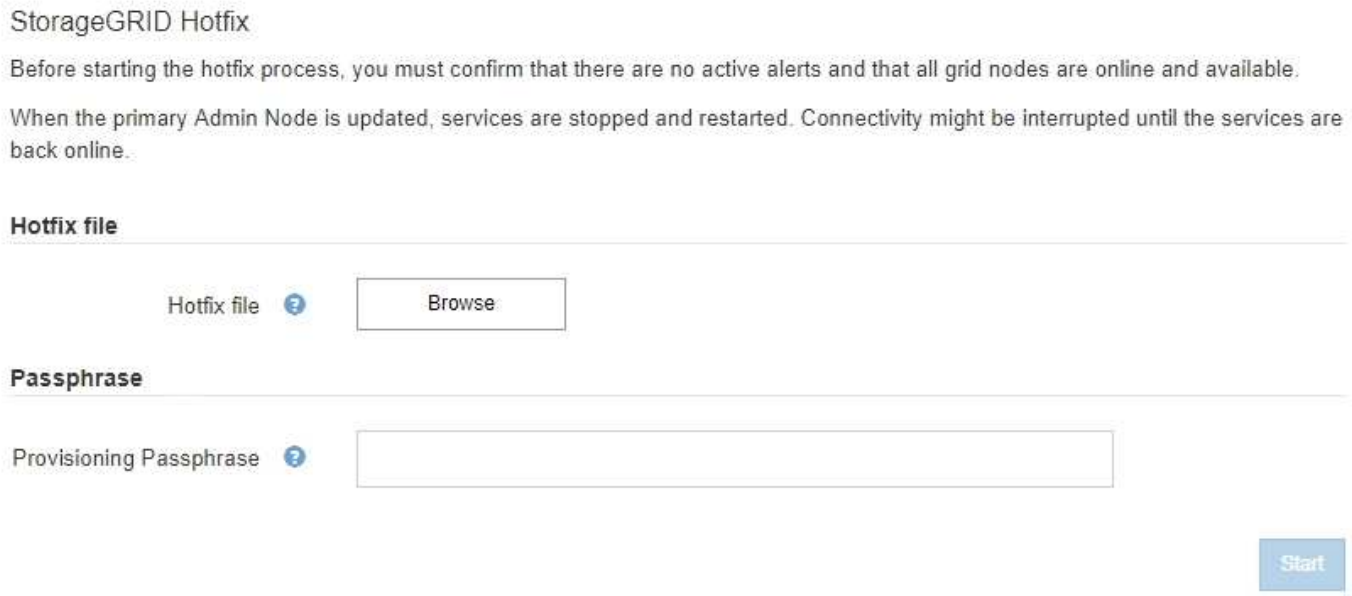
Bei einem StorageGRID Software-Upgrade können Client-Applikationen weiterhin Objektdaten aufnehmen und abrufen.

Hotfixes

Wenn Probleme mit der Software zwischen Funktionsversionen erkannt und behoben werden, müssen Sie möglicherweise ein Hotfix auf Ihr StorageGRID-System anwenden.

StorageGRID Hotfixes enthalten Software-Änderungen, die außerhalb einer Feature- oder Patch-Freigabe verfügbar gemacht werden. Die gleichen Änderungen sind in einer zukünftigen Version enthalten.

Auf der unten gezeigten Seite StorageGRID Hotfix können Sie eine Hotfix-Datei hochladen.



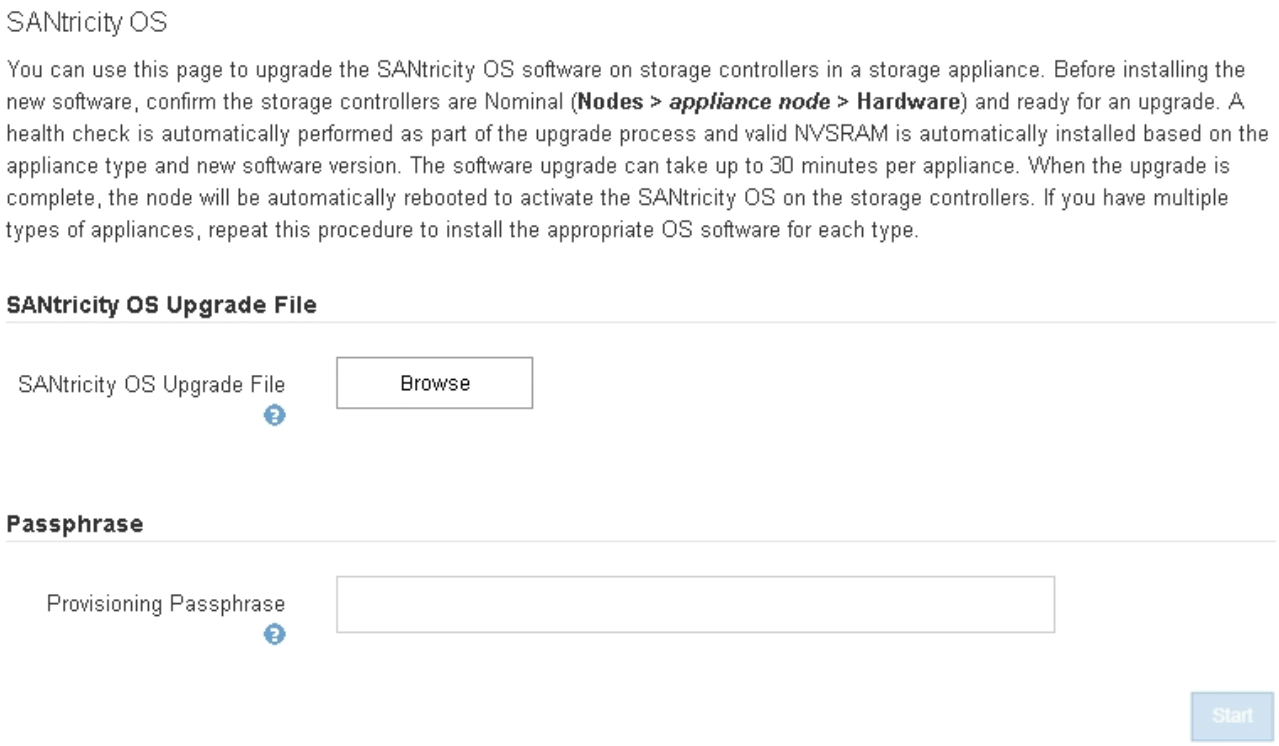
Der Hotfix wird zuerst auf den primären Admin-Knoten angewendet. Anschließend müssen Sie die Anwendung des Hotfix für andere Grid-Knoten genehmigen, bis alle Knoten im StorageGRID-System dieselbe Softwareversion ausführen. Sie können die Genehmigungssequenz anpassen, indem Sie auswählen, ob einzelne Grid-Nodes, Gruppen von Grid-Nodes oder alle Grid-Nodes genehmigt werden sollen.

> Während alle Grid-Knoten mit der neuen Hotfix-Version aktualisiert werden, können die tatsächlichen Änderungen in einem Hotfix nur bestimmte Dienste auf bestimmten Knotentypen beeinflussen. Ein Hotfix wirkt sich beispielsweise nur auf den LDR-Service auf Storage Nodes aus.

Upgrades für SANtricity OS

Möglicherweise müssen Sie die SANtricity OS Software auf den Storage Controllern Ihrer Storage Appliances aktualisieren, falls die Controller nicht optimal funktionieren. Sie können die SANtricity OS-Datei auf den primären Admin-Knoten in Ihrem StorageGRID-System hochladen und das Upgrade vom Grid-Manager anwenden.

Auf der unten gezeigten SANtricity-Seite können Sie die SANtricity OS-Aktualisierungsdatei hochladen.

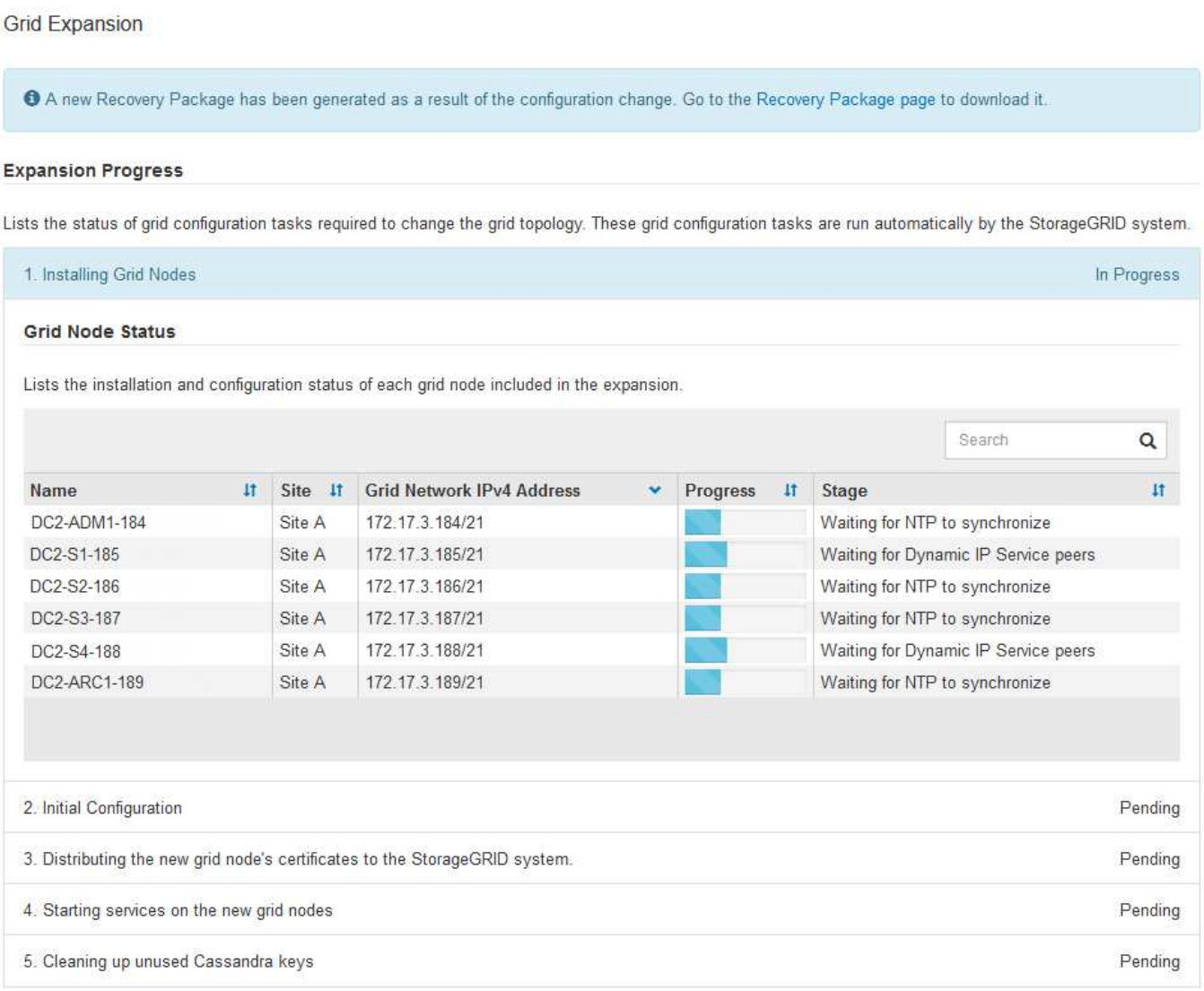


Nach dem Hochladen der Datei können Sie das Upgrade auf einzelnen Storage-Nodes oder allen Nodes genehmigen. Die Möglichkeit, Nodes selektiv zu genehmigen, erleichtert Ihnen die Planung des Upgrades. Nachdem Sie einen Node für das Upgrade genehmigt haben, führt das System eine Zustandsprüfung durch und installiert das Upgrade, sofern es auf den Node anwendbar ist.

Erweiterungsverfahren

Ein StorageGRID System lässt sich mit folgenden Methoden erweitern: Storage-Nodes erhalten mehr Storage-Volumes, ein Datacenter wird um neue Grid-Nodes erweitert oder es wird ein neues Datacenter hinzugefügt. Wenn Storage-Nodes die SG6060 Storage Appliance verwenden, können Sie ein oder zwei Erweiterungs-Shelfs hinzufügen, um die Storage-Kapazität des Nodes zu verdoppeln oder zu verdreifachen.

Eine Erweiterung kann vorgenommen werden, ohne den Betrieb des aktuellen Systems zu unterbrechen. Wenn Sie Nodes oder einen Standort hinzufügen, implementieren Sie zunächst die neuen Nodes und führen dann die Erweiterungsverfahren auf der Seite „Grid Expansion“ aus.

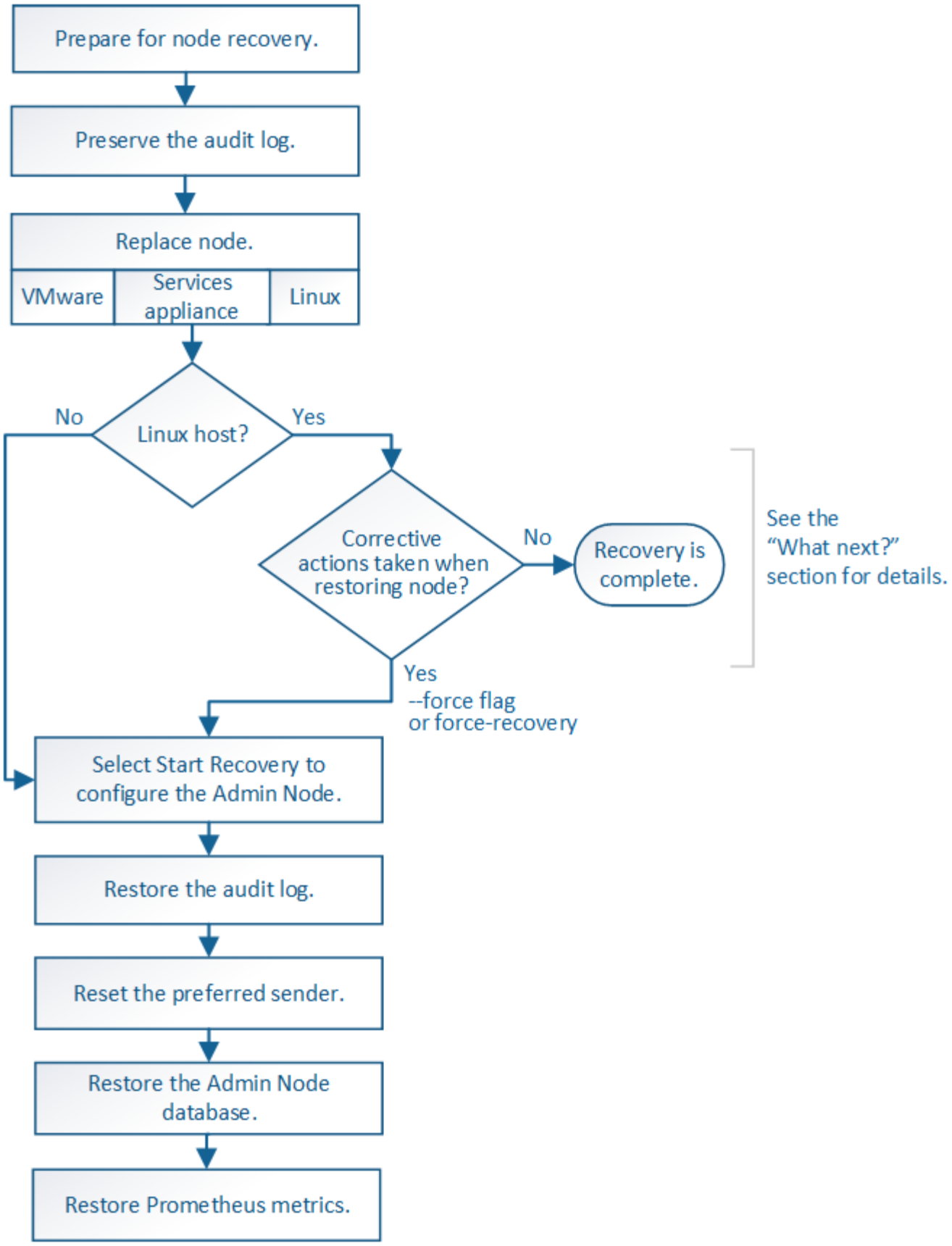


Recovery-Verfahren für die Nodes

Grid Nodes können ausfallen, wenn ein Hardware-, Virtualisierungs-, Betriebssystem- oder Softwarefehler den Node funktionsunfähig oder unzuverlässig macht.

Die Schritte zur Wiederherstellung eines Grid-Node hängen von der Plattform ab, 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, sofern möglich Daten vom ausgefallenen Grid Node beizubehalten, den ausgefallenen Node zu reparieren oder zu ersetzen, verwenden Sie die Seite Recovery, um den Ersatz-Node zu konfigurieren und die Daten des Node wiederherzustellen.

In diesem Flussdiagramm wird beispielsweise der Wiederherstellungsvorgang angezeigt, wenn ein Admin-Node ausgefallen ist.



Verfahren zur Deaktivierung

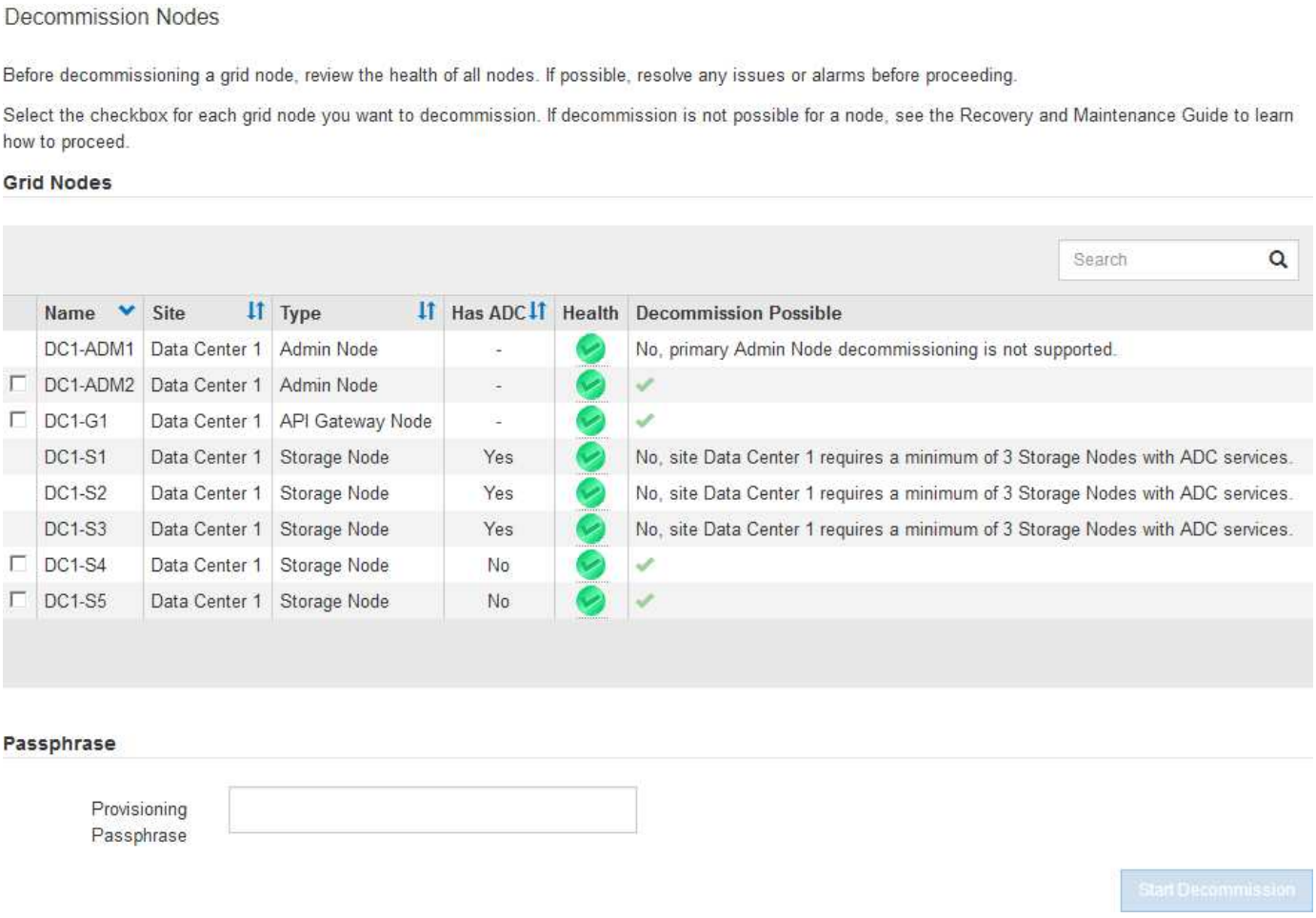
Es besteht die Möglichkeit, die Grid-Nodes oder den gesamten Datacenter-Standort vom StorageGRID-System entfernt zu werden.

In folgenden Fällen möchten Sie beispielsweise einen oder mehrere Grid-Nodes außer Betrieb nehmen:

- 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 oder einen nicht-primären Admin-Node mehr.
- Das Grid enthält einen getrennten Node, den Sie nicht wiederherstellen können oder wieder online schalten können.

Sie können die Seite Decommission Nodes im Grid Manager verwenden, um die folgenden Typen von Grid-Nodes zu entfernen:

- Storage-Nodes, es sei denn, nicht genügend Nodes würden am Standort verbleiben, um bestimmte Anforderungen zu unterstützen
- Gateway-Nodes
- Nicht primäre Admin-Nodes



Sie können die Seite „Decommission Site“ im Grid Manager verwenden, um eine Site zu entfernen. Durch die Stilllegung einer verbundenen Website wird ein operativer Standort entfernt und Daten beibehalten. Durch die Stilllegung eines getrennten Standorts wird ein ausgefallener Standort entfernt, Daten werden jedoch nicht aufbewahrt. Der Assistent „Decommission Site“ führt Sie durch die Auswahl der Site, das Anzeigen von Standortdetails, die Überprüfung der ILM-Richtlinie, das Entfernen von Standortverweisen aus ILM-Regeln und das Beheben von Knotenkonflikten.

Netzwerkwartungsverfahren

Einige der erforderlichen Netzwerkwartungsverfahren sind u. a.:

- Subnetze im Grid-Netzwerk aktualisieren
- Verwenden des Change IP-Tools zur Änderung der Netzwerkkonfiguration, die ursprünglich während der Grid-Implementierung festgelegt wurde
- Hinzufügen, Entfernen oder Aktualisieren von DNS-Servern (Domain Name System
- Hinzufügen, Entfernen oder Aktualisieren von NTP-Servern (Network Time Protocol) stellt sicher, dass die Daten zwischen den Grid-Nodes korrekt synchronisiert werden
- Wiederherstellung der Netzwerkverbindung zu Nodes, die möglicherweise vom Rest des Grid isoliert wurden

Verfahren auf Host-Ebene und Middleware

Einige Wartungsverfahren sind speziell für StorageGRID Nodes erhältlich, die unter Linux oder VMware implementiert werden oder sich speziell für andere Komponenten der StorageGRID Lösung eignen. Beispielsweise möchten Sie einen Grid-Node zu einem anderen Linux-Host migrieren oder einen Archiv-Node, der mit Tivoli Storage Manager (TSM) verbunden ist, warten.

Klonen von Appliance-Nodes

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. Klonen bietet einen einfach zu handhabenden Hardware-Upgrade-Prozess und stellt eine alternative Methode für den Austausch von Appliances dar.

Grid Node Prozeduren

Möglicherweise müssen Sie bestimmte Verfahren auf einem bestimmten Grid-Node durchführen. Beispielsweise müssen Sie einen Grid-Node neu booten oder einen bestimmten Grid-Node-Service manuell beenden und neu starten. Einige Verfahren für Grid-Nodes können über den Grid-Manager ausgeführt werden. Bei anderen müssen Sie sich am Grid-Node einloggen und die Befehlszeile des Node verwenden.

Verwandte Informationen

"StorageGRID verwalten"

"Software-Upgrade"

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

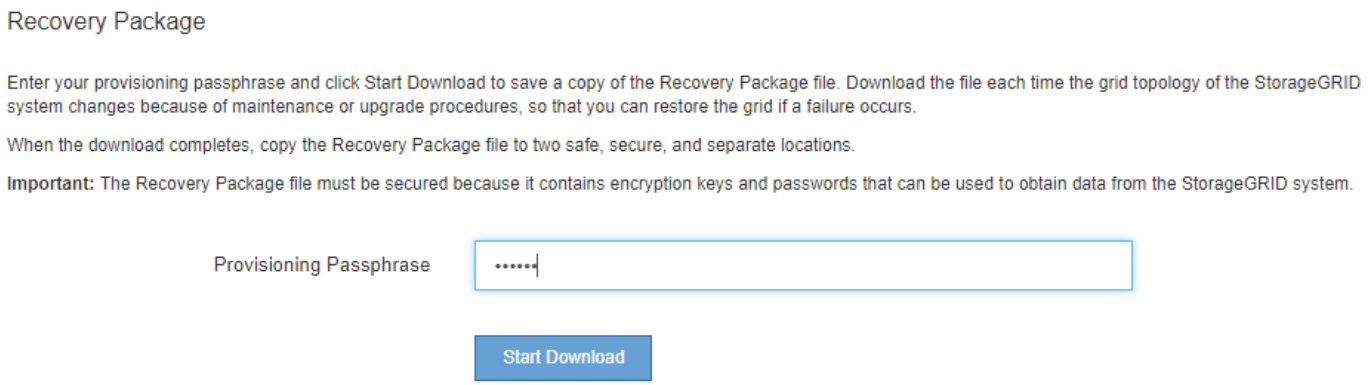
Herunterladen des Wiederherstellungspakets

Das Recovery-Paket ist eine ZIP-Datei zum Herunterladen, die Implementierungsspezifische Dateien und Software enthält, die zur Installation, Erweiterung, Aktualisierung und Wartung eines StorageGRID Systems erforderlich sind.

Die Recovery Package-Datei enthält auch systemspezifische Konfigurations- und Integrationsinformationen, einschließlich Server-Hostnamen und IP-Adressen sowie hochvertrauliche Passwörter, die während der

Systemwartung, beim Upgrade und bei der Erweiterung benötigt werden. Das Wiederherstellungspaket ist für die Wiederherstellung nach dem Ausfall des primären Admin-Knotens erforderlich.

Bei der Installation eines StorageGRID-Systems müssen Sie die Recovery Package-Datei herunterladen und bestätigen, dass Sie erfolgreich auf den Inhalt dieser Datei zugreifen können. Zudem sollten Sie die Datei jedes Mal herunterladen, wenn sich die Grid-Topologie des StorageGRID Systems aufgrund von Wartungs- oder Upgrade-Verfahren ändert.



Nach dem Herunterladen der Recovery Package-Datei und der Bestätigung können Sie den Inhalt extrahieren, kopieren Sie die Recovery Package-Datei an zwei sichere und getrennte 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.

Verwandte Informationen

"Software-Upgrade"

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

Verwenden von StorageGRID Support-Optionen

Der Grid Manager bietet Optionen, die Ihnen bei der Zusammenarbeit mit dem technischen Support helfen, falls ein Problem auf Ihrem StorageGRID-System auftritt.

AutoSupport wird konfiguriert

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.

Informationen, die in AutoSupport Meldungen enthalten sind

AutoSupport Meldungen enthalten Informationen, z. B. die folgenden:

- StorageGRID Softwareversion

- Betriebssystemversion
- Attributinformationen auf System- und Standortebene
- Aktuelle Warnmeldungen und Alarme (Altsystem)
- Aktueller Status aller Grid-Aufgaben, einschließlich historischer Daten
- Informationen zu Ereignissen, die auf der Seite **Nodes *Node*** * Events* aufgeführt sind
- 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 ManagerDashboard eine Meldung angezeigt. Die Meldung enthält einen Link zur AutoSupport-Konfigurationsseite.

Sie können das Symbol „x“ auswählen Um die Meldung zu schließen. Die Nachricht wird erst wieder angezeigt, wenn Ihr Browser-Cache gelöscht wird, auch wenn AutoSupport deaktiviert bleibt.

Verwenden von Active IQ

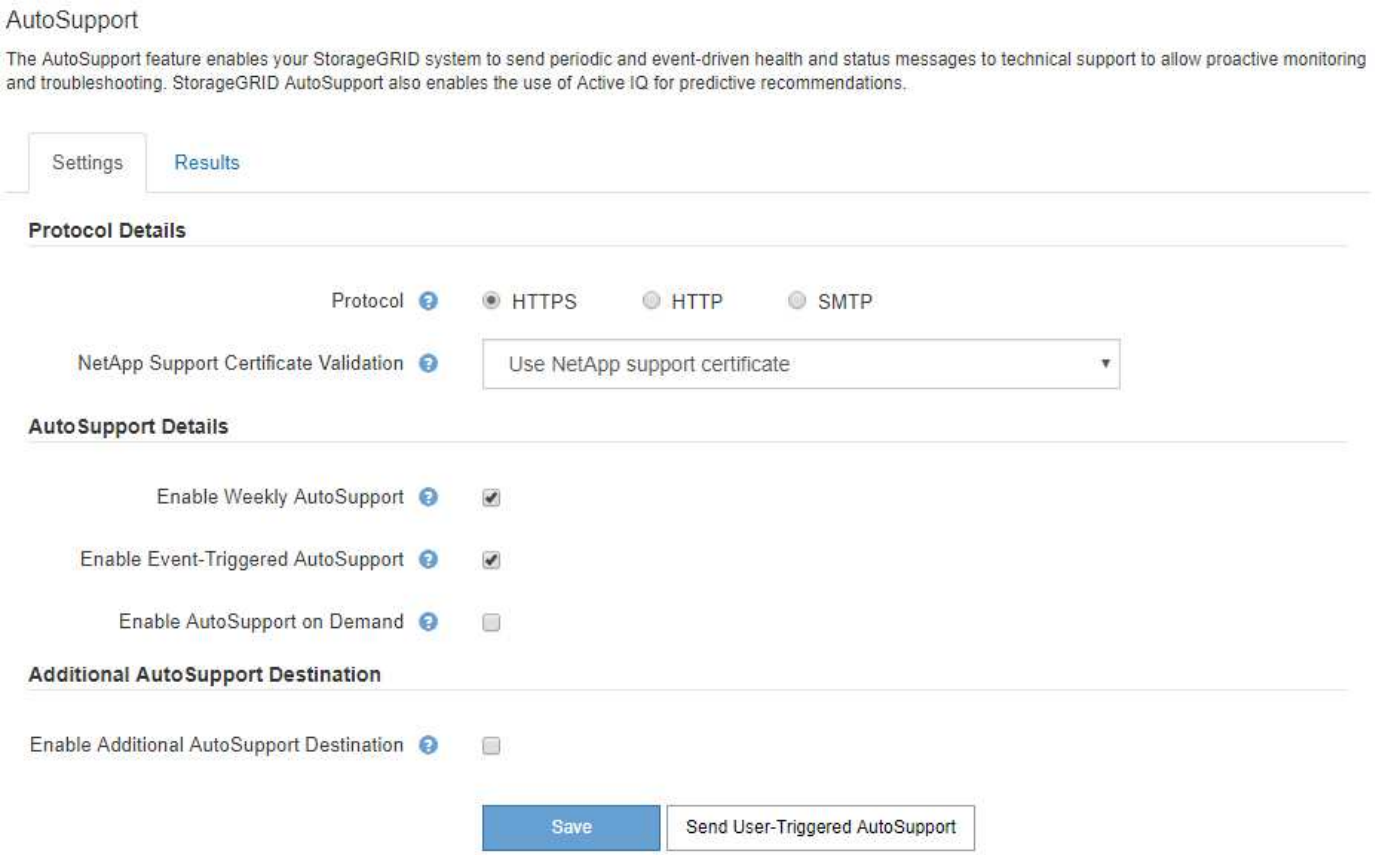
Active IQ ist ein Cloud-basierter digitaler Berater, der prädiktive Analysen und Community-Wissen aus der installierten Basis von NetApp nutzt. Kontinuierliche Risikobewertungen, prädiktive Warnungen, beschreibende Tipps und automatisierte Aktionen helfen Ihnen, Probleme zu vermeiden, bevor sie auftreten. Dies führt zu verbesserter Systemintegrität und höherer Systemverfügbarkeit.

Sie müssen AutoSupport aktivieren, wenn Sie die Active IQ Dashboards und Funktionen auf der NetApp Support-Website nutzen möchten.

"Active IQ Digital Advisor Dokumentation"

Zugriff auf AutoSupport-Einstellungen

Sie konfigurieren AutoSupport mit dem Grid Manager (**Support Tools AutoSupport**). Die **AutoSupport** Seite hat zwei Registerkarten: **Einstellungen** und **Ergebnisse**.



Protokolle zum Senden von AutoSupport Meldungen

Sie können eines von drei Protokollen zum Senden von AutoSupport Meldungen wählen:

- HTTPS
- HTTP
- SMTP

Wenn Sie AutoSupport-Meldungen über HTTPS oder HTTP senden, können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und dem technischen Support konfigurieren.

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.

Verwandte Informationen

"StorageGRID verwalten"

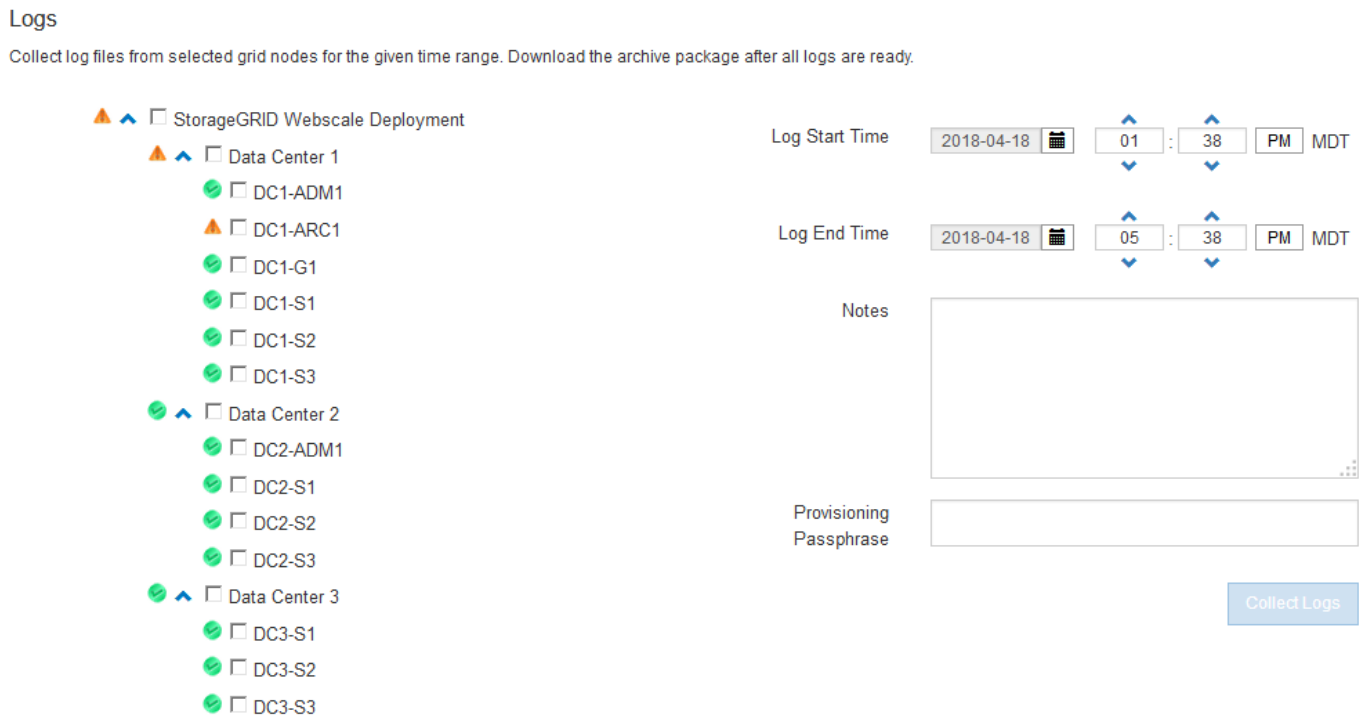
"Netzwerkeinstellungen werden konfiguriert"

Erfassen von StorageGRID-Protokollen

Um bei der Fehlerbehebung zu helfen, müssen Sie möglicherweise Protokolldateien sammeln und an den technischen Support weiterleiten.

StorageGRID verwendet Log-Dateien, um Ereignisse, Diagnosemeldungen und Fehlerbedingungen zu erfassen. Die Datei bycast.log wird für jeden Grid-Node aufbewahrt und ist die primäre Fehlerbehebungsdatei. StorageGRID erstellt zudem Log-Dateien für einzelne StorageGRID-Services, Log-Dateien für Bereitstellungs- und Wartungsaktivitäten und Log-Dateien mit Drittanbieterapplikationen.

Benutzer, die über die entsprechenden Berechtigungen verfügen und die Provisionierungs-Passphrase für Ihr StorageGRID-System kennen, können mithilfe der Seite Protokolle im Grid Manager Protokolldateien, Systemdaten und Konfigurationsdaten erfassen. Wenn Sie Protokolle sammeln, wählen Sie einen Node oder Nodes aus und geben einen Zeitraum an. Daten werden in einem erfasst und archiviert `.tar.gz` Datei, die Sie auf einen lokalen Computer herunterladen können. Innerhalb dieser Datei gibt es für jeden Grid-Knoten ein Protokolldateiarchiv.



Verwandte Informationen

"Monitor Fehlerbehebung"

"StorageGRID verwalten"

Verwenden von Kennzahlen und Ausführen der Diagnose

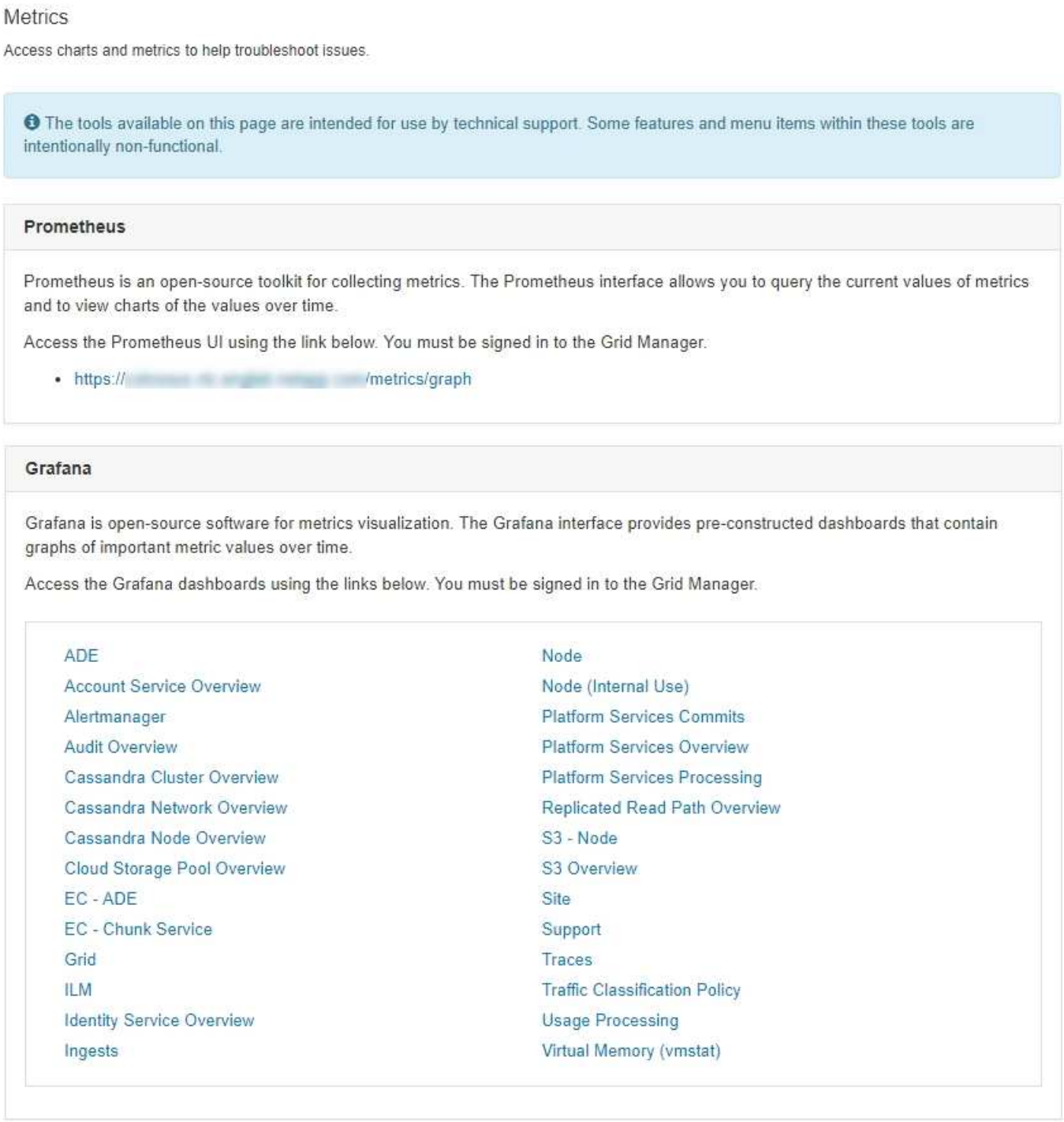
Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte

Metriken und Diagramme für Ihr StorageGRID System prüfen. Sie können außerdem vorkonfigurierte Diagnoseabfragen durchführen, um die Schlüsselwerte für Ihr StorageGRID System proaktiv einzuschätzen.

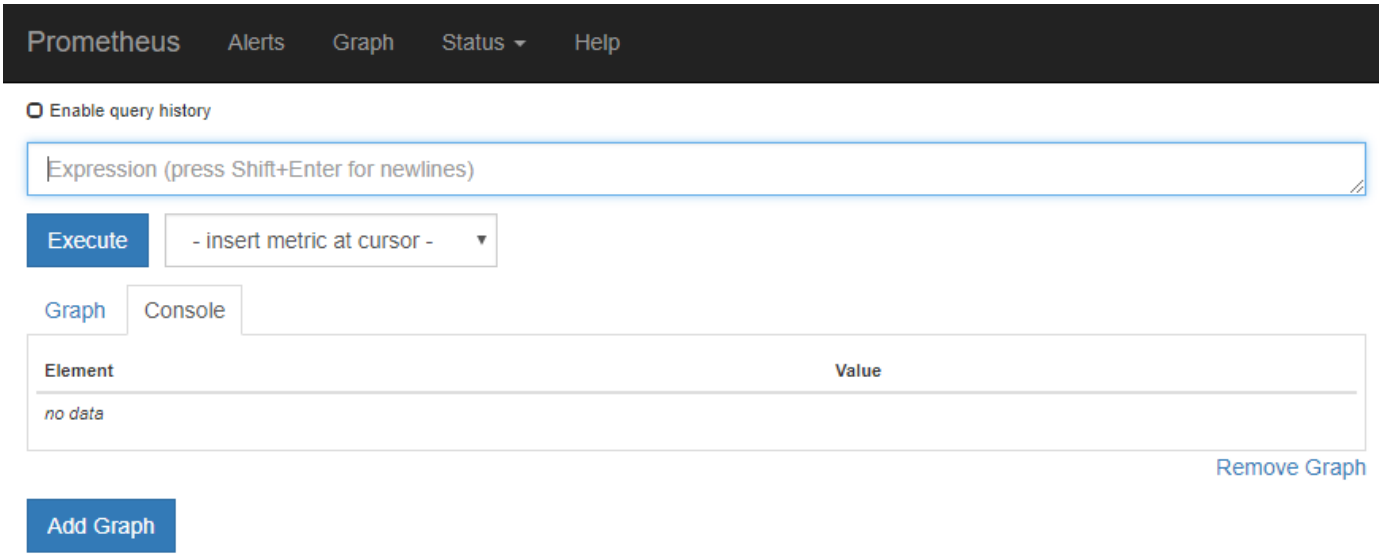
Seite „Kennzahlen“

Auf der Seite Metrics 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.



Über den Link im Bereich Prometheus auf der Seite Metriken können Sie die aktuellen Werte der StorageGRID Metriken abfragen und Diagramme der Werte im Zeitverlauf anzeigen.

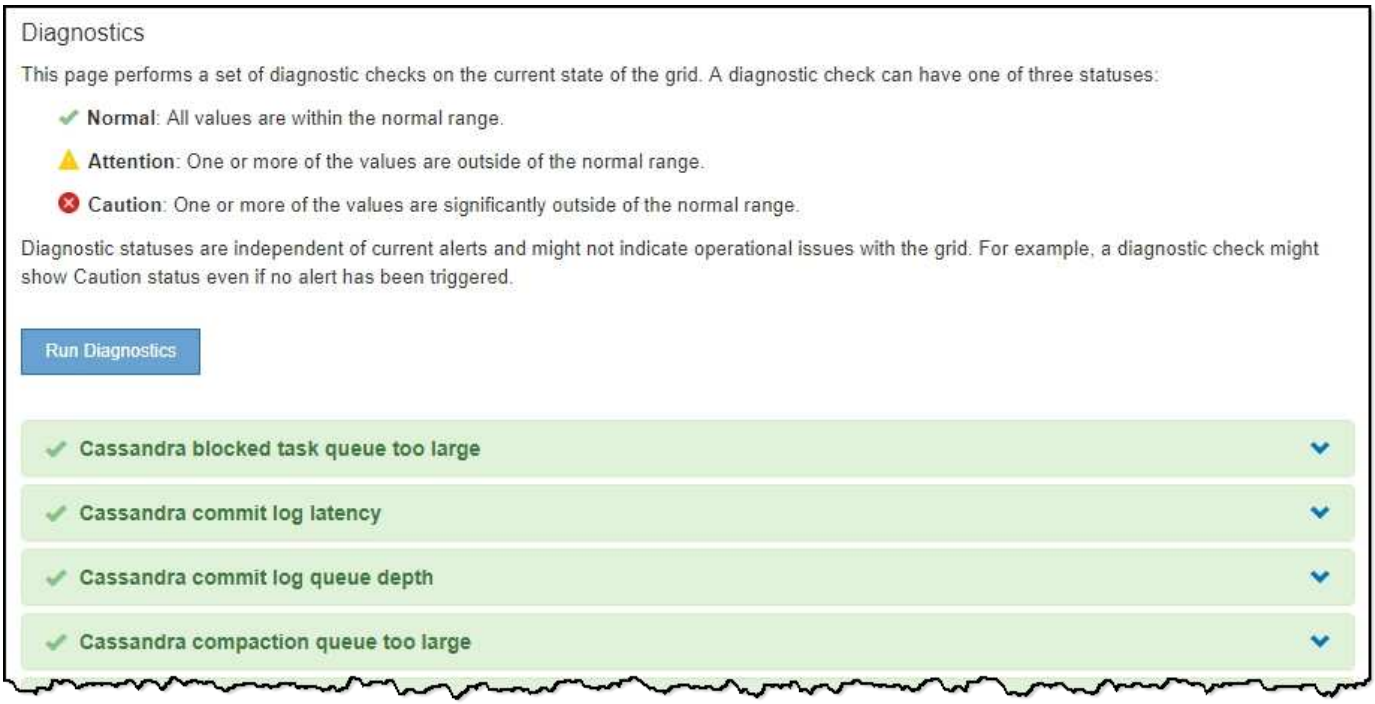


Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

Über die Links im Abschnitt Grafana der Seite Metriken können Sie im Laufe der Zeit auf vorkonfigurierte Dashboards mit Diagrammen zu StorageGRID-Metriken zugreifen.

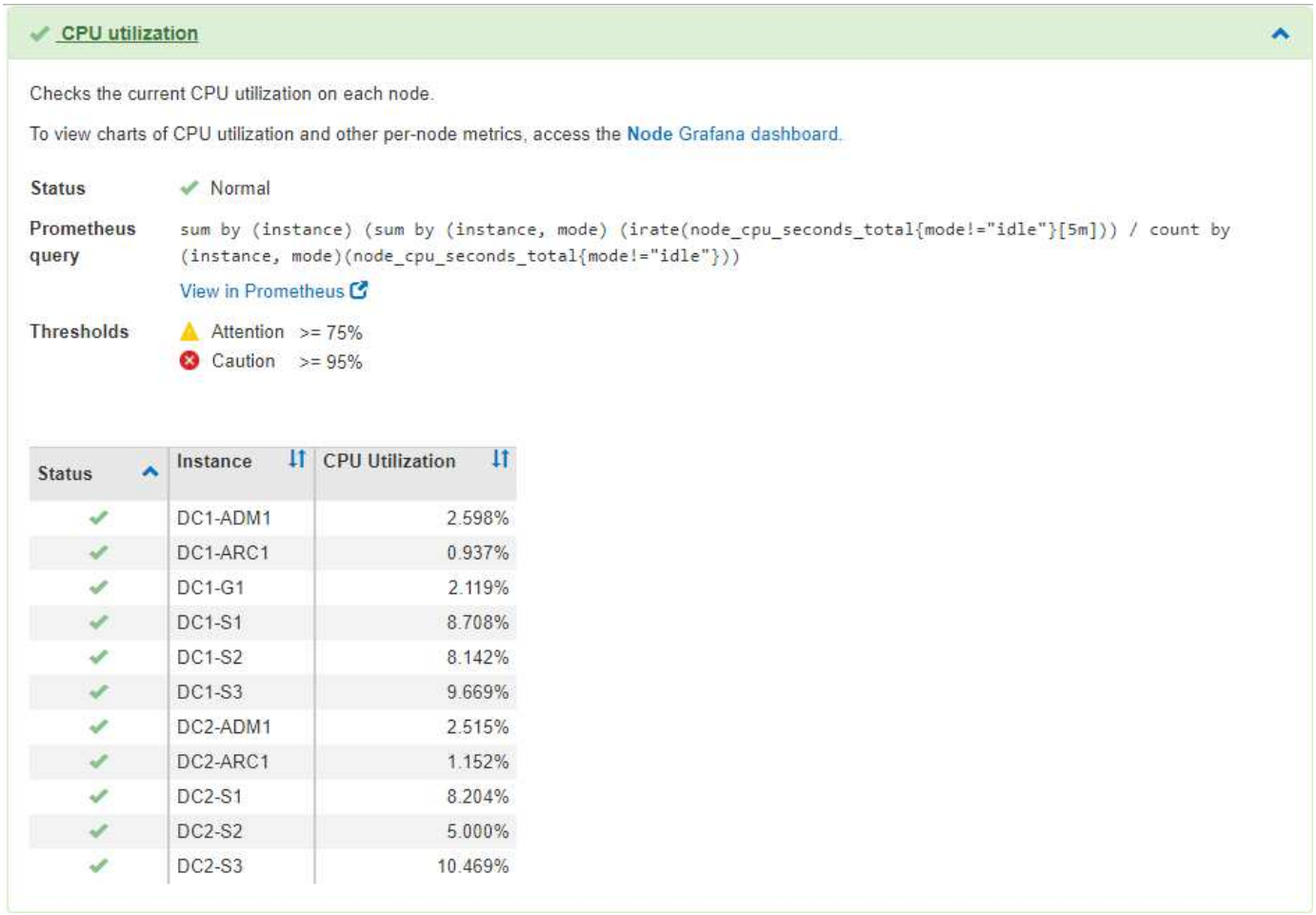
Diagnoseseite

Die Seite Diagnose führt eine Reihe vorkonstruierter Diagnosesecks zum aktuellen Status des Rasters durch. Im Beispiel haben alle Diagnosen einen normalen Status.



Durch Klicken auf eine bestimmte Diagnose können Sie Details zur Diagnose und ihren aktuellen Ergebnissen anzeigen.

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.



Verwandte Informationen

"Monitor Fehlerbehebung"

Netzwerkrichtlinien

StorageGRID Architektur und Netzwerktopologien Machen Sie sich mit den Anforderungen für die Netzwerkkonfiguration und Provisionierung vertraut.

- "Überblick über das StorageGRID Networking"
- "Netzwerkanforderungen und Richtlinien"
- "Implementierungs-spezifische Netzwerküberlegungen"
- "Netzwerkinstallation und -Bereitstellung"
- "Richtlinien nach der Installation"
- "Referenz für Netzwerk-Ports"

Überblick über das StorageGRID Networking

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

Bevor Sie das Networking konfigurieren, machen Sie sich mit der StorageGRID-Architektur vertraut, wie im *Grid Primer* beschrieben.

Bevor Sie StorageGRID implementieren und konfigurieren, müssen Sie die Netzwerkinfrastruktur konfigurieren. Die Kommunikation muss zwischen allen Knoten im Grid und zwischen dem Grid und externen Clients und Diensten erfolgen.

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.

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

Verwandte Informationen

"Gittergrundierung"

"StorageGRID verwalten"

"Versionshinweise"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

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)
Client-Traffic	Der Datenverkehr zwischen externen Client-Applikationen und dem Grid, einschließlich aller Objekt-Storage-Anforderungen von S3 und Swift Clients	Client-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.

Netzwerkschnittstellen

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

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

Weitere Informationen über das Zuordnen virtueller oder physischer Ports zu Node-Netzwerkschnittstellen finden Sie in den Installationsanweisungen.

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 (High Availability groups, HA-Gruppen) bieten die Möglichkeit, virtuelle IP-Adressen zur Grid- oder Client Network-Schnittstelle hinzuzufügen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

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-Netzwerk:

- 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.

Durch die Verwendung eines Admin-Netzwerks muss der Verwaltungs- und Wartungsverkehr nicht über das Grid-Netzwerk geleitet werden. Typische Anwendungen des Admin Network umfassen Zugriff auf die Grid Manager Benutzeroberfläche; Zugriff auf wichtige Dienste wie NTP, DNS, externes Verschlüsselungsmanagement (KMS) und Lightweight Directory Access Protocol (LDAP); Zugriff auf Prüfprotokolle auf Admin-Nodes und 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-Netzwerk:

- 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 selben Client-Netzwerk befinden, und Knoten kommunizieren nie miteinander über das Client-Netzwerk. 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. Weitere Informationen über die Funktion nicht vertrauenswürdiges Clientnetzwerk und den Lastverteilungsservice finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Datenverkehr nicht über das Grid-Netzwerk geleitet werden. Der Netznetzwerkverkehr 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-Netzwerk verwenden zu müssen.

Beachten Sie Folgendes für das Client-Netzwerk:

- 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.

Verwandte Informationen

"Netzwerkanforderungen und Richtlinien"

"StorageGRID verwalten"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

Beispiele für Netzwerktopologie

Neben dem erforderlichen Grid-Netzwerk können Sie auswählen, ob Sie Admin-Netzwerk- und Client-Netzwerk-Schnittstellen bei der Entwicklung der Netzwerktopologie für eine Bereitstellung an einem oder mehreren Standorten konfigurieren möchten.

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. Weitere Informationen zu internen und externen Ports finden Sie unter Netzwerkanschlussreferenz.

Wenn Sie angeben, dass die Client-Netzwerk-Schnittstelle eines Node nicht vertrauenswürdig ist, konfigurieren Sie einen Load Balancer-Endpunkt, um den eingehenden Datenverkehr zu akzeptieren. Informationen zum Konfigurieren nicht vertrauenswürdiger Clientnetzwerke und Load Balancer-Endpunkte finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

"Referenz für Netzwerk-Ports"

Grid-Netzwerktopologie

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

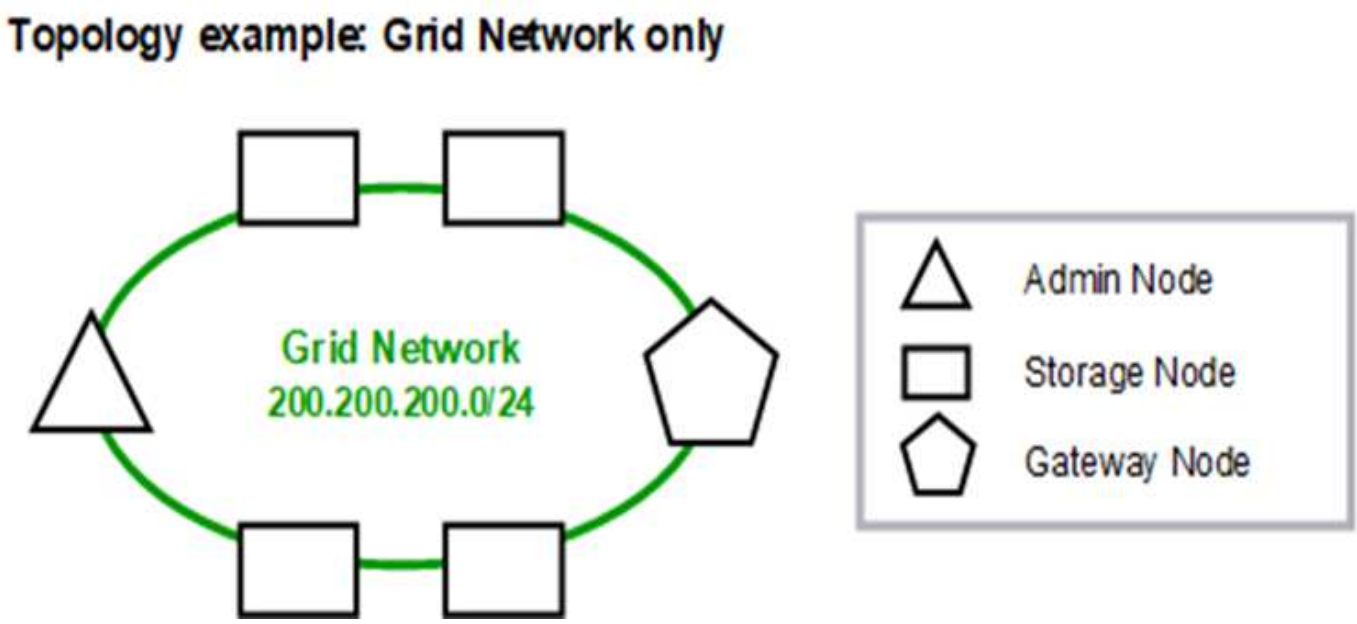
Wenn Sie das Grid-Netzwerk konfigurieren, stellen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Node ein.

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 Standort, die nicht extern verfügbar sind, Proof-of-Concept- oder Testimplementierungen sind oder wenn der Load Balancer eines Drittanbieters als Client-Zugriffsgrenze 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.



Provisioned

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

System Generated

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

Admin-Netzwerktopologie

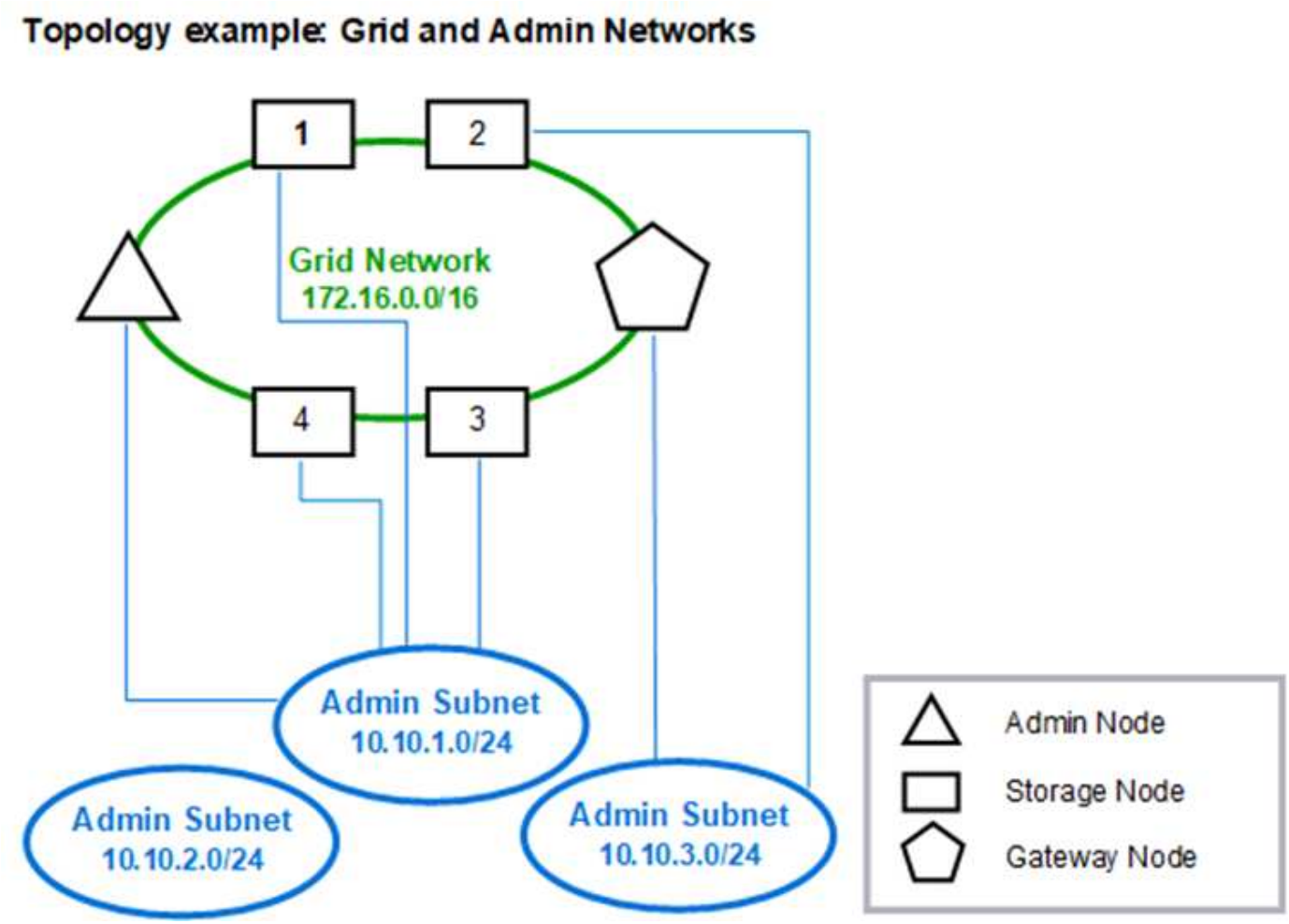
Die Verwendung eines Admin-Netzwerks ist optional. Eine Möglichkeit, wie Sie ein Admin-Netzwerk und ein Grid-Netzwerk verwenden können, besteht darin, ein

routingbares Grid-Netzwerk und ein verbundes 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.



Provisioned

GNSL → 172.16.0.0/16

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

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

System Generated

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

Client-Netzwerktopologie

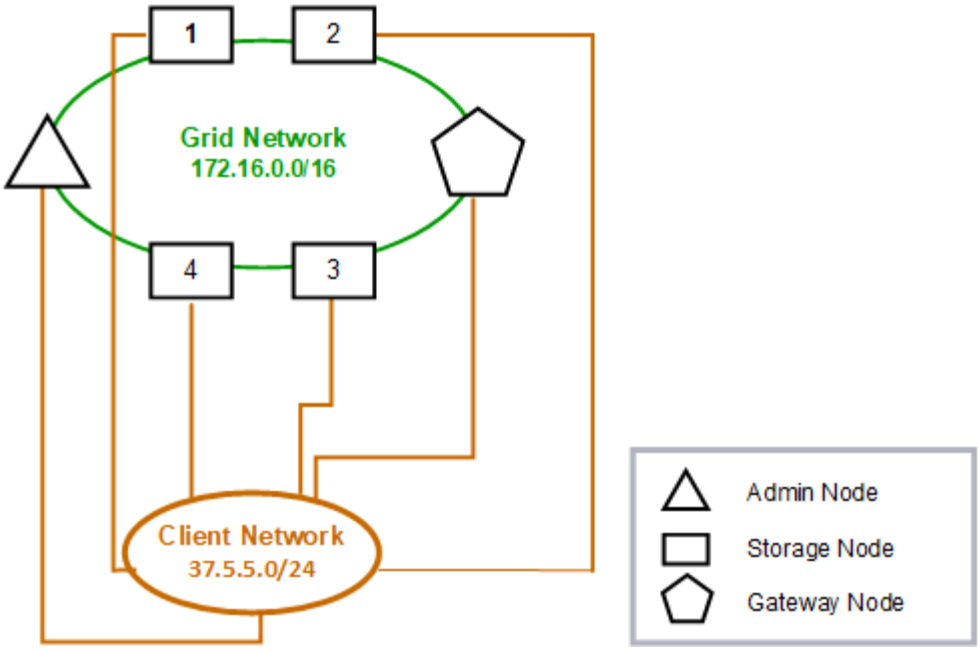
Ein Client-Netzwerk ist optional. Über ein Client-Netzwerk kann der Netzwerk-Traffic des Clients (z. B. S3 und Swift) vom internen Grid-Datenverkehr getrennt werden, wodurch die Sicherheit des Grid-Netzwerks erhöht wird. Wenn das Admin-Netzwerk nicht konfiguriert ist, kann der administrative Datenverkehr 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



Provisioned

GNSL → 172.16.0.0/16

Nodes	Grid Network IP/mask	Client Network IP/mask	Client Network 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

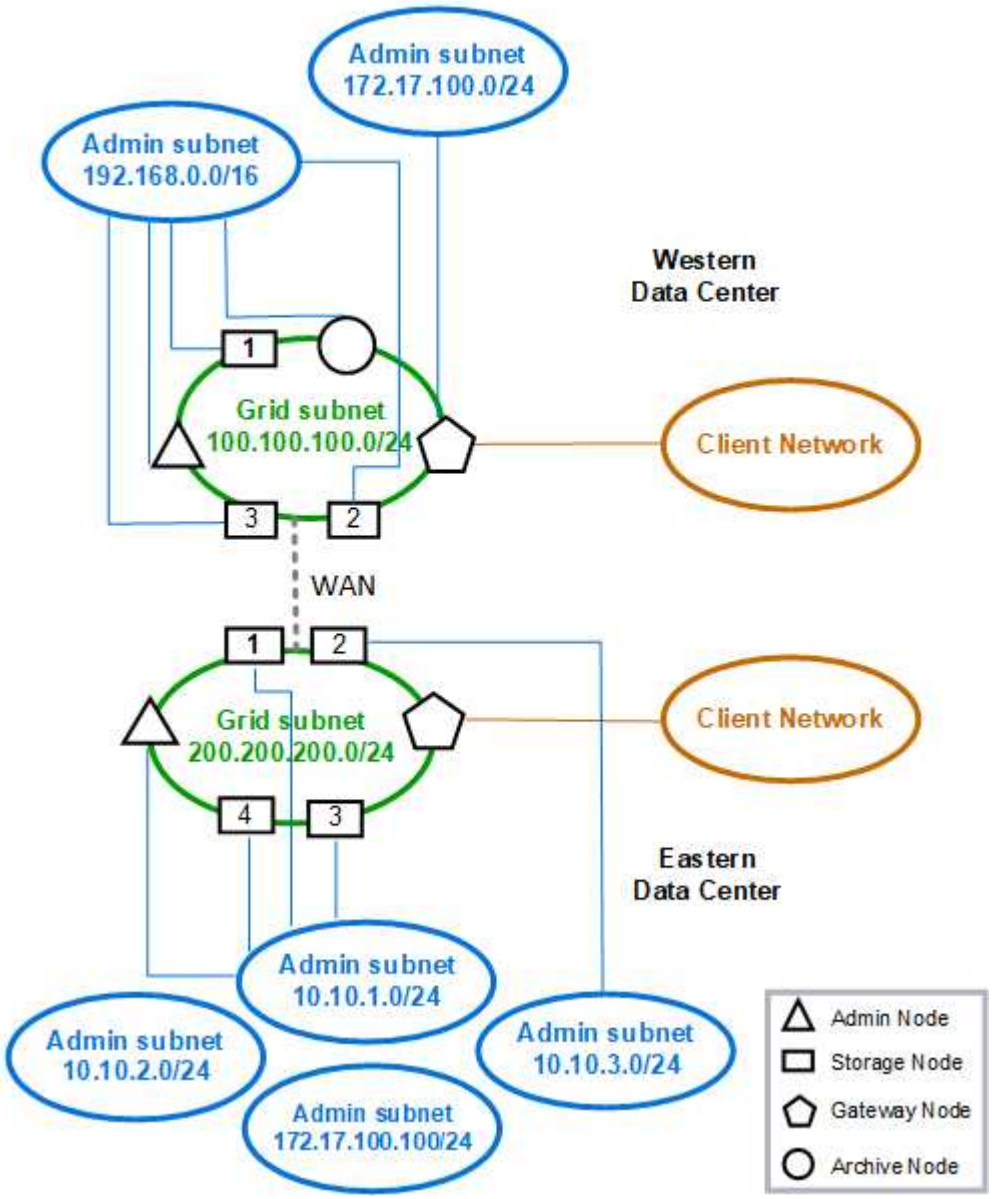
Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, eingeschränkten standortspezifischen Admin-Netzwerken und

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 eithersupport.netapp.com oder einem 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 Replizierung mit Cloud Mirror oder von Cloud-Storage-Pools.

Wenn StorageGRID mit den Standard-Routingregeln keinen Kontakt zu einem der bereitgestellten NTP- oder DNS-Server herstellen kann, wird automatisch versucht, in allen Netzwerken (Grid, Administrator 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 Administrator- und Client-Netzwerke zu konfigurieren, können Sie diese Netzwerke konfigurieren, wenn Sie Grid-Knoten während der Konfigurationsschritte genehmigen. Darüber hinaus können Sie diese Netzwerke konfigurieren, nachdem die Installation abgeschlossen wurde, indem Sie das Change IP-Tool verwenden, wie in den Recovery- und Wartungsanweisungen beschrieben.

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. Informationen zu Hochverfügbarkeitsgruppen finden Sie in der Anleitung zur Administration von StorageGRID.

Verwendung von NAT (Network Address Translation)

Verwenden Sie keine NAT (Network Address Translation) 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.

Verwandte Informationen

"Gittergrundierung"

"StorageGRID verwalten"

"Verwalten Sie erholen"

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 Netzwerk-IP-Adresse darf nicht 255.255.255.254 oder 255.255.255.255 (/31 oder /32 in CIDR-Notation) sein.
- Das durch eine Netzwerkschnittstelle definierte Subnetz-IP-Adresse und Subnetzmaske (CIDR) kann das Subnetz anderer Schnittstellen, die auf demselben Knoten konfiguriert sind, nicht überlappen.
- Das Grid-Netzwerk-Subnetz für jeden Node muss in der GNSL enthalten sein.
- Das Subnetz Admin-Netzwerk kann das Subnetz Grid-Netzwerk, das Subnetz Client-Netzwerk oder ein

beliebiges Subnetz in der GNSL nicht überlappen.

- Die Subnetze im AESL können nicht mit Teilnetzen im GNSL überlappen.
- Das Subnetz Client-Netzwerk kann das Subnetz Grid-Netzwerk, das Subnetz Admin-Netzwerk, ein beliebiges Subnetz in der GNSL oder ein beliebiges Subnetz in der AESL nicht 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.

Admin-Netzwerk

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

Typische Anwendungen des Admin-Netzwerks umfassen 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. Weitere Informationen zum Verwalten des Lastausgleichs und zum Verwalten nicht vertrauenswürdiger Clientnetzwerke finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Implementierungs-spezifische Netzwerküberlegungen

Je nach den verwendeten Implementierungsplattformen können weitere Überlegungen für Ihr StorageGRID-Netzwerkdesign erforderlich sein.

Grid-Nodes können wie folgt implementiert werden:

- Softwarebasierte Grid-Nodes, die als Virtual Machines im VMware vSphere Web Client implementiert sind
- Softwarebasierte Grid-Nodes, die in Docker Containern auf Linux Hosts implementiert werden
- Appliance-basierte Nodes

Weitere Informationen zu Gitterknoten finden Sie im Abschnitt „*Grid Primer*“.

Verwandte Informationen

"Gittergrundierung"

Linux Implementierungen

Das StorageGRID System wird unter Linux als Sammlung von Docker Containern ausgeführt, um Effizienz, Zuverlässigkeit und Sicherheit zu gewährleisten. Eine Docker-bezogene Netzwerkkonfiguration ist für ein 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/CentOS oder Ubuntu/Debian-Bereitstellungen.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Host-Netzwerkkonfiguration für Docker Implementierungen

Bevor Sie Ihre StorageGRID-Implementierung auf einer Docker-Container-Plattform starten, ermitteln Sie, welche Netzwerke (Grid, Administrator, Client) jeder Node verwenden soll. 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 IP-Adressen nicht gemeinsam nutzen.

- Öffnen Sie die erforderlichen Ports zum Host.

Empfehlungen für die minimale Bandbreite

In der folgenden Tabelle sind die Mindestempfehlungen für die jeweilige Art von StorageGRID Node und jeden Netzwerktyp aufgeführt. 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
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	1 Gbit/S	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.

Empfohlene Methoden zur Konfiguration physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung der StorageGRID-Bereitstellung finden Sie in den Informationen zur Konfiguration des Hostnetzwerks in den Installationsanweisungen für Ihre Linux-Plattform.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie 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. Zu den Plattform-Services gehören externe Services, die Integration von Suchvorgängen, Ereignisbenachrichtigungen und CloudMirror Replizierung ermöglichen.

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. In diesem Beispiel kann die Funktion UnTrusted Client Network verwendet werden, um eingehende Verbindungen einzuschränken.

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.

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

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

Ein anderer Port kann angegeben werden, wenn der Endpunkt erstellt oder bearbeitet wird.

Wenn Sie einen nicht transparenten Proxy-Server verwenden, müssen Sie auch Proxy-Einstellungen konfigurieren, damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einen Endpunkt im Internet. Weitere Informationen zum Konfigurieren der Proxy-Einstellungen finden Sie unter Verwalten von StorageGRID.

Weitere Informationen zu nicht vertrauenswürdigen Clientnetzwerken finden Sie in den Anweisungen zum Verwalten von StorageGRID. Weitere Informationen zu Plattform-Services finden Sie in der Anleitung zur Verwendung von Mandantenkonten. Weitere Informationen zu Cloud-Storage-Pools finden Sie in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Verwandte Informationen

"Referenz für Netzwerk-Ports"

"Gittergrundierung"

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"Objektmanagement mit ILM"

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 Ports finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

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 nach Abschluss der Installation verwenden. Weitere Informationen zu den Verfahren zur Netzwerkwartung finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Verwandte Informationen

"Verwalten Sie erholen"

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. Sie können DHCP während der Konfiguration nicht einrichten.

  > 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. Informationen zum Konfigurieren von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- 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. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise neu herstellen.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"Verwalten Sie erholen"

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.

Ermitteln Sie anhand der bereitgestellten Details für die interne Kommunikation zwischen Grid-Nodes und externe Kommunikation, wie die einzelnen erforderlichen Ports konfiguriert werden.

- "Interne Kommunikation mit Grid-Nodes"
- "Externe Kommunikation"

Interne Kommunikation mit Grid-Nodes

Die interne StorageGRID-Firewall erlaubt nur eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk, mit Ausnahme der Ports 22, 80, 123 und 443 (siehe Informationen zur externen Kommunikation). 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. Das erlauben von ICMP-Datenverkehr kann die Failover-Performance verbessern, wenn ein Grid-Knoten nicht erreicht werden kann.

Zusätzlich zu ICMP und den in der Tabelle aufgeführten Ports verwendet StorageGRID das Virtual Router Redundancy Protocol (VRRP). VRRP ist ein Internetprotokoll, das IP-Protokoll Nummer 112 verwendet. StorageGRID verwendet VRRP nur im Unicast-Modus. VRRP ist nur erforderlich, wenn HA-Gruppen (High Availability, Hochverfügbarkeit) konfiguriert sind.

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 Parameter für die Portumzuordnung und die Bereitstellungskonfiguration finden Sie in den Installationsanweisungen für Ihre Linux-Plattform.

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 der Implementierung finden Sie in den Installationsanweisungen für VMware.

Richtlinien für Appliance-Speicherknoten

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Weitere Informationen zur Port-Neuzuordnung von Appliances finden Sie in den Installationsanweisungen für Ihre Storage Appliance.

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.
1139	TCP	Storage-Nodes	Storage-Nodes	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Nodes	Storage-Nodes mit ADC	Reporting-, Audit- und Konfigurationsdaten verkehr.

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:
5353	UDP	Alle Nodes	Alle Nodes	Optional wird er für vollGrid-IP-Änderungen und für die primäre Admin Node-Erkennung während der Installation, Erweiterung und Recovery verwendet.
7001	TCP	Storage-Nodes	Storage-Nodes	Cassandra TLS zwischen Nodes-Cluster-Kommunikation

7443	TCP	Alle Nodes	Admin-Nodes	Interner Datenverkehr für Wartungsvorgänge und Fehlerberichte.
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.
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:
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"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

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.

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf beliebige Ports einschränken, können Sie über Load Balancer-Endpunkte den Zugriff auf benutzerdefinierte Ports zulassen. Die Funktion nicht vertrauenswürdige Client-Netzwerke kann verwendet werden, um nur den Zugriff auf Endpunktports des Load

Balancer zu ermöglichen.

> 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 keine Balancer-Endpunkte neu zuordnen. Informationen zum Ummappen von Ports finden Sie in den Installationsanweisungen für Ihre Plattform.

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

> Diese Liste enthält keine Ports, die als Load Balancer-Endpunkte konfiguriert werden können. Weitere Informationen finden Sie in den Anweisungen zum Konfigurieren von Load Balancer-Endpunkten.

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 das Domain Name System 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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
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.
111	TCP/UDP	Rpcbind	NFS Client	Admin-Nodes	Wird vom NFS-basierten Audit-Export verwendet (Portmap). **Hinweis:** dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist.
123	UDP	NTP	Primäre NTP-Knoten	Externe NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Nodes synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
137	UDP	NetBIOS	SMB-Client	Admin-Nodes	Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen. **Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.
138	UDP	NetBIOS	SMB-Client	Admin-Nodes	Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen. **Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.
139	TCP	SMB	SMB-Client	Admin-Nodes	Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen. **Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
161	TCP/UDP	SNMP	SNMP-Client	Alle Nodes	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. **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. **Hinweis:** um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Nodes	Benachrichtigungsziele	Ausgehende SNMP-Benachrichtigungen und Traps standardmäßig auf UDP-Port 162. **Hinweis:** dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.
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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
443	TCP	HTTPS	Browser	Admin-Nodes	Wird von Webbrowsern und Management-API-Clients für den Zugriff auf Grid Manager und Tenant Manager verwendet.
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.
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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
903	TCP	NFS	NFS Client	Admin-Nodes	Wird vom NFS-basierten Audit-Export verwendet (`rpc.mountd`). **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 (nfs). **Hinweis:** dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist.
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.
8082	TCP	HTTPS	S3-Clients	Gateway-Nodes	Externer S3-Datenverkehr zu Gateway Nodes (HTTPS).
8083	TCP	HTTPS	Swift Clients	Gateway-Nodes	Swift-bezogener externer Datenverkehr zu Gateway Nodes (HTTPS).
8084	TCP	HTTP	S3-Clients	Gateway-Nodes	Externer S3-Datenverkehr zu Gateway Nodes (HTTP).
8085	TCP	HTTP	Swift Clients	Gateway-Nodes	Swift-bezogener externer Datenverkehr zu Gateway Nodes (HTTP).
8443	TCP	HTTPS	Browser	Admin-Nodes	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.
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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
9091	TCP	HTTPS	Externer Grafana-Service	Admin-Nodes	Wird von externen Grafana Services für sicheren Zugriff auf den StorageGRID Prometheus Service verwendet. **Hinweis:** dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist.
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	Externer S3-Datenverkehr zu Storage-Nodes (HTTPS).
18083	TCP	HTTPS	Swift Clients	Storage-Nodes	Swift-bezogener externer Datenverkehr zu Speicherknoten (HTTPS).
18084	TCP	HTTP	S3-Clients	Storage-Nodes	Externer S3-Datenverkehr zu Storage Nodes (HTTP).
18085	TCP	HTTP	Swift Clients	Storage-Nodes	Swift-bezogener externer Datenverkehr zu Speicherknoten (HTTP).

Verwandte Informationen

"Interne Kommunikation mit Grid-Nodes"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Installation und Upgrade von Software

Installieren Sie Red hat Enterprise Linux oder CentOS

Erfahren Sie mehr über die Installation von StorageGRID Software in Red hat Enterprise Linux oder CentOS Implementierungen.

- "Übersicht über die Installation"
- "Planung und Vorbereitung"
- "Implementierung virtueller Grid-Nodes"
- "Grid wird konfiguriert und die Installation abgeschlossen"
- "Automatisierung der Installation"
- "Überblick über DIE REST API zur Installation"
- "Weitere Schritte"
- "Fehlerbehebung bei Installationsproblemen"
- "Beispiel /etc/sysconfig/Network-scripts"

Übersicht über die Installation

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 des StorageGRID Networking, damit Sie Ihr Netzwerk entsprechend konfigurieren können. Weitere Informationen finden Sie in den StorageGRID Netzwerkrichtlinien.
    - 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 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 Installationsverfahren für StorageGRID enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

3. **Konfiguration**: Wenn alle Knoten bereitgestellt wurden, verwenden Sie den StorageGRIDGrid 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 von Docker und dem StorageGRID Host Service sowie 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.

Verwandte Informationen

"Planung und Vorbereitung"

"Implementierung virtueller Grid-Nodes"

"Grid wird konfiguriert und die Installation abgeschlossen"

"Automatisierung der Installation"

"Überblick über DIE REST API zur Installation"

"Netzwerkrichtlinien"

Planung und Vorbereitung

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 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:

- Informieren Sie sich über die Computing-Anforderungen von StorageGRID, 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.
- Informieren Sie sich über die Anforderungen für die Node-Migration, wenn Sie geplante Wartungsarbeiten an physischen Hosts ohne Service-Unterbrechung durchführen möchten.
- Sammeln Sie alle Netzwerkinformationen im Voraus. Wenn Sie nicht DHCP verwenden, sammeln Sie die IP-Adressen, die jedem Grid-Node zugewiesen werden sollen, und die IP-Adressen des Domain Name System (DNS) und der von Ihnen verwendeten NTP-Server (Network Time Protocol).
- Installation, Anschluss und Konfiguration der gesamten erforderlichen Hardware – einschließlich aller StorageGRID Appliances – gemäß den Spezifikationen

> Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im Installationsverfahren für StorageGRID enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

- Legen Sie fest, welche der verfügbaren Implementierungs- und Konfigurationstools Sie verwenden möchten.

Verwandte Informationen

"Netzwerkrichtlinien"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

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	Sie müssen das StorageGRID-Installationsarchiv herunterladen und die Dateien extrahieren.

Element	Hinweise
Service-Laptop	Das StorageGRID System wird über einen Service-Laptop installiert. Der Service-Laptop muss Folgendes haben: • Netzwerkport • SSH-Client (z. B. PuTTY) • Unterstützter Webbrowser
StorageGRID-Dokumentation	• Versionshinweise • Anweisungen für die Administration von StorageGRID

Verwandte Informationen

"Herunterladen und Extrahieren der StorageGRID-Installationsdateien"

"Anforderungen an einen Webbrowser"

"StorageGRID verwalten"

"Versionshinweise"

Herunterladen und Extrahieren der StorageGRID-Installationsdateien

Sie müssen das StorageGRID-Installationsarchiv herunterladen und die erforderlichen Dateien extrahieren.

Schritte

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "NetApp Downloads: 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 Warnung/MusterLeseanweisung 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 den Recovery- und Wartungsanleitungen.

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.
6. Wählen Sie in der Spalte **Install StorageGRID** die entsprechende Software aus.

   Laden Sie die herunter `.tgz` Oder `.zip` Archivieren Sie die Datei für Ihre Plattform.

   Die komprimierten Dateien enthalten die RPM-Dateien und Skripte für Red hat Enterprise Linux oder CentOS.

Verwenden Sie die `.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 `configure-storagegrid.py` Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` 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.

Verwandte Informationen

"Verwalten Sie erholen"

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.

Weitere Informationen zu unterstützten Servern finden Sie in der Interoperabilitäts-Matrix.

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 dediziert für die Ausführung von StorageGRID sind (nicht empfohlen), sollten Sie die Ressourcenanforderungen der anderen Applikationen berücksichtigen.

> 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 und zum Monitoring der CPU- und Arbeitsspeicherauslastung finden Sie in den Anweisungen für die Administration, das Monitoring und das Upgrade von 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 die Informationen über Speicheranforderungen.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Storage- und Performance-Anforderungen erfüllt"

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

"Software-Upgrade"

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. Es ist möglich, Shared- oder lokalen RAID-Storage für eine beliebige Storage-Kategorie zu verwenden. Wenn Sie jedoch die Möglichkeit zur Migration der StorageGRID Nodes nutzen möchten, müssen Sie sowohl Systemdaten als auch Objektdaten auf einem Shared Storage speichern.

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 AFF Storage nutzen

Wenn der StorageGRID-Node Storage verwendet, der einem NetApp AFF 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 Speicherknoten 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
Docker Storage-Pool	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.	4,000 GB 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
Admin-Node-Tabellen	Systemdaten	1 für jeden Admin-Node auf diesem Host	200 GB

Je nach konfiguriertem Audit Level, Größe der Benutzereingaben wie z. B. S3-Objektschlüsselname und wie viele Audit-Protokoll-Daten Sie erhalten müssen, müssen Sie möglicherweise die Größe der Audit-Protokoll-LUN auf jedem Admin-Node erhöhen. In der Regel generiert ein Grid etwa 1 KB Audit-Daten pro S3-Betrieb. Dies bedeutet, dass ein 200 GB-LUN 70 Millionen Operationen pro Tag und 800 Operationen pro Sekunde für zwei bis drei Tage unterstützen würde.

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 zum Wiederherstellen von Grid-Nodes verwendet werden. Beachten Sie stattdessen die Recovery- und Wartungsabläufe 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)	*Nicht zutreffend*
Gateway-Node	100 GB	90 GB	*Nicht zutreffend*
Archiv-Node	100 GB	90 GB	*Nicht zutreffend*

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	4,000 GB
Admin-Node	`/var/local` Datenmenge	1	90 GB
Admin-Node	Prüfprotokolle für Admin-Node	1	200 GB

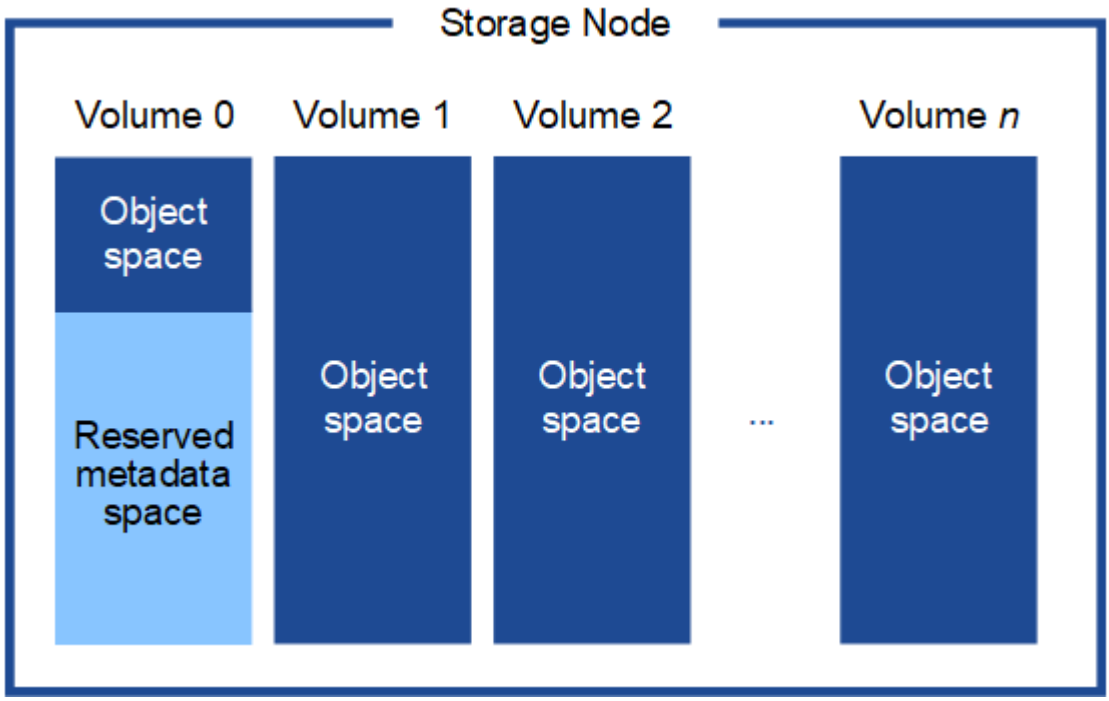
Node-Typ	LUN-Zweck	Anzahl LUNs	Die LUN-Größe
Admin-Node	Admin-Node-Tabellen	1	200 GB
Gateway-Node	`/var/local` Datenmenge	1	90 GB
Gesamt		**9**	**Container-Pool:** 300 GB **Systemdaten:** 670 GB **Objektdaten:** 12,000 GB

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 ein neues StorageGRID 11.5-System installieren und jeder Speicherknoten 128 GB oder mehr RAM hat, sollten Sie Volume 0 8 TB oder mehr zuweisen. 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 Anweisungen zum Verwalten von StorageGRID und suchen nach „`managing Objekt-Metadaten-Storage`“.

"StorageGRID verwalten"

Verwandte Informationen

"Anforderungen für die Container-Migration für Nodes"

"Verwalten Sie erholen"

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 einfach alle StorageGRID Nodes nacheinander auf einen anderen Host, bevor Sie den physischen Host offline schalten. 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 Netzwerkschnittstellennnamen 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-Ebene die VM-Migration unterstützt, ist diese Funktion anstelle der Node-Migrationsfunktion von StorageGRID wahrscheinlich sinnvoll. In diesem Fall können Sie diese zusätzlichen Anforderungen ignorieren.

Bevor Sie eine Migration oder eine Hypervisor-Wartung durchführen, müssen Sie die Nodes ordnungsgemäß herunterfahren. Informationen zum Herunterfahren eines Grid-Node finden Sie in den Anweisungen zur Recovery und Wartung.

VMware Live Migration wird nicht unterstützt

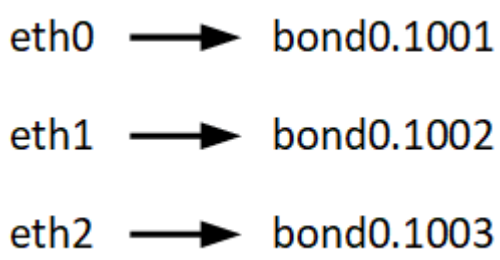
OpenStack Live Migration und VMware Live vMotion sorgen dafür, dass die Virtual Machine-Uhr springen und für Grid-Nodes jeglicher Art nicht unterstützt wird. Obwohl selten, falsche Uhrzeiten können zum Verlust von Daten oder Konfigurations-Updates führen.

Cold-Migration wird unterstützt. Bei der „Cold"-Migration sollten Sie die StorageGRID Nodes herunterfahren, bevor Sie sie zwischen Hosts migrieren. Siehe das Verfahren zum Herunterfahren eines Grid-Node in der Wiederherstellungsanleitung und Wartungsanleitung.

Konsistente Namen von Netzwerkschnittstellen

Um einen Node von einem Host zum anderen zu verschieben, muss der StorageGRID-Hostdienst die Gewissheit haben, dass die externe Netzwerkverbindung, die der Node an seinem aktuellen Standort besitzt, an dem 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:



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, um eine konsistente Netzwerkschnittstelle zu erreichen, die über mehrere Hosts hinweg benennt; einige Beispiele finden Sie unter „`Konfigurieren des Hostnetzwerks`".

Shared Storage

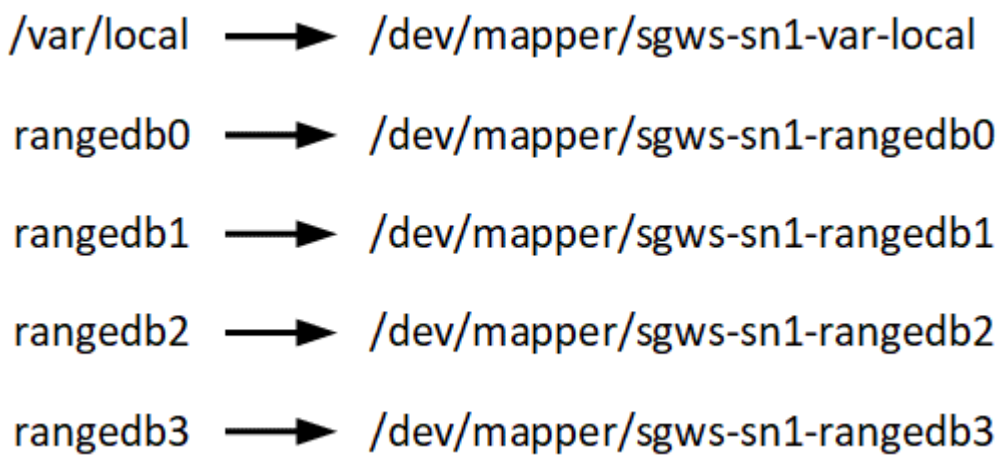
Für schnelle Node-Migrationen mit geringem Overhead werden Node-Daten durch die StorageGRID Node-Migrationsfunktion nicht physisch verschoben. Stattdessen werden die Node-Migration als Export- und Importpaar durchgeführt:

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 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 Blockgerätnamen zu liefern, die auf allen Hosts verfügbar sind.



Verwandte Informationen

"Konfigurieren des Hostnetzwerks"

"Verwalten Sie erholen"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

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 daran interessiert sind, Ihre StorageGRID-Implementierung vollständig oder teilweise zu automatisieren, lesen Sie vor Beginn des Installationsprozesses „`Automatisieren der Installation`“ durch.

Verwandte Informationen

"Überblick über DIE REST API zur Installation"

"Automatisierung der Installation"

Vorbereiten der Hosts

Sie müssen die folgenden Schritte durchführen, um Ihre physischen oder virtuellen Hosts für StorageGRID vorzubereiten. Beachten Sie, dass Sie viele oder alle dieser Schritte mit Standard-Server-Konfigurations-Frameworks wie Ansible, Puppet oder Chef automatisieren können.

Verwandte Informationen

"Automatisierung der Installation und Konfiguration des StorageGRID Host Service"

Linux Wird Installiert

Sie müssen Red hat Enterprise Linux oder CentOS Linux auf allen Grid Hosts installieren. Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

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-Repositorys haben, einschließlich des Extras-Kanals.

   Möglicherweise benötigen Sie diese zusätzlichen Pakete später in diesem Installationsvorgang.

3. Wenn Swap aktiviert ist:

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

   b. Entfernen Sie alle Swap-Einträge aus `/etc/fstab` Um die Einstellungen zu erhalten.

   Wenn Sie den Auslagerungsaustausch nicht vollständig deaktivieren, kann die Leistung erheblich gesenkt werden.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Konfigurieren des Hostnetzwerks

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.

Was Sie benötigen

- Sie haben sich die StorageGRID Netzwerkrichtlinien durchgelesen.

  "Netzwerkrichtlinien"

- Sie haben die Informationen zu den Anforderungen für die Container-Migration von Nodes überprüft.

  "Anforderungen für die Container-Migration für Nodes"

- Wenn Sie virtuelle Hosts verwenden, haben Sie vor der Konfiguration des Hostnetzwerks die Überlegungen und Empfehlungen zum Klonen von MAC-Adressen gelesen.

  "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"

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 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 den Hosts um virtuelle Maschinen handelt und Sie einen oder zwei StorageGRID-Nodes für jeden Host implementieren, können Sie im Hypervisor einfach die richtige Anzahl an Netzwerkschnittstellen 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 kein der folgenden 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.

Verwandte Informationen

"Netzwerkrichtlinien"

"Anforderungen für die Container-Migration für Nodes"

"Erstellen von Knoten-Konfigurationsdateien"

Überlegungen und Empfehlungen zum Klonen von MAC-Adressen

Das Klonen VON MAC-Adressen führt dazu, dass der Docker-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 Docker Container die MAC-Adresse der dedizierten NIC auf dem Host nutzen soll, können Sie keine Kompromissmodus-Netzwerkkonfigurationen 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 Docker 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 kein Klonen der MAC-Adresse verwenden möchten und lieber alle Schnittstellen Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen empfangen und übertragen möchten, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene der virtuellen Switch- und Portgruppen auf **Accept** für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen eingestellt 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

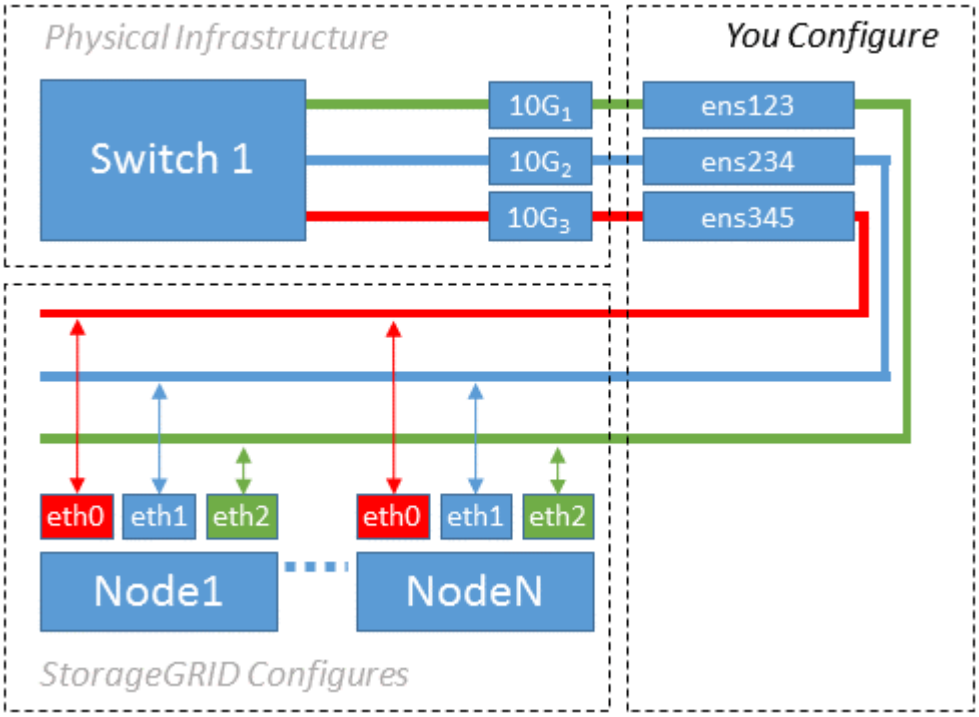
Beispiel für das MAC-Klonen bei einem Host mit einer MAC-Adresse von 11:22:33:44:55:66 für die Schnittstelle ensens256 und die folgenden Schlüssel in der Node-Konfigurationsdatei:

- `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 Betriebssystem Linux erstellt den `ensXYZ` Schnittstellen werden automatisch während der Installation oder beim Booten oder beim Hot-Added-Schnittstellen bereitgestellt. Es ist keine andere Konfiguration erforderlich als sicherzustellen, dass die Schnittstellen nach dem Booten automatisch eingerichtet werden. Sie

müssen herausfinden, welche `ensXYZ` Entspricht dem StorageGRID-Netzwerk (Grid, Administrator oder Client), sodass 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 in den entsprechenden VLANs platzieren.

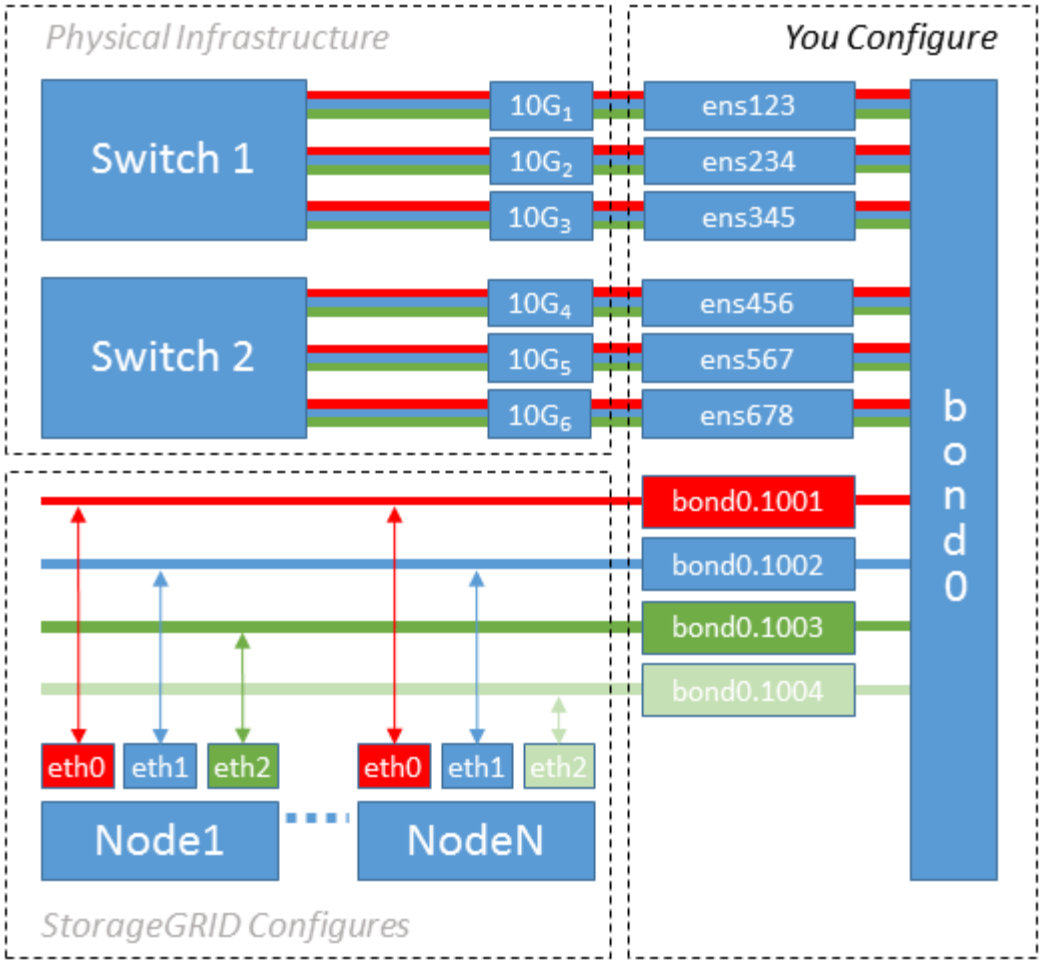
Beispiel 2: LACP Bond mit VLANs

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.

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 zugehörisches „`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 wird konfiguriert

Jedem Host müssen Block Storage Volumes zugewiesen werden.

Was Sie benötigen

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 „SStorage-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 keine dieser Volumes partitionieren, formatieren oder mounten; Sie 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 Multipath-Aliase in Betracht ziehen `/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-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

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 von StorageGRID-Node-Migration einrichten und unter Verwendung von Device Mapper Multipathing einen gemeinsamen Speicher 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

"Installation Von Docker"

Konfiguration 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-Volume zu verwenden und über genügend Speicherplatz auf der Host-Partition mit verfügen `/var/lib`.

Schritte

1. Dateisystem auf dem Docker-Storage-Volume erstellen:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Mounten des Docker-Storage-Volumes:

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

3. Fügen Sie einen Eintrag für Docker-Storage-Volume-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 Red hat Enterprise Linux oder CentOS 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 1.10.3 oder höher sein.

```
Client:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64

Server:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64
```

Verwandte Informationen

"Hostspeicher wird konfiguriert"

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 virtueller Grid-Nodes

Zum Bereitstellen von virtuellen Grid-Nodes auf Red hat Enterprise Linux- oder CentOS-Hosts erstellen Sie Node-Konfigurationsdateien für alle Nodes, validieren die Dateien und starten den StorageGRID-Hostdienst, der die Nodes startet. Wenn Sie Speicherknoten von StorageGRID Appliances bereitstellen müssen, lesen Sie die Installations- und Wartungsanleitung für die Appliance, nachdem Sie alle virtuellen Knoten bereitgestellt haben.

- "Erstellen von Knoten-Konfigurationsdateien"
- "Überprüfung der StorageGRID-Konfiguration"
- "Starten des StorageGRID Host Service"

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG5600 Storage Appliances"

"SG5700 Storage-Appliances"

"SG6000 Storage-Appliances"

Erstellen von Knoten-Konfigurationsdateien

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. Die 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 benamе 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` Wenn diese Namenskonventionen nicht eingehalten werden, wird dies vom Host-Service nicht geparst.

Wenn das Grid eine Topologie mit mehreren Standorten geplant ist, ist unter Umständen ein typisches Benennungsschema für Node möglich:

```
site-nodetype-nodenumber.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	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. Siehe „`wie Grid Nodes den primären Admin-Node ermitteln`“. **Hinweis**: Dieser Wert wird auf dem primären Admin-Node ignoriert und kann möglicherweise nicht verwendet werden.
ADMIN_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT
ADMIN_NETWORK_ESL	O	Kommagetrennte Liste von Subnetzen in CIDR-Notation, mit denen dieser Knoten über das Admin Network-Gateway kommunizieren soll. Beispiel: 172.16.0.0/21,172.17.0.0/21

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_GATEWAY	O (**R**)	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. **Hinweis**: Dieser Parameter ist erforderlich, wenn ADMIN_NETWORK_ESL angegeben wird. Beispiele: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_IP	O	IPv4-Adresse dieses Knotens im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_MAC	O	Die MAC-Adresse für die Admin-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden. Beispiel: b2:9c:02:c2:27:10

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_MASKE	O	IPv4-Netmask für diesen Node im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 255.255.255.0 • 255.255.248.0
ADMIN_NETWORK_MTU	O	Die maximale Übertragungseinheit (MTU) für diesen Knoten im Admin-Netzwerk. Geben Sie nicht an, ob ADMIN_NETWORK_CONFIG = DHCP ist. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 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. **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. Beispiele: • 1500 • 8192

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_TARGET	BP	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. **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). **Best Practice:** Geben Sie einen Wert an, auch 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. Beispiele: • Bond0.1002 • Ensen256
ADMIN_NETWORK_TARGET_TYPE	O	Schnittstelle (Dies ist der einzige unterstützte Wert.)

Taste	R, BP ODER O?	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 promiskuious-Modus erforderlich wäre, verwenden Sie stattdessen DEN ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC-Adressen finden Sie in den Überlegungen und Empfehlungen zum Klonen von MAC-Adressen. "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"
ADMIN_ROLLE	**R**	Primärer oder nicht primärer Storage Dieser Schlüssel ist nur erforderlich, wenn NODE_TYPE = VM_Admin_Node; nicht für andere Node-Typen angeben.

Taste	R, BP ODER O?	Wert
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 Knoten mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-audit-logs`

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_RANGEDB_00 BLOCK_DEVICE_RANGEDB_01 BLOCK_DEVICE_RANGEDB_02 BLOCK_DEVICE_RANGEDB_03 BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_05 BLOCK_DEVICE_RANGEDB_06 BLOCK_DEVICE_RANGEDB_07 BLOCK_DEVICE_RANGEDB_08 BLOCK_DEVICE_RANGEDB_09 BLOCK_DEVICE_RANGEDB_10 BLOCK_DEVICE_RANGEDB_11 BLOCK_DEVICE_RANGEDB_12 BLOCK_DEVICE_RANGEDB_13 BLOCK_DEVICE_RANGEDB_14 BLOCK_DEVICE_RANGEDB_15	**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 Node-Typen an. Es ist nur BLOCK_DEVICE_RANGEDB_00 erforderlich; der Rest ist optional. Das für BLOCK_DEVICE_RANGEDB_00 angegebene Blockgerät muss mindestens 4 TB betragen; die anderen können kleiner sein. **Hinweis**: Keine Lücken hinterlassen. Wenn Sie BLOCK_DEVICE_RANGEDB_05 angeben, müssen Sie auch BLOCK_DEVICE_RANGEDB_04 angeben. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-rangedb-0`

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_TABLES	**R**	Pfad und Name der Sonderdatei des Blockgerätes, die dieser Knoten für die dauerhafte Speicherung von Datenbanktabellen verwendet. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-tables`
BLOCK_DEVICE_VAR_LOCAL	**R**	Pfad und Name der Sonderdatei für das Blockgerät wird dieser Node für seinen persistenten Speicher /var/local verwenden. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-var-local`
CLIENT_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_GATEWAY	O	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. Beispiele: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_IP	O	IPv4-Adresse dieses Knotens im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_MAC	O	Die MAC-Adresse für die Client-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden. Beispiel: b2:9c:02:c2:27:20

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_MASK	O	IPv4-Netzmaske für diesen Knoten im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 255.255.255.0 • 255.255.248.0
CLIENT_NETWORK_MTU	O	Die maximale Übertragungseinheit (MTU) für diesen Knoten im Client-Netzwerk. Geben Sie nicht an, ob CLIENT_NETWORK_CONFIG = DHCP ist. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 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. **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. Beispiele: • 1500 • 8192

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_TARGET	BP	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. **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). **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. Beispiele: • Bond0.1003 • Ens423
CLIENT_NETWORK_TARGET_TYPE	O	Schnittstelle (Dieser Wert wird nur unterstützt.)

Taste	R, BP ODER O?	Wert
CLIENT_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 Client-Netzwerk verwenden kann. **Best Practice:** in Netzwerken, in denen der promiskuious-Modus erforderlich wäre, verwenden Sie stattdessen DEN CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC-Adressen finden Sie in den Überlegungen und Empfehlungen zum Klonen von MAC-Adressen. "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"
GRID_NETWORK_CONFIG	BP	STATISCH oder DHCP (Ist standardmäßig STATISCH, wenn nicht angegeben.)
GRID_NETWORK_GATEWAY	**R**	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. 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.

Taste	R, BP ODER O?	Wert
GRID_NETWORK_IP	**R**	IPv4-Adresse dieses Knotens im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 1.1.1.1 • 10.224.4.81
GRID_NETWORK_MAC	O	Die MAC-Adresse für die Grid-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden. Beispiel: b2:9c:02:c2:27:30
GRID_NETWORK_MASKE	O	IPv4-Netzmaske für diesen Knoten im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 255.255.255.0 • 255.255.248.0

Taste	R, BP ODER O?	Wert
GRID_NETWORK_MTU	O	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. 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. **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. **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 identisch sein. Beispiele: • 1500 • 8192

Taste	R, BP ODER O?	Wert
GRID_NETWORK_TARGET	**R**	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. **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). Beispiele: • Bond0.1001 • Ens192
GRID_NETWORK_TARGET_TYPE	O	Schnittstelle (Dies ist der einzige unterstützte Wert.)

Taste	R, BP ODER O?	Wert
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	Richtig oder falsch 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. **Best Practice:** in Netzwerken, in denen der promiskuious-Modus erforderlich wäre, verwenden Sie stattdessen DEN GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC-Adressen finden Sie in den Überlegungen und Empfehlungen zum Klonen von MAC-Adressen. "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"

Taste	R, BP ODER O?	Wert
MAXIMUM_RAM	O	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. **Hinweis**: Der RAM-Wert wirkt sich auf den tatsächlich reservierten Metadatenspeicherplatz eines Knotens aus. Eine Beschreibung des reservierten Speicherplatzes für Metadaten finden Sie in der Anleitung zum Verwalten von StorageGRID. Das Format für dieses Feld lautet `<number><unit>`, Wo `<unit>` Kann sein `b`, `k`, `m`, Oder `g`. Beispiele: 24 g 38654705664b **Hinweis**: Wenn Sie diese Option verwenden möchten, müssen Sie Kernel-Unterstützung für Speicher-cgroups aktivieren.
NODE_TYPE	**R**	Node-Typ: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway

Taste	R, BP ODER O?	Wert
PORT_NEU ZUORDNEN	O	Ordnet alle von einem Node verwendeten Ports für interne Grid Node-Kommunikation oder externe Kommunikation neu zu. Ports müssen neu zugeordnet werden, wenn Netzwerkrichtlinien eines oder mehrere von StorageGRID verwendete Ports beschränken. Dies wird unter „`Kommunikation mit internen Grid-Nodes`“ oder „`Externe Kommunikation`“ beschrieben. **WICHTIG**: Die Ports, die Sie für die Konfiguration von Load Balancer-Endpunkten planen, nicht neu zuordnen. **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. 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. Beispiel: `PORT_REMAP = client/tcp/18082/443`

Taste	R, BP ODER O?	Wert
PORT_REMAP_INBOUND	O	Ordnet die eingehende Kommunikation dem angegebenen Port erneut zu. Wenn Sie PORT_REMAP_INBOUND angeben, jedoch keinen Wert für PORT_REMAP angeben, wird die ausgehende Kommunikation für den Port nicht geändert. **WICHTIG**: Die Ports, die Sie für die Konfiguration von Load Balancer-Endpunkten planen, nicht neu zuordnen. 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. Beispiel: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Verwandte Informationen

"Ermitteln der primären Admin-Node durch Grid-Nodes"

"Netzwerkrichtlinien"

"StorageGRID verwalten"

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 mit einem Multicast Domain Name System (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 jedoch nicht normalerweise über Subnetze routingfähig ist, können Nodes in anderen Subnetzen die IP-Adresse des primären Admin-Node nicht direkt erfassen.

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-Netzwerkaddressinformationen (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/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

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

Beispiel für Speicherknoten

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-sn1.conf`

Beispieldateiinhalt:

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

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

Beispiel für Archivknoten

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-arc1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-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`

Beispieldateiinhalt:

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

Beispiel für einen nicht-primären Admin-Node

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-adm2.conf`

Beispieldateiinhalt:

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

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

Überprüfung der StorageGRID-Konfiguration

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

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

Starten des 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
```

Führen Sie für jeden Node, der den Status „`not-running`“ oder „`Stoured`“ zurückgibt, den folgenden Befehl aus:

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

3. 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 wird konfiguriert und die Installation abgeschlossen

Die Installation wird durch Konfiguration des StorageGRID-Systems vom Grid-Manager auf dem primären Admin-Node abgeschlossen.

- "Navigieren zum Grid Manager"
- "Angeben der StorageGRID-Lizenzinformationen"
- "Hinzufügen von Sites"
- "Angeben von Grid-Netzwerknetzen"
- "Genehmigung ausstehender Grid-Knoten"
- "Angeben von Informationen zum Network Time Protocol-Server"
- "Angeben von Informationen zum DNS-Server"
- "Festlegen der Passwörter für das StorageGRID-System"
- "Überprüfung Ihrer Konfiguration und Abschluss der Installation"
- "Richtlinien nach der Installation"

Navigieren zum Grid Manager

Mit dem Grid Manager können Sie alle Informationen definieren, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Was Sie benötigen

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`

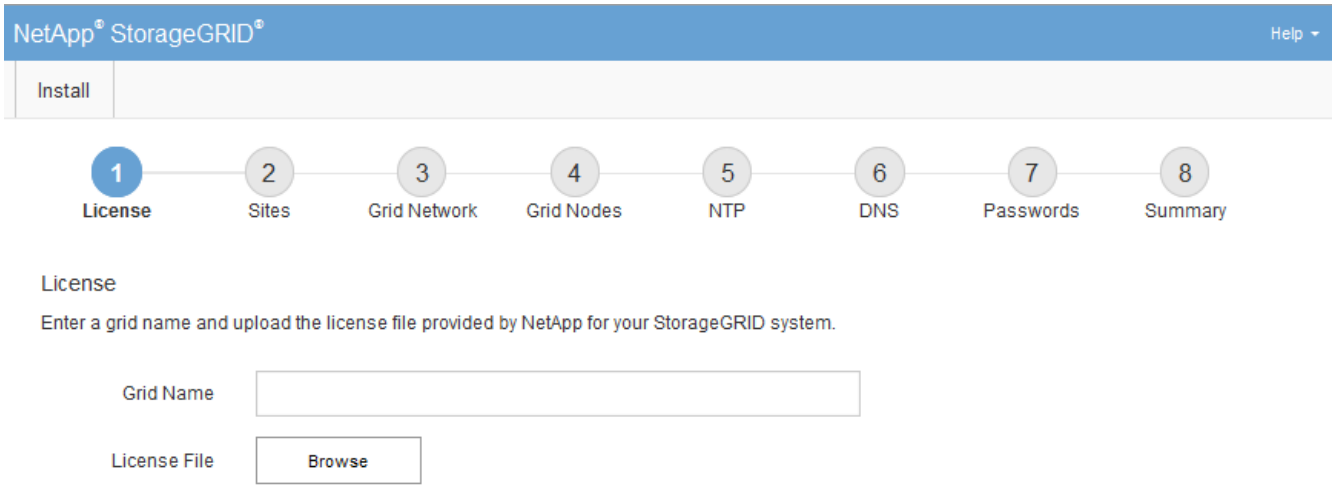
Alternativ können Sie auf den Grid Manager an Port 8443 zugreifen:

`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. Klicken Sie auf **StorageGRID-System installieren**.

   Die Seite zum Konfigurieren eines StorageGRID-Systems wird angezeigt.



Angeben der StorageGRID-Lizenzinformationen

Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Schritte

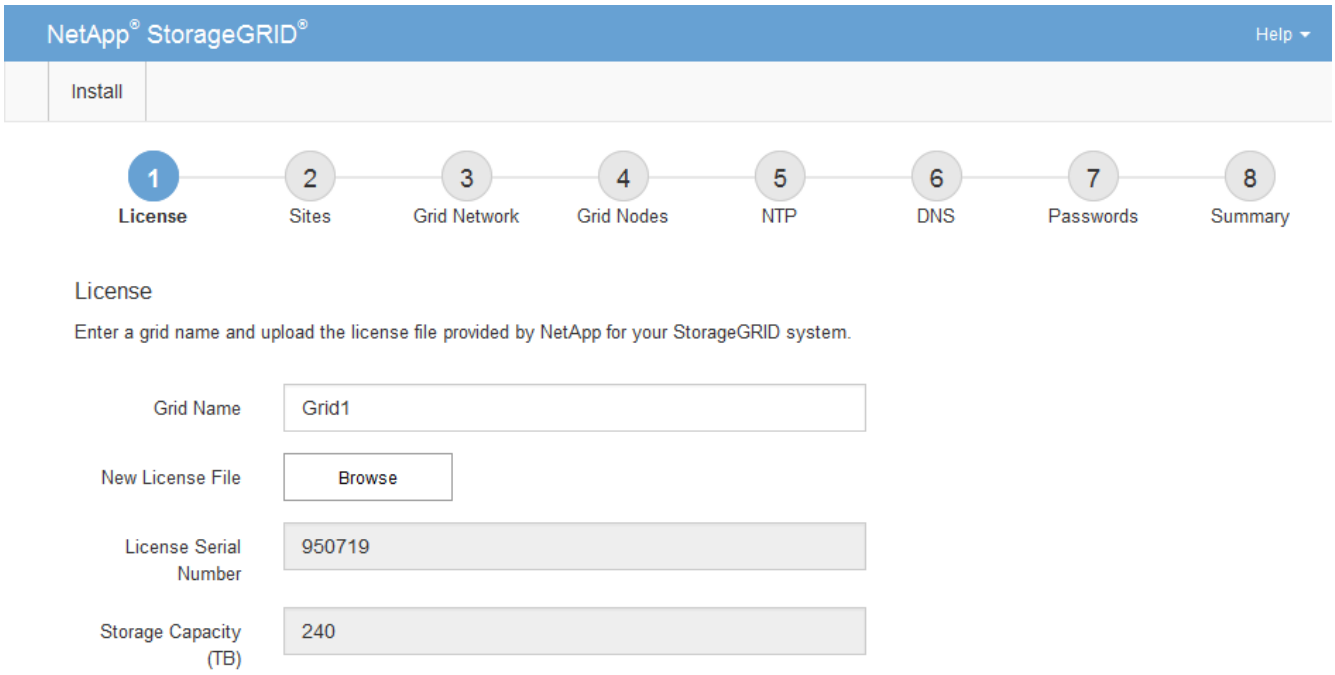
1. Geben Sie auf der Seite Lizenz einen aussagekräftigen Namen für Ihr StorageGRID-System in **Rastername** ein.

   Nach der Installation wird der Name oben im Menü Nodes angezeigt.

2. Klicken Sie auf **Durchsuchen** und suchen Sie die NetApp Lizenzdatei (`NLFunique_id.txt`Und klicken Sie auf **Öffnen**.

   Die Lizenzdatei wird validiert, die Seriennummer und die lizenzierte Speicherkapazität werden 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.



3. Klicken Sie Auf **Weiter**.

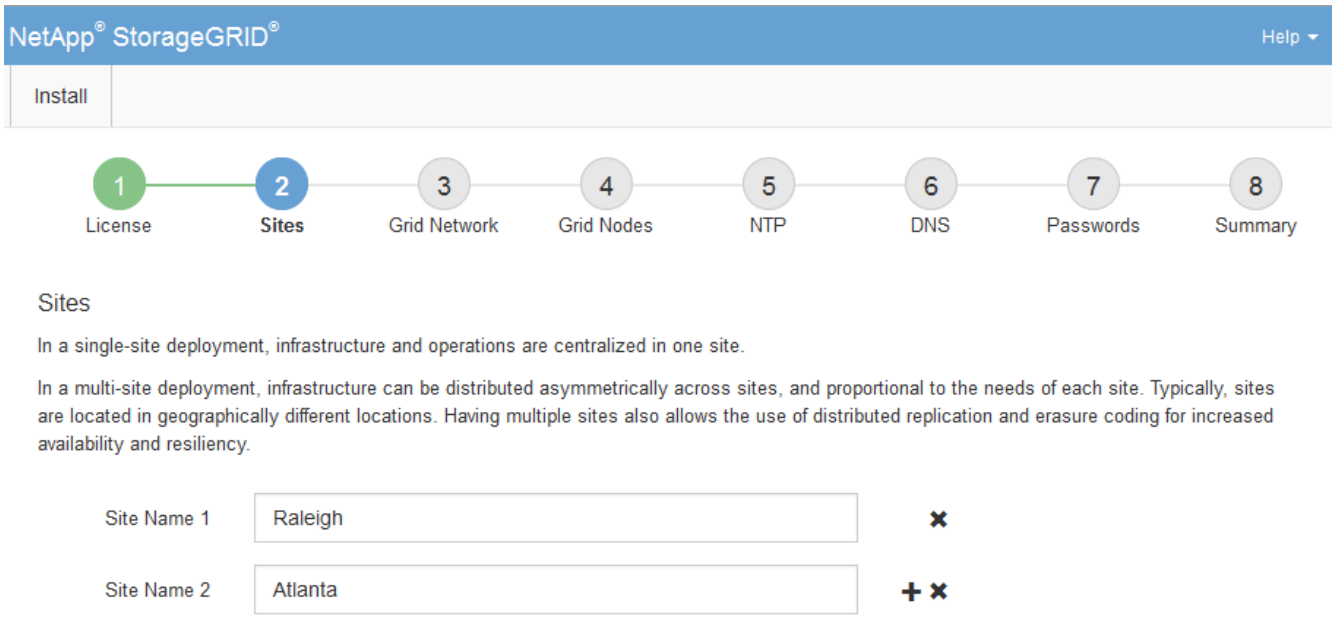
Hinzufügen von Sites

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.



3. Klicken Sie Auf **Weiter**.

Angeben von Grid-Netzwerknetzen

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

Über diese Aufgabe

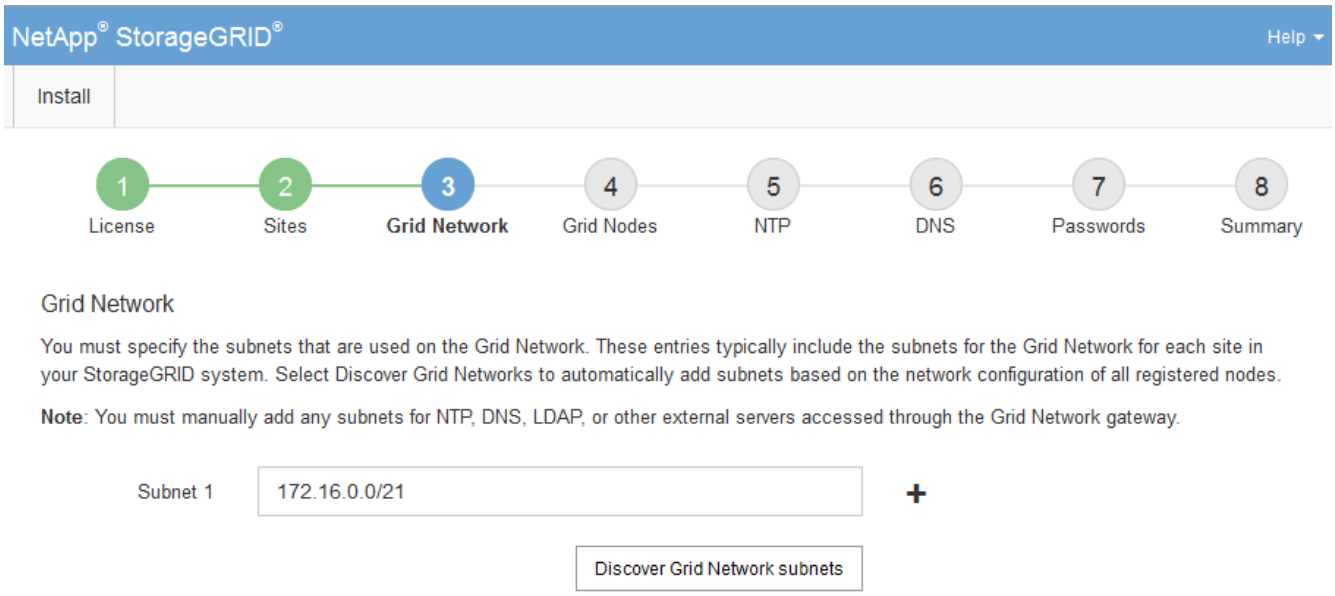
Die Subnetzeinträge enthalten die Subnetze für das Grid-Netzwerk für jeden Standort im StorageGRID-System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen.

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 **Netznetze-Subnetze ermitteln**, um die Netznetzwerksubnetz-Liste automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die beim Grid Manager registriert sind.



3. Klicken Sie Auf **Weiter**.

Genehmigung ausstehender Grid-Knoten

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

Was Sie benötigen

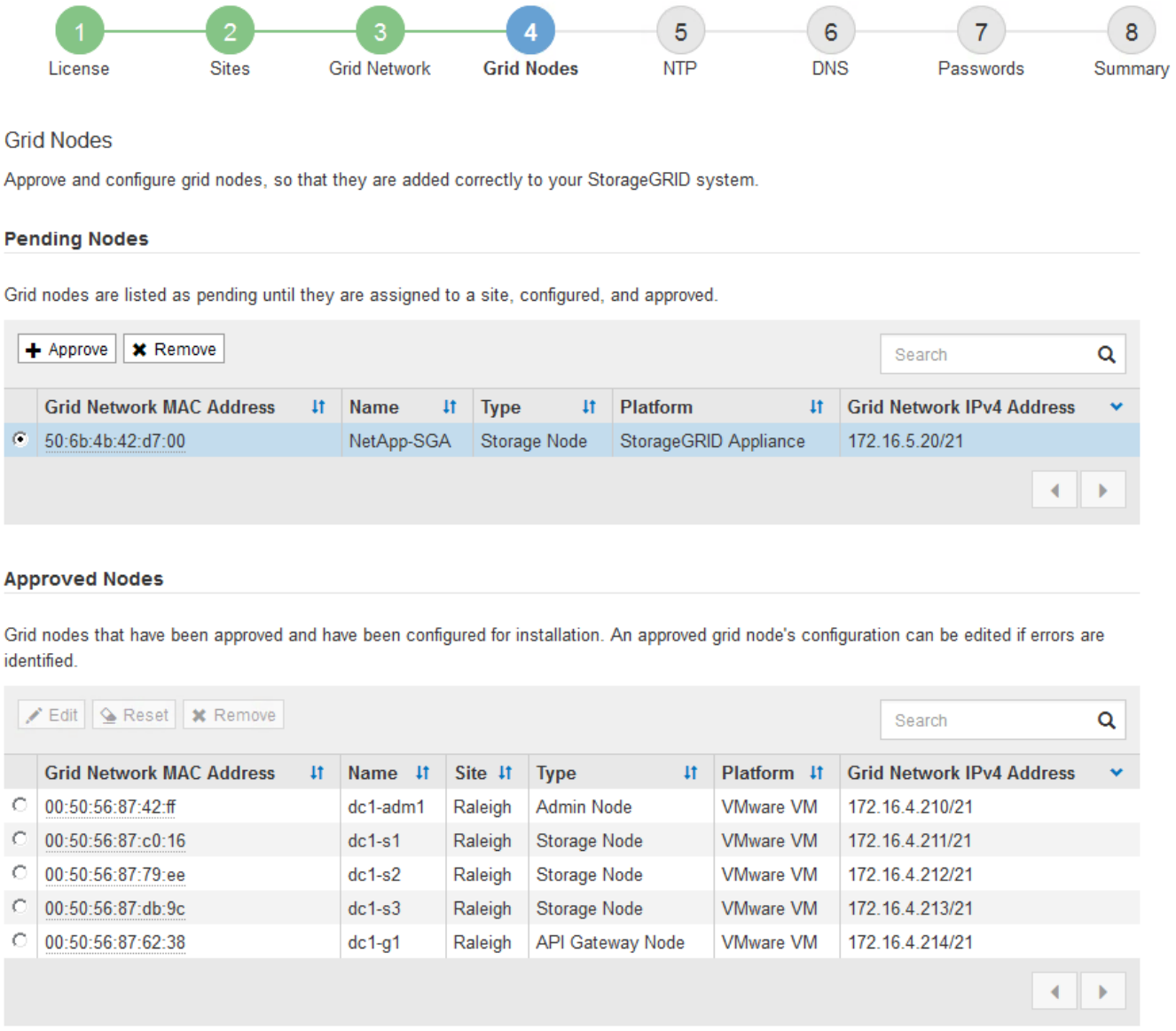
Alle Grid-Nodes von virtuellen und StorageGRID Appliances müssen bereitgestellt worden sein.

Schritte

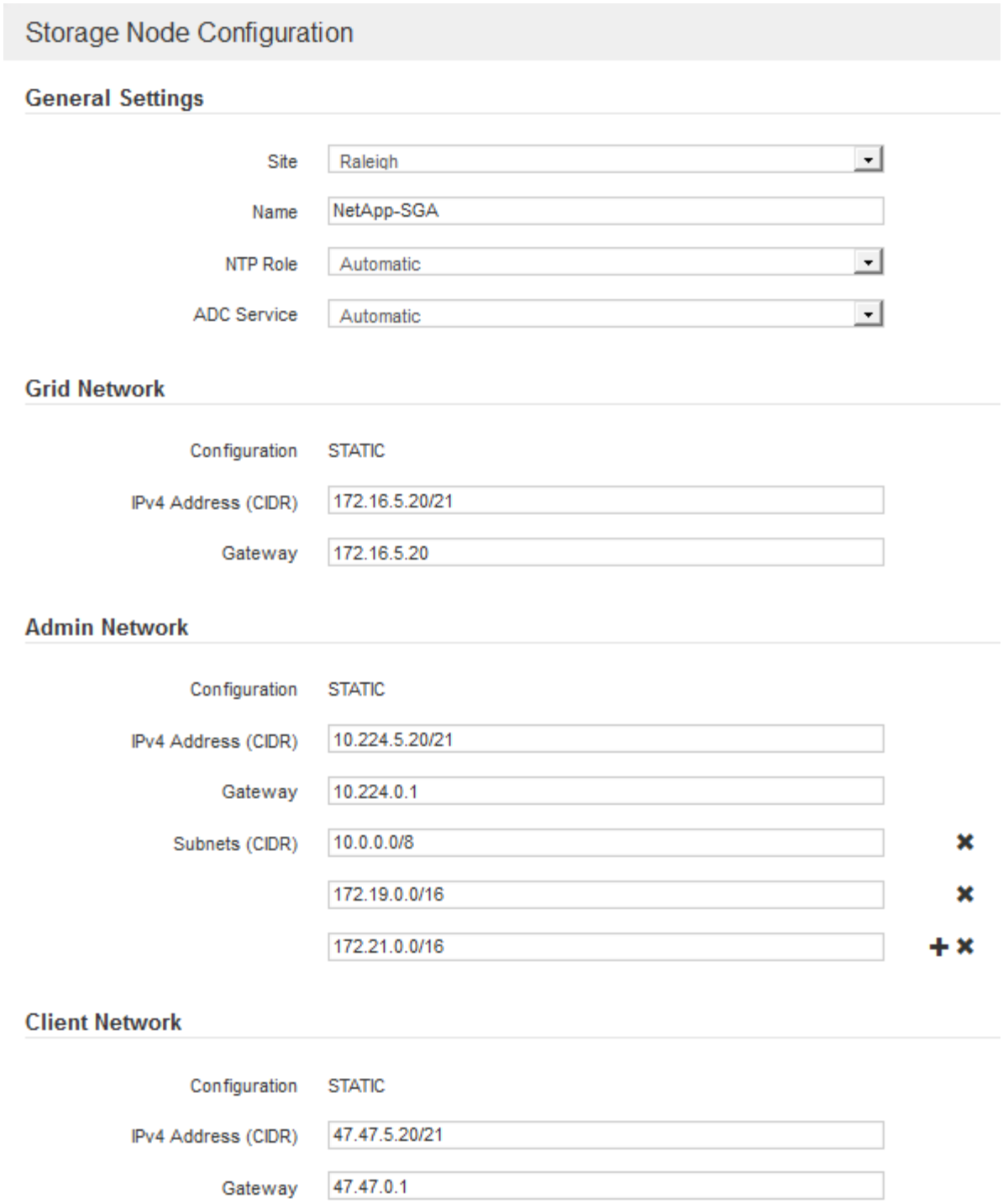
1. Prüfen Sie die Liste ausstehender Nodes und bestätigen Sie, dass alle von Ihnen bereitgestellten Grid-Nodes angezeigt werden.

   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.



3. Klicken Sie Auf **Genehmigen**.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften, falls erforderlich:



- **Standort**: Der Name der Site, mit der dieser Grid-Knoten verknüpft wird.
- **Name**: Der Name, der dem Knoten zugewiesen wird, und der Name, der im Grid Manager angezeigt wird. Der Name ist standardmäßig auf den Namen eingestellt, den Sie beim Konfigurieren des Nodes angegeben haben. In diesem Schritt des Installationsprozesses können Sie den Namen nach Bedarf ändern.

> Nachdem Sie die Installation abgeschlossen haben, können Sie den Namen des Node nicht 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. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, 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-Netzwerkkonfiguration 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: für eine StorageGRID-Appliance, wenn das Admin-Netzwerk während der Erstinstallation mit dem StorageGRID Appliance Installer nicht konfiguriert wurde, kann es in diesem Dialogfeld „Grid Manager“ nicht 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. In Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.

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 angegeben haben.

   Weitere Informationen finden Sie in der Installations- und Wartungsanleitung 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-Netzwerkkonfiguration 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: für eine StorageGRID-Appliance, wenn das Clientnetzwerk während der Erstinstallation mit dem StorageGRID-Appliance-Installationsprogramm nicht konfiguriert wurde, kann es in diesem Dialogfeld „Grid Manager“ nicht 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. In Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.

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

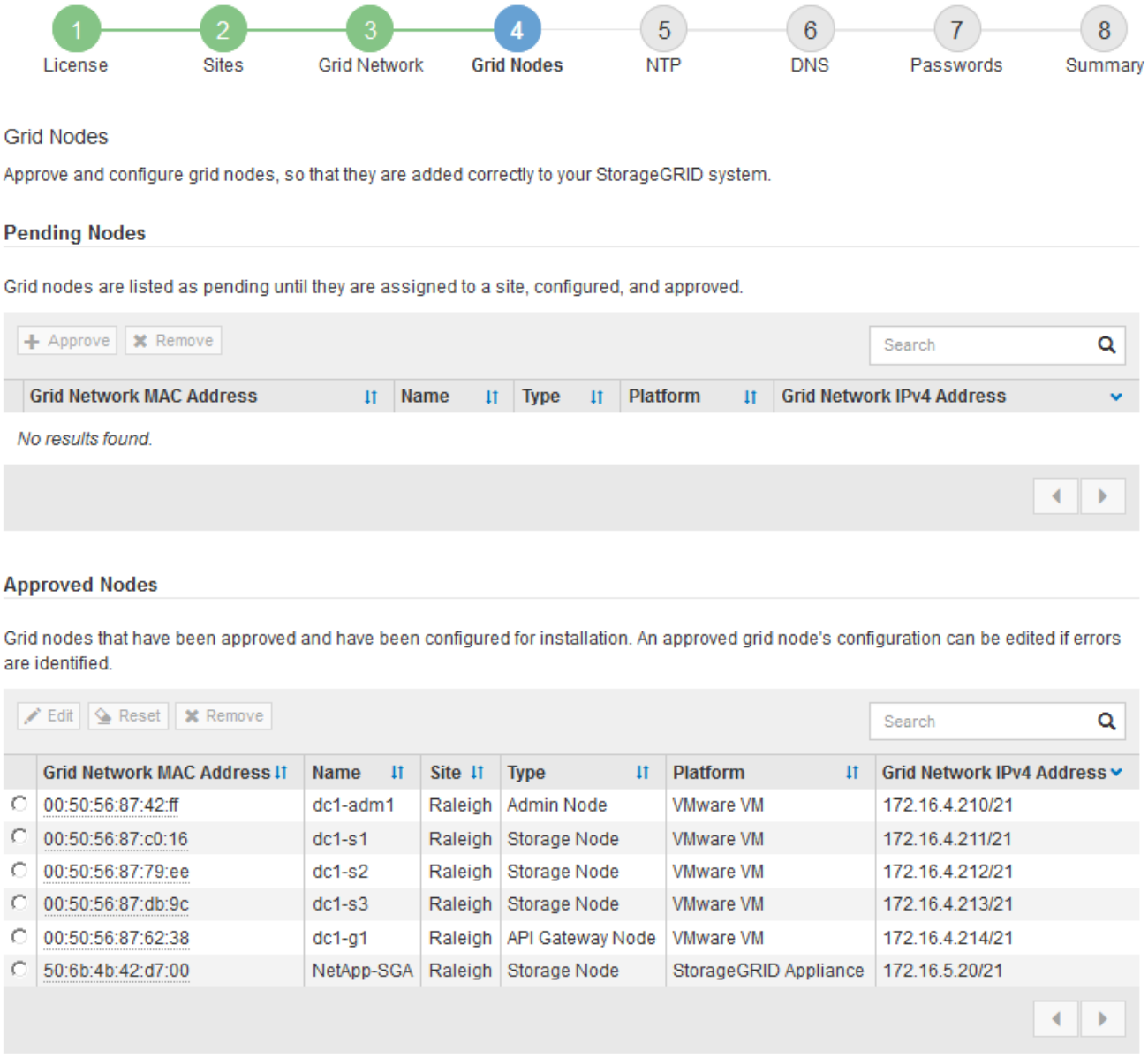
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.

   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 angegeben haben.

      Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

8. Klicken Sie Auf **Speichern**.

Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



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**.

Angeben von Informationen zum Network Time Protocol-Server

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.

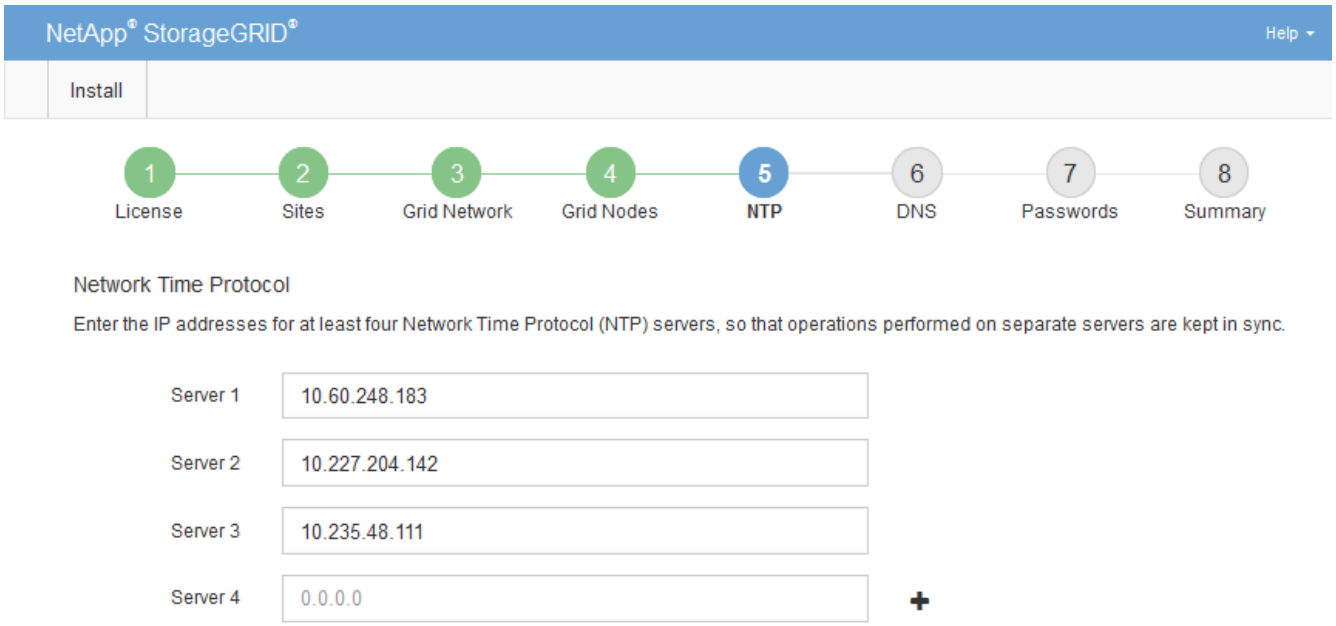
> ⓘ Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt. Siehe "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.



3. Wählen Sie **Weiter**.

Angeben von Informationen zum DNS-Server

Sie müssen DNS-Informationen (Domain Name System) für Ihr StorageGRID-System angeben, damit Sie auf externe Server zugreifen können, indem Sie Hostnamen anstelle von IP-Adressen verwenden.

Über diese Aufgabe

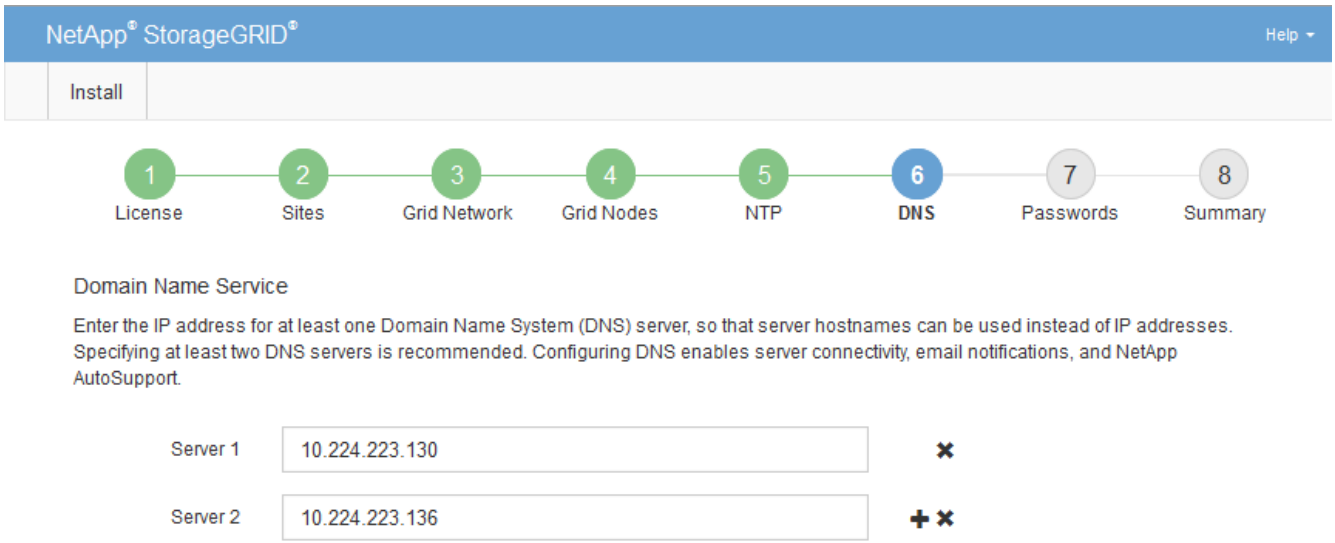
Wenn Sie DNS-Serverinformationen angeben, können Sie vollständig qualifizierte Domänennamen (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport verwenden. Es wird empfohlen, mindestens zwei DNS-Server anzugeben.

> Geben Sie zwei bis sechs IPv4-Adressen für DNS-Server an. Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen. Weitere Informationen finden Sie in den Informationen zum Ändern der DNS-Konfiguration in den Wiederherstellungsanleitungen und Wartungsanweisungen.

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.



   Als Best Practice empfehlen wir, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Festlegen der Passwörter für das StorageGRID-System

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 müssen über die Provisionierungs-Passphrase für Installation, Erweiterung und Wartung verfügen, 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 der Grid-Verwaltung kann mit dem Grid Manager geändert werden.
- Zufällig generierte Befehlszeilenkonsole und SSH-Passwörter werden in der Datei Passwords.txt im Wiederherstellungspaket gespeichert.

Schritte

1. Geben Sie unter **Provisioning-Passphrase** das Provisioning-Passphrase ein, das für Änderungen an der Grid-Topologie Ihres StorageGRID-Systems erforderlich ist.

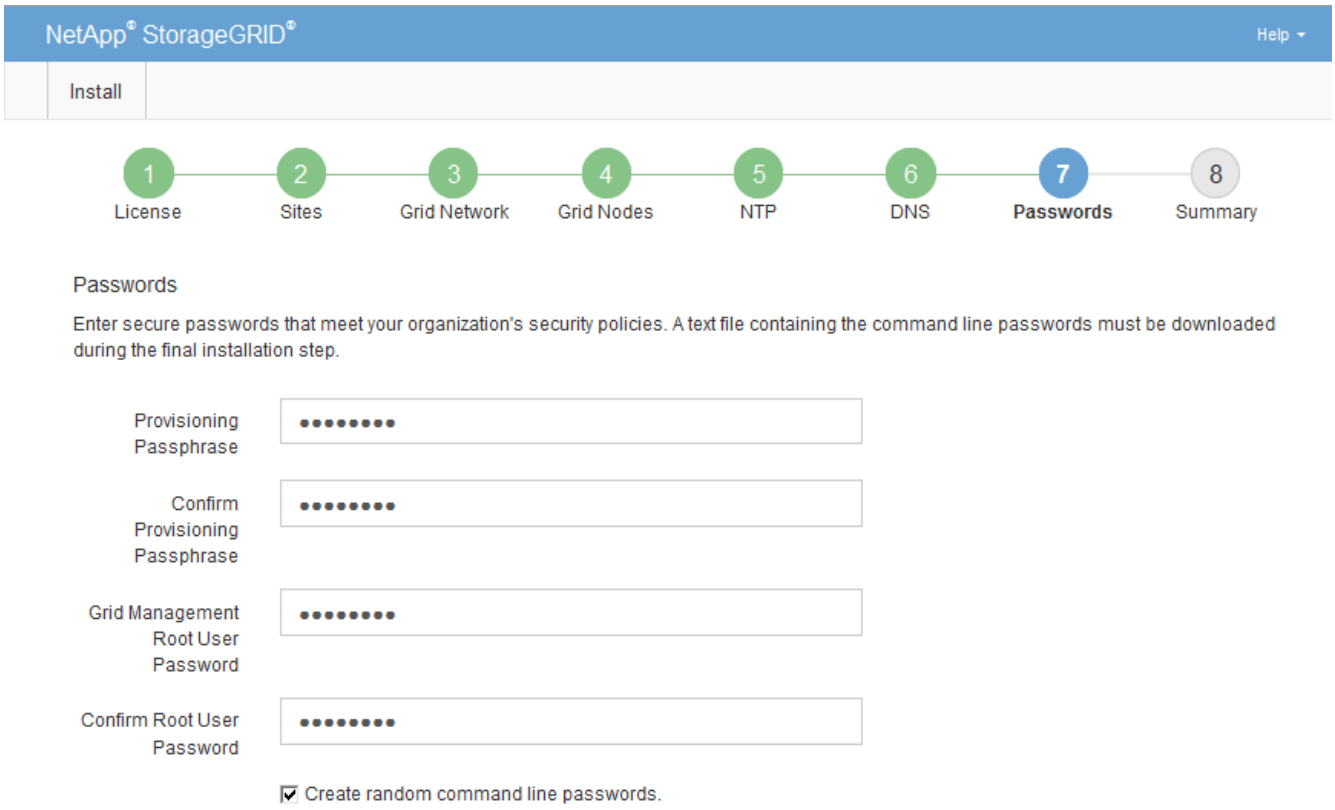
   Speichern Sie die Provisionierungs-Passphrase an einem sicheren Ort.

   > 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.



5. Wenn Sie ein Raster für Proof of Concept- oder Demo-Zwecke installieren, deaktivieren Sie optional das Kontrollkästchen **Create Random command line passwords**.

   Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Deaktivieren Sie **Erstellen von zufälligen Befehlszeilenpasswörtern** nur für Demo-Raster, wenn Sie Standardkennwörter für den Zugriff auf Grid-Knoten aus der Befehlszeile mit dem „`root`“- oder „`admin`“-Konto verwenden möchten.

   Sie werden aufgefordert, die Recovery Package-Datei herunterzuladen (`sgws-recovery-package-id-revision.zip`Nach dem Klick auf **Installieren** auf der Übersichtsseite. Sie müssen diese Datei herunterladen, 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.

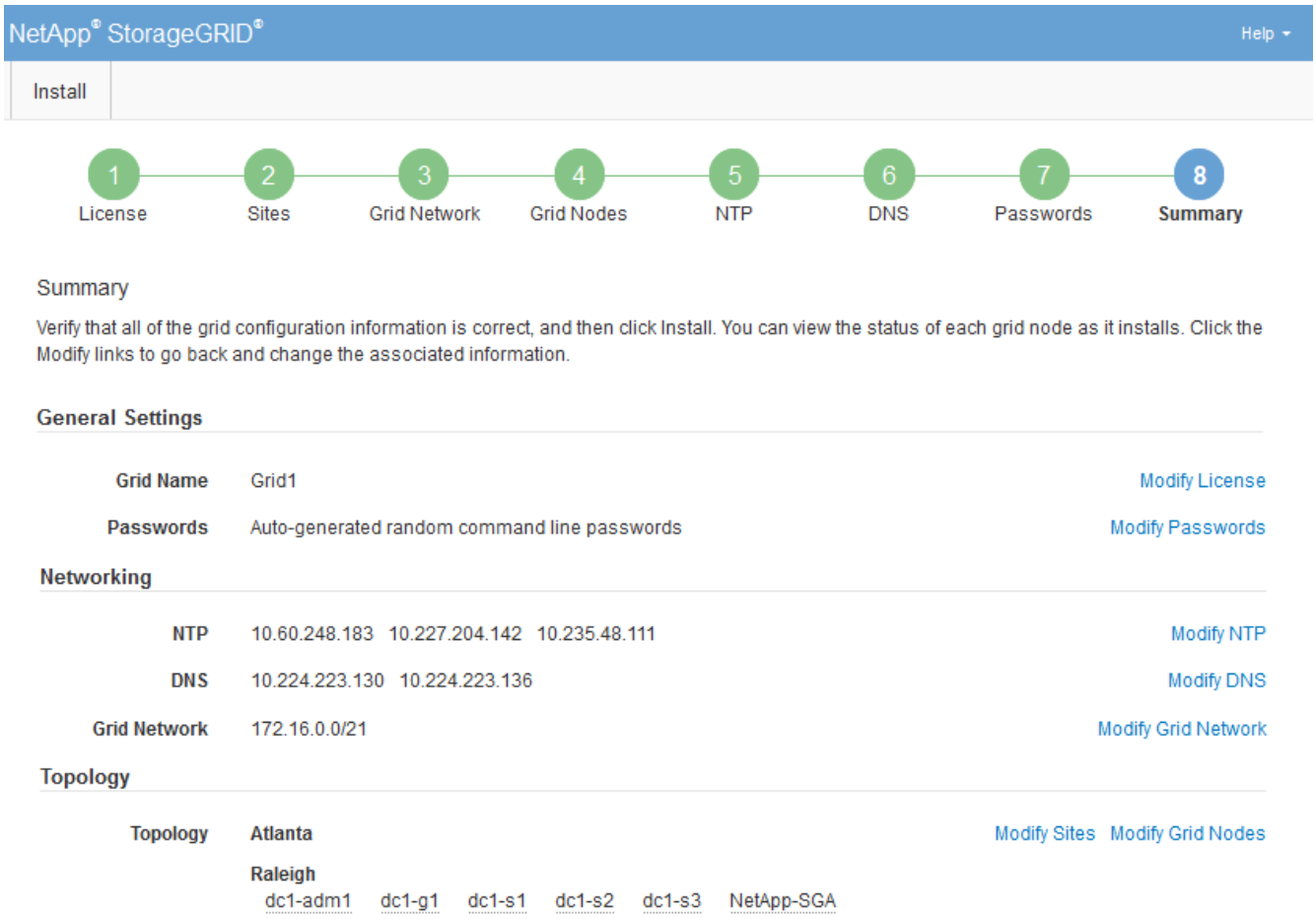
6. Klicken Sie Auf **Weiter**.

Überprüfung Ihrer Konfiguration und Abschluss der 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**.



2. 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.
3. Klicken Sie Auf **Installieren**.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf **Installieren** klicken. Wenn die Verbindung unterbrochen wird, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Siehe "Netzwerkrichtlinien" Entsprechende Details.

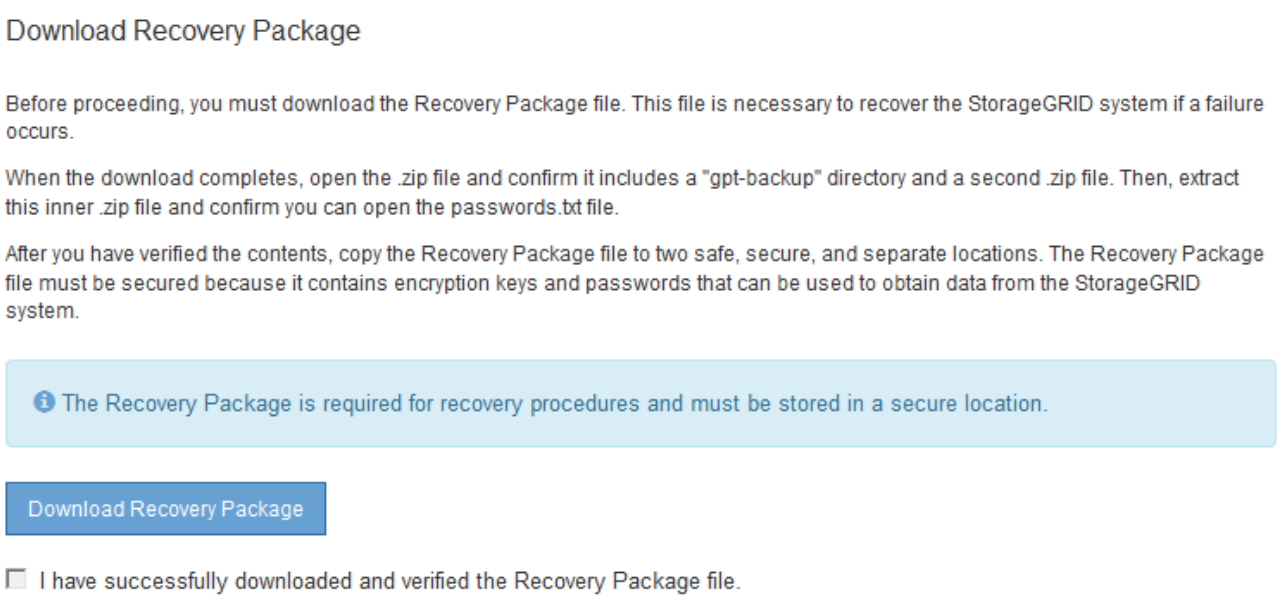
4. Klicken Sie Auf **Download Wiederherstellungspaket**.

   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, Sie können die Installation jedoch erst abschließen und auf das StorageGRID-System zugreifen, wenn Sie diese Datei herunterladen und überprüfen.

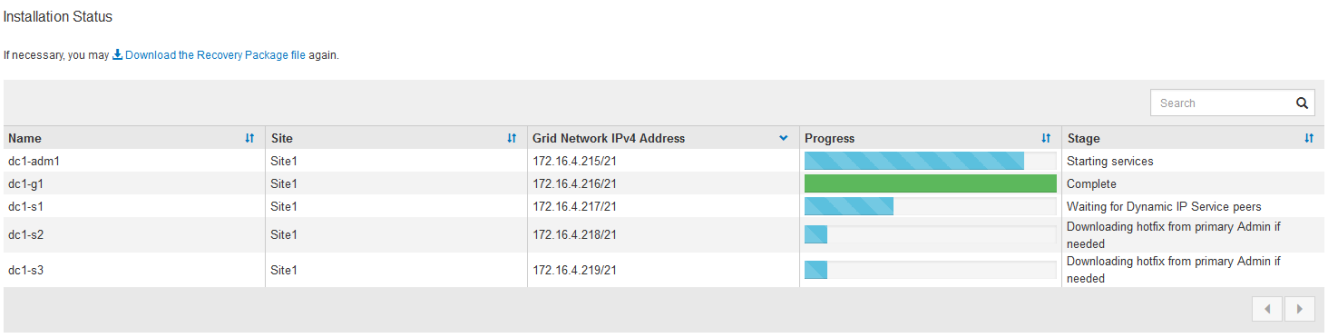
5. Stellen Sie sicher, dass Sie den Inhalt des extrahieren können `.zip` Speichern Sie die Datei an zwei sicheren und separaten Speicherorten.

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 das Recovery Package File** erfolgreich heruntergeladen und verifiziert und klicken Sie auf **Next**.



Wenn die Installation noch läuft, wird die Statusseite angezeigt. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



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. Sie können DHCP während der Konfiguration nicht einrichten.

> 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. Informationen zum Konfigurieren von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- 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. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise neu herstellen.

Automatisierung der Installation

Die Installation des StorageGRID Host Service und die Konfiguration der Grid-Nodes lassen sich automatisieren.

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.

Wenn Sie daran interessiert sind, Ihre StorageGRID-Implementierung vollständig oder teilweise zu automatisieren, lesen Sie vor Beginn des Installationsprozesses „`Automatisieren der Installation`“ durch.

Automatisierung der 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 vorab (oder programmgesteuert) für eine automatisierte Installation vorbereitet werden 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.

Eine Beispiel-Rolle und ein Ansible-Playbook werden im mit dem Installationsarchiv bereitgestellt `/extras`

Ordner. 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.

Automatisierung der Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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, 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.
```

Verwandte Informationen

"Grid wird konfiguriert und die Installation abgeschlossen"

"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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

Weitere Schritte

Nach Abschluss einer Installation müssen Sie eine Reihe von Integrations- und Konfigurationsschritten durchführen. Einige Schritte sind erforderlich, andere sind optional.

Erforderliche Aufgaben

- Erstellen Sie für jedes Client-Protokoll (Swift oder S3) ein Mandantenkonto, das zur Speicherung von Objekten auf Ihrem StorageGRID System verwendet wird.
- Steuern Sie den Systemzugriff, indem Sie Gruppen und Benutzerkonten konfigurieren. Optional können Sie eine föderierte Identitätsquelle (z. B. Active Directory oder OpenLDAP) konfigurieren, sodass Sie Verwaltungsgruppen und Benutzer importieren können. Oder Sie können lokale Gruppen und Benutzer erstellen.

- Integrieren und testen Sie die S3- oder Swift-API-Client-Applikationen zum Hochladen von Objekten auf Ihr StorageGRID System.
- Wenn Sie bereit sind, konfigurieren Sie die Regeln für Information Lifecycle Management (ILM) und die ILM-Richtlinie, die Sie zum Schutz von Objektdaten verwenden möchten.

> Bei der Installation von StorageGRID ist die ILM-Standardrichtlinie, Richtlinie für 2-Basis-Kopien, aktiv. Diese Richtlinie beinhaltet die ILM-Regel (2 Kopien erstellen) für den Bestand und gilt, wenn keine andere Richtlinie aktiviert wurde.

- Wenn in Ihrer Installation Appliance Storage Nodes enthalten sind, führen Sie die folgenden Aufgaben mithilfe der SANtricity Software durch:
  - Stellen Sie Verbindungen zu jeder StorageGRID Appliance her.
  - Eingang der AutoSupport-Daten überprüfen.
- Wenn Ihr StorageGRID-System beliebige Archiv-Knoten enthält, konfigurieren Sie die Verbindung des Archiv-Knotens zum externen Archiv-Speichersystem des Ziels.

> Wenn ein Archiv-Knoten Tivoli Storage Manager als externes Archiv-Speichersystem verwendet, müssen Sie auch Tivoli Storage Manager konfigurieren.

- StorageGRID Richtlinien zur Systemhärtung prüfen und befolgen, um Sicherheitsrisiken zu beseitigen
- Konfigurieren von E-Mail-Benachrichtigungen für Systemalarme.

Optionale Aufgaben

- Wenn Sie Benachrichtigungen vom (alten) Alarmsystem empfangen möchten, konfigurieren Sie Mailinglisten und E-Mail-Benachrichtigungen für Alarme.
- Aktualisieren Sie die IP-Adressen der Grid-Knoten, wenn sie sich seit der Planung der Bereitstellung geändert haben und das Recovery-Paket generiert haben. Weitere Informationen zum Ändern von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- Konfiguration der Storage-Verschlüsselung, falls erforderlich
- Konfigurieren Sie bei Bedarf die Storage-Komprimierung, um die Größe der gespeicherten Objekte zu verringern.
- Konfigurieren des Zugriffs auf Audit-Clients Sie können den Zugriff auf das System für Audit-Zwecke über eine NFS- oder CIFS-Dateifreigabe konfigurieren. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

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 in den Anweisungen zum Überwachen und Beheben von StorageGRID. Informationen zur Fehlerbehebung bei Problemen mit der Installation finden Sie in den Installations- und Wartungsanweisungen für Ihre Geräte. Wenn Sie weitere Hilfe benötigen, wenden Sie sich an den technischen Support.

Verwandte Informationen

"Monitor Fehlerbehebung"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"NetApp Support"

Beispiel /etc/sysconfig/Network-scripts

Sie können die Beispieldateien verwenden, um vier physische Linux-Schnittstellen in einer einzigen LACP-Verbindung zu aggregieren. Anschließend können Sie drei VLAN-Schnittstellen einrichten, die die Verbindung als StorageGRID Grid, Administrator 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

Erfahren Sie, wie Sie StorageGRID-Software in Ubuntu- oder Debian-Bereitstellungen installieren.

- "Übersicht über die Installation"
- "Planung und Vorbereitung"
- "Implementierung virtueller Grid-Nodes"
- "Grid wird konfiguriert und die Installation abgeschlossen"
- "Automatisierung der Installation"
- "Überblick über DIE REST API zur Installation"
- "Weitere Schritte"
- "Fehlerbehebung bei Installationsproblemen"
- "Beispiel /etc/Netzwerk/Schnittstellen"

Übersicht über die Installation

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 des StorageGRID Networking, damit Sie Ihr Netzwerk entsprechend konfigurieren können. Weitere Informationen finden Sie in den StorageGRID Netzwerkrichtlinien.
   - 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 Ubuntu oder Debian
     - 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 Ubuntu- oder Debian-Befehlszeile und Node-Konfigurationsdateien, um virtuelle Grid-Knoten auf den Hosts 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 Installationsverfahren für StorageGRID enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

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.

Verwandte Informationen

"Planung und Vorbereitung"

"Implementierung virtueller Grid-Nodes"

"Grid wird konfiguriert und die Installation abgeschlossen"

"Automatisierung der Installation und Konfiguration des StorageGRID Host Service"

"Überblick über DIE REST API zur Installation"

"Netzwerkrichtlinien"

Planung und Vorbereitung

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 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:

- Informieren Sie sich über die Computing-Anforderungen von StorageGRID, 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.

- Informieren Sie sich über die Anforderungen für die Node-Migration, wenn Sie geplante Wartungsarbeiten an physischen Hosts ohne Service-Unterbrechung durchführen möchten.
- Sammeln Sie alle Netzwerkinformationen im Voraus. Wenn Sie nicht DHCP verwenden, sammeln Sie die IP-Adressen, die jedem Grid-Node zugewiesen werden sollen, und die IP-Adressen des Domain Name System (DNS) und der von Ihnen verwendeten NTP-Server (Network Time Protocol).
- Installation, Anschluss und Konfiguration der gesamten erforderlichen Hardware – einschließlich aller StorageGRID Appliances – gemäß den Spezifikationen

> Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im Installationsverfahren für StorageGRID enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

- Legen Sie fest, welche der verfügbaren Implementierungs- und Konfigurationstools Sie verwenden möchten.

Verwandte Informationen

"Netzwerkrichtlinien"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"Anforderungen für die Container-Migration für Nodes"

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	Sie müssen das StorageGRID-Installationsarchiv herunterladen und die Dateien extrahieren.

Element	Hinweise
Service-Laptop	Das StorageGRID System wird über einen Service-Laptop installiert. Der Service-Laptop muss Folgendes haben: • Netzwerkport • SSH-Client (z. B. PuTTY) • Unterstützter Webbrowser
StorageGRID-Dokumentation	• Versionshinweise • Anweisungen für die Administration von StorageGRID

Verwandte Informationen

"Herunterladen und Extrahieren der StorageGRID-Installationsdateien"

"Anforderungen an einen Webbrowser"

"StorageGRID verwalten"

"Versionshinweise"

Herunterladen und Extrahieren der StorageGRID-Installationsdateien

Sie müssen das StorageGRID-Installationsarchiv herunterladen und die erforderlichen Dateien extrahieren.

Schritte

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "NetApp Downloads: 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 Warnung/MusterLeseanweisung 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 den Recovery- und Wartungsanleitungen.

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.

   Die Download-Seite für die ausgewählte Version wird angezeigt. Die Seite enthält drei Spalten:

6. Wählen Sie in der Spalte **Install StorageGRID** die entsprechende Software aus.

Wählen Sie die aus `.tgz` Oder `.zip` Archivieren Sie die Datei für Ihre Plattform.

- `StorageGRID-Webscale-version-DEB-uniqueID.zip`
- `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

Die komprimierten Dateien enthalten die DEB-Dateien und Skripte für Ubuntu oder Debian.

Verwenden Sie die `.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`.
	DEB-Paket zur Installation des StorageGRID-Hostdienstes auf Ubuntu oder Debian-Hosts.
Skript-Tool zur Bereitstellung	**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.

Pfad und Dateiname	Beschreibung
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` 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.

Verwandte Informationen

"Verwalten Sie erholen"

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.

Weitere Informationen zu unterstützten Servern finden Sie in der Interoperabilitäts-Matrix.

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 dediziert für die Ausführung von StorageGRID sind (nicht empfohlen), sollten Sie die Ressourcenanforderungen der anderen Applikationen berücksichtigen.

> 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 und zum Monitoring der CPU- und Arbeitsspeicherauslastung finden Sie in den Anweisungen für die Administration, das Monitoring und das Upgrade von 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 die Informationen über Speicheranforderungen.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Storage- und Performance-Anforderungen erfüllt"

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

"Software-Upgrade"

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. Es ist möglich, Shared- oder lokalen RAID-Storage für eine beliebige Storage-Kategorie zu verwenden. Wenn Sie jedoch die Möglichkeit zur Migration der StorageGRID Nodes nutzen möchten, müssen Sie sowohl Systemdaten als auch Objektdaten auf einem Shared Storage speichern.

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 AFF Storage nutzen

Wenn der StorageGRID-Node Storage verwendet, der einem NetApp AFF 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 Speicherknoten 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
Docker Storage-Pool	Container-Pool	1	Gesamtzahl der Nodes × 100 GB
`/var/local` Datenmenge	Systemdaten	1 für jeden Node auf diesem Host	90 GB

LUN-Zweck	Storage-Kategorie	Anzahl LUNs	Minimale Größe/LUN
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.	4,000 GB Weitere Informationen finden Sie unter Speicheranforderungen für Speicherknoten.
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 konfiguriertem Audit Level, Größe der Benutzereingaben wie z. B. S3-Objektschlüsselname und wie viele Audit-Protokoll-Daten Sie erhalten müssen, müssen Sie möglicherweise die Größe der Audit-Protokoll-LUN auf jedem Admin-Node erhöhen. In der Regel generiert ein Grid etwa 1 KB Audit-Daten pro S3-Betrieb. Dies bedeutet, dass ein 200 GB-LUN 70 Millionen Operationen pro Tag und 800 Operationen pro Sekunde für zwei bis drei Tage unterstützen würde.

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 zum Wiederherstellen von Grid-Nodes verwendet werden. Beachten Sie stattdessen die Recovery- und Wartungsabläufe 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)	*Nicht zutreffend*
Gateway-Node	100 GB	90 GB	*Nicht zutreffend*
Archiv-Node	100 GB	90 GB	*Nicht zutreffend*

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.

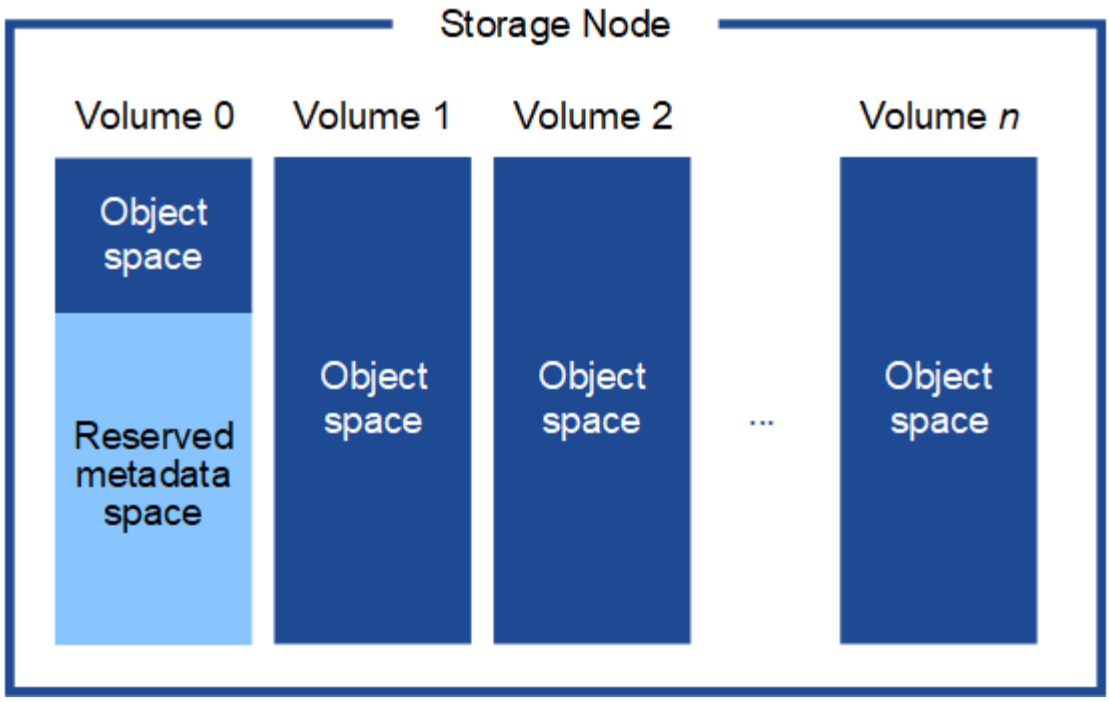
Node-Typ	LUN-Zweck	Anzahl LUNs	Die LUN-Größe
Storage-Node	Docker Storage-Pool	1	300 GB (100 GB/Node)
Storage-Node	`/var/local` Datenmenge	1	90 GB
Storage-Node	Objektdaten	3	4,000 GB
Admin-Node	`/var/local` Datenmenge	1	90 GB
Admin-Node	Prüfprotokolle für Admin-Node	1	200 GB
Admin-Node	Admin-Node-Tabellen	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 ein neues StorageGRID 11.5-System installieren und jeder Speicherknoten 128 GB oder mehr RAM hat, sollten Sie Volume 0 8 TB oder mehr zuweisen. 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 Anweisungen zum Verwalten von StorageGRID und suchen nach „`managing Objekt-Metadaten-Storage`“.

"StorageGRID verwalten"

Verwandte Informationen

"Anforderungen für die Container-Migration für Nodes"

"Verwalten Sie erholen"

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 einfach alle StorageGRID Nodes nacheinander auf einen anderen Host, bevor Sie den physischen Host offline schalten. 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 Netzwerkschnittstellennnamen 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-Ebene die VM-Migration unterstützt, ist diese Funktion anstelle der Node-Migrationsfunktion von StorageGRID wahrscheinlich sinnvoll. In diesem Fall können Sie diese zusätzlichen Anforderungen ignorieren.

Bevor Sie eine Migration oder eine Hypervisor-Wartung durchführen, müssen Sie die Nodes ordnungsgemäß herunterfahren. Informationen zum Herunterfahren eines Grid-Node finden Sie in den Anweisungen zur Recovery und Wartung.

VMware Live Migration wird nicht unterstützt

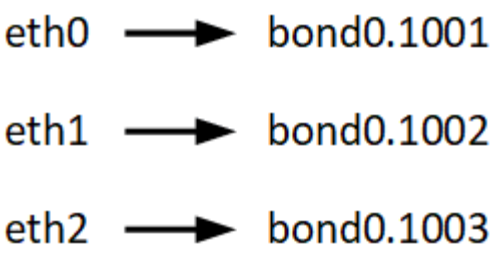
OpenStack Live Migration und VMware Live vMotion sorgen dafür, dass die Virtual Machine-Uhr springen und für Grid-Nodes jeglicher Art nicht unterstützt wird. Obwohl selten, falsche Uhrzeiten können zum Verlust von Daten oder Konfigurations-Updates führen.

Cold-Migration wird unterstützt. Bei der „Cold“-Migration sollten Sie die StorageGRID Nodes herunterfahren, bevor Sie sie zwischen Hosts migrieren. Siehe das Verfahren zum Herunterfahren eines Grid-Node in der Wiederherstellungsanleitung und Wartungsanleitung.

Konsistente Namen von Netzwerkschnittstellen

Um einen Node von einem Host zum anderen zu verschieben, muss der StorageGRID-Hostdienst die Gewissheit haben, dass die externe Netzwerkverbindung, die der Node an seinem aktuellen Standort besitzt, an dem 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:



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, um eine konsistente Netzwerkschnittstelle zu erreichen, die über mehrere Hosts hinweg benennt; einige Beispiele finden Sie unter „`Konfigurieren des Hostnetzwerks`".

Shared Storage

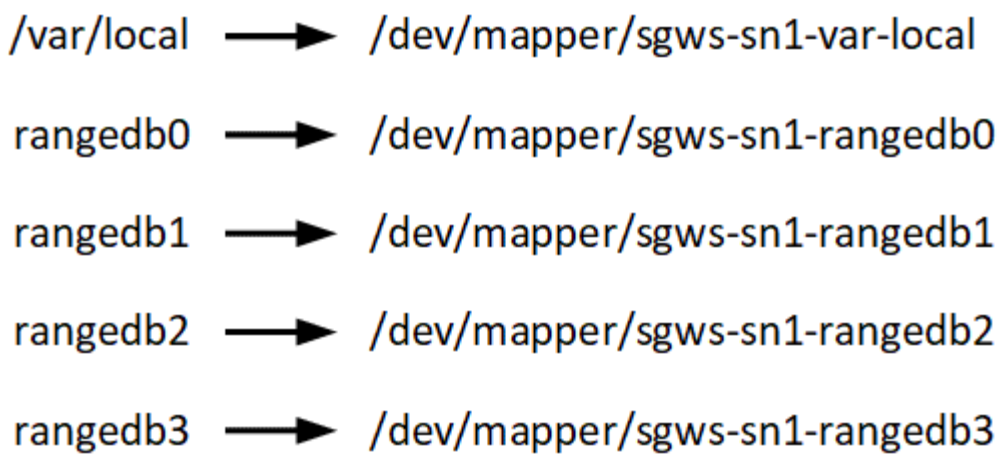
Für schnelle Node-Migrationen mit geringem Overhead werden Node-Daten durch die StorageGRID Node-Migrationsfunktion nicht physisch verschoben. Stattdessen werden die Node-Migration als Export- und Importpaar durchgeführt:

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 Blockgerätnamen zu liefern, die auf allen Hosts verfügbar sind.



Verwandte Informationen

"Konfigurieren des Hostnetzwerks"

"Verwalten Sie erholen"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

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 daran interessiert sind, Ihre StorageGRID-Implementierung vollständig oder teilweise zu automatisieren, lesen Sie vor Beginn des Installationsprozesses „`Automatisieren der Installation`“ durch.

Verwandte Informationen

"Automatisierung der Installation"

Vorbereiten der Hosts

Sie müssen die folgenden Schritte durchführen, um Ihre physischen oder virtuellen Hosts für StorageGRID vorzubereiten. Beachten Sie, dass Sie viele oder alle dieser Schritte mit Standard-Server-Konfigurations-Frameworks wie Ansible, Puppet oder Chef automatisieren können.

Verwandte Informationen

"Automatisierung der Installation und Konfiguration des StorageGRID Host Service"

Linux Wird Installiert

Sie müssen Ubuntu oder Debian auf allen Grid-Hosts installieren. Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Schritte

1. Installieren Sie Ubuntu oder Debian auf allen physischen oder virtuellen Grid-Hosts gemäß den Anweisungen des Distributors oder Ihrem 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 nicht ausgewählt werden.

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.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Informationen zur Installation des AppArmor-Profils

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".

  Wenn Sie AppArmor deaktivieren, werden in den StorageGRID-Protokolldateien keine Einträge angezeigt, die darauf hinweisen, dass AppArmor aktiviert ist.

Konfigurieren des Hostnetzwerks

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.

Was Sie benötigen

- Sie haben sich die StorageGRID Netzwerkrichtlinien durchgelesen.

  "Netzwerkrichtlinien"

- Sie haben die Informationen zu den Anforderungen für die Container-Migration von Nodes überprüft.

  "Anforderungen für die Container-Migration für Nodes"

- Wenn Sie virtuelle Hosts verwenden, haben Sie vor der Konfiguration des Hostnetzwerks die Überlegungen und Empfehlungen zum Klonen von MAC-Adressen gelesen.

  "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"

> 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 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 den Hosts um virtuelle Maschinen handelt und Sie einen oder zwei StorageGRID-Nodes für jeden Host implementieren, können Sie im Hypervisor einfach die richtige Anzahl an Netzwerkschnittstellen 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 kein der folgenden 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 führt dazu, dass der Docker-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 Docker Container die MAC-Adresse der dedizierten NIC auf dem Host nutzen soll, können Sie keine Kompromissmodus-Netzwerkkonfigurationen 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 Docker 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 kein Klonen der MAC-Adresse verwenden möchten und lieber alle Schnittstellen Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen empfangen und übertragen möchten, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene der virtuellen Switch- und Portgruppen auf **Accept** für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen eingestellt 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 in den Anweisungen zum Erstellen von Node-Konfigurationsdateien.

"Erstellen von Knoten-Konfigurationsdateien"

BEISPIEL FÜR DAS Klonen VON MAC

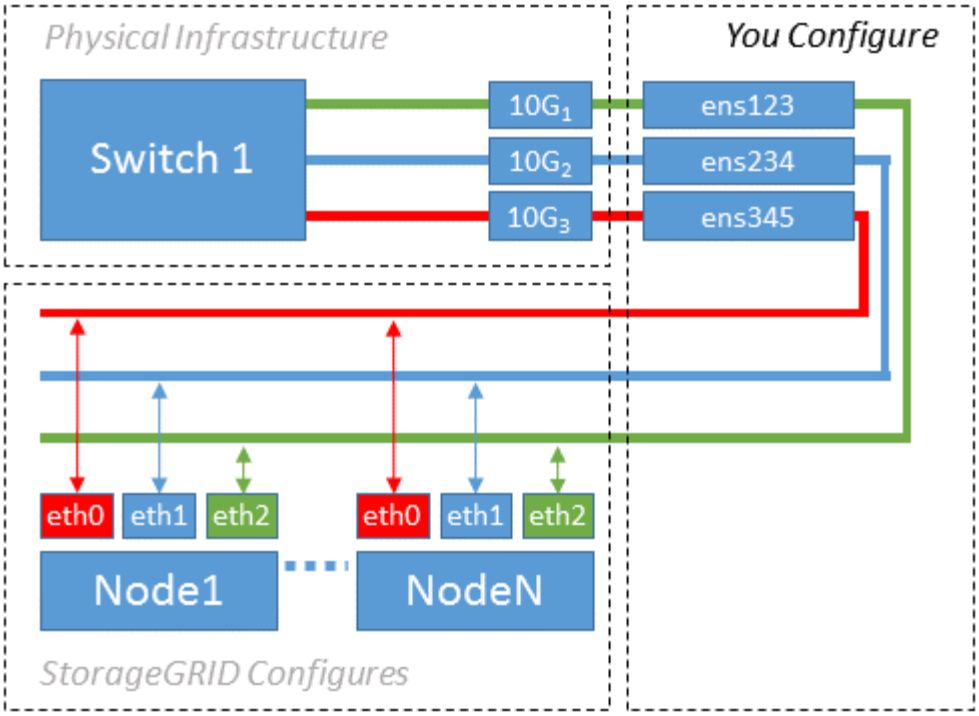
Beispiel für das MAC-Klonen bei einem Host mit einer MAC-Adresse von 11:22:33:44:55:66 für die Schnittstelle ensens256 und die folgenden Schlüssel in der Node-Konfigurationsdatei:

- `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 $10G_1$ bis $10G_3$ verbundenen Ports für den Zugriffsmodus konfigurieren und sie auf die entsprechenden VLANs platzieren.

Beispiel 2: LACP Bond mit VLANs

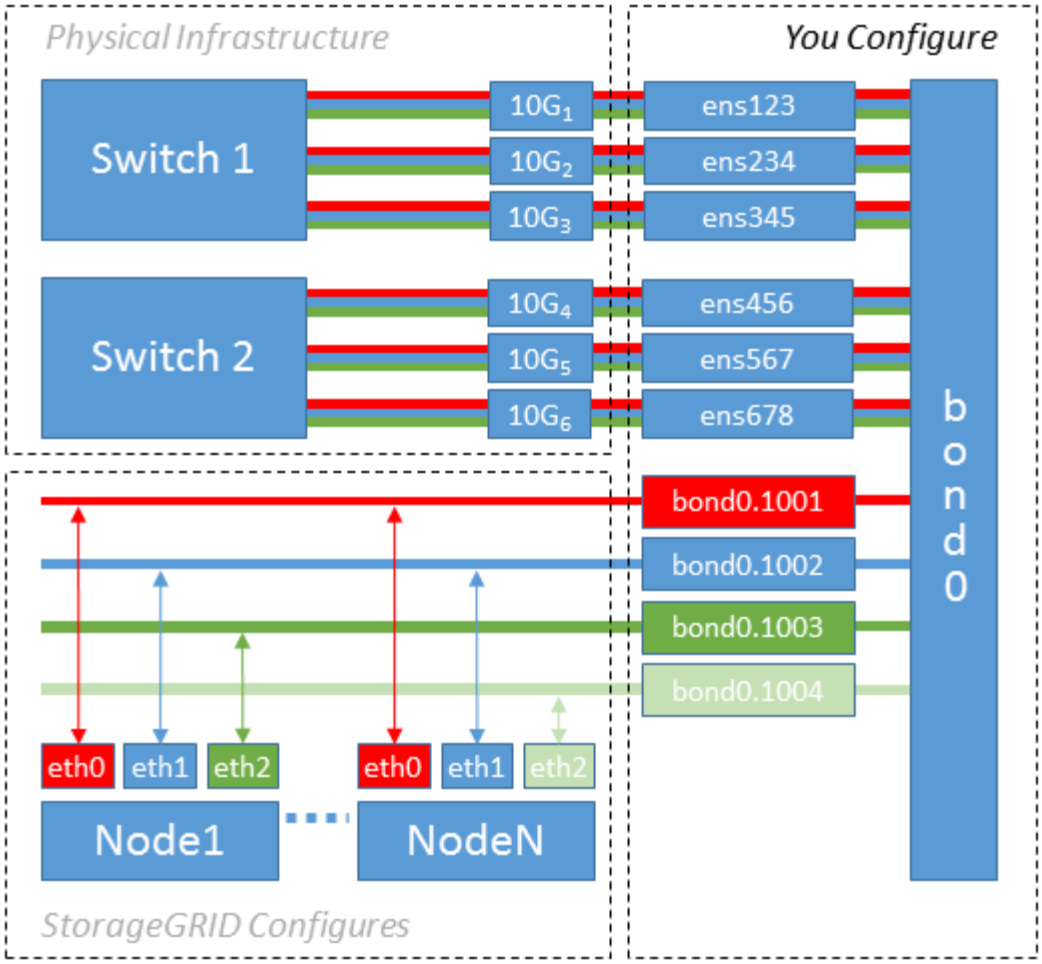
Beispiel 2 geht davon aus, dass Sie mit der Verbindung von Netzwerkschnittstellen und der Erstellung von VLAN-Schnittstellen auf der von Ihnen verwendeten Linux-Distribution vertraut sind.

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 zugehörisches „`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 wird konfiguriert

Jedem Host müssen Block Storage Volumes zugewiesen werden.

Was Sie benötigen

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 „`SStorage-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 keine dieser Volumes partitionieren, formatieren oder mounten; Sie 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 Multipath-Aliase in Betracht ziehen `/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-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

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 von StorageGRID-Node-Migration einrichten und unter Verwendung von Device Mapper Multipathing einen gemeinsamen Speicher 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"

Konfiguration 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-Volume zu verwenden und über genügend Speicherplatz auf der Host-Partition mit verfügen `/var/lib`.

Schritte

1. Dateisystem auf dem Docker-Storage-Volume erstellen:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Mounten des Docker-Storage-Volumes:

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

3. Fügen Sie einen Eintrag für Docker-Storage-Volume-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 1.10.3 oder höher sein.

```
Client:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64

Server:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64
```

Verwandte Informationen

"Hostspeicher wird konfiguriert"

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.

Implementierung virtueller Grid-Nodes

Wenn Sie Grid-Knoten in einer Ubuntu- oder Debian-Umgebung implementieren, erstellen Sie Knoten-Konfigurationsdateien für alle Knoten, validieren die Dateien und starten den StorageGRID-Hostdienst, der die Knoten startet. Wenn Sie Speicherknoten von StorageGRID Appliances bereitstellen müssen, lesen Sie die Installations- und Wartungsanleitung für die Appliance, nachdem Sie alle virtuellen Knoten bereitgestellt haben.

- "Erstellen von Knoten-Konfigurationsdateien"
- "Überprüfung der StorageGRID-Konfiguration"
- "Starten des StorageGRID Host Service"

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG5600 Storage Appliances"

"SG5700 Storage-Appliances"

"SG6000 Storage-Appliances"

Erstellen von Knoten-Konfigurationsdateien

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. Die 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 benane 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` Wenn diese Namenskonventionen nicht eingehalten werden, wird dies vom Host-Service nicht geparst.

Wenn das Grid eine Topologie mit mehreren Standorten geplant ist, ist unter Umständen ein typisches Benennungsschema für Node möglich:

```
<site>-<node type>-<node number>.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	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. Siehe „`wie Grid Nodes den primären Admin-Node ermitteln`“. **Hinweis**: Dieser Wert wird auf dem primären Admin-Node ignoriert und kann möglicherweise nicht verwendet werden.
ADMIN_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT
ADMIN_NETWORK_ESL	O	Kommagetrennte Liste von Subnetzen in CIDR-Notation, mit denen dieser Knoten über das Admin Network-Gateway kommunizieren soll. Beispiel: 172.16.0.0/21,172.17.0.0/21

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_GATEWAY	O (**R**)	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. **Hinweis**: Dieser Parameter ist erforderlich, wenn ADMIN_NETWORK_ESL angegeben wird. Beispiele: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_IP	O	IPv4-Adresse dieses Knotens im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_MAC	O	Die MAC-Adresse für die Admin-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden. Beispiel: b2:9c:02:c2:27:10

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_MASKE	O	IPv4-Netmask für diesen Node im Admin-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn ADMIN_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 255.255.255.0 • 255.255.248.0
ADMIN_NETWORK_MTU	O	Die maximale Übertragungseinheit (MTU) für diesen Knoten im Admin-Netzwerk. Geben Sie nicht an, ob ADMIN_NETWORK_CONFIG = DHCP ist. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 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. **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. Beispiele: • 1500 • 8192

Taste	R, BP ODER O?	Wert
ADMIN_NETWORK_TARGET	BP	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. **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). **Best Practice:** Geben Sie einen Wert an, auch 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. Beispiele: • Bond0.1002 • Ensen256
ADMIN_NETWORK_TARGET_TYPE	O	Schnittstelle (Dies ist der einzige unterstützte Wert.)

Taste	R, BP ODER O?	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 promiskuious-Modus erforderlich wäre, verwenden Sie stattdessen DEN ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC-Adressen finden Sie in den Überlegungen und Empfehlungen zum Klonen von MAC-Adressen. "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"
ADMIN_ROLLE	**R**	Primärer oder nicht primärer Storage Dieser Schlüssel ist nur erforderlich, wenn NODE_TYPE = VM_Admin_Node; nicht für andere Node-Typen angeben.

Taste	R, BP ODER O?	Wert
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 Knoten mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-audit-logs`

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_RANGEDB_00 BLOCK_DEVICE_RANGEDB_01 BLOCK_DEVICE_RANGEDB_02 BLOCK_DEVICE_RANGEDB_03 BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_05 BLOCK_DEVICE_RANGEDB_06 BLOCK_DEVICE_RANGEDB_07 BLOCK_DEVICE_RANGEDB_08 BLOCK_DEVICE_RANGEDB_09 BLOCK_DEVICE_RANGEDB_10 BLOCK_DEVICE_RANGEDB_11 BLOCK_DEVICE_RANGEDB_12 BLOCK_DEVICE_RANGEDB_13 BLOCK_DEVICE_RANGEDB_14 BLOCK_DEVICE_RANGEDB_15	**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 Node-Typen an. Es ist nur BLOCK_DEVICE_RANGEDB_00 erforderlich; der Rest ist optional. Das für BLOCK_DEVICE_RANGEDB_00 angegebene Blockgerät muss mindestens 4 TB betragen; die anderen können kleiner sein. **Hinweis**: Keine Lücken hinterlassen. Wenn Sie BLOCK_DEVICE_RANGEDB_05 angeben, müssen Sie auch BLOCK_DEVICE_RANGEDB_04 angeben. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-rangedb-0`

Taste	R, BP ODER O?	Wert
BLOCK_DEVICE_TABLES	**R**	Pfad und Name der Sonderdatei des Blockgerätes, die dieser Knoten für die dauerhafte Speicherung von Datenbanktabellen verwendet. Dieser Schlüssel ist nur für Knoten mit NODE_TYPE = VM_Admin_Node erforderlich; geben Sie ihn nicht für andere Node-Typen an. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-tables`
BLOCK_DEVICE_VAR_LOCAL	**R**	Pfad und Name der Sonderdatei für das Blockgerät wird dieser Node für seinen persistenten Speicher /var/local verwenden. Beispiele: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-var-local`
CLIENT_NETWORK_CONFIG	O	DHCP, STATISCH ODER DEAKTIVIERT

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_GATEWAY	O	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. Beispiele: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_IP	O	IPv4-Adresse dieses Knotens im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_MAC	O	Die MAC-Adresse für die Client-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden. Beispiel: b2:9c:02:c2:27:20

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_MASK	O	IPv4-Netzmaske für diesen Knoten im Client-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn CLIENT_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 255.255.255.0 • 255.255.248.0
CLIENT_NETWORK_MTU	O	Die maximale Übertragungseinheit (MTU) für diesen Knoten im Client-Netzwerk. Geben Sie nicht an, ob CLIENT_NETWORK_CONFIG = DHCP ist. Wenn angegeben, muss der Wert zwischen 1280 und 9216 liegen. Wenn weggelassen wird, wird 1500 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. **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. Beispiele: • 1500 • 8192

Taste	R, BP ODER O?	Wert
CLIENT_NETWORK_TARGET	BP	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. **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). **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. Beispiele: • Bond0.1003 • Ens423
CLIENT_NETWORK_TARGET_TYPE	O	Schnittstelle (Dieser Wert wird nur unterstützt.)

Taste	R, BP ODER O?	Wert
CLIENT_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 Client-Netzwerk verwenden kann. **Best Practice:** in Netzwerken, in denen der promiskuious-Modus erforderlich wäre, verwenden Sie stattdessen DEN CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC-Adressen finden Sie in den Überlegungen und Empfehlungen zum Klonen von MAC-Adressen. "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"
GRID_NETWORK_CONFIG	BP	STATISCH oder DHCP (Ist standardmäßig STATISCH, wenn nicht angegeben.)
GRID_NETWORK_GATEWAY	**R**	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. 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.

Taste	R, BP ODER O?	Wert
GRID_NETWORK_IP	**R**	IPv4-Adresse dieses Knotens im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 1.1.1.1 • 10.224.4.81
GRID_NETWORK_MAC	O	Die MAC-Adresse für die Grid-Netzwerkschnittstelle im Container. Dieses Feld ist optional. Wenn keine Angabe erfolgt, wird automatisch eine MAC-Adresse generiert. Muss aus 6 Hexadezimalziffern bestehen, die durch Doppelpunkte getrennt werden. Beispiel: b2:9c:02:c2:27:30
GRID_NETWORK_MASKE	O	IPv4-Netzmaske für diesen Knoten im Grid-Netzwerk. Dieser Schlüssel ist nur erforderlich, wenn GRID_NETWORK_CONFIG = STATISCH; nicht für andere Werte angeben. Beispiele: • 255.255.255.0 • 255.255.248.0

Taste	R, BP ODER O?	Wert
GRID_NETWORK_MTU	O	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. 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. **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. **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 identisch sein. Beispiele: • 1500 • 8192

Taste	R, BP ODER O?	Wert
GRID_NETWORK_TARGET	**R**	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. **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). Beispiele: • Bond0.1001 • Ens192
GRID_NETWORK_TARGET_TYPE	O	Schnittstelle (Dies ist der einzige unterstützte Wert.)

Taste	R, BP ODER O?	Wert
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	Richtig oder falsch 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. **Best Practice:** in Netzwerken, in denen der promiskuious-Modus erforderlich wäre, verwenden Sie stattdessen DEN GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC-Schlüssel. Weitere Informationen zum Klonen von MAC-Adressen finden Sie in den Überlegungen und Empfehlungen zum Klonen von MAC-Adressen. "Überlegungen und Empfehlungen zum Klonen von MAC-Adressen"

Taste	R, BP ODER O?	Wert
MAXIMUM_RAM	O	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. **Hinweis**: Der RAM-Wert wirkt sich auf den tatsächlich reservierten Metadatenspeicherplatz eines Knotens aus. Eine Beschreibung des reservierten Speicherplatzes für Metadaten finden Sie in der Anleitung zum Verwalten von StorageGRID. Das Format für dieses Feld lautet `<number><unit>`, Wo `<unit>` Kann sein `b`, `k`, `m`, Oder `g`. Beispiele: 24 g 38654705664b **Hinweis**: Wenn Sie diese Option verwenden möchten, müssen Sie Kernel-Unterstützung für Speicher-cgroups aktivieren.
NODE_TYPE	**R**	Node-Typ: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway

Taste	R, BP ODER O?	Wert
PORT_NEU ZUORDNEN	O	Ordnet alle von einem Node verwendeten Ports für interne Grid Node-Kommunikation oder externe Kommunikation neu zu. Ports müssen neu zugeordnet werden, wenn Netzwerkrichtlinien eines oder mehrere von StorageGRID verwendete Ports beschränken. Dies wird unter „`Kommunikation mit internen Grid-Nodes`“ oder „`Externe Kommunikation`“ beschrieben. **WICHTIG**: Die Ports, die Sie für die Konfiguration von Load Balancer-Endpunkten planen, nicht neu zuordnen. **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. 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`

Taste	R, BP ODER O?	Wert
PORT_REMAP_INBOUND	O	Ordnet die eingehende Kommunikation dem angegebenen Port erneut zu. Wenn Sie PORT_REMAP_INBOUND angeben, jedoch keinen Wert für PORT_REMAP angeben, wird die ausgehende Kommunikation für den Port nicht geändert. **WICHTIG**: Die Ports, die Sie für die Konfiguration von Load Balancer-Endpunkten planen, nicht neu zuordnen. Das verwendete Format ist: `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`, Wobei der Netzwerktyp Grid, admin oder Client ist, und das Protokoll tcp oder udp ist. Beispiel: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Verwandte Informationen

"Ermitteln der primären Admin-Node durch Grid-Nodes"

"Netzwerkrichtlinien"

"StorageGRID verwalten"

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 mit einem Multicast Domain Name System (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 jedoch nicht normalerweise über Subnetze routingfähig ist, können Nodes in anderen Subnetzen die IP-Adresse des primären Admin-Node nicht direkt erfassen.

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-Netzwerkaddressinformationen (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/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

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

Beispiel für Speicherknoten

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-sn1.conf`

Beispieldateiinhalt:

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

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

Beispiel für Archivknoten

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-arc1.conf`

Beispieldateiinhalt:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-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`

Beispieldateiinhalt:

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

Beispiel für einen nicht-primären Admin-Node

Beispiel Dateiname: `/etc/storagegrid/nodes/dc1-adm2.conf`

Beispieldateiinhalt:

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

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

Überprüfung der StorageGRID-Konfiguration

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

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

Starten des 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
```

Führen Sie für jeden Node, der den Status „`not running`“ oder „`Stopped`“ zurückgibt, den folgenden Befehl aus:

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

3. 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 wird konfiguriert und die Installation abgeschlossen

Die Installation wird durch Konfiguration des StorageGRID-Systems vom Grid-Manager auf dem primären Admin-Node abgeschlossen.

- "Navigieren zum Grid Manager"
- "Angeben der StorageGRID-Lizenzinformationen"
- "Hinzufügen von Sites"
- "Angeben von Grid-Netzwerknetzen"
- "Genehmigung ausstehender Grid-Knoten"
- "Angeben von Informationen zum Network Time Protocol-Server"
- "Angeben von Informationen zum DNS-Server"
- "Festlegen der Passwörter für das StorageGRID-System"
- "Überprüfung Ihrer Konfiguration und Abschluss der Installation"
- "Richtlinien nach der Installation"

Navigieren zum Grid Manager

Mit dem Grid Manager können Sie alle Informationen definieren, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Was Sie benötigen

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
```

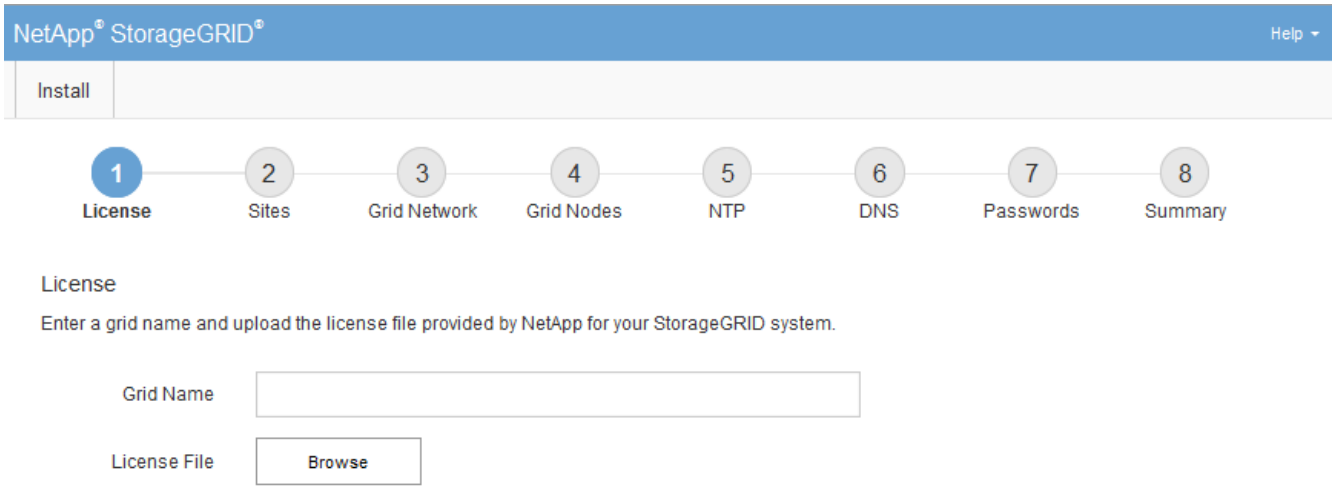
Alternativ können Sie auf den Grid Manager an Port 8443 zugreifen:

```
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.

1. Klicken Sie auf **StorageGRID-System installieren**.

   Die Seite zum Konfigurieren eines StorageGRID-Rasters wird angezeigt.



Angeben der StorageGRID-Lizenzinformationen

Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Schritte

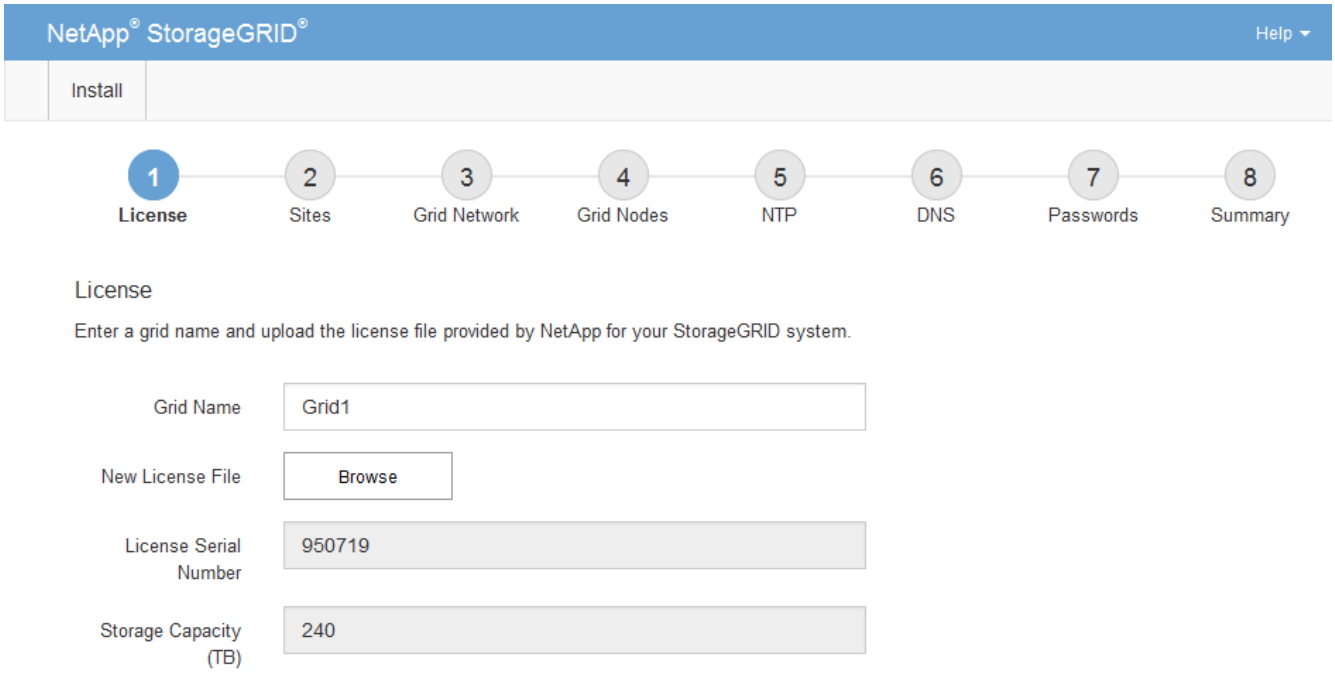
1. Geben Sie auf der Seite Lizenz einen aussagekräftigen Namen für Ihr StorageGRID-System in **Rastername** ein.

   Nach der Installation wird der Name oben im Menü Nodes angezeigt.

2. Klicken Sie auf **Durchsuchen** und suchen Sie die NetApp Lizenzdatei (`NLFunique_id.txt`Und klicken Sie auf **Öffnen**.

   Die Lizenzdatei wird validiert, die Seriennummer und die lizenzierte Speicherkapazität werden 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.



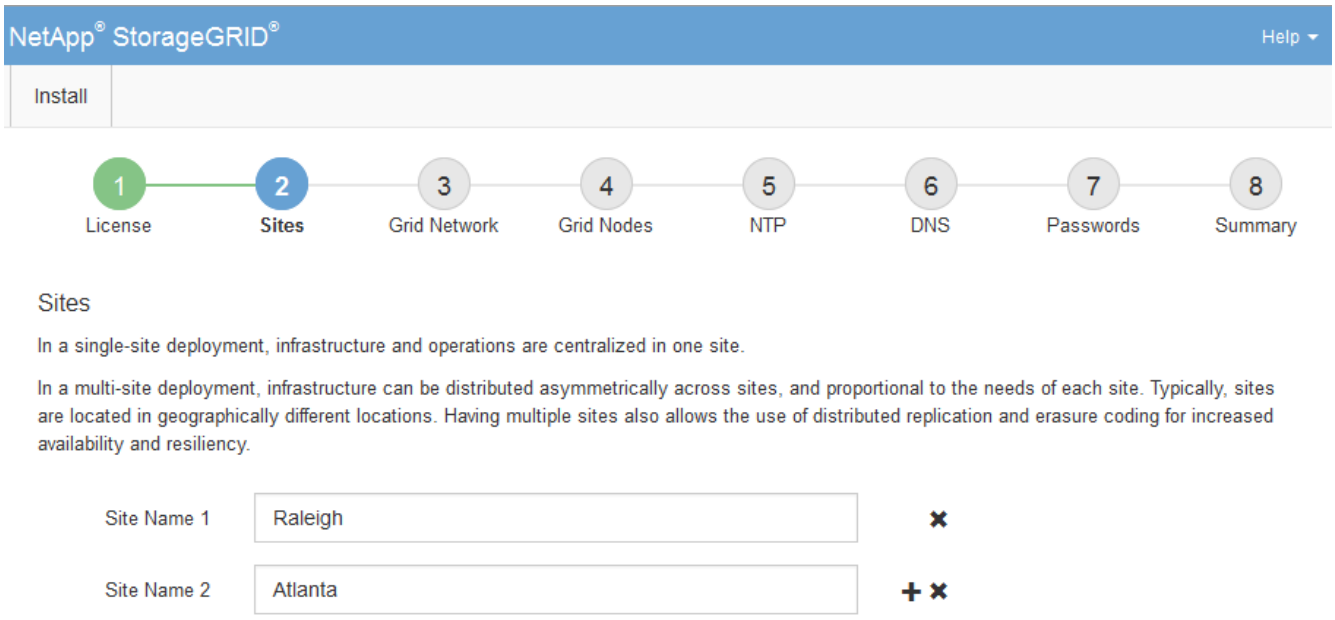
3. Klicken Sie Auf **Weiter**.

Hinzufügen von Sites

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.



3. Klicken Sie Auf **Weiter**.

Angeben von Grid-Netzwerknetzen

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

Über diese Aufgabe

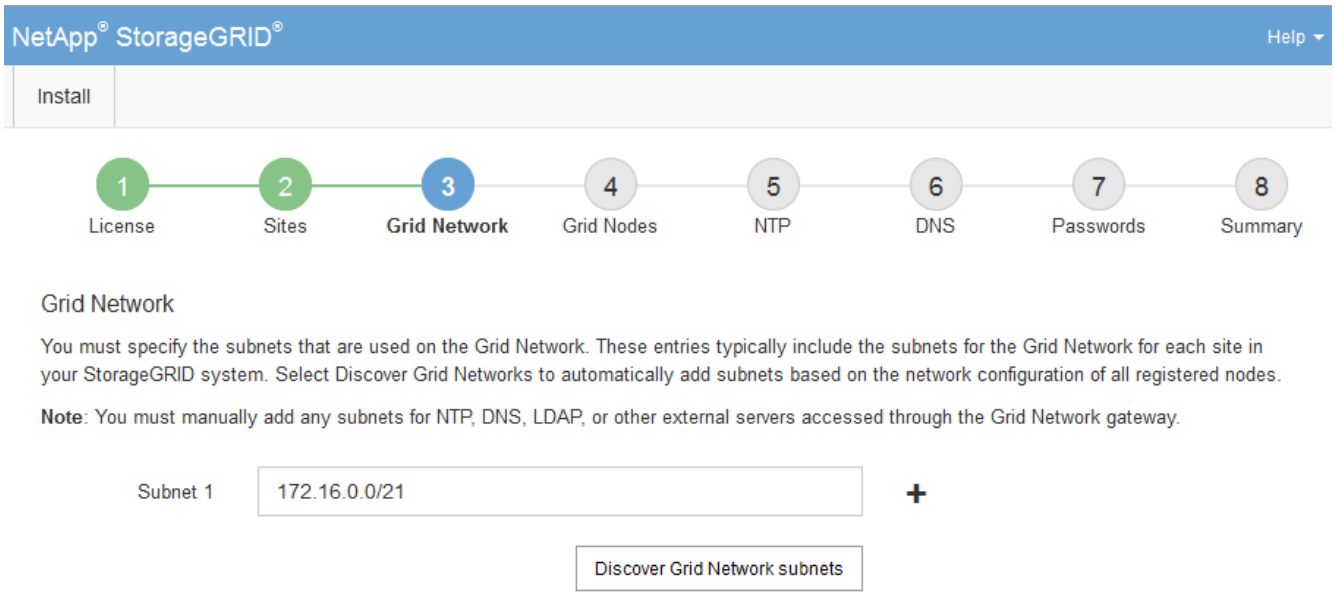
Die Subnetzeinträge enthalten die Subnetze für das Grid-Netzwerk für jeden Standort im StorageGRID-System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen.

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 **Netznetze-Subnetze ermitteln**, um die Netznetzwerksubnetz-Liste automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die beim Grid Manager registriert sind.



3. Klicken Sie Auf **Weiter**.

Genehmigung ausstehender Grid-Knoten

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

Was Sie benötigen

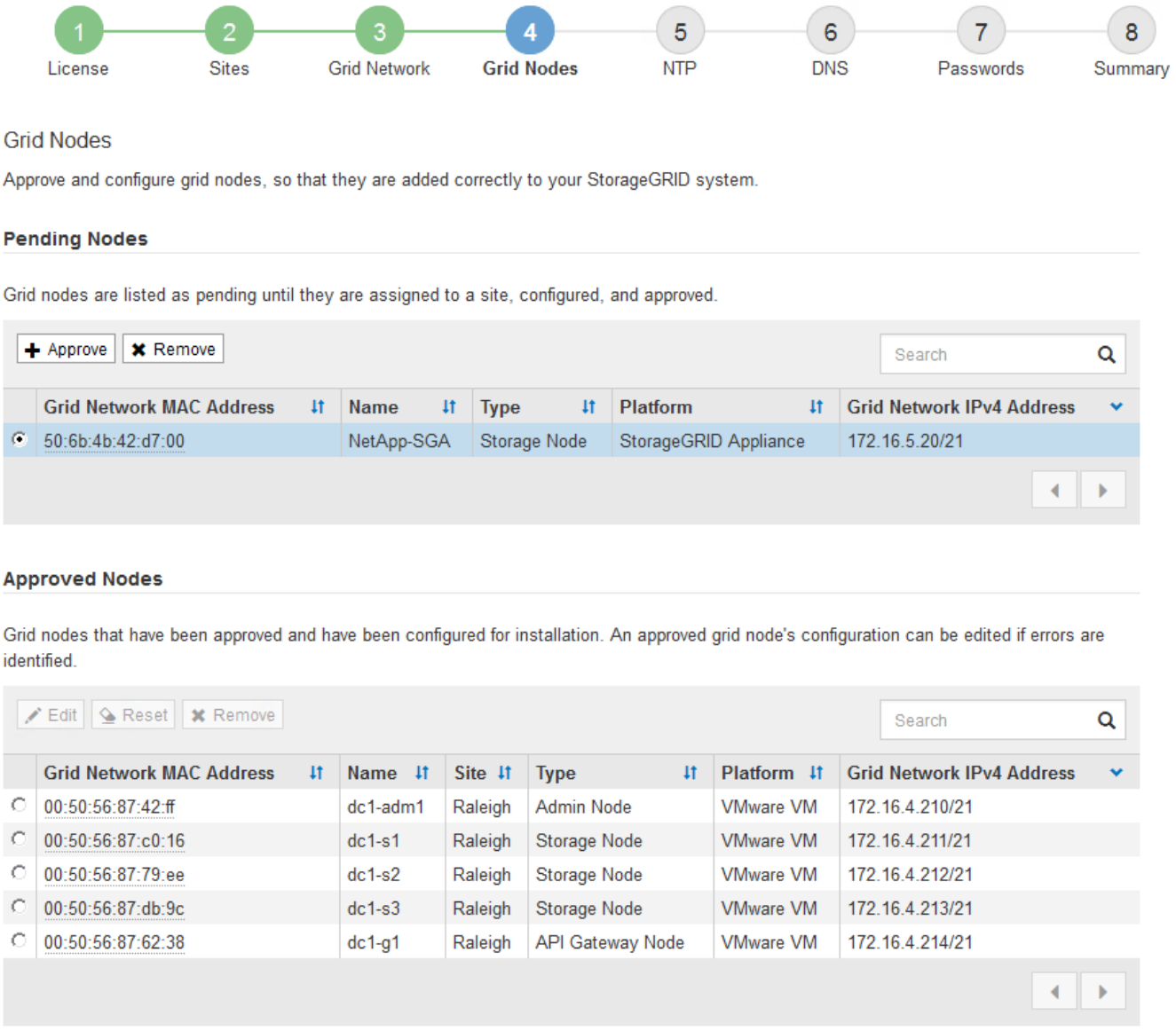
Alle Grid-Nodes von virtuellen und StorageGRID Appliances müssen bereitgestellt worden sein.

Schritte

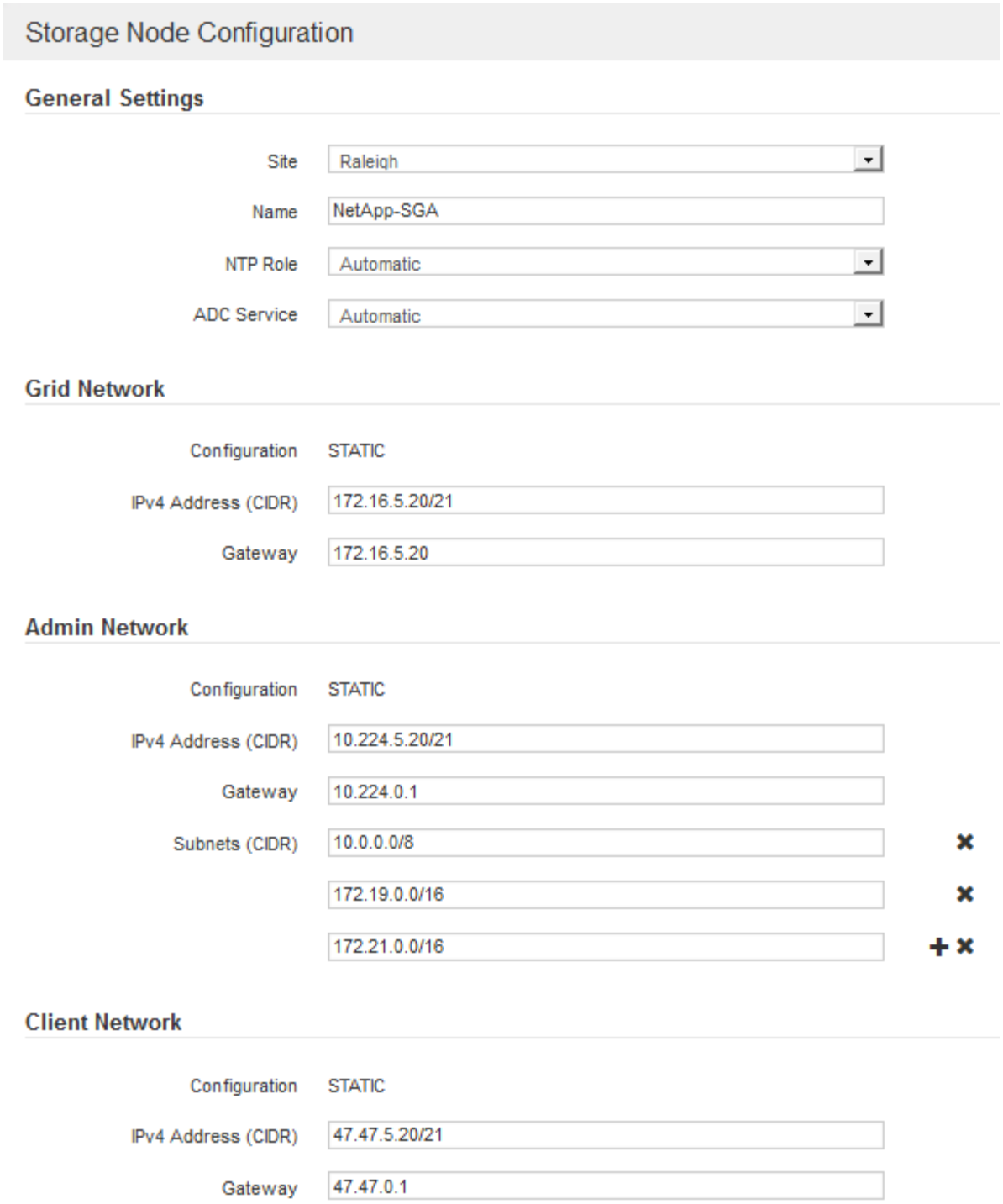
1. Prüfen Sie die Liste ausstehender Nodes und bestätigen Sie, dass alle von Ihnen bereitgestellten Grid-Nodes angezeigt werden.

   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.



3. Klicken Sie Auf **Genehmigen**.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften, falls erforderlich:



- **Standort**: Der Name der Site, mit der dieser Grid-Knoten verknüpft wird.
- **Name**: Der Name, der dem Knoten zugewiesen wird, und der Name, der im Grid Manager angezeigt wird. Der Name ist standardmäßig auf den Namen eingestellt, den Sie beim Konfigurieren des Nodes angegeben haben. In diesem Schritt des Installationsprozesses können Sie den Namen nach Bedarf ändern.

> Nachdem Sie die Installation abgeschlossen haben, können Sie den Namen des Node nicht 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. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, 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-Netzwerkkonfiguration 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: für eine StorageGRID-Appliance, wenn das Admin-Netzwerk während der Erstinstallation mit dem StorageGRID Appliance Installer nicht konfiguriert wurde, kann es in diesem Dialogfeld „Grid Manager“ nicht 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. In Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.

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 angegeben haben.

   Weitere Informationen finden Sie in der Installations- und Wartungsanleitung 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-Netzwerkkonfiguration 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: für eine StorageGRID-Appliance, wenn das Clientnetzwerk während der Erstinstallation mit dem StorageGRID-Appliance-Installationsprogramm nicht konfiguriert wurde, kann es in diesem Dialogfeld „Grid Manager“ nicht 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. In Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.

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

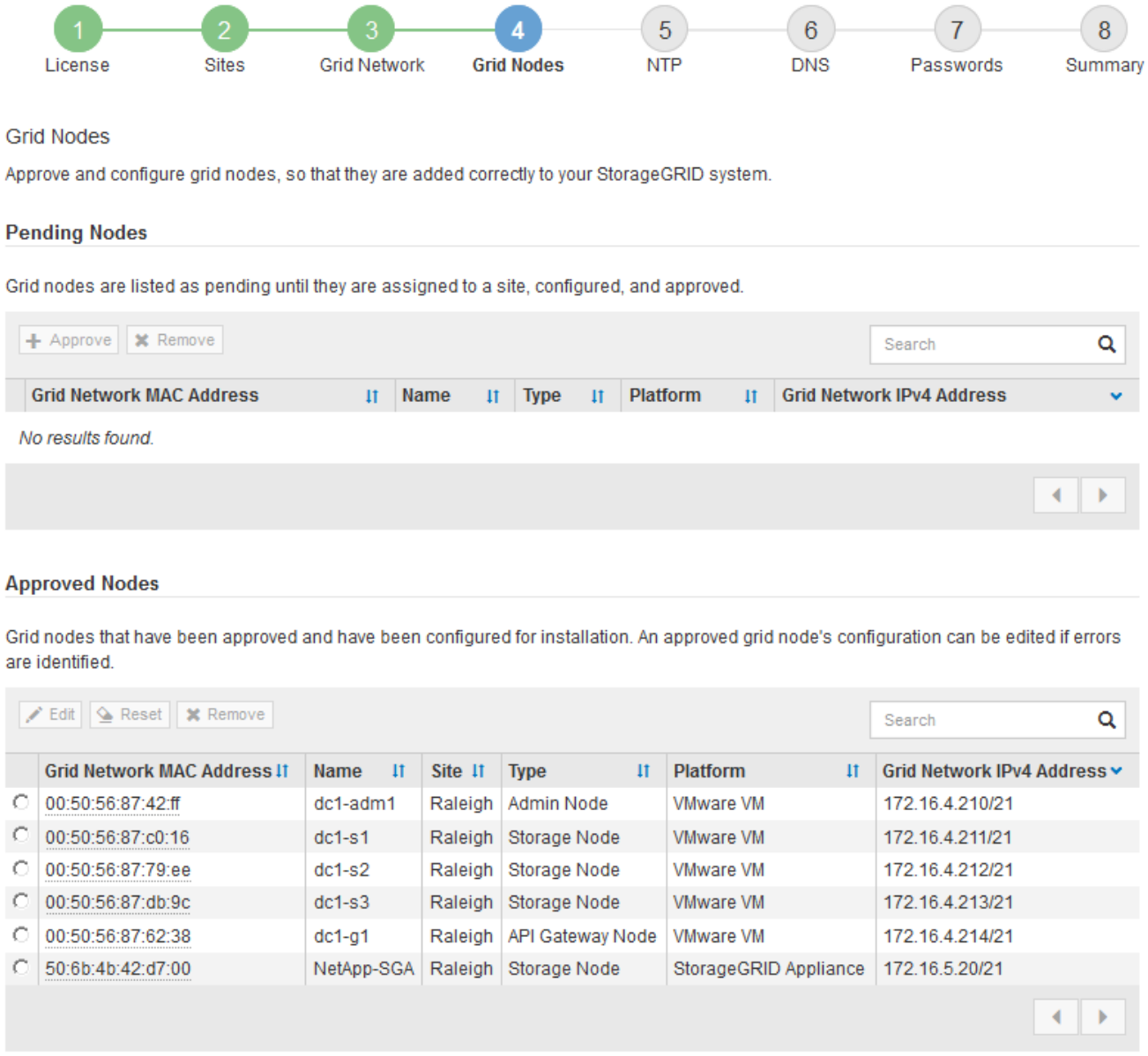
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.

   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 angegeben haben.

      Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

8. Klicken Sie Auf **Speichern**.

Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



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**.

Angeben von Informationen zum Network Time Protocol-Server

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.

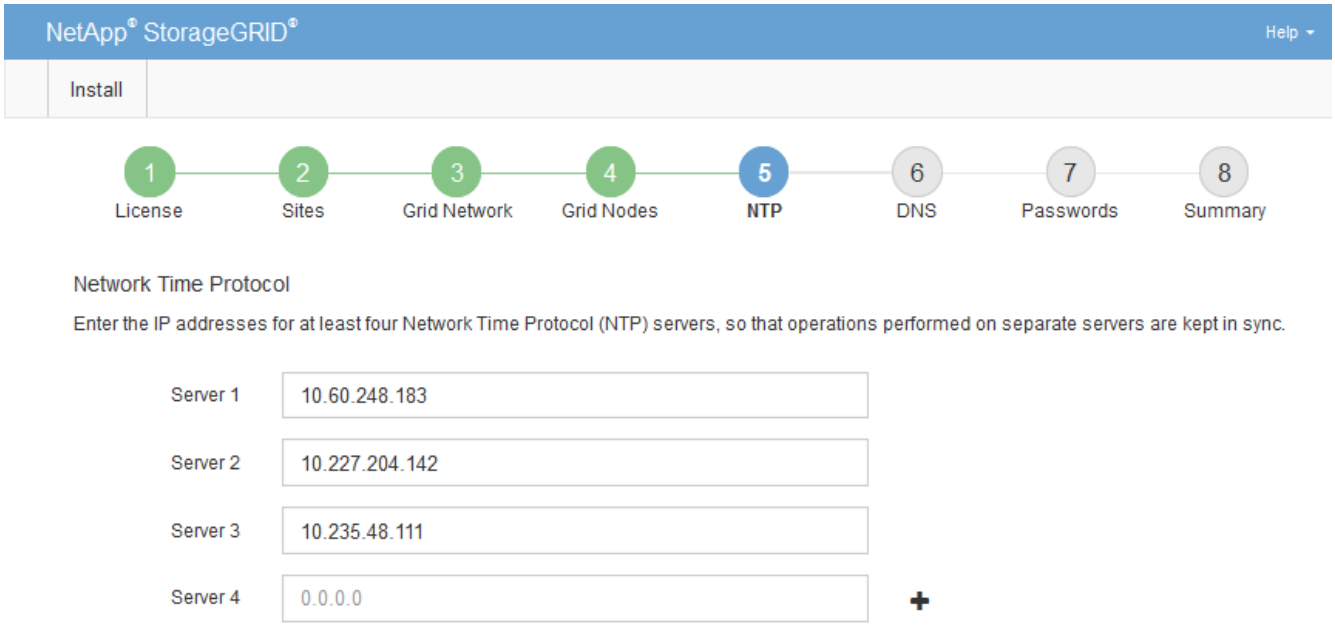
> Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht 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.



3. Wählen Sie **Weiter**.

Verwandte Informationen

"Netzwerkrichtlinien"

Angeben von Informationen zum DNS-Server

Sie müssen DNS-Informationen (Domain Name System) für Ihr StorageGRID-System angeben, damit Sie auf externe Server zugreifen können, indem Sie Hostnamen anstelle von IP-Adressen verwenden.

Über diese Aufgabe

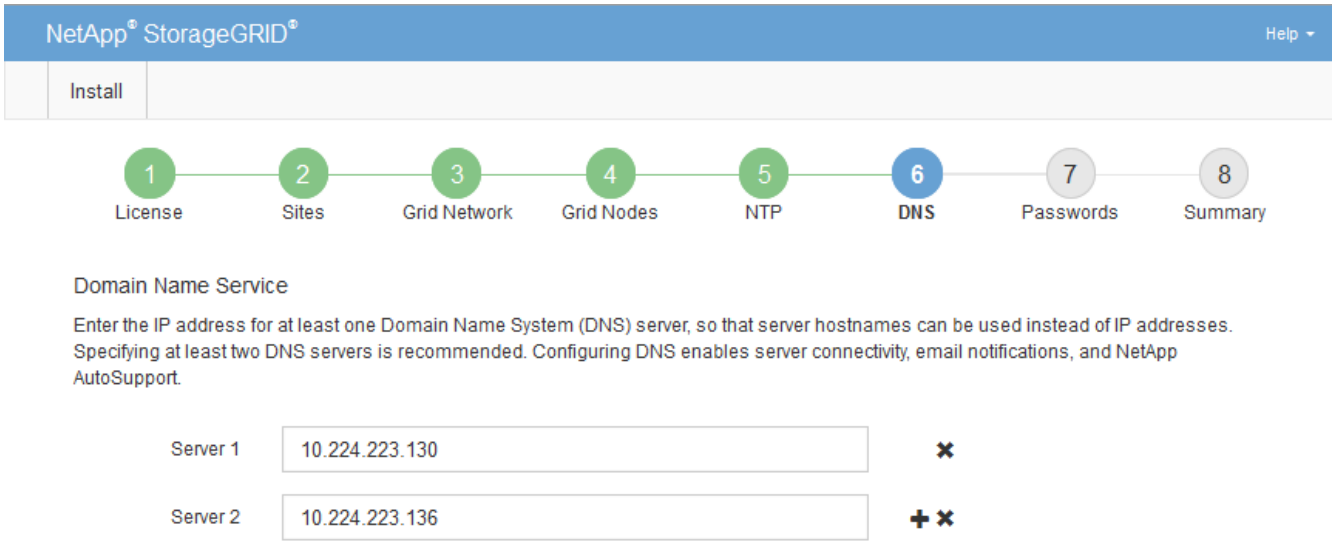
Wenn Sie DNS-Serverinformationen angeben, können Sie vollständig qualifizierte Domänennamen (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport verwenden. Es wird empfohlen, mindestens zwei DNS-Server anzugeben.

> ⓘ Geben Sie zwei bis sechs IPv4-Adressen für DNS-Server an. Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen. Weitere Informationen finden Sie in den Informationen zum Ändern der DNS-Konfiguration in den Wiederherstellungsanleitungen und Wartungsanweisungen.

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.



   Als Best Practice empfehlen wir, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Festlegen der Passwörter für das StorageGRID-System

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 müssen über die Provisionierungs-Passphrase für Installation, Erweiterung und Wartung verfügen, 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 der Grid-Verwaltung kann mit dem Grid Manager geändert werden.
- Zufällig generierte Befehlszeilenkonsole und SSH-Passwörter werden in der Datei Passwords.txt im Wiederherstellungspaket gespeichert.

Schritte

1. Geben Sie unter **Provisioning-Passphrase** das Provisioning-Passphrase ein, das für Änderungen an der Grid-Topologie Ihres StorageGRID-Systems erforderlich ist.

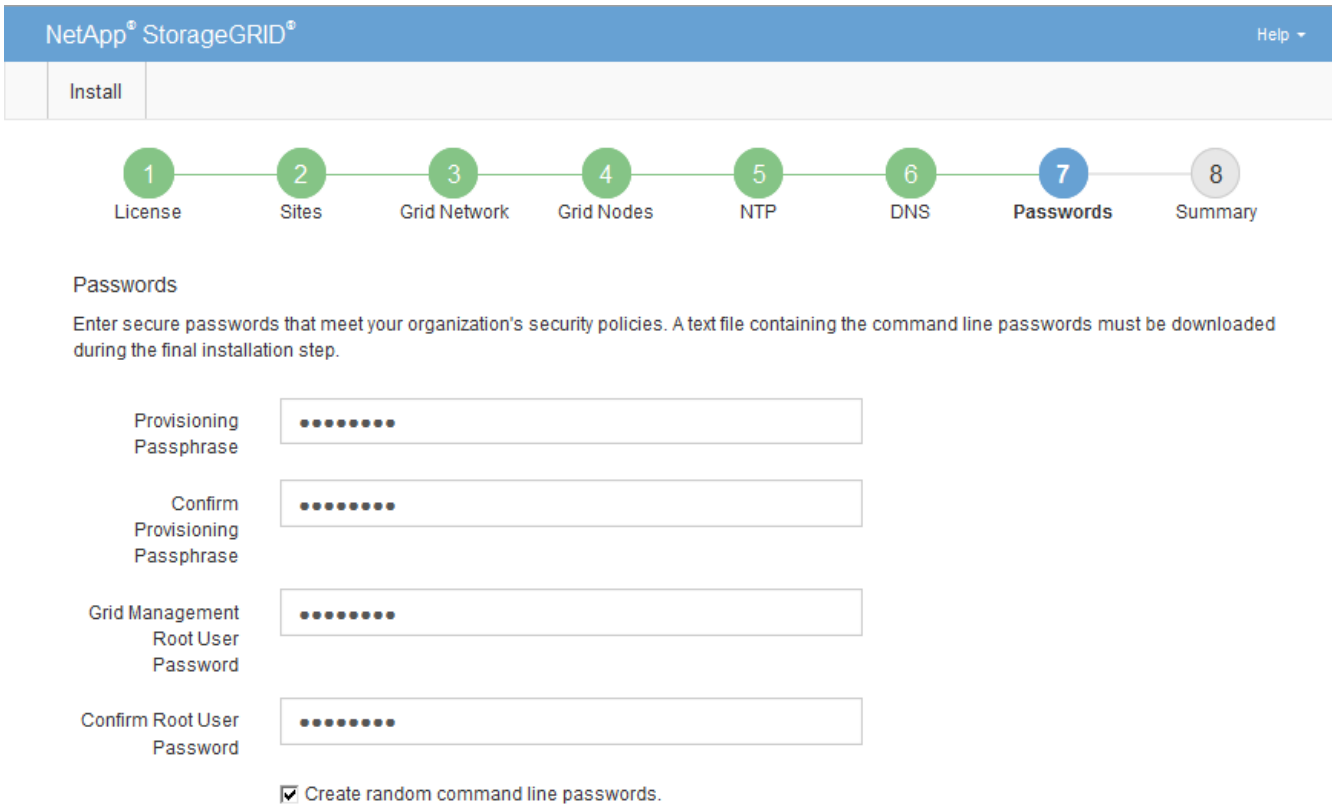
   Speichern Sie die Provisionierungs-Passphrase an einem sicheren Ort.

   > 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.



5. Wenn Sie ein Raster für Proof of Concept- oder Demo-Zwecke installieren, deaktivieren Sie optional das Kontrollkästchen **Create Random command line passwords**.

   Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Deaktivieren Sie **Erstellen von zufälligen Befehlszeilenpasswörtern** nur für Demo-Raster, wenn Sie Standardkennwörter für den Zugriff auf Grid-Knoten aus der Befehlszeile mit dem „`root`“- oder „`admin`“-Konto verwenden möchten.

   > Sie werden aufgefordert, die Recovery Package-Datei herunterzuladen (`sgws-recovery-package-id-revision.zip`Nach dem Klick auf **Installieren** auf der Übersichtsseite. Sie müssen diese Datei herunterladen, um die Installation abzuschließen. Die Passwörter, die für den Zugriff auf das System erforderlich sind, werden in der Datei „Wiederherstellungspaket“ von Passwords.txt gespeichert.

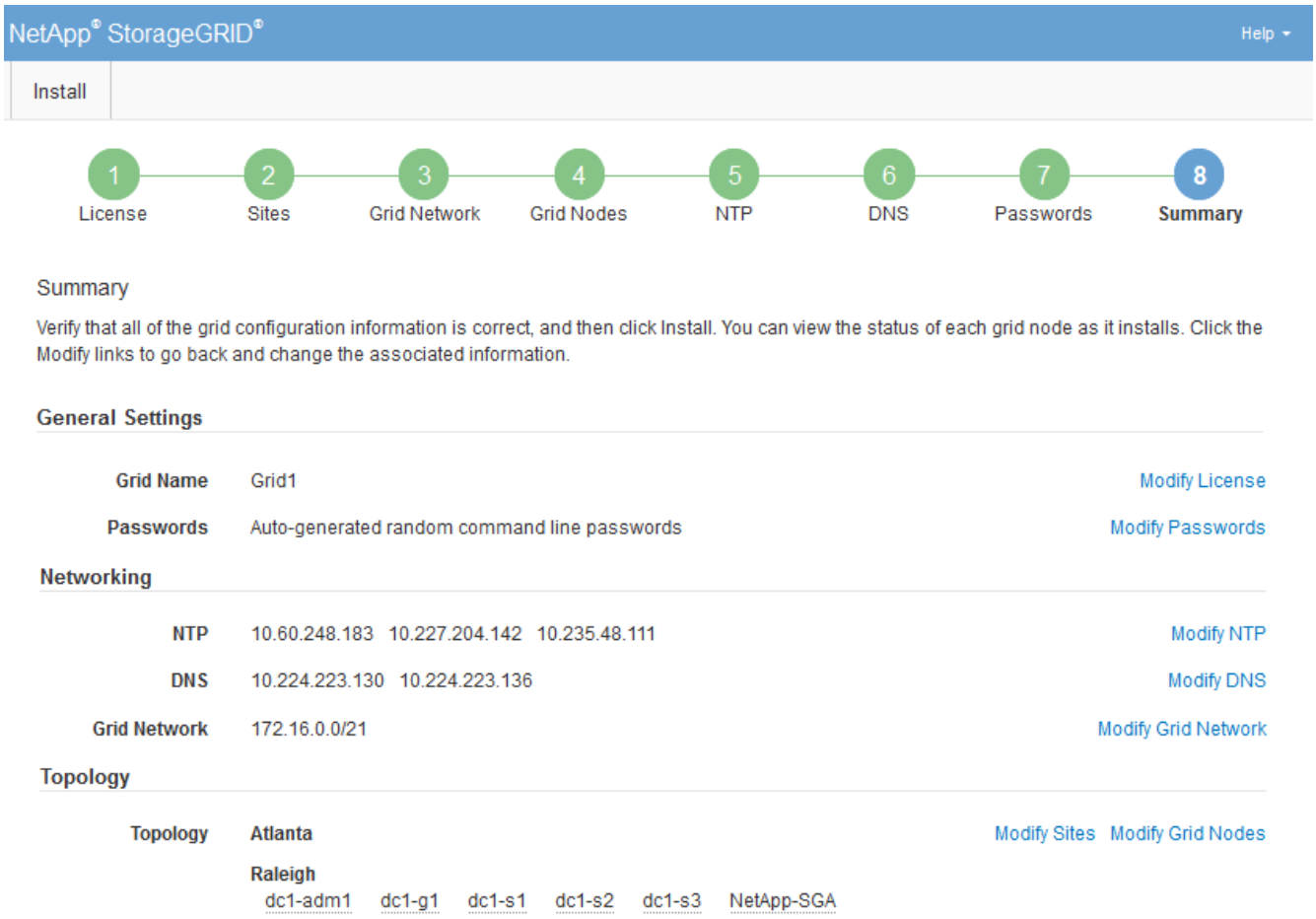
6. Klicken Sie Auf **Weiter**.

Überprüfung Ihrer Konfiguration und Abschluss der 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**.



2. 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.
3. Klicken Sie Auf **Installieren**.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf **Installieren** klicken. Wenn die Verbindung unterbrochen wird, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Siehe "Netzwerkrichtlinien" Entsprechende Details.

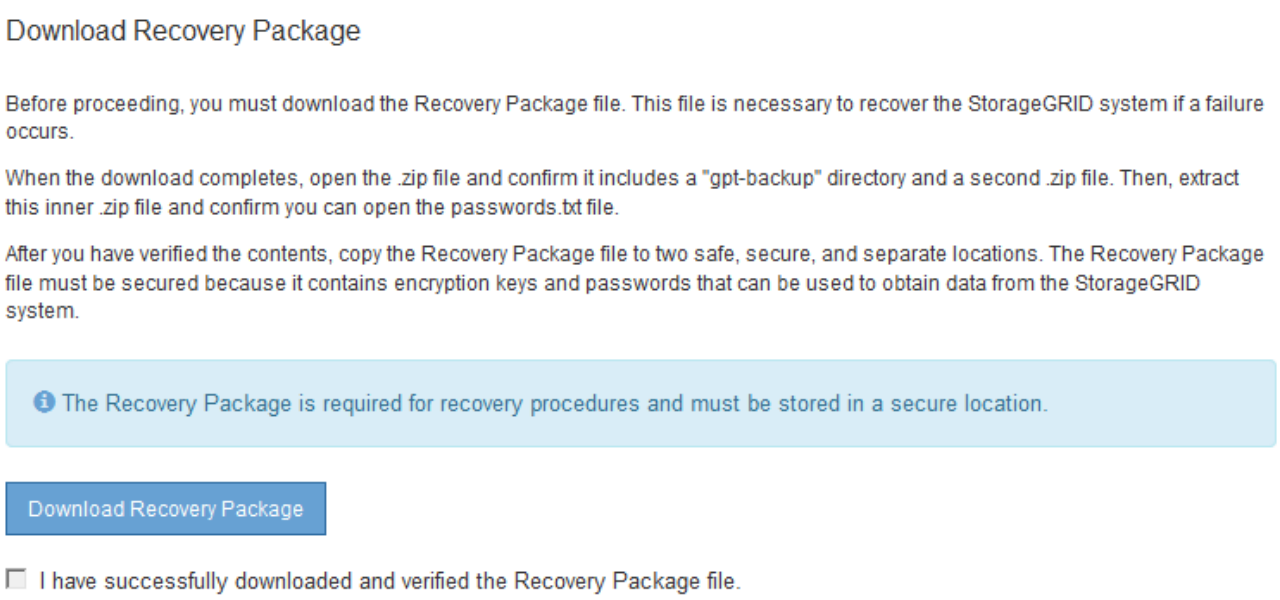
4. Klicken Sie Auf **Download Wiederherstellungspaket**.

   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, Sie können die Installation jedoch erst abschließen und auf das StorageGRID-System zugreifen, wenn Sie diese Datei herunterladen und überprüfen.

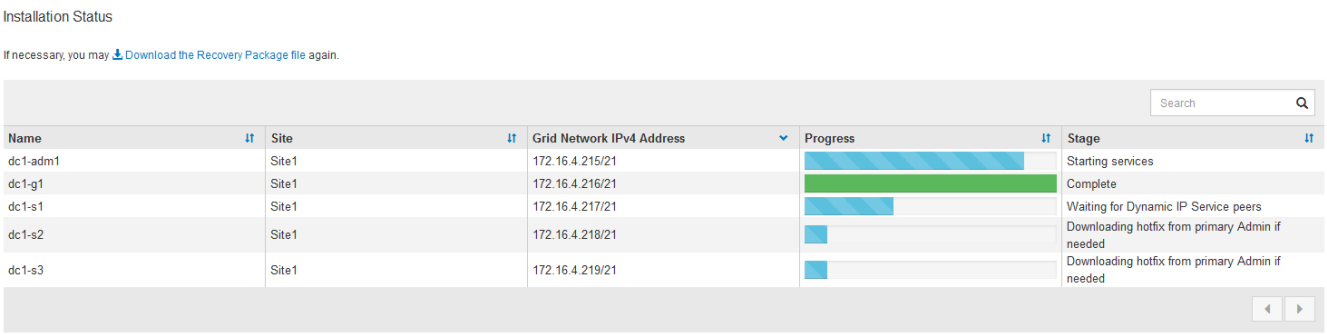
5. Stellen Sie sicher, dass Sie den Inhalt des extrahieren können `.zip` Speichern Sie die Datei an zwei sicheren und separaten Speicherorten.

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 das Recovery Package File** erfolgreich heruntergeladen und verifiziert und klicken Sie auf **Next**.



Wenn die Installation noch läuft, wird die Statusseite angezeigt. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



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. Sie können DHCP während der Konfiguration nicht einrichten.

> 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. Informationen zum Konfigurieren von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- 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. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise neu herstellen.

Automatisierung der Installation

Die Installation des StorageGRID Host Service und die Konfiguration der Grid-Nodes lassen sich automatisieren.

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.

Automatisierung der 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.

Automatisierung der Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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, 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.
```

Verwandte Informationen

"Grid wird konfiguriert und die Installation abgeschlossen"

"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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

Verwandte Informationen

"Automatisierung der Installation"

Weitere Schritte

Nach Abschluss einer Installation müssen Sie eine Reihe von Integrations- und Konfigurationsschritten durchführen. Einige Schritte sind erforderlich, andere sind optional.

Erforderliche Aufgaben

- Erstellen Sie für jedes Client-Protokoll (Swift oder S3) ein Mandantenkonto, das zur Speicherung von Objekten auf Ihrem StorageGRID System verwendet wird.
- Steuern Sie den Systemzugriff, indem Sie Gruppen und Benutzerkonten konfigurieren. Optional können Sie eine föderierte Identitätsquelle (z. B. Active Directory oder OpenLDAP) konfigurieren, sodass Sie Verwaltungsgruppen und Benutzer importieren können. Oder Sie können lokale Gruppen und Benutzer erstellen.
- Integrieren und testen Sie die S3- oder Swift-API-Client-Applikationen zum Hochladen von Objekten auf Ihr StorageGRID System.
- Wenn Sie bereit sind, konfigurieren Sie die Regeln für Information Lifecycle Management (ILM) und die ILM-Richtlinie, die Sie zum Schutz von Objektdaten verwenden möchten.

> Bei der Installation von StorageGRID ist die ILM-Standardrichtlinie, Richtlinie für 2-Basis-Kopien, aktiv. Diese Richtlinie beinhaltet die ILM-Regel (2 Kopien erstellen) für den Bestand und gilt, wenn keine andere Richtlinie aktiviert wurde.

- Wenn in Ihrer Installation Appliance Storage Nodes enthalten sind, führen Sie die folgenden Aufgaben mithilfe der SANtricity Software durch:
  - Stellen Sie Verbindungen zu jeder StorageGRID Appliance her.
  - Eingang der AutoSupport-Daten überprüfen.
- Wenn Ihr StorageGRID-System beliebige Archiv-Knoten enthält, konfigurieren Sie die Verbindung des Archiv-Knotens zum externen Archiv-Speichersystem des Ziels.

> Wenn ein Archiv-Knoten Tivoli Storage Manager als externes Archiv-Speichersystem verwendet, müssen Sie auch Tivoli Storage Manager konfigurieren.

- StorageGRID Richtlinien zur Systemhärtung prüfen und befolgen, um Sicherheitsrisiken zu beseitigen
- Konfigurieren von E-Mail-Benachrichtigungen für Systemalarme.

Optionale Aufgaben

- Wenn Sie Benachrichtigungen vom (alten) Alarmsystem empfangen möchten, konfigurieren Sie Mailinglisten und E-Mail-Benachrichtigungen für Alarme.
- Aktualisieren Sie die IP-Adressen der Grid-Knoten, wenn sie sich seit der Planung der Bereitstellung geändert haben und das Recovery-Paket generiert haben. Weitere Informationen zum Ändern von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- Konfiguration der Storage-Verschlüsselung, falls erforderlich
- Konfigurieren Sie bei Bedarf die Storage-Komprimierung, um die Größe der gespeicherten Objekte zu verringern.
- Konfigurieren des Zugriffs auf Audit-Clients Sie können den Zugriff auf das System für Audit-Zwecke über eine NFS- oder CIFS-Dateifreigabe konfigurieren. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

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 in den Anweisungen zum Überwachen und Beheben von StorageGRID. Informationen zur Fehlerbehebung bei Problemen mit der Installation finden Sie in den Installations- und Wartungsanweisungen für Ihre Geräte. Wenn Sie weitere Hilfe benötigen, wenden Sie sich an den technischen Support.

Verwandte Informationen

"Monitor Fehlerbehebung"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"NetApp Support"

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

Erfahren Sie, wie Sie StorageGRID in VMware Implementierungen installieren.

- "Übersicht über die Installation"
- "Planung und Vorbereitung"
- "Grid-Nodes von Virtual Machines in VMware vSphere Web Client werden implementiert"
- "Grid wird konfiguriert und die Installation abgeschlossen"
- "Automatisierung der Installation"
- "Überblick über DIE REST API zur Installation"
- "Weitere Schritte"
- "Fehlerbehebung bei Installationsproblemen"

Übersicht über die Installation

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 des StorageGRID Networking, damit Sie Ihr Netzwerk entsprechend konfigurieren können. Weitere Informationen finden Sie in den StorageGRID Netzwerkrichtlinien.
   - 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 Installationsverfahren für StorageGRID enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

3. **Konfiguration**: Wenn alle Knoten bereitgestellt wurden, verwenden Sie den StorageGRIDGrid 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.

Verwandte Informationen

"Planung und Vorbereitung"

"Grid-Nodes von Virtual Machines in VMware vSphere Web Client werden implementiert"

"Grid wird konfiguriert und die Installation abgeschlossen"

"Automatisierung der Installation"

"Überblick über DIE REST API zur Installation"

"Netzwerkrichtlinien"

Planung und Vorbereitung

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

> Hardware-spezifische Installations- und Integrationsanweisungen sind nicht im Installationsverfahren für StorageGRID enthalten. Informationen zur Installation von StorageGRID Appliances finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

- Kenntnis der verfügbaren Netzwerkoptionen und Implementierung der einzelnen Netzwerkoptionen auf Grid Nodes Siehe StorageGRID Netzwerkrichtlinien.
- Sammeln Sie alle Netzwerkinformationen im Voraus. Wenn Sie nicht DHCP verwenden, sammeln Sie die IP-Adressen, die jedem Grid-Node zugewiesen werden sollen, und die IP-Adressen des Domain Name System (DNS) und der von Ihnen verwendeten NTP-Server (Network Time Protocol).
- Legen Sie fest, welche der verfügbaren Implementierungs- und Konfigurationstools Sie verwenden möchten.

Verwandte Informationen

"Netzwerkrichtlinien"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

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 für VMware	Sie müssen das StorageGRID-Installationsarchiv herunterladen und die Dateien extrahieren.

Element	Hinweise
VMware Software und Dokumentation	Während der Installation implementieren Sie virtuelle Grid-Knoten auf virtuellen Maschinen in VMware vSphere Web Client.Unterstützte Versionen finden Sie in der Interoperabilitäts-Matrix.
Service-Laptop	Das StorageGRID-System wird über einen Service-Laptop installiert der Service-Laptop muss Folgendes haben: • Netzwerkport • SSH-Client (z. B. PuTTY) • Unterstützter Webbrowser
StorageGRID-Dokumentation	• Versionshinweise • Anweisungen für die Administration von StorageGRID

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Herunterladen und Extrahieren der StorageGRID-Installationsdateien"

"Anforderungen an einen Webbrowser"

"StorageGRID verwalten"

"Versionshinweise"

Herunterladen und Extrahieren der StorageGRID-Installationsdateien

Sie müssen die StorageGRID-Installationsarchive herunterladen und die Dateien extrahieren.

Schritte

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "NetApp Downloads: 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 Warnung/MusterLeseanweisung 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 den Recovery- und Wartungsanleitungen.

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.

6. Wählen Sie in der Spalte **Install StorageGRID** die entsprechende Software aus.

   Laden Sie die herunter `.tgz` Oder `.zip` Archivieren Sie die Datei für Ihre Plattform.

   - `StorageGRID-Webscale-version-VMware-uniqueID.zip`
   - `StorageGRID-Webscale-version-VMware-uniqueID.tgz`

   Verwenden Sie die `.zip` Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

1. Speichern und extrahieren Sie die Archivdatei.
2. 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.
	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 Speicherknoten.

Pfad und Dateiname	Beschreibung
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 `deploy-vsphere-ovftool.sh` Skript:
	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.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:

Verwandte Informationen

"Verwalten Sie erholen"

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.

Weitere Informationen zu unterstützten Versionen von VMware vSphere Hypervisor und VMware vCenter Server Software finden Sie in der Interoperabilitäts-Matrix.

Die Schritte zur Installation dieser VMware-Produkte finden Sie in der VMware-Dokumentation.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

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.

Weitere Informationen zu unterstützten Servern finden Sie in der Interoperabilitäts-Matrix.

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 dediziert für die Ausführung von StorageGRID sind (nicht empfohlen), sollten Sie die Ressourcenanforderungen der anderen Applikationen berücksichtigen.

> 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 und zum Monitoring der CPU- und Arbeitsspeicherauslastung finden Sie in den Anweisungen für die Administration, das Monitoring und das Upgrade von 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 die Informationen über Speicheranforderungen.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Storage- und Performance-Anforderungen erfüllt"

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

"Software-Upgrade"

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 AFF Storage nutzen

Wenn Sie einen StorageGRID Node als Virtual Machine mit Storage implementieren, der einem NetApp AFF System zugewiesen ist, haben Sie bestätigt, dass für das Volume keine FabricPool Tiering-Richtlinie aktiviert ist. Wenn ein StorageGRID Node beispielsweise als virtuelle Maschine auf einem VMware-Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datastore für den 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.

Anzahl der erforderlichen Virtual Machines

Jeder StorageGRID Standort erfordert mindestens drei Storage-Nodes.

Führen Sie in einer Produktionsimplementierung nicht mehr als einen Speicherknoten auf einem virtuellen Maschinenserver 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 Nodes desselben Typs haben (z. B. zwei Gateway-Nodes), installieren Sie nicht alle Instanzen auf demselben Virtual-Machine-Host.

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 zum Wiederherstellen von Grid-Nodes verwendet werden. Beachten Sie stattdessen die Recovery- und Wartungsabläufe 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
Storage-Node	100 GB LUN FÜR OS 3 LUNs für jeden Speicherknoten auf diesem Host **Hinweis**: Ein Speicherknoten kann 1 bis 16 Speicher-LUNs haben; mindestens 3 Speicher-LUNs werden empfohlen. Mindestgröße pro LUN: 4 TB Maximale getestete LUN-Größe: 39 TB.
Gateway-Node	100 GB LUN FÜR OS
Archiv-Node	100 GB LUN FÜR OS

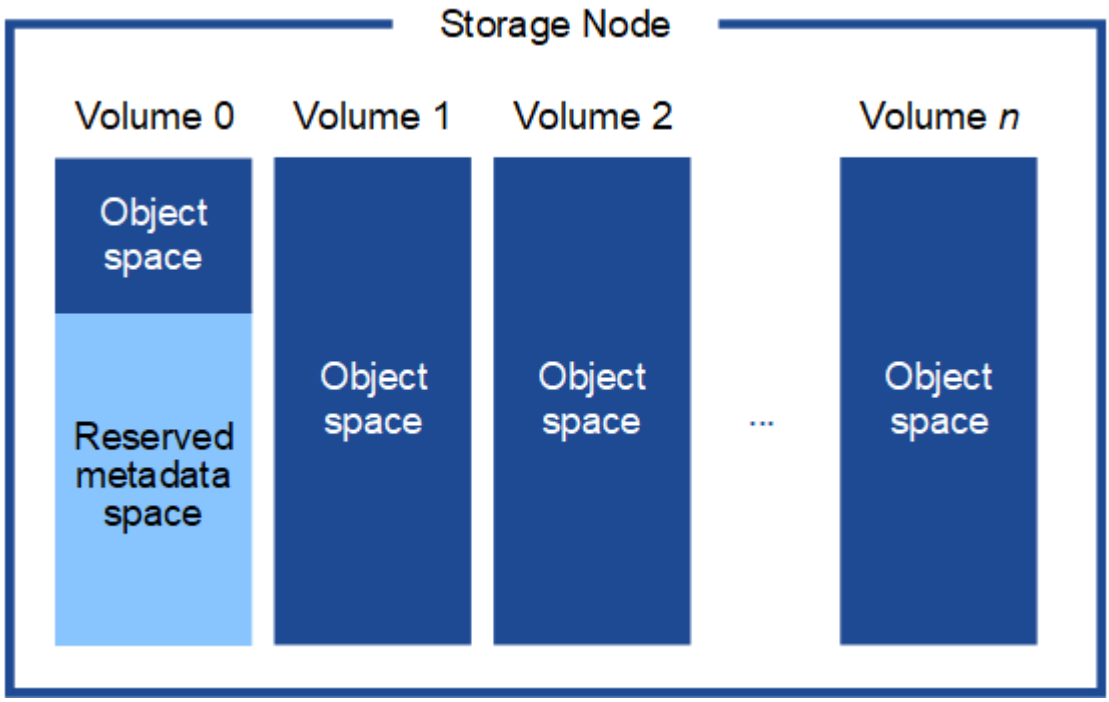
Je nach konfiguriertem Audit Level, Größe der Benutzereingaben wie z. B. S3-Objektschlüsselname und wie viele Audit-Protokoll-Daten Sie erhalten müssen, müssen Sie möglicherweise die Größe der Audit-Protokoll-LUN auf jedem Admin-Node erhöhen. In der Regel generiert ein Grid etwa 1 KB Audit-Daten pro S3-Betrieb. Dies bedeutet, dass ein 200 GB-LUN 70 Millionen Operationen pro Tag und 800 Operationen pro Sekunde für zwei bis drei Tage unterstützen würde.

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 ein neues StorageGRID 11.5-System installieren und jeder Speicherknoten 128 GB oder mehr RAM hat, sollten Sie Volume 0 8 TB oder mehr zuweisen. 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 Anweisungen zum Verwalten von StorageGRID und suchen nach „`managing Objekt-Metadaten-Storage`“.

"StorageGRID verwalten"

Verwandte Informationen

"Verwalten Sie erholen"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Grid-Nodes von Virtual Machines in VMware vSphere Web Client werden implementiert

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 Netzwerken verbunden. Wenn Sie Speicherknoten für StorageGRID-Appliances bereitstellen müssen, lesen Sie die Installations- und Wartungsanleitung für die Appliance, nachdem Sie alle Grid-Nodes für Virtual Machines bereitgestellt haben.

- "Sammeln von Informationen über die Bereitstellungsumgebung"
- "Ermitteln der primären Admin-Node durch Grid-Nodes"
- "StorageGRID-Knoten als virtuelle Maschine implementieren"

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG5600 Storage Appliances"

"SG5700 Storage-Appliances"

"SG6000 Storage-Appliances"

Sammeln von Informationen über die Bereitstellungsumgebung

Bevor Sie Grid-Nodes bereitstellen, müssen Sie Informationen über Ihre Netzwerkkonfiguration und die VMware Umgebung erfassen.

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 DHCP nicht verwenden, erhalten Sie die erforderlichen Netzwerkdetails für jeden Grid-Node (IP-Adresse, Gateway und Netzwerkmaske).
- Wenn Sie DHCP nicht verwenden, lautet die IP-Adresse des primären Admin-Nodes im Grid-Netzwerk. 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.

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 „SStorage- 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 (Domain Name System

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 mit einem Multicast Domain Name System (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 jedoch nicht normalerweise über Subnetze routingfähig ist, können Nodes in anderen Subnetzen die IP-Adresse des primären Admin-Node nicht direkt erfassen.

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.

StorageGRID-Knoten als virtuelle Maschine implementieren

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. Optional können Sie Node-Ports neu zuordnen oder die CPU- oder Speichereinstellungen für den Node erhöhen, bevor Sie den Node einschalten.

Was Sie benötigen

- Sie haben die Planungs- und Vorbereitungsthemen besprochen und die Anforderungen an Software, CPU und RAM sowie Speicher und Leistung verstanden.

  "Planung und Vorbereitung"

- 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:

```
NetApp-<em>SG-version</em>-SHA.vmdk
```

- 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.

Dateiname	Beschreibung
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 Speicherknoten.

- 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 Speicherknoten auf einem virtuellen Maschinenserver 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, verfügen Sie über die Anweisungen zum erweitern eines StorageGRID Systems bzw. der Recovery- und Wartungsanweisungen.
  - "Erweitern Sie Ihr Raster"
  - "Verwalten Sie erholen"
- Wenn Sie einen StorageGRID Node als Virtual Machine mit Storage implementieren, der einem NetApp AFF System zugewiesen ist, haben Sie bestätigt, dass für das Volume keine FabricPool Tiering-Richtlinie aktiviert ist. Wenn ein StorageGRID Node beispielsweise als virtuelle Maschine auf einem VMware-Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datastore für den 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.

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 Ports des Node neu zuordnen müssen, schalten Sie den neuen Node erst ein, wenn die Port-Konfiguration neu zugeordnet 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-<em>SG-version</em>-SHA.vmdk
   vsphere-<em>node</em>.ovf
   vsphere-<em>node</em>.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-<em>SG-version</em>-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 leichter zu managen. RDMs können eine bessere Performance für Workloads mit größeren Objektgrößen bieten (z. B. über 100 MB).

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 Clientnetzwerk 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 leichter zu managen. RDMs können eine bessere Performance für Workloads mit größeren Objektgrößen bieten (z. B. über 100 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.

"Netzwerkrichtlinien"

> Weisen Sie die in den Load Balancer-Endpunkten verwendeten Ports nicht erneut zu.

a. Wählen Sie die neue VM aus.
b. Wählen Sie auf der Registerkarte Konfigurieren die Option **Einstellungen** > **vApp Optionen**.

> Der Standort von **vApp Options** 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, wird die ausgehende Kommunikation für den Port nicht geändert.

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 wird konfiguriert und die Installation abgeschlossen

Die Installation wird durch Konfiguration des StorageGRID-Systems vom Grid-Manager auf dem primären Admin-Node abgeschlossen.

- "Navigieren zum Grid Manager"
- "Angeben der StorageGRID-Lizenzinformationen"
- "Hinzufügen von Sites"
- "Angeben von Grid-Netzwerknetzen"
- "Genehmigung ausstehender Grid-Knoten"
- "Angeben von Informationen zum Network Time Protocol-Server"
- "Angeben von Informationen zum DNS-Server"
- "Festlegen der Passwörter für das StorageGRID-System"
- "Überprüfung Ihrer Konfiguration und Abschluss der Installation"
- "Richtlinien nach der Installation"

Navigieren zum Grid Manager

Mit dem Grid Manager können Sie alle Informationen definieren, die für die Konfiguration des StorageGRID Systems erforderlich sind.

Was Sie benötigen

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`

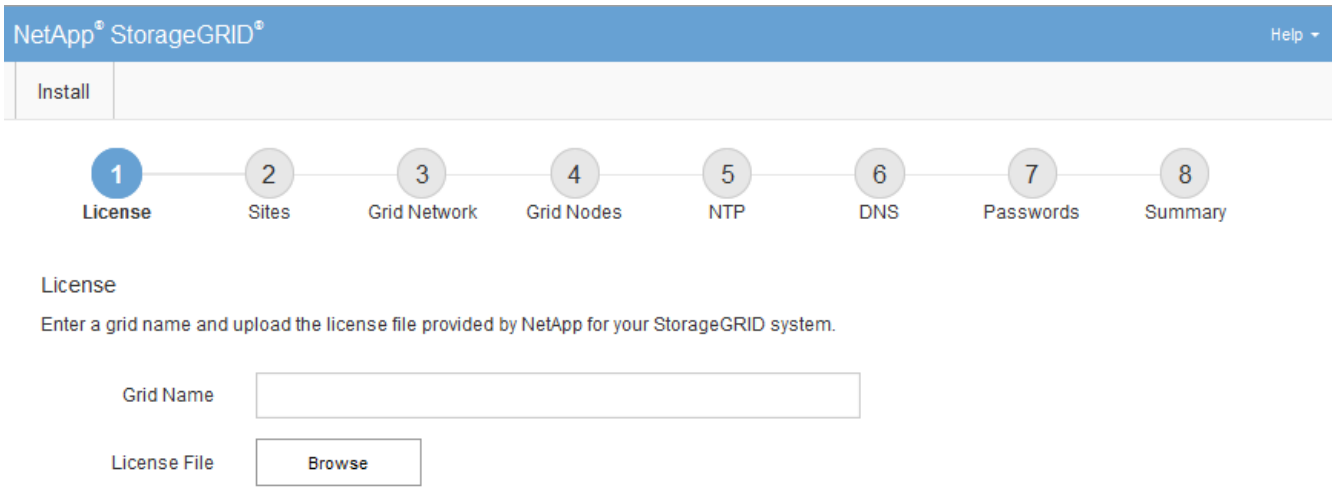
   Alternativ können Sie auf den Grid Manager an Port 8443 zugreifen:

   `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. Klicken Sie auf **StorageGRID-System installieren**.

   Die Seite zum Konfigurieren eines StorageGRID-Rasters wird angezeigt.



Angeben der StorageGRID-Lizenzinformationen

Sie müssen den Namen Ihres StorageGRID Systems angeben und die Lizenzdatei von NetApp hochladen.

Schritte

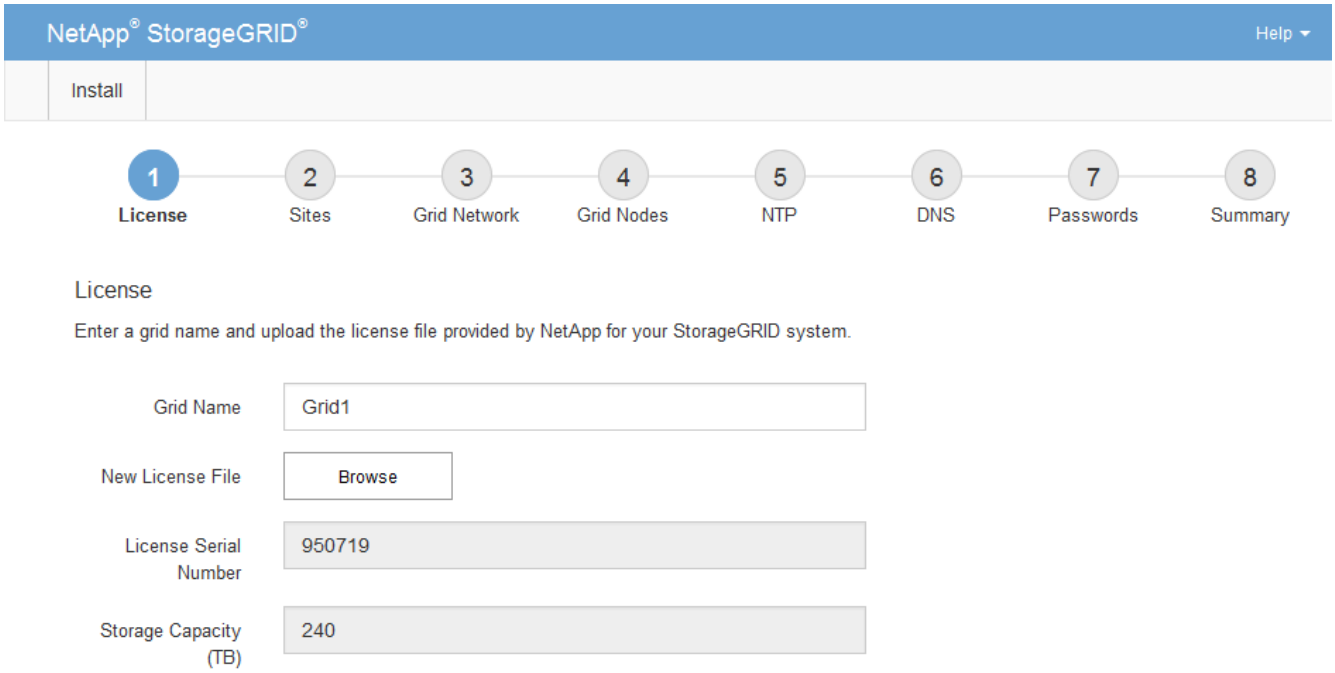
1. Geben Sie auf der Seite Lizenz einen aussagekräftigen Namen für Ihr StorageGRID-System in **Rastername** ein.

   Nach der Installation wird der Name oben im Menü Nodes angezeigt.

2. Klicken Sie auf **Durchsuchen** und suchen Sie die NetApp Lizenzdatei (`NLFunique_id.txt`Und klicken Sie auf **Öffnen**.

   Die Lizenzdatei wird validiert, die Seriennummer und die lizenzierte Speicherkapazität werden 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.



3. Klicken Sie Auf **Weiter**.

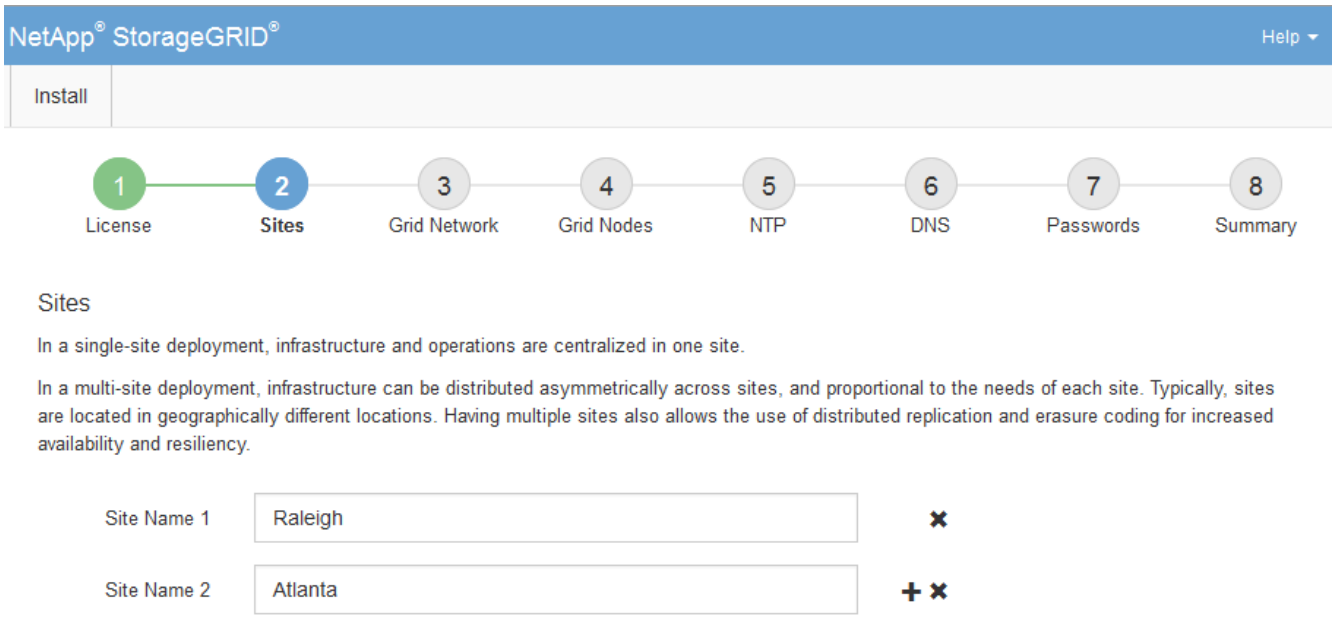
Hinzufügen von Sites

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.



3. Klicken Sie Auf **Weiter**.

Angeben von Grid-Netzwerknetzen

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

Über diese Aufgabe

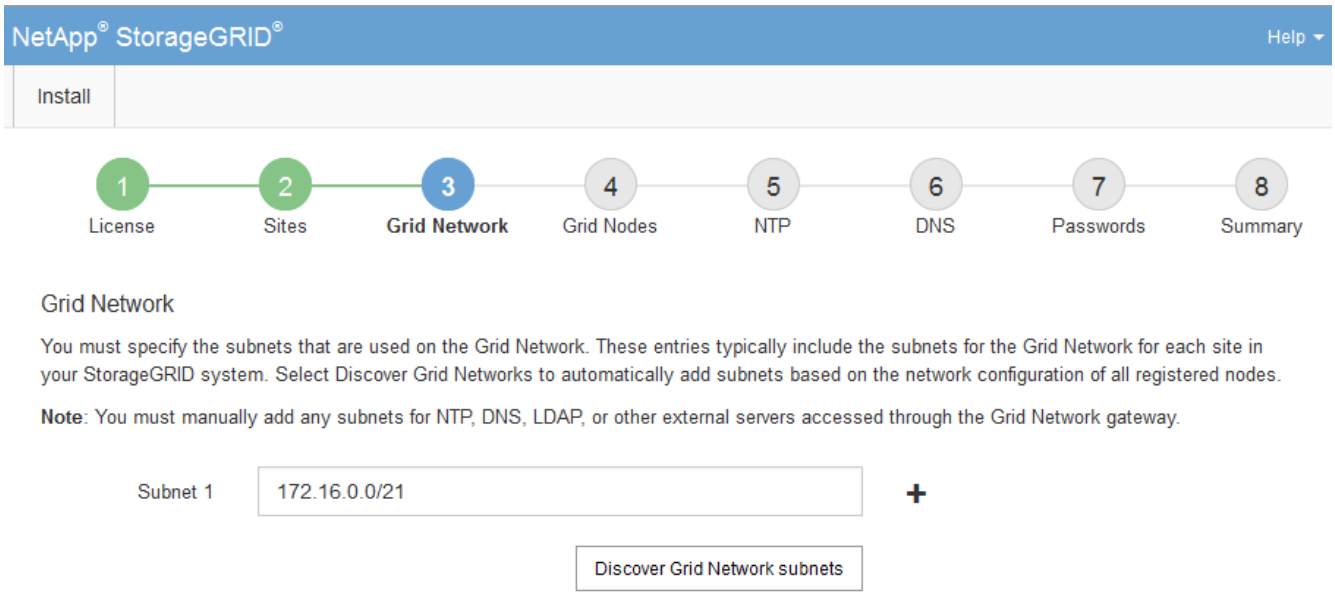
Die Subnetzeinträge enthalten die Subnetze für das Grid-Netzwerk für jeden Standort im StorageGRID-System sowie alle Subnetze, die über das Grid-Netzwerk erreichbar sein müssen.

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 **Netznetze-Subnetze ermitteln**, um die Netznetzwerksubnetz-Liste automatisch mit den Subnetzen zu füllen, die von Grid-Nodes gemeldet wurden, die beim Grid Manager registriert sind.



3. Klicken Sie Auf **Weiter**.

Genehmigung ausstehender Grid-Knoten

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

Was Sie benötigen

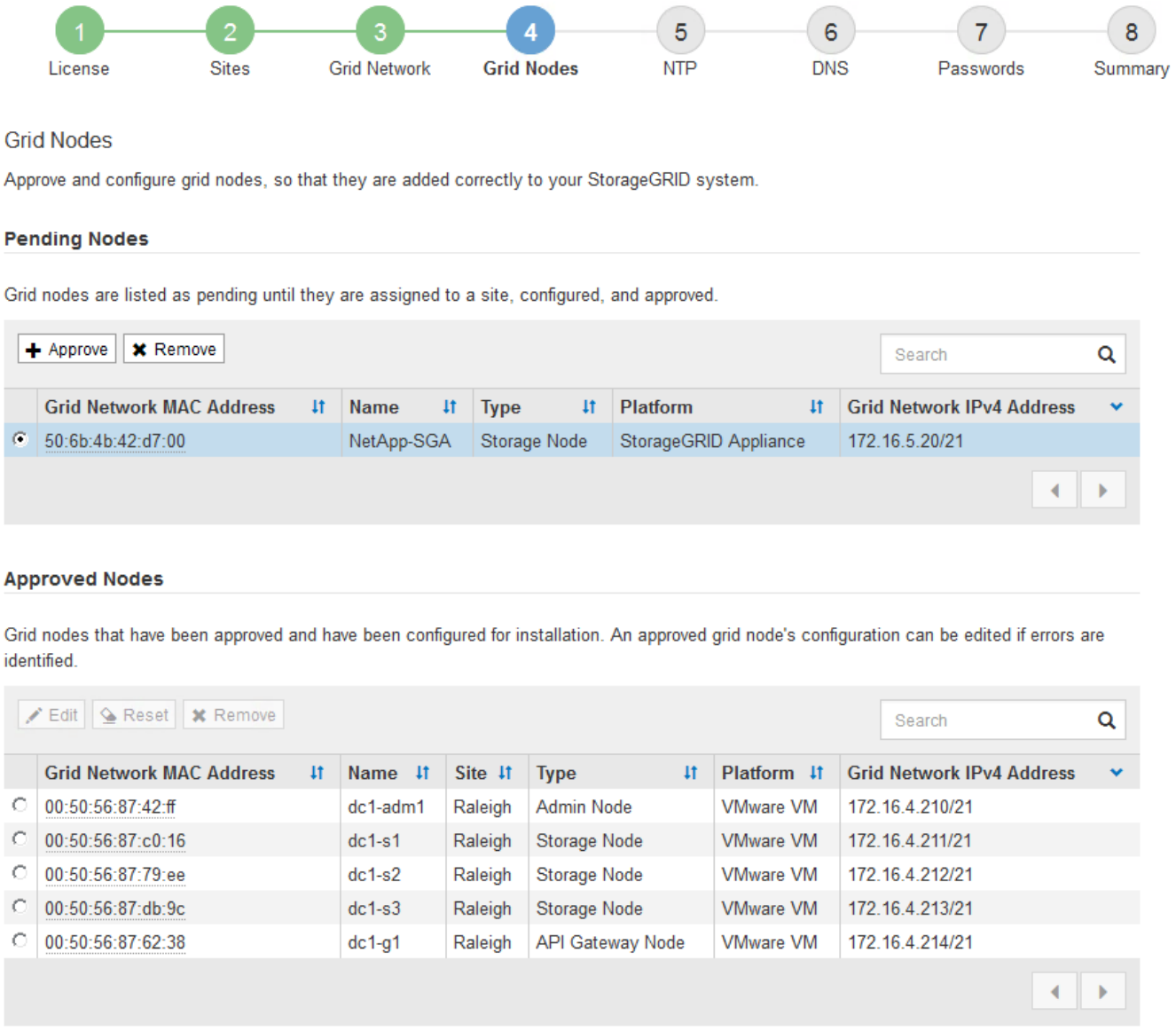
Alle Grid-Nodes von virtuellen und StorageGRID Appliances müssen bereitgestellt worden sein.

Schritte

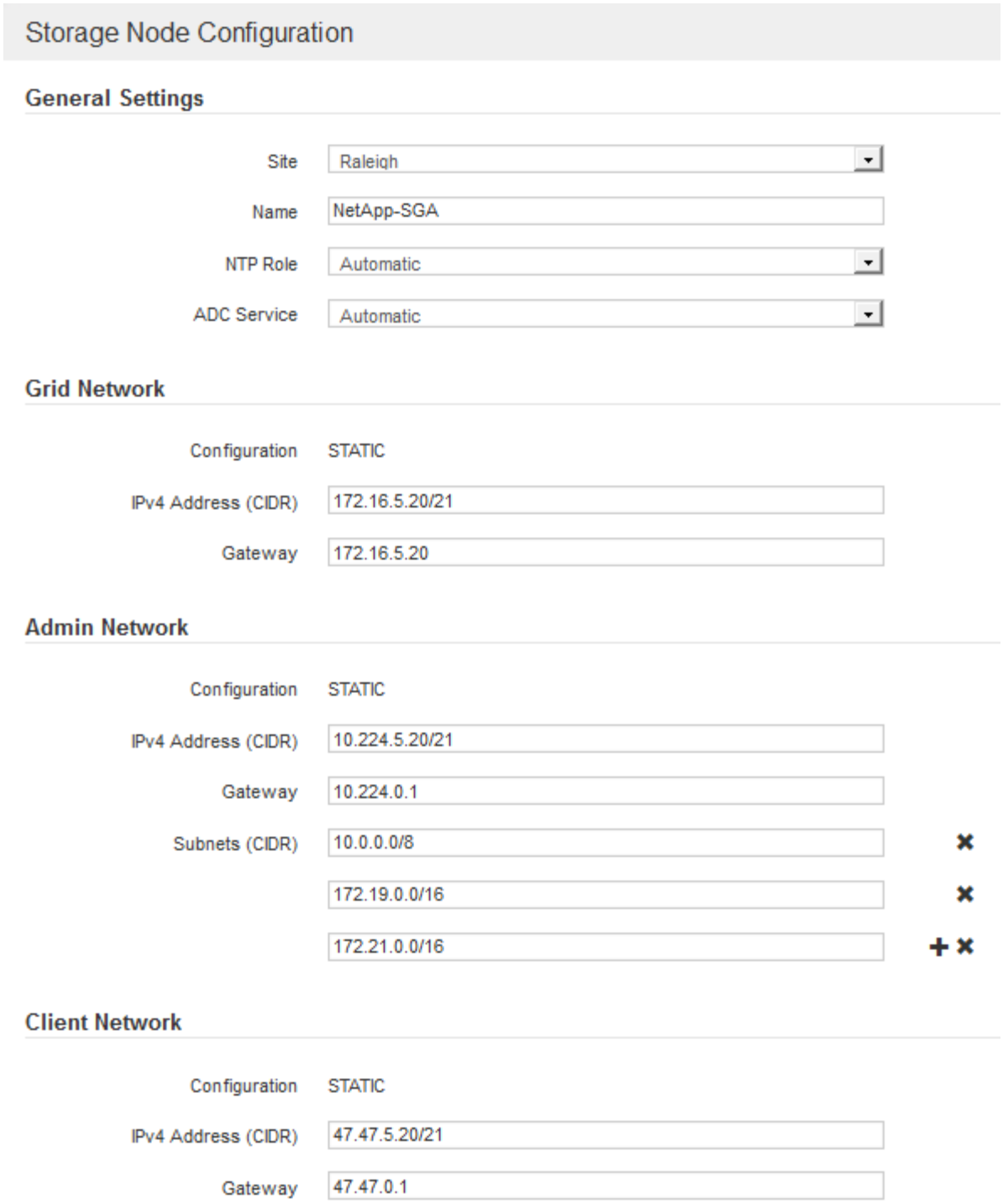
1. Prüfen Sie die Liste ausstehender Nodes und bestätigen Sie, dass alle von Ihnen bereitgestellten Grid-Nodes angezeigt werden.

   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.



3. Klicken Sie Auf **Genehmigen**.
4. Ändern Sie unter Allgemeine Einstellungen die Einstellungen für die folgenden Eigenschaften, falls erforderlich:



- **Standort**: Der Name der Site, mit der dieser Grid-Knoten verknüpft wird.
- **Name**: Der Name, der dem Knoten zugewiesen wird, und der Name, der im Grid Manager angezeigt wird. Der Name ist standardmäßig auf den Namen eingestellt, den Sie beim Konfigurieren des Nodes angegeben haben. In diesem Schritt des Installationsprozesses können Sie den Namen nach Bedarf ändern.

> Nachdem Sie die Installation abgeschlossen haben, können Sie den Namen des Node nicht 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. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, 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-Netzwerkkonfiguration 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: für eine StorageGRID-Appliance, wenn das Admin-Netzwerk während der Erstinstallation mit dem StorageGRID Appliance Installer nicht konfiguriert wurde, kann es in diesem Dialogfeld „Grid Manager“ nicht 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. In Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.

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 angegeben haben.

   Weitere Informationen finden Sie in der Installations- und Wartungsanleitung 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-Netzwerkkonfiguration 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: für eine StorageGRID-Appliance, wenn das Clientnetzwerk während der Erstinstallation mit dem StorageGRID-Appliance-Installationsprogramm nicht konfiguriert wurde, kann es in diesem Dialogfeld „Grid Manager“ nicht 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. In Grid Manager: Wenn der Knoten in der Tabelle genehmigte Knoten aufgeführt ist, setzen Sie den Knoten zurück.

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

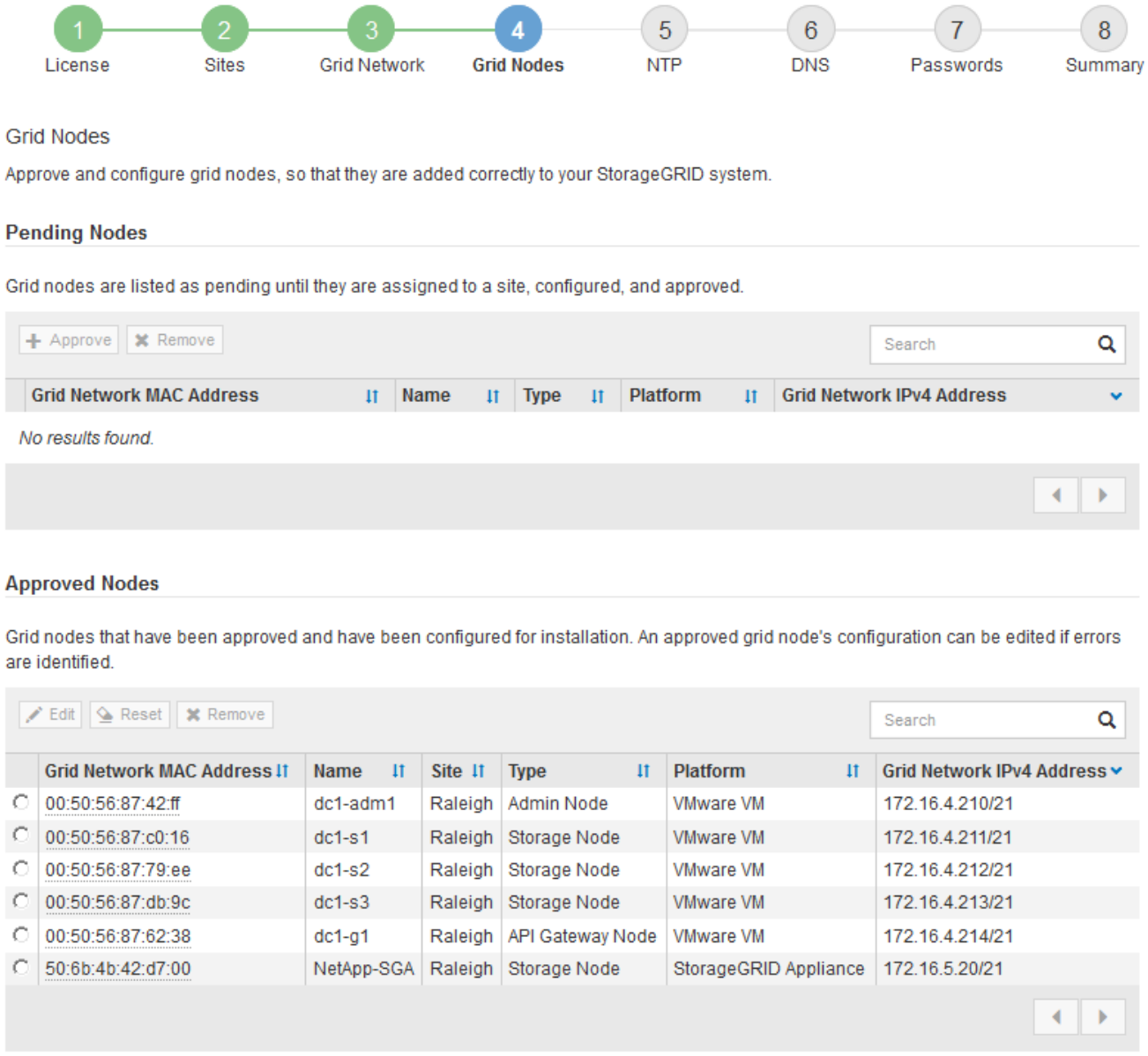
   g. Warten Sie, bis der Knoten wieder in der Liste Ausstehende Knoten angezeigt wird.

   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 angegeben haben.

      Weitere Informationen finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

8. Klicken Sie Auf **Speichern**.

Der Eintrag des Rasterknoten wird in die Liste der genehmigten Knoten verschoben.



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**.

Angeben von Informationen zum Network Time Protocol-Server

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 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"

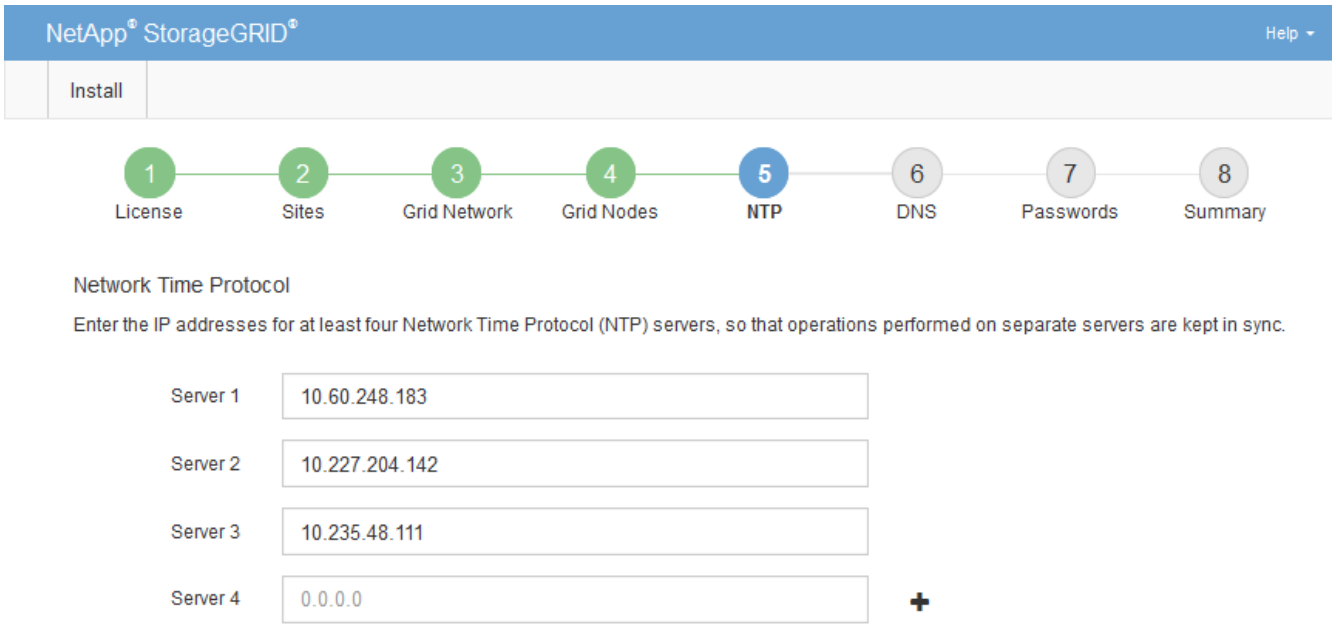
Die externen NTP-Server werden von den Nodes verwendet, denen Sie zuvor primäre NTP-Rollen zugewiesen haben.

> ⓘ 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.



3. Wählen Sie **Weiter**.

Angeben von Informationen zum DNS-Server

Sie müssen DNS-Informationen (Domain Name System) für Ihr StorageGRID-System angeben, damit Sie auf externe Server zugreifen können, indem Sie Hostnamen anstelle von IP-Adressen verwenden.

Über diese Aufgabe

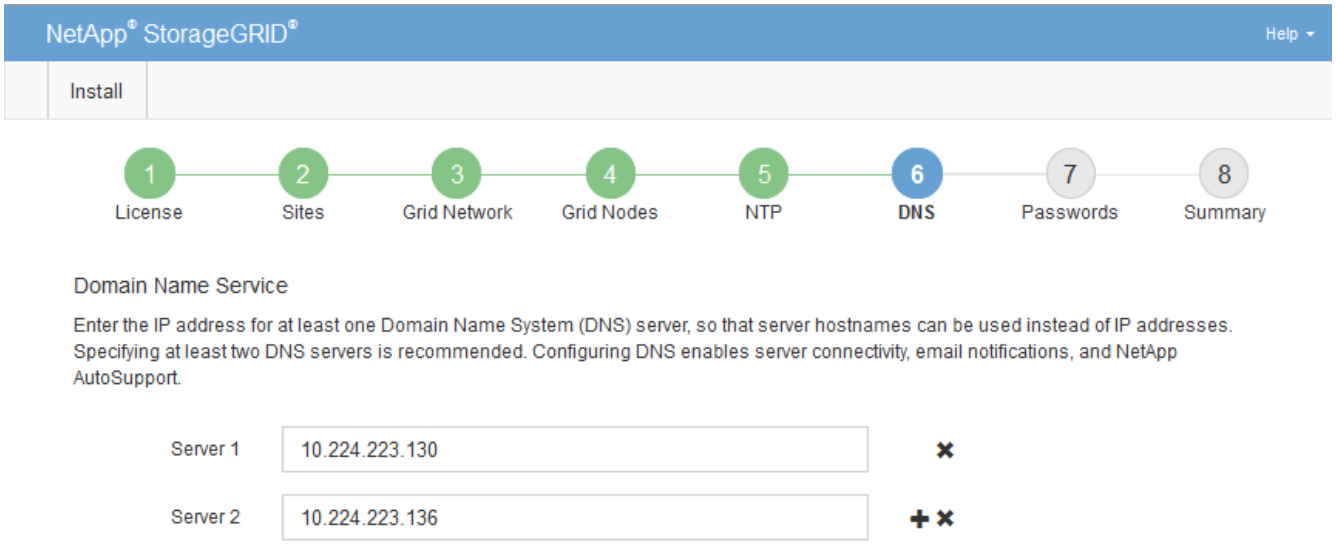
Wenn Sie DNS-Serverinformationen angeben, können Sie vollständig qualifizierte Domänennamen (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail-Benachrichtigungen und AutoSupport verwenden. Es wird empfohlen, mindestens zwei DNS-Server anzugeben.

> ⓘ Geben Sie zwei bis sechs IPv4-Adressen für DNS-Server an. Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen. Weitere Informationen finden Sie in den Informationen zum Ändern der DNS-Konfiguration in den Wiederherstellungsanleitungen und Wartungsanweisungen.

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.



   Als Best Practice empfehlen wir, mindestens zwei DNS-Server anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Wählen Sie **Weiter**.

Verwandte Informationen

"Verwalten Sie erholen"

Festlegen der Passwörter für das StorageGRID-System

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 müssen über die Provisionierungs-Passphrase für Installation, Erweiterung und Wartung verfügen, 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 der Grid-Verwaltung 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.

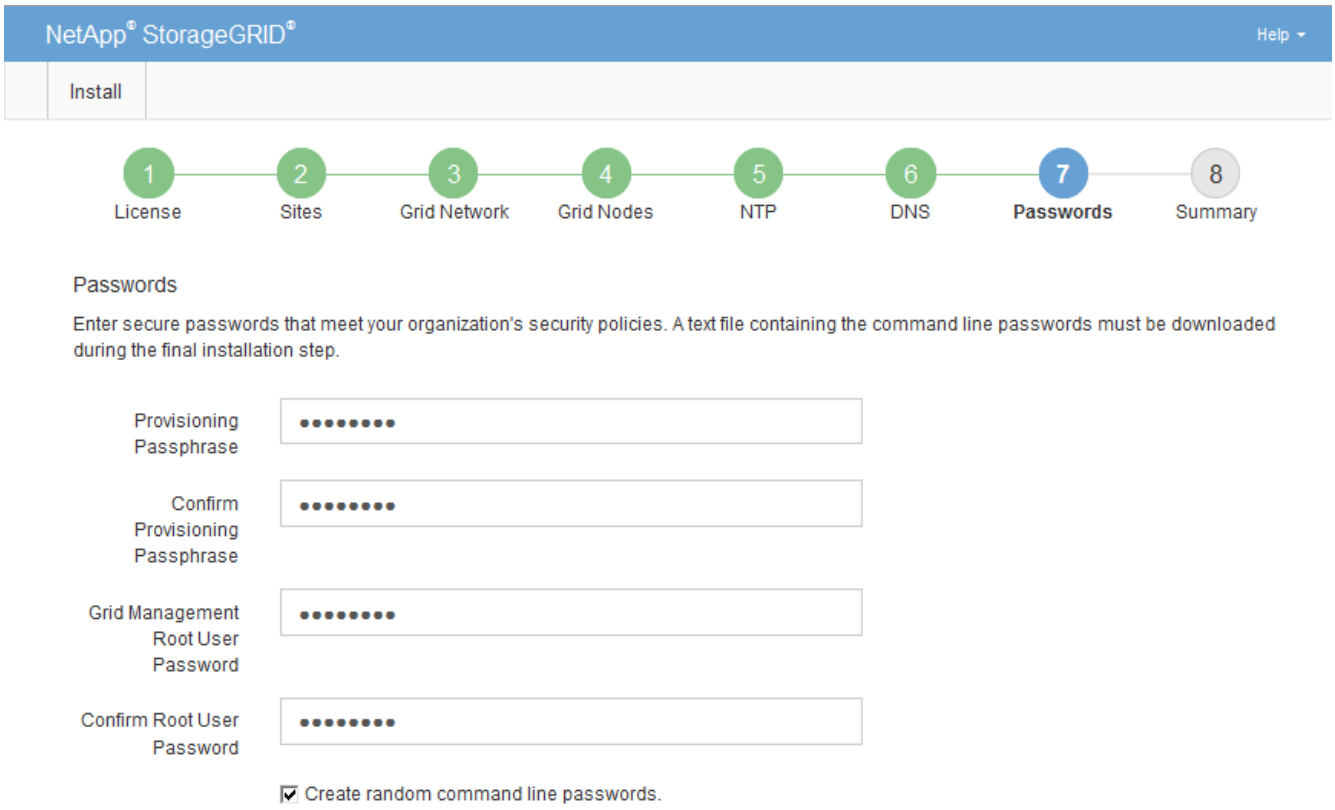
   Speichern Sie die Provisionierungs-Passphrase an einem sicheren Ort.

   > ⓘ 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.



5. Wenn Sie ein Raster für Proof of Concept- oder Demo-Zwecke installieren, deaktivieren Sie optional das Kontrollkästchen **Create Random command line passwords**.

   Bei Produktionsimplementierungen sollten zufällige Passwörter immer aus Sicherheitsgründen verwendet werden. Deaktivieren Sie **Erstellen von zufälligen Befehlszeilenpasswörtern** nur für Demo-Raster, wenn Sie Standardkennwörter für den Zugriff auf Grid-Knoten aus der Befehlszeile mit dem „`root`“- oder „`admin`“-Konto verwenden möchten.

   Sie werden aufgefordert, die Recovery Package-Datei herunterzuladen (`sgws-recovery-package-id-revision.zip`Nach dem Klick auf **Installieren** auf der Übersichtsseite. Sie müssen diese Datei herunterladen, 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.

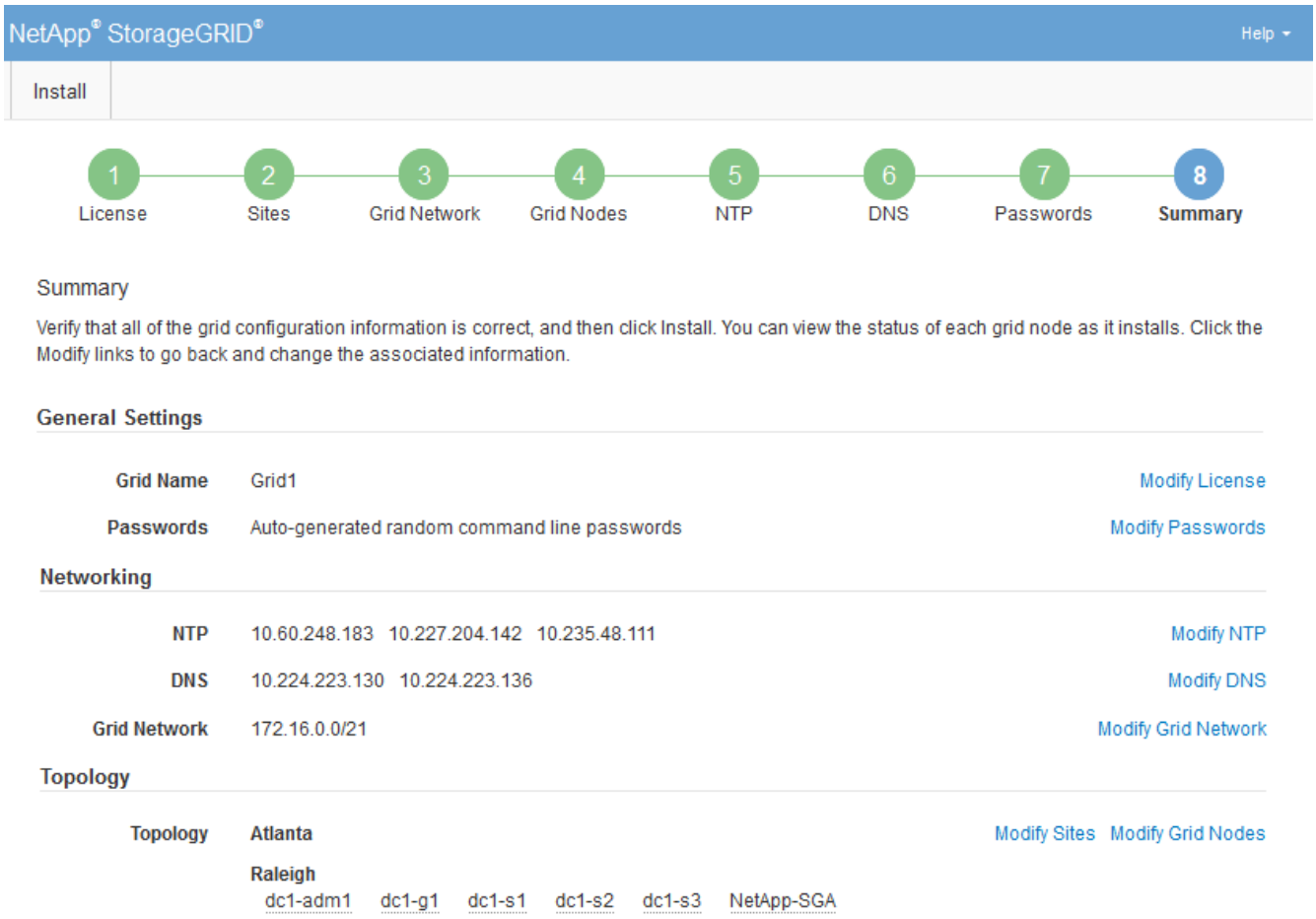
6. Klicken Sie Auf **Weiter**.

Überprüfung Ihrer Konfiguration und Abschluss der 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**.



2. 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.
3. Klicken Sie Auf **Installieren**.

> Wenn ein Knoten für die Verwendung des Client-Netzwerks konfiguriert ist, wechselt das Standard-Gateway für diesen Knoten vom Grid-Netzwerk zum Client-Netzwerk, wenn Sie auf **Installieren** klicken. Wenn die Verbindung unterbrochen wird, müssen Sie sicherstellen, dass Sie über ein zugängliches Subnetz auf den primären Admin-Node zugreifen. Siehe "Netzwerkrichtlinien" Entsprechende Details.

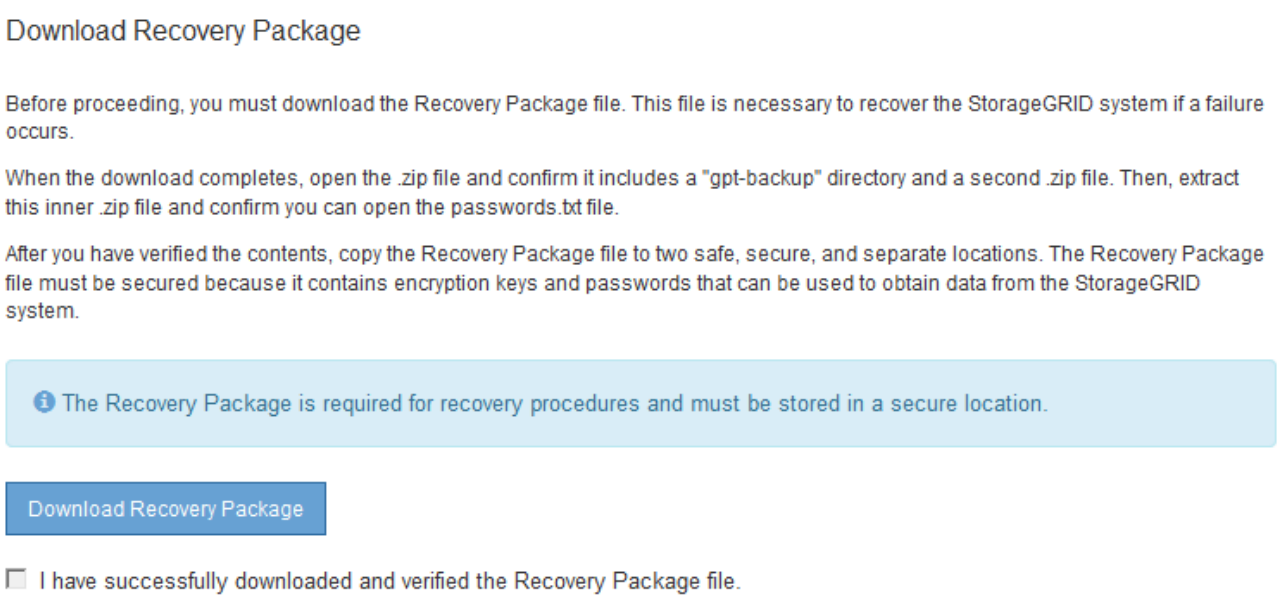
4. Klicken Sie Auf **Download Wiederherstellungspaket**.

   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, Sie können die Installation jedoch erst abschließen und auf das StorageGRID-System zugreifen, wenn Sie diese Datei herunterladen und überprüfen.

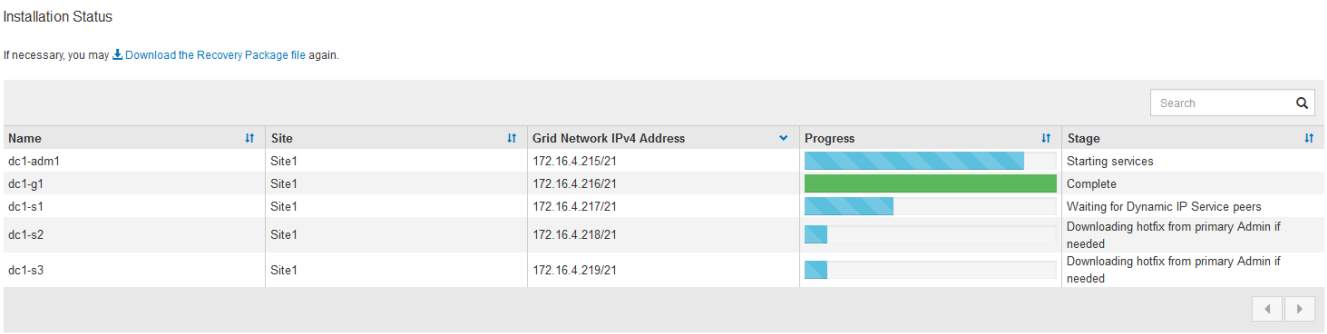
5. Stellen Sie sicher, dass Sie den Inhalt des extrahieren können `.zip` Speichern Sie die Datei an zwei sicheren und separaten Speicherorten.

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 das Recovery Package File** erfolgreich heruntergeladen und verifiziert und klicken Sie auf **Next**.



Wenn die Installation noch läuft, wird die Statusseite angezeigt. Auf dieser Seite wird der Installationsfortschritt für jeden Grid-Knoten angezeigt.



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. Sie können DHCP während der Konfiguration nicht einrichten.

> 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. Informationen zum Konfigurieren von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- 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. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise neu herstellen.

Automatisierung der Installation

Die Implementierung von VMware Virtual Grid-Nodes, die Konfiguration von Grid-Nodes und die Konfiguration von StorageGRID Appliances können automatisiert werden.

- "Automatisierung der Grid Node-Implementierung in VMware vSphere"
- "Automatisierung der Konfiguration von StorageGRID"

Automatisierung der Grid Node-Implementierung in VMware vSphere

Die Implementierung von StorageGRID Grid-Nodes in VMware vSphere lässt sich automatisieren.

Was Sie benötigen

- 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 "Sammeln 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 `.ovf` Und `.mf` Dateien:
vsphere-Primary-admin.ovf vsphere-Primary-admin.mf	Die Vorlagendatei „Open Virtualization Format“ (`.ovf`) Und Manifest-Datei (`.mf`) Für die Bereitstellung des primären Admin-Knotens.
vsphere-nicht-Primary-admin.ovf vsphere-nicht-Primary-admin.mf	Die Vorlagendatei (`.ovf`) Und Manifest-Datei (`.mf`) Für die Bereitstellung von nicht-primären Admin-Knoten.
vsphere-Archive.ovf vsphere-Archive.mf	Die Vorlagendatei (`.ovf`) Und Manifest-Datei (`.mf`) Für die Bereitstellung von Archiv-Knoten.
vsphere-Gateway.ovf vsphere-Gateway.mf	Die Vorlagendatei (`.ovf`) Und Manifest-Datei (`.mf`) Für die Bereitstellung von Gateway-Knoten.
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 `deploy-vsphere-ovftool.sh` Skript:

Definieren der Konfigurationsdatei für Ihre Bereitstellung

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, damit 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=thin
--datastore='<em>datastore_name</em>'
```

  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-<em>version</em>/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 identisch 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 ist. 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 ist. 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".

  Ordnen Sie die Ports, die Sie für die Konfiguration von Load Balancer-Endpunkten 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, jedoch keinen Wert für PORT_REMAP angeben, wird die ausgehende Kommunikation für den Port nicht geändert.

  Ordnen Sie die Ports, die Sie für die Konfiguration von Load Balancer-Endpunkten 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 Neuzuordnung 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.

Verwandte Informationen

"Ermitteln der primären Admin-Node durch Grid-Nodes"

"Netzwerkrichtlinien"

Das Bash-Skript wird ausgeführt

Sie können das verwenden `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.

Was Sie benötigen

- 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
   ```

3. 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
   ```

4. 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               |
+------------------------------+----------+----------------------+
```

Automatisierung der Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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`).

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

Während des Konfigurationsprozesses wird eine ZIP-Datei für das Wiederherstellungspaket erstellt 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 Datei Passwords.txt extrahieren und nach den Kennwörtern suchen, 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 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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. Sie können eine Site erstellen, anzeigen, löschen und ändern.

Weitere Schritte

Nach Abschluss einer Installation müssen Sie eine Reihe von Integrations- und Konfigurationsschritten durchführen. Einige Schritte sind erforderlich, andere sind optional.

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 für jedes Client-Protokoll (Swift oder S3) ein Mandantenkonto, das zur Speicherung von Objekten auf Ihrem StorageGRID System verwendet wird.
- Steuern Sie den Systemzugriff, indem Sie Gruppen und Benutzerkonten konfigurieren. Optional können Sie eine föderierte Identitätsquelle (z. B. Active Directory oder OpenLDAP) konfigurieren, sodass Sie Verwaltungsgruppen und Benutzer importieren können. Oder Sie können lokale Gruppen und Benutzer erstellen.
- Integrieren und testen Sie die S3- oder Swift-API-Client-Applikationen zum Hochladen von Objekten auf Ihr StorageGRID System.
- Wenn Sie bereit sind, konfigurieren Sie die Regeln für Information Lifecycle Management (ILM) und die ILM-Richtlinie, die Sie zum Schutz von Objektdaten verwenden möchten.

  Bei der Installation von StorageGRID ist die ILM-Standardrichtlinie, Richtlinie für 2-Basis-Kopien, aktiv. Diese Richtlinie beinhaltet die ILM-Regel (2 Kopien erstellen) für den Bestand und gilt, wenn keine andere Richtlinie aktiviert wurde.

- Wenn in Ihrer Installation Appliance Storage Nodes enthalten sind, führen Sie die folgenden Aufgaben mithilfe der SANtricity Software durch:
  - Stellen Sie Verbindungen zu jeder StorageGRID Appliance her.
  - Eingang der AutoSupport-Daten überprüfen.
- Wenn Ihr StorageGRID-System beliebige Archiv-Knoten enthält, konfigurieren Sie die Verbindung des Archiv-Knotens zum externen Archiv-Speichersystem des Ziels.

  Wenn ein Archiv-Knoten Tivoli Storage Manager als externes Archiv-Speichersystem verwendet, müssen Sie auch Tivoli Storage Manager konfigurieren.

- StorageGRID Richtlinien zur Systemhärtung prüfen und befolgen, um Sicherheitsrisiken zu beseitigen
- Konfigurieren von E-Mail-Benachrichtigungen für Systemalarme.

Optionale Aufgaben

- Wenn Sie Benachrichtigungen vom (alten) Alarmsystem empfangen möchten, konfigurieren Sie Mailinglisten und E-Mail-Benachrichtigungen für Alarme.
- Aktualisieren Sie die IP-Adressen der Grid-Knoten, wenn sie sich seit der Planung der Bereitstellung geändert haben und das Recovery-Paket generiert haben. Weitere Informationen zum Ändern von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.
- Konfiguration der Storage-Verschlüsselung, falls erforderlich
- Konfigurieren Sie bei Bedarf die Storage-Komprimierung, um die Größe der gespeicherten Objekte zu verringern.
- Konfigurieren des Zugriffs auf Audit-Clients Sie können den Zugriff auf das System für Audit-Zwecke über eine NFS- oder CIFS-Dateifreigabe konfigurieren. Lesen Sie die Anweisungen zum Verwalten von

StorageGRID.

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

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)

Informationen zum Zugriff auf die Protokolldateien finden Sie in den Anweisungen zum Überwachen und Beheben von StorageGRID. Informationen zur Fehlerbehebung bei Problemen mit der Installation finden Sie in den Installations- und Wartungsanweisungen für Ihre Geräte. Wenn Sie weitere Hilfe benötigen, wenden Sie sich an den technischen Support.

Verwandte Informationen

"Monitor Fehlerbehebung"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"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 die 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.

Software-Upgrade

Erfahren Sie, wie Sie ein StorageGRID System auf eine neue Version aktualisieren.

- "Informationen zu StorageGRID 11.5"
- "Planung und Vorbereitung von Upgrades"
- "Durchführen des Upgrades"
- "Fehlerbehebung bei Upgrade-Problemen"

Informationen zu StorageGRID 11.5

Bevor Sie ein Upgrade starten, lesen Sie diesen Abschnitt, um mehr über die neuen Funktionen und Verbesserungen in StorageGRID 11.5 zu erfahren. Sie können ermitteln, ob Funktionen veraltet bzw. entfernt wurden, und erfahren Sie mehr über die Änderungen an StorageGRID APIs.

- "Die Neuheiten in StorageGRID 11.5"
- "Funktionen entfernt oder veraltet"
- "Änderungen an der Grid-Management-API"
- "Änderungen an der Mandantenmanagement-API"

Was ist neu in StorageGRID 11.5

StorageGRID 11.5 führt S3 Object Lock ein, unterstützt die KMIP-Verschlüsselung von Daten, Verbesserungen der Benutzerfreundlichkeit beim ILM, eine neu konzipierte Mandanten-Manager-Benutzeroberfläche, Unterstützung für die Stilllegung eines StorageGRID Standorts und ein Verfahren für Appliance-Node-Klone.

S3 Objektsperre für konforme Daten

Die S3-Objektsperre in StorageGRID 11.5 ist eine Objektschutzlösung, die äquivalent zur S3-Objektsperre in Amazon Simple Storage Service (Amazon S3) ist. Sie können die globale S3-Objektsperre für ein StorageGRID-System aktivieren, damit S3-Mandantenkonten Buckets erstellen können, wobei S3-Objektsperre aktiviert ist. Der Mandant kann dann mithilfe einer S3-Client-Applikation optional Aufbewahrungseinstellungen und Einstellungen für die Aufbewahrung gemäß den gesetzlichen Bestimmungen

in diesen Buckets festlegen.

Mit der S3 Object Lock können Mandantenbenutzer Vorschriften einhalten, nach denen bestimmte Objekte für eine bestimmte Zeit oder für eine bestimmte Dauer aufbewahrt werden müssen.

Weitere Informationen .

- "Objektmanagement mit ILM"
- "S3 verwenden"
- "Verwenden Sie ein Mandantenkonto"

VERSCHLÜSSELUNGSMANAGEMENT NACH KM

Im Grid Manager kann ein oder mehrere externe KMS (Key Management Server) konfiguriert werden, um StorageGRID Services und Storage Appliances Verschlüsselungen zu übermitteln. Jeder KMS- oder KMS-Cluster verwendet das KMIP (Key Management Interoperability Protocol), um einen Verschlüsselungsschlüssel für die Appliance-Nodes am zugehörigen StorageGRID-Standort bereitzustellen. Nachdem die Appliance-Volumes verschlüsselt sind, können Sie erst auf sämtliche Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

> Wenn Sie die Verschlüsselungsschlüsselverwaltung verwenden möchten, müssen Sie die Einstellung **Node Encryption** für die Appliance mit dem Installationsprogramm von StorageGRID Appliance aktivieren, bevor Sie die Appliance zum Grid hinzufügen.

Weitere Informationen .

- "StorageGRID verwalten"

Verbesserungen der Benutzerfreundlichkeit beim Information Lifecycle Management (ILM)

- Sie können jetzt die Gesamtkapazität eines Speicherpools einschließlich des belegten und freien Speicherplatzes anzeigen. Sie können auch sehen, welche Nodes in einem Storage-Pool enthalten sind und welche ILM-Regeln und Erasure Coding-Profile den Storage-Pool verwenden.
- Sie können jetzt ILM-Regeln entwerfen, die für mehr als ein Mandantenkonto gelten.
- Wenn Sie eine ILM-Regel für das Erasure Coding erstellen, werden Sie nun daran erinnert, den erweiterten Filter für Objektgröße (MB) auf größer als 0.2 zu setzen, um sicherzustellen, dass sehr kleine Objekte nicht gelöscht werden.
- Die ILM-Richtlinienschnittstelle stellt nun sicher, dass die Standard-ILM-Regel immer für Objekte verwendet wird, die nicht mit einer anderen Regel übereinstimmen. Ab StorageGRID 11.5 kann die Standardregel keine grundlegenden oder erweiterten Filter verwenden und wird automatisch als letzte Regel in der Richtlinie platziert.

> Wenn Ihre aktuelle ILM-Richtlinie den neuen Anforderungen nicht entspricht, können Sie sie nach einem Upgrade auf StorageGRID 11.5 weiterhin verwenden. Wenn Sie jedoch nach dem Upgrade versuchen, eine nicht konforme Richtlinie zu klonen, werden Sie aufgefordert, eine Standardregel auszuwählen, die keine Filter enthält, und Sie müssen die Standardregel am Ende der Richtlinie platzieren.

- Der Speicherpool Alle Speicherknoten auf Lager ist standardmäßig nicht mehr ausgewählt, wenn Sie eine neue ILM-Regel oder ein neues Erasure Coding-Profil erstellen. Außerdem können Sie jetzt den Speicherpool Alle Speicherknoten entfernen, solange er in keiner Regel verwendet wird.

> Die Verwendung des Speicherpools für alle Speicherknoten wird nicht empfohlen, da dieser Speicherpool alle Standorte enthält. Mehrere Kopien eines Objekts können auf demselben Standort platziert werden, wenn Sie diesen Storage-Pool mit einem StorageGRID System verwenden, das mehr als einen Standort umfasst.

- Sie können nun die Regel „Vorrat 2 Kopien erstellen“ entfernen (die den Speicherpool „Alle Speicherknoten“ verwendet), solange sie nicht in einer aktiven oder vorgeschlagenen Richtlinie verwendet wird.
- In einem Cloud-Storage-Pool gespeicherte Objekte können jetzt sofort gelöscht werden (synchrones Löschen).

Weitere Informationen .

- "Objektmanagement mit ILM"

Verbesserungen am Grid Manager

- Auf der Seite „neu gestaltete Mandantenkonten“ können Sie die Nutzung des Mandantenkontos einfacher anzeigen. Die Zusammenfassungstabelle für Mandanten enthält jetzt Spalten für genutzten Speicherplatz, Kontingentnutzung, Kontingente und Objektanzahl. Ein neuer **Details anzeigen** Button greift auf eine Übersicht der einzelnen Mandanten sowie Details zu den S3 Buckets oder Swift Containern des Kontos zu. Außerdem können Sie jetzt zwei exportieren `.csv` Dateien zur Mandantennutzung: Eine mit Nutzungswerten für alle Mandanten und eine mit Details zu den Buckets oder Containern eines Mandanten.

  Im Zusammenhang mit dieser Änderung wurden drei neue Prometheus-Kennzahlen hinzugefügt, um die Nutzung von Mandantenkonten nachzuverfolgen:

  - `storagegrid_tenant_usage_data_bytes`
  - `storagegrid_tenant_usage_object_count`
  - `storagegrid_tenant_usage_quota_bytes`
- Im neuen Feld **Zugriffsmodus** auf der Seite Admin Groups (**Configuration** > **Access Control**) können Sie festlegen, ob die Verwaltungsberechtigungen für die Gruppe schreibgeschützt (Standard) oder schreibgeschützt sind. Benutzer, die zu einer Gruppe mit Lese-/Schreibzugriff gehören, können Einstellungen ändern und Vorgänge im Grid Manager und der Grid Management API ausführen. Benutzer, die zu einer Gruppe mit schreibgeschütztem Zugriffsmodus gehören, können nur die für die Gruppe ausgewählten Einstellungen und Funktionen anzeigen.

  > Wenn Sie ein Upgrade auf StorageGRID 11.5 durchführen, ist die Option „Lese-/Schreibzugriff“ für alle vorhandenen Admin-Gruppen ausgewählt.

- Die Benutzeroberfläche von AutoSupport wurde neu gestaltet. Sie können nun ereignisgesteuerte, vom Benutzer ausgelöste und wöchentliche AutoSupport Meldungen über eine einzige Seite im Grid Manager konfigurieren. Sie können auch ein zusätzliches Ziel für AutoSupport Meldungen konfigurieren.

  > Wenn AutoSupport nicht aktiviert wurde, wird jetzt im Grid ManagerDashboard eine Erinnerungsmeldung angezeigt.

- Wenn Sie das Diagramm **verwendete Speicherelemente - Objektdaten** auf der Seite Knoten anzeigen, sehen Sie jetzt Schätzungen für die Menge der replizierten Objektdaten und die Menge der mit Löschungscode gekennzeichneten Daten im Raster, am Standort oder Storage Node (**Nodes** > ***Grid/site/Storage Node*** > **Storage**).

- Die Menüoptionen im Grid Manager wurden neu organisiert, um Optionen einfacher zu finden. Zum Beispiel wurde ein neues Untermenü **Network Settings** zum Menü **Configuration** hinzugefügt und Optionen in den Menüs **Wartung** und **Support** sind nun alphabetisch aufgelistet.

Weitere Informationen .

- "StorageGRID verwalten"

Verbesserungen am Tenant Manager

- Das Erscheinungsbild und die Organisation der Tenant Manager-Benutzeroberfläche wurden komplett neu gestaltet, um die Benutzerfreundlichkeit zu verbessern.
- Das neue Mandanten-Manager-Dashboard bietet einen allgemeinen Überblick über jedes Konto: Es bietet Bucket-Details und zeigt die Anzahl der Buckets oder Container, Gruppen, Benutzer und Endpunkte der Plattform-Services (falls konfiguriert) an.

Weitere Informationen .

- "Verwenden Sie ein Mandantenkonto"

Client-Zertifikate für Prometheus Kennzahlenexport

Sie können nun Clientzertifikate (**Konfiguration** > **Zugriffskontrolle** > **Clientzertifikate**) hochladen oder generieren, die für einen sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank verwendet werden können. Sie können beispielsweise Clientzertifikate verwenden, wenn Sie StorageGRID extern mit Grafana überwachen müssen.

Weitere Informationen .

- "StorageGRID verwalten"

Verbesserungen für den Load Balancer

- Beim Umgang mit Routinganfragen an einem Standort führt der Load Balancer-Service nun ein Load-aware-Routing durch: Er berücksichtigt die CPU-Verfügbarkeit der Storage Nodes am selben Standort. In manchen Fällen sind die Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich der Load Balancer Service befindet.

> ⓘ Die CPU-Bekanntheit wird erst aktiviert, wenn mindestens zwei Drittel der Storage-Nodes an einem Standort auf StorageGRID 11.5 aktualisiert wurden und CPU-Statistiken gemeldet wurden.

- Für zusätzliche Sicherheit können Sie nun für jeden Load Balancer-Endpunkt einen Bindungsmodus festlegen. Mit Endpoint Pinning können Sie die Zugänglichkeit jedes Endpunkts auf bestimmte Hochverfügbarkeitsgruppen oder Node-Schnittstellen beschränken.

Weitere Informationen .

- "StorageGRID verwalten"

Änderungen an Objektmetadaten

- **Neue Metrik für den tatsächlich reservierten Speicherplatz**: Um Ihnen zu helfen, die Auslastung von Objektmetadaten auf jedem Speicherknoten zu verstehen und zu überwachen, wird eine neue Prometheus-Metrik auf der Speichernutzung - Objektmetadaten für einen Speicherknoten (**Knoten** > ***Speicherknoten*** > **Speicher**) angezeigt.

```
storagegrid_storage_utilization_metadata_reserved
```

Die Metrik **tatsächlich reservierter Speicherplatz** gibt an, wie viel Speicherplatz StorageGRID für Objektmetadaten auf einem bestimmten Speicherknoten reserviert hat.

- **Bei Installationen mit größeren Speicherknoten erhöht sich der Metadatenspeicherplatz**: Bei StorageGRID-Systemen mit Speicherknoten mit mindestens 128 GB RAM wurde die Einstellung systemweiter reservierter reservierter Speicherplatz erhöht:
  - **8 TB für Neuinstallationen**: Wenn Sie ein neues StorageGRID 11.5 System installieren und jeder Speicherknoten im Raster 128 GB oder mehr RAM hat, wird die Einstellung für systemweiten reservierten Speicherplatz auf 8 TB anstatt 3 TB gesetzt.
  - **4 TB für Upgrades**: Wenn Sie auf StorageGRID 11.5 aktualisieren und jeder Speicherknoten an einem Standort 128 GB oder mehr RAM hat, ist die Einstellung für systemweiten reservierten Speicherplatz auf 4 TB anstatt 3 TB gesetzt.

    Die neuen Werte für die Einstellung „Metadatenreservierter Speicherplatz“ erhöhen den zulässigen Metadatenspeicherplatz für diese größeren Storage-Nodes auf bis zu 2.64 TB und stellen sicher, dass für zukünftige Hardware- und Softwareversionen ausreichend Metadatenspeicherplatz reserviert ist.

    > ⓘ Wenn Ihre Speicherknoten genügend RAM und genügend Speicherplatz auf dem Datenträger 0 haben, können Sie den Einstellungen für reservierten Metadatenspeicherplatz nach dem Upgrade manuell auf 8 TB erhöhen. Die Reservierung von zusätzlichem Metadaten-Speicherplatz nach dem StorageGRID 11.5 Upgrade vereinfacht zukünftige Hardware- und Software-Upgrades.
    >
    > "Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten"

    +

    > ⓘ Wenn Ihr StorageGRID System mehr als 2.64 TB Metadaten auf jedem Storage-Node speichert (oder voraussichtlich gespeichert werden), kann der zulässige Metadatenspeicherplatz in einigen Fällen erhöht werden. Wenn jeweils Ihre Storage-Nodes freien Speicherplatz auf dem Storage-Volume 0 und mehr als 128 GB RAM zur Verfügung haben, wenden Sie sich an Ihren NetApp Ansprechpartner. NetApp überprüft ggf. die Anforderungen und erhöht den zulässigen Metadatenspeicherplatz für jeden Storage-Node.

- **Automatische Bereinigung gelöschter Metadaten**: Wenn 20% oder mehr der auf einem Speicherknoten gespeicherten Metadaten entfernt werden können (weil die entsprechenden Objekte gelöscht wurden), kann StorageGRID nun eine automatische Data-Compaction auf diesem Speicherknoten durchführen. Dieser Hintergrundprozess wird nur ausgeführt, wenn die Belastung des Systems niedrig ist – also wenn CPU, Speicherplatz und Arbeitsspeicher verfügbar sind. Bei dem neuen Data-Compaction-Prozess werden Metadaten für gelöschte Objekte schneller entfernt als in früheren Versionen. Zudem wird Speicherplatz für neue zu speichernde Objekte verfügbar.

Weitere Informationen .

- "StorageGRID verwalten"

Änderungen an der Unterstützung für die S3-REST-API

- Sie können jetzt die S3-REST-API verwenden, um anzugeben S3-Objektsperre Einstellungen:

    - Verwenden Sie zum Erstellen eines Buckets mit aktivierter S3-Objektsperre eine PUT-Bucket-Anforderung beim `x-amz-bucket-object-lock-enabled` Kopfzeile.
    - Um festzustellen, ob die S3-Objektsperre für einen Bucket aktiviert ist, verwenden Sie eine Konfigurationsanforderung FÜR GET Object Lock.
    - Wenn Sie eine Objektversion zu einem Bucket hinzufügen, bei dem die S3-Objektsperre aktiviert ist, verwenden Sie die folgenden Anfrageböpfe, um die Einstellungen für Aufbewahrung und Aufbewahrung der gesetzlichen Aufbewahrungspflichten festzulegen: `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, und `x-amz-object-lock-legal-hold`.
- ES können nun mehrere Objekte in einem versionierten Bucket GELÖSCHT werden.
- Sie können nun Bucket-Verschlüsselungsanfragen PER PUT, GET und DELETE verwenden, um die Verschlüsselung für einen vorhandenen S3-Bucket zu managen.
- Es wurde eine kleine Änderung an einem Feldnamen für den vorgenommen `Expiration` Parameter. Dieser Parameter wird in der Antwort auf EINE PUT-Objekt-, HEAD-Objekt- oder GET-Objekt-Anforderung enthalten, wenn eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt angewendet wird. Das Feld, das angibt, welche Ablaufregel übereinstimmen wurde, wurde zuvor benannt `rule_id`. Dieses Feld wurde in umbenannt `rule-id` Das muss auch auf die AWS-Implementierung abgestimmt sein.
- Standardmäßig versucht die Anforderung GET Storage Usage durch starke globale Konsistenz, den von einem Mandantenkonto verwendeten Storage und seine Buckets abzurufen. Wenn keine „stabile globale“ Konsistenz erreicht werden kann, versucht StorageGRID, die Nutzungsdaten mithilfe der starken Standortkonsistenz abzurufen.
- Der `Content-MD5` Die Anforderungsüberschrift wird jetzt korrekt unterstützt.

Weitere Informationen .

- "S3 verwenden"

Die maximale Größe für CloudMirror-Objekte wurde auf 5 TB erhöht

Die maximale Größe für Objekte, die vom CloudMirror-Replizierungsservice auf einen Ziel-Bucket repliziert werden können, wurde auf 5 TB erhöht. Dies ist die von StorageGRID unterstützte maximale Objektgröße.

Weitere Informationen .

- "S3 verwenden"
- "Verwenden Sie Swift"

Neue Warnmeldungen hinzugefügt

Für StorageGRID 11.5 wurden die folgenden neuen Warnmeldungen hinzugefügt:

- Fehler bei der BMC-Kommunikation des Geräts
- Fibre-Channel-Fehler des Geräts erkannt
- Fehler des Fibre-Channel-HBA-Ports des Geräts
- Geräte-LACP-Port fehlt
- Cassandra Auto-Kompaktor-Fehler
- Cassandra Auto-Kompaktor-Kennzahlen veraltet
- Cassandra-Kompensation überlastet

- Die Festplatten-I/O ist sehr langsam
- ABLAUF DES KMS-CA-Zertifikats
- ABLAUF DES KMS-Clientzertifikats
- KMS-Konfiguration konnte nicht geladen werden
- KMS-Verbindungsfehler
- DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden
- DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen
- KM ist nicht konfiguriert
- KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
- Ablauf DES KMS-Serverzertifikats
- Wenig freier Speicherplatz für den Speicherpool
- Node-Netzwerkannahme-Frame-Fehler
- Die Speicherkonnektivität der Services-Appliance ist herabgesetzt
- Storage-Konnektivität der Storage-Appliance ist herabgesetzt (zuvor unter dem Namen „Storage-Konnektivität der Appliance“ beeinträchtigt)
- Hohe Kontingentnutzung für Mandanten
- Unerwarteter Node-Neustart

Weitere Informationen .

- "Monitor Fehlerbehebung"

TCP-Unterstützung für SNMP-Traps

Sie können nun als Protokoll für SNMP-Trap-Ziele das Transmission Control Protocol (TCP) auswählen. Zuvor wurde nur das Protokoll (User Datagram Protocol) (UDP) unterstützt.

Weitere Informationen .

- "Monitor Fehlerbehebung"

Installation und Netzwerkverbesserungen

- **MAC-Adressenklonierung**: Sie können jetzt MAC-Adressenklonierung verwenden, um die Sicherheit bestimmter Umgebungen zu erhöhen. Mit dem Klonen VON MAC-Adressen können Sie eine dedizierte virtuelle NIC für das Grid-Netzwerk, das Admin-Netzwerk und das Client-Netzwerk verwenden. Wenn der Docker Container die MAC-Adresse der dedizierten NIC auf dem Host nutzen soll, können Sie keine Kompromissmodus-Netzwerkkonfigurationen verwenden. Die Node-Konfigurationsdatei für Linux-basierte (Bare Metal-)Nodes wurde um drei neue Klon-Schlüssel für MAC-Adressen erweitert.
- **Automatische Ermittlung von DNS- und NTP-Hostrouten**: Zuvor gab es Einschränkungen, mit welchem Netzwerk Ihre NTP- und DNS-Server verbunden werden mussten, wie z.B. die Anforderung, dass Sie nicht alle Ihre NTP- und DNS-Server im Client-Netzwerk haben konnten. Diese Einschränkungen werden nun entfernt.

Weitere Informationen .

- "Installieren Sie Red hat Enterprise Linux oder CentOS"
- "Installieren Sie Ubuntu oder Debian"

Unterstützung für das Ausbalancieren von EC-Daten (Erasure Coding) nach der Storage-Node-Erweiterung

Das EC-Ausgleichverfahren ist ein neues Befehlszeilenskript, das nach dem Hinzufügen neuer Storage-Nodes erforderlich sein kann. Bei der Durchführung des Verfahrens verteilt StorageGRID nach dem Erasure-Coding-Verfahren Fragmente auf die vorhandenen und neu erweiterten Storage-Nodes an einem Standort neu.

> Sie sollten das EC-Ausgleichverfahren nur in begrenzten Fällen durchführen. Wenn Sie beispielsweise nicht die empfohlene Anzahl von Speicherknoten zu einer Erweiterung hinzufügen können, können Sie das EC-Ausgleichverfahren verwenden, um zusätzliche Objekte mit Löschungscode zu speichern.

Weitere Informationen .

- "Erweitern Sie Ihr Raster"

Neue und überarbeitete Wartungsabläufe

- **Deaktivierung der Website**: Sie können nun eine funktionsfähige Website aus Ihrem StorageGRID-System entfernen. Durch die Stilllegung einer verbundenen Website wird ein operativer Standort entfernt und Daten beibehalten. Der neue Decommission Site Wizard führt Sie durch den Prozess (**Wartung** > **Dekommission** > **Decommission Site**).
- **Appliance Node Cloning**: Sie können jetzt einen vorhandenen Appliance-Knoten klonen, um den Knoten auf ein neues Appliance-Modell zu aktualisieren. Beispielsweise können Sie einen Appliance Node mit geringerer Kapazität in einer Appliance mit höherer Kapazität klonen. Sie können auch einen Appliance-Knoten klonen, um neue Funktionen zu implementieren, wie z. B. die neue **Node Encryption**-Einstellung, die für die KMS-Verschlüsselung erforderlich ist.
- **Möglichkeit, die Provisioning-Passphrase zu ändern**: Sie können jetzt die Provisioning-Passphrase (**Konfiguration** > **Zugriffskontrolle** > **Grid-Passwörter**) ändern. Die Passphrase ist für Recovery-, Erweiterungs- und Wartungsvorgänge erforderlich.
- **Erweitertes SSH-Passwortverhalten**: Um die Sicherheit von StorageGRID-Geräten zu erhöhen, wird das SSH-Passwort nicht mehr geändert, wenn Sie eine Appliance in den Wartungsmodus versetzen. Darüber hinaus werden beim Upgrade eines Node auf StorageGRID 11.5 neue SSH-Host-Zertifikate und Hostschlüssel generiert.

> Wenn Sie SSH zum Anmelden bei einem Node nach dem Upgrade auf StorageGRID 11.5 verwenden, wird die Warnung ausgegeben, dass sich der Host-Schlüssel geändert hat. Dieses Verhalten wird erwartet, und Sie können den neuen Schlüssel sicher genehmigen.

Weitere Informationen .

- "Verwalten Sie erholen"

Änderungen an StorageGRID Appliances

- **Direkter Zugriff auf SANtricity System Manager für Storage Appliances**: Sie können jetzt vom StorageGRID Appliance Installer und über den Grid Manager auf die Benutzeroberfläche des E-Series SANtricity System Managers zugreifen. Mit diesen neuen Methoden kann auf SANtricity System Manager zugegriffen werden, ohne den Management-Port der Appliance zu verwenden. Benutzer, die vom Grid Manager aus auf SANtricity System Manager zugreifen müssen, müssen über die neue Administrator-Berechtigung für Speichergeräte verfügen.
- **Knotenverschlüsselung**: Als Teil der neuen KMS-Verschlüsselungsfunktion wurde dem StorageGRID-Appliance-Installer eine neue **Node-Verschlüsselung**-Einstellung hinzugefügt. Wenn Sie zum Schutz von Appliance-Daten das Verschlüsselungskeymanagement verwenden möchten, müssen Sie diese

Einstellung während der Hardware-Konfigurationsphase der Appliance-Installation aktivieren.

- **UDP-Port-Konnektivität**: Sie können jetzt die Netzwerkverbindung eines StorageGRID-Geräts auf UDP-Ports testen, wie sie für einen externen NFS- oder DNS-Server verwendet werden. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren** > **Port Connectivity Test (nmap)** aus.
- **Automatisierte Installation und Konfiguration**: Dem StorageGRID Appliance Installer wurde eine neue Seite zum Hochladen der JSON-Konfiguration hinzugefügt (**Erweitert** > **Appliance-Konfiguration aktualisieren**). Auf dieser Seite können Sie eine Datei verwenden, um mehrere Geräte in großen Grids zu konfigurieren. Darüber hinaus der `configure-sga.py` Python-Skript wurde aktualisiert, um den Fähigkeiten des StorageGRID-Appliance-Installationsprogramms gerecht zu werden.

Weitere Informationen .

- "SG100 SG1000 Services-Appliances"
- "SG6000 Storage-Appliances"
- "SG5700 Storage-Appliances"
- "SG5600 Storage Appliances"

Änderungen an Audit-Meldungen

- **Automatische Bereinigung von überschreibten Objekten**: Zuvor wurden Objekte, die überschrieben wurden, in bestimmten Fällen nicht von der Festplatte entfernt, was zu einem zusätzlichen Platzbedarf führte. Diese überschreibbaren Objekte, die für Benutzer nicht zugänglich sind, werden jetzt automatisch entfernt, um Speicherplatz zu sparen. Weitere Informationen finden Sie in der LKCU-Überwachungsmeldung.
- **Neue Audit-Codes für S3 Object Lock**: Die SPUT-Audit-Nachricht wurde um vier neue Audit-Codes ergänzt S3-Objektsperre Anfragezeilen:
  - LKEN: Objektsperre aktiviert
  - LKLH: Objektsperre Legal Hold
  - LKMD: Objektsperrmodus
  - LKRU: Objektsperre bis Datum beibehalten
- **Neue Felder für letzte geänderte Zeit und Vorherige Objektgröße**: Sie können jetzt verfolgen, wann ein Objekt überschrieben wurde, sowie die ursprüngliche Objektgröße.
  - Das Feld MTME (letzte geänderte Zeit) wurde den folgenden Audit-Meldungen hinzugefügt:
    - SDEL (S3 DELETE)
    - SPUT (S3 PUT)
    - WDEL (Swift LÖSCHEN)
    - WPUT (Swift PUT)
  - Das Feld CSIZ (Vorherige Objektgröße) wurde der OVWR-Meldung (Objekt-Überschreiben) hinzugefügt.

Weitere Informationen .

- "Prüfung von Audit-Protokollen"

Neue nms.requestlog-Datei

Eine neue Protokolldatei, `/var/local/log/nms.requestlog`, Wird auf allen Admin-Knoten gepflegt. Diese

Datei enthält Informationen über ausgehende Verbindungen von der Management-API zu internen StorageGRID-Diensten.

Weitere Informationen .

- "Monitor Fehlerbehebung"

Änderungen in der StorageGRID-Dokumentation

- Damit die Netzwerkinformationen und -Anforderungen leichter zu finden sind und klarzustellen ist, dass die Informationen auch für StorageGRID-Appliance-Knoten gelten, wurde die Netzwerkdokumentation von den softwarebasierten Installationshandbüchern (RedHat Enterprise Linux/CentOS, Ubuntu/Debian und VMware) in einen neuen Netzwerkleitfaden verschoben.

  "Netzwerkrichtlinien"

- Um die Suche nach ILM-bezogenen Anweisungen und Beispielen zu erleichtern, wurde die Dokumentation für das Management von Objekten mit Information Lifecycle Management vom *Administrator Guide* in einen neuen ILM-Leitfaden verschoben.

  "Objektmanagement mit ILM"

- Ein neuer FabricPool Leitfaden bietet einen Überblick über die Konfiguration von StorageGRID als NetApp FabricPool Cloud Tier und beschreibt die Best Practices für die Konfiguration von ILM-Optionen und anderen StorageGRID-Optionen für einen FabricPool-Workload.

  "Konfigurieren Sie StorageGRID für FabricPool"

- Sie können jetzt auf mehrere Anleitungsvideos vom Grid Manager zugreifen. Die aktuellen Videos enthalten Anweisungen zum Management von Warnmeldungen, benutzerdefinierten Warnmeldungen, ILM-Regeln und ILM-Richtlinien.

Funktionen entfernt oder veraltet

Einige Funktionen wurden in StorageGRID 11.5 entfernt oder veraltet. Sie müssen diese Elemente überprüfen, um zu verstehen, ob Sie Clientanwendungen aktualisieren oder Ihre Konfiguration ändern müssen, bevor Sie ein Upgrade durchführen.

Schwache Konsistenzkontrolle entfernt

Die schwache Konsistenzkontrolle wurde für StorageGRID 11.5 entfernt. Nach dem Upgrade gelten folgende Verhaltensweisen:

- Anfragen zur Festlegung einer schwachen Konsistenz für einen S3-Bucket oder Swift-Container sind erfolgreich. Die Konsistenzstufe steht jedoch tatsächlich zur Verfügung.
- Vorhandene Buckets und Container, die eine schwache Konsistenz verwenden, werden im Hintergrund aktualisiert, um die verfügbare Konsistenz zu nutzen.
- Anforderungen, die einen schwachen Header zur Consistency-Control haben, verwenden tatsächlich verfügbare Konsistenz, falls zutreffend.

Die verfügbare Consistency Control verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet jedoch nur eventuelle Konsistenz für DEN KOPFBETRIEB. Die verfügbare Consistency Control bietet eine höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Speicherknoten nicht verfügbar sind.

Alarm für den Zustand des Rasters ist veraltet

Der `/grid/health/topology` Die API, die auf aktive *Alarme* von Nodes überprüft, ist veraltet. An ihrem Platz ein neues `/grid/node-health` endpunkt wurde hinzugefügt. Diese API gibt den aktuellen Status jedes Knotens zurück, indem sie auf aktive „*Alerts*“ auf Knoten überprüft.

Compliance-Funktion veraltet

Die S3-Objektsperrfunktion in StorageGRID 11.5 ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die neue S3-Objektsperrfunktion den Amazon S3-Anforderungen entspricht, depretiert sie die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „`` Legacy-Compliance“ bezeichnet wird.

Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, wird die neue globale S3-Objektsperre beim Upgrade auf StorageGRID 11.5 automatisch aktiviert. Mandantenbenutzer können keine neuen Buckets erstellen, für die Compliance in StorageGRID aktiviert ist. Mandantenbenutzer können jedoch nach Bedarf vorhandene, konforme Buckets weiterhin verwenden und managen.

Im Mandanten-Manager wird ein Shield-Symbol angezeigt Zeigt einen veralteten, konformen Bucket an. Auch für ältere, konforme Buckets ist ein Hold-Abzeichen vorhanden

Um anzugeben, dass der Bucket unter einer gesetzlichen Aufbewahrungspflichten steht.

"KB: Wie verwaltet man ältere, konforme Buckets in StorageGRID 11.5"

"Objektmanagement mit ILM"

Warnung „`s 3 mehrtei. zu klein`“ entfernt

Die Warnung **S3 mehrtei. zu klein** wurde entfernt. Zuvor wurde diese Warnmeldung ausgelöst, wenn ein S3-Client einen mehrteiligen Upload mit Teilen durchführen wollte, die die Größenlimits für Amazon S3 nicht erfüllen. Nach dem Upgrade auf StorageGRID 11.5 werden alle Anforderungen für mehrteilige Uploads, die die folgenden Größenlimits nicht erfüllen, fehlschlagen:

- 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 einzigartiges Objekt betrachtet wird, verringert der StorageGRID-Metadaten-Overhead durch große Teilgrößen.
- Verwenden Sie für Objekte, die kleiner als 5 gib sind, stattdessen einen Upload ohne mehrere Teile.

Warnmeldungen „Appliance-Verbindung im Grid-Netzwerk deaktiviert“ entfernt

Die folgenden Meldungen wurden entfernt. Wenn das Grid-Netzwerk ausgefallen ist, sind die Metriken, die diese Warnmeldungen auslösen würden, nicht verfügbar:

- Services-Appliance-Verbindung im Grid-Netzwerk deaktiviert
- Verbindung der Storage Appliance im Grid-Netzwerk deaktiviert

Unterstützung für vollständig qualifizierte Domain Name aus SNMP-Konfiguration entfernt

Wenn Sie einen SNMP-Server im Baseboard Management Controller (BMC) für SG6000, SG100 oder SG1000 konfigurieren, müssen Sie jetzt eine IP-Adresse anstelle eines vollständig qualifizierten Domänennamens

angeben. Wenn zuvor ein vollständig qualifizierter Domänenname konfiguriert war, ändern Sie ihn in eine IP-Adresse, bevor Sie ein Upgrade auf StorageGRID 11.5 durchführen.

Alte Attribute entfernt

Die folgenden älteren Attribute wurden entfernt. Bei Bedarf werden die äquivalenten Informationen zu den Prometheus Kennzahlen bereitgestellt:

Altes Attribut	Äquivalenter Prometheus-Wert
BREC	storagegrid_Service_Network_received_Byte
BTRA	storagegrid_Service_Network_transmited_Byte
CQST	storagegrid_Metadatenabfragen_average_Latency_Millisekunden
HAIS	storagegrid_http_Sessions_Incoming_versuchte
HCCS	storagegrid_http_Sessions_Incoming_derzeit_etabliertes
HEIS	storagegrid_http_Sessions_INCOMING_FAILED
HISC	storagegrid_http_Sessions_Incoming_successful
LHAC	*None*
NREC	*None*
NTSO (ausgewähltes Zeitquelloffset)	storagegrid_ntp_Chooed_time_source_Offset_Millisekunden
NTRA	*None*
SLOD	storagegrid_Service_Load
SMEM	storagegrid_Service_Memory_Usage_Byte
SUTM	storagegrid_Service_cpu_Sekunden
SVUT	storagegrid_Service_Uptime_Sekunden
TRBS (empfangene Bits pro Sekunde)	*None*
TRXB	storagegrid_Network_received_Byte

Altes Attribut	Äquivalenter Prometheus-Wert
TTBS (Bits insgesamt pro Sekunde übertragen)	*None*
TTXB	storagegrid_Network_transmited_Byte

Es wurden auch folgende Änderungen vorgenommen:

- Der `network_received_bytes` Und `network_transmitted_bytes` Die Kennzahlen von Prometheus wurden von den Messwerten zu Zählern geändert, da die Werte dieser Kennzahlen nur noch zunehmen. Wenn Sie diese Metriken derzeit in Prometheus-Abfragen verwenden, sollten Sie mit dem beginnen `increase()` Funktion in der Abfrage.
- Die Tabelle „Netzwerkressourcen“ wurde aus der Registerkarte „Ressourcen“ für StorageGRID-Services entfernt. (Wählen Sie **Support** > **Tools** > **Grid Topology** und dann ***Node*** > ***Service*** > **Ressourcen**.)
- Die Seite HTTP-Sitzungen wurde für Speicherknoten entfernt. Bisher konnten Sie auf diese Seite zugreifen, indem Sie **Support** > **Tools** > **Grid Topology** und dann ***Storage Node*** > **LDR** > **HTTP** wählen.
- Der HCCS-Alarm (Currently Creved Incoming Sessions) wurde entfernt.
- Der NTSO-Alarm (ausgewählter Zeitquelle Offset) wurde entfernt.

Änderungen an der Grid-Management-API

StorageGRID 11.5 verwendet Version 3 der Grid Management API. Version 3 depretiert Version 2; jedoch werden Version 1 und Version 2 weiterhin unterstützt.

> Sie können weiterhin Version 1 und Version 2 der Management-API mit StorageGRID 11.5 verwenden. Die Unterstützung für diese Versionen der API wird jedoch in einem zukünftigen Release von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.5 können die veralteten v1- und v2-APIs mit dem deaktiviert werden `PUT /grid/config/management` API:

Abschnitt „Neue Clientzertifikate“

Der neue Abschnitt, `/grid/client-certificates`, Ermöglicht es Ihnen, Client-Zertifikate zu konfigurieren, um sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank bereitzustellen. Sie können StorageGRID beispielsweise extern mit Grafana überwachen.

Ältere Compliance-Endpunkte werden in den Abschnitt mit der neuen s3-Objektsperre verschoben

Mit der Einführung der StorageGRID S3-Objektsperre wurden die APIs, mit denen die bisherigen Compliance-Einstellungen für das Grid verwaltet werden, in einen neuen Abschnitt der Swagger-Benutzeroberfläche verschoben. Der Abschnitt **s3-Object-Lock** enthält die beiden `/grid/compliance-global` API-Endpunkte, die jetzt die globale S3-Objektsperre steuern. Die Endpunkt-URIs bleiben unverändert, um die Kompatibilität mit vorhandenen Anwendungen zu gewährleisten.

Swift-admin-Passwort-Konten Endpunkt entfernt

Der folgende API-Endpunkt für Konten, der in StorageGRID 10.4 veraltet war, wurde jetzt entfernt:

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

Abschnitt „Neue Grid-Passwörter“

Der Abschnitt * Grid-passwords* ermöglicht die Verwaltung von Grid-Kennwörtern. Der Abschnitt enthält zwei Abschnitte `/grid/change-provisioning-passphrase` API-Endpunkte: Mit den Endpunkten können Benutzer die Passphrase für die StorageGRID-Bereitstellung ändern und den Status der Änderung der Passphrase abrufen.

SpeicherAdmin-Berechtigung zur Gruppen-API hinzugefügt

Der `/grid/groups` API enthält jetzt die Berechtigung „Storage Admin“.

Neuer Parameter für die Storage-Verwendung-API

Der `GET /grid/accounts/{id}/usage` API hat jetzt eine `strictConsistency` Parameter. Um beim Abrufen von Speichernutzungsdaten über Speicherknoten eine stabile globale Konsistenz durchzusetzen, setzen Sie diesen Parameter auf `true`. Wenn dieser Parameter auf festgelegt ist `false` (Standard), StorageGRID versucht, Nutzungsdaten mit einer starken globalen Konsistenz abzurufen, kehrt aber zurück zu starker Standortkonsistenz, wenn starke globale Konsistenz nicht erreicht werden kann.

Neue Node Health API

Eine neue `/grid/node-health` endpunkt wurde hinzugefügt. Diese API gibt den aktuellen Status jedes Node zurück, indem sie auf den Nodes auf aktive „*Alerts*“ überprüft. Der `/grid/health/topology` Die API, die auf aktive *Alarme* von Nodes überprüft, ist veraltet.

Ändern Sie in „ApplianceWatch StorageShelvesPowerSupplyDegraded“ Warnregel-ID

Die Warnregel-ID „ApplianceWatch StorageShelvesPowerSupplyDegraded“ wurde in „ApplianceWatch StorageShelvesDegraded“ umbenannt, um das tatsächliche Verhalten der Warnmeldung besser widerzuspiegeln.

Verwandte Informationen

"StorageGRID verwalten"

Änderungen an der Mandantenmanagement-API

StorageGRID 11.5 verwendet Version 3 der Mandantenmanagement-API. Version 3 depretiert Version 2; jedoch werden Version 1 und Version 2 weiterhin unterstützt.

> Sie können weiterhin Version 1 und Version 2 der Management-API mit StorageGRID 11.5 verwenden. Die Unterstützung für diese Versionen der API wird jedoch in einem zukünftigen Release von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.5 können die veralteten v1- und v2-APIs mit dem deaktiviert werden `PUT /grid/config/management` API:

Neuer Parameter für die Mandanten-Storage-Nutzung-API

Der `GET /org/usage` API hat jetzt eine `strictConsistency` Parameter. Um beim Abrufen von Speichernutzungsdaten über Speicherknoten eine stabile globale Konsistenz durchzusetzen, setzen Sie

diesen Parameter auf `true`. Wenn dieser Parameter auf festgelegt ist `false` (Standard), StorageGRID versucht, Nutzungsdaten mit einer starken globalen Konsistenz abzurufen, kehrt aber zurück zu starker Standortkonsistenz, wenn starke globale Konsistenz nicht erreicht werden kann.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie ein Mandantenkonto"

Planung und Vorbereitung von Upgrades

Sie müssen das Upgrade Ihres StorageGRID Systems planen, um sicherzustellen, dass das System für das Upgrade bereit ist und dass das Upgrade mit minimalen Unterbrechungen abgeschlossen werden kann.

Schritte

1. "Schätzung der Zeit für die Durchführung eines Upgrades"
2. "Auswirkungen des Upgrades auf Ihr System"
3. "Auswirkungen eines Upgrades auf Gruppen und Benutzerkonten"
4. "Überprüfen der installierten Version von StorageGRID"
5. "Beschaffung der erforderlichen Materialien für ein Software-Upgrade"
6. "StorageGRID-Upgrade-Dateien werden heruntergeladen"
7. "Herunterladen des Wiederherstellungspakets"
8. "Überprüfen Sie den Zustand des Systems, bevor Sie die Software aktualisieren"

Schätzung der Zeit für die Durchführung eines Upgrades

Wenn Sie ein Upgrade auf StorageGRID 11.5 planen, müssen Sie je nach Dauer des Upgrades in Betracht ziehen, wann ein Upgrade durchgeführt werden soll. Außerdem muss bekannt sein, welche Vorgänge in jeder Phase des Upgrades ausgeführt werden 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.

> Beim Upgrade von StorageGRID 11.4 auf 11.5 werden die Cassandra-Datenbanktabellen auf Storage-Nodes aktualisiert. Die Aufgabe **Upgrade Database** tritt im Hintergrund auf, erfordert jedoch möglicherweise viel Zeit. Während die Datenbank aktualisiert wird, können Sie sicher neue Funktionen verwenden, Hotfixes anwenden und Node-Recovery-Vorgänge durchführen. Sie können jedoch daran gehindert werden, andere Wartungsarbeiten durchzuführen.

> Falls eine Erweiterung dringend erforderlich ist, die Erweiterung vor dem Upgrade auf 11.5 durchführen.

Aufgabe aktualisieren	Beschreibung	Ungefähre Zeit erforderlich	Während dieser Aufgabe
Starten Sie Den Upgrade Service	Vorabprüfungen werden durchgeführt, die Software-Datei wird verteilt und der Upgrade-Service wird gestartet.	3 Minuten pro Grid-Node, es sei denn, Validierungsfehler werden gemeldet	Falls erforderlich, können Sie die Vorabprüfungen für das Upgrade manuell vor dem geplanten Wartungsfenster für die Aktualisierung durchführen.
Grid-Nodes aktualisieren (primärer Admin-Node)	Der primäre Admin-Node wird angehalten, aktualisiert und neu gestartet.	Bis zu 30 Minuten	Sie können nicht auf den primären Admin-Node zugreifen. Verbindungsfehler werden gemeldet, die Sie ignorieren können.
Grid-Nodes aktualisieren (alle anderen Nodes)	Die Software auf allen anderen Grid-Knoten wird aktualisiert, in der Reihenfolge, in der Sie die Knoten genehmigen. Jeder Knoten in Ihrem System wird einzeln für jeweils mehrere Minuten heruntergefahren.	15 bis 45 Minuten pro Node, wobei Appliance-Storage-Nodes am dringendsten benötigt werden **Hinweis:** für Appliance-Knoten wird das StorageGRID-Appliance-Installationsprogramm automatisch auf die neueste Version aktualisiert.	• Ändern Sie die Grid-Konfiguration nicht. • Ändern Sie nicht die Konfiguration der Prüfungsstufe. • Aktualisieren Sie die ILM-Konfiguration nicht. • Führen Sie keine weiteren Wartungsvorgänge durch, wie z. B. Hotfix, Stilllegen oder Erweiterung. **Hinweis:** Wenn Sie ein Wiederherstellungsverfahren durchführen müssen, wenden Sie sich an den technischen Support.

Aufgabe aktualisieren	Beschreibung	Ungefähre Zeit erforderlich	Während dieser Aufgabe
Aktivieren Sie Die Funktionen	Die neuen Funktionen für die neue Version sind aktiviert.	Weniger als 5 Minuten	• Ändern Sie die Grid-Konfiguration nicht. • Ändern Sie nicht die Konfiguration der Prüfungsstufe. • Aktualisieren Sie die ILM-Konfiguration nicht. • Führen Sie keine weiteren Wartungsarbeiten durch.
Upgrade Von Datenbanken	Cassandra-Datenbanktabellen, die auf allen Storage-Nodes vorhanden sind, werden aktualisiert.	Stunden oder Tage, basierend auf der Menge der Metadaten im System	Während der Task **Upgrade Database** funktioniert das aktualisierte Grid normal; das Upgrade läuft jedoch noch. Während dieser Aufgabe können Sie: • Nutzen Sie die neuen Funktionen der neuen Version von StorageGRID. • Ändern Sie die Konfiguration der Prüfungsstufe. • Aktualisieren Sie die ILM-Konfiguration. • Verwenden Sie einen Hotfix. • Stellen Sie einen Node wieder her. **Hinweis:** Sie können keine Stilllegen- oder Erweiterungsprozedur durchführen, bis die Schritte **Final Upgrade** abgeschlossen sind.

Aufgabe aktualisieren	Beschreibung	Ungefähre Zeit erforderlich	Während dieser Aufgabe
Letzte Schritte Zur Aktualisierung	Temporäre Dateien werden entfernt und das Upgrade auf die neue Version wird abgeschlossen.	5 Minuten	Wenn die Aufgabe * Final Upgrade Steps* abgeschlossen ist, können Sie alle Wartungsarbeiten durchführen.

Schritte

1. Schätzen Sie den Zeitaufwand für das Upgrade aller Grid-Knoten (berücksichtigen Sie alle Upgrade-Aufgaben außer **Upgrade Database**).
   a. Multiplizieren Sie die Anzahl der Nodes in Ihrem StorageGRID System mit 30 Minuten/Node (durchschnittlich).
   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. Schätzen Sie den Zeitaufwand für das Upgrade der Datenbank ein.
   a. Wählen Sie im Grid Manager die Option **Nodes** aus.
   b. Wählen Sie den ersten Eintrag in der Struktur (gesamtes Raster) aus, und wählen Sie die Registerkarte **Speicherung** aus.
   c. Bewegen Sie den Cursor über das Diagramm **verwendete Speicherdaten - Objektmetadaten** und suchen Sie den Wert **verwendet**, der angibt, wie viele Bytes von Objektmetadaten in Ihrem Raster sind.
   d. Teilen Sie den Wert **used** um 1.5 TB/Tag, um zu ermitteln, wie viele Tage für ein Upgrade der Datenbank benötigt werden.
4. Berechnen Sie die geschätzte Gesamtdauer für das Upgrade, indem Sie die Ergebnisse der Schritte 1, 2 und 3 hinzufügen.

Beispiel: Wie lange ist ein Upgrade von StorageGRID 11.4 auf 11.5

Angenommen, Ihr System verfügt über 14 Grid-Nodes, von denen 8 Linux-Nodes sind. Nehmen wir auch an, dass der **verwendete**-Wert für Objektmetadaten 6 TB beträgt.

1. Multiplizieren Sie 14 mit 30 Minuten/Node und fügen Sie 1 Stunde hinzu. Die geschätzte Zeit für ein Upgrade aller Nodes beträgt 8 Stunden.
2. Mehrere 8 x 15 Minuten/Node, um die Zeit zur Installation des RPM- oder DEB-Pakets auf den Linux-Knoten zu berücksichtigen. Die voraussichtliche Zeit für diesen Schritt beträgt 2 Stunden.
3. Dividieren Sie 6 durch 1.5 TB/Tag. Die geschätzte Anzahl der Tage für die Aufgabe **Upgrade Database** beträgt 4 Tage.

> Während die Aufgabe **Upgrade Database** ausgeführt wird, können Sie sicher neue Funktionen verwenden, Hotfixes anwenden und Knoten Recovery Operationen durchführen.

4. Fügen Sie die Werte zusammen. Sie sollten 5 Tage Zeit haben, das Upgrade Ihres Systems auf StorageGRID 11.5 abzuschließen.

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. Während des Upgrades werden Grid-Nodes nacheinander heruntergefahren. Daher ist nicht zu der Zeit gekommen, dass alle Grid-Nodes nicht verfügbar sind.

Um die kontinuierliche Verfügbarkeit zu gewährleisten, müssen Sie sicherstellen, dass Objekte mit den entsprechenden ILM-Richtlinien redundant gespeichert werden. Es muss zudem sichergestellt werden, dass alle externen S3- oder Swift-Clients für das Senden von Anforderungen an eine der folgenden Komponenten konfiguriert sind:

- Ein StorageGRID Endpunkt, der als HA-Gruppe (Hochverfügbarkeit) konfiguriert ist
- Einen hochverfügbaren Drittanbieter-Load Balancer
- Mehrere Gateway-Nodes für jeden Client
- Mehrere Storage-Nodes für jeden Client

Die Appliance-Firmware wird aktualisiert

Während des Upgrades auf StorageGRID 11.5:

- Alle Knoten der StorageGRID Appliance werden automatisch auf die StorageGRID Appliance Installer Firmware Version 3.5 aktualisiert.
- SG6060- und SGF6024-Appliances werden automatisch auf die BIOS-Firmware-Version 3B03.EX und BMC-Firmware-Version BMC 3.90.07 aktualisiert.
- SG100- und SG1000-Appliances werden automatisch auf die BIOS-Firmware-Version 3B08.EC und BMC-Firmware-Version 4.64.07 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). Zum Beispiel wird die Meldung **mit Knoten** nicht kommunizieren kann, wenn Dienste beendet werden, oder Sie sehen möglicherweise die Meldung **Cassandra Kommunikationsfehler**, wenn einige Knoten auf StorageGRID 11.5 aktualisiert wurden, aber andere Knoten laufen noch mit StorageGRID 11.4.

Im Allgemeinen werden diese Meldungen nach Abschluss des Upgrades gelöscht.

Nach Abschluss des Upgrades können Sie alle Warnmeldungen zu Upgrades überprüfen, indem Sie im Grid Manager Dashboard * kürzlich behobene Warnmeldungen* auswählen.

Während des Upgrades auf StorageGRID 11.5 wird möglicherweise die Warnung für die **ILM-Platzierung nicht erreichbar** ausgelöst, wenn Storage-Nodes angehalten werden. Dieser Alarm wird möglicherweise einen Tag nach dem erfolgreichen Abschluss des Upgrades bestehen bleiben.

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 übermäßige Benachrichtigungen zu vermeiden, deaktivieren Sie das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren** (**Konfiguration** > **Überwachung** > **SNMP-Agent**), um SNMP-Benachrichtigungen zu deaktivieren, bevor Sie das Upgrade starten. Aktivieren Sie dann die Benachrichtigungen wieder, nachdem das Upgrade abgeschlossen ist.

Konfigurationsänderungen sind eingeschränkt

Bis die Aufgabe **Neues Feature** aktivieren abgeschlossen ist:

- Nehmen Sie keine Änderungen an der Grid-Konfiguration vor.
- Ändern Sie nicht die Konfiguration der Prüfungsstufe.
- Aktivieren oder deaktivieren Sie keine neuen Funktionen.
- Aktualisieren Sie die ILM-Konfiguration nicht. Andernfalls kann es zu inkonsistenten und unerwarteten ILM-Verhaltensweisen kommen.
- Wenden Sie keinen Hotfix an, oder stellen Sie einen Gitterknoten wieder her.

Bis die Aufgabe * Final Upgrade Steps* abgeschlossen ist:

- Führen Sie keine Erweiterungsverfahren durch.
- Führen Sie keine Außerbetriebnahme durch.

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 11.5 können Sie optional die folgenden neuen Berechtigungen und Optionen auswählen (**Konfiguration** > **Zugriffskontrolle** > **Admin-Gruppen**).

Berechtigung oder Option	Beschreibung
Storage Appliance Administrator	Erforderlich für den Zugriff auf die Benutzeroberfläche des SANtricity System Managers über den Grid Manager.
Zugriffsmodus	Beim Verwalten von Gruppen können Sie **Schreibgeschützt** für diese neue Option auswählen, um zu verhindern, dass Benutzer die Einstellungen und Funktionen ändern, die für die Gruppe ausgewählt wurden. Benutzer in Gruppen mit schreibgeschütztem Zugriffsmodus können Einstellungen anzeigen, können sie jedoch nicht ändern.

Verwandte Informationen

"StorageGRID verwalten"

Überprüfen der installierten Version von StorageGRID

Bevor Sie mit dem Upgrade beginnen, müssen Sie überprüfen, ob die vorherige Version von StorageGRID derzeit mit dem neuesten verfügbaren Hotfix installiert ist.

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. Wählen Sie **Hilfe** > **Info**.
3. Überprüfen Sie, ob die **Version** 11.4.*x.y* lautet.

   In der StorageGRID 11.4.*x.y* Versionsnummer:

   - Die Hauptversion hat einen *x*-Wert von 0 (11.4.0).
   - Eine kleine Version hat, falls verfügbar, einen anderen *x*-Wert als 0 (z. B. 11.4.1).
   - Ein Hotfix, falls verfügbar, hat einen *y*-Wert (z. B. 11.4.0.1).

   > Wenn Sie eine frühere Version von StorageGRID haben, müssen Sie vor dem Upgrade auf StorageGRID 11.5 ein Upgrade auf eine beliebige Version 11.4 durchführen. Für ein Upgrade auf StorageGRID 11.5 müssen Sie sich nicht auf die höchste Version von 11.4 Minor-Version befinden.

4. Wenn Sie keine StorageGRID 11.4-Version haben, müssen Sie auf Version 11.4, eine neue Version auf einmal, unter Verwendung der Anweisungen für jede Version aktualisieren.

   Vor dem Upgrade auf die nächste Stufe müssen Sie außerdem den aktuellen Hotfix für jede StorageGRID-Version anwenden.

   Ein möglicher Upgrade-Pfad wird im Beispiel dargestellt.

5. Sobald Sie StorageGRID 11.4 erreicht haben, rufen Sie die NetApp Downloads-Seite für StorageGRID auf und überprüfen Sie, ob Hotfixes für Ihre StorageGRID 11.4.*x*-Version verfügbar sind.

   "NetApp Downloads: StorageGRID"

6. Überprüfen Sie, ob die StorageGRID 11.4.*x*-Version den neuesten Hotfix angewendet hat.
7. Laden Sie ggf. den aktuellen StorageGRID 11.4.*x.y* Hotfix für Ihre StorageGRID 11.4.*x*-Version herunter.

   Informationen zur Anwendung von Hotfixes finden Sie in der Recovery- und Wartungsanleitung.

Beispiel: Upgrade auf StorageGRID 11.5 ab Version 11.3.0.8 wird vorbereitet

Das folgende Beispiel zeigt die Schritte zur Vorbereitung auf ein Upgrade von StorageGRID Version 11.3.0.8 auf Version 11.5. Bevor Sie ein Upgrade auf StorageGRID 11.5 durchführen können, muss auf Ihrem System eine StorageGRID 11.4-Version mit dem neuesten Hotfix installiert sein.

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. (Sie müssen keine 11.4.*x* Minor-Versionen installieren.)
3. Wenden Sie den aktuellen StorageGRID 11.4.0.*y* Hotfix an.

Verwandte Informationen

"StorageGRID verwalten"

"Verwalten Sie erholen"

Beschaffung 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
StorageGRID-Upgrade-Dateien	Sie müssen die erforderlichen Dateien auf Ihren Service-Laptop herunterladen: • * Alle Plattformen*: `.upgrade` Datei • **Beliebiger Knoten auf Red hat Enterprise Linux oder CentOS**: `.upgrade` Datei- und RPM-Datei (`.zip` Oder `.tgz`) • **Jeder Knoten auf Ubuntu oder Debian**: `.upgrade` Datei und DEB-Datei (`.zip` Oder `.tgz`)
Service-Laptop	Der Service-Laptop muss Folgendes haben: • Netzwerkport • SSH-Client (z. B. PuTTY)
Unterstützter Webbrowser	Sie müssen bestätigen, dass der Webbrowser auf dem Service-Laptop für die Verwendung mit StorageGRID 11.5 unterstützt wird. "Anforderungen an einen Webbrowser" **Hinweis:** die Browser-Unterstützung wurde für StorageGRID 11.5 geändert. Vergewissern Sie sich, dass Sie eine unterstützte Version verwenden.
Wiederherstellungspaket (`.zip`) Datei	Vor dem Upgrade sollten Sie die aktuellste Wiederherstellungspaket-Datei herunterladen, falls während des Upgrades Probleme auftreten. Nachdem Sie den primären Admin-Knoten aktualisiert haben, müssen Sie eine neue Kopie der Recovery Package-Datei herunterladen und an einem sicheren Ort speichern. Mit der aktualisierten Wiederherstellungspaket-Datei können Sie das System wiederherstellen, wenn ein Fehler auftritt. "Herunterladen des Wiederherstellungspakets"

Element	Hinweise
`Passwords.txt` Datei	Diese Datei ist im GENANNTEN Paket enthalten, das Teil des Wiederherstellungspakets ist `.zip` Datei: Sie müssen die neueste Version des Wiederherstellungspakets erhalten.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase wird im nicht aufgeführt `Passwords.txt` Datei:
Zugehörige Dokumentation	• Versionshinweise zu StorageGRID 11.5. Lesen Sie diese vor Beginn des Upgrades sorgfältig durch. • Anweisungen für die Administration von StorageGRID • Wenn Sie eine Linux-Bereitstellung aktualisieren, lesen Sie die StorageGRID-Installationsanweisungen für Ihre Linux-Plattform. • Andere StorageGRID-Dokumentation, falls erforderlich.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"StorageGRID verwalten"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"StorageGRID-Upgrade-Dateien werden heruntergeladen"

"Herunterladen des Wiederherstellungspakets"

"Versionshinweise"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

StorageGRID-Upgrade-Dateien werden heruntergeladen

Sie müssen die erforderlichen Dateien auf einen Service-Laptop herunterladen, bevor Sie Ihr StorageGRID-System aktualisieren.

Was Sie benötigen

Sie müssen alle erforderlichen Hotfixes für die StorageGRID-Softwareversion, die Sie aktualisieren, installiert haben. Siehe das Hotfix-Verfahren in den Recovery- und Wartungsanweisungen.

Über diese Aufgabe

Sie müssen die herunterladen `.upgrade` Archivierung für jede Plattform: Wenn Nodes auf Linux-Hosts bereitgestellt werden, müssen Sie auch ein RPM- oder DEB-Archiv herunterladen, das Sie installieren, bevor Sie mit dem Upgrade beginnen.

Schritte

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "NetApp Downloads: 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**.

   Die StorageGRID-Softwareversionen haben dieses Format: 11.*x.y*. StorageGRID-Hotfixes haben dieses Format: 11.*x. y.y.z*.

3. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
4. Wenn eine Warnung/MusterLeseanweisung angezeigt wird, lesen Sie sie, und aktivieren Sie das Kontrollkästchen.

   Diese Anweisung wird angezeigt, wenn für das Release ein Hotfix erforderlich ist.

5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.

   Die Download-Seite für die ausgewählte Version wird angezeigt. Die Seite enthält drei Spalten:

   - Installation von StorageGRID
   - Upgrade von StorageGRID
   - Unterstützen von Dateien für StorageGRID Appliances

6. Wählen Sie in der Spalte **Upgrade StorageGRID** die aus, und laden Sie den herunter `.upgrade` Archivierung:

   Jede Plattform erfordert das `.upgrade` Archivierung:

7. Wenn Nodes auf Linux-Hosts bereitgestellt werden, laden Sie in beiden auch das RPM- oder DEB-Archiv herunter `.tgz` Oder `.zip` Formatieren.

   Sie müssen das RPM- oder DEB-Archiv auf allen Linux-Knoten installieren, bevor Sie das Upgrade starten.

   Für SG100 oder SG1000 sind keine zusätzlichen Dateien erforderlich.

   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`

Verwandte Informationen

"Linux: Installieren des RPM- oder DEB-Pakets auf allen Hosts"

"Verwalten Sie erholen"

Herunterladen des Wiederherstellungspakets

Die Wiederherstellungspakedatei ermöglicht Ihnen die Wiederherstellung des StorageGRID-Systems bei einem Fehler.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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:
   a. Öffnen Sie das `.zip` Datei:
   b. Bestätigen Sie, dass es ein enthält `gpt-backup` Telefonbuch und eine Innenausstattung `.zip` Datei:
   c. Entnehmen Sie die Innenseite `.zip` Datei:

d. Bestätigen Sie, dass Sie den öffnen können `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.

Verwandte Informationen

"StorageGRID verwalten"

Überprüfen Sie den Zustand des Systems, bevor Sie die Software aktualisieren

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 über einen unterstützten Browser beim Grid Manager an.
2. Aktive Warnmeldungen prüfen und beheben.

   Informationen zu bestimmten Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung.

3. Bestätigen Sie, dass keine in Konflikt stehenden Grid-Aufgaben aktiv oder ausstehend sind.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** 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. Lesen Sie die Liste der internen und externen Ports in der Version 11.5 der Netzwerkrichtlinien und stellen Sie sicher, dass alle erforderlichen Ports geöffnet sind, bevor Sie ein Upgrade durchführen.

> 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.

Verwandte Informationen

"Monitor Fehlerbehebung"

"StorageGRID verwalten"

"Verwalten Sie erholen"

"Netzwerkrichtlinien"

Durchführen des Upgrades

Die Seite Software-Upgrade führt Sie durch den Prozess des Uploads der erforderlichen Datei und des Upgrades aller Grid-Knoten in Ihrem StorageGRID-System.

Was Sie benötigen

Sie kennen Folgendes:

- Sie müssen alle Grid-Nodes für alle Datacenter-Standorte vom primären Admin-Node mithilfe des Grid Manager aktualisieren.
- Zur Erkennung und Behebung von Problemen können Sie die Vorabprüfungen manuell durchführen, bevor Sie das tatsächliche Upgrade starten. Die gleichen Vorabprüfungen werden durchgeführt, wenn Sie das Upgrade starten. Durch eine Vorabprüfung der Fehler wird der Upgrade-Prozess gestoppt und es kann erforderlich sein, dass der technische Support einbezogen wird, um das Problem zu lösen.
- Wenn Sie das Upgrade starten, wird der primäre Admin-Node automatisch aktualisiert.
- Nachdem der primäre Admin-Node aktualisiert wurde, können Sie auswählen, welche Grid-Nodes als Nächstes aktualisiert werden sollen.
- Sie müssen alle Grid-Nodes in Ihrem StorageGRID System aktualisieren, um das Upgrade abzuschließen. Aber Sie können einzelne Grid-Nodes in beliebiger Reihenfolge aktualisieren. Sie können einzelne Grid-Nodes, Gruppen von Grid-Nodes oder alle Grid-Nodes auswählen. Sie können den Vorgang der Auswahl von Grid-Nodes so oft wie nötig wiederholen, bis alle Grid-Nodes an allen Standorten aktualisiert werden.
- Wenn das Upgrade auf einem Grid-Node startet, werden die Services auf diesem Node angehalten. Später wird der Grid-Node neu gebootet. Genehmigen Sie das Upgrade für einen Grid-Node nicht, es sei denn, Sie sind sicher, dass der Node bereit ist, angehalten und neu gebootet zu werden.
- Wenn alle Grid-Knoten aktualisiert wurden, sind neue Funktionen aktiviert und Sie können den Betrieb wieder aufnehmen. Sie müssen jedoch warten, bis der Hintergrund **Upgrade Database** Task und die Aufgabe **Final Upgrade Steps** abgeschlossen sind.
- Sie müssen das Upgrade auf derselben Hypervisor-Plattform, mit der Sie begonnen haben, durchführen.

Schritte

1. "Linux: Installieren des RPM- oder DEB-Pakets auf allen Hosts"
2. "Starten des Upgrades"
3. "Aktualisieren der Grid-Nodes und Abschließen des Upgrades"
4. "Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten"

Verwandte Informationen

"StorageGRID verwalten"

"Schätzung der Zeit für die Durchführung eines Upgrades"

Linux: Installieren des RPM- oder DEB-Pakets auf allen Hosts

Wenn StorageGRID Nodes auf Linux-Hosts bereitgestellt werden, müssen auf jedem dieser Hosts ein zusätzliches RPM oder DEB-Paket installiert werden, bevor Sie das

Upgrade starten.

Was Sie benötigen

Sie müssen eine der folgenden Komponenten heruntergeladen haben `.tgz` Oder `.zip` Dateien von der NetApp Downloads Seite für StorageGRID.

Verwenden Sie die `.zip` Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

Linux Plattform	Zusätzliche Datei (eine auswählen)
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`

Schritte

1. Extrahieren Sie die RPM- oder DEB-Pakete aus der Installationsdatei.
2. Installieren Sie die RPM- oder DEB-Pakete auf allen Linux-Hosts.

   Lesen Sie die Schritte zum Installieren von StorageGRID-Hostservices in den Installationsanweisungen für Ihre Linux-Plattform.

   "Installieren Sie Red hat Enterprise Linux oder CentOS"

   "Installieren Sie Ubuntu oder Debian"

   Die neuen Pakete werden als zusätzliche Pakete installiert. Entfernen Sie die vorhandenen Pakete nicht.

Starten des Upgrades

Wenn Sie bereit sind, das Upgrade auszuführen, wählen Sie die heruntergeladene Datei aus, und geben Sie die Provisionierungs-Passphrase ein. Als Option können Sie die Upgrade-Vorabprüfungen durchführen, bevor Sie das tatsächliche Upgrade durchführen.

Was Sie benötigen

Sie haben alle Überlegungen geprüft und alle Schritte unter durchgeführt "Planung und Vorbereitung von Upgrades".

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. Wählen Sie **Wartung System Software-Update**.

   Die Seite Software-Aktualisierung wird angezeigt.

3. Wählen Sie **StorageGRID-Upgrade**.

   Die Seite StorageGRID-Upgrade wird angezeigt und zeigt Datum und Uhrzeit des zuletzt abgeschlossenen

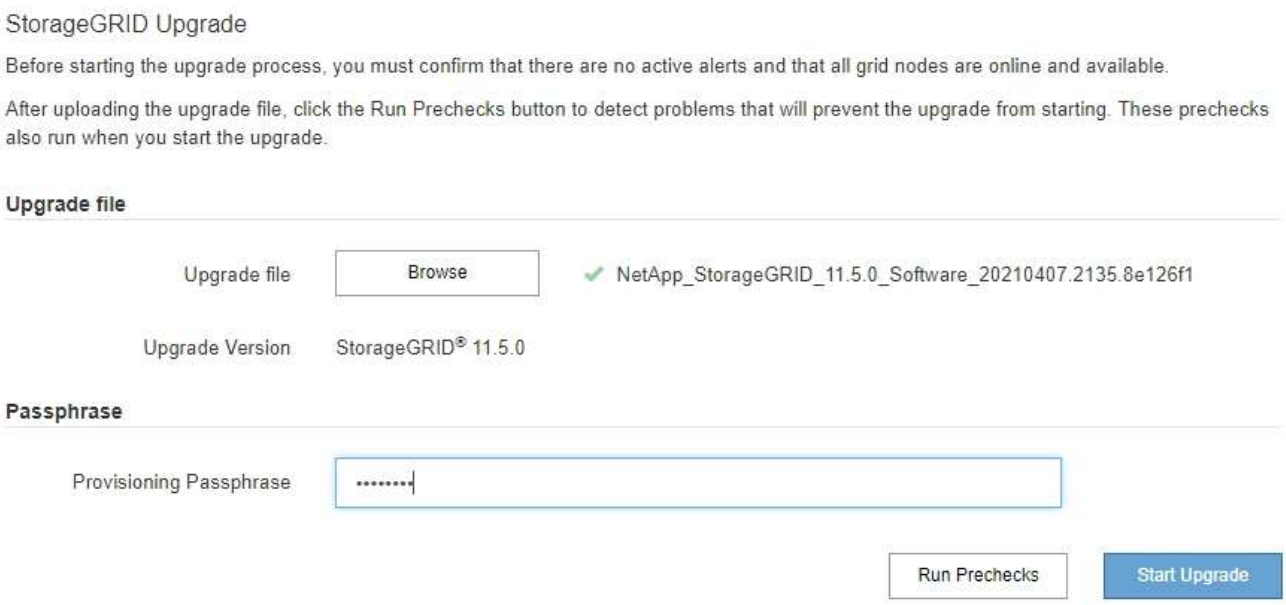
Upgrades an, es sei denn, der primäre Admin-Node wurde neu gestartet oder die Management-API wurde seit der Durchführung des Upgrades neu gestartet.

4. Wählen Sie die aus `.upgrade` Heruntergeladene Datei.
   a. Wählen Sie **Durchsuchen**.
   b. Datei suchen und auswählen: `NetApp_StorageGRID_version_Software_uniqueID.upgrade`
   c. Wählen Sie **Offen**.

      Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird neben dem Dateinamen der Aktualisierungsdatei ein grünes Häkchen angezeigt.

5. Geben Sie die Provisionierungs-Passphrase in das Textfeld ein.

   Die Schaltflächen **Run Prechecks** und **Start Upgrade** werden aktiviert.



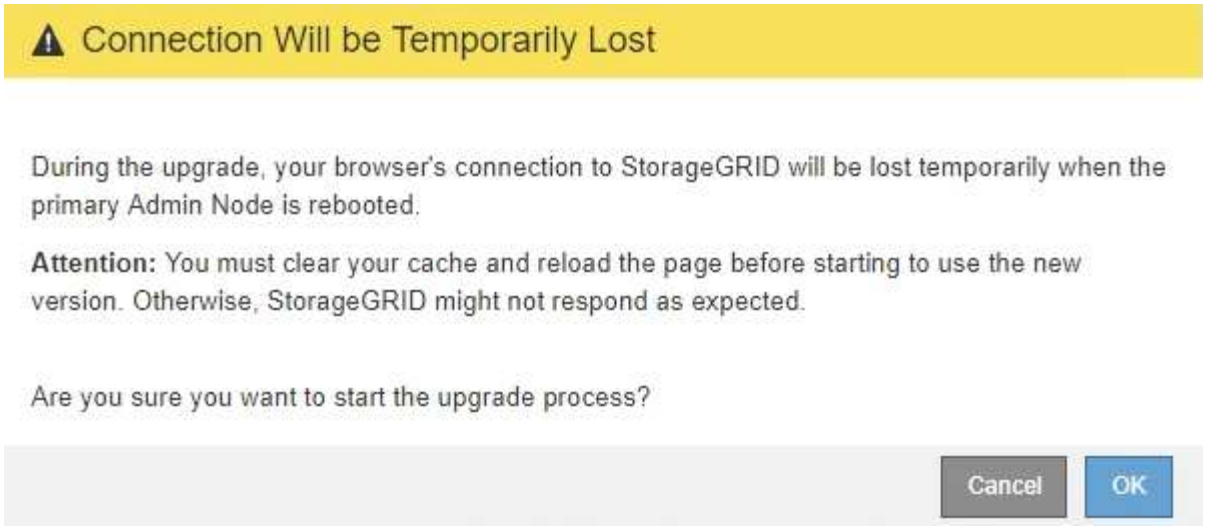
6. Wenn Sie den Zustand Ihres Systems vor dem eigentlichen Upgrade validieren möchten, wählen Sie **Prechecks ausführen**. Lösen Sie dann alle Fehler, die vor der Prüfung gemeldet werden.

   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.

   Die gleichen Vorabprüfungen werden durchgeführt, wenn Sie **Upgrade starten** auswählen. Durch die Auswahl von **Vorprüfungen ausführen** können Sie Probleme erkennen und beheben, bevor Sie das Upgrade starten.

7. Wenn Sie bereit sind, das Upgrade auszuführen, wählen Sie **Upgrade starten**.

   Es wird eine Warnung angezeigt, die Sie daran erinnert, dass die Verbindung Ihres Browsers beim Neustart des primären Admin-Knotens unterbrochen wird. Wenn der primäre Admin-Node wieder verfügbar ist, müssen Sie den Cache Ihres Webbrowsers löschen und die Seite Software-Upgrade neu laden.



8. Wählen Sie * OK*, um die Warnung zu bestätigen und den Aktualisierungsvorgang zu starten.

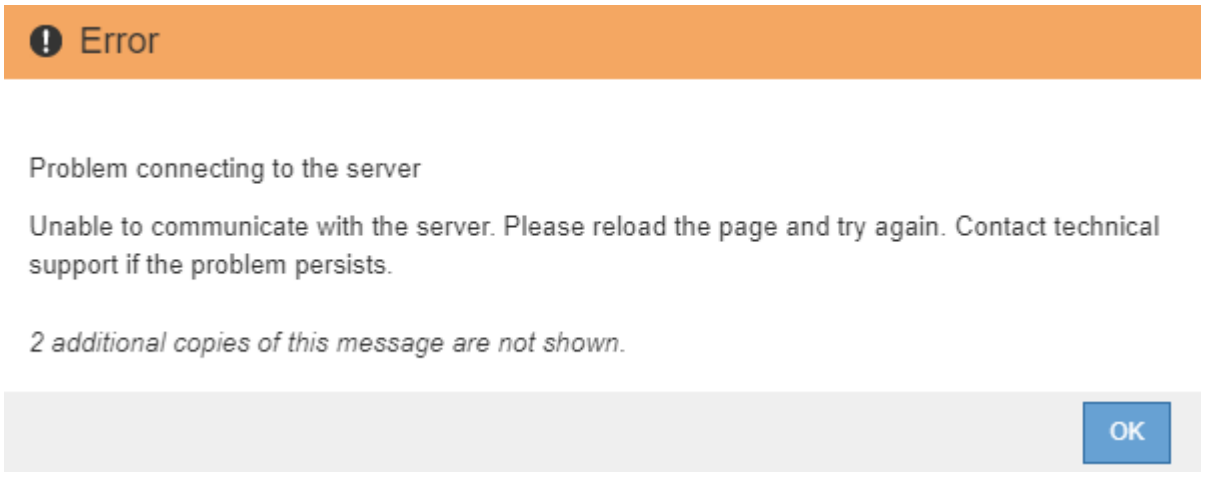
   Wenn das Upgrade beginnt:

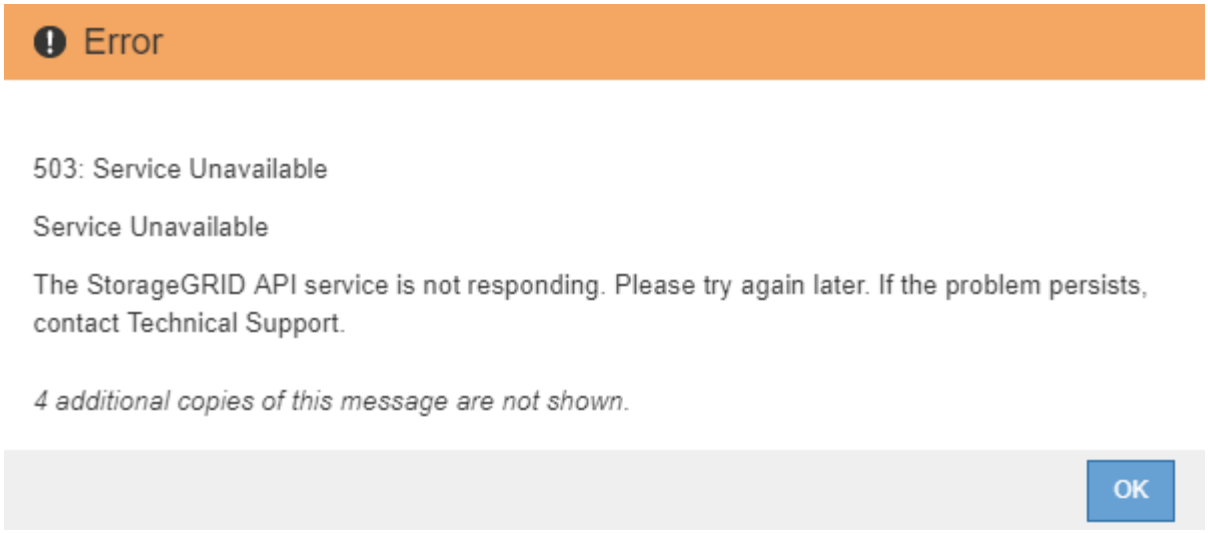
   a. Die Upgrade-Vorabprüfungen werden durchgeführt.

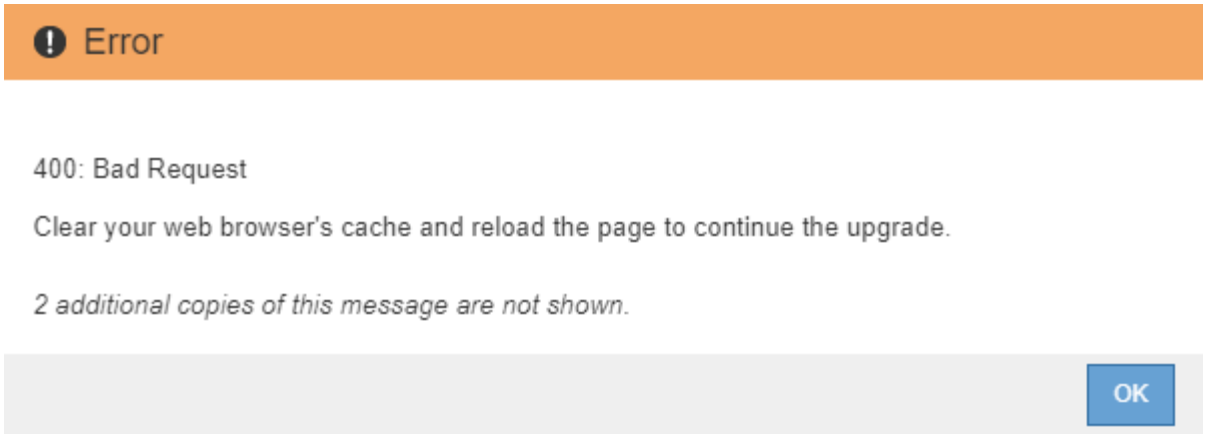
      Wenn Fehler bei der Vorprüfung gemeldet werden, beheben Sie diese und wählen Sie erneut **Upgrade starten**.

   b. Der primäre Admin-Node wird aktualisiert, was auch das Beenden von Diensten, das Aktualisieren der Software und den Neustart von Diensten umfasst. Sie können nicht auf den Grid Manager zugreifen, während der primäre Admin-Node aktualisiert wird. Auch Audit-Protokolle sind nicht verfügbar. Dieses Upgrade kann bis zu 30 Minuten in Anspruch nehmen.

      Während der primäre Admin-Node aktualisiert wird, werden mehrere Kopien der folgenden Fehlermeldungen angezeigt, die Sie ignorieren können.







9. Nachdem der primäre Admin-Node aktualisiert wurde, löschen Sie den Cache Ihres Webbrowsers, melden Sie sich wieder an und laden Sie die Seite Software-Upgrade neu.

   Anweisungen hierzu finden Sie in der Dokumentation Ihres Webbrowsers.

   Sie müssen den Cache des Webbrowsers löschen, um veraltete Ressourcen zu entfernen, die von der vorherigen Version der Software verwendet werden.

Verwandte Informationen

"Planung und Vorbereitung von Upgrades"

Aktualisieren der Grid-Nodes und Abschließen des Upgrades

Nach dem Upgrade des primären Admin-Knotens müssen Sie alle anderen Grid-Knoten in Ihrem StorageGRID-System aktualisieren. Sie können die Upgrade-Sequenz anpassen, indem Sie auswählen, um einzelne Grid-Nodes, Gruppen von Grid-Nodes oder alle Grid-Nodes zu aktualisieren.

Schritte

1. Lesen Sie den Abschnitt Aktualisierungsfortschritt auf der Seite Software-Upgrade, auf der Sie Informationen zu allen wichtigen Aktualisierungsaufgaben erhalten.
   a. **Start Upgrade Service** ist die erste Upgrade-Aufgabe. Während dieser Aufgabe wird die

Softwaredatei auf die Grid-Nodes verteilt und der Upgrade-Service gestartet.

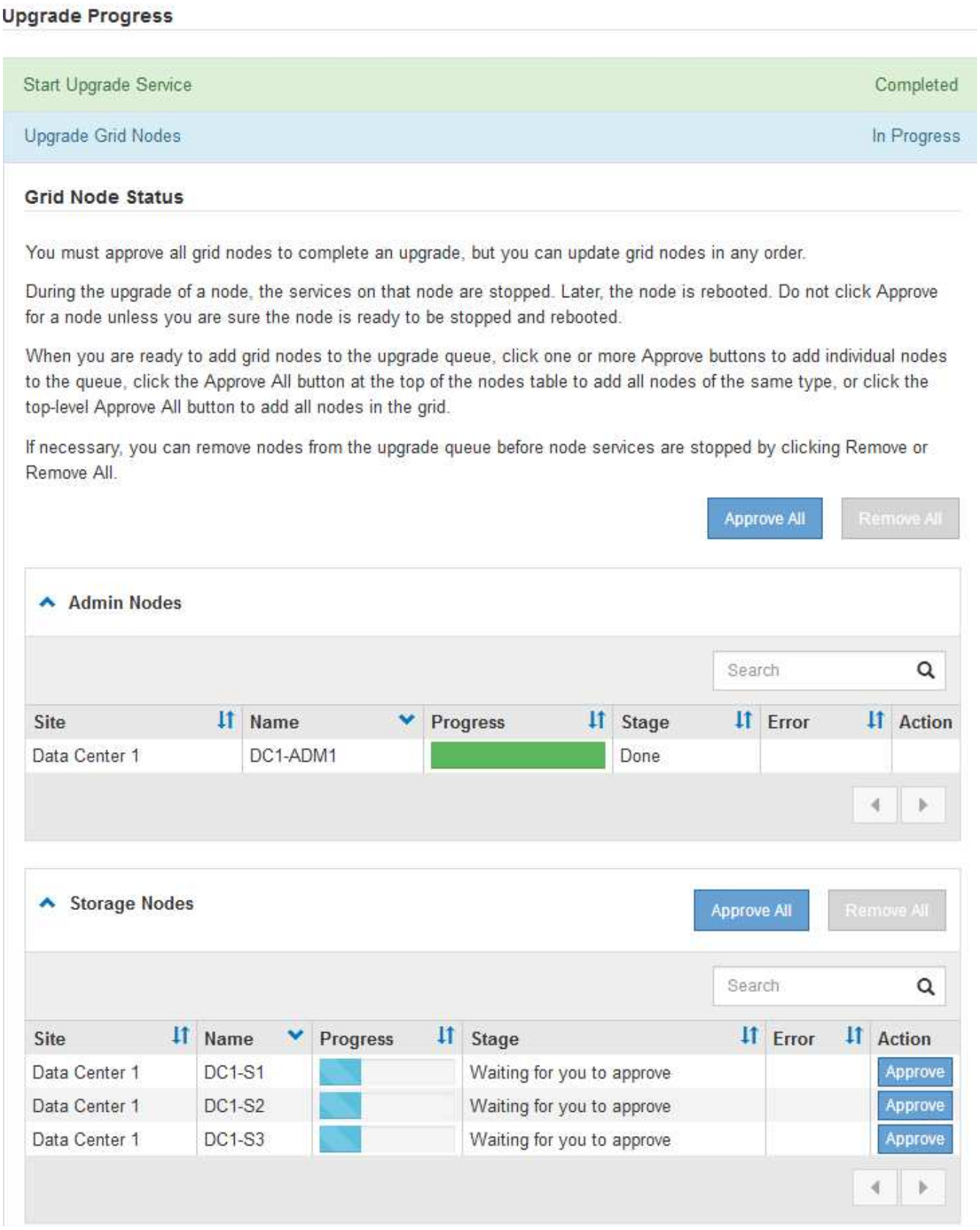
b. Wenn die Aufgabe **Upgrade Service** starten abgeschlossen ist, startet die Aufgabe **Grid Nodes aktualisieren**.

c. Während der Task **Grid-Knoten aktualisieren** ausgeführt wird, wird die Tabelle Status des Grid-Knotens angezeigt und die Aktualisierungsstufe für jeden Grid-Knoten in Ihrem System angezeigt.

2. Nachdem die Grid-Knoten in der Tabelle „Grid Node Status“ angezeigt wurden, laden Sie jedoch vor Genehmigung von Grid-Knoten eine neue Kopie des Wiederherstellungspakets herunter.

> Sie müssen eine neue Kopie der Wiederherstellungspaket-Datei herunterladen, nachdem Sie die Softwareversion auf dem primären Admin-Knoten aktualisiert haben. Die Recovery Package-Datei ermöglicht es Ihnen, das System wiederherzustellen, wenn ein Fehler auftritt.

3. Überprüfen Sie die Informationen in der Tabelle Status des Grid-Knotens. Die Grid-Nodes sind in Abschnitten nach Typ angeordnet: Admin Nodes, API-Gateway-Nodes, Storage-Nodes und Archiv-Nodes.



Ein Rasterknoten kann sich in einer dieser Phasen befinden, wenn diese Seite zuerst angezeigt wird:

- Fertig (nur primärer Admin-Node)
- Upgrade wird vorbereitet

- Software-Download in Warteschlange
- Download
- Warten auf Genehmigung

4. Genehmigen Sie die Grid-Knoten, die Sie zur Upgrade-Warteschlange hinzufügen möchten. Genehmigte Nodes desselben Typs werden nacheinander aktualisiert.

   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. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren. Genehmigen Sie das Upgrade für einen Node nicht, es sei denn, Sie sind sicher, dass der Node bereit ist, angehalten und neu gebootet zu werden.

   - Wählen Sie eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere einzelne Knoten zur Upgrade-Warteschlange hinzuzufügen.
   - Wählen Sie in jedem Abschnitt die Schaltfläche **Alle genehmigen** aus, um alle Knoten desselben Typs zur Upgrade-Warteschlange hinzuzufügen.
   - Wählen Sie die oberste Ebene **Alle genehmigen**-Taste, um alle Knoten im Raster zur Upgrade-Warteschlange hinzuzufügen.

5. Wenn Sie einen Knoten oder alle Knoten aus der Upgrade-Warteschlange entfernen müssen, wählen Sie **Entfernen** oder **Alle entfernen**.

   Wie im Beispiel gezeigt, wird die **Stoppdienste**-Schaltfläche **Entfernen** ausgeblendet, und Sie können den Knoten nicht mehr entfernen.

6. Warten Sie, bis jeder Node die Upgrade-Phasen durchlaufen hat, einschließlich Queued, Stoppen von Services, Stoppen von Containern, Reinigen von Docker-Images, Aktualisieren von Basis-BS-Paketen, Neustarten und Starten von Services.

   > Wenn ein Appliance-Knoten die Phase der Upgrade-Base-BS-Pakete erreicht, wird die Installationssoftware für die StorageGRID-Appliance auf der Appliance aktualisiert. Durch diesen automatisierten Prozess wird sichergestellt, dass die Installationsversion der StorageGRID Appliance mit der StorageGRID-Softwareversion synchronisiert bleibt.

   Wenn alle Grid-Knoten aktualisiert wurden, wird die Aufgabe **Grid-Knoten aktualisieren** als abgeschlossen angezeigt. Die verbleibenden Upgrade-Aufgaben werden automatisch und im Hintergrund ausgeführt.

7. Sobald die Aufgabe **Features** aktivieren abgeschlossen ist (die sich schnell abspielt), können Sie die neuen Funktionen in der aktualisierten StorageGRID-Version nutzen.

   Wenn Sie beispielsweise ein Upgrade auf StorageGRID 11.5 durchführen, können Sie jetzt die S3-Objektsperre aktivieren, einen Schlüsselverwaltungsserver konfigurieren oder die Einstellung für reservierten Metadatenspeicherplatz erhöhen.

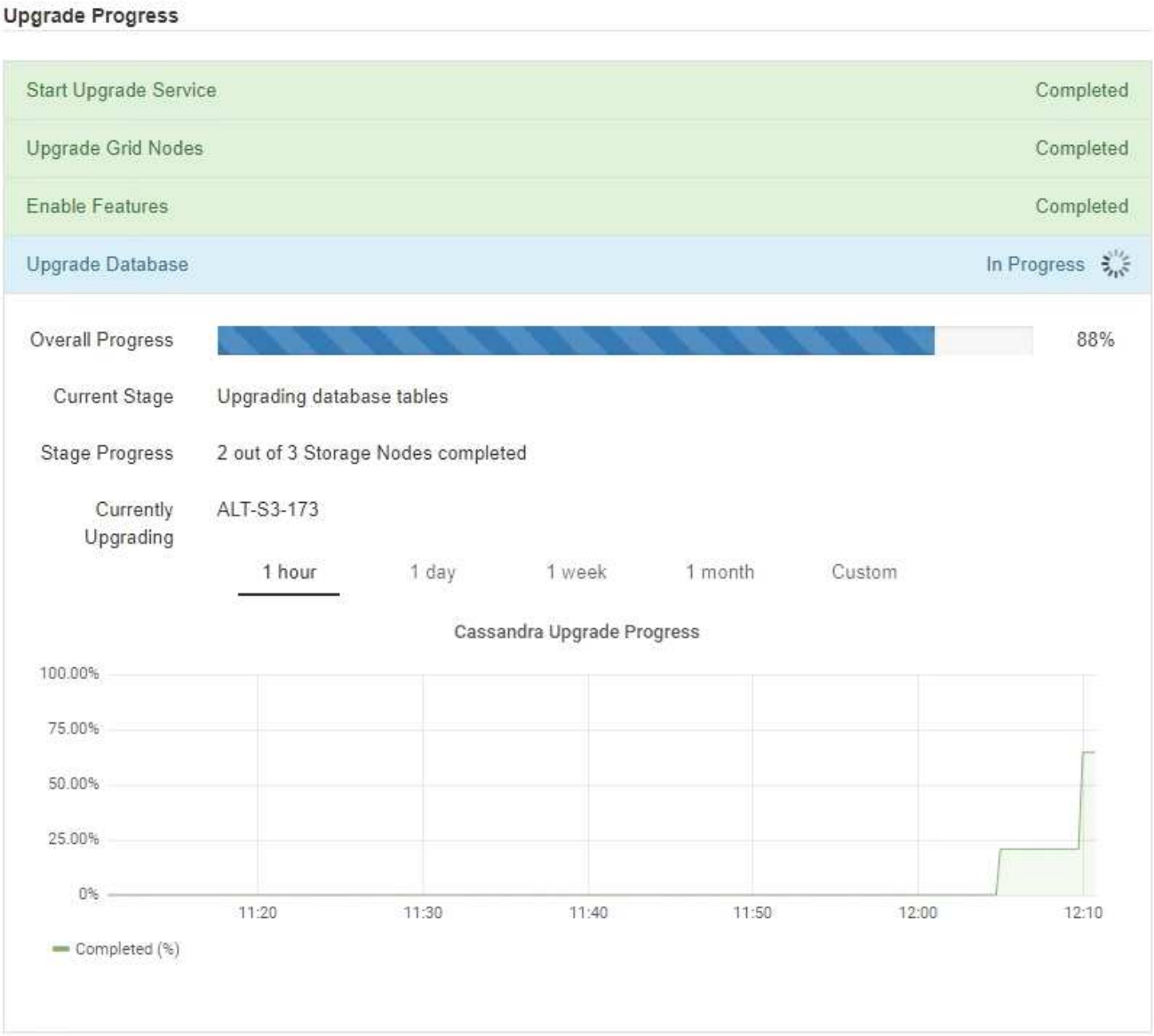
   "Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten"

8. Überwachen Sie regelmäßig den Fortschritt der Aufgabe * Upgrade Database*.

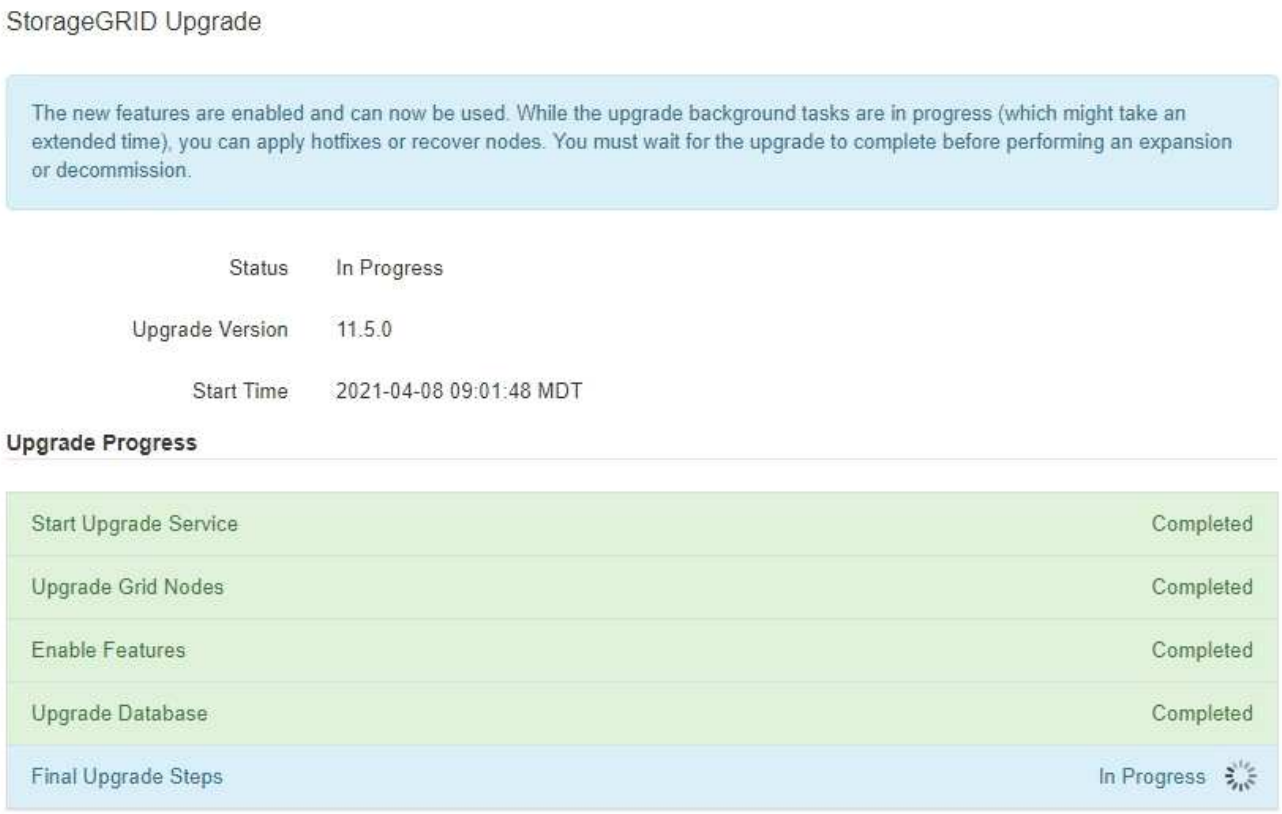
   Während dieser Aufgabe wird die Cassandra-Datenbank auf jedem Storage-Node aktualisiert.

   > Die Aufgabe **Upgrade Database** kann Tage dauern. Wenn diese Hintergrundaufgabe ausgeführt wird, können Sie Hotfixes anwenden oder Knoten wiederherstellen. Sie müssen jedoch warten, bis die Aufgabe * Final Upgrade Steps* abgeschlossen ist, bevor Sie eine Erweiterung durchführen oder den Vorgang stilllegen.

   Sie können das Diagramm überprüfen, um den Fortschritt für jeden Speicherknoten zu überwachen.

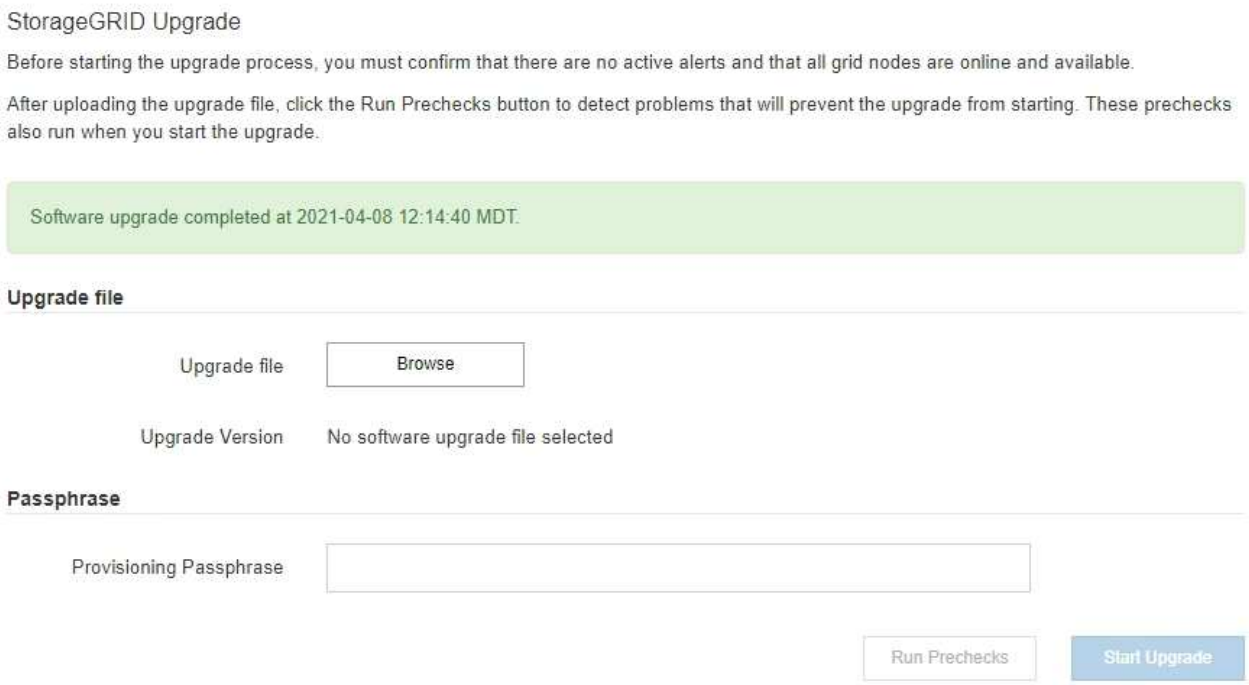


9. Wenn der Task **Upgrade Database** abgeschlossen ist, warten Sie einige Minuten, bis die Aufgabe **Final Upgrade Steps** abgeschlossen ist.



Nach Abschluss der Aufgabe „Letzte Upgrade-Schritte“ wird das Upgrade durchgeführt.

10. Bestätigen Sie, dass das Upgrade erfolgreich abgeschlossen wurde.
    a. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
    b. Wählen Sie **Hilfe** > **Info**.
    c. Vergewissern Sie sich, dass die angezeigte Version den Erwartungen entspricht.
    d. Wählen Sie **Wartung** > **System** > **Software-Update**. Wählen Sie dann **StorageGRID-Upgrade**.
    e. Vergewissern Sie sich, dass das grüne Banner zeigt, dass das Software-Upgrade an dem erwarteten Datum und der erwarteten Uhrzeit abgeschlossen wurde.



11. 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.
12. Prüfen Sie die StorageGRID-Seite zu NetApp Downloads, um zu sehen, ob Hotfixes für die von Ihnen gerade installierte StorageGRID-Version verfügbar sind.

    "NetApp Downloads: StorageGRID"

    In der StorageGRID 11.5.*x.y* Versionsnummer:

    - Die Hauptversion hat einen *x*-Wert von 0 (11.5.0).
    - Eine kleine Version hat, falls verfügbar, einen anderen *x*-Wert als 0 (z. B. 11.5.1).
    - Ein Hotfix, falls verfügbar, hat einen *y*-Wert (z. B. 11.5.0.1).
13. Falls verfügbar, laden Sie den neuesten Hotfix für Ihre StorageGRID-Version herunter und wenden Sie ihn an.

    Informationen zur Anwendung von Hotfixes finden Sie in der Recovery- und Wartungsanleitung.

Verwandte Informationen

"Herunterladen des Wiederherstellungspakets"

"Verwalten Sie erholen"

Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten

Nach dem Upgrade auf StorageGRID 11.5 können Sie die Einstellung für das System „Metadaten reserviert Speicherplatz“ möglicherweise erhöhen, wenn Ihre Speicherknoten

spezifische Anforderungen an RAM und verfügbaren Speicherplatz erfüllen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder die Rastertopologie-Seitenkonfiguration und andere Grid-Konfigurationsberechtigungen verfügen.
- Sie haben das StorageGRID 11.5 Upgrade gestartet und die Upgrade-Aufgabe **Neue Funktionen** aktivieren ist abgeschlossen.

Über diese Aufgabe

Möglicherweise können Sie den reservierten Speicherplatz für systemweite Metadaten nach dem Upgrade auf StorageGRID 11.5 manuell auf 8 TB erhöhen. Durch die Reservierung von zusätzlichem Metadatenspeicherplatz nach dem Upgrade 11.5 werden zukünftige Hardware- und Software-Upgrades vereinfacht.

Sie können nur den Wert der Einstellung für systemweiten reservierten Speicherplatz für Metadaten erhöhen, wenn beide dieser Anweisungen wahr sind:

- Die Speicherknoten an einem beliebigen Standort in Ihrem System haben jeweils 128 GB oder mehr RAM.
- Die Speicherknoten an jedem Standort in Ihrem System verfügen jeweils über genügend Platz auf dem Speichervolumen 0.

Wenn Sie diese Einstellung erhöhen, reduzieren Sie gleichzeitig den für den Objektspeicher verfügbaren Platz auf dem Speichervolumen 0 aller Storage-Nodes. Aus diesem Grund möchten Sie möglicherweise den reservierten Speicherplatz für Metadaten auf einen Wert kleiner als 8 TB setzen, der auf den erwarteten Anforderungen für Objektmetadaten basiert.

> Im Allgemeinen ist es besser, einen höheren Wert anstelle eines niedrigeren Wertes zu verwenden. Wenn die Einstellung für reservierten Speicherplatz für Metadaten zu groß ist, können Sie sie später verkleinern. Wenn Sie den Wert später erhöhen, muss das System dagegen möglicherweise Objektdaten verschieben, um Speicherplatz freizugeben.

Eine detaillierte Erläuterung der Auswirkung der Einstellung „Metadatenreservierter Speicherplatz“ auf den zulässigen Speicherplatz für Objekt-Metadaten-Storage auf einem bestimmten Storage-Node finden Sie in den Anweisungen zum Verwalten von StorageGRID und suchen nach „`managing-Objekt-Metadaten-Storage`“.

"StorageGRID verwalten"

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. Legen Sie die aktuelle Einstellung für den reservierten Metadatenspeicherplatz fest.
   a. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Speicheroptionen**.
   b. Notieren Sie im Abschnitt SpeicherWatermarks den Wert von **Metadaten Reserved Space**.
3. Stellen Sie sicher, dass auf dem Speicher-Volume 0 jedes Speicherknoten genügend Speicherplatz zur Verfügung steht, um diesen Wert zu erhöhen.
   a. Wählen Sie **Knoten**.
   b. Wählen Sie den ersten Storage-Node im Raster aus.
   c. Wählen Sie die Registerkarte Storage aus.

d. Suchen Sie im Abschnitt Volumes den Eintrag **/var/local/rangedb/0**.

e. Vergewissern Sie sich, dass der verfügbare Wert gleich oder größer ist als der Unterschied zwischen dem neuen Wert, den Sie verwenden möchten, und dem aktuellen Wert für reservierten Metadatenspeicherplatz.

   Wenn die Einstellung für reservierten Speicherplatz für Metadaten beispielsweise aktuell 4 TB beträgt und Sie diesen auf 6 TB erhöhen möchten, muss der verfügbare Wert 2 TB oder mehr sein.

f. Wiederholen Sie diese Schritte für alle Speicherknoten.

   - Wenn ein oder mehrere Speicherknoten nicht über genügend Speicherplatz verfügen, kann der Wert für den reservierten Metadatenspeicherplatz nicht erhöht werden. Fahren Sie mit diesem Verfahren nicht fort.
   - Wenn jeder Speicherknoten genügend Platz auf Volume 0 hat, fahren Sie mit dem nächsten Schritt fort.

4. Stellen Sie sicher, dass Sie mindestens 128 GB RAM auf jedem Speicherknoten haben.

   a. Wählen Sie **Knoten**.

   b. Wählen Sie den ersten Storage-Node im Raster aus.

   c. Wählen Sie die Registerkarte **Hardware** aus.

   d. Bewegen Sie den Mauszeiger über das Diagramm „Speicherauslastung“. Vergewissern Sie sich, dass **Total Memory** mindestens 128 GB beträgt.

   e. Wiederholen Sie diese Schritte für alle Speicherknoten.

      - Wenn mindestens ein Speicherknoten nicht über genügend Gesamtspeicher verfügt, kann der Wert für den reservierten Metadatenspeicherplatz nicht erhöht werden. Fahren Sie mit diesem Verfahren nicht fort.
      - Wenn jeder Speicherknoten mindestens 128 GB Gesamtspeicher hat, fahren Sie mit dem nächsten Schritt fort.

5. Aktualisieren Sie die Einstellung für reservierten Metadatenspeicherplatz.

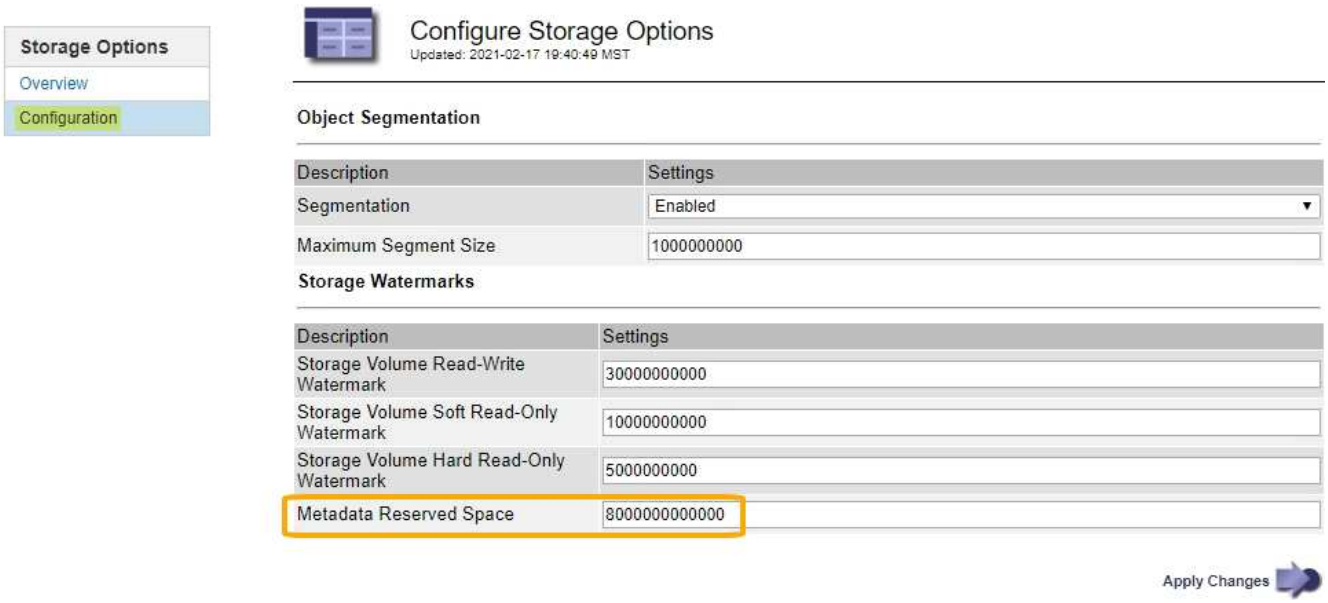
   a. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Speicheroptionen**.

   b. Wählen Sie die Registerkarte Konfiguration aus.

   c. Wählen Sie im Abschnitt SpeicherWatermarks die Option **Metadatenreservierter Speicherplatz** aus.

   d. Geben Sie den neuen Wert ein.

      Um beispielsweise 8 TB einzugeben, geben Sie **8000000000000** (8, gefolgt von 12 Nullen) ein.



a. Wählen Sie **Änderungen Anwenden**.

Fehlerbehebung bei Upgrade-Problemen

Wenn das Upgrade nicht erfolgreich abgeschlossen wird, können Sie das Problem möglicherweise selbst beheben. Falls ein Problem nicht behoben werden kann, sollten Sie die erforderlichen Informationen erfassen, bevor Sie sich an den technischen Support wenden.

In den folgenden Abschnitten wird die Wiederherstellung in Situationen beschrieben, in denen das Upgrade teilweise fehlgeschlagen ist. Wenden Sie sich an den technischen Support, wenn ein Upgrade-Problem nicht behoben werden kann.

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. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen.

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 Datenaufnahme oder -Abfrage bei keinem Upgrade eines Grid-Node unerwartet unterbrochen wird, wenden Sie sich an den technischen Support.

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"

Fehlerbehebung bei Problemen mit der Benutzeroberfläche

Nach dem Upgrade auf eine neue Version der StorageGRID-Software sind möglicherweise Probleme mit dem Grid Manager oder dem Tenant Manager zu sehen.

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 einen unterstützten Browser verwenden.

  Die Browser-Unterstützung wurde für StorageGRID 11.5 geändert. Vergewissern Sie sich, dass Sie eine unterstützte Version verwenden.

- 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.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

Fehlermeldungen bei der „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 kann nicht ermittelt werden `{node_name}`.	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. Weitere Informationen finden Sie in der Installationsanleitung für Ihre Linux-Plattform.
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.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Installation und Wartung von Hardware

SG6000 Storage-Appliances

So installieren und warten Sie die StorageGRID SG6060 und SGF6024 Appliances.

- "SG6000 Appliances – Übersicht"
- "Übersicht über Installation und Implementierung"
- "Installation wird vorbereitet"
- "Installieren der Hardware"
- "Konfigurieren der Hardware"
- "Implementieren eines Appliance-Storage-Node"
- "Monitoring der Installation der Speicher-Appliance"
- "Automatisierung der Installation und Konfiguration von Appliances"
- "Überblick über die Installations-REST-APIs"
- "Fehlerbehebung bei der Hardwareinstallation"
- "Warten des SG6000-Geräts"

SG6000 Appliances – Übersicht

Die StorageGRIDSG6000 Appliances sind integrierte Storage- und Computing-Plattformen, die als Storage-Nodes in einem StorageGRID System betrieben werden. Diese Appliances können in einer hybriden Grid-Umgebung eingesetzt werden, in der Appliance Storage Nodes und virtuelle (softwarebasierte) Storage-Nodes kombiniert werden.

Die SG6000-Appliances bieten folgende Funktionen:

- Erhältlich in zwei Modellen:
  - SG6060, das 60 Laufwerke umfasst und Erweiterungs-Shelfs unterstützt.
  - SGF6024 mit 24 Solid State-Laufwerken (SSDs)
- 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.
- Schließen Sie den SANtricity System Manager zum Managen und Überwachen von Storage Controllern und Laufwerken an.
- Schließen Sie einen Baseboard Management Controller (BMC) für die Überwachung und Diagnose der Hardware im Compute-Controller an.
- Unterstützung für bis zu vier 10-GbE- oder 25-GbE-Verbindungen mit dem StorageGRID-Grid-Netzwerk und dem Client-Netzwerk.
- Unterstützung von FIPS-Laufwerken (Federal Information Processing Standard). Wenn diese Laufwerke mit der Laufwerksicherheitsfunktion in SANtricity System Manager verwendet werden, wird ein nicht autorisierter Zugriff auf die Daten verhindert.

SG6060 Übersicht

Die StorageGRIDSG6060 Appliance umfasst einen Computing-Controller und ein Storage-Controller-Shelf, das zwei Storage-Controller und 60 Laufwerke enthält. Optionale Erweiterungs-Shelfs mit 60 Laufwerken können der Appliance hinzugefügt werden.

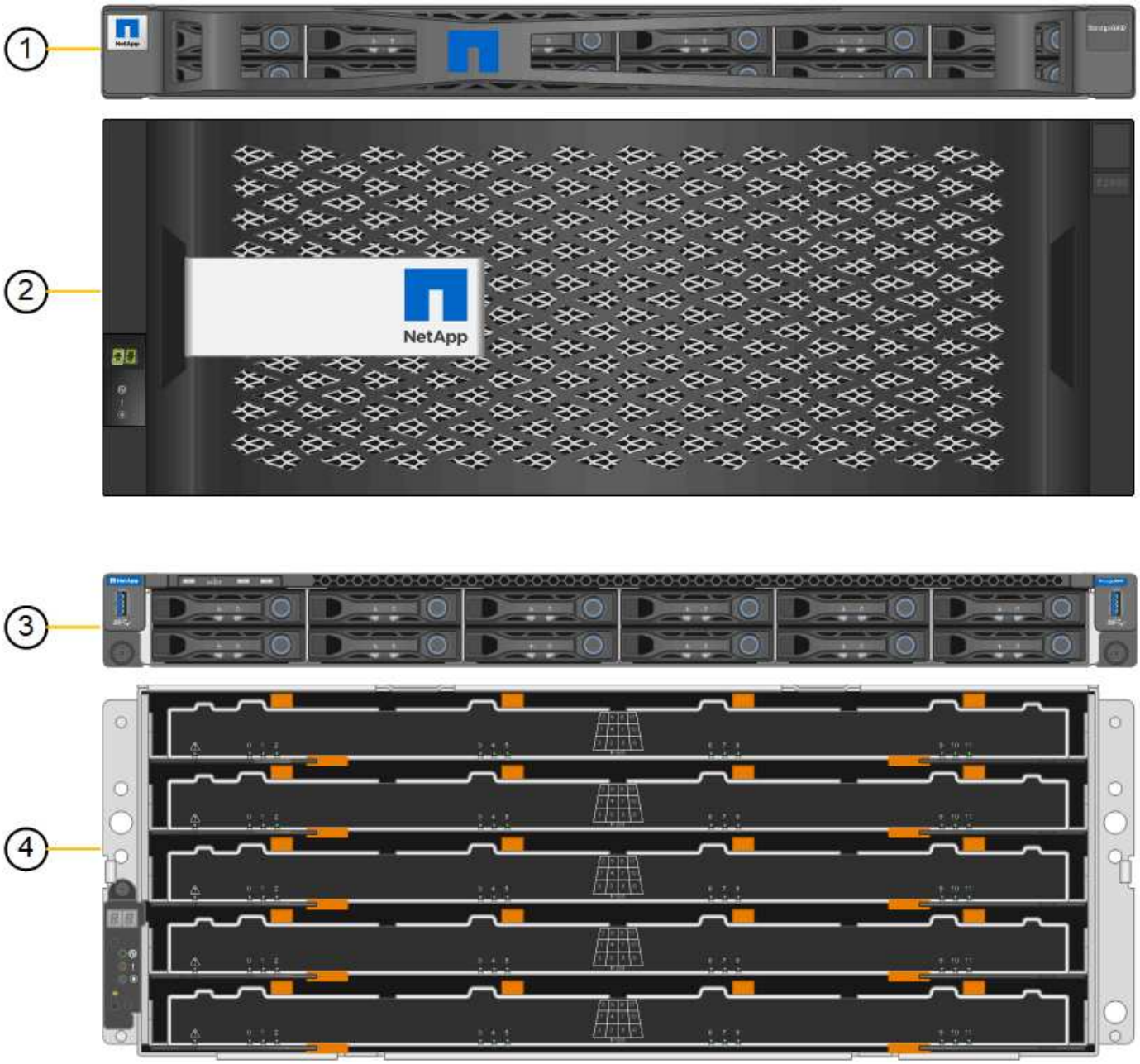
SG6060-Komponenten

Die SG6060 Appliance umfasst die folgenden Komponenten:

Komponente	Beschreibung
Computing-Controller	SG6000-CN-Controller, ein 1U-Server (1 Rack-Einheit) mit folgenden Komponenten: • 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
Storage Controller Shelf	E-Series E2860 Controller-Shelf (Storage-Array), ein 4-HE-Shelf mit folgenden Komponenten: • Zwei E-Series E2800 Controller (Duplexkonfiguration) für die Unterstützung von Storage-Controller-Failover • 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
Optional: Storage-Erweiterungs-Shelfs **Hinweis:** Erweiterungseinschübe können bei der ersten Implementierung installiert oder später hinzugefügt werden.	E-Series DE460C Gehäuse, ein 4-HE-Shelf mit folgenden Komponenten: • Zwei Eingangs-/Ausgangsmodule (IOMs) • Fünf Schubladen mit jeweils 12 NL-SAS-Laufwerken für insgesamt 60 Laufwerke • Redundante Netzteile und Lüfter Jede SG6060 Appliance kann ein oder zwei Erweiterungs-Shelfs für insgesamt 180 Laufwerke enthalten.

SG6060-Diagramme

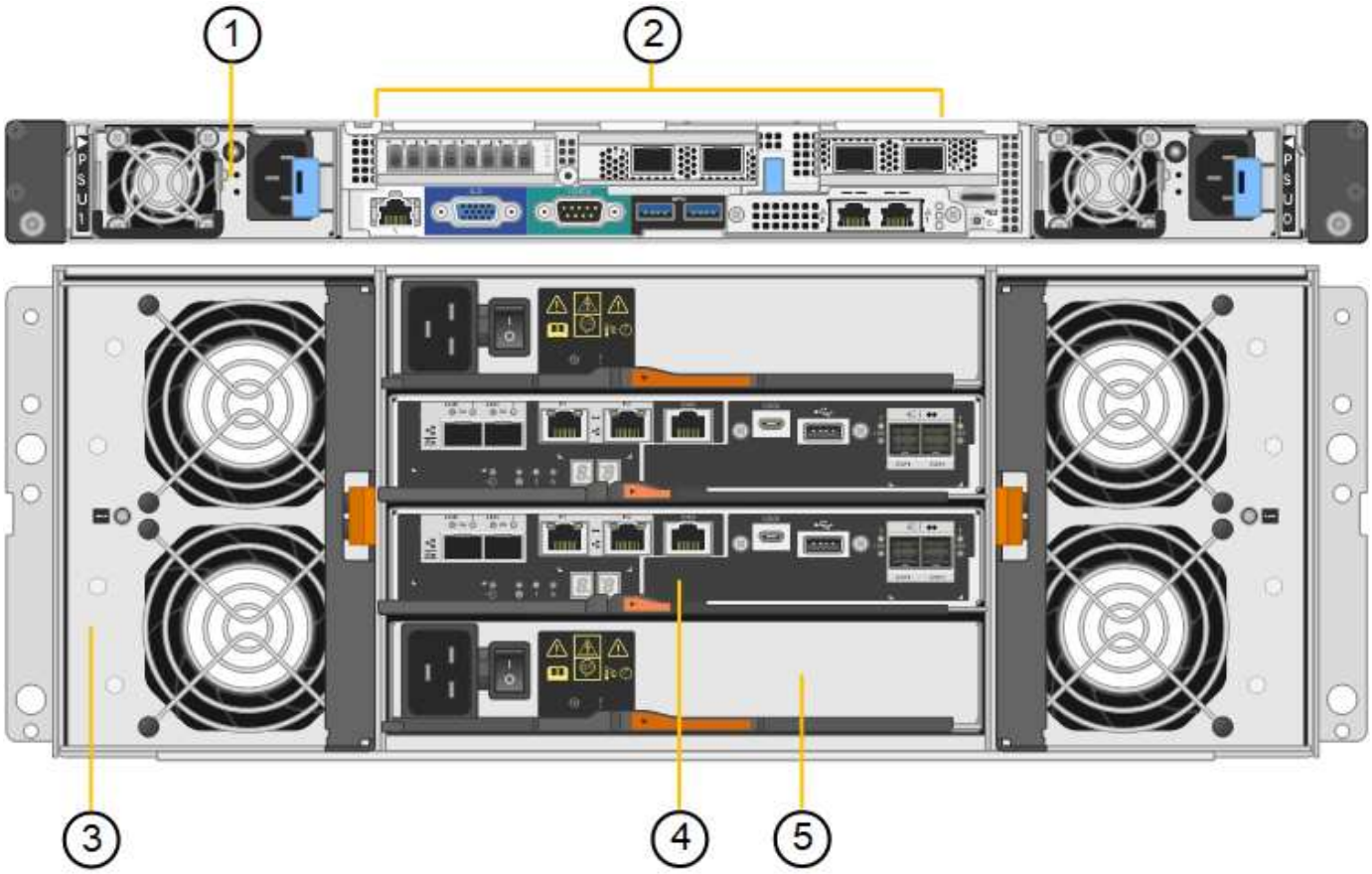
Diese Abbildung zeigt die Vorderseite des SG6060, das einen 1-HE-Computing-Controller und ein 4-HE-Shelf mit zwei Storage-Controllern und 60 Laufwerken in fünf LaufwerkSchubladen enthält.



	Beschreibung
1	SG6000-CN Computing Controller mit Frontblende
2	E2860 Controller-Shelf mit Frontblende (optionales Erweiterungs-Shelf sieht identisch aus)
3	SG6000-CN Computing Controller mit abnehmbarer Frontblende

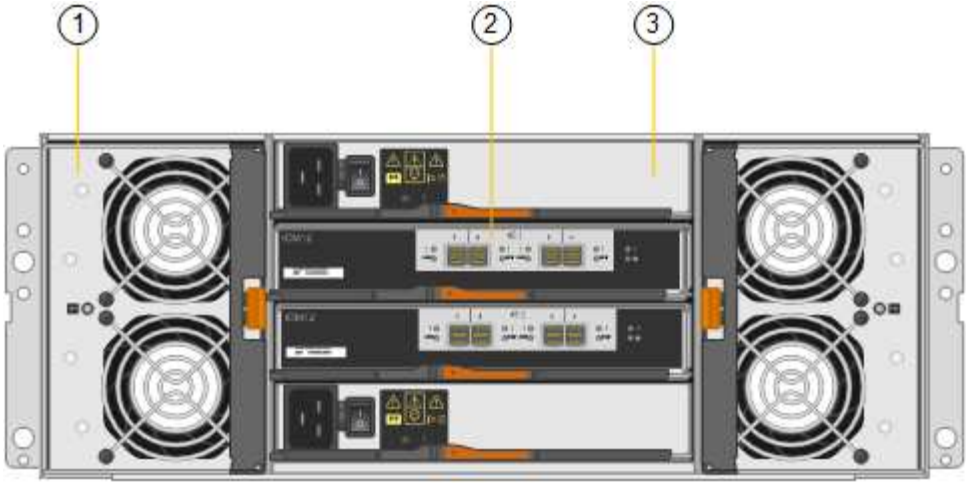
	Beschreibung
4	E2860 Controller-Shelf mit entfernter Frontblende (optionales Erweiterungs-Shelf sieht identisch aus)

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



	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 E2800 Storage-Controller (1 von 2) und Anschlüsse
5	Netzteil (1 von 2) für E2860 Controller-Shelf

Diese Abbildung zeigt die Rückseite des optionalen Erweiterungs-Shelf für das SG6060, 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.



	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

SGF6024 Übersicht

StorageGRIDSGF6024 umfasst einen Computing-Controller und ein Storage-Controller-Shelf für 24 Solid State-Laufwerke.

SGF6024-Komponenten

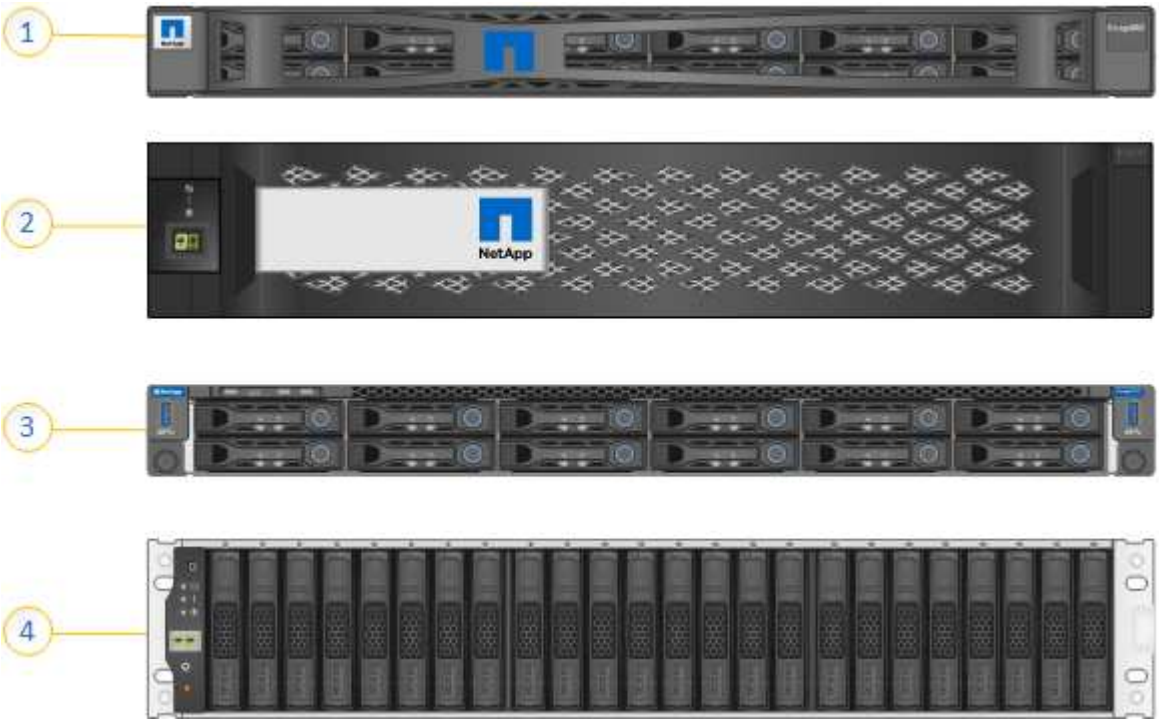
Die SGF6024 Appliance umfasst die folgenden Komponenten:

Komponente	Beschreibung
Computing-Controller	SG6000-CN-Controller, ein 1U-Server (1 Rack-Einheit) mit folgenden Komponenten: • 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
Flash-Array (Controller-Shelf)	E-Series EF570 Flash-Array (auch als Controller-Shelf bekannt), ein 2-HE-Shelf mit folgenden Vorteilen: • Zwei E-Series EF570 Controller (Duplexkonfiguration) für Storage-Controller-Failover-Unterstützung • 24 Solid State-Laufwerke (auch als SSDs oder Flash-Laufwerke bekannt) • Redundante Netzteile und Lüfter

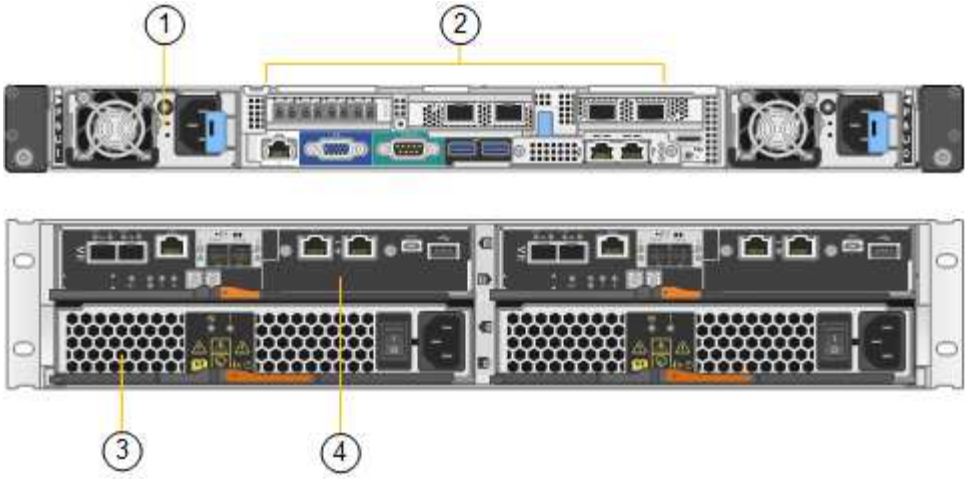
SGF6024-Diagramme

Diese Abbildung zeigt die Vorderseite des SGF6024 mit einem 1-HE-Computing-Controller und einem 2-HE-Gehäuse mit zwei Storage-Controllern und 24 Flash-Laufwerken.



	Beschreibung
1	SG6000-CN Computing Controller mit Frontblende
2	EF570 Flash-Array mit Frontblende
3	SG6000-CN Computing Controller mit abnehmbarer Frontblende
4	EF570 Flash-Array mit abnehmbarer Frontblende

Diese Abbildung zeigt die Rückseite des SGF6024, einschließlich der Computing- und Storage-Controller, Lüfter und Netzteile.



	Beschreibung
1	Netzteil (1 von 2) für SG6000-CN Compute Controller
2	Anschlüsse für SG6000-CN Compute Controller
3	Netzteil (1 von 2) für EF570 Flash-Array
4	E-Series EF570 Storage-Controller (1 von 2) und Anschlüsse

Controller in SG6000 Appliances

Jedes Modell der StorageGRIDSG6000 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.

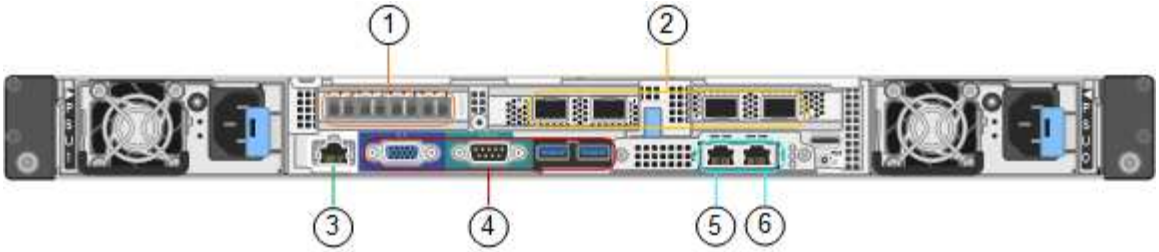
Alle Appliances: SG6000-CN Computing Controller

- 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.

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des SG6000-CN.



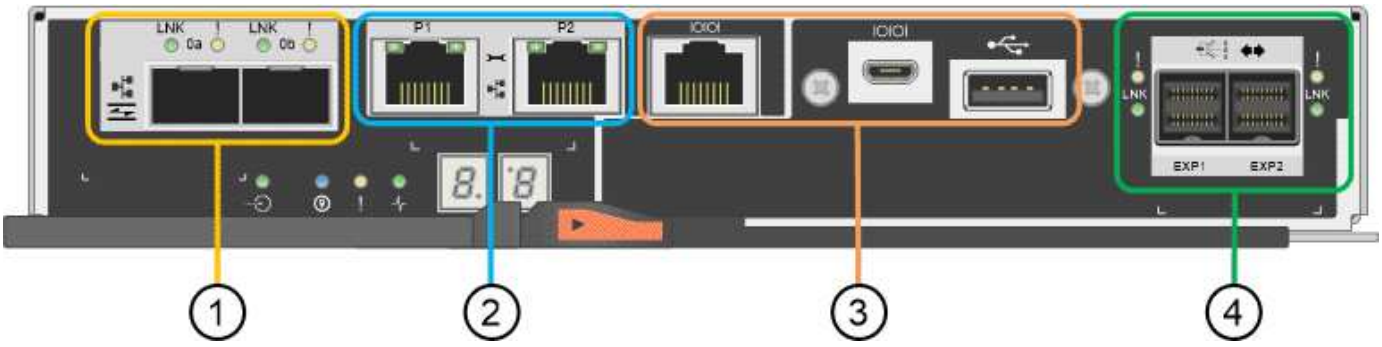
	Port	Typ	Nutzung
1	Interconnect-Ports 1-4	16 Gbit/s Fibre Channel (FC) mit integrierter Optik	Verbinden Sie den SG6000-CN Controller mit den E2800 Controllern (zwei Verbindungen zu jedem E2800).
2	Netzwerkanschlüsse 1-4	10-GbE oder 25-GbE auf Basis von Kabel- oder SFP-Transceiver, Switch-Geschwindigkeit 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	• 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.

	Port	Typ	Nutzung
6	Admin – Netzwerkanschluss 2	1 GbE (RJ-45)	Optionen: • 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.

SG6060: 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.

Diese Abbildung zeigt die Anschlüsse der Rückseite jedes E2800 Controllers.

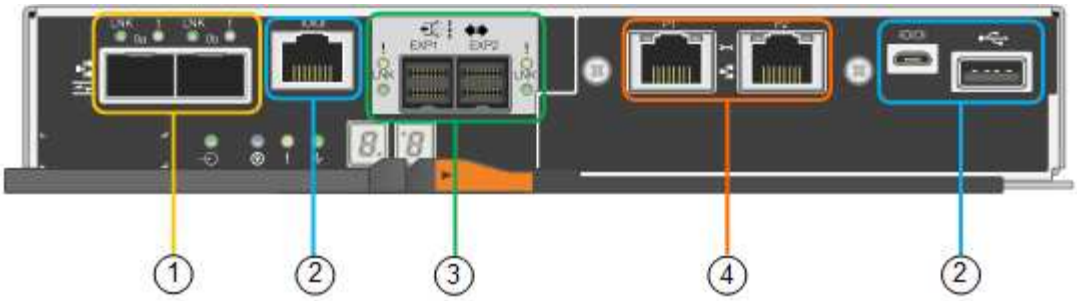


	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	16 Gbit/s FC optisch SFPA	Verbinden Sie jeden der E2800 Controller mit dem SG6000-CN Controller. Es sind vier Verbindungen zum SG6000-CN Controller vorhanden (zwei von jedem E2800).
2	Management-Ports 1 und 2	1-GB-Ethernet (RJ-45	• Port 1 stellt eine Verbindung zum Netzwerk her, in dem Sie in einem Browser auf SANtricity System Manager zugreifen. • Port 2 ist für den technischen Support reserviert.
3	Diagnose- und Supportports	• 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.

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.

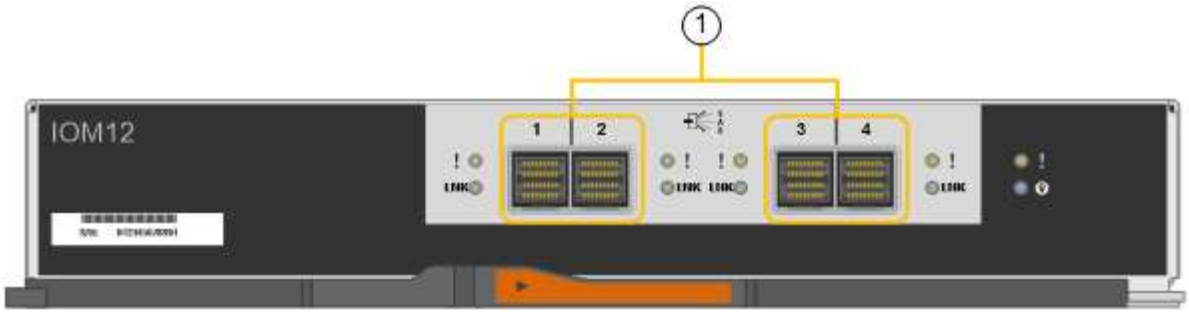
Diese Abbildung zeigt die Anschlüsse auf der Rückseite jedes EF570 Controllers.



	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	16 Gbit/s FC optisch SFPA	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	• 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	• 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: Ein-/Ausgabemodule für optionale Erweiterungs-Shelfs

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



	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).

Übersicht über Installation und Implementierung

Sie können eine oder mehrere StorageGRID Storage Appliances installieren, wenn Sie StorageGRID zum ersten Mal implementieren. Alternativ können Sie Appliance Storage-Nodes später im Rahmen einer Erweiterung hinzufügen. Möglicherweise müssen Sie auch einen Appliance-Speicherknoten im Rahmen eines Wiederherstellungsvorgangs installieren.

Was Sie benötigen

Ihr StorageGRID System verwendet die erforderliche Version der StorageGRID Software.

Appliance	Erforderliche StorageGRID Version
SG6060 ohne Erweiterungs-Shelfs	11.1.1 oder höher
SG6060 mit Erweiterungs-Shelfs (ein oder zwei)	11.3 oder höher **Hinweis:** Wenn Sie Erweiterungs-Shelfs nach der ersten Implementierung hinzufügen, müssen Sie Version 11.4 oder höher verwenden.
SGF6024	11.3 oder höher

Installations- und Implementierungsaufgaben

Das Hinzufügen einer StorageGRID Storage Appliance zu einem StorageGRID System umfasst vier primäre Schritte:

1. Installation vorbereiten:
   - Vorbereiten des Installationsstandorts

- Auspacken der Schachteln und Prüfen des Inhalts
- Zusätzliche Ausrüstung und Werkzeuge
- Sammeln von IP-Adressen und Netzwerkinformationen
- Optional: Konfiguration eines externen Verschlüsselungsmanagement-Servers (KMS), wenn Sie alle Appliance-Daten verschlüsseln möchten. Weitere Informationen zum externen Verschlüsselungsmanagement finden Sie in der Anleitung zur Administration von StorageGRID.

2. Installieren der Hardware:
   - Registrieren der Hardware
   - Installieren des Geräts in einem Schrank oder Rack
   - Installieren der Laufwerke
   - Installation optionaler Erweiterungs-Shelfs (nur Modell SG6060, maximal zwei Erweiterungs-Shelfs)
   - Verkabeln Sie das Gerät
   - Anschließen der Stromkabel und Strom anschließen
   - Anzeigen von Boot-Statuscodes
3. Konfigurieren der Hardware:
   - Zugriff auf SANtricity System Manager zur Konfiguration von SANtricity System Manager Einstellungen
   - Zugriff auf das Installationsprogramm von StorageGRID Appliance, Festlegen einer statischen IP-Adresse für Management Port 1 auf dem Storage Controller und Konfiguration der Link- und Netzwerk-IP-Einstellungen, die für die Verbindung mit StorageGRID-Netzwerken erforderlich sind
   - Zugriff auf die Schnittstelle des Baseboard Management Controller (BMC) auf dem SG6000-CN Controller
   - Optional: Aktivieren der Node-Verschlüsselung, wenn Sie zur Verschlüsselung von Appliance-Daten einen externen KMS verwenden möchten.
   - Optional: Ändern des RAID-Modus.
4. Bereitstellen der Appliance als Storage-Node:

Aufgabe	Anweisungen
Bereitstellen eines Appliance-Speicherknoten in einem neuen StorageGRID-System	"Implementieren eines Appliance-Storage-Node"
Hinzufügen eines Appliance-Speicherknotens zu einem vorhandenen StorageGRID-System	Anweisungen zum erweitern eines StorageGRID-Systems
Bereitstellen eines Appliance-Speicherknotens als Teil eines Speicherknotenwiederherstellungsvorgangs	Anweisungen zur Wiederherstellung und Wartung

Verwandte Informationen

"Installation wird vorbereitet"

"Installieren der Hardware"

"Konfigurieren der Hardware"

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

"StorageGRID verwalten"

Installation wird vorbereitet

Die Vorbereitung der Installation einer StorageGRID Appliance umfasst die Vorbereitung des Standorts und den Erwerb aller erforderlichen Hardware, Kabel und Tools. Außerdem sollten Sie IP-Adressen und Netzwerkinformationen erfassen.

Schritte

- "Vorbereiten der Site (SG6000)"
- "Auspacken der Boxen (SG6000)"
- "Beschaffung zusätzlicher Geräte und Werkzeuge (SG6000)"
- "Anforderungen an einen Webbrowser"
- "Überprüfen von Appliance-Netzwerkverbindungen"
- "Sammeln von Installationsinformationen (SG6000)"

Vorbereiten der Site (SG6000)

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. Weitere Informationen finden Sie im NetApp Hardware Universe.
2. Stellen Sie sicher, dass Ihr Standort 240-Volt-Wechselstrom für die SG6060- oder 120-Volt-Wechselstromversorgung des SGF6024 bereitstellt.
3. Passen Sie zu 48.3 Shelfs dieser Größe (ohne Kabel) ein 19-cm-Gehäuse oder -Rack an:

Typ des Shelfs	Höhe	Breite	Tiefe	Maximales Gewicht
E2860 Controller-Shelf für SG6060	6.87 Zoll (17.46 cm)	17.66 Zoll (44.86 cm)	38.25 Zoll (97.16 cm)	250 lb. (113 kg)
Optionales Erweiterungs-Shelf für SG6060 (ein oder zwei)	6.87 Zoll (17.46 cm)	17.66 Zoll (44.86 cm)	38.25 Zoll (97.16 cm)	250 lb. (113 kg)

Typ des Shelfs	Höhe	Breite	Tiefe	Maximales Gewicht
EF570 Controller Shelf für 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-Controller für jedes Gerät	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 im Lieferumfang des Geräts enthaltenen 0,5-m-Glasfaserkabel oder -Kabel lang genug für das geplante Layout sind.

Verwandte Informationen

"NetApp Hardware Universe"

"NetApp Interoperabilitäts-Matrix-Tool"

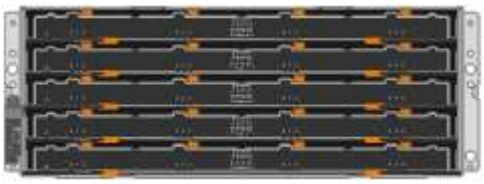
Auspacken der Boxen (SG6000)

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

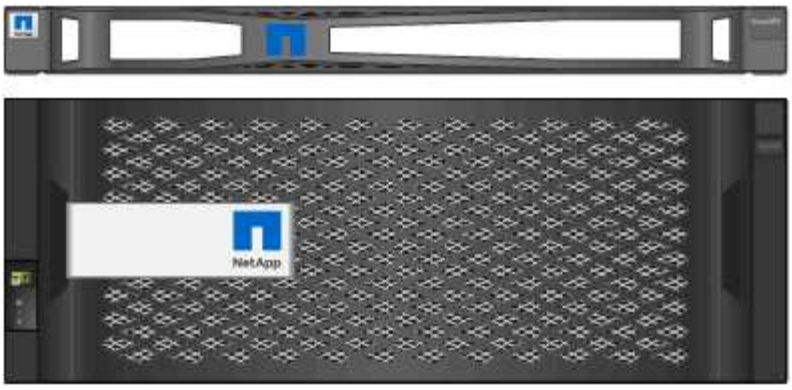
SG6060

- **SG6000-CN-Controller**

- **E2860 Controller-Shelf ohne Laufwerke installiert**

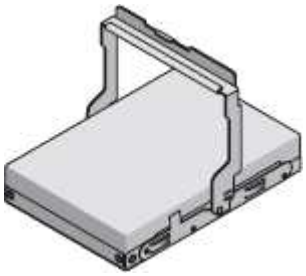


- **Zwei Vorderkämpfe**

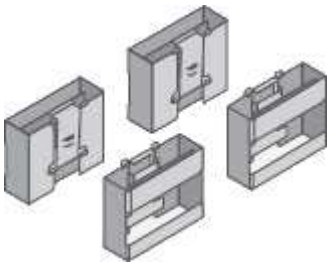


- **Zwei Schienen-Kits mit Anweisungen**

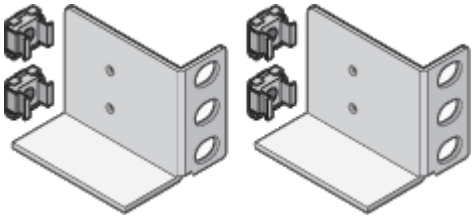
- **60 Laufwerke (2 SSD und 58 NL-SAS)**



- **Vier Griffe**



- **Hintere Halterungen und Käfigmuttern für quadratische Rackmontage**

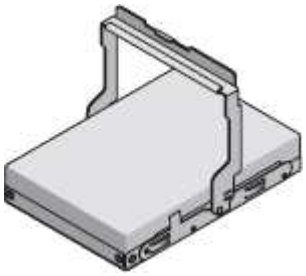


SG6060 Erweiterungs-Shelf

- **Erweiterungs-Shelf ohne installierte Laufwerke**

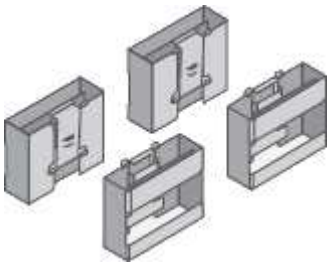
- **Frontblende**

- **60 NL-SAS-Laufwerke**

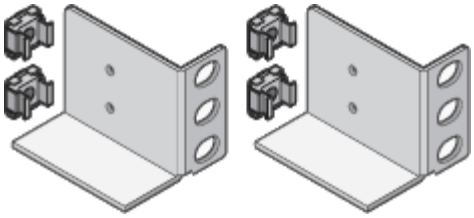


- **Ein Schienen-Kit mit Anweisungen**

- **Vier Griffe**



- **Hintere Halterungen und Käfigmuttern für quadratische Rackmontage**



SGF6024

- **SG6000-CN-Controller**

- **EF570 Flash-Array mit installierten 24 Solid State-Laufwerken**

- **Zwei Vorderkämpfe**

- **Zwei Schienen-Kits mit Anweisungen**

- **Regal Endcaps**

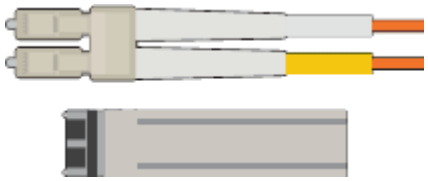
Kabel und Anschlüsse

Der Versand für das StorageGRID Gerät umfasst die folgenden Kabel und Anschlüsse:

- **Vier Netzkabel für Ihr Land**

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

- **Optische Kabel und SFP-Transceiver**



Vier optische Kabel für die FC Interconnect Ports

Vier SFP+-Transceiver, die 16 Gbit/s FC unterstützen

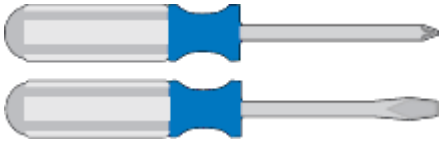
- **Optional: Zwei SAS-Kabel zum Anschließen jedes SG6060 Erweiterungs-Shelf**

Beschaffung zusätzlicher Geräte und Werkzeuge (SG6000)

Vergewissern Sie sich vor der Installation der StorageGRID Appliance, dass alle zusätzlichen Geräte und Tools zur Verfügung stehen, die Sie benötigen.

Sie benötigen die folgende zusätzliche Ausrüstung für die Installation und Konfiguration der Hardware:

- **Schraubendreher**

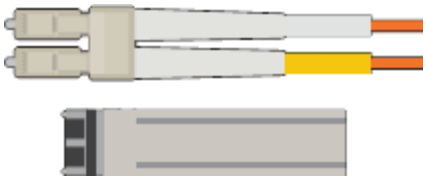


Phillips Nr. 2 Schraubendreher

Mittlerer Schlitzschraubendreher

- **ESD-Handgelenkschlaufe**

- **Optische Kabel und SFP-Transceiver**



Sie benötigen eine der folgenden Optionen:

  - Ein bis vier Twinax-Kabel oder optische Kabel für die 10/25-GbE-Ports, die Sie auf dem SG6000-CN Controller verwenden möchten
  - Ein bis vier SFP+-Transceiver für die 10/25-GbE-Ports, wenn Sie optische Kabel und 10-GbE-Verbindungsgeschwindigkeit verwenden
  - Ein bis vier SFP28-Transceiver für die 10/25-GbE-Ports, wenn Sie optische Kabel und 25-GbE-Verbindungsgeschwindigkeit verwenden werden

- * RJ-45 (Cat5/Cat5e/Cat6) Ethernet-Kabel*

- **Service-Laptop**

Unterstützter Webbrowser

1-GbE-Port (RJ-45

- **Optionale Werkzeuge**

Kraftbohrer mit Kreuzschlitz

Taschenlampe

Mechanisierter Lift für 60-Laufwerk-Shelfs

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Überprüfen von Appliance-Netzwerkverbindungen

Vor der Installation der StorageGRID Appliance sollten Sie wissen, welche Netzwerke mit der Appliance verbunden werden können.

Wenn Sie eine StorageGRID-Appliance als Speicherknoten in einem StorageGRID-System bereitstellen, können Sie sie mit folgenden Netzwerken verbinden:

- **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. Das Client-Netzwerk ist optional.
- **Managementnetzwerk für SANtricity System Manager**: Dieses Netzwerk bietet Zugriff auf SANtricity System Manager auf dem Storage Controller, so dass Sie die Hardwarekomponenten im Storage 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-Verwaltungsnetzwerk für den SG6000-CN-Controller:** Dieses Netzwerk bietet Zugriff auf den Baseboard-Management-Controller im SG6000-CN, sodass Sie die Hardwarekomponenten des SG6000-CN-Controllers überwachen und verwalten können. Dieses Managementnetzwerk kann das gleiche sein wie das Admin-Netzwerk für StorageGRID, oder es kann ein unabhängiges Managementnetzwerk sein.

Ausführliche Informationen zu StorageGRID-Netzwerken finden Sie unter *Rasterprimer*.

Verwandte Informationen

"Sammeln von Installationsinformationen (SG6000)"

"Verkabeln des Geräts (SG6000)"

"Port Bond-Modi für den SG6000-CN-Controller"

"Netzwerkrichtlinien"

Port Bond-Modi für den SG6000-CN-Controller

Wenn Sie Netzwerkverbindungen für das SG6000-CN konfigurieren, können Sie die Portbindung für die 10/25-GbE-Ports verwenden, die eine Verbindung zum Grid-Netzwerk und dem optionalen Client-Netzwerk herstellen, sowie 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.

Verwandte Informationen

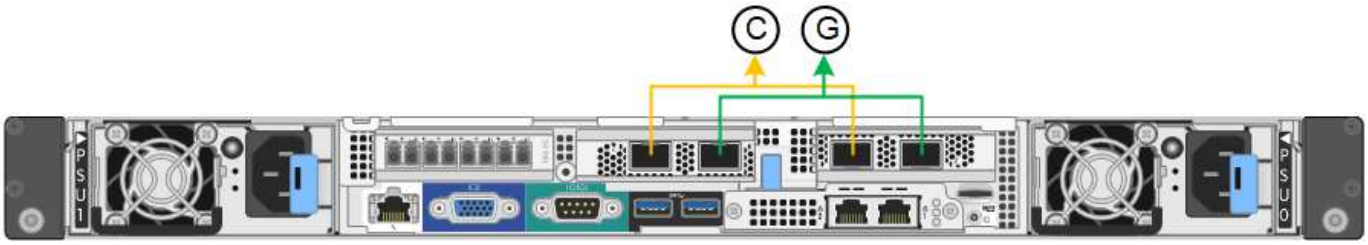
"Konfigurieren von Netzwerkverbindungen (SG6000)"

Netzwerk-Bond-Modi für die 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.



	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.

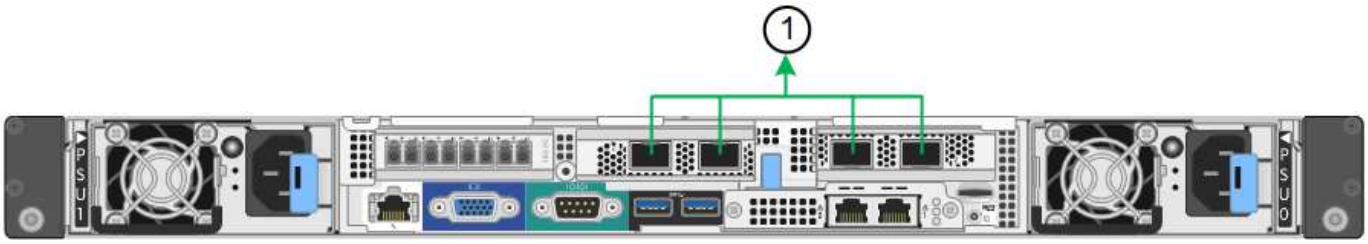
- Im LACP-Modus bildet jedes Port-Paar einen logischen Kanal zwischen dem Controller und dem Netzwerk, wodurch ein höherer Durchsatz ermöglicht wird. Wenn ein Port ausfällt, stellt der andere Port den Kanal weiterhin bereit. Der Durchsatz wird verringert, die Konnektivität wird jedoch nicht beeinträchtigt.

> 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.



	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 müssen wissen, wie die Switches konfiguriert werden, um VLAN, LACP und MLAG zu verwenden.

Wenn Sie nicht alle vier 10/25-GbE-Ports verwenden möchten, können Sie ein, 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 die 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.

	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).

Sammeln von Installationsinformationen (SG6000)

Bei der Installation und Konfiguration der StorageGRID Appliance sind Entscheidungen zu treffen und Informationen zu Ethernet Switch-Ports, IP-Adressen sowie zu Port- und Netzwerk-Bond-Modi zu sammeln.

Über diese Aufgabe

Die folgenden Tabellen enthalten die erforderlichen Informationen für jedes Netzwerk, das Sie mit der Appliance verbinden. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.

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

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

- SG6060: 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.		
Statische IP-Adresse, die Sie für die Appliance im Managementnetzwerk verwenden möchten	Für IPv4: • IPv4-Adresse: • Subnetzmaske: • Gateway: Für IPv6: • IPv6-Adresse: • Routingfähige IP-Adresse: • IP-Adresse des Storage Controller-Routers:	Für IPv4: • IPv4-Adresse: • Subnetzmaske: • Gateway: Für IPv6: • IPv6-Adresse: • Routingfähige IP-Adresse: • IP-Adresse des Storage Controller-Routers:
IP-Adressformat	Bitte auswählen: • IPv4 • IPv6	Bitte auswählen: • IPv4 • IPv6

Erforderliche Informationen	Ihr Wert für Controller A	Ihr Wert für Controller B
Geschwindigkeit und Duplexmodus **Hinweis:** Sie müssen sicherstellen, dass der Ethernet-Switch für das SANtricity-System-Manager-Managementnetzwerk auf Autonegotiation gesetzt ist.	Muss sein: • Autonegotiation (Standard)	Muss sein: • Autonegotiation (Standard)

Informationen, die für die Verbindung des SG6000-CN-Controllers mit dem Admin-Netzwerk erforderlich sind

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: • Nein • Ja (Standard)
Netzwerk-Bond-Modus	Bitte auswählen: • Unabhängig (Standard) • Aktiv/Backup
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)	

Erforderliche Informationen	Ihr Wert
MAC-Adresse für den Netzwerkport Admin **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.	
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.	• 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.	• IPv4-Adresse (CIDR): • Gateway:
Admin-Netzwerk-Subnetze (CIDR)	

Erforderliche Informationen zum Verbinden und Konfigurieren der 10/25-GbE-Ports auf dem 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	Bitte auswählen: • Auto (Standard) • 10 GBitE • 25 GBitE

Erforderliche Informationen	Ihr Wert
Port Bond-Modus	Bitte auswählen: • 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)	

Zum Anschließen des SG6000-CN-Controllers an das 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 SG6000-CN-Controllers mit dem Grid-Netzwerk verbunden.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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	• IPv4-Adresse (CIDR): • Gateway:

Erforderliche Informationen	Ihr Wert
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.	• 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: • Nein (Standard) • Ja.
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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	• 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.	• IPv4-Adresse (CIDR): • Gateway:

Zum Anschließen des SG6000-CN Controllers an das BMC-Managementnetzwerk erforderliche Informationen

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).

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	• IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den BMC-Verwaltungsport verwenden möchten	• IPv4-Adresse (CIDR): • Gateway:

Verwandte Informationen

"Controller in SG6000 Appliances"

"Überprüfen von Appliance-Netzwerkverbindungen"

"Port Bond-Modi für den SG6000-CN-Controller"

"Verkabeln des Geräts (SG6000)"

"StorageGRID-IP-Adressen werden konfiguriert"

Installieren der Hardware

Bei der Hardware-Installation wird der SG6000-CN Controller und das Storage Controller Shelf in ein Gehäuse oder Rack installiert, die Kabel angeschlossen und mit Strom versorgt.

Schritte

- "Registrieren der Hardware"
- "SG6060: Installieren von Shelfs mit 60 Laufwerken in einem Schrank oder Rack"
- "SG6060: Installieren der Laufwerke"
- "SGF6024: Installieren von Shelfs mit 24 Laufwerken in einem Rack oder Schrank"
- "SG6000-CN: Einbau in einen Schrank oder Rack"
- "Verkabeln des Geräts (SG6000)"
- "SG6060: Verkabelung der optionalen Erweiterungs-Shelfs"

- "Anschließen von Netzkabeln und Anwenden der Stromversorgung (SG6000)"
- "Anzeigen von Statusanzeigen und -Tasten auf dem SG6000-CN-Controller"
- "Anzeigen von Boot-Statuscodes für die SG6000-Speicher-Controller"

Registrieren der Hardware

Die Registrierung der Appliance-Hardware bietet Support-Vorteile.

Schritte

1. Suchen Sie die Seriennummer des Chassis für das Storage Controller Shelf.

   Sie finden die Nummer auf dem Packzettel, in Ihrer Bestätigungs-E-Mail oder auf dem Gerät nach dem Auspacken.

   Auf der Storage Appliance befinden sich mehrere Seriennummern. Die Seriennummer auf dem Storage-Controller-Shelf ist diejenige, die registriert werden muss und verwendet werden muss, wenn Sie Service oder Support für die Appliance benötigen.

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	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.
Neuer NetApp Kunde	a. Klicken Sie auf **Jetzt registrieren** und erstellen Sie ein Konto. b. Wählen Sie **Produkte** > **Produkte Registrieren**. c. Geben Sie die Seriennummer des Produkts und die angeforderten Details ein. Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.

SG6060: Installieren von Shelfs mit 60 Laufwerken in einem Schrank oder Rack

Sie müssen einen Satz Schienen für das E2860 Controller-Shelf in Ihrem Schrank oder Rack installieren und dann das Controller-Shelf auf die Schienen schieben. Bei Installation der Erweiterungs-Shelfs für 60 Laufwerke gilt dasselbe Verfahren.

Was Sie benötigen

- 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.

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 Shelfs müssen alle Laufwerke entfernt werden.

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 im Lieferumfang des Geräts enthaltenen 0,5-m-Glasfaserkabel oder -Kabel lang genug für das geplante Layout sind.

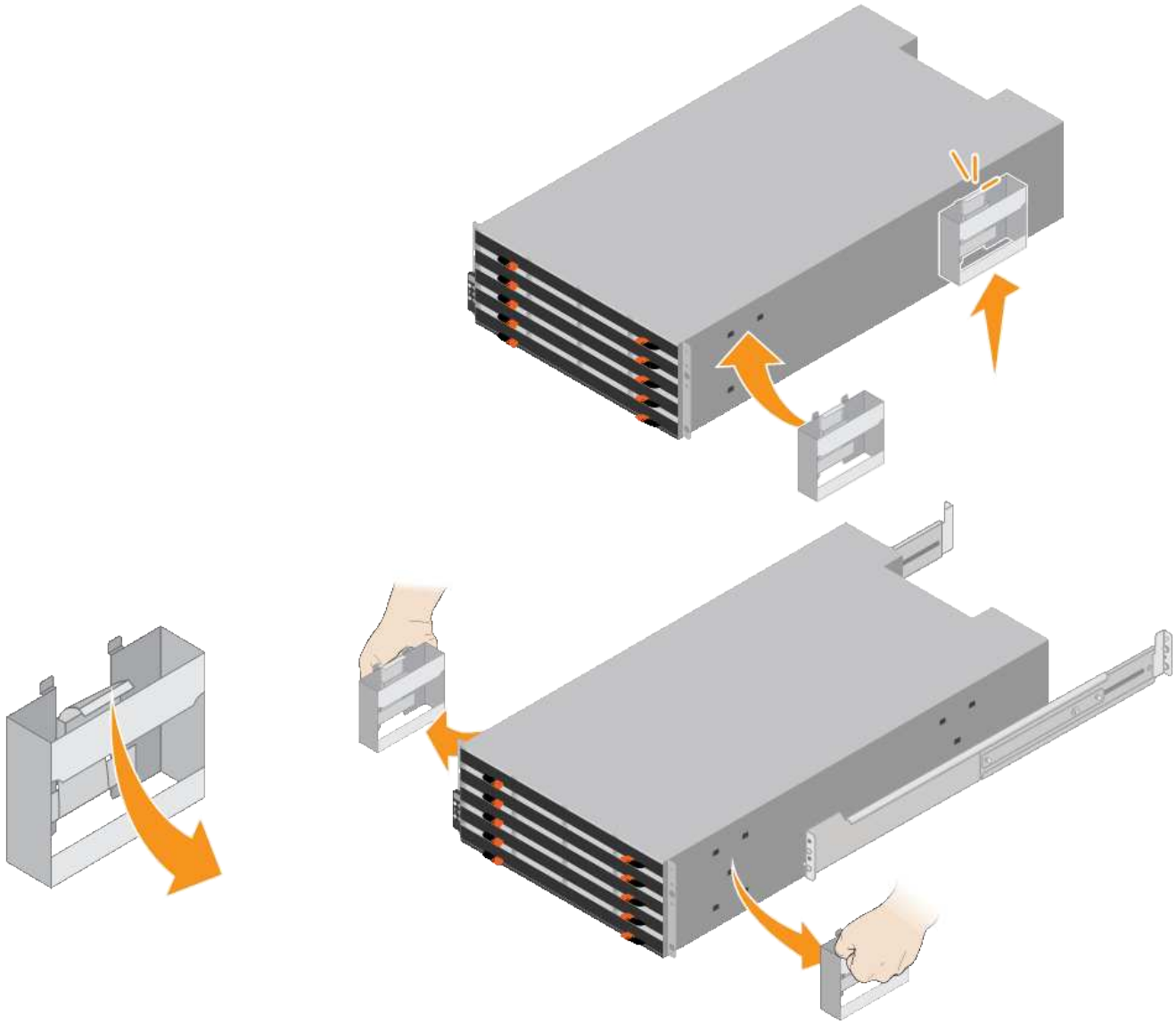
Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.

   Bei quadratischen Lochschränken müssen Sie zuerst die mitgelieferten Käfigmuttern einbauen, um die Vorder- und Rückseite des Regals mit Schrauben zu befestigen.

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.

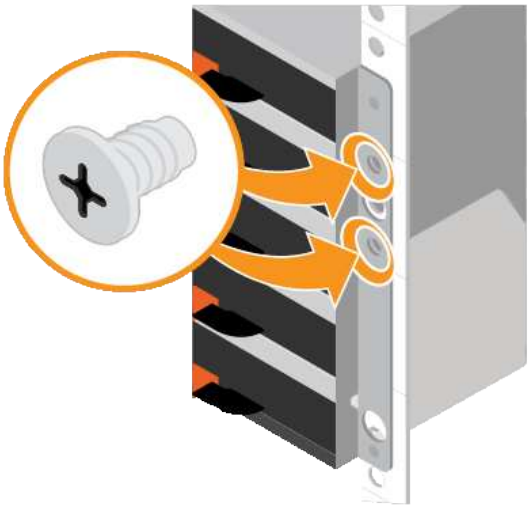
   Um die Griffe zu entfernen, ziehen Sie den Entriegelungshebel nach unten und ziehen Sie dann aus dem Shelf heraus.

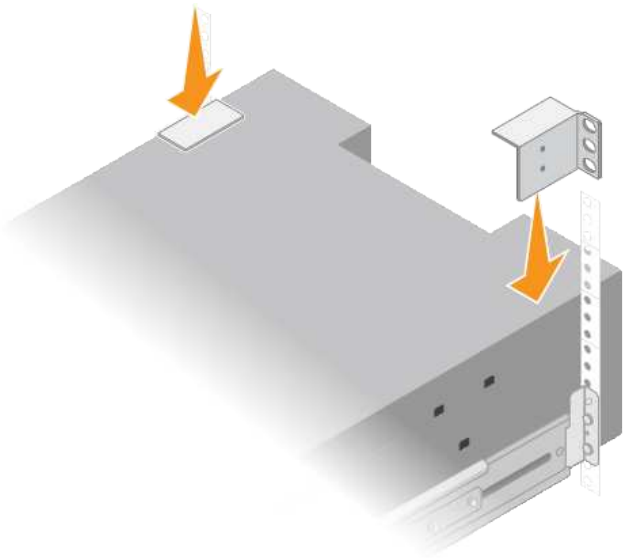
6. Befestigen Sie das Regal an der Vorderseite des Schranks.

   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.

SG6060: Installieren der Laufwerke

Nach der Installation des Shelf für 60 Laufwerke in einem Rack oder Rack müssen alle 60 Laufwerke im Shelf installiert werden. 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.

Was Sie benötigen

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 Shelfs müssen alle Laufwerke entfernt werden.

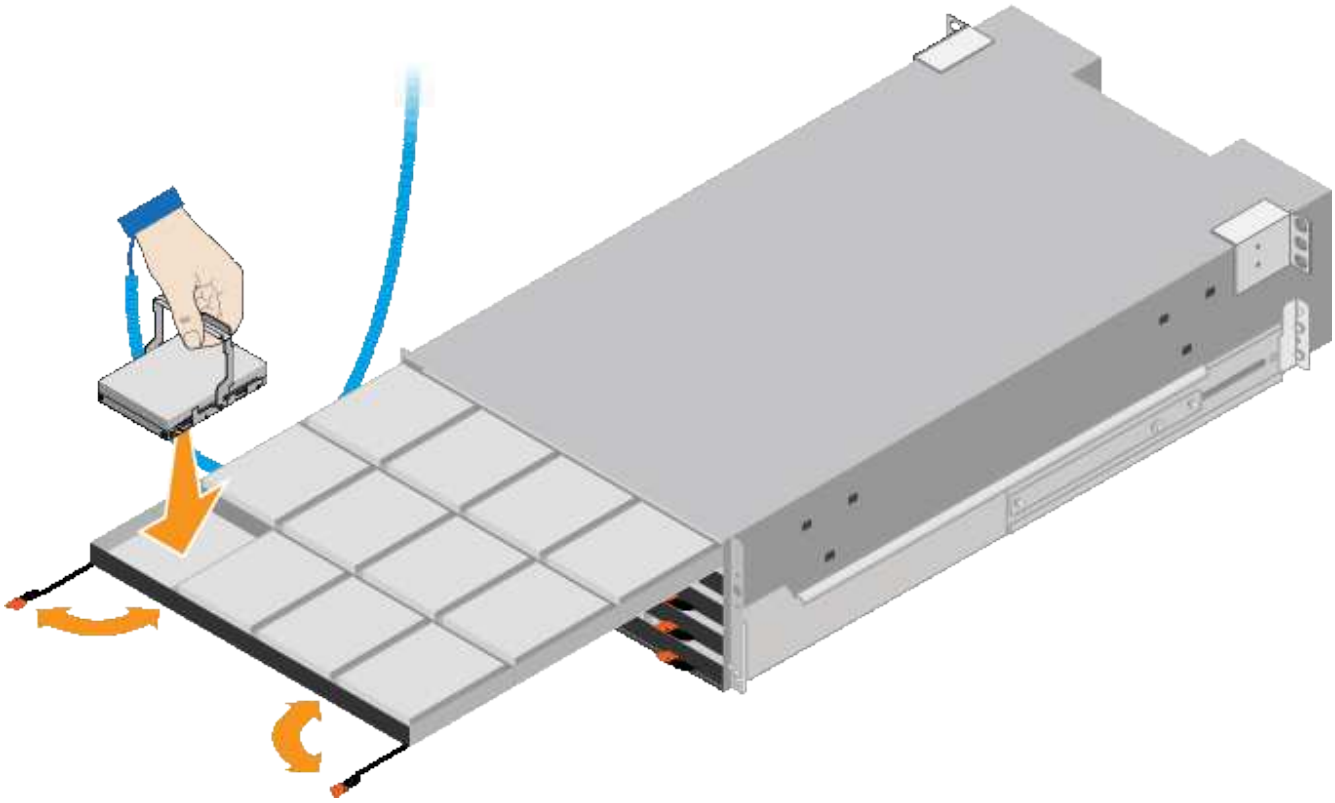
Schritte

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.

SGF6024: Installieren von Shelfs mit 24 Laufwerken in einem Rack oder Schrank

Sie müssen einen Satz Schienen für das EF570 Controller-Shelf in Ihrem Schrank oder Rack installieren und dann das Array auf die Schienen schieben.

Was Sie benötigen

- 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 quadratischen Lochschränken müssen Sie zuerst die mitgelieferten Käfigmuttern einbauen, um die Vorder- und Rückseite des Regals mit Schrauben zu befestigen.

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). Zwei Personen sind erforderlich, um das Gehäuse sicher zu bewegen.

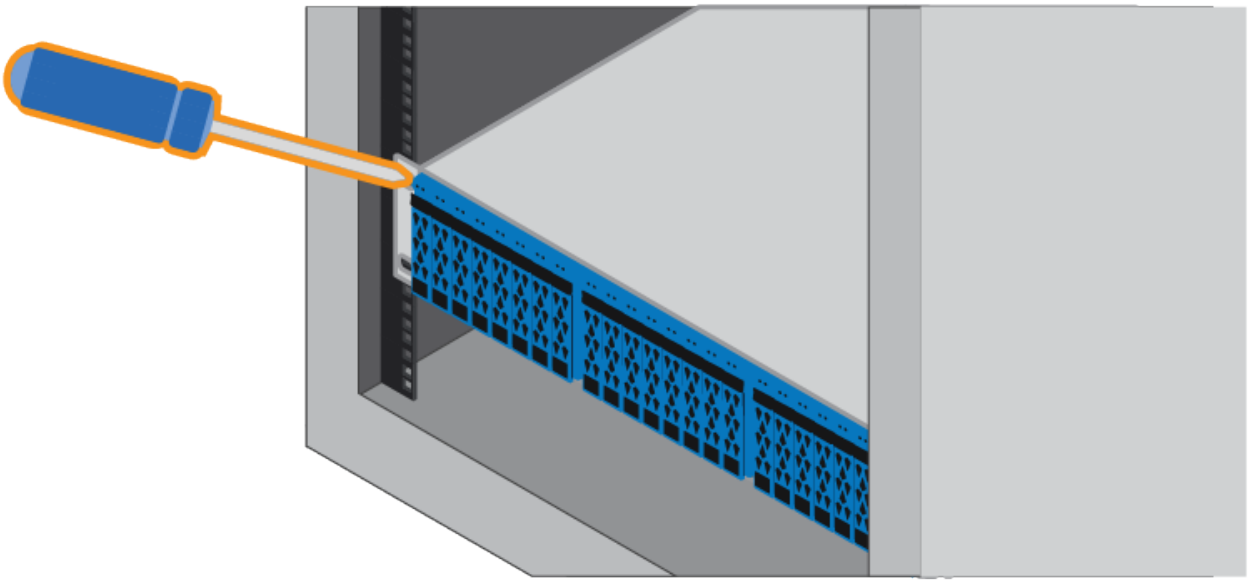
4. Schieben Sie das Gehäuse vorsichtig ganz auf die Schienen.

   Möglicherweise müssen Sie die Schienen anpassen, um sicherzustellen, dass das Gehäuse den ganzen Weg auf die Schienen führt.

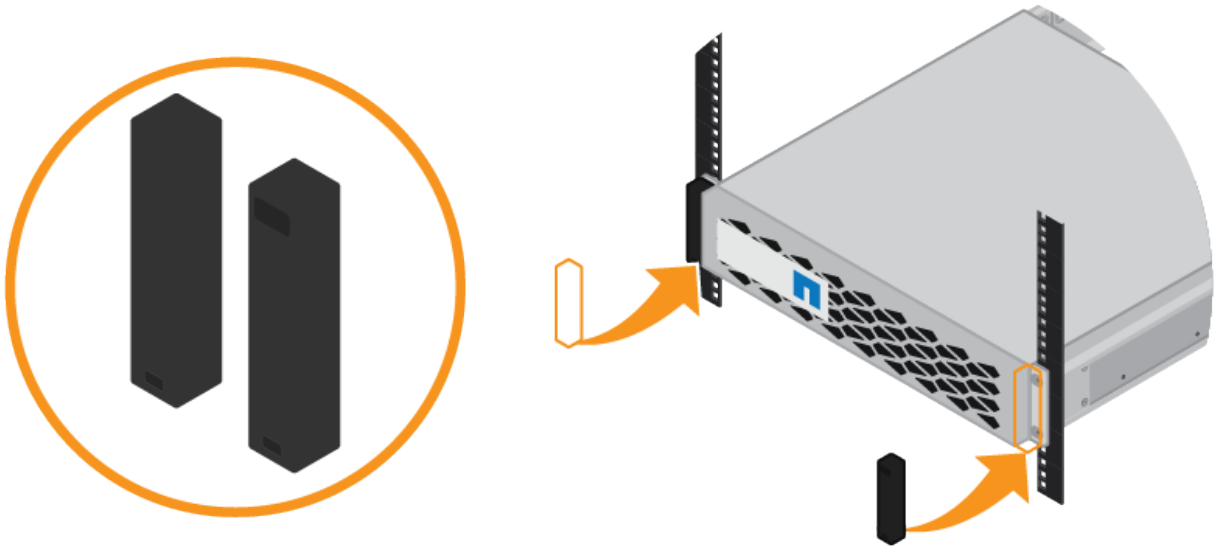
   Setzen Sie nach der Installation des Gehäuses keine zusätzlichen Geräte auf die Schienen. Die Schienen sind nicht für zusätzliches Gewicht ausgelegt.

   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.



SG6000-CN: Einbau in einen Schrank oder Rack

Sie müssen einen Satz Schienen für den SG6000-CN-Controller in Ihrem Schrank oder Rack installieren und dann den Controller auf die Schienen schieben.

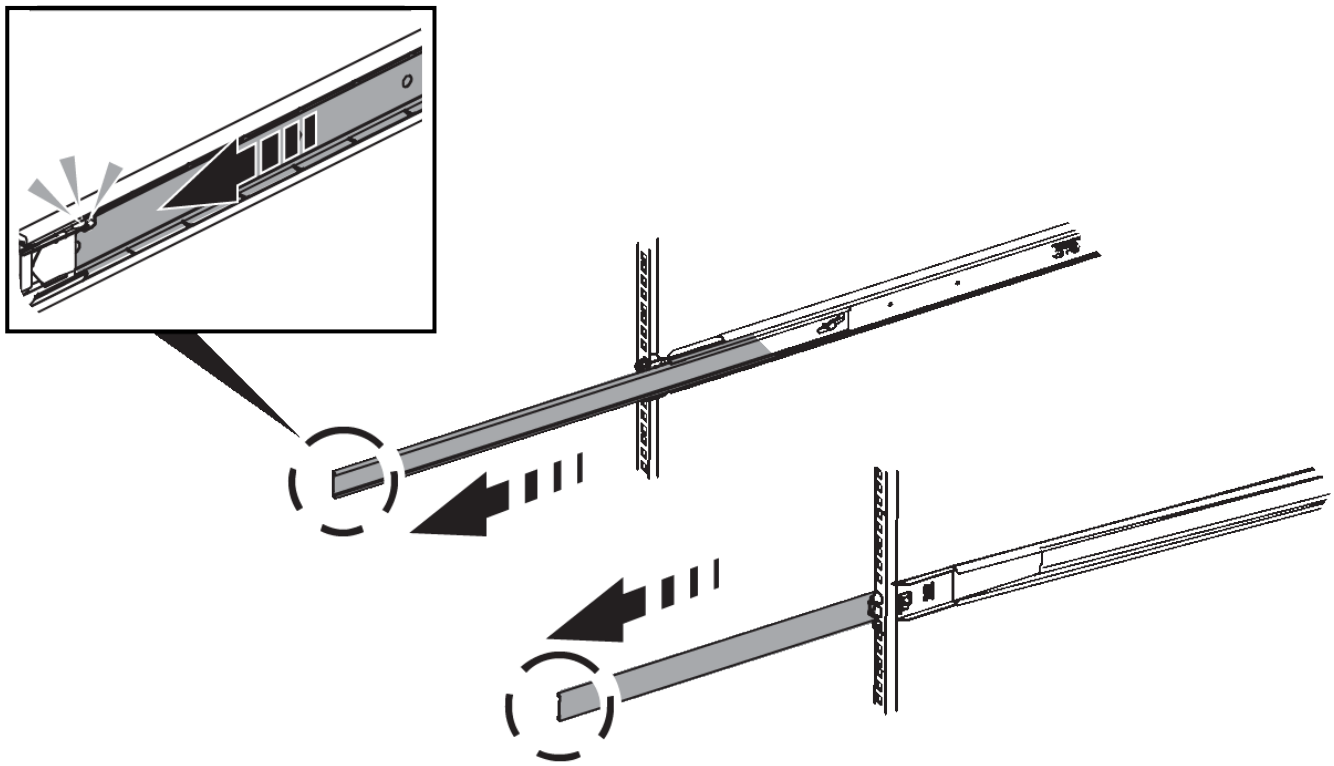
Was Sie benötigen

- 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.

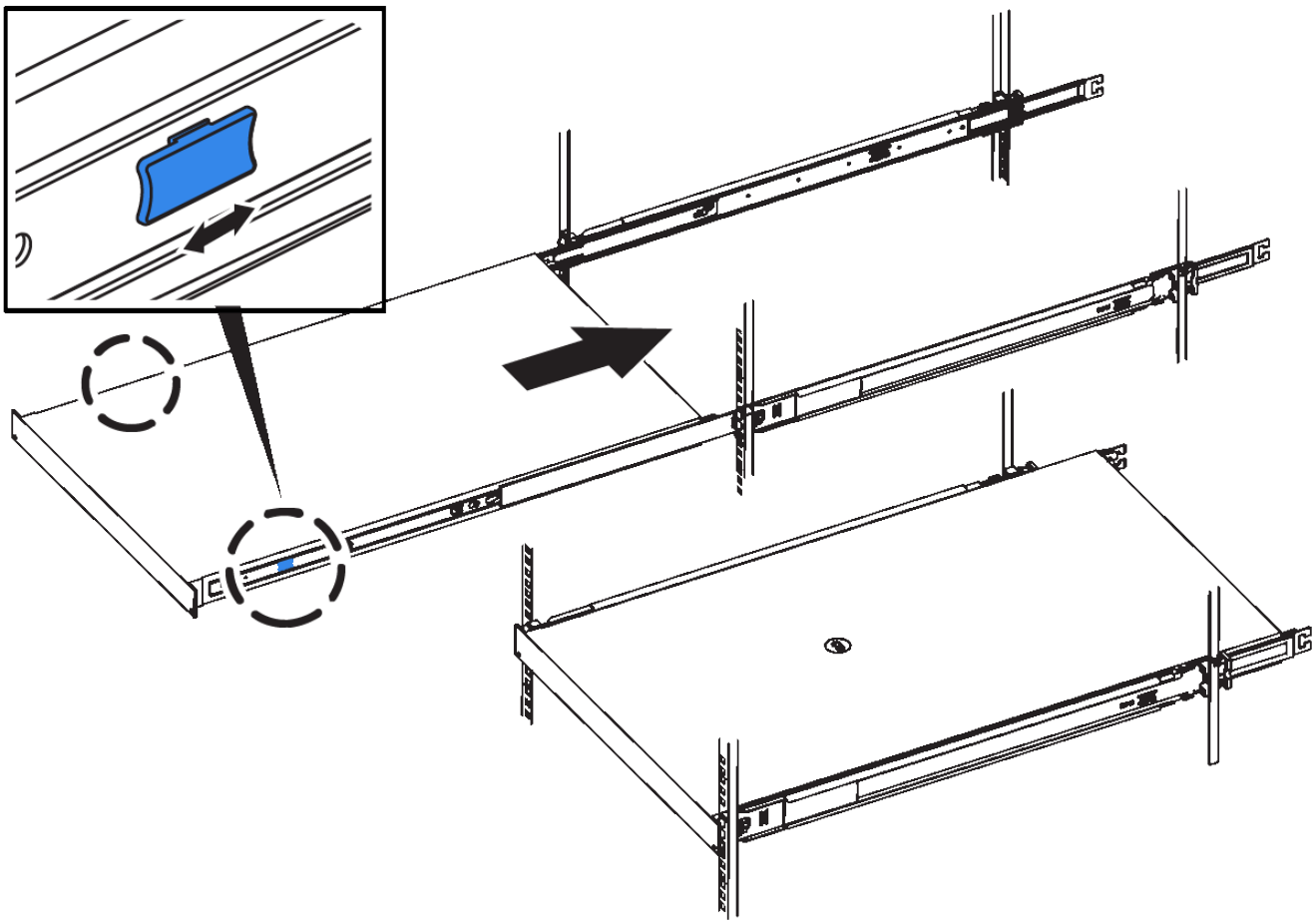
Schritte

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 mehr bewegen können, ziehen Sie die blauen Verriegelungen auf beiden Seiten des Chassis, um den Controller nach innen zu schieben.



Befestigen Sie die Frontverkleidung erst, wenn Sie den Controller eingeschaltet haben.

5. Ziehen Sie die unverlierbaren Schrauben an der Vorderseite des Controllers fest, um den Controller im Rack zu befestigen.

Verkabeln des Geräts (SG6000)

Sie müssen die Speicher-Controller mit dem SG6000-CN-Controller verbinden, die Management-Ports auf allen drei Controllern verbinden und die Netzwerkports des SG6000-CN-Controllers mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID verbinden.

Was Sie benötigen

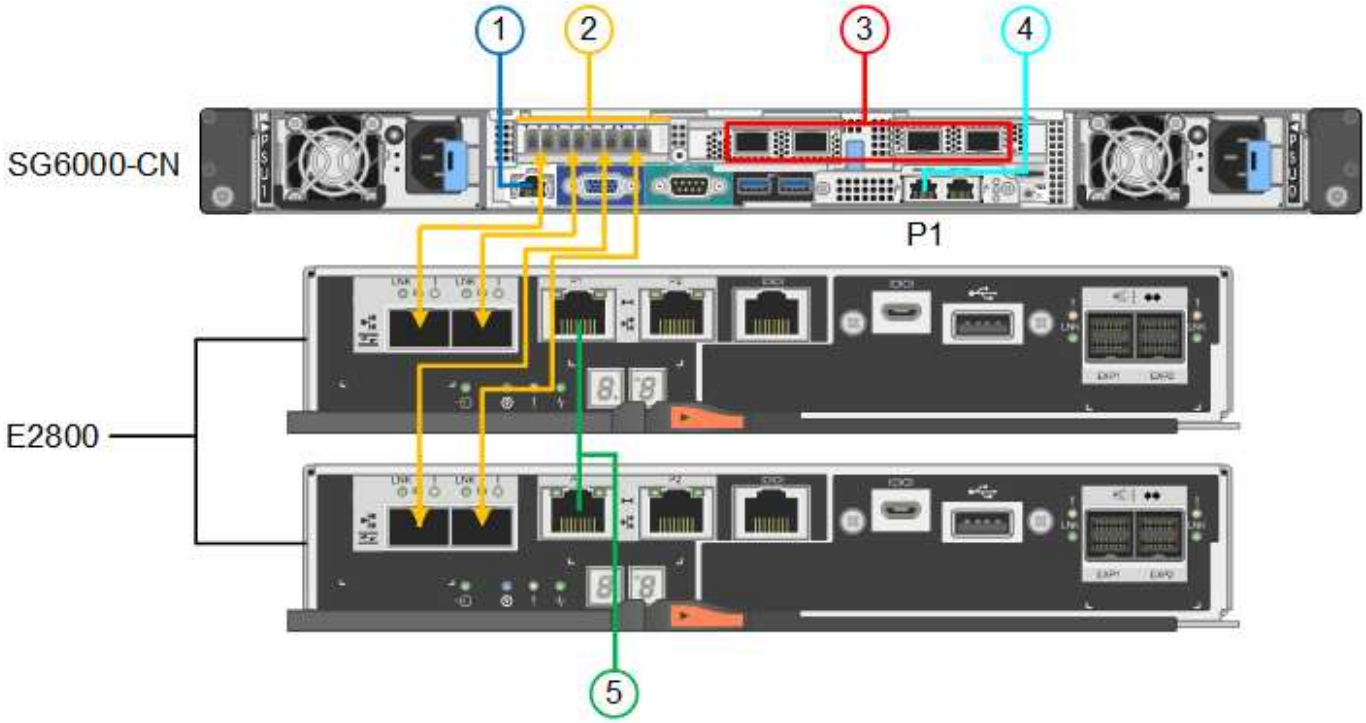
- Das Gerät verfügt über die vier optischen Kabel zum Anschließen der beiden Speicher-Controller an den SG6000-CN-Controller.
- Sie verfügen über RJ-45-Ethernet-Kabel (mindestens vier) für den Anschluss der Management-Ports.
- Sie haben eine der folgenden Optionen für die Netzwerkanschlüsse. Diese Artikel 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.

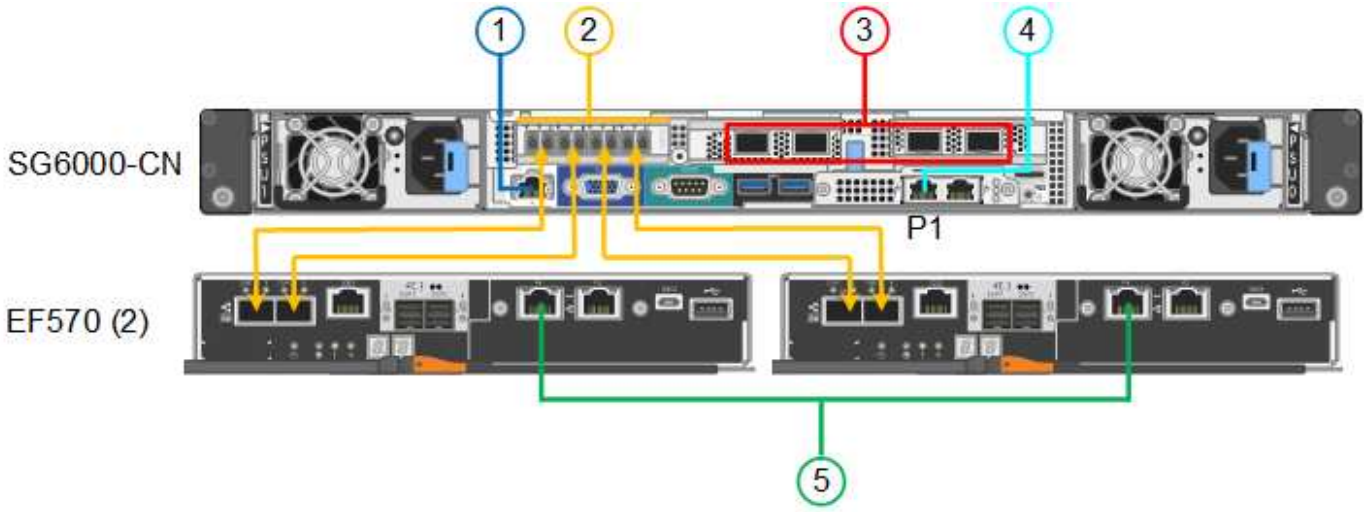
> **Gefahr der Laserstrahlung** — kein Teil eines SFP-Transceivers zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

Über diese Aufgabe

Die folgende Abbildung zeigt die drei Controller in der SG6060 Appliance mit dem SG6000-CN Computing Controller oben und den beiden E2800 Storage Controllern unten.



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.



	Port	Typ des Ports	Funktion
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.
2	FC-Verbindungs-Ports: • 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 auf 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.
4	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.	• 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). • Während der Installation kann der SG6000-CN-Controller mit einem Service-Laptop verbunden werden, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.

	Port	Typ des Ports	Funktion
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.
5	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. Verbinden Sie den Management-Port 1 (P1) auf jedem Storage Controller (der RJ-45 Port auf der linken Seite) mit dem Managementnetzwerk für SANtricity System Manager über ein Ethernet-Kabel.

Verwenden Sie keinen Management-Port 2 (P2) auf den Storage Controllern (RJ-45-Port auf der rechten Seite). Dieser Port ist für technischen Support reserviert.

Verwandte Informationen

"Port Bond-Modi für den SG6000-CN-Controller"

"Installieren Sie den SG6000-CN Controller wieder in ein Gehäuse oder Rack"

SG6060: Verkabelung der optionalen Erweiterungs-Shelfs

Wenn Sie Erweiterungs-Shelfs verwenden, müssen Sie sie mit dem E2860 Controller-Shelf verbinden. Es können maximal zwei Erweiterungs-Shelfs für jede SG6060 Appliance verwendet werden.

Was Sie benötigen

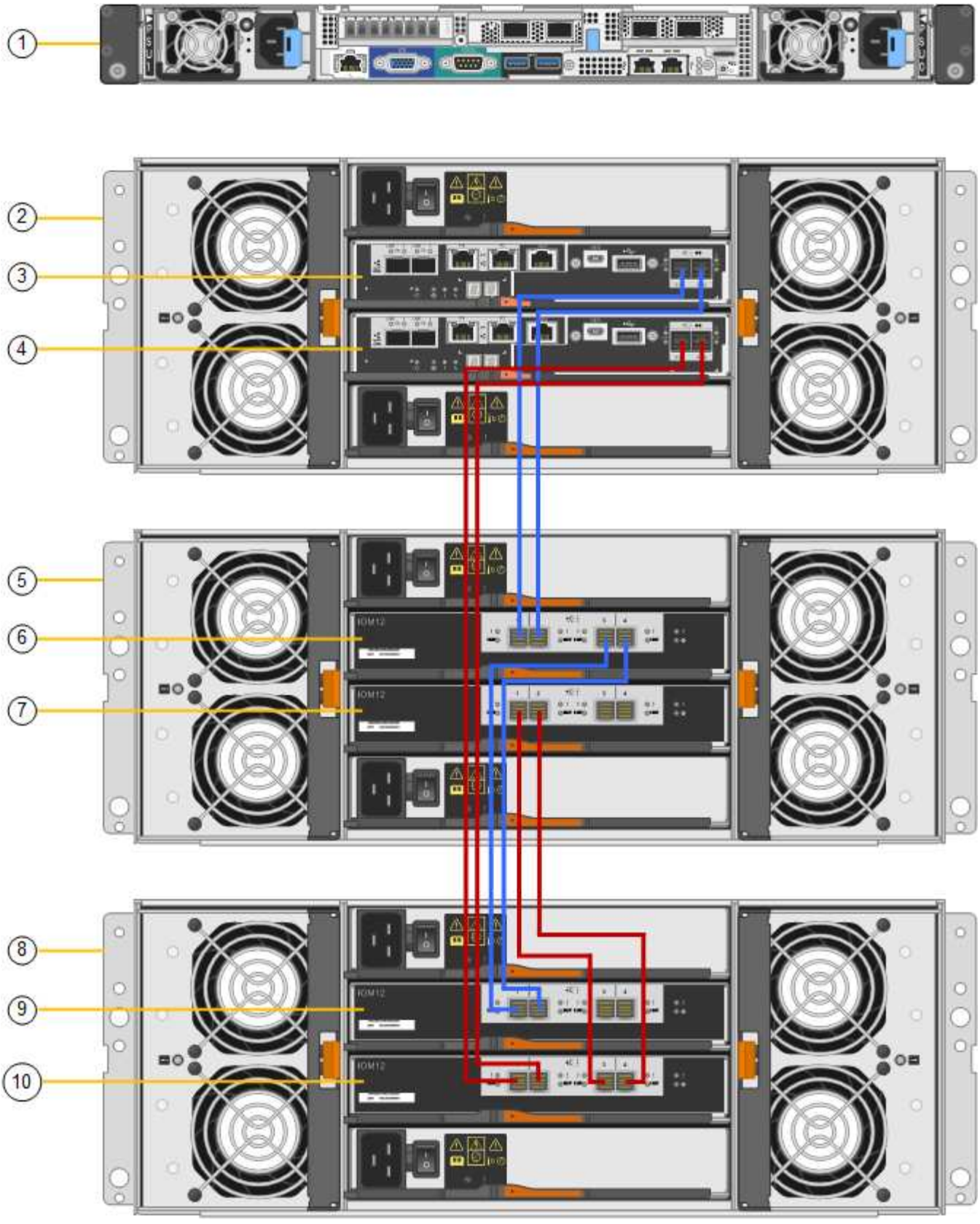
- Sie haben die beiden SAS-Kabel mit jedem Erweiterungs-Shelf geliefert.
- Sie haben die Erweiterungs-Shelfs im Rack oder Rack mit dem E2860 Controller-Shelf installiert.

  "SG6060: Installieren von Shelfs mit 60 Laufwerken in einem Schrank oder Rack"

Schritt

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



	Beschreibung
1	SG6000-CN

	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

Anschließen von Netzkabeln und Anwenden der Stromversorgung (SG6000)

Nach dem Anschließen der Netzwerkkabel 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 Einschaltvorgangs 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 Einschaltvorgangs 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 am SG6000-CN Controller.

Verwandte Informationen

"Anzeigen von Boot-Statuscodes für die SG6000-Speicher-Controller"

"Anzeigen von Statusanzeigen und -Tasten auf dem SG6000-CN-Controller"

"Installieren Sie den SG6000-CN Controller wieder in ein Gehäuse oder Rack"

Anzeigen von Statusanzeigen und -Tasten auf dem SG6000-CN-Controller

Der SG6000-CN-Controller enthält Anzeigen, mit denen Sie den Status des Controllers bestimmen können, einschließlich der folgenden Anzeigen und Schaltflächen.

	Anzeige	Beschreibung
1	Ein-/aus-Schalter	• Blau: Der Controller ist eingeschaltet. • Aus: Der Controller ist ausgeschaltet.
2	Reset-Taste	*Kein Indikator* Mit dieser Taste können Sie den Controller auf einen harten Reset zurücksetzen.

	Anzeige	Beschreibung
3	Schaltfläche „Identifizierung“	• 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	• Gelb: Ein Fehler ist aufgetreten. **Hinweis:** um den Start und Fehlercodes anzuzeigen, müssen Sie auf die BMC-Schnittstelle zugreifen. • 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.

   Um die Boot- und Fehlercodes anzuzeigen, müssen Sie auf die BMC-Schnittstelle zugreifen.

Verwandte Informationen

"Fehlerbehebung bei der Hardwareinstallation"

"Konfigurieren der BMC-Schnittstelle"

"Einschalten des SG6000-CN Controllers und Überprüfen des Betriebs"

Anzeigen von Boot-Statuscodes für die 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.

Über diese Aufgabe

Beschreibungen dieser Codes finden Sie in den Informationen zur Systemüberwachung der E-Series für Ihren Storage Controller-Typ.

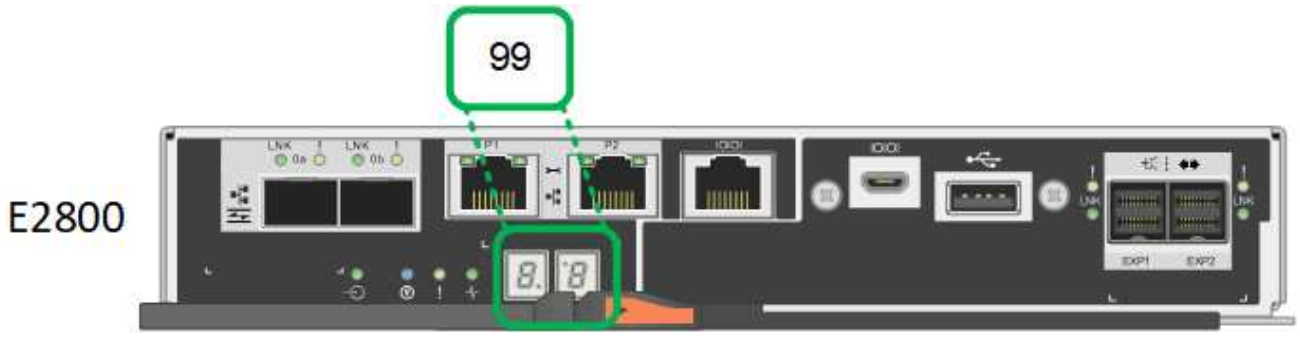
Schritte

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 oder beide Controller andere Werte anzeigen, lesen Sie die Informationen zur Fehlerbehebung bei der Hardware-Installation, 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

"E5700 und E2800 – System Monitoring Guide"

"Fehlerbehebung bei der Hardwareinstallation"

"NetApp Support"

"Einschalten des SG6000-CN Controllers und Überprüfen des Betriebs"

Konfigurieren der Hardware

Nach dem Einschalten der Appliance müssen Sie die Netzwerkverbindungen konfigurieren, die von StorageGRID verwendet werden sollen. Sie müssen SANtricity System Manager konfigurieren. Dies ist die Software, mit der Sie die Storage Controller und andere Hardware im Controller-Shelf überwachen. Sie müssen außerdem sicherstellen, dass Sie auf die BMC-Schnittstelle für den SG6000-CN-Controller zugreifen können.

Schritte

- "Konfigurieren von StorageGRID-Verbindungen"
- "Zugriff auf und Konfigurieren von SANtricity System Manager"
- "Konfigurieren der BMC-Schnittstelle"
- "Optional: Aktivieren der Node-Verschlüsselung"

- "Optional: Ändern des RAID-Modus (nur SG6000)"
- "Optional: Neu zuordnen von Netzwerkports für die Appliance"

Konfigurieren von StorageGRID-Verbindungen

Bevor Sie eine StorageGRID-Appliance als Speicherknoten in einem StorageGRID-System bereitstellen können, müssen Sie die Verbindungen zwischen der Appliance und den zu verwendenden Netzwerken konfigurieren. Sie können Netzwerke konfigurieren, indem Sie das Installationsprogramm der StorageGRID-Appliance durchsuchen, das auf dem SG6000-CN-Controller (dem Compute-Controller) vorinstalliert ist.

Schritte

- "Zugriff auf das Installationsprogramm der StorageGRID-Appliance"
- "Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance"
- "Konfigurieren von Netzwerkverbindungen (SG6000)"
- "StorageGRID-IP-Adressen werden konfiguriert"
- "Netzwerkverbindungen werden überprüft"
- "Überprüfen von Netzwerkverbindungen auf Portebene"

Zugriff auf das Installationsprogramm der StorageGRID-Appliance

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).

Was Sie benötigen

- 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.
- Der SG6000-CN-Controller ist mit allen StorageGRID-Netzwerken verbunden, die Sie verwenden möchten.
- Sie kennen die IP-Adresse, das Gateway und das Subnetz für den SG6000-CN-Controller in diesen Netzwerken.
- Sie haben die geplanten Netzwerk-Switches konfiguriert.

Über diese Aufgabe

Um zunächst auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, können Sie die über DHCP zugewiesene IP-Adresse für den Admin-Netzwerkport auf dem SG6000-CN-Controller verwenden (vorausgesetzt, der Controller ist mit dem Admin-Netzwerk verbunden). Alternativ können Sie einen Service-Laptop direkt mit dem SG6000-CN-Controller verbinden.

Schritte

1. Wenn möglich, verwenden Sie die DHCP-Adresse für den Netzwerkanschluss des Administrators am SG6000-CN-Controller, um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen.

a. Suchen Sie das MAC-Adressenetikett auf der Vorderseite des SG6000-CN-Controllers und legen Sie die MAC-Adresse für den Admin-Netzwerkanschluss fest.

   Auf dem MAC-Adressenetikett wird die MAC-Adresse für den BMC-Verwaltungsport aufgelistet.

   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.

b. Geben Sie die MAC-Adresse an Ihren Netzwerkadministrator an, damit er die DHCP-Adresse für die Appliance im Admin-Netzwerk nachsuchen kann.

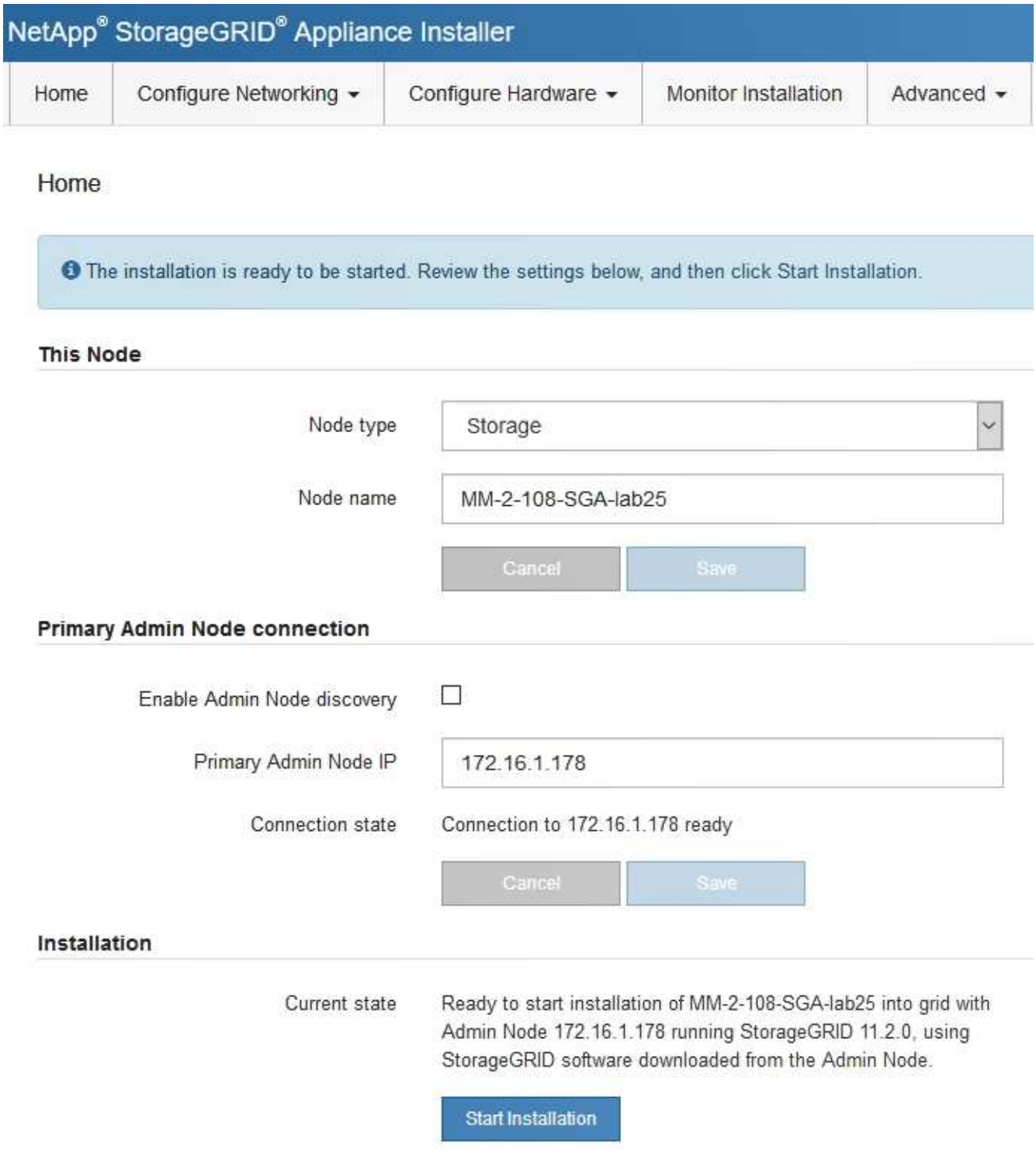
c. Geben Sie auf dem Client diese URL für den StorageGRID-Appliance-Installer ein:
   `https://Appliance_Controller_IP:8443`

   Für *`SG6000-CN_Controller_IP`*, Verwenden Sie die DHCP-Adresse.

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.



2. Wenn Sie keine IP-Adresse über DHCP erhalten können, können Sie eine Link-lokale Verbindung verwenden.

   a. Schließen Sie einen Service-Laptop mithilfe eines Ethernet-Kabels direkt an den rechtesten RJ-45-Anschluss des SG6000-CN Controllers an.

b. Öffnen Sie einen Webbrowser auf dem Service-Laptop.

c. 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 das Gerät aktuell verbunden ist.

> Wenn Sie über eine lokale 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.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

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.

Was Sie benötigen

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 das StorageGRID-Appliance-Installationsprogramm 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 im Grid Manager **Hilfe** > **Info**).

Die zweite Ziffer in den beiden Versionen sollte übereinstimmen. Wenn auf Ihrem StorageGRID-System beispielsweise die Version 11.**5**.*x.y* ausgeführt wird, sollte die StorageGRID Appliance Installer-Version 3.**5**.*z* sein.

3. Wenn die Appliance über eine übergeordnete Version des Installationsprogramms für StorageGRID Appliances verfügt, wechseln Sie zur Seite NetApp Downloads für StorageGRID.

   "NetApp Downloads: StorageGRID"

   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 Datei Support für StorageGRID Appliances ist eine `.zip` Archiv, das die aktuellen und vorherigen Firmware-Versionen für alle StorageGRID Appliance-Modelle enthält, in Unterverzeichnissen für jeden Controller-Typ.

   Nach dem Herunterladen der Datei Support für StorageGRID Appliances extrahieren Sie den `.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 des Installationsprogramms für StorageGRID-Geräte, um die folgenden Schritte auszuführen:
   a. Laden Sie die entsprechende Support-Datei (Firmware-Image) für den Controller-Typ und die Prüfsummendatei hoch.
   b. Aktualisieren Sie die inaktive Partition.
   c. Starten Sie neu und tauschen Sie die Partitionen aus.
   d. Aktualisieren Sie die zweite Partition.

Verwandte Informationen

"Zugriff auf das Installationsprogramm der StorageGRID-Appliance"

Konfigurieren von Netzwerkverbindungen (SG6000)

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.

Was Sie benötigen

Wenn Sie einen Appliance-Node klonen, konfigurieren Sie für alle vom Node der Quell-Appliance verwendeten Links für die Ziel-Appliance.

Wenn Sie die 25-GbE-Verbindungsgeschwindigkeit verwenden möchten:

- Sie verwenden SFP28 Twinax-Kabel, oder Sie haben SFP28-Transceiver in den Netzwerkports installiert, die Sie verwenden möchten.
- Sie haben die Netzwerk-Ports mit Switches verbunden, die diese Funktionen unterstützen.

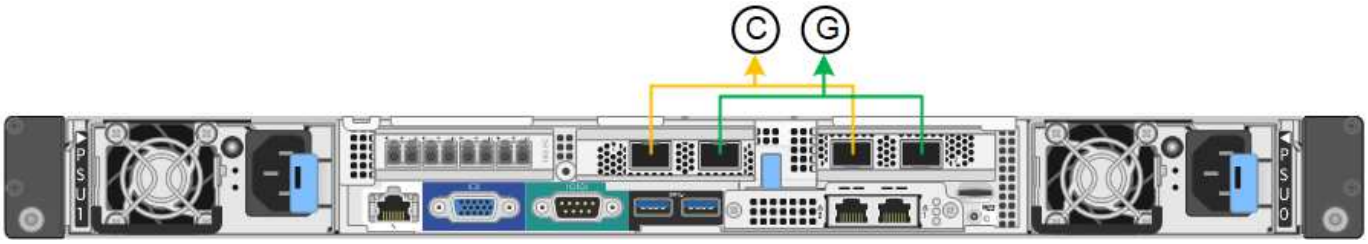
- Sie verstehen, wie Sie die Switches konfigurieren, um diese höhere Geschwindigkeit zu verwenden.

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

Diese Abbildung zeigt, wie die vier Netzwerk-Ports im Bond-Modus mit festen Ports verbunden sind (Standardkonfiguration).



	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.

Die Abbildung zeigt, wie die vier Netzwerk-Ports im Bond-Modus für aggregierte Ports verbunden sind.

	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. Die Standardeinstellungen werden fett dargestellt. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standardeinstellung verwenden möchten.

- **Festes (Standard) Port Bond-Modus**

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Active-Backup (Standard)	• 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.	• 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)	• 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.	• 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.

- * Aggregat-Port-Bond-Modus*

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad	• Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. • Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete.	• 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.

Weitere Informationen zu Port Bond- und Netzwerk-Bond-Modi finden Sie unter „`Network Port Connections for the SG6000-CN Controller`“.

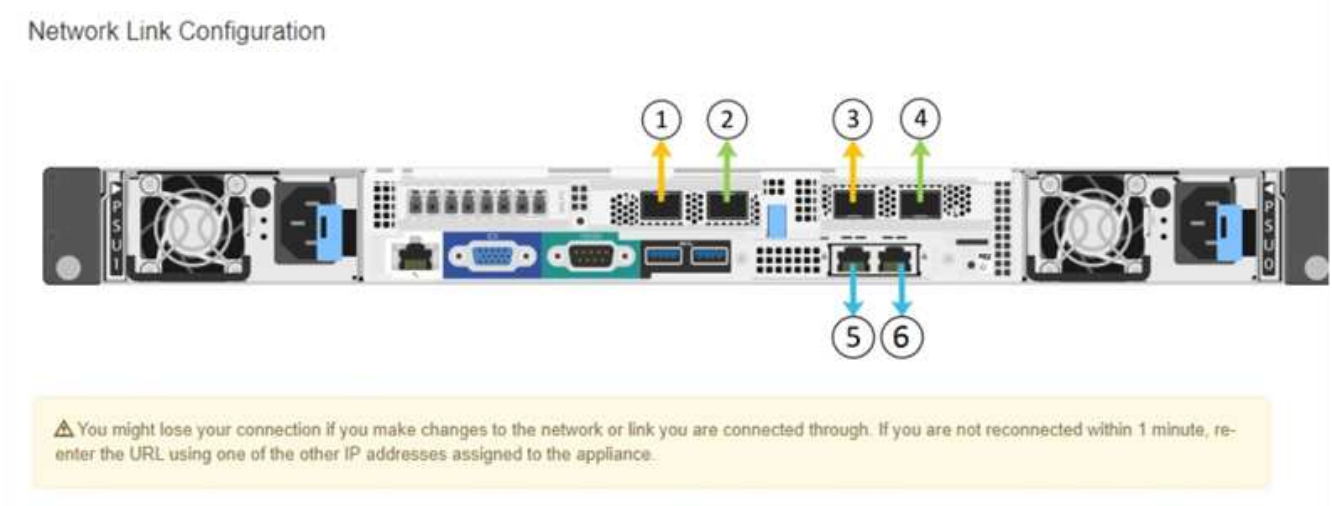
Diese Abbildung zeigt, wie die beiden 1-GbE-Management-Ports des SG6000-CN-Controllers im Active-Backup-Netzwerk-Bond-Modus des Admin-Netzwerks verbunden sind.

Schritte

1. Klicken Sie im Installationsprogramm der StorageGRID-Appliance 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.



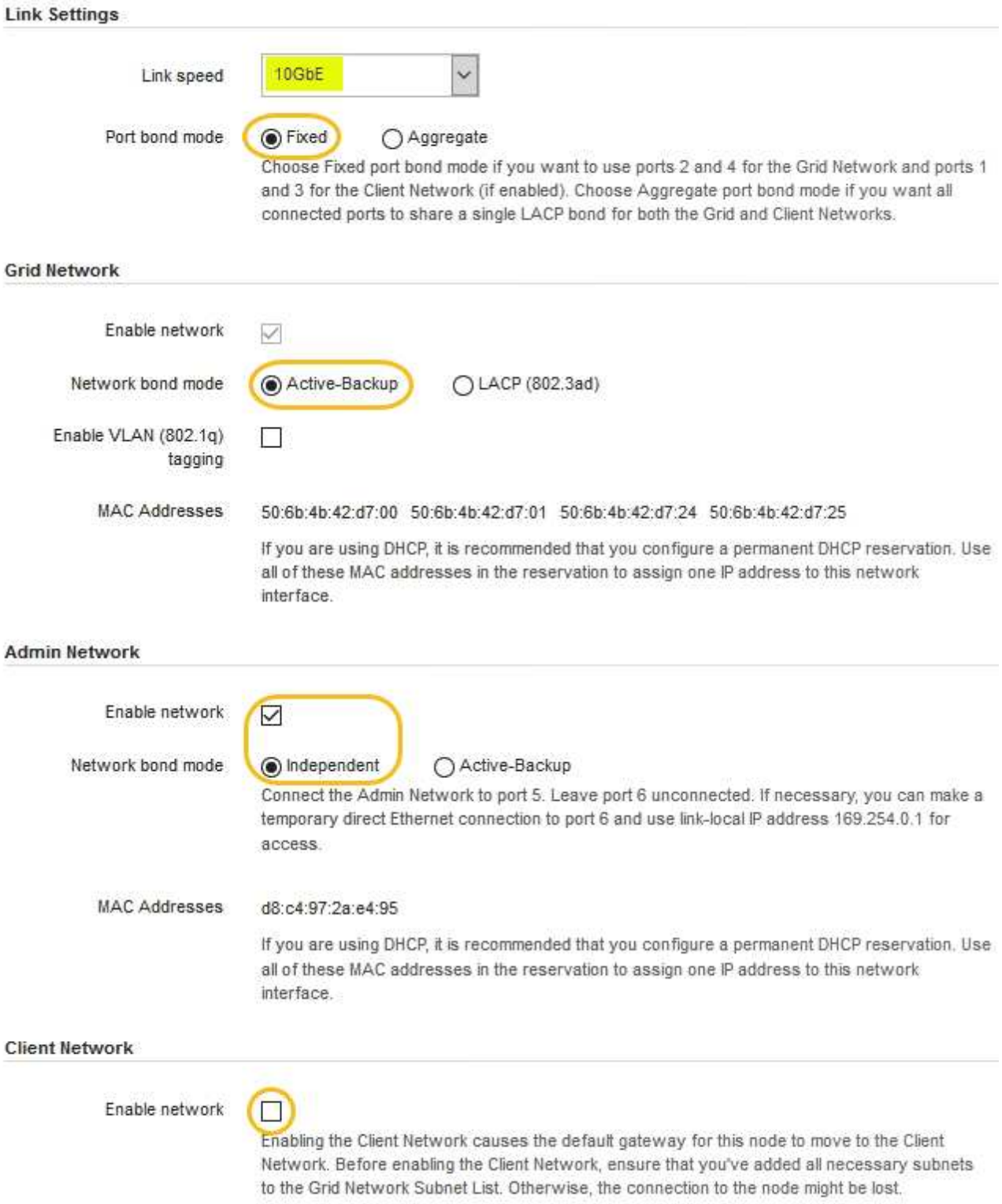
In der Tabelle „Link-Status“ werden der Verbindungsstatus (nach oben/unten) und die Geschwindigkeit (1/10/25/40/100 Gbit/s) der nummerierten Ports aufgeführt.

Link Status

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

Das erste Mal, wenn Sie diese Seite aufrufen:

- **Link Speed** ist auf **10GbE** 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.



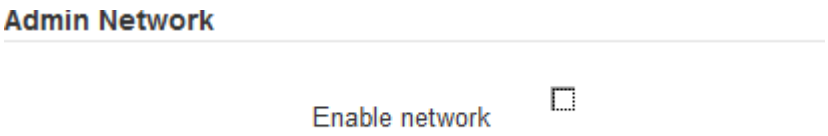
2. Wenn Sie die 25-GbE-Verbindungsgeschwindigkeit für die Netzwerkanschlüsse verwenden möchten, wählen Sie in der Dropdown-Liste Link Speed * 25 GbE aus.

   Die Netzwerk-Switches, die Sie für das Grid-Netzwerk und das Client-Netzwerk verwenden, müssen ebenfalls für diese Geschwindigkeit konfiguriert sein. Sie müssen SFP28 Twinax-Kabel oder optische Kabel und SFP28-Transceiver verwenden.

3. Aktivieren oder deaktivieren Sie die StorageGRID-Netzwerke, die Sie verwenden möchten.

Das Grid-Netzwerk ist erforderlich. Sie können dieses Netzwerk nicht deaktivieren.

a. Wenn das Gerät nicht mit dem Admin-Netzwerk verbunden ist, deaktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Admin-Netzwerk.



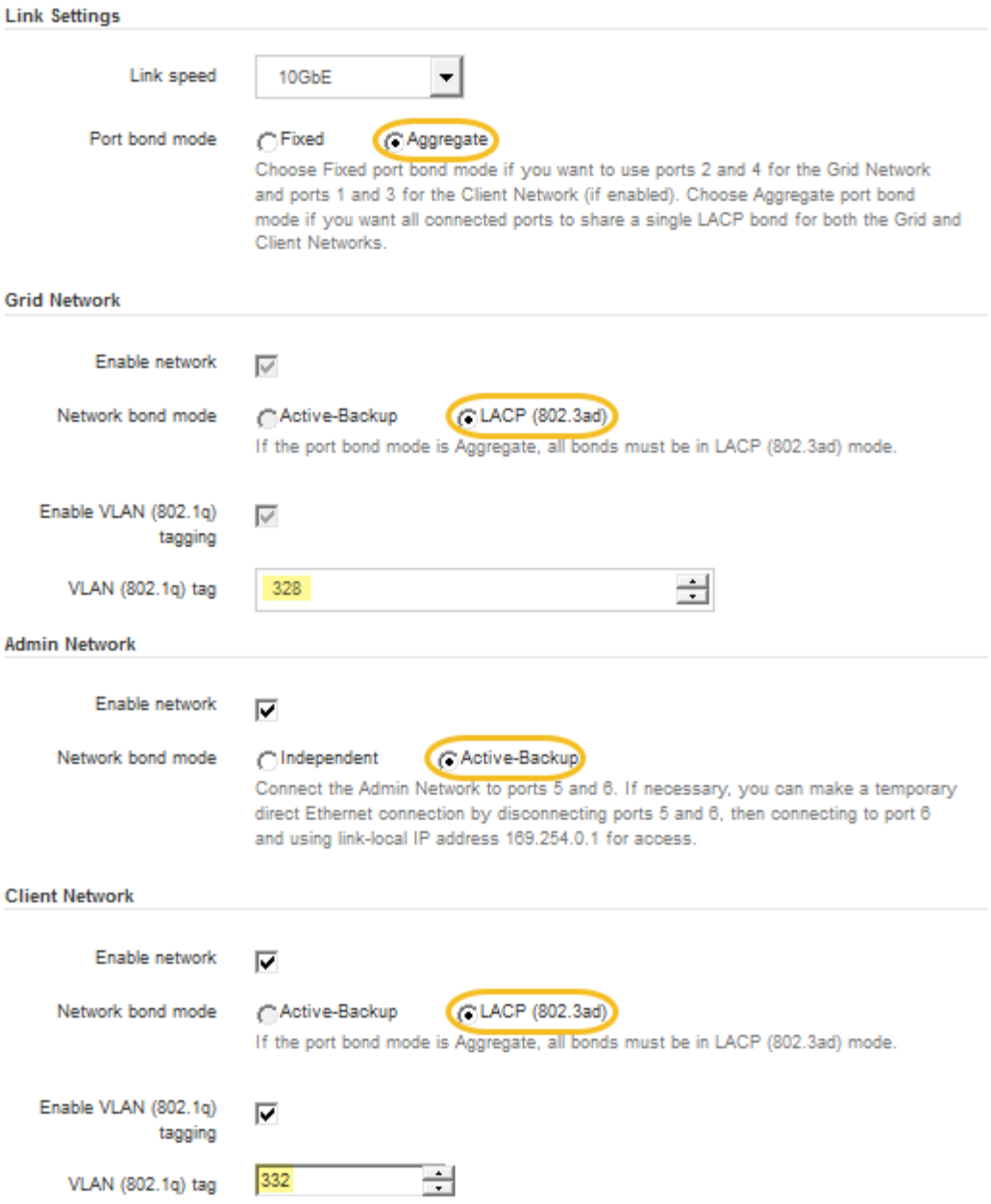
b. Wenn das Gerät mit dem Client-Netzwerk verbunden ist, aktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Client-Netzwerk.

   Die Client-Netzwerkeinstellungen für die Netzwerkanschlüsse werden jetzt 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.



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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:
> `https://SG6000-CN_Controller_IP:8443`

Verwandte Informationen

"Port Bond-Modi für den SG6000-CN-Controller"

"StorageGRID-IP-Adressen werden konfiguriert"

Mit dem Installationsprogramm der StorageGRID-Appliance können Sie die für den Appliance-Speicherknoten verwendeten IP-Adressen und Routing-Informationen im StorageGRID-Raster, Administrator und Client-Netzwerke konfigurieren.

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.

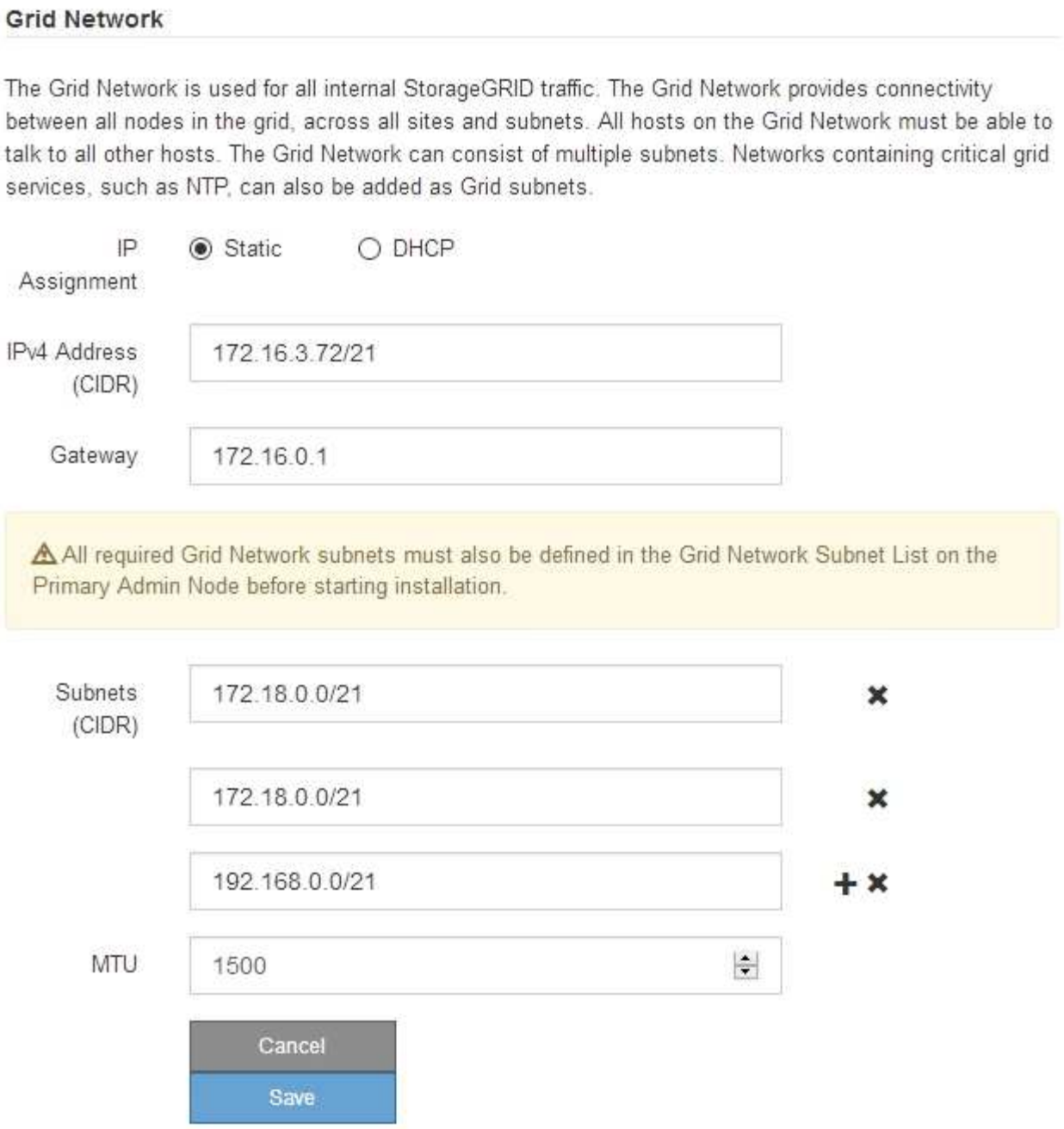
Wenn Sie die Link-Konfiguration ändern möchten, lesen Sie die Anweisungen zum Ändern der Link-Konfiguration des SG6000-CN Controllers.

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 identisch 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://services_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 Löschsymbol ✖.

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.

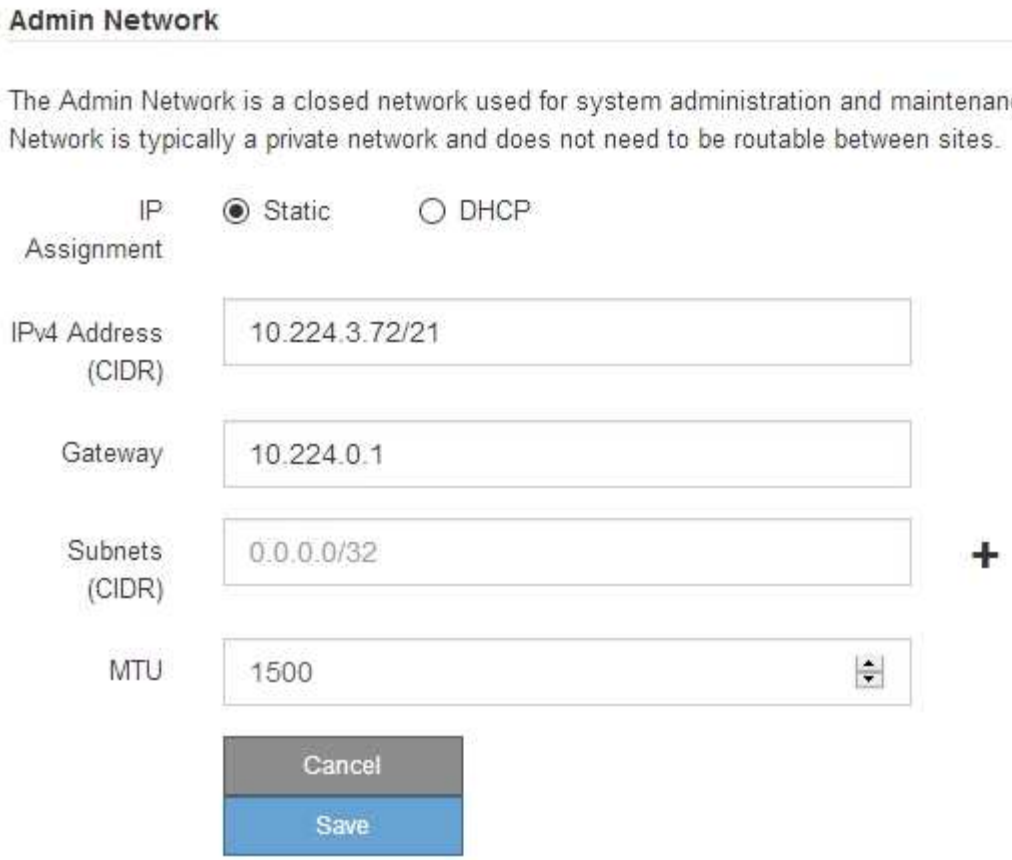
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch 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, müssen Sie das Admin-Netzwerk auf der Seite Link Configuration aktivieren.



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://services_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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

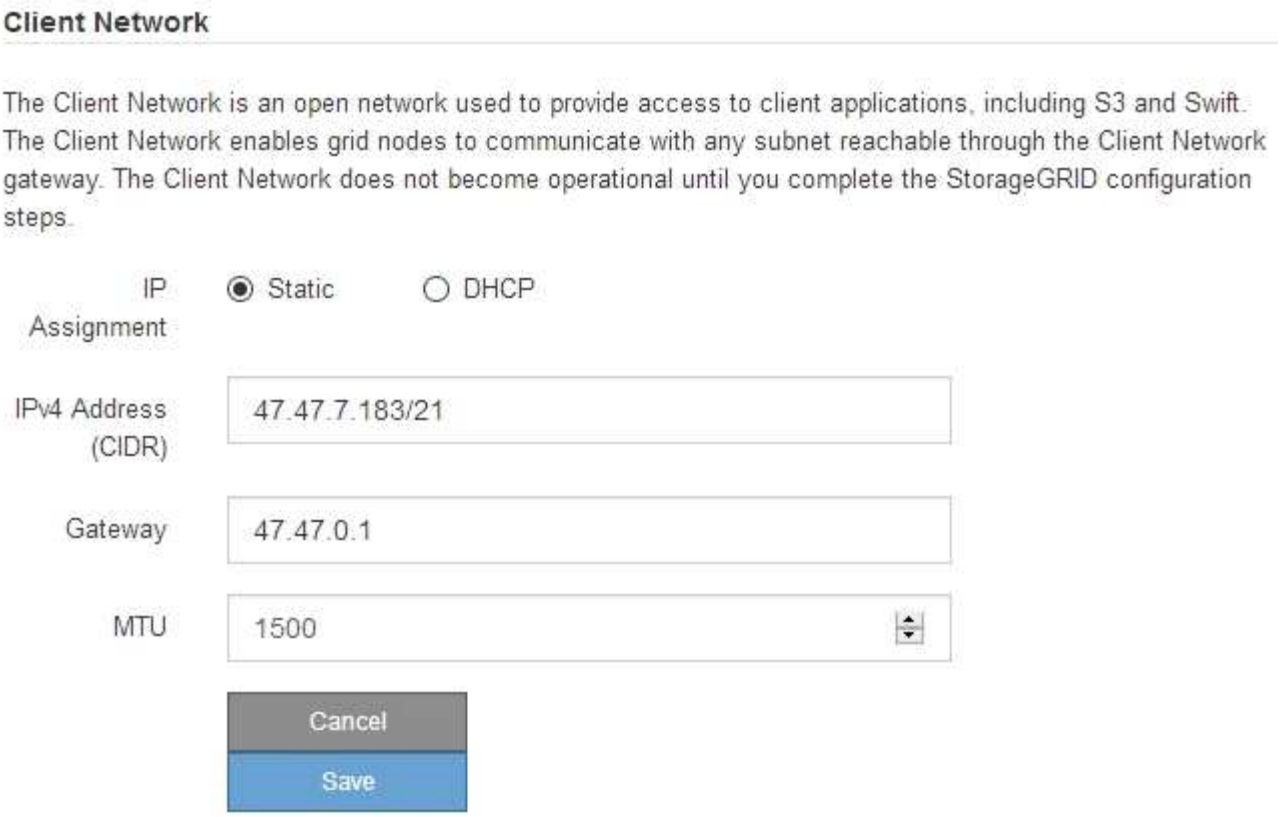
c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.

> 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, müssen Sie das Client-Netzwerk auf der Seite Link Configuration aktivieren.



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.

Verwandte Informationen

"Ändern der Verbindungskonfiguration des SG6000-CN Controllers"

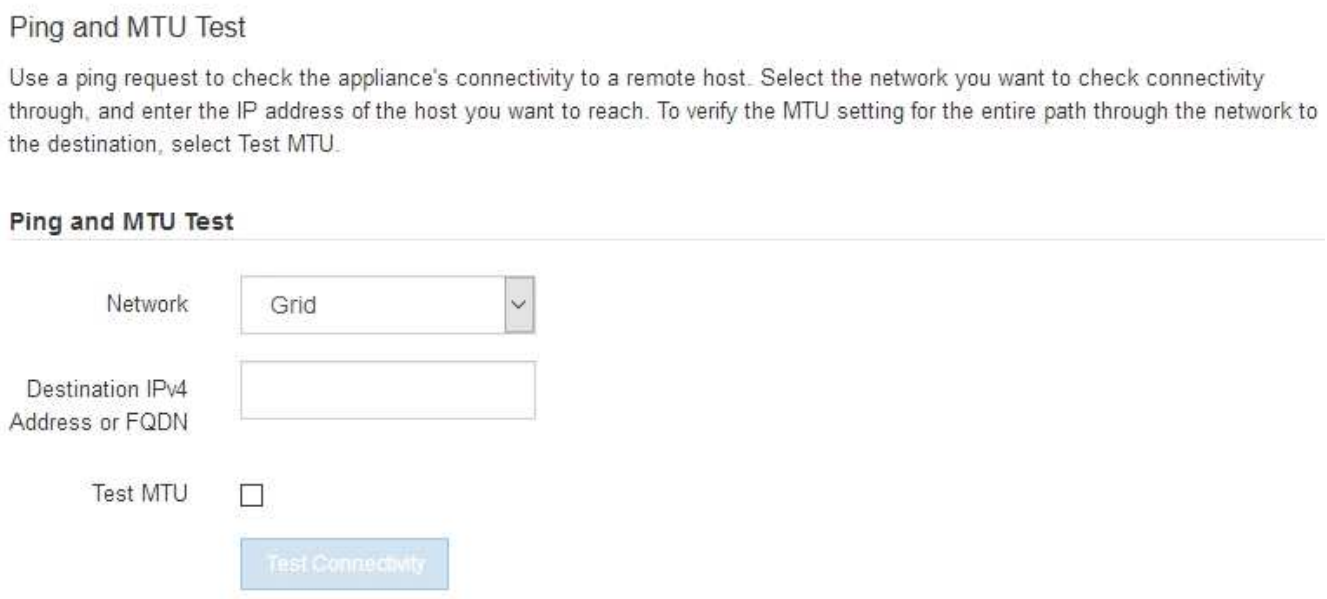
Netzwerkverbindungen werden überprüft

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.



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 Domänennamen (FQDN) für einen Host in diesem Netzwerk ein.

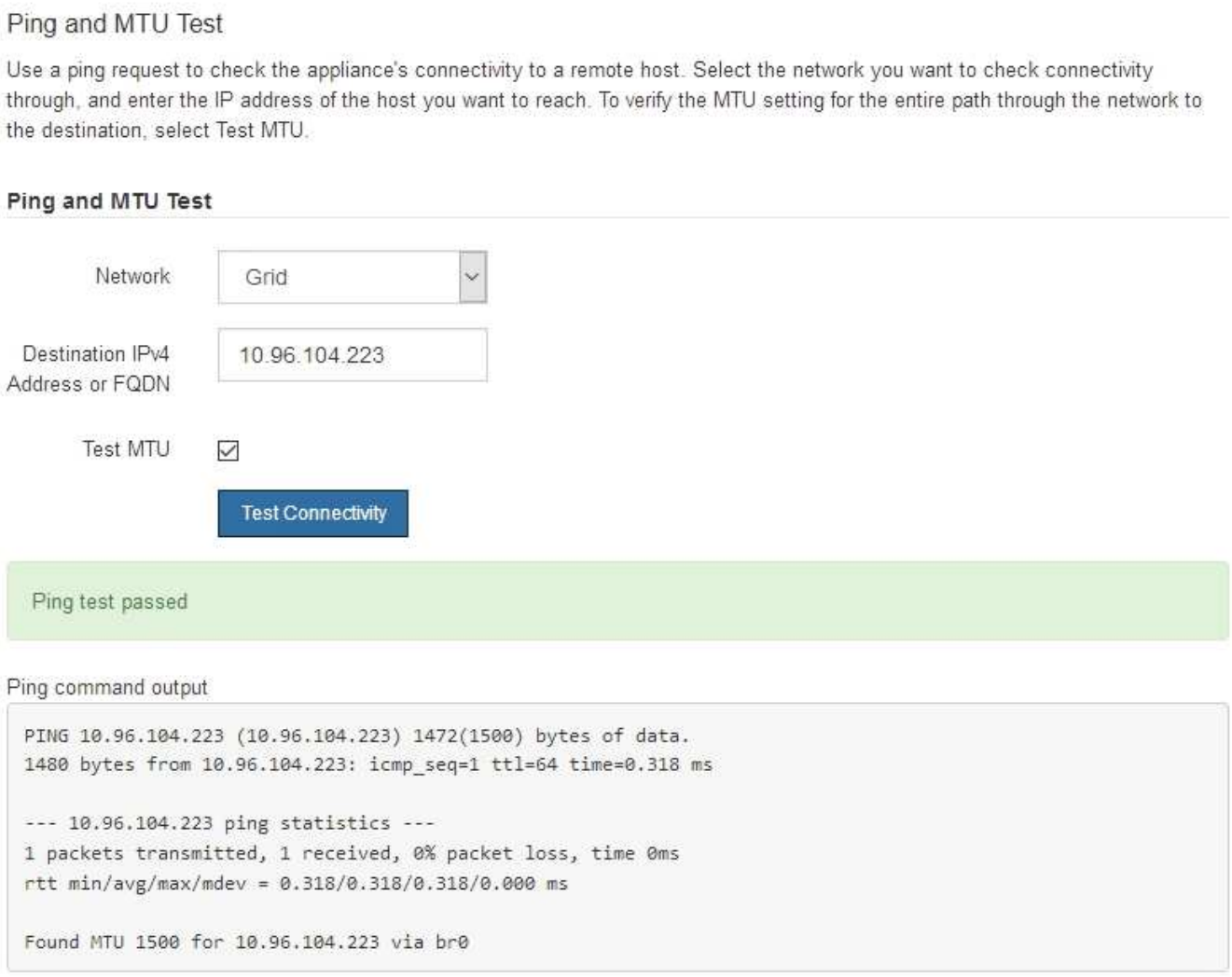
   Beispielsweise möchten Sie das Gateway im Netzwerk oder den primären Admin-Node pingen.

4. Aktivieren Sie optional das Kontrollkästchen **MTU-Test**, 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.



Verwandte Informationen

"Konfigurieren von Netzwerkverbindungen (SG6000)"

"Ändern der MTU-Einstellung"

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 unter der Portreferenz in den Netzwerkrichtlinien von StorageGRID.

> ⓘ Die in der Tabelle für die Portkonnektivität aufgeführten Grid-Netzwerkports sind nur für StorageGRID Version 11.5 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.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

   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.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

Port Connectivity Test

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

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.

- Wenn für einen oder mehrere ausgewählte Ports keine Netzwerkverbindung auf Portebene hergestellt werden kann, wird die Meldung „`Verbindungstest 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.

Verwandte Informationen

"Netzwerkrichtlinien"

Zugriff auf und Konfigurieren von SANtricity System Manager

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.

Schritte

- "Einrichten von SANtricity System Manager und Zugriff auf diese zugreifen"
- "Überprüfen des Hardwarestatus in SANtricity System Manager"
- "Festlegen der IP-Adressen für die Speichercontroller mithilfe des StorageGRID-Appliance-Installationsprogramms"

Einrichten von SANtricity System Manager und Zugriff auf diese zugreifen

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.

Was Sie benötigen

- Sie verwenden einen unterstützten Webbrowser.
- Um über den Grid Manager auf SANtricity-System-Manager zuzugreifen, müssen Sie StorageGRID installiert haben, und Sie müssen über die Berechtigung zum Administrator der Speichergeräte oder Root-Zugriff verfügen.
- Um mit dem StorageGRID-Appliance-Installationsprogramm auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity-System-Managers verfügen.
- Um direkt über einen Webbrowser auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity System Managers verfügen.

> 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, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring 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 den StorageGRID-Appliance-Installer oder den Grid-Manager nicht verwenden können, können Sie über einen Webbrowser, der mit dem Management-Port verbunden ist, direkt auf 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 Konfigurieren von Warnmeldungen zur Hardware Schritt:

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 zum E-Series AutoSupport finden Sie im Dokumentationszentrum zur E-Series.

  "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 **Knoten** > ***appliance Storage Node*** > **SANtricity System Manager**

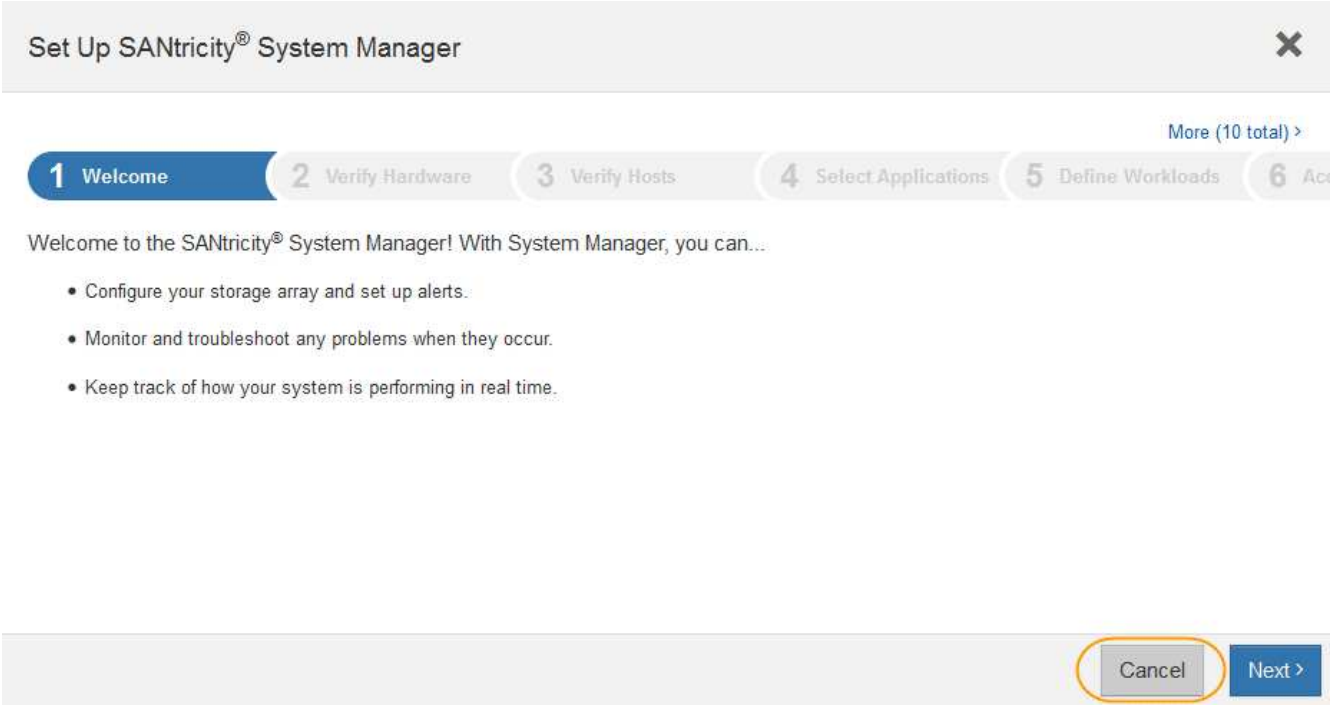
     Wenn diese Optionen nicht verfügbar sind oder die Anmeldeseite nicht angezeigt wird, müssen Sie die IP-Adresse des Storage Controllers verwenden. Greifen Sie auf SANtricity System Manager zu, indem Sie die Storage Controller-IP aufrufen:
     `https://Storage_Controller_IP`

Die Anmeldeseite für den SANtricity System Manager wird angezeigt.

2. Legen Sie das Administratorpasswort fest oder geben Sie es ein.

> SANtricity System Manager verwendet ein einziges Administratorkennwort, das von allen Benutzern verwendet wird.

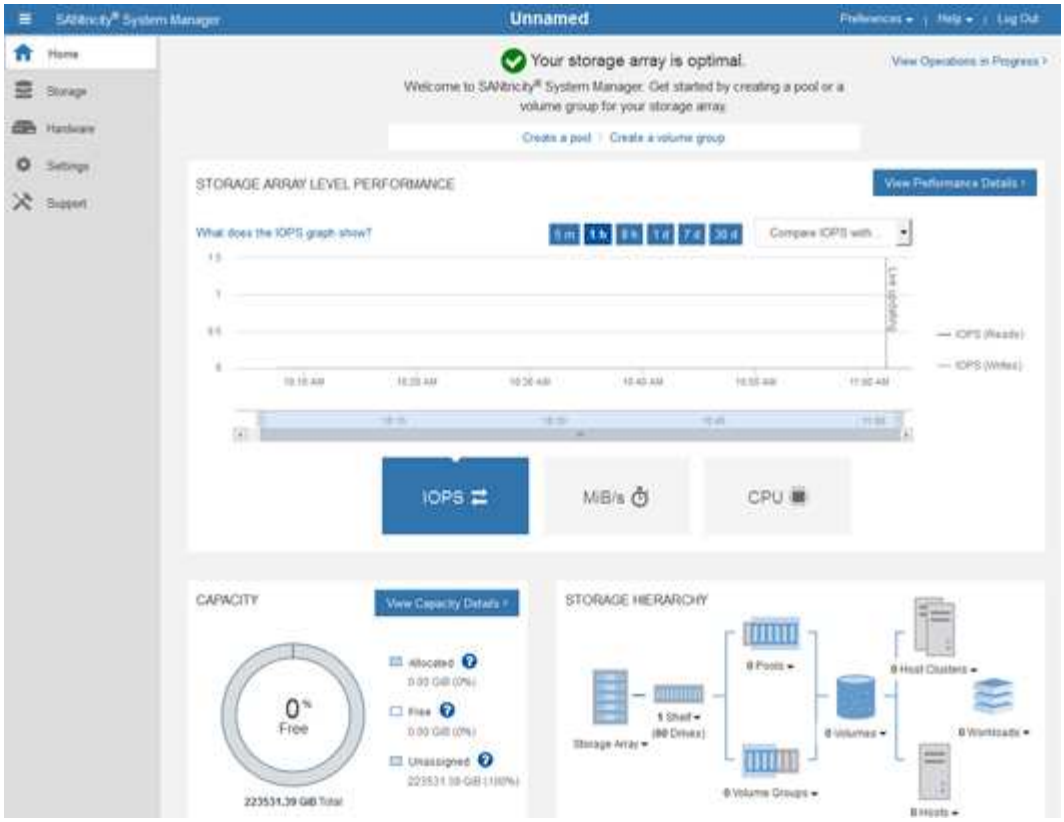
Der Einrichtungsassistent wird angezeigt.



3. Wählen Sie **Abbrechen**, um den Assistenten zu schließen.

> Schließen Sie den Setup-Assistenten für eine StorageGRID Appliance nicht ab.

Die Startseite von SANtricity System Manager wird angezeigt.



1. Konfigurieren von Warnmeldungen zur Hardware
   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.
2. 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. Verwenden Sie den Abschnitt **Support** > **Support Center** der Online-Hilfe, um mehr über die AutoSupport-Funktion zu erfahren.
   c. Folgen Sie den Anweisungen „`Anleitung`“, um AutoSupport zu managen.

      Genaue Anweisungen zur Konfiguration eines StorageGRID Proxy zum Senden von AutoSupport Nachrichten der E-Series ohne Verwendung des Management Ports finden Sie unter den Anweisungen für die Administration der StorageGRID. Suchen Sie nach „Proxy-Einstellungen für E-Series AutoSupport“.

   "StorageGRID verwalten"
3. 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.

4. 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.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"Festlegen der IP-Adressen für die Speichercontroller mithilfe des StorageGRID-Appliance-Installationsprogramms"

Überprüfen des 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. Komponententententententemperaturen oder Problemen mit den Laufwerken, überprüft.

Was Sie benötigen

- Sie verwenden einen unterstützten Webbrowser.
- Um über den Grid Manager auf SANtricity System Manager zuzugreifen, müssen Sie über die Administratorberechtigung für die Speicheranwendung oder über die Berechtigung für den Root-Zugriff verfügen.
- Um mit dem StorageGRID-Appliance-Installationsprogramm auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity-System-Managers verfügen.
- Um direkt über einen Webbrowser auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity System Managers verfügen.

> 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, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Installations- und Wartungsanweisungen für Ihr Gerät.

Schritte

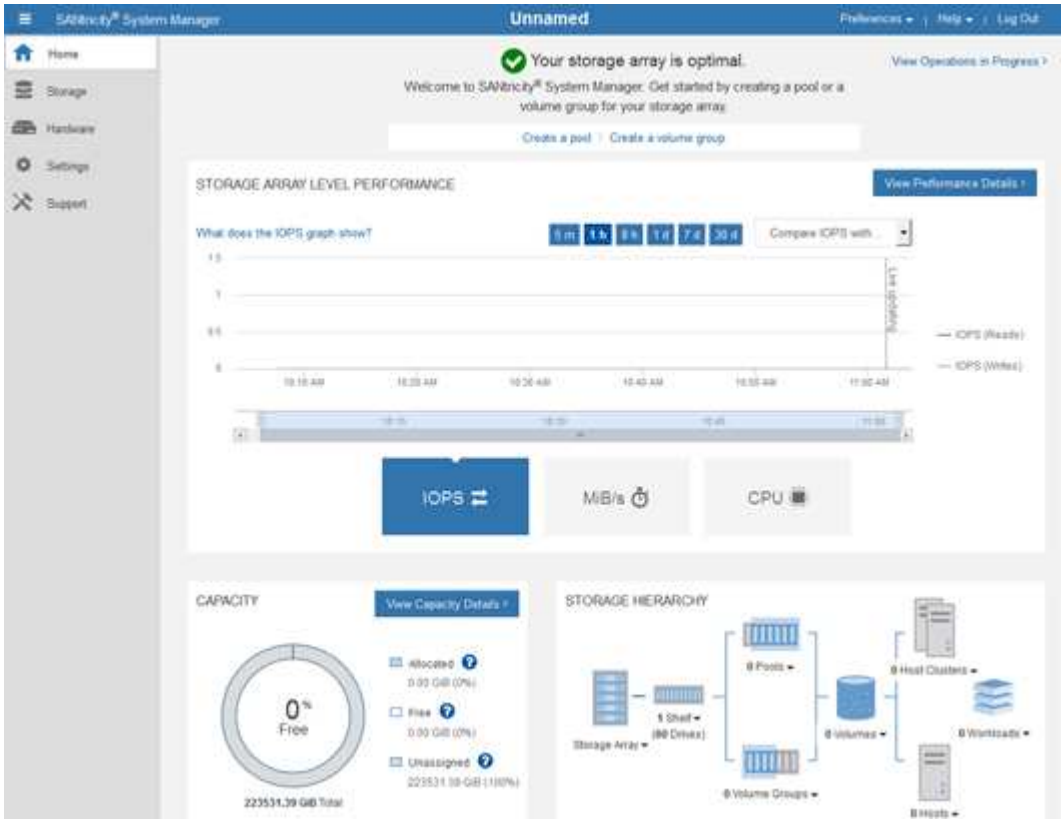
1. Greifen Sie auf SANtricity System Manager zu.

   "Einrichten von SANtricity System Manager und Zugriff auf diese zugreifen"

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.

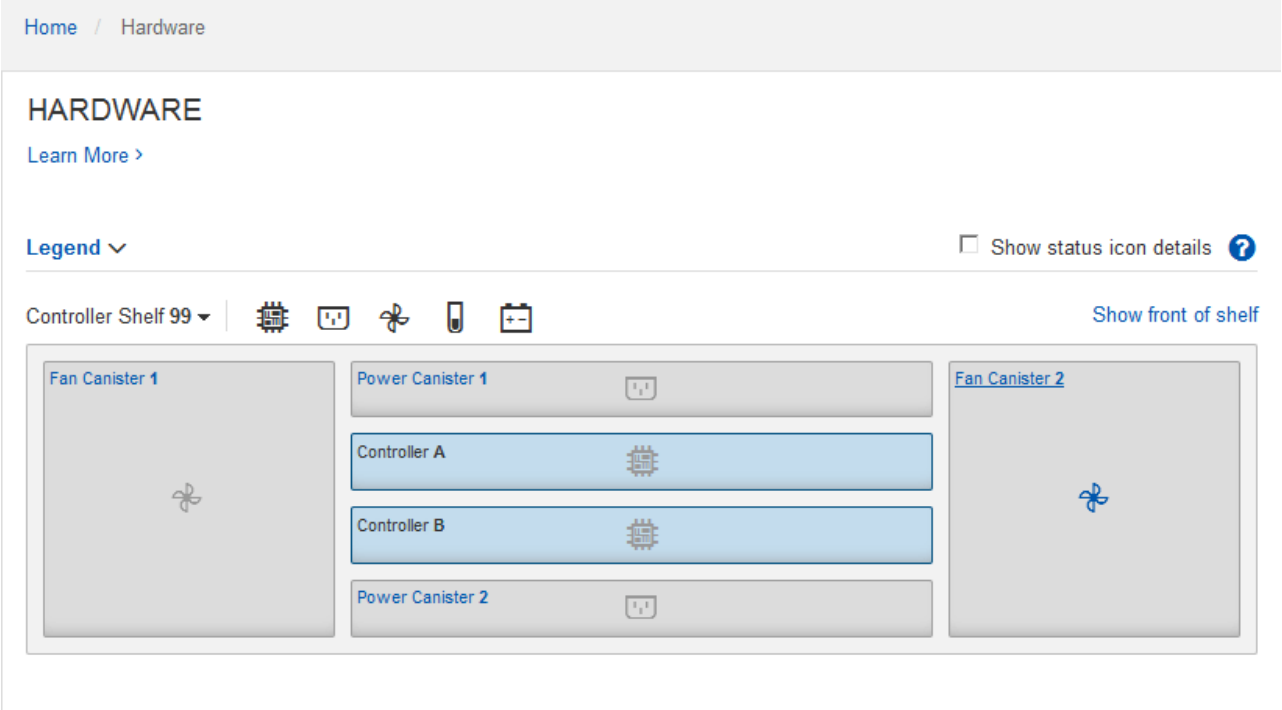
   Die Startseite von SANtricity System Manager wird angezeigt. In SANtricity System Manager wird das Controller Shelf als Storage-Array bezeichnet.



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 Shelfs können Sie sowohl Storage-Controller als auch den Akku in jedem Storage Controller, die beiden Power Kanister, die beiden Lüfter-Kanister und Erweiterungs-Shelfs (falls vorhanden) anzeigen. Sie können auch Komponententententemperaturen 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 Shelfs können die Laufwerke und die Laufwerksfächer für das Storage Controller-Shelf oder die Erweiterungs-Shelfs (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.

Festlegen der IP-Adressen für die Speichercontroller mithilfe des StorageGRID-Appliance-Installationsprogramms

Management-Port 1 auf jedem Storage-Controller verbindet die Appliance mit dem Managementnetzwerk für SANtricity System Manager. Wenn Sie vom StorageGRID Appliance Installer nicht auf den SANtricity System Manager zugreifen können, müssen Sie für jeden Storage Controller eine statische IP-Adresse festlegen, um sicherzustellen, dass die Managementverbindung zur Hardware und der Controller-Firmware im Controller-Shelf nicht unterbrochen wird.

Was Sie benötigen

- 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.

> Führen Sie diese Schritte nur aus, wenn Sie über den StorageGRID Appliance Installer (**Erweitert** > **SANtricity System Manager**) oder Grid Manager (**Knoten** > **SANtricity System Manager**) keinen Zugriff auf den 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-Netzwerkkonfiguration**.

   Die Seite Speichercontroller-Netzwerkkonfiguration wird angezeigt.

3. Wählen Sie je nach Netzwerkkonfiguration **aktiviert** für IPv4, IPv6 oder beides.
4. Notieren Sie sich die automatisch angezeigte IPv4-Adresse.

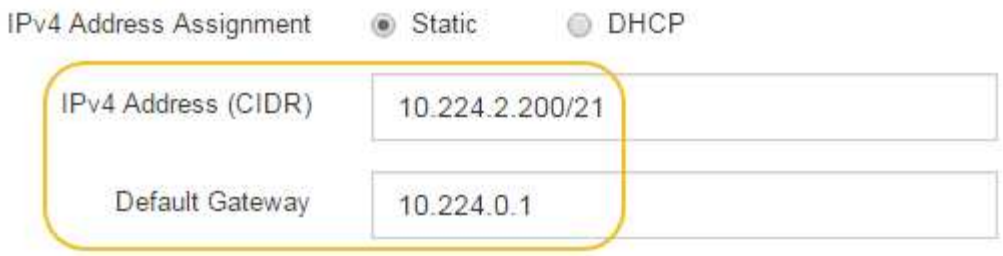
   DHCP ist die Standardmethode, um dem Management-Port des Storage Controllers eine IP-Adresse zuzuweisen.

   > Es kann einige Minuten dauern, bis die DHCP-Werte angezeigt werden.

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.

   a. Wählen Sie **Statisch**.
   b. Geben Sie die IPv4-Adresse unter Verwendung der CIDR-Schreibweise ein.
   c. Geben Sie das Standard-Gateway ein.



d. 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*

Konfigurieren der BMC-Schnittstelle

Die Benutzeroberfläche für den Baseboard Management Controller (BMC) auf dem SG6000-CN Controller bietet Statusinformationen über die Hardware und ermöglicht die Konfiguration von SNMP-Einstellungen und anderen Optionen für den SG6000-CN Controller.

Schritte

- "Ändern des Root-Passworts für die BMC-Schnittstelle"
- "Einstellen der IP-Adresse für den BMC-Managementport"
- "Zugriff auf die BMC-Schnittstelle"
- "Konfigurieren von SNMP-Einstellungen für den SG6000-CN-Controller"
- "Einrichten von E-Mail-Benachrichtigungen für Meldungen"

Ändern des Root-Passworts für die BMC-Schnittstelle

Aus Sicherheitsgründen müssen Sie das Kennwort für den Root-Benutzer von BMC ändern.

Was Sie benötigen

- Der Management-Client verwendet einen unterstützten Webbrowser.

Über diese Aufgabe

Bei der ersten Installation des Geräts verwendet der BMC ein Standardpasswort für den Root-Benutzer (`root/calvin`). Sie müssen das Passwort für den Root-Benutzer ändern, um Ihr System zu sichern.

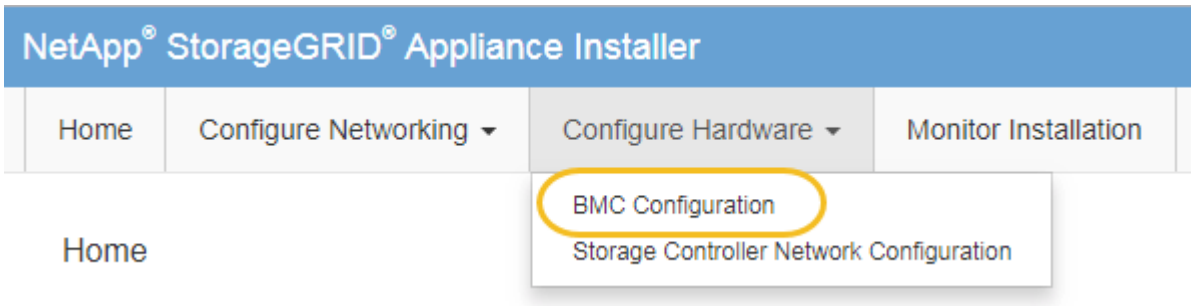
Schritte

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.

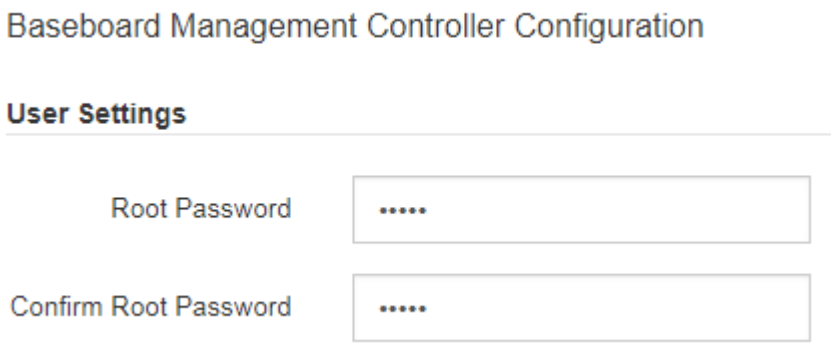
Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware konfigurieren** > **BMC-Konfiguration**.



Die Seite Baseboard Management Controller Configuration wird angezeigt.

3. Geben Sie in den beiden Feldern ein neues Passwort für das Root-Konto ein.



4. Klicken Sie Auf **Speichern**.

Einstellen der IP-Adresse für den BMC-Managementport

Bevor Sie auf die BMC-Schnittstelle zugreifen können, müssen Sie die IP-Adresse für den BMC-Management-Port des SG6000-CN-Controllers konfigurieren.

Was Sie benötigen

- Der Management-Client verwendet einen unterstützten 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.

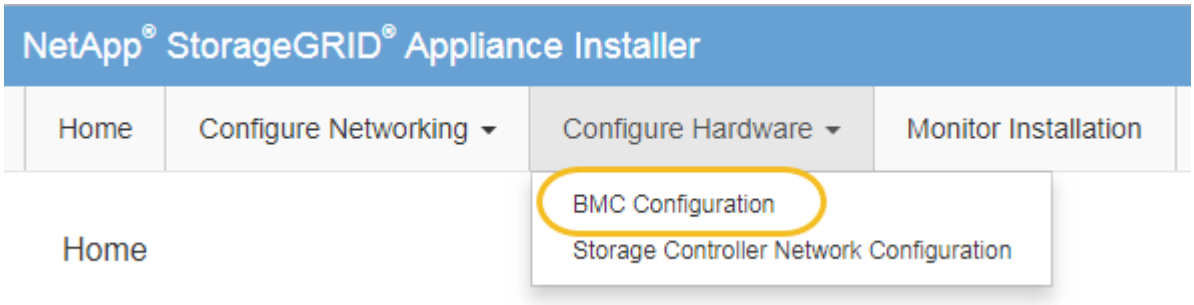
Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:
   `https://SG6000-CN_Controller_IP:8443`

   Für `SG6000-CN_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** > **BMC-Konfiguration**.

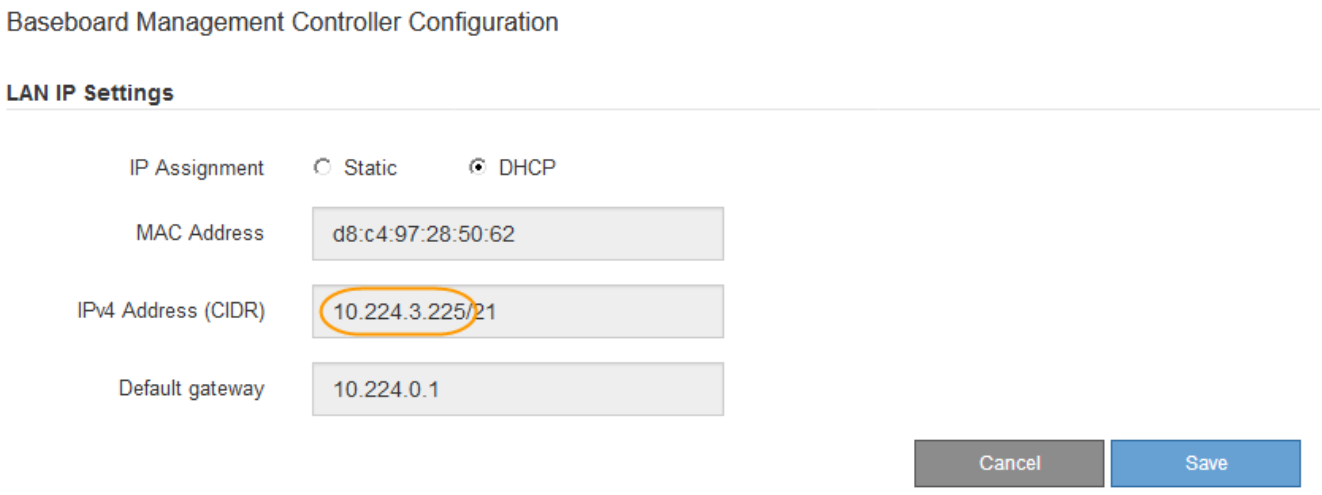


   Die Seite Baseboard Management Controller Configuration wird angezeigt.

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.



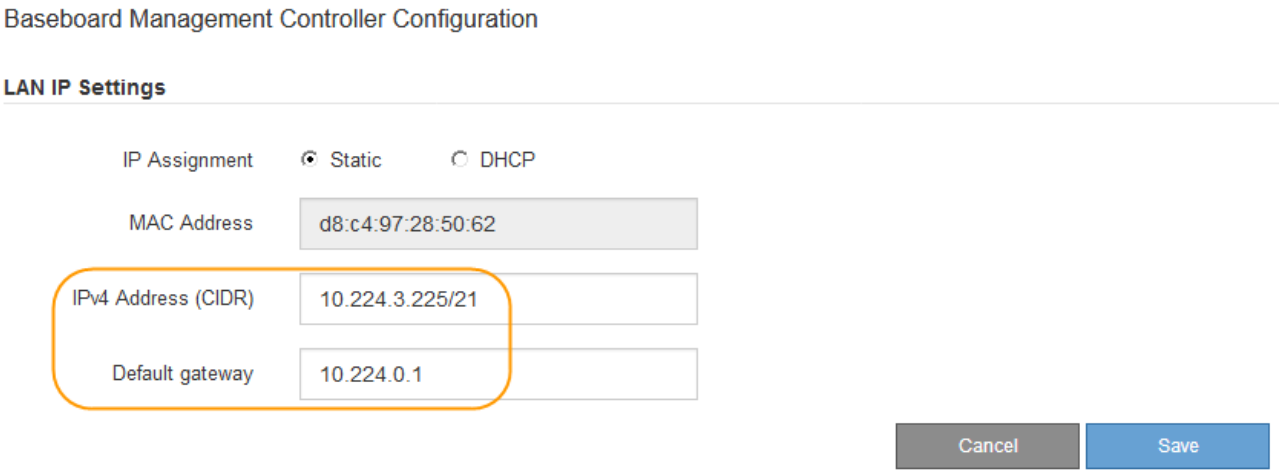
4. Legen Sie optional eine statische IP-Adresse für den BMC-Verwaltungsport fest.

Sie sollten entweder eine statische IP für den BMC-Verwaltungsport 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.



d. Klicken Sie Auf **Speichern**.

Es kann einige Minuten dauern, bis Ihre Änderungen angewendet werden.

Zugriff auf die BMC-Schnittstelle

Sie können über die DHCP- oder statische IP-Adresse für den BMC-Management-Port auf die BMC-Schnittstelle des SG6000-CN-Controllers zugreifen.

Was Sie benötigen

- Der BMC-Management-Port des SG6000-CN Controllers ist mit dem Managementnetzwerk verbunden, das Sie verwenden möchten.

- Der Management-Client verwendet einen unterstützten Webbrowser.

Schritte

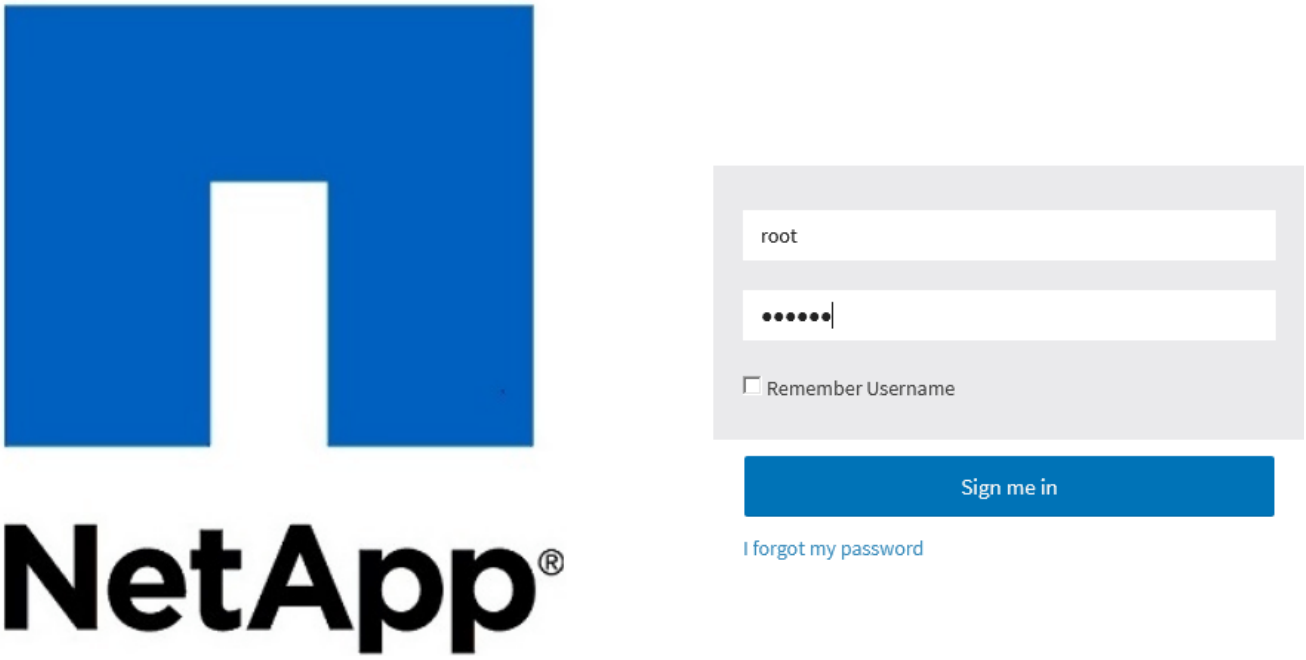
1. Geben Sie die URL für die BMC-Schnittstelle ein:
   `https://BMC_Port_IP`

   Für *`BMC_Port_IP`*, Verwenden Sie die DHCP- oder statische IP-Adresse für den BMC-Management-Port.

   Die BMC-Anmeldeseite wird angezeigt.

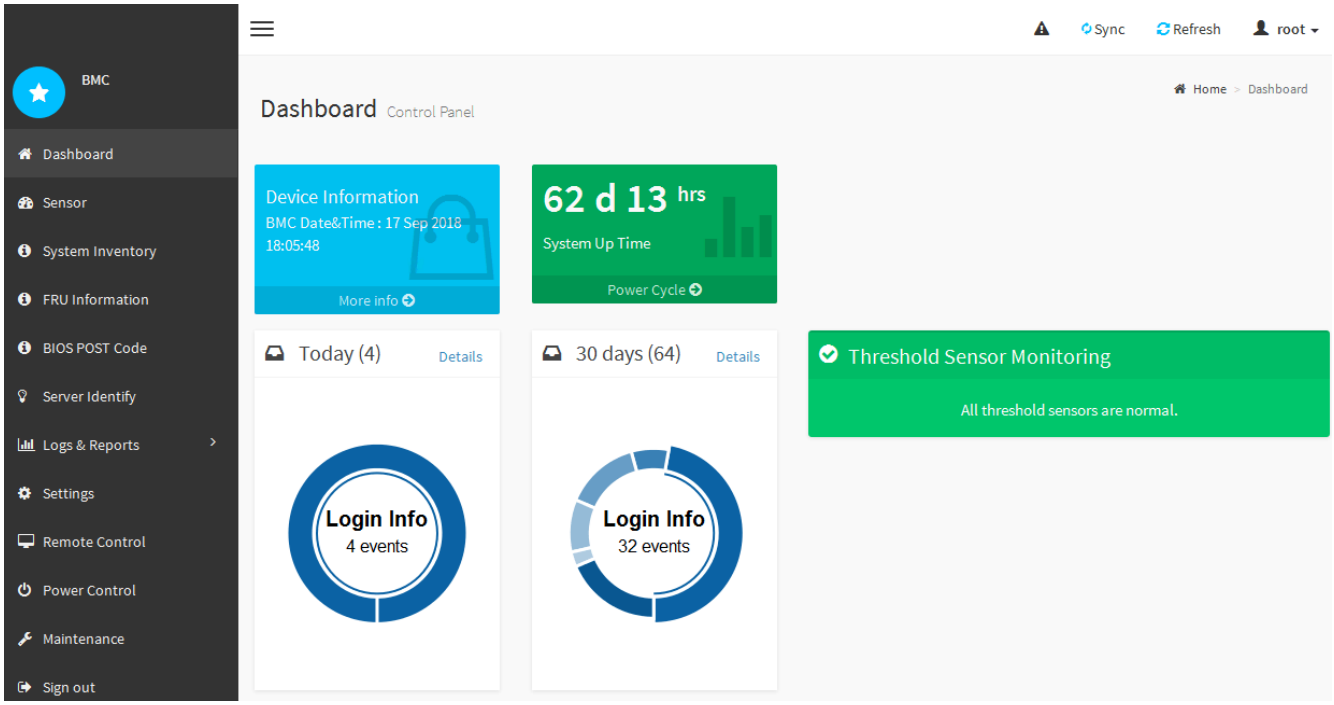
2. Geben Sie den Root-Benutzernamen und das Kennwort ein. Verwenden Sie dazu das Passwort, das Sie beim Ändern des Standard-Root-Passworts festgelegt haben:

`root`
`password`



3. Wählen Sie **Sign me in** aus.

   Das BMC-Dashboard wird angezeigt.



4. 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.

Verwandte Informationen

"Ändern des Root-Passworts für die BMC-Schnittstelle"

Konfigurieren von SNMP-Einstellungen für den SG6000-CN-Controller

Wenn Sie mit der Konfiguration von SNMP für Hardware vertraut sind, können Sie die SNMP-Einstellungen für den SG6000-CN-Controller über die BMC-Schnittstelle konfigurieren. Sie können sichere Community-Strings bereitstellen, SNMP-Trap aktivieren und bis zu fünf SNMP-Ziele angeben.

Was Sie benötigen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Sie haben Erfahrung in der Konfiguration von SNMP-Einstellungen für SNMPv1-v2c Geräte.

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 Domain-Namen werden nicht unterstützt.

   Aktivieren Sie Traps, wenn der SG6000-CN-Controller sofortige Benachrichtigungen an eine SNMP-Konsole senden soll, wenn sie sich in einem ungewöhnlichen Zustand befindet. Traps können zeigen, dass Hardwareausfälle von verschiedenen Komponenten oder Temperaturschwellenwerten überschritten werden.

4. Klicken Sie optional auf **Test-Trap senden**, um Ihre Einstellungen zu testen.
5. Wenn die Einstellungen korrekt sind, klicken Sie auf **Speichern**.

Einrichten von E-Mail-Benachrichtigungen für Meldungen

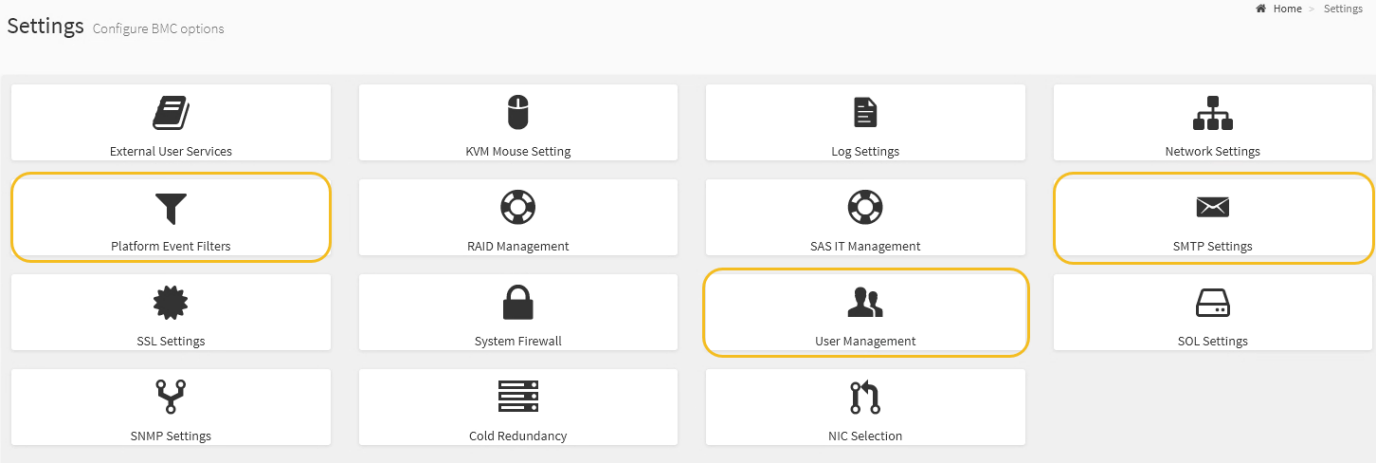
Wenn E-Mail-Benachrichtigungen gesendet werden sollen, wenn Warnmeldungen auftreten, müssen Sie SMTP-Einstellungen, Benutzer, LAN-Ziele, Warnrichtlinien und Ereignisfilter über die BMC-Schnittstelle konfigurieren.

Was Sie benötigen

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 SMTP-Einstellungen.
   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 alle Benutzer Benachrichtigungen erhalten möchten, müssen Sie für jeden Benutzer ein LAN-Ziel hinzufügen.
   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: Aktivieren der Node-Verschlüsselung

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. Bei der Installation der Appliance müssen Sie die Node-Verschlüsselung auswählen und aktivieren. Die Auswahl der Node-Verschlüsselung kann nicht rückgängig gemacht werden, sobald der KMS-Verschlüsselungsprozess gestartet wird.

Was Sie benötigen

Lesen Sie die Informationen über KMS in den Anweisungen zur Administration von StorageGRID durch.

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.

> ⓘ Alle Daten, die vor einer Appliance mit aktivierter Node-Verschlüsselung vorhanden sind, werden mit einem nichtsicheren temporären Schlüssel verschlüsselt. Das Gerät ist erst dann vor dem Entfernen oder Diebstahl geschützt, wenn der Schlüssel auf einen vom KMS angegebenen Wert gesetzt wird.

Ohne den KMS-Schlüssel, der zur Entschlüsselung der Festplatte benötigt wird, können die Daten auf der Appliance nicht abgerufen und effektiv verloren gehen. 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.

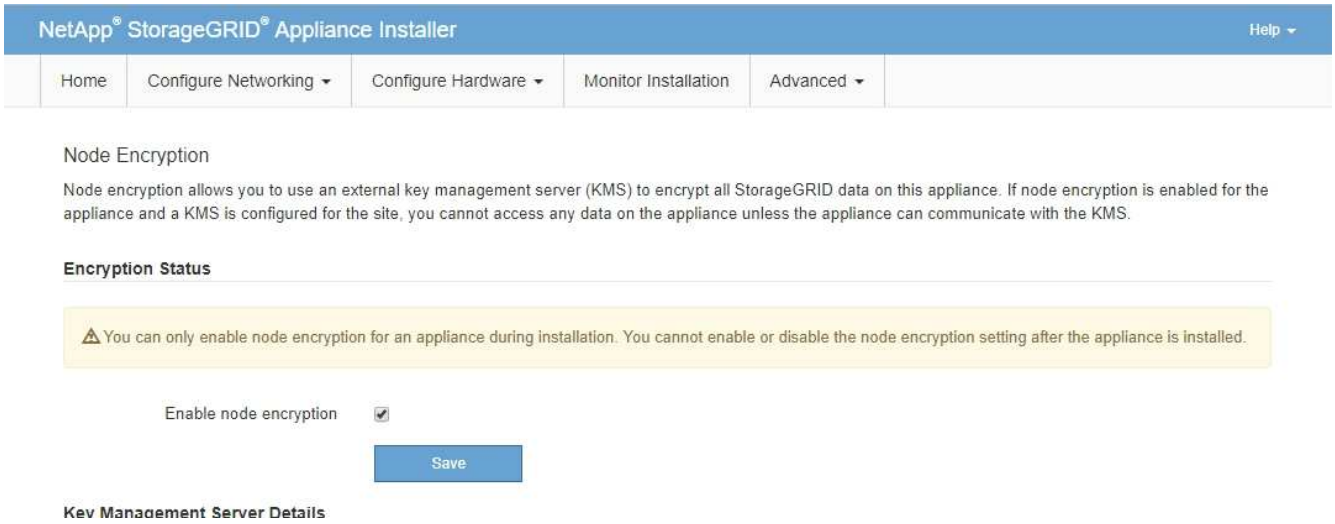
   `https://Controller_IP:8443`

   `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 Appliance-Festplatten nicht entschlüsselt werden, ohne dabei den gleichen KMS-Schlüssel zu verwenden.

2. Wählen Sie **Hardware Konfigurieren** > **Node Encryption**.



3. Wählen Sie **Node-Verschlüsselung aktivieren**.

   Sie können die Auswahl **Enable Node Encryption** ohne Gefahr eines Datenverlusts aufheben, bis Sie **Save** auswählen und der Appliance Node auf die KMS-Verschlüsselungsschlüssel in Ihrem StorageGRID-System zugreift und mit der Festplattenverschlüsselung beginnt. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht deaktivieren.

   > Nachdem Sie einer StorageGRID Site mit KMS eine Appliance hinzugefügt haben, für die die Node-Verschlüsselung aktiviert ist, kann die KMS-Verschlüsselung für den Node nicht angehalten werden.

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.

Verwandte Informationen

"StorageGRID verwalten"

"Monitoring der Node-Verschlüsselung im Wartungsmodus"

Optional: Ändern des RAID-Modus (nur SG6000)

Sie können zu einem anderen RAID-Modus auf der Appliance wechseln, um Ihre Anforderungen an Storage und Recovery zu erfüllen. Sie können den Modus nur ändern, bevor Sie den Appliance-Speicherknoten bereitstellen.

Was Sie benötigen

- Sie verwenden jeden Client, der eine Verbindung zu StorageGRID herstellen kann.
- Der Client verfügt über einen unterstützten Webbrowser.

Über diese Aufgabe

Vor der Bereitstellung der Appliance als Storage Node können Sie eine der folgenden Volume-Konfigurationsoptionen wählen:

- **DDP**: Dieser Modus verwendet zwei Paritätslaufwerke pro acht Datenlaufwerke. Dies ist der Standard- und empfohlene Modus für alle Appliances. Im Vergleich zu RAID 6 bietet DDP eine bessere System-Performance, geringere Wiederherstellungszeiten nach Laufwerksausfällen und einfaches Management. DDP bietet auch Schutz vor Schubladenverlust bei Appliances mit 60 Laufwerken.
- **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 System-Performance, geringere Wiederherstellungszeiten nach Laufwerksausfällen, einfaches 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. 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 erhöhen 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.

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**.

Verwandte Informationen

"NetApp E-Series Systems Documentation Site"

Optional: Neu zuordnen von Netzwerkports für die Appliance

Möglicherweise müssen Sie die internen Ports auf dem Appliance Storage Node zu verschiedenen externen Ports neu zuordnen. Aufgrund eines Firewall-Problems müssen Sie möglicherweise Ports neu zuordnen.

Was Sie benötigen

- Sie haben zuvor auf das Installationsprogramm für StorageGRID-Geräte zugegriffen.
- Sie sind nicht konfiguriert und planen keine Konfiguration von Load Balancer-Endpunkten.

> Wenn Sie Ports neu zuordnen, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Wenn Sie Load Balancer-Endpunkte konfigurieren und bereits neu zugeordnete Ports haben möchten, befolgen Sie die Schritte in den Recovery- und Wartungsanweisungen zum Entfernen von Port-Remaps.

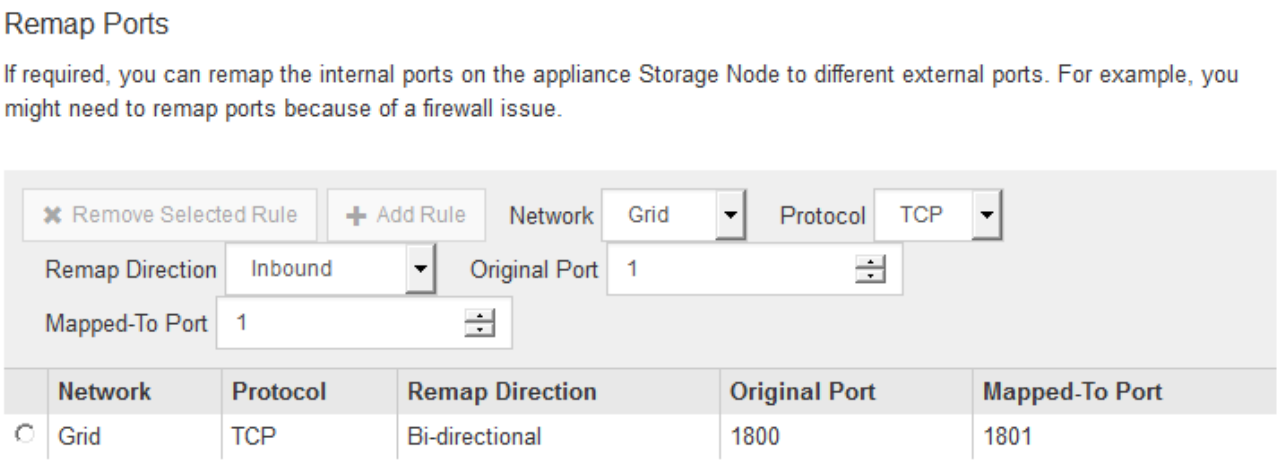
Schritte

1. Klicken Sie im Installationsprogramm der StorageGRID-Appliance auf **Netzwerke konfigurieren** > **Ports für den Remap**.

   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. Klicken Sie Auf **Regel Hinzufügen**.

Die neue Port-Zuordnung wird der Tabelle hinzugefügt, und die erneute Zuordnung wird sofort wirksam.



8. Um eine Portzuordnung zu entfernen, aktivieren Sie das Optionsfeld für die Regel, die Sie entfernen möchten, und klicken Sie auf **Ausgewählte Regel entfernen**.

Implementieren eines Appliance-Storage-Node

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.

Was Sie benötigen

- Wenn Sie einen Appliance-Node klonen, fahren Sie den Recovery- und Wartungsvorgang fort.

  "Verwalten Sie erholen"

- 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.

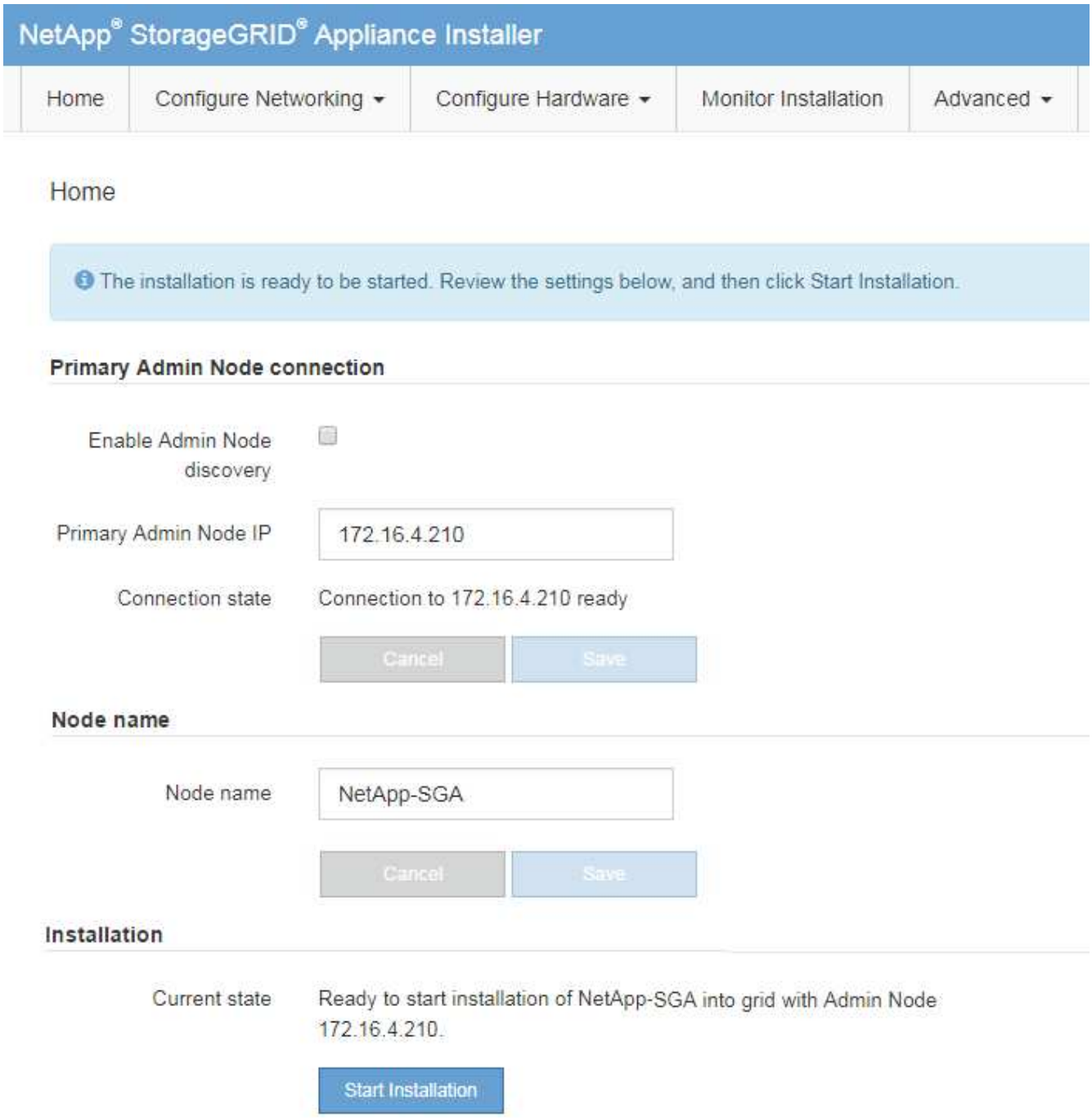
> Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisieren `configure-sga.py` Installationsskript für Geräte.

- Wenn Sie eine Erweiterung oder Wiederherstellung durchführen, befolgen Sie die entsprechenden Anweisungen:
  - Informationen zum Hinzufügen eines Appliance-Speicherknoten zu einem vorhandenen StorageGRID-System finden Sie in den Anweisungen zum erweitern eines StorageGRID-Systems.
  - Informationen zum Bereitstellen eines Appliance Storage Node im Rahmen eines Wiederherstellungsvorgangs finden Sie in den Anweisungen für Recovery und Wartung.

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	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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 klicken Sie auf **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 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 Installations- und Wartungsanleitung für Ihr Gerät.

   Wenn Sie die Storage Node Appliance als Ziel für das Klonen eines Node implementieren, beenden Sie den Implementierungsprozess hier und setzen Sie das Klonverfahren für den Node bei Recovery und Wartung fort. +"Verwalten Sie erholen"

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 automatisieren `configure-sga.py` Installationsskript für Geräte. Dieses Skript gilt nur für Speicherknoten.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

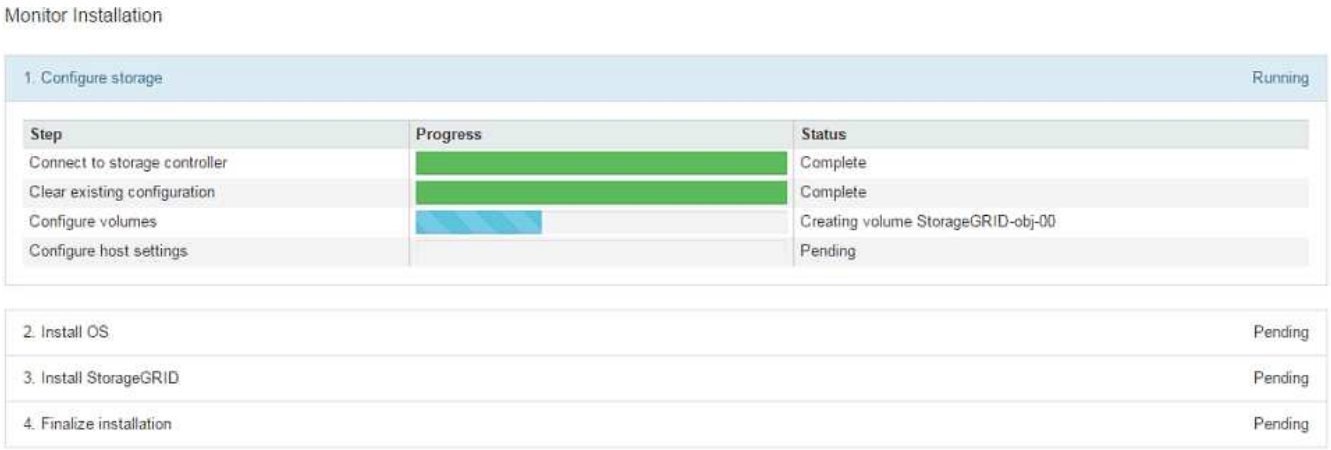
Monitoring der Installation der Speicher-Appliance

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 auf **Installation überwachen**.

   Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.



   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 „`Skipped.`“ angezeigt.

2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

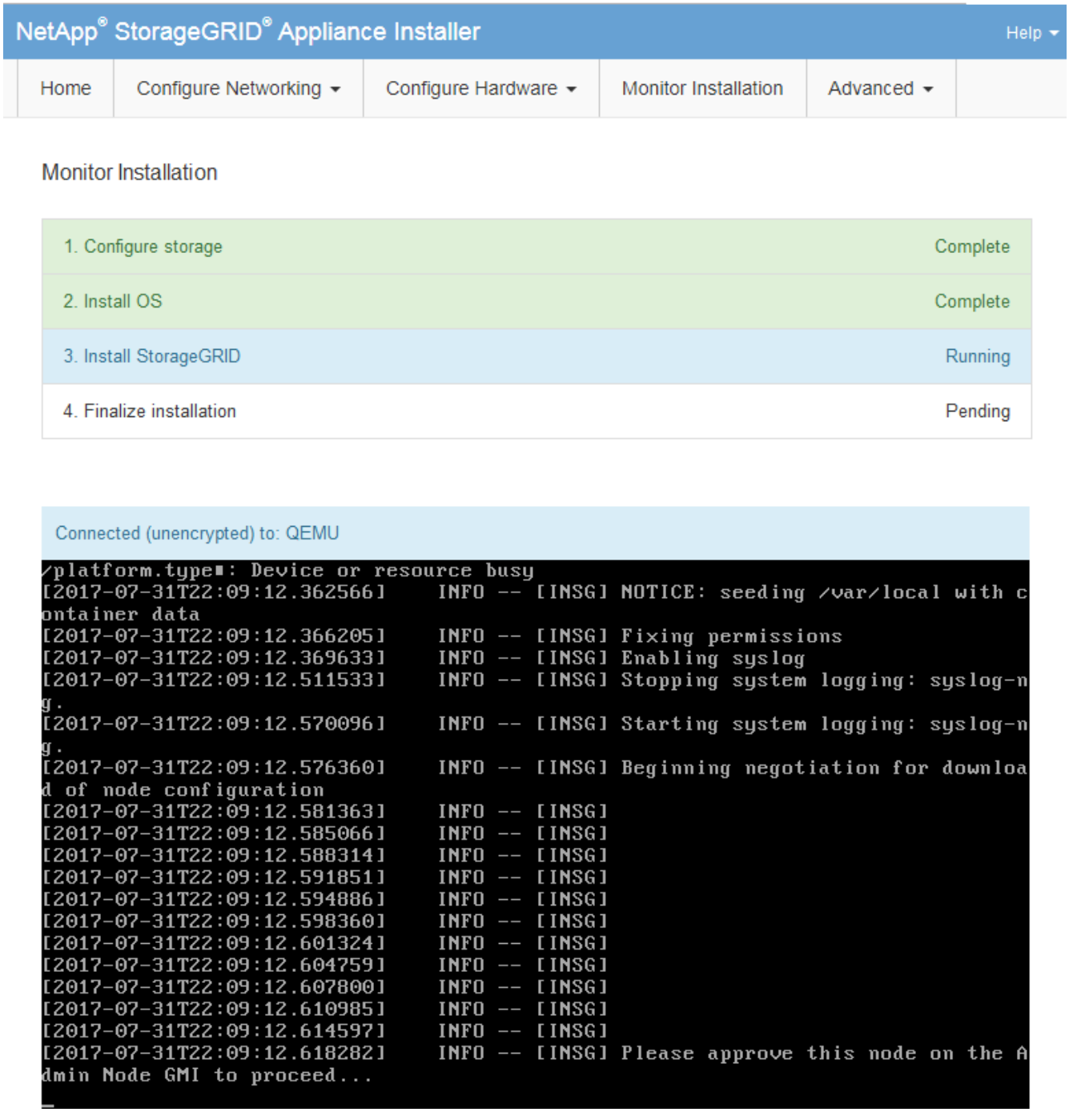
   1. Speicher konfigurieren

   In dieser Phase stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.

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.



4. Wechseln Sie zum Grid Manager, genehmigen Sie den ausstehenden Storage-Node und führen Sie den StorageGRID-Installationsprozess aus.

   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.

Automatisierung der Installation und Konfiguration von Appliances

Sie können die Installation und Konfiguration Ihrer Appliances und die Konfiguration des gesamten StorageGRID Systems automatisieren.

Über diese Aufgabe

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

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

- Erstellen Sie eine JSON-Datei, in der die Konfigurationseinstellungen für Ihre Appliances angegeben sind. Laden Sie die JSON-Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

  Sie können dieselbe Datei verwenden, um mehr als ein Gerät zu konfigurieren.

- Verwenden Sie die StorageGRID`configure-sga.py` Python-Skript zur Automatisierung der Konfiguration Ihrer Appliances.
- Zusätzliche Python-Skripte verwenden, um andere Komponenten des gesamten StorageGRID-Systems (das „Grid“) zu konfigurieren.

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. Weitere Informationen zum Herunterladen und Extrahieren der StorageGRID-Installationsdateien finden Sie in den Anweisungen zum Wiederherstellen und Verwalten.

Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer

Sie können die Konfiguration einer Appliance mithilfe einer JSON-Datei mit den Konfigurationsinformationen automatisieren. Sie laden die Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

Was Sie benötigen

- Ihr Gerät muss mit der neuesten Firmware ausgestattet sein, die mit StorageGRID 11.5 oder höher kompatibel ist.
- Sie müssen mit dem Installationsprogramm für StorageGRID-Geräte auf der Appliance verbunden sein, die Sie mit einem unterstützten Browser konfigurieren.

Über diese Aufgabe

Sie können Appliance-Konfigurationsaufgaben automatisieren, z. B. die Konfiguration folgender Komponenten:

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

- Netzwerk-Bond-Modus
- Verbindungsgeschwindigkeit

Die Konfiguration Ihrer Appliance mit einer hochgeladenen JSON-Datei ist häufig effizienter als die manuelle Ausführung der Konfiguration mit mehreren Seiten im StorageGRID-Appliance-Installationsprogramm, insbesondere wenn Sie viele Knoten konfigurieren müssen. Sie müssen die Konfigurationsdatei für jeden Knoten einzeln anwenden.

> Erfahrene Benutzer, die sowohl die Installation als auch die Konfiguration ihrer Appliances automatisieren möchten, können das verwenden `configure-sga.py` Skript: +"Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

Schritte

1. Generieren Sie die JSON-Datei mit einer der folgenden Methoden:
   - Die ConfigBuilder-Anwendung

     "ConfigBuilder.netapp.com"

   - Der `configure-sga.py` Konfigurationsskript für die Appliance Sie können das Skript vom Installationsprogramm für StorageGRID-Geräte herunterladen (**Hilfe** > **Konfigurationsskript für Geräte**). Lesen Sie die Anweisungen zur Automatisierung der Konfiguration mit dem Skript configure-sga.py.

     "Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

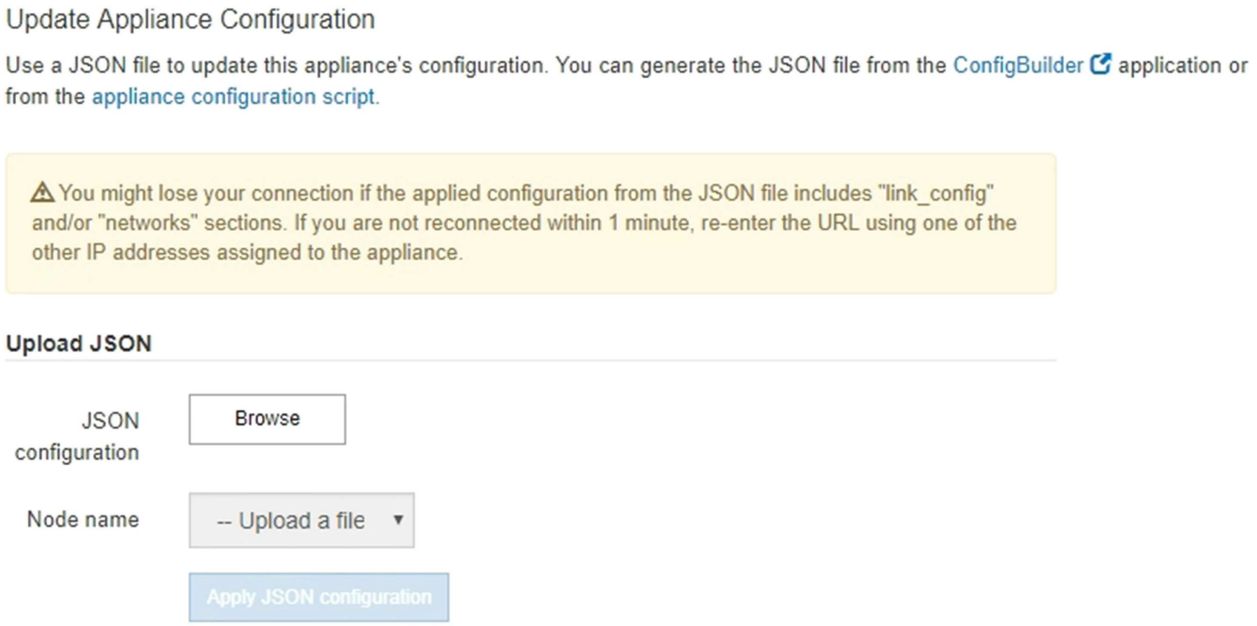
     Die Node-Namen in der JSON-Datei müssen die folgenden Anforderungen erfüllen:

   - Muss ein gültiger Hostname mit mindestens 1 und nicht mehr als 32 Zeichen sein
   - Es können Buchstaben, Ziffern und Bindestriche verwendet werden
   - Sie können nicht mit einem Bindestrich beginnen oder enden oder nur Zahlen enthalten

     > Stellen Sie sicher, dass die Node-Namen (die Top-Level-Namen) in der JSON-Datei eindeutig sind, oder Sie können mit der JSON-Datei nicht mehr als einen Node konfigurieren.

2. Wählen Sie **Erweitert** > **Appliance-Konfiguration Aktualisieren**.

   Die Seite Gerätekonfiguration aktualisieren wird angezeigt.



3. Wählen Sie die JSON-Datei mit der Konfiguration aus, die Sie hochladen möchten.

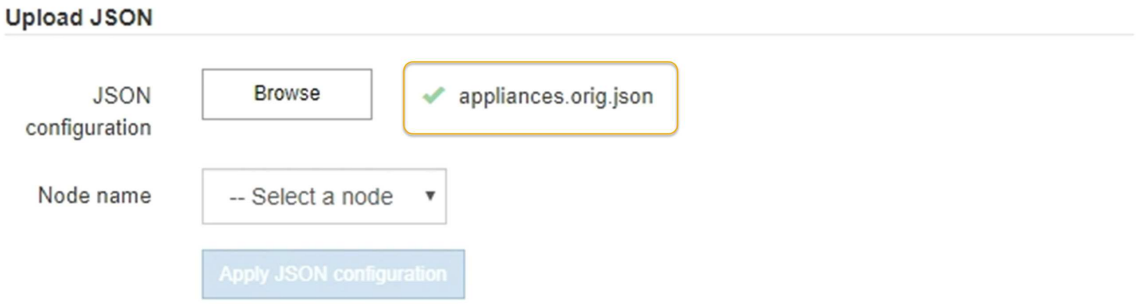
   a. Wählen Sie **Durchsuchen**.

   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 neben einem grünen Häkchen angezeigt.

   > Möglicherweise verlieren Sie die Verbindung zur Appliance, wenn die Konfiguration aus der JSON-Datei Abschnitte für „Link_config“, „Netzwerke“ oder beide enthält. Wenn Sie nicht innerhalb einer Minute eine Verbindung hergestellt haben, geben Sie die Appliance-URL mithilfe einer der anderen IP-Adressen, die der Appliance zugewiesen sind, erneut ein.

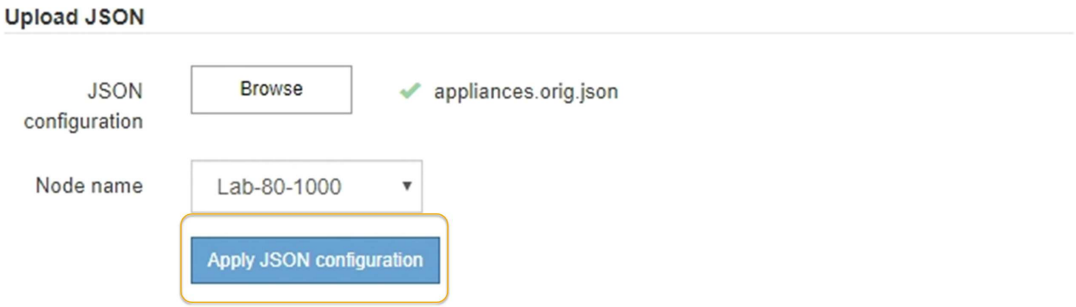


   Das Dropdown-Menü **Node Name** enthält die in der JSON-Datei definierten Node-Namen auf oberster Ebene.

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. Sie können ConfigBuilder verwenden, um sicherzustellen, dass Sie über eine gültige JSON-Datei verfügen.

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

   Die Schaltfläche **JSON-Konfiguration anwenden** ist aktiviert.



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

   Die Konfiguration wird auf den ausgewählten Knoten angewendet.

Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py

Sie können 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.

Was Sie benötigen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des StorageGRID Appliance Installer wurden Netzwerkverbindungen und IP-Adressen für den primären Administratorknoten konfiguriert.
- Wenn Sie den primären Admin-Node installieren, kennen Sie dessen IP-Adresse.
- Wenn Sie andere Knoten installieren und konfigurieren, wurde der primäre Admin-Node bereitgestellt, und Sie kennen seine IP-Adresse.
- Für alle anderen Nodes als den primären Admin-Node wurden alle auf der Seite IP-Konfiguration des Installationsprogramms der StorageGRID-Appliance aufgeführten Grid-Netzwerknetze in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- 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.

Dieses Verfahren richtet sich an fortgeschrittene Benutzer, die Erfahrung mit der Verwendung von Befehlszeilenschnittstellen haben. Alternativ können Sie die Konfiguration auch mit dem StorageGRID Appliance Installer automatisieren. +"Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer"

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`

3. Um die aktuelle Konfiguration des Appliance-Knotens zu bestätigen, geben Sie hier Folgendes ein *`SGA-install-ip`* Ist eine der IP-Adressen für den Appliance-Knoten:
   `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. #####
#####################################################################
```

4. 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`
5. Wenn Sie die Appliance-Konfiguration in einer JSON-Datei sichern möchten, verwenden Sie das `advanced` 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 diese Datei nur dann vor, wenn Sie ein erfahrener Benutzer sind und über die StorageGRID APIs verfügen.

6. 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`
7. Wenn Sie das Gerät neu starten möchten, geben Sie Folgendes ein:
   `configure-sga.py reboot SGA-INSTALL-IP`

Automatisierung der Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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.

   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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. 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 von Knotenklonen.
- **Verschlüsselung** — Operationen zur Verwaltung der Verschlüsselung und Anzeige des Verschlüsselungsstatus.
- **Hardwarekonfiguration** — Betrieb zur Konfiguration der Systemeinstellungen auf angeschlossener Hardware.
- **Installation** — Betrieb zum Starten der Gerätesallation und zur Überwachung des Installationsstatus.
- **Networking** — Vorgänge im Zusammenhang mit der Konfiguration von Grid-, Admin- und Client-Netzwerken für eine StorageGRID-Appliance und Appliance-Port-Einstellungen.
- **Setup** — Operationen zur Unterstützung bei der Ersteinrichtung der Appliance einschließlich Anfragen zum Abrufen von Informationen über das System und zur Aktualisierung der primären Admin-Node-IP.
- **Support** — Betrieb für den Neustart des Controllers und das Abrufen von Protokollen.
- **Upgrade** — Operationen im Zusammenhang mit der Aktualisierung der Appliance-Firmware.
- **Uploadsg** — Operationen zum Hochladen von StorageGRID-Installationsdateien.

Fehlerbehebung bei der Hardwareinstallation

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Verwandte Informationen

"Die Hardware-Einrichtung scheint zu hängen"

"Fehlerbehebung bei Verbindungsproblemen"

Anzeigen von Boot-Codes für den 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.

Was Sie benötigen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Wenn Sie eine kernelbasierte virtuelle Maschine (KVM) verwenden möchten, ist es Ihnen Erfahrung mit der Bereitstellung und Verwendung von KVM-Anwendungen.
- 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	• VGA-fähiger Monitor • VGA-Kabel
KVM	• KVM-Anwendung • RJ-45-Kabel
Serieller Port	• SERIELLES DB-9-Kabel • Serielles virtuelles Terminal
SOL	• 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-Management-Port her, und melden Sie sich bei der BMC Web-Schnittstelle 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 10.224.3.91 -U root -P calvin 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.
ER	Nur für Appliance-Storage-Node: Das System wartet auf die Konnektivität mit den Storage Controllern und die Synchronisierung mit dem Betriebssystem SANtricity. **Hinweis:** Wenn der Start-up-Vorgang nicht über diese Phase läuft, führen Sie folgende Schritte aus: a. Vergewissern Sie sich, dass die vier Verbindungskabel zwischen dem SG6000-CN Controller und den beiden Speichercontrollern sicher angeschlossen sind. b. Ersetzen Sie bei Bedarf ein oder mehrere Kabel, und versuchen Sie es erneut. c. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.
HZ	Das System prüft gerade auf vorhandene StorageGRID Installationsdaten.

Codieren	Zeigt An
HO	Das Installationsprogramm für StorageGRID-Appliance wird ausgeführt.
HOCHVERFÜGBARKEIT	StorageGRID wird ausgeführt.

Anzeigen von Fehlercodes für den 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.

Was Sie benötigen

- 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

Codieren	Zeigt An
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
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

Codieren	Zeigt An
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
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

Die Hardware-Einrichtung scheint zu hängen

Das Installationsprogramm von StorageGRID Appliance ist möglicherweise nicht verfügbar, wenn Hardwarefehler oder Verkabelungsfehler die Speichercontroller oder den SG6000-CN-Controller daran hindern, ihre Boot-Verarbeitung abzuschließen.

Schritte

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.

Verwandte Informationen

"Anzeigen von Boot-Statuscodes für die SG6000-Speicher-Controller"

"E5700 und E2800 – System Monitoring Guide"

"Anzeigen von Statusanzeigen und -Tasten auf dem SG6000-CN-Controller"

"Anzeigen von Boot-Codes für den SG6000-CN-Controller"

"Anzeigen von Fehlercodes für den SG6000-CN-Controller"

Fehlerbehebung bei Verbindungsproblemen

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Es konnte keine Verbindung zum Gerät 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.

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://SG6000-CN_Controller_IP:8443`

Die Startseite wird angezeigt.

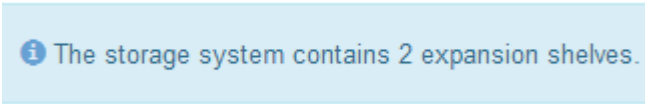
Erweiterungs-Shelfs werden nicht im Appliance Installer angezeigt

Wenn Sie Erweiterungseinschübe für das SG6060 installiert haben und diese nicht im Installationsprogramm für StorageGRID Appliance angezeigt werden, sollten Sie überprüfen, ob die Shelfs vollständig installiert und eingeschaltet wurden.

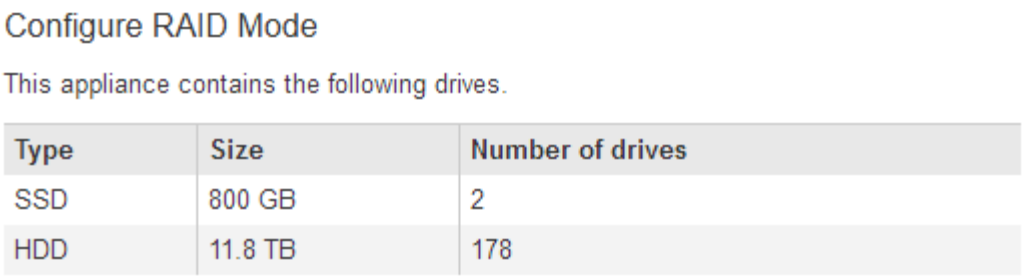
Über diese Aufgabe

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.



- 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.



Wenn die Installationsseiten der StorageGRID Appliance nicht angeben, dass Erweiterungs-Shelfs vorhanden sind, befolgen Sie diese Vorgehensweise.

Schritte

1. Vergewissern Sie sich, dass alle erforderlichen Kabel fest angeschlossen sind.
2. Stellen Sie sicher, dass Sie die Erweiterungs-Shelfs eingeschaltet haben.
3. Wenn Sie Hilfe bei der Behebung eines Problems benötigen, wenden Sie sich an den technischen Support.

Verwandte Informationen

"SG6060: Verkabelung der optionalen Erweiterungs-Shelfs"

"Anschließen von Netzkabeln und Anwenden der Stromversorgung (SG6000)"

Neustart des SG6000-CN-Controllers während des StorageGRID-Appliance-Installationsprogramms

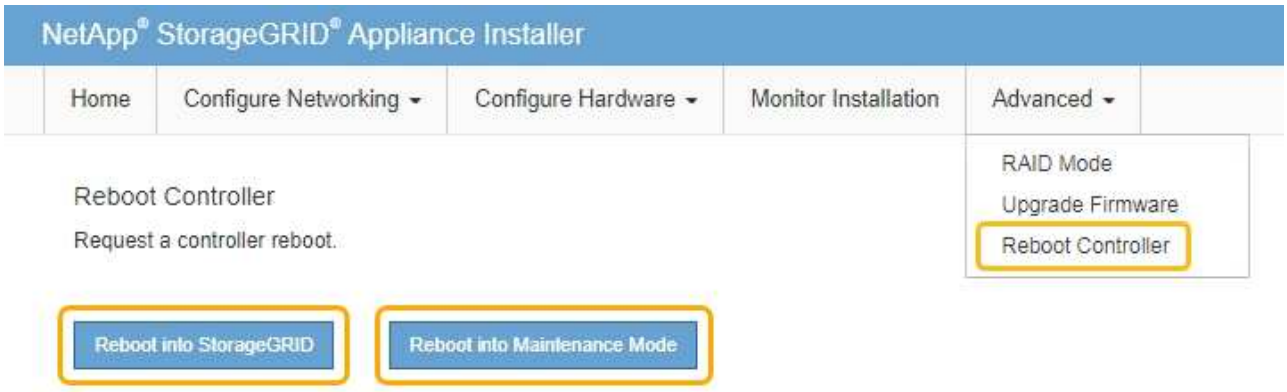
Möglicherweise müssen Sie den SG6000-CN-Controller neu starten, während das Installationsprogramm der StorageGRID-Appliance ausgeführt wird. Beispielsweise müssen Sie möglicherweise den Controller neu booten, wenn die Installation fehlschlägt.

Über diese Aufgabe

Dieses Verfahren gilt nur, wenn der SG6000-CN-Controller das Installationsprogramm der 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. Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Der SG6000-CN Controller wird neu gestartet.

Warten des SG6000-Geräts

Möglicherweise müssen Sie auf der SG6000-Appliance Wartungsarbeiten durchführen. Bei den in diesem Abschnitt beschriebenen Verfahren wird davon ausgegangen, dass die Appliance bereits als Storage-Node in einem StorageGRID-System bereitgestellt wurde.

Schritte

- "Versetzen einer Appliance in den Wartungsmodus"
- "Aktualisieren des SANtricity Betriebssystems auf den Storage Controllern"
- "Aktualisieren der Laufwerk-Firmware mit SANtricity System Manager"
- "Hinzufügen eines Erweiterungs-Shelf zu einem implementierten SG6060"
- "Durch ein- und Ausschalten des Controllers wird die LED angezeigt"
- "Lokalisierung des Controllers in einem Rechenzentrum"
- "Austauschen eines Storage Controllers"
- "Austauschen von Hardwarekomponenten im Storage-Controller-Shelf"
- "Austausch von Hardwarekomponenten in dem optionalen Erweiterungs-Shelf für 60 Laufwerke"
- "Herunterfahren des SG6000-CN Controllers"
- "Einschalten des SG6000-CN Controllers und Überprüfen des Betriebs"
- "Austauschen des SG6000-CN Controllers"
- "Ersetzen eines Netzteils im SG6000-CN-Controller"
- "Entfernen des SG6000-CN Controllers aus einem Schrank oder Rack"
- "Installieren Sie den SG6000-CN Controller wieder in ein Gehäuse oder Rack"
- "Entfernen der SG6000-CN Controller-Abdeckung"
- "Bringen Sie die Abdeckung des SG6000-CN Controllers wieder an"
- "Austauschen des Fibre-Channel-HBA im SG6000-CN-Controller"
- "Ändern der Verbindungskonfiguration des SG6000-CN Controllers"

- "Ändern der MTU-Einstellung"
- "Überprüfen der DNS-Serverkonfiguration"
- "Monitoring der Node-Verschlüsselung im Wartungsmodus"

Versetzen einer Appliance in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

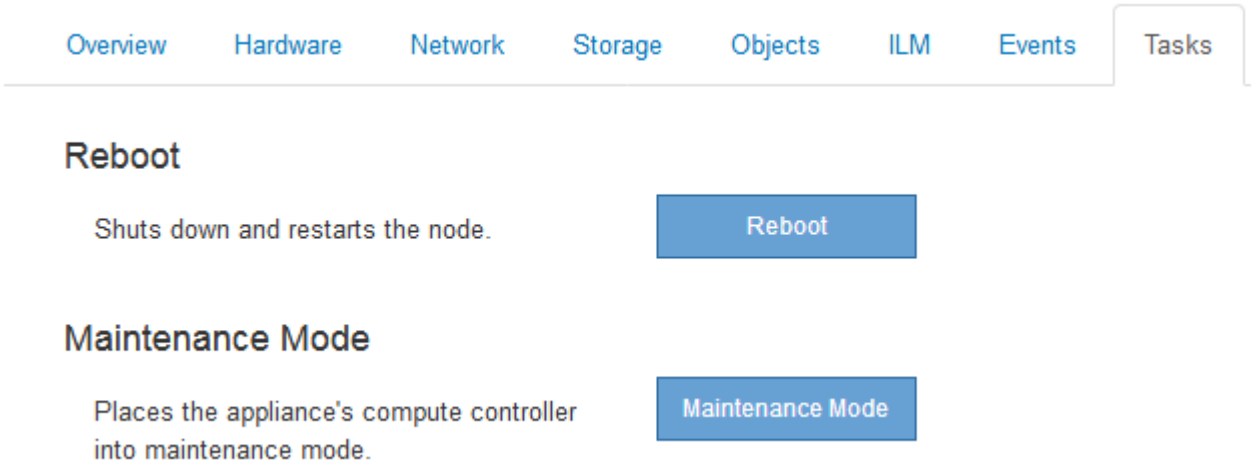
Über diese Aufgabe

Wenn Sie eine StorageGRID Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

> Das Passwort und der Hostschlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem, als das Gerät in Betrieb war.

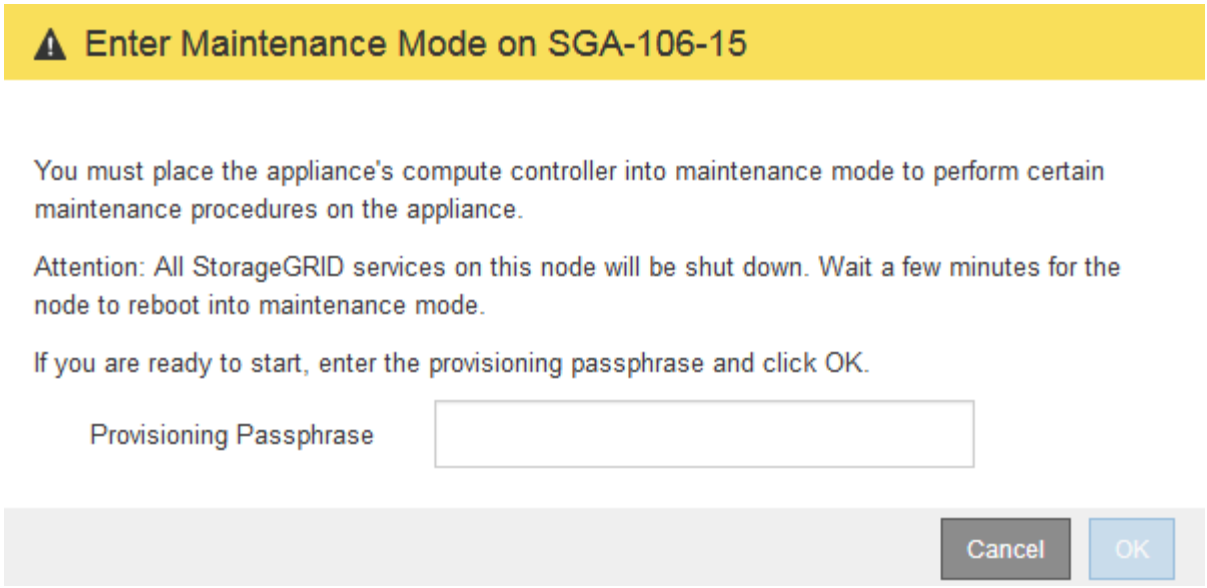
Schritte

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**.



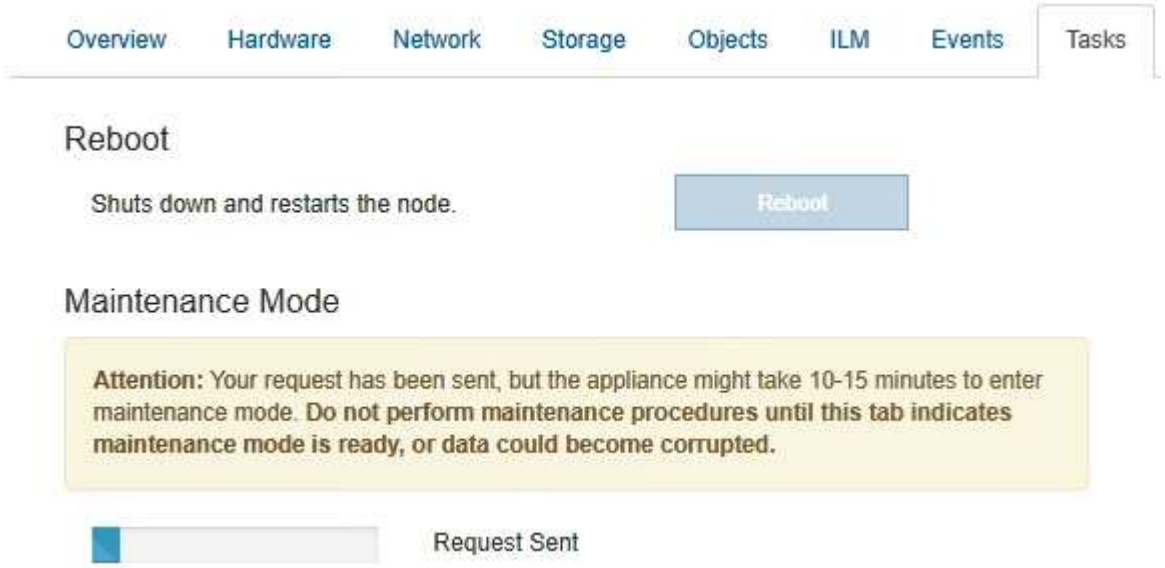
4. Wählen Sie **Wartungsmodus**.

   Ein Bestätigungsdialogfeld wird angezeigt.

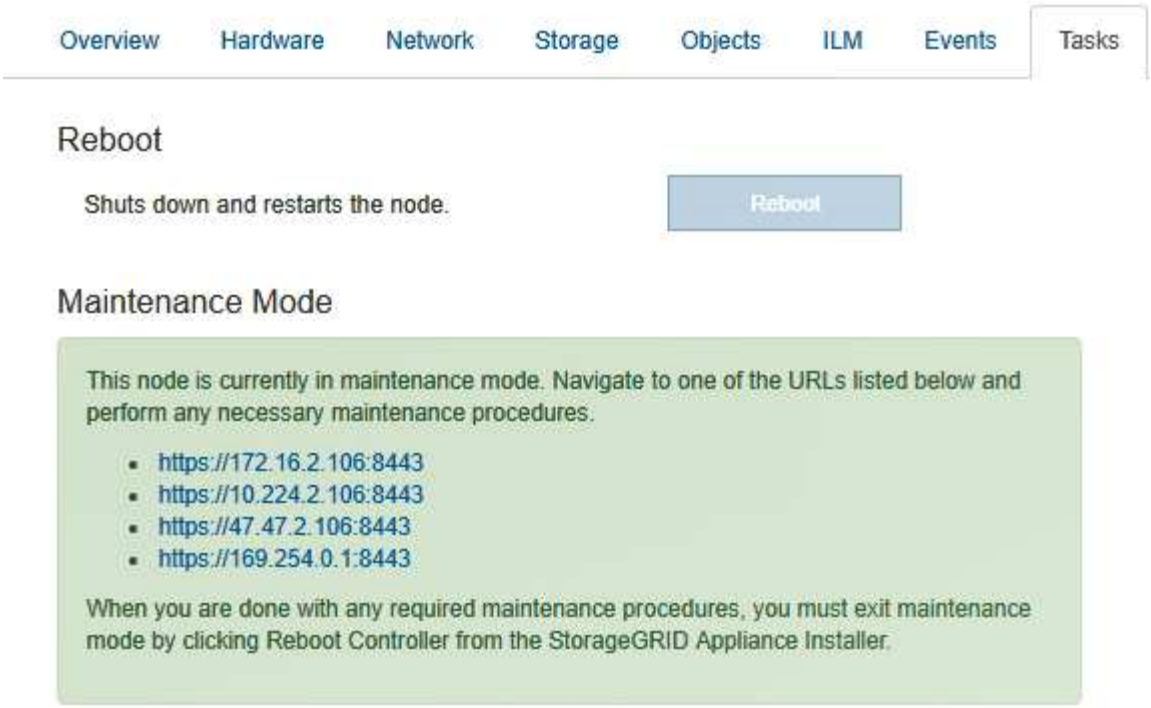


5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

   Eine Fortschrittsleiste und eine Reihe von Meldungen, einschließlich „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.



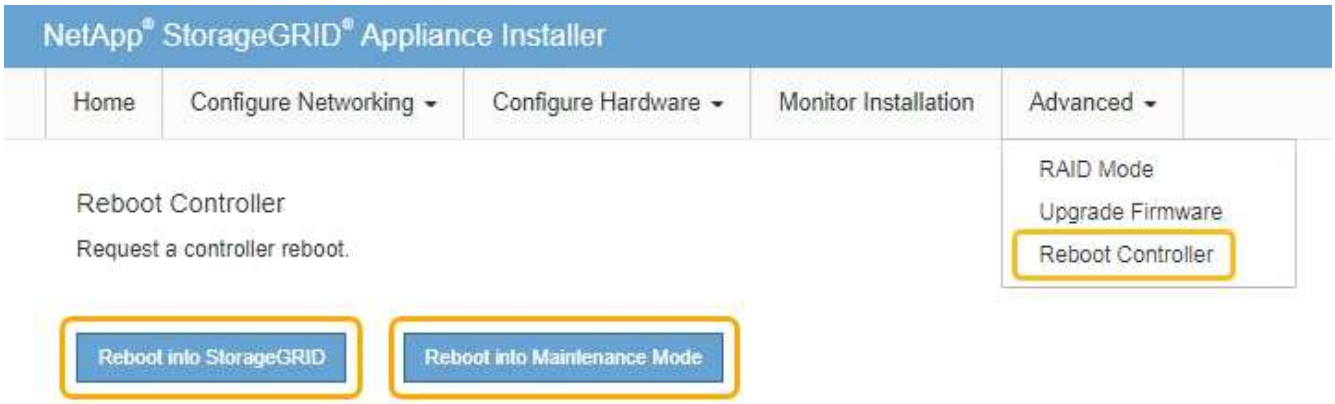
6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

   Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.

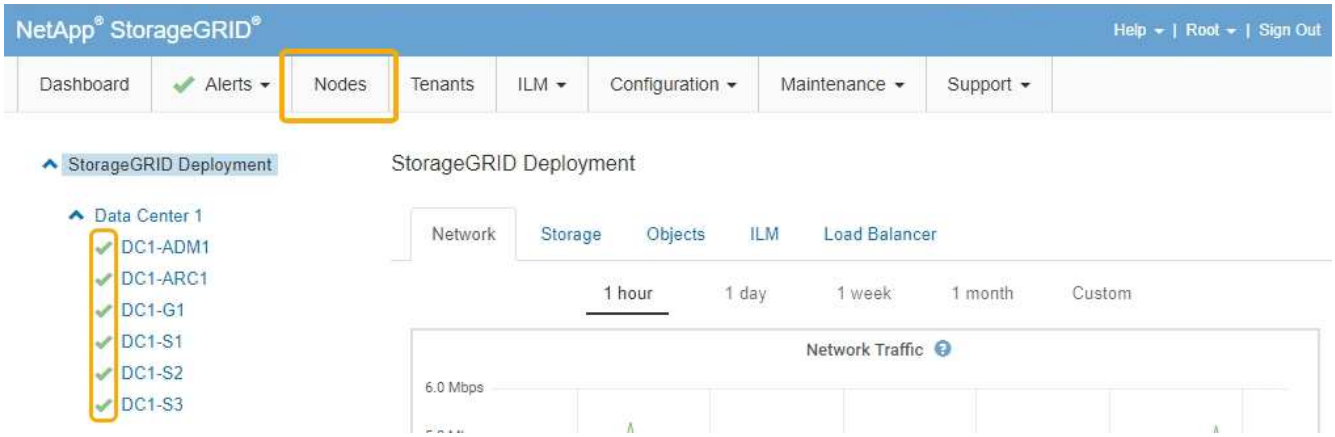
   > Zugriff Auf `https://169.254.0.1:8443` Erfordert eine direkte Verbindung zum lokalen Management-Port.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

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.



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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Aktualisieren des SANtricity Betriebssystems auf den 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. Ermitteln Sie mithilfe des NetApp Interoperabilitäts-Matrix-Tools (IMT), welche Version Sie verwenden sollten. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen.

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 von SANtricity OS auf den 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 des SANtricity OS auf den Storage Controllern mithilfe des 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.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"NetApp Downloads mit SANtricity OS"

"Monitor Fehlerbehebung"

Aktualisieren von SANtricity OS auf den 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.

Was Sie benötigen

- Sie haben das NetApp Interoperabilitäts-Matrix-Tool (IMT) konsultiert, um zu überprüfen, ob die für das Upgrade verwendete SANtricity Betriebssystemversion mit Ihrer Appliance kompatibel ist.
- Sie müssen über die Berechtigung zur Wartung verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen auf die NetApp Download-Seite für SANtricity OS zugreifen können.

Über diese Aufgabe

Sie können keine anderen Softwareupdates (StorageGRID Software-Upgrade oder Hotfix) durchführen, bis Sie den SANtricity OS-Upgrade-Prozess abgeschlossen haben. 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. Das Laden des SANtricity Betriebssystems auf jedem Node kann länger als 30 Minuten und ein Neustart jeder StorageGRID Storage Appliance bis zu 90 Minuten dauern.

Die folgenden Schritte sind nur anwendbar, wenn Sie den Grid Manager zur Durchführung des Upgrades verwenden. Die Speicher-Controller in Appliances der SG6000-Serie können nicht mit Grid Manager aktualisiert werden, wenn die Controller SANtricity OS verwenden, die älter als 08.42.20.00 sind (11.42).

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.

Schritte

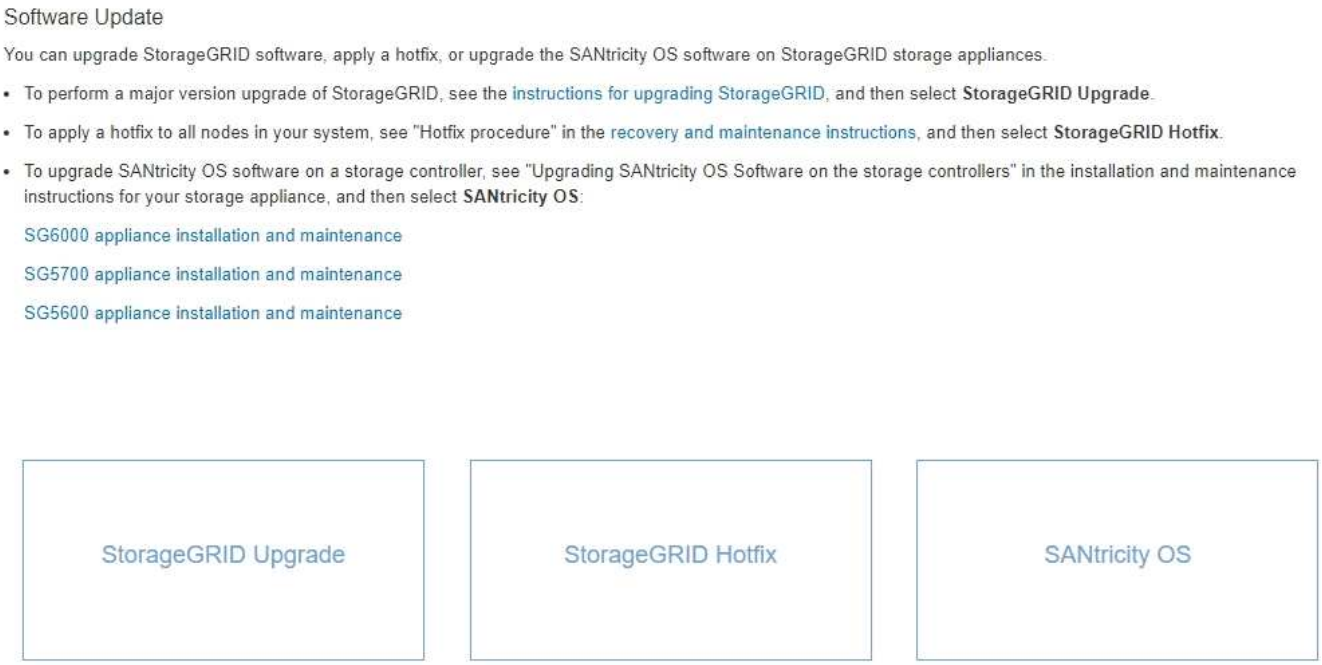
1. Laden Sie von einem Service-Laptop die neue Datei für die SANtricity OS Software von der NetApp Support Website herunter.

Stellen Sie sicher, dass Sie die richtige SANtricity Betriebssystemversion für die Storage-Controller in Ihrer Appliance auswählen. Der SG6060 verwendet den E2800 Controller, während der SGF6024 den EF570 Controller verwendet.

"NetApp Downloads mit SANtricity OS"

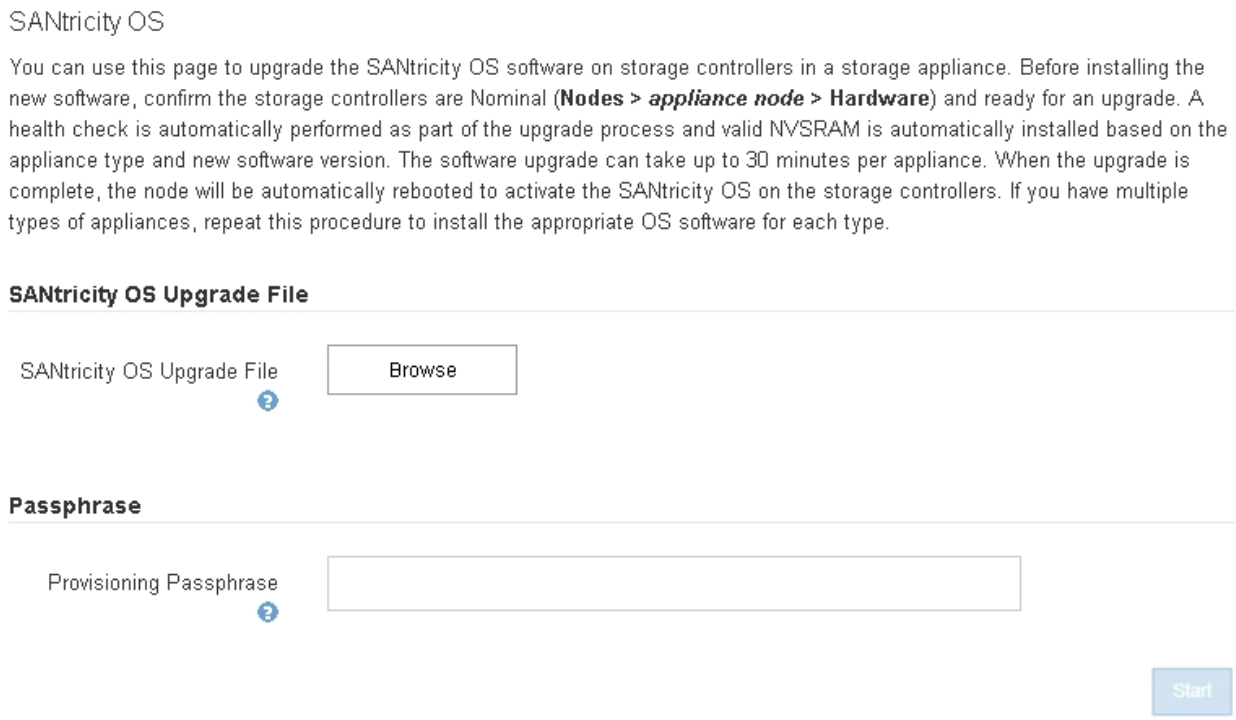
2. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
3. Wählen Sie **Wartung**. Wählen Sie dann im Bereich System des Menüs die Option **Software Update** aus.

   Die Seite Software-Aktualisierung wird angezeigt.



4. Klicken Sie auf **SANtricity OS**.

   Die Seite SANtricity OS wird angezeigt.



5. Wählen Sie die Upgrade-Datei für das SANtricity OS aus, die Sie von der NetApp Support-Website heruntergeladen haben.

   a. Klicken Sie Auf **Durchsuchen**.

   b. Suchen und wählen Sie die Datei aus.

   c. Klicken Sie Auf **Offen**.

   Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird der Dateiname im Feld Details angezeigt.

   > Ändern Sie den Dateinamen nicht, da er Teil des Verifizierungsvorgangs ist.

6. Geben Sie die Provisionierungs-Passphrase ein.

   Die Schaltfläche **Start** ist aktiviert.

7. Klicken Sie Auf **Start**.

Ein Warnfeld zeigt an, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf Knoten, die aktualisiert werden, neu gestartet werden.

8. Klicken Sie auf **OK**, um die SANtricity OS-Aktualisierungsdatei auf den primären Admin-Knoten zu stellen.

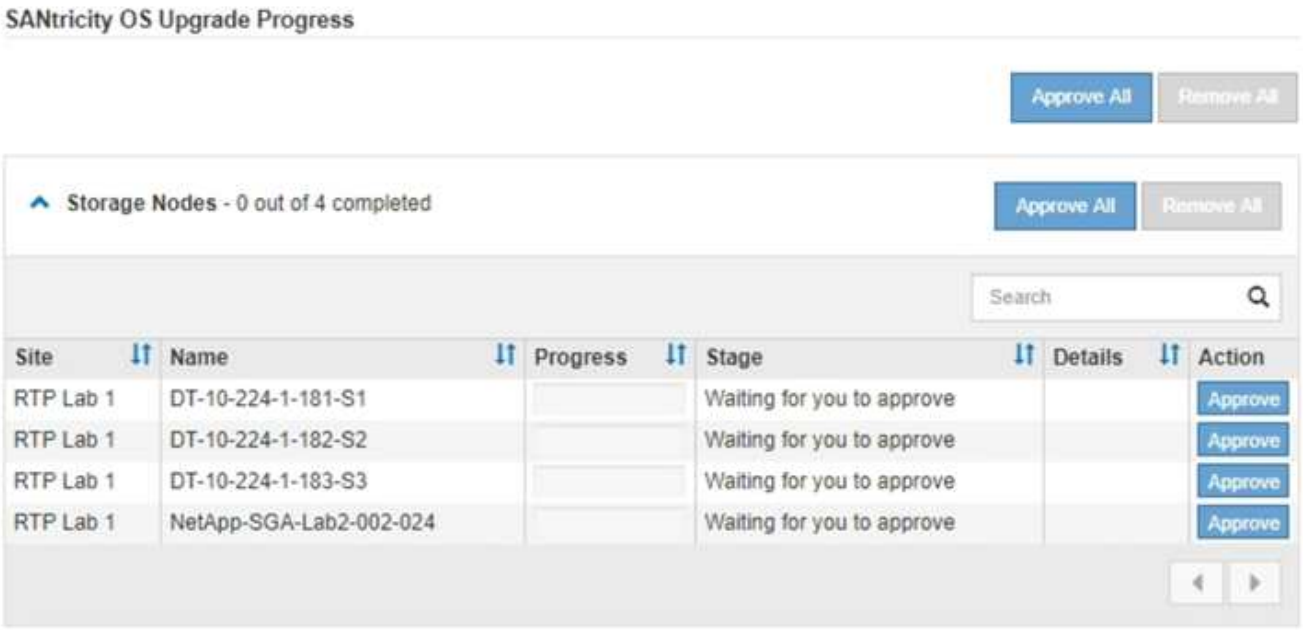
   Wenn das SANtricity OS Upgrade startet:

   a. Die Integritätsprüfung wird ausgeführt. Dieser Prozess überprüft, dass für keine Nodes der Status „Aufmerksamkeit erforderlich“ angezeigt wird.

      Wenn Fehler gemeldet werden, lösen Sie sie und klicken Sie erneut auf **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 werden alle Storage-Nodes einschließlich softwarebasierter Storage-Nodes aufgeführt. Sie müssen das Upgrade für alle Storage-Nodes genehmigen, obwohl ein Upgrade des SANtricity Betriebssystems keine Auswirkungen auf softwarebasierte Storage-Nodes hat. Die für softwarebasierte Storage-Nodes zurückgegebene Upgrade-Meldung lautet „`SANtricity OS Upgrade ist für diesen Node nicht anwendbar.`“



9. Sortieren Sie die Liste der Knoten 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.

   Sie können durch die Liste der Knoten blättern, indem Sie die Pfeile links und rechts unten rechts im Abschnitt verwenden.

10. Genehmigen Sie die Grid-Knoten, die Sie zur Upgrade-Warteschlange hinzufügen möchten. Genehmigte Nodes desselben Typs werden nacheinander aktualisiert.

Genehmigen Sie das SANtricity OS Upgrade für einen Appliance-Storage-Node nicht, es sei denn, Sie sind sicher, dass der Node bereit ist, angehalten und neu gebootet zu werden.Wenn das Upgrade des SANtricity OS auf einem Node genehmigt wird, werden die Services auf diesem Node angehalten. Wenn der Node später aktualisiert wird, wird der Appliance-Node neu gebootet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

- Klicken Sie auf eine der Schaltflächen **Alle genehmigen**, um alle Speicherknoten zur Upgrade-Warteschlange des SANtricity OS hinzuzufügen.

  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.

- Klicken Sie auf eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere Knoten zur SANtricity OS-Upgrade-Warteschlange hinzuzufügen.

  Sie können das Anwenden eines SANtricity OS Upgrades auf einen Node verzögern. Der Upgrade-Prozess für SANtricity OS ist jedoch erst abgeschlossen, wenn Sie das Upgrade von SANtricity OS auf allen aufgeführten Storage-Nodes genehmigen.

  Nach dem Klicken auf **Genehmigen** bestimmt der Upgrade-Prozess, ob der Knoten aktualisiert werden kann. Wenn ein Knoten aktualisiert werden kann, wird er der Upgrade-Warteschlange hinzugefügt. +

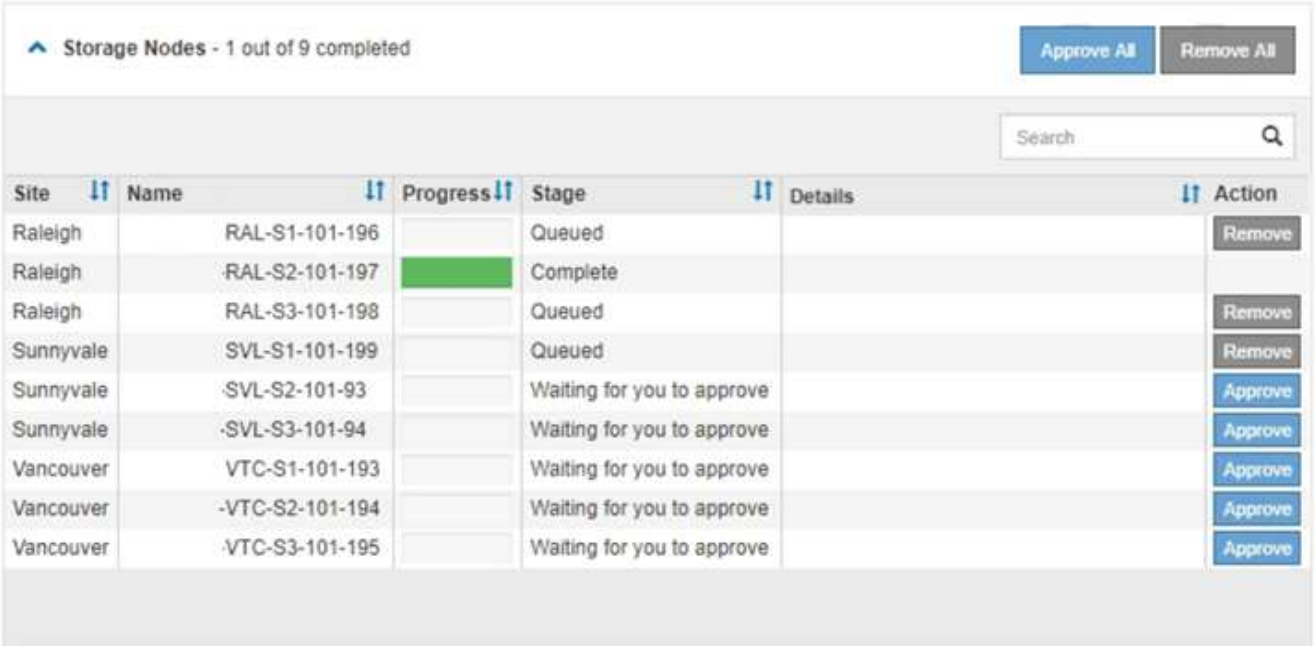
  Bei einigen Nodes wird die ausgewählte Upgrade-Datei absichtlich nicht angewendet. Sie können das Upgrade abschließen, ohne dass Sie ein Upgrade dieser spezifischen Nodes durchführen müssen. Bei Nodes, die absichtlich keine Aktualisierung durchgeführt haben, wird der Prozess mit einer der folgenden Meldungen in der Spalte Details angezeigt:

  - Storage-Node wurde bereits aktualisiert.
  - Das SANtricity OS Upgrade ist für diesen Node nicht verfügbar.
  - Die SANtricity OS-Datei ist mit diesem Node nicht kompatibel.

  Die Meldung „`SANtricity OS Upgrade ist für diesen Node` nicht verfügbar“ gibt an, dass der Node keinen Storage Controller besitzt, der vom StorageGRID System gemanagt werden kann. Diese Meldung wird für nicht-Appliance-Speicherknoten angezeigt. Sie können den Upgrade-Prozess von SANtricity OS abschließen, ohne dass ein Upgrade des Node ausgeführt wird, der diese Meldung anzeigt. + die Meldung „`SANtricity OS File is not compatible with this Node`“ gibt an, dass der Knoten eine SANtricity OS Datei erfordert, die sich von dem Prozess unterscheidet, der zu installieren versucht. Nachdem Sie das aktuelle Upgrade von SANtricity OS abgeschlossen haben, laden Sie das für den Node geeignete SANtricity OS herunter, und wiederholen Sie den Upgrade-Prozess.

11. Wenn Sie einen Knoten oder alle Knoten aus der SANtricity OS Upgrade-Warteschlange entfernen müssen, klicken Sie auf **Entfernen** oder **Alle entfernen**.

    Wie im Beispiel gezeigt, ist die **Remove**-Schaltfläche ausgeblendet, wenn die Phase über Queued hinausgeht und Sie können den Knoten nicht mehr aus dem SANtricity OS-Upgrade-Prozess entfernen.



12. Warten Sie, während das SANtricity OS Upgrade auf jeden genehmigten Grid-Node angewendet wird.

> Wenn während des SANtricity OS Upgrades auf einem beliebigen Node eine Fehlerstufe angezeigt wird, ist das Upgrade für diesen Node fehlgeschlagen. Das Gerät muss möglicherweise in den Wartungsmodus versetzt werden, um nach dem Ausfall eine Wiederherstellung durchzuführen. Wenden Sie sich an den technischen Support, bevor Sie fortfahren.

Wenn die Firmware auf dem Node zu alt ist, um ein Upgrade mit dem Grid Manager durchzuführen, zeigt der Node eine Fehlerstufe an. Die Details: „`Sie müssen den Wartungsmodus verwenden, um ein Upgrade von SANtricity OS auf diesem Node durchzuführen. Siehe Installations- und Wartungsanleitung für Ihr Gerät. Nach dem Upgrade können Sie dieses Dienstprogramm für zukünftige Upgrades verwenden.`" Gehen Sie wie folgt vor, um den Fehler zu beheben:

a. Verwenden Sie den Wartungsmodus, um ein Upgrade von SANtricity OS auf dem Node durchzuführen, auf dem eine Fehlerstufe angezeigt wird.
b. Verwenden Sie den Grid-Manager, um das SANtricity OS-Upgrade erneut zu starten und abzuschließen.

   Wenn das SANtricity OS Upgrade auf allen genehmigten Nodes abgeschlossen ist, wird die Fortschrittstabelle des SANtricity OS Upgrades geschlossen, und ein grünes Banner zeigt das Datum und die Uhrzeit des Ababgeschlossenen Upgrades des SANtricity OS an.

13. 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 des SANtricity OS auf den Storage Controllern mithilfe des Wartungsmodus"

Aktualisieren des SANtricity OS auf den Storage Controllern 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.

Was Sie benötigen

- Sie haben das NetApp Interoperabilitäts-Matrix-Tool (IMT) konsultiert, um zu überprüfen, ob die für das Upgrade verwendete SANtricity Betriebssystemversion mit Ihrer Appliance kompatibel ist.
- Wenn die StorageGRID-Appliance in einem StorageGRID-System ausgeführt wird, wurde der SG6000-CN-Controller in den Wartungsmodus versetzt.

> Im Wartungsmodus wird die Verbindung zum Storage Controller unterbrochen.

"Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Aktualisieren Sie das SANtricity Betriebssystem und NVSRAM im E-Series Controller nicht auf mehr als einer StorageGRID Appliance gleichzeitig.

> Wenn Sie mehrere StorageGRID Appliances gleichzeitig aktualisieren, kann dies in Abhängigkeit von Ihrem Implementierungsmodell und den ILM-Richtlinien zu Datenunverfügbarkeit führen.

Schritte

1. Greifen Sie über ein Service-Laptop auf den SANtricity System Manager zu und melden Sie sich an.
2. Laden Sie die neue SANtricity OS Software-Datei und die NVSRAM-Datei auf den Management-Client herunter.

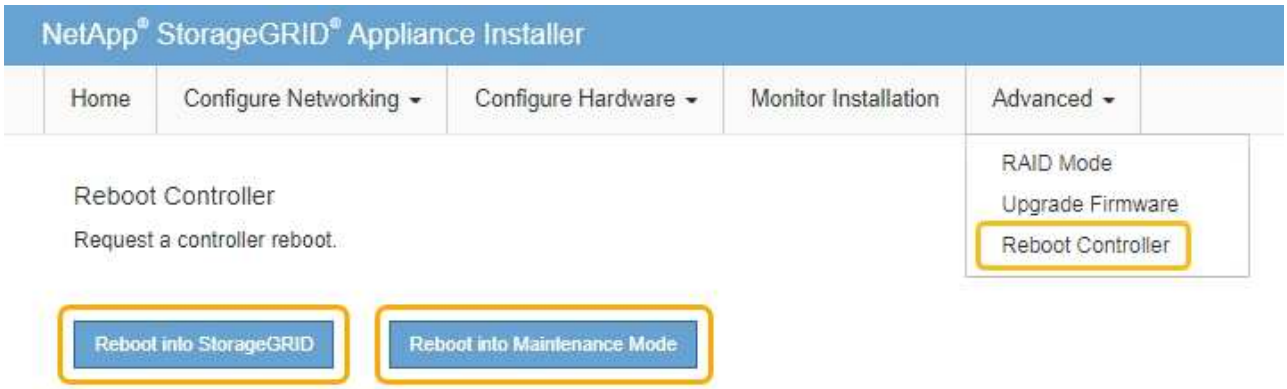
> Das NVSRAM bezieht sich auf die StorageGRID Appliance. Verwenden Sie nicht den Standard-NVSRAM-Download.

3. Folgen Sie den Anweisungen im Handbuch „ *Upgrade SANtricity OS*“ oder der Online-Hilfe von SANtricity System Manager, um die Firmware und NVSRAM zu aktualisieren.

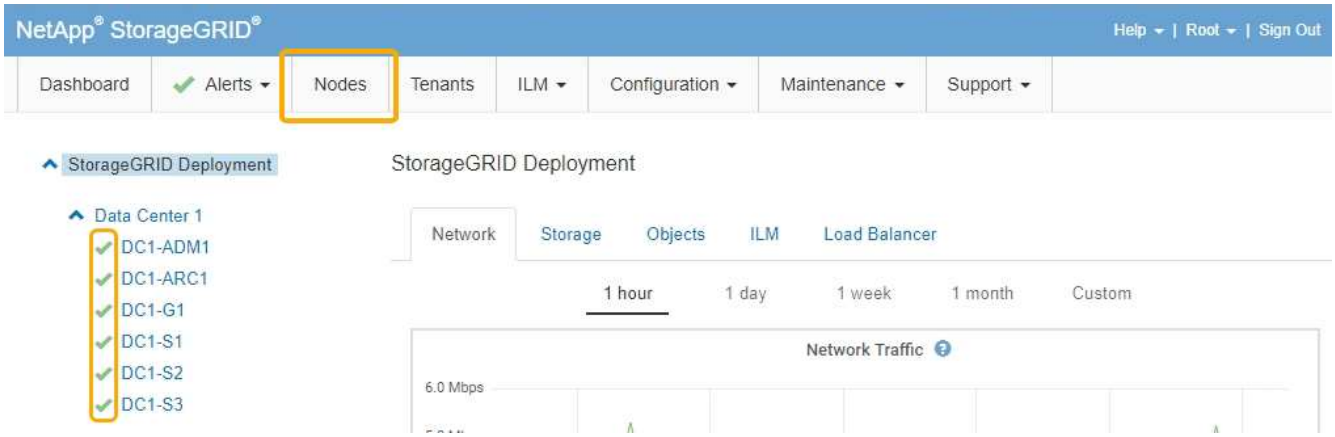
> Aktivieren Sie die Upgrade-Dateien sofort. Die Aktivierung nicht verschieben.

4. Sobald der Upgrade-Vorgang abgeschlossen ist, 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Aktualisieren von SANtricity OS auf den Storage Controllern mit Grid Manager"

Aktualisieren der Laufwerk-Firmware mit SANtricity System Manager

Sie aktualisieren Ihre Laufwerk-Firmware, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen.

Was Sie benötigen

- Die Storage Appliance hat einen optimalen Status.
- Alle Laufwerke haben einen optimalen Status.
- Die aktuelle Version von SANtricity System Manager ist mit Ihrer StorageGRID-Version kompatibel.
- Sie haben die StorageGRID-Appliance in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

> Im Wartungsmodus wird die Verbindung zum Storage Controller unterbrochen, alle I/O-Aktivitäten werden angehalten und alle Laufwerke werden offline geschaltet.

> Aktualisieren Sie die Laufwerk-Firmware nicht auf mehr als einer StorageGRID Appliance gleichzeitig. Dadurch kann je nach Implementierungsmodell und ILM-Richtlinien die Nichtverfügbarkeit von Daten auftreten.

Schritte

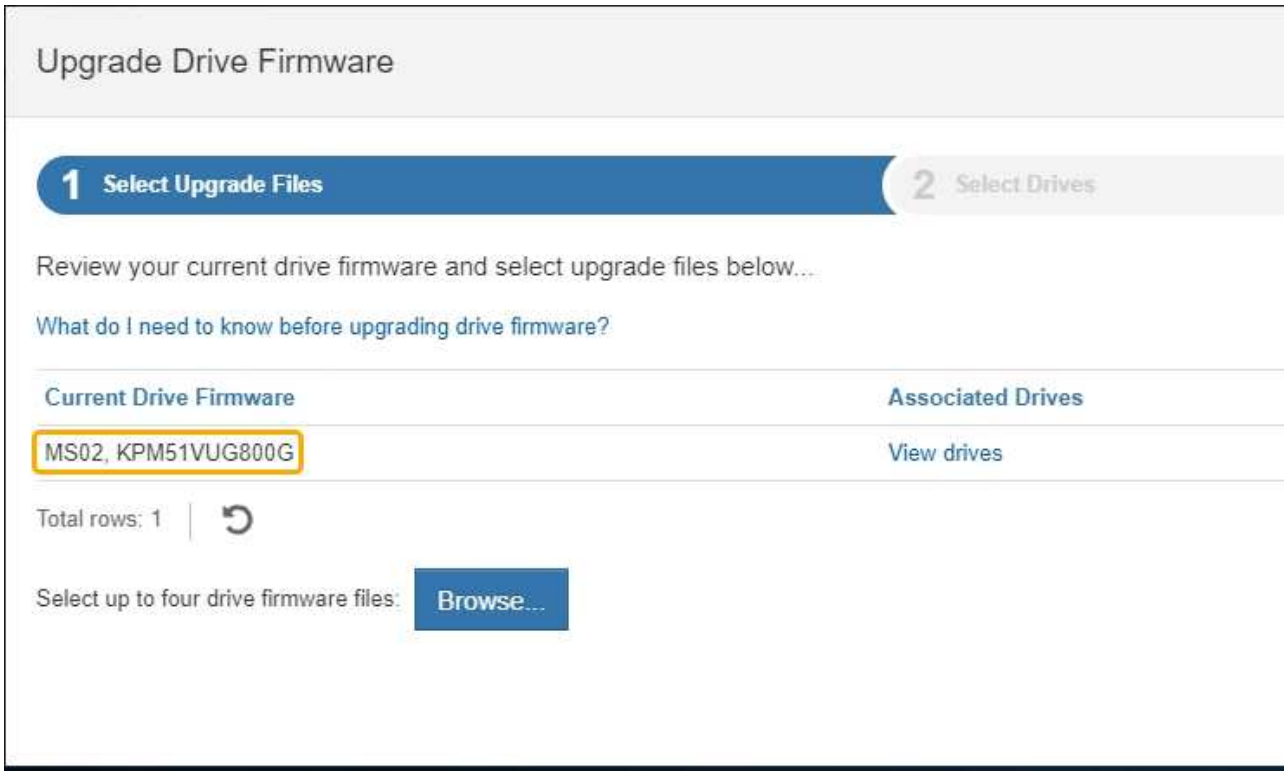
1. Greifen Sie mit einer der folgenden Methoden auf SANtricity System Manager zu:
   - Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert** > **SANtricity-Systemmanager**
   - Verwenden Sie den Grid Manager, und wählen Sie **Knoten** > ***appliance Storage Node*** > **SANtricity System Manager**

   > Wenn diese Optionen nicht verfügbar sind oder die Anmeldeseite des SANtricity System Managers nicht angezeigt wird, rufen Sie den SANtricity System Manager auf, indem Sie die Storage-Controller-IP aufrufen:
   > **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 die Option **Support** > **Upgrade Center** aus.
   b. Wählen Sie unter Laufwerk-Firmware-Upgrade die Option **Upgrade starten** aus.

      Auf der Upgrade Drive Firmware werden die zurzeit installierten Firmware-Dateien des Laufwerks angezeigt.

   c. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerkskennungen in der Spalte Aktueller Laufwerk-Firmware.



In diesem Beispiel:

- Die Version der Laufwerk-Firmware lautet **MS02**.
- Die Laufwerk-ID lautet **KPM51VUG800G**.

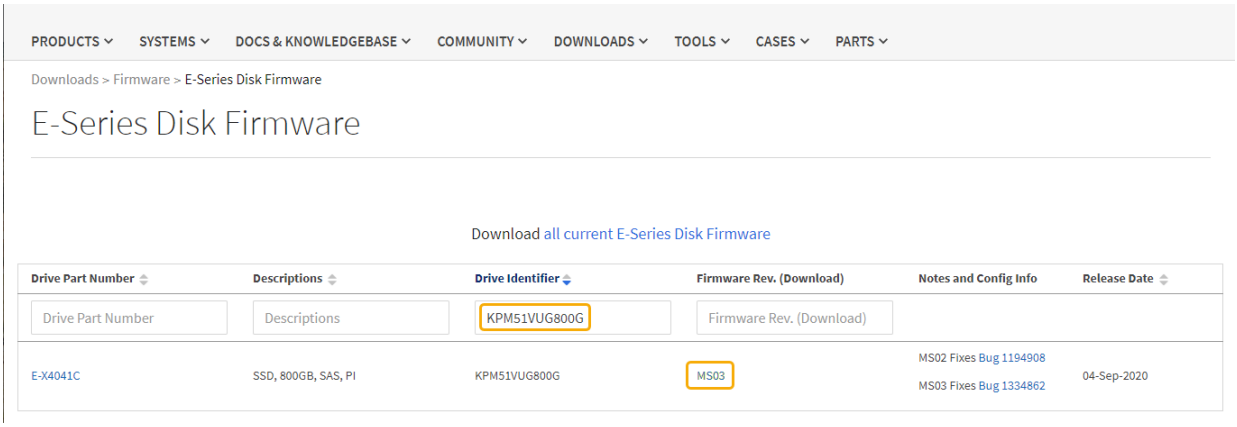
Wählen Sie in der Spalte „verbundene Laufwerke“ die Option **Laufwerke anzeigen** aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.

a. 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 Laufwerkkennung die neueste Firmware-Version hat.
      - Wenn die Firmware-Version kein Link ist, hat diese Laufwerkkennung 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.



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 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 **vorgeschlagene Firmware** angezeigt. Wenn Sie diese Firmware ändern müssen, wählen Sie **Zurück**.

d. Wählen Sie * Offline (Parallel)* Upgrade.

   Sie können die Offline-Upgrade-Methode verwenden, weil sich die Appliance im Wartungsmodus befindet, wobei I/O-Aktivitäten für alle Laufwerke und alle Volumes angehalten werden.

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`.

Wenn während des Aktualisierungsvorgangs eines der folgenden Fehler auftritt, ergreifen Sie die entsprechende empfohlene Maßnahme.

- **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 an den Controller angeschlossenen Kabel 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**

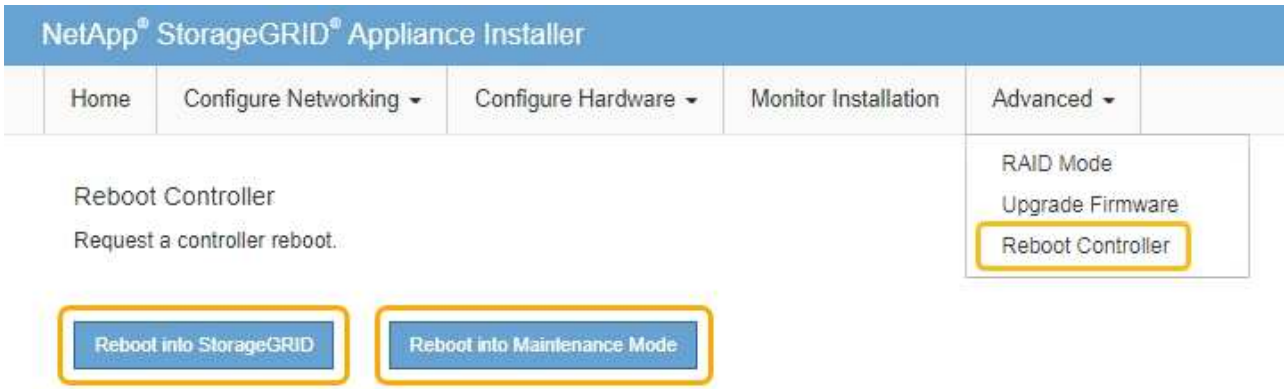
  Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Mehr als 4 kritische MEL-Einträge in den letzten 7 Tagen**

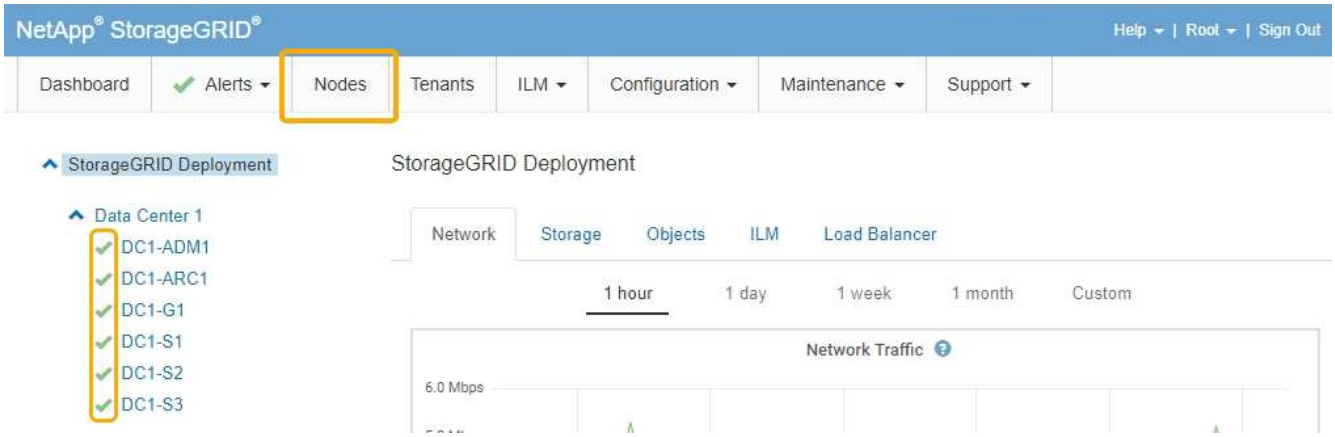
  Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

6. Starten Sie die Appliance nach Abschluss des Aktualisierungsvorgangs 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"Aktualisieren des SANtricity Betriebssystems auf den Storage Controllern"

Hinzufügen eines Erweiterungs-Shelf zu einem implementierten SG6060

Zur Erhöhung der Storage-Kapazität können einem SG6060, das in einem StorageGRID System implementiert wird, ein oder zwei Erweiterungs-Shelfs hinzugefügt werden.

Was Sie benötigen

- 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.

  "Lokalisierung des Controllers in einem Rechenzentrum"

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, um Shelfs mit 60 Laufwerken in einem Schrank oder Rack zu installieren.

   "SG6060: Installieren von Shelfs mit 60 Laufwerken in einem Schrank oder Rack"

2. Befolgen Sie die Anweisungen zur Installation der Laufwerke.

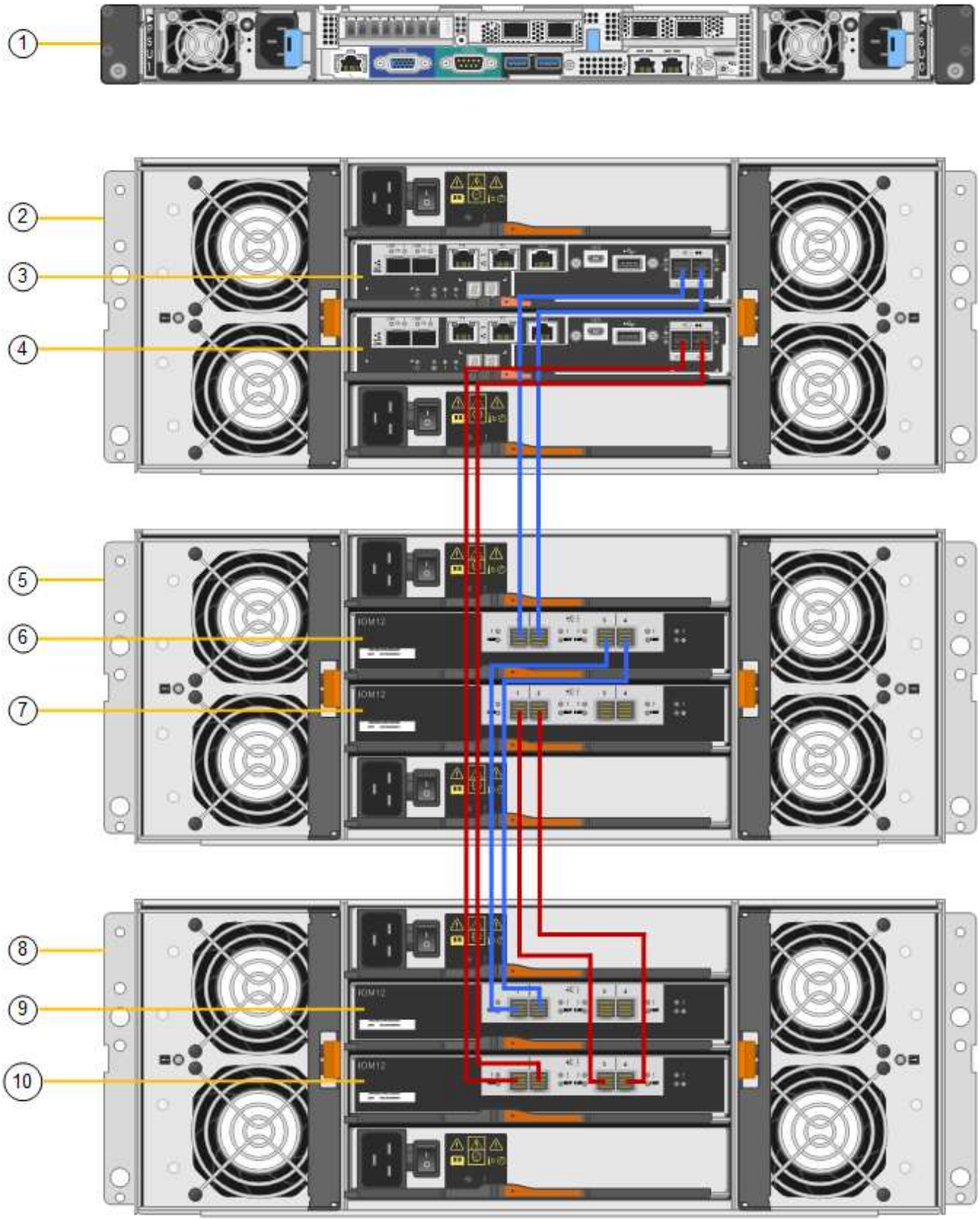
   "SG6060: Installieren der Laufwerke"

3. Versetzen Sie den SG6000-CN-Controller über den Grid Manager in den Wartungsmodus.

   "Versetzen einer Appliance 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



	Beschreibung
1	SG6000-CN

	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 Einschaltvorgangs 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-Shelfs 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.

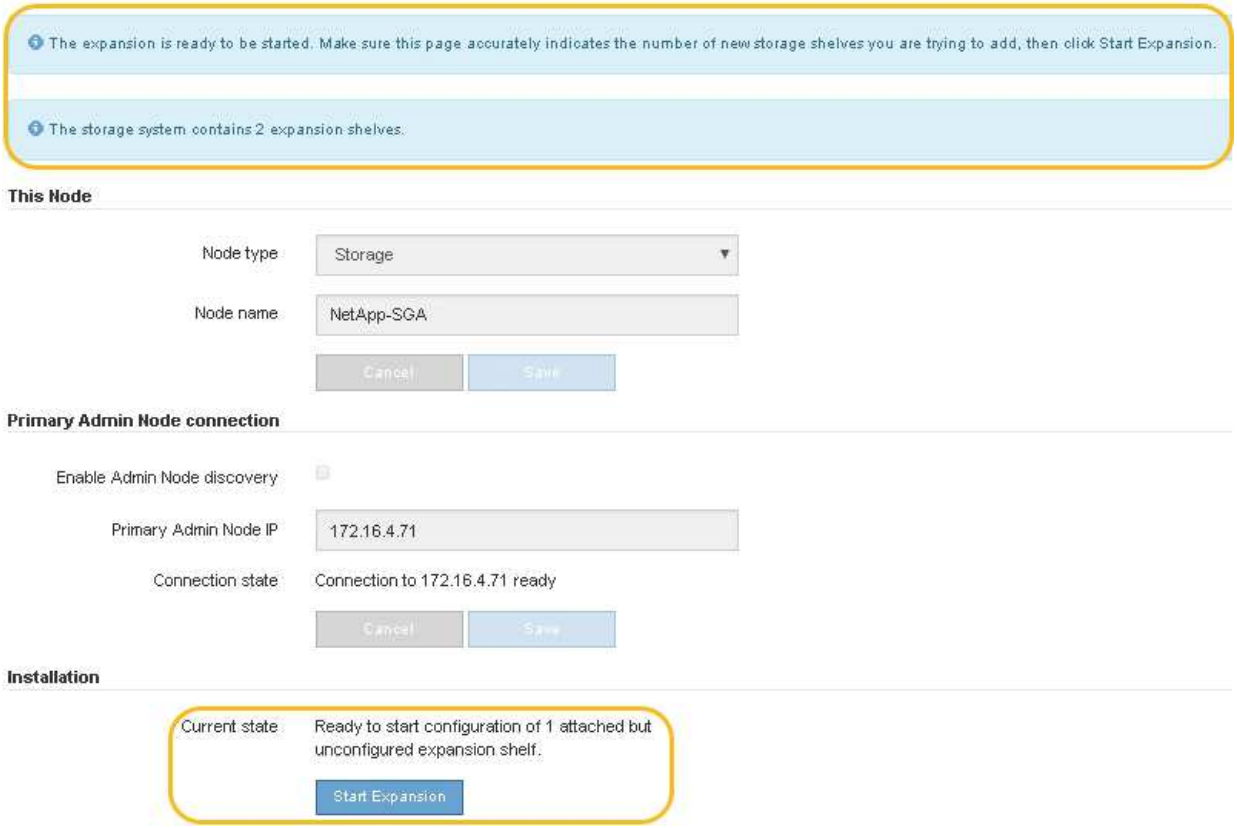
   Der Screenshot zeigt Beispiele für Meldungen, die auf der Startseite angezeigt werden können, je nach Anzahl der vorhandenen oder neuen Erweiterungs-Shelfs, wie folgt:

   - Das oben auf der Seite eingekreiste Banner zeigt die Gesamtzahl der erkannten Erweiterungs-Shelfs an.
     - Das Banner zeigt die Gesamtzahl der Erweiterungs-Shelfs an, unabhängig davon, ob die Shelfs konfiguriert und implementiert oder neu und nicht konfiguriert sind.
     - Wenn keine Erweiterungs-Shelfs 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-Shelfs 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 implementierte 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 neue Erweiterungs-Shelfs nicht erkannt werden.



7. Lösen Sie bei Bedarf alle in den Meldungen auf der Startseite beschriebenen Probleme.

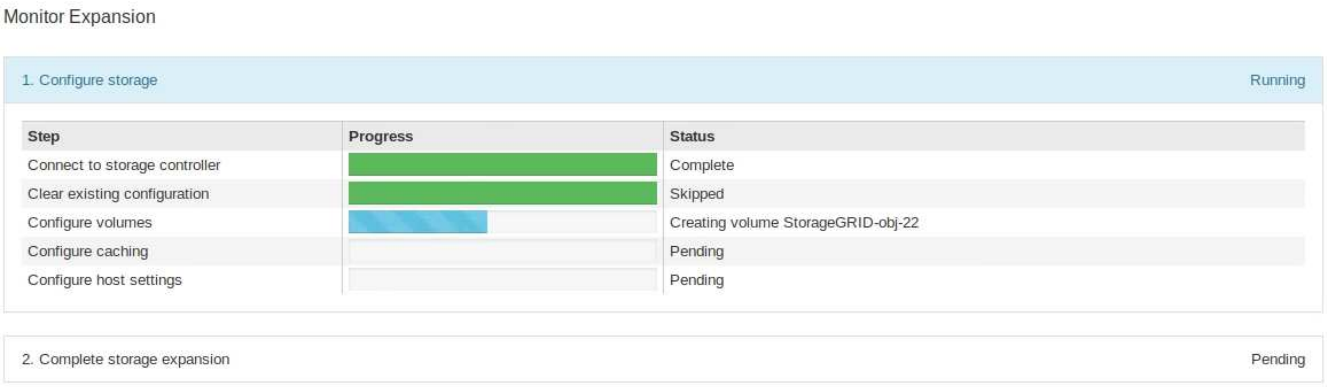
   Verwenden Sie beispielsweise den SANtricity System Manager, um alle Probleme mit der Storage-Hardware zu beheben.

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 sie für 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.



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.

> Wenn das Gerät nicht wieder in das Raster integriert wird, gehen Sie zur Startseite des StorageGRID Appliance Installer, wählen Sie **Erweitert** > **Controller neu starten** und wählen Sie dann **Neustart in den Wartungsmodus** aus.

Wenn der Neustart abgeschlossen ist, sieht die Registerkarte **Tasks** wie der folgende Screenshot aus:

11. Überprüfen Sie den Status des Appliance Storage Node und der neuen Erweiterungs-Shelfs.
    a. Wählen Sie im Grid Manager die Option **Nodes** aus, und überprüfen Sie, ob der Appliance Storage Node ein grünes Häkchen aufweist.

       Das grüne Häkchen bedeutet, dass keine Alarme aktiv sind und der Knoten mit dem Raster verbunden ist. Eine Beschreibung der Node-Symbole finden Sie in den Anweisungen für das Monitoring und die Fehlerbehebung von StorageGRID.

    b. Wählen Sie die Registerkarte **Storage** aus, und bestätigen Sie, dass in der Objektspeichertabelle für jedes hinzugefügte Erweiterungs-Shelf 16 neue Objektspeichern angezeigt werden.
    c. Vergewissern Sie sich, dass jedes neue Erweiterungs-Shelf den Shelf-Status „Nominal“ sowie den Konfigurationsstatus von „konfiguriert“ aufweist.

Storage Shelves

Shelf Chassis Serial Number	Shelf ID	Shelf Status	IOM Status	Power Supply Status	Drawer Status	Fan Status	Drive Slots	Data Drives	Data Drive Size	Cache Drives	Cache Drive Size	Configuration Status
721924500063	99	Nominal	N/A	Nominal	Nominal	Nominal	60	58	9.80 TB	2	800.17 GB	Configured (in use)
721929500038	0	Nominal	Nominal	Nominal	Nominal	Nominal	60	60	9.80 TB	0	0 bytes	Configured (in use)
721929500039	1	Nominal	Nominal	Nominal	Nominal	Nominal	60	60	9.80 TB	0	0 bytes	Configured (in use)

Verwandte Informationen

"Auspacken der Boxen (SG6000)"

"SG6060: Installieren von Shelfs mit 60 Laufwerken in einem Schrank oder Rack"

"SG6060: Installieren der Laufwerke"

"Monitor Fehlerbehebung"

Durch ein- und Ausschalten des Controllers wird die LED angezeigt

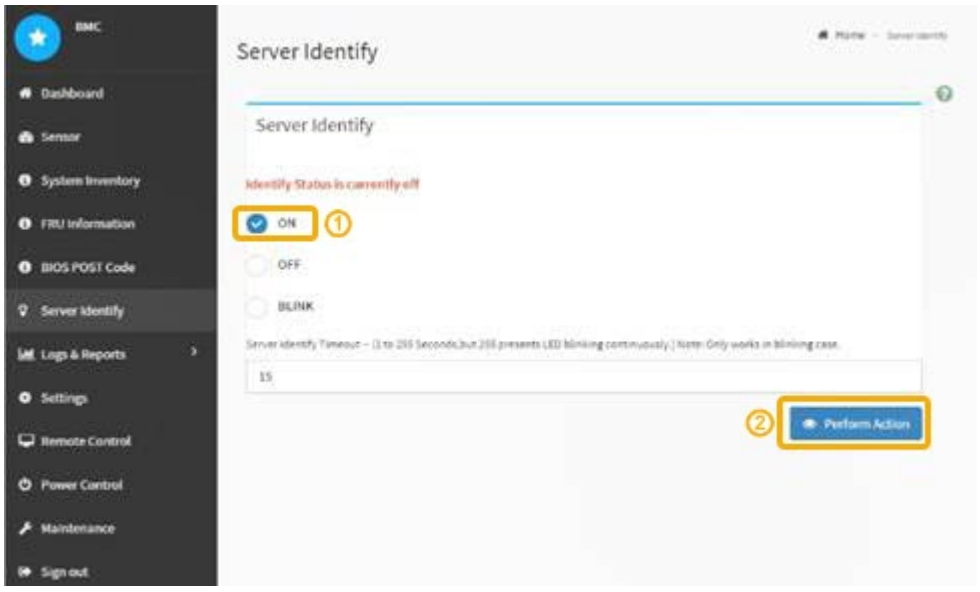
Die blaue Identify-LED auf der Vorder- und Rückseite des Controllers kann eingeschaltet werden, um das Gerät in einem Datacenter zu lokalisieren.

Was Sie benötigen

Sie müssen über die BMC-IP-Adresse des Controllers verfügen, den Sie identifizieren möchten.

Schritte

1. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.
2. Wählen Sie **Server Identify** Aus.
3. Wählen Sie **EIN** und dann **Aktion durchführen** aus.



Ergebnis

Die blaue LED-Leuchte an der Vorder- (Abbildung) und Rückseite des Controllers.

Wenn eine Blende auf dem Controller installiert ist, kann es schwierig sein, die vordere Identify-LED zu erkennen.

Nachdem Sie fertig sind

Um den Controller auszuschalten, identifizieren Sie die LED:

- Drücken Sie den Schalter Identifikation LED an der Vorderseite des Controllers.
- Wählen Sie auf der BMC-Controller-Schnittstelle **Server Identify**, wählen Sie **AUS** und dann **Aktion** ausführen.

Die blauen LEDs an der Vorder- und der Rückseite des Controllers werden ausgeschaltet.

Verwandte Informationen

"Überprüfen, ob der Fibre-Channel-HBA ausgetauscht werden soll"

"Lokalisierung des Controllers in einem Rechenzentrum"

"Zugriff auf die BMC-Schnittstelle"

Lokalisierung des Controllers in einem Rechenzentrum

Suchen Sie den Controller, um Hardware-Wartungsarbeiten oder Upgrades durchzuführen.

Was Sie benötigen

- Sie haben festgestellt, welcher Controller gewartet werden muss.

(Optional) um den Controller in Ihrem Rechenzentrum zu finden, schalten Sie die blaue Identify-LED ein.

"Durch ein- und Ausschalten des Controllers wird die LED angezeigt"

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.

     "Durch ein- und Ausschalten des Controllers wird die LED angezeigt"

Verwandte Informationen

"Entfernen des Fibre Channel HBA"

"Entfernen des SG6000-CN Controllers aus einem Schrank oder Rack"

"Herunterfahren des SG6000-CN Controllers"

Austauschen eines Storage Controllers

Möglicherweise müssen Sie einen E2800 Controller oder einen EF570 Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Was Sie benötigen

- 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 verfügen über die Anweisungen für den Austausch eines Controllers in der Duplexkonfiguration.

> Beachten Sie nur bei der Anleitung zur E-Series oder wenn Sie weitere Details für einen bestimmten Schritt benötigen. Verlassen Sie sich beim Austausch eines Controllers in der StorageGRID Appliance nicht auf die Anweisungen der E-Series, da sich die Verfahren nicht unterscheiden.

- Sie haben die Storage Appliance physisch gefunden, an der der Controller im Datacenter ausgetauscht wird.

  "Lokalisierung des Controllers in einem Rechenzentrum"

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.

Da das Storage-Controller-Shelf zwei Storage-Controller enthält, können Sie einen der Controller ersetzen, während das System eingeschaltet ist und Lese-/Schreibvorgänge durchführen, 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 mit „Yes“ angezeigt, dass diese Komponente sicher entfernt werden kann.

> Wenn der zweite Controller-Behälter im Regal keinen optimalen Status hat oder wenn der Recovery Guru angibt, dass es nicht in Ordnung ist, den Controller-Behälter 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.

> Die Storage Controller im Gerät enthalten keine Host-Schnittstellenkarten (HIC).

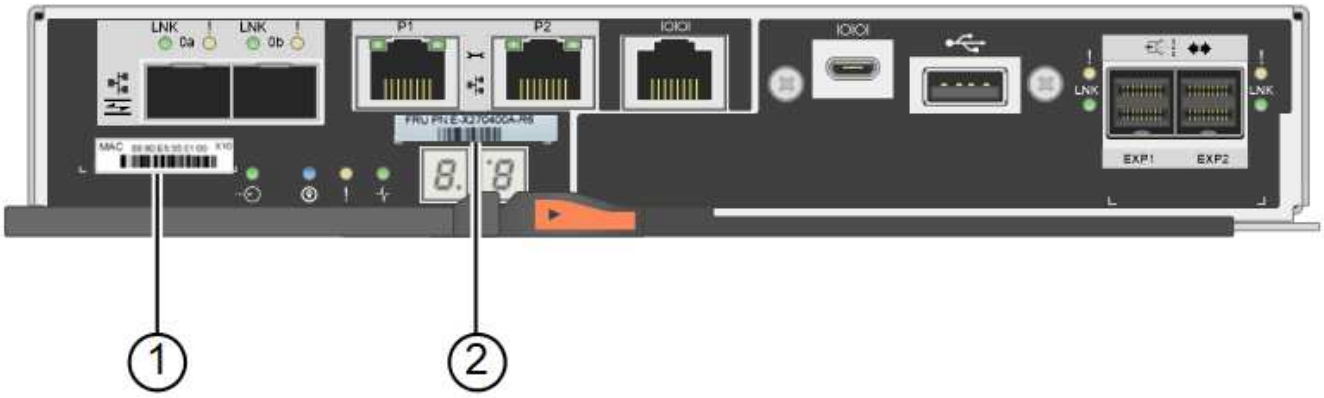
Schritte

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 Abbildung zeigt den E2800 Controller. Das Verfahren zum Austausch des EF570 Controllers ist identisch.



Etikett	Etikett	Beschreibung
1	MAC-Adresse	Die MAC-Adresse für Management-Port 1 („`P1`"). Wenn Sie die IP-Adresse des Original-Controllers über DHCP erhalten haben, benötigen Sie diese Adresse, um eine Verbindung zum neuen Controller herzustellen.
2	FRU-Teilenummer	Die FRU-Teilenummer. Diese Nummer muss der Teilenummer des derzeit installierten Controllers entsprechen.

3. Bereiten Sie das Entfernen des Controllers vor.

   Sie führen die folgenden Schritte mit SANtricity System Manager aus. Weitere Informationen finden Sie in der E-Series Anleitung zum Austauschen des Storage Controllers.

   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 Datenzugangs -- Wenn die beiden Teilenummern nicht gleich sind, versuchen Sie dieses Verfahren nicht.

   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

Das Erfassen von Supportdaten vor und nach dem Ersetzen einer Komponente stellt sicher, dass Sie einen vollständigen Satz von Protokollen an den technischen Support senden können, falls das Problem durch den Austausch nicht behoben wird.

c. Nehmen Sie den Controller, den Sie ersetzen möchten, in den Offline-Modus.

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 eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht 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.

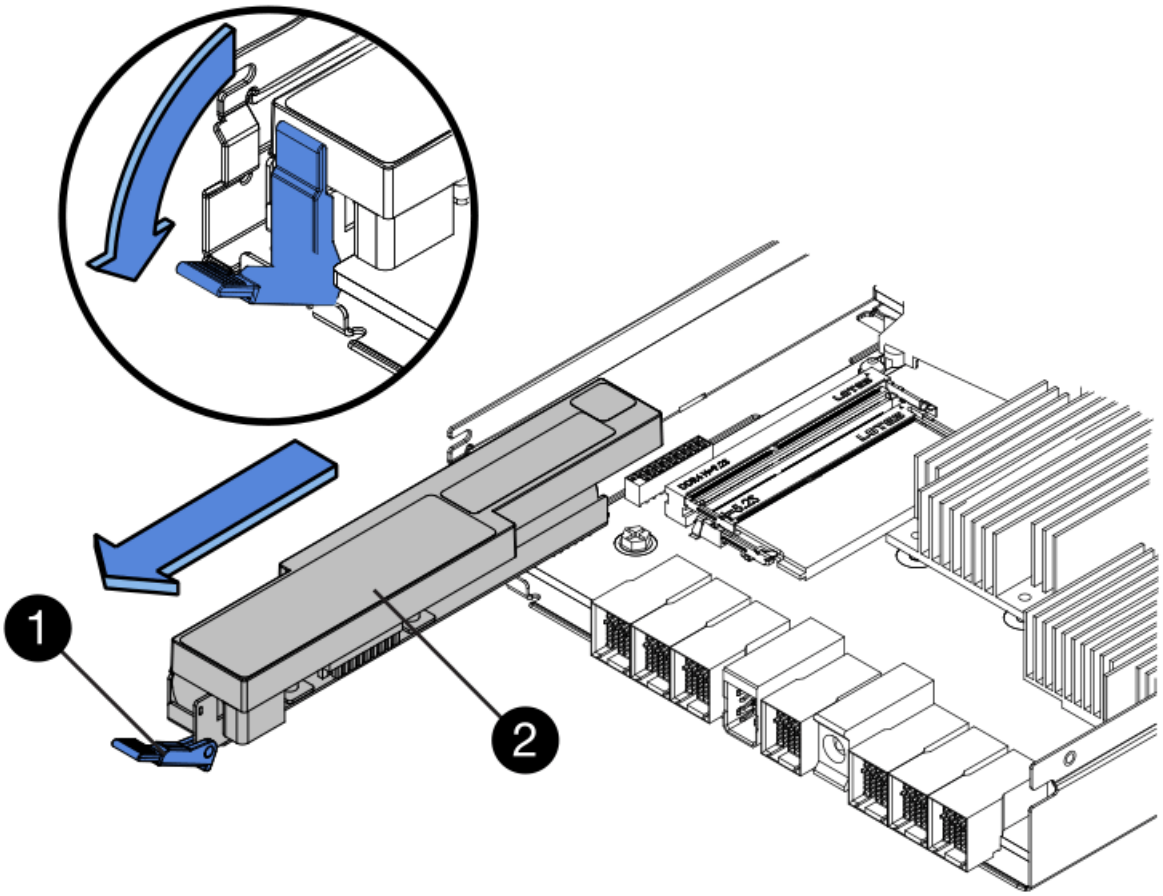
   e. Stellen Sie den Controller auf eine flache, statische Oberfläche, wobei die abnehmbare Abdeckung nach oben zeigt.
   f. Entfernen Sie die Abdeckung, indem Sie die Taste nach unten drücken und die Abdeckung abnehmen.
5. Entfernen Sie den Akku aus dem ausgefallenen Controller, und setzen Sie ihn in den Ersatzcontroller ein:
   a. 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

b. Suchen Sie den blauen Freigabehebel für die Batterie.

c. Entriegeln Sie den Akku, indem Sie den Entriegelungshebel nach unten und aus dem Controller entfernen.



Element	Beschreibung
	Akkufreigaberiegel
	Batterie

d. Heben Sie den Akku an, und schieben Sie ihn aus dem Controller.

e. Entfernen Sie die Abdeckung vom Ersatzcontroller.

f. Richten Sie den Ersatz-Controller so aus, dass der Steckplatz für die Batterie zu Ihnen zeigt.

g. 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.

h. Schieben Sie die Akkuverriegelung nach oben, um die Batterie zu sichern.

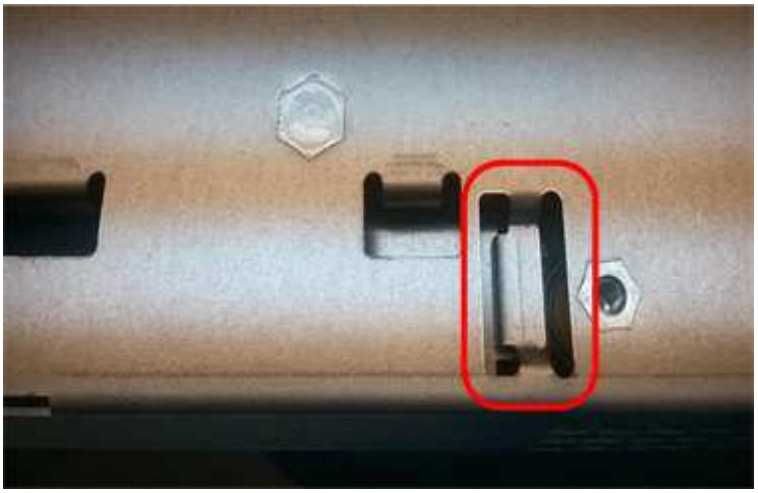
   Wenn die Verriegelung einrastet, Haken unten an der Verriegelung in einen Metallschlitz am Gehäuse.

i. 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 komplett in den Schlitz am Controller eingelegt:**

- **Falsch — der Metallflansch der Batterie ist nicht in den Steckplatz an der Steuerung eingefügt:**



j. Bringen Sie die Controllerabdeckung wieder an.

6. 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. 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.

7. 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`.
8. Vergewissern Sie sich, dass der neue Controller optimal ist, und sammeln Sie Support-Daten.

Verwandte Informationen

"NetApp E-Series Systems Documentation Site"

Austauschen von Hardwarekomponenten im Storage-Controller-Shelf

Wenn ein Hardwareproblem auftritt, müssen Sie möglicherweise eine Komponente im Storage-Controller-Shelf ersetzen.

Was Sie benötigen

- 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.

  "Lokalisierung des Controllers in einem Rechenzentrum"

Über diese Aufgabe

Informationen zum Austauschen des Akkus im Speicher-Controller finden Sie in den Anweisungen zum Austauschen eines Speichercontrollers. 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: • Laufwerk austauschen (60 Laufwerke) • Auswechseln des Laufwerks (12 Laufwerke oder 24 Laufwerke)

FRU	Siehe Anweisungen
Leistungsbehälter	E-Series • Ersetzen Sie den Netzbehälter (60 Laufwerke). • Ersetzen Sie das Netzteil (12 oder 24 Laufwerke).
Lüfterbehälter (nur Shelfs mit 60 Laufwerken)	E-Series: Lüfterbehälter ersetzen (60 Laufwerke)
Laufwerkseinschub (nur Shelfs mit 60 Laufwerken)	E-Series: Auswechseln der Laufwerkschublade (60 Laufwerke)

Verwandte Informationen

"NetApp E-Series Systems Documentation Site"

"Austauschen eines Storage Controllers"

Austausch von Hardwarekomponenten in dem optionalen Erweiterungs-Shelf für 60 Laufwerke

Möglicherweise müssen Sie ein ein ein-/Ausgabemodul, ein Netzteil oder einen Lüfter im Erweiterungs-Shelf ersetzen.

Was Sie benötigen

- 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.

  "Lokalisierung des Controllers in einem Rechenzentrum"

Über diese Aufgabe

Um ein Input/Output-Modul (IOM) in einem Erweiterungs-Shelf mit 60 Laufwerken zu ersetzen, lesen Sie die Anweisungen in diesen Anleitungen zum Austauschen eines Storage-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).
Gebläsebehälter	Lüfterbehälter austauschen (60 Laufwerke)

Herunterfahren des SG6000-CN Controllers

Fahren Sie den SG6000-CN-Controller herunter, um die Hardware zu warten.

Was Sie benötigen

- Der SG6000-CN Controller ist physisch zu finden, der im Datacenter gewartet werden muss.

  "Lokalisierung des Controllers in einem Rechenzentrum"

- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Um Serviceunterbrechungen zu vermeiden, bestätigen Sie, dass alle anderen Storage-Nodes mit dem Grid verbunden sind, bevor Sie den Controller herunterfahren oder den Controller während eines geplanten Wartungsfensters herunterfahren, wenn normalerweise Zeiträume der Serviceunterbrechung erwartet werden. Informationen zum Bestimmen von Knotenverbindungsstatus finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

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. Wenn das Gerät in den Wartungsmodus versetzt wurde, fahren Sie den SG6000-CN-Controller herunter:

   Sie müssen das Herunterfahren des Controllers steuern, indem Sie die unten angegebenen Befehle eingeben. Wenn Sie den Controller mit dem Netzschalter herunterfahren, führt dies zu Datenverlust.

   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:

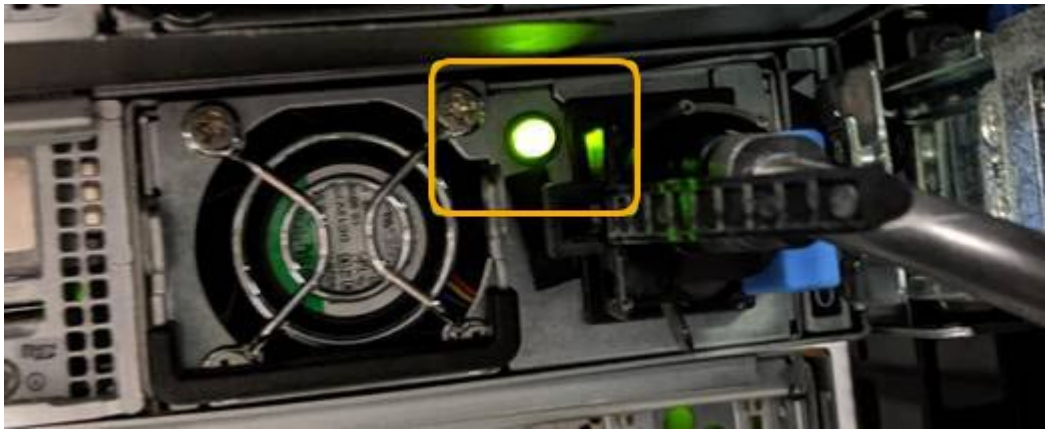
      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

   b. 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.

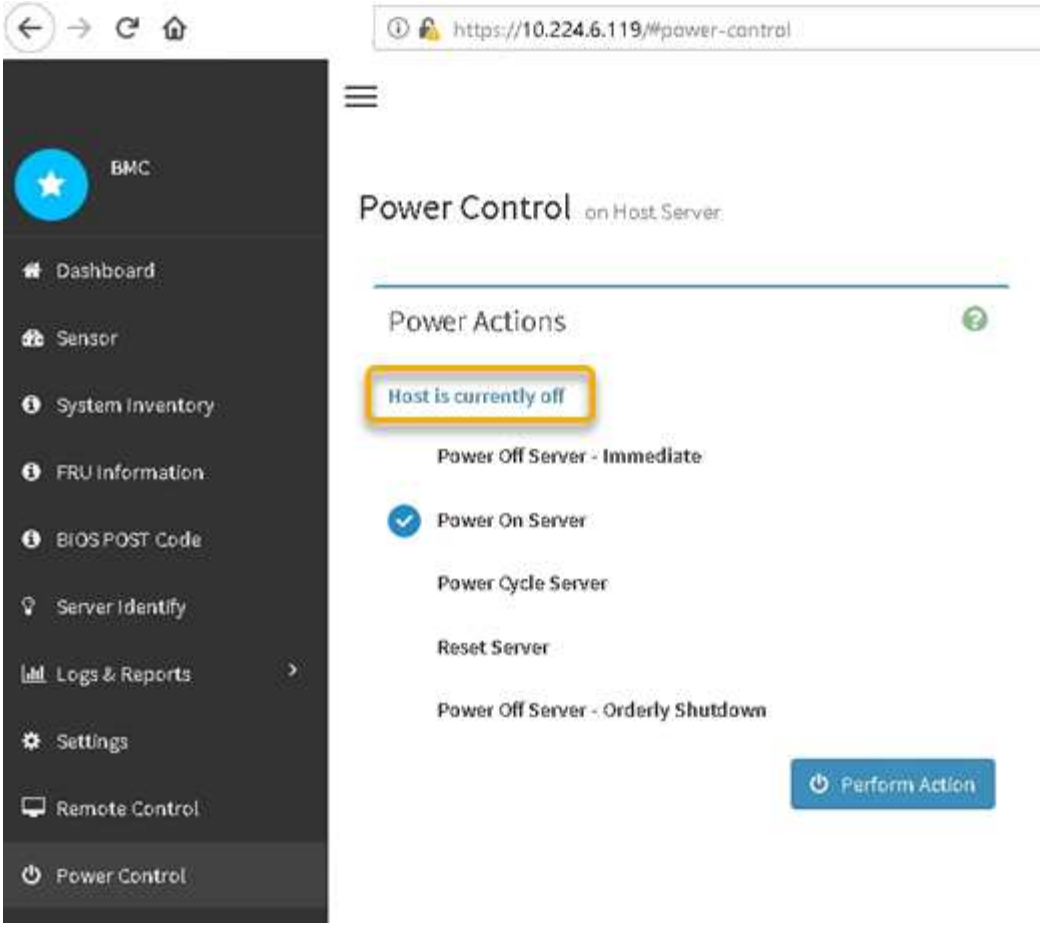
- Schauen Sie sich die grünen LEDs an den beiden Netzteilen auf der Rückseite des Controllers an und bestätigen Sie, dass sie mit einer normalen Geschwindigkeit (etwa ein Blinken pro Sekunde) blinken.



- Verwenden Sie die BMC-Schnittstelle des Controllers:
  i. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.

     "Zugriff auf die BMC-Schnittstelle"

  ii. Wählen Sie **Power Control**.
  iii. Stellen Sie sicher, dass die Strommaßnahmen darauf hindeuten, dass der Host derzeit ausgeschaltet ist.



Verwandte Informationen

"Entfernen des SG6000-CN Controllers aus einem Schrank oder Rack"

Einschalten des SG6000-CN Controllers und Überprüfen des Betriebs

Schalten Sie den Controller nach dem Abschluss der Wartung ein.

Was Sie benötigen

- Der Controller wurde in einem Rack oder Rack installiert und die Daten- und Stromkabel angeschlossen.

  "Installieren Sie den SG6000-CN Controller wieder in ein Gehäuse oder Rack"

- Der Controller befindet sich physisch im Datacenter.

  "Lokalisierung des Controllers in einem Rechenzentrum"

Schritte

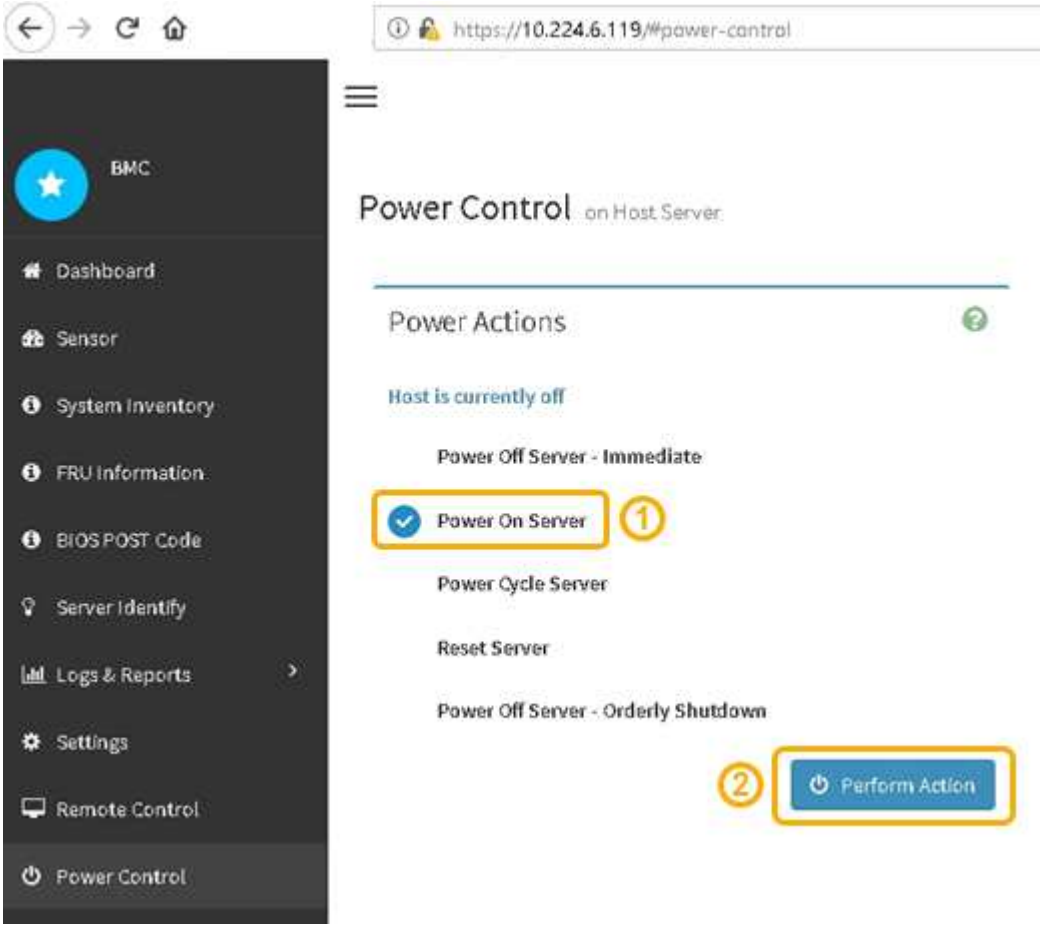
1. Schalten Sie den SG6000-CN-Controller ein, und überwachen Sie die Controller-LEDs und den Startcode mithilfe einer der folgenden Methoden:

   - 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.

     "Zugriff auf die BMC-Schnittstelle"

  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
   ```

   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 Gbit16 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 keinen anderen Appliance-Node offline, es sei denn, dieses Gerät verfügt über ein grünes Symbol.

4. Optional: Befestigen Sie die Frontverkleidung, falls eine entfernt wurde.

Verwandte Informationen

"Anzeigen von Statusanzeigen und -Tasten auf dem SG6000-CN-Controller"

"Anzeigen von Boot-Statuscodes für die SG6000-Speicher-Controller"

Austauschen des SG6000-CN Controllers

Möglicherweise müssen Sie den SG6000-CN-Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Was Sie benötigen

- 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.

  "Lokalisierung des Controllers in einem Rechenzentrum"

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. Während Sie von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm für StorageGRID-Geräte zugreifen können, können Sie 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. Wenn der SG6000-CN-Controller ausreichend funktioniert, um ein kontrolliertes Herunterfahren zu ermöglichen, fahren Sie den SG6000-CN-Controller herunter.

   "Herunterfahren des SG6000-CN Controllers"

   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. Überprüfen Sie anhand einer von zwei Methoden, ob die Stromversorgung für den SG6000-CN-Controller ausgeschaltet ist:
   - Die Betriebsanzeige-LED an der Vorderseite des Controllers leuchtet nicht.
   - Die Seite Power Control der BMC-Schnittstelle zeigt an, dass der Controller aus ist.
3. Wenn die mit dem Controller verbundenen StorageGRID-Netzwerke DHCP-Server verwenden, aktualisieren Sie die Einstellungen für DNS/Netzwerk und IP-Adresse.

   a. Suchen Sie das MAC-Adressenetikett auf der Vorderseite des SG6000-CN-Controllers und legen Sie die MAC-Adresse für den Admin-Netzwerkanschluss fest.

Auf dem MAC-Adressenetikett wird die MAC-Adresse für den BMC-Verwaltungsport aufgelistet. + 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.

b. Bitten Sie den Netzwerkadministrator, die DNS/Netzwerk- und IP-Adresse des entfernten Controllers mit der MAC-Adresse des Ersatzcontrollers zu verknüpfen.

Sie müssen sicherstellen, dass alle 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.

Wenn der ursprüngliche Controller statische IP-Adresse verwendet hat, übernimmt der neue Controller automatisch die IP-Adressen des entfernten Controllers.

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 eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht 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. Vergewissern Sie sich, dass der Appliance Storage Node im Grid Manager angezeigt wird und keine Alarme angezeigt werden.
6. Wählen Sie im Grid Manager **Nodes** aus, und überprüfen Sie, ob die BMC-IP-Adresse für den Knoten-Controller korrekt ist.

   Wenn die Node-Controller-IP-Adresse ungültig ist oder sich nicht im erwarteten Bereich befindet, konfigurieren Sie die IP-Adresse gemäß den Recovery- und Wartungsanweisungen neu.

   "Verwalten Sie erholen"

Verwandte Informationen

"SG6000-CN: Einbau in einen Schrank oder Rack"

"Anzeigen von Statusanzeigen und -Tasten auf dem SG6000-CN-Controller"

"Anzeigen von Boot-Codes für den SG6000-CN-Controller"

Ersetzen eines Netzteils im SG6000-CN-Controller

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.

Was Sie benötigen

- Sie haben das Ersatznetzteil entpackt.
- Sie befinden sich physisch auf dem Controller, an dem das Netzteil im Datacenter ersetzt wird.

  "Lokalisierung des Controllers in einem Rechenzentrum"

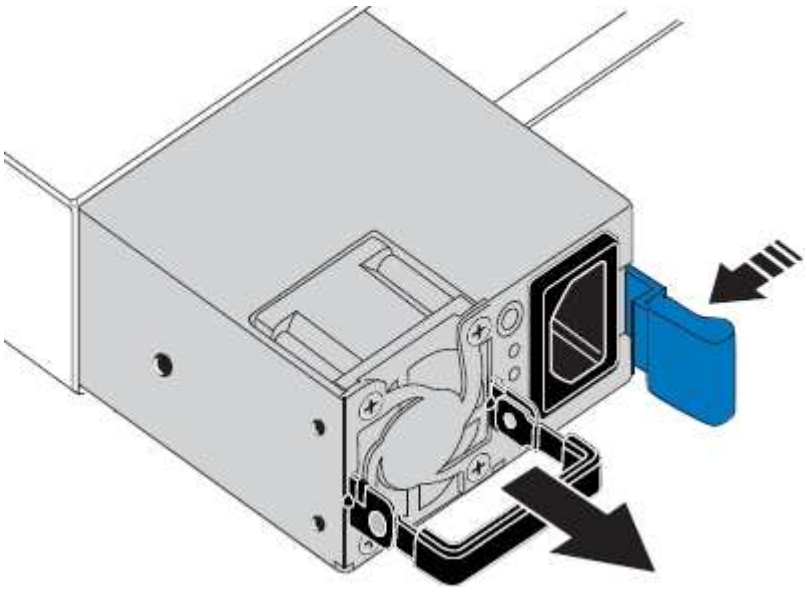
- Sie haben bestätigt, dass das andere Netzteil installiert ist und in Betrieb ist.

Über diese Aufgabe

Die Abbildung zeigt die beiden Netzteile des SG6000-CN Controllers, auf die über die Rückseite des Controllers zugegriffen werden kann.

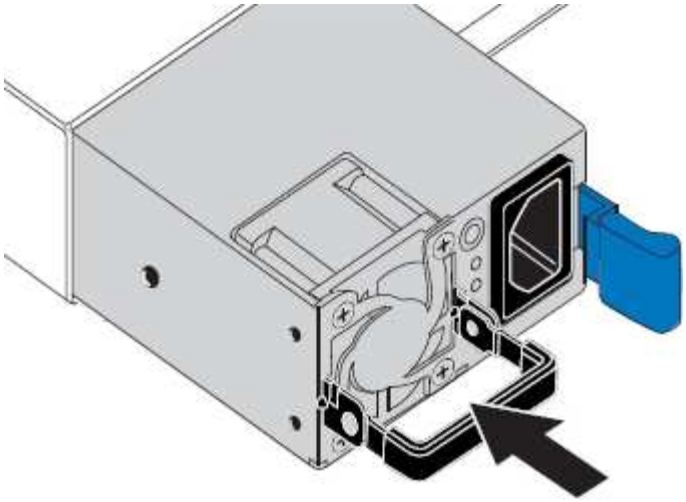
Schritte

1. Ziehen Sie das Netzkabel vom Netzteil ab.
2. Heben Sie den Nockengriff an.
3. Drücken Sie auf den blauen Riegel, und ziehen Sie das Netzteil heraus.



4. Schieben Sie das Ersatznetzteil in das Gehäuse.

   Stellen Sie sicher, dass sich der blaue Riegel auf der rechten Seite befindet, wenn Sie das Gerät einschieben.



5. Drücken Sie den Nockengriff nach unten, um die Stromversorgung zu sichern.
6. Schließen Sie das Netzkabel an das Netzteil an, und stellen Sie sicher, dass die grüne LED leuchtet.

Entfernen des SG6000-CN Controllers aus einem 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.

Was Sie benötigen

- 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.

  "Lokalisierung des Controllers in einem Rechenzentrum"

- Sie haben den SG6000-CN-Controller heruntergefahren.

  "Herunterfahren des SG6000-CN Controllers"

  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 eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht 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.

Verwandte Informationen

"Entfernen der SG6000-CN Controller-Abdeckung"

Installieren Sie den SG6000-CN Controller wieder in ein Gehäuse oder Rack

Setzen Sie den Controller nach Abschluss der Hardwarewartung in ein Rack oder Rack ein.

Was Sie benötigen

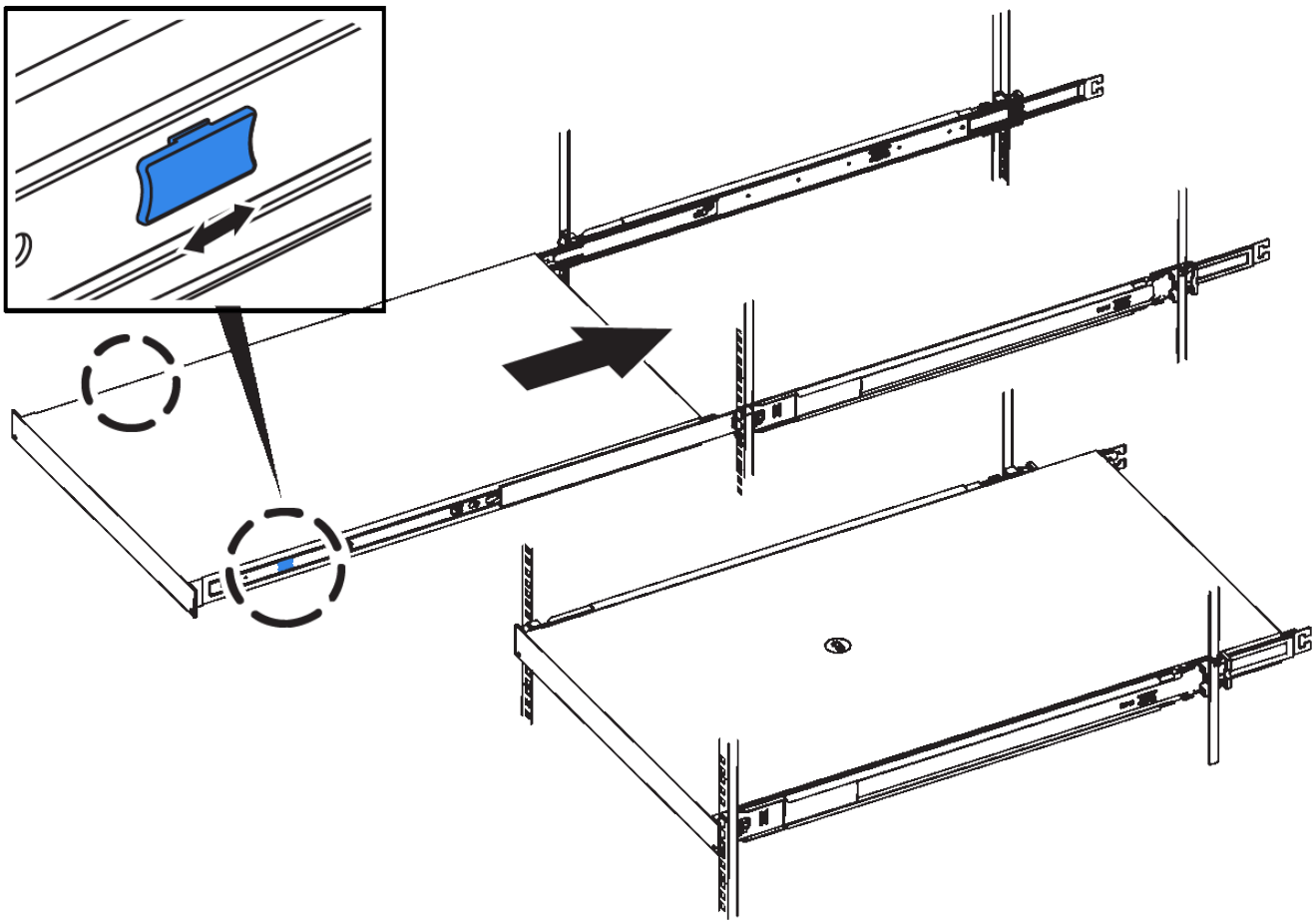
Sie haben die Controller-Abdeckung wieder installiert.

"Bringen Sie die Abdeckung des SG6000-CN Controllers 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 mehr bewegen können, ziehen Sie die blauen Verriegelungen auf beiden Seiten des Chassis, um den Controller nach innen zu schieben.



Befestigen Sie die Frontverkleidung erst, wenn 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 eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht oder treten.

"Verkabeln des Geräts (SG6000)"

5. Schließen Sie die Controller-Stromkabel wieder an.

"Anschließen von Netzkabeln und Anwenden der Stromversorgung (SG6000)"

Nachdem Sie fertig sind

Der Controller kann neu gestartet werden.

"Einschalten des SG6000-CN Controllers und Überprüfen des Betriebs"

Entfernen der SG6000-CN Controller-Abdeckung

Entfernen Sie die Controllerabdeckung, um zu Wartungszwecken auf interne Komponenten zuzugreifen.

Was Sie benötigen

Entfernen Sie den Controller aus dem Schrank oder Rack, um auf die obere Abdeckung zuzugreifen.

"Entfernen des SG6000-CN Controllers aus einem 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.

Verwandte Informationen

"Entfernen des Fibre Channel HBA"

Bringen Sie die Abdeckung des SG6000-CN Controllers wieder an

Setzen Sie die Controllerabdeckung wieder ein, wenn die interne Hardwarewartung abgeschlossen ist.

Was Sie benötigen

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 ein Gehäuse oder Rack"

Austauschen des Fibre-Channel-HBA im SG6000-CN-Controller

Möglicherweise müssen Sie den Fibre-Channel-Hostbus-Adapter (HBA) im SG6000-CN-Controller ersetzen, wenn dieser nicht optimal funktioniert oder wenn er ausgefallen ist.

Überprüfen, ob der Fibre-Channel-HBA ausgetauscht 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.

Was Sie benötigen

- Sie haben die Seriennummer der Speicher-Appliance oder SG6000-CN-Controller, wo der Fibre Channel HBA ersetzt werden muss.

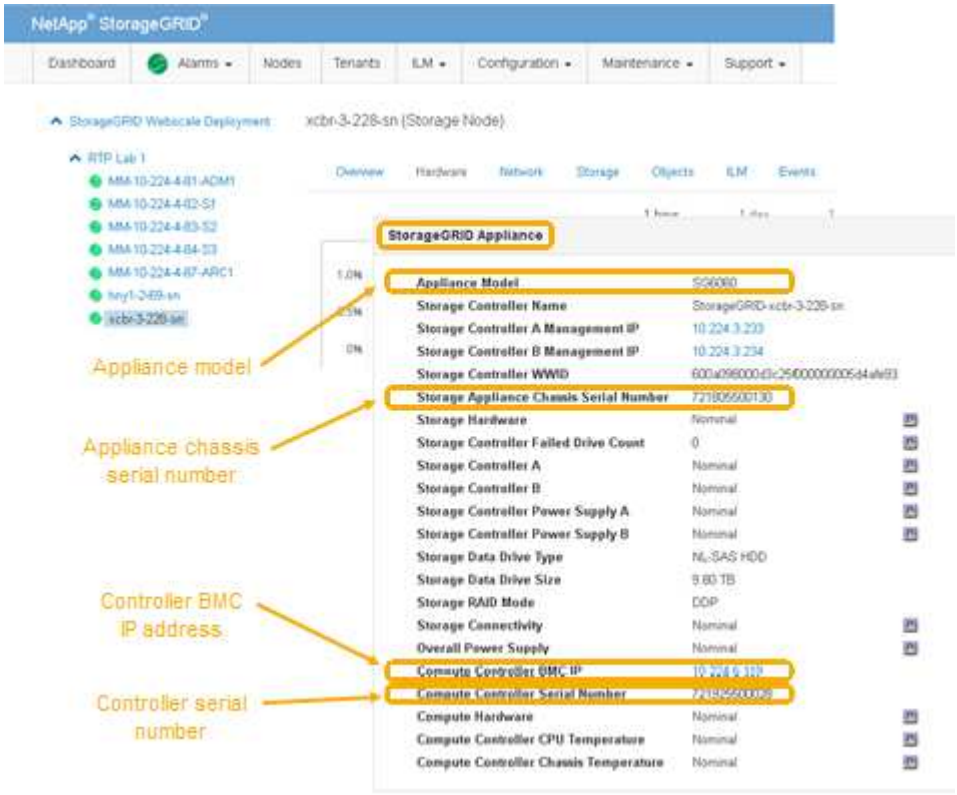
> Wenn die Seriennummer der Speicheranwendung, die den Fibre-Channel-HBA enthält, den Sie ersetzen, mit dem Buchstaben Q beginnt, wird sie nicht im Grid Manager aufgeführt. Sie müssen die an der Vorderseite der einzelnen SG6000-CN-Controller im Rechenzentrum angebrachten Tags überprüfen, bis Sie eine Übereinstimmung finden.

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie im Grid Manager die Option **Nodes** aus.
2. Wählen Sie auf der Seite Knoten in der Strukturansicht einen Appliance-Speicherknoten aus.
3. Wählen Sie die Registerkarte **Hardware** aus.

   Überprüfen Sie die Seriennummer des Storage Appliance Chassis und die Seriennummer des Compute Controller im Abschnitt StorageGRID Appliance, um zu ermitteln, ob eine dieser Seriennummern der Seriennummer der Storage Appliance entspricht, an der Sie den Fibre Channel HBA austauschen. Wenn eine der Seriennummern übereinstimmt, haben Sie die richtige Appliance gefunden.



   - 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 ist, wählen Sie einen anderen Knoten aus der Strukturansicht aus.
   - Wenn die Seriennummern nicht übereinstimmen, wählen Sie in der Strukturansicht einen anderen Knoten 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.

   "Durch ein- und Ausschalten des Controllers wird die LED angezeigt"

Verwandte Informationen

"Entfernen des Fibre Channel HBA"

Entfernen des 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.

Was Sie benötigen

- Sie haben den richtigen Fibre Channel HBA für den Austausch.
- Sie haben festgestellt, welcher SG6000-CN-Controller den zu ersetzenden Fibre Channel HBA enthält.

  "Überprüfen, ob der Fibre-Channel-HBA ausgetauscht werden soll"

- Der SG6000-CN-Controller befindet sich physisch, wo der Fibre Channel HBA im Datacenter ausgetauscht wird.

  "Lokalisierung des Controllers in einem Rechenzentrum"

- Sie haben die Controller-Abdeckung entfernt.

  "Entfernen der SG6000-CN Controller-Abdeckung"

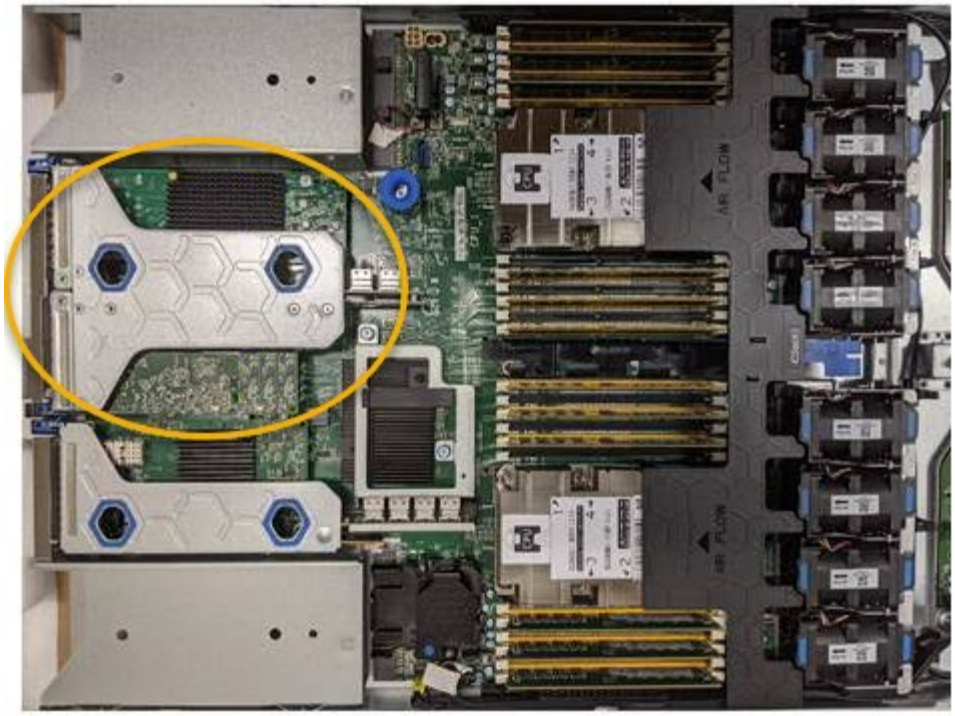
Über diese Aufgabe

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. Informationen zum Bestimmen von Knotenverbindungsstatus finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

> 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. + Weitere Informationen zum Verwalten von Objekten mit Information Lifecycle Management finden Sie unter.

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. Keine übermäßige Kraft verwenden.
6. Setzen Sie den Adapter auf eine flache antistatische Oberfläche.

Nachdem Sie fertig sind

Installieren Sie den Ersatz-Fibre-Channel-HBA.

"Installieren des Fibre Channel-HBA"

Verwandte Informationen

"Installieren des Fibre Channel-HBA"

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

"Objektmanagement mit ILM"

Installieren des Fibre Channel-HBA

Der Ersatz-Fibre Channel HBA wird an demselben Standort installiert wie der zuvor entfernte.

Was Sie benötigen

- Sie haben den richtigen Fibre Channel HBA für den Austausch.
- Sie haben den vorhandenen Fibre Channel HBA entfernt.

  "Entfernen des 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 Abdeckung des SG6000-CN Controllers wieder an"

Ändern der Verbindungskonfiguration 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.

Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

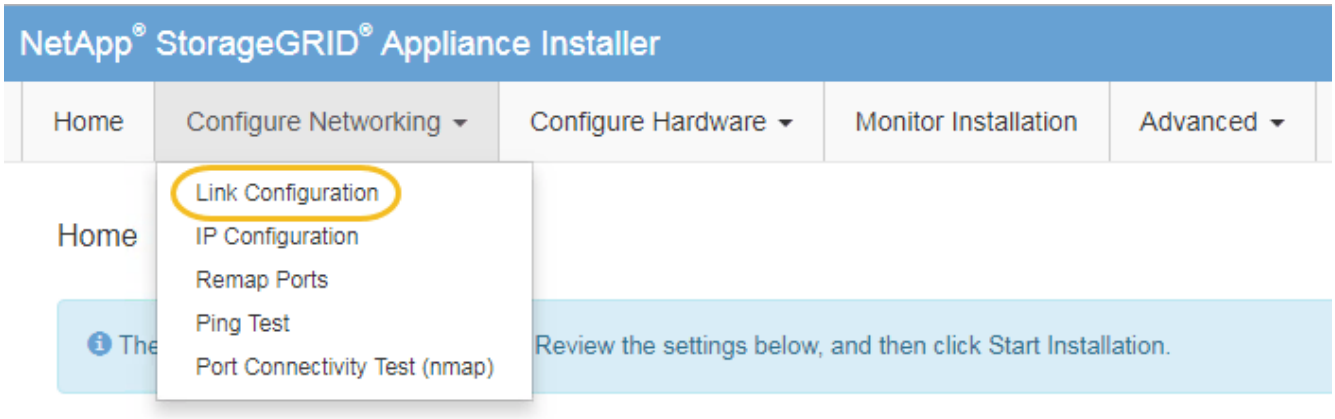
Über diese Aufgabe

Zum Ändern der Ethernet-Link-Konfiguration des SG6000-CN Controllers gehören folgende Optionen:

- Ändern des **Port Bond Modus** von Fixed zu Aggregate oder von 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.



1. Nehmen Sie die gewünschten Änderungen an der Verbindungskonfiguration vor.

   Weitere Informationen zu den Optionen finden Sie unter "Konfigurieren von Netzwerkverbindungen (SG6000)".

2. 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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten 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 Anweisungen zum Konfigurieren von IP-Adressen.

   "StorageGRID-IP-Adressen werden konfiguriert"

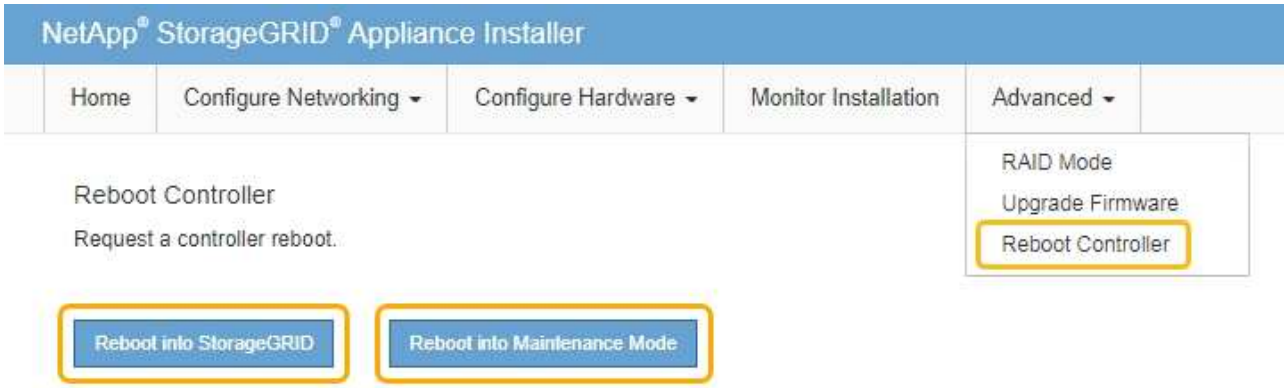
3. Wählen Sie im Menü die Option **Netzwerk konfigurieren** > **Ping-Test** aus.
4. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in allen Netzwerken zu überprüfen, die möglicherweise von den in vorgenommenen Änderungen der Verbindungskonfiguration betroffen sind Änderungen der Linkkonfiguration 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 pingen können. Falls erforderlich, kehren Sie zum zurück Änderungen der Linkkonfiguration Führen Sie Schritte aus, und beheben Sie alle Probleme mit der Link-Konfiguration.

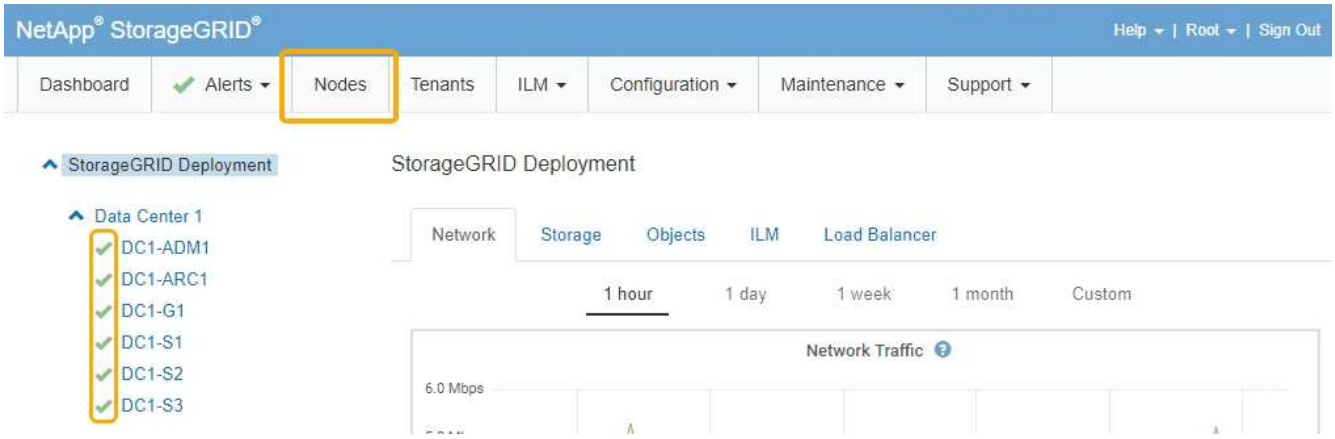
5. Wenn Sie zufrieden sind, dass die Änderungen an der Link-Konfiguration funktionieren, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Ändern der MTU-Einstellung

Sie können die MTU-Einstellung ändern, die Sie beim Konfigurieren von IP-Adressen für den Appliance-Node zugewiesen haben.

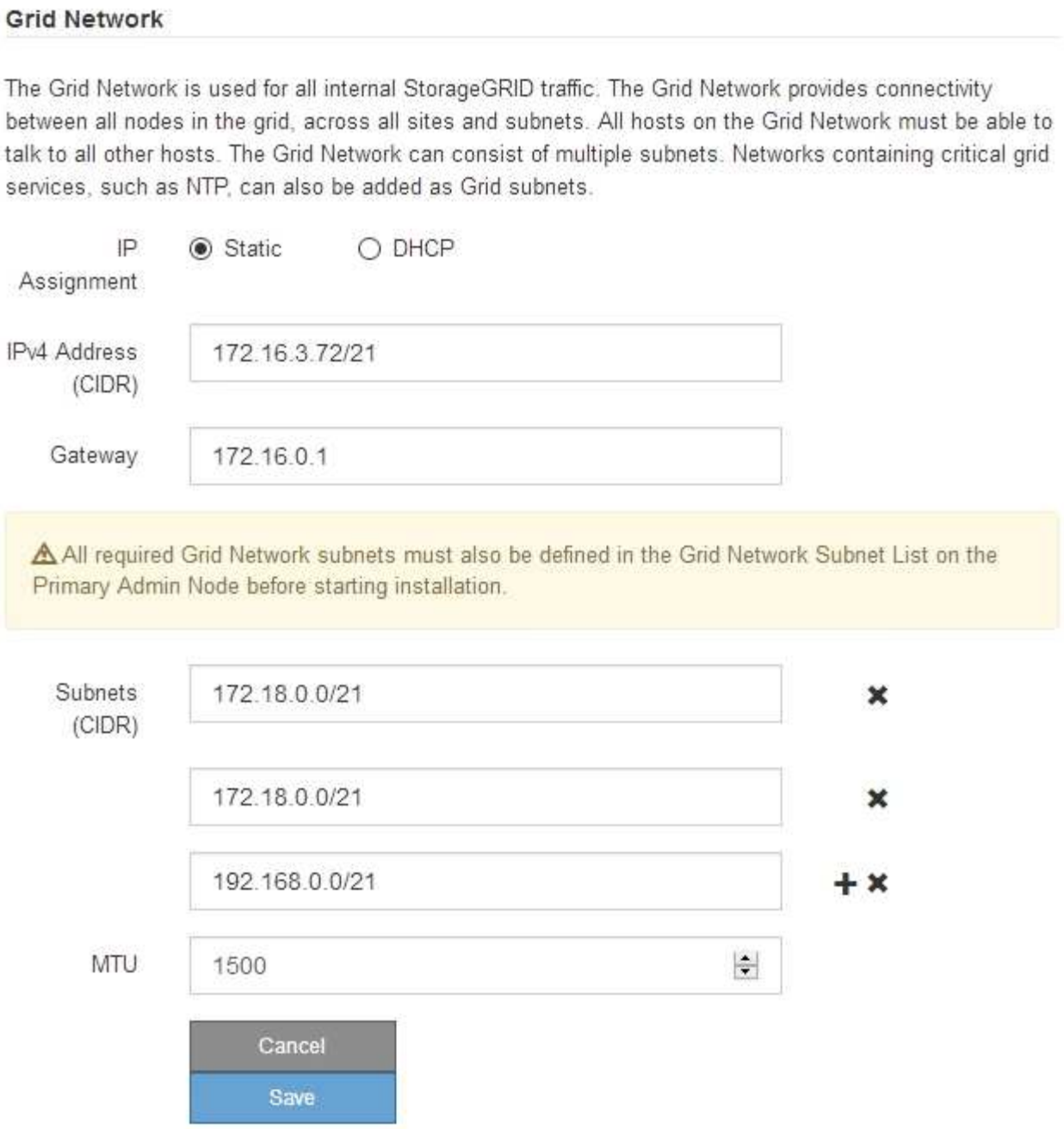
Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

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.



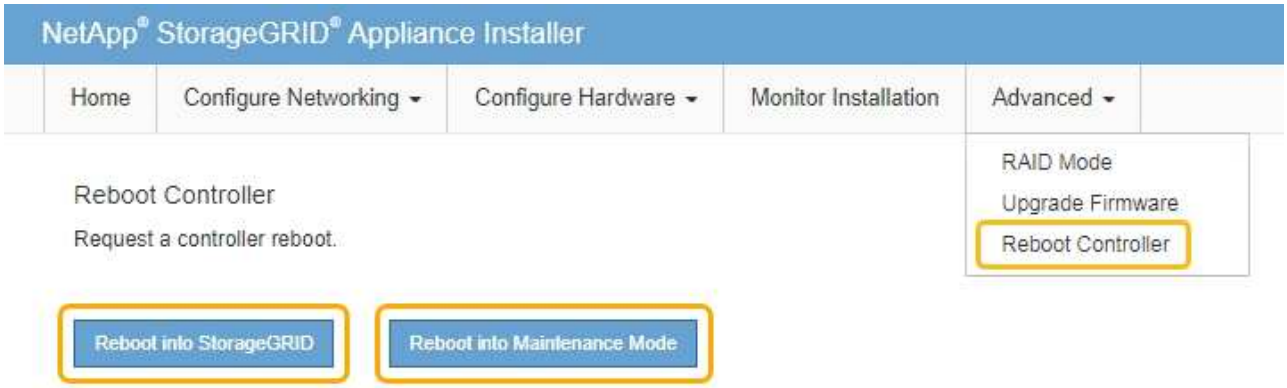
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch sein.

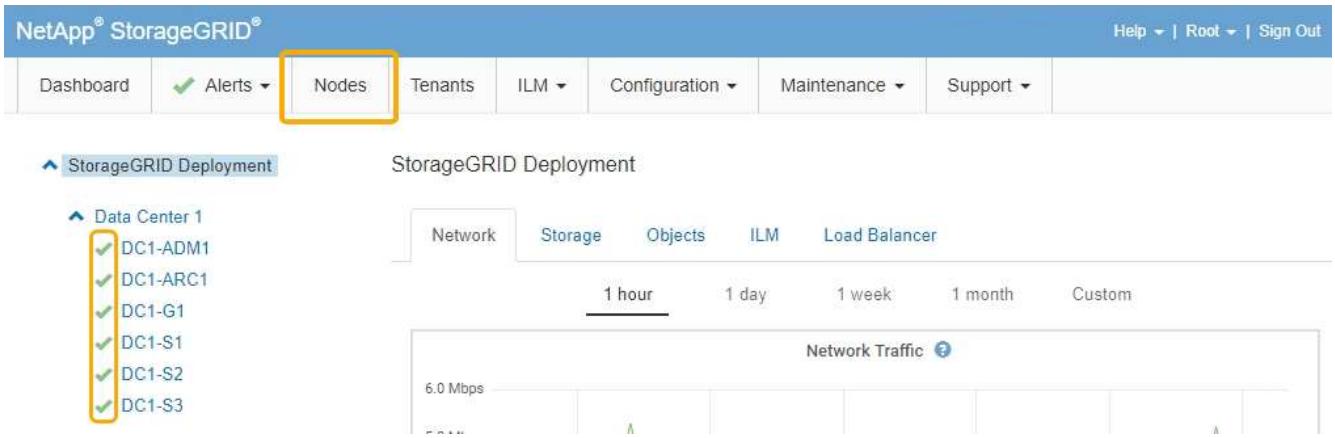
3. Wenn Sie mit den Einstellungen zufrieden sind, wählen Sie **Speichern**.
4. Booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option

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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Überprüfen der DNS-Serverkonfiguration

Sie können die DNS-Server (Domain Name System), die derzeit von diesem Appliance-Node verwendet werden, überprüfen und vorübergehend ändern.

Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Möglicherweise müssen Sie die DNS-Servereinstellungen ändern, wenn eine verschlüsselte Appliance sich nicht mit dem Verschlüsselungsmanagement-Server (KMS) oder dem KMS-Cluster verbinden kann, da der Hostname des 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 durchzuführen, geben Sie die DNS-Server im Grid Manager an (**Wartung** > **Netzwerk** > **DNS-Server**).

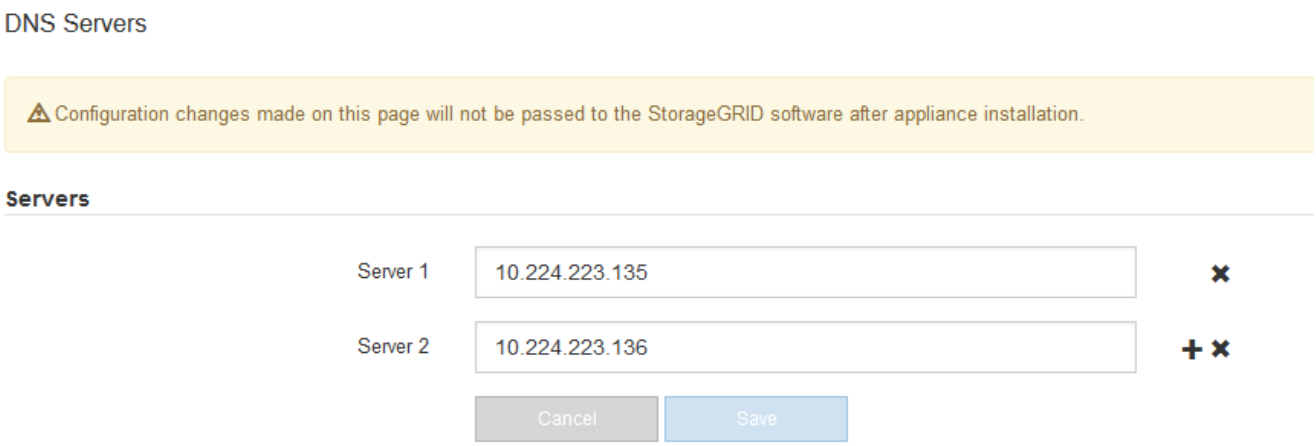
- Temporäre Änderungen an der DNS-Konfiguration sind nur für Node-verschlüsselte Appliances erforderlich, bei denen der KMS-Server mithilfe eines vollständig qualifizierten Domänennamens anstelle einer IP-Adresse für den Hostnamen definiert wird.
- Wenn eine Node-verschlüsselte Appliance über einen Domänennamen 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 Node keinen DNS-Server für das Grid erreichen kann oder wenn die DNS-Einstellungen für das gesamte Grid geändert wurden, wenn ein Node-verschlüsselter Appliance-Node offline war, kann der Node keine Verbindung mit dem KMS herstellen. Verschlüsselte Daten auf der Appliance können erst entschlüsselt werden, wenn das DNS-Problem behoben ist.

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 Node offline war, kann der Node nach seinem Wechsel wieder online den KMS nicht erreichen, 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.



3. Ändern Sie bei Bedarf die DNS-Server.

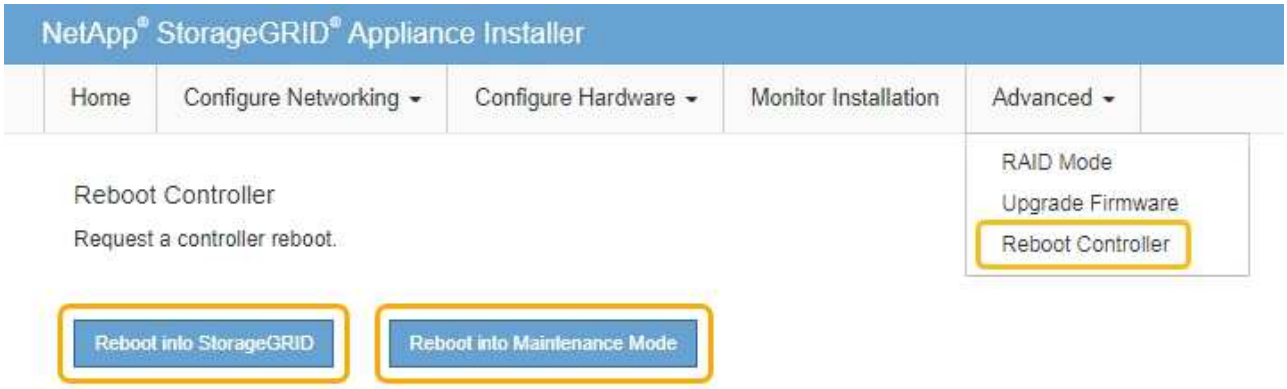
> Änderungen an den DNS-Einstellungen erfolgen temporär und gehen verloren, wenn Sie den Wartungsmodus beenden.

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.

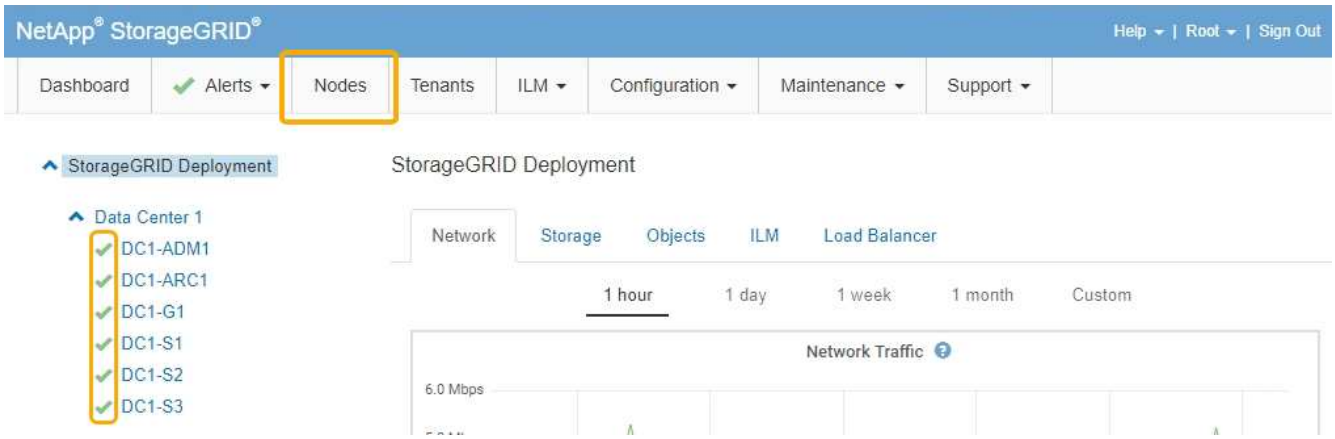
5. Nachdem die Node-Daten entschlüsselt wurden, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 befand.

   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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Monitoring 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).

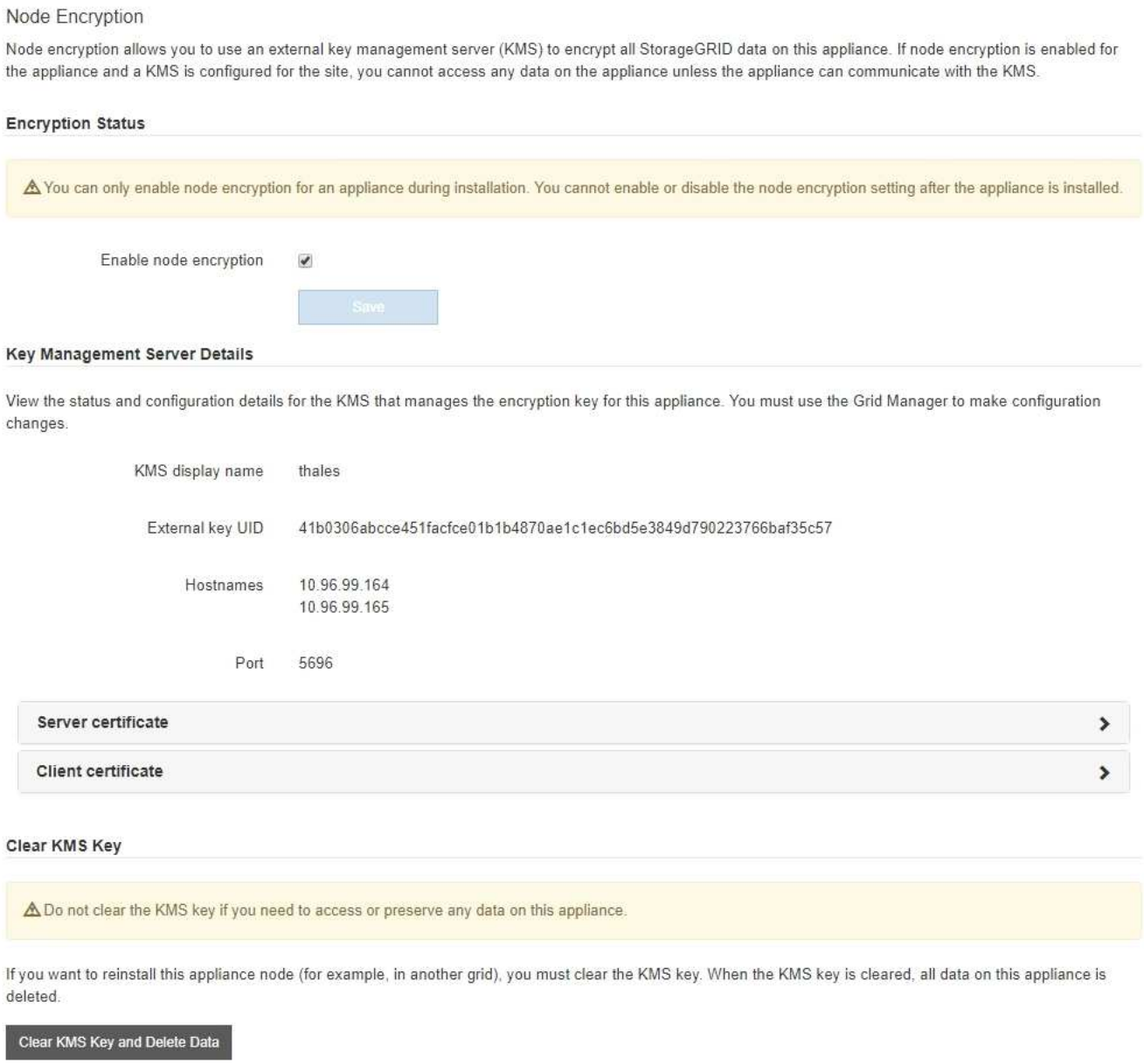
Was Sie benötigen

- Die Node-Verschlüsselung muss während der Installation für die Appliance aktiviert sein. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht aktivieren.
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Hardware konfigurieren** > **Node-Verschlüsselung**.



Die Seite Node Encryption umfasst die folgenden 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.
  - Wenn Sie Probleme mit den Zertifikaten selbst beheben möchten, z. B. die Verlängerung abgelaufener Zertifikate, lesen Sie die Informationen zu KMS in den Anweisungen zur Verwaltung von StorageGRID.
  - Wenn bei der Verbindung zu KMS-Hosts unerwartete Probleme auftreten, überprüfen Sie, ob die DNS-Server (Domain Name System) korrekt sind und das Netzwerk der Appliance korrekt konfiguriert ist.

    "Überprüfen der DNS-Serverkonfiguration"

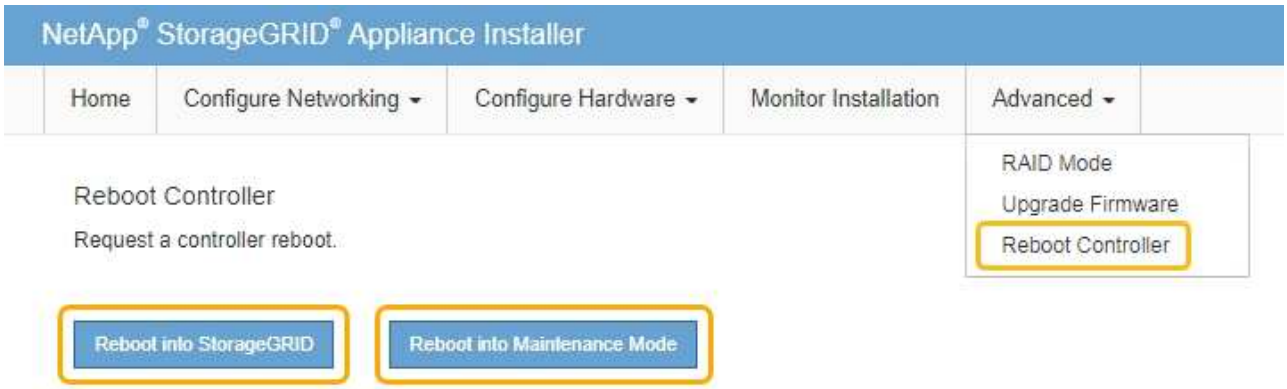
    - Wenden Sie sich an den technischen Support, wenn Sie Ihre Zertifikatsprobleme nicht lösen können.
  - Der klare KMS-Schlüssel deaktiviert die Node-Verschlüsselung für die Appliance, entfernt die Zuordnung zwischen der Appliance und dem für den StorageGRID-Standort konfigurierten Schlüsselmanagementserver und löscht alle Daten von der Appliance. Sie müssen den KMS-Schlüssel löschen, bevor Sie die Appliance in einem anderen StorageGRID-System installieren können.

    "Löschen der Konfiguration des Schlüsselverwaltungsservers"

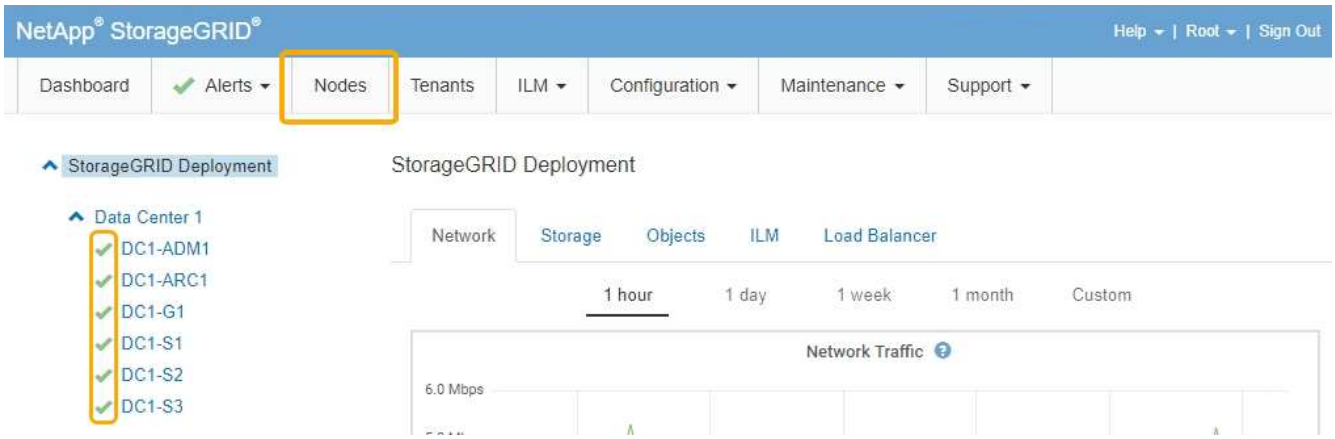
    Durch das Löschen der KMS-Konfiguration werden Daten von der Appliance gelöscht, sodass dauerhaft kein Zugriff darauf besteht. Diese Daten können nicht wiederhergestellt werden.

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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Löschen der Konfiguration des Schlüsselverwaltungsservers

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.

Was Sie benötigen

Wenn Daten auf der Appliance aufbewahrt werden müssen, müssen Sie einen Node außer Betrieb nehmen, 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.

Den Node muss deaktiviert werden, um alle in ihm enthaltenen Daten auf anderen Nodes in StorageGRID zu verschieben. Anweisungen zur Ausmusterung von Grid-Nodes finden Sie in den Angaben zu Recovery und Wartung.

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 Vorgang 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 eine Neuinstallation eines Appliance-Node in einem StorageGRID-System planen, das denselben KMS-Schlüssel verwendet.

- 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.

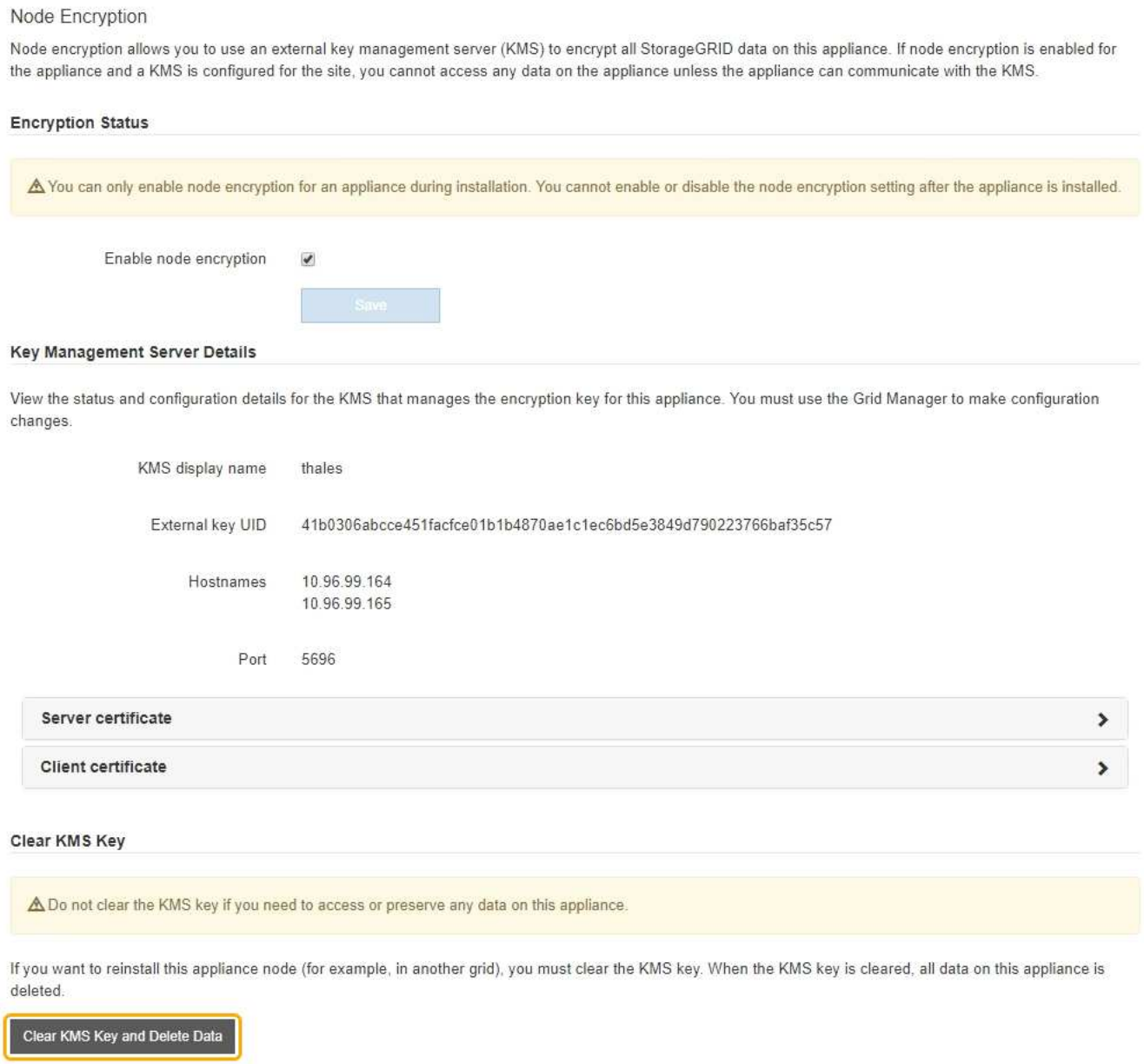
Schritte

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.

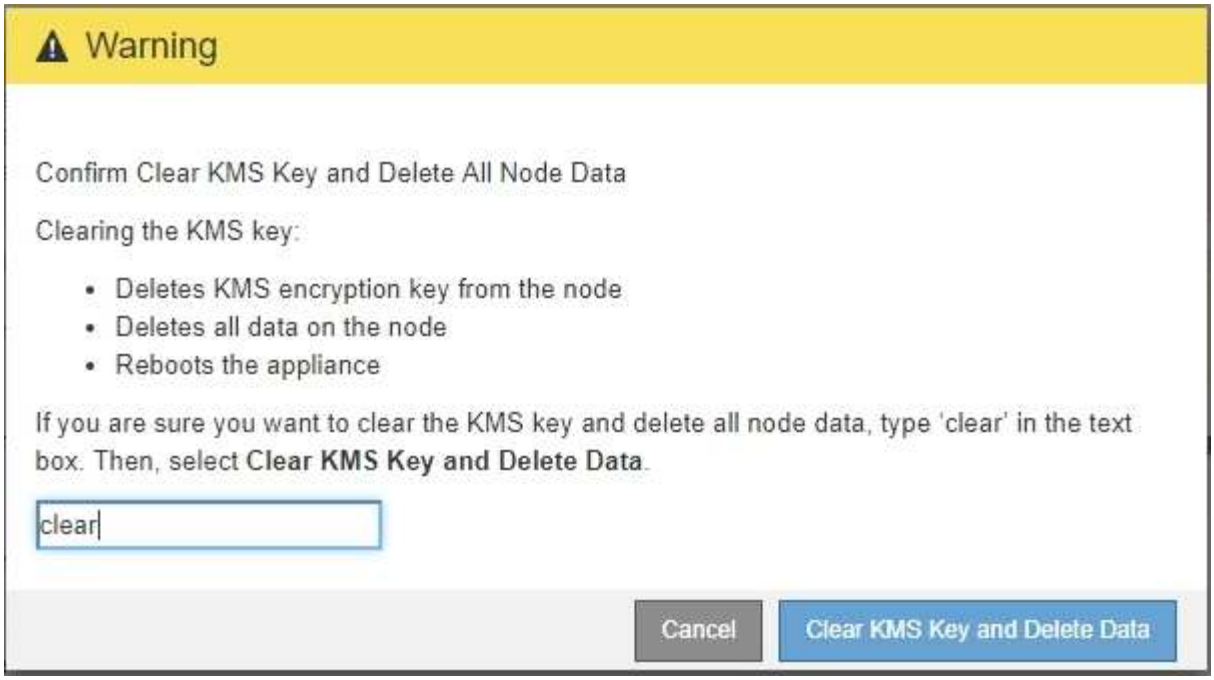
   Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

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` + und wählen Sie **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. Informationen zur Vorbereitung einer Appliance für die Neuinstallation finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Verwandte Informationen

"StorageGRID verwalten"

"Verwalten Sie erholen"

SG5700 Storage-Appliances

Lernen Sie, wie StorageGRID SG5712 und SG5760 Appliances installiert und gewartet werden.

- "Übersicht über die StorageGRID Appliance"
- "Übersicht über Installation und Implementierung"
- "Installation wird vorbereitet"
- "Installieren der Hardware"
- "Konfigurieren der Hardware"
- "Implementieren eines Appliance-Storage-Node"
- "Monitoring der Installation der Speicher-Appliance"
- "Automatisierung der Installation und Konfiguration von Appliances"
- "Überblick über die Installations-REST-APIs"
- "Fehlerbehebung bei der Hardwareinstallation"
- "Warten der SG5700 Appliance"

Übersicht über die StorageGRID Appliance

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 StorageGRID SG5700 Appliance bietet folgende Funktionen:

- 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 E-Series SANtricity System Manager für Hardware-Management und Monitoring.
- Unterstützt bis zu vier 10-GbE- oder 25-GbE-Verbindungen mit dem StorageGRID-Grid-Netzwerk und dem Client-Netzwerk.
- Unterstützt vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard). 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 zwei Modellen erhältlich: Der SG5712 und der SG5760. Beide Modelle enthalten die folgenden Komponenten:

Komponente	SG5712	SG5760
Computing-Controller	E5700SG Controller	E5700SG Controller
Storage Controller	E-Series E2800 Controller	E-Series E2800 Controller

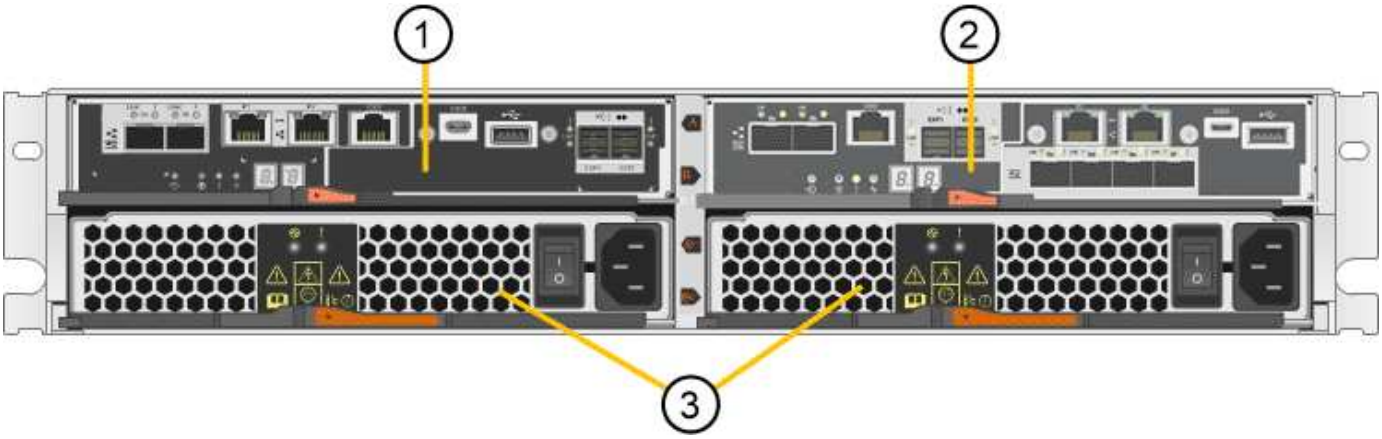
Komponente	SG5712	SG5760
Chassis	E-Series DE212C-Gehäuse, ein 2-HE-Gehäuse (Rack-Unit)	E-Series DE460C Gehäuse, ein 4-HE-Gehäuse (Rack-Unit
Laufwerke	12 NL-SAS-Laufwerke (3.5 Zoll)	60 NL-SAS-Laufwerke (3.5 Zoll)
Redundante Netzteile und Lüfter	Zwei Power-Fan-Kanister	Zwei Leistungskanister und zwei Lüfterkanister

Der maximale Rohkapazität, der in der StorageGRID-Appliance verfügbar ist, richtet sich nach der Anzahl der Laufwerke in jedem Gehäuse. Der verfügbare Storage kann nicht erweitert werden, indem ein Shelf mit zusätzlichen Laufwerken hinzugefügt wird.

Modell SG5712

Diese Abbildung zeigt die Vorder- und Rückseite des SG5712-Modells, ein 2-HE-Gehäuse für 12 Laufwerke.

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

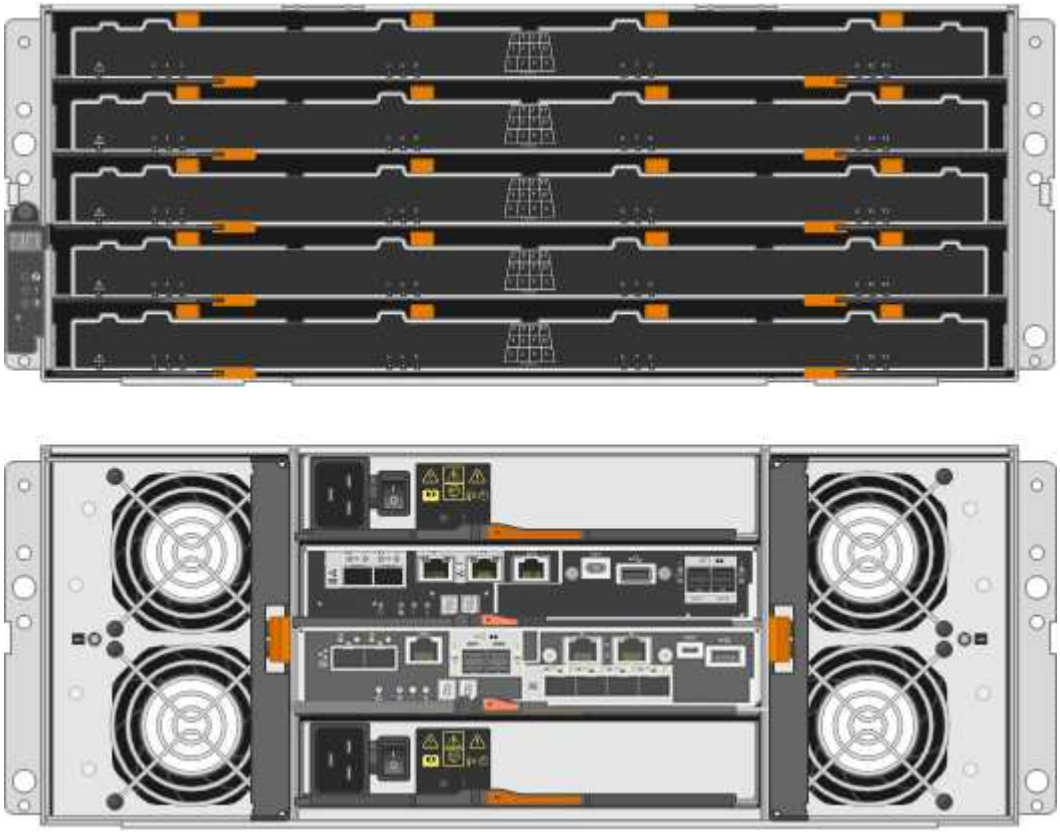


	Beschreibung
1	E2800-Controller (Storage-Controller)
2	E5700SG Controller (Compute-Controller)

	Beschreibung
3	Power-Fan-Behälter

Modell SG5760

Diese Abbildung zeigt die Vorder- und Rückseite des SG5760-Modells, ein 4-HE-Gehäuse für 60 Laufwerke in 5 Laufwerksfächer.



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

	Beschreibung
1	E2800-Controller (Storage-Controller)
2	E5700SG Controller (Compute-Controller)
3	Gebläsebehälter (1 von 2)
4	Leistungsbehälter (1 von 2)

Verwandte Informationen

"NetApp E-Series Systems Documentation Site"

Controller in der StorageGRID Appliance

Die SG5712 und SG5760 Modelle der StorageGRID Appliance umfassen einen E5700SG Controller und einen E2800 Controller. Sie sollten sich die Diagramme ansehen, um sich über die Unterschiede zwischen den Controllern zu informieren.

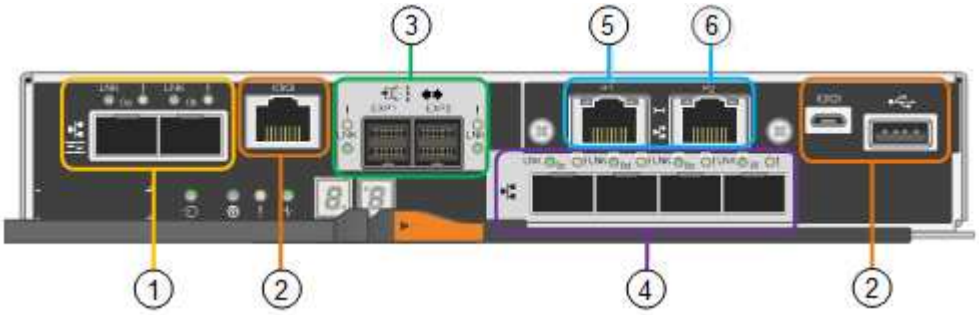
E5700SG Controller

- 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.

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des E5700SG-Controllers.



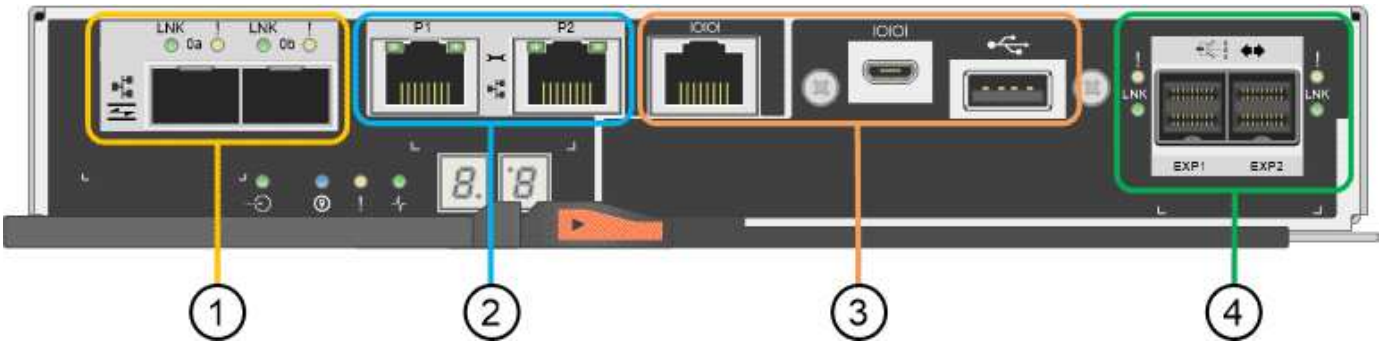
	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	16 Gbit/s Fibre Channel (FC), optisch SFPA	Verbinden Sie den E5700SG Controller mit dem E2800 Controller.
2	Diagnose- und Supportports	• Serieller RJ-45-Anschluss • Serieller Micro-USB-Anschluss • USB-Anschluss	Reserviert für technischen Support.
3	Ports zur Laufwerkserweiterung	12 GB/s SAS	Nicht verwendet. StorageGRID Appliances unterstützen keine Festplatten-Shelfs mit Erweiterung.

	Port	Typ	Nutzung
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.
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: • 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 Controller

- 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.

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des E2800 Controllers.



	Port	Typ	Nutzung
1	Interconnect-Ports 1 und 2	16 Gbit/s FC optisch SFPA	Verbinden Sie den E2800 Controller mit dem E5700SG Controller.
2	Management-Ports 1 und 2	1-GB-Ethernet (RJ-45	• 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.
3	Diagnose- und Supportports	• 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. StorageGRID Appliances unterstützen keine Festplatten-Shelfs mit Erweiterung.

Übersicht über Installation und Implementierung

Sie können eine oder mehrere StorageGRID Appliances installieren, wenn Sie StorageGRID zum ersten Mal implementieren. Alternativ können Sie Appliance Storage-Nodes später im Rahmen einer Erweiterung hinzufügen. Möglicherweise müssen Sie auch einen Appliance-Speicherknoten im Rahmen eines Wiederherstellungsvorgangs installieren.

Das Hinzufügen einer StorageGRID Storage Appliance zu einem StorageGRID System umfasst vier primäre Schritte:

1. Installation vorbereiten:
   - Vorbereiten des Installationsstandorts
   - Auspacken der Schachteln und Prüfen des Inhalts
   - Zusätzliche Ausrüstung und Werkzeuge
   - Sammeln von IP-Adressen und Netzwerkinformationen
   - Optional: Konfiguration eines externen Verschlüsselungsmanagement-Servers (KMS), wenn Sie alle Appliance-Daten verschlüsseln möchten. Weitere Informationen zum externen Verschlüsselungsmanagement finden Sie in der Anleitung zur Administration von StorageGRID.
2. Installieren der Hardware:
   - Registrieren der Hardware
   - Installieren des Geräts in einem Schrank oder Rack
   - Installieren der Laufwerke (nur SG5760)

- Verkabeln Sie das Gerät
- Anschließen der Stromkabel und Strom anschließen
- Anzeigen von Boot-Statuscodes

3. Konfigurieren der Hardware:
   - Zugriff auf SANtricity System Manager, Festlegen einer statischen IP-Adresse für den Management-Port 1 auf dem E2800-Controller und Konfigurieren von SANtricity System Manager-Einstellungen
   - Zugriff auf das Installationsprogramm von StorageGRID Appliance und Konfiguration der für die Verbindung mit StorageGRID-Netzwerken erforderlichen Link- und Netzwerk-IP-Einstellungen
   - Optional: Aktivieren der Node-Verschlüsselung, wenn Sie zur Verschlüsselung von Appliance-Daten einen externen KMS verwenden möchten.
   - Optional: Ändern des RAID-Modus.
4. Bereitstellen der Appliance als Storage-Node:

Aufgabe	Anweisungen
Bereitstellen eines Appliance-Speicherknoten in einem neuen StorageGRID-System	"Implementieren eines Appliance-Storage-Node"
Hinzufügen eines Appliance-Speicherknotens zu einem vorhandenen StorageGRID-System	Anweisungen zum erweitern eines StorageGRID-Systems
Bereitstellen eines Appliance-Speicherknotens als Teil eines Speicherknotenwiederherstellungsvorgangs	Anweisungen zur Wiederherstellung und Wartung

Verwandte Informationen

"Installation wird vorbereitet"

"Installieren der Hardware"

"Konfigurieren der Hardware"

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"SG100 SG1000 Services-Appliances"

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

"StorageGRID verwalten"

Installation wird vorbereitet

Die Vorbereitung der Installation einer StorageGRID Appliance umfasst die Vorbereitung des Standorts und den Erwerb aller erforderlichen Hardware, Kabel und Tools. Außerdem

sollten Sie IP-Adressen und Netzwerkinformationen erfassen.

Schritte

- "Vorbereiten des Standorts (SG5700)"
- "Auspacken der Boxen (SG5700)"
- "Zusätzliche Ausrüstung und Tools (SG5700)"
- "Anforderungen an einen Webbrowser"
- "Überprüfen von Appliance-Netzwerkverbindungen"
- "Sammeln von Installationsinformationen (SG5700)"

Vorbereiten des Standorts (SG5700)

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. Weitere Informationen finden Sie im NetApp Hardware Universe.
2. Wenn Sie das SG5760-Modell installieren, vergewissern Sie sich, dass Ihr Standort 240-Volt-Wechselstromversorgung bietet.
3. Passen Sie zu 48.3 Shelfs dieser Größe (ohne Kabel) ein 19-cm-Gehäuse oder -Rack an:

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)

4. Installieren Sie alle erforderlichen Netzwerk-Switches. Informationen zur Kompatibilität sind im NetApp Interoperabilitäts-Matrix-Tool verfügbar.

Verwandte Informationen

"NetApp Hardware Universe"

"NetApp Interoperabilitäts-Matrix-Tool"

Auspacken der Boxen (SG5700)

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

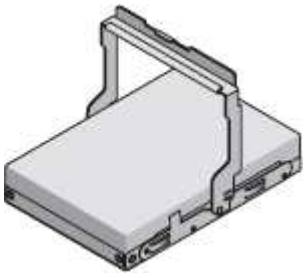
- **SG5712-Appliance mit 12 installierten Laufwerken**

- **SG5760 Appliance ohne installierte Laufwerke**

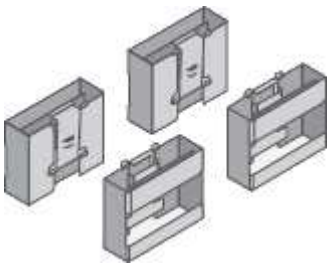
- **Frontblende für das Gerät**

- **Rail Kit mit Anweisungen**

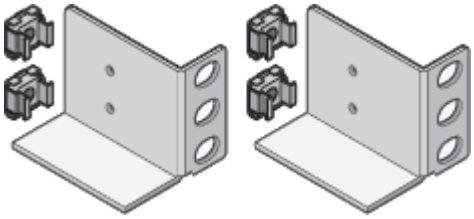
- **SG5760: 60 Laufwerke**



- **SG5760: Griffe**



- **SG5760: Rückenhalterungen und Käfigmuttern für quadratische Rackmontage**



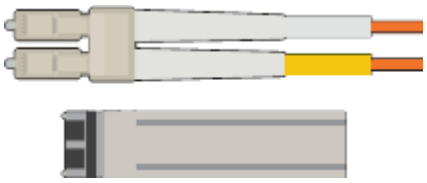
Kabel und Anschlüsse

Der Versand für das StorageGRID Gerät umfasst die folgenden Kabel und Anschlüsse:

- * Zwei Netzkabel für Ihr Land*

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

- **Optische Kabel und SFP-Transceiver**



  Zwei optische Kabel für die FC Interconnect Ports

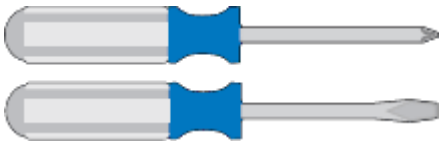
  Acht SFP+-Transceiver, kompatibel mit den vier 16-Gbit/s-FC-Interconnect-Ports und den vier 10-GbE-Netzwerkports

Zusätzliche Ausrüstung und Tools (SG5700)

Vergewissern Sie sich vor der Installation der StorageGRID Appliance, dass alle zusätzlichen Geräte und Tools zur Verfügung stehen, die Sie benötigen.

Sie benötigen die folgende zusätzliche Ausrüstung für die Installation und Konfiguration der Hardware:

- **Schraubendreher**

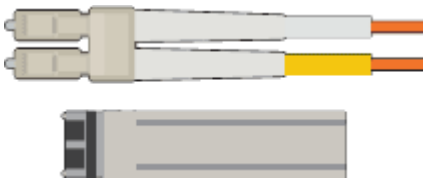


  Phillips Nr. 2 Schraubendreher

  Mittlerer Schlitzschraubendreher

- **ESD-Handgelenkschlaufe**

- **Optische Kabel und SFP-Transceiver**



Optische Kabel für die 10/25-GbE-Ports, die Sie verwenden möchten

Optional: SFP28 Transceiver, wenn Sie 25-GbE-Verbindungsgeschwindigkeit verwenden möchten

- * Ethernet-Kabel*

- **Service-Laptop**

Unterstützter Webbrowser

SSH-Client, z. B. PuTTY

1-GB-Ethernet-Port (RJ-45)

- **Optionale Werkzeuge**

Kraftbohrer mit Kreuzschlitz

Taschenlampe

Mechanisierter Lift für SG5760

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Überprüfen von 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.

StorageGRID Appliance-Netzwerke

Wenn Sie eine StorageGRID Appliance als Storage Node in einem StorageGRID Grid implementieren, können Sie sie mit folgenden Netzwerken verbinden:

- **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

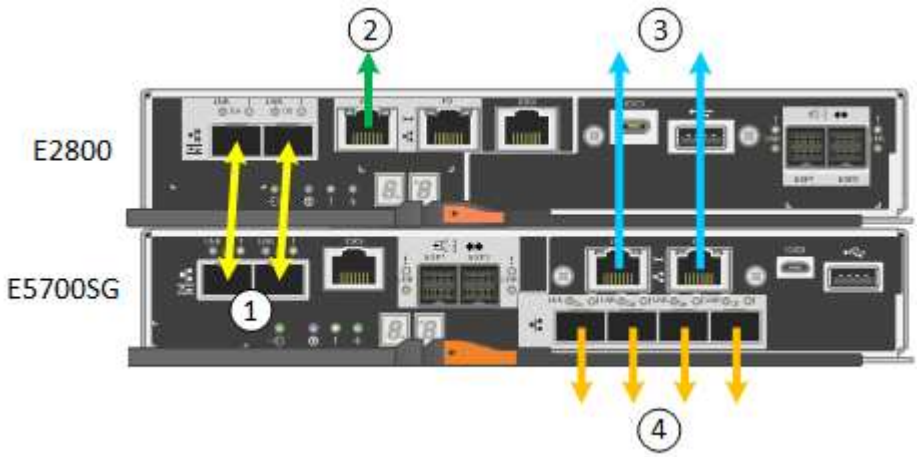
Systemadministration und Wartung verwendet wird. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routingfähig sein. Das Admin-Netzwerk ist optional.

- **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. Das Client-Netzwerk ist optional.
- **Managementnetzwerk für SANtricity System Manager**: Dieses Netzwerk bietet Zugriff auf SANtricity System Manager auf dem E2800 Controller, sodass Sie die Hardwarekomponenten 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.

Ausführliche Informationen zu StorageGRID-Netzwerken finden Sie unter *Rasterprimer*.

Verbindungen zu StorageGRID-Appliances

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



	Port	Typ des Ports	Funktion
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.
2	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.

	Port	Typ des Ports	Funktion
3	Management-Port 2 am E5700SG Controller	1 GbE (RJ-45)	• 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). • Während der Installation kann 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 „`10/25-GbE-Portverbindungen für den E5700SG Controller`“.

Verwandte Informationen

"Sammeln von Installationsinformationen (SG5700)"

"Verkabelung der Appliance (SG5700)"

"Port Bond-Modi für E5700SG Controller-Ports"

"Netzwerkrichtlinien"

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Port Bond-Modi für E5700SG Controller-Ports

Wenn Sie Netzwerkverbindungen für die Controller-Ports des E5700SG konfigurieren, können Sie die Portbindung für die 10/25-GbE-Ports verwenden, die mit dem Grid-

Netzwerk und dem optionalen Client-Netzwerk verbunden sind, sowie 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.

Verwandte Informationen

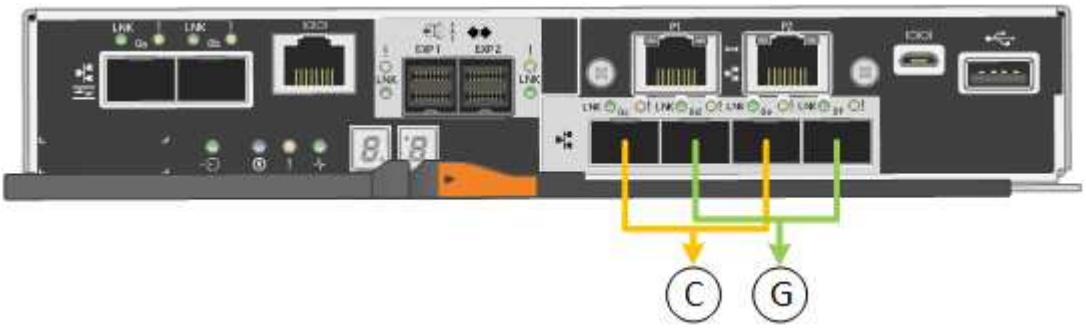
"Konfigurieren von Netzwerk-Links (SG5700)"

Netzwerk-Bond-Modi für die 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.



	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.

	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 müssen wissen, wie die Switches konfiguriert werden, um VLAN, LACP und MLAG zu verwenden.

Wenn Sie nicht alle vier 10/25-GbE-Ports verwenden möchten, können Sie ein, 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.

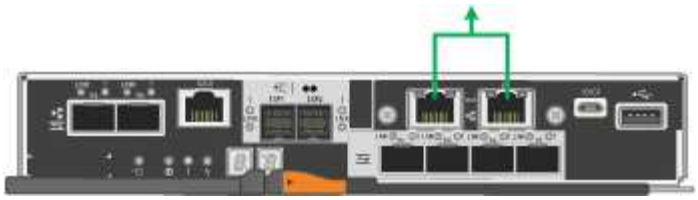
Netzwerk-Bond-Modi für die 1-GbE-Management-Ports

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.



Sammeln von Installationsinformationen (SG5700)

Bei der Installation und Konfiguration der StorageGRID Appliance sind Entscheidungen zu treffen und Informationen zu Ethernet Switch-Ports, IP-Adressen sowie zu Port- und Netzwerk-Bond-Modi zu sammeln.

Über diese Aufgabe

Die folgenden Tabellen enthalten die erforderlichen Informationen für jedes Netzwerk, das Sie mit der Appliance verbinden. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.

Informationen, die für die Verbindung mit SANtricity System Manager auf dem E2800 Controller erforderlich sind

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

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)	
Über DHCP zugewiesene IP-Adresse für Management-Port 1, sofern nach dem Einschalten verfügbar **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.	
Geschwindigkeit und Duplexmodus **Hinweis:** Sie müssen sicherstellen, dass der Ethernet-Switch für das SANtricity-System-Manager-Managementnetzwerk auf Autonegotiation gesetzt ist.	Muss sein: • Autonegotiation (Standard)
IP-Adressformat	Bitte auswählen: • IPv4 • IPv6

Erforderliche Informationen	Ihr Wert
Statische IP-Adresse, die Sie für die Appliance im Managementnetzwerk verwenden möchten	Für IPv4: • IPv4-Adresse: • Subnetzmaske: • Gateway: Für IPv6: • IPv6-Adresse: • Routingfähige IP-Adresse: • E2800 Controller-Router-IP-Adresse:

Zum Verbinden 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
Admin-Netzwerk aktiviert	Bitte auswählen: • Nein • Ja (Standard)
Netzwerk-Bond-Modus	Bitte auswählen: • 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.	• IPv4-Adresse (CIDR): • Gateway:

Erforderliche Informationen	Ihr Wert
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.	• IPv4-Adresse (CIDR): • Gateway:
Admin-Netzwerk-Subnetze (CIDR)	

Erforderliche Informationen zum Verbinden und Konfigurieren der 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.

> Weitere Informationen zu den Optionen dieser Ports finden Sie unter „10/25-GbE-Portverbindungen für den E5700SG-Controller“.

Erforderliche Informationen	Ihr Wert
Verbindungsgeschwindigkeit **Hinweis:** Wenn Sie 25 GbE wählen, müssen Sie SPF28-Transceiver installieren. Die automatische Aushandlung wird nicht unterstützt. Sie müssen also auch die Ports und die verbundenen Switches für 25 GbE konfigurieren.	Bitte auswählen: • 10 GbE (Standard) • 25 GBitE
Port Bond-Modus	Bitte auswählen: • Fest (Standard) • Aggregat
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.

Weitere Informationen zu den Optionen dieser Ports finden Sie unter „10/25-GbE-Portverbindungen für den E5700SG-Controller“.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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.	• 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.	• IPv4-Adresse (CIDR): • Gateway:
Grid-Netzwerknetze (CIDR) **Hinweis:** Wenn das Client-Netzwerk nicht aktiviert ist, verwendet die Standardroute auf dem Controller das hier angegebene Gateway.	

Zum Verbinden 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.

Weitere Informationen zu den Optionen dieser Ports finden Sie unter „10/25-GbE-Portverbindungen für den E5700SG-Controller“.

Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: • Nein (Standard) • Ja.
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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	• 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.	• IPv4-Adresse (CIDR): • Gateway:

Verwandte Informationen

"Überprüfen von Appliance-Netzwerkverbindungen"

"Port Bond-Modi für E5700SG Controller-Ports"

"Konfigurieren der Hardware"

Installieren der Hardware

Die Hardware-Installation umfasst die Installation des Geräts in einem Schrank oder Rack, den Anschluss der Kabel und den Strom-Einsatz.

Schritte

- "Registrieren der Hardware"
- "Installieren der Appliance in einem Rack oder Rack (SG5700)"
- "Verkabelung der Appliance (SG5700)"

- "Anschließen der Stromkabel und Anschließen der Stromversorgung (SG5700)"
- "Anzeigen der SG5700-Boot-Statuscodes"

Registrieren der Hardware

Die Registrierung der Appliance-Hardware bietet Support-Vorteile.

Schritte

1. Suchen Sie die Seriennummer des Chassis.

   Sie finden die Nummer auf dem Packzettel, in Ihrer Bestätigungs-E-Mail oder auf dem Gerät nach dem Auspacken.

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	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.
Neuer NetApp Kunde	a. Klicken Sie auf **Jetzt registrieren** und erstellen Sie ein Konto. b. Wählen Sie **Produkte** > **Produkte Registrieren**. c. Geben Sie die Seriennummer des Produkts und die angeforderten Details ein. Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.

Installieren der Appliance in einem Rack oder Rack (SG5700)

Sie müssen Schienen in Ihrem Schrank oder Rack installieren und das Gerät dann auf die Schienen schieben. Wenn Sie eine SG5760 haben, müssen Sie nach der Installation der Appliance auch die Laufwerke installieren.

Was Sie benötigen

- 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 verfügen über die *Installations- und Setup-Anleitung* für das Gerät.

> Installieren Sie die Hardware von der Unterseite des Racks oder Racks bis zu, um ein Umkippen des Geräts zu verhindern.

> 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.

> 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

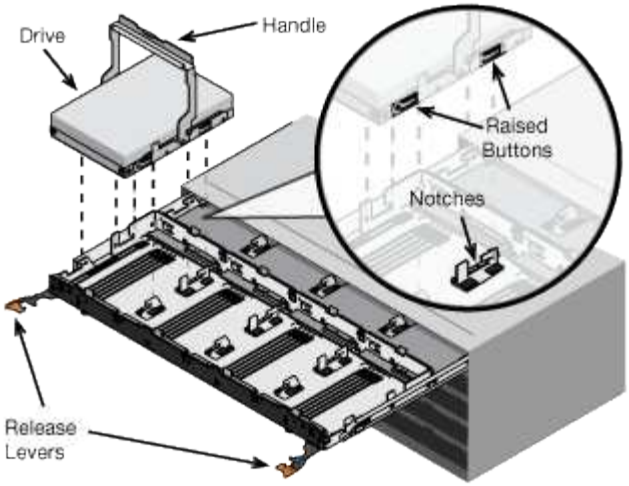
1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.
2. Wenn Sie eine SG5760 haben, befolgen Sie diese Schritte, um das Verschieben der Appliance vorzubereiten.
   a. Entfernen Sie den äußeren Verpackungskasten. Falten Sie dann die Klappen auf dem inneren Kasten nach unten.
   b. 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. Siehe Anweisungen zur Installation und Einrichtung_ und schieben Sie das Gerät in den Schrank oder das Rack.
4. Siehe die Anweisungen zur Installation und Einrichtung_, und befestigen Sie das Gerät am Schrank oder Rack.

   Wenn Sie eine SG5760 haben, befestigen Sie das Gerät mithilfe der hinteren Halterungen an der Rückseite des Racks oder der Ablage. Verwenden Sie die Käfigmuttern, wenn Ihr Rack oder Schrank quadratische Löcher hat.
5. Wenn Sie eine SG5760 haben, installieren Sie 12 Laufwerke in jedem der 5 Laufwerk-Schubladen.

   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 Schubladen.

6. Befestigen Sie die Frontverkleidung.

Verkabelung der Appliance (SG5700)

Sie müssen die beiden Controller miteinander verbinden, die Management-Ports auf jedem Controller verbinden und die 10/25-GbE-Ports des E5700SG-Controllers mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID verbinden.

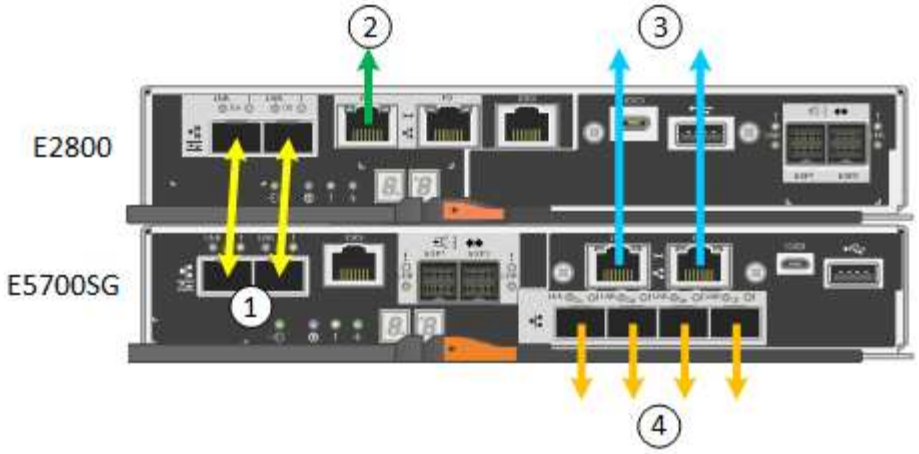
Was Sie benötigen

- 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 die folgenden Artikel 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 — kein Teil eines SFP-Transceivers zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

Über diese Aufgabe

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, wenn er von hinten betrachtet wird.



	Port	Typ des Ports	Funktion
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.
2	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.

	Port	Typ des Ports	Funktion
3	Management-Port 2 am E5700SG Controller	1 GbE (RJ-45)	• 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). • Während der Installation kann 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 „`10/25-GbE-Portverbindungen für den 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

Diesen Port verbinden…	Zu diesem Port…
Interconnect-Port 2 auf dem E2800 Controller	Interconnect-Port 2 am E5700SG Controller

2. Verbinden Sie den Management-Port 1 (P1) am E2800 Controller (der RJ-45-Port auf der linken Seite) mit dem Managementnetzwerk für SANtricity System Manager über ein Ethernet-Kabel.

   Verwenden Sie keinen Management-Port 2 (P2) am E2800 Controller (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

"Zugriff auf das Installationsprogramm der StorageGRID-Appliance"

"Port Bond-Modi für E5700SG Controller-Ports"

Anschließen der Stromkabel und Anschließen der Stromversorgung (SG5700)

Wenn Sie das Gerät mit Strom versorgen, werden beide Controller gestartet.

Was Sie benötigen

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 Einschaltvorgangs 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.

Anzeigen der SG5700-Boot-Statuscodes

Die sieben-Segment-Anzeigen auf jedem Controller zeigen Status- und Fehlercodes an, wenn das Gerät eingeschaltet wird.

Über diese Aufgabe

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	*E5700 and E2800 System Monitoring Guide* **Hinweis:** die für den E-Series E5700 Controller aufgeführten Codes gelten nicht für den E5700SG Controller in der Appliance.
E5700SG Controller	„status-Indikatoren am E5700SG-Controller“

Schritte

1. 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.
2. 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	Zeigt **HO**, gefolgt von einer sich wiederholenden Sequenz von zwei Zahlen. `HO -- IP address for Admin Network -- IP address for Grid Network HO` 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. **Hinweis:** konnte eine IP-Adresse nicht über DHCP zugewiesen werden, wird 0.0.0.0 angezeigt.

3. Wenn in den sieben Segmenten andere Werte angezeigt werden, lesen Sie unter „`Fehlerbehebung bei der Hardwareinstallation`“ 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

"Statusanzeigen auf dem E5700SG-Controller"

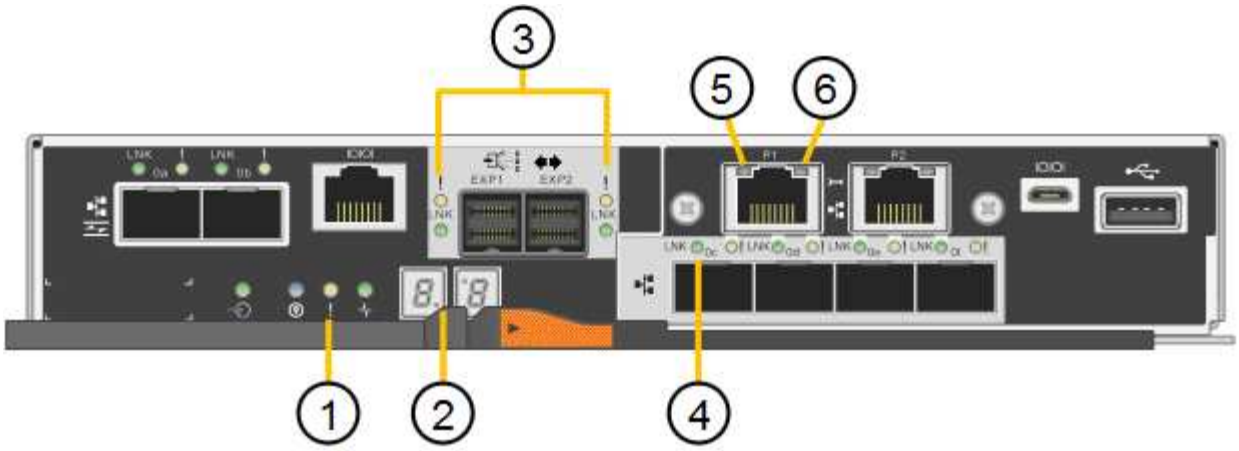
"Fehlerbehebung bei der Hardwareinstallation"

"E5700 und E2800 – System Monitoring Guide"

Statusanzeigen auf dem 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.



	Anzeige	Beschreibung
1	Warnungs-LED	Gelb: Der Controller ist fehlerhaft und erfordert eine Bedienerwarnung, oder das Installationsskript 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.
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.
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.
E8	Kein Speicher installiert.
EU	Das Installationsskript wurde nicht gefunden.
EP	Installation oder Kommunikation mit dem E2800-Controller ist fehlgeschlagen.

Verwandte Informationen

"Fehlerbehebung bei der Hardwareinstallation"

"NetApp Support"

Konfigurieren der Hardware

Nachdem Sie das Gerät mit Strom versorgt haben, müssen Sie SANtricity System Manager konfigurieren. Hierbei handelt es sich um die Software, mit der Sie die Hardware überwachen. Sie müssen auch die Netzwerkverbindungen konfigurieren, die von StorageGRID verwendet werden.

Schritte

- "Konfigurieren von StorageGRID-Verbindungen"

- "Zugriff auf und Konfigurieren von SANtricity System Manager"
- "Optional: Aktivieren der Node-Verschlüsselung"
- "Optional: Ändern des RAID-Modus (nur SG5760)"
- "Optional: Neu zuordnen von Netzwerkports für die Appliance"

Konfigurieren von StorageGRID-Verbindungen

Bevor Sie eine StorageGRID Appliance als Storage Node in einem StorageGRID-Grid bereitstellen können, müssen Sie die Verbindungen zwischen der Appliance und den zu verwendenden Netzwerken konfigurieren. Sie können das Netzwerk konfigurieren, indem Sie im StorageGRID Appliance Installer navigieren, der im E5700SG Controller (dem Computing-Controller in der Appliance) enthalten ist.

Schritte

- "Zugriff auf das Installationsprogramm der StorageGRID-Appliance"
- "Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance"
- "Konfigurieren von Netzwerk-Links (SG5700)"
- "Einstellen der IP-Konfiguration"
- "Netzwerkverbindungen werden überprüft"
- "Überprüfen von Netzwerkverbindungen auf Portebene"

Zugriff auf das Installationsprogramm der StorageGRID-Appliance

Sie müssen auf das Installationsprogramm der StorageGRID Appliance zugreifen, um die Verbindungen zwischen der Appliance und den drei StorageGRID-Netzwerken zu konfigurieren: Das Grid-Netzwerk, das Admin-Netzwerk (optional) und das Client-Netzwerk (optional).

Was Sie benötigen

- Sie verwenden einen unterstützten Webbrowser.
- Die Appliance ist mit allen von Ihnen geplanten StorageGRID-Netzwerken verbunden.
- In diesen Netzwerken kennen Sie die IP-Adresse, das Gateway und das Subnetz für die Appliance.
- Sie haben die geplanten Netzwerk-Switches konfiguriert.

Über diese Aufgabe

Wenn Sie zum ersten Mal auf das Installationsprogramm der StorageGRID-Appliance zugreifen, können Sie die vom DHCP zugewiesene IP-Adresse für das Admin-Netzwerk verwenden (vorausgesetzt, die Appliance ist mit dem Admin-Netzwerk verbunden) oder die durch DHCP zugewiesene IP-Adresse für das Grid-Netzwerk. Die Verwendung der IP-Adresse für das Admin-Netzwerk ist vorzuziehen. Wenn Sie andernfalls über die DHCP-Adresse für das Grid-Netzwerk auf das Installationsprogramm von StorageGRID-Appliances zugreifen, kann die Verbindung zum StorageGRID-Appliance-Installationsprogramm verloren gehen, wenn Sie die Link-Einstellungen ändern und wenn Sie eine statische IP eingeben.

Schritte

1. Beziehen Sie die DHCP-Adresse für das Gerät im Admin-Netzwerk (wenn es verbunden ist) oder das Grid-Netzwerk (wenn das Admin-Netzwerk nicht verbunden ist).

Sie können eine der folgenden Aktionen ausführen:

- 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.

- Geben Sie dem Netzwerkadministrator die MAC-Adresse für den Management-Port 1 an, damit er die DHCP-Adresse für diesen Port im Admin-Netzwerk nachsehen kann. Die MAC-Adresse ist auf einem Etikett des E5700SG-Controllers neben dem Port gedruckt.

2. Wenn Sie eine der DHCP-Adressen abrufen konnten:

   a. Öffnen Sie einen Webbrowser auf dem Service-Laptop.

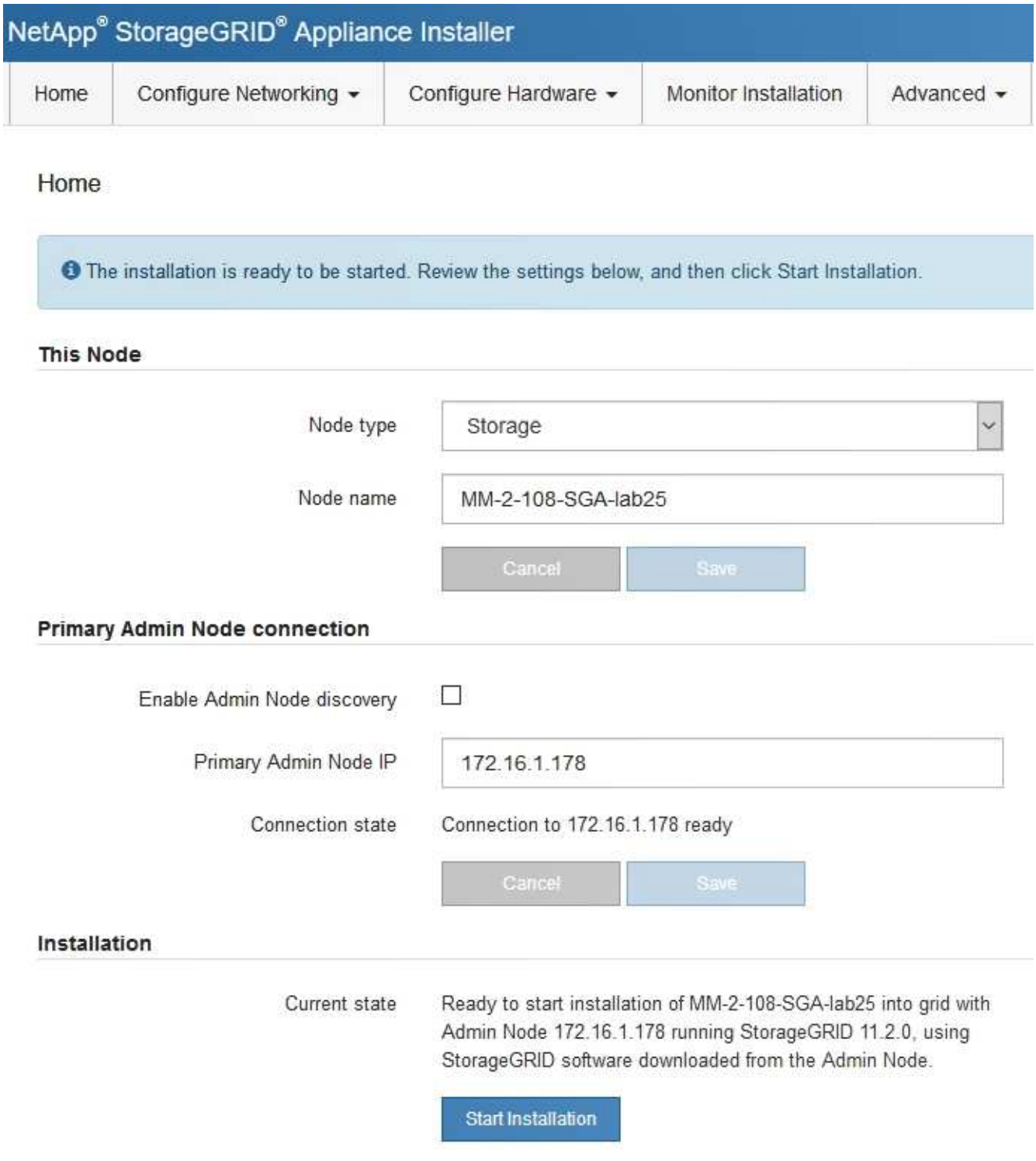
   b. Geben Sie diese URL für das StorageGRID-Appliance-Installationsprogramm ein:
   `https://E5700SG_Controller_IP:8443`

   Für *`E5700SG_Controller_IP`*, Verwenden Sie die DHCP-Adresse für den Controller. (Verwenden Sie die IP-Adresse für das Admin-Netzwerk, wenn Sie ihn haben).

   c. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, zeigen Sie das Zertifikat mithilfe des Browser-Installationsassistenten an und installieren Sie es.

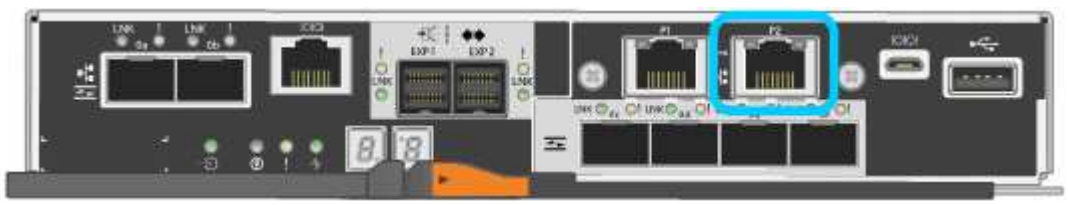
   Die Meldung wird beim nächsten Zugriff auf diese URL nicht angezeigt.

   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.



3. Wenn der E5700SG-Controller keine IP-Adresse über DHCP erhalten konnte:

   a. Verbinden Sie den Service-Laptop über ein Ethernet-Kabel mit dem Management-Port 2 des E5700SG Controllers.



b. Öffnen Sie einen Webbrowser auf dem Service-Laptop.

c. 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 das Gerät aktuell verbunden ist.

Wenn Sie über eine lokale Verbindung nicht auf die Startseite zugreifen können, konfigurieren Sie die Service-Laptop-IP-Adresse als `169.254.0.2`, Und versuchen Sie es erneut.

4. Überprüfen Sie alle Meldungen, die auf der Startseite angezeigt werden, und konfigurieren Sie die Verbindungskonfiguration und die IP-Konfiguration nach Bedarf.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

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.

Was Sie benötigen

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 das StorageGRID-Appliance-Installationsprogramm 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 im Grid Manager **Hilfe** > **Info**).

   Die zweite Ziffer in den beiden Versionen sollte übereinstimmen. Wenn auf Ihrem StorageGRID-System beispielsweise die Version 11.**5**.*x*.*y* ausgeführt wird, sollte die StorageGRID Appliance Installer-Version 3.**5**.*z* sein.

3. Wenn die Appliance über eine übergeordnete Version des Installationsprogramms für StorageGRID Appliances verfügt, wechseln Sie zur Seite NetApp Downloads für StorageGRID.

   "NetApp Downloads: StorageGRID"

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 Datei Support für StorageGRID Appliances ist eine `.zip` Archiv, das die aktuellen und vorherigen Firmware-Versionen für alle StorageGRID Appliance-Modelle enthält, in Unterverzeichnissen für jeden Controller-Typ.

   Nach dem Herunterladen der Datei Support für StorageGRID Appliances extrahieren Sie den `.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 des Installationsprogramms für StorageGRID-Geräte, um die folgenden Schritte auszuführen:
   a. Laden Sie die entsprechende Support-Datei (Firmware-Image) für den Controller-Typ und die Prüfsummendatei hoch.
   b. Aktualisieren Sie die inaktive Partition.
   c. Starten Sie neu und tauschen Sie die Partitionen aus.
   d. Aktualisieren Sie die zweite Partition.

Verwandte Informationen

"Zugriff auf das Installationsprogramm der StorageGRID-Appliance"

Konfigurieren von Netzwerk-Links (SG5700)

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.

Was Sie benötigen

Wenn Sie Vorhaben, die 25-GbE-Linkgeschwindigkeit für die 10/25-GbE-Ports zu verwenden:

- Sie haben SFP28-Transceiver in den Ports installiert, die Sie verwenden möchten.
- Sie haben die Ports mit Switches verbunden, die diese Funktionen unterstützen.
- Sie verstehen, wie Sie die Switches konfigurieren, um diese höhere Geschwindigkeit zu verwenden.

Wenn Sie planen, den aggregierten Port Bond-Modus, den LACP Network Bond-Modus oder das VLAN-Tagging für die 10/25-GbE-Ports zu verwenden:

- Sie haben die 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.

- Wenn Sie den Active-Backup-Modus für das Admin-Netzwerk verwenden möchten, haben Sie Ethernet-Kabel mit beiden Management-Ports am Controller verbunden.

Über diese Aufgabe

Die Abbildung zeigt, wie die vier 10/25-GbE-Ports im Bond-Modus mit festen Ports (Standardkonfiguration) verbunden sind.

	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.

Diese Abbildung zeigt, wie die vier 10/25-GbE-Ports im Bond-Modus für aggregierte Ports verbunden sind.

	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. Die Standardeinstellungen werden fett dargestellt. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standardeinstellung verwenden möchten.

- **Festes (Standard) Port Bond-Modus**

Netzwerk-Bond-Modus	**Client-Netzwerk deaktiviert (Standard)**	**Client-Netzwerk aktiviert**
Active-Backup (Standard)	• 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.	• 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.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
LACP (802.3ad)	• 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.	• 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.

- * Aggregat-Port-Bond-Modus*

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad	• Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. • Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete.	• 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.

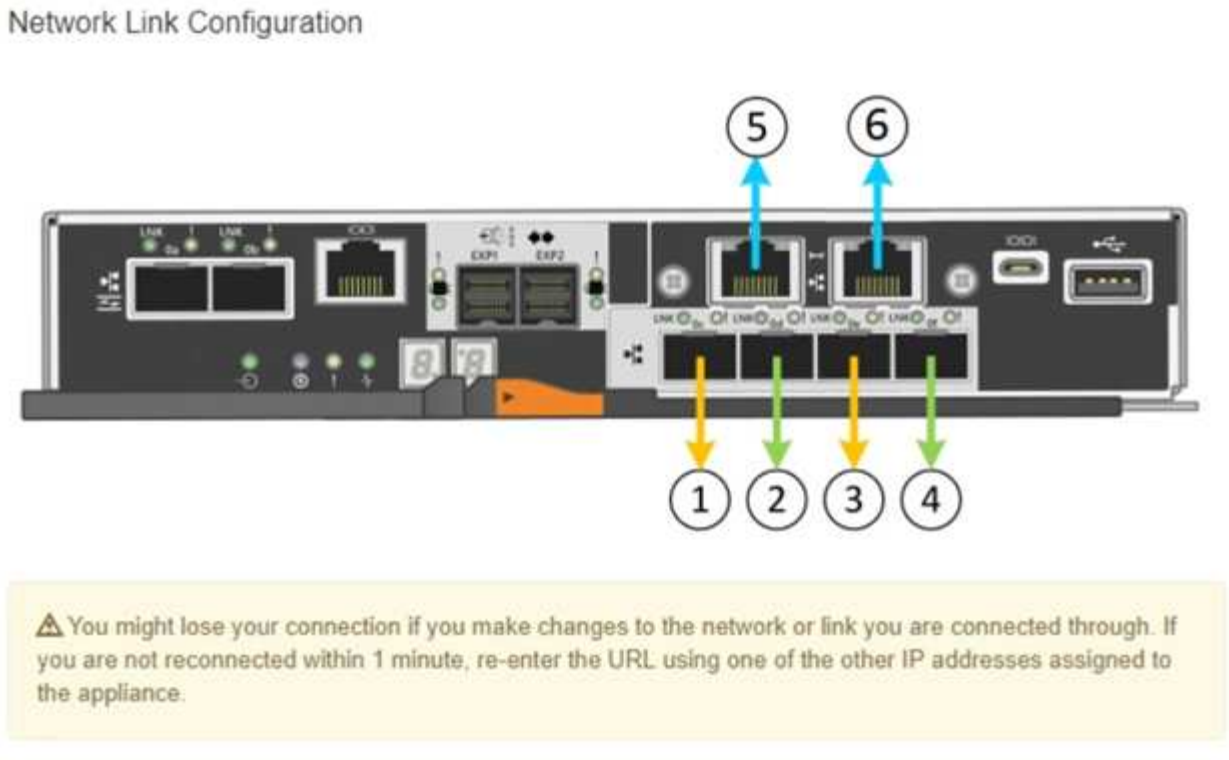
Weitere Informationen zu Port Bond- und Netzwerk-Bond-Modi finden Sie in den Informationen zu 10/25-GbE-Port-Verbindungen für den E5700SG Controller.

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.

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.



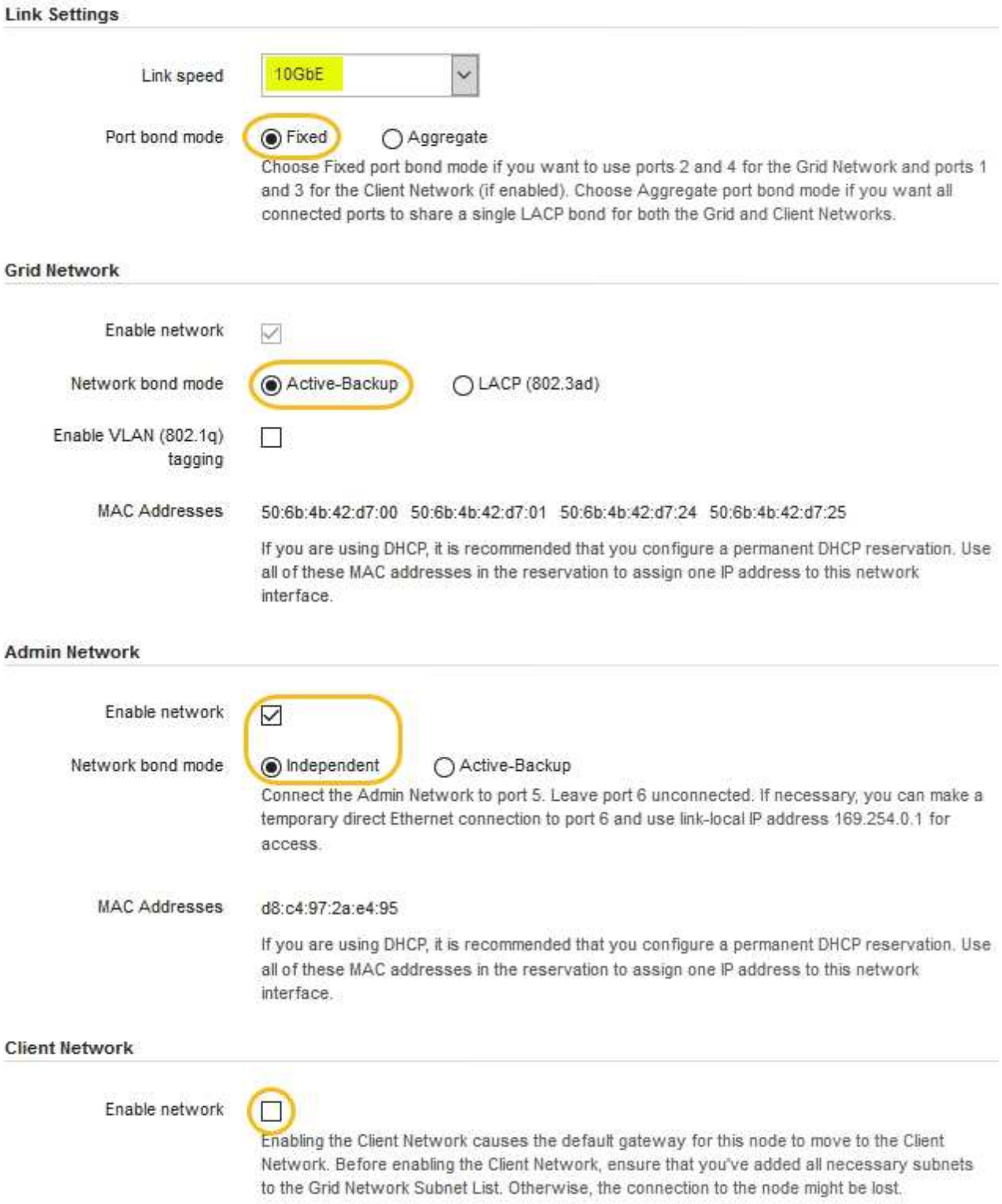
In der Tabelle „Link-Status“ werden der Verbindungsstatus (nach oben/unten) und die Geschwindigkeit (1/10/25/40/100 Gbit/s) der nummerierten Ports aufgeführt.

Link Status

Link	State	Speed (Gbps)
1	Up	25
2	Up	25
3	Up	25
4	Up	25
5	Up	1
6	Up	1

Das erste Mal, wenn Sie diese Seite aufrufen:

- **Link Speed** ist auf **10GbE** eingestellt.
- **Port Bond Modus** ist auf **fest** eingestellt.
- **Network Bond-Modus** für das Grid-Netzwerk ist auf **Active-Backup** eingestellt.
- Das **Admin-Netzwerk** ist aktiviert, und der Netzwerk-Bond-Modus ist auf **unabhängig** eingestellt.
- Das **Client-Netzwerk** ist deaktiviert.



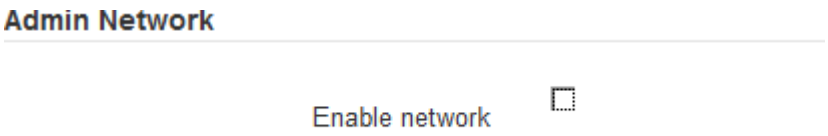
2. Wenn Sie die 25-GbE-Verbindungsgeschwindigkeit für die 10/25-GbE-Ports verwenden möchten, wählen Sie in der Dropdown-Liste Link Speed * 25 GbE* aus.

   Die Netzwerk-Switches, die Sie für das Grid-Netzwerk und das Client-Netzwerk verwenden, müssen ebenfalls für diese Geschwindigkeit konfiguriert sein. SFP28 Transceiver müssen in den Ports installiert sein.

3. Aktivieren oder deaktivieren Sie die StorageGRID-Netzwerke, die Sie verwenden möchten.

Das Grid-Netzwerk ist erforderlich. Sie können dieses Netzwerk nicht deaktivieren.

a. Wenn das Gerät nicht mit dem Admin-Netzwerk verbunden ist, deaktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Admin-Netzwerk.



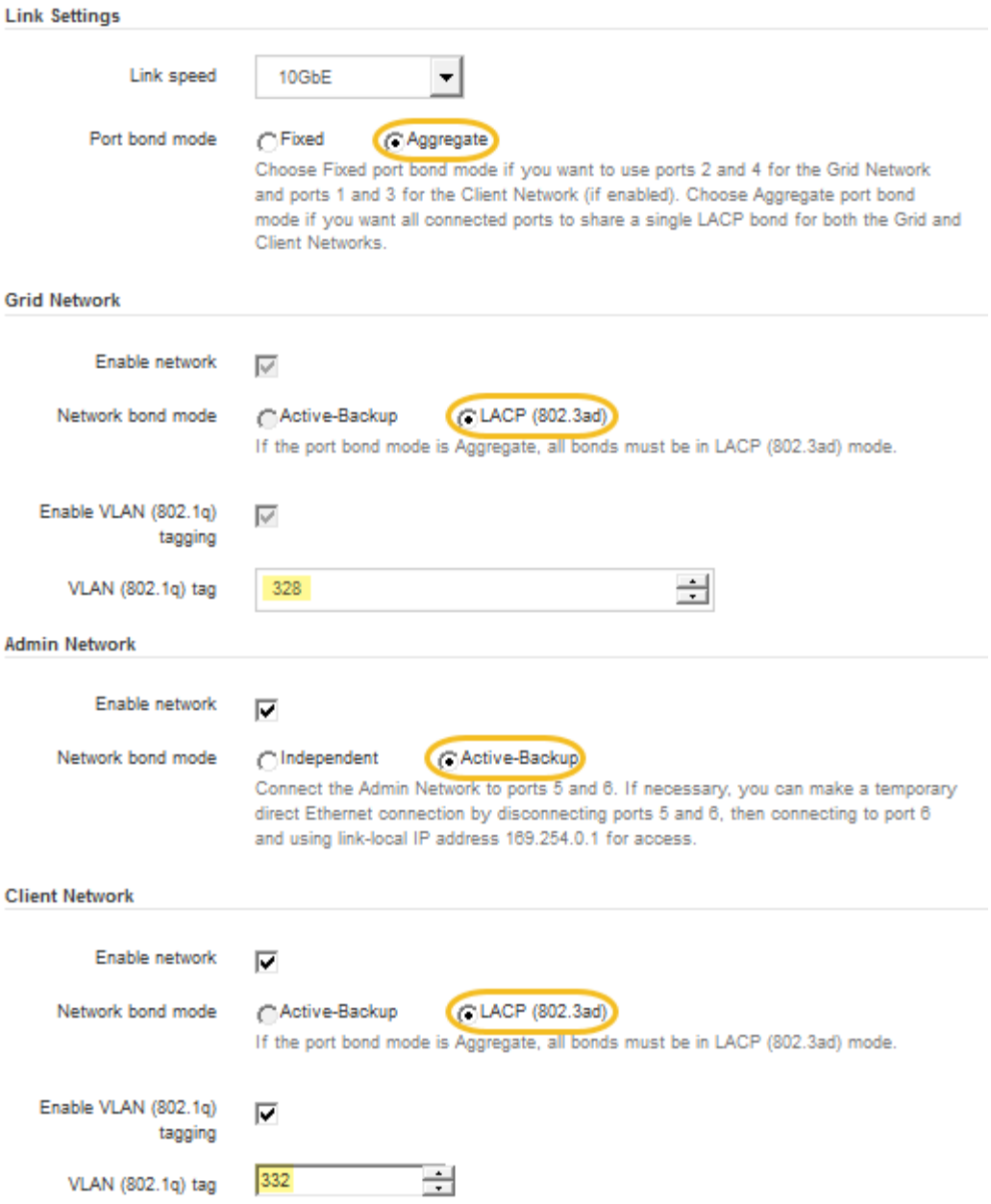
b. Wenn das Gerät mit dem Client-Netzwerk verbunden ist, aktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Client-Netzwerk.

   Die Client-Netzwerk-Einstellungen für die 10/25-GbE-Ports werden nun angezeigt.

4. In der Tabelle finden Sie Informationen zum Konfigurieren des Port-Bond-Modus und des Netzwerk-Bond-Modus.

   Das 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.



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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:
> **`https://E5700SG_Controller_IP:8443`**

Verwandte Informationen

"Port Bond-Modi für E5700SG Controller-Ports"

Einstellen der IP-Konfiguration

Mit dem Installationsprogramm der StorageGRID-Appliance können Sie die für den

Appliance-Speicherknoten verwendeten IP-Adressen und Routing-Informationen im StorageGRID-Raster, Administrator und Client-Netzwerke konfigurieren.

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.

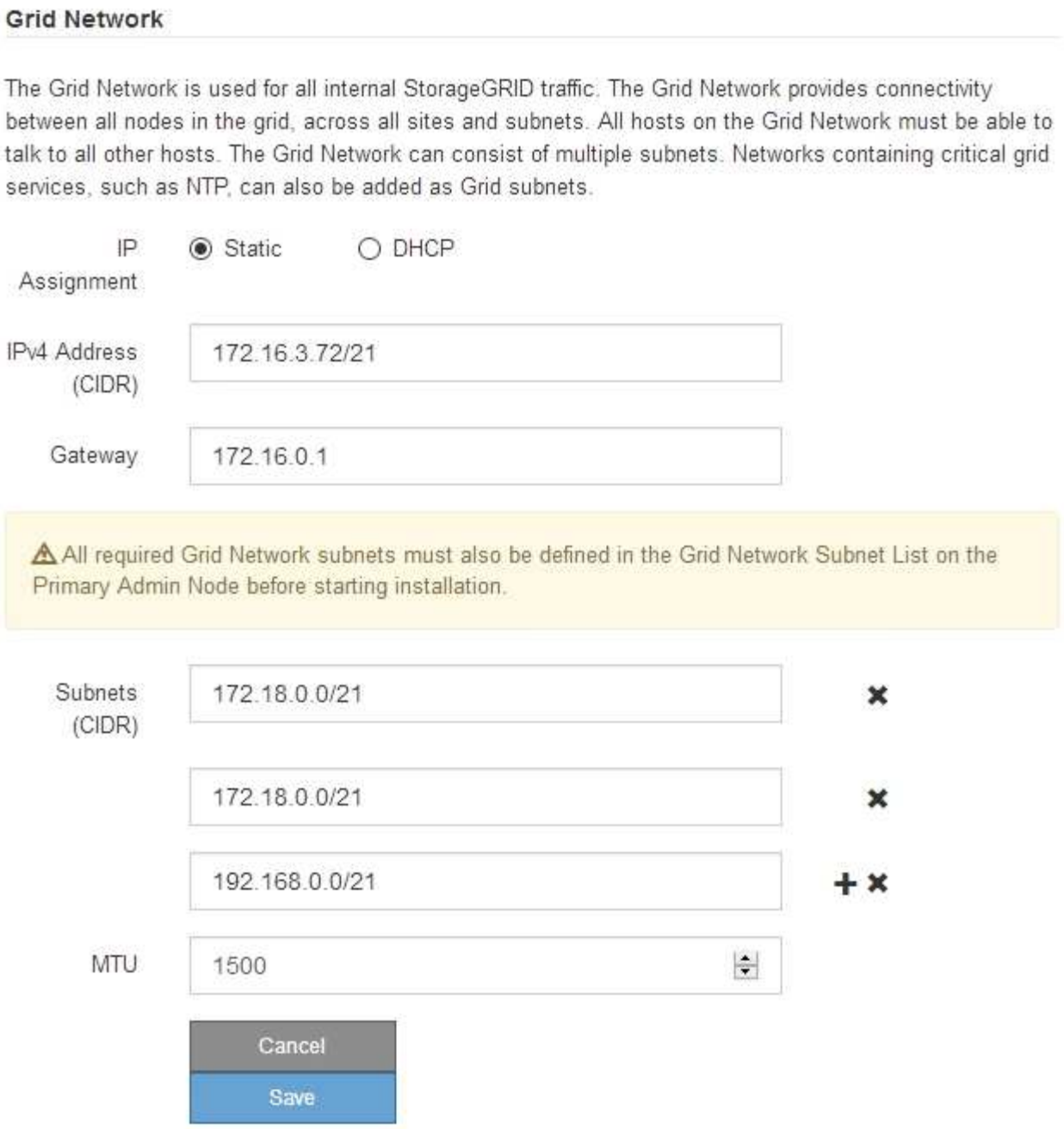
Wenn Sie die Link-Konfiguration ändern möchten, lesen Sie die Anweisungen zum Ändern der Link-Konfiguration des E5700SG-Controllers.

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 identisch 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://services_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 Löschsymbol ✖.

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.

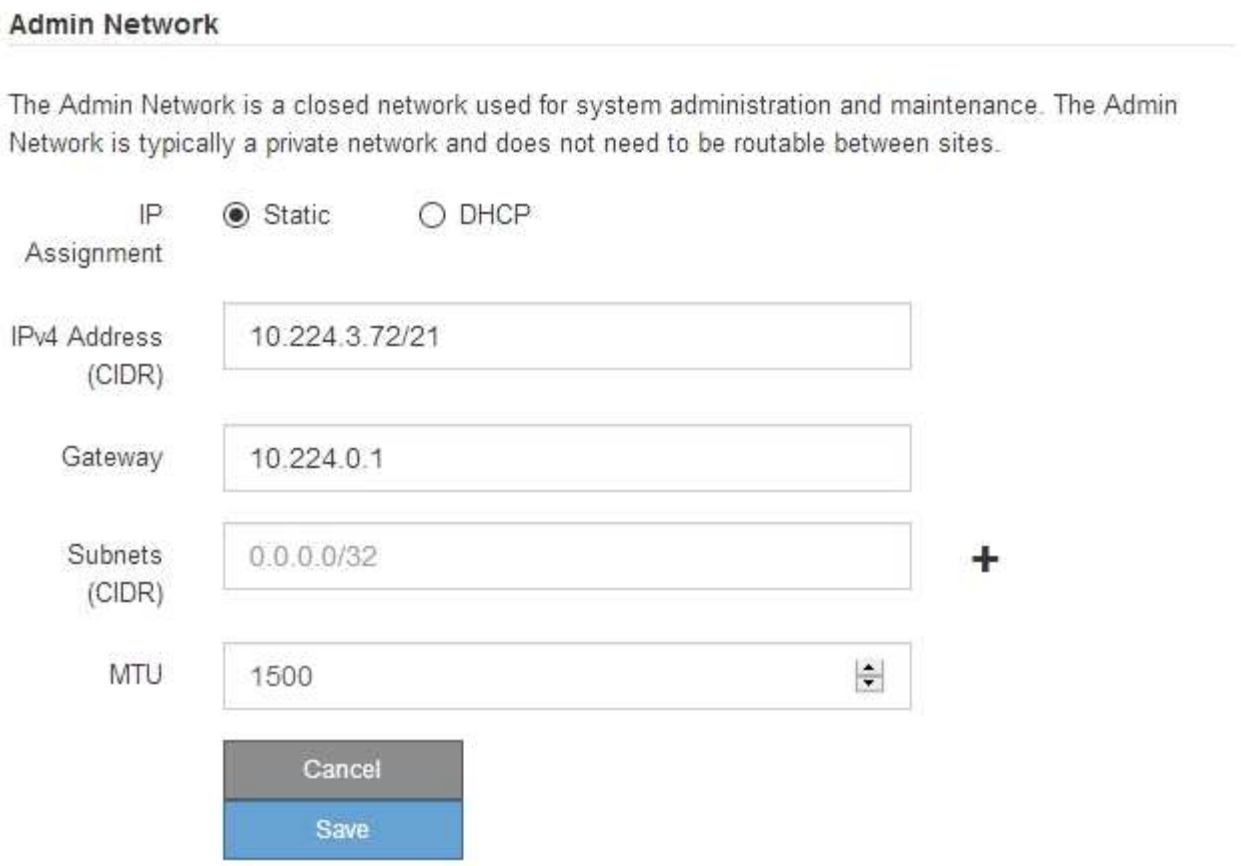
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch 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, müssen Sie das Admin-Netzwerk auf der Seite Link Configuration aktivieren.



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://services_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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

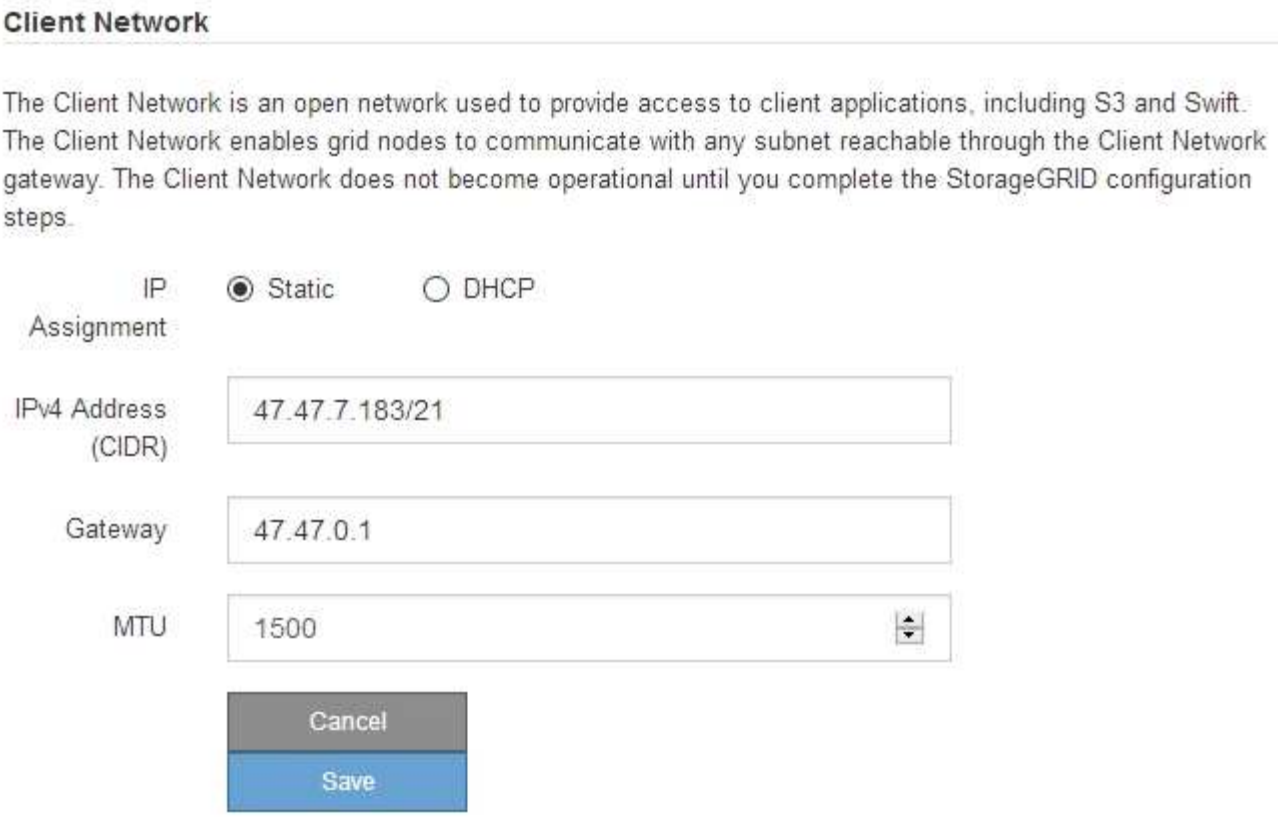
c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.

> 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, müssen Sie das Client-Netzwerk auf der Seite Link Configuration aktivieren.



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.

Verwandte Informationen

"Ändern der Link-Konfiguration des E5700SG-Controllers"

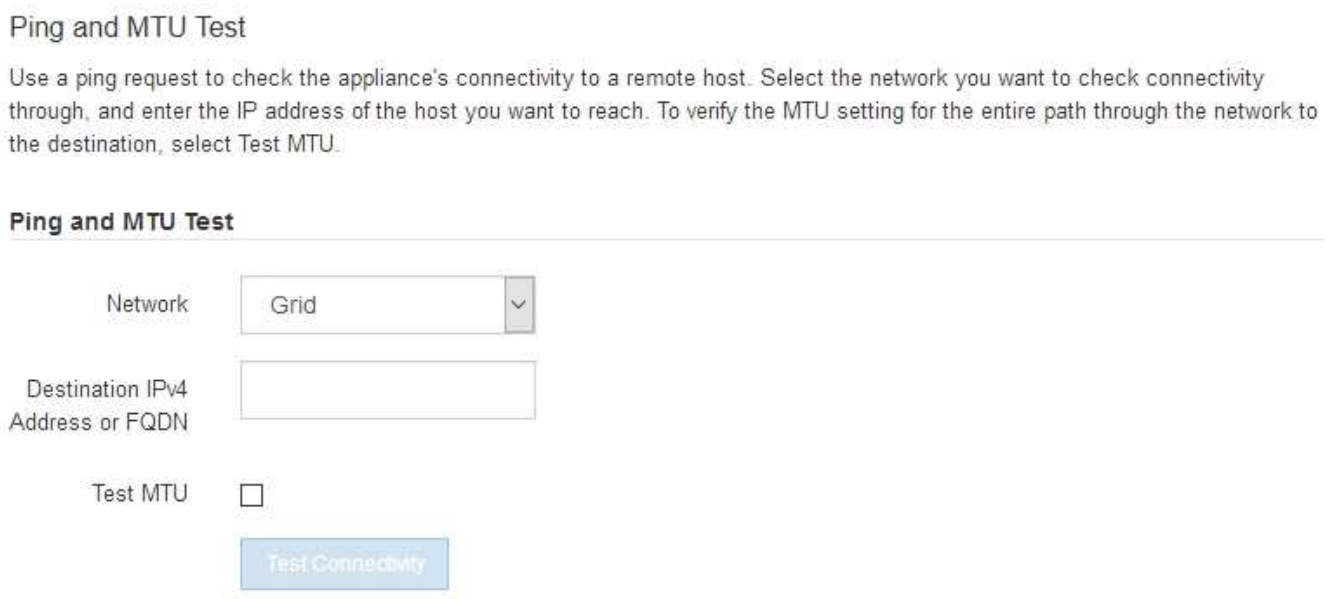
Netzwerkverbindungen werden überprüft

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.



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 Domänennamen (FQDN) für einen Host in diesem Netzwerk ein.

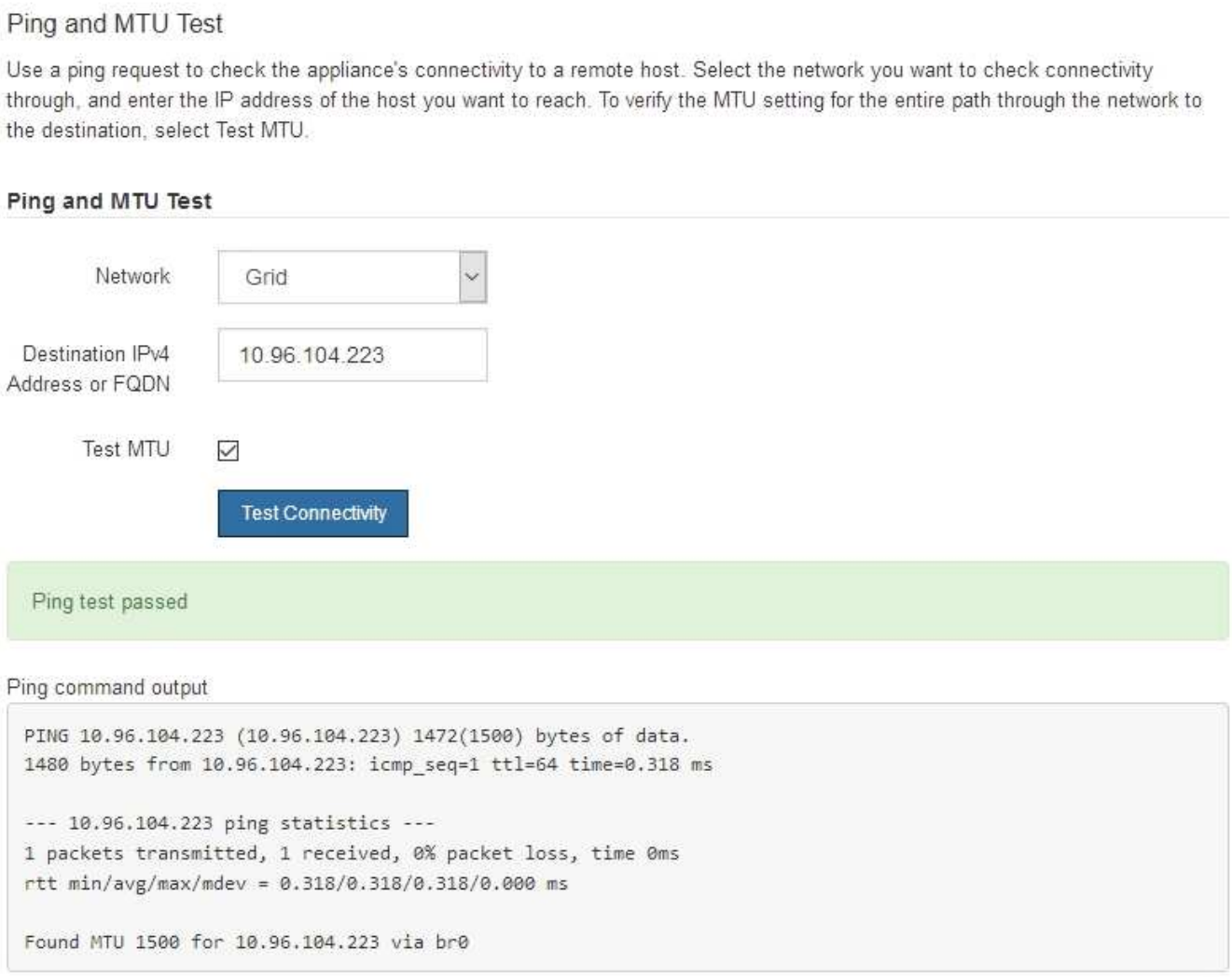
   Beispielsweise möchten Sie das Gateway im Netzwerk oder den primären Admin-Node pingen.

4. Aktivieren Sie optional das Kontrollkästchen **MTU-Test**, 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.



Verwandte Informationen

"Konfigurieren von Netzwerk-Links (SG5700)"

"Ändern der MTU-Einstellung"

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 unter der Portreferenz in den Netzwerkrichtlinien von StorageGRID.

> Die in der Tabelle für die Portkonnektivität aufgeführten Grid-Netzwerkports sind nur für StorageGRID Version 11.5 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.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

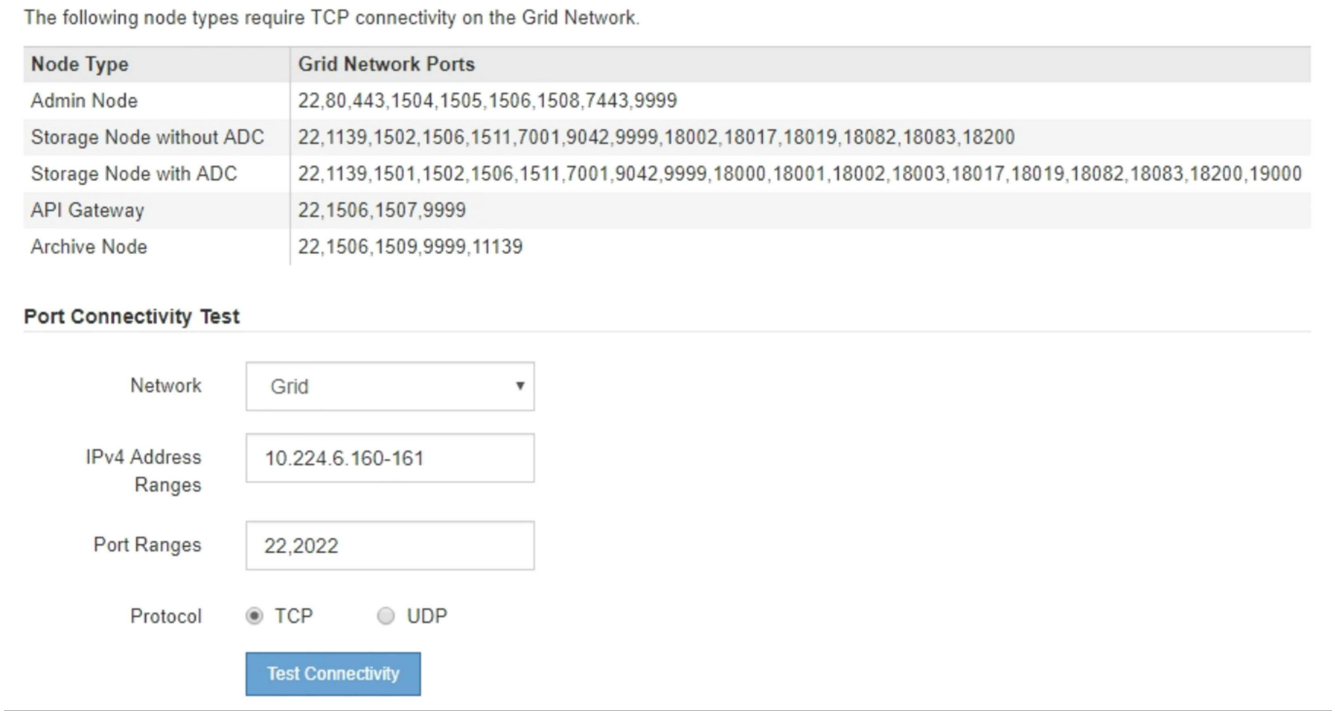
   Sie können die Verbindung zwischen den in der Tabelle aufgeführten Appliance-Ports und den anderen Nodes im Grid-Netzwerk testen.

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.



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.

   - 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.

- Wenn für einen oder mehrere ausgewählte Ports keine Netzwerkverbindung auf Portebene hergestellt werden kann, wird die Meldung „`Verbindungstest 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.

Verwandte Informationen

"Netzwerkrichtlinien"

Zugriff auf und Konfigurieren von SANtricity System Manager

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 von SANtricity System Manager und Zugriff auf diese zugreifen

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.

Was Sie benötigen

- Sie verwenden einen unterstützten Webbrowser.
- Um über den Grid Manager auf SANtricity-System-Manager zuzugreifen, müssen Sie StorageGRID installiert haben, und Sie müssen über die Berechtigung zum Administrator der Speichergeräte oder Root-Zugriff verfügen.
- Um mit dem StorageGRID-Appliance-Installationsprogramm auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity-System-Managers verfügen.
- Um direkt über einen Webbrowser auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity System Managers verfügen.

> 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, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring 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 den StorageGRID-Appliance-Installer oder den Grid-Manager nicht verwenden können, können

Sie über einen Webbrowser, der mit dem Management-Port verbunden ist, direkt auf 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 Konfigurieren von Warnmeldungen zur Hardware Schritt:

> 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 zum E-Series AutoSupport finden Sie im Dokumentationszentrum zur E-Series.

  "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 **Knoten** > ***appliance Storage Node*** > **SANtricity System Manager**

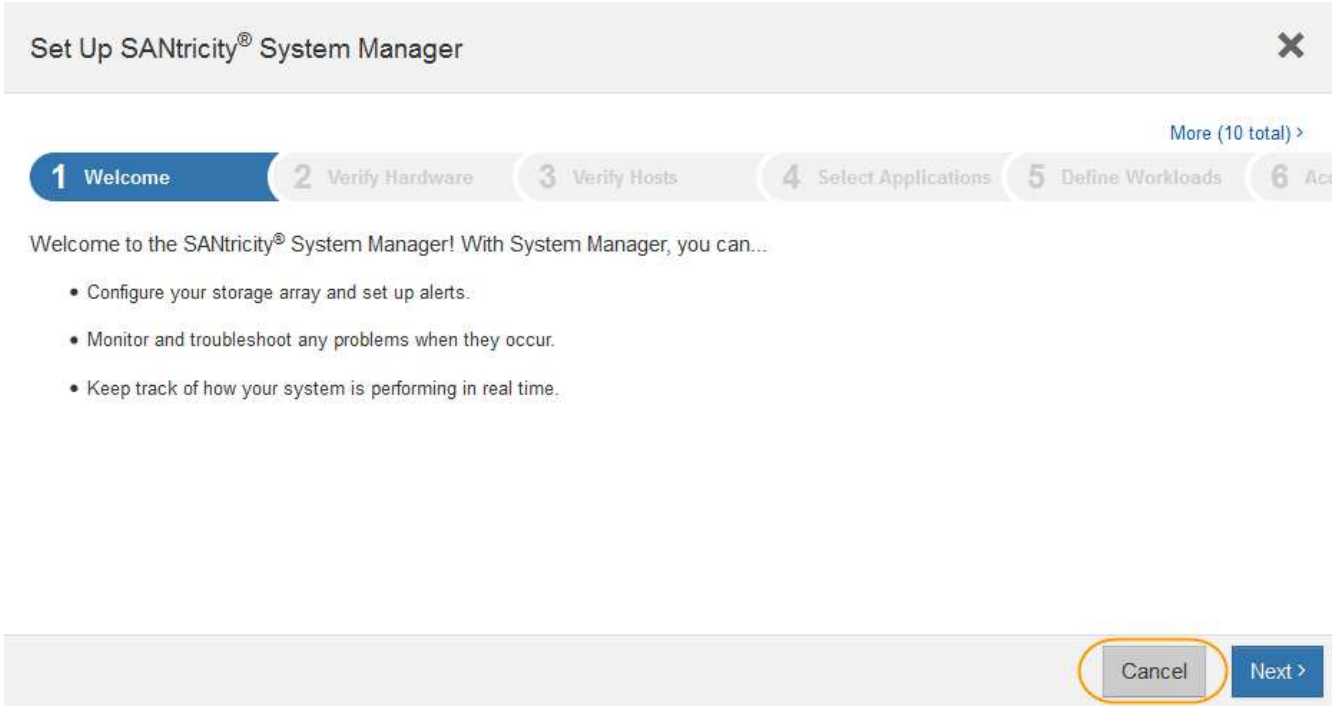
     > Wenn diese Optionen nicht verfügbar sind oder die Anmeldeseite nicht angezeigt wird, müssen Sie die IP-Adresse des Storage Controllers verwenden. Greifen Sie auf SANtricity System Manager zu, indem Sie die Storage Controller-IP aufrufen: **`https://Storage_Controller_IP`**

   Die Anmeldeseite für den SANtricity System Manager wird angezeigt.

2. Legen Sie das Administratorpasswort fest oder geben Sie es ein.

   > SANtricity System Manager verwendet ein einziges Administratorkennwort, das von allen Benutzern verwendet wird.

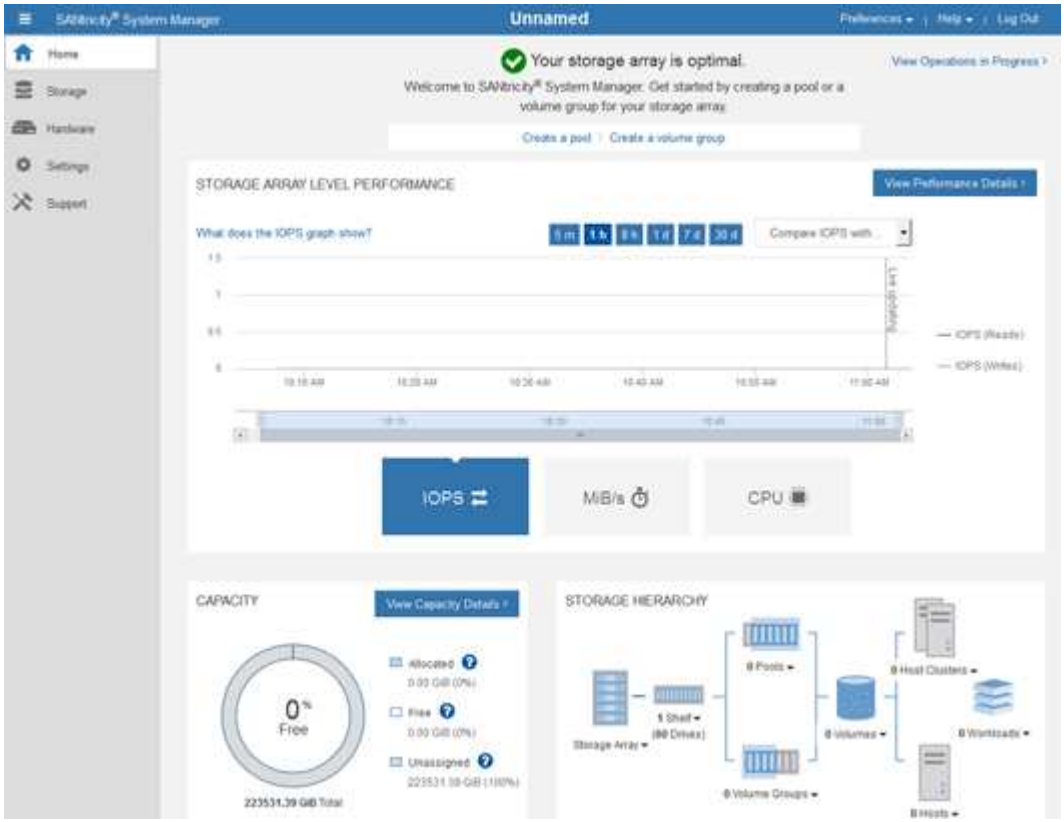
Der Einrichtungsassistent wird angezeigt.



3. Wählen Sie **Abbrechen**, um den Assistenten zu schließen.

> Schließen Sie den Setup-Assistenten für eine StorageGRID Appliance nicht ab.

Die Startseite von SANtricity System Manager wird angezeigt.



1. Konfigurieren von Warnmeldungen zur Hardware
   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.
2. 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. Verwenden Sie den Abschnitt **Support** > **Support Center** der Online-Hilfe, um mehr über die AutoSupport-Funktion zu erfahren.
   c. Folgen Sie den Anweisungen „`Anleitung`“, um AutoSupport zu managen.

      Genaue Anweisungen zur Konfiguration eines StorageGRID Proxy zum Senden von AutoSupport Nachrichten der E-Series ohne Verwendung des Management Ports finden Sie unter den Anweisungen für die Administration der StorageGRID. Suchen Sie nach „Proxy-Einstellungen für E-Series AutoSupport“.

   "StorageGRID verwalten"
3. 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.
4. 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 zum Ändern des Kennworts.

Überprüfen des 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. Komponententententententemperaturen oder Problemen mit den Laufwerken, überprüft.

Was Sie benötigen

- Sie verwenden einen unterstützten Webbrowser.
- Um über den Grid Manager auf SANtricity System Manager zuzugreifen, müssen Sie über die Administratorberechtigung für die Speicheranwendung oder über die Berechtigung für den Root-Zugriff verfügen.
- Um mit dem StorageGRID-Appliance-Installationsprogramm auf SANtricity System Manager zuzugreifen,

müssen Sie über den Benutzernamen und das Kennwort des SANtricity-System-Managers verfügen.

- Um direkt über einen Webbrowser auf SANtricity System Manager zuzugreifen, müssen Sie über den Benutzernamen und das Kennwort des SANtricity System Managers verfügen.

> 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, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Installations- und Wartungsanweisungen für Ihr Gerät.

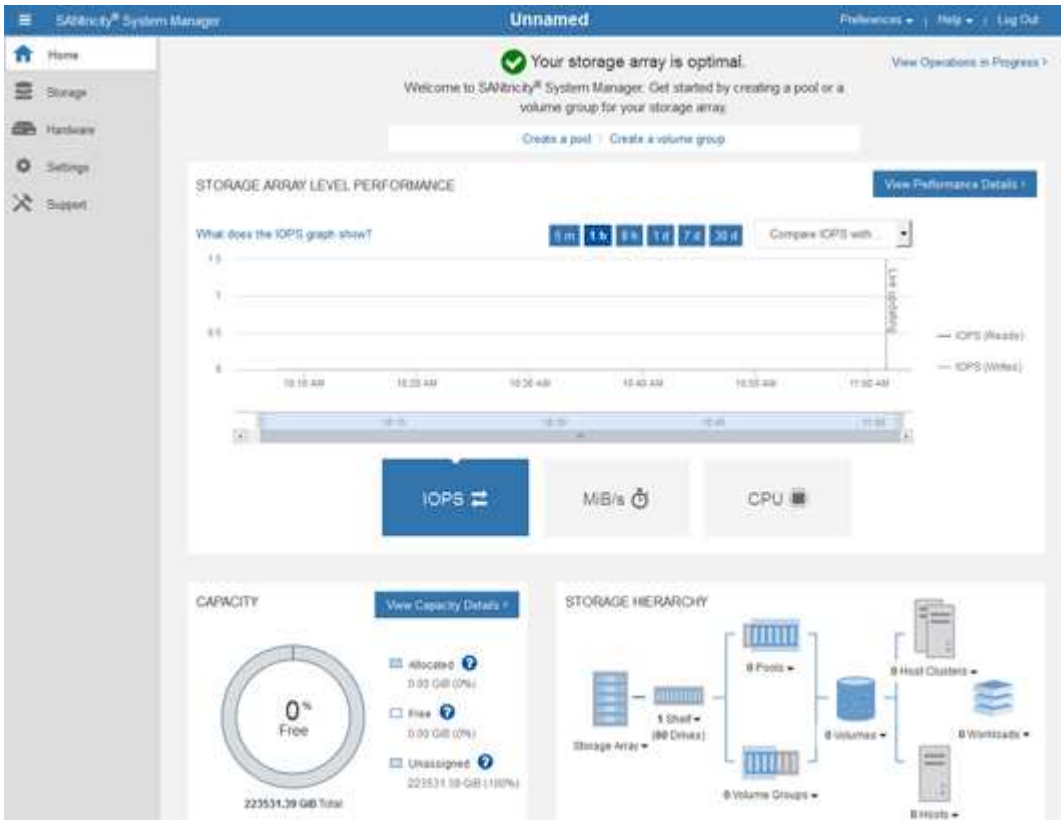
Schritte

1. Greifen Sie auf SANtricity System Manager zu.

   "Einrichten von SANtricity System Manager und Zugriff auf diese zugreifen"

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.

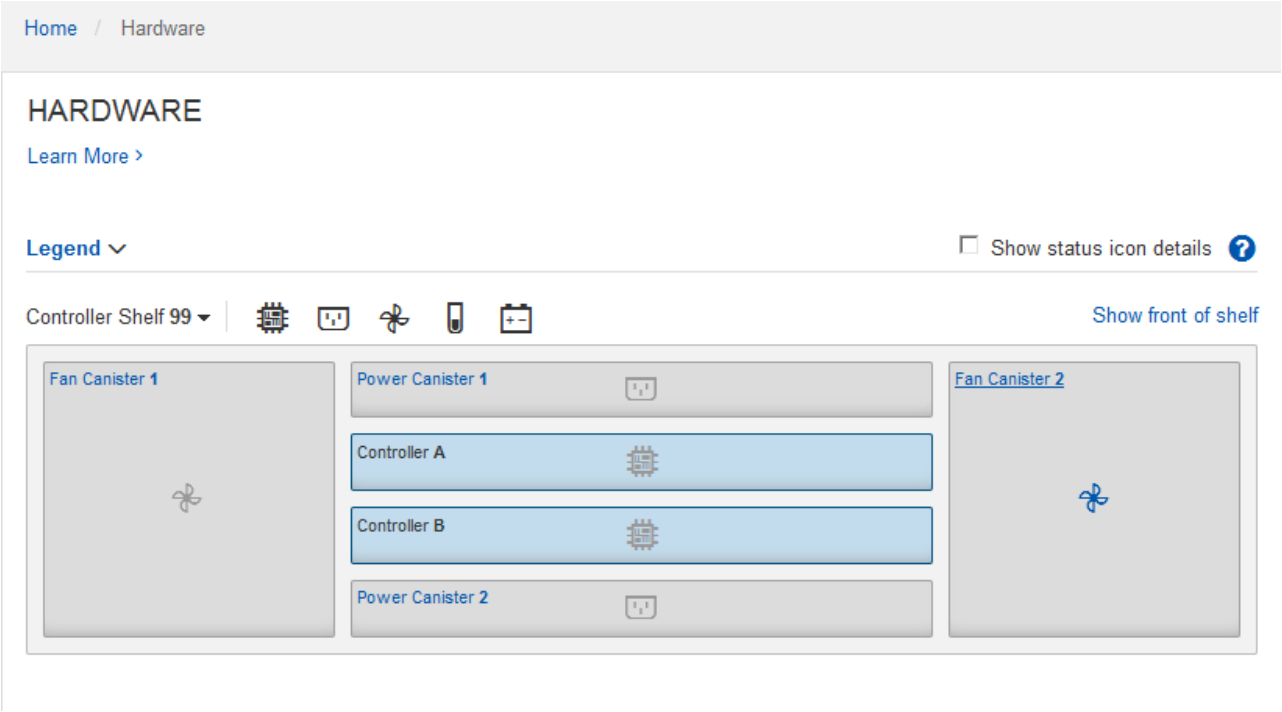
   Die Startseite von SANtricity System Manager wird angezeigt. In SANtricity System Manager wird das Controller Shelf als Storage-Array bezeichnet.



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 Shelfs können Sie sowohl Storage-Controller als auch den Akku in jedem Storage Controller, die beiden Power Kanister, die beiden Lüfter-Kanister und Erweiterungs-Shelfs (falls vorhanden) anzeigen. Sie können auch Komponententententemperaturen 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 Shelfs können die Laufwerke und die Laufwerksfächer für das Storage Controller-Shelf oder die Erweiterungs-Shelfs (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.

Festlegen der IP-Adressen für die Speichercontroller mithilfe des StorageGRID-Appliance-Installationsprogramms

Management-Port 1 auf jedem Storage-Controller verbindet die Appliance mit dem Managementnetzwerk für SANtricity System Manager. Wenn Sie vom StorageGRID Appliance Installer nicht auf den SANtricity System Manager zugreifen können, müssen Sie für jeden Storage Controller eine statische IP-Adresse festlegen, um sicherzustellen, dass die Managementverbindung zur Hardware und der Controller-Firmware im Controller-Shelf nicht unterbrochen wird.

Was Sie benötigen

- 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.

> Führen Sie diese Schritte nur aus, wenn Sie über den StorageGRID Appliance Installer (**Erweitert** > **SANtricity System Manager**) oder Grid Manager (**Knoten** > **SANtricity System Manager**) keinen Zugriff auf den 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-Netzwerkkonfiguration**.

   Die Seite Speichercontroller-Netzwerkkonfiguration wird angezeigt.

3. Wählen Sie je nach Netzwerkkonfiguration **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.

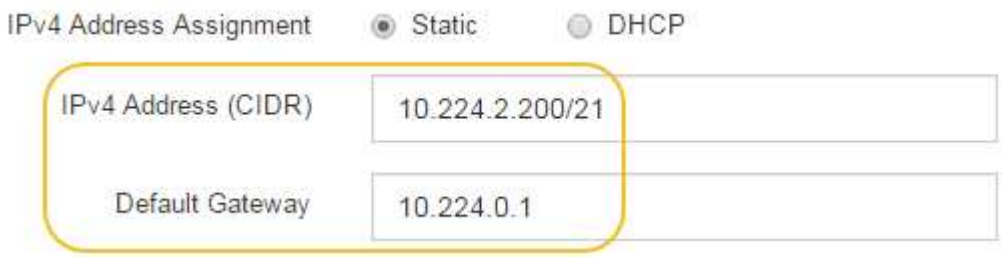
   > Es kann einige Minuten dauern, bis die DHCP-Werte angezeigt werden.

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.

   a. Wählen Sie **Statisch**.
   b. Geben Sie die IPv4-Adresse unter Verwendung der CIDR-Schreibweise ein.

c. Geben Sie das Standard-Gateway ein.



d. 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`

Optional: Aktivieren der Node-Verschlüsselung

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. Bei der Installation der Appliance müssen Sie die Node-Verschlüsselung auswählen und aktivieren. Die Auswahl der Node-Verschlüsselung kann nicht rückgängig gemacht werden, sobald der KMS-Verschlüsselungsprozess gestartet wird.

Was Sie benötigen

Lesen Sie die Informationen über KMS in den Anweisungen zur Administration von StorageGRID durch.

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.

Alle Daten, die vor einer Appliance mit aktivierter Node-Verschlüsselung vorhanden sind, werden mit einem nichtsicheren temporären Schlüssel verschlüsselt. Das Gerät ist erst dann vor dem Entfernen oder Diebstahl geschützt, wenn der Schlüssel auf einen vom KMS angegebenen Wert gesetzt wird.

Ohne den KMS-Schlüssel, der zur Entschlüsselung der Festplatte benötigt wird, können die Daten auf der Appliance nicht abgerufen und effektiv verloren gehen. 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

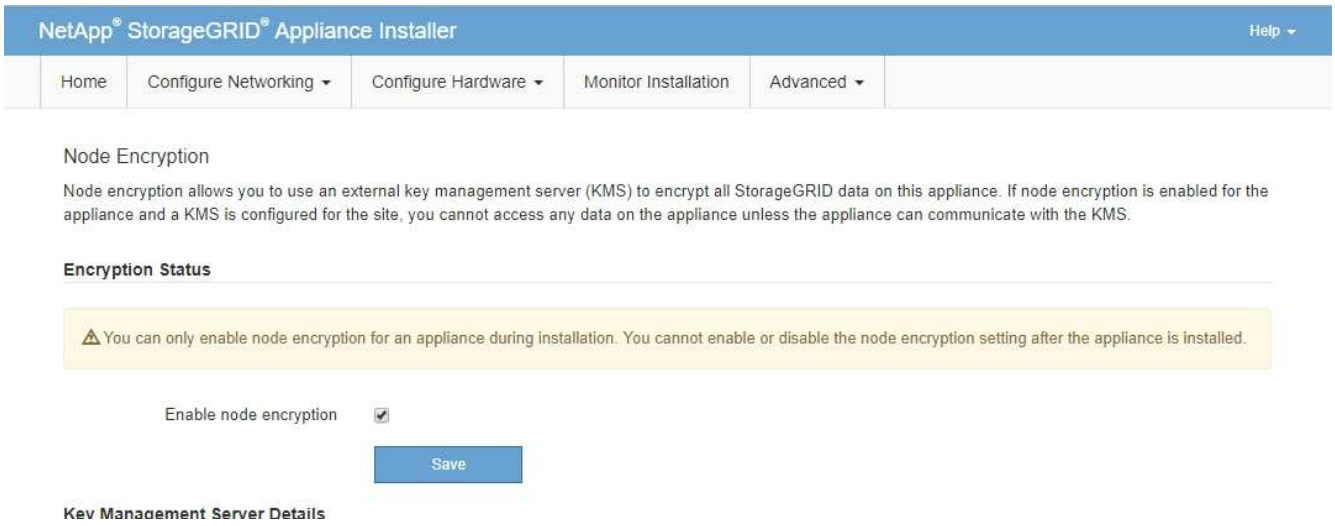
1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.
   `https://Controller_IP:8443`

   `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 Appliance-Festplatten nicht entschlüsselt werden, ohne dabei den gleichen KMS-Schlüssel zu verwenden.

2. Wählen Sie **Hardware Konfigurieren** > **Node Encryption**.



3. Wählen Sie **Node-Verschlüsselung aktivieren**.

   Sie können die Auswahl **Enable Node Encryption** ohne Gefahr eines Datenverlusts aufheben, bis Sie **Save** auswählen und der Appliance Node auf die KMS-Verschlüsselungsschlüssel in Ihrem StorageGRID-System zugreift und mit der Festplattenverschlüsselung beginnt. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht deaktivieren.

   Nachdem Sie einer StorageGRID Site mit KMS eine Appliance hinzugefügt haben, für die die Node-Verschlüsselung aktiviert ist, kann die KMS-Verschlüsselung für den Node nicht angehalten werden.

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.

Verwandte Informationen

"StorageGRID verwalten"

"Monitoring der Node-Verschlüsselung im Wartungsmodus"

Optional: Ändern des RAID-Modus (nur SG5760)

Wenn Sie eine SG5760 mit 60 Laufwerken haben, können Sie einen anderen RAID-Modus wechseln, um Ihre Storage- und Recovery-Anforderungen zu erfüllen. Sie können den Modus nur ändern, bevor Sie den Speicherknoten der StorageGRID-Appliance bereitstellen.

Was Sie benötigen

- Sie haben eine SG5760. Wenn Sie eine SG5712 haben, müssen Sie den DDP-Modus verwenden.
- Sie verwenden jeden Client, der eine Verbindung zu StorageGRID herstellen kann.
- Der Client verfügt über einen unterstützten Webbrowser.

Über diese Aufgabe

Vor der Bereitstellung der SG5760 Appliance als Storage-Node können Sie eine der folgenden Volume-Konfigurationsoptionen wählen:

- **DDP**: Dieser Modus verwendet zwei Paritätslaufwerke pro acht Datenlaufwerke. Dies ist der Standard- und empfohlene Modus für alle Appliances. Im Vergleich zu RAID 6 bietet DDP eine bessere System-Performance, geringere Wiederherstellungszeiten nach Laufwerksausfällen und einfaches Management. DDP bietet auch Schutz vor Schubladenverlust bei Appliances mit 60 Laufwerken.
- **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 System-Performance, geringere Wiederherstellungszeiten nach Laufwerksausfällen, einfaches 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. 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 erhöhen 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.

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: Neu zuordnen von Netzwerkports für die Appliance

Möglicherweise müssen Sie die internen Ports auf dem Appliance Storage Node zu verschiedenen externen Ports neu zuordnen. Aufgrund eines Firewall-Problems müssen Sie möglicherweise Ports neu zuordnen.

Was Sie benötigen

- Sie haben zuvor auf das Installationsprogramm für StorageGRID-Geräte zugegriffen.
- Sie sind nicht konfiguriert und planen keine Konfiguration von Load Balancer-Endpunkten.

> Wenn Sie Ports neu zuordnen, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Wenn Sie Load Balancer-Endpunkte konfigurieren und bereits neu zugeordnete Ports haben möchten, befolgen Sie die Schritte in den Recovery- und Wartungsanweisungen zum Entfernen von Port-Remaps.

Schritte

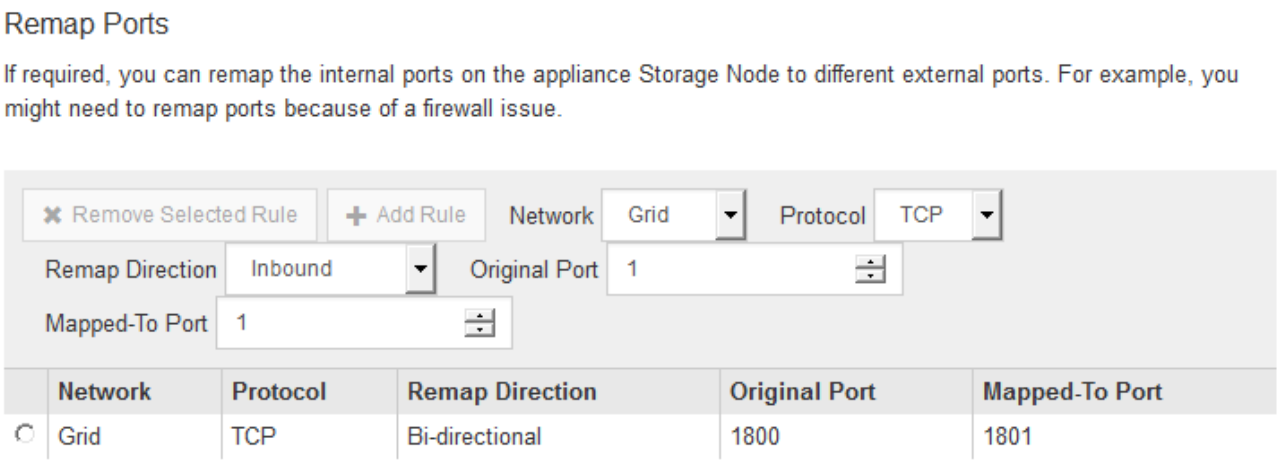
1. Klicken Sie in der Menüleiste des Installationsprogramms für StorageGRID-Geräte auf **Netzwerke konfigurieren** > **Ports für die Erinnerung**.

   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. Klicken Sie Auf **Regel Hinzufügen**.

   Die neue Port-Zuordnung wird der Tabelle hinzugefügt, und die erneute Zuordnung wird sofort wirksam.



8. Um eine Portzuordnung zu entfernen, aktivieren Sie das Optionsfeld für die Regel, die Sie entfernen möchten, und klicken Sie auf **Ausgewählte Regel entfernen**.

Implementieren eines Appliance-Storage-Node

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.

Was Sie benötigen

- Wenn Sie einen Appliance-Node klonen, fahren Sie den Recovery- und Wartungsvorgang fort.

  "Verwalten Sie erholen"

- 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.

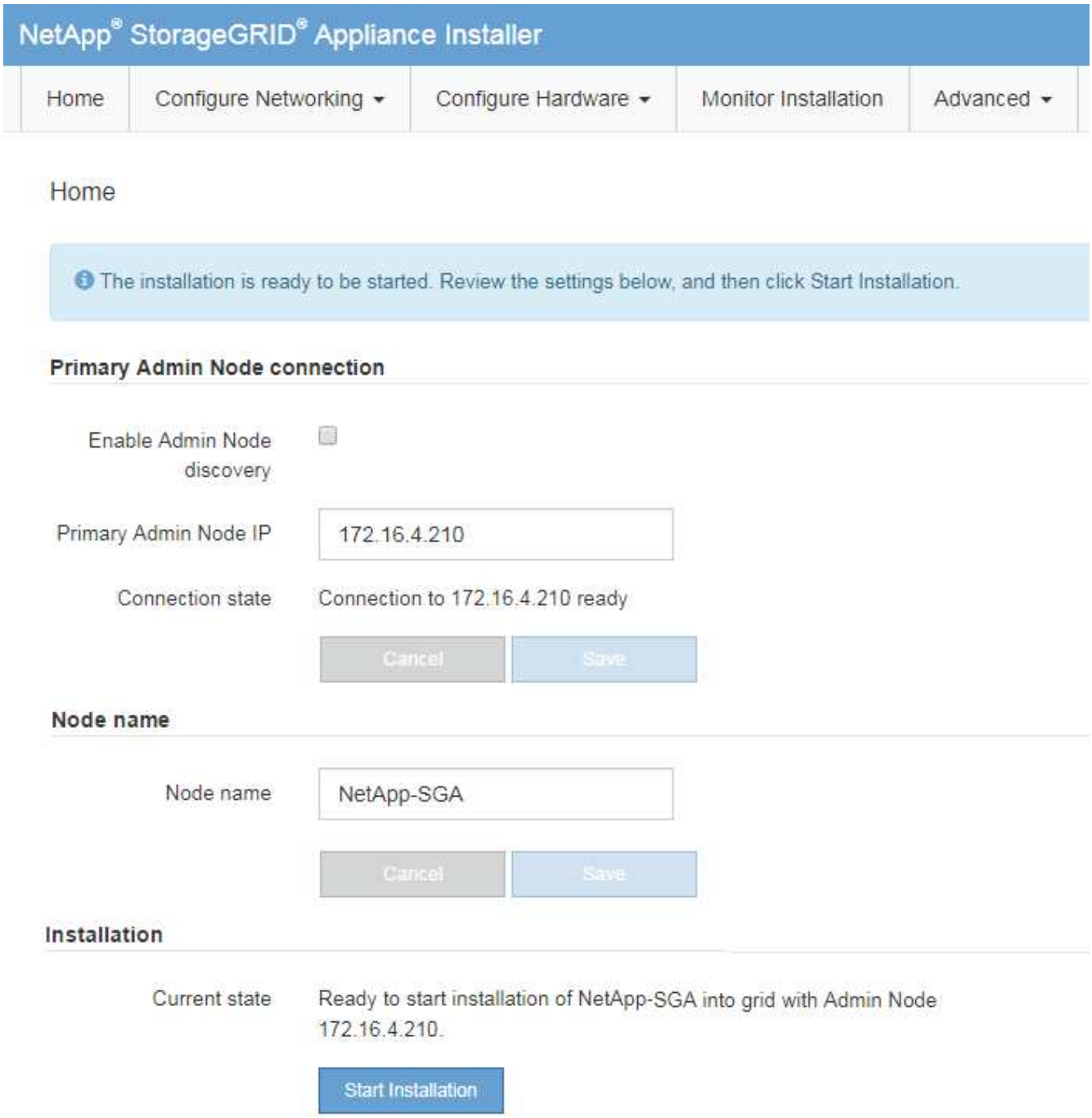
> Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisieren `configure-sga.py` Installationsskript für Geräte.

- Wenn Sie eine Erweiterung oder Wiederherstellung durchführen, befolgen Sie die entsprechenden Anweisungen:
  - Informationen zum Hinzufügen eines Appliance-Speicherknoten zu einem vorhandenen StorageGRID-System finden Sie in den Anweisungen zum erweitern eines StorageGRID-Systems.
  - Informationen zum Bereitstellen eines Appliance Storage Node im Rahmen eines Wiederherstellungsvorgangs finden Sie in den Anweisungen für Recovery und Wartung.

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	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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 klicken Sie auf **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 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 Installations- und Wartungsanleitung für Ihr Gerät.

   Wenn Sie die Storage Node Appliance als Ziel für das Klonen eines Node implementieren, beenden Sie den Implementierungsprozess hier und fahren Sie das Klonverfahren für den Node in fort "Verwalten Sie erholen".

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 automatisieren `configure-sga.py` Installationsskript für Geräte. Dieses Skript gilt nur für Speicherknoten.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

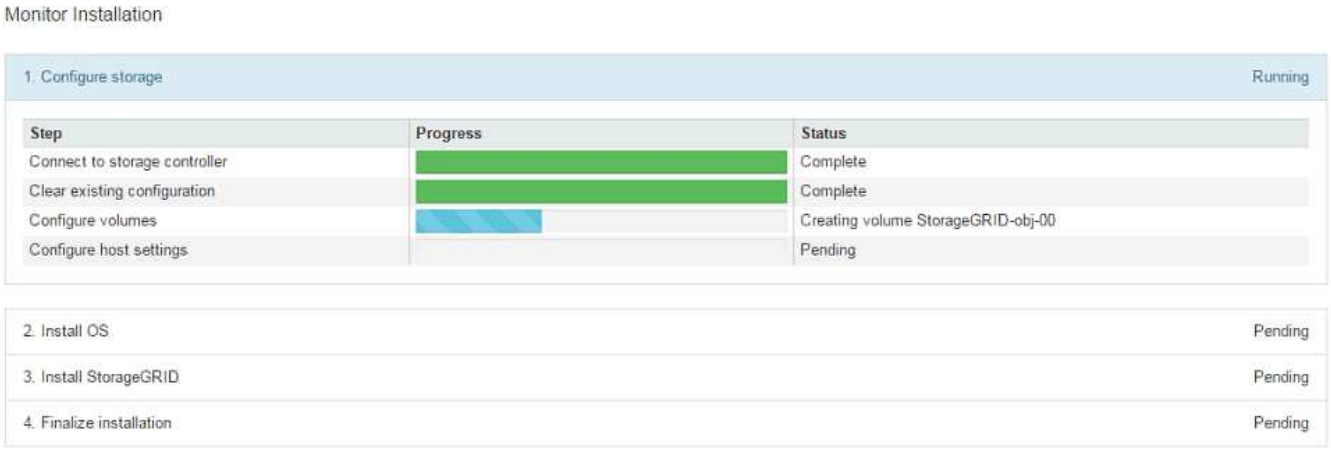
Monitoring der Installation der Speicher-Appliance

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 auf **Installation überwachen**.

   Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.



   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 „`Skipped.`“ angezeigt.

2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

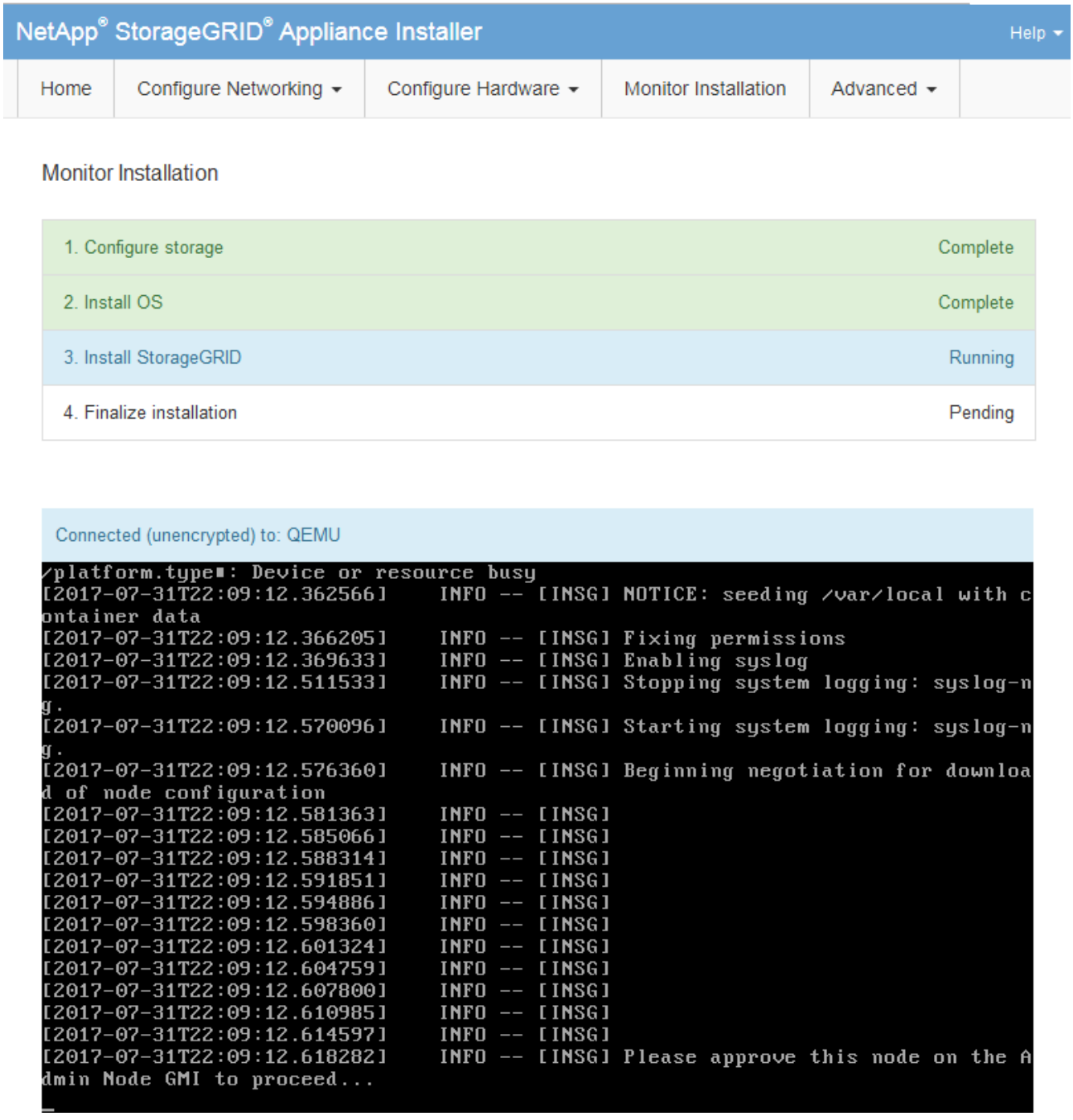
   1. Speicher konfigurieren

   In dieser Phase stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.

   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.



4. Wechseln Sie zum Grid Manager, genehmigen Sie den ausstehenden Storage-Node und führen Sie den StorageGRID-Installationsprozess aus.

   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.

Automatisierung der Installation und Konfiguration von Appliances

Sie können die Installation und Konfiguration Ihrer Appliances und die Konfiguration des gesamten StorageGRID Systems automatisieren.

Über diese Aufgabe

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

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

- Erstellen Sie eine JSON-Datei, in der die Konfigurationseinstellungen für Ihre Appliances angegeben sind. Laden Sie die JSON-Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

  Sie können dieselbe Datei verwenden, um mehr als ein Gerät zu konfigurieren.

- Verwenden Sie die StorageGRID`configure-sga.py` Python-Skript zur Automatisierung der Konfiguration Ihrer Appliances.
- Zusätzliche Python-Skripte verwenden, um andere Komponenten des gesamten StorageGRID-Systems (das „Grid“) zu konfigurieren.

  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. Weitere Informationen zum Herunterladen und Extrahieren der StorageGRID-Installationsdateien finden Sie in den Anweisungen zum Wiederherstellen und Verwalten.

Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer

Sie können die Konfiguration einer Appliance mithilfe einer JSON-Datei mit den Konfigurationsinformationen automatisieren. Sie laden die Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

Was Sie benötigen

- Ihr Gerät muss mit der neuesten Firmware ausgestattet sein, die mit StorageGRID 11.5 oder höher kompatibel ist.
- Sie müssen mit dem Installationsprogramm für StorageGRID-Geräte auf der Appliance verbunden sein, die Sie mit einem unterstützten Browser konfigurieren.

Über diese Aufgabe

Sie können Appliance-Konfigurationsaufgaben automatisieren, z. B. die Konfiguration folgender Komponenten:

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

- Verbindungsgeschwindigkeit

Die Konfiguration Ihrer Appliance mit einer hochgeladenen JSON-Datei ist häufig effizienter als die manuelle Ausführung der Konfiguration mit mehreren Seiten im StorageGRID-Appliance-Installationsprogramm, insbesondere wenn Sie viele Knoten konfigurieren müssen. Sie müssen die Konfigurationsdatei für jeden Knoten einzeln anwenden.

Erfahrene Benutzer, die sowohl die Installation als auch die Konfiguration ihrer Appliances automatisieren möchten, können das verwenden `configure-sga.py` Skript: +"Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

Schritte

1. Generieren Sie die JSON-Datei mit einer der folgenden Methoden:
   - Die ConfigBuilder-Anwendung

     "ConfigBuilder.netapp.com"

   - Der `configure-sga.py` Konfigurationsskript für die Appliance Sie können das Skript vom Installationsprogramm für StorageGRID-Geräte herunterladen (**Hilfe** > **Konfigurationsskript für Geräte**). Lesen Sie die Anweisungen zur Automatisierung der Konfiguration mit dem Skript configure-sga.py.

     "Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

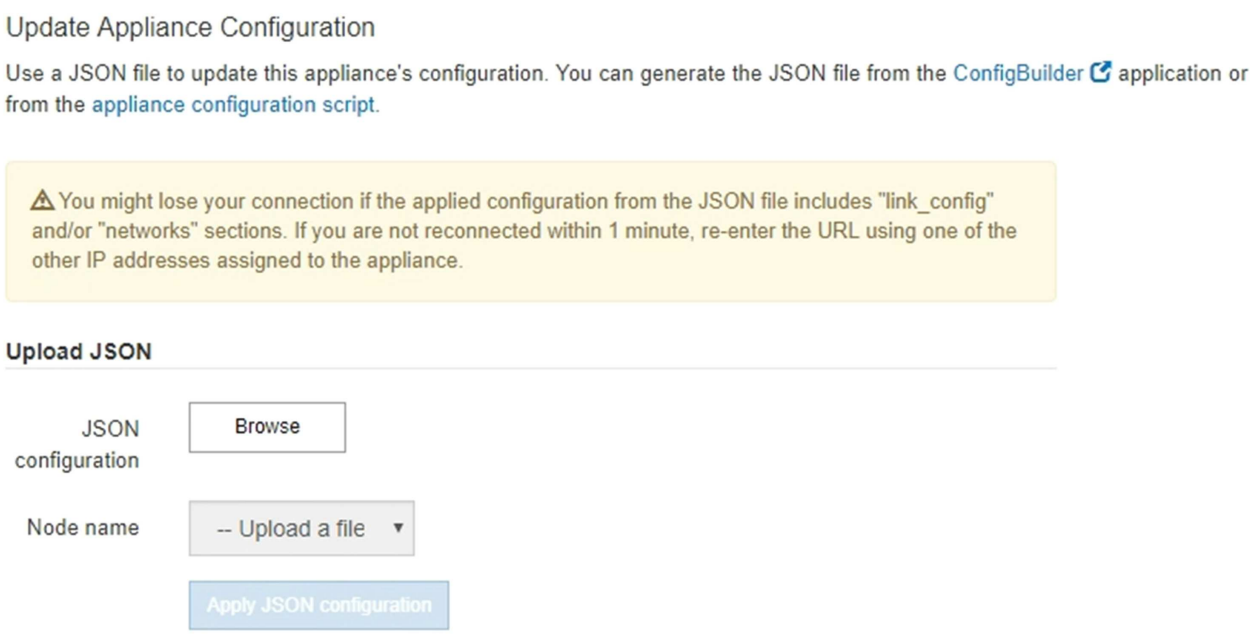
     Die Node-Namen in der JSON-Datei müssen die folgenden Anforderungen erfüllen:

     - Muss ein gültiger Hostname mit mindestens 1 und nicht mehr als 32 Zeichen sein
     - Es können Buchstaben, Ziffern und Bindestriche verwendet werden
     - Sie können nicht mit einem Bindestrich beginnen oder enden oder nur Zahlen enthalten

     Stellen Sie sicher, dass die Node-Namen (die Top-Level-Namen) in der JSON-Datei eindeutig sind, oder Sie können mit der JSON-Datei nicht mehr als einen Node konfigurieren.

2. Wählen Sie **Erweitert** > **Appliance-Konfiguration Aktualisieren**.

   Die Seite Gerätekonfiguration aktualisieren wird angezeigt.



3. Wählen Sie die JSON-Datei mit der Konfiguration aus, die Sie hochladen möchten.

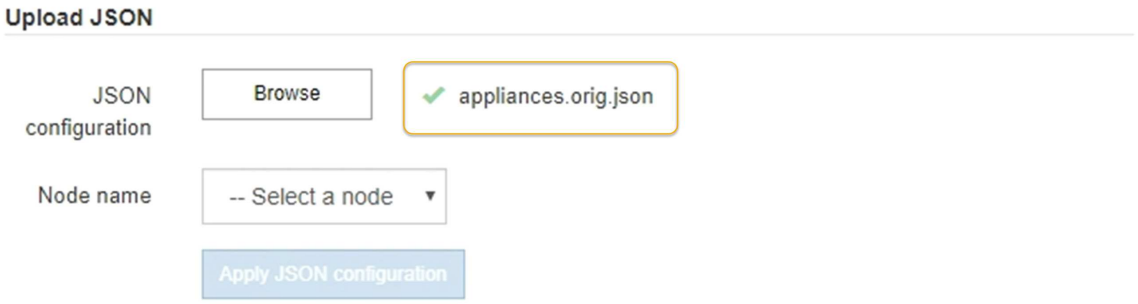
   a. Wählen Sie **Durchsuchen**.

   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 neben einem grünen Häkchen angezeigt.

   > Möglicherweise verlieren Sie die Verbindung zur Appliance, wenn die Konfiguration aus der JSON-Datei Abschnitte für „Link_config“, „Netzwerke“ oder beide enthält. Wenn Sie nicht innerhalb einer Minute eine Verbindung hergestellt haben, geben Sie die Appliance-URL mithilfe einer der anderen IP-Adressen, die der Appliance zugewiesen sind, erneut ein.

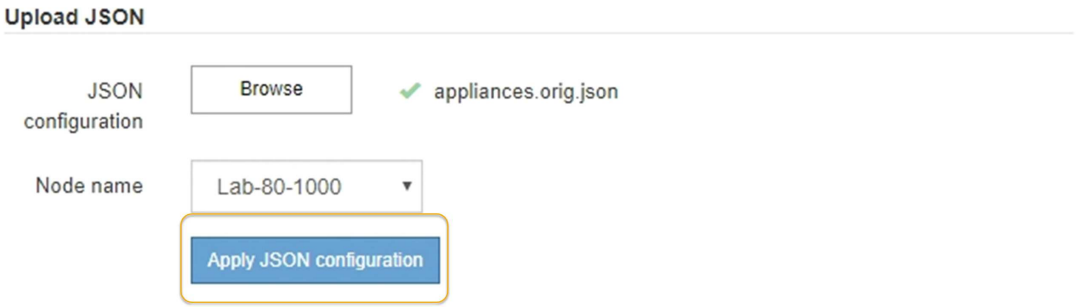


   Das Dropdown-Menü **Node Name** enthält die in der JSON-Datei definierten Node-Namen auf oberster Ebene.

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. Sie können ConfigBuilder verwenden, um sicherzustellen, dass Sie über eine gültige JSON-Datei verfügen.

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

   Die Schaltfläche **JSON-Konfiguration anwenden** ist aktiviert.



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

   Die Konfiguration wird auf den ausgewählten Knoten angewendet.

Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py

Sie können 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.

Über diese Aufgabe

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des StorageGRID Appliance Installer wurden Netzwerkverbindungen und IP-Adressen für den primären Administratorknoten konfiguriert.
- Wenn Sie den primären Admin-Node installieren, kennen Sie dessen IP-Adresse.
- Wenn Sie andere Knoten installieren und konfigurieren, wurde der primäre Admin-Node bereitgestellt, und Sie kennen seine IP-Adresse.
- Für alle anderen Nodes als den primären Admin-Node wurden alle auf der Seite IP-Konfiguration des Installationsprogramms der StorageGRID-Appliance aufgeführten Grid-Netzwerknetze in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- 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.

Dieses Verfahren richtet sich an fortgeschrittene Benutzer, die Erfahrung mit der Verwendung von Befehlszeilenschnittstellen haben. Alternativ können Sie die Konfiguration auch mit dem StorageGRID Appliance Installer automatisieren. +"Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer"

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`

3. Um die aktuelle Konfiguration des Appliance-Knotens zu bestätigen, geben Sie hier Folgendes ein *`SGA-install-ip`* Ist eine der IP-Adressen für den Appliance-Knoten:
   `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. #####
#####################################################################
```

4. 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`
5. Wenn Sie die Appliance-Konfiguration in einer JSON-Datei sichern möchten, verwenden Sie das `advanced` 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 diese Datei nur dann vor, wenn Sie ein erfahrener Benutzer sind und über die StorageGRID APIs verfügen.

6. 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`
7. Wenn Sie das Gerät neu starten möchten, geben Sie Folgendes ein:
   `configure-sga.py reboot SGA-INSTALL-IP`

Automatisierung der Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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.

   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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. 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 von Knotenklonen.
- **Verschlüsselung** — Operationen zur Verwaltung der Verschlüsselung und Anzeige des Verschlüsselungsstatus.
- **Hardwarekonfiguration** — Betrieb zur Konfiguration der Systemeinstellungen auf angeschlossener Hardware.
- **Installation** — Betrieb zum Starten der Gerätesallation und zur Überwachung des Installationsstatus.
- **Networking** — Vorgänge im Zusammenhang mit der Konfiguration von Grid-, Admin- und Client-Netzwerken für eine StorageGRID-Appliance und Appliance-Port-Einstellungen.
- **Setup** — Operationen zur Unterstützung bei der Ersteinrichtung der Appliance einschließlich Anfragen zum Abrufen von Informationen über das System und zur Aktualisierung der primären Admin-Node-IP.
- **Support** — Betrieb für den Neustart des Controllers und das Abrufen von Protokollen.
- **Upgrade** — Operationen im Zusammenhang mit der Aktualisierung der Appliance-Firmware.
- **Uploadsg** — Operationen zum Hochladen von StorageGRID-Installationsdateien.

Fehlerbehebung bei der Hardwareinstallation

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Verwandte Informationen

"Die Hardware-Einrichtung scheint zu hängen"

"Fehlerbehebung bei Verbindungsproblemen"

Die Hardware-Einrichtung scheint zu hängen

Das Installationsprogramm von StorageGRID Appliance ist möglicherweise nicht verfügbar, wenn Hardwarefehler oder Verkabelungsfehler verhindern, dass der E5700SG-Controller die Boot-Verarbeitung abschließt.

Schritte

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. In einigen Installationsphasen werden dem Installationsprogramm der StorageGRID-Appliance für mehrere Minuten keine Aktualisierungen gemeldet.

   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	• „status-Indikatoren am E5700SG-Controller“ • „HE error: Fehler beim Synchronisieren mit SANtricity OS Software“
E2800 Controller	*E5700 and E2800 System Monitoring Guide* **Hinweis:** die für den E-Series E5700 Controller 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 auf dem E5700SG-Controller"

"HE-Fehler: Fehler beim Synchronisieren mit SANtricity OS Software"

"NetApp E-Series Systems Documentation Site"

HE-Fehler: Fehler beim Synchronisieren mit SANtricity OS Software

Die sieben-Segment-Anzeige auf dem Compute-Controller zeigt EINEN HE-Fehlercode an, wenn das Installationsprogramm der StorageGRID-Appliance nicht mit 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 beiden Verbindungskabel zwischen den beiden Controllern und vergewissern Sie sich, dass die Kabel und SFP+-Transceiver sicher angeschlossen sind.
2. Ersetzen Sie je nach Bedarf ein oder beide Kabel bzw. SFP+-Transceiver, und versuchen Sie es erneut.
3. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

Fehlerbehebung bei Verbindungsproblemen

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Es konnte keine Verbindung zum Gerät 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.

Neustart des Controllers bei Ausführung des StorageGRID-Appliance-Installationsprogramms

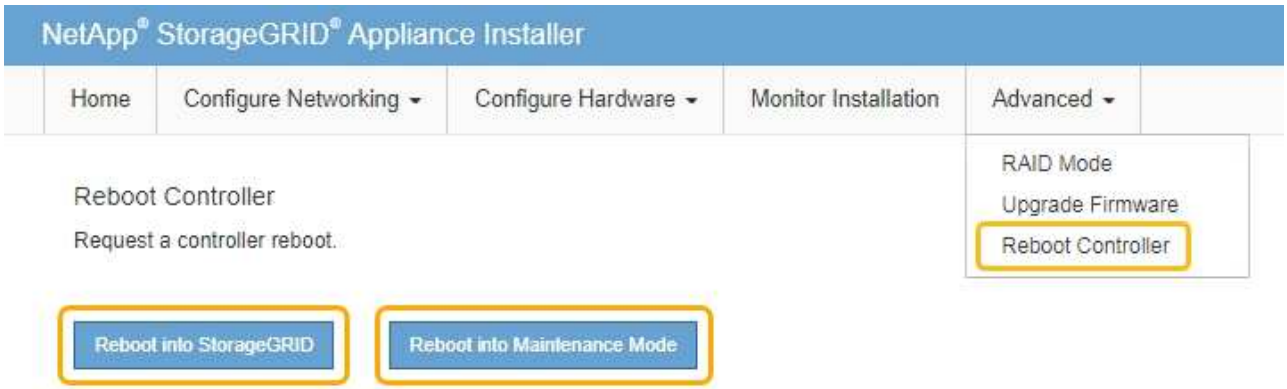
Möglicherweise müssen Sie den Compute-Controller neu starten, während das StorageGRID-Appliance-Installationsprogramm ausgeführt wird. Beispielsweise müssen Sie möglicherweise den Controller neu booten, wenn die Installation fehlschlägt.

Über diese Aufgabe

Dieses Verfahren gilt nur, wenn der Compute-Controller das Installationsprogramm der 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. Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Der SG6000-CN Controller wird neu gestartet.

Warten der SG5700 Appliance

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.

Schritte

- "Versetzen einer Appliance in den Wartungsmodus"
- "Aktualisieren des SANtricity OS auf dem Storage Controller"
- "Aktualisieren der Laufwerk-Firmware mit SANtricity System Manager"
- "Austausch des E2800 Controllers"
- "Austauschen des E5700SG-Controllers"
- "Austausch anderer Hardwarekomponenten"
- "Ändern der Link-Konfiguration des E5700SG-Controllers"
- "Ändern der MTU-Einstellung"
- "Überprüfen der DNS-Serverkonfiguration"
- "Monitoring der Node-Verschlüsselung im Wartungsmodus"

Versetzen einer Appliance in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen. Weitere Informationen finden Sie

in den Anweisungen zum Verwalten von StorageGRID.

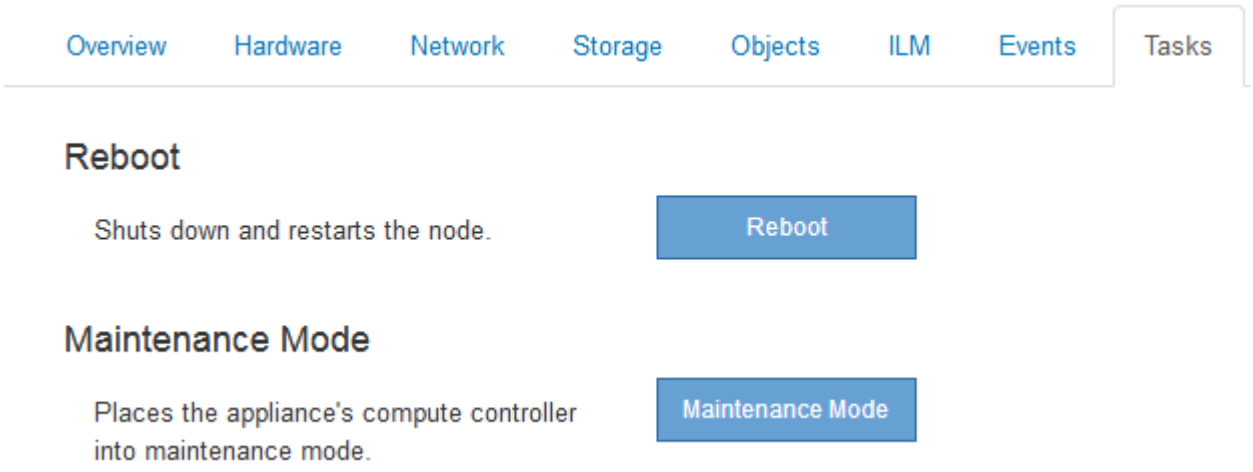
Über diese Aufgabe

Wenn Sie eine StorageGRID Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

> Das Passwort und der Hostschlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem, als das Gerät in Betrieb war.

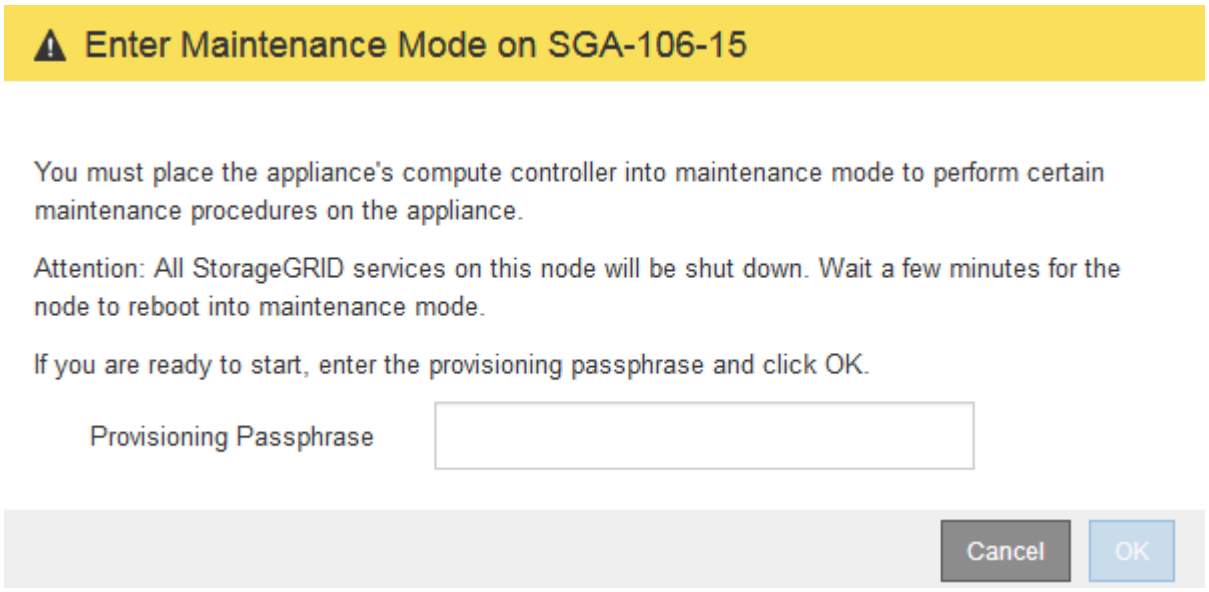
Schritte

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**.



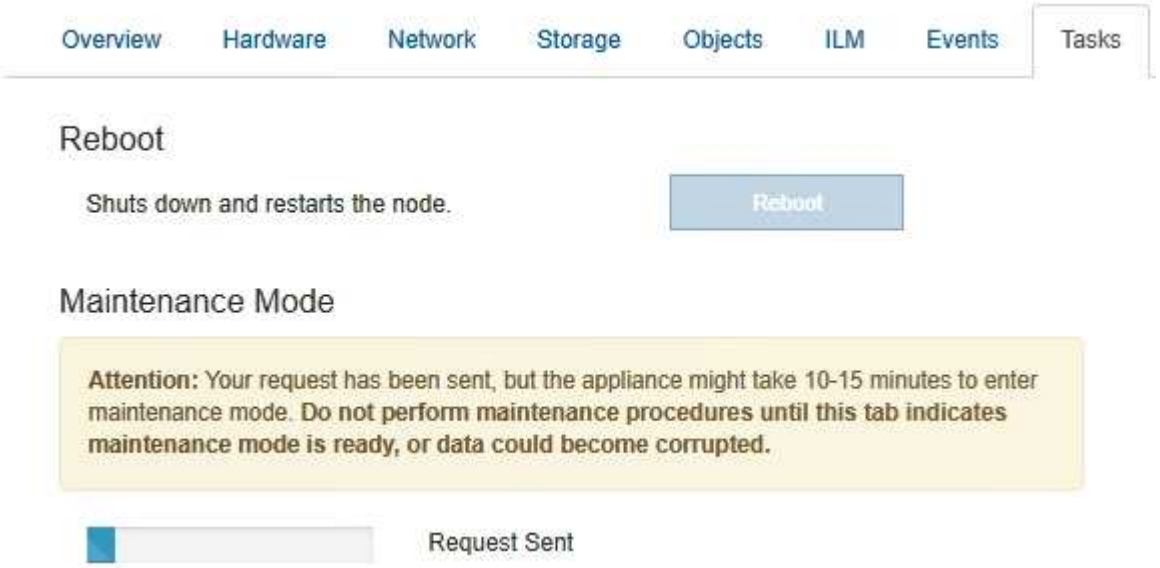
4. Wählen Sie **Wartungsmodus**.

   Ein Bestätigungsdialogfeld wird angezeigt.

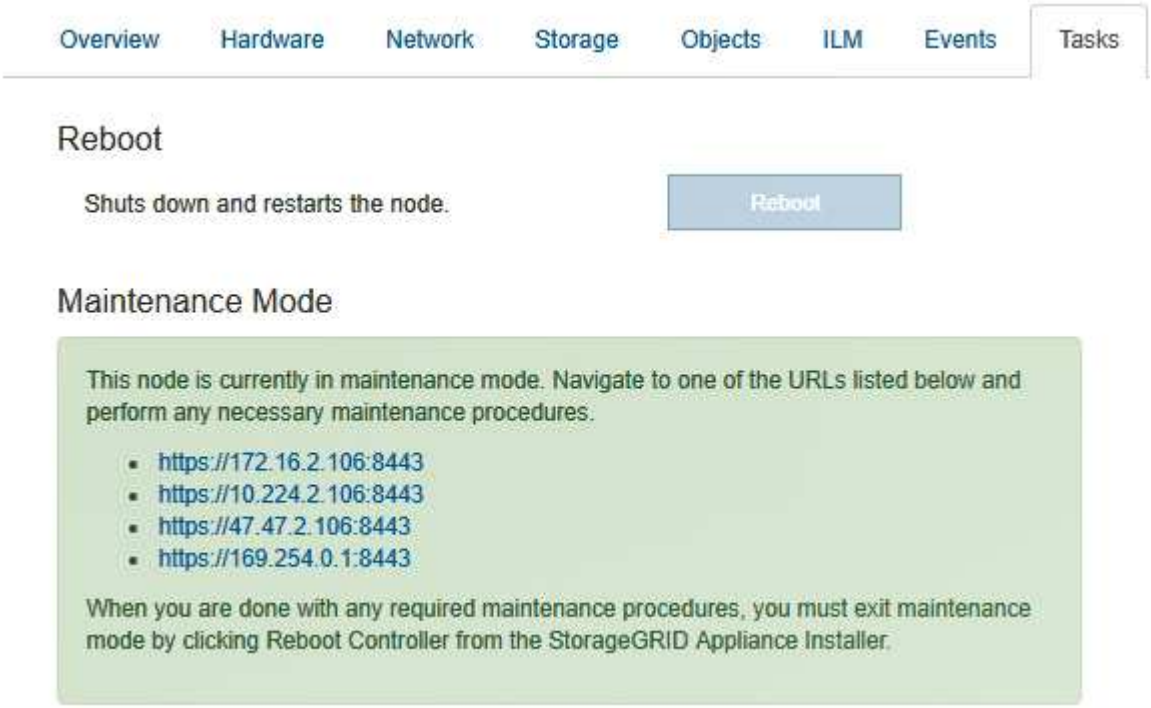


5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

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.



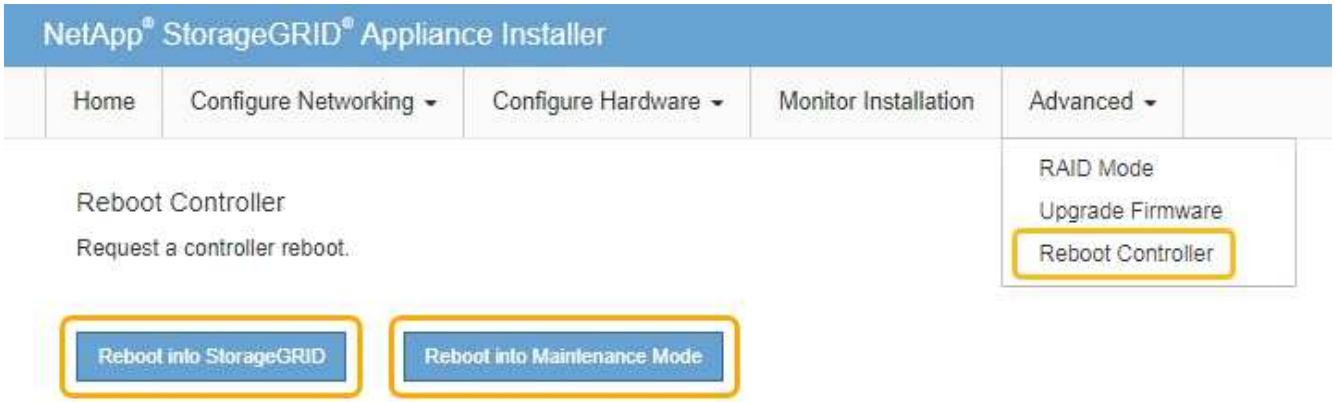
6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

   Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.

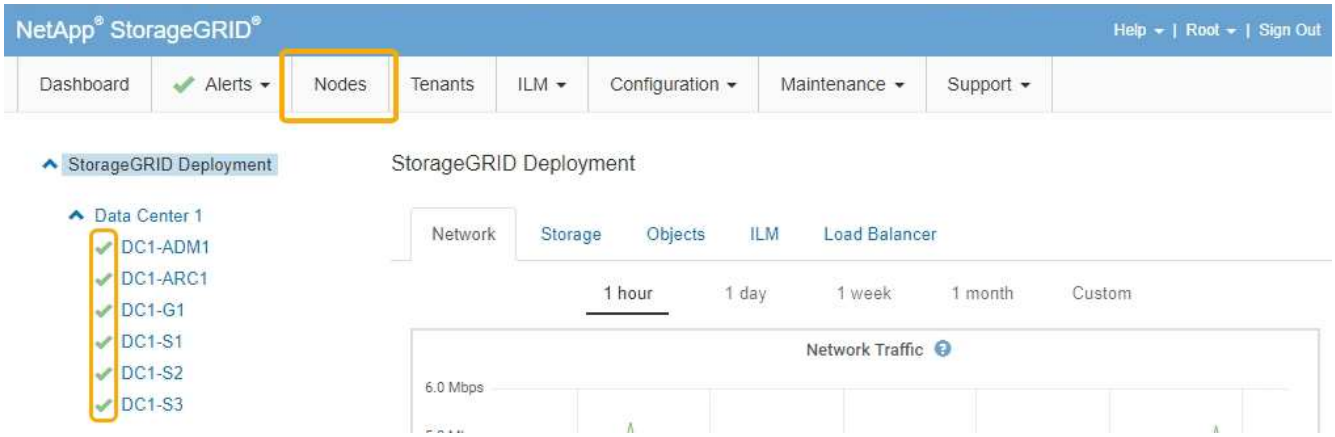
Zugriff Auf `https://169.254.0.1:8443` Erfordert eine direkte Verbindung zum lokalen Management-Port.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

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.



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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Aktualisieren des SANtricity OS auf dem 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. Ermitteln Sie mithilfe des NetApp Interoperabilitäts-Matrix-Tools (IMT), welche Version Sie verwenden sollten. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen.

- 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 von SANtricity OS auf den 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 von SANtricity OS auf dem E2800 Controller mithilfe des Wartungsmodus"

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"NetApp Downloads mit SANtricity OS"

"Monitor Fehlerbehebung"

Aktualisieren von SANtricity OS auf den 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.

Was Sie benötigen

- Sie haben das NetApp Interoperabilitäts-Matrix-Tool (IMT) konsultiert, um zu überprüfen, ob die für das Upgrade verwendete SANtricity Betriebssystemversion mit Ihrer Appliance kompatibel ist.
- Sie müssen über die Berechtigung zur Wartung verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen auf die NetApp Download-Seite für SANtricity OS zugreifen können.

Über diese Aufgabe

Sie können keine anderen Softwareupdates (StorageGRID Software-Upgrade oder Hotfix) durchführen, bis Sie den SANtricity OS-Upgrade-Prozess abgeschlossen haben. 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. Das Laden des SANtricity Betriebssystems auf jedem Node kann länger als 30 Minuten und ein Neustart jeder StorageGRID Storage Appliance bis zu 90 Minuten dauern.

Die folgenden Schritte sind nur anwendbar, wenn Sie den Grid Manager zur Durchführung des Upgrades verwenden. Die Storage-Controller in der SG5700 Series Appliance können nicht mit Grid Manager aktualisiert werden, wenn die Controller SANtricity OS verwenden, die älter als 08.42.20.00 sind (11.42).

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.

Schritte

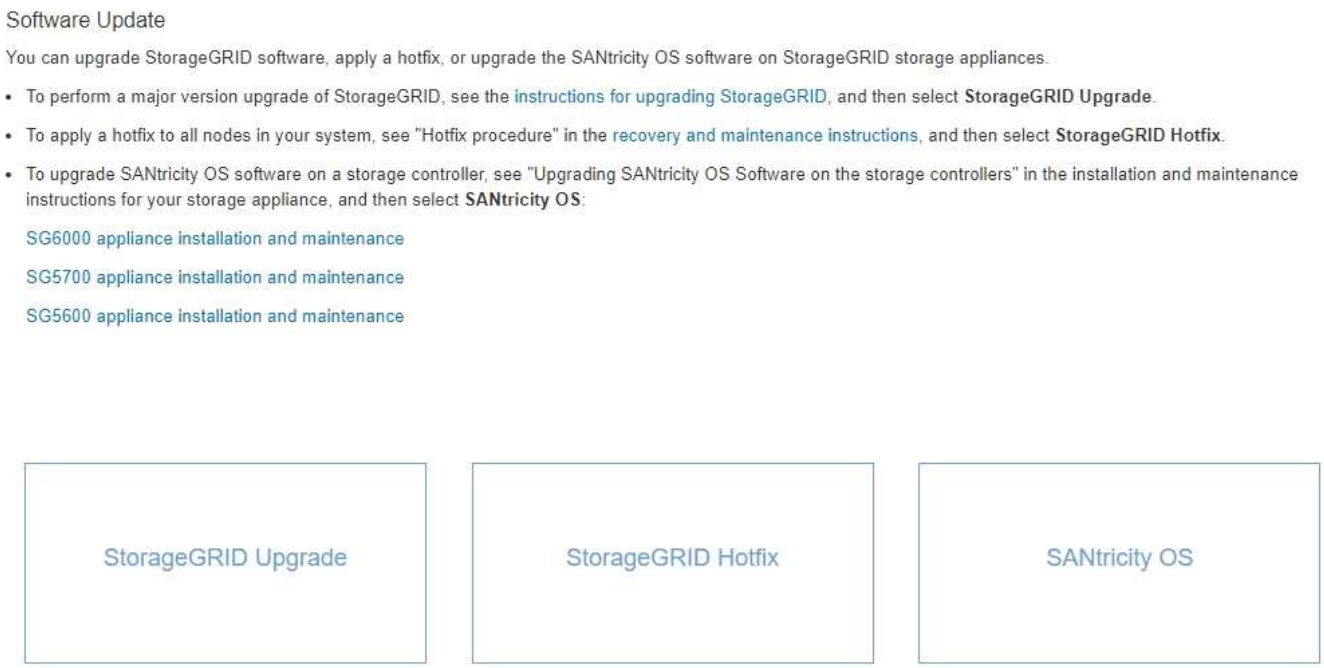
1. Laden Sie von einem Service-Laptop die neue Datei für die SANtricity OS Software von der NetApp Support Website herunter.

   Denken Sie daran, die SANtricity Betriebssystemversion für die E2800 Storage-Controller auszuwählen.

   "NetApp Downloads mit SANtricity OS"

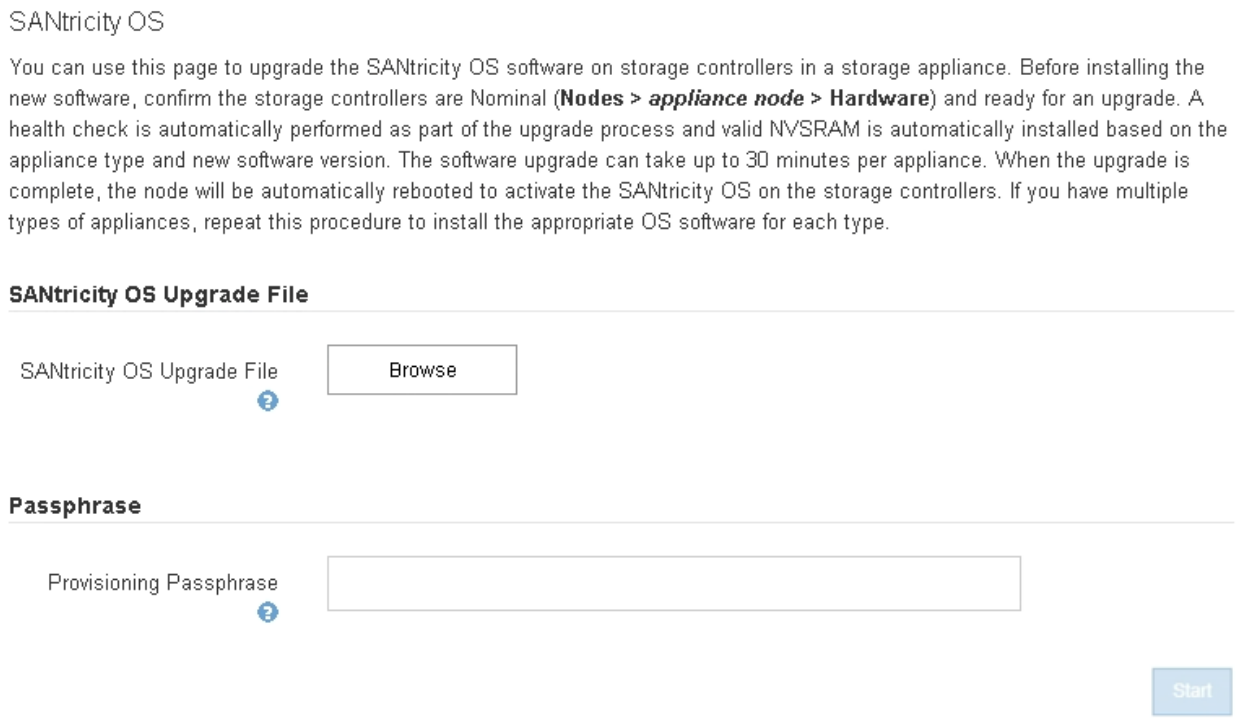
2. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
3. Wählen Sie **Wartung**. Wählen Sie dann im Bereich System des Menüs die Option **Software Update** aus.

   Die Seite Software-Aktualisierung wird angezeigt.



4. Klicken Sie auf **SANtricity OS**.

   Die Seite SANtricity OS wird angezeigt.



5. Wählen Sie die Upgrade-Datei für das SANtricity OS aus, die Sie von der NetApp Support-Website heruntergeladen haben.

   a. Klicken Sie Auf **Durchsuchen**.

   b. Suchen und wählen Sie die Datei aus.

   c. Klicken Sie Auf **Offen**.

   Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird der Dateiname im Feld Details angezeigt.

   > Ändern Sie den Dateinamen nicht, da er Teil des Verifizierungsvorgangs ist.

6. Geben Sie die Provisionierungs-Passphrase ein.

   Die Schaltfläche **Start** ist aktiviert.

7. Klicken Sie Auf **Start**.

Ein Warnfeld zeigt an, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf Knoten, die aktualisiert werden, neu gestartet werden.

8. Klicken Sie auf **OK**, um die SANtricity OS-Aktualisierungsdatei auf den primären Admin-Knoten zu stellen.

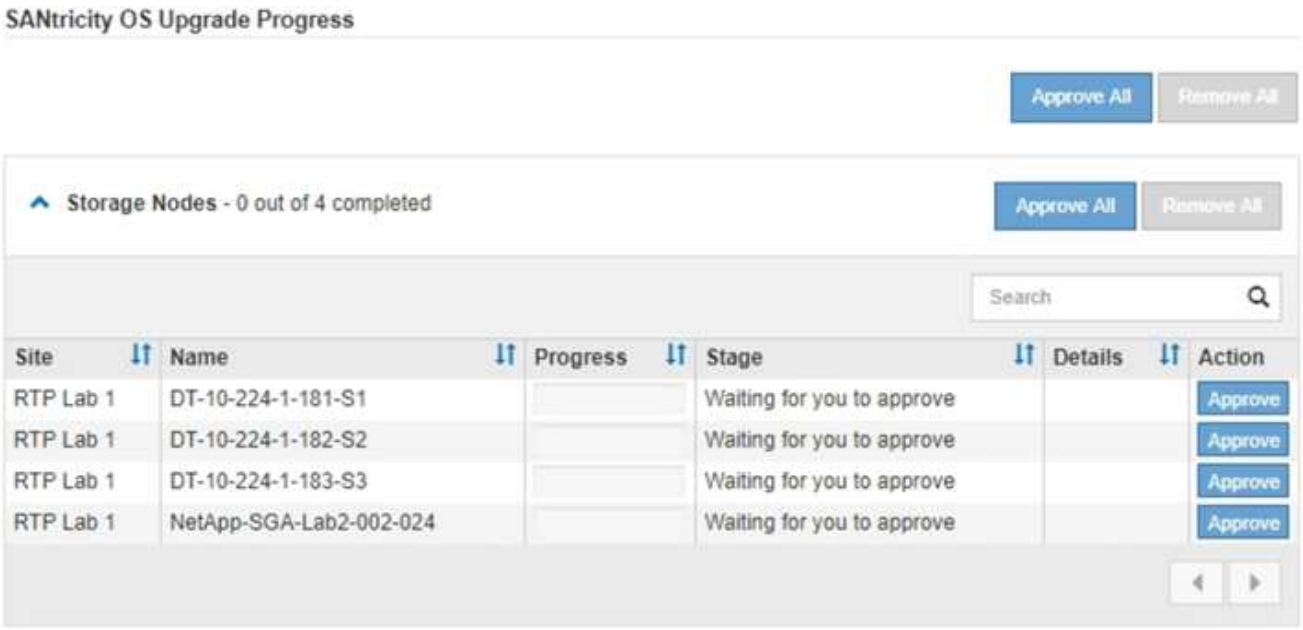
   Wenn das SANtricity OS Upgrade startet:

   a. Die Integritätsprüfung wird ausgeführt. Dieser Prozess überprüft, dass für keine Nodes der Status „Aufmerksamkeit erforderlich“ angezeigt wird.

      Wenn Fehler gemeldet werden, lösen Sie sie und klicken Sie erneut auf **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 werden alle Storage-Nodes einschließlich softwarebasierter Storage-Nodes aufgeführt. Sie müssen das Upgrade für alle Storage-Nodes genehmigen, obwohl ein Upgrade des SANtricity Betriebssystems keine Auswirkungen auf softwarebasierte Storage-Nodes hat. Die für softwarebasierte Storage-Nodes zurückgegebene Upgrade-Meldung lautet „`SANtricity OS Upgrade ist für diesen Node nicht anwendbar.`“



9. Sortieren Sie die Liste der Knoten 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.

   Sie können durch die Liste der Knoten blättern, indem Sie die Pfeile links und rechts unten rechts im Abschnitt verwenden.

10. Genehmigen Sie die Grid-Knoten, die Sie zur Upgrade-Warteschlange hinzufügen möchten. Genehmigte Nodes desselben Typs werden nacheinander aktualisiert.

Genehmigen Sie das SANtricity OS Upgrade für einen Appliance-Storage-Node nicht, es sei denn, Sie sind sicher, dass der Node bereit ist, angehalten und neu gebootet zu werden.Wenn das Upgrade des SANtricity OS auf einem Node genehmigt wird, werden die Services auf diesem Node angehalten. Wenn der Node später aktualisiert wird, wird der Appliance-Node neu gebootet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

- Klicken Sie auf eine der Schaltflächen **Alle genehmigen**, um alle Speicherknoten zur Upgrade-Warteschlange des SANtricity OS hinzuzufügen.

  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.

- Klicken Sie auf eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere Knoten zur SANtricity OS-Upgrade-Warteschlange hinzuzufügen.

  Sie können das Anwenden eines SANtricity OS Upgrades auf einen Node verzögern. Der Upgrade-Prozess für SANtricity OS ist jedoch erst abgeschlossen, wenn Sie das Upgrade von SANtricity OS auf allen aufgeführten Storage-Nodes genehmigen.

  Nach dem Klicken auf **Genehmigen** bestimmt der Upgrade-Prozess, ob der Knoten aktualisiert werden kann. Wenn ein Knoten aktualisiert werden kann, wird er der Upgrade-Warteschlange hinzugefügt. +

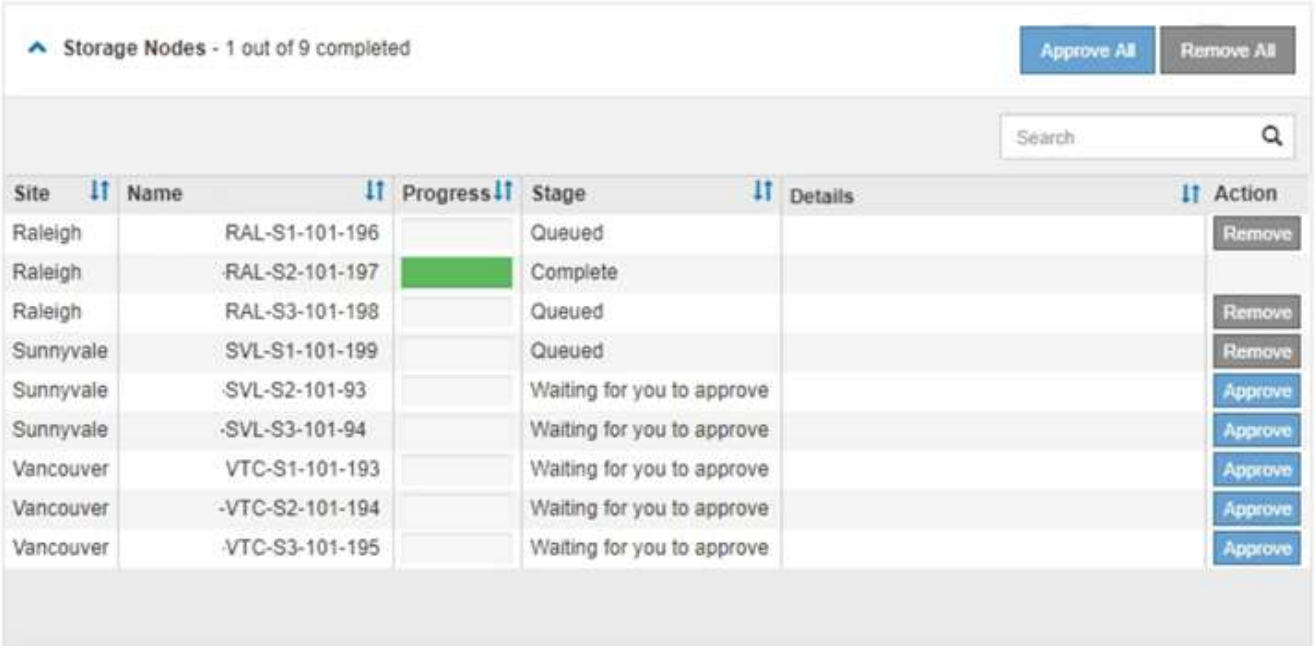
  Bei einigen Nodes wird die ausgewählte Upgrade-Datei absichtlich nicht angewendet. Sie können das Upgrade abschließen, ohne dass Sie ein Upgrade dieser spezifischen Nodes durchführen müssen. Bei Nodes, die absichtlich keine Aktualisierung durchgeführt haben, wird der Prozess mit einer der folgenden Meldungen in der Spalte Details angezeigt:

  - Storage-Node wurde bereits aktualisiert.
  - Das SANtricity OS Upgrade ist für diesen Node nicht verfügbar.
  - Die SANtricity OS-Datei ist mit diesem Node nicht kompatibel.

  Die Meldung „`SANtricity OS Upgrade ist für diesen Node` nicht verfügbar“ gibt an, dass der Node keinen Storage Controller besitzt, der vom StorageGRID System gemanagt werden kann. Diese Meldung wird für nicht-Appliance-Speicherknoten angezeigt. Sie können den Upgrade-Prozess von SANtricity OS abschließen, ohne dass ein Upgrade des Node ausgeführt wird, der diese Meldung anzeigt. + die Meldung „`SANtricity OS File is not compatible with this Node`“ gibt an, dass der Knoten eine SANtricity OS Datei erfordert, die sich von dem Prozess unterscheidet, der zu installieren versucht. Nachdem Sie das aktuelle Upgrade von SANtricity OS abgeschlossen haben, laden Sie das für den Node geeignete SANtricity OS herunter, und wiederholen Sie den Upgrade-Prozess.

11. Wenn Sie einen Knoten oder alle Knoten aus der SANtricity OS Upgrade-Warteschlange entfernen müssen, klicken Sie auf **Entfernen** oder **Alle entfernen**.

    Wie im Beispiel gezeigt, ist die **Remove**-Schaltfläche ausgeblendet, wenn die Phase über Queued hinausgeht und Sie können den Knoten nicht mehr aus dem SANtricity OS-Upgrade-Prozess entfernen.



12. Warten Sie, während das SANtricity OS Upgrade auf jeden genehmigten Grid-Node angewendet wird.

> Wenn während des SANtricity OS Upgrades auf einem beliebigen Node eine Fehlerstufe angezeigt wird, ist das Upgrade für diesen Node fehlgeschlagen. Das Gerät muss möglicherweise in den Wartungsmodus versetzt werden, um nach dem Ausfall eine Wiederherstellung durchzuführen. Wenden Sie sich an den technischen Support, bevor Sie fortfahren.

Wenn die Firmware auf dem Node zu alt ist, um ein Upgrade mit dem Grid Manager durchzuführen, zeigt der Node eine Fehlerstufe an. Die Details: „`Sie müssen den Wartungsmodus verwenden, um ein Upgrade von SANtricity OS auf diesem Node durchzuführen. Siehe Installations- und Wartungsanleitung für Ihr Gerät. Nach dem Upgrade können Sie dieses Dienstprogramm für zukünftige Upgrades verwenden.`" Gehen Sie wie folgt vor, um den Fehler zu beheben:

a. Verwenden Sie den Wartungsmodus, um ein Upgrade von SANtricity OS auf dem Node durchzuführen, auf dem eine Fehlerstufe angezeigt wird.
b. Verwenden Sie den Grid-Manager, um das SANtricity OS-Upgrade erneut zu starten und abzuschließen.

   Wenn das SANtricity OS Upgrade auf allen genehmigten Nodes abgeschlossen ist, wird die Fortschrittstabelle des SANtricity OS Upgrades geschlossen, und ein grünes Banner zeigt das Datum und die Uhrzeit des Ababgeschlossenen Upgrades des SANtricity OS an.

13. 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

"Aktualisieren von SANtricity OS auf dem E2800 Controller mithilfe des Wartungsmodus"

Aktualisieren von SANtricity OS auf dem 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.

Was Sie benötigen

- Sie haben das NetApp Interoperabilitäts-Matrix-Tool (IMT) konsultiert, um zu überprüfen, ob die für das Upgrade verwendete SANtricity Betriebssystemversion mit Ihrer Appliance kompatibel ist.
- Sie müssen den E5700SG Controller in den Wartungsmodus versetzen, sodass die Verbindung zum E2800 Controller unterbrochen wird. Wenn eine StorageGRID Appliance in den Wartungsmodus versetzt wird, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

  "Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Aktualisieren Sie das SANtricity Betriebssystem und NVSRAM im E-Series Controller nicht auf mehr als einer StorageGRID Appliance gleichzeitig.

> Wenn Sie mehrere StorageGRID Appliances gleichzeitig aktualisieren, kann dies in Abhängigkeit von Ihrem Implementierungsmodell und den ILM-Richtlinien zu Datenunverfügbarkeit führen.

Schritte

1. Greifen Sie über ein Service-Laptop auf den SANtricity System Manager zu und melden Sie sich an.
2. Laden Sie die neue SANtricity OS Software-Datei und die NVSRAM-Datei auf den Management-Client herunter.

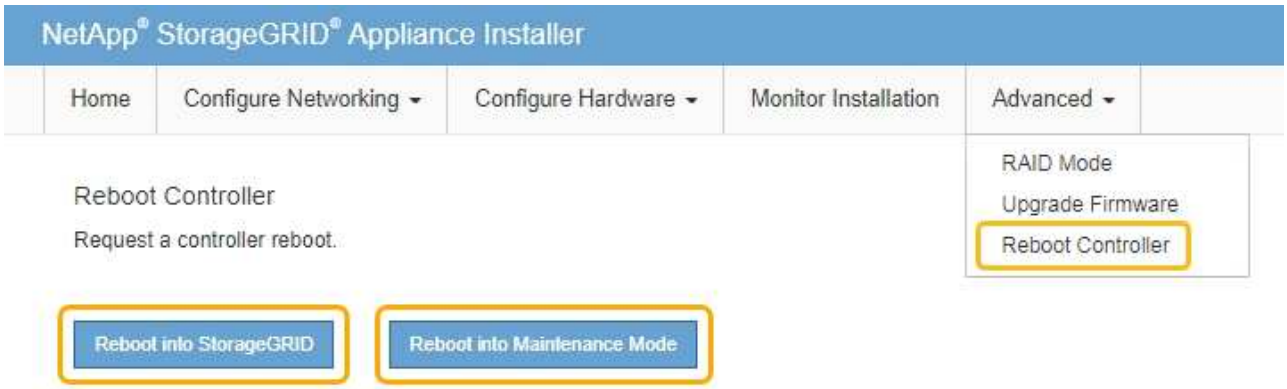
   > Das NVSRAM bezieht sich auf die StorageGRID Appliance. Verwenden Sie nicht den Standard-NVSRAM-Download.

3. 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.

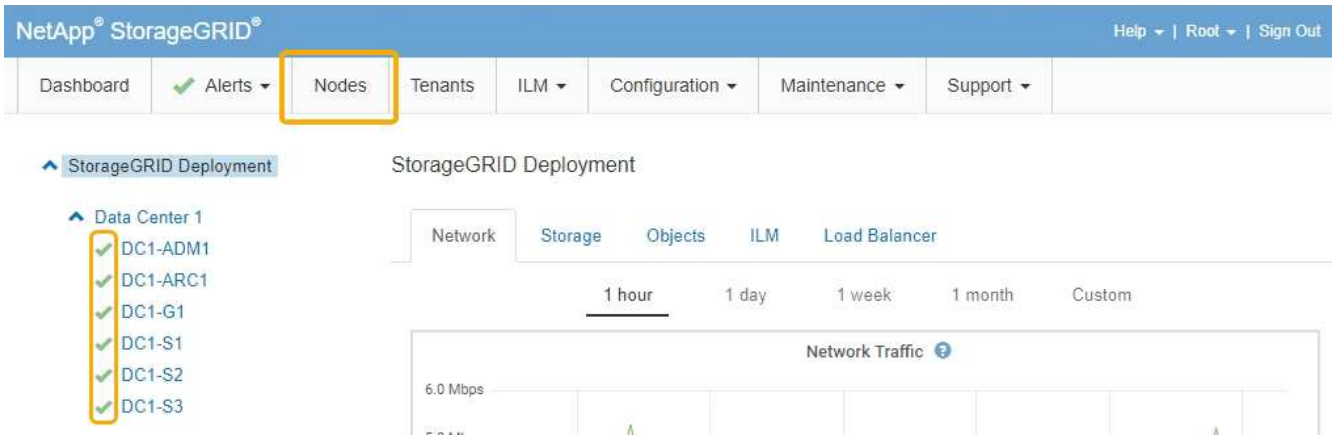
   > Aktivieren Sie die Upgrade-Dateien sofort. Die Aktivierung nicht verschieben.

4. Sobald der Upgrade-Vorgang abgeschlossen ist, 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"Aktualisieren von SANtricity OS auf den Storage Controllern mit Grid Manager"

Aktualisieren der Laufwerk-Firmware mit SANtricity System Manager

Sie aktualisieren Ihre Laufwerk-Firmware, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen.

Was Sie benötigen

- Die Storage Appliance hat einen optimalen Status.

- Alle Laufwerke haben einen optimalen Status.
- Die aktuelle Version von SANtricity System Manager ist mit Ihrer StorageGRID-Version kompatibel.
- Sie haben die StorageGRID-Appliance in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

> Im Wartungsmodus wird die Verbindung zum Storage Controller unterbrochen, alle I/O-Aktivitäten werden angehalten und alle Laufwerke werden offline geschaltet.

> Aktualisieren Sie die Laufwerk-Firmware nicht auf mehr als einer StorageGRID Appliance gleichzeitig. Dadurch kann je nach Implementierungsmodell und ILM-Richtlinien die Nichtverfügbarkeit von Daten auftreten.

Schritte

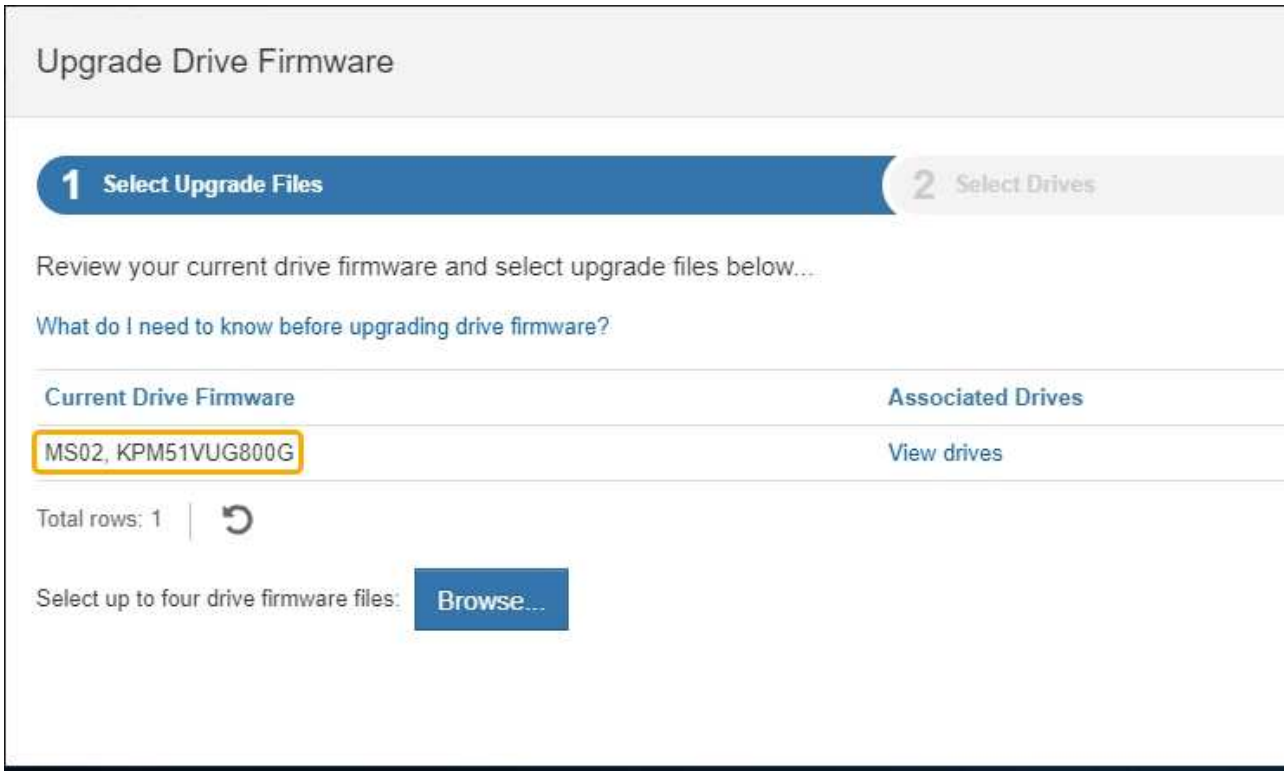
1. Greifen Sie mit einer der folgenden Methoden auf SANtricity System Manager zu:
   - Verwenden Sie das StorageGRID-Appliance-Installationsprogramm, und wählen Sie **Erweitert** > **SANtricity-Systemmanager**
   - Verwenden Sie den Grid Manager, und wählen Sie **Knoten** > ***appliance Storage Node*** > **SANtricity System Manager**

     > Wenn diese Optionen nicht verfügbar sind oder die Anmeldeseite des SANtricity System Managers nicht angezeigt wird, rufen Sie den SANtricity System Manager auf, indem Sie die Storage-Controller-IP aufrufen:
     > **`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 die Option **Support** > **Upgrade Center** aus.
   b. Wählen Sie unter Laufwerk-Firmware-Upgrade die Option **Upgrade starten** aus.

      Auf der Upgrade Drive Firmware werden die zurzeit installierten Firmware-Dateien des Laufwerks angezeigt.

   c. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerkskennungen in der Spalte Aktueller Laufwerk-Firmware.



In diesem Beispiel:

- Die Version der Laufwerk-Firmware lautet **MS02**.
- Die Laufwerk-ID lautet **KPM51VUG800G**.

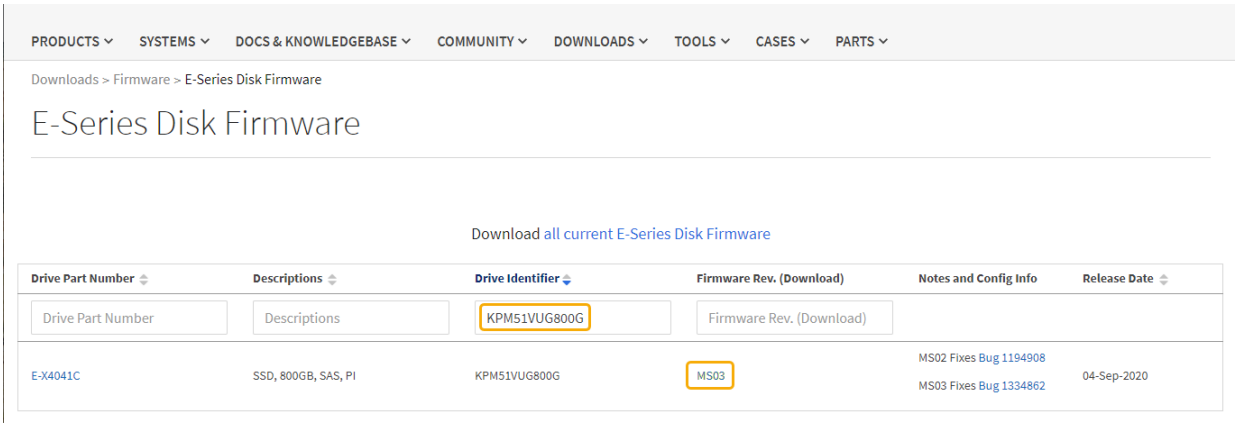
Wählen Sie in der Spalte „verbundene Laufwerke“ die Option **Laufwerke anzeigen** aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.

a. 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 Laufwerkkennung die neueste Firmware-Version hat.
      - Wenn die Firmware-Version kein Link ist, hat diese Laufwerkkennung 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.



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 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 **vorgeschlagene Firmware** angezeigt. Wenn Sie diese Firmware ändern müssen, wählen Sie **Zurück**.

d. Wählen Sie * Offline (Parallel)* Upgrade.

Sie können die Offline-Upgrade-Methode verwenden, weil sich die Appliance im Wartungsmodus befindet, wobei I/O-Aktivitäten für alle Laufwerke und alle Volumes angehalten werden.

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`.

Wenn während des Aktualisierungsvorgangs eines der folgenden Fehler auftritt, ergreifen Sie die entsprechende empfohlene Maßnahme.

- **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 an den Controller angeschlossenen Kabel 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**

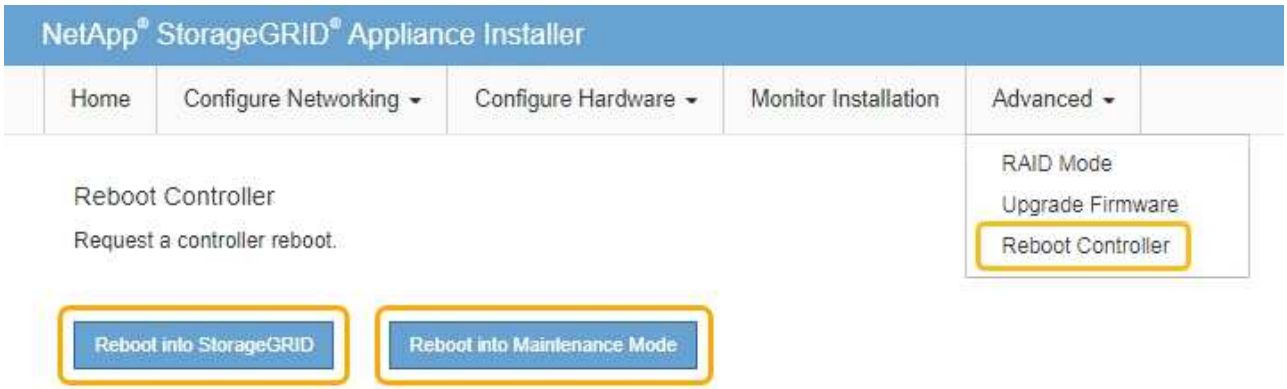
  Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

- **Mehr als 4 kritische MEL-Einträge in den letzten 7 Tagen**

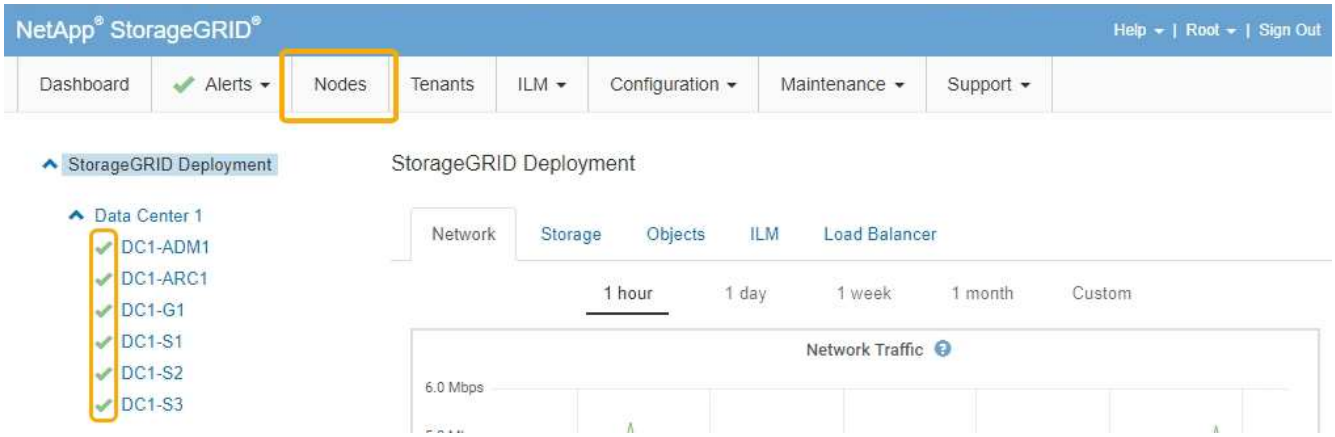
  Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

6. Starten Sie die Appliance nach Abschluss des Aktualisierungsvorgangs 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"Aktualisieren des SANtricity OS auf dem Storage Controller"

Austausch des E2800 Controllers

Möglicherweise müssen Sie den E2800 Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Über diese Aufgabe

- Sie verfügen über einen Ersatzcontroller mit derselben Teilenummer wie der zu ersetzenden Controller.
- Sie haben die Anweisungen für den Austausch der Simplexkonfiguration eines ausgefallenen E2800 Controller-Kanisters heruntergeladen.

> ⓘ Beachten Sie nur bei der Anleitung zur E-Series oder wenn Sie weitere Details für einen bestimmten Schritt benötigen. Verlassen Sie sich beim Austausch eines Controllers in der StorageGRID Appliance nicht auf die Anweisungen der E-Series, da sich die Verfahren nicht unterscheiden.

- 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 Simplex-Verfahren zum Austausch des E2800 Controllers überprüft. Dazu gehören der Download und die Installation des E-Series SANtricity Storage Managers von der NetApp Support Site. Anschließend können Sie die gesicherten Laufwerke über das Enterprise Management Window (EMW) entsperren, nachdem Sie den Controller ersetzt haben.

> Sie können das Gerät erst dann verwenden, wenn Sie die Laufwerke mit dem gespeicherten Schlüssel entsperren.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

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 E2800 Controller ausreichend funktioniert, können Sie den E5700SG Controller in den Wartungsmodus versetzen.

"Versetzen einer Appliance in den Wartungsmodus"

Wenn Sie einen Controller austauschen, müssen Sie den Akku aus dem ursprünglichen Controller entfernen und in den Ersatzcontroller einsetzen.

> Der E2800 Controller in der Appliance enthält keine Host-Schnittstellenkarte (HIC).

Schritte

1. 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.

   a. Notieren Sie sich, welche Version der SANtricity OS Software derzeit auf dem Controller installiert ist.
   b. Notieren Sie sich, welche NVSRAM-Version derzeit installiert ist.
   c. 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 im Gerät sicher sind, kann der neue Controller erst dann auf das Gerät zugreifen, wenn Sie die gesicherten Laufwerke mit dem Unternehmensverwaltungsfenster im SANtricity Storage Manager entsperren.

   d. Sichern Sie die Konfigurationsdatenbank.

      Wenn beim Entfernen eines Controllers ein Problem auftritt, können Sie die gespeicherte Datei verwenden, um Ihre Konfiguration wiederherzustellen.

e. Sammeln von Support-Daten für die Appliance

> Das Erfassen von Supportdaten vor und nach dem Ersetzen einer Komponente stellt sicher, dass Sie einen vollständigen Satz von Protokollen an den technischen Support senden können, falls das Problem durch den Austausch nicht behoben wird.

2. Wenn die StorageGRID Appliance in einem StorageGRID System ausgeführt wird, versetzen Sie den E5700SG Controller in den Wartungsmodus.

   "Versetzen einer Appliance in den Wartungsmodus"

3. Wenn der E2800 Controller ausreichend funktioniert, um ein kontrolliertes Herunterfahren zu ermöglichen, bestätigen Sie, dass alle Operationen abgeschlossen wurden.
   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.
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 eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht 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.

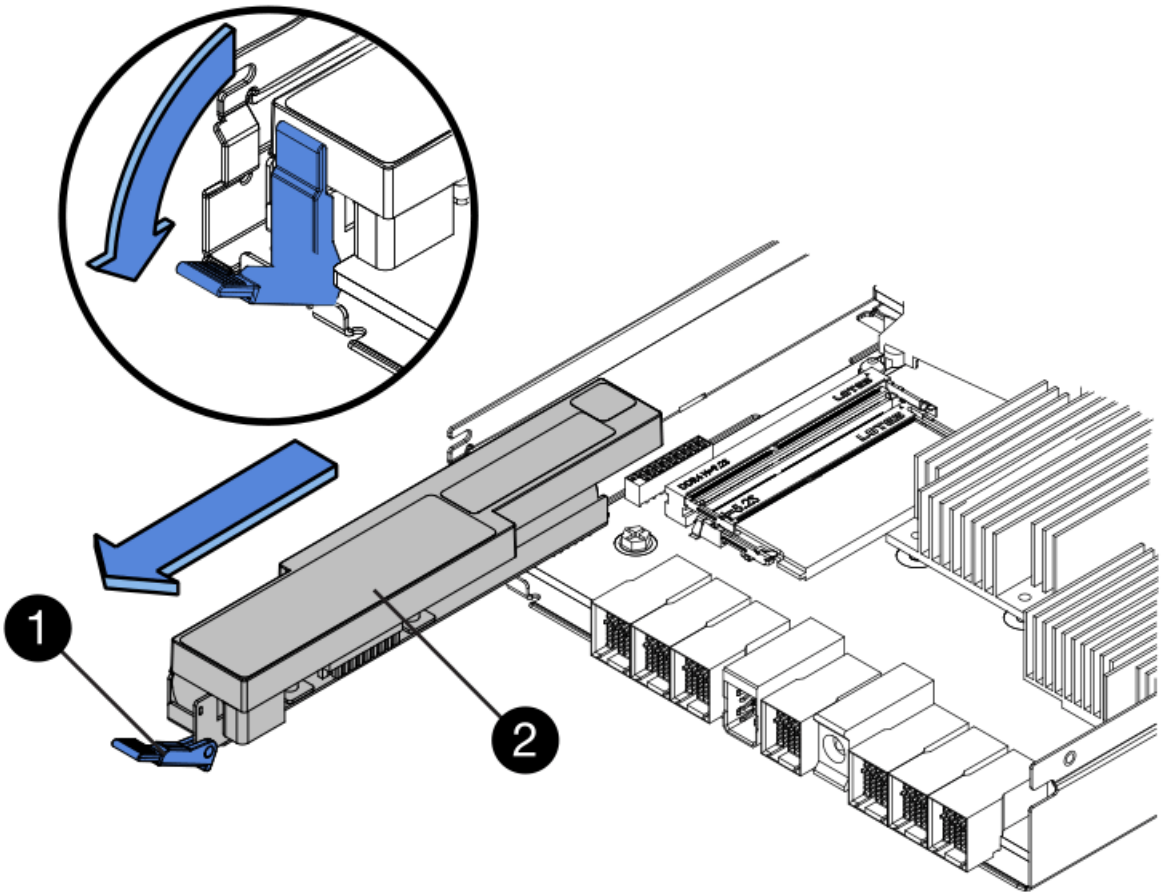
   e. Stellen Sie den Controller auf eine flache, statische Oberfläche, wobei die abnehmbare Abdeckung nach oben zeigt.
   f. Entfernen Sie die Abdeckung, indem Sie die Taste nach unten drücken und die Abdeckung abnehmen.
5. Entfernen Sie den Akku aus dem ausgefallenen Controller, und setzen Sie ihn in den Ersatzcontroller ein:
   a. 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
	Interne LED für aktiven Cache
	Batterie

b. Suchen Sie den blauen Freigabehebel für die Batterie.

c. Entriegeln Sie den Akku, indem Sie den Entriegelungshebel nach unten und aus dem Controller entfernen.



Element	Beschreibung
	Akkufreigaberiegel
	Batterie

d. Heben Sie den Akku an, und schieben Sie ihn aus dem Controller.

e. Entfernen Sie die Abdeckung vom Ersatzcontroller.

f. Richten Sie den Ersatz-Controller so aus, dass der Steckplatz für die Batterie zu Ihnen zeigt.

g. 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.

h. Schieben Sie die Akkuverriegelung nach oben, um die Batterie zu sichern.

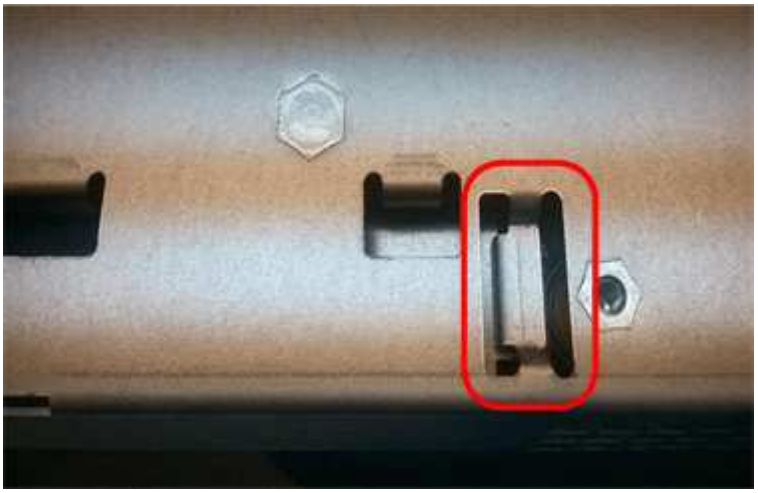
   Wenn die Verriegelung einrastet, Haken unten an der Verriegelung in einen Metallschlitz am Gehäuse.

i. 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 komplett in den Schlitz am Controller eingelegt:**

- **Falsch — der Metallflansch der Batterie ist nicht in den Steckplatz an der Steuerung eingefügt:**



j. Bringen Sie die Controllerabdeckung wieder an.

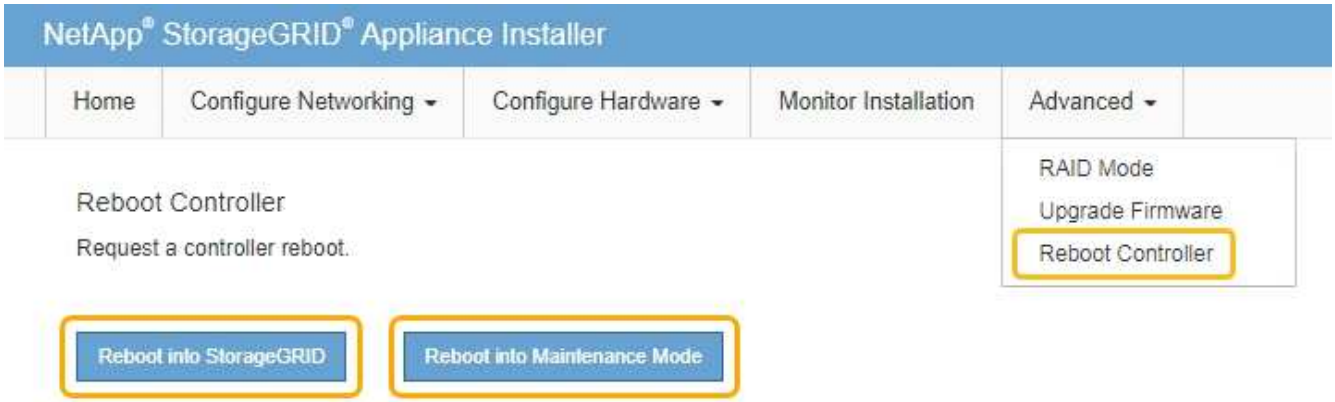
6. Setzen Sie den Ersatzcontroller in das Gerät ein.
   a. Drehen Sie den Controller um, so dass die abnehmbare Abdeckung nach unten zeigt.
   b. Schieben Sie den Steuerknebel in die geöffnete Stellung, und schieben Sie ihn bis zum Gerät.
   c. Bewegen Sie den Nockengriff nach links, um die Steuerung zu verriegeln.
   d. Ersetzen Sie die Kabel und SFPs.
   e. Warten Sie, bis der E2800 Controller neu gestartet wurde. Vergewissern Sie sich, dass auf der 7-Segment-Anzeige ein Status von angezeigt wird `99`.

f. Legen Sie fest, wie Sie dem Ersatz-Controller eine IP-Adresse zuweisen.

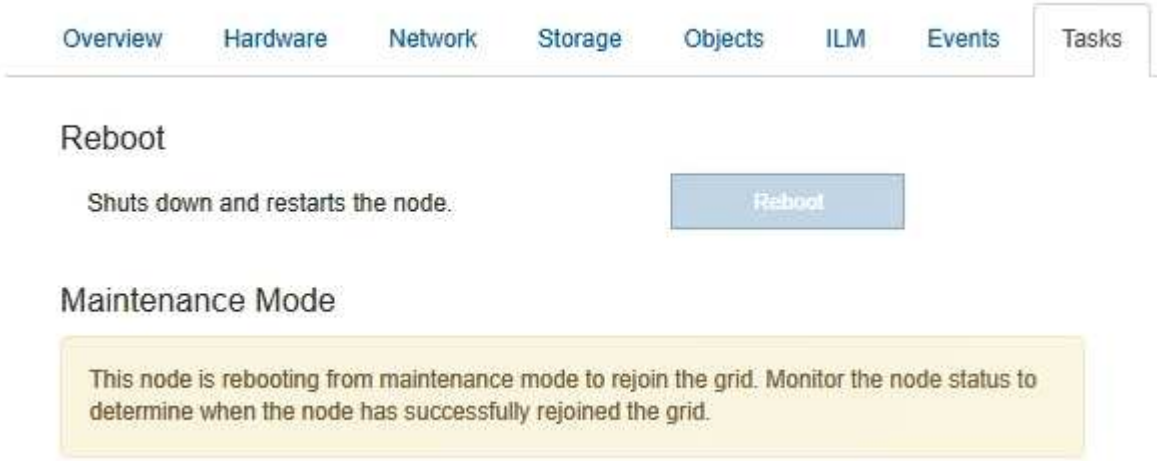
> Die Schritte zum Zuweisen einer IP-Adresse zum Ersatz-Controller hängen davon ab, ob Sie Management-Port 1 mit einem Netzwerk mit einem DHCP-Server verbunden haben und ob alle Laufwerke gesichert sind.

- 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.
- Wenn alle Laufwerke gesichert sind, müssen Sie das Enterprise Management-Fenster (EMW) im SANtricity Storage Manager verwenden, um die gesicherten Laufwerke zu entsperren. Sie können erst dann auf den neuen Controller zugreifen, wenn Sie die Laufwerke mit dem gespeicherten Schlüssel entsperren. In der Anleitung zur E-Series ist der Austausch eines E2800 Simplex-Controllers beschrieben.

7. Wenn die Appliance gesicherte Laufwerke verwendet, befolgen Sie die Anweisungen beim Austausch des E2800 Controllers, um den Sicherheitsschlüssel des Laufwerks zu importieren.
8. 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.

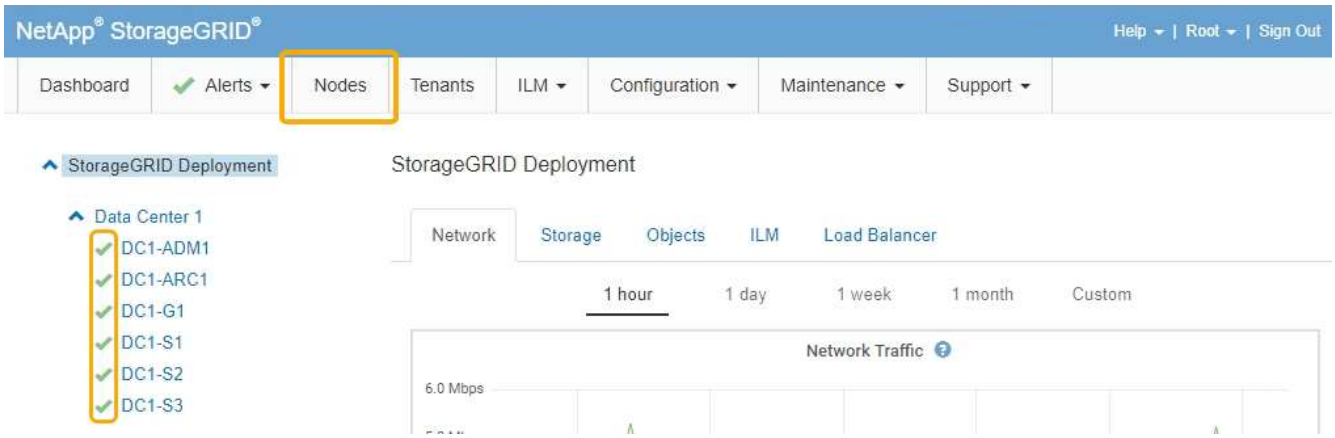


Während des Neustarts wird der folgende Bildschirm angezeigt:



Das Gerät wird neu gestartet und wieder in das Raster integriert. Dieser Vorgang kann bis zu 20 Minuten dauern.

9. 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 Registerkarte **Nodes** ein normaler Status angezeigt wird ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



10. Vom SANtricity System Manager sollte sichergestellt werden, dass der neue Controller optimal ist, und er sammelt Support-Daten.

Verwandte Informationen

"NetApp E-Series Systems Documentation Site"

Austauschen des E5700SG-Controllers

Möglicherweise müssen Sie den E5700SG-Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

Was Sie benötigen

- 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 der E-Series, da sich die Verfahren nicht unterscheiden. 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 Controller E5700SG.

- Sie verfügen über Etiketten, um jedes Kabel, das mit dem Controller verbunden ist, zu identifizieren.
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

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. Während Sie von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm für StorageGRID-Geräte zugreifen können, können Sie 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. Wenn das Gerät in den Wartungsmodus versetzt wurde, 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 eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht 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:

   - E2800 Controller:

     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.

Verwandte Informationen

"NetApp E-Series Systems Documentation Site"

Austausch anderer Hardwarekomponenten

Möglicherweise müssen Sie einen Controller-Akku, ein Laufwerk, einen Lüfter oder ein Netzteil in dem StorageGRID-Gerät austauschen.

Was Sie benötigen

- Sie haben das Verfahren zum Austausch der E-Series Hardware.
- Das Gerät wurde in den Wartungsmodus versetzt, wenn Sie das Gerät beim Austausch der Komponenten herunterfahren müssen.

  "Versetzen einer Appliance in den Wartungsmodus"

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 Laufwerkschublade 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 Shelfs der E2800 mit 12 Laufwerken oder mit 24 Laufwerken
Lüfter-Behälter	Austausch eines Power-Fan-Behälters in E2800 Shelfs

Anweisungen zum Austausch der SG5760 Komponenten

FRU	Weitere Informationen finden Sie in den Anweisungen zur E-Series
Laufwerk	Ersetzen eines Laufwerks in E2860 Shelfs
Leistungsbehälter	Austausch eines Netzkanisters in E2860 Shelfs
Gebläsebehälter	Austausch eines Lüftergehäuses in E2860 Shelfs
Laufwerksschublade	Austauschen eines Laufwerksschubs in E2860 Shelfs

Verwandte Informationen

"Austausch des E2800 Controllers"

"NetApp E-Series Systems Documentation Site"

Ändern der 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.

Was Sie benötigen

Sie müssen den E5700SG Controller in den Wartungsmodus versetzen. Wenn eine StorageGRID Appliance in den Wartungsmodus versetzt wird, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

"Versetzen einer Appliance in den Wartungsmodus"

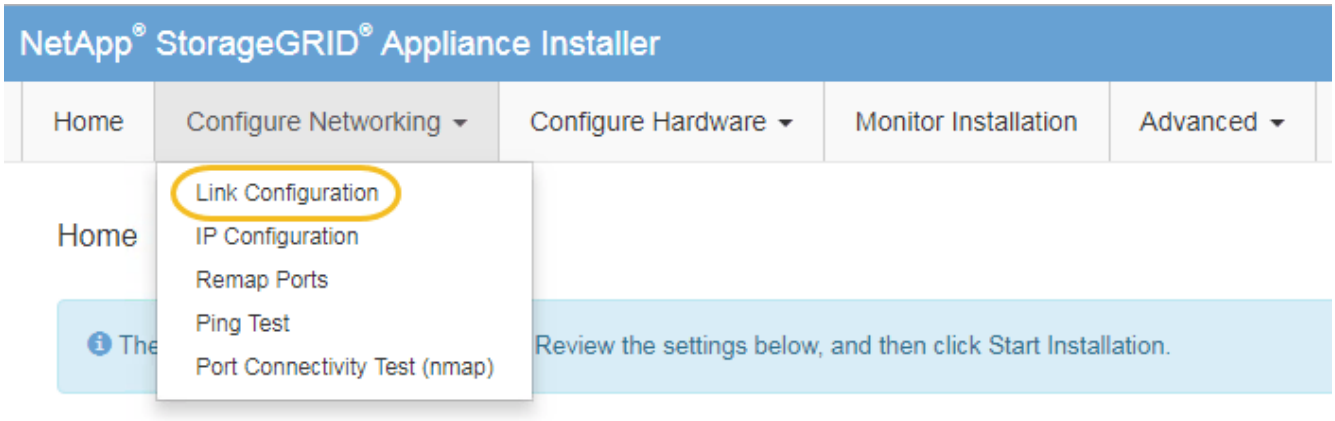
Über diese Aufgabe

Die Ethernet-Link-Konfiguration des E5700SG-Controllers kann wie folgt geändert werden:

- Ändern des **Port Bond Modus** von Fixed zu Aggregate oder von 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 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.



1. Nehmen Sie die gewünschten Änderungen an der Verbindungskonfiguration vor.

   Weitere Informationen zu den Optionen finden Sie unter „`Konfigurieren von Netzwerkverbindungen`“.

2. 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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten 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 Anweisungen zum Konfigurieren von IP-Adressen.

   "Einstellen der IP-Konfiguration"

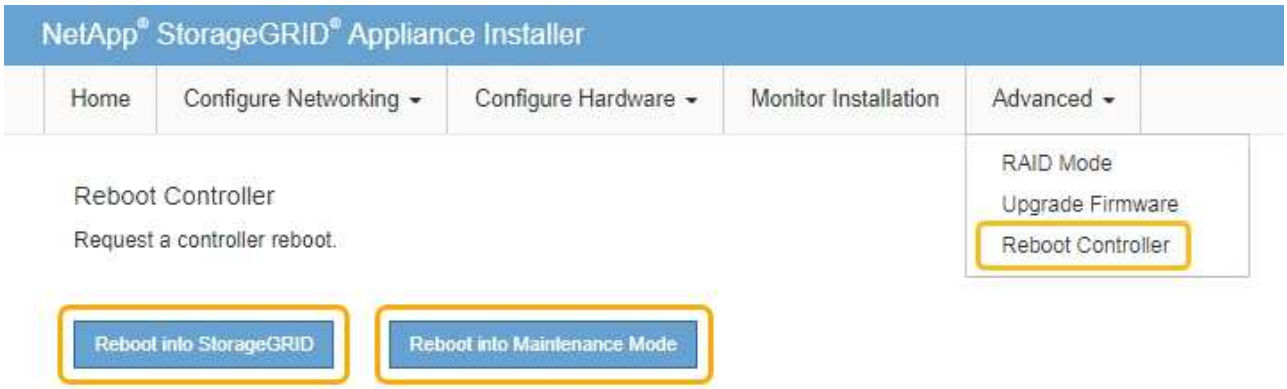
3. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren** > **Ping-Test** aus.
4. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in allen Netzwerken zu überprüfen, die möglicherweise von den in vorgenommenen Änderungen der Verbindungskonfiguration betroffen sind Verbindungskonfiguration ändern Schritt:

   Zusätzlich zu allen anderen Tests, die Sie durchführen möchten, bestätigen Sie, dass Sie die Grid-IP-

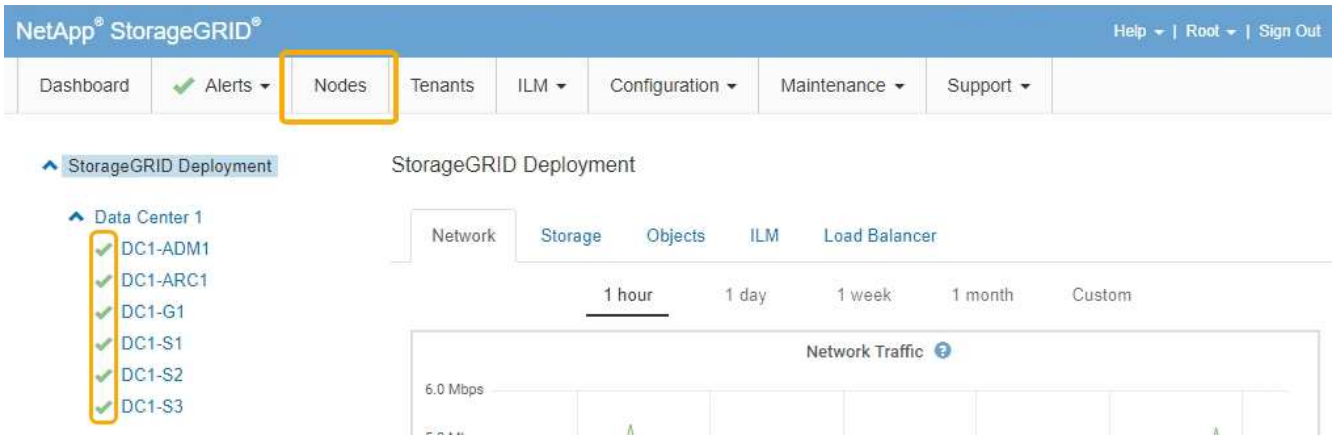
Adresse des primären Admin-Knotens und die Grid-IP-Adresse von mindestens einem anderen Speicherknoten pingen können. Korrigieren Sie ggf. alle Probleme mit der Verbindungskonfiguration.

5. 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"Konfigurieren von Netzwerk-Links (SG5700)"

Ändern der MTU-Einstellung

Sie können die MTU-Einstellung ändern, die Sie beim Konfigurieren von IP-Adressen für den Appliance-Node zugewiesen haben.

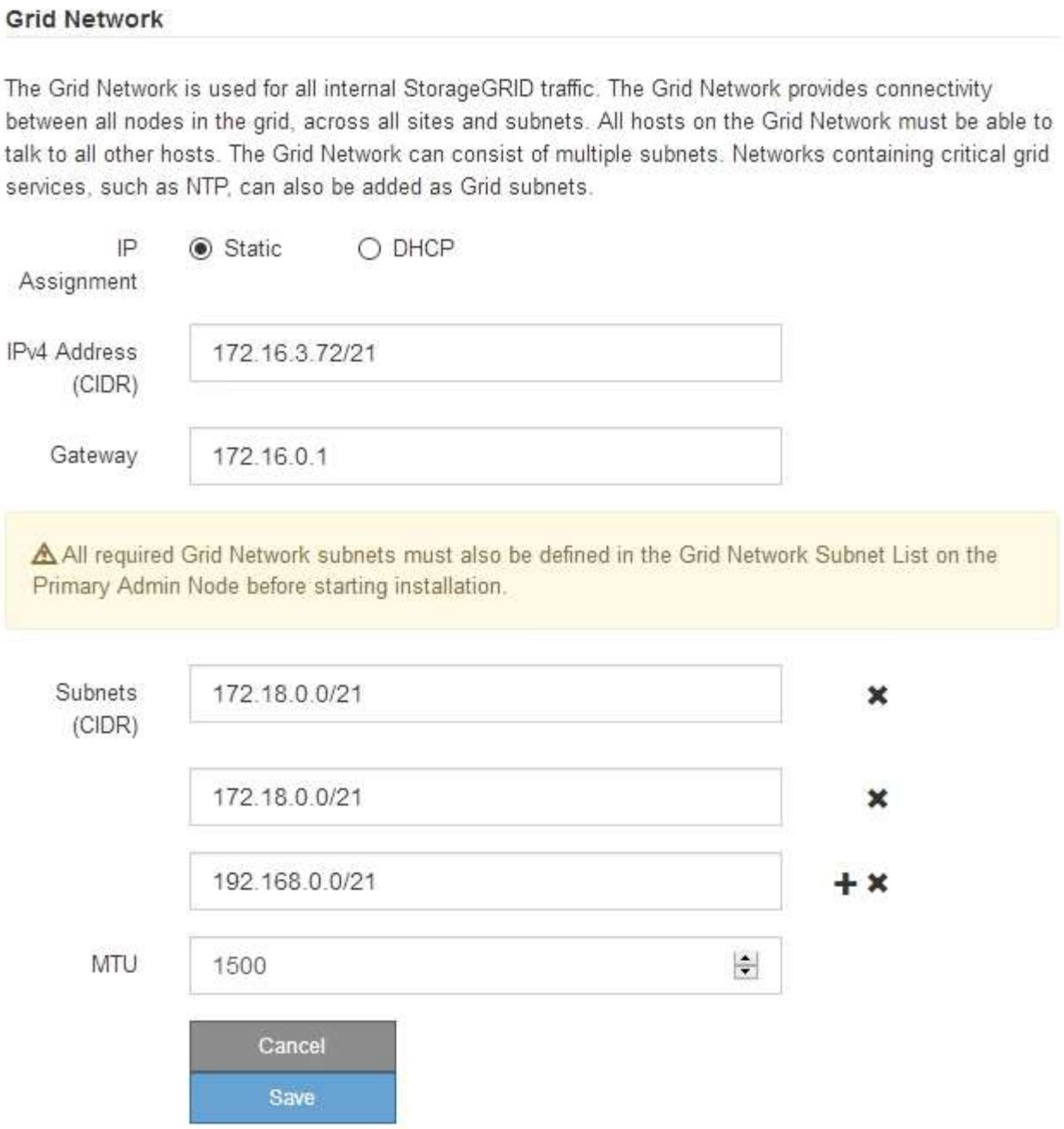
Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

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.



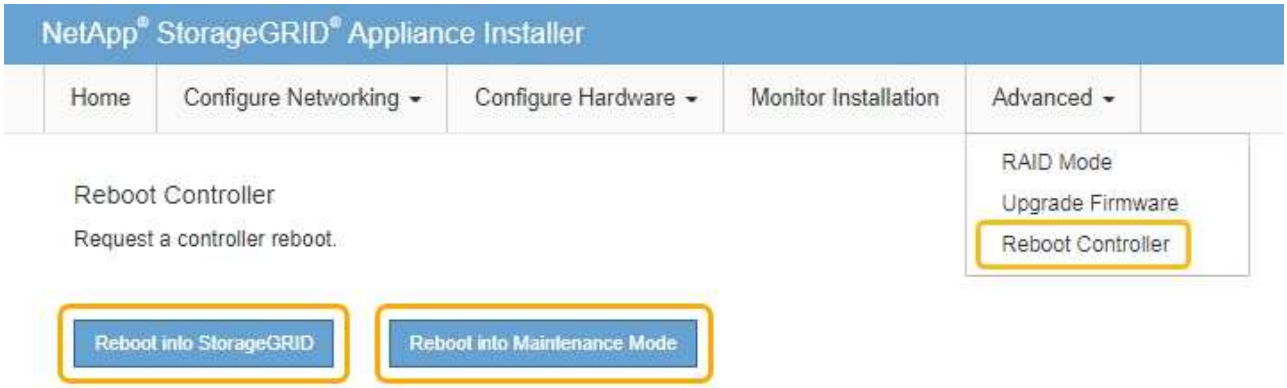
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch sein.

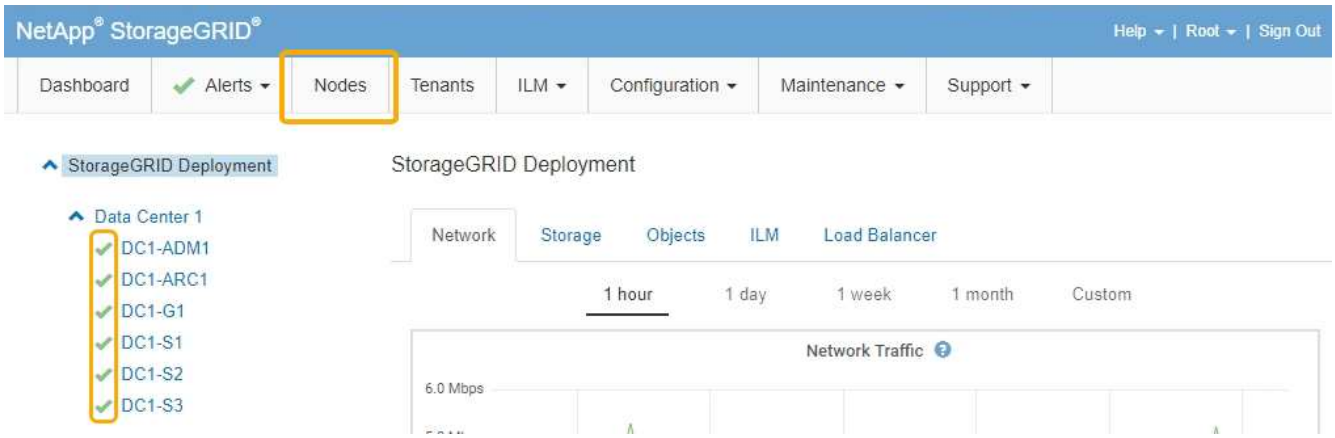
3. Wenn Sie mit den Einstellungen zufrieden sind, wählen Sie **Speichern**.
4. Booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option

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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Überprüfen der DNS-Serverkonfiguration

Sie können die DNS-Server (Domain Name System), die derzeit von diesem Appliance-Node verwendet werden, überprüfen und vorübergehend ändern.

Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Möglicherweise müssen Sie die DNS-Servereinstellungen ändern, wenn eine verschlüsselte Appliance sich nicht mit dem Verschlüsselungsmanagement-Server (KMS) oder dem KMS-Cluster verbinden kann, da der Hostname des 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 durchzuführen, geben Sie die DNS-Server im Grid Manager an (**Wartung** > **Netzwerk** > **DNS-Server**).

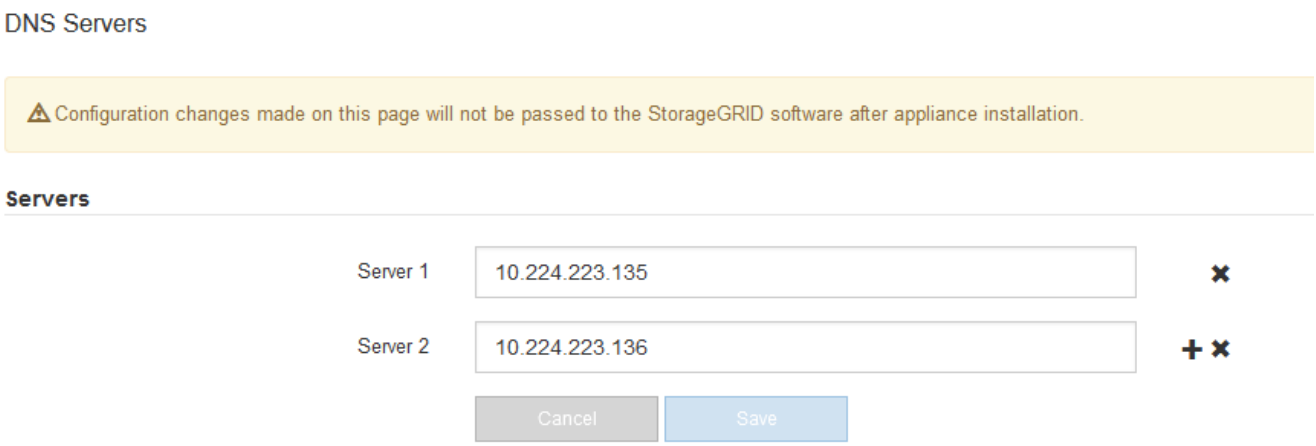
- Temporäre Änderungen an der DNS-Konfiguration sind nur für Node-verschlüsselte Appliances erforderlich, bei denen der KMS-Server mithilfe eines vollständig qualifizierten Domänennamens anstelle einer IP-Adresse für den Hostnamen definiert wird.
- Wenn eine Node-verschlüsselte Appliance über einen Domänennamen 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 Node keinen DNS-Server für das Grid erreichen kann oder wenn die DNS-Einstellungen für das gesamte Grid geändert wurden, wenn ein Node-verschlüsselter Appliance-Node offline war, kann der Node keine Verbindung mit dem KMS herstellen. Verschlüsselte Daten auf der Appliance können erst entschlüsselt werden, wenn das DNS-Problem behoben ist.

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 Node offline war, kann der Node nach seinem Wechsel wieder online den KMS nicht erreichen, 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.



3. Ändern Sie bei Bedarf die DNS-Server.

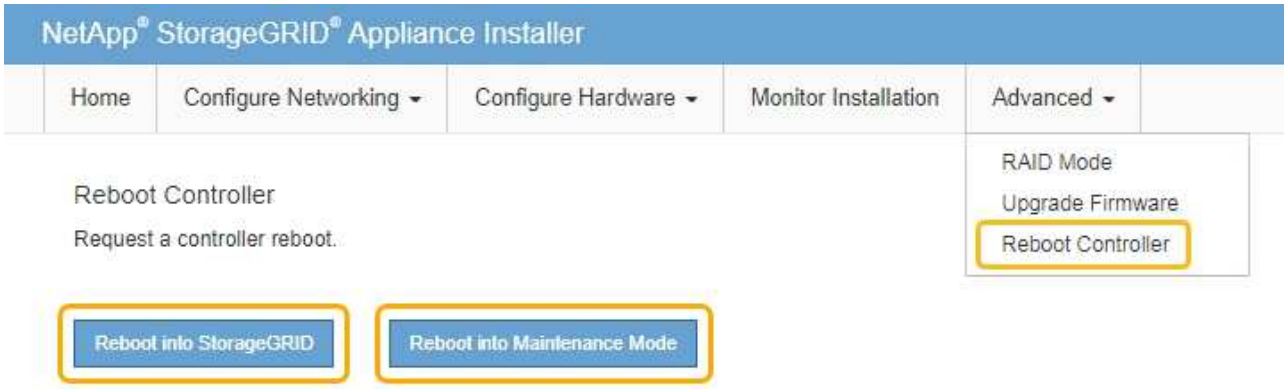
> Änderungen an den DNS-Einstellungen erfolgen temporär und gehen verloren, wenn Sie den Wartungsmodus beenden.

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.

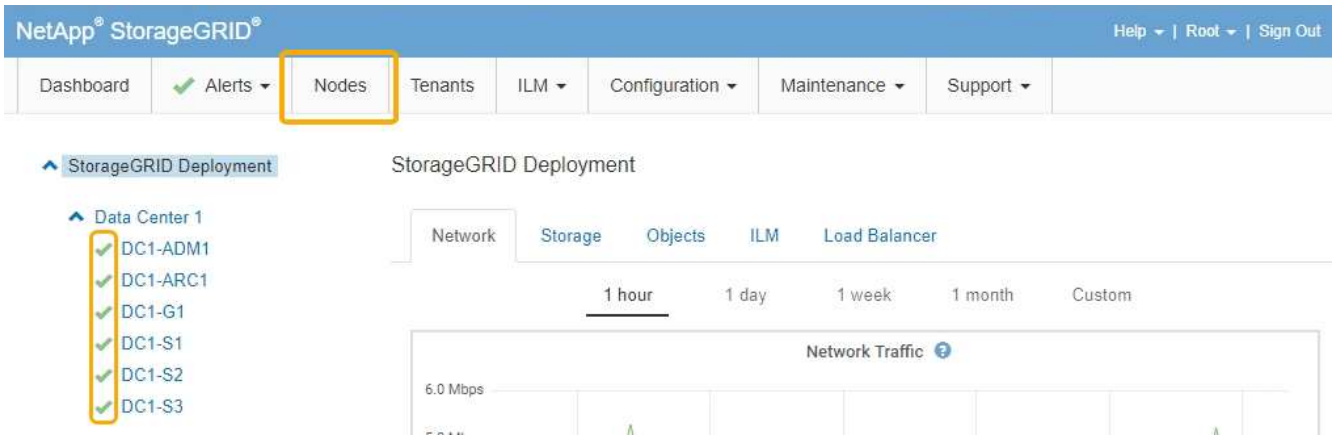
5. Nachdem die Node-Daten entschlüsselt wurden, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 befand.

   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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Monitoring 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).

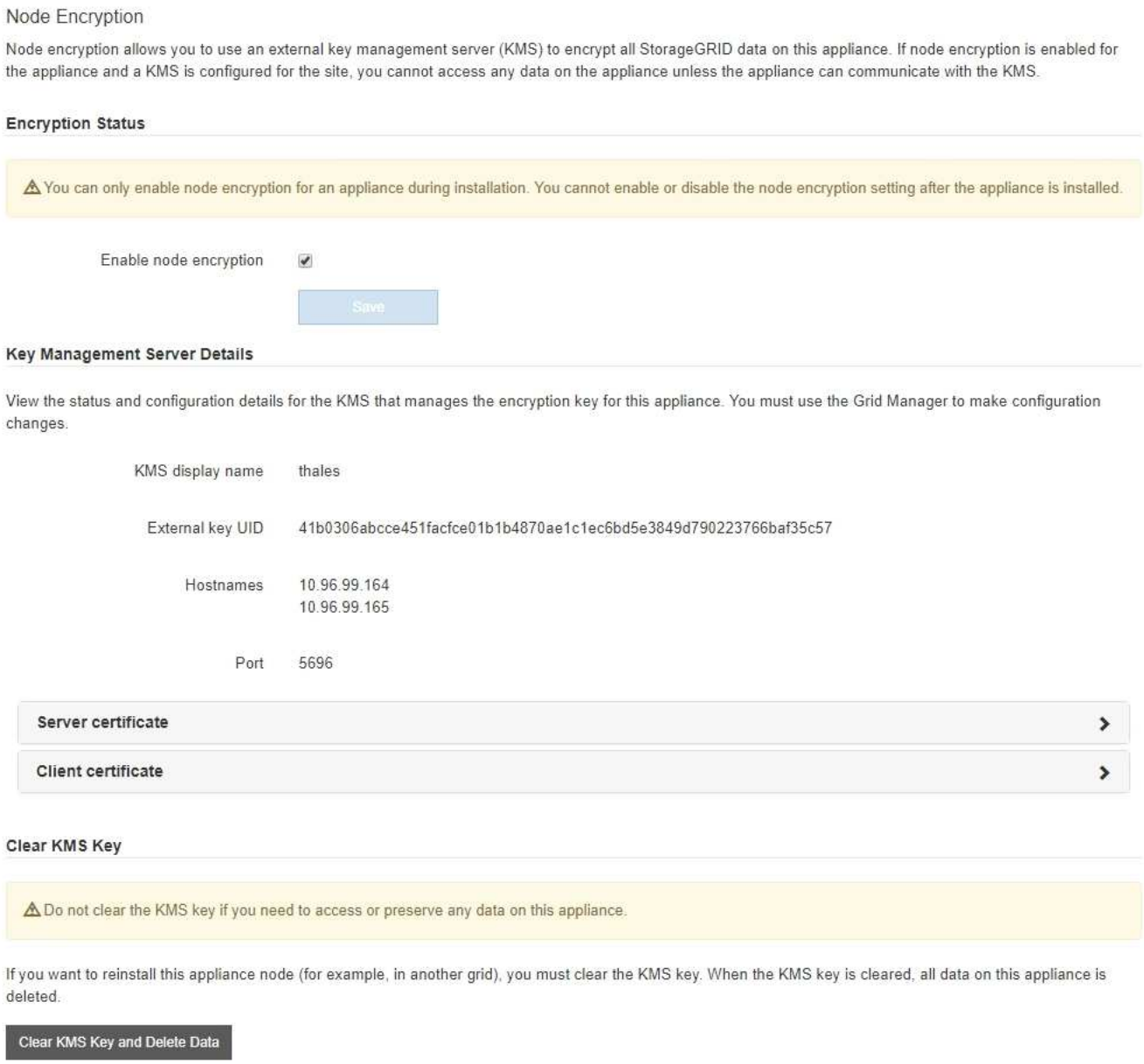
Was Sie benötigen

- Die Node-Verschlüsselung muss während der Installation für die Appliance aktiviert sein. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht aktivieren.
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Hardware konfigurieren** > **Node-Verschlüsselung**.



Die Seite Node Encryption umfasst die folgenden 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.
  - Wenn Sie Probleme mit den Zertifikaten selbst beheben möchten, z. B. die Verlängerung abgelaufener Zertifikate, lesen Sie die Informationen zu KMS in den Anweisungen zur Verwaltung von StorageGRID.
  - Wenn bei der Verbindung zu KMS-Hosts unerwartete Probleme auftreten, überprüfen Sie, ob die DNS-Server (Domain Name System) korrekt sind und das Netzwerk der Appliance korrekt konfiguriert ist.

    "Überprüfen der DNS-Serverkonfiguration"

- 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. Sie müssen den KMS-Schlüssel löschen, bevor Sie die Appliance in einem anderen StorageGRID-System installieren können.

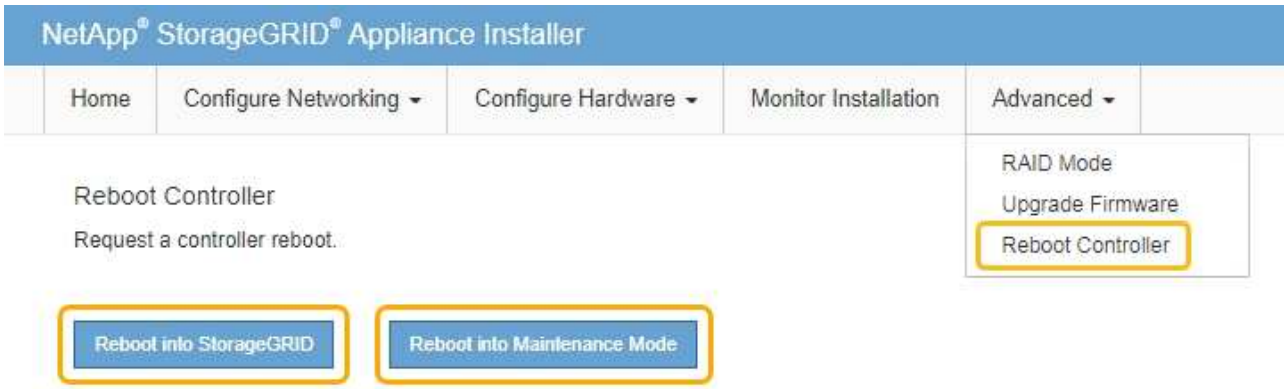
"Löschen der Konfiguration des Schlüsselverwaltungsservers"

Durch das Löschen der KMS-Konfiguration werden Daten von der Appliance gelöscht, sodass dauerhaft kein Zugriff darauf besteht. Diese Daten können nicht wiederhergestellt werden.

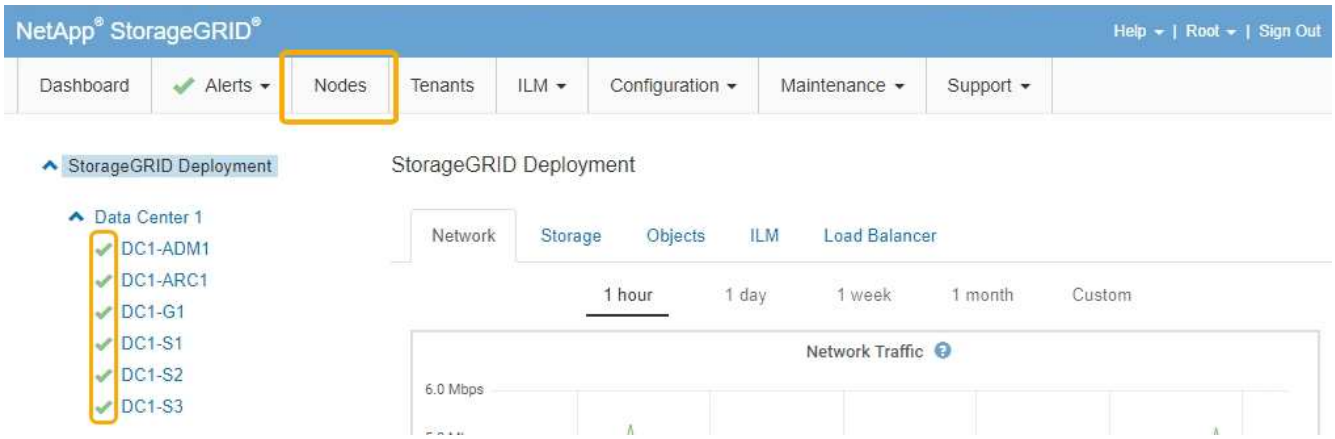
2. Wenn Sie den Status der Node-Verschlüsselung überprüfen, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

◦ 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Löschen der Konfiguration des Schlüsselverwaltungsservers

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.

Was Sie benötigen

Wenn Daten auf der Appliance aufbewahrt werden müssen, müssen Sie einen Node außer Betrieb nehmen, 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.

Den Node muss deaktiviert werden, um alle in ihm enthaltenen Daten auf anderen Nodes in StorageGRID zu verschieben. Anweisungen zur Ausmusterung von Grid-Nodes finden Sie in den Angaben zu Recovery und Wartung.

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 Vorgang 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 eine Neuinstallation eines Appliance-Node in einem StorageGRID-System planen, das denselben KMS-Schlüssel verwendet.

- 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.

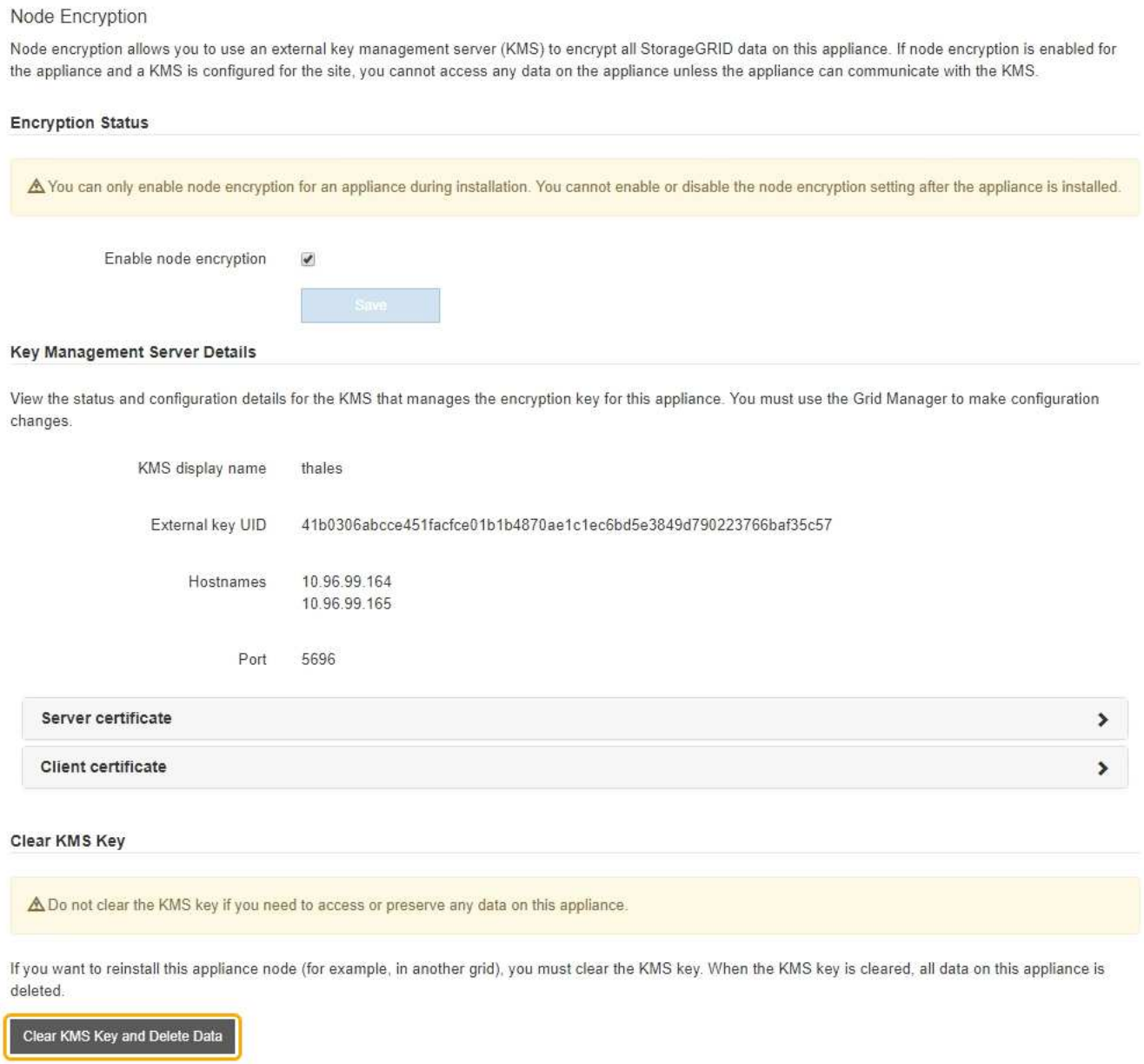
Schritte

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.

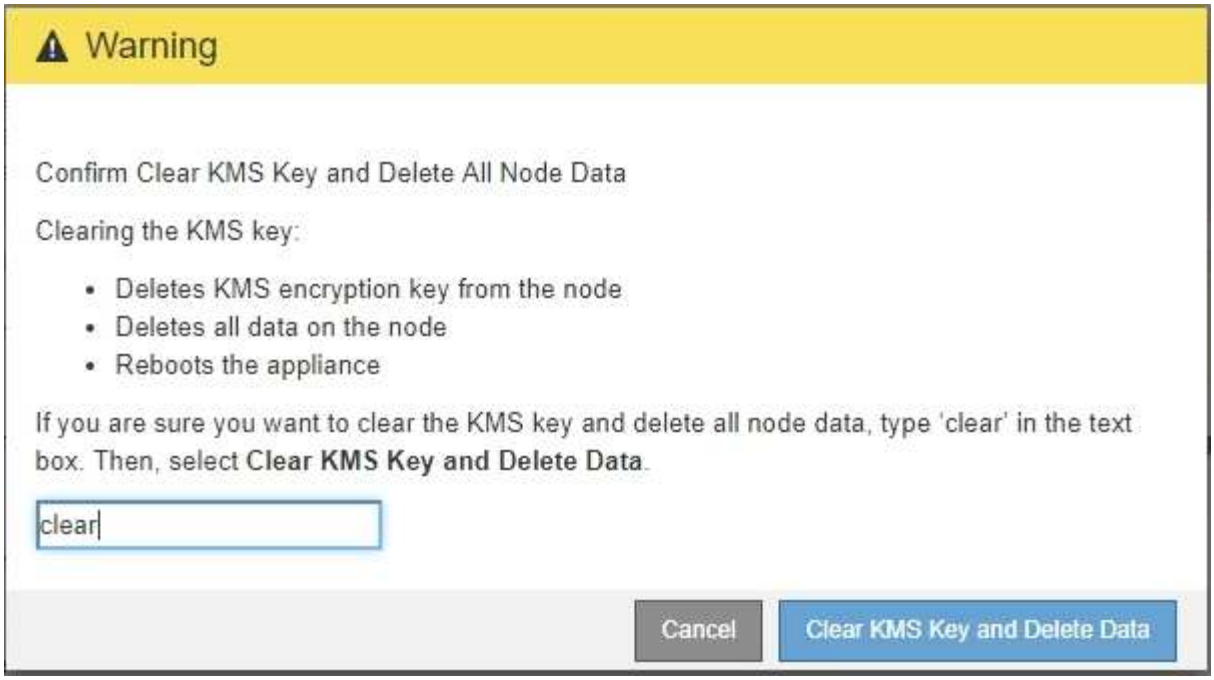
   Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

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` + und wählen Sie **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. Informationen zur Vorbereitung einer Appliance für die Neuinstallation finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Verwandte Informationen

"StorageGRID verwalten"

"Verwalten Sie erholen"

SG5600 Storage Appliances

StorageGRID SG5612 und SG5660 Appliances installieren und warten

- "Übersicht über die StorageGRID Appliance"
- "Übersicht über Installation und Implementierung"
- "Installation wird vorbereitet"
- "Installieren der Hardware"
- "Konfigurieren der Hardware"
- "Implementieren eines Appliance-Storage-Node"
- "Monitoring der Installation der Speicher-Appliance"
- "Automatisierung der Installation und Konfiguration von Appliances"
- "Überblick über die Installations-REST-APIs"
- "Fehlerbehebung bei der Hardwareinstallation"
- "Warten der SG5600 Appliance"

Übersicht über die StorageGRID Appliance

Die StorageGRID SG5600 Appliance ist eine integrierte Storage- und Computing-Plattform, die als Storage Node in einem StorageGRID Grid ausgeführt wird.

Die StorageGRID SG5600 Appliance enthält die folgenden Komponenten:

Komponente	Beschreibung
E5600SG-Controller	Server berechnen der E5600SG-Controller führt das Betriebssystem Linux und die StorageGRID-Software aus. Dieser Controller stellt eine Verbindung zu folgenden Komponenten her: • Die Admin-, Grid- und Client-Netzwerke für das StorageGRID-System • Der E2700 Controller mit dualen SAS-Pfaden (aktiv/aktiv) und der E5600SG Controller arbeitet als Initiator

Komponente	Beschreibung
E2700 Controller	Storage Controller der E2700 fungiert als Standard-Storage-Array der E-Series im Simplexmodus und führt das Betriebssystem SANtricity (Controller-Firmware) aus. Dieser Controller stellt eine Verbindung zu folgenden Komponenten her: • Das Managementnetzwerk, in dem SANtricity Storage Manager installiert ist • Der E5600SG Controller mit dualen SAS-Pfaden (aktiv/aktiv) wobei der E2700 Controller als Ziel arbeitet

Die SG5600 Appliance enthält je nach Modell außerdem die folgenden Komponenten:

Komponente	Modell SG5612	Modell SG5660
Laufwerke	12 NL-SAS-Laufwerke	60 NL-SAS-Laufwerke
Gehäuse	DE1600 Gehäuse: Ein 2-HE-Chassis mit zwei Höheneinheiten und Controllern	DE6600-Gehäuse, ein 4-HE-Chassis (Rack-Unit), das die Laufwerke und die Controller beherbergt
Netzteile und Lüfter	Zwei Power-Fan-Kanister	Zwei Netzteile und zwei Lüfter

Der E5600SG Controller ist stark auf den Einsatz im StorageGRID-Gerät zugeschnitten. Alle anderen Komponenten arbeiten wie in der Dokumentation zur E-Series beschrieben, mit Ausnahme dieser Anweisungen.

Der maximale Rohkapazität, der auf jedem StorageGRID-Appliance-Storage-Node verfügbar ist, kann anhand des Appliance-Modells und der Konfiguration festgelegt werden. Der verfügbare Storage kann nicht erweitert werden, indem ein Shelf mit zusätzlichen Laufwerken hinzugefügt wird.

Funktionen der StorageGRID Appliance

Die StorageGRID SG5600 Appliance ist eine integrierte Storage-Lösung zum Erstellen eines neuen StorageGRID Systems oder zur Erweiterung der Kapazität eines vorhandenen Systems.

Die StorageGRID Appliance bietet folgende Funktionen:

- StorageGRID Storage Node Computing und Storage-Elemente in einer einzelnen, effizienten und integrierten Lösung kombiniert
- Vereinfacht die Installation und Konfiguration eines Storage Node und automatisiert den Großteil des erforderlichen Prozesses

- Bietet eine hochdichte Storage-Lösung mit zwei Gehäuseoptionen: Eine für 2 HE und eine für 4 HE
- Verwendet 10-GbE-IP-Schnittstellen direkt zum Storage Node ohne Bedarf an Zwischen-Storage-Schnittstellen wie FC oder iSCSI
- Kann in einer hybriden Grid-Umgebung verwendet werden, die StorageGRID Appliances und virtuelle (softwarebasierte) Storage-Nodes verwendet
- Enthält vorkonfigurierten Storage und wird vorab mit dem StorageGRID Appliance Installer (auf dem E5600SG Controller) für praxiserprobe Software-Implementierung und -Integration geliefert

Hardwarediagramme

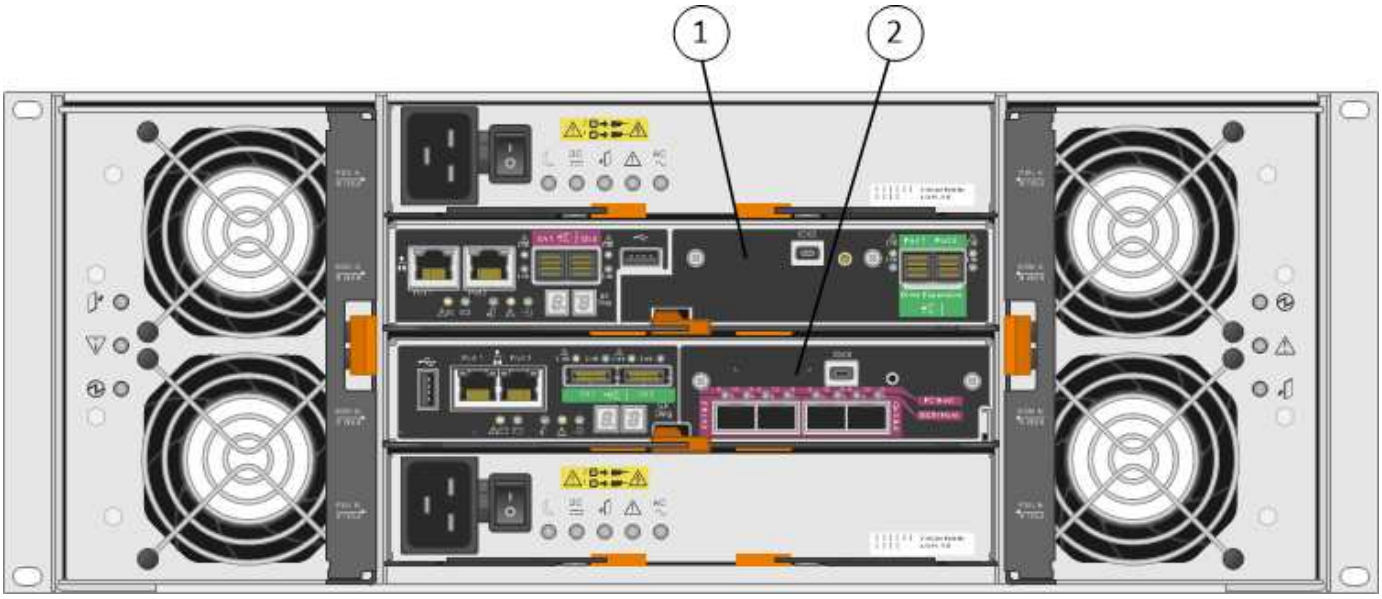
Die SG5612 und SG5660 Modelle der StorageGRID Appliance umfassen einen E2700 Controller und einen E5600SG Controller. Sie sollten sich die Diagramme ansehen, um sich über die Unterschiede zwischen den Modellen und den Controllern zu informieren.

Modell SG5612 2 HE: Rückansicht des E2700 Controllers und des E5600SG Controllers

	Beschreibung
1	E2700 Controller
2	E5600SG-Controller

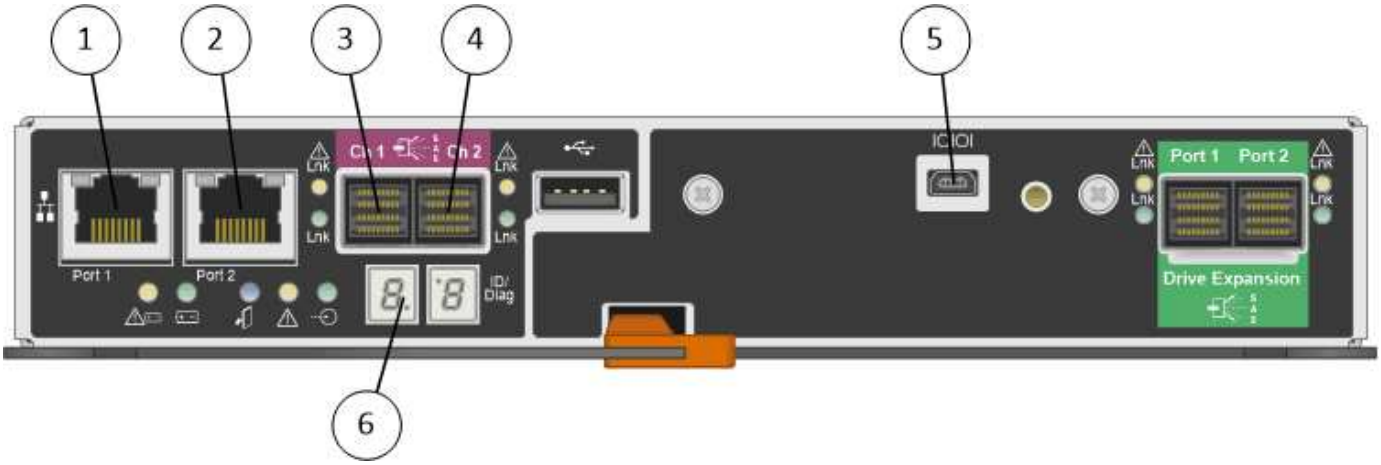
Modell SG5660 4U: Rückansicht des E2700 Controllers und des E5600SG Controllers

Der E2700 Controller befindet sich über dem E5600SG Controller.



	Beschreibung
1	E2700 Controller
2	E5600SG-Controller

Rückansicht des E2700 Controllers

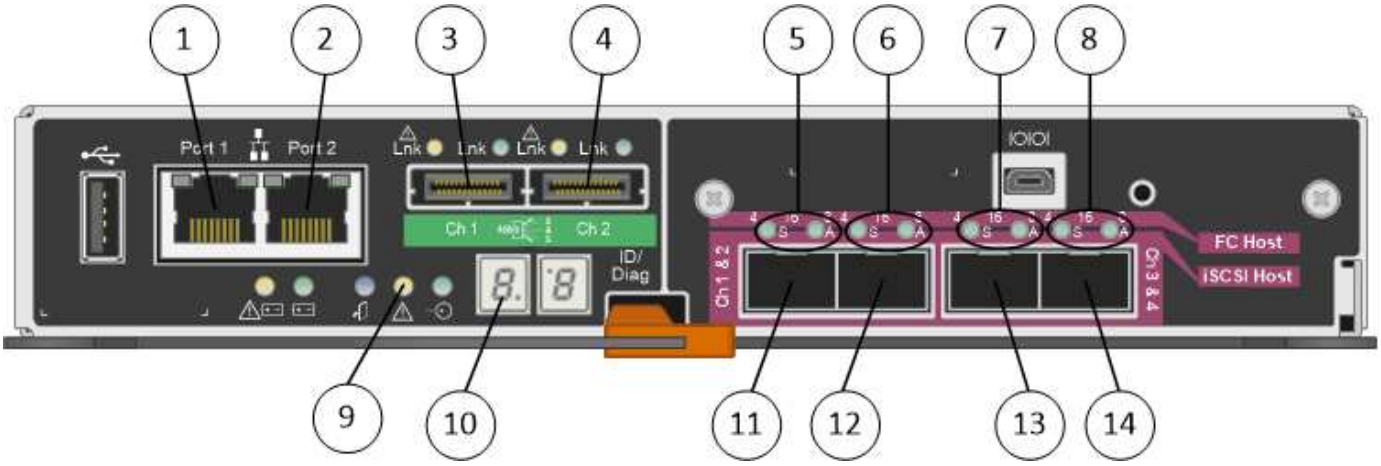


	Beschreibung
1	Management-Port 1 (Verbinden Sie mit dem Netzwerk, in dem SANtricity Storage Manager installiert ist.)
2	Management-Port 2 (bei der Installation zum Herstellen einer Verbindung zu einem Laptop verwenden)
3	SAS-Interconnect-Port 1
4	SAS-Interconnect-Port 2

	Beschreibung
5	Serieller Anschluss
6	Sieben-Segment-Anzeige

Es werden nicht die beiden SAS-Ports namens Drive Expansion (grün) auf der Rückseite des E2700 Controllers verwendet. Die StorageGRID Appliance unterstützt keine Festplatten-Shelfs zur Erweiterung.

Rückansicht des E5600SG-Controllers



	Beschreibung
1	Management-Port 1 (Verbinden Sie mit dem Admin-Netzwerk für StorageGRID.)
2	Management-Port 2 Optionen: • 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 für die IP-Konfiguration, wenn DHCP-zugeordnete IP-Adressen nicht verfügbar sind.
3	SAS-Interconnect-Port 1
4	SAS-Interconnect-Port 2
5	Fehler- und aktiv-LEDs für 10-GbE-Netzwerkanschluss 1
6	Fehler- und aktiv-LEDs für 10-GbE-Netzwerkanschluss 2
7	Fehler- und aktiv-LEDs für 10-GbE-Netzwerkanschluss 3

	Beschreibung
8	Fehler- und aktiv-LEDs für 10-GbE-Netzwerkanschluss 4
9	LED für Warnung
10	Sieben-Segment-Anzeige
11	10-GbE-Netzwerkanschluss 1
12	10-GbE-Netzwerkanschluss 2
13	10-GbE-Netzwerkanschluss 3
14	10-GbE-Netzwerkanschluss 4

Die Host Interface Card (HIC) des StorageGRID Appliance E5600SG Controllers unterstützt nur 10-GB-Ethernet-Verbindungen. Er kann nicht für iSCSI-Verbindungen verwendet werden.

Übersicht über Installation und Implementierung

Sie können eine oder mehrere StorageGRID Appliances installieren, wenn Sie StorageGRID zum ersten Mal implementieren. Alternativ können Sie Appliance Storage-Nodes später im Rahmen einer Erweiterung hinzufügen. Möglicherweise müssen Sie auch einen Appliance-Speicherknoten im Rahmen eines Wiederherstellungsvorgangs installieren.

Das Hinzufügen einer StorageGRID Storage Appliance zu einem StorageGRID System umfasst vier primäre Schritte:

1. Installation vorbereiten:
   - Vorbereiten des Installationsstandorts
   - Auspacken der Schachteln und Prüfen des Inhalts
   - Zusätzliche Ausrüstung und Werkzeuge
   - Sammeln von IP-Adressen und Netzwerkinformationen
   - Optional: Konfiguration eines externen Verschlüsselungsmanagement-Servers (KMS), wenn Sie alle Appliance-Daten verschlüsseln möchten. Weitere Informationen zum externen Verschlüsselungsmanagement finden Sie in der Anleitung zur Administration von StorageGRID.
2. Installieren der Hardware:
   - Registrieren der Hardware
   - Installieren des Geräts in einem Schrank oder Rack
   - Installieren der Laufwerke (nur SG5660)
   - Verkabeln Sie das Gerät
   - Anschließen der Stromkabel und Strom anschließen

- Anzeigen von Boot-Statuscodes

3. Konfigurieren der Hardware:
   - Zugriff auf SANtricity Storage Manager, Festlegen einer statischen IP-Adresse für den Management-Port 1 auf dem E2700 Controller und Konfigurieren von SANtricity Storage Manager-Einstellungen
   - Zugriff auf das Installationsprogramm von StorageGRID Appliance und Konfiguration der für die Verbindung mit StorageGRID-Netzwerken erforderlichen Link- und Netzwerk-IP-Einstellungen
   - Optional: Aktivieren der Node-Verschlüsselung, wenn Sie zur Verschlüsselung von Appliance-Daten einen externen KMS verwenden möchten.
   - Optional: Ändern des RAID-Modus.
4. Bereitstellen der Appliance als Storage-Node:

Aufgabe	Siehe
Bereitstellen eines Appliance-Speicherknoten in einem neuen StorageGRID-System	"Implementieren eines Appliance-Storage-Node"
Hinzufügen eines Appliance-Speicherknotens zu einem vorhandenen StorageGRID-System	Anweisungen zum erweitern eines StorageGRID-Systems
Bereitstellen eines Appliance-Speicherknotens als Teil eines Speicherknotenwiederherstellungsvorgangs	Anweisungen zur Wiederherstellung und Wartung

Verwandte Informationen

"Installation wird vorbereitet"

"Installieren der Hardware"

"Konfigurieren der Hardware"

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

"StorageGRID verwalten"

Installation wird vorbereitet

Die Vorbereitung der Installation einer StorageGRID Appliance umfasst die Vorbereitung des Standorts und den Erwerb aller erforderlichen Hardware, Kabel und Tools. Außerdem sollten Sie IP-Adressen und Netzwerkinformationen erfassen.

Schritte

- "Vorbereiten des Standorts (SG5600)"
- "Auspacken der Boxen (SG5600)"
- "Beschaffung zusätzlicher Geräte und Werkzeuge (SG5600)"
- "Anforderungen an Service-Laptops"
- "Anforderungen an einen Webbrowser"

- "Überprüfen von Appliance-Netzwerkverbindungen"
- "Sammeln von Installationsinformationen (SG5600)"

Vorbereiten des Standorts (SG5600)

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. Weitere Informationen finden Sie im NetApp Hardware Universe.
2. Passen Sie zu 48.3 Shelfs dieser Größe (ohne Kabel) ein 19-cm-Gehäuse oder -Rack an:

Appliance-Modell	Höhe	Breite	Tiefe	Maximales Gewicht
SG5612 (12 Festplatten)	3.40 Zoll (8.64 cm)	19.0 Zoll (48.26 cm)	21.75 Zoll (55.25 cm)	59.5 lb (27 kg)
SG5660 (60 Festplatten)	7.00 Zoll (17.78 cm)	17.75 Zoll (45.08 cm)	32.50 Zoll (82.55 cm)	236.2 lb. (107.1 kg)

3. Installieren Sie alle erforderlichen Netzwerk-Switches. Informationen zur Kompatibilität sind im NetApp Interoperabilitäts-Matrix-Tool verfügbar.

Verwandte Informationen

"NetApp Hardware Universe"

"NetApp Interoperabilität"

Auspacken der Boxen (SG5600)

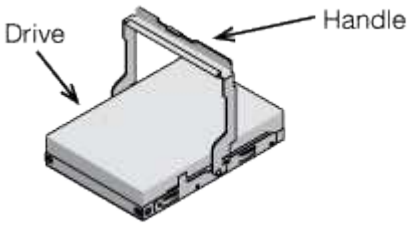
Packen Sie vor der Installation des StorageGRID-Geräts alle Kartons aus und vergleichen Sie den Inhalt mit den Artikeln auf dem Verpackungsschein.

- **SG5660 Gehäuse, ein 4-HE-Gehäuse mit 60 Laufwerken**

- **SG5612-Gehäuse, 2-HE-Chassis mit 12 Laufwerken**

- **4U-Blende oder 2U-Endkappen**

- **NL-SAS-Laufwerke**



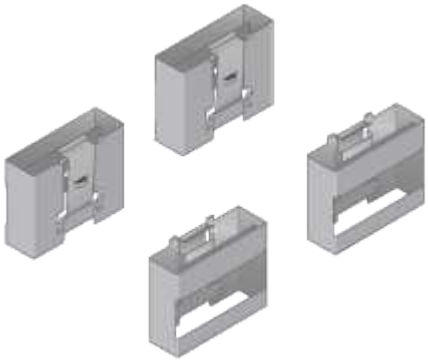
  Laufwerke sind zur Sicherheit beim Versand in der SG5612 mit 2 HE vorinstalliert, jedoch nicht in der 4 HE SG5660.

- * E5600SG Controller*

- **E2700 Controller**

- **Befestigungsschienen und Schrauben**

- **Gehäusegriffe (nur 4-HE-Gehäuse)**



Kabel und Anschlüsse

Der Versand für das StorageGRID Gerät umfasst die folgenden Kabel und Anschlüsse:

- **Stromkabel für Ihr Land**

  Das Gerät wird mit zwei Wechselstromkabeln an eine externe Stromquelle, z. B. an einen Netzstecker, angeschlossen. Ihr Schrank verfügt möglicherweise über spezielle Netzkabel, die Sie anstelle der Netzkabel verwenden, die Sie zur Einheit mit dem Gerät anschließen.

- **SAS-Verbindungskabel**

Zwei 0.5-Meter-SAS-Verbindungskabel mit Mini-SAS-HD- und Mini-SAS-Anschlüssen.

Der quadratische Stecker wird an den E2700 Controller angeschlossen und der rechteckige Stecker wird an den E5600SG Controller angeschlossen.

Beschaffung zusätzlicher Geräte und Werkzeuge (SG5600)

Vergewissern Sie sich vor der Installation der SG5600 Appliance, dass alle zusätzlichen Geräte und Tools zur Verfügung stehen, die Sie benötigen.

- **Schraubendreher**

Phillips Nr. 2 Schraubendreher

Mittlere Flachschraubendreher

- **ESD-Handgelenkschlaufe**

- * Ethernet-Kabel*

- **Ethernet-Switch**

- **Service-Laptop**

Anforderungen an Service-Laptops

Bevor Sie die Hardware der StorageGRID-Appliance installieren, sollten Sie prüfen, ob der Service-Laptop über die mindestens erforderlichen Ressourcen verfügt.

Der Service-Laptop, der für die Hardwareinstallation benötigt wird, muss die folgenden Anforderungen erfüllen:

- Microsoft Windows Betriebssysteme
- Netzwerkport
- Unterstützter Webbrowser
- NetApp SANtricity Storage Manager Version 11.40 oder höher
- SSH-Client (z. B. PuTTY)

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"NetApp Dokumentation: SANtricity Storage Manager"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87

Webbrowser	Unterstützte Mindestversion
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Überprüfen von 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.

StorageGRID Appliance-Netzwerke

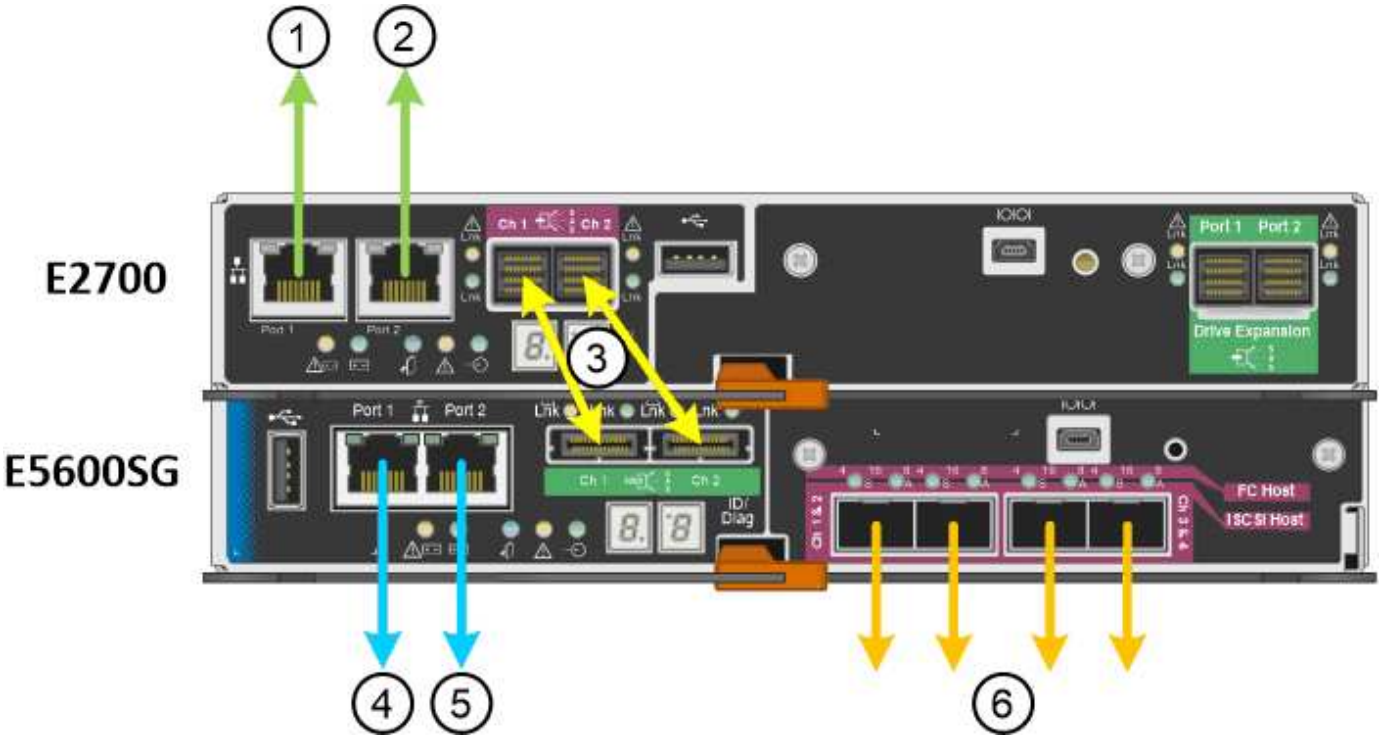
Wenn Sie eine StorageGRID Appliance als Storage Node bereitstellen, können Sie sie mit folgenden Netzwerken verbinden:

- **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 Network forStorageGRID**: 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. Das Client-Netzwerk ist optional.
- **Managementnetzwerk für SANtricity Storage Manager**: Der E2700 Controller ist mit dem Managementnetzwerk verbunden, in dem SANtricity Storage Manager installiert ist. Damit können Sie die Hardwarekomponenten der Appliance überwachen und verwalten. Dieses Managementnetzwerk kann das gleiche sein wie das Admin-Netzwerk für StorageGRID, oder es kann ein unabhängiges Managementnetzwerk sein.

Ausführliche Informationen zu StorageGRID-Netzwerken finden Sie unter *Rasterprimer*.

Verbindungen zu StorageGRID-Appliances

Wenn Sie eine StorageGRID-Appliance installieren, müssen Sie die beiden Controller miteinander und mit den erforderlichen Netzwerken verbinden. Die Abbildung zeigt die beiden Controller in der SG5660, wobei der E2700 Controller oben und der E5600SG Controller unten gezeigt werden. In der SG5612 befindet sich der E2700 Controller links vom E5600SG Controller.



Element	Port	Typ des Ports	Funktion
1	Management-Port 1 am E2700 Controller	1-GB-Ethernet (RJ-45	Verbindet den E2700 Controller mit dem Netzwerk, in dem SANtricity Storage Manager installiert wird.
2	Management-Port 2 am E2700 Controller	1-GB-Ethernet (RJ-45	Verbindet den E2700 Controller während der Installation mit einem Service-Laptop.
3	Zwei SAS Interconnect Ports an jedem Controller, gekennzeichnet mit CH 1 und CH 2	E2700 Controller: Mini-SAS-HD E5600SG Controller: Mini-SAS	Verbinden Sie die beiden Controller miteinander.
4	Management-Port 1 am E5600SG-Controller	1-GB-Ethernet (RJ-45	Verbindet den E5600SG-Controller mit dem Admin-Netzwerk für StorageGRID.

Element	Port	Typ des Ports	Funktion
5	Management-Port 2 am E5600SG-Controller	1-GB-Ethernet (RJ-45	• 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 verwendet werden, um den E5600SG-Controller während der Installation mit einem Service-Laptop zu verbinden, wenn keine DHCP-zugewiesene IP-Adresse verfügbar ist.
6	Vier Netzwerk-Ports am E5600SG Controller	10 GbE (optisch)	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her. Siehe „10-GbE-Port-Verbindungen für den E5600SG-Controller“.

Verwandte Informationen

"Port Bond-Modi für die E5600SG Controller-Ports"

"Sammeln von Installationsinformationen (SG5600)"

"Verkabeln der Appliance (SG5600)"

"Netzwerkrichtlinien"

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Port Bond-Modi für die E5600SG Controller-Ports

Wenn Sie Netzwerkverbindungen für die Controller-Ports E5600SG konfigurieren, können Sie die Portbindung für die 10-GbE-Ports verwenden, die mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk verbunden sind, sowie 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.

Verwandte Informationen

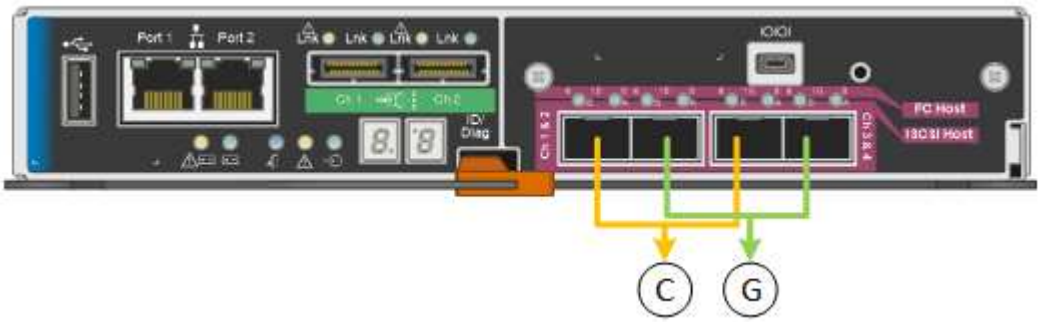
"Konfigurieren von Netzwerkverbindungen (SG5600)"

Netzwerk-Bond-Modi für die 10-GbE-Ports

Die 10-GbE-Netzwerk-Ports auf dem E5600SG Controller unterstützen den Bond-Modus „fester Port“ oder den Bond-Aggregat-Port für Grid-Netzwerk- und Client-Netzwerkverbindungen.

Bond-Modus mit festem Port

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



	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 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.

	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 müssen wissen, wie die Switches konfiguriert werden, um VLAN, LACP und MLAG zu verwenden.

Wenn Sie nicht alle vier 10-GbE-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 10-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 die 1-GbE-Management-Ports

Für die beiden 1-GbE-Management-Ports des E5600SG-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 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 E5600SG-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 Verwaltungsport 2 an und greifen Sie über die IP-Adresse 169.254.0 auf das Gerät zu.

Sammeln von Installationsinformationen (SG5600)

Bei der Installation und Konfiguration der StorageGRID Appliance sind Entscheidungen zu treffen und Informationen zu Ethernet Switch-Ports, IP-Adressen sowie zu Port- und Netzwerk-Bond-Modi zu sammeln.

Über diese Aufgabe

Mithilfe der folgenden Tabellen können Sie Informationen für jedes Netzwerk, das Sie mit der Appliance verbinden, aufzeichnen. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.

Erforderliche Informationen für die Verbindung des E2700 Controllers mit dem SANtricity Storage Manager

Sie müssen den E2700 Controller mit dem Managementnetzwerk verbinden, das Sie für SANtricity Storage 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)	
Über DHCP zugewiesene IP-Adresse für Management-Port 1, sofern nach dem Einschalten verfügbar **Hinweis:** Wenn das Netzwerk, das Sie mit dem E2700 Controller verbinden, einen DHCP-Server enthält, kann der Netzwerkadministrator die MAC-Adresse verwenden, um die vom DHCP-Server zugewiesene IP-Adresse zu ermitteln.	
Geschwindigkeit und Duplexmodus **Hinweis:** Sie müssen sicherstellen, dass der Ethernet-Switch für das SANtricity Storage Manager-Managementnetzwerk auf Autonegotiation gesetzt ist.	Muss sein: • Autonegotiation (Standard)

Erforderliche Informationen	Ihr Wert
IP-Adressformat	Bitte auswählen: • IPv4 • IPv6
Statische IP-Adresse, die Sie für die Appliance im Managementnetzwerk verwenden möchten	Für IPv4: • IPv4-Adresse: • Subnetzmaske: • Gateway: Für IPv6: • IPv6-Adresse: • Routingfähige IP-Adresse: • E2700 Controller-Router-IP-Adresse:

Informationen zum Anschließen des E5600SG-Controllers an das Admin-Netzwerk erforderlich

Das Admin-Netzwerk für StorageGRID ist ein optionales Netzwerk, das zur Systemadministration und -Wartung verwendet wird. Die Appliance stellt über die 1-GbE-Management-Ports des E5600SG-Controllers eine Verbindung zum Admin-Netzwerk her.

Erforderliche Informationen	Ihr Wert
Admin-Netzwerk aktiviert	Bitte auswählen: • Nein • Ja (Standard)
Netzwerk-Bond-Modus	Bitte auswählen: • Unabhängig • Aktiv/Backup
Switch-Port für Management-Port 1 (P1)	
Switch-Port für Management Port 2 (P2; nur aktiv/Backup-Netzwerk-Bond-Modus)	
MAC-Adresse für Management-Port 1 (auf einem Etikett in der Nähe von Port P1 gedruckt)	

Erforderliche Informationen	Ihr Wert
Über DHCP zugewiesene IP-Adresse für Management-Port 1, sofern nach dem Einschalten verfügbar **Hinweis:** enthält das Admin-Netzwerk einen DHCP-Server, zeigt der E5600SG-Controller nach dem Start die DHCP-zugewiesene IP-Adresse auf seinem siebensegmentreichen 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.	• 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.	• IPv4-Adresse (CIDR): • Gateway:
Admin-Netzwerk-Subnetze (CIDR)	

Zum Verbinden und Konfigurieren der 10-GbE-Ports am E5600SG-Controller erforderliche Informationen

Die vier 10-GbE-Ports des E5600SG-Controllers verbinden das StorageGRID-Grid-Netzwerk und das Client-Netzwerk.

Weitere Informationen zu den Optionen für diese Ports finden Sie unter „10-GbE-Portverbindungen für den E5600SG-Controller“.

Erforderliche Informationen	Ihr Wert
Port Bond-Modus	Bitte auswählen: • 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)	

Erforderliche Informationen	Ihr Wert
Switch-Port für Port 4 (Grid-Netzwerk für Fixed-Modus)	

Zum Anschließen des E5600SG-Controllers an das 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-GbE-Ports des E5600SG-Controllers mit dem Grid-Netzwerk verbunden.

Weitere Informationen zu den Optionen für diese Ports finden Sie unter „10-GbE-Portverbindungen für den E5600SG-Controller“.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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 E5600SG-Controller nach dem Booten die DHCP-zugewiesene IP-Adresse für das Grid-Netzwerk auf seiner 7-Segment-Anzeige an.	• 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.	• IPv4-Adresse (CIDR): • Gateway:
Grid-Netzwerknetze (CIDR) **Hinweis:** Wenn das Client-Netzwerk nicht aktiviert ist, verwendet die Standardroute auf dem Controller das hier angegebene Gateway.	

Informationen zum Anschließen des E5600SG-Controllers an das Client-Netzwerk erforderlich

Das Client-Netzwerk für StorageGRID ist ein optionales Netzwerk, das Client-Protokollzugriff auf das Grid ermöglicht. Die Appliance wird über die 10-GbE-Ports des E5600SG-Controllers mit dem Client-Netzwerk verbunden.

Weitere Informationen zu den Optionen für diese Ports finden Sie unter „10-GbE-Portverbindungen für den E5600SG-Controller“.

Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: • Nein (Standard) • Ja.
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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	• 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.	• IPv4-Adresse (CIDR): • Gateway:

Verwandte Informationen

"Überprüfen von Appliance-Netzwerkverbindungen"

"Konfigurieren der Hardware"

"Port Bond-Modi für die E5600SG Controller-Ports"

Installieren der Hardware

Die Hardwareinstallation umfasst mehrere wichtige Aufgaben, einschließlich Installation

von Hardwarekomponenten, Verkabelung dieser Komponenten und Konfiguration von Ports.

Schritte

- "Registrieren der Hardware"
- "Installieren des Geräts in einem Schrank oder Rack (SG5600)"
- "Verkabeln der Appliance (SG5600)"
- "Anschließen der Netzstromkabel (SG5600)"
- "Einschalten (SG5600)"
- "Anzeigen des Boot-Status und Überprüfen von Fehlercodes auf den SG5600-Controllern"

Registrieren der Hardware

Die Registrierung der Appliance-Hardware bietet Support-Vorteile.

Schritte

1. Suchen Sie die Seriennummer des Chassis.

   Sie finden die Nummer auf dem Packzettel, in Ihrer Bestätigungs-E-Mail oder auf dem Gerät nach dem Auspacken.

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	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.
Neuer NetApp Kunde	a. Klicken Sie auf **Jetzt registrieren** und erstellen Sie ein Konto. b. Wählen Sie **Produkte** > **Produkte Registrieren**. c. Geben Sie die Seriennummer des Produkts und die angeforderten Details ein. Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.

Installieren des Geräts in einem Schrank oder Rack (SG5600)

Sie müssen Schienen in Ihrem Schrank oder Rack installieren und das Gerät dann auf die Schienen schieben. Wenn Sie über eine SG5660 verfügen, müssen Sie die Laufwerke auch nach der Installation der Appliance installieren.

Was Sie benötigen

- Sie haben das im Lieferumfang enthaltene Sicherheitshinweisen geprüft und die Vorsichtsmaßnahmen für das Bewegen und Installieren von Hardware verstanden.
- Sie verfügen über die Installationsanweisungen für die Hardware der E-Series.

> Installieren Sie die Hardware von der Unterseite des Racks oder Racks bis zu, um ein Umkippen des Geräts zu verhindern.

> Die SG5612 wiegt bei voller Beladung mit Laufwerken ca. 27 kg (60 lb). Für das sichere Verschieben der SG5612 sind zwei Personen oder ein mechanisierter Lift erforderlich.

> Die SG5660 wiegt etwa 60 kg (132 lb), ohne dass Laufwerke installiert werden. Um eine leere SG5660 sicher zu bewegen, sind vier Personen oder ein mechanisierter Hub erforderlich.

> Um Hardware-Schäden zu vermeiden, verschieben Sie niemals eine SG5660, wenn Laufwerke installiert sind. Vor dem Umstellen des Geräts müssen alle Laufwerke entfernt werden.

Über diese Aufgabe

Führen Sie die folgenden Aufgaben aus, um die SG5660 Appliance in einem Rack oder Schrank zu installieren.

- **Installieren Sie die Befestigungsschienen**

  Installieren Sie die Befestigungsschienen im Schrank oder Rack.

  Anweisungen zur Installation der E2700 oder der E5600 finden Sie in der Installationsanleitung für die E-Series.

- **Installieren Sie das Gerät im Schrank oder Rack**

  Schieben Sie das Gerät in das Gehäuse oder Rack und sichern Sie es.

  > Wenn Sie die SG5660 von Hand anheben, befestigen Sie die vier Griffe an den Seiten des Gehäuses. Sie entfernen diese Griffe, während Sie das Gerät auf die Schienen schieben.

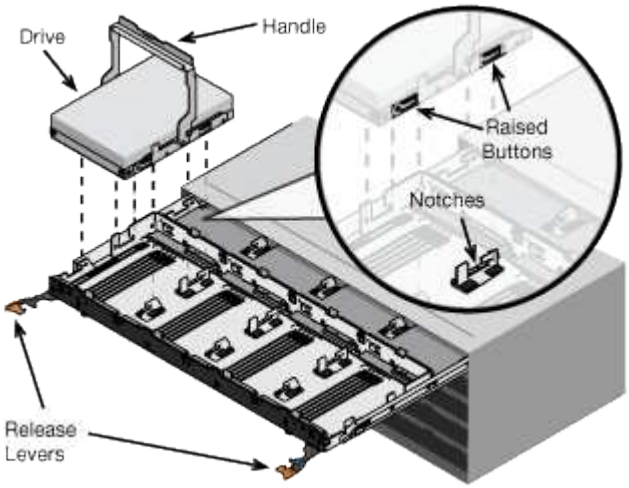
- **Installieren Sie die Laufwerke**

  Wenn Sie über eine SG5660 verfügen, installieren Sie 12 Laufwerke in jedem der 5 Laufwerksfächer.

  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 Schubladen.

- **Befestigen Sie die Frontblende**

  SG5612: Befestigen Sie die linken und rechten Endkappen an der Vorderseite.

  SG5660: Befestigen Sie die Blende an der Vorderseite.

Verwandte Informationen

"E2700 – Installationshandbuch für Controller-Laufwerke und zugehörige Laufwerksfächer"

"E5600 – Installationshandbuch für Controller-Laufwerke und zugehörige Laufwerksfächer"

Verkabeln der Appliance (SG5600)

Sie müssen die beiden Controller über SAS Interconnect-Kabel miteinander verbinden, die Management-Ports mit dem entsprechenden Managementnetzwerk verbinden und die 10 GbE-Ports des E5600SG Controllers mit dem Grid-Netzwerk und dem optionalen Client-Netzwerk für StorageGRID verbinden.

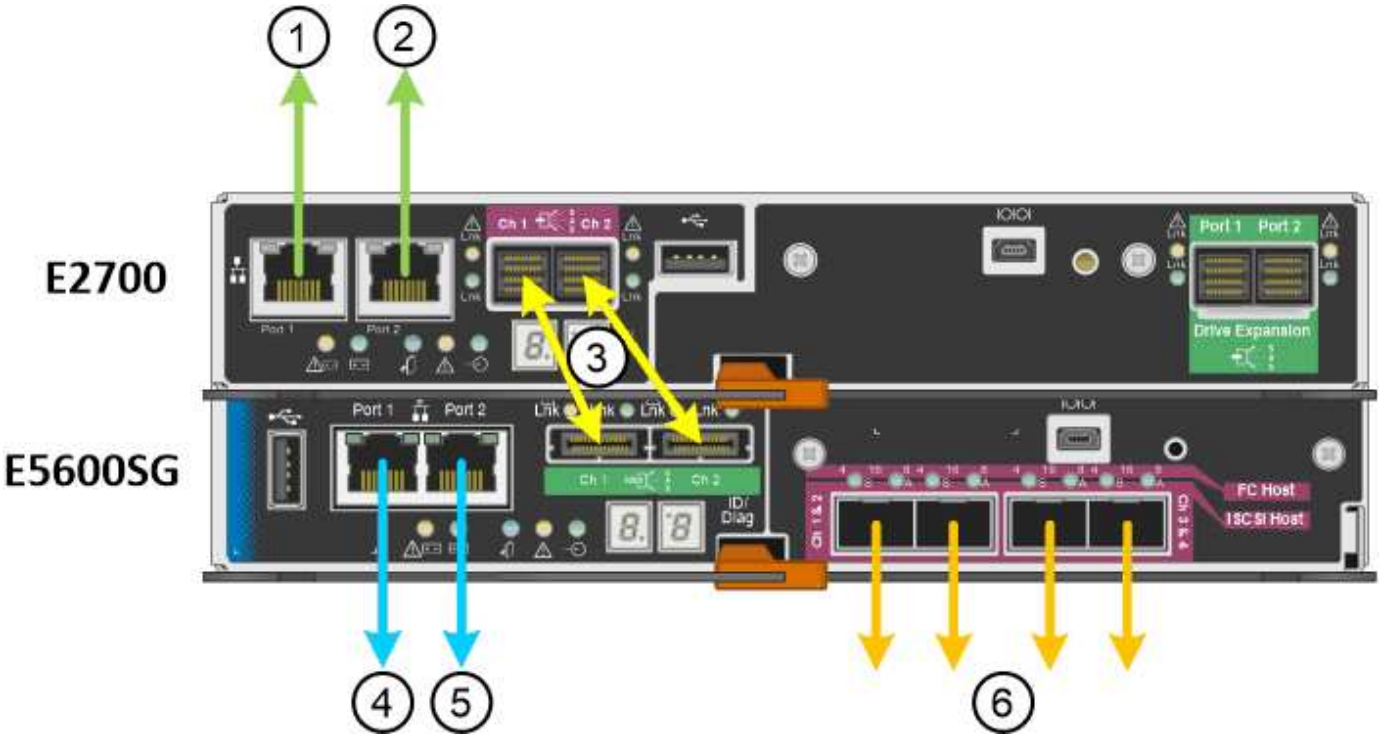
Was Sie benötigen

- Sie verfügen über Ethernet-Kabel für die Verbindung der Management-Ports.
- Sie haben optische Kabel zum Anschließen der vier 10-GbE-Ports (diese sind nicht im Lieferumfang des Geräts enthalten).

Gefahr der Laserstrahlung — kein Teil eines SFP-Transceivers zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

Über diese Aufgabe

Beachten Sie beim Anschließen der Kabel das folgende Diagramm, das den E2700 Controller oben und den E5600SG Controller unten zeigt. Das Diagramm zeigt das SG5660 Modell; die Controller des SG5612 Modells befinden sich nebeneinander anstatt in Stapeln.



Element	Port	Typ des Ports	Funktion
1	Management-Port 1 am E2700 Controller	1-GB-Ethernet (RJ-45	Verbindet den E2700 Controller mit dem Netzwerk, in dem SANtricity Storage Manager installiert wird.
2	Management-Port 2 am E2700 Controller	1-GB-Ethernet (RJ-45	Verbindet den E2700 Controller während der Installation mit einem Service-Laptop.
3	Zwei SAS Interconnect Ports an jedem Controller, gekennzeichnet mit CH 1 und CH 2	E2700 Controller: Mini-SAS-HD E5600SG Controller: Mini-SAS	Verbinden Sie die beiden Controller miteinander.
4	Management-Port 1 am E5600SG-Controller	1-GB-Ethernet (RJ-45	Verbindet den E5600SG-Controller mit dem Admin-Netzwerk für StorageGRID.

Element	Port	Typ des Ports	Funktion
5	Management-Port 2 am E5600SG-Controller	1-GB-Ethernet (RJ-45	• 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 verwendet werden, um den E5600SG-Controller während der Installation mit einem Service-Laptop zu verbinden, wenn DHCP-zugewiesene IP-Adressen nicht verfügbar sind.
6	Vier Netzwerk-Ports am E5600SG Controller	10 GbE (optisch)	Verbinden Sie den E5600SG-Controller mit dem Grid-Netzwerk und (falls verwendet) mit dem Client-Netzwerk für StorageGRID. Die Ports können miteinander verbunden werden, um dem Controller redundante Pfade bereitzustellen.

Schritte

1. Verbinden Sie den E2700 Controller über die beiden SAS-Verbindungskabel mit dem E5600SG Controller.

Diesen Port verbinden…	Zu diesem Port…
SAS Interconnect Port 1 (gekennzeichnet mit CH 1) am E2700 Controller	SAS-Interconnect-Port 1 (mit CH 1 beschriftet) am E5600SG-Controller
SAS Interconnect Port 2 (mit CH 2 beschriftet) am E2700 Controller	SAS-Interconnect-Port 2 (mit CH 2 beschriftet) am E5600SG-Controller

Verwenden Sie den quadratischen Anschluss (Mini-SAS HD) für den E2700 Controller, und verwenden Sie den rechteckigen Anschluss (Mini-SAS) für den E5600SG Controller.

Stellen Sie sicher, dass sich die Zuglaschen an den SAS-Anschlüssen unten befinden und setzen Sie jeden Anschluss vorsichtig ein, bis er einrastet. Drücken Sie den Stecker nicht auf, wenn ein Widerstand besteht. Überprüfen Sie die Position der Zuglasche, bevor Sie fortfahren.

2. Verbinden Sie den E2700 Controller über ein Ethernet-Kabel mit dem Managementnetzwerk, in dem die SANtricity Storage Manager Software installiert ist.

Diesen Port verbinden…	Zu diesem Port…
Port 1 am E2700 Controller (der RJ-45 Port auf der linken Seite)	Switch-Port auf dem für SANtricity Storage Manager verwendeten Managementnetzwerk
Port 2 auf dem E2700 Controller	Service-Laptop, wenn nicht DHCP verwendet wird

3. Wenn Sie das Admin-Netzwerk für StorageGRID verwenden möchten, schließen Sie den E5600SG-Controller über ein Ethernet-Kabel an.

Diesen Port verbinden…	Zu diesem Port…
Port 1 am E5600SG-Controller (RJ-45-Port links)	Switch-Port am Admin-Netzwerk für StorageGRID
Port 2 am E5600SG-Controller	Service-Laptop, wenn nicht DHCP verwendet wird

4. Verbinden Sie die 10-GbE-Ports des E5600SG-Controllers mit den entsprechenden Netzwerk-Switches mit optischen Kabeln und SFP+-Transceivern.
   - 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

"Port Bond-Modi für die E5600SG Controller-Ports"

"Zugriff auf das Installationsprogramm der StorageGRID-Appliance"

Anschließen der Netzstromkabel (SG5600)

Sie müssen die Netzkabel an die externe Stromquelle und an den Netzanschluss an jedem Controller anschließen. Nachdem Sie die Netzkabel angeschlossen haben, können Sie das Netzkabel einschalten.

Was Sie benötigen

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.

Über diese Aufgabe

- Sie sollten für jedes Netzteil separate Stromquellen verwenden.

  Beim Anschluss an unabhängige Stromquellen bleibt die Stromredundanz erhalten.

- Sie können die mit dem Controller gelieferten Netzkabel mit typischen Steckdosen verwenden, die im Zielland verwendet werden, z. B. Wandsteckdosen mit einer unterbrechungsfreien Stromversorgung (USV).

  Diese Netzkabel sind jedoch nicht für die meisten EIA-konformen Cabinets geeignet.

Schritte

1. Schalten Sie die Netzschalter im Gehäuse oder Gehäuse aus.
2. Schalten Sie die Netzschalter an den Controllern aus.
3. Schließen Sie die primären Netzkabel des Cabinets an die externen Stromquellen an.
4. Schließen Sie die Stromkabel an den Netzanschluss an jedem Controller an.

Einschalten (SG5600)

Wenn das Gehäuse eingeschaltet wird, werden beide Controller mit Strom versorgt.

Schritte

1. Schalten Sie die beiden Netzteilschalter an der Rückseite des Gehäuses ein.

   Während der Strom eingeschaltet wird, leuchten die LEDs an den Controllern zeitweise auf und ab.

   Der Einschalprozess kann bis zu zehn Minuten dauern. Die Controller werden während der ersten Startsequenz mehrmals neu gestartet, sodass die Lüfter sich nach oben oder unten befinden und die LEDs blinken.

2. Überprüfen Sie die ein/aus-LED und die aktiven LEDs für den Host Link auf jedem Controller, um zu überprüfen, ob der Strom eingeschaltet wurde.
3. Warten Sie, bis alle Laufwerke eine dauerhaft grüne LED zeigen, die angibt, dass sie online sind.
4. Überprüfen Sie die grünen LEDs an der Vorder- und Rückseite des Gehäuses.

   Wenn gelbe LEDs angezeigt werden, notieren Sie sich die Positionen der LEDs.

5. Sehen Sie sich die sieben-Segment-Anzeige für den E5600SG-Controller an.

Dieses Display zeigt **HO**, gefolgt von einer sich wiederholenden Sequenz von zwei Ziffern.

```
HO -- IP address for Admin Network -- IP address for Grid Network HO
```

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.

Wenn eine IP-Adresse nicht über DHCP zugewiesen werden konnte, wird 0.0.0.0 angezeigt.

Anzeigen des Boot-Status und Überprüfen von Fehlercodes auf den SG5600-Controllern

Die sieben-Segment-Anzeige auf jedem Controller zeigt Status- und Fehlercodes an, wenn das Gerät eingeschaltet wird, während die Hardware initialisiert wird und wenn die Hardware ausfällt und die Initialisierung wieder aus der Zeit ist. Wenn Sie den Fortschritt oder die Fehlerbehebung überwachen, sollten Sie die Reihenfolge der Codes beobachten, wie sie angezeigt werden.

Über diese Aufgabe

Die Status- und Fehlercodes des E5600SG-Controllers entsprechen nicht den Status- und Fehlercodes des E2700 Controllers.

Schritte

1. Zeigen Sie während des Startvorgangs die Codes an, die auf den sieben Segment-Displays angezeigt werden, um den Fortschritt zu überwachen.
2. Informationen zum Überprüfen von Fehlercodes für den E5600SG-Controller finden Sie in den Anzeigestatus- und Fehlercodeinformationen für sieben Segmente.
3. Fehlercodes für den E2700 Controller werden in der E2700 Controller-Dokumentation auf der Support-Website geprüft.

Verwandte Informationen

"E5600SG-Controller-Anzeigecodes für sieben Segmente"

"NetApp Dokumentation: E2700 Serie"

E5600SG-Controller-Anzeigecodes für sieben Segmente

Die sieben-Segment-Anzeige auf dem E5600SG-Controller zeigt Status- und Fehlercodes an, während das Gerät eingeschaltet wird und die Hardware initialisiert wird. Sie können diese Codes verwenden, um den Status zu bestimmen und Fehler zu beheben.

Beim Überprüfen von Status- und Fehlercodes auf dem E5600SG-Controller sollten Sie sich die folgenden Codes ansehen:

- **Allgemeine Startcodes**

Stellt die standardmäßigen Startereignisse dar.

- **Normale Startcodes**

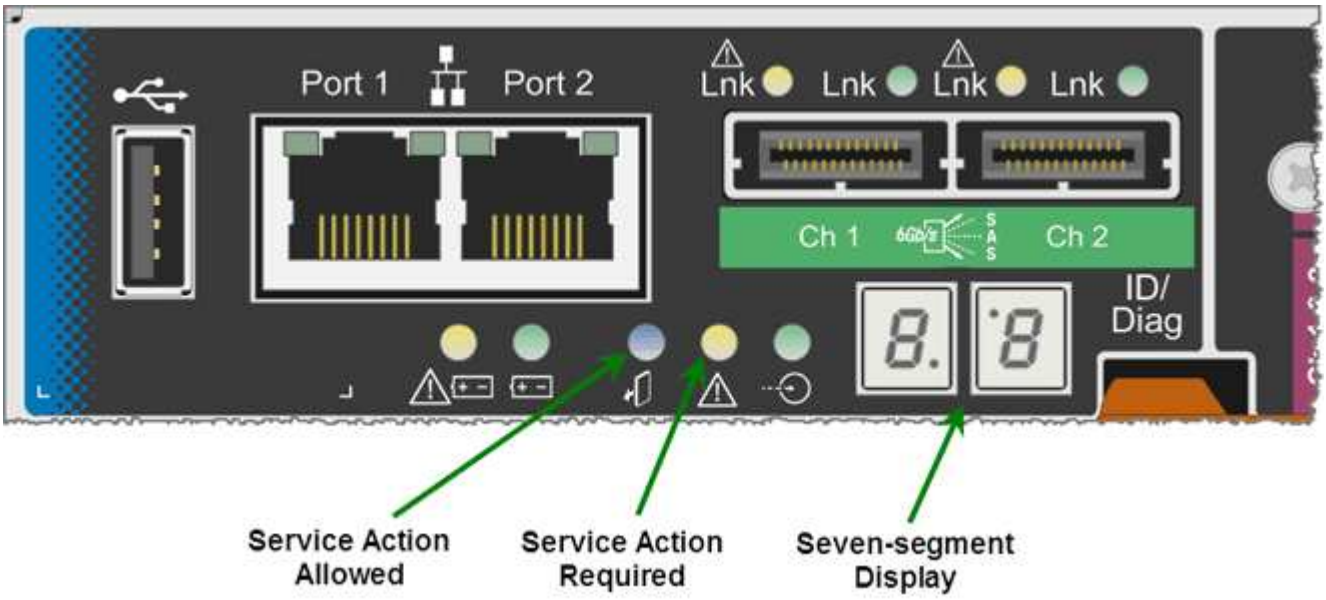
  Stellt die normalen Startereignisse dar, die im Gerät auftreten.

- **Fehlercodes**

  Zeigen Sie Probleme während der Startereignisse an.

StorageGRID steuert nur die folgenden LEDs am E5600SG-Controller und erst nach dem Start des StorageGRID-Appliance-Installationsprogramms:

- LED für Serviceaktion zulässig
- LED für Serviceaktion erforderlich
- Sieben-Segment-Anzeige



Die Dezimalstellen auf der Anzeige von sieben Segmenten werden von der StorageGRID Appliance nicht verwendet:

- Der obere Dezimalpunkt neben der am wenigsten signifikanten Ziffer ist die Diagnose-LED der Plattform.

  Diese Funktion wird während des Reset und der Erstkonfiguration der Hardware eingeschaltet. Andernfalls ist sie ausgeschaltet.

- Der untere Dezimalpunkt neben der wichtigsten Ziffer ist deaktiviert.

Um andere Probleme zu diagnostizieren, sollten Sie sich die folgenden Ressourcen ansehen:

- Weitere Informationen zu Hardware- und Umgebungsdiagnosen finden Sie in der Hardwarediagnose des Betriebssystems der E-Series.

  Dazu gehört die Suche nach Hardware-Problemen wie Stromversorgung, Temperatur und Festplattenlaufwerken. Die Appliance überwacht sämtliche Umgebungsstatus der Plattform auf das Betriebssystem E-Series.

- Um Firmware- und Treiberprobleme zu ermitteln, sehen Sie sich die Link-LEDs an der SAS-Seite und den Netzwerkports an.

  Weitere Informationen finden Sie in der Dokumentation zur E-Series E5600.

Allgemeine Startcodes

Während des Startvorgangs oder nach einem harten Reset der Hardware leuchten die LEDs für die Serviceaktion zulässig und für die Serviceaktion erforderliche LEDs auf, während die Hardware initialisiert wird. Das siebenSegment-Display zeigt eine Reihe von Codes an, die für E-Series Hardware identisch sind und nicht für den E5600SG Controller spezifisch sind.

Während des Startvorgangs steuert das Field Programmable Gate Array (FPGA) die Funktionen und die Initialisierung der Hardware.

Codieren	Anzeige
19	FPGA-Initialisierung
68	FPGA-Initialisierung
…	FPGA-Initialisierung.Dies ist eine schnelle Folge von Codes.
AA	Booten des Plattform-BIOS.
FF	BIOS-Hochfahren abgeschlossen.Dies ist ein Zwischenzustand, bevor der E5600SG-Controller die LEDs initialisiert und verwaltet, um den Status anzuzeigen.

Nachdem die AA- und FF-Codes angezeigt wurden, werden entweder die normalen Startcodes angezeigt oder es werden Fehlercodes angezeigt. Außerdem sind die LEDs für zulässige Serviceaktion und Serviceaktion erforderlich deaktiviert.

Normale Startcodes

Diese Codes stellen die normalen Startereignisse dar, die in chronologischer Reihenfolge im Gerät auftreten.

Codieren	Anzeige
HI	Das Master-Boot-Skript wurde gestartet.
PP	Die FPGA-Plattform-Firmware wird auf Updates überprüft.
HP	Die Host Interface Card (HIC) wird auf Updates überprüft.

Codieren	Anzeige
RB	Nach Firmware-Updates wird das System ggf. neu gebootet.
FP	Die Firmware-Update-Prüfungen wurden abgeschlossen. Starten des Prozesses (utmagent) für die Kommunikation mit dem E2700 Controller und das Management. Dieser Prozess erleichtert die Appliance-Bereitstellung.
ER	Das System synchronisiert sich mit dem Betriebssystem E-Series.
HZ	Die StorageGRID-Installation wird überprüft.
HO	Installationsmanagement und aktive Schnittstelle finden statt.
HOCHVERFÜGBARKEIT	Das Linux-Betriebssystem und die StorageGRID werden ausgeführt.

E5600SG-Controller-Fehlercodes

Diese Codes stellen Fehlerbedingungen dar, die beim Booten des Geräts auf dem E5600SG-Controller angezeigt werden können. 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	Anzeige
22	Kein Master-Boot-Datensatz auf einem Boot-Gerät gefunden.
23	Kein SATA-Laufwerk installiert.
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.

Codieren	Anzeige
92 bis 96	PCI-Bus-Initialisierung
A0 bis A3	SATA-Laufwerk-Initialisierung
AB	Alternativer Startcode:
AE	Booten von OS:
EA	DDR3-Training fehlgeschlagen.
E8	Kein Speicher installiert.
EU	Das Installationsskript wurde nicht gefunden.
EP	Der „ManageSGA“-Code zeigt an, dass die vorGrid-Kommunikation mit dem E2700 Controller fehlgeschlagen ist.

Verwandte Informationen

"Fehlerbehebung bei der Hardwareinstallation"

"NetApp Support"

Konfigurieren der Hardware

Nachdem Sie das Gerät mit Strom versorgt haben, müssen Sie SANtricity Storage Manager konfigurieren. Dies ist die Software, mit der Sie die Hardware überwachen. Sie müssen auch die Netzwerkverbindungen konfigurieren, die von StorageGRID verwendet werden.

Schritte

- "Konfigurieren von StorageGRID-Verbindungen"
- "SANtricity Storage Manager wird konfiguriert"
- "Optional: Aktivieren der Node-Verschlüsselung"
- "Optional: Wechseln in den RAID-6-Modus (nur SG5660)"
- "Optional: Neu zuordnen von Netzwerkports für die Appliance"

Konfigurieren von StorageGRID-Verbindungen

Bevor Sie eine StorageGRID Appliance als Storage Node in einem StorageGRID-Grid bereitstellen können, müssen Sie die Verbindungen zwischen der Appliance und den zu verwendenden Netzwerken konfigurieren. Sie können das Netzwerk konfigurieren, indem Sie im StorageGRID Appliance Installer navigieren, der im E5600SG Controller (dem Computing-Controller in der Appliance) enthalten ist.

Schritte

- "Zugriff auf das Installationsprogramm der StorageGRID-Appliance"
- "Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance"
- "Konfigurieren von Netzwerkverbindungen (SG5600)"
- "Einstellen der IP-Konfiguration"
- "Netzwerkverbindungen werden überprüft"
- "Überprüfen von Netzwerkverbindungen auf Portebene"

Zugriff auf das Installationsprogramm der StorageGRID-Appliance

Sie müssen auf das Installationsprogramm der StorageGRID Appliance zugreifen, um die Verbindungen zwischen der Appliance und den drei StorageGRID-Netzwerken zu konfigurieren: Das Grid-Netzwerk, das Admin-Netzwerk (optional) und das Client-Netzwerk (optional).

Was Sie benötigen

- Sie verwenden einen unterstützten Webbrowser.
- Die Appliance ist mit allen von Ihnen geplanten StorageGRID-Netzwerken verbunden.
- In diesen Netzwerken kennen Sie die IP-Adresse, das Gateway und das Subnetz für die Appliance.
- Sie haben die geplanten Netzwerk-Switches konfiguriert.

Über diese Aufgabe

Wenn Sie zum ersten Mal auf das Installationsprogramm der StorageGRID-Appliance zugreifen, können Sie die vom DHCP zugewiesene IP-Adresse für das Admin-Netzwerk verwenden (vorausgesetzt, die Appliance ist mit dem Admin-Netzwerk verbunden) oder die durch DHCP zugewiesene IP-Adresse für das Grid-Netzwerk. Die Verwendung der IP-Adresse für das Admin-Netzwerk ist vorzuziehen. Wenn Sie andernfalls über die DHCP-Adresse für das Grid-Netzwerk auf das Installationsprogramm von StorageGRID-Appliances zugreifen, kann die Verbindung zum StorageGRID-Appliance-Installationsprogramm verloren gehen, wenn Sie die Link-Einstellungen ändern und wenn Sie eine statische IP eingeben.

Schritte

1. Beziehen Sie die DHCP-Adresse für das Gerät im Admin-Netzwerk (wenn es verbunden ist) oder das Grid-Netzwerk (wenn das Admin-Netzwerk nicht verbunden ist).

   Sie können eine der folgenden Aktionen ausführen:

   - Geben Sie dem Netzwerkadministrator die MAC-Adresse für den Management-Port 1 an, damit er die DHCP-Adresse für diesen Port im Admin-Netzwerk nachsehen kann. Die MAC-Adresse wird auf einem Etikett am E5600SG-Controller neben dem Port gedruckt.
   - Sehen Sie sich die Sieben-Segment-Anzeige auf dem E5600SG-Controller an. Wenn Management-Port 1 und 10-GbE-Ports 2 und 4 des E5600SG-Controllers 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 E5600SG-Controllers zugewiesen.
- Der zweite Zahlensatz ist die DHCP-Adresse für den Appliance-Speicherknoten im Grid-Netzwerk. Diese IP-Adresse wird 10-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.

2. Wenn Sie eine der DHCP-Adressen abrufen konnten:

   a. Öffnen Sie einen Webbrowser auf dem Service-Laptop.

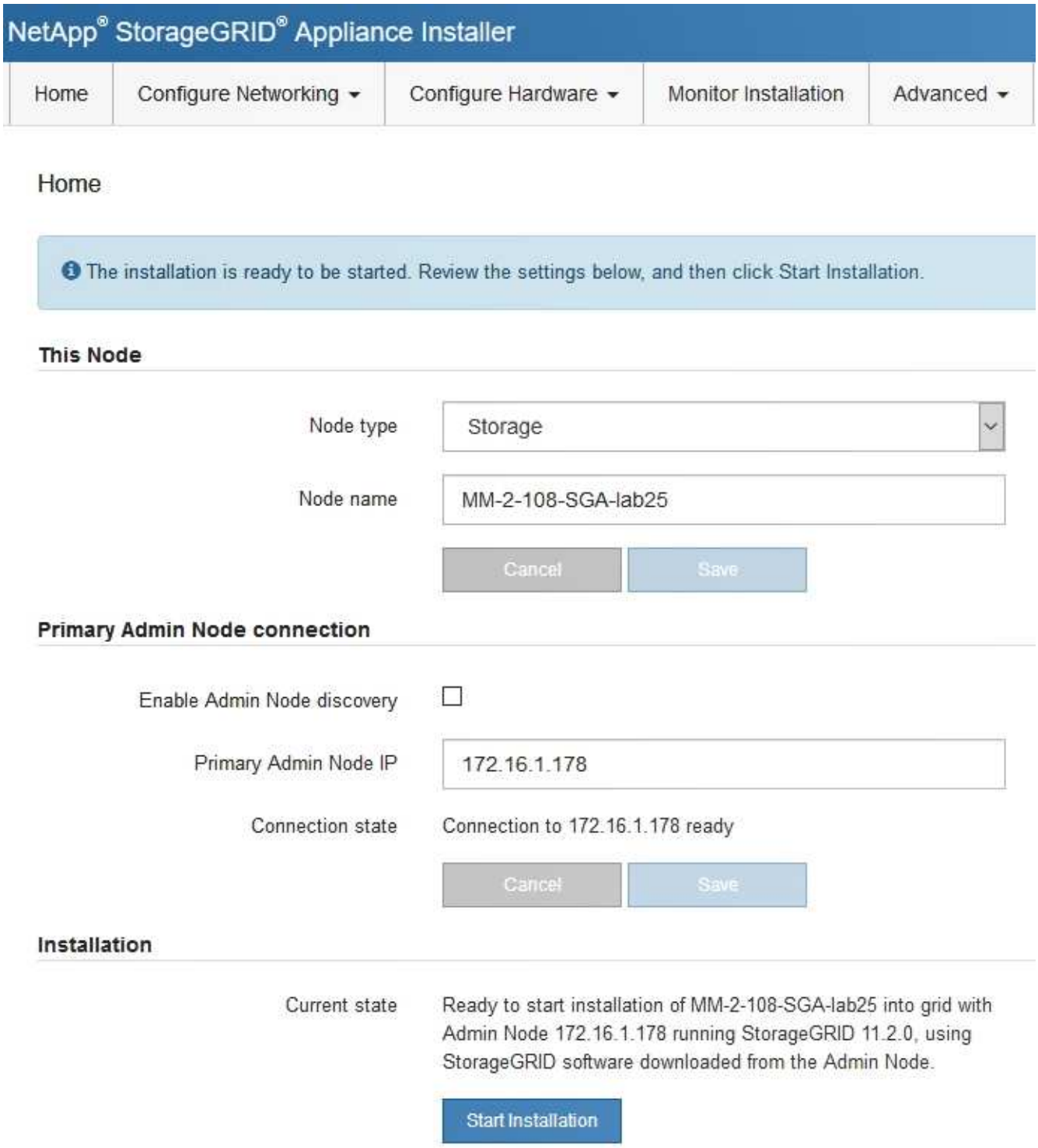
   b. Geben Sie diese URL für das StorageGRID-Appliance-Installationsprogramm ein:
   `https://E5600SG_Controller_IP:8443`

   Für *`E5600SG_Controller_IP`*, Verwenden Sie die DHCP-Adresse für den Controller. (Verwenden Sie die IP-Adresse für das Admin-Netzwerk, wenn Sie ihn haben).

   c. 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.



3. Wenn der E5600SG-Controller keine IP-Adresse über DHCP erhalten konnte:

   a. Schließen Sie den Service-Laptop über ein Ethernet-Kabel an den Management-Port 2 des E5600SG-Controllers an.

b. Öffnen Sie einen Webbrowser auf dem Service-Laptop.

c. 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 das Gerät aktuell verbunden ist.

> Wenn Sie über eine lokale Verbindung nicht auf die Startseite zugreifen können, konfigurieren Sie die Service-Laptop-IP-Adresse als `169.254.0.2`, Und versuchen Sie es erneut.

4. Überprüfen Sie alle Meldungen, die auf der Startseite angezeigt werden, und konfigurieren Sie die Verbindungskonfiguration und die IP-Konfiguration nach Bedarf.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

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.

Was Sie benötigen

Sie haben auf das Installationsprogramm für StorageGRID-Geräte zugegriffen.

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 das StorageGRID-Appliance-Installationsprogramm 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 im Grid Manager **Hilfe** > **Info**).

   Die zweite Ziffer in den beiden Versionen sollte übereinstimmen. Wenn auf Ihrem StorageGRID-System beispielsweise die Version 11.**5**.*x*.*y* ausgeführt wird, sollte die StorageGRID Appliance Installer-Version 3.**5**

.*z* sein.

3. Wenn die Appliance über eine übergeordnete Version des Installationsprogramms für StorageGRID Appliances verfügt, wechseln Sie zur Seite NetApp Downloads für StorageGRID.

   "NetApp Downloads: StorageGRID"

   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 Datei Support für StorageGRID Appliances ist eine `.zip` Archiv, das die aktuellen und vorherigen Firmware-Versionen für alle StorageGRID Appliance-Modelle enthält, in Unterverzeichnissen für jeden Controller-Typ.

   Nach dem Herunterladen der Datei Support für StorageGRID Appliances extrahieren Sie den `.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 des Installationsprogramms für StorageGRID-Geräte, um die folgenden Schritte auszuführen:
   a. Laden Sie die entsprechende Support-Datei (Firmware-Image) für den Controller-Typ und die Prüfsummendatei hoch.
   b. Aktualisieren Sie die inaktive Partition.
   c. Starten Sie neu und tauschen Sie die Partitionen aus.
   d. Aktualisieren Sie die zweite Partition.

Verwandte Informationen

"Zugriff auf das Installationsprogramm der StorageGRID-Appliance"

Konfigurieren von Netzwerkverbindungen (SG5600)

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.

Was Sie benötigen

Wenn Sie den aggregierten Port Bond-Modus, den LACP Network Bond-Modus oder VLAN-Tagging verwenden möchten:

- Sie haben die 10-GbE-Ports an der Appliance an Switches angeschlossen, 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

Diese Abbildung zeigt, wie die vier 10-GbE-Ports im Bond-Modus mit festen Ports verbunden sind (Standardkonfiguration).

	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.

Diese Abbildung zeigt, wie die vier 10-GbE-Ports im Bond-Modus für aggregierte Ports verbunden sind.

	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-GbE-Ports zusammengefasst. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standardeinstellung verwenden möchten.

- **Festes (Standard) Port Bond-Modus**

Netzwerk-Bond-Modus	**Client-Netzwerk deaktiviert (Standard)**	**Client-Netzwerk aktiviert**
Active-Backup (Standard)	• 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.	• 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)	• 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.	• 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.

- * Aggregat-Port-Bond-Modus*

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad	• Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. • Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete.	• 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.

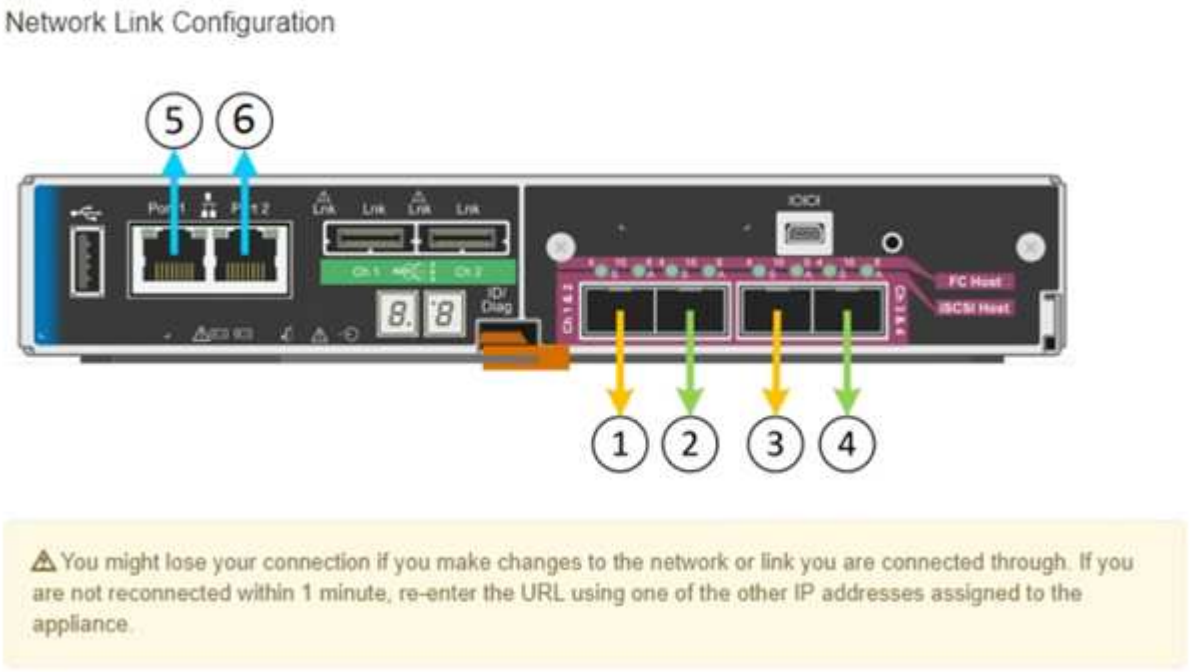
Weitere Informationen zu Port Bond- und Netzwerk-Bond-Modi finden Sie unter „`10-GbE-Port-Verbindungen für den E5600SG Controller`“.

Diese Abbildung zeigt, wie die zwei 1-GbE-Management-Ports des E5600SG-Controllers im Active-Backup-Netzwerk-Bond-Modus des Admin-Netzwerks verbunden sind.

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.



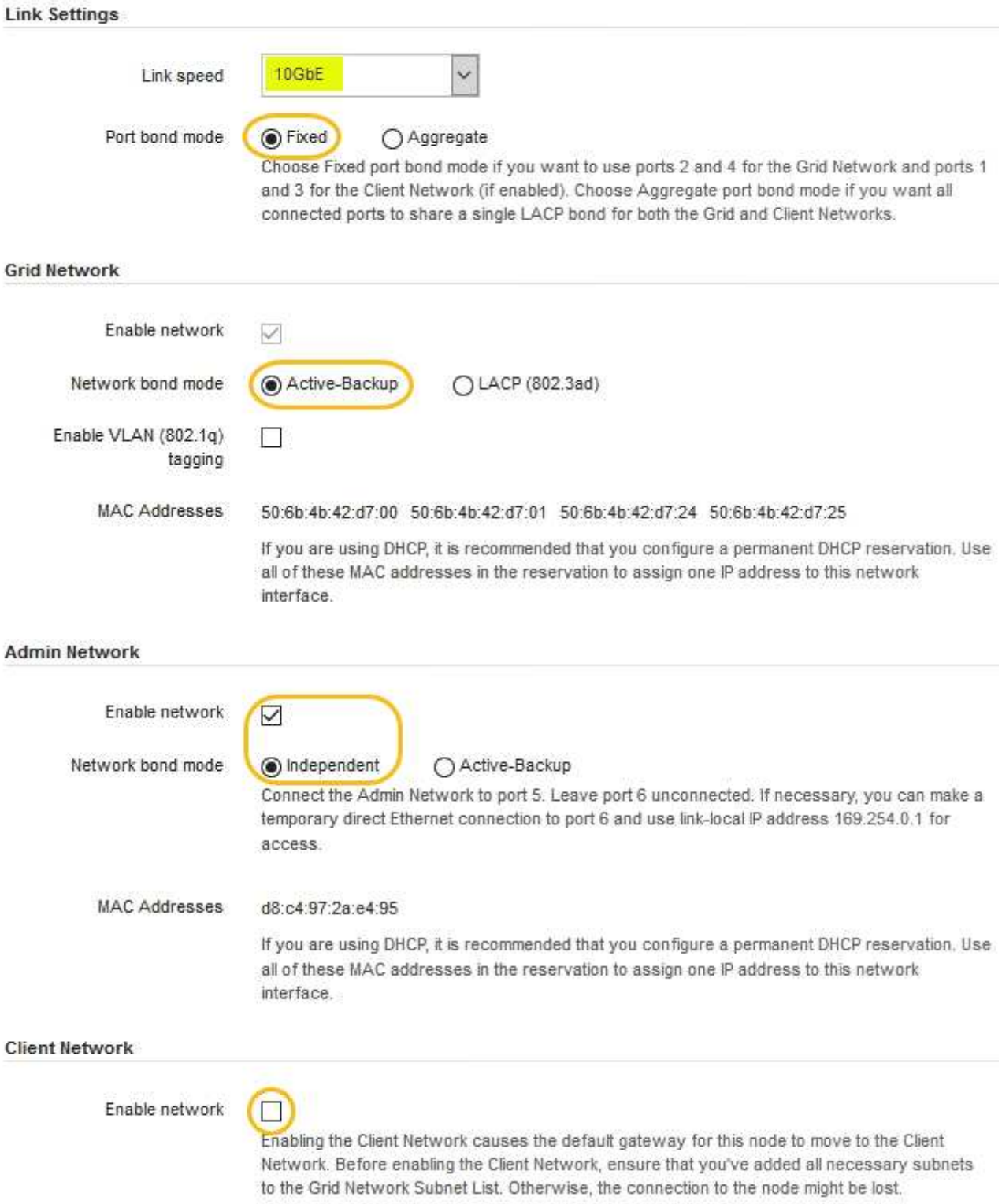
In der Tabelle „Link-Status“ werden der Verbindungsstatus (nach oben/unten) und die Geschwindigkeit (1/10/25/40/100 Gbit/s) der nummerierten Ports aufgeführt.

Link Status

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

Das erste Mal, wenn Sie diese Seite aufrufen:

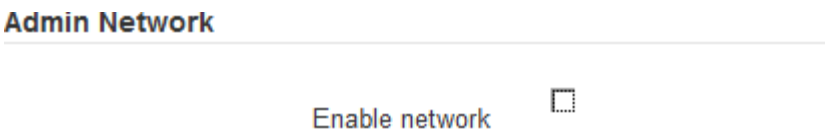
- **Link Speed** ist auf **10GbE** eingestellt. Dies ist die einzige Verbindungsgeschwindigkeit, die für den E5600SG Controller verfügbar ist.
- **Port Bond Modus** ist auf **fest** eingestellt.
- **Network Bond-Modus** für das Grid-Netzwerk ist auf **Active-Backup** eingestellt.
- Das **Admin-Netzwerk** ist aktiviert, und der Netzwerk-Bond-Modus ist auf **unabhängig** eingestellt.
- Das **Client-Netzwerk** ist deaktiviert.



2. Aktivieren oder deaktivieren Sie die StorageGRID-Netzwerke, die Sie verwenden möchten.

   Das Grid-Netzwerk ist erforderlich. Sie können dieses Netzwerk nicht deaktivieren.

   a. Wenn das Gerät nicht mit dem Admin-Netzwerk verbunden ist, deaktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Admin-Netzwerk.



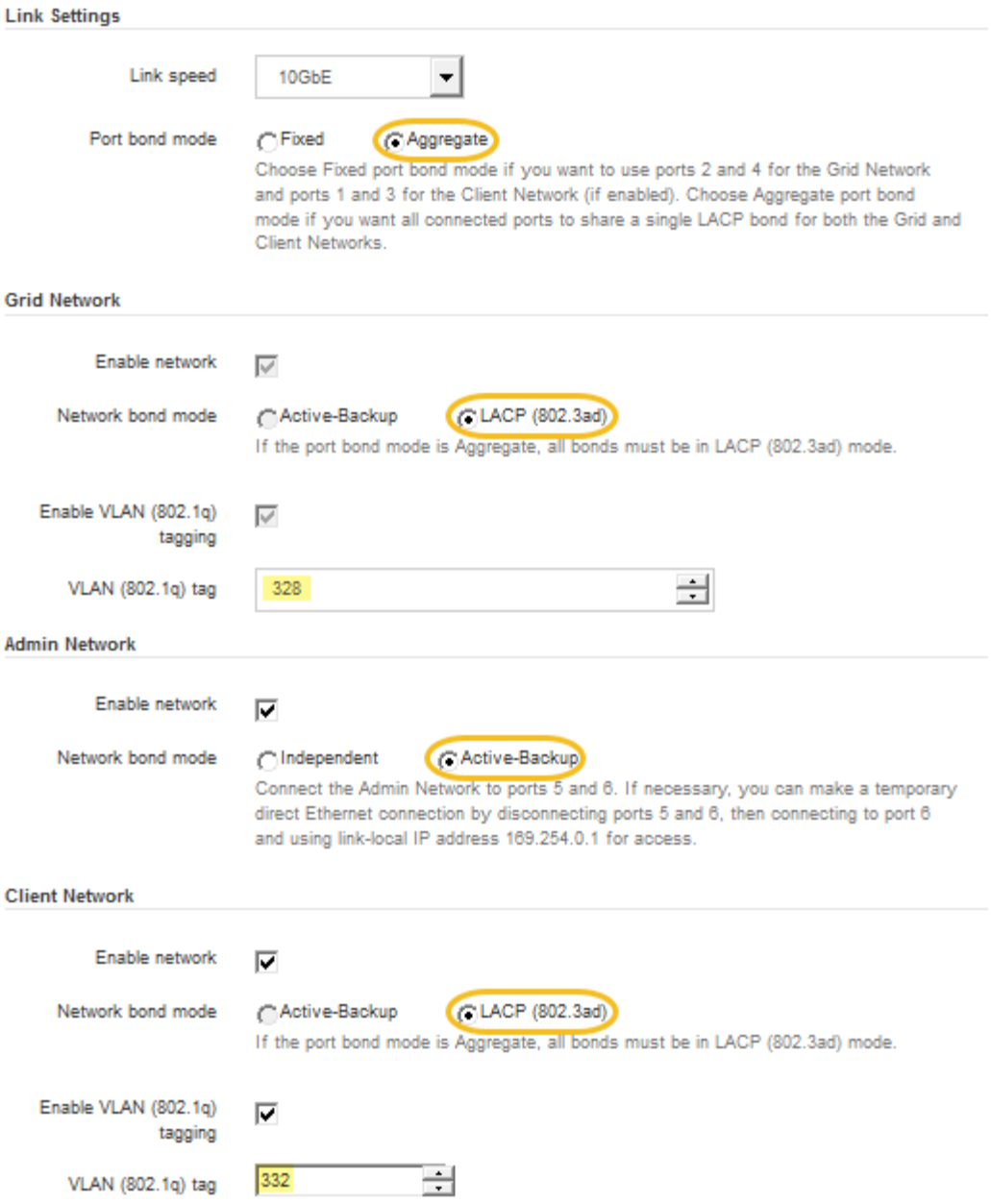
b. Wenn das Gerät mit dem Client-Netzwerk verbunden ist, aktivieren Sie das Kontrollkästchen **Netzwerk aktivieren** für das Client-Netzwerk.

   Die Client-Netzwerk-Einstellungen für die 10-GbE-Ports werden nun angezeigt.

3. In der Tabelle finden Sie Informationen zum Konfigurieren des Port-Bond-Modus und des Netzwerk-Bond-Modus.

   Das 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.



4. 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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:
> **`https://E5600SG_Controller_IP:8443`**

Verwandte Informationen

"Port Bond-Modi für die E5600SG Controller-Ports"

Einstellen der IP-Konfiguration

Mit dem Installationsprogramm der StorageGRID-Appliance können Sie die für den

Appliance-Speicherknoten verwendeten IP-Adressen und Routing-Informationen im StorageGRID-Raster, Administrator und Client-Netzwerke konfigurieren.

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.

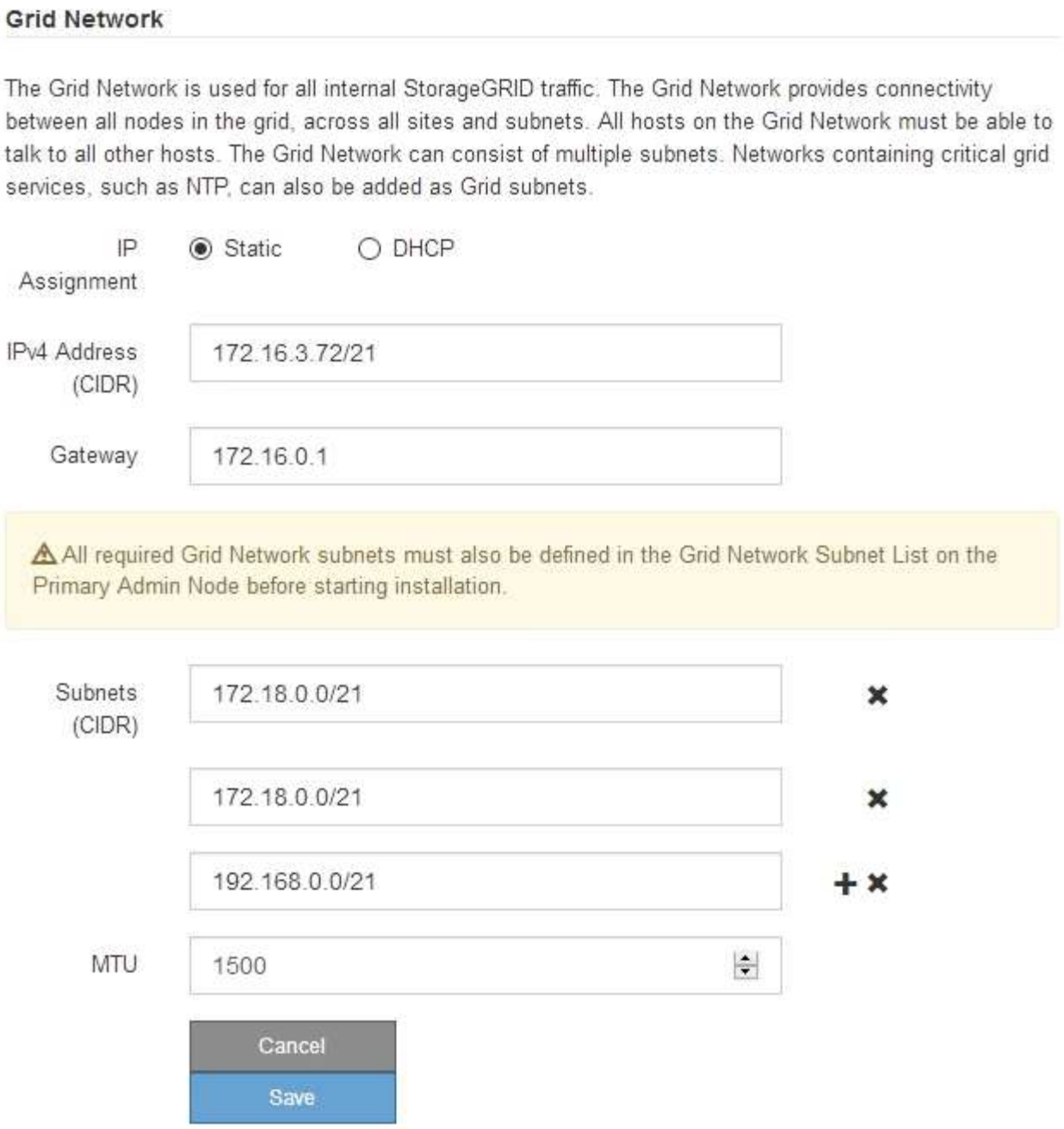
Wenn Sie die Link-Konfiguration ändern möchten, lesen Sie die Anweisungen zum Ändern der Link-Konfiguration des E5600SG-Controllers.

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 identisch 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://services_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 Löschsymbol ✖.

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.

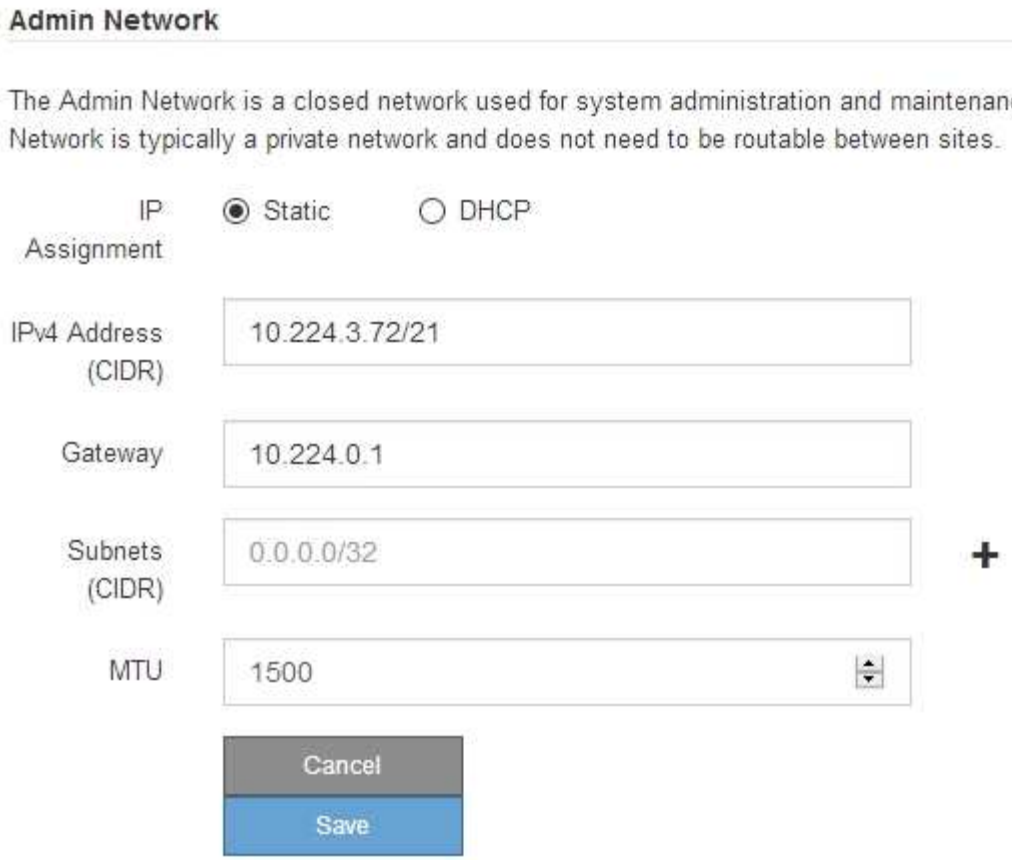
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch 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, müssen Sie das Admin-Netzwerk auf der Seite Link Configuration aktivieren.



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://services_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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

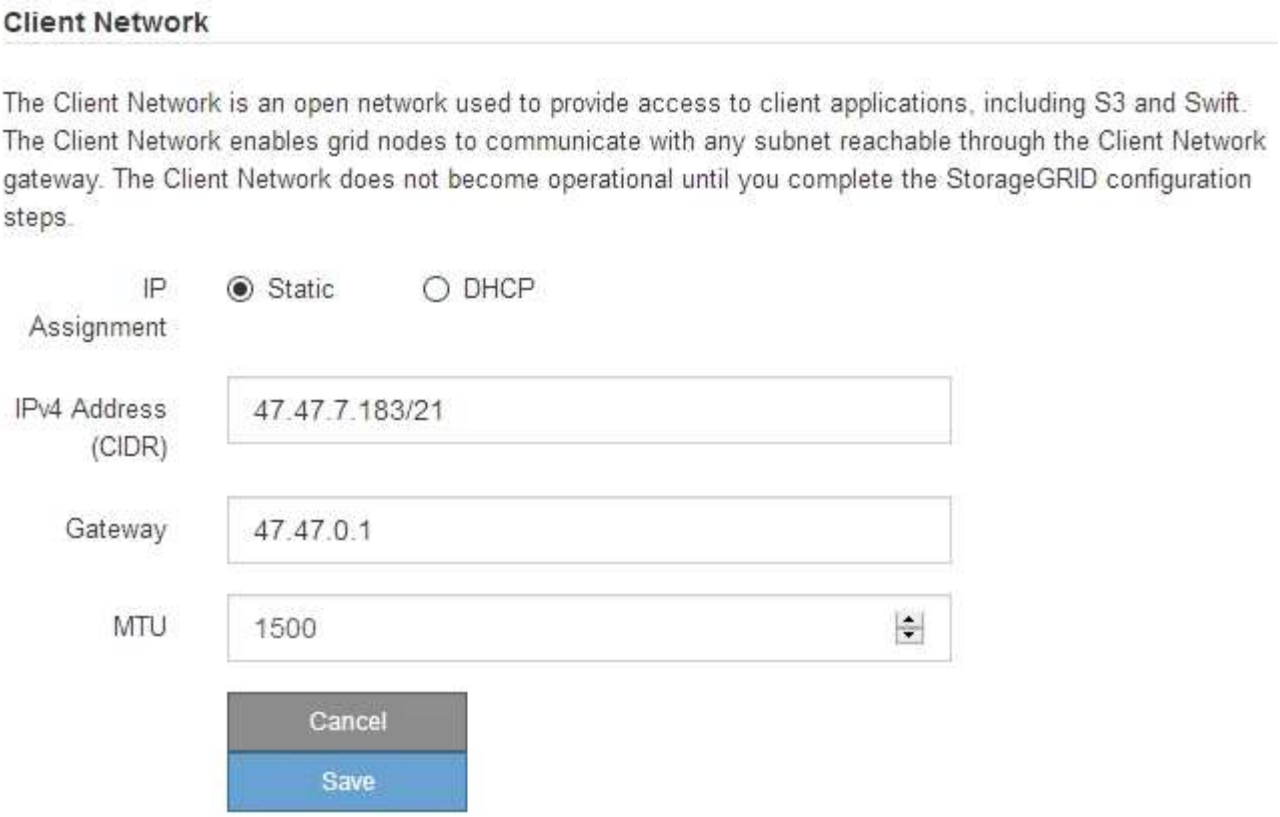
c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.

> 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, müssen Sie das Client-Netzwerk auf der Seite Link Configuration aktivieren.



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.

Verwandte Informationen

"Ändern der Link-Konfiguration des E5600SG-Controllers"

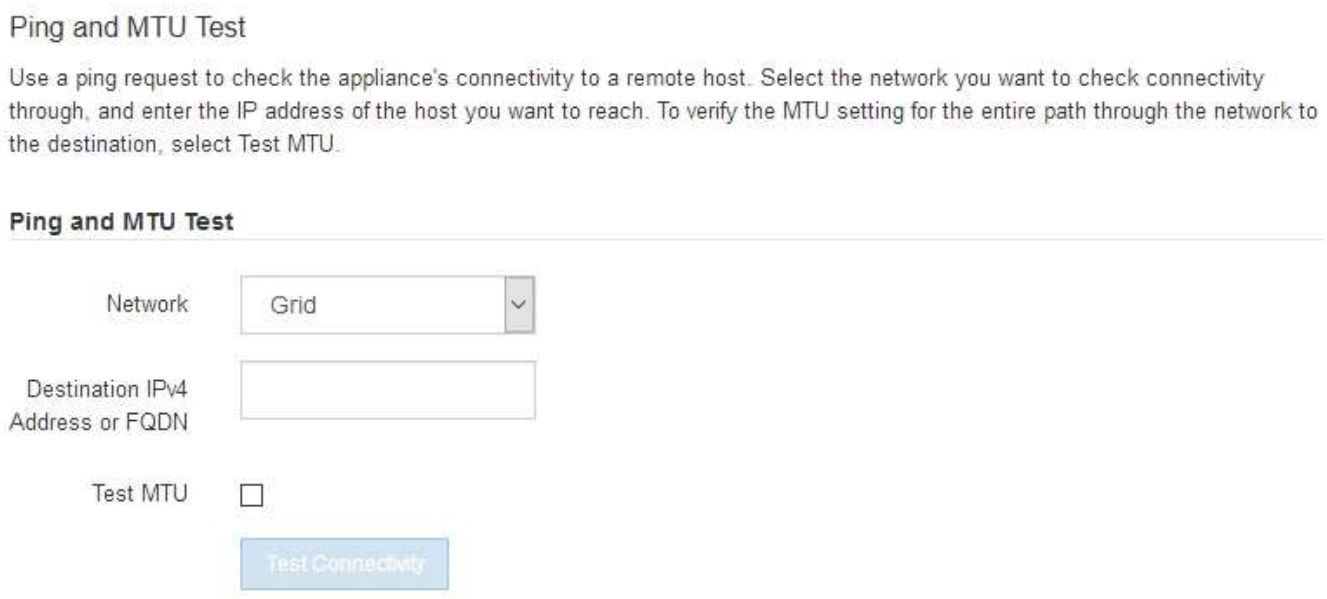
Netzwerkverbindungen werden überprüft

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.



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 Domänennamen (FQDN) für einen Host in diesem Netzwerk ein.

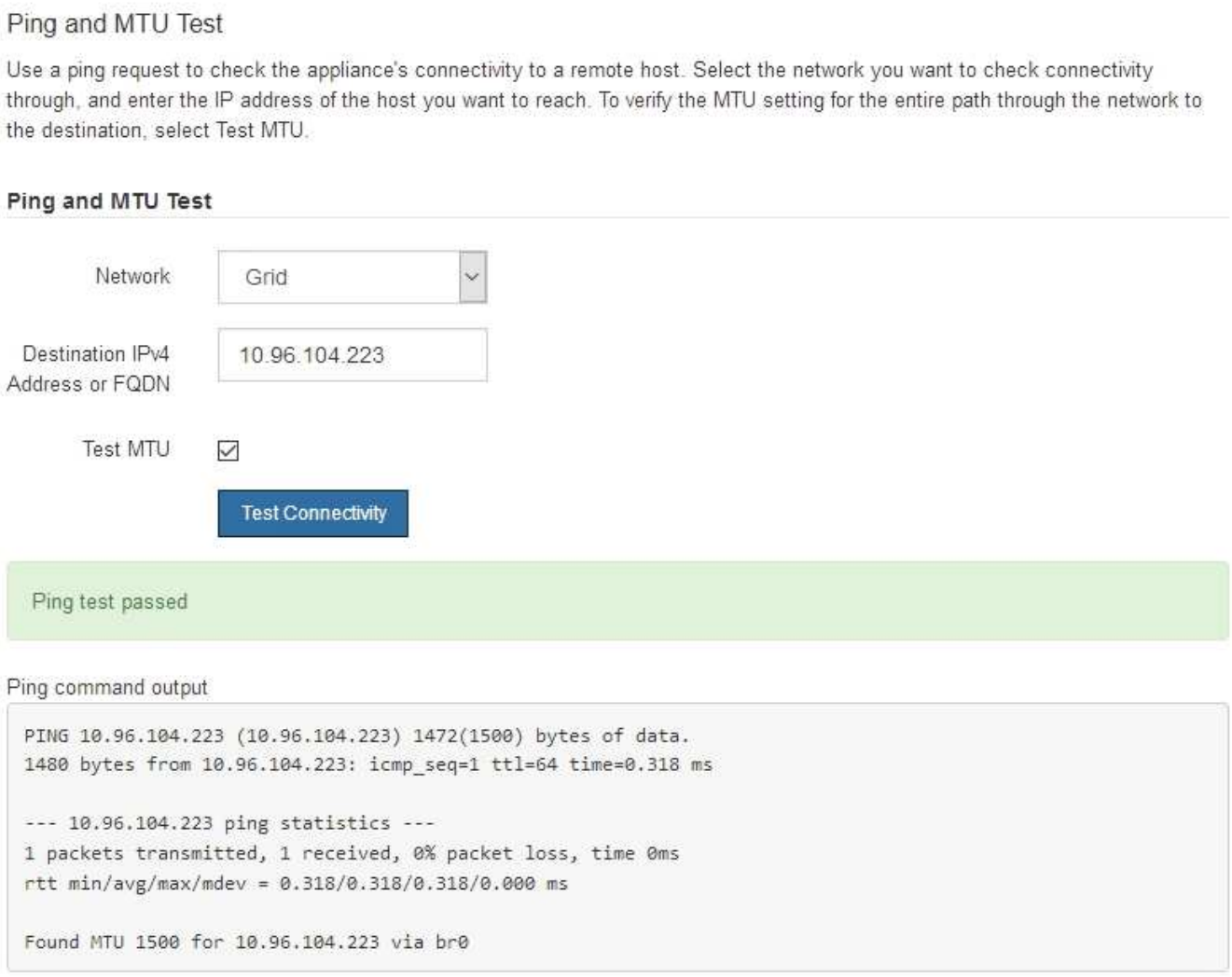
   Beispielsweise möchten Sie das Gateway im Netzwerk oder den primären Admin-Node pingen.

4. Aktivieren Sie optional das Kontrollkästchen **MTU-Test**, 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.



Verwandte Informationen

"Konfigurieren von Netzwerkverbindungen (SG5600)"

"Ändern der MTU-Einstellung"

Überprüfen von 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 unter der Portreferenz in den Netzwerkrichtlinien von StorageGRID.

> Die in der Tabelle für die Portkonnektivität aufgeführten Grid-Netzwerkports sind nur für StorageGRID Version 11.5 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.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

   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.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

Port Connectivity Test

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

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.

- Wenn für einen oder mehrere ausgewählte Ports keine Netzwerkverbindung auf Portebene hergestellt werden kann, wird die Meldung „`Verbindungstest 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.

Verwandte Informationen

"Netzwerkrichtlinien"

SANtricity Storage Manager wird konfiguriert

Mit SANtricity Storage Manager lässt sich der Status der Storage-Festplatten und Hardwarekomponenten Ihrer StorageGRID Appliance überwachen. Um auf diese Software zuzugreifen, müssen Sie die IP-Adresse des Managementports 1 auf dem E2700 Controller (der Storage Controller in der Appliance) kennen.

Schritte

- "Festlegen der IP-Adresse für den E2700 Controller"
- "Hinzufügen der Appliance zum SANtricity Storage Manager"
- "Einrichten von SANtricity-Storage-Manager"

Festlegen der IP-Adresse für den E2700 Controller

Management Port 1 auf dem E2700 Controller verbindet die Appliance mit dem Managementnetzwerk für SANtricity Storage Manager. Sie müssen eine statische IP-Adresse für den E2700 Controller festlegen, um sicherzustellen, dass die Verbindung zwischen Management und Hardware und der Controller-Firmware in der StorageGRID Appliance nicht unterbrochen wird.

Was Sie benötigen

Sie verwenden einen unterstützten Webbrowser.

Über diese Aufgabe

DHCP-zugewiesene Adressen können sich jederzeit ändern. Weisen Sie dem Controller eine statische IP-Adresse zu, um einen konsistenten Zugriff zu gewährleisten.

Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:
   `https://E5600SG_Controller_IP:8443`

   Für *`E5600SG_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-Konfiguration** > **Storage Controller-Netzwerkkonfiguration**.

   Die Seite Speichercontroller-Netzwerkkonfiguration wird angezeigt.

3. Wählen Sie je nach Netzwerkkonfiguration **aktiviert** für IPv4, IPv6 oder beides.
4. 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.

5. Legen Sie optional eine statische IP-Adresse für den E2700 Controller-Management-Port fest.

> Sie sollten entweder eine statische IP für den Management-Port 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.

   d. Klicken Sie Auf **Speichern**.

      Es kann einige Minuten dauern, bis Ihre Änderungen angewendet werden.

Wenn Sie eine Verbindung zu SANtricity Storage Manager herstellen, verwenden Sie die neue statische IP-Adresse als URL:
`https://E2700_Controller_IP`

Verwandte Informationen

"NetApp Dokumentation: SANtricity Storage Manager"

Hinzufügen der Appliance zum SANtricity Storage Manager

Der E2700 Controller in der Appliance wird mit dem SANtricity Storage Manager verbunden und dann die Appliance als Storage-Array hinzugefügt.

Was Sie benötigen

Sie verwenden einen unterstützten Webbrowser.

Über diese Aufgabe

Ausführliche Anweisungen finden Sie in der Dokumentation zum SANtricity-Storage-Manager.

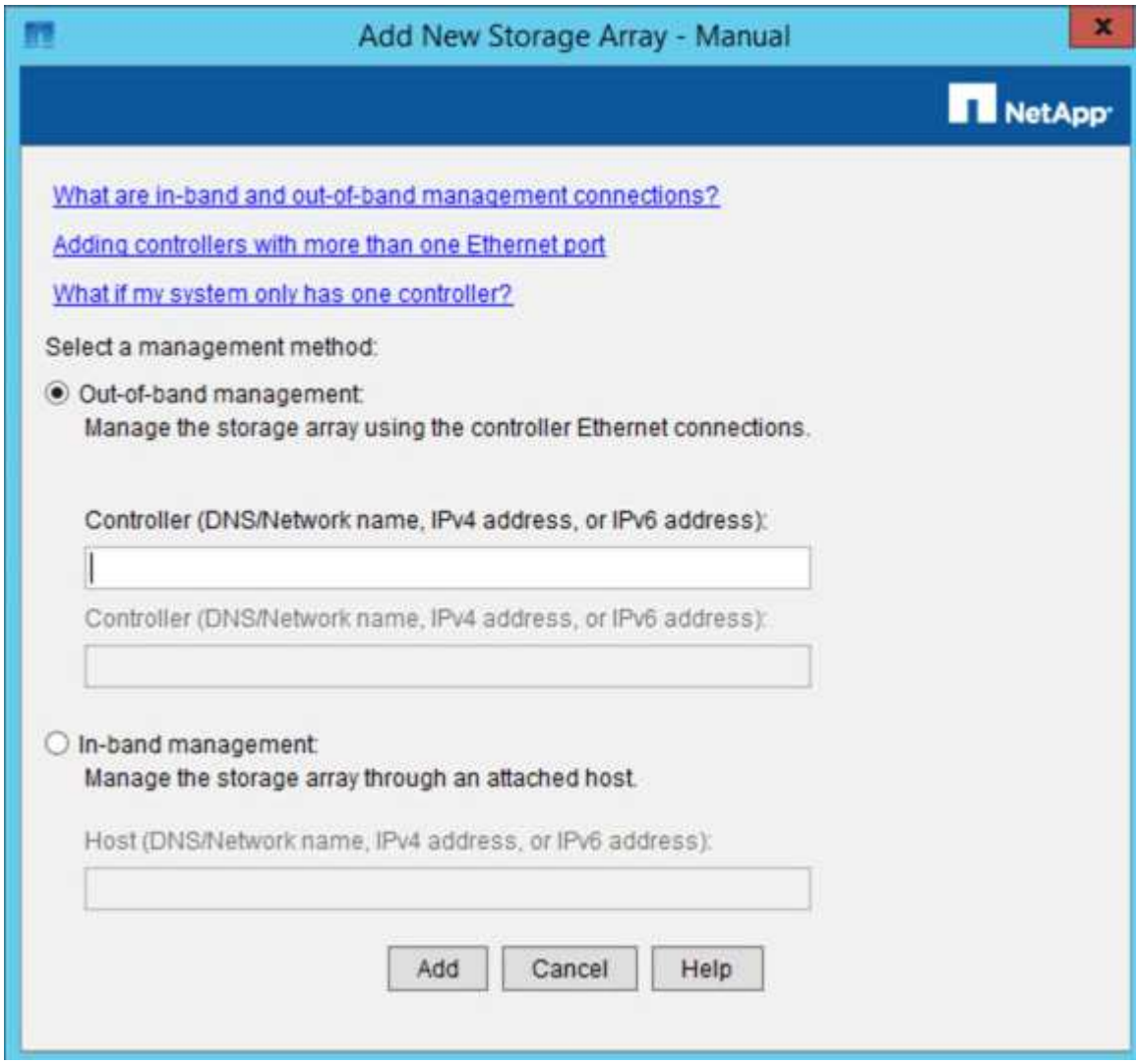
Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse als URL für SANtricity-Speichermanager ein:
`https://E2700_Controller_IP`

Die Anmeldeseite für den SANtricity-Storage-Manager wird angezeigt.

2. Wählen Sie auf der Seite **Zuschlagsmethode auswählen** die Option **manuell** und klicken Sie auf **OK**.
3. Wählen Sie **Bearbeiten** > **Speicher-Array Hinzufügen**.

   Die Seite Neues Speicher-Array hinzufügen - Manual wird angezeigt.



4. Geben Sie im Feld **Out-of-Band Management** einen der folgenden Werte ein:
   - **Mittels DHCP:** die vom DHCP Server zugewiesene IP-Adresse zum Management-Port 1 am E2700 Controller
   - **Nicht mit DHCP:** `192.168.128.101`

   > Nur einer der Controller der Appliance ist mit dem SANtricity Storage Manager verbunden. Sie müssen also nur eine IP-Adresse eingeben.

5. Klicken Sie Auf **Hinzufügen**.

Verwandte Informationen

"NetApp Dokumentation: SANtricity Storage Manager"

Nach dem Zugriff auf den SANtricity Storage Manager können Sie damit Hardwareeinstellungen konfigurieren. In der Regel konfigurieren Sie diese Einstellungen, bevor Sie die Appliance als Speicherknoten in einem StorageGRID-System bereitstellen.

Schritte

- "AutoSupport wird konfiguriert"
- "Empfang von AutoSupport wird überprüft"
- "Konfigurieren von E-Mail- und SNMP-Trap-Warnungsbenachrichtigungen"
- "Festlegen von Passwörtern für SANtricity Storage Manager"

AutoSupport wird konfiguriert

Das AutoSupport Tool erfasst Daten in einem Kunden-Support-Bundle von der Appliance und sendet die Daten automatisch an den technischen Support. Konfigurieren von AutoSupport unterstützt den technischen Support durch Remote-Fehlerbehebung und Problemanalyse.

Was Sie benötigen

- Die AutoSupport-Funktion muss auf der Appliance aktiviert sein.

  Die AutoSupport-Funktion wird global auf einer Storage Management Station aktiviert und deaktiviert.

- Der Storage Manager-Ereignismonitor muss auf mindestens einem Gerät mit Zugang zum Gerät und vorzugsweise auf maximal einer Maschine ausgeführt werden.

Über diese Aufgabe

Alle Daten werden an dem von Ihnen angegebenen Speicherort in ein einziges komprimiertes Archivdateiformat (.7z) komprimiert.

AutoSupport bietet die folgenden Meldungsarten:

Nachrichtentypen	Beschreibung
Ereignismeldungen	• Wird gesendet, wenn ein Supportereignis auf der verwalteten Appliance auftritt • Nehmen Sie Informationen zur Systemkonfiguration und Diagnose mit auf
Tägliche Nachrichten	• Wird einmal täglich während eines vom Benutzer konfigurierbaren Zeitintervalls in der lokalen Zeit der Appliance gesendet • Berücksichtigen Sie die aktuellen Systemereignisprotokolle und Performance-Daten

Nachrichtentypen	Beschreibung
Wöchentliche Nachrichten	• Wird einmal wöchentlich während eines vom Benutzer konfigurierbaren Zeitintervalls in der lokalen Zeit der Appliance gesendet • Konfigurations- und Informationen für den Systemstatus einschließen

Schritte

1. Wählen Sie im Fenster Enterprise Management im SANtricity Storage Manager die Registerkarte **Geräte** aus, und wählen Sie dann **erkannte Speicherarrays** aus.
2. Wählen Sie **Extras** > **AutoSupport** > **Konfiguration**.
3. Verwenden Sie die Online-Hilfe des SANtricity Storage Managers, falls erforderlich, um die Aufgabe abzuschließen.

Verwandte Informationen

"NetApp Dokumentation: SANtricity Storage Manager"

Empfang von AutoSupport wird überprüft

Sie sollten überprüfen, ob der technische Support Ihre AutoSupport Meldungen erhält. Den Status von AutoSupport für Ihre Systeme finden Sie im Active IQ Portal. Durch die Überprüfung des Eingangs dieser Nachrichten wird sichergestellt, dass der technische Support Ihre Informationen enthält, wenn Sie Hilfe benötigen.

Über diese Aufgabe

AutoSupport kann einen der folgenden Status anzeigen:

- **EIN**

  Ein „EIN“-Status gibt an, dass der technische Support derzeit AutoSupport Meldungen vom System empfängt.

- **AUS**

  Ein „OFF“-Status empfiehlt, dass Sie AutoSupport deaktiviert haben, da der technische Support in den letzten 15 Kalendertagen kein wöchentliches Protokoll vom System erhalten hat, oder es gab möglicherweise eine Änderung in Ihrer Umgebung oder Konfiguration (z. B.).

- **RÜCKGANG**

  SIE haben den technischen Support benachrichtigt, dass Sie AutoSupport nicht aktivieren.

Nachdem der technische Support ein wöchentliches Protokoll aus dem System erhält, ändert sich der AutoSupport-Status in EIN.

Schritte

1. Wechseln Sie zur NetApp Support Site unter "mysupport.netapp.com", Und melden Sie sich im Active IQ Portal.
2. Wenn DER AutoSupport-Status NICHT AKTIVIERT ist und Sie der Meinung sind, dass er falsch ist, führen

Sie Folgendes aus:

a. Überprüfen Sie die Systemkonfiguration, um sicherzustellen, dass AutoSupport aktiviert ist.

b. Überprüfen Sie Ihre Netzwerkumgebung und -Konfiguration, um sicherzustellen, dass das System Meldungen an den technischen Support senden kann.

Konfigurieren von E-Mail- und SNMP-Trap-Warnungsbenachrichtigungen

Der SANtricity Storage Manager kann Sie benachrichtigen, wenn sich der Status der Appliance oder einer der Komponenten ändert. Dies wird als Alarmbenachrichtigung bezeichnet. Sie können Warnbenachrichtigungen durch zwei verschiedene Methoden erhalten: E-Mail und SNMP-Traps. Sie müssen die Benachrichtigungen konfigurieren, die Sie empfangen möchten.

Schritte

1. Wählen Sie im Fenster Enterprise Management im SANtricity Storage Manager die Registerkarte **Devices** aus, und wählen Sie dann einen Knoten aus.
2. Wählen Sie **Bearbeiten** > **Alarme Konfigurieren**.
3. Wählen Sie die Registerkarte **E-Mail**, um E-Mail-Benachrichtigungen zu konfigurieren.
4. Wählen Sie die Registerkarte **SNMP** aus, um SNMP-Trap-Warnungsbenachrichtigungen zu konfigurieren.
5. Verwenden Sie die Online-Hilfe des SANtricity Storage Managers, falls erforderlich, um die Aufgabe abzuschließen.

Festlegen von Passwörtern für SANtricity Storage Manager

Sie können die Passwörter festlegen, die für die Appliance in SANtricity Storage Manager verwendet werden. Durch das Festlegen von Passwörtern wird die Systemsicherheit gewahrt.

Schritte

1. Doppelklicken Sie im Enterprise Management-Fenster in SANtricity Storage Manager auf den Controller.
2. Wählen Sie im Array Management-Fenster das Menü **Storage Array** aus, und wählen Sie **Sicherheit** > **Passwort festlegen**.
3. Konfigurieren Sie die Passwörter.
4. Verwenden Sie die Online-Hilfe des SANtricity Storage Managers, falls erforderlich, um die Aufgabe abzuschließen.

Optional: Aktivieren der Node-Verschlüsselung

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. Bei der Installation der Appliance müssen Sie die Node-Verschlüsselung auswählen und aktivieren. Die Auswahl der Node-Verschlüsselung kann nicht rückgängig gemacht werden, sobald der KMS-Verschlüsselungsprozess gestartet wird.

Was Sie benötigen

Lesen Sie die Informationen über KMS in den Anweisungen zur Administration von StorageGRID durch.

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.

> Alle Daten, die vor einer Appliance mit aktivierter Node-Verschlüsselung vorhanden sind, werden mit einem nichtsicheren temporären Schlüssel verschlüsselt. Das Gerät ist erst dann vor dem Entfernen oder Diebstahl geschützt, wenn der Schlüssel auf einen vom KMS angegebenen Wert gesetzt wird.

Ohne den KMS-Schlüssel, der zur Entschlüsselung der Festplatte benötigt wird, können die Daten auf der Appliance nicht abgerufen und effektiv verloren gehen. 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

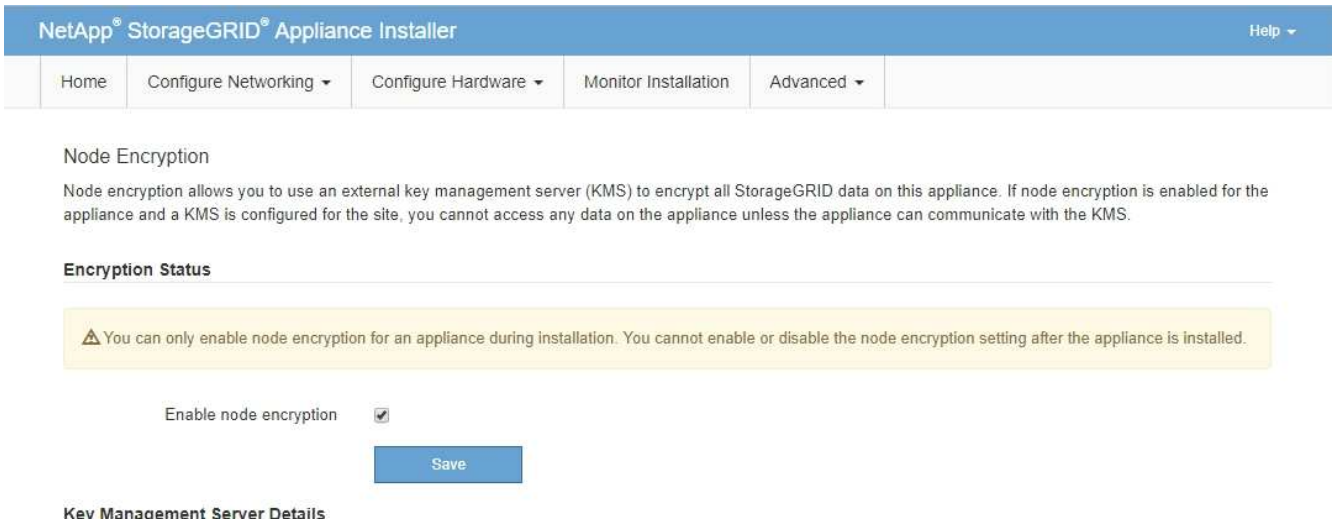
1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.
   `https://Controller_IP:8443`

   `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 Appliance-Festplatten nicht entschlüsselt werden, ohne dabei den gleichen KMS-Schlüssel zu verwenden.

2. Wählen Sie **Hardware Konfigurieren** > **Node Encryption**.



3. Wählen Sie **Node-Verschlüsselung aktivieren**.

   Sie können die Auswahl **Enable Node Encryption** ohne Gefahr eines Datenverlusts aufheben, bis Sie **Save** auswählen und der Appliance Node auf die KMS-Verschlüsselungsschlüssel in Ihrem StorageGRID-System zugreift und mit der Festplattenverschlüsselung beginnt. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht deaktivieren.

   > Nachdem Sie einer StorageGRID Site mit KMS eine Appliance hinzugefügt haben, für die die Node-Verschlüsselung aktiviert ist, kann die KMS-Verschlüsselung für den Node nicht angehalten werden.

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.

Verwandte Informationen

"StorageGRID verwalten"

"Monitoring der Node-Verschlüsselung im Wartungsmodus"

Optional: Wechseln in den RAID-6-Modus (nur SG5660)

Wenn Sie eine SG5660 mit 60 Laufwerken besitzen, können Sie die Volume-Konfiguration von der standardmäßigen und empfohlenen Einstellung Dynamic Disk Pools (DDP) auf RAID 6 ändern. Sie können den Modus nur ändern, bevor Sie den Speicherknoten der StorageGRID-Appliance bereitstellen.

Was Sie benötigen

- Sie haben eine SG5660. Die SG5612 unterstützt RAID6 nicht. Sollten Sie über eine SG5612 verfügen, müssen Sie den DDP-Modus nutzen.

> 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.

Über diese Aufgabe

Vor der Bereitstellung eines StorageGRID Appliance Storage Node können Sie zwischen zwei Optionen zur Volume-Konfiguration wählen:

- **Dynamic Disk Pools (DDP)** — Dies ist die Standardeinstellung und empfohlene Einstellung. DDP ist ein verbessertes Hardware-Datensicherungsschema, das über eine bessere Systemperformance, kürzere Wiederherstellungszeiten nach Laufwerksausfällen und ein vereinfachtes Management verfügt.
- **RAID 6** — Dies ist ein Hardware-Schutzschema, das auf jeder Festplatte Paritäts-Stripes verwendet und vor dem Verlust von Daten zwei Festplattenausfälle im RAID-Satz zulässt.

> Die Verwendung von RAID 6 wird für die meisten StorageGRID Umgebungen nicht empfohlen. Zwar kann RAID-6 die Storage-Effizienz auf bis zu 88 % steigern (im Vergleich zu 80 % bei DDP), doch bietet der DDP-Modus eine effizientere Recovery nach Laufwerksausfällen.

Schritte

1. Öffnen Sie mithilfe des Service-Laptops einen Webbrowser, und greifen Sie auf das Installationsprogramm der StorageGRID-Appliance: + zu
   `https://E5600SG_Controller_IP:8443`

   Wo *`E5600SG_Controller_IP`* Ist eine der IP-Adressen für den E5600SG-Controller.

2. Wählen Sie in der Menüleiste **Erweitert** > **RAID-Modus**.
3. Wählen Sie auf der Seite **RAID-Modus konfigurieren** aus der Dropdown-Liste Modus die Option **RAID 6** aus.
4. Klicken Sie Auf **Speichern**.

Optional: Neu zuordnen von Netzwerkports für die Appliance

Möglicherweise müssen Sie die internen Ports auf dem Appliance Storage Node zu verschiedenen externen Ports neu zuordnen. Aufgrund eines Firewall-Problems müssen Sie möglicherweise Ports neu zuordnen.

Was Sie benötigen

- Sie haben zuvor auf das Installationsprogramm für StorageGRID-Geräte zugegriffen.
- Sie sind nicht konfiguriert und planen keine Konfiguration von Load Balancer-Endpunkten.

> Wenn Sie Ports neu zuordnen, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Wenn Sie Load Balancer-Endpunkte konfigurieren und bereits neu zugeordnete Ports haben möchten, befolgen Sie die Schritte in den Recovery- und Wartungsanweisungen zum Entfernen von Port-Remaps.

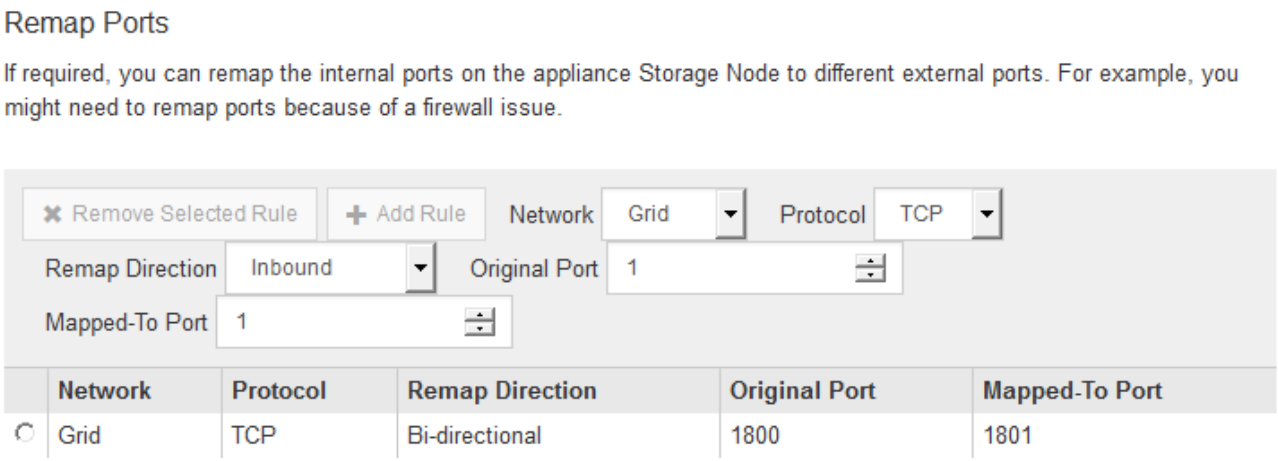
Schritte

1. Klicken Sie in der Menüleiste des Installationsprogramms für StorageGRID-Geräte auf **Netzwerke konfigurieren** > **Ports für die Erinnerung**.

   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. Klicken Sie Auf **Regel Hinzufügen**.

   Die neue Port-Zuordnung wird der Tabelle hinzugefügt, und die erneute Zuordnung wird sofort wirksam.



8. Um eine Portzuordnung zu entfernen, aktivieren Sie das Optionsfeld für die Regel, die Sie entfernen möchten, und klicken Sie auf **Ausgewählte Regel entfernen**.

Verwandte Informationen

"Verwalten Sie erholen"

Implementieren eines Appliance-Storage-Node

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.

Was Sie benötigen

- Wenn Sie einen Appliance-Node klonen, fahren Sie den Recovery- und Wartungsvorgang fort.

  "Verwalten Sie erholen"

- 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.

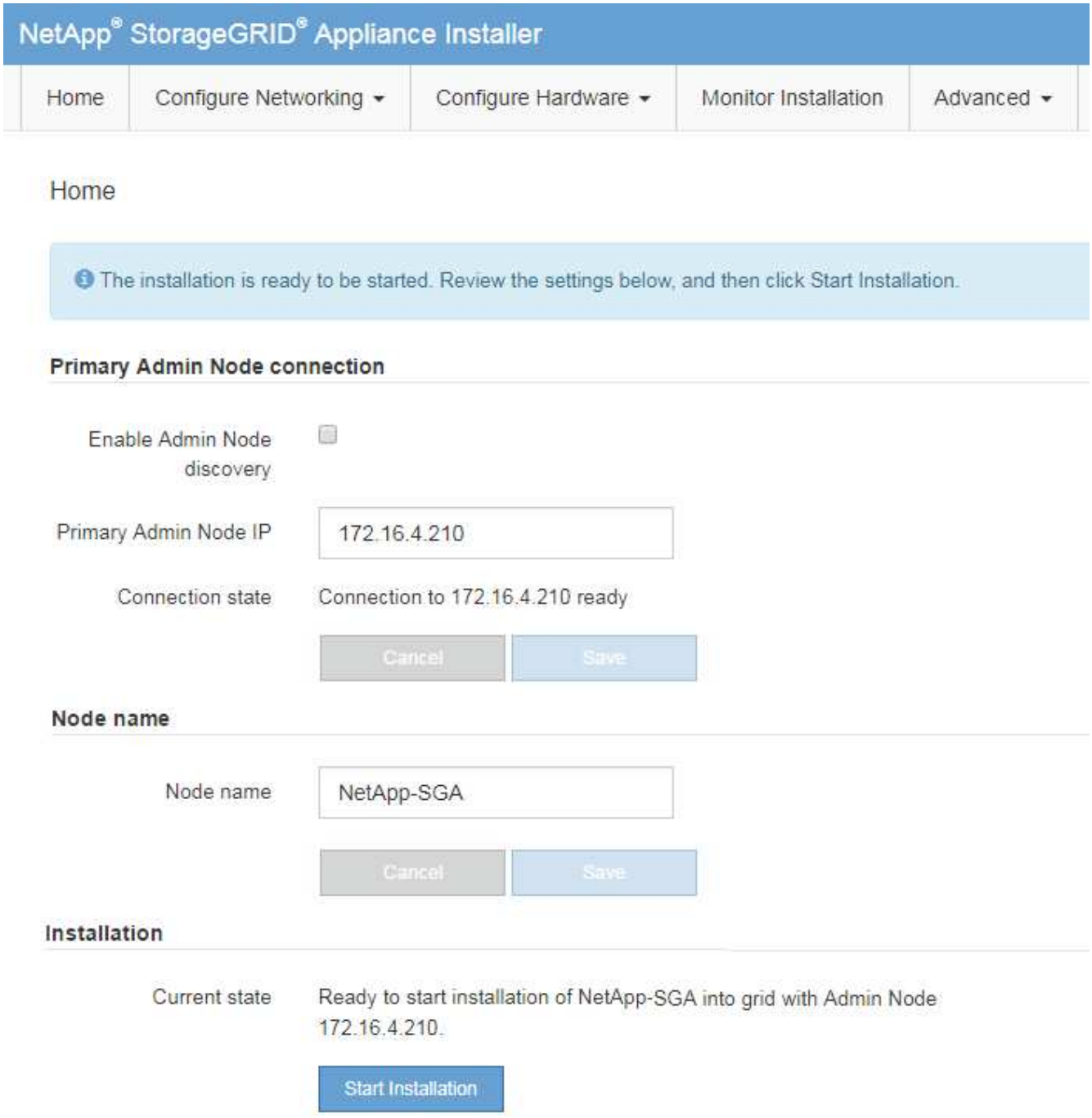
> Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisieren `configure-sga.py` Installationsskript für Geräte.

- Wenn Sie eine Erweiterung oder Wiederherstellung durchführen, befolgen Sie die entsprechenden Anweisungen:
  - Informationen zum Hinzufügen eines Appliance-Speicherknoten zu einem vorhandenen StorageGRID-System finden Sie in den Anweisungen zum erweitern eines StorageGRID-Systems.
  - Informationen zum Bereitstellen eines Appliance Storage Node im Rahmen eines Wiederherstellungsvorgangs finden Sie in den Anweisungen für Recovery und Wartung.

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	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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 klicken Sie auf **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. 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 Installations- und Wartungsanleitung für Ihr Gerät.

   > Wenn Sie die Storage Node Appliance als Ziel für das Klonen eines Node implementieren, beenden Sie den Implementierungsprozess hier und setzen Sie das Klonverfahren für den Node bei Recovery und Wartung fort.

   "Verwalten Sie erholen"

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 automatisieren `configure-sga.py` Installationsskript für die Appliance Dieses Skript gilt nur für Speicherknoten.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

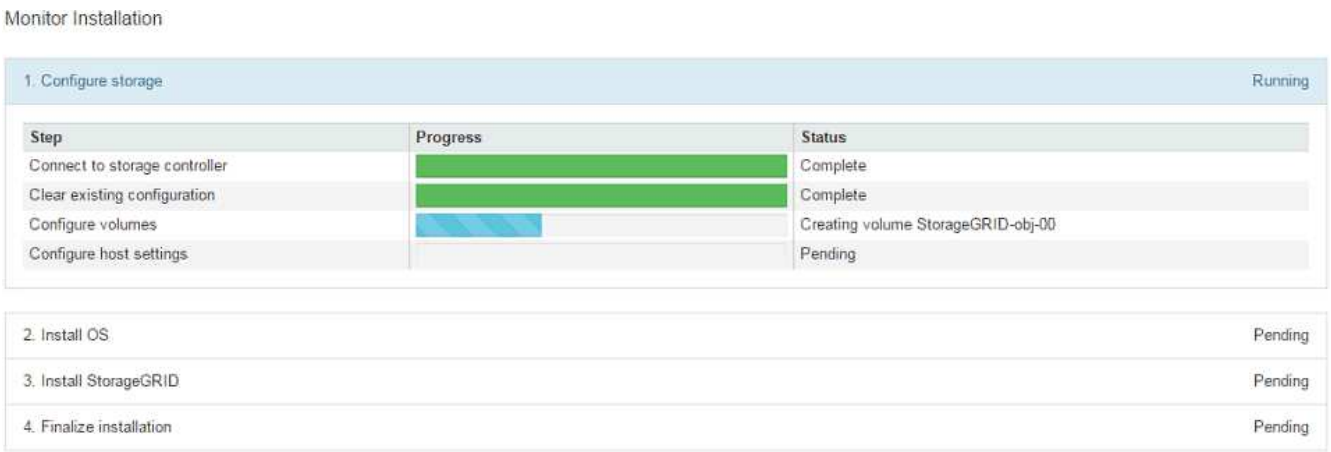
Monitoring der Installation der Speicher-Appliance

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 auf **Installation überwachen**.

   Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.



   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 „`Skipped.`“ angezeigt.

2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

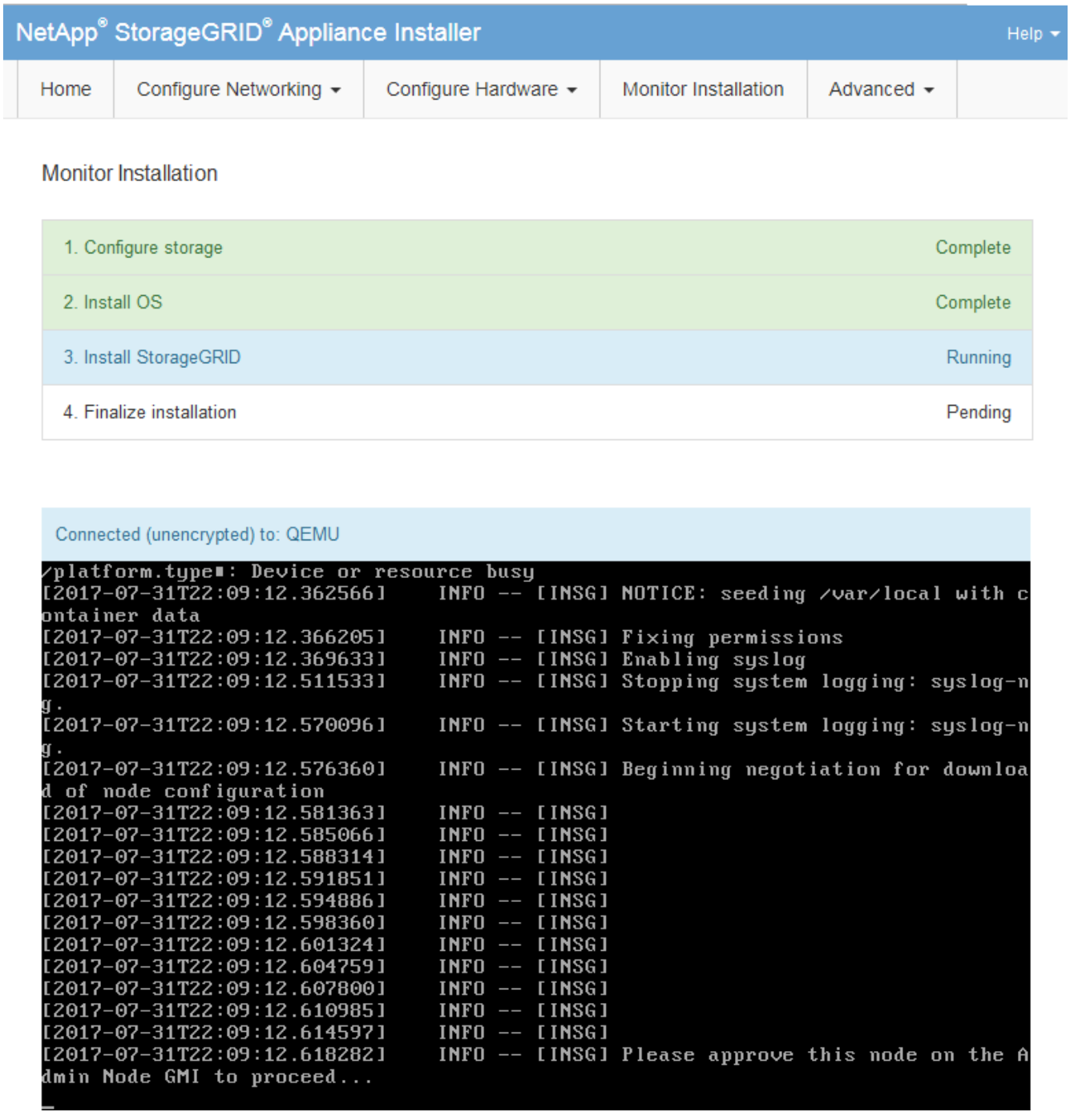
   1. Speicher konfigurieren

   In dieser Phase stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.

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.



4. Wechseln Sie zum Grid Manager, genehmigen Sie den ausstehenden Storage-Node und führen Sie den StorageGRID-Installationsprozess aus.

   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.

Automatisierung der Installation und Konfiguration von Appliances

Sie können die Installation und Konfiguration Ihrer Appliances und die Konfiguration des gesamten StorageGRID Systems automatisieren.

Über diese Aufgabe

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

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

- Erstellen Sie eine JSON-Datei, in der die Konfigurationseinstellungen für Ihre Appliances angegeben sind. Laden Sie die JSON-Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

  Sie können dieselbe Datei verwenden, um mehr als ein Gerät zu konfigurieren.

- Verwenden Sie die StorageGRID`configure-sga.py` Python-Skript zur Automatisierung der Konfiguration Ihrer Appliances.
- Zusätzliche Python-Skripte verwenden, um andere Komponenten des gesamten StorageGRID-Systems (das „Grid“) zu konfigurieren.

  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. Weitere Informationen zum Herunterladen und Extrahieren der StorageGRID-Installationsdateien finden Sie in den Anweisungen zum Wiederherstellen und Verwalten.

Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer

Sie können die Konfiguration einer Appliance mithilfe einer JSON-Datei mit den Konfigurationsinformationen automatisieren. Sie laden die Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

Was Sie benötigen

- Ihr Gerät muss mit der neuesten Firmware ausgestattet sein, die mit StorageGRID 11.5 oder höher kompatibel ist.
- Sie müssen mit dem Installationsprogramm für StorageGRID-Geräte auf der Appliance verbunden sein, die Sie mit einem unterstützten Browser konfigurieren.

Über diese Aufgabe

Sie können Appliance-Konfigurationsaufgaben automatisieren, z. B. die Konfiguration folgender Komponenten:

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

- Netzwerk-Bond-Modus
- Verbindungsgeschwindigkeit

Die Konfiguration Ihrer Appliance mit einer hochgeladenen JSON-Datei ist häufig effizienter als die manuelle Ausführung der Konfiguration mit mehreren Seiten im StorageGRID-Appliance-Installationsprogramm, insbesondere wenn Sie viele Knoten konfigurieren müssen. Sie müssen die Konfigurationsdatei für jeden Knoten einzeln anwenden.

Erfahrene Benutzer, die sowohl die Installation als auch die Konfiguration ihrer Appliances automatisieren möchten, können das verwenden `configure-sga.py` Skript: +"Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

Schritte

1. Generieren Sie die JSON-Datei mit einer der folgenden Methoden:
   - Die ConfigBuilder-Anwendung

     "ConfigBuilder.netapp.com"

   - Der `configure-sga.py` Konfigurationsskript für die Appliance Sie können das Skript vom Installationsprogramm für StorageGRID-Geräte herunterladen (**Hilfe** > **Konfigurationsskript für Geräte**). Lesen Sie die Anweisungen zur Automatisierung der Konfiguration mit dem Skript configure-sga.py.

     "Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

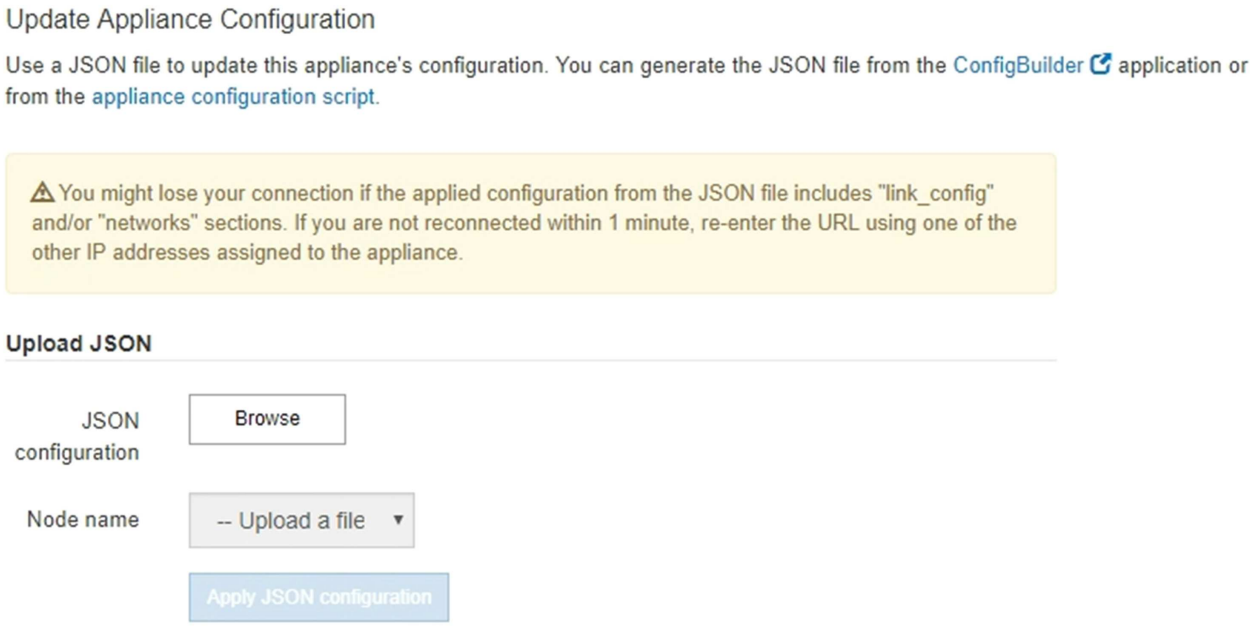
     Die Node-Namen in der JSON-Datei müssen die folgenden Anforderungen erfüllen:

     - Muss ein gültiger Hostname mit mindestens 1 und nicht mehr als 32 Zeichen sein
     - Es können Buchstaben, Ziffern und Bindestriche verwendet werden
     - Sie können nicht mit einem Bindestrich beginnen oder enden oder nur Zahlen enthalten

     Stellen Sie sicher, dass die Node-Namen (die Top-Level-Namen) in der JSON-Datei eindeutig sind, oder Sie können mit der JSON-Datei nicht mehr als einen Node konfigurieren.

2. Wählen Sie **Erweitert** > **Appliance-Konfiguration Aktualisieren**.

   Die Seite Gerätekonfiguration aktualisieren wird angezeigt.



3. Wählen Sie die JSON-Datei mit der Konfiguration aus, die Sie hochladen möchten.

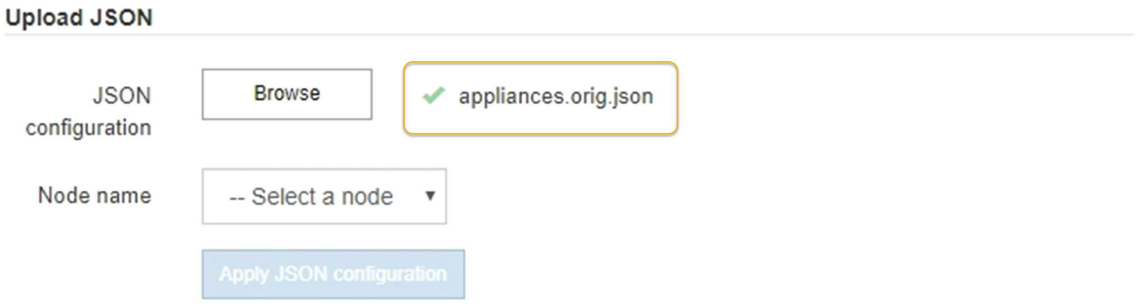
   a. Wählen Sie **Durchsuchen**.

   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 neben einem grünen Häkchen angezeigt.

   > Möglicherweise verlieren Sie die Verbindung zur Appliance, wenn die Konfiguration aus der JSON-Datei Abschnitte für „Link_config“, „Netzwerke“ oder beide enthält. Wenn Sie nicht innerhalb einer Minute eine Verbindung hergestellt haben, geben Sie die Appliance-URL mithilfe einer der anderen IP-Adressen, die der Appliance zugewiesen sind, erneut ein.

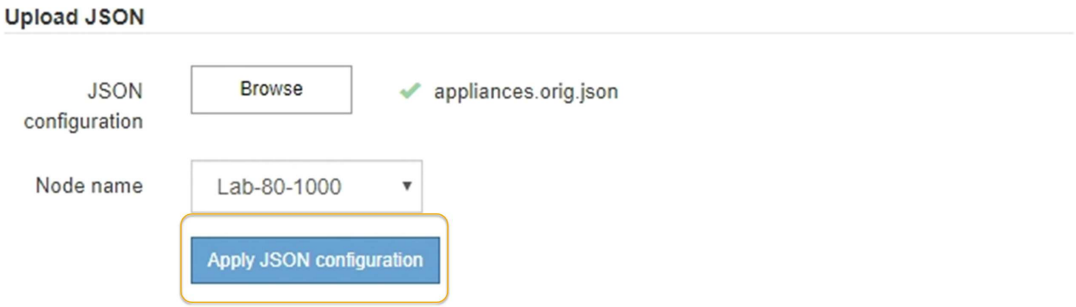


   Das Dropdown-Menü **Node Name** enthält die in der JSON-Datei definierten Node-Namen auf oberster Ebene.

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. Sie können ConfigBuilder verwenden, um sicherzustellen, dass Sie über eine gültige JSON-Datei verfügen.

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

   Die Schaltfläche **JSON-Konfiguration anwenden** ist aktiviert.



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

   Die Konfiguration wird auf den ausgewählten Knoten angewendet.

Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py

Sie können 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.

Was Sie benötigen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des StorageGRID Appliance Installer wurden Netzwerkverbindungen und IP-Adressen für den primären Administratorknoten konfiguriert.
- Wenn Sie den primären Admin-Node installieren, kennen Sie dessen IP-Adresse.
- Wenn Sie andere Knoten installieren und konfigurieren, wurde der primäre Admin-Node bereitgestellt, und Sie kennen seine IP-Adresse.
- Für alle anderen Nodes als den primären Admin-Node wurden alle auf der Seite IP-Konfiguration des Installationsprogramms der StorageGRID-Appliance aufgeführten Grid-Netzwerknetze in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- 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.

Dieses Verfahren richtet sich an fortgeschrittene Benutzer, die Erfahrung mit der Verwendung von Befehlszeilenschnittstellen haben. Alternativ können Sie die Konfiguration auch mit dem StorageGRID Appliance Installer automatisieren. +"Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer"

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`

3. Um die aktuelle Konfiguration des Appliance-Knotens zu bestätigen, geben Sie hier Folgendes ein *`SGA-install-ip`* Ist eine der IP-Adressen für den Appliance-Knoten:
   `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. #####
#####################################################################
```

4. 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`
5. Wenn Sie die Appliance-Konfiguration in einer JSON-Datei sichern möchten, verwenden Sie das `advanced` 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 diese Datei nur dann vor, wenn Sie ein erfahrener Benutzer sind und über die StorageGRID APIs verfügen.

6. 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`
7. Wenn Sie das Gerät neu starten möchten, geben Sie Folgendes ein:
   `configure-sga.py reboot SGA-INSTALL-IP`

Automatisierung der Konfiguration von StorageGRID

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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.

   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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. 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 von Knotenklonen.
- **Verschlüsselung** — Operationen zur Verwaltung der Verschlüsselung und Anzeige des Verschlüsselungsstatus.
- **Hardwarekonfiguration** — Betrieb zur Konfiguration der Systemeinstellungen auf angeschlossener Hardware.
- **Installation** — Betrieb zum Starten der Gerätesallation und zur Überwachung des Installationsstatus.
- **Networking** — Vorgänge im Zusammenhang mit der Konfiguration von Grid-, Admin- und Client-Netzwerken für eine StorageGRID-Appliance und Appliance-Port-Einstellungen.
- **Setup** — Operationen zur Unterstützung bei der Ersteinrichtung der Appliance einschließlich Anfragen zum Abrufen von Informationen über das System und zur Aktualisierung der primären Admin-Node-IP.
- **Support** — Betrieb für den Neustart des Controllers und das Abrufen von Protokollen.
- **Upgrade** — Operationen im Zusammenhang mit der Aktualisierung der Appliance-Firmware.
- **Uploadsg** — Operationen zum Hochladen von StorageGRID-Installationsdateien.

Fehlerbehebung bei der Hardwareinstallation

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Verwandte Informationen

"Die Hardware-Einrichtung scheint zu hängen"

"Fehlerbehebung bei Verbindungsproblemen"

Die Hardware-Einrichtung scheint zu hängen

Der Installationsassistent von StorageGRID steht möglicherweise nicht zur Verfügung, wenn Hardware-Fehler oder Verkabelungsfehler eine Ausführung der Boot-Verarbeitung durch den E5600SG-Controller verhindern.

Schritte

1. Prüfen Sie die Warn-LED für die Controller und suchen Sie nach einem blinkenden Fehlercode.

   Während des Hochschalens werden die LEDs „Serviceaktion zulässig“ und „Serviceaktion erforderlich“ eingeschaltet, während die Hardware initialisiert wird. Auch der obere Dezimalpunkt der unteren Ziffer, genannt *Diagnose-LED*, leuchtet auf. Die Sieben-Segment-Anzeige führt eine Reihe von Codes durch, die für beide Controller üblich sind. Dies ist normal und kein Hinweis auf einen Fehler. Wenn die Hardware erfolgreich gebootet wird, sind die Service-Aktion-LEDs ausgeschaltet, und die Anzeigen werden durch die Firmware gesteuert.

2. Überprüfen Sie die Codes auf der siebensegmentreichen Anzeige für den E5600SG-Controller.

   > Installation und Bereitstellung nehmen Zeit in Anspruch. In einigen Installationsphasen werden dem Installationsprogramm der StorageGRID-Appliance für mehrere Minuten keine Aktualisierungen gemeldet.

   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
E5600SG-Controller	• „HE error: Fehler beim Synchronisieren mit SANtricity OS Software“ • „E5600SG Controller-Anzeigecodes für sieben Segmente“
E2700 Controller	E-Series Dokumentation **Hinweis:** die für den E-Series E5600 Controller beschriebenen Codes gelten nicht für den E5600SG Controller im Gerät.

4. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.

Verwandte Informationen

"E5600SG-Controller-Anzeigecodes für sieben Segmente"

"HE-Fehler: Fehler beim Synchronisieren mit SANtricity OS Software"

"E2700 – Installationshandbuch für Controller-Laufwerke und zugehörige Laufwerksfächer"

"NetApp Dokumentation: E2700 Serie"

HE-Fehler: Fehler beim Synchronisieren mit SANtricity OS Software

Die sieben-Segment-Anzeige auf dem Compute-Controller zeigt EINEN HE-Fehlercode an, wenn das Installationsprogramm der StorageGRID-Appliance nicht mit 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 Verbindungsproblemen

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Es konnte keine Verbindung zur StorageGRID Appliance über das Netzwerk hergestellt werden

Wenn Sie keine Verbindung zur Appliance herstellen können, liegt möglicherweise ein Netzwerkproblem vor, oder die Hardwareinstallation wurde möglicherweise nicht erfolgreich abgeschlossen.

- **Ausgabe**

  Sie können keine Verbindung zum Gerät herstellen.

- **Ursache**

  Dies kann auftreten, wenn ein Netzwerkproblem auftritt oder die Hardwareinstallation nicht erfolgreich abgeschlossen wurde.

- **Korrekturmaßnahmen**

  a. Pingen des Geräts:
  `ping E5600_controller_IP`

  b. Öffnen Sie den StorageGRID Appliance Installer, indem Sie einen Browser öffnen und Folgendes eingeben:
  `https://Management_Port_IP:8443`

  Geben Sie für Management_Port_IP die IP-Adresse für Management-Port 1 auf dem E5600SG-Controller ein (während der physischen Installation bereitgestellt).

  c. Klicken Sie auf **Admin-Netzwerk konfigurieren**, und überprüfen Sie die IP.

d. Wenn Sie eine Antwort vom Ping erhalten, überprüfen Sie, ob Port 8443 in den Firewalls geöffnet ist.

e. Starten Sie die Appliance neu.

f. Aktualisieren Sie die Installationsseite.

g. Wenn das Verbindungsproblem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support über die NetApp Support Site unter "mysupport.netapp.com".

Verwandte Informationen

"E5600SG-Controller-Anzeigecodes für sieben Segmente"

Neustart des Controllers bei Ausführung des StorageGRID-Appliance-Installationsprogramms

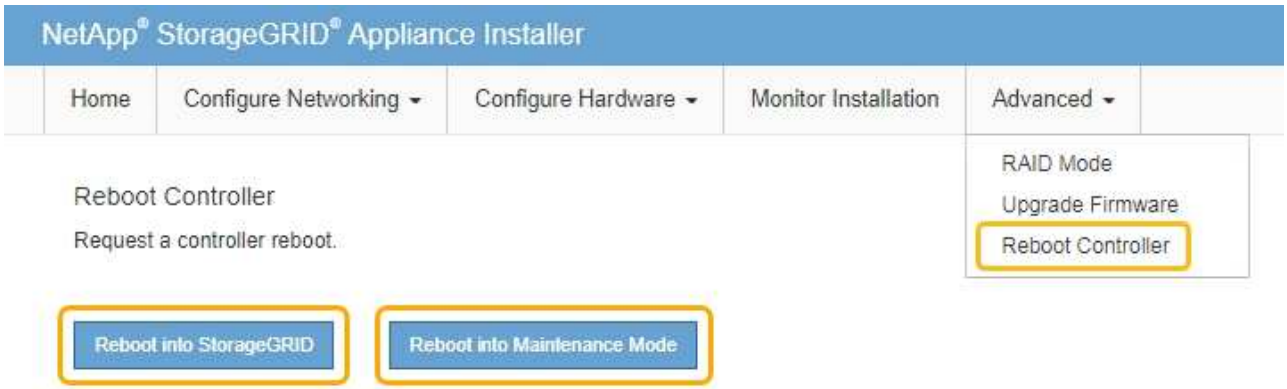
Möglicherweise müssen Sie den Compute-Controller neu starten, während das StorageGRID-Appliance-Installationsprogramm ausgeführt wird. Beispielsweise müssen Sie möglicherweise den Controller neu booten, wenn die Installation fehlschlägt.

Über diese Aufgabe

Dieses Verfahren gilt nur, wenn der Compute-Controller das Installationsprogramm der 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. Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Der SG6000-CN Controller wird neu gestartet.

Warten der SG5600 Appliance

Möglicherweise müssen Sie die SANtricity OS Software auf dem E2700 Controller aktualisieren, den E2700 Controller oder den E5600SG Controller ersetzen 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.

Schritte

- "Versetzen einer Appliance in den Wartungsmodus"
- "Aktualisieren von SANtricity OS auf den Storage Controllern mit Grid Manager"
- "Aktualisieren des SANtricity OS Systems auf dem E2700 Controller mithilfe des Wartungsmodus"
- "Aktualisieren der Laufwerk-Firmware mithilfe von SANtricity Storage Manager"
- "Austausch des E2700 Controllers"
- "Austauschen des E5600SG-Controllers"
- "Austausch anderer Hardwarekomponenten"
- "Ändern der Link-Konfiguration des E5600SG-Controllers"
- "Ändern der MTU-Einstellung"
- "Überprüfen der DNS-Serverkonfiguration"
- "Monitoring der Node-Verschlüsselung im Wartungsmodus"

Versetzen einer Appliance in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

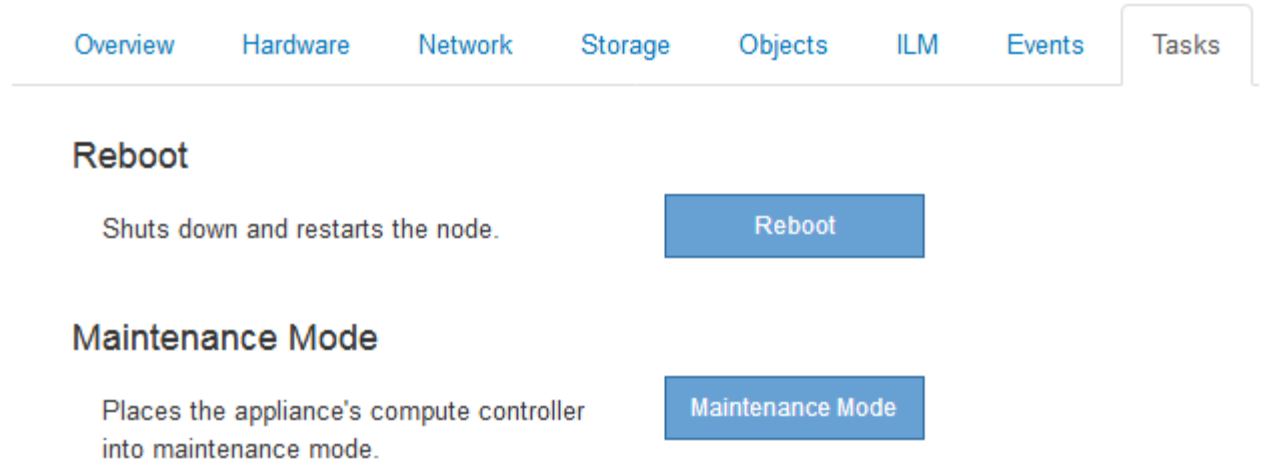
Über diese Aufgabe

Wenn Sie eine StorageGRID Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

> Das Passwort und der Hostschlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem, als das Gerät in Betrieb war.

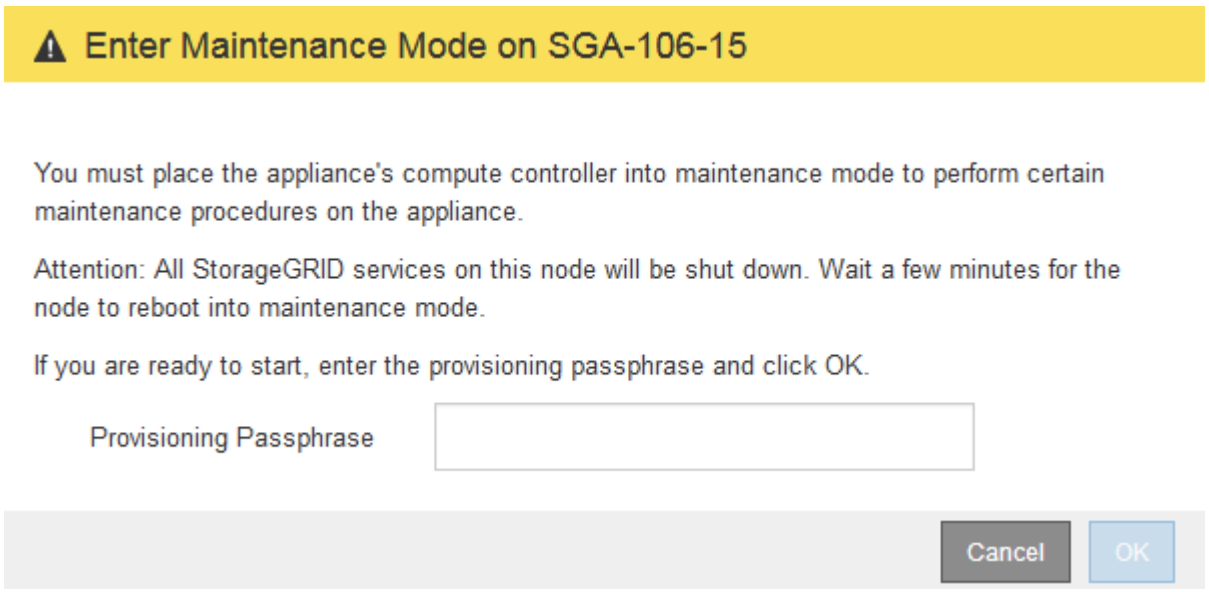
Schritte

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**.



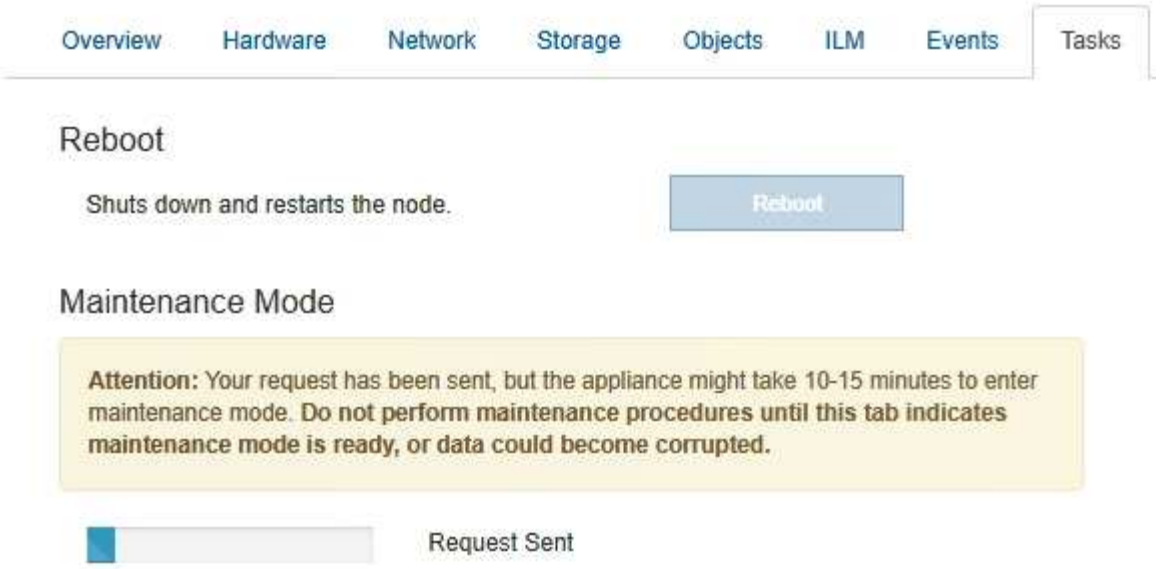
4. Wählen Sie **Wartungsmodus**.

   Ein Bestätigungsdialogfeld wird angezeigt.

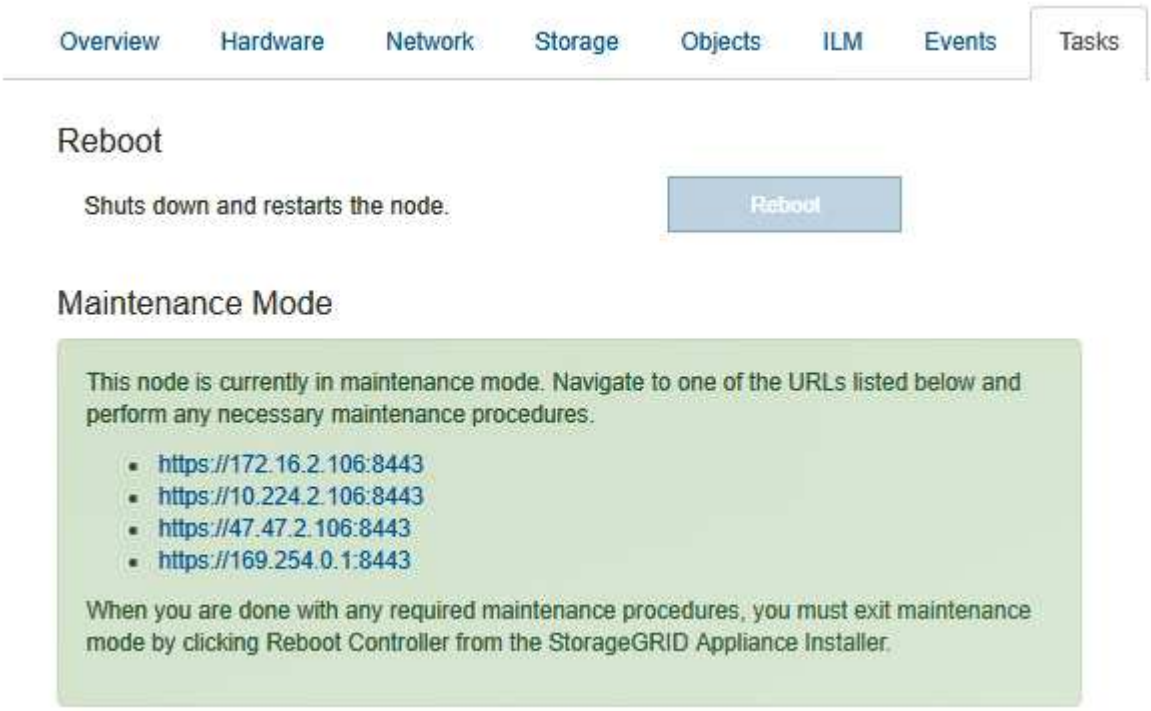


5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

   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.



6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

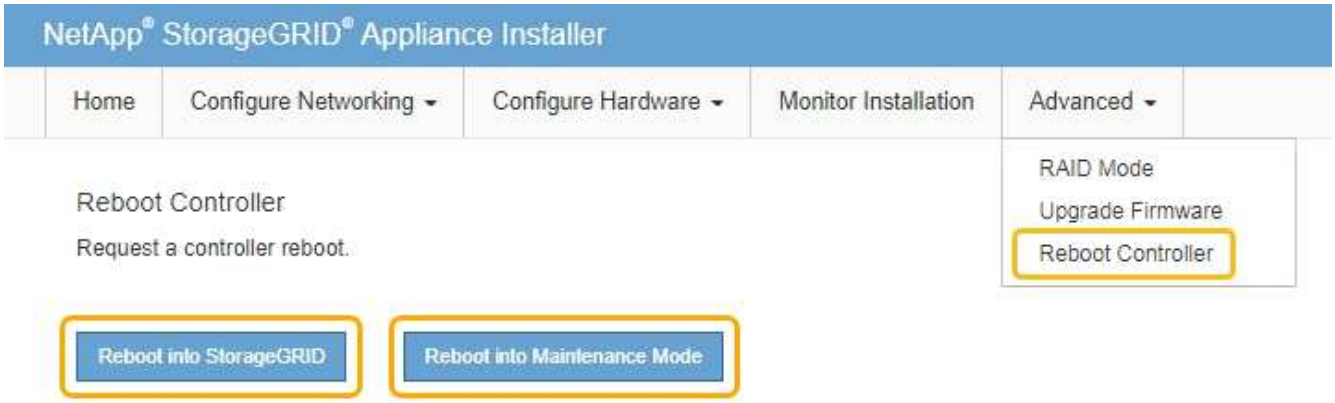
   Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.

   > Zugriff Auf `https://169.254.0.1:8443` Erfordert eine direkte Verbindung zum lokalen Management-Port.

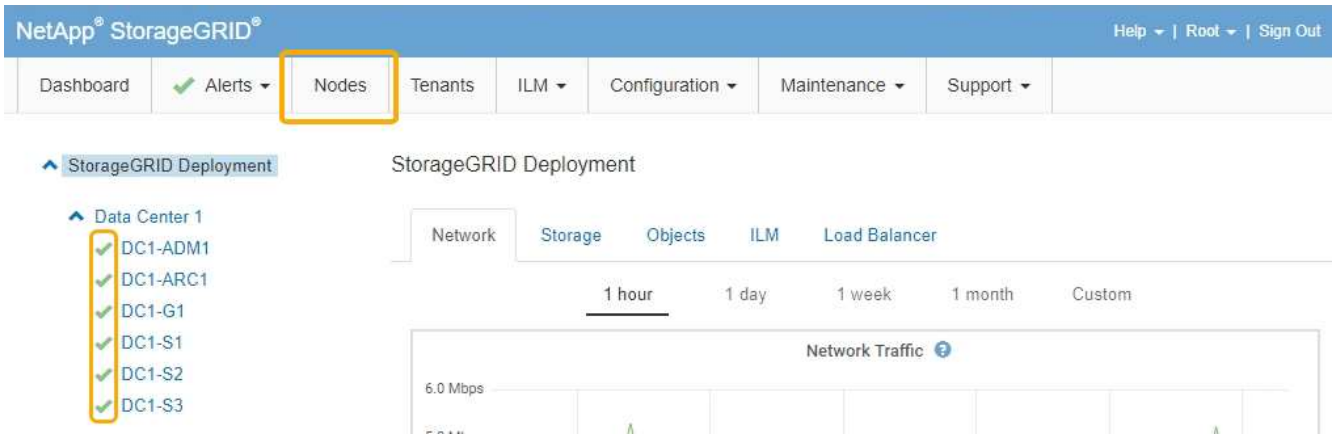
7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im

Wartungsmodus befindet.

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.



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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Aktualisieren von SANtricity OS auf den Storage Controllern mit Grid Manager

Verwenden Sie den Grid-Manager, um ein SANtricity OS-Upgrade anzuwenden.

Was Sie benötigen

- Sie haben das NetApp Interoperabilitäts-Matrix-Tool (IMT) konsultiert, um zu überprüfen, ob die für das Upgrade verwendete SANtricity Betriebssystemversion mit Ihrer Appliance kompatibel ist.

- Sie müssen über die Berechtigung zur Wartung verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen auf die NetApp Download-Seite für SANtricity OS zugreifen können.

Über diese Aufgabe

Sie können keine anderen Softwareupdates (StorageGRID Software-Upgrade oder Hotfix) durchführen, bis Sie den SANtricity OS-Upgrade-Prozess abgeschlossen haben. 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. Das Laden des SANtricity Betriebssystems auf jedem Node kann länger als 30 Minuten und ein Neustart jeder StorageGRID Storage Appliance bis zu 90 Minuten dauern.

Die folgenden Schritte sind nur anwendbar, wenn Sie den Grid Manager zur Durchführung des Upgrades verwenden.

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.

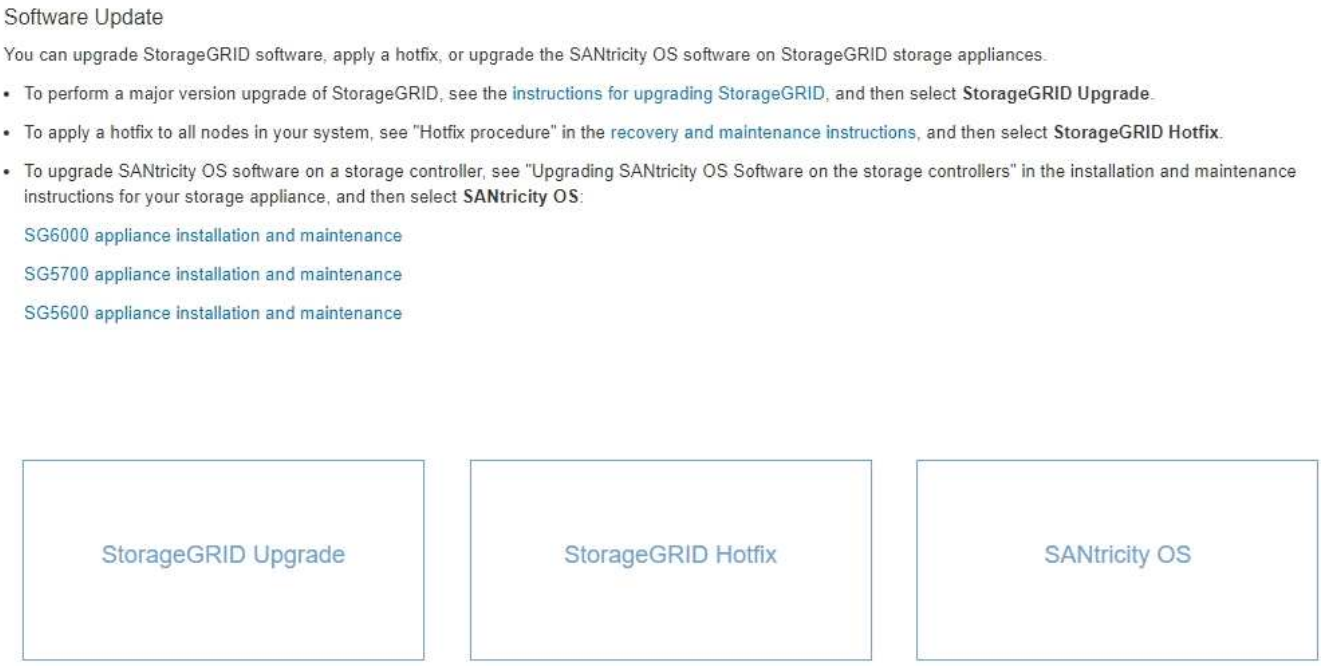
Schritte

1. Laden Sie von einem Service-Laptop die neue SANtricity OS Datei von der NetApp Support Website herunter.

   Denken Sie daran, die SANtricity Betriebssystemversion für den E2700 Storage Controller auszuwählen.

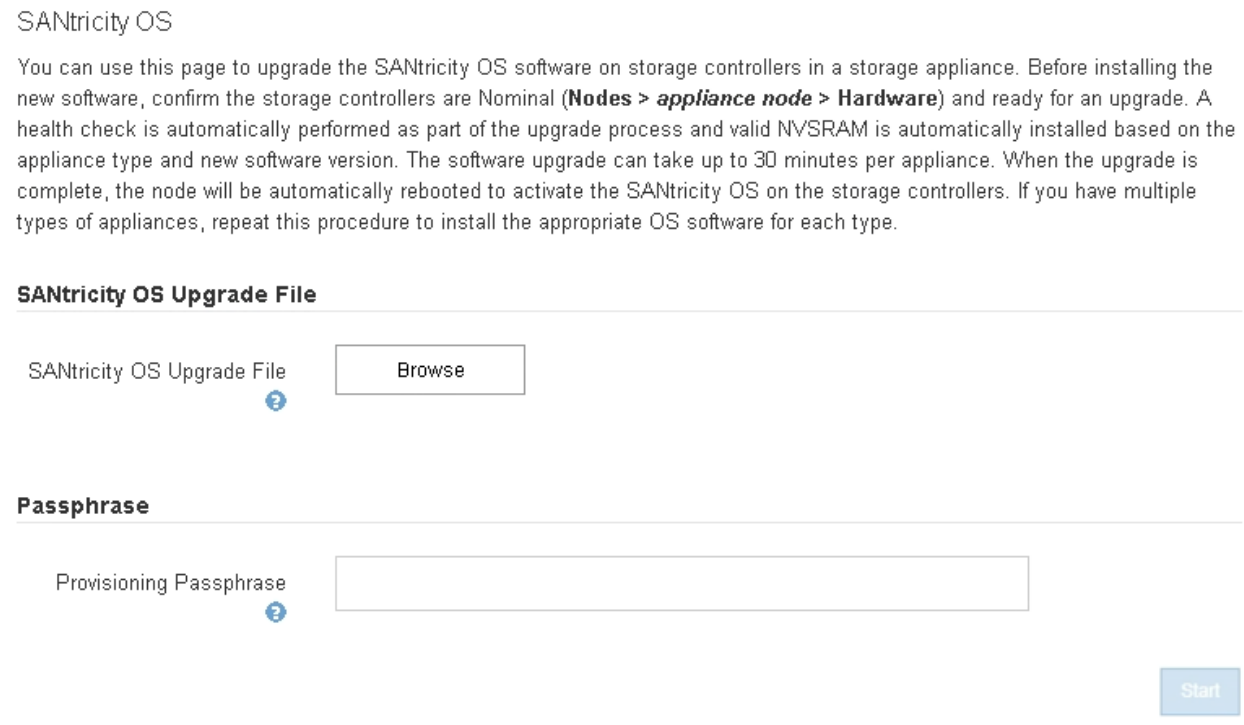
2. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
3. Wählen Sie **Wartung**. Wählen Sie dann im Bereich System des Menüs die Option **Software Update** aus.

   Die Seite Software-Aktualisierung wird angezeigt.



4. Klicken Sie auf **SANtricity OS**.

   Die Seite SANtricity OS wird angezeigt.



5. Wählen Sie die Upgrade-Datei für das SANtricity OS aus, die Sie von der NetApp Support-Website heruntergeladen haben.

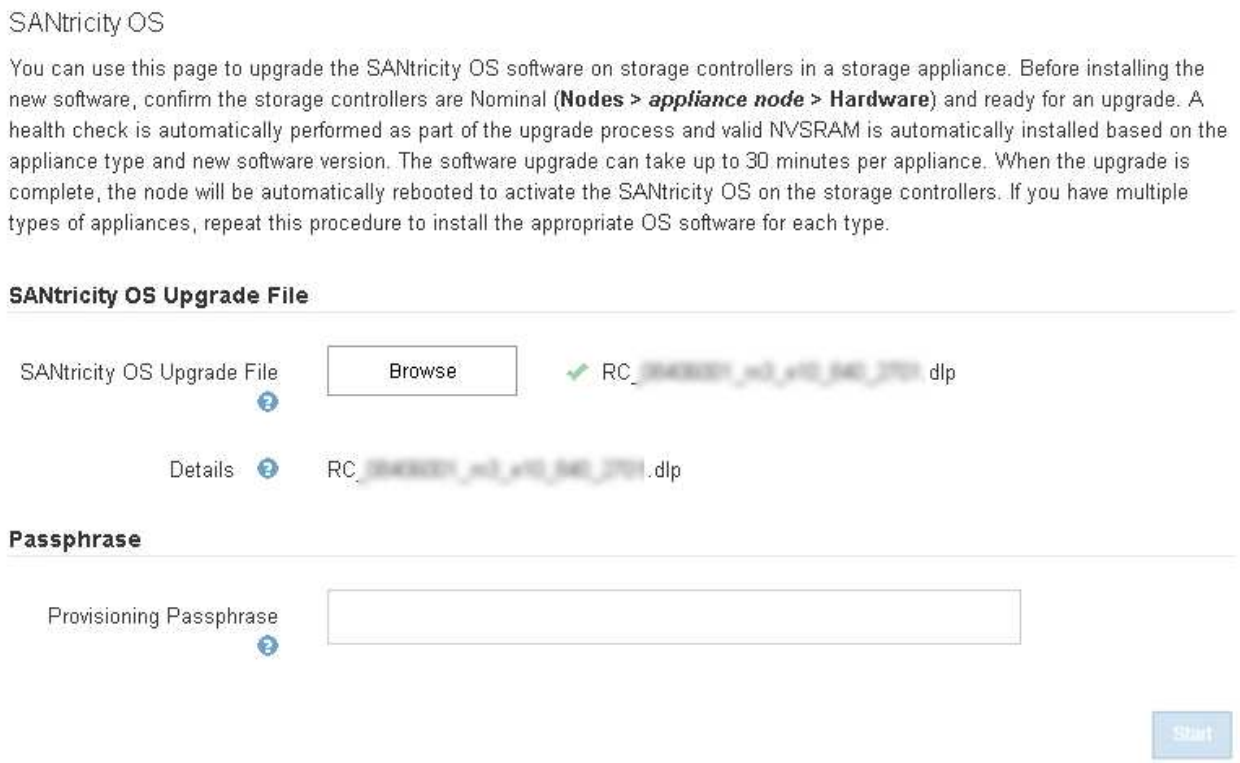
   a. Klicken Sie Auf **Durchsuchen**.

b. Suchen und wählen Sie die Datei aus.

c. Klicken Sie Auf **Offen**.

Die Datei wird hochgeladen und validiert. Wenn der Validierungsprozess abgeschlossen ist, wird der Dateiname im Feld Details angezeigt.

Ändern Sie den Dateinamen nicht, da er Teil des Verifizierungsvorgangs ist.



6. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start** ist aktiviert.

7. Klicken Sie Auf **Start**.

   Ein Warnfeld zeigt an, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf Knoten, die aktualisiert werden, neu gestartet werden.

8. Klicken Sie auf **OK**, um die SANtricity OS-Aktualisierungsdatei auf den primären Admin-Knoten zu stellen.

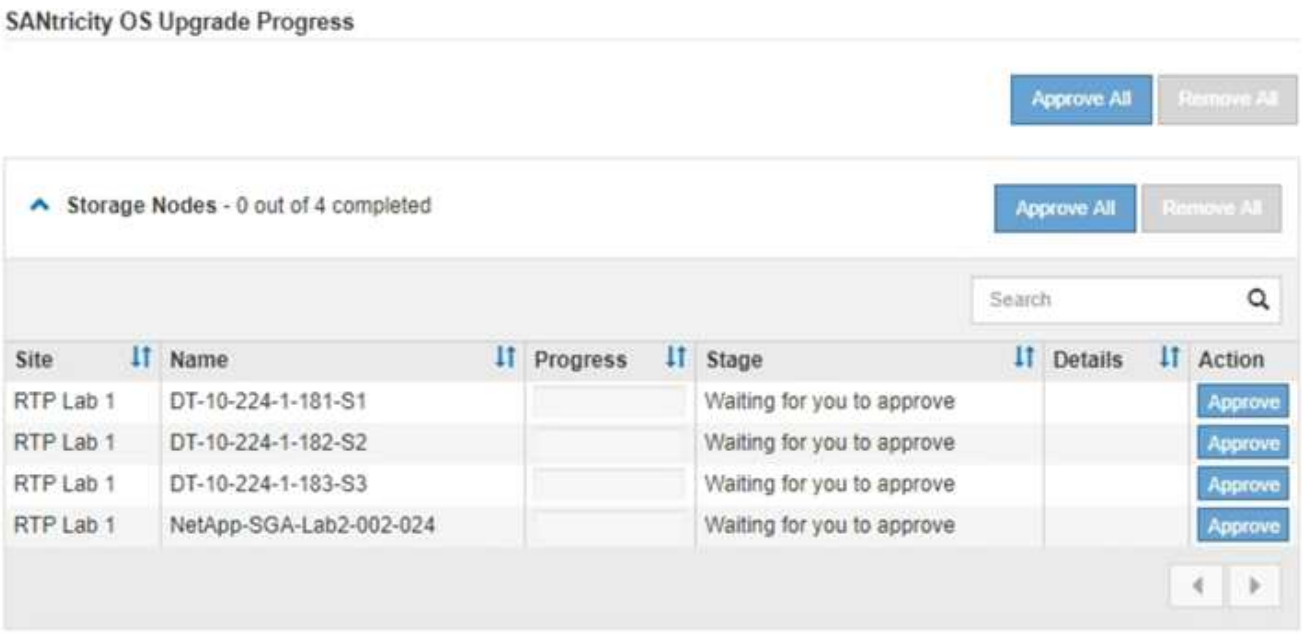
   Wenn das SANtricity OS Upgrade startet:

   a. Die Integritätsprüfung wird ausgeführt. Dieser Prozess überprüft, dass für keine Nodes der Status „Aufmerksamkeit erforderlich“ angezeigt wird.

      Wenn Fehler gemeldet werden, lösen Sie sie und klicken Sie erneut auf **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 werden alle Storage-Nodes einschließlich softwarebasierter Storage-Nodes aufgeführt. Sie müssen das Upgrade für alle Storage-Nodes genehmigen, obwohl ein Upgrade des SANtricity Betriebssystems keine Auswirkungen auf softwarebasierte Storage-Nodes hat. Die für softwarebasierte Storage-Nodes zurückgegebene Upgrade-Meldung lautet „`SANtricity OS Upgrade ist für diesen Node nicht anwendbar.`“



9. Sortieren Sie die Liste der Knoten 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.

   Sie können durch die Liste der Knoten blättern, indem Sie die Pfeile links und rechts unten rechts im Abschnitt verwenden.

10. Genehmigen Sie die Grid-Knoten, die Sie zur Upgrade-Warteschlange hinzufügen möchten. Genehmigte Nodes desselben Typs werden nacheinander aktualisiert.

    > ⓘ Genehmigen Sie das SANtricity OS Upgrade für einen Appliance-Storage-Node nicht, es sei denn, Sie sind sicher, dass der Node bereit ist, angehalten und neu gebootet zu werden.Wenn das Upgrade des SANtricity OS auf einem Node genehmigt wird, werden die Services auf diesem Node angehalten. Wenn der Node später aktualisiert wird, wird der Appliance-Node neu gebootet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

    - Klicken Sie auf eine der Schaltflächen **Alle genehmigen**, um alle Speicherknoten zur Upgrade-Warteschlange des SANtricity OS hinzuzufügen.

      > ⓘ 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.

    - Klicken Sie auf eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere Knoten zur SANtricity OS-Upgrade-Warteschlange hinzuzufügen.

      > ⓘ Sie können das Anwenden eines SANtricity OS Upgrades auf einen Node verzögern. Der Upgrade-Prozess für SANtricity OS ist jedoch erst abgeschlossen, wenn Sie das Upgrade von SANtricity OS auf allen aufgeführten Storage-Nodes genehmigen.

    Nach dem Klicken auf **Genehmigen** bestimmt der Upgrade-Prozess, ob der Knoten aktualisiert werden kann. Wenn ein Knoten aktualisiert werden kann, wird er der Upgrade-Warteschlange hinzugefügt. +

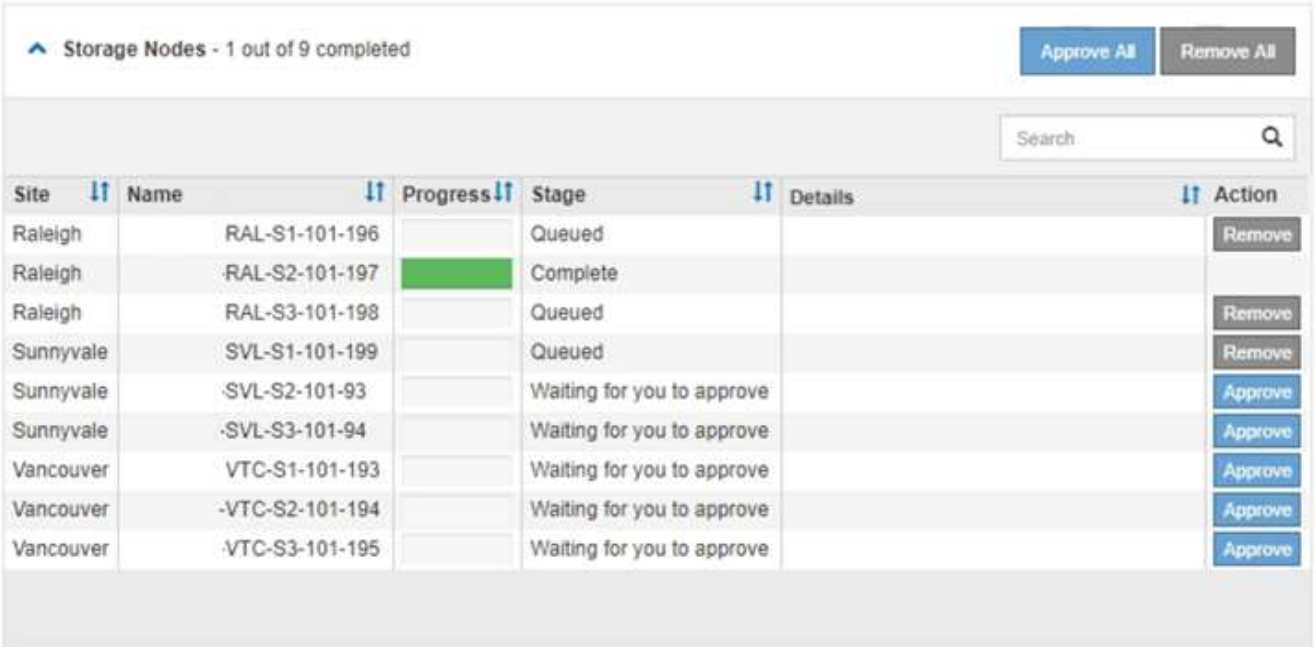
Bei einigen Nodes wird die ausgewählte Upgrade-Datei absichtlich nicht angewendet. Sie können das Upgrade abschließen, ohne dass Sie ein Upgrade dieser spezifischen Nodes durchführen müssen. Bei Knoten, die absichtlich keine Aktualisierung durchgeführt haben, wird der Prozess mit einer der folgenden Meldungen in der Spalte Details angezeigt: +

- Storage-Node wurde bereits aktualisiert.
- Das SANtricity OS Upgrade ist für diesen Node nicht verfügbar.
- Die SANtricity OS-Datei ist mit diesem Node nicht kompatibel.

Die Meldung „`SANtricity OS Upgrade ist für diesen Node` nicht verfügbar“ gibt an, dass der Node keinen Storage Controller besitzt, der vom StorageGRID System gemanagt werden kann. Diese Meldung wird für nicht-Appliance-Speicherknoten angezeigt. Sie können den Upgrade-Prozess von SANtricity OS abschließen, ohne dass ein Upgrade des Node ausgeführt wird, der diese Meldung anzeigt. + die Meldung „`SANtricity OS File is not compatible with this Node`“ gibt an, dass der Knoten eine SANtricity OS Datei erfordert, die sich von dem Prozess unterscheidet, der zu installieren versucht. Nachdem Sie das aktuelle Upgrade von SANtricity OS abgeschlossen haben, laden Sie das für den Node geeignete SANtricity OS herunter, und wiederholen Sie den Upgrade-Prozess.

11. Wenn Sie einen Knoten oder alle Knoten aus der SANtricity OS Upgrade-Warteschlange entfernen müssen, klicken Sie auf **Entfernen** oder **Alle entfernen**.

    Wie im Beispiel gezeigt, ist die **Remove**-Schaltfläche ausgeblendet, wenn die Phase über Queued hinausgeht und Sie können den Knoten nicht mehr aus dem SANtricity OS-Upgrade-Prozess entfernen.



12. Warten Sie, während das SANtricity OS Upgrade auf jeden genehmigten Grid-Node angewendet wird.

> Wenn während des SANtricity OS Upgrades auf einem beliebigen Node eine Fehlerstufe angezeigt wird, ist das Upgrade für diesen Node fehlgeschlagen. Das Gerät muss möglicherweise in den Wartungsmodus versetzt werden, um nach dem Ausfall eine Wiederherstellung durchzuführen. Wenden Sie sich an den technischen Support, bevor Sie fortfahren.

Wenn die Firmware auf dem Node zu alt ist, um ein Upgrade mit dem Grid Manager durchzuführen, zeigt der Node eine Fehlerstufe an. Die Details: „`Sie müssen den Wartungsmodus verwenden, um ein Upgrade

von SANtricity OS auf diesem Node durchzuführen. Siehe Installations- und Wartungsanleitung für Ihr Gerät. Nach dem Upgrade können Sie dieses Dienstprogramm für zukünftige Upgrades verwenden.`" Gehen Sie wie folgt vor, um den Fehler zu beheben:

a. Verwenden Sie den Wartungsmodus, um ein Upgrade von SANtricity OS auf dem Node durchzuführen, auf dem eine Fehlerstufe angezeigt wird.
b. Verwenden Sie den Grid-Manager, um das SANtricity OS-Upgrade erneut zu starten und abzuschließen.

   Wenn das SANtricity OS Upgrade auf allen genehmigten Nodes abgeschlossen ist, wird die Fortschrittstabelle des SANtricity OS Upgrades geschlossen, und ein grünes Banner zeigt das Datum und die Uhrzeit des Ababgeschlossenen Upgrades des SANtricity OS an.

13. 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

"Aktualisieren des SANtricity OS Systems auf dem E2700 Controller mithilfe des Wartungsmodus"

Aktualisieren des SANtricity OS Systems auf dem E2700 Controller mithilfe des Wartungsmodus

Wenn Sie die SANtricity OS-Software nicht mithilfe des Grid-Managers aktualisieren können, wenden Sie das Upgrade im Wartungsmodus an.

Was Sie benötigen

- Sie haben das NetApp Interoperabilitäts-Matrix-Tool (IMT) konsultiert, um zu überprüfen, ob die für das Upgrade verwendete SANtricity Betriebssystemversion mit Ihrer Appliance kompatibel ist.
- Wenn Sie den Grid Manager nicht verwenden, müssen Sie den E5600SG-Controller in den Wartungsmodus versetzen. Wenn der Controller in den Wartungsmodus versetzt wird, wird die Verbindung zum E2700 Controller unterbrochen. Bevor Sie die Link-Konfiguration ändern, müssen Sie den E5600SG-Controller in den Wartungsmodus versetzen. Wenn eine StorageGRID Appliance in den Wartungsmodus versetzt wird, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

  "Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Aktualisieren Sie das SANtricity Betriebssystem und NVSRAM im E-Series Controller nicht auf mehr als einer

StorageGRID Appliance gleichzeitig.

> Wenn Sie mehrere StorageGRID Appliances gleichzeitig aktualisieren, kann dies in Abhängigkeit von Ihrem Implementierungsmodell und den ILM-Richtlinien zu Datenunverfügbarkeit führen.

Schritte

1. Greifen Sie über ein Service-Laptop auf den SANtricity Storage Manager zu und melden Sie sich an.
2. 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 nicht den Standard-NVSRAM-Download.

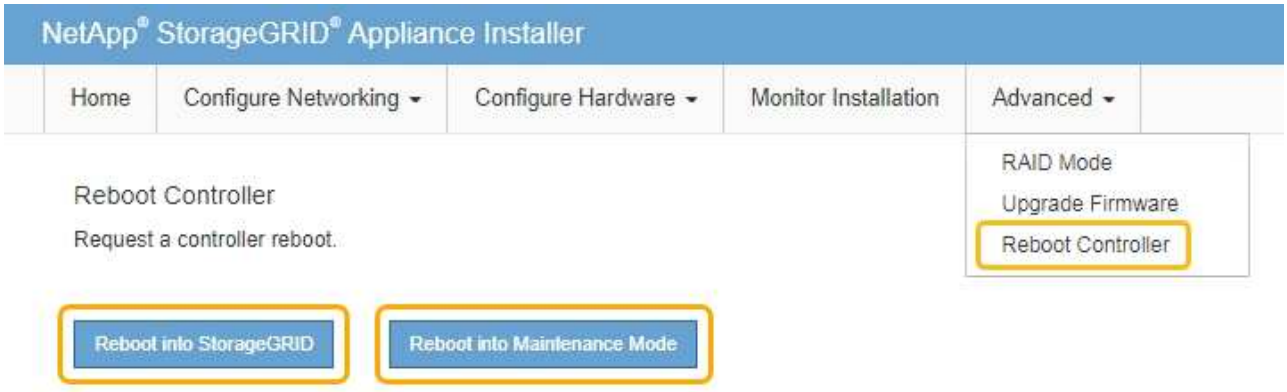
3. Folgen Sie den Anweisungen in der Online-Hilfe des E2700 und der E5600 SANtricity-Software und Firmware-Upgrades_ oder der SANtricity Storage Manager und aktualisieren Sie die Firmware des E2700 Controllers, NVSRAM oder beides.

   > Wenn Sie NVSRAM im E2700 Controller aktualisieren müssen, müssen Sie bestätigen, dass die heruntergeladene SANtricity Betriebssystemdatei mit StorageGRID Appliances kompatibel ist.

   > Aktivieren Sie die Upgrade-Dateien sofort. Die Aktivierung nicht verschieben.

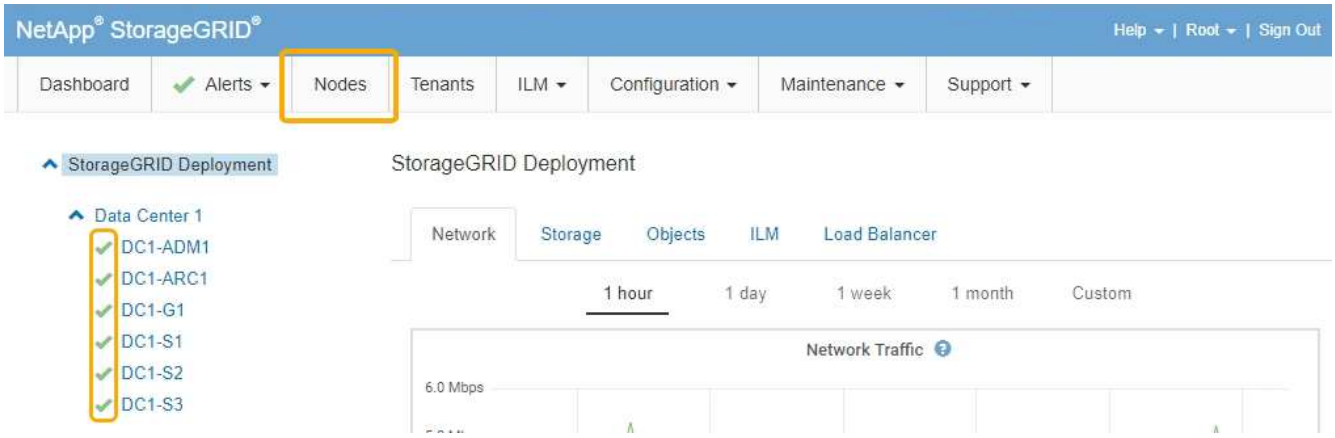
4. Sobald der Upgrade-Vorgang abgeschlossen ist, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Aktualisieren der Laufwerk-Firmware mithilfe von SANtricity Storage Manager

Sie aktualisieren Ihre Laufwerk-Firmware, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen.

Was Sie benötigen

- Die Storage Appliance hat einen optimalen Status.
- Alle Laufwerke haben einen optimalen Status.
- Sie haben die aktuelle Version des SANtricity Storage Managers installiert, der mit Ihrer StorageGRID-Version kompatibel ist.

  "Aktualisieren von SANtricity OS auf den Storage Controllern mit Grid Manager"

  "Aktualisieren des SANtricity OS Systems auf dem E2700 Controller mithilfe des Wartungsmodus"

- Sie haben die StorageGRID-Appliance in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

> ⓘ Im Wartungsmodus wird die Verbindung zum Storage Controller unterbrochen, alle I/O-Aktivitäten werden angehalten und alle Laufwerke werden offline geschaltet.

> ⓘ Aktualisieren Sie die Laufwerk-Firmware nicht auf mehr als einer StorageGRID Appliance gleichzeitig. Dadurch kann je nach Implementierungsmodell und ILM-Richtlinien die Nichtverfügbarkeit von Daten auftreten.

Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse als URL für SANtricity-Speichermanager ein: `https://E2700_Controller_IP`
2. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des SANtricity Storage Manager-Administrators ein.

3. Wählen Sie in SANtricity Enterprise Management die Registerkarte **Geräte** aus.

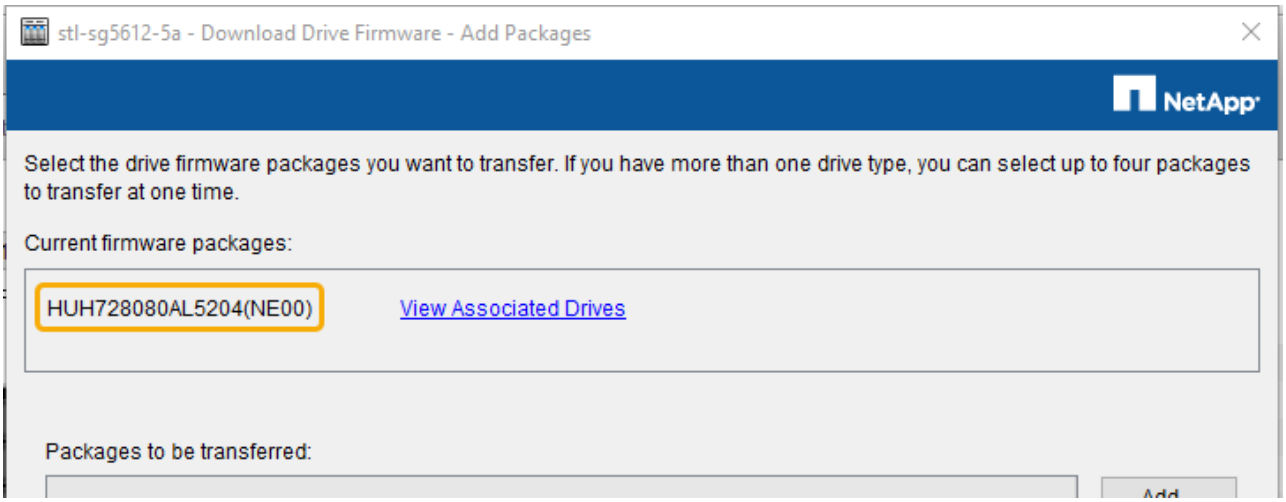
   Das Fenster SANtricity-Array-Verwaltung wird geöffnet.

4. Doppelklicken Sie in der SANtricity-Array-Verwaltung auf das Speicher-Array mit den zu aktualisierenden Laufwerken.
5. Vergewissern Sie sich, dass sowohl das Speicher-Array als auch die Laufwerke den optimalen Status haben.
6. Überprüfen Sie die Version der Laufwerk-Firmware, die derzeit in der Speicher-Appliance installiert ist:

   a. Wählen Sie in SANtricity Enterprise Management die Option **Upgrade** > **Laufwerk-Firmware**.

      Im Fenster Laufwerk-Firmware herunterladen – Pakete hinzufügen werden die aktuell verwendeten Firmware-Dateien des Laufwerks angezeigt.

   b. Beachten Sie die aktuellen Versionen der Laufwerk-Firmware und die Laufwerk-IDs unter Aktuelle Firmware-Pakete.



   In diesem Beispiel:

   - Die Version der Laufwerk-Firmware lautet **NE00**.
   - Die Laufwerk-ID lautet **HUH728080AL5204**.

   Wählen Sie * zugeordnete Laufwerke anzeigen* aus, um anzuzeigen, wo diese Laufwerke in Ihrem Speichergerät installiert sind.

7. Laden Sie das verfügbare Laufwerk-Firmware-Upgrade herunter, und bereiten Sie es vor:

   a. Öffnen Sie Ihren Webbrowser, navigieren Sie zur NetApp Support Website und melden Sie sich mit Ihrer ID und Ihrem Passwort an.

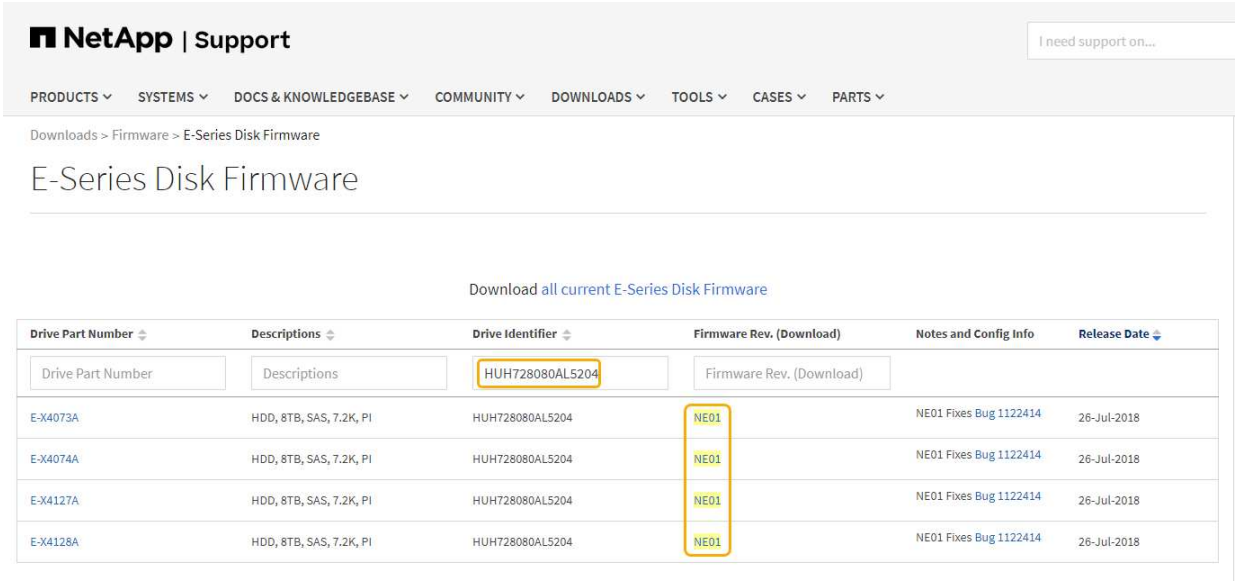
      "NetApp Support"

   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 Laufwerkkennung die neueste Firmware-Version hat.

- Wenn die Firmware-Version kein Link ist, hat diese Laufwerkkennung 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.



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).

8. Installieren Sie das Laufwerk-Firmware-Upgrade:

a. Wählen Sie im Fenster SANtricity Storage Manager Laufwerk-Firmware herunterladen - Pakete hinzufügen die Option **Hinzufügen** aus.

b. Navigieren Sie zum Verzeichnis, das die Firmware-Dateien enthält, und wählen Sie bis zu vier Firmware-Dateien aus.

Die Firmware-Dateien des Laufwerks haben einen Dateinamen wie `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

Wenn Sie mehrere Firmware-Dateien auswählen, um die Firmware des gleichen Laufwerks zu aktualisieren, kann dies zu einem Dateikonflikt führen. Wenn ein Dateikonflikt auftritt, wird ein Fehlerdialogfeld angezeigt. Um diesen Fehler zu beheben, wählen Sie **OK** aus, und entfernen Sie alle anderen Firmware-Dateien außer denen, die Sie für die Aktualisierung der Firmware des Laufwerks verwenden möchten. Um eine Firmware-Datei zu entfernen, wählen Sie die Firmware-Datei im Informationsbereich Pakete aus, die übertragen werden sollen, und wählen Sie **Entfernen** aus. Darüber hinaus können Sie nur bis zu vier Laufwerk-Firmware-Pakete gleichzeitig auswählen.

c. Wählen Sie **OK**.

Das System aktualisiert den Informationsbereich Pakete, die mit den ausgewählten Firmware-Dateien übertragen werden sollen.

d. Wählen Sie **Weiter**.

Das Fenster Laufwerk-Firmware herunterladen – Laufwerke auswählen wird geöffnet.

- Alle Laufwerke in der Appliance werden nach Konfigurationsinformationen und nach den Voraussetzungen für Upgrades durchsucht.
- Sie werden mit einer Auswahl (je nachdem, welche Anzahl von Laufwerken Sie im Speicher-Array haben) von kompatiblen Laufwerken angezeigt, die mit der ausgewählten Firmware aktualisiert werden können. Die Laufwerke, die als Online-Vorgang aktualisiert werden können, werden standardmäßig angezeigt.
- Die ausgewählte Firmware für das Laufwerk wird im Bereich der vorgeschlagenen Firmware-Informationen angezeigt. Wenn Sie die Firmware ändern müssen, wählen Sie **Zurück** aus, um zum vorherigen Dialogfeld zurückzukehren.

e. Wählen Sie aus der Upgrade-Funktion des Laufwerks den Download-Vorgang **parallel** oder **All** aus.

Sie können eine dieser Upgrade-Methoden verwenden, da sich die Appliance im Wartungsmodus befindet, wobei die I/O-Aktivität für alle Laufwerke und alle Volumes angehalten wird.

f. Wählen Sie in kompatiblen Laufwerken die Laufwerke aus, für die Sie die ausgewählten Firmware-Dateien aktualisieren möchten.
   - Wählen Sie für ein oder mehrere Laufwerke jedes Laufwerk aus, das Sie aktualisieren möchten.
   - Wählen Sie für alle kompatiblen Laufwerke * Alle auswählen*.

     Als Best Practice wird empfohlen, alle Laufwerke desselben Modells auf dieselbe Firmware-Version zu aktualisieren.

g. Wählen Sie **Fertig**, und geben Sie dann ein `yes` Und wählen Sie **OK**.
   - Das Herunterladen und Upgrade der Laufwerk-Firmware beginnt mit der Firmware des Download-Laufwerks. Der Fortschritt zeigt den Status der Firmware-Übertragung für alle Laufwerke an.
   - Der Status jedes Laufwerks, das an der Aktualisierung beteiligt ist, wird in der Spalte Status des Übertragungsfortschritts der aktualisierten Geräte angezeigt.

     Ein Upgrade der parallelen Festplatten-Firmware kann bis zu 90 Sekunden dauern, wenn alle Laufwerke auf einem System mit 24 Laufwerken aktualisiert werden. Bei einem größeren System ist die Ausführungszeit etwas länger.

h. Während der Firmware-Aktualisierung können Sie: +
   - Wählen Sie **Stopp**, um die Firmware-Aktualisierung zu beenden. Alle derzeit laufenden Firmware-Aktualisierungen sind abgeschlossen. Alle Laufwerke, bei denen ein Firmware-Upgrade durchgeführt wurde, zeigen ihren individuellen Status an. Alle verbleibenden Laufwerke werden mit dem Status „nicht versucht“ aufgeführt.

     Wenn Sie die Aktualisierung der Laufwerk-Firmware beenden, kann dies zu Datenverlust oder nicht verfügbaren Laufwerken führen.

   - Wählen Sie **Speichern unter** aus, um einen Textbericht der Fortschrittszusammenfassung der Firmware-Aktualisierung zu speichern. Der Bericht wird mit einer standardmäßigen .log-Dateierweiterung gespeichert. Wenn Sie die Dateierweiterung oder das Verzeichnis ändern möchten, ändern Sie die Parameter in Save Drive Download Log.

i. Verwenden Sie Download Drive Firmware - Fortschritt, um den Fortschritt der Laufwerk-Firmware-Upgrades zu überwachen. Der Bereich „Laufwerke aktualisiert“ enthält eine Liste der Laufwerke, die für das Firmware-Upgrade geplant sind, sowie den Übertragungsstatus des Downloads und Upgrades

jedes Laufwerks.

Der Fortschritt und der Status jedes Laufwerks, das an der Aktualisierung beteiligt ist, wird in der Spalte „Fortschritt übertragen“ angezeigt. Nehmen Sie die entsprechende empfohlene Aktion vor, wenn während des Upgrades Fehler auftreten.

- **Ausstehend**

  Dieser Status wird für einen Online-Firmware-Download-Vorgang angezeigt, der zwar geplant, aber noch nicht gestartet wurde.

- **In Bearbeitung**

  Die Firmware wird auf das Laufwerk übertragen.

- **Rekonstruktion läuft**

  Dieser Status wird angezeigt, wenn eine Volume-Übertragung während der schnellen Rekonstruktion eines Laufwerks stattfindet. Dies liegt normalerweise daran, dass der Controller zurückgesetzt oder ausfällt und der Controller-Eigentümer das Volume überträgt.

Das System initiiert eine vollständige Rekonstruktion des Laufwerks.

- **Fehlgeschlagen - Teil**

  Die Firmware wurde nur teilweise auf das Laufwerk übertragen, bevor ein Problem die Übertragung der restlichen Datei verhindert hat.

- **Fehlgeschlagen - ungültiger Status**

  Die Firmware ist ungültig.

- **Fehlgeschlagen - Sonstiges**

  Die Firmware konnte nicht heruntergeladen werden, möglicherweise aufgrund eines physischen Problems mit dem Laufwerk.

- **Nicht versucht**

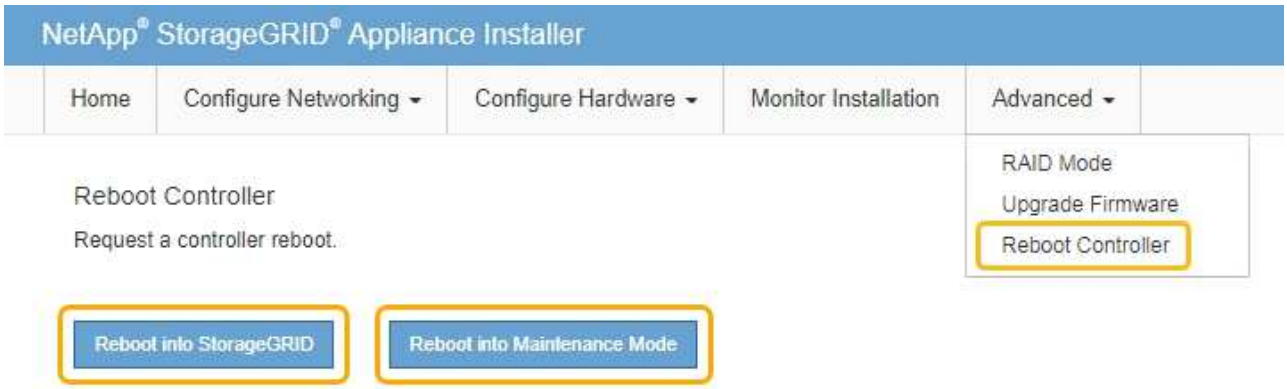
  Die Firmware wurde nicht heruntergeladen. Dies kann auf verschiedene Gründe zurückzuführen sein, wie z. B. der Download wurde angehalten, bevor es auftreten konnte, oder das Laufwerk hat sich nicht für das Upgrade qualifiziert, oder der Download konnte aufgrund eines Fehlers nicht auftreten.

- **Erfolgreich**

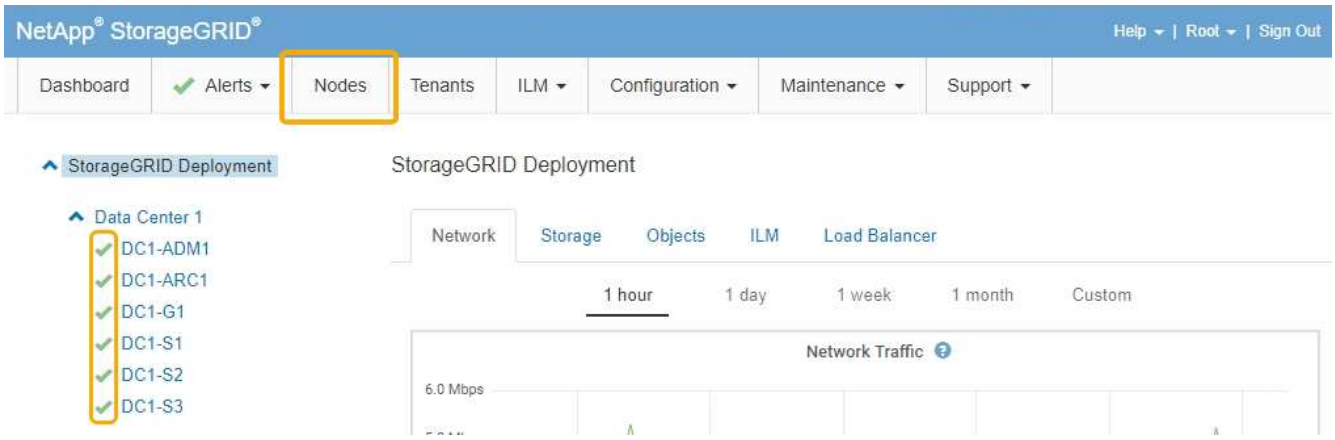
  Die Firmware wurde erfolgreich heruntergeladen.

9. Nach Abschluss des Upgrades der Laufwerk-Firmware:
   - Um den Assistenten zum Herunterladen der Laufwerk-Firmware zu schließen, wählen Sie **Schließen**.
   - Um den Assistenten erneut zu starten, wählen Sie **Mehr übertragen**.
10. Starten Sie die Appliance nach Abschluss des Aktualisierungsvorgangs 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Austausch des E2700 Controllers

Möglicherweise müssen Sie den E2700 Controller austauschen, wenn er nicht optimal funktioniert oder ausgefallen ist.

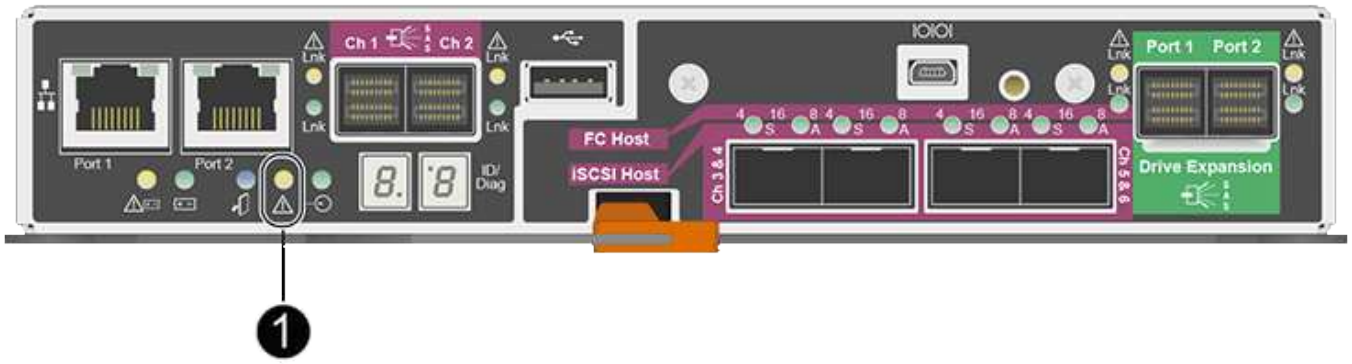
Was Sie benötigen

- 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 antistatischen Schutz.

- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Über diese Aufgabe

Sie können feststellen, ob ein ausgefallener Controller vorhanden ist, indem Sie die gelbe Service Action required LED am Controller überprüfen (in der Abbildung 1). Wenn diese LED leuchtet, sollte der Controller ersetzt werden.



Auf den Appliance-Speicherknoten kann nicht zugegriffen werden, wenn Sie den Controller austauschen. Wenn der E2700 Controller ausreichend funktioniert, können Sie den E5600SG Controller in den Wartungsmodus versetzen.

Wenn Sie einen Controller austauschen, müssen Sie den Akku aus dem ursprünglichen Controller entfernen und in den Ersatzcontroller einsetzen.

Schritte

1. Bereiten Sie das Entfernen des Controllers vor.

   Sie führen diese Schritte mit SANtricity Storage Manager aus.

   a. Notieren Sie sich, welche Version der SANtricity OS Software derzeit auf dem Controller installiert ist.
   b. Notieren Sie sich, welche NVSRAM-Version derzeit installiert ist.
   c. 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 im Gerät sicher sind, kann der neue Controller erst dann auf das Gerät zugreifen, wenn Sie die gesicherten Laufwerke mit dem Unternehmensverwaltungsfenster im SANtricity Storage Manager entsperren.

   d. Sichern Sie die Konfigurationsdatenbank.

      Wenn beim Entfernen eines Controllers ein Problem auftritt, können Sie die gespeicherte Datei verwenden, um Ihre Konfiguration wiederherzustellen.

   e. Sammeln von Support-Daten für die Appliance

Das Erfassen von Supportdaten vor und nach dem Ersetzen einer Komponente stellt sicher, dass Sie einen vollständigen Satz von Protokollen an den technischen Support senden können, falls das Problem durch den Austausch nicht behoben wird.

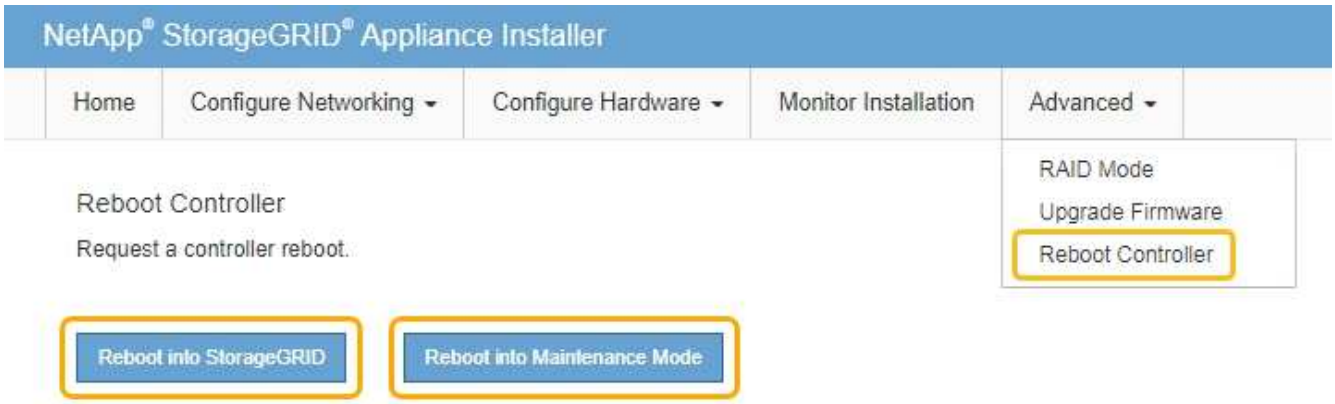
2. Wenn die StorageGRID Appliance in einem StorageGRID System ausgeführt wird, versetzen Sie den E5600SG Controller in den Wartungsmodus.

   "Versetzen einer Appliance in den Wartungsmodus"

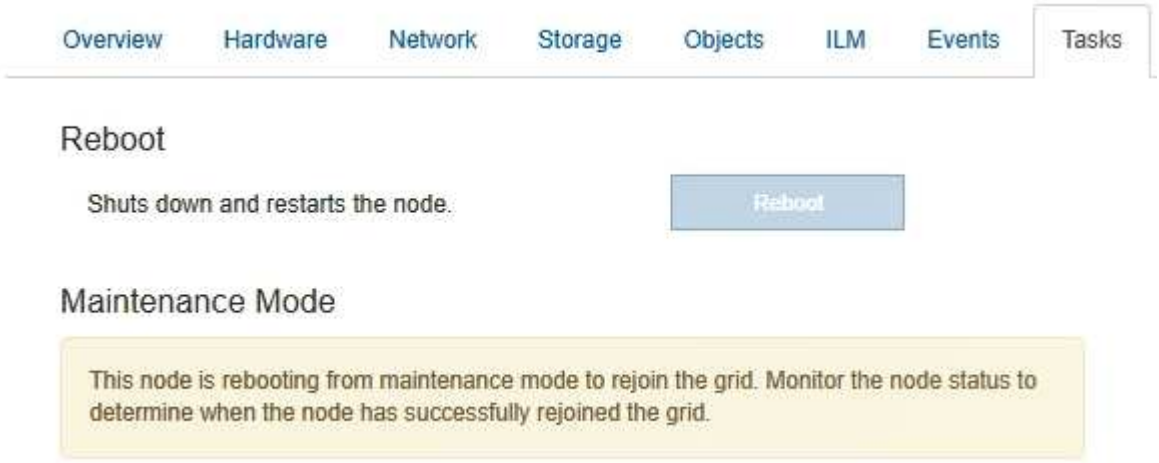
3. Wenn der E2700 Controller ausreichend funktioniert, um ein kontrolliertes Herunterfahren zu ermöglichen, bestätigen Sie, dass alle Operationen abgeschlossen wurden.
   a. Wählen Sie in der Titelleiste des Array Management-Fensters die Option **Monitor** > **Berichte** > **laufende Operationen** aus.
   b. Vergewissern Sie sich, dass alle Vorgänge abgeschlossen sind.
4. Befolgen Sie die Anweisungen im Ersatzverfahren für einen Simplex E2700 Controller, um die folgenden Schritte auszuführen:
   a. Beschriften Sie die Kabel, und ziehen Sie die Kabel ab.

      Um eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht oder treten.

   b. Entfernen Sie den fehlerhaften Controller aus dem Gerät.
   c. Entfernen Sie die Controllerabdeckung.
   d. Lösen Sie die Flügelschraube, und entfernen Sie die Batterie vom defekten Controller.
   e. Setzen Sie den Akku in den Ersatzcontroller ein, und bringen Sie die Controllerabdeckung wieder an.
   f. Setzen Sie den Ersatzcontroller in das Gerät ein.
   g. Ersetzen Sie die Kabel.
   h. Warten Sie, bis der E2700 Controller neu gestartet wurde. Vergewissern Sie sich, dass auf der 7-Segment-Anzeige ein Status von angezeigt wird `99`.
5. Wenn das Gerät gesicherte Laufwerke verwendet, importieren Sie den Sicherheitsschlüssel des Laufwerks.
6. 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.

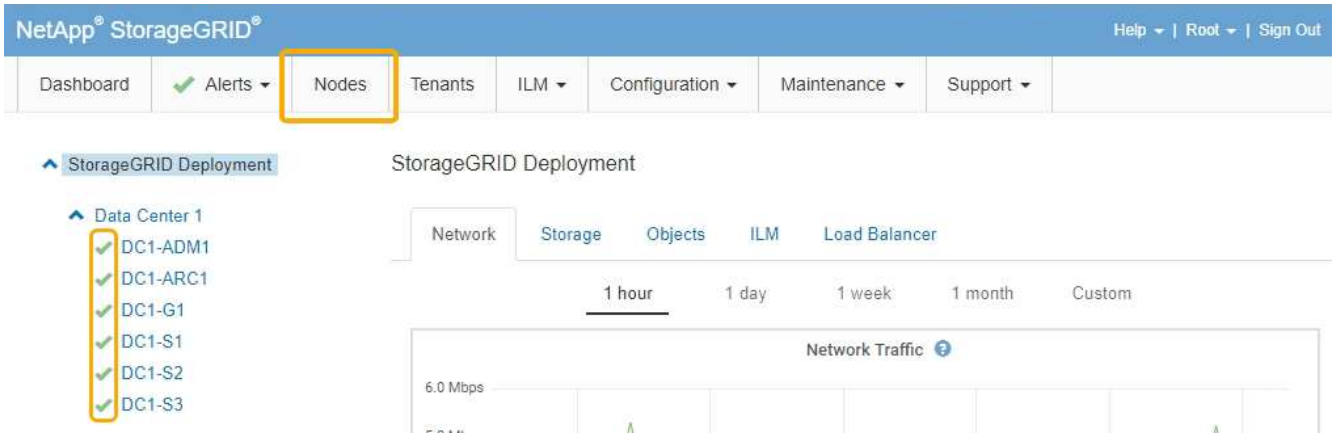


Während des Neustarts wird der folgende Bildschirm angezeigt:



Das Gerät wird neu gestartet und wieder in das Raster integriert. Dieser Vorgang kann bis zu 20 Minuten dauern.

7. 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 Registerkarte **Nodes** ein normaler Status angezeigt wird ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



8. Überprüfen Sie vom SANtricity Storage Manager, ob der neue Controller optimal ist, und sammeln Sie Support-Daten.

Verwandte Informationen

"Verfahren zum Austausch von Hardware der NetApp E-Series und EF-Series"

"NetApp Dokumentation: E2700 Serie"

Austauschen des E5600SG-Controllers

Möglicherweise müssen Sie den E5600SG-Controller austauschen.

Was Sie benötigen

Sie müssen Zugriff auf die folgenden Ressourcen haben:

- Informationen zum Austausch der E-Series Hardware auf der NetApp Support-Website unter +http://mysupport.netapp.com/["mysupport.netapp.com"^]
- E5600 Dokumentation auf der Support Site
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Wenn beide Controller ausreichend funktionieren, um eine kontrollierte Abschaltung zu ermöglichen, können Sie zuerst den E5600SG Controller herunterfahren, um die Verbindung zum E2700 Controller zu unterbrechen.

> ⓘ 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. Während Sie von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm für StorageGRID-Geräte zugreifen können, können Sie 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. Verwenden Sie einen antistatischen Schutz.
2. Beschriften Sie jedes Kabel, das an den E5600SG-Controller angeschlossen ist, damit Sie die Kabel korrekt wieder anschließen können.

   > ⓘ Um eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht oder treten. Die Kabel nicht enger als ein 5 cm (2 Zoll) Radius biegen.

3. Wenn das Gerät in den Wartungsmodus versetzt wurde, schalten Sie den E5600SG-Controller aus.
   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 E5600SG-Controller: + aus
`shutdown -h now`

4. Schalten Sie das Gehäuse aus und warten Sie, bis alle LED- und siebenSegment-Anzeigeaktivitäten auf der Rückseite des Controllers angehalten sind.
5. Entfernen Sie die Kabel.
6. Entfernen Sie den Controller wie in der Dokumentation des E5600SG-Controllers beschrieben.
7. Setzen Sie den neuen Controller ein, wie in der Dokumentation des E5600SG-Controllers beschrieben.
8. Ersetzen Sie alle Kabel.
9. Schalten Sie das Gehäuse wieder ein.
10. Überwachen Sie die sieben-Segment-Codes.
    - E2700 Controller:

      Der endgültige LED-Status lautet `99`.

    - E5600SG-Controller:

      Der endgültige LED-Status lautet `HA`.

11. Überwachen Sie den Status des Appliance Storage Node im Grid Manager.

    Vergewissern Sie sich, dass die Appliance Storage Nodes den erwarteten Status aufweisen.

Verwandte Informationen

"Verfahren zum Austausch von Hardware der NetApp E-Series und EF-Series"

"NetApp Dokumentation: E5600 Serie"

Austausch anderer Hardwarekomponenten

Möglicherweise müssen Sie ein Laufwerk, einen Lüfter, ein Netzteil oder einen Akku im StorageGRID-Gerät austauschen.

Was Sie benötigen

- Sie haben das Verfahren zum Austausch der E-Series Hardware.
- Das Gerät wurde in den Wartungsmodus versetzt, wenn Sie das Gerät beim Austausch der Komponenten herunterfahren müssen.

  "Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Zum Austausch eines Antriebs, des Power-Lüfterbehälter, des Ventilatorkanals, des Stromkanisters, der Batterie, Oder Laufwerkseinschub finden Sie in den Standardverfahren für die E2700 und E5600 Storage-Arrays. Konzentrieren Sie sich auf die Schritt-für-Schritt-Anleitung zum Entfernen und Austauschen der Hardware selbst. Viele der SANtricity Storage Manager Verfahren gelten nicht für eine Appliance.

SG5612 – Anweisungen zum Austausch von Komponenten

FRU	Siehe
Laufwerk	Folgen Sie den Schritten in der Anleitung zur E-Series, um ein Laufwerk in den Schäfchen E2600, E2700, E5400, E5500, E5600, 12 Laufwerke oder 24 Laufwerke zu ersetzen.
Lüfter-Behälter	Befolgen Sie die Schritte in der Anleitung zur E-Series, um einen Behälter mit einem defekten Lüfter im E5612 oder E5624-Controller-Laufwerksfach zu ersetzen
Batterie im E2700 Controller (Entfernen des Controllers erforderlich)	Befolgen Sie die Schritte unter "Austausch des E2700 Controllers", Aber installieren Sie den neuen Akku in der vorhandenen Steuerung.

Anweisungen für den Austausch von SG5660 Komponenten

FRU	Siehe
Laufwerk	Befolgen Sie die Schritte in der Anleitung zur E-Series, um ein Laufwerk in den Schäfchen E2660, E2760, E5460, E5560 oder E5660 zu ersetzen.
Leistungsbehälter	Befolgen Sie die Schritte in der Anleitung zur E-Series, um einen defekten Netzbehälter im E5660 Controller-Laufwerksfach zu ersetzen
Gebläsebehälter	Befolgen Sie die Schritte in der Anleitung zur E-Series, um einen Lüfterbehälter für fehlerhafte Lüfter im E5660 Controller-Laufwerksfach zu ersetzen
Batterie im E2700 Controller (Entfernen des Controllers erforderlich)	Befolgen Sie die Schritte unter "Austausch des E2700 Controllers", Aber installieren Sie den neuen Akku in der vorhandenen Steuerung.

Verwandte Informationen

"Verfahren zum Austausch von Hardware der NetApp E-Series und EF-Series"

"NetApp Dokumentation: E2700 Serie"

"NetApp Dokumentation: E5600 Serie"

Ändern der Link-Konfiguration des E5600SG-Controllers

Sie können die Ethernet-Link-Konfiguration des E5600SG-Controllers ändern. Sie können den Port Bond-Modus, den Netzwerk-Bond-Modus und die Verbindungsgeschwindigkeit ändern.

Was Sie benötigen

- Sie müssen den E5600SG-Controller in den Wartungsmodus versetzen. Wenn der Controller in den Wartungsmodus versetzt wird, wird die Verbindung zum E2700 Controller unterbrochen. Wenn eine StorageGRID Appliance in den Wartungsmodus versetzt wird, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

  "Versetzen einer Appliance in den Wartungsmodus"

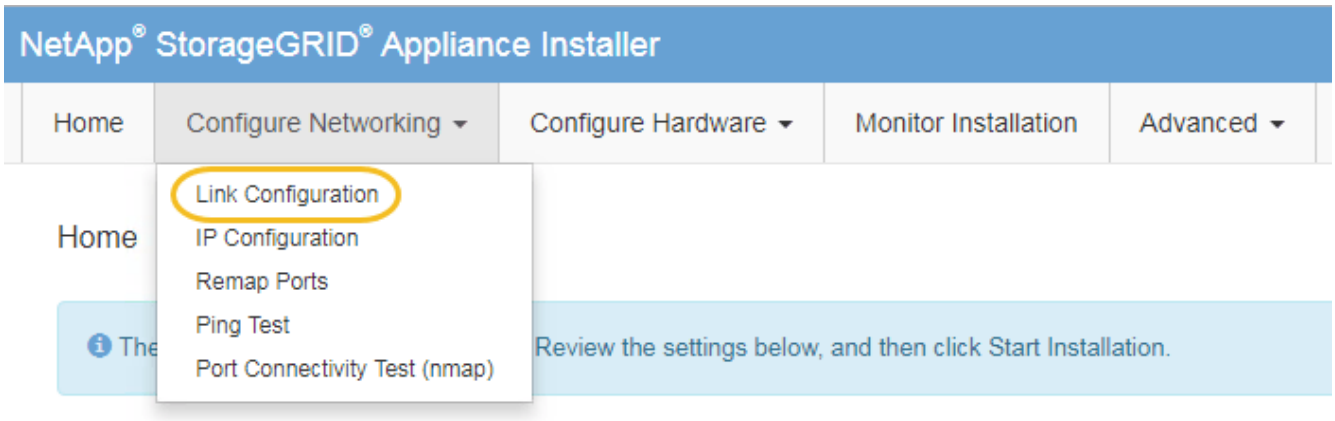
Über diese Aufgabe

Die Ethernet-Link-Konfiguration des E5600SG-Controllers 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 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.



1. Nehmen Sie die gewünschten Änderungen an der Verbindungskonfiguration vor.

   Weitere Informationen zu den Optionen finden Sie unter „`Konfigurieren von Netzwerkverbindungen`“.

2. 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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:
   `https://E5600SG_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 Anweisungen zum Konfigurieren von IP-Adressen.

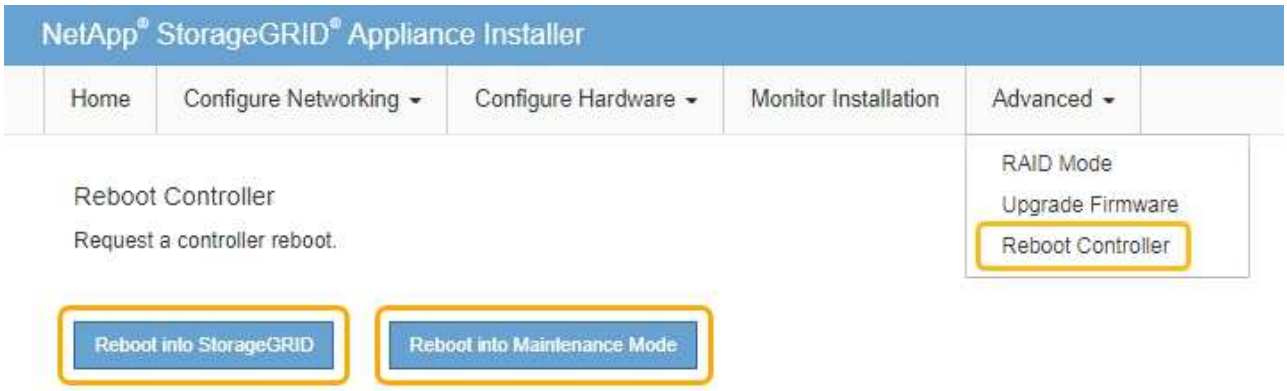
   "Einstellen der IP-Konfiguration"

3. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren** > **Ping-Test** aus.
4. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in Netzwerken zu prüfen, die möglicherweise von den in vorgenommenen Änderungen der Verbindungskonfiguration betroffen sind Verbindungskonfiguration ändern Schritt:

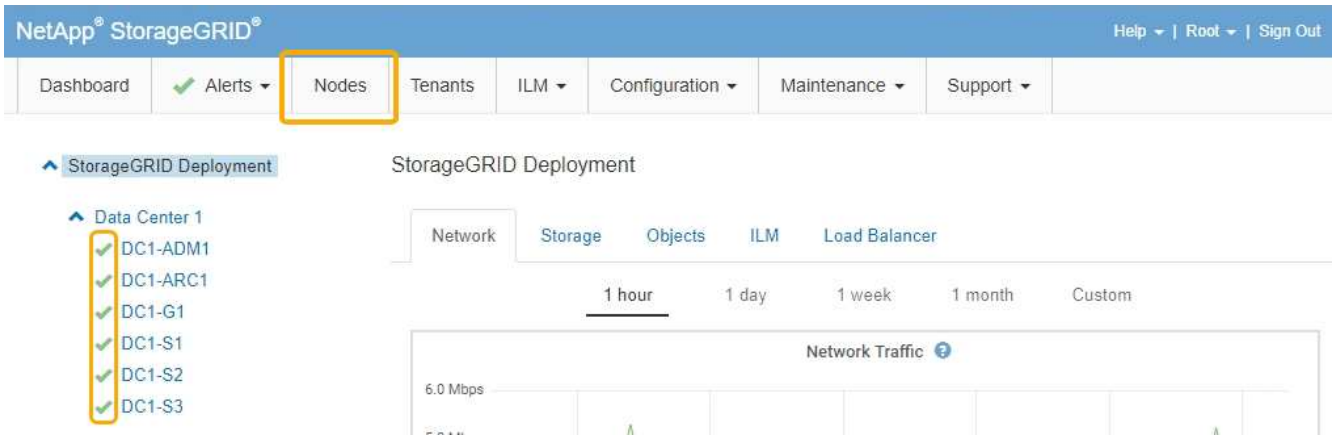
   Zusätzlich zu allen anderen Tests, die Sie durchführen möchten, bestätigen Sie, dass Sie die Grid-IP-Adresse des primären Admin-Knotens und die Grid-IP-Adresse von mindestens einem anderen Speicherknoten pingen können. Korrigieren Sie ggf. alle Probleme mit der Verbindungskonfiguration.

5. 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"Konfigurieren von Netzwerkverbindungen (SG5600)"

Ändern der MTU-Einstellung

Sie können die MTU-Einstellung ändern, die Sie beim Konfigurieren von IP-Adressen für den Appliance-Node zugewiesen haben.

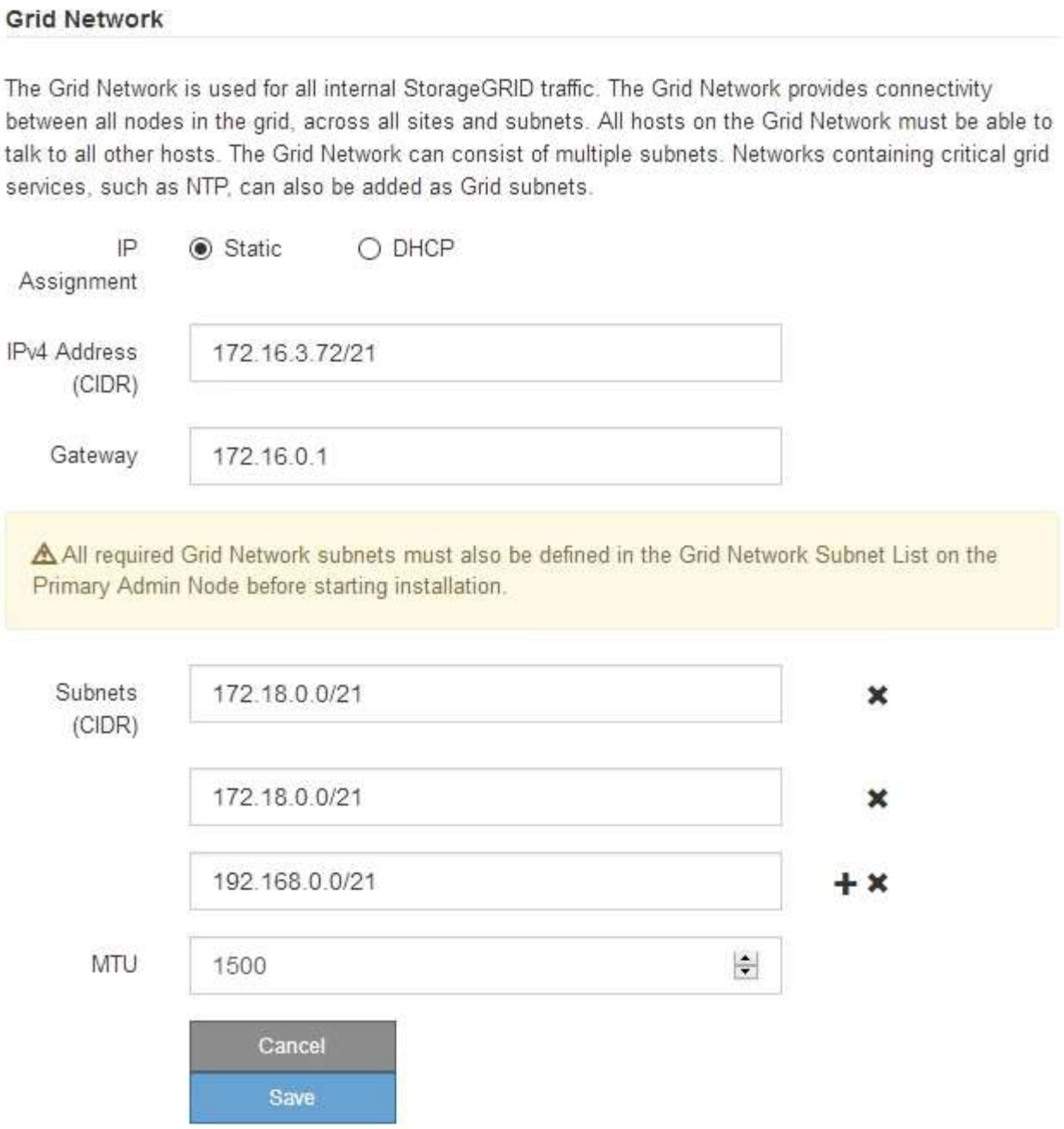
Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

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.



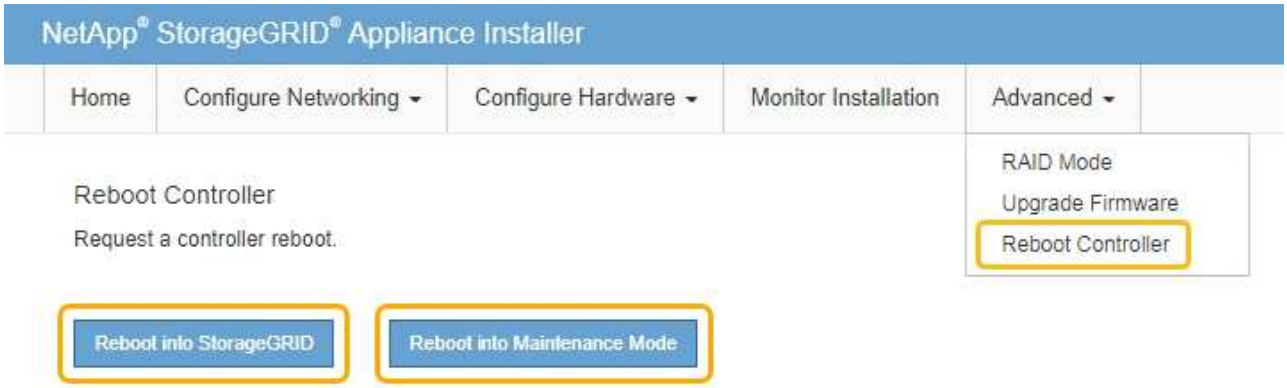
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch sein.

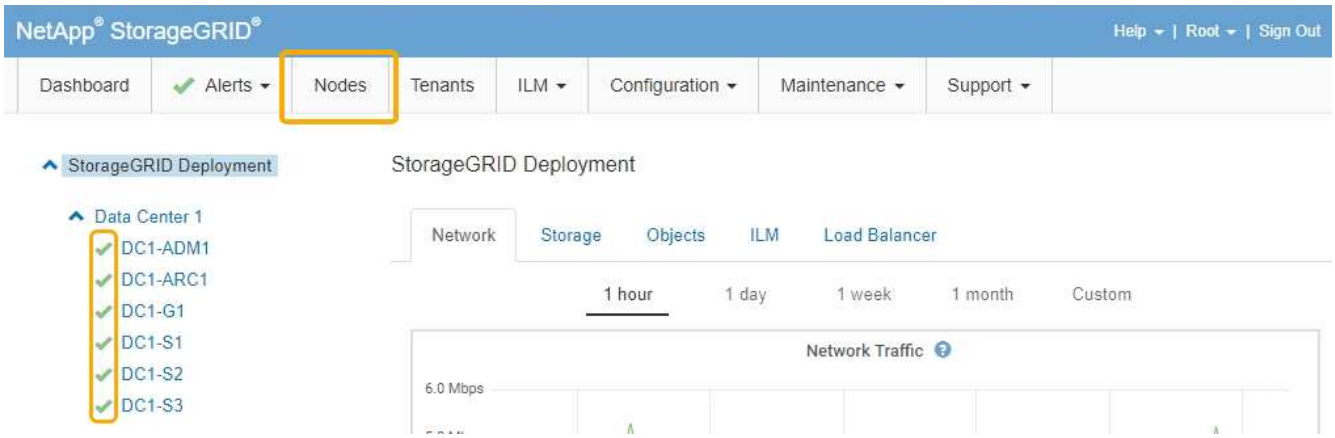
3. Wenn Sie mit den Einstellungen zufrieden sind, wählen Sie **Speichern**.
4. Booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option

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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Überprüfen der DNS-Serverkonfiguration

Sie können die DNS-Server (Domain Name System), die derzeit von diesem Appliance-Node verwendet werden, überprüfen und vorübergehend ändern.

Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Möglicherweise müssen Sie die DNS-Servereinstellungen ändern, wenn eine verschlüsselte Appliance sich nicht mit dem Verschlüsselungsmanagement-Server (KMS) oder dem KMS-Cluster verbinden kann, da der Hostname des 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 durchzuführen, geben Sie die DNS-Server im Grid Manager an (**Wartung** > **Netzwerk** > **DNS-Server**).

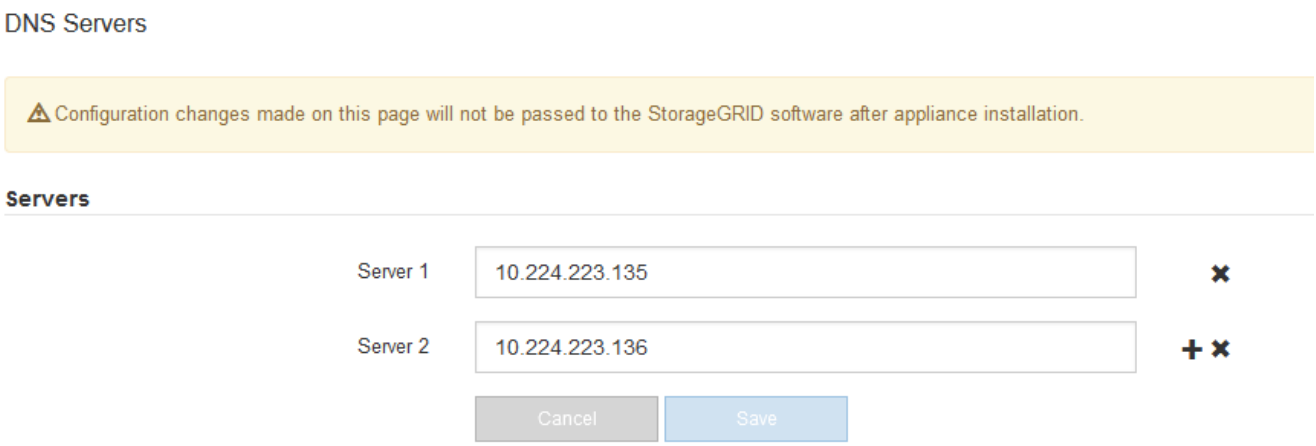
- Temporäre Änderungen an der DNS-Konfiguration sind nur für Node-verschlüsselte Appliances erforderlich, bei denen der KMS-Server mithilfe eines vollständig qualifizierten Domänennamens anstelle einer IP-Adresse für den Hostnamen definiert wird.
- Wenn eine Node-verschlüsselte Appliance über einen Domänennamen 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 Node keinen DNS-Server für das Grid erreichen kann oder wenn die DNS-Einstellungen für das gesamte Grid geändert wurden, wenn ein Node-verschlüsselter Appliance-Node offline war, kann der Node keine Verbindung mit dem KMS herstellen. Verschlüsselte Daten auf der Appliance können erst entschlüsselt werden, wenn das DNS-Problem behoben ist.

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 Node offline war, kann der Node nach seinem Wechsel wieder online den KMS nicht erreichen, 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.



3. Ändern Sie bei Bedarf die DNS-Server.

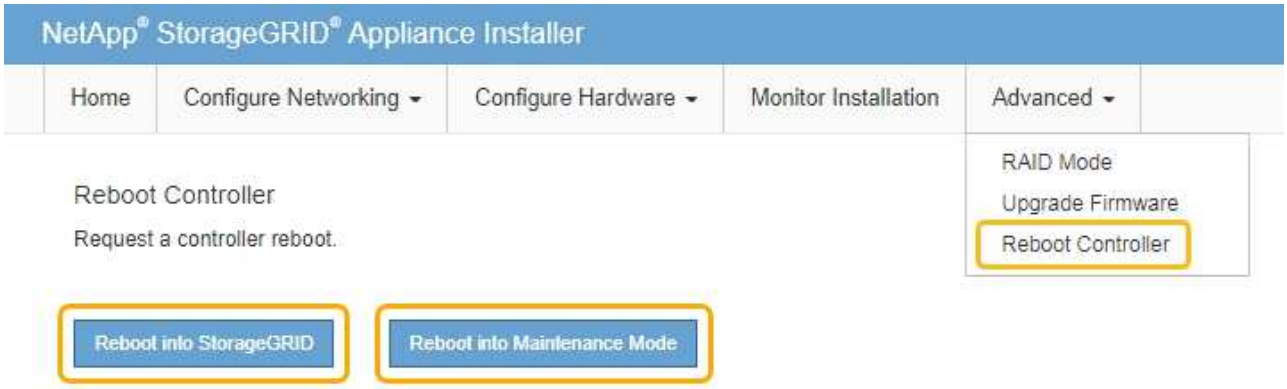
> Änderungen an den DNS-Einstellungen erfolgen temporär und gehen verloren, wenn Sie den Wartungsmodus beenden.

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.

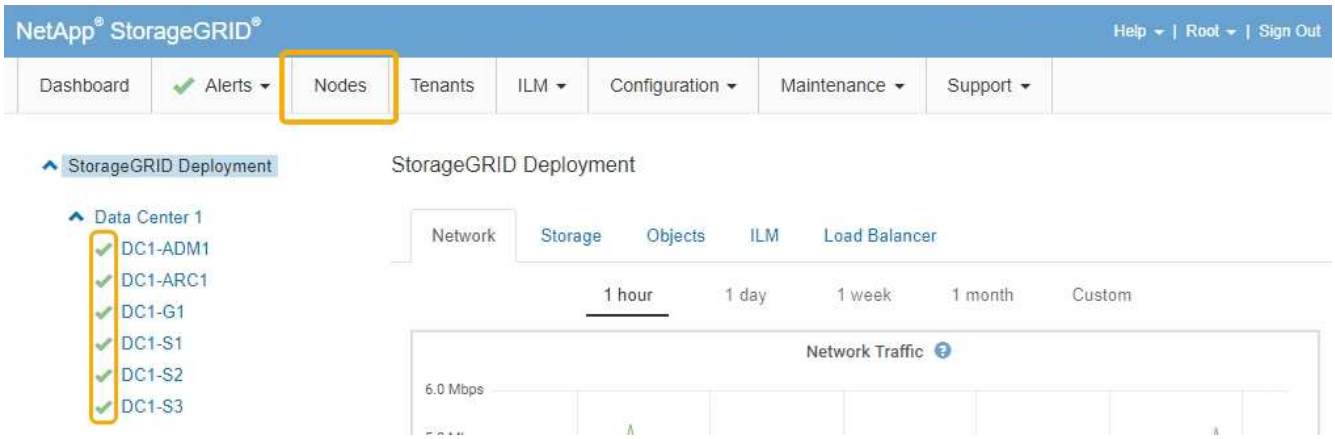
5. Nachdem die Node-Daten entschlüsselt wurden, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 befand.

   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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Monitoring 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).

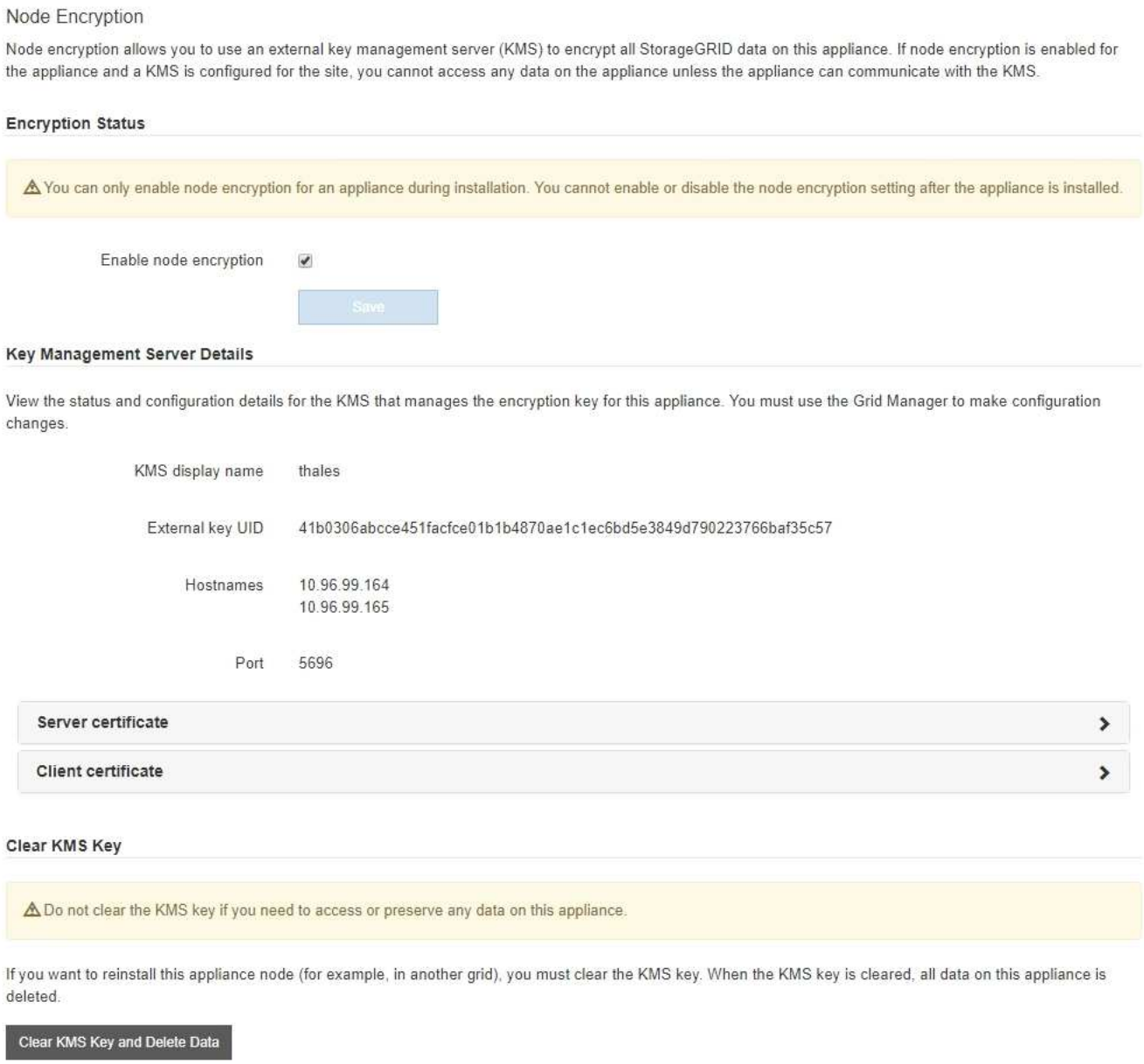
Was Sie benötigen

- Die Node-Verschlüsselung muss während der Installation für die Appliance aktiviert sein. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht aktivieren.
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Hardware konfigurieren** > **Node-Verschlüsselung**.



Die Seite Node Encryption umfasst die folgenden 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.
  - Wenn Sie Probleme mit den Zertifikaten selbst beheben möchten, z. B. die Verlängerung abgelaufener Zertifikate, lesen Sie die Informationen zu KMS in den Anweisungen zur Verwaltung von StorageGRID.
  - Wenn bei der Verbindung zu KMS-Hosts unerwartete Probleme auftreten, überprüfen Sie, ob die DNS-Server (Domain Name System) korrekt sind und das Netzwerk der Appliance korrekt konfiguriert ist.

    "Überprüfen der DNS-Serverkonfiguration"

- 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. Sie müssen den KMS-Schlüssel löschen, bevor Sie die Appliance in einem anderen StorageGRID-System installieren können.

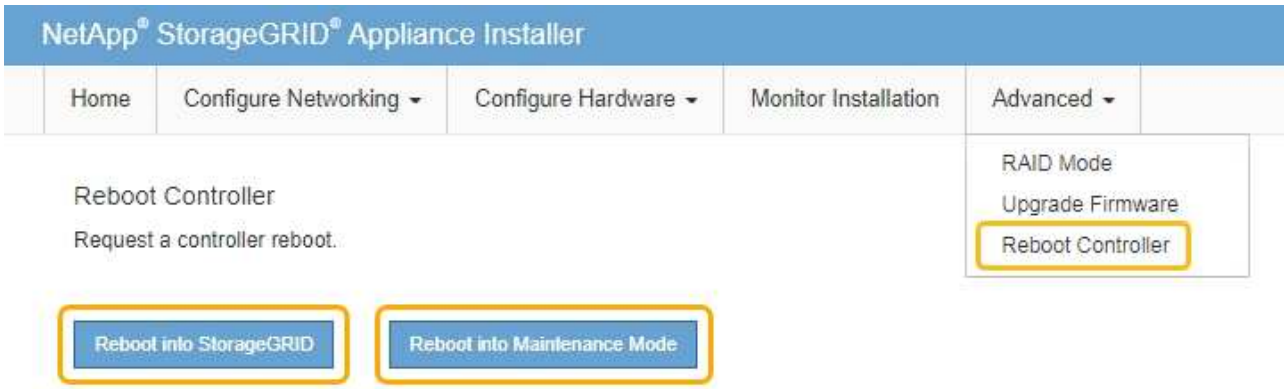
"Löschen der Konfiguration des Schlüsselverwaltungsservers"

Durch das Löschen der KMS-Konfiguration werden Daten von der Appliance gelöscht, sodass dauerhaft kein Zugriff darauf besteht. Diese Daten können nicht wiederhergestellt werden.

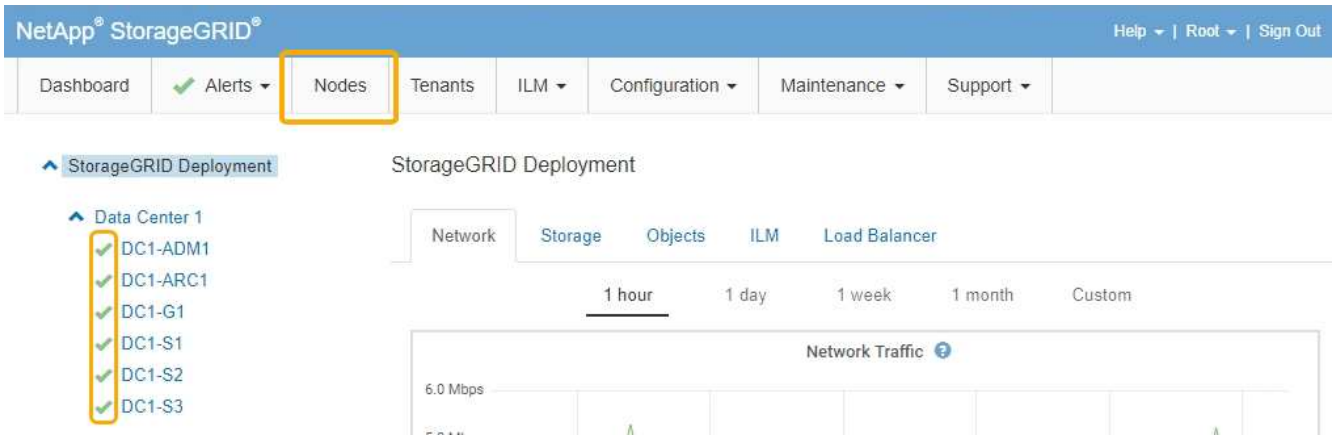
2. Wenn Sie den Status der Node-Verschlüsselung überprüfen, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

◦ 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Löschen der Konfiguration des Schlüsselverwaltungsservers

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.

Was Sie benötigen

Wenn Daten auf der Appliance aufbewahrt werden müssen, müssen Sie einen Node außer Betrieb nehmen, 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.

Den Node muss deaktiviert werden, um alle in ihm enthaltenen Daten auf anderen Nodes in StorageGRID zu verschieben. Anweisungen zur Ausmusterung von Grid-Nodes finden Sie in den Angaben zu Recovery und Wartung.

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 Vorgang 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 eine Neuinstallation eines Appliance-Node in einem StorageGRID-System planen, das denselben KMS-Schlüssel verwendet.

- 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.

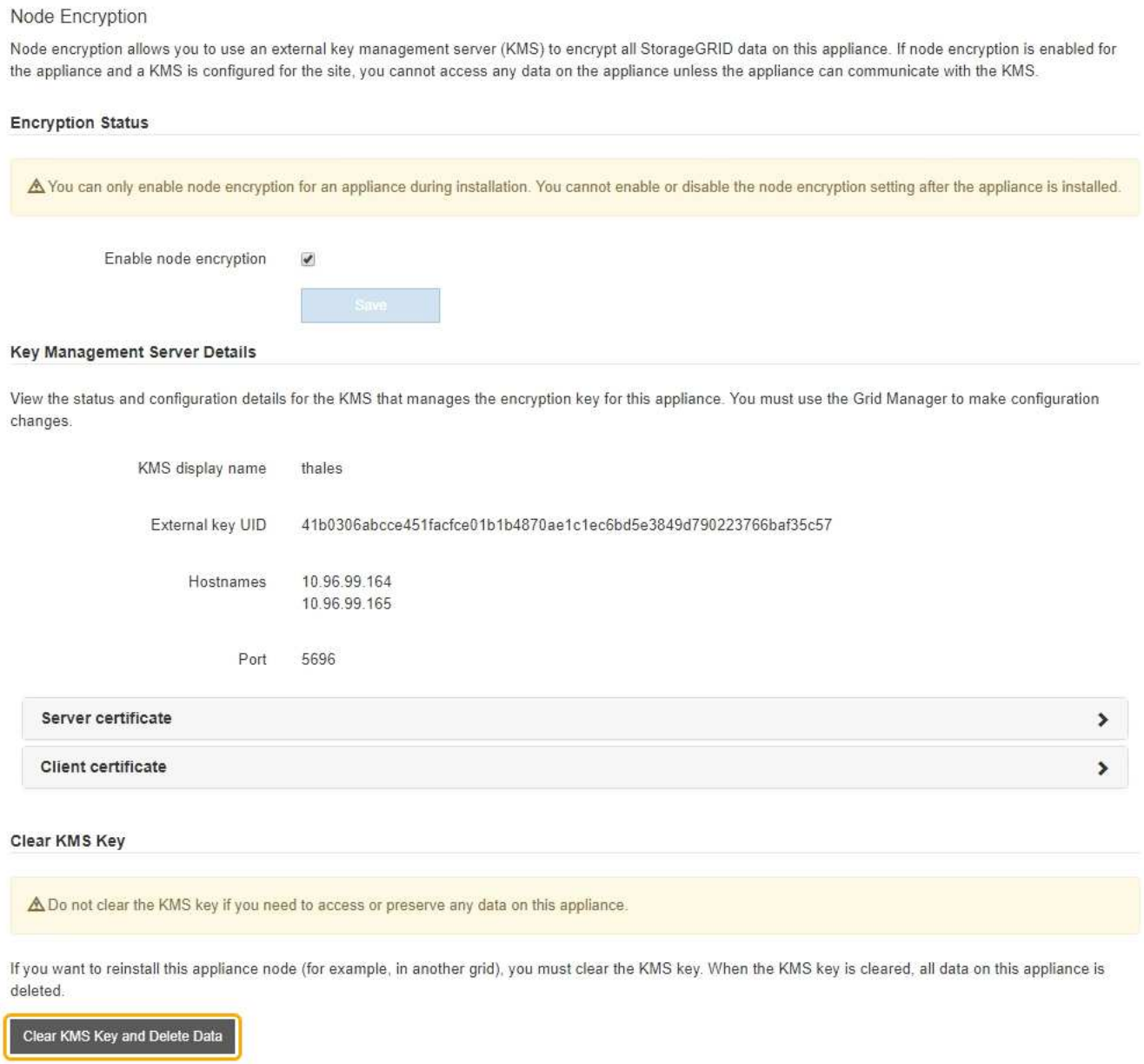
Schritte

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.

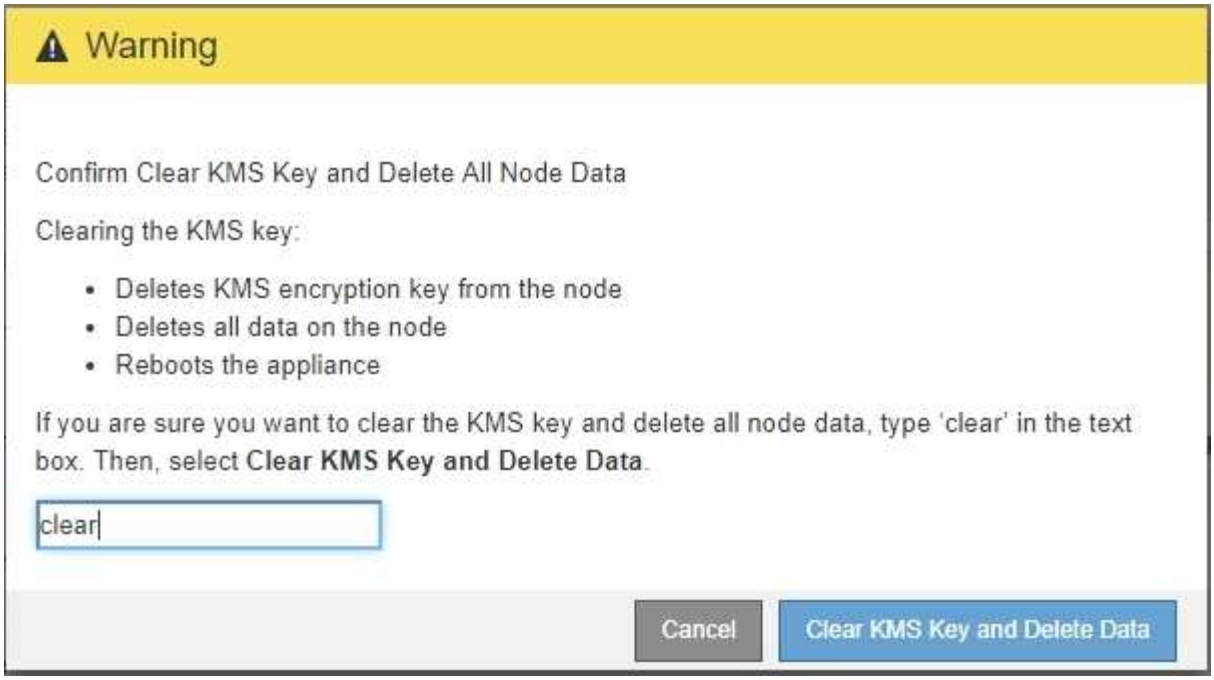
   Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

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` + und wählen Sie **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. Informationen zur Vorbereitung einer Appliance für die Neuinstallation finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Verwandte Informationen

"StorageGRID verwalten"

"Verwalten Sie erholen"

SG100- und SG1000-Services-Appliances

Lesen Sie, wie Sie die StorageGRID SG100- und SG1000-Appliances installieren und warten.

- "SG100- und SG1000-Geräte im Überblick"
- "SG100- und SG1000-Applikationen"
- "Übersicht über Installation und Implementierung"
- "Installation wird vorbereitet"
- "Installieren der Hardware"
- "Konfigurieren von StorageGRID-Verbindungen"
- "Konfigurieren der BMC-Schnittstelle"
- "Optional: Aktivieren der Node-Verschlüsselung"
- "Implementieren eines Service-Appliance-Nodes"
- "Fehlerbehebung bei der Hardwareinstallation"
- "Warten des Geräts"

SG100- und SG1000-Geräte im 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.

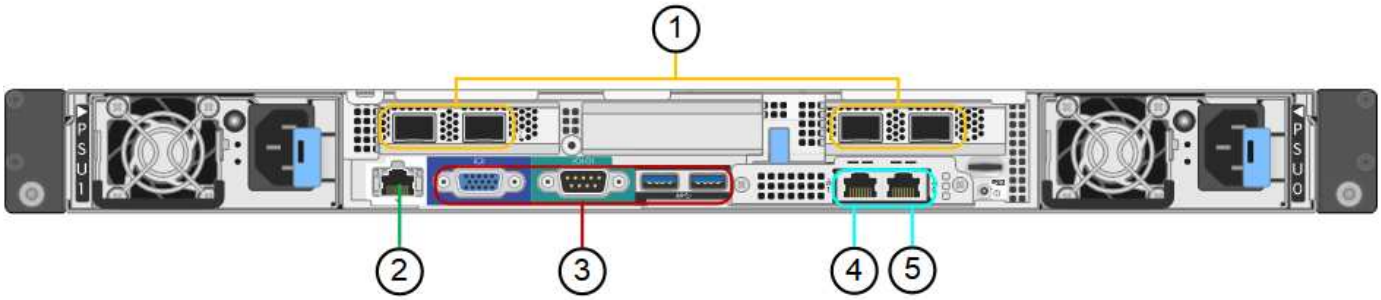
Von der Vorderseite sind die beiden Geräte identisch, mit Ausnahme des Produktnamens auf der Blende.

Die zwei über die orangefarbene Kontur angezeigten Solid State Drives (SSDs) werden zum Speichern des StorageGRID Betriebssystems verwendet und werden mithilfe von RAID1 für Redundanz 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.

Anschlüsse auf der Rückseite des SG100

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des SG100.

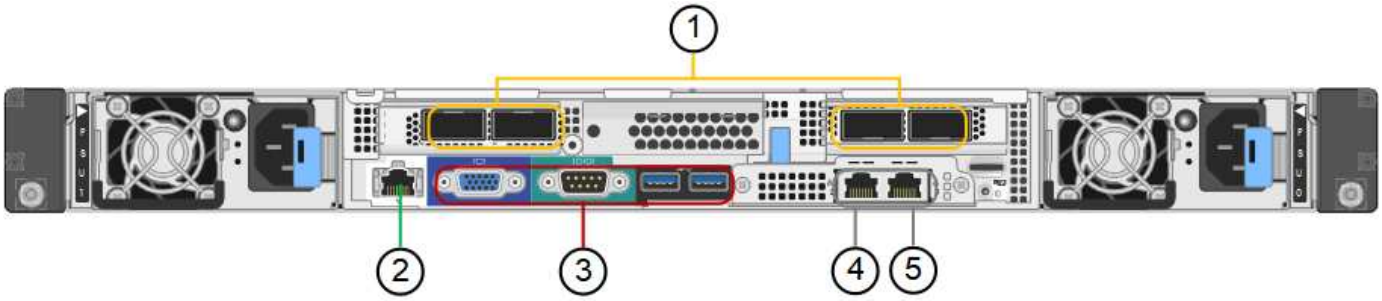


	Port	Typ	Nutzung
1	Netzwerkanschlüsse 1-4	10/25-GbE, basierend auf Kabel- oder SFP-Transceiver-Typ (SFP28 und SFP+ Module werden unterstützt), Switch-Geschwindigkeit und konfigurierter Link-Geschwindigkeit	Stellen Sie eine Verbindung zum Grid-Netzwerk und dem Client-Netzwerk für StorageGRID her.
2	BMC-Management-Port	1 GbE (RJ-45)	Stellen Sie eine Verbindung mit dem Management Controller der Hauptplatine des Geräts her.
3	Diagnose- und Supportports	• 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.

	Port	Typ	Nutzung
5	Admin – Netzwerkanschluss 2	1 GbE (RJ-45)	Optionen: • 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.

Anschlüsse auf der Rückseite des SG1000

Diese Abbildung zeigt die Anschlüsse auf der Rückseite des SG1000.



	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.
2	BMC-Management-Port	1 GbE (RJ-45)	Stellen Sie eine Verbindung mit dem Management Controller der Hauptplatine des Geräts her.

	Port	Typ	Nutzung
3	Diagnose- und Supportports	• 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)	Optionen: • 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 Service-Appliances SG100 und SG1000 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, fallen CLB-Ports (Connection Load Balancer) und reine Admin-Node-Ports kein Failover an. Anweisungen zum Konfigurieren von HA-Gruppen finden Sie in den Anweisungen für das Verwalten von StorageGRID.

> Der CLB-Service ist veraltet.

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.

Verwandte Informationen

"StorageGRID verwalten"

Übersicht über Installation und Implementierung

Bei der ersten Implementierung von StorageGRID können Sie eine oder mehrere StorageGRID Services Appliances installieren oder Nodes von Services-Appliances später im Rahmen einer Erweiterung hinzufügen.

Was Sie benötigen

Ihr StorageGRID System verwendet die erforderliche Version der StorageGRID Software.

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

Installations- und Implementierungsaufgaben

Die Vorbereitung und das Hinzufügen einer StorageGRID Appliance zum Grid umfasst vier Hauptschritte:

1. Installation vorbereiten:
   - Vorbereiten des Installationsstandorts
   - Auspacken der Schachteln und Prüfen des Inhalts
   - Zusätzliche Ausrüstung und Werkzeuge
   - Netzwerkkonfiguration wird überprüft
   - Optional: Konfiguration eines externen Verschlüsselungsmanagement-Servers (KMS), wenn Sie alle Appliance-Daten verschlüsseln möchten. Weitere Informationen zum externen Verschlüsselungsmanagement finden Sie in der Anleitung zur Administration von StorageGRID.

2. Installieren der Hardware:
    - Registrieren der Hardware
    - Installieren des Geräts in einem Schrank oder Rack
    - Verkabeln Sie das Gerät
    - Anschließen des Netzkabels und Einstecken des Netzkabels
    - Anzeigen von Boot-Statuscodes
3. Konfigurieren der Hardware:
    - Zugriff auf das Installationsprogramm von StorageGRID Appliance und Konfiguration der für die Verbindung mit StorageGRID-Netzwerken erforderlichen Link- und Netzwerk-IP-Einstellungen
    - Zugriff auf die Schnittstelle des Baseboard Management Controller (BMC) auf der Appliance.
    - Optional: Aktivieren der Node-Verschlüsselung, wenn Sie zur Verschlüsselung von Appliance-Daten einen externen KMS verwenden möchten.
4. Implementieren eines Appliance-Gateways oder eines Admin-Node

    Nach der Installation und Konfiguration der Appliance-Hardware können Sie die Appliance als Gateway-Node und als Admin-Node in einem StorageGRID-System bereitstellen. Sowohl die SG100- als auch die SG1000-Appliances können gleichzeitig als Gateway-Nodes und Admin-Nodes (primär und nicht primär) betrieben werden.

Aufgabe	Anweisungen
Appliance-Gateway oder Admin-Node in einem neuen StorageGRID System implementieren	"Implementieren eines Service-Appliance-Nodes"
Hinzufügen eines Appliance-Gateways oder eines Admin-Node zu einem vorhandenen StorageGRID-System	"Anweisungen zum erweitern eines StorageGRID-Systems"
Implementieren eines Appliance-Gateways oder eines Admin-Nodes im Rahmen einer Node-Recovery-Operation	"Anweisungen zur Wiederherstellung und Wartung"

Verwandte Informationen

"Installation wird vorbereitet"

"Installieren der Hardware"

"Konfigurieren von StorageGRID-Verbindungen"

"Erweitern Sie Ihr Raster"

"Verwalten Sie erholen"

"StorageGRID verwalten"

Installation wird vorbereitet

Die Vorbereitung der Installation einer StorageGRID Appliance umfasst die Vorbereitung des Standorts und den Erwerb aller erforderlichen Hardware, Kabel und Tools. Außerdem sollten Sie IP-Adressen und Netzwerkinformationen erfassen.

Schritte

- "Vorbereiten des Standorts (SG100 und SG1000)"
- "Auspacken der Boxen (SG100 und SG1000)"
- "Beschaffung zusätzlicher Geräte und Werkzeuge (SG100 und SG1000)"
- "Anforderungen an einen Webbrowser"
- "Überprüfen von Appliance-Netzwerkverbindungen"
- "Sammeln von Installationsinformationen (SG100 und SG1000)"

Vorbereiten des Standorts (SG100 und SG1000)

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. Weitere Informationen finden Sie im NetApp Hardware Universe.
2. Stellen Sie sicher, dass Ihr Standort die richtige Spannung der Wechselstromversorgung bereitstellt (im Bereich von 120 bis 240 Volt Wechselstrom).
3. Passen Sie zu 48.3 Shelfs dieser Größe (ohne Kabel) ein 19-cm-Gehäuse oder -Rack an:

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.

Verwandte Informationen

"NetApp Hardware Universe"

"NetApp Interoperabilitäts-Matrix-Tool"

Auspacken der Boxen (SG100 und SG1000)

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

Appliance-Hardware

- **SG100 oder SG1000**

- **Rail Kit mit Anweisungen**

Stromkabel

Die im Lieferumfang der StorageGRID Appliance aufgeführten Netzkabel sind enthalten:

- * Zwei Netzkabel für Ihr Land*

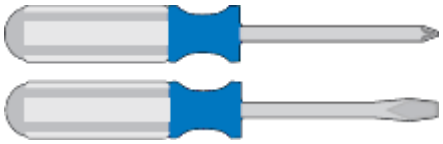
  Ihr Schrank verfügt möglicherweise über spezielle Netzkabel, die Sie anstelle der Netzkabel verwenden, die Sie zur Einheit mit dem Gerät anschließen.

Beschaffung zusätzlicher Geräte und Werkzeuge (SG100 und SG1000)

Vergewissern Sie sich vor der Installation der StorageGRID Appliance, dass alle zusätzlichen Geräte und Tools zur Verfügung stehen, die Sie benötigen.

Sie benötigen die folgende zusätzliche Ausrüstung für die Installation und Konfiguration der Hardware:

- **Schraubendreher**

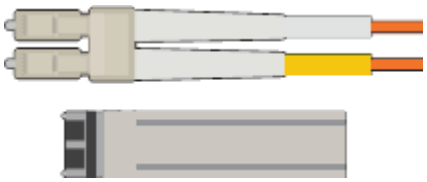


  Phillips Nr. 2 Schraubendreher

  Mittlerer Schlitzschraubendreher

- **ESD-Handgelenkschlaufe**

- **Optische Kabel und Transceiver**



  - Kabel
    - Twinax/Kupferkabel (1 bis 4)

      Oder

    - Glasfaser/optisch (1 bis 4)
  - 1 bis 4 dieser Transceiver/Adapter je nach Verbindungsgeschwindigkeit (gemischte Geschwindigkeiten werden nicht unterstützt)
    - SG100:

Verbindungsgeschwindigkeit (GbE)	Erforderliche Ausrüstung
10	SFP+-Transceiver
25	SFP28-Transceiver

    - SG1000:

Verbindungsgeschwindigkeit (GbE)	Erforderliche Ausrüstung
10	QSFP-to-SFP Adapter (QSA) und SFP+ Transceiver
25	QSFP-to-SFP Adapter (QSA) und SFP28-Transceiver
40	QSFP+-Transceiver
100	QFSP28-Transceiver

- * RJ-45 (Cat5/Cat5e/Cat6/Cat6a) Ethernet-Kabel*

- **Service-Laptop**

Unterstützter Webbrowser

1-GbE-Port (RJ-45

Einige Ports unterstützen möglicherweise keine 10/100 Ethernet-Geschwindigkeiten.

- **Optionale Werkzeuge**

Kraftbohrer mit Kreuzschlitz

Taschenlampe

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Überprüfen von Appliance-Netzwerkverbindungen

Vor der Installation der StorageGRID Appliance sollten Sie wissen, welche Netzwerke mit der Appliance verbunden werden können.

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.
- **BMC-Managementnetzwerk für die Services-Appliance:** Dieses Netzwerk bietet Zugriff auf den Baseboard-Management-Controller im SG100 und SG1000, Appliances, mit denen Sie die Hardwarekomponenten 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.

Verwandte Informationen

"Sammeln von Installationsinformationen (SG100 und SG1000)"

"Verkabelung der Appliance SG100 und SG1000)"

"Netzwerkrichtlinien"

"Gittergrundierung"

Port Bond-Modi für die SG100- und SG1000-Geräte

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.

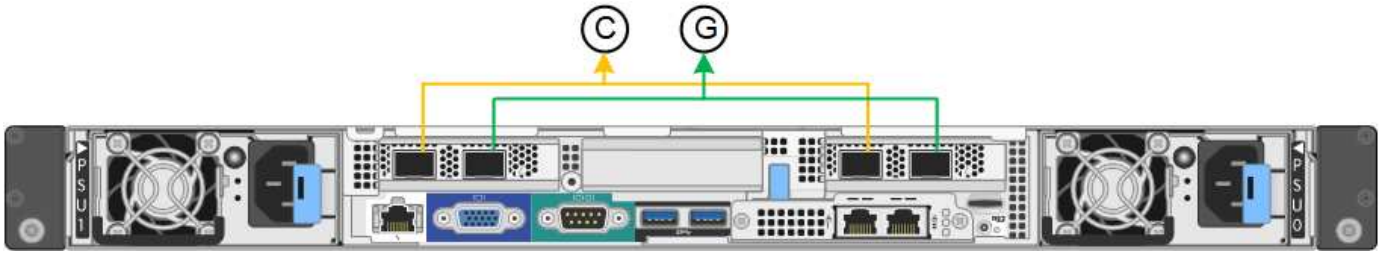
Netzwerk-Bond-Modi

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.

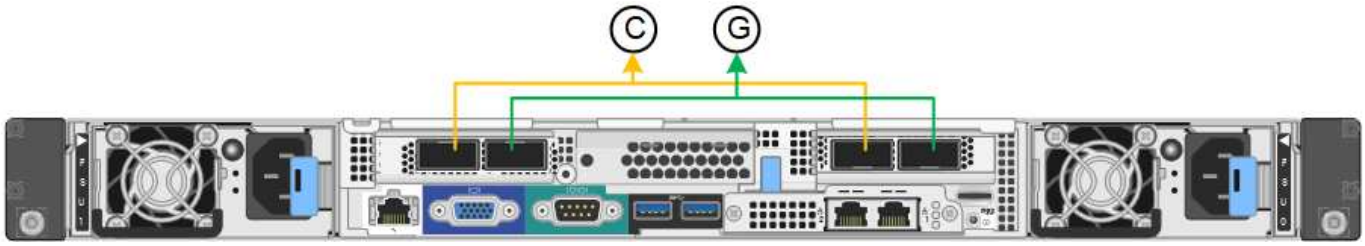
Bond-Modus mit festem Port

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

SG100 Festanschluss-Modus



SG1000 Festanschlussmodus



	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.

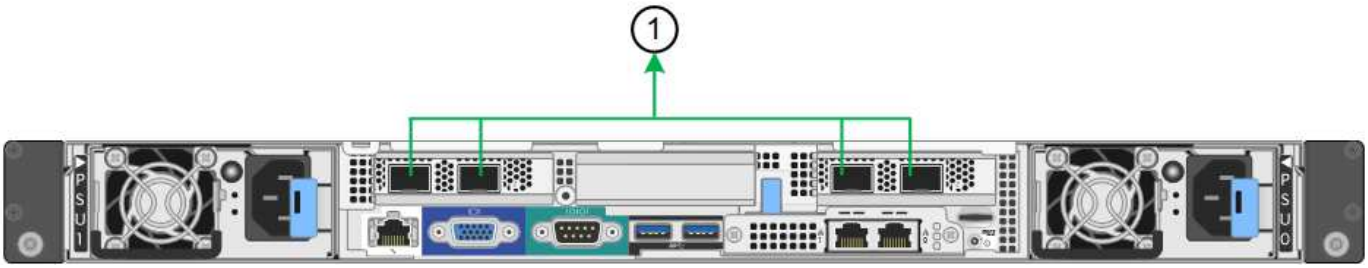
- Im aktiv-Backup-Modus (Standard) ist jeweils nur ein Port aktiv. Wenn der aktive Port ausfällt, stellt sein Backup-Port automatisch eine Failover-Verbindung bereit. Port 4 bietet einen Sicherungspfad für Port 2 (Grid Network), und Port 3 stellt einen Sicherungspfad für Port 1 (Client Network) bereit.
- 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.

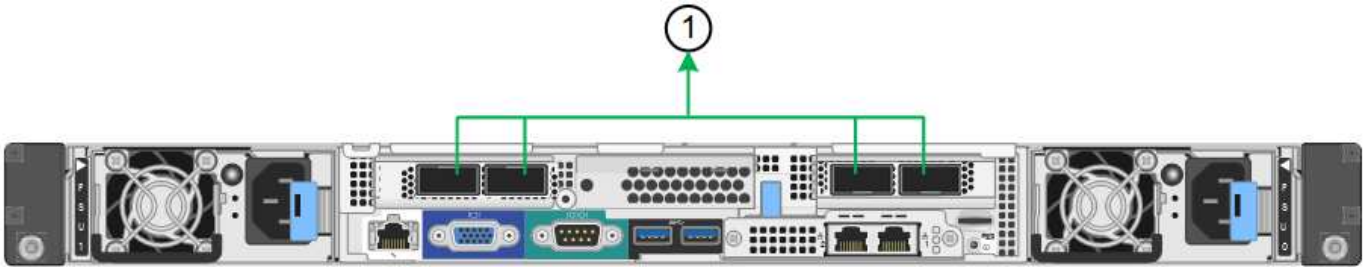
Bond-Modus für aggregierten Ports

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

SG100 Aggregat-Port-Bond-Modus



SG1000 Aggregat-Port-Bond-Modus



	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 müssen wissen, wie die Switches konfiguriert werden, um VLAN, LACP und MLAG zu verwenden.

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.

Netzwerk-Bond-Modi für die 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.

SG100 Netzwerkverwaltungs-Ports

SG1000 Netzwerk-Management-Ports

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.

	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).

Sammeln von Installationsinformationen (SG100 und SG1000)

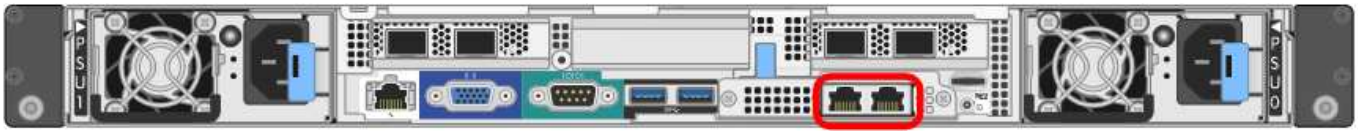
Bei der Installation und Konfiguration der StorageGRID Appliance sind Entscheidungen

zu treffen und Informationen zu Ethernet Switch-Ports, IP-Adressen sowie zu Port- und Netzwerk-Bond-Modi zu sammeln. Notieren Sie die erforderlichen Informationen für jedes Netzwerk, das Sie mit der Appliance verbinden. Diese Werte sind für die Installation und Konfiguration der Hardware erforderlich.

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-Anschlüsse*



SG1000 RJ-45-Anschlüsse

Verwaltungs- und Wartungsanschlüsse

Erforderliche Informationen	Ihr Wert
Admin-Netzwerk aktiviert	Bitte auswählen: • Nein • Ja (Standard)
Netzwerk-Bond-Modus	Bitte auswählen: • 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)	

Erforderliche Informationen	Ihr Wert
MAC-Adresse für den Netzwerkport Admin **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-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.	• 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.	• 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.

Netzwerkverbindungen

Erforderliche Informationen	Ihr Wert
Verbindungsgeschwindigkeit	Wählen Sie für das SG100 eine der folgenden Optionen aus: • Auto (Standard) • 10 GBitE • 25 GBitE Wählen Sie für den SG1000 eine der folgenden Optionen aus: • Auto (Standard) • 10 GBitE • 25 GBitE • 40 GBitE • 100 GBitE **Hinweis:** für die SG1000-, 10- und 25-GbE-Geschwindigkeiten sind QSA-Adapter erforderlich.
Port Bond-Modus	Bitte auswählen: • 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.

Grid-Netzwerkverbindungen

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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	• 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.	• 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.

Client-Netzwerkverbindungen

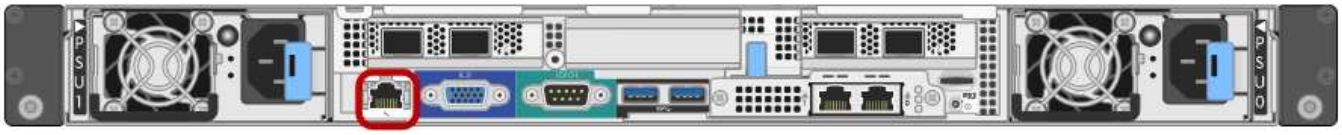
Erforderliche Informationen	Ihr Wert
Client-Netzwerk aktiviert	Bitte auswählen: • Nein (Standard) • Ja.

Erforderliche Informationen	Ihr Wert
Netzwerk-Bond-Modus	Bitte auswählen: • Aktiv/Backup (Standard) • LACP (802.3ad)
VLAN-Tagging aktiviert	Bitte auswählen: • 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	• 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.	• 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).

- SG100 BMC Management Port*



SG1000 BMC-Management-Port

- BMC-Management-Netzwerkverbindungen*

Erforderliche Informationen	Ihr Wert
Ethernet-Switch-Port Sie stellen eine Verbindung zum BMC-Management-Port her (im Diagramm eingekreist).	

Erforderliche Informationen	Ihr Wert
DHCP-zugewiesene IP-Adresse für das BMC-Managementnetzwerk, sofern nach dem Einschalten verfügbar	• IPv4-Adresse (CIDR): • Gateway:
Statische IP-Adresse, die Sie für den BMC-Verwaltungsport verwenden möchten	• IPv4-Adresse (CIDR): • Gateway:

Verwandte Informationen

"SG100- und SG1000-Geräte im Überblick"

"Verkabelung der Appliance SG100 und SG1000)"

"StorageGRID-IP-Adressen werden konfiguriert"

Installieren der Hardware

Die Hardware-Installation umfasst die Installation des Geräts in einem Schrank oder Rack, den Anschluss der Kabel und den Strom-Einsatz.

Schritte

- "Registrieren der Hardware"
- "Installieren des Geräts in einem Schrank oder Rack (SG100 und SG1000)"
- "Verkabelung der Appliance SG100 und SG1000)"
- "Anschließen von Netzkabeln und Einschalten der Stromzufuhr (SG100 und SG1000)"
- "Anzeigen von Statusanzeigen an den SG100- und SG1000-Geräten"

Registrieren der Hardware

Die Registrierung der Appliance-Hardware bietet Support-Vorteile.

Schritte

1. Suchen Sie die Seriennummer des Gehäuses für das Gerät.

   Sie finden die Nummer auf dem Packzettel, in Ihrer Bestätigungs-E-Mail oder auf dem Gerät nach dem Auspacken.

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	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.
Neuer NetApp Kunde	a. Klicken Sie auf **Jetzt registrieren** und erstellen Sie ein Konto. b. Wählen Sie **Produkte** > **Produkte Registrieren**. c. Geben Sie die Seriennummer des Produkts und die angeforderten Details ein. Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.

Installieren des Geräts in einem Schrank oder Rack (SG100 und SG1000)

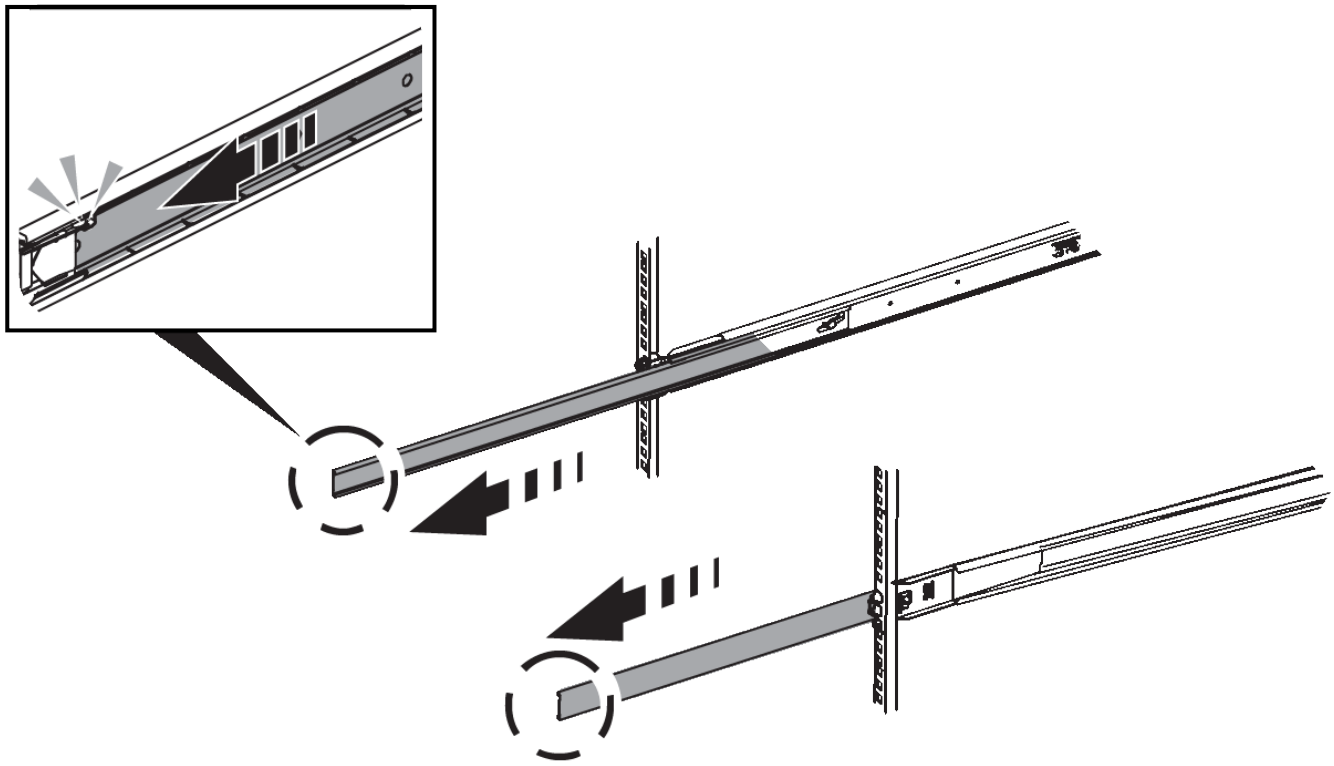
Sie müssen einen Satz Schienen für das Gerät in Ihrem Schrank oder Rack installieren und das Gerät dann auf die Schienen schieben.

Was Sie benötigen

- 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.

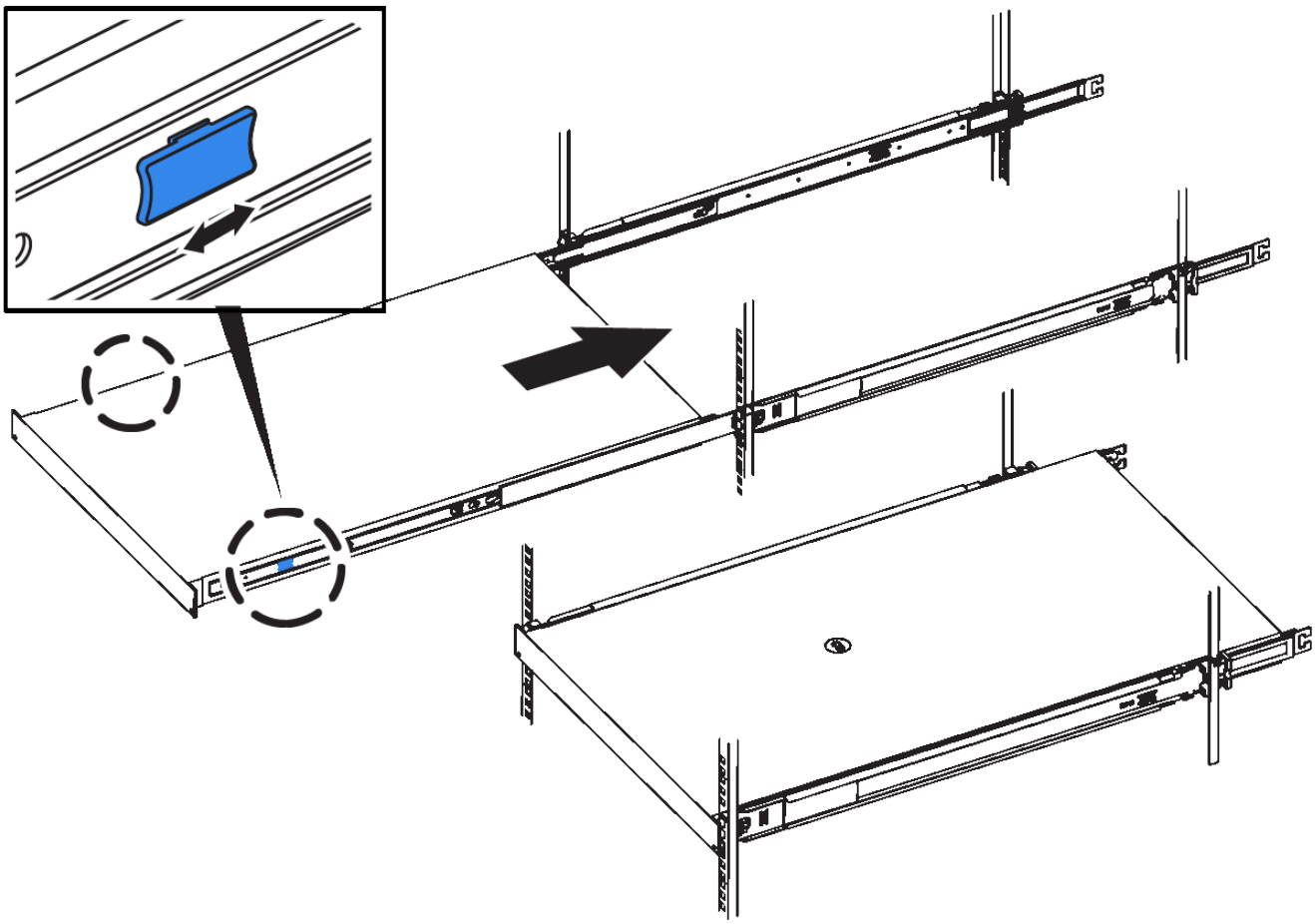
Schritte

1. Befolgen Sie die Anweisungen für den Schienensatz, um die Schienen in Ihrem Schrank oder Rack zu installieren.
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 die blauen Verriegelungen auf beiden Seiten des Gehäuses, um das Gerät ganz nach innen zu schieben.



Befestigen Sie die Frontverkleidung erst, nachdem Sie das Gerät eingeschaltet haben.

Verkabeln Sie das Gerät 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.

Was Sie benötigen

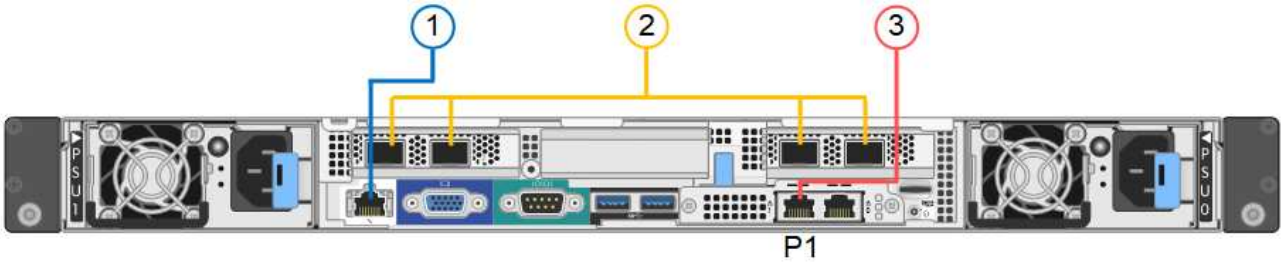
- Sie verfügen über ein RJ-45-Ethernet-Kabel zum Anschließen des Management-Ports.
- Sie haben eine der folgenden Optionen für die Netzwerkanschlüsse. Diese Artikel sind nicht im Lieferumfang des Geräts enthalten.
  - Ein bis vier Twinax-Kabel zum Anschließen der vier Netzwerk-Ports.
  - Für das SG100 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 zerlegen oder entfernen. Sie können Laserstrahlung ausgesetzt sein.

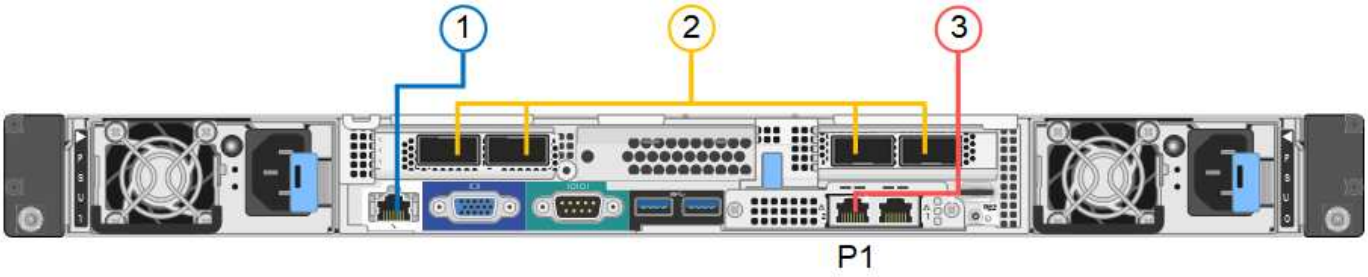
Über diese Aufgabe

Die folgenden Abbildungen zeigen die Anschlüsse auf der Rückseite des Geräts.

SG100-Anschlüsse



SG1000-Anschlüsse



	Port	Typ des Ports	Funktion
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	• 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 auf 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.

	Port	Typ des Ports	Funktion
3	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.	• 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 das Gerät mit einem Service-Laptop verbunden werden, 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.

   Die vier Netzwerkanschlüsse müssen dieselbe Verbindungsgeschwindigkeit verwenden. In den folgenden Tabellen finden Sie die erforderlichen Geräte, die auf Ihrer Hardware und der Verbindungsgeschwindigkeit basieren.

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.

Anschließen von Netzkabeln und Einschalten der Stromzufuhr (SG100 und SG1000)

Nach dem Anschließen der Netzwerkkabel 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 Einschaltvorgangs nicht erneut.
4. Wenn Fehler auftreten, beheben Sie alle Probleme.
5. Befestigen Sie die Frontverkleidung am Gerät.

Verwandte Informationen

"Anzeigen von Statusanzeigen an den SG100- und SG1000-Geräten"

Anzeigen von Statusanzeigen an den SG100- und SG1000-Geräten

Die Appliance enthält Anzeigen, mit denen Sie den Status des Appliance-Controllers und der beiden SSDs ermitteln können.

Gerätesteuchten und -Tasten

	Anzeige	Bundesland
1	Ein-/aus-Schalter	• 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“	Diese Taste kann auf „Blinken“, „ein“ (Festkörper) oder „aus“ eingestellt werden. • 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	• Gelb, konstant: Ein Fehler ist aufgetreten. **Hinweis:** um den Start und Fehlercodes anzuzeigen, müssen Sie auf die BMC-Schnittstelle zugreifen. • Aus: Es sind keine Fehler vorhanden.

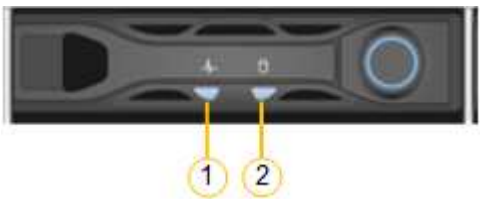
Allgemeine Startcodes

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.

   Um die Boot- und Fehlercodes anzuzeigen, müssen Sie auf die BMC-Schnittstelle zugreifen.

SSD-LEDs



LED	Anzeige	Bundesland
1	Laufwerksstatus/-Fehler	• Blau (fest): Laufwerk ist online • Gelb (blinkend): Laufwerksausfall • Aus: Steckplatz ist leer
2	Laufwerk aktiv	Blau (blinkend): Auf das Laufwerk wird zugegriffen

Verwandte Informationen

"Fehlerbehebung bei der Hardwareinstallation"

"Konfigurieren der BMC-Schnittstelle"

Konfigurieren von StorageGRID-Verbindungen

Bevor Sie die Services-Appliance als Node in einem StorageGRID-System bereitstellen können, müssen Sie die Verbindungen zwischen der Appliance und den zu verwendenden Netzwerken konfigurieren. Sie können Netzwerke konfigurieren, indem Sie im StorageGRID Appliance Installer navigieren, der auf der Services Appliance vorinstalliert ist.

Schritte

- "Zugriff auf das Installationsprogramm der StorageGRID-Appliance"
- "Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance"
- "Konfigurieren von Netzwerkverbindungen (SG100 und SG1000)"
- "StorageGRID-IP-Adressen werden konfiguriert"
- "Netzwerkverbindungen werden überprüft"
- "Überprüfen von Netzwerkverbindungen auf Portebene"

Zugriff auf das Installationsprogramm der StorageGRID-Appliance

Sie müssen auf das Installationsprogramm der StorageGRID Appliance zugreifen, um die Verbindungen zwischen der Appliance und den drei StorageGRID-Netzwerken zu konfigurieren: Das Grid-Netzwerk, das Admin-Netzwerk (optional) und das Client-Netzwerk (optional).

Was Sie benötigen

- Sie verwenden einen beliebigen Management-Client, der eine Verbindung zum StorageGRID-Admin-Netzwerk herstellen kann.
- Der Client verfügt über einen unterstützten Webbrowser.
- Die Services-Appliance ist mit allen von Ihnen geplanten StorageGRID-Netzwerken verbunden.
- Sie kennen die IP-Adresse, das Gateway und das Subnetz der Services-Appliance in diesen Netzwerken.
- Sie haben die geplanten Netzwerk-Switches konfiguriert.

Über diese Aufgabe

Um zunächst auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, können Sie die vom DHCP zugewiesene IP-Adresse für den Admin-Netzwerkport auf der Services-Appliance verwenden (vorausgesetzt, er ist mit dem Admin-Netzwerk verbunden). Alternativ können Sie einen Service-Laptop direkt mit der Services-Appliance verbinden.

Schritte

1. Verwenden Sie, falls möglich, die DHCP-Adresse für den Netzwerkanschluss des Administrators auf der Services-Appliance, um auf das Installationsprogramm der StorageGRID Appliance zuzugreifen.

   SG100 Admin Network Port

   SG1000 Admin-Netzwerkanschluss

   a. Suchen Sie das MAC-Adressenetikett auf der Vorderseite der serrvices-Appliance und legen Sie die MAC-Adresse für den Admin-Netzwerkport fest.

      Auf dem MAC-Adressenetikett wird die MAC-Adresse für den BMC-Verwaltungsport aufgelistet.

      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.

   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://services-appliance_IP:8443`

      Für *`services-appliance_IP`*, Verwenden Sie die DHCP-Adresse.

   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.

2. Wenn Sie alternativ keine IP-Adresse über DHCP erhalten können, verwenden Sie eine Link-lokale Verbindung, um auf das Installationsprogramm für StorageGRID Appliance zuzugreifen.

a. Schließen Sie einen Service-Laptop mithilfe eines Ethernet-Kabels direkt an den rechtesten RJ-45-Port des Services-Geräts an.

SG100 Link-Local-Verbindung

SG1000-Link-Local-Verbindung

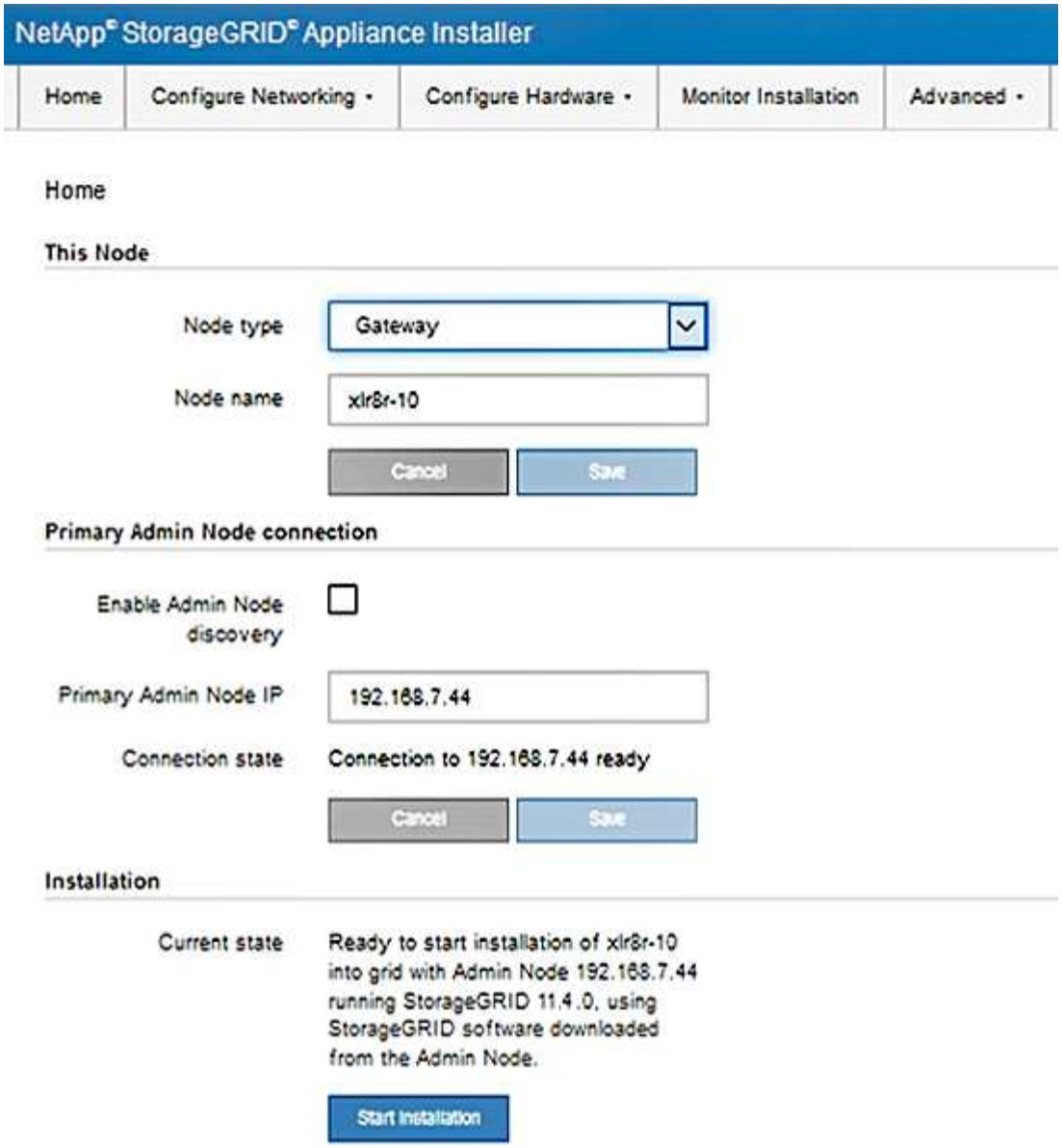
b. Öffnen Sie einen Webbrowser.

c. 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 lokale Verbindung nicht auf die Startseite zugreifen können, konfigurieren Sie die Service-Laptop-IP-Adresse als `169.254.0.2`, Und versuchen Sie es erneut.

3. Überprüfen Sie alle Meldungen, die auf der Startseite angezeigt werden, und konfigurieren Sie die Verbindungskonfiguration und die IP-Konfiguration nach Bedarf.



Verwandte Informationen

"Anforderungen an einen Webbrowser"

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.

Was Sie benötigen

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 das StorageGRID-Appliance-Installationsprogramm 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 im Grid Manager **Hilfe** > **Info**).

   Die zweite Ziffer in den beiden Versionen sollte übereinstimmen. Wenn auf Ihrem StorageGRID-System beispielsweise die Version 11.**5**.*x.y* ausgeführt wird, sollte die StorageGRID Appliance Installer-Version 3.**5**.*z* sein.

3. Wenn die Appliance über eine übergeordnete Version des Installationsprogramms für StorageGRID Appliances verfügt, wechseln Sie zur Seite NetApp Downloads für StorageGRID.

   "NetApp Downloads: StorageGRID"

   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 Datei Support für StorageGRID Appliances ist eine `.zip` Archiv, das die aktuellen und vorherigen Firmware-Versionen für alle StorageGRID Appliance-Modelle enthält, in Unterverzeichnissen für jeden Controller-Typ.

   Nach dem Herunterladen der Datei Support für StorageGRID Appliances extrahieren Sie den `.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 des Installationsprogramms für StorageGRID-Geräte, um die folgenden Schritte auszuführen:
   a. Laden Sie die entsprechende Support-Datei (Firmware-Image) für den Controller-Typ und die Prüfsummendatei hoch.
   b. Aktualisieren Sie die inaktive Partition.
   c. Starten Sie neu und tauschen Sie die Partitionen aus.
   d. Aktualisieren Sie die zweite Partition.

Verwandte Informationen

"Zugriff auf das Installationsprogramm der StorageGRID-Appliance"

Konfigurieren von Netzwerkverbindungen (SG100 und SG1000)

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.

Was Sie benötigen

- Sie haben die für Ihren Kabeltyp und die Verbindungsgeschwindigkeit erforderlichen zusätzlichen Geräte erhalten.
- Sie haben die Netzwerk-Ports mit Switches verbunden, die Ihre gewählte Geschwindigkeit unterstützen.

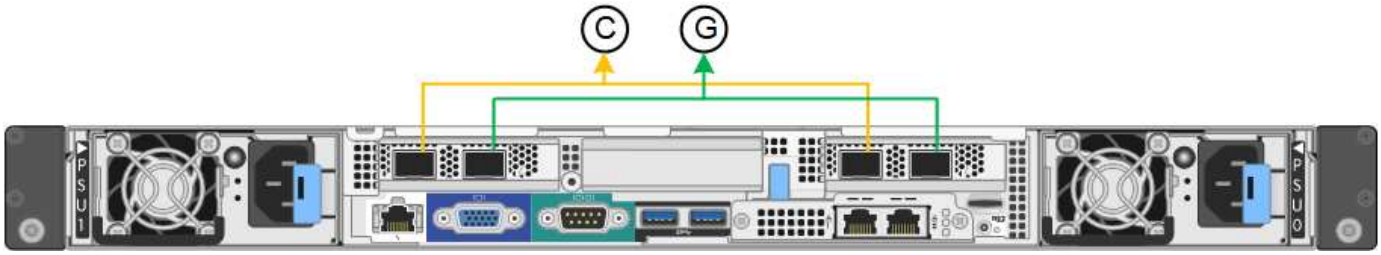
Wenn Sie den aggregierten Port Bond-Modus, den LACP Network Bond-Modus oder VLAN-Tagging verwenden möchten:

- 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.

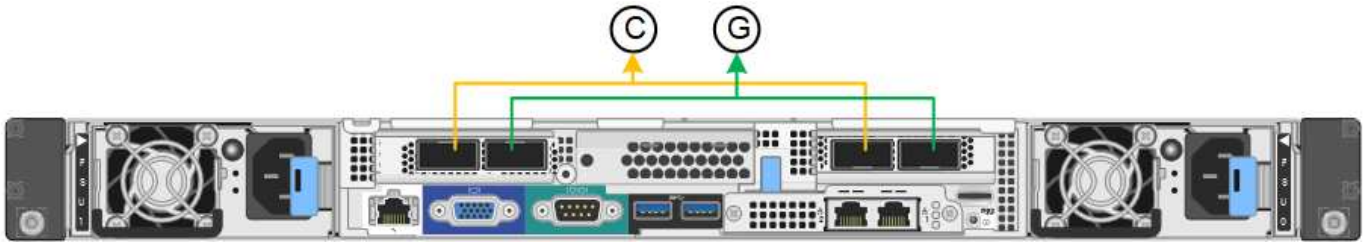
Über diese Aufgabe

Die Abbildungen zeigen, wie die vier Netzwerk-Ports im Bond-Modus mit festen Ports verbunden sind (Standardkonfiguration).

SG100 Festanschluss-Modus



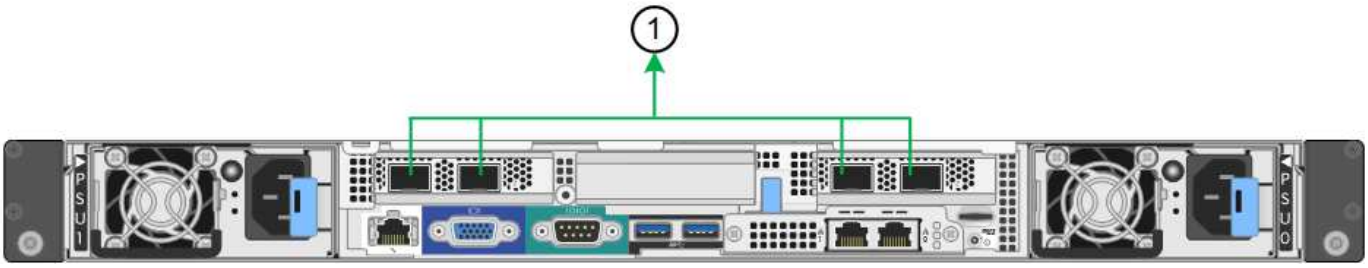
SG1000 Festanschlussmodus



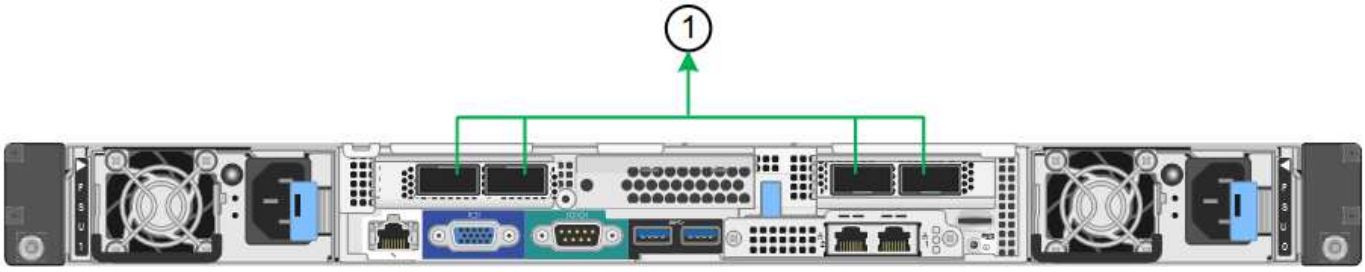
	Welche Ports sind verbunden
C	Die Ports 1 und 3 sind für das Client-Netzwerk verbunden, falls dieses Netzwerk verwendet wird.
G	Die Ports 2 und 4 sind für das Grid-Netzwerk verbunden.

Die Abbildung zeigt, wie die vier Netzwerk-Ports im Bond-Modus für aggregierte Ports verbunden sind.

SG100 Aggregat-Port-Bond-Modus



SG1000 Aggregat-Port-Bond-Modus



	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. Die Standardeinstellungen werden fett dargestellt. Sie müssen nur die Einstellungen auf der Seite Link Configuration konfigurieren, wenn Sie eine nicht-Standardeinstellung verwenden möchten.

Die LACP sende Hash-Richtlinie ist standardmäßig im layer2+3-Modus verfügbar. Bei Bedarf können Sie die Grid Management API verwenden, um sie in den layer3+4 Modus zu ändern.

- **Festes (Standard) Port Bond-Modus**

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Active-Backup (Standard)	• 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.	• 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.

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
LACP (802.3ad)	• 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.	• 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.

- * Aggregat-Port-Bond-Modus*

Netzwerk-Bond-Modus	Client-Netzwerk deaktiviert (Standard)	Client-Netzwerk aktiviert
Nur LACP (802.3ad	• Die Ports 1-4 verwenden einen einzelnen LACP Bond für das Grid Network. • Ein einzelnes VLAN-Tag identifiziert Grid-Netzwerkpakete.	• 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.

Weitere Informationen finden Sie im Artikel über GbE-Portverbindungen für die Services-Appliance.

Diese Abbildung zeigt, wie die beiden 1-GbE-Management-Ports des SG100 im Active-Backup Netzwerk-Bond-Modus des Admin-Netzwerks verbunden sind.

Diese Abbildungen zeigen, wie die beiden 1-GbE-Management-Ports auf der Appliance im Active-Backup Netzwerk-Bond-Modus des Admin-Netzwerks verbunden sind.

SG100 Admin Netzwerkanschlüsse gebunden

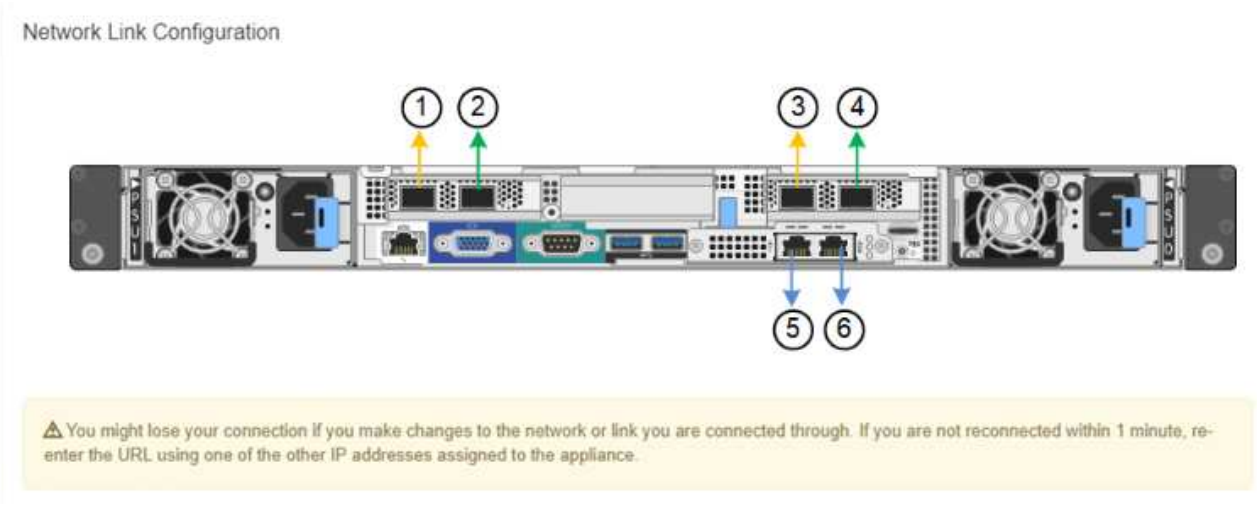
SG1000 Admin Netzwerkanschlüsse gebunden

Schritte

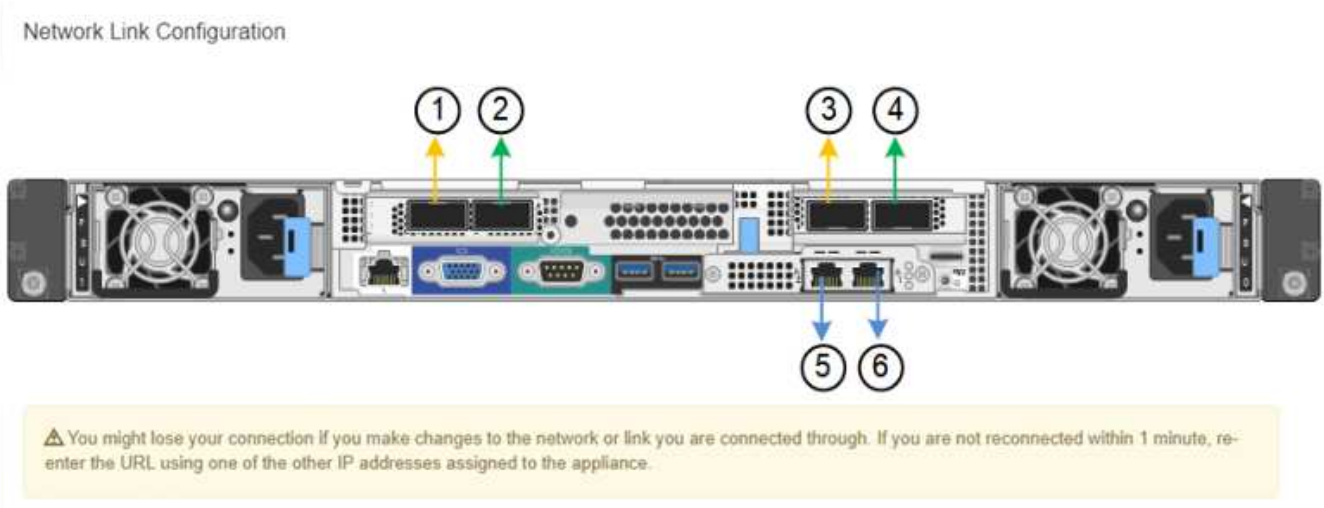
1. Klicken Sie in der Menüleiste des StorageGRID-Appliance-Installationsprogramms auf **Netzwerke konfigurieren** > **Link-Konfiguration**.

   Auf der Seite Network Link Configuration wird ein Diagramm der Appliance angezeigt, in dem die Netzwerk- und Verwaltungsports nummeriert sind.

   SG100-Anschlüsse



   SG1000-Ports



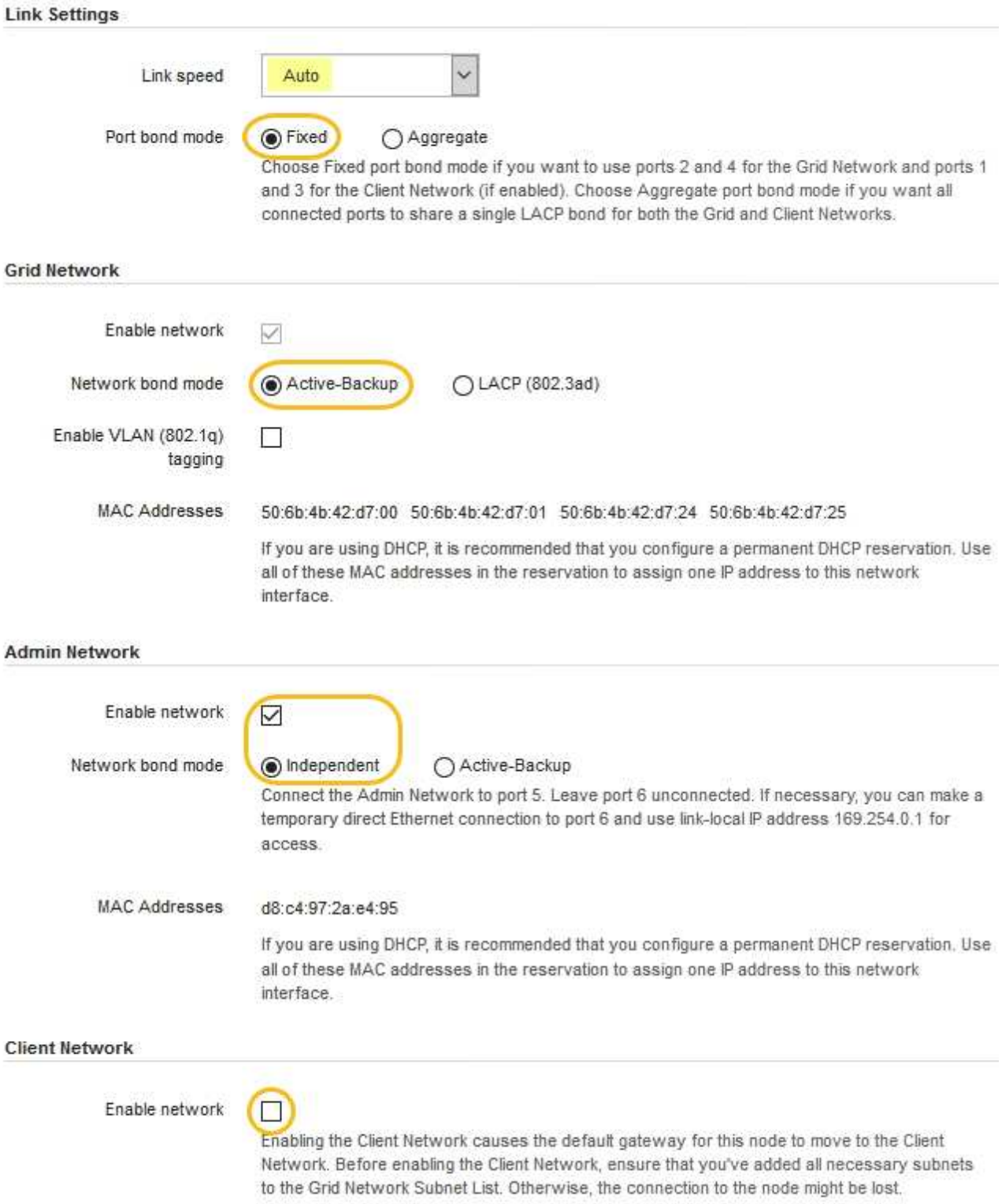
   In der Tabelle „Link-Status“ werden der Verbindungsstatus und die Geschwindigkeit der nummerierten Ports (SG1000) angezeigt.

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Down	N/A
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

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.



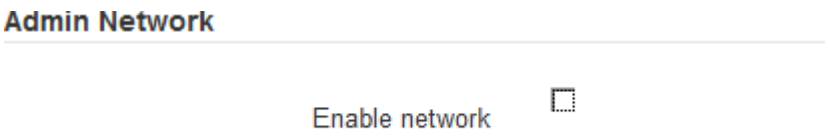
2. Wählen Sie die Verbindungsgeschwindigkeit für die Netzwerkanschlüsse aus der Dropdown-Liste **Link Speed** aus.

   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.

3. Aktivieren oder deaktivieren Sie die StorageGRID-Netzwerke, die Sie verwenden möchten.

   Das Grid-Netzwerk ist erforderlich. Sie können dieses Netzwerk nicht deaktivieren.

   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.

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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten erneut ein. Verwenden Sie dazu eine der anderen IP-Adressen, die der Appliance zugewiesen sind:

`https://services_appliance_IP:8443`

Verwandte Informationen

"Beschaffung zusätzlicher Geräte und Werkzeuge (SG100 und SG1000)"

StorageGRID-IP-Adressen werden konfiguriert

Mit dem Installationsprogramm der StorageGRID Appliance können Sie die IP-Adressen und Routing-Informationen konfigurieren, die für die Services-Appliance in StorageGRID Grid, Administrator und Client-Netzwerken verwendet werden.

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.

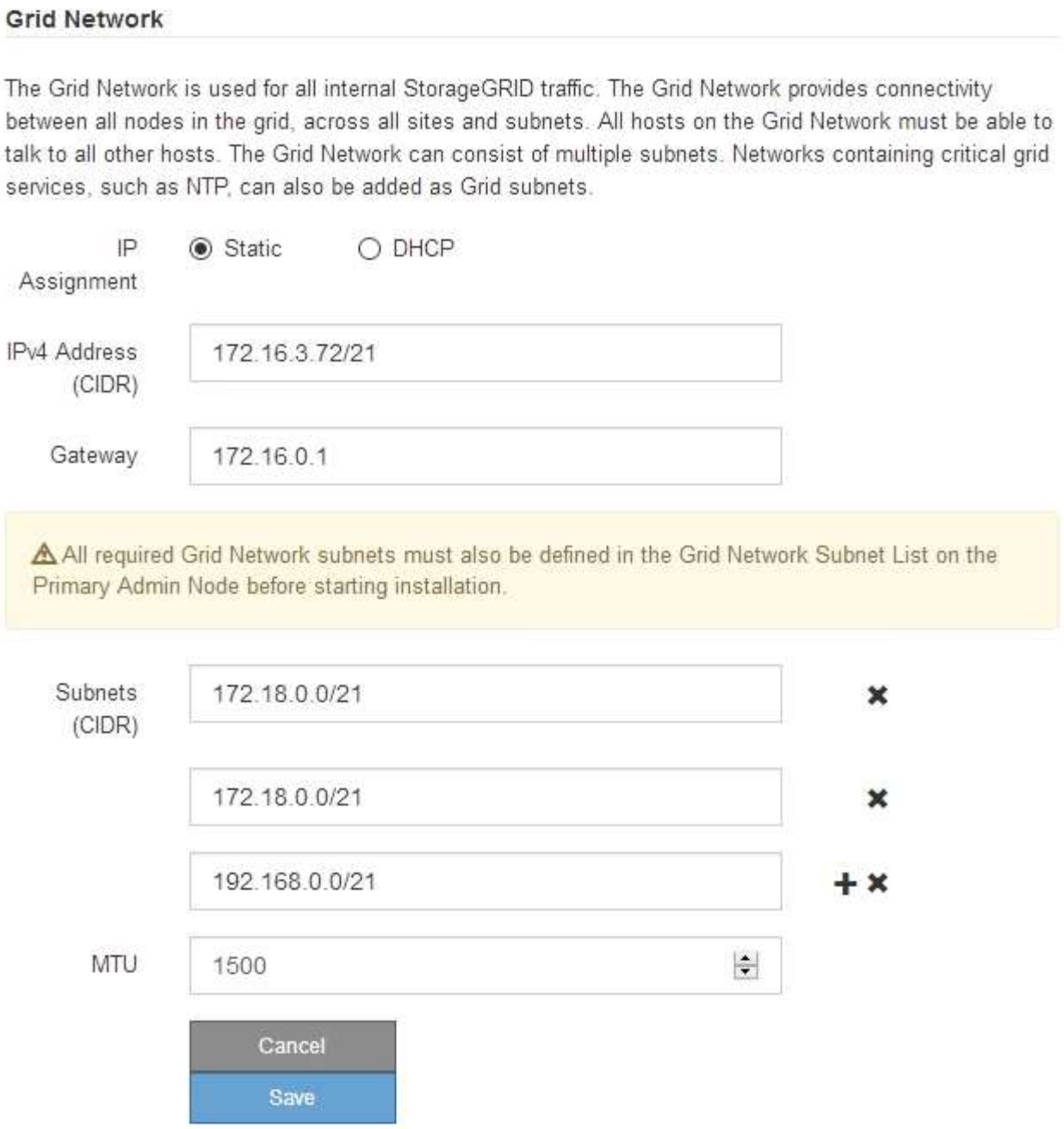
Wenn Sie die Verbindungskonfiguration ändern möchten, lesen Sie die Anweisungen zum Ändern der Link-Konfiguration der Services Appliance.

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 identisch 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://services_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 Löschsymbol ✖.

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.

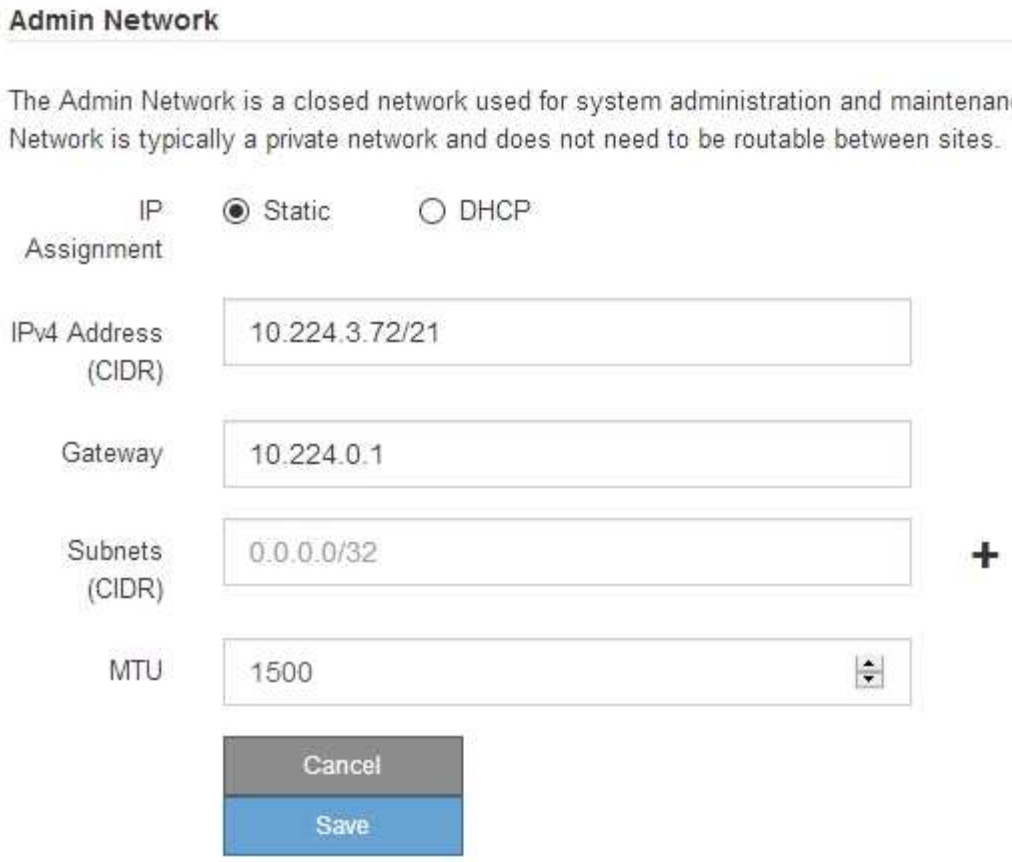
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch 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, müssen Sie das Admin-Netzwerk auf der Seite Link Configuration aktivieren.



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://services_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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

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 zur Verwendung des Admin-Netzwerk-Gateways verwendet 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 ✖.

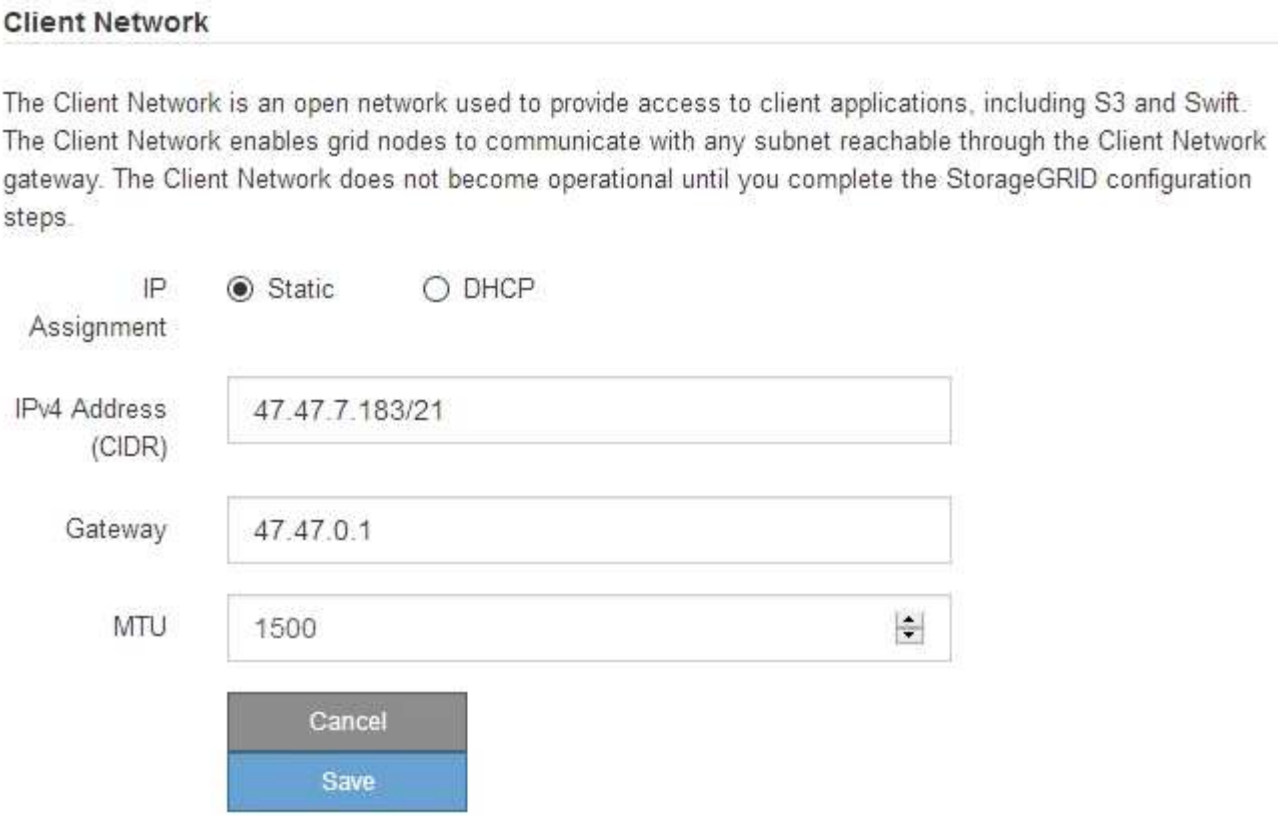
c. Wenn Sie Jumbo Frames verwenden möchten, ändern Sie das MTU-Feld in einen für Jumbo Frames geeigneten Wert, z. B. 9000. Behalten Sie andernfalls den Standardwert 1500 bei.

> 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, müssen Sie das Client-Netzwerk auf der Seite Link Configuration aktivieren.



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.

Verwandte Informationen

"Ändern der Link-Konfiguration der Services Appliance"

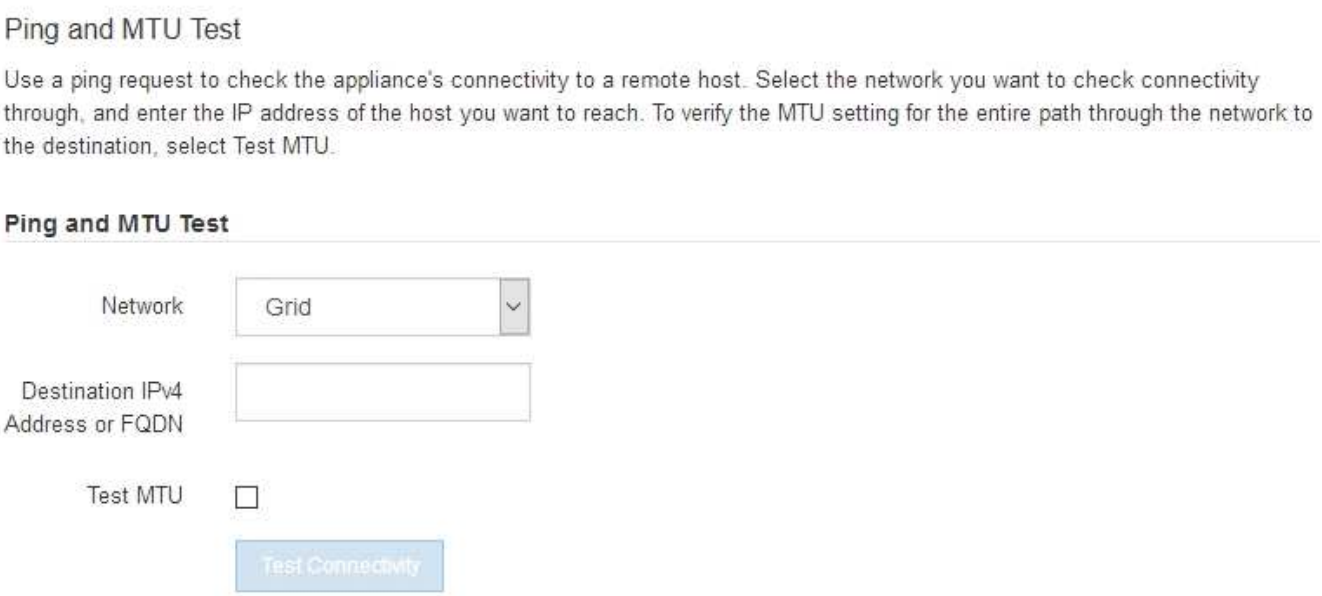
Netzwerkverbindungen werden überprüft

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.



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 Domänennamen (FQDN) für einen Host in diesem Netzwerk ein.

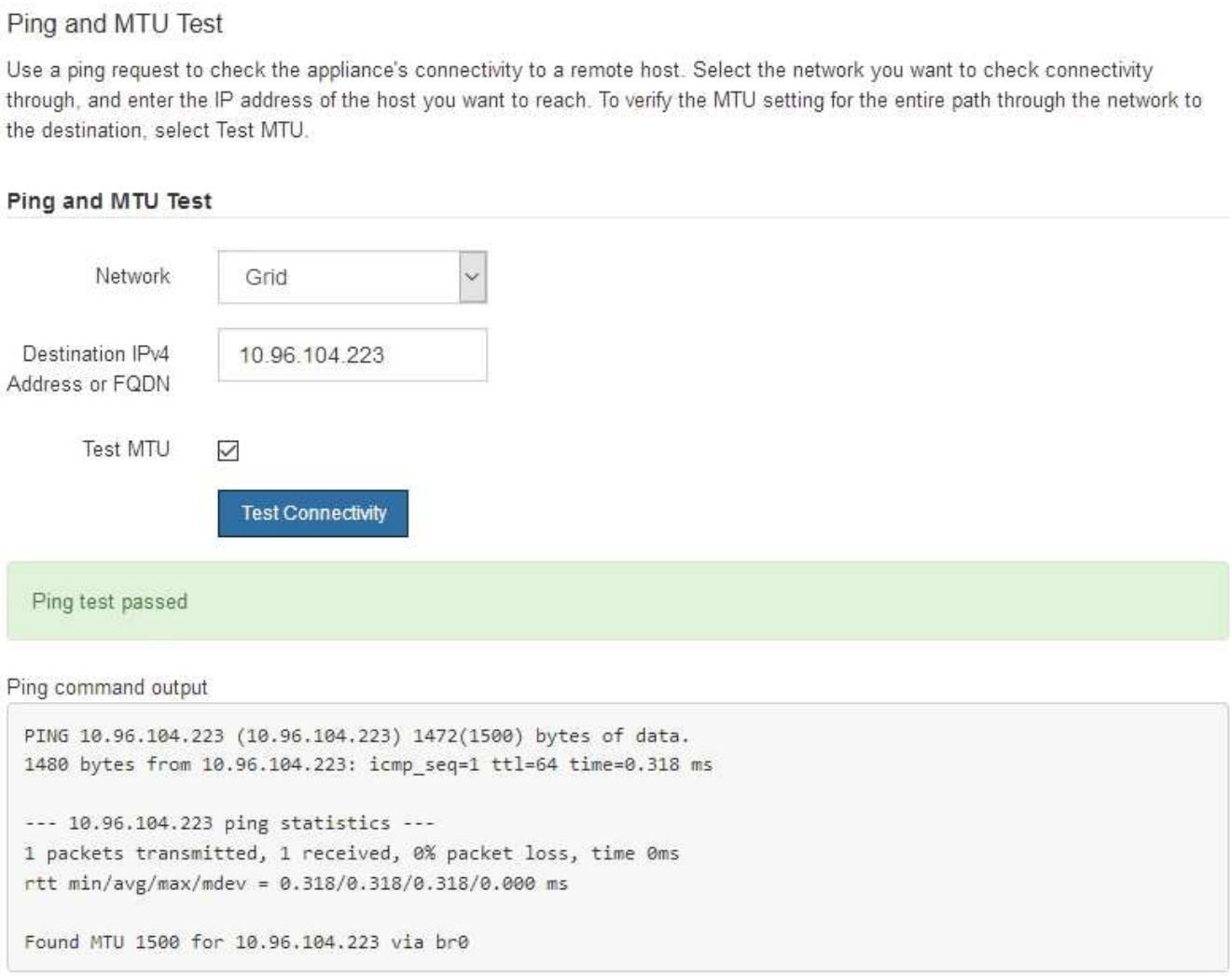
   Beispielsweise möchten Sie das Gateway im Netzwerk oder den primären Admin-Node pingen.

4. Aktivieren Sie optional das Kontrollkästchen **MTU-Test**, 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.



Verwandte Informationen

"Konfigurieren von Netzwerkverbindungen (SG100 und SG1000)"

"Ändern der MTU-Einstellung"

Überprüfen von 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 unter der Portreferenz in den Netzwerkrichtlinien von StorageGRID.

> Die in der Tabelle für die Portkonnektivität aufgeführten Grid-Netzwerkports sind nur für StorageGRID Version 11.5 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.

   The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

   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.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

Port Connectivity Test

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

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.

- Wenn für einen oder mehrere ausgewählte Ports keine Netzwerkverbindung auf Portebene hergestellt werden kann, wird die Meldung „`Verbindungstest 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.

Verwandte Informationen

"Netzwerkrichtlinien"

Konfigurieren der BMC-Schnittstelle

Die Benutzeroberfläche für den Baseboard Management Controller (BMC) auf der Services Appliance bietet Statusinformationen über die Hardware und ermöglicht die Konfiguration von SNMP-Einstellungen und anderen Optionen für die Services Appliance.

Schritte

- "Ändern des Root-Passworts für die BMC-Schnittstelle"
- "Einstellen der IP-Adresse für den BMC-Managementport"
- "Zugriff auf die BMC-Schnittstelle"
- "Konfigurieren von SNMP-Einstellungen für die Services-Appliance"
- "Einrichten von E-Mail-Benachrichtigungen für Meldungen"

Ändern des Root-Passworts für die BMC-Schnittstelle

Aus Sicherheitsgründen müssen Sie das Kennwort für den Root-Benutzer von BMC ändern.

Was Sie benötigen

Der Management-Client verwendet einen unterstützten Webbrowser.

Über diese Aufgabe

Bei der ersten Installation des Geräts verwendet der BMC ein Standardpasswort für den Root-Benutzer (`root/calvin`). Sie müssen das Passwort für den Root-Benutzer ändern, um Ihr System zu sichern.

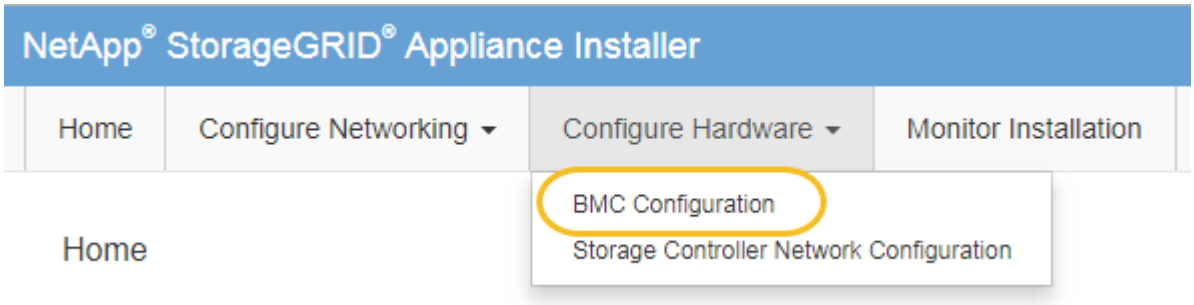
Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:
   `https://services_appliance_IP:8443`

   Für `services_appliance_IP`, Verwenden Sie die IP-Adresse für die Appliance in einem beliebigen StorageGRID-Netzwerk.

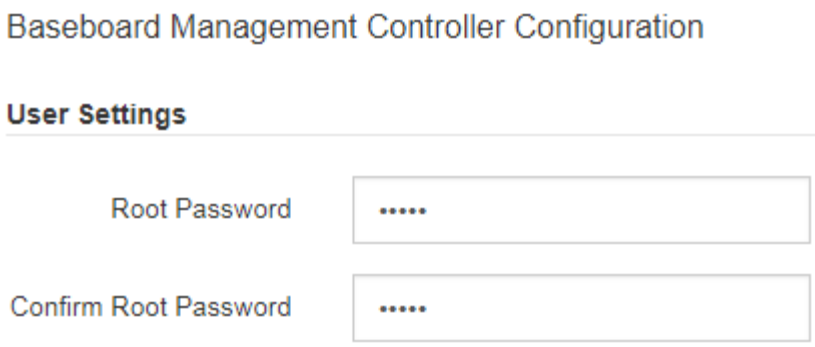
   Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

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 Root-Konto ein.



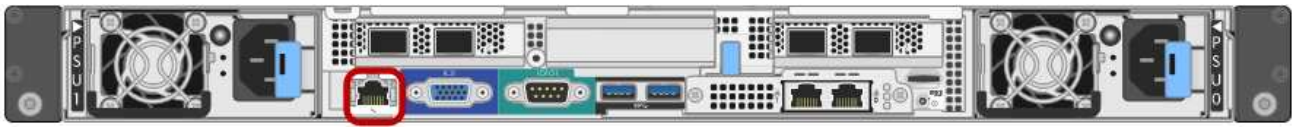
4. Klicken Sie Auf **Speichern**.

Einstellen der IP-Adresse für den BMC-Managementport

Bevor Sie auf die BMC-Schnittstelle zugreifen können, müssen Sie die IP-Adresse für den BMC-Management-Port auf der Services-Appliance konfigurieren.

Was Sie benötigen

- Der Management-Client verwendet einen unterstützten 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.
- SG100 BMC Management Port*



SG1000 BMC-Management-Port

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.

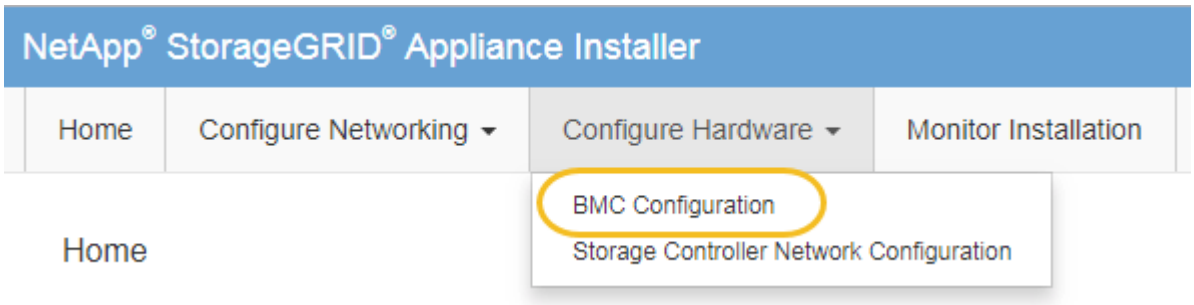
Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:
   `https://services_appliance_IP:8443`

   Für *`services_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**.

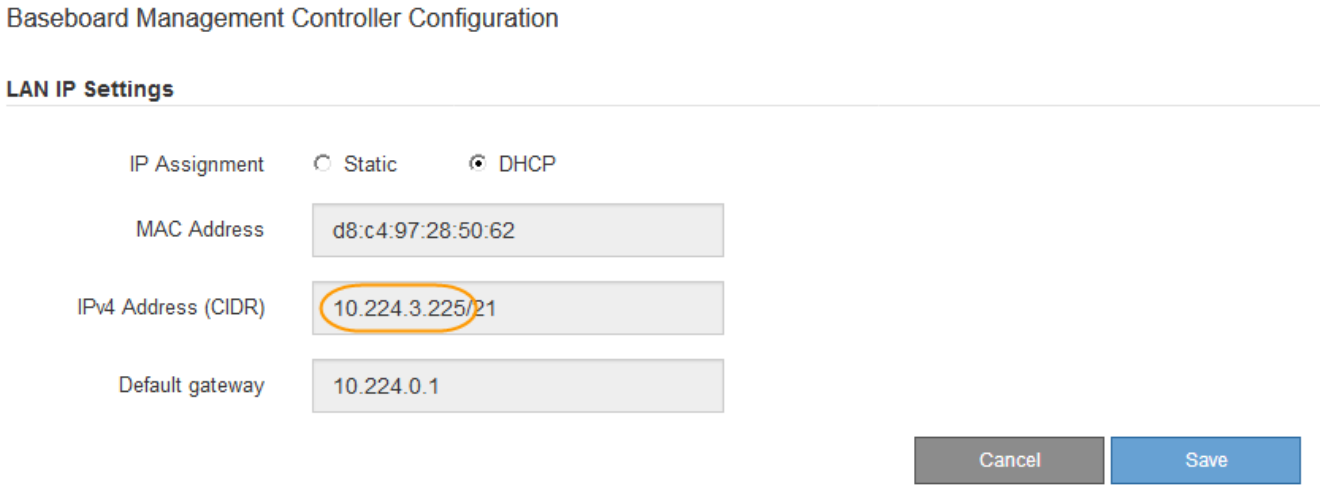


Die Seite Baseboard Management Controller Configuration wird angezeigt.

3. Notieren Sie sich die automatisch angezeigte IPv4-Adresse.

DHCP ist die Standardmethode zum Zuweisen einer IP-Adresse zu diesem Port.

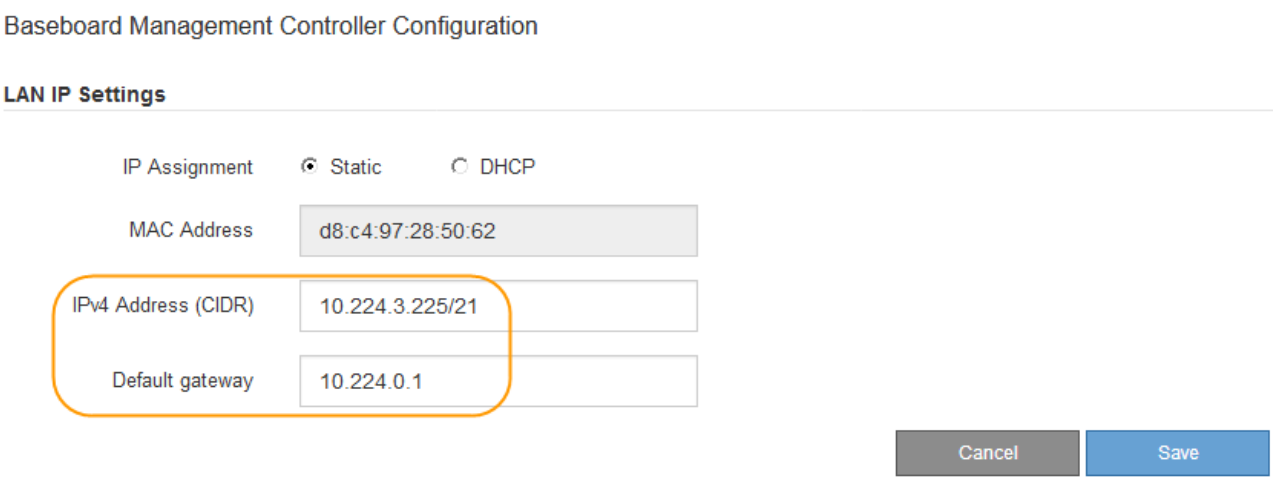
Es kann einige Minuten dauern, bis die DHCP-Werte angezeigt werden.



4. Legen Sie optional eine statische IP-Adresse für den BMC-Verwaltungsport fest.

Sie sollten entweder eine statische IP für den BMC-Verwaltungsport 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.



d. Klicken Sie Auf **Speichern**.

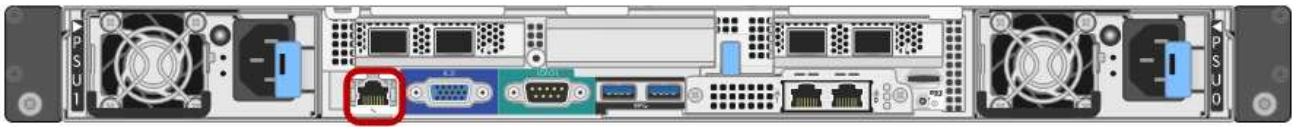
Es kann einige Minuten dauern, bis Ihre Änderungen angewendet werden.

Zugriff auf die BMC-Schnittstelle

Sie können auf die BMC-Schnittstelle auf der Services-Appliance mit der DHCP- oder statischen IP-Adresse für den BMC-Management-Port zugreifen.

Was Sie benötigen

- Der Management-Client verwendet einen unterstützten Webbrowser.
- Der BMC-Management-Port der Services-Appliance ist mit dem Managementnetzwerk verbunden, das Sie verwenden möchten.
- SG100 BMC Management Port*



SG1000 BMC-Management-Port

Schritte

1. Geben Sie die URL für die BMC-Schnittstelle ein:
`https://BMC_Port_IP`

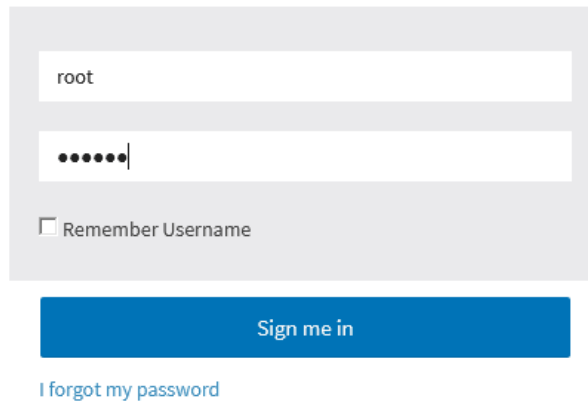
Für *`BMC_Port_IP`*, Verwenden Sie die DHCP- oder statische IP-Adresse für den BMC-Management-Port.

Die BMC-Anmeldeseite wird angezeigt.

2. Geben Sie den Root-Benutzernamen und das Kennwort ein. Verwenden Sie dazu das Passwort, das Sie beim Ändern des Standard-Root-Passworts festgelegt haben:

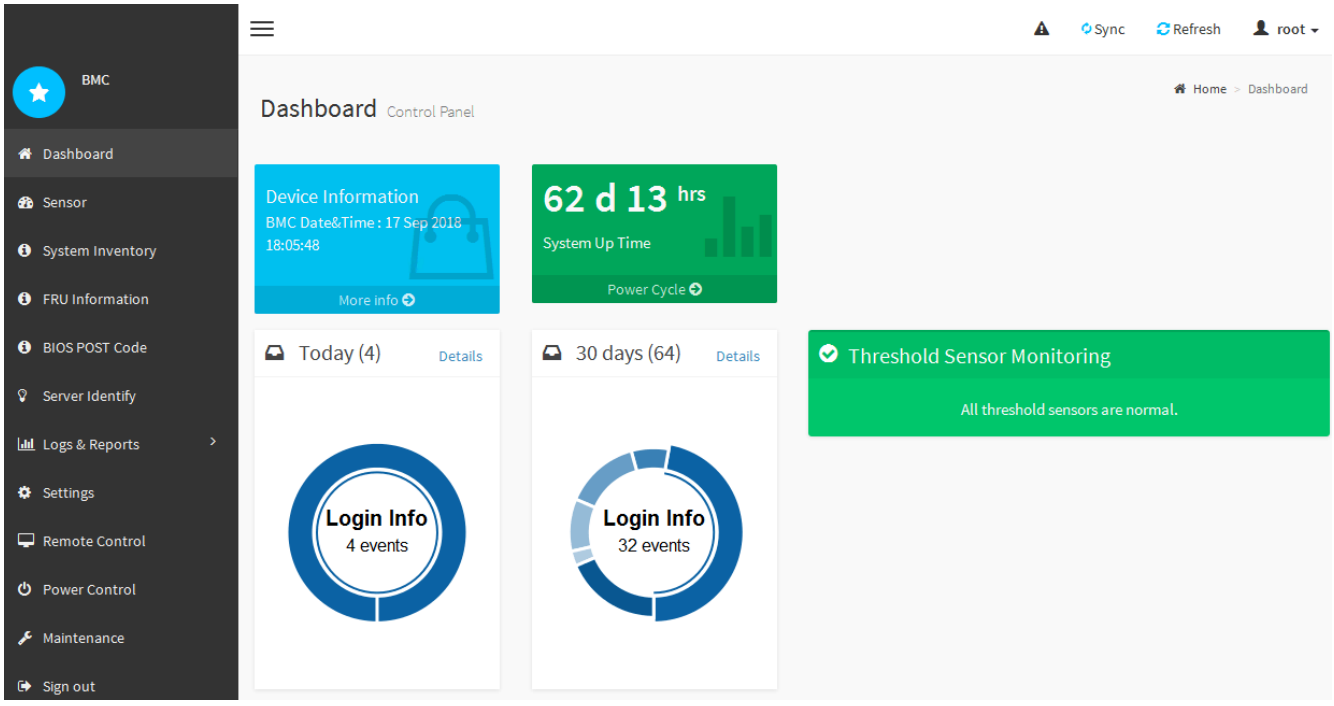
root

password



3. Klicken Sie auf **Sign me in**

   Das BMC-Dashboard wird angezeigt.



4. 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.

Verwandte Informationen

"Ändern des Root-Passworts für die BMC-Schnittstelle"

Konfigurieren von SNMP-Einstellungen für die Services-Appliance

Wenn Sie mit der Konfiguration von SNMP für Hardware vertraut sind, können Sie die BMC-Schnittstelle verwenden, um die SNMP-Einstellungen für die Services-Appliance zu konfigurieren. Sie können sichere Community-Strings bereitstellen, SNMP-Trap aktivieren und bis zu fünf SNMP-Ziele angeben.

Was Sie benötigen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Sie haben Erfahrung in der Konfiguration von SNMP-Einstellungen für SNMPv1-v2c Geräte.

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 Domain-Namen werden nicht unterstützt.

   Aktivieren Sie Traps, wenn die Services-Appliance sofortige Benachrichtigungen an eine SNMP-Konsole senden soll, wenn sie sich in einem ungewöhnlichen Zustand befindet. Möglicherweise sind Verbindungsfallen nach oben/unten, Temperaturen über bestimmten Schwellenwerten oder hohen Datenverkehr hindeuten.

4. Klicken Sie optional auf **Test-Trap senden**, um Ihre Einstellungen zu testen.
5. Wenn die Einstellungen korrekt sind, klicken Sie auf **Speichern**.

Einrichten von E-Mail-Benachrichtigungen für Meldungen

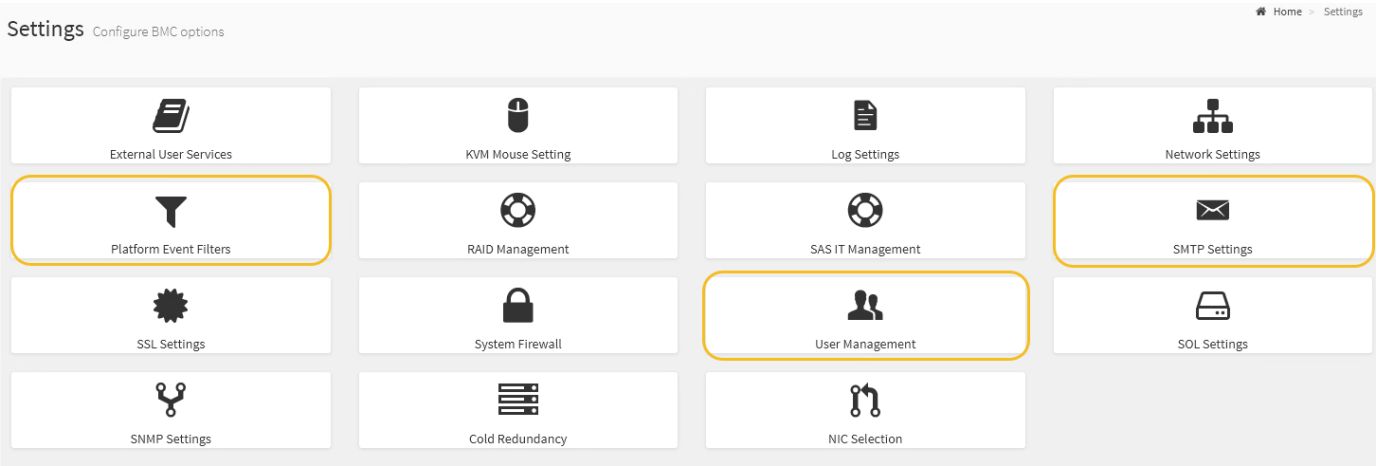
Wenn E-Mail-Benachrichtigungen gesendet werden sollen, wenn Warnmeldungen auftreten, müssen Sie SMTP-Einstellungen, Benutzer, LAN-Ziele, Warnrichtlinien und Ereignisfilter über die BMC-Schnittstelle konfigurieren.

Was Sie benötigen

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 SMTP-Einstellungen.
   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 alle Benutzer Benachrichtigungen erhalten möchten, müssen Sie für jeden Benutzer ein LAN-Ziel hinzufügen.
   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: Aktivieren der Node-Verschlüsselung

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. Bei der Installation der Appliance müssen Sie die Node-Verschlüsselung auswählen und aktivieren. Die Auswahl der Node-Verschlüsselung kann nicht rückgängig gemacht werden, sobald der KMS-Verschlüsselungsprozess gestartet wird.

Was Sie benötigen

Lesen Sie die Informationen über KMS in den Anweisungen zur Administration von StorageGRID durch.

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.

> Alle Daten, die vor einer Appliance mit aktivierter Node-Verschlüsselung vorhanden sind, werden mit einem nichtsicheren temporären Schlüssel verschlüsselt. Das Gerät ist erst dann vor dem Entfernen oder Diebstahl geschützt, wenn der Schlüssel auf einen vom KMS angegebenen Wert gesetzt wird.

Ohne den KMS-Schlüssel, der zur Entschlüsselung der Festplatte benötigt wird, können die Daten auf der

Appliance nicht abgerufen und effektiv verloren gehen. 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

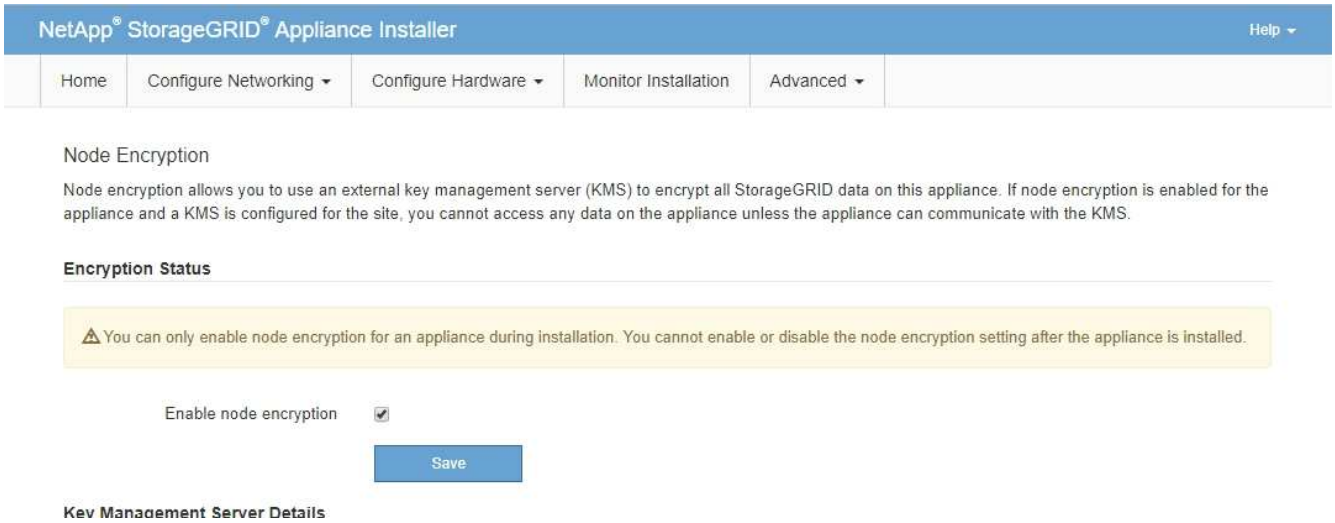
1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.
   `https://Controller_IP:8443`

   `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 Appliance-Festplatten nicht entschlüsselt werden, ohne dabei den gleichen KMS-Schlüssel zu verwenden.

2. Wählen Sie **Hardware Konfigurieren** > **Node Encryption**.



3. Wählen Sie **Node-Verschlüsselung aktivieren**.

   Sie können die Auswahl **Enable Node Encryption** ohne Gefahr eines Datenverlusts aufheben, bis Sie **Save** auswählen und der Appliance Node auf die KMS-Verschlüsselungsschlüssel in Ihrem StorageGRID-System zugreift und mit der Festplattenverschlüsselung beginnt. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht deaktivieren.

   > Nachdem Sie einer StorageGRID Site mit KMS eine Appliance hinzugefügt haben, für die die Node-Verschlüsselung aktiviert ist, kann die KMS-Verschlüsselung für den Node nicht angehalten werden.

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.

Verwandte Informationen

"StorageGRID verwalten"

"Monitoring der Node-Verschlüsselung im Wartungsmodus"

Implementieren eines Service-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.

Bereitstellen einer Services Appliance als primärer Admin-Node

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.

Was Sie benötigen

- 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.

> Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte in der Recovery- und Wartungsanleitung zum Entfernen von Port-Remaps.

> Der CLB-Service ist veraltet.

- Sie verfügen über einen Service-Laptop mit einem unterstützten 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.

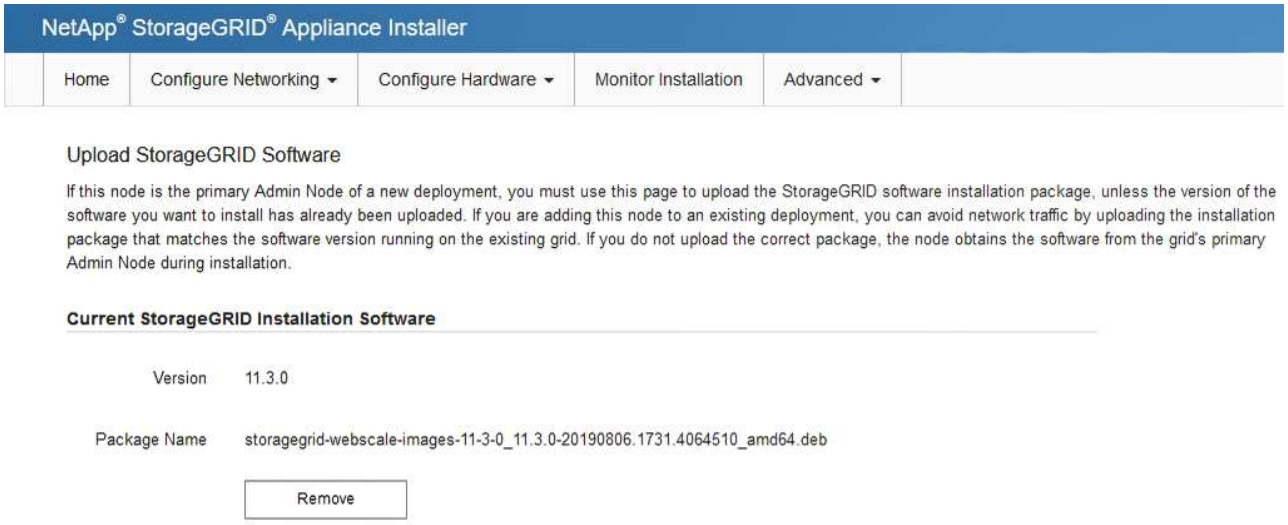
2. Wählen Sie im Abschnitt **dieser Knoten** die Option **Hauptadministrator** aus.
3. Geben Sie im Feld **Knotenname** den Namen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und klicken Sie auf **Speichern**.

   Der Node-Name wird diesem Appliance-Node im StorageGRID-System zugewiesen. Sie wird auf der Seite Grid Nodes im Grid Manager angezeigt.

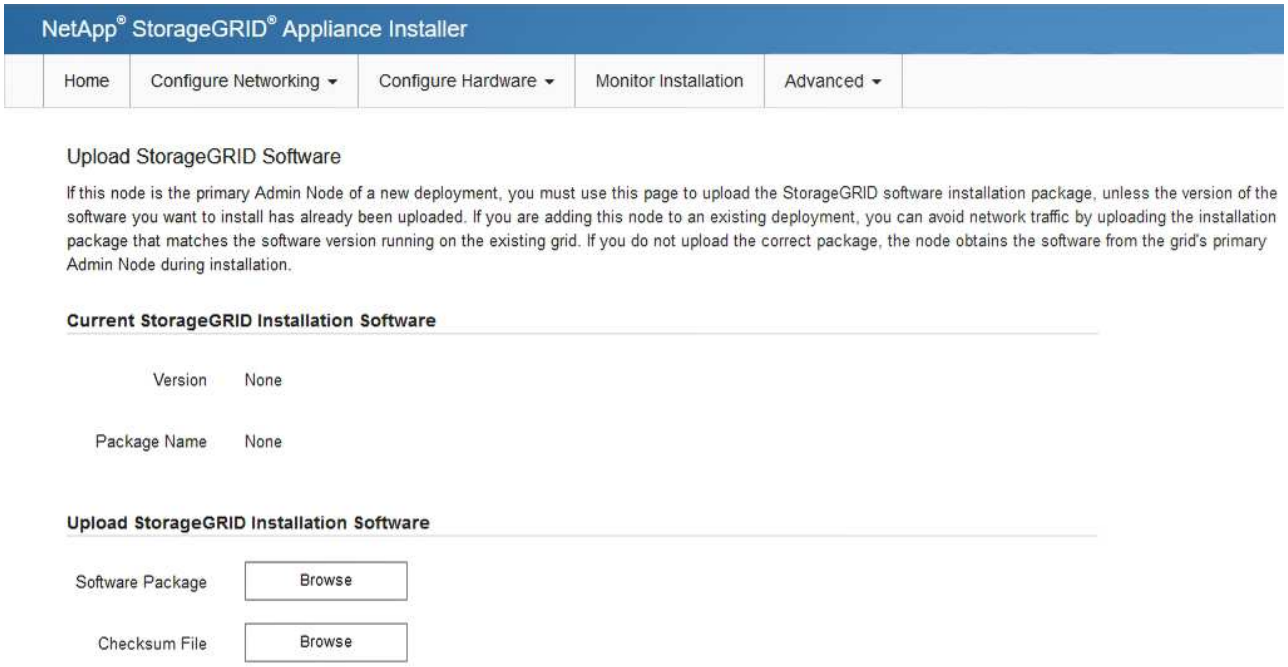
4. Führen Sie optional folgende Schritte aus, um eine andere Version der StorageGRID-Software zu installieren:
   a. Laden Sie das Installationsarchiv von der NetApp Downloads Seite zu StorageGRID herunter.

      "NetApp Downloads: StorageGRID"

   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.



e. Klicken Sie auf **Durchsuchen** für das Softwarepaket, das Sie heruntergeladen und extrahiert haben, und klicken Sie dann auf **Durchsuchen** für die Prüfsummendatei.



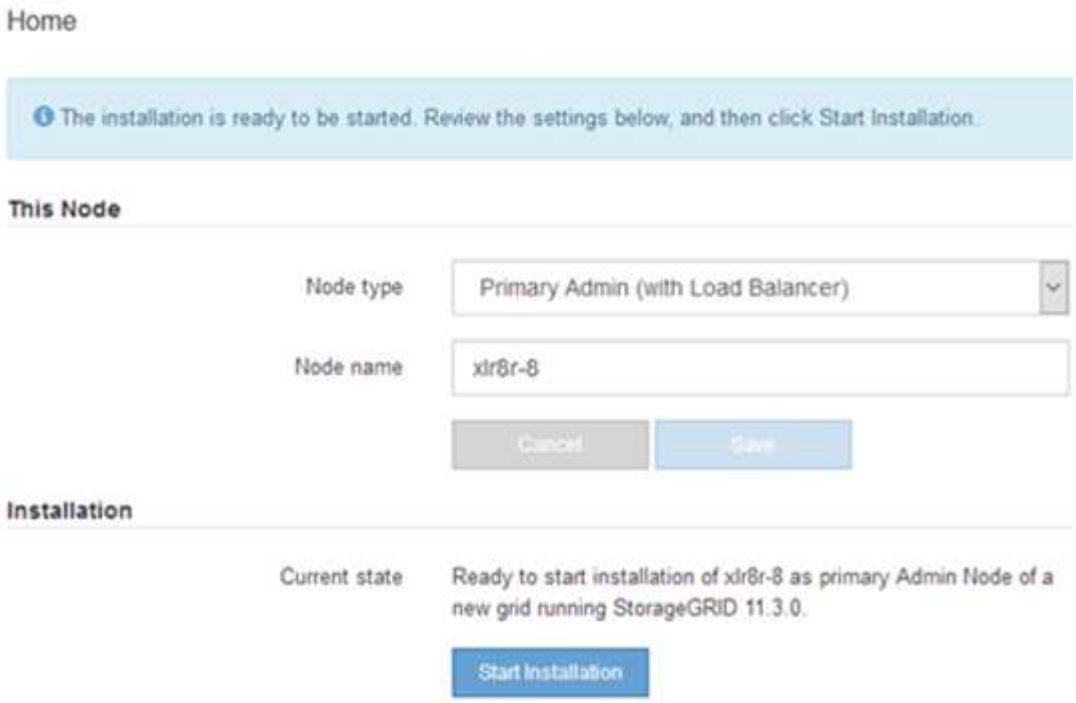
f. Wählen Sie **Home**, um zur Startseite zurückzukehren.

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 eines Node implementieren, beenden Sie den Implementierungsprozess hier und setzen Sie das Klonverfahren für den Node bei Recovery und Wartung fort.

"Verwalten Sie erholen"

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 in der Menüleiste auf **Monitor-Installation**.

Verwandte Informationen

"Services-Appliance wird als Gateway- oder nicht-primärer Admin-Node implementiert"

Services-Appliance wird als Gateway- oder nicht-primärer Admin-Node implementiert

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.

Was Sie benötigen

- 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.

Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte in der Recovery- und Wartungsanleitung zum Entfernen von Port-Remaps.

Der CLB-Service ist veraltet.

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

> Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisieren `configure-sga.py` Installationsskript für Geräte. Sie können das Appliance Installer auch zum Hochladen einer JSON-Datei verwenden, die Konfigurationsinformationen enthält. Siehe "Automatisierung der Installation und Konfiguration von Appliances".

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	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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.

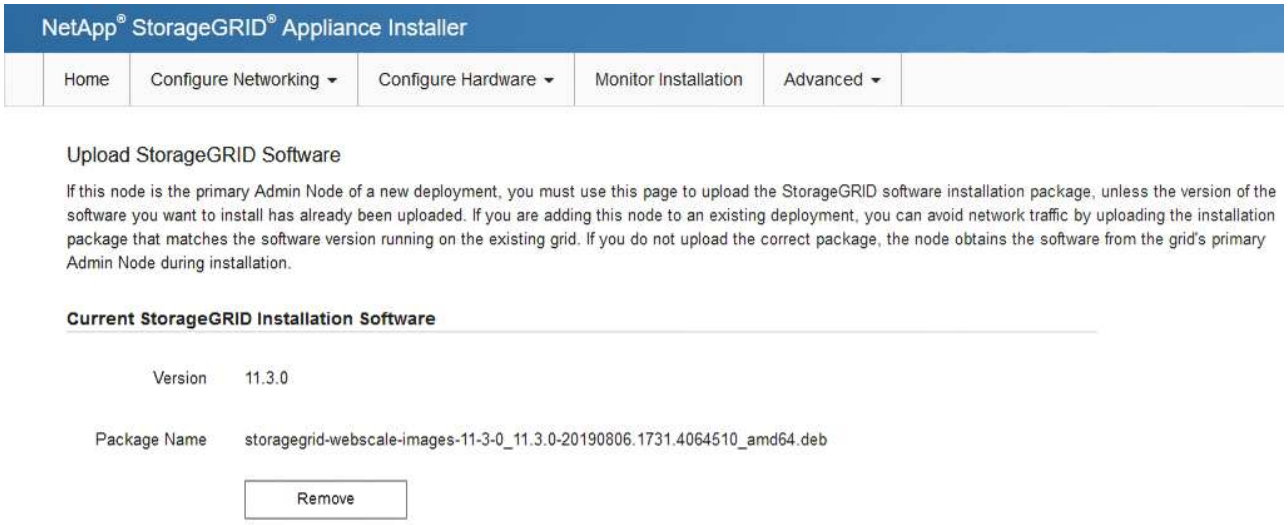
4. Geben Sie im Feld **Knotenname** den Namen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und klicken Sie auf **Speichern**.

   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.

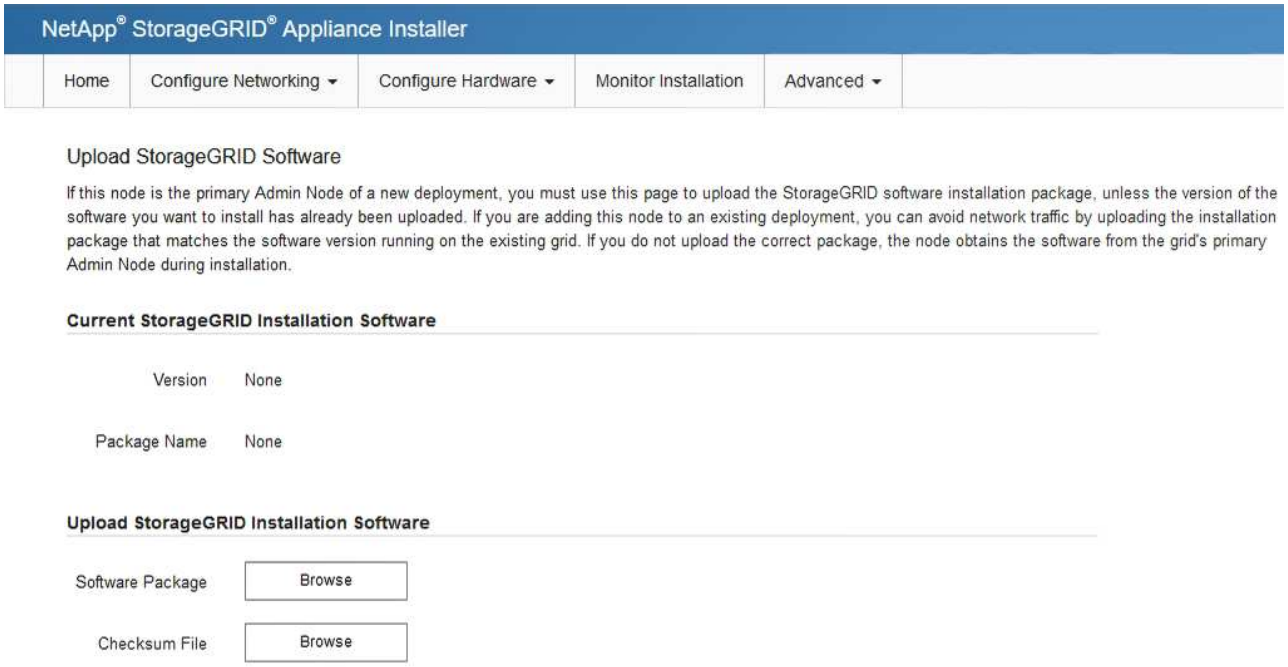
5. Führen Sie optional folgende Schritte aus, um eine andere Version der StorageGRID-Software zu installieren:
   a. Laden Sie das Installationsarchiv von der NetApp Downloads Seite zu StorageGRID herunter.

      "NetApp Downloads: StorageGRID"

   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.



e. Klicken Sie auf **Durchsuchen** für das Softwarepaket, das Sie heruntergeladen und extrahiert haben, und klicken Sie dann auf **Durchsuchen** für die Prüfsummendatei.

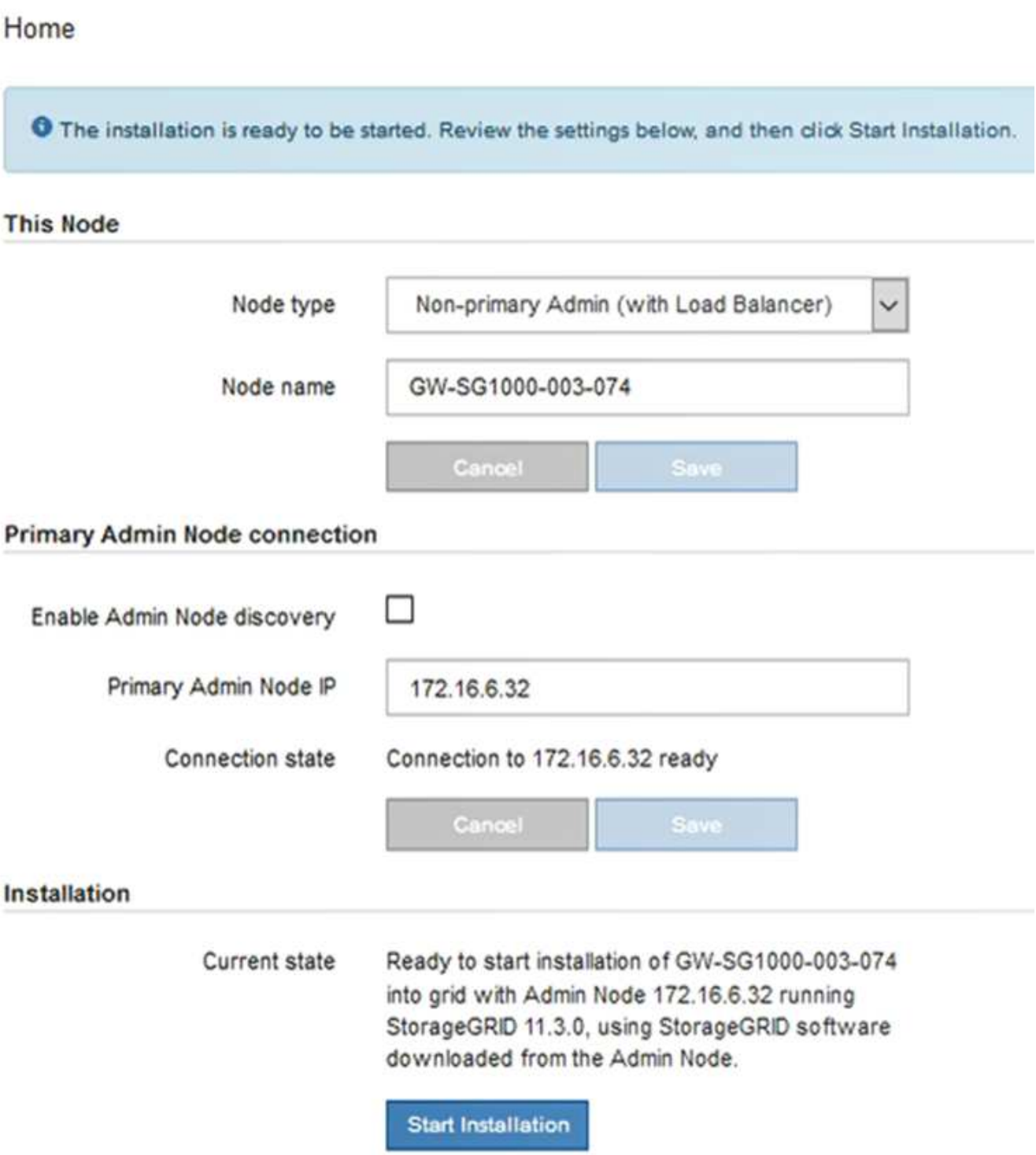


f. Wählen Sie **Home**, um zur Startseite zurückzukehren.

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 Installations- und Wartungsanleitung für Ihr Gerät.

7. 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**.

8. Wenn Ihr Grid mehrere Appliance-Nodes enthält, wiederholen Sie die vorherigen Schritte für jede Appliance.

Verwandte Informationen

"Bereitstellen einer Services Appliance als primärer Admin-Node"

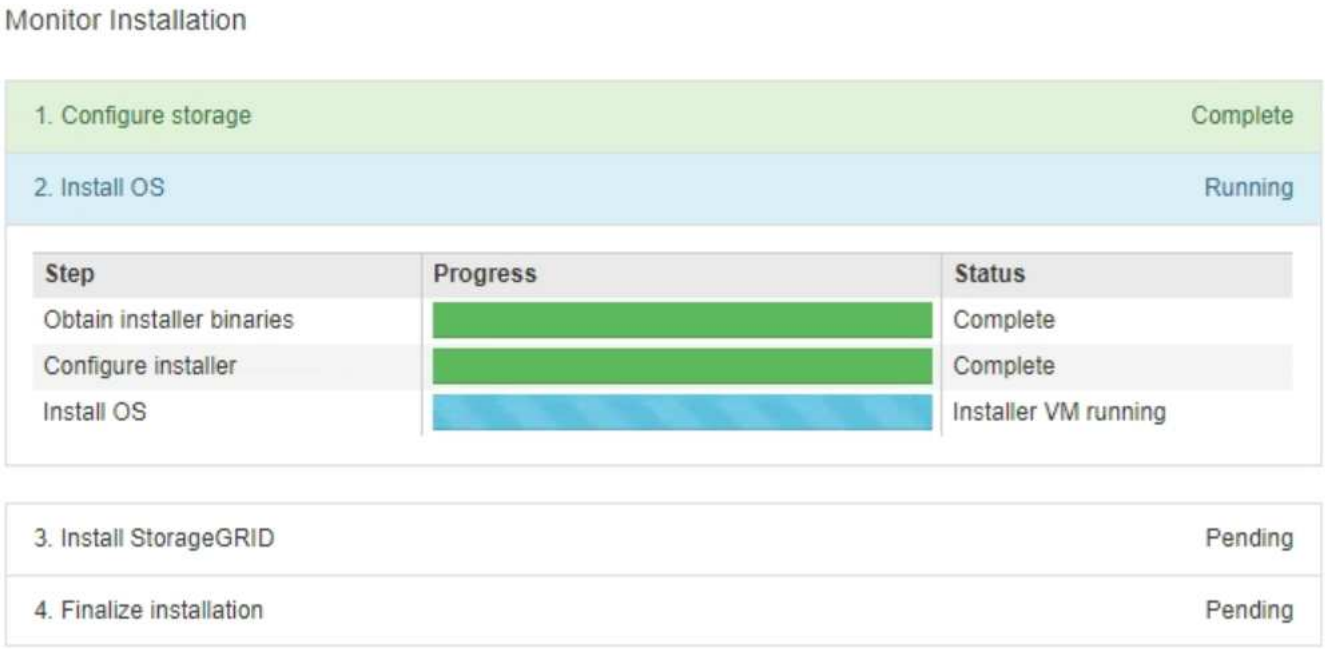
Überwachen der Installation der Services-Appliance

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.



   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 „`Skipped.`“ 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.

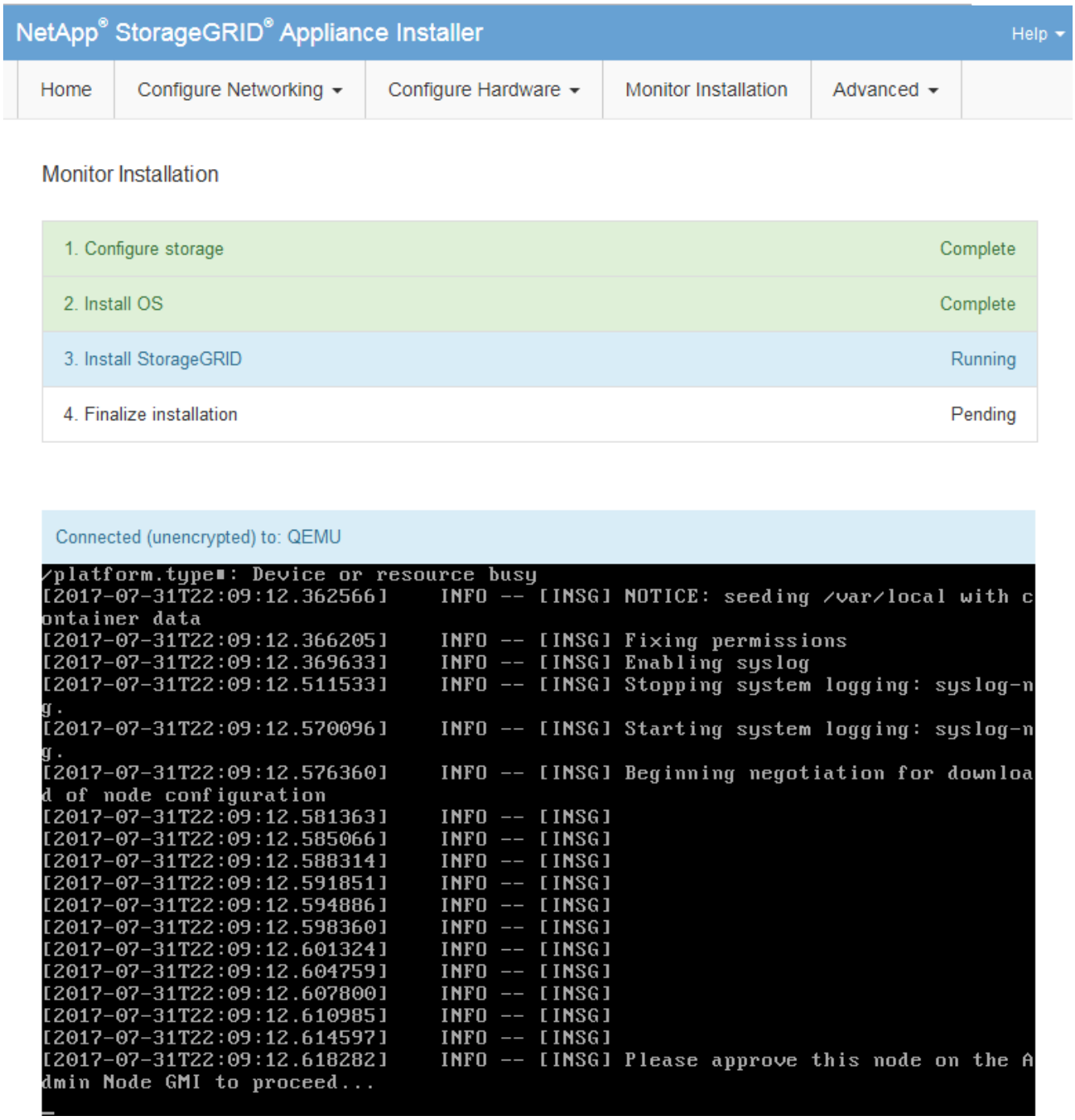
   - **2. Installieren Sie das Betriebssystem**

     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.
   - Bei der Installation des primären Administrator-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.



4. Wechseln Sie zum Grid-Manager, genehmigen Sie den ausstehenden Grid-Node und führen Sie den StorageGRID-Installationsprozess aus.

   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.

Automatisierung der Installation und Konfiguration von Appliances

Sie können die Installation und Konfiguration Ihrer Appliances und die Konfiguration des gesamten StorageGRID Systems automatisieren.

Über diese Aufgabe

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

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

- Erstellen Sie eine JSON-Datei, in der die Konfigurationseinstellungen für Ihre Appliances angegeben sind. Laden Sie die JSON-Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

  Sie können dieselbe Datei verwenden, um mehr als ein Gerät zu konfigurieren.

- Verwenden Sie die StorageGRID`configure-sga.py` Python-Skript zur Automatisierung der Konfiguration Ihrer Appliances.
- Zusätzliche Python-Skripte verwenden, um andere Komponenten des gesamten StorageGRID-Systems (das „Grid“) zu konfigurieren.

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. Weitere Informationen zum Herunterladen und Extrahieren der StorageGRID-Installationsdateien finden Sie in den Anweisungen zum Wiederherstellen und Verwalten.

Verwandte Informationen

"Verwalten Sie erholen"

Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer

Sie können die Konfiguration einer Appliance mithilfe einer JSON-Datei mit den Konfigurationsinformationen automatisieren. Sie laden die Datei mithilfe des StorageGRID-Appliance-Installationsprogramms hoch.

Was Sie benötigen

- Ihr Gerät muss mit der neuesten Firmware ausgestattet sein, die mit StorageGRID 11.5 oder höher kompatibel ist.
- Sie müssen mit dem Installationsprogramm für StorageGRID-Geräte auf der Appliance verbunden sein, die Sie mit einem unterstützten Browser konfigurieren.

Über diese Aufgabe

Sie können Appliance-Konfigurationsaufgaben automatisieren, z. B. die Konfiguration folgender Komponenten:

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

Die Konfiguration Ihrer Appliance mit einer hochgeladenen JSON-Datei ist häufig effizienter als die manuelle Ausführung der Konfiguration mit mehreren Seiten im StorageGRID-Appliance-Installationsprogramm,

insbesondere wenn Sie viele Knoten konfigurieren müssen. Sie müssen die Konfigurationsdatei für jeden Knoten einzeln anwenden.

> Erfahrene Benutzer, die sowohl die Installation als auch die Konfiguration ihrer Appliances automatisieren möchten, können das verwenden `configure-sga.py` Skript: +"Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

Schritte

1. Generieren Sie die JSON-Datei mit einer der folgenden Methoden:
   - Die ConfigBuilder-Anwendung

     "ConfigBuilder.netapp.com"

   - Der `configure-sga.py` Konfigurationsskript für die Appliance Sie können das Skript vom Installationsprogramm für StorageGRID-Geräte herunterladen (**Hilfe** > **Konfigurationsskript für Geräte**). Lesen Sie die Anweisungen zur Automatisierung der Konfiguration mit dem Skript configure-sga.py.

     "Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py"

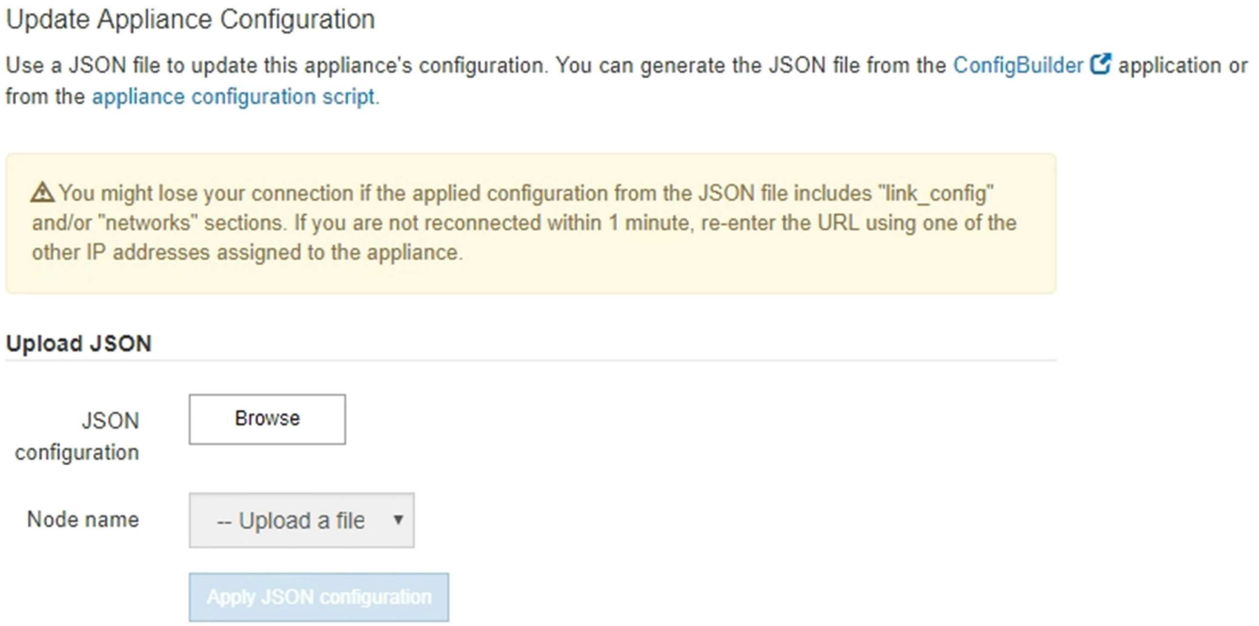
     Die Node-Namen in der JSON-Datei müssen die folgenden Anforderungen erfüllen:

     - Muss ein gültiger Hostname mit mindestens 1 und nicht mehr als 32 Zeichen sein
     - Es können Buchstaben, Ziffern und Bindestriche verwendet werden
     - Sie können nicht mit einem Bindestrich beginnen oder enden oder nur Zahlen enthalten

     > Stellen Sie sicher, dass die Node-Namen (die Top-Level-Namen) in der JSON-Datei eindeutig sind, oder Sie können mit der JSON-Datei nicht mehr als einen Node konfigurieren.

2. Wählen Sie **Erweitert** > **Appliance-Konfiguration Aktualisieren**.

   Die Seite Gerätekonfiguration aktualisieren wird angezeigt.



3. Wählen Sie die JSON-Datei mit der Konfiguration aus, die Sie hochladen möchten.

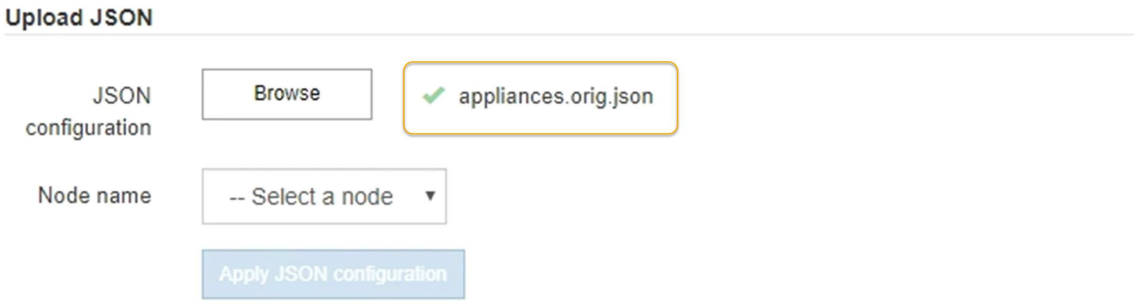
   a. Wählen Sie **Durchsuchen**.

   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 neben einem grünen Häkchen angezeigt.

   > Möglicherweise verlieren Sie die Verbindung zur Appliance, wenn die Konfiguration aus der JSON-Datei Abschnitte für „Link_config“, „Netzwerke“ oder beide enthält. Wenn Sie nicht innerhalb einer Minute eine Verbindung hergestellt haben, geben Sie die Appliance-URL mithilfe einer der anderen IP-Adressen, die der Appliance zugewiesen sind, erneut ein.

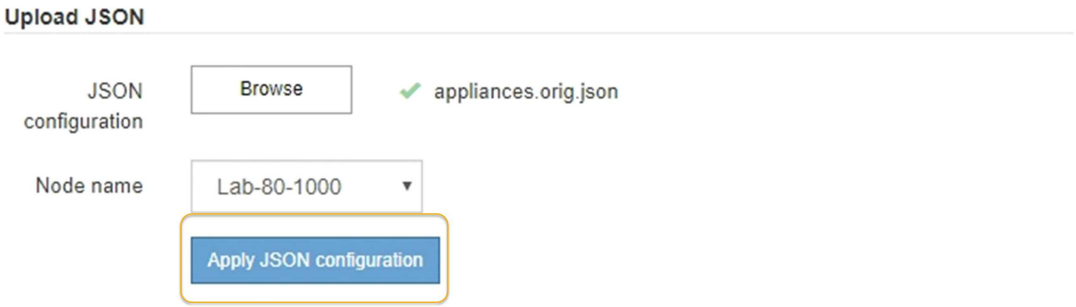


   Das Dropdown-Menü **Node Name** enthält die in der JSON-Datei definierten Node-Namen auf oberster Ebene.

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. Sie können ConfigBuilder verwenden, um sicherzustellen, dass Sie über eine gültige JSON-Datei verfügen.

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

   Die Schaltfläche **JSON-Konfiguration anwenden** ist aktiviert.



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

   Die Konfiguration wird auf den ausgewählten Knoten angewendet.

Automatische Installation und Konfiguration von Appliance-Knoten mithilfe des Skripts configure-sga.py

Sie können 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.

Was Sie benötigen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des StorageGRID Appliance Installer wurden Netzwerkverbindungen und IP-Adressen für den primären Administratorknoten konfiguriert.
- Wenn Sie den primären Admin-Node installieren, kennen Sie dessen IP-Adresse.
- Wenn Sie andere Knoten installieren und konfigurieren, wurde der primäre Admin-Node bereitgestellt, und Sie kennen seine IP-Adresse.
- Für alle anderen Nodes als den primären Admin-Node wurden alle auf der Seite IP-Konfiguration des Installationsprogramms der StorageGRID-Appliance aufgeführten Grid-Netzwerknetze in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- 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.

Dieses Verfahren richtet sich an fortgeschrittene Benutzer, die Erfahrung mit der Verwendung von Befehlszeilenschnittstellen haben. Alternativ können Sie die Konfiguration auch mit dem StorageGRID Appliance Installer automatisieren. +"Automatisierung der Appliance-Konfiguration mit dem StorageGRID Appliance Installer"

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`

3. Um die aktuelle Konfiguration des Appliance-Knotens zu bestätigen, geben Sie hier Folgendes ein *`SGA-install-ip`* Ist eine der IP-Adressen für den Appliance-Knoten:
   `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. #####
#####################################################################
```

4. 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`
5. 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 diese Datei nur dann vor, wenn Sie ein erfahrener Benutzer sind und über die StorageGRID APIs verfügen.

6. 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`
7. Wenn Sie das Gerät neu starten möchten, geben Sie Folgendes ein:
   `configure-sga.py reboot SGA-INSTALL-IP`

Nach der Implementierung der Grid-Nodes können Sie die Konfiguration des StorageGRID Systems automatisieren.

Was Sie benötigen

- 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.

   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 (JavaScript Object Notation) 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 Ihr StorageGRID-System zu Beginn konfigurieren, und wenn Sie eine primäre Admin-Knoten-Wiederherstellung durchführen müssen. Der Zugriff auf die Installations-API erfolgt über HTTPS vom Grid Manager.

Um die API-Dokumentation aufzurufen, gehen Sie zur Installations-Webseite auf dem primären Admin-Knoten 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 Bereitstellungsvorgang starten und den Status des Bereitstellungsvorgangs anzeigen.
- **Wiederherstellung** — primäre Admin-Knoten-Recovery-Operationen. Sie können Informationen zurücksetzen, das Wiederherstellungspaket hochladen, die Wiederherstellung starten und den Status des Wiederherstellungsvorgangs anzeigen.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Standorte** — Konfigurationsvorgänge auf Standortebene. 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 von Knotenklonen.
- **Verschlüsselung** — Operationen zur Verwaltung der Verschlüsselung und Anzeige des Verschlüsselungsstatus.
- **Hardwarekonfiguration** — Betrieb zur Konfiguration der Systemeinstellungen auf angeschlossener Hardware.
- **Installation** — Betrieb zum Starten der Gerätesallation und zur Überwachung des Installationsstatus.
- **Networking** — Vorgänge im Zusammenhang mit der Konfiguration von Grid-, Admin- und Client-Netzwerken für eine StorageGRID-Appliance und Appliance-Port-Einstellungen.
- **Setup** — Operationen zur Unterstützung bei der Ersteinrichtung der Appliance einschließlich Anfragen zum Abrufen von Informationen über das System und zur Aktualisierung der primären Admin-Node-IP.
- **Support** — Betrieb für den Neustart des Controllers und das Abrufen von Protokollen.
- **Upgrade** — Operationen im Zusammenhang mit der Aktualisierung der Appliance-Firmware.
- **Uploadsg** — Operationen zum Hochladen von StorageGRID-Installationsdateien.

Fehlerbehebung bei der Hardwareinstallation

Wenn während der Installation Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu Hardware-Setup- und Konnektivitätsproblemen überprüfen.

Verwandte Informationen

"Die Hardware-Einrichtung scheint zu hängen"

"Fehlerbehebung bei Verbindungsproblemen"

Anzeigen von Boot-Codes für das Gerät

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.

Was Sie benötigen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Wenn Sie eine kernelbasierte virtuelle Maschine (KVM) verwenden möchten, ist es Ihnen Erfahrung mit der Bereitstellung und Verwendung von KVM-Anwendungen.
- 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	• VGA-fähiger Monitor • VGA-Kabel
KVM	• KVM-Anwendung • RJ-45-Kabel
Serieller Port	• SERIELLES DB-9-Kabel • Serielles virtuelles Terminal
SOL	• 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-Management-Port her, und melden Sie sich bei der BMC Web-Schnittstelle 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 10.224.3.91 -U root -P calvin 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

"Zugriff auf die BMC-Schnittstelle"

Anzeigen von Fehlercodes für das Gerät

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.

Was Sie benötigen

- 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
0x5C	PEI-Phase BMC Selbsttest fehlgeschlagen
0xD0	CPU-Initialisierungsfehler

Codieren	Zeigt An
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

Die Hardware-Einrichtung scheint zu hängen

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

"Anzeigen von Boot-Codes für das Gerät"

"Anzeigen von Fehlercodes für das Gerät"

Fehlerbehebung bei Verbindungsproblemen

Wenn während der Installation der StorageGRID-Appliance Verbindungsprobleme auftreten, führen Sie die hier aufgeführten Korrekturmaßnahmen durch.

Es konnte keine Verbindung zum Gerät hergestellt werden

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 pingen :
   `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.

   Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.
4. Wenn der Ping erfolgreich war, öffnen Sie einen Webbrowser.
5. Geben Sie die URL für das StorageGRID-Appliance-Installationsprogramm ein:
   `https://appliances_controller_IP:8443`

   Die Startseite wird angezeigt.

Starten Sie die Services-Appliance neu, während das Installationsprogramm für StorageGRID-Appliances ausgeführt wird

Möglicherweise müssen Sie die Services-Appliance neu starten, während das Installationsprogramm für die StorageGRID-Appliance ausgeführt wird. Beispielsweise müssen Sie die Services-Appliance möglicherweise neu booten, wenn die Installation fehlschlägt.

Über diese Aufgabe

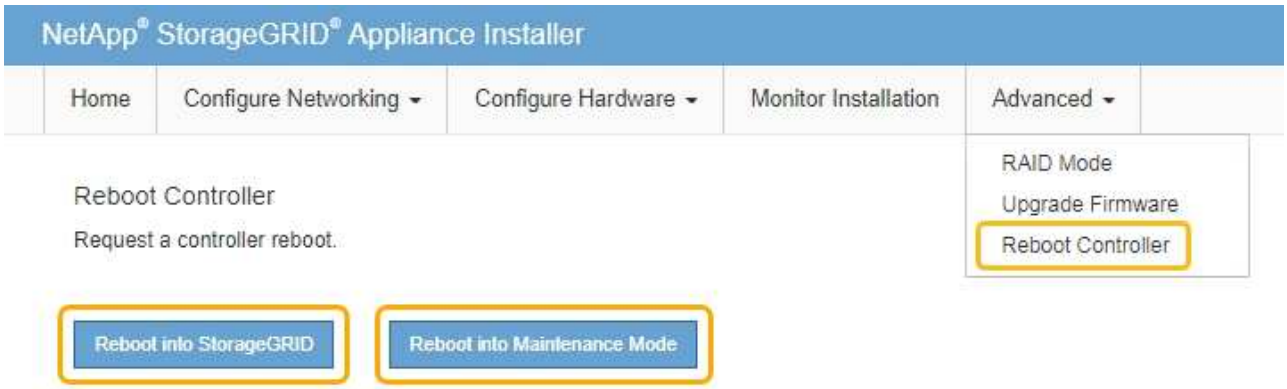
Dieses Verfahren gilt nur, wenn auf der Services-Appliance das Installationsprogramm der StorageGRID-Appliance ausgeführt wird. Nach Abschluss der Installation funktioniert dieser Schritt nicht mehr, da das Installationsprogramm für StorageGRID-Geräte nicht mehr verfügbar ist.

Schritte

1. Klicken Sie in der Menüleiste des StorageGRID-Appliance-Installationsprogramms auf **Erweitert** > **Controller neu starten**.

   Die Seite Controller neu booten wird angezeigt.
2. 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. Wählen Sie diese Option aus, wenn weitere Wartungsmaßnahmen erforderlich sind, die Sie auf dem Node durchführen müssen, bevor Sie das Raster neu beitreten.



Die Services-Appliance wird neu gestartet.

Warten des Geräts

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.

Schritte

- "Versetzen einer Appliance in den Wartungsmodus"
- "Durch ein- und Ausschalten des Controllers wird die LED angezeigt"
- "Lokalisierung des Controllers in einem Rechenzentrum"
- "Ersetzen der Service Appliance"
- "Ersetzen eines Netzteils in der Serviceanwendung"
- "Austausch eines Lüfters in der Service-Appliance"
- "Ersetzen eines Laufwerks in der Services-Appliance"
- "Ändern der Link-Konfiguration der Services Appliance"
- "Ändern der MTU-Einstellung"
- "Überprüfen der DNS-Serverkonfiguration"
- "Monitoring der Node-Verschlüsselung im Wartungsmodus"

Versetzen einer Appliance in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

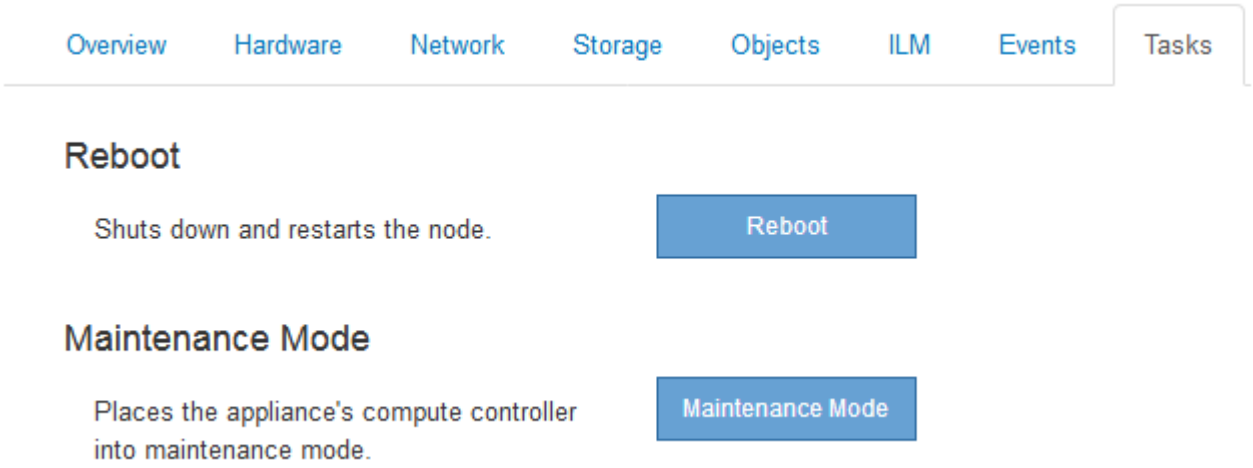
Über diese Aufgabe

Wenn Sie eine StorageGRID Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

> Das Passwort und der Hostschlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem, als das Gerät in Betrieb war.

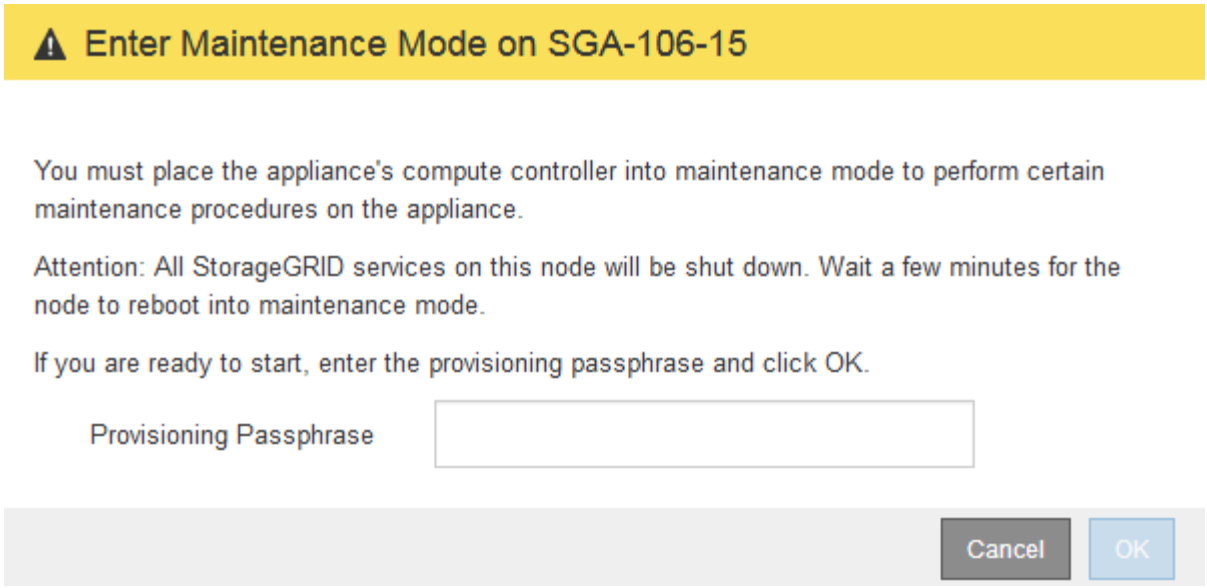
Schritte

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**.



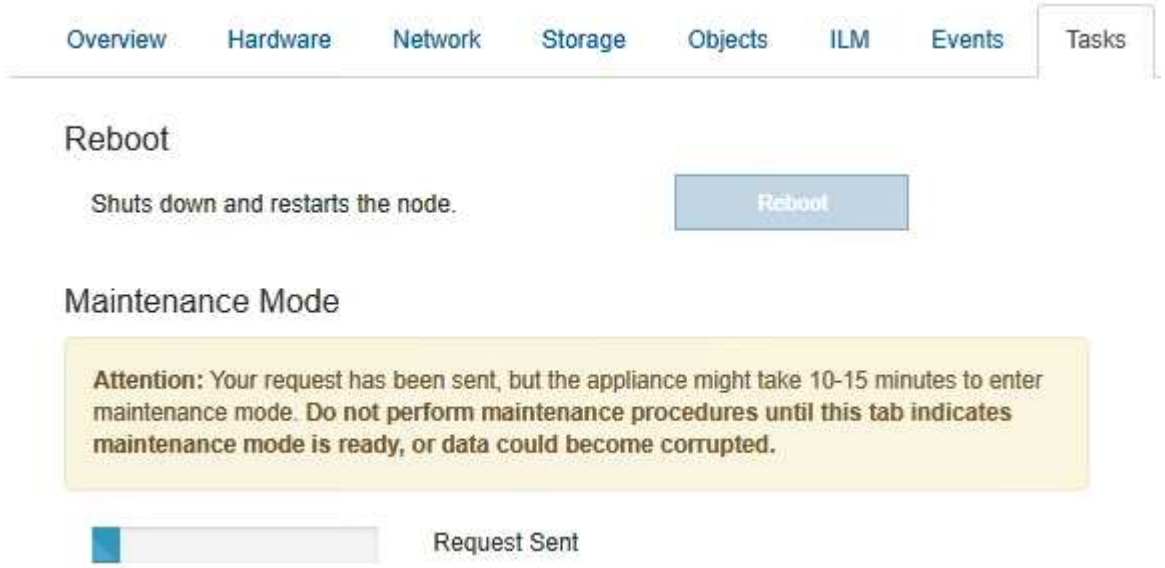
4. Wählen Sie **Wartungsmodus**.

   Ein Bestätigungsdialogfeld wird angezeigt.

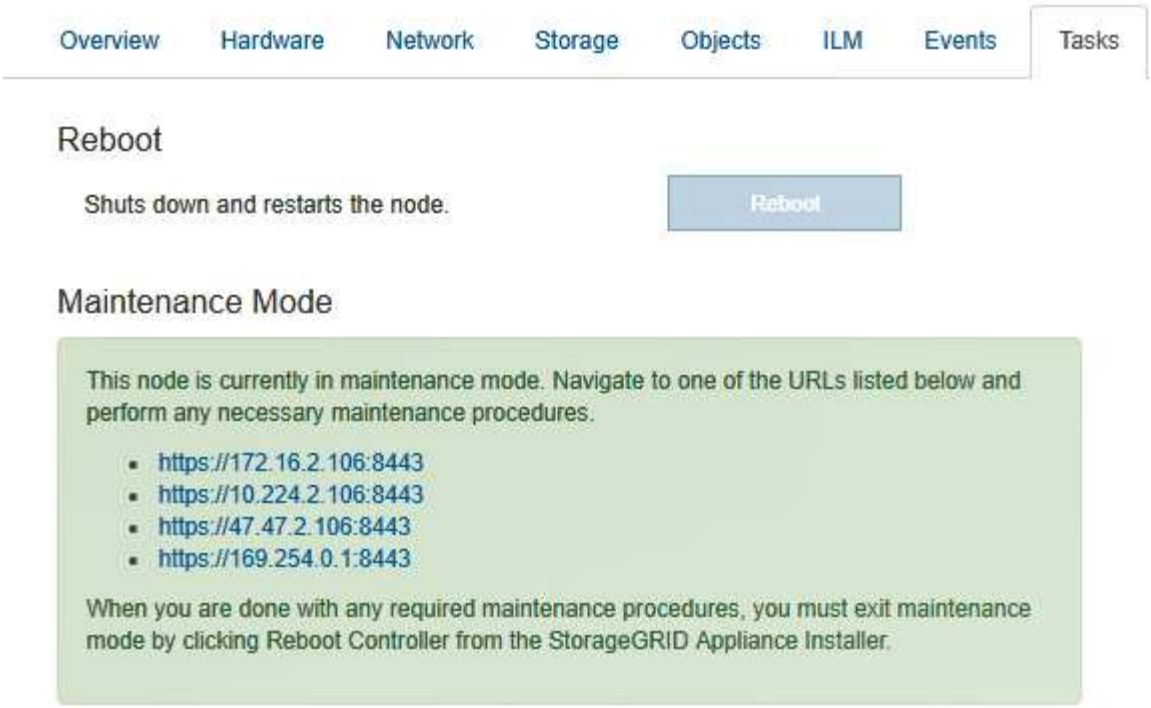


5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

   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.



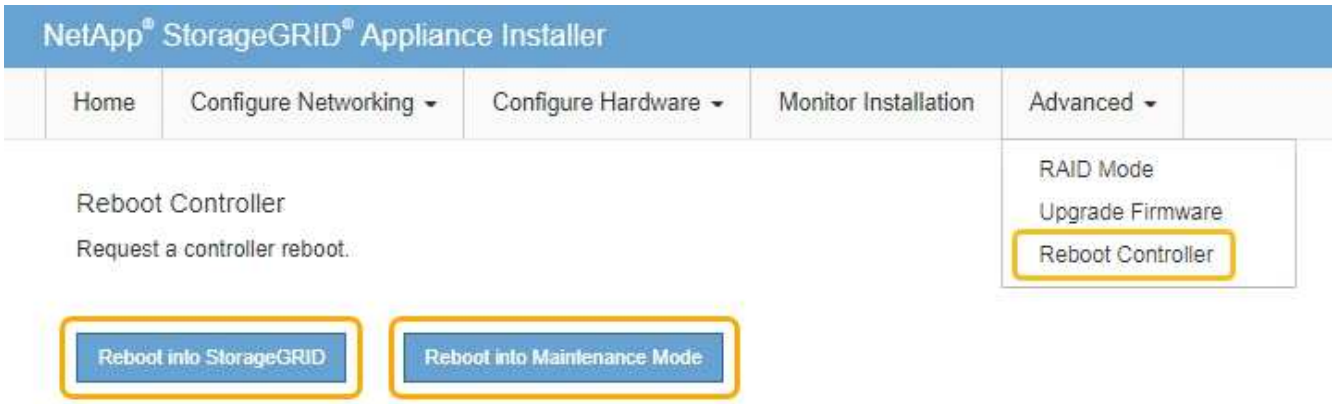
6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

   Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.

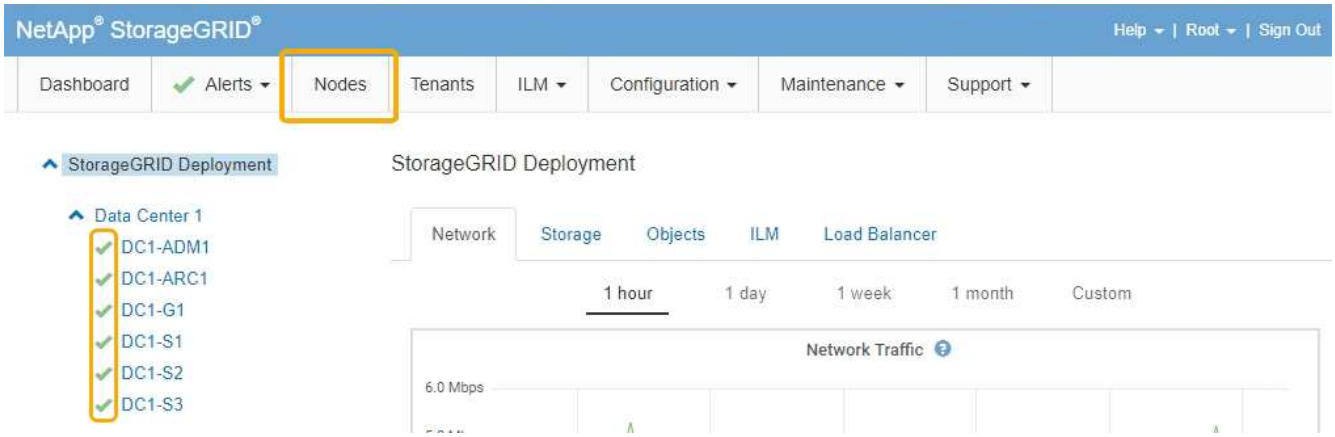
   > Zugriff Auf `https://169.254.0.1:8443` Erfordert eine direkte Verbindung zum lokalen Management-Port.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

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.



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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Durch ein- und Ausschalten des Controllers wird die LED angezeigt

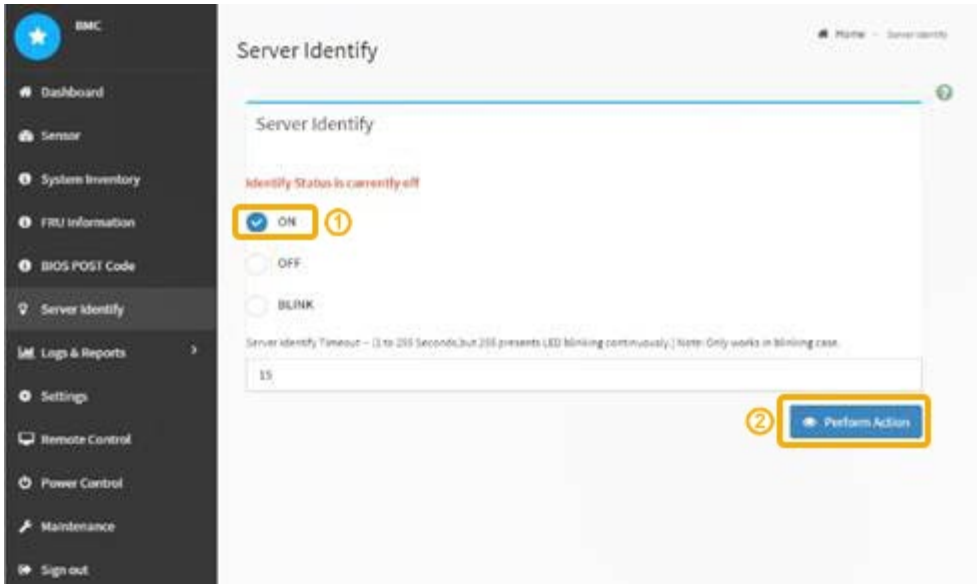
Die blaue Identify-LED auf der Vorder- und Rückseite des Controllers kann eingeschaltet werden, um das Gerät in einem Datacenter zu lokalisieren.

Was Sie benötigen

Sie müssen über die BMC-IP-Adresse des Controllers verfügen, den Sie identifizieren möchten.

Schritte

1. Greifen Sie auf die BMC-Schnittstelle des Controllers zu.
2. Wählen Sie **Server Identify** Aus.
3. Wählen Sie **EIN** und dann **Aktion durchführen** aus.



Ergebnis

Die blaue LED-Leuchte an der Vorder- (Abbildung) und Rückseite des Controllers.

Wenn eine Blende auf dem Controller installiert ist, kann es schwierig sein, die vordere Identify-LED zu erkennen.

Nachdem Sie fertig sind

Um den Controller auszuschalten, identifizieren Sie die LED:

- Drücken Sie den Schalter Identifikation LED an der Vorderseite des Controllers.
- Wählen Sie auf der BMC-Controller-Schnittstelle **Server Identify**, wählen Sie **AUS** und dann **Aktion** ausführen.

Die blauen LEDs an der Vorder- und der Rückseite des Controllers werden ausgeschaltet.

Verwandte Informationen

"Lokalisierung des Controllers in einem Rechenzentrum"

"Zugriff auf die BMC-Schnittstelle"

Lokalisierung des Controllers in einem Rechenzentrum

Suchen Sie den Controller, um Hardware-Wartungsarbeiten oder Upgrades durchzuführen.

Was Sie benötigen

- Sie haben festgestellt, welcher Controller gewartet werden muss.

  (Optional) um den Controller in Ihrem Rechenzentrum zu finden, schalten Sie die blaue Identify-LED ein.

  "Durch ein- und Ausschalten des Controllers wird die LED angezeigt"

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.

     "Durch ein- und Ausschalten des Controllers wird die LED angezeigt"

Ersetzen der Service Appliance

Möglicherweise müssen Sie das Gerät austauschen, wenn es nicht optimal funktioniert oder es ausgefallen ist.

Was Sie benötigen

- 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.
- Sie haben die Appliance, die Sie im Datacenter ersetzen, physisch gefunden. Siehe "Lokalisierung des Controllers in einem Rechenzentrum".
- Das Gerät wurde in den Wartungsmodus versetzt. Siehe "Versetzen einer Appliance in den Wartungsmodus".

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. Während Sie von anderen Hosts im selben Subnetz wie die Appliance auf das Installationsprogramm für StorageGRID-Geräte zugreifen können, können Sie 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. Wenn das Gerät in den Wartungsmodus versetzt wurde, fahren Sie das Gerät 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 das Gerät aus:

```
shutdown -h now
```

2. Überprüfen Sie anhand einer von zwei Methoden, ob das Gerät 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. Wenn die mit der Appliance verbundenen StorageGRID-Netzwerke DHCP-Server verwenden, aktualisieren Sie die Einstellungen für DNS/Netzwerk und IP-Adresse.
   a. Suchen Sie das MAC-Adressenetikett auf der Vorderseite des Geräts, und legen Sie die MAC-Adresse für den Admin-Netzwerkport fest.

      Auf dem MAC-Adressenetikett wird die MAC-Adresse für den BMC-Verwaltungsport aufgelistet.

      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.

   b. 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 neue 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.

4. Entfernen und ersetzen Sie das Gerät:
   a. Beschriften Sie die Kabel und trennen Sie dann die Kabel und alle Netzwerk-Transceiver.

      Um eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht 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.

      Befolgen Sie die Anweisungen zum Austausch dieser Komponenten.

   d. Setzen Sie das Ersatzgerät in den Schrank oder Rack ein.
   e. Ersetzen Sie die Kabel und optische Transceiver.
   f. 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.

5. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Verwandte Informationen

"Installieren des Geräts in einem Schrank oder Rack (SG100 und SG1000)"

"Anzeigen von Statusanzeigen an den SG100- und SG1000-Geräten"

"Anzeigen von Boot-Codes für das Gerät"

Ersetzen eines Netzteils in der Serviceanwendung

Das Services-Gerät 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.

Was Sie benötigen

- Sie haben das Ersatznetzteil entpackt.
- Sie haben das Gerät in physischer Lage, wo Sie das Netzteil im Datacenter ersetzen.

  "Lokalisierung des Controllers in einem Rechenzentrum"

- Sie können bestätigen, dass das andere Netzteil installiert ist und in Betrieb ist.

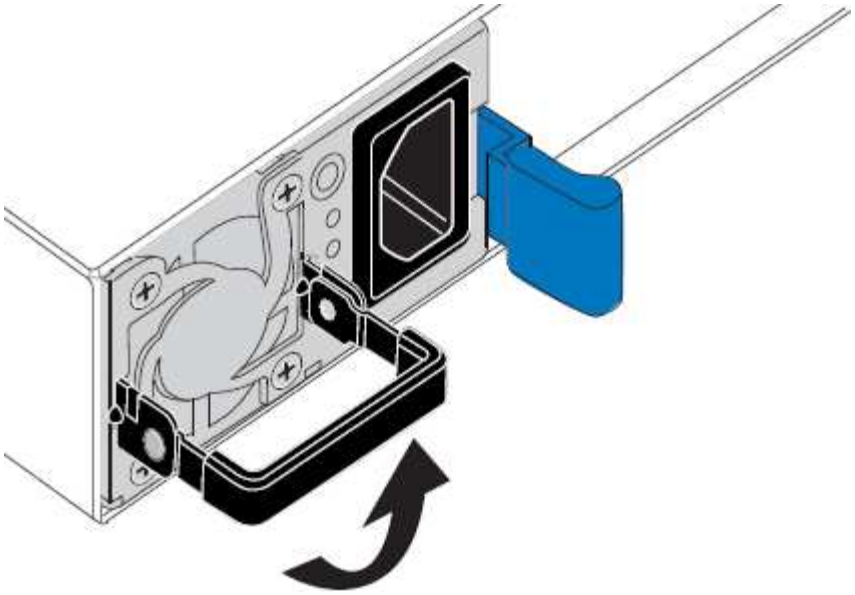
Über diese Aufgabe

Die Abbildung zeigt die beiden Netzteile des SG100, auf die von der Rückseite des Geräts zugegriffen werden kann.

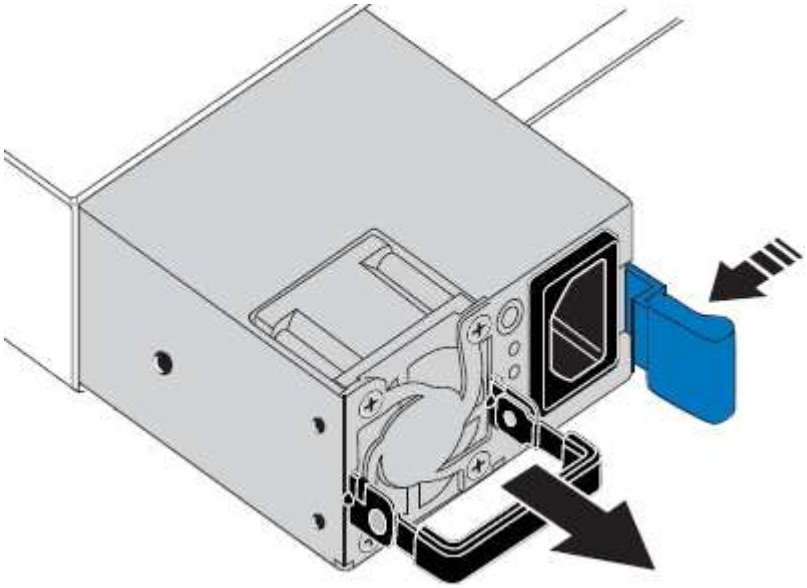
Die Netzteile für den SG1000 sind identisch.

Schritte

1. Ziehen Sie das Netzkabel vom Netzteil ab.
2. Heben Sie den Nockengriff an.

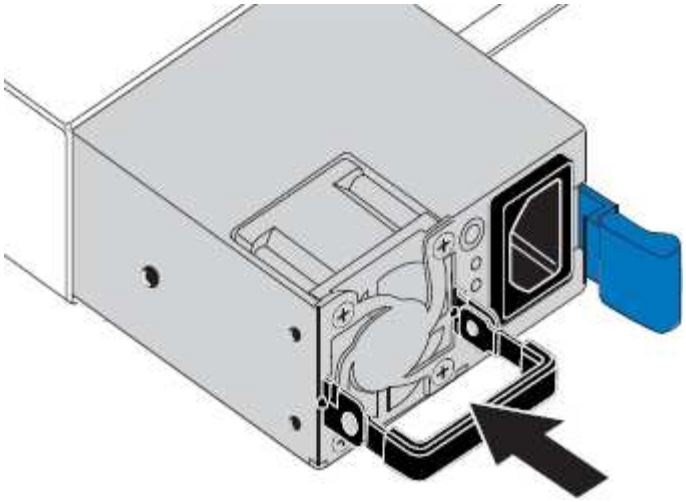


3. Drücken Sie auf den blauen Riegel, und ziehen Sie das Netzteil heraus.



4. Schieben Sie das Ersatznetzteil in das Gehäuse.

   Stellen Sie sicher, dass sich der blaue Riegel auf der rechten Seite befindet, wenn Sie das Gerät einschieben.



5. Drücken Sie den Nockengriff nach unten, um die Stromversorgung zu sichern.
6. Schließen Sie das Netzkabel an das Netzteil an, und stellen Sie sicher, dass die grüne LED leuchtet.

Austausch eines Lüfters 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.

Was Sie benötigen

- Sie haben den Ersatzlüfter ausgepackt.
- Sie haben die Appliance in physischer Lage, wo Sie den Lüfter im Datacenter austauschen.

  "Lokalisierung des Controllers in einem Rechenzentrum"

- Sie haben bestätigt, dass die anderen Lüfter installiert sind und ausgeführt werden.
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

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 Kühllüfter sind zugänglich, nachdem Sie die obere Abdeckung aus dem Gerät nehmen.

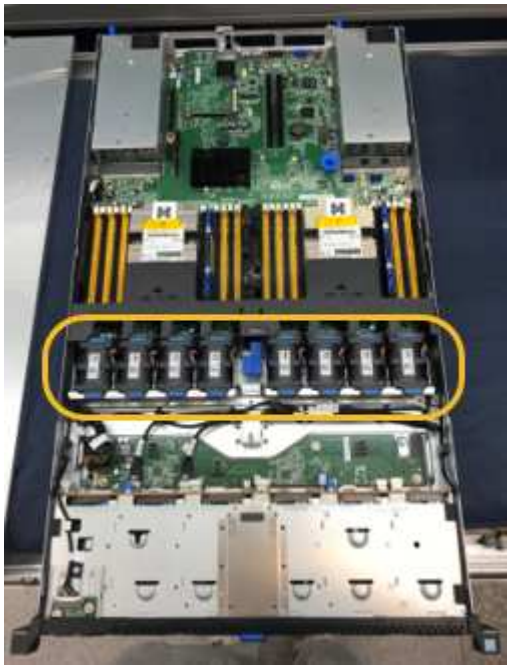
> Jede der beiden Netzteile enthält zudem einen Lüfter. Diese Lüfter sind in diesem Verfahren nicht enthalten.

Schritte

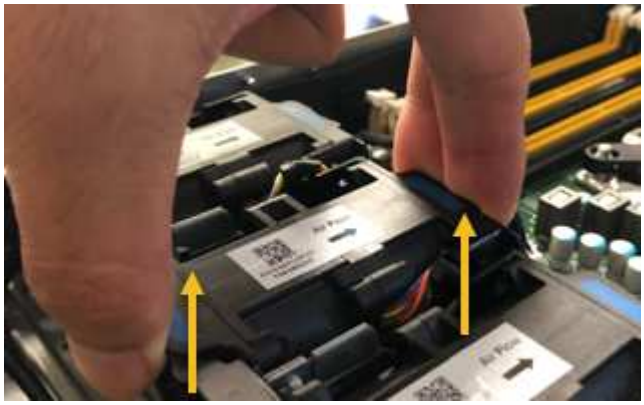
1. Wenn das Gerät in den Wartungsmodus versetzt wurde, fahren Sie das Gerät herunter.
   a. Melden Sie sich beim Grid-Node an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden 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 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. Heben Sie die Verriegelung an der oberen Abdeckung an, und entfernen Sie die Abdeckung vom Gerät.
4. Suchen Sie den Lüfter, der ausgefallen ist.

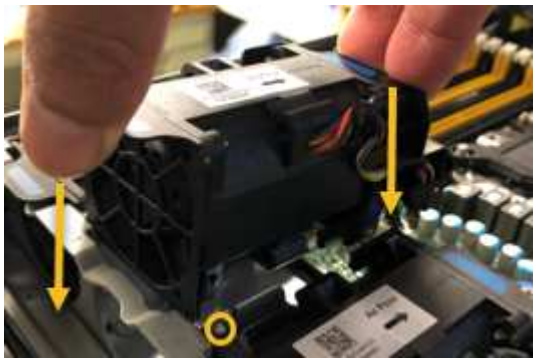


5. Heben Sie den defekten Lüfter aus dem Gehäuse.

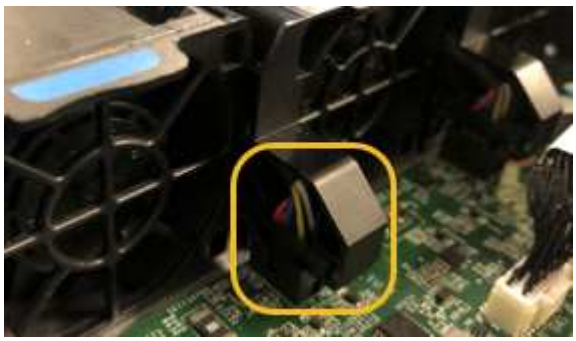


6. Schieben Sie den Ersatzlüfter in den offenen Steckplatz des Gehäuses.

   Führen Sie die Kante des Lüfters mit dem Führungsstift nach oben. Der Stift ist im Foto eingekreist.



7. Drücken Sie den Lüfteranschluss fest in die Leiterplatte.



8. Setzen Sie die obere Abdeckung wieder auf das Gerät, und drücken Sie die Verriegelung nach unten, um die Abdeckung zu sichern.
9. 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.

10. Vergewissern Sie sich, dass der Appliance-Node im Grid Manager angezeigt wird und keine Meldungen angezeigt werden.

Ersetzen eines Laufwerks 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.

Was Sie benötigen

- Sie haben die Appliance physisch gefunden, wo Sie das Laufwerk im Datacenter ersetzen.

  "Lokalisierung des Controllers in einem Rechenzentrum"

- Sie haben überprüft, welches Laufwerk ausgefallen ist, indem Sie die linke LED gelb blinken.

  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

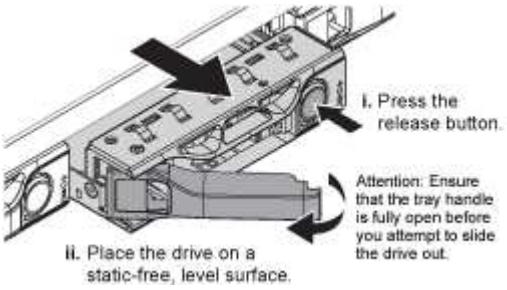
1. Stellen Sie sicher, dass die linke LED des Laufwerks gelb blinkt.

   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.

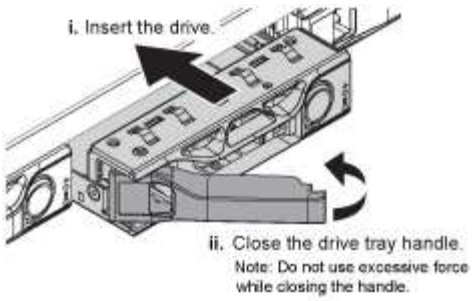
4. Drücken Sie die Entriegelungstaste am ausgefallenen Laufwerk.



   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 verwenden.

   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.

8. Wenden Sie sich an den technischen Support, um das Laufwerk auszutauschen.

   Der technische Support enthält Anweisungen zum Zurücksenden des ausgefallenen Laufwerks.

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.

Was Sie benötigen

- Sie müssen das Gerät in den Wartungsmodus versetzen. Wenn eine StorageGRID Appliance in den Wartungsmodus versetzt wird, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

  "Versetzen einer Appliance in den Wartungsmodus"

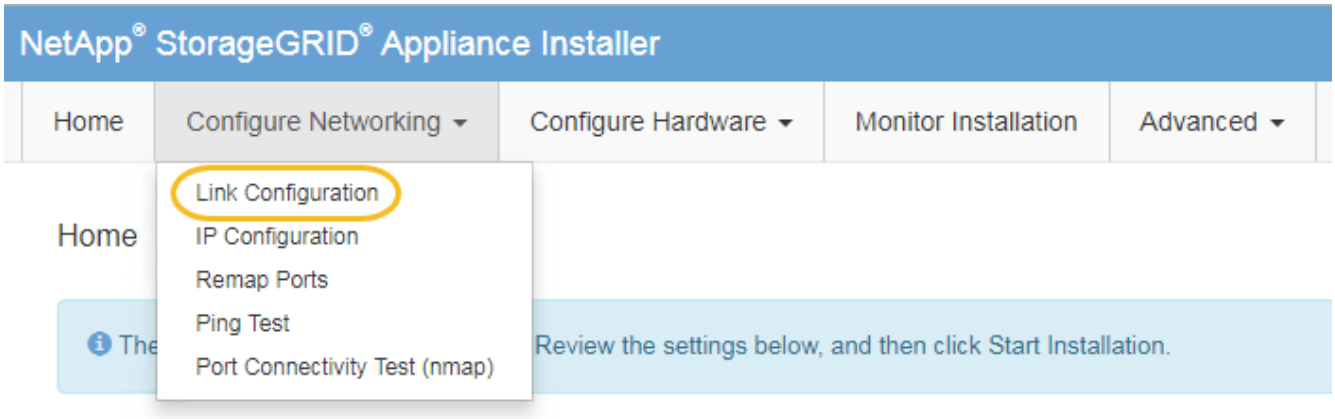
Über diese Aufgabe

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 „`Konfigurieren von Netzwerkverbindungen`“.

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 Sie nicht innerhalb einer Minute eine erneute Verbindung hergestellt haben, geben Sie die URL für das Installationsprogramm von StorageGRID-Geräten 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. Wenn Sie die IP-Adressen für die Appliance ändern müssen, befolgen Sie die Anweisungen zum Konfigurieren von IP-Adressen.

   "StorageGRID-IP-Adressen werden konfiguriert"

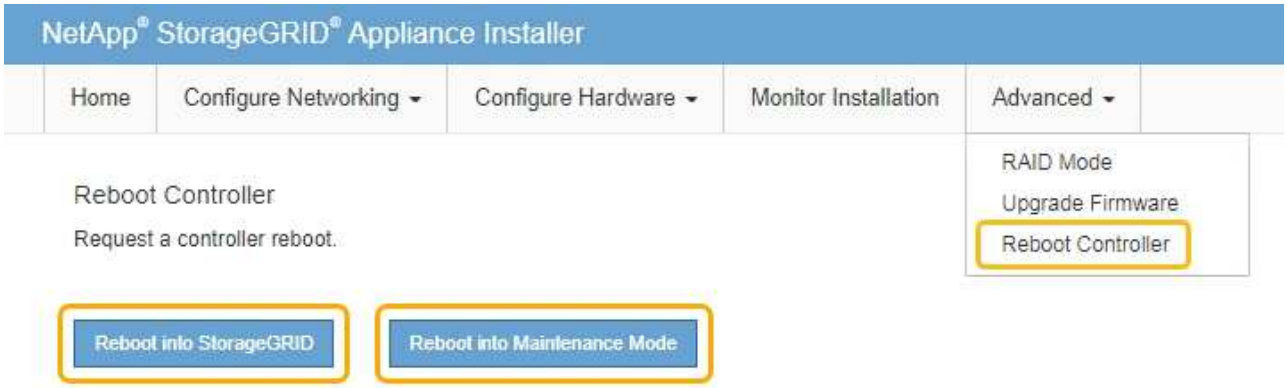
5. Wählen Sie im Menü die Option **Netzwerk konfigurieren** > **Ping-Test** aus.
6. Verwenden Sie das Ping-Test-Tool, um die Verbindung zu IP-Adressen in Netzwerken zu prüfen, die möglicherweise von den Änderungen der Verbindungskonfiguration betroffen sind, die Sie bei der Konfiguration der Appliance 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 pingen können. Gehen Sie gegebenenfalls zu den Anweisungen für die Konfiguration von Netzwerkverbindungen zurück, und beheben Sie etwaige Probleme.

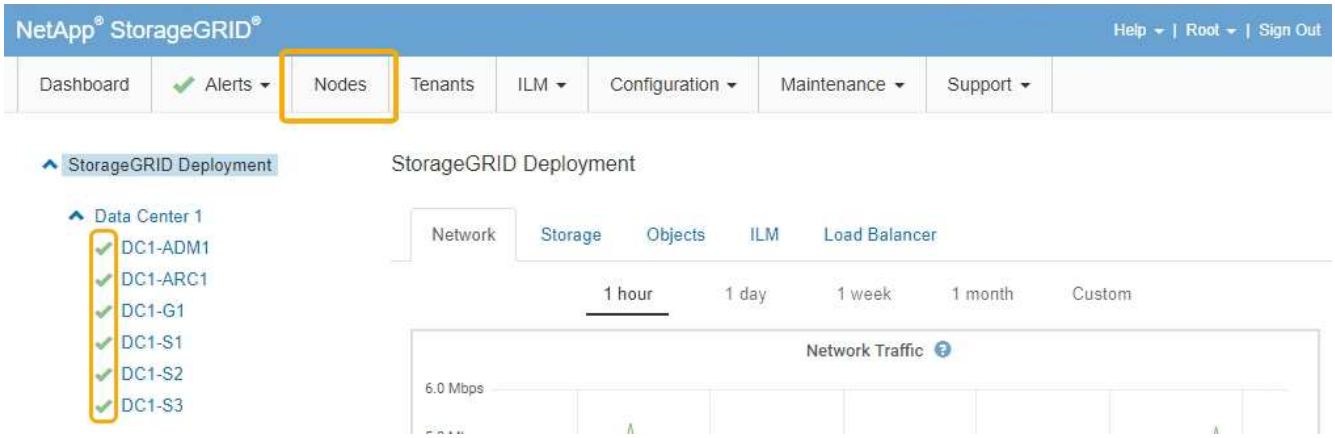
7. Sobald Sie zufrieden sind, dass die Änderungen an der Link-Konfiguration funktionieren, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Ändern der MTU-Einstellung

Sie können die MTU-Einstellung ändern, die Sie beim Konfigurieren von IP-Adressen für den Appliance-Node zugewiesen haben.

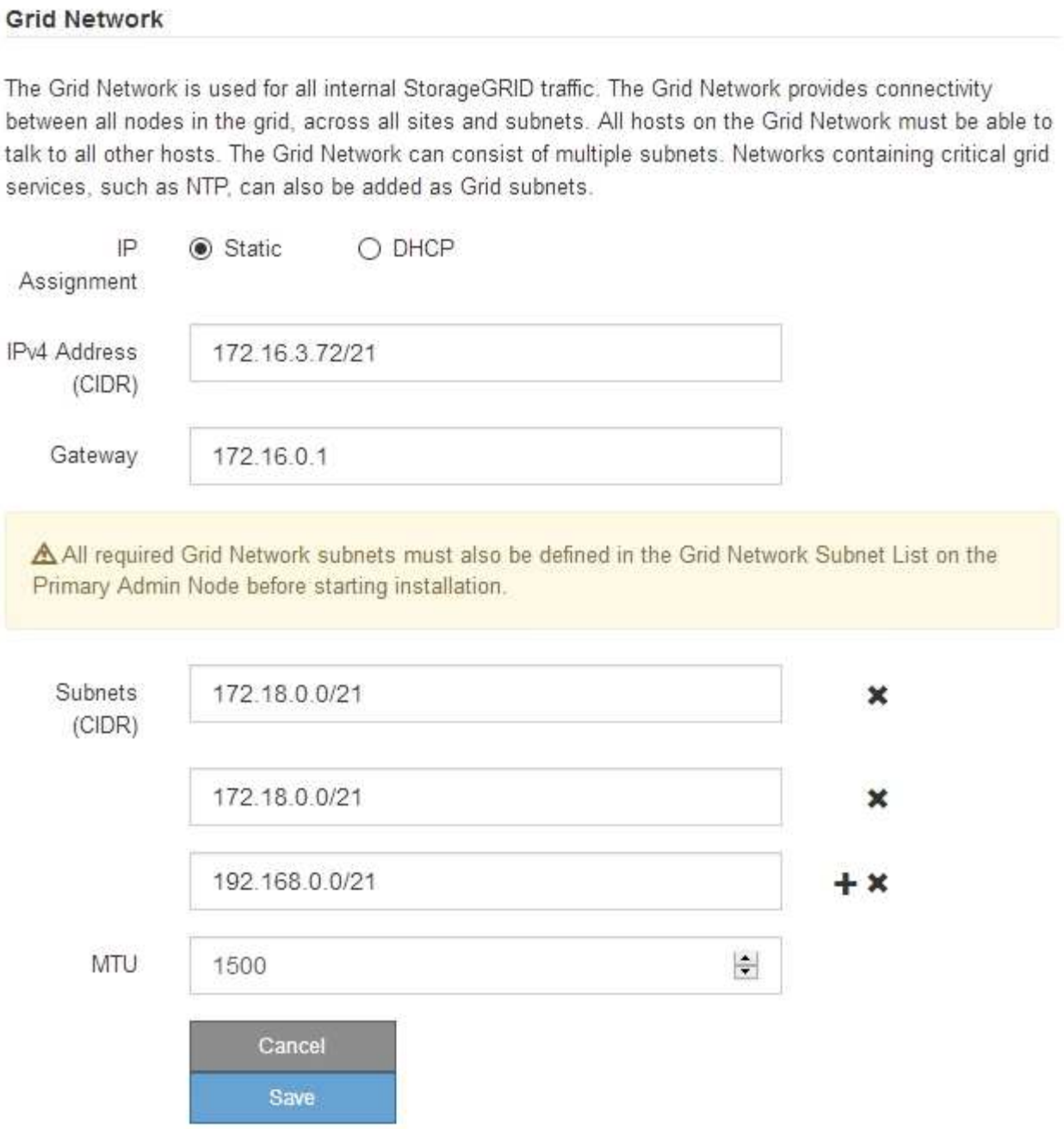
Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

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.



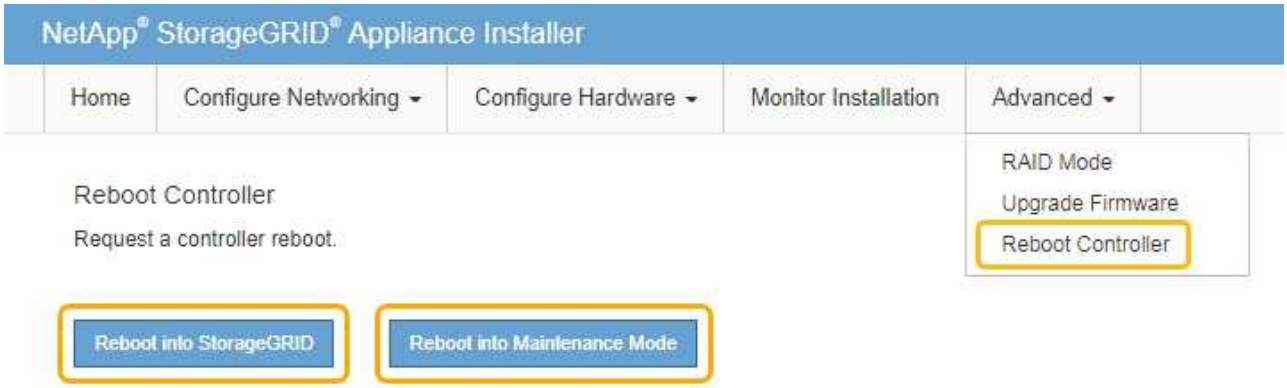
Der MTU-Wert des Netzwerks muss mit dem Wert übereinstimmen, der auf dem Switch-Port konfiguriert ist, mit dem der Node verbunden ist. Andernfalls können Probleme mit der Netzwerkleistung oder Paketverluste auftreten.

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 identisch sein.

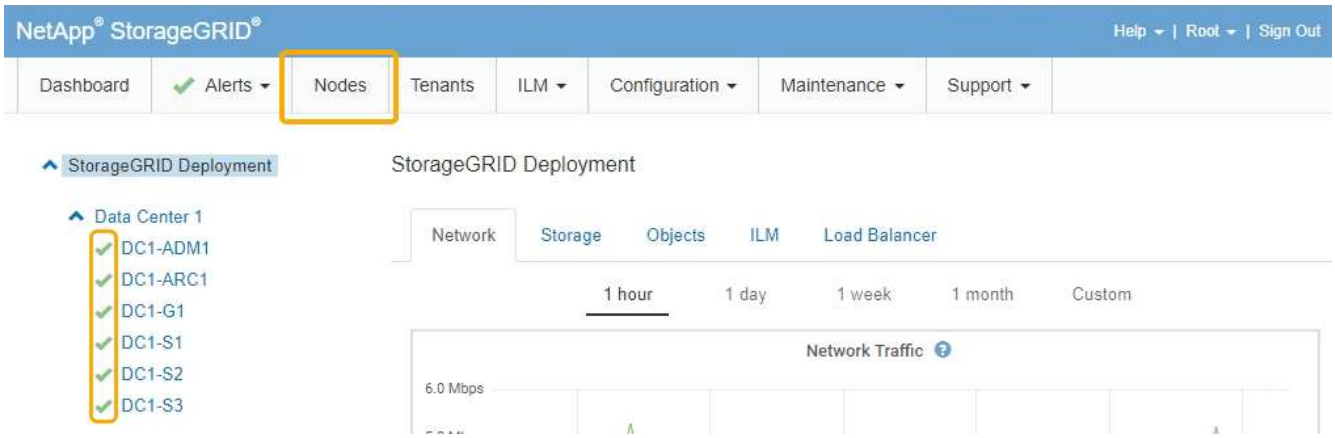
3. Wenn Sie mit den Einstellungen zufrieden sind, wählen Sie **Speichern**.
4. Booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option

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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Überprüfen der DNS-Serverkonfiguration

Sie können die DNS-Server (Domain Name System), die derzeit von diesem Appliance-Node verwendet werden, überprüfen und vorübergehend ändern.

Was Sie benötigen

Das Gerät wurde in den Wartungsmodus versetzt.

"Versetzen einer Appliance in den Wartungsmodus"

Über diese Aufgabe

Möglicherweise müssen Sie die DNS-Servereinstellungen ändern, wenn eine verschlüsselte Appliance sich nicht mit dem Verschlüsselungsmanagement-Server (KMS) oder dem KMS-Cluster verbinden kann, da der Hostname des 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 durchzuführen, geben Sie die DNS-Server im Grid Manager an (**Wartung** > **Netzwerk** > **DNS-Server**).

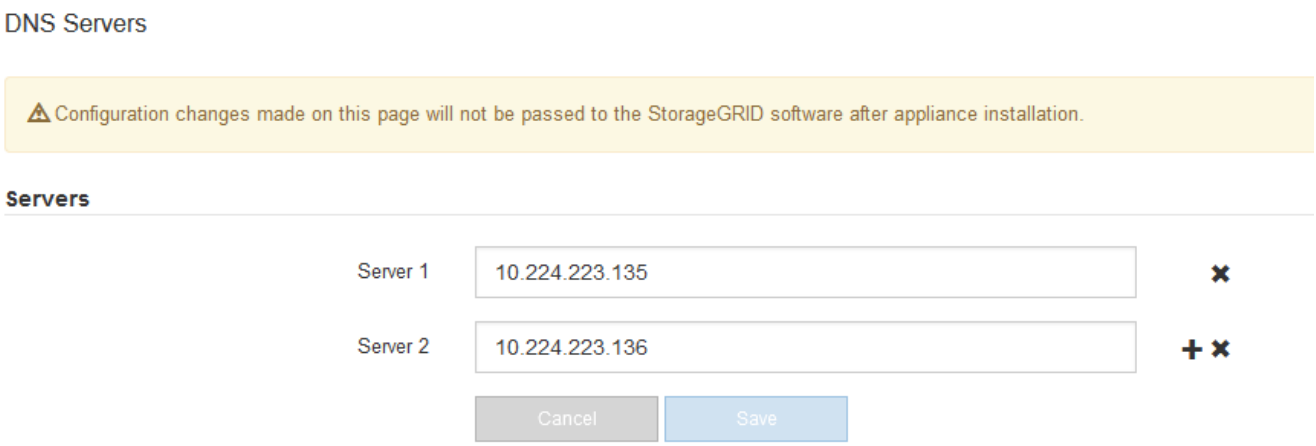
- Temporäre Änderungen an der DNS-Konfiguration sind nur für Node-verschlüsselte Appliances erforderlich, bei denen der KMS-Server mithilfe eines vollständig qualifizierten Domänennamens anstelle einer IP-Adresse für den Hostnamen definiert wird.
- Wenn eine Node-verschlüsselte Appliance über einen Domänennamen 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 Node keinen DNS-Server für das Grid erreichen kann oder wenn die DNS-Einstellungen für das gesamte Grid geändert wurden, wenn ein Node-verschlüsselter Appliance-Node offline war, kann der Node keine Verbindung mit dem KMS herstellen. Verschlüsselte Daten auf der Appliance können erst entschlüsselt werden, wenn das DNS-Problem behoben ist.

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 Node offline war, kann der Node nach seinem Wechsel wieder online den KMS nicht erreichen, 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.



3. Ändern Sie bei Bedarf die DNS-Server.

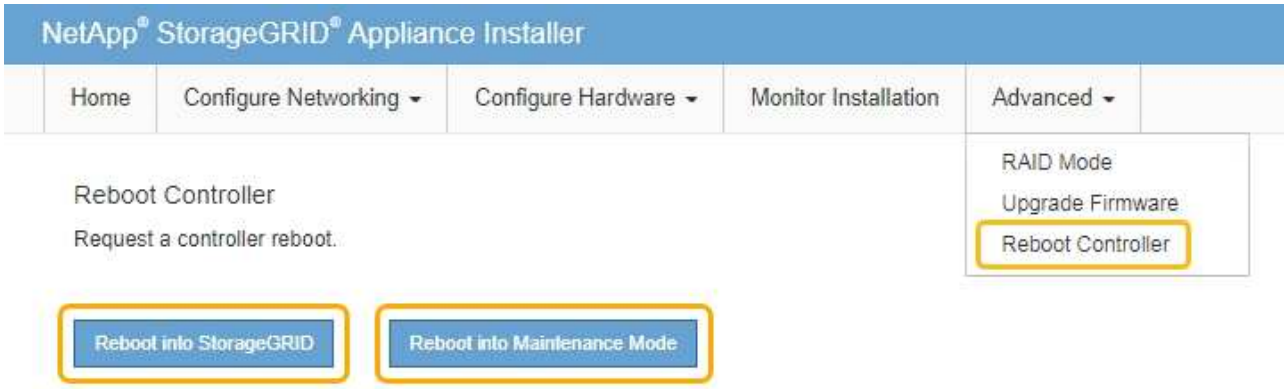
> Änderungen an den DNS-Einstellungen erfolgen temporär und gehen verloren, wenn Sie den Wartungsmodus beenden.

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.

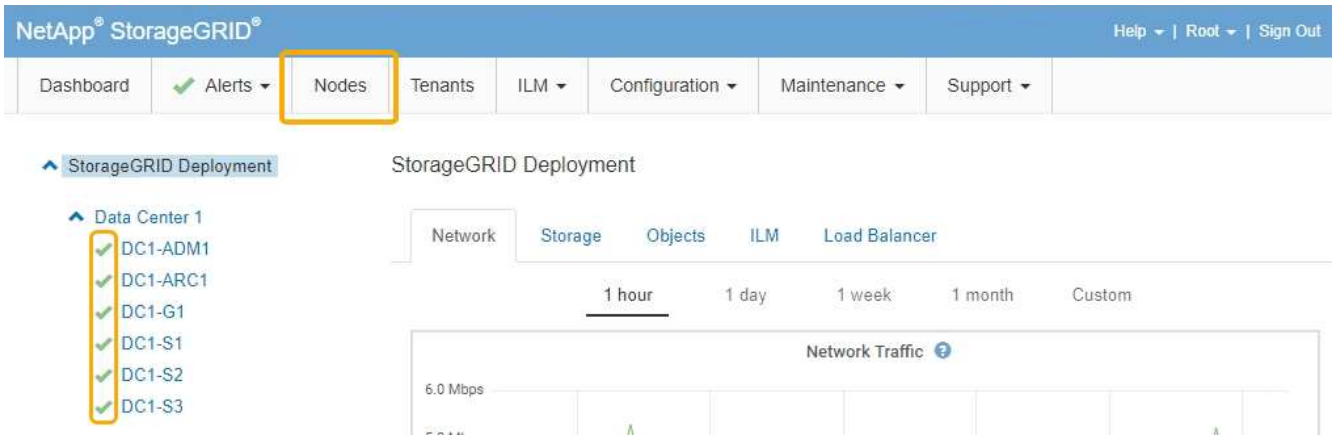
5. Nachdem die Node-Daten entschlüsselt wurden, booten Sie den Node neu. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert** > **Controller neu starten** aus, und wählen Sie dann eine der folgenden Optionen aus:

   - 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. 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 befand.

   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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Monitoring 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).

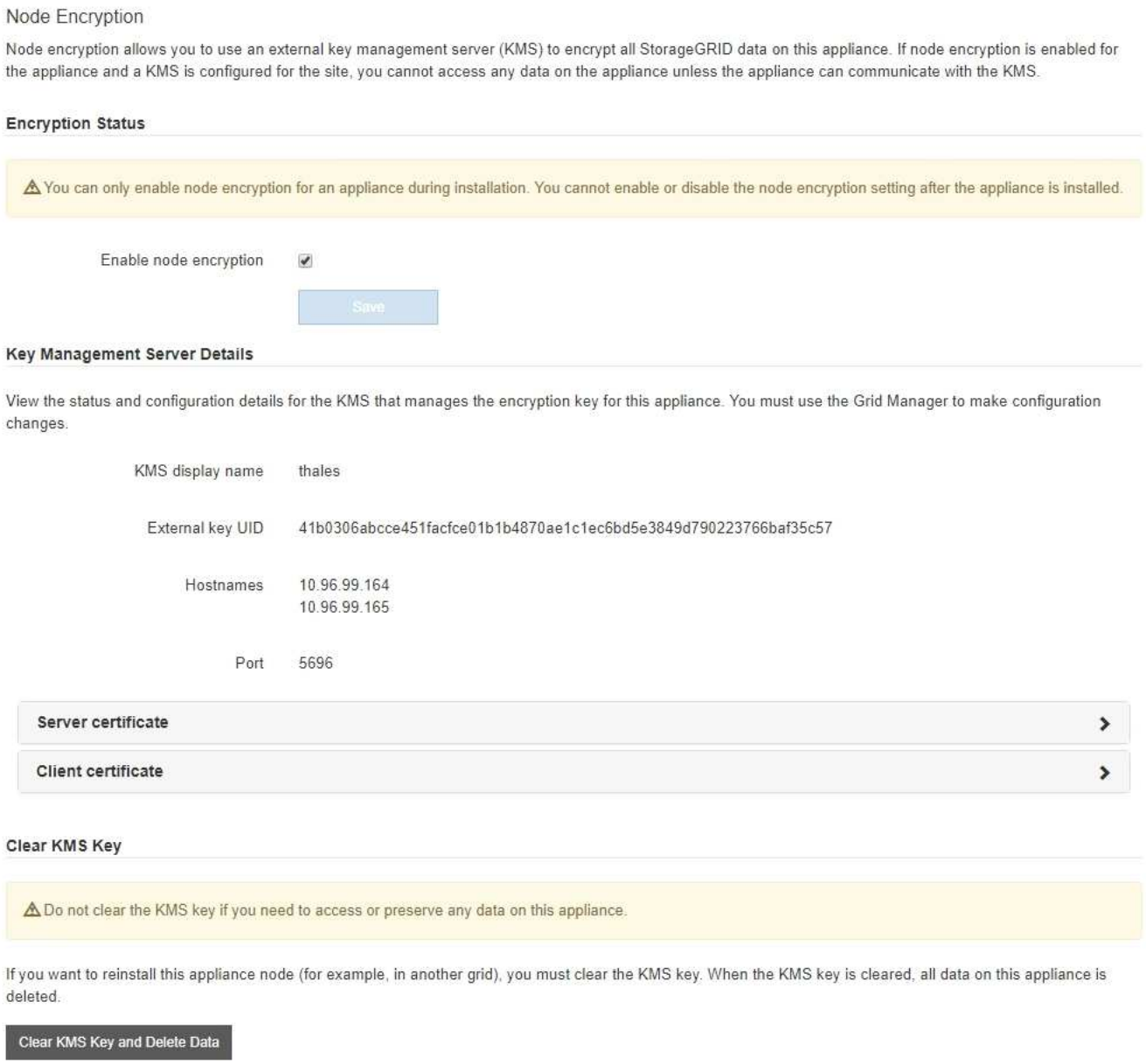
Was Sie benötigen

- Die Node-Verschlüsselung muss während der Installation für die Appliance aktiviert sein. Nach der Installation der Appliance können Sie die Node-Verschlüsselung nicht aktivieren.
- Das Gerät wurde in den Wartungsmodus versetzt.

  "Versetzen einer Appliance in den Wartungsmodus"

Schritte

1. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Hardware konfigurieren** > **Node-Verschlüsselung**.



Die Seite Node Encryption umfasst die folgenden 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.
  - Wenn Sie Probleme mit den Zertifikaten selbst beheben möchten, z. B. die Verlängerung abgelaufener Zertifikate, lesen Sie die Informationen zu KMS in den Anweisungen zur Verwaltung von StorageGRID.
  - Wenn bei der Verbindung zu KMS-Hosts unerwartete Probleme auftreten, überprüfen Sie, ob die DNS-Server (Domain Name System) korrekt sind und das Netzwerk der Appliance korrekt konfiguriert ist.

    "Überprüfen der DNS-Serverkonfiguration"

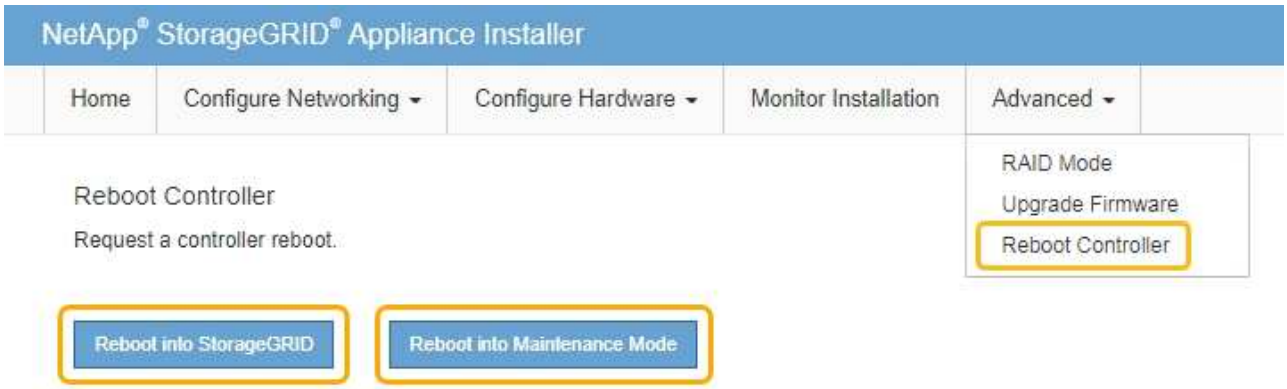
        - Wenden Sie sich an den technischen Support, wenn Sie Ihre Zertifikatsprobleme nicht lösen können.
    - Der klare KMS-Schlüssel deaktiviert die Node-Verschlüsselung für die Appliance, entfernt die Zuordnung zwischen der Appliance und dem für den StorageGRID-Standort konfigurierten Schlüsselmanagementserver und löscht alle Daten von der Appliance. Sie müssen den KMS-Schlüssel löschen, bevor Sie die Appliance in einem anderen StorageGRID-System installieren können.

      "Löschen der Konfiguration des Schlüsselverwaltungsservers"

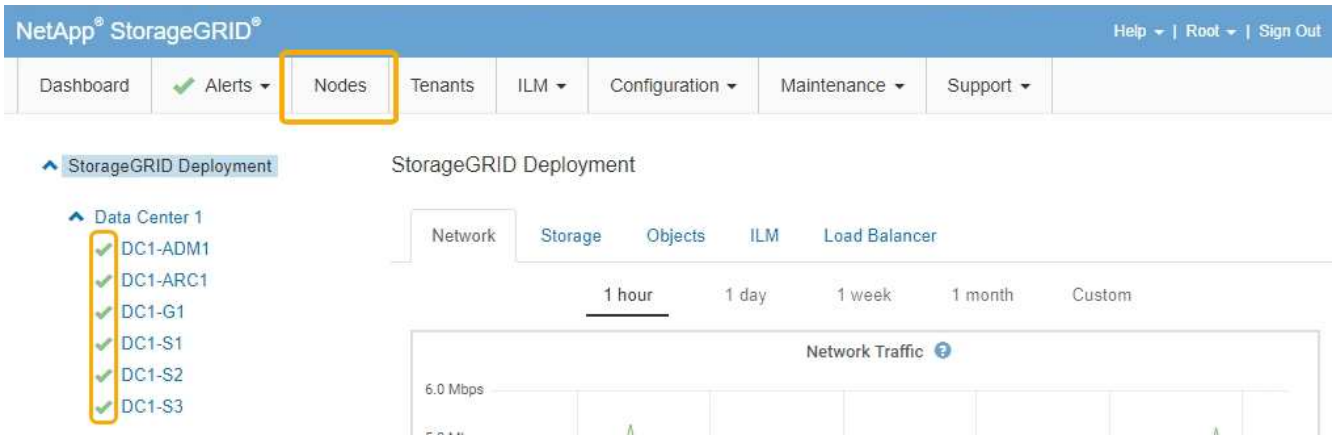
      Durch das Löschen der KMS-Konfiguration werden Daten von der Appliance gelöscht, sodass dauerhaft kein Zugriff darauf besteht. Diese Daten können nicht wiederhergestellt werden.

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. 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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Verwandte Informationen

"StorageGRID verwalten"

Löschen der Konfiguration des Schlüsselverwaltungsservers

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.

Was Sie benötigen

Wenn Daten auf der Appliance aufbewahrt werden müssen, müssen Sie einen Node außer Betrieb nehmen, 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.

Den Node muss deaktiviert werden, um alle in ihm enthaltenen Daten auf anderen Nodes in StorageGRID zu verschieben. Anweisungen zur Ausmusterung von Grid-Nodes finden Sie in den Angaben zu Recovery und Wartung.

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 Vorgang 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 eine Neuinstallation eines Appliance-Node in einem StorageGRID-System planen, das denselben KMS-Schlüssel verwendet.

- 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.

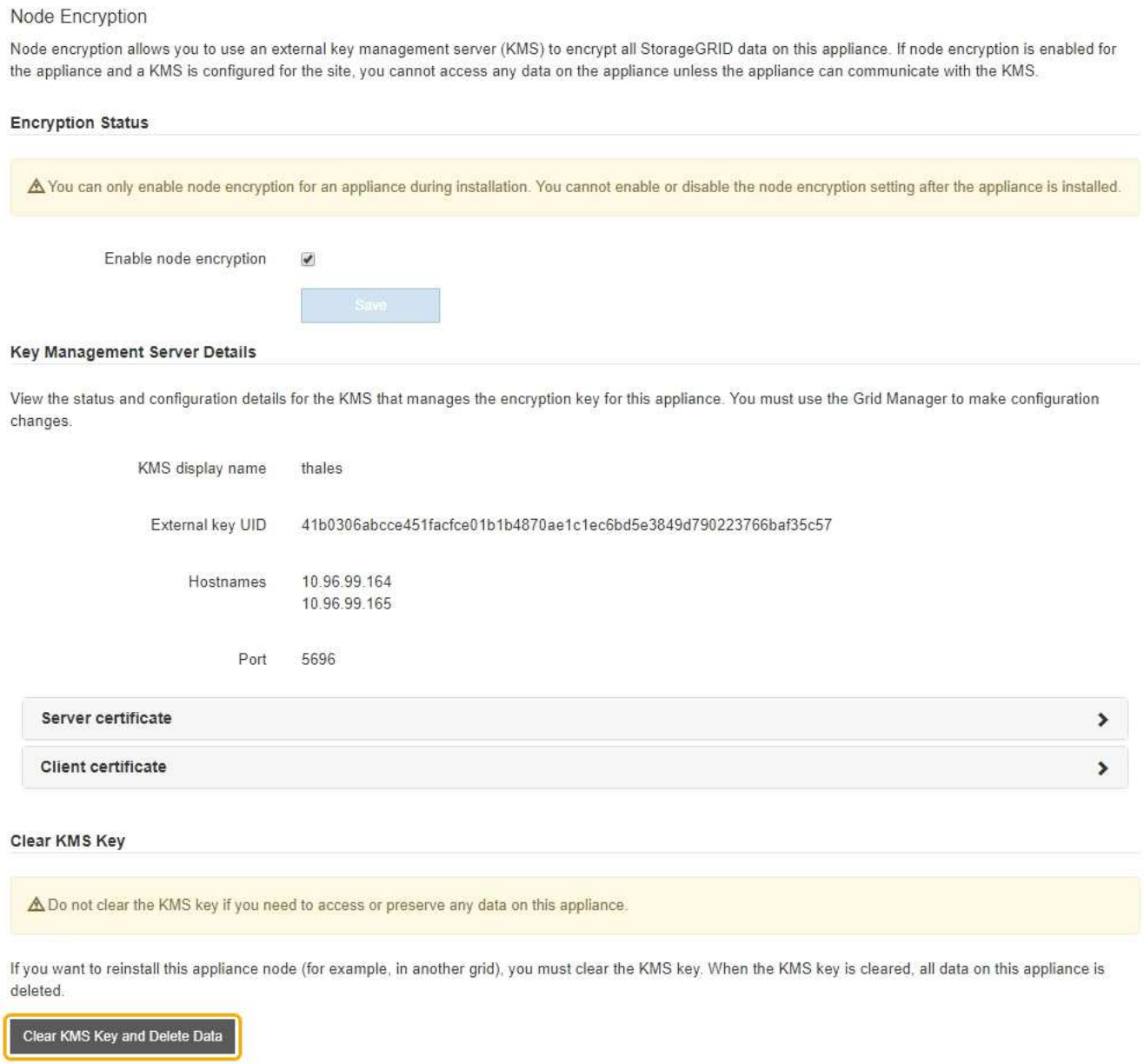
Schritte

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.

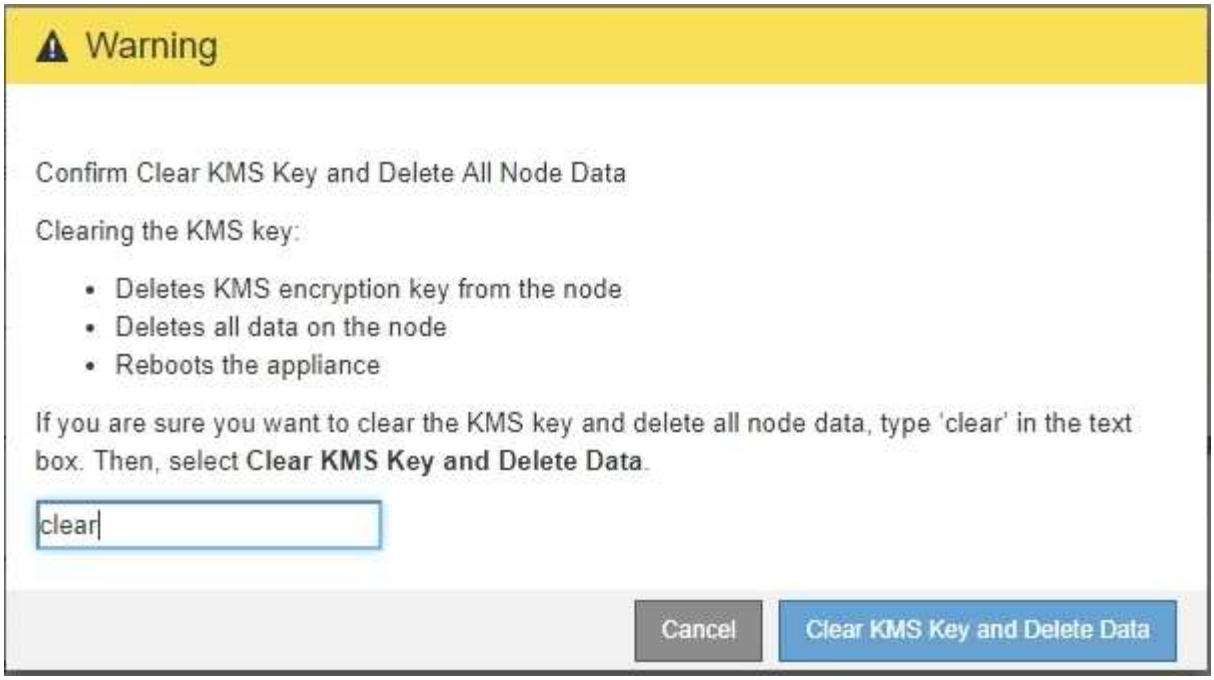
   Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

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` Und wählen Sie **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. Informationen zur Vorbereitung einer Appliance für die Neuinstallation finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Verwandte Informationen

"StorageGRID verwalten"

"Verwalten Sie erholen"

Konfiguration und Management

StorageGRID verwalten

Erfahren Sie, wie das StorageGRID System konfiguriert wird.

- "Verwalten eines StorageGRID-Systems"
- "Kontrolle des Administratorzugriffs auf StorageGRID"
- "Konfigurieren von Verschlüsselungsmanagement-Servern"
- "Management von Mandanten"
- "Konfigurieren von S3- und Swift-Client-Verbindungen"
- "Verwalten von StorageGRID-Netzwerken und -Verbindungen"
- "AutoSupport wird konfiguriert"
- "Verwalten Von Storage-Nodes"
- "Verwalten Von Admin-Nodes"
- "Verwalten Von Archivierungs-Knoten"
- "Datenmigration zu StorageGRID"

Verwalten eines StorageGRID-Systems

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

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.

> Die Anweisungen zum Management von Objekten mit Regeln und Richtlinien für das Information Lifecycle Management (ILM) wurden in verschoben"Objektmanagement mit ILM".

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

Was Sie benötigen

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

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Grid Manager an

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

Was Sie benötigen

- Sie müssen über Ihre Anmeldedaten verfügen.
- Sie müssen über die URL für den Grid Manager verfügen.
- Sie müssen einen unterstützten Webbrowser verwenden.
- Cookies müssen in Ihrem Webbrowser aktiviert sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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 genau die gleichen:

- Die auf einem Admin-Knoten ausgemachten Alarmbestätigungen (Legacy-System) werden nicht auf 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.

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

Schritte

1. Starten Sie einen unterstützten Webbrowser.

2. Geben Sie in der Adressleiste des Browsers die URL für den Grid Manager ein:

   `https://FQDN_or_Admin_Node_IP/`

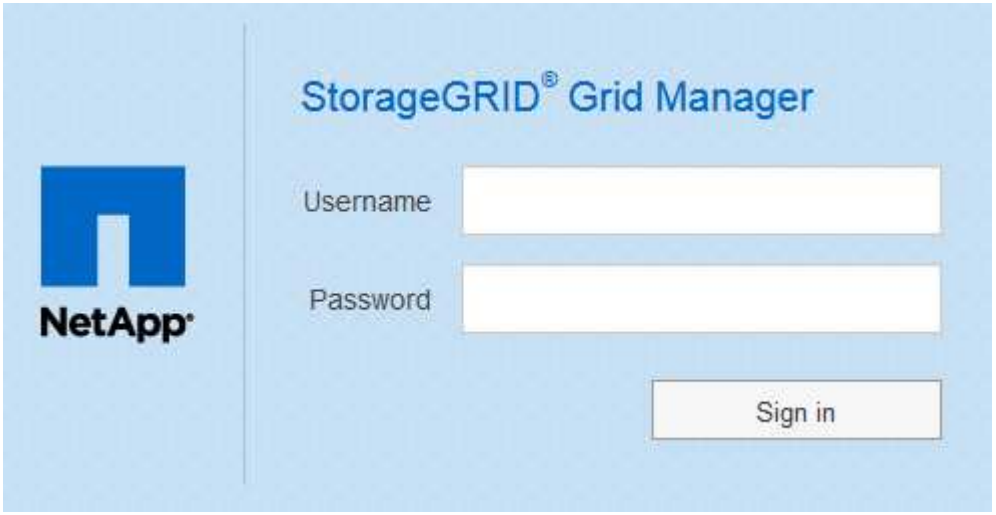
   Wo *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Nodes.

   Wenn Sie auf den Grid Manager auf einem anderen Port als dem Standard-Port für HTTPS (443) zugreifen müssen, geben Sie Folgendes ein, wobei *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder IP-Adresse und Port ist die Port-Nummer:

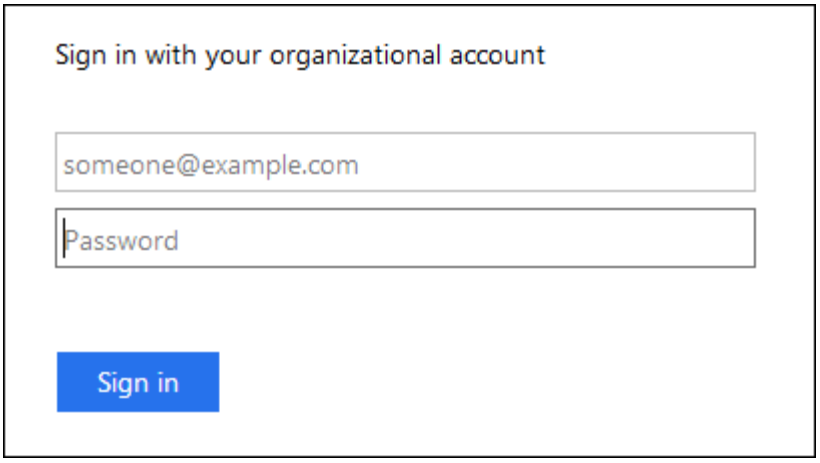
   `https://FQDN_or_Admin_Node_IP:port/`

3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie sich beim Grid Manager an:

   - Wenn Single Sign On (SSO) nicht für Ihr StorageGRID-System verwendet wird:
     i. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
     ii. Klicken Sie Auf **Anmelden**.



   - Wenn SSO für Ihr StorageGRID-System aktiviert ist und Sie in diesem Browser zum ersten Mal auf die URL zugreifen:
     i. Klicken Sie auf **Anmelden**. Sie können das Feld Konto-ID leer lassen.
     ii. Geben Sie auf der SSO-Anmeldeseite Ihres Unternehmens Ihre Standard-SSO-Anmeldedaten ein. Beispiel:

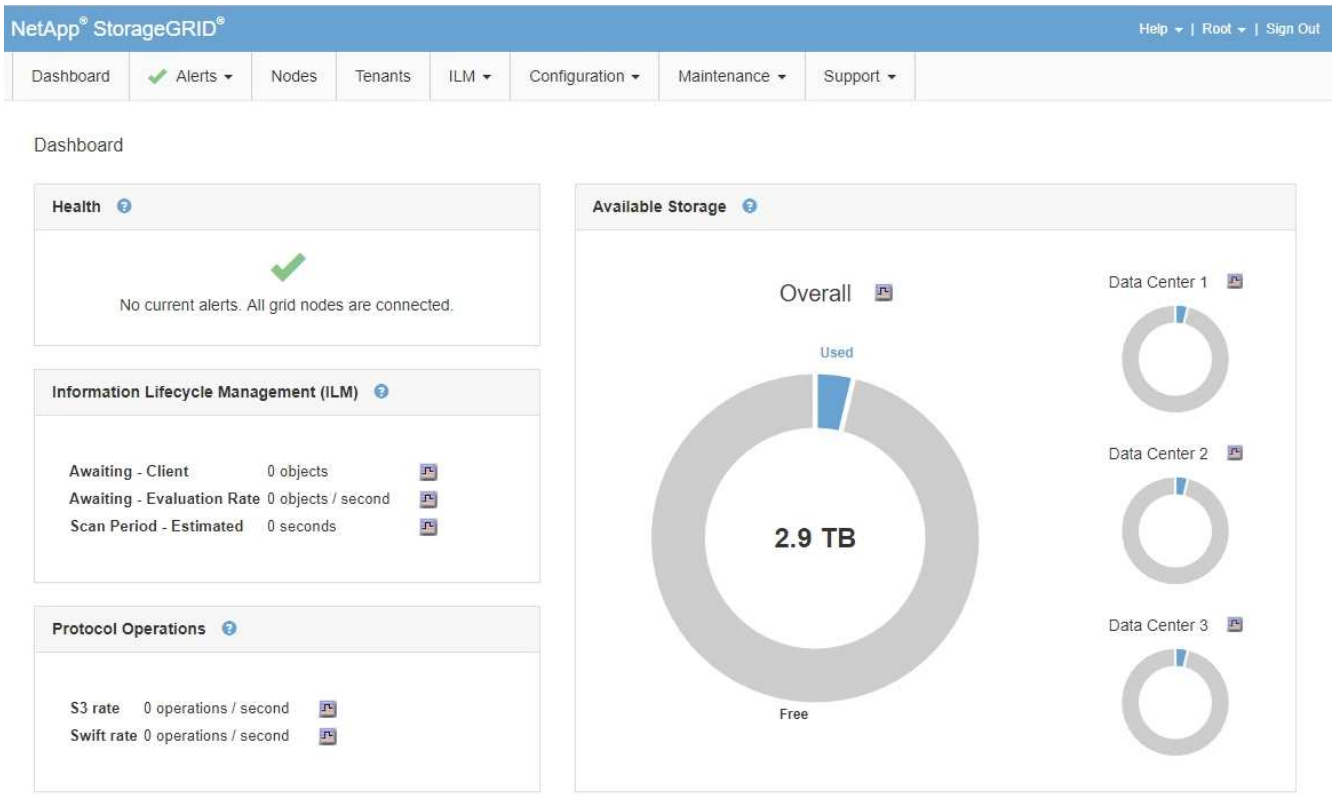


- Wenn SSO für Ihr StorageGRID-System aktiviert ist und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

  i. Führen Sie einen der folgenden Schritte aus:

     - Geben Sie **0** (die Konto-ID für den Grid Manager) ein, und klicken Sie auf **Anmelden**.
     - Wählen Sie **Grid Manager** aus, wenn er in der Liste der letzten Konten angezeigt wird, und klicken Sie auf **Anmelden**.

  ii. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an. Wenn Sie sich angemeldet haben, wird die Startseite des Grid Managers angezeigt, die das Dashboard enthält. Informationen zu den bereitgestellten Informationen finden Sie unter „`Viewing the Dashboard`“ in den Monitoring- und Fehlerbehebungsanweisungen für StorageGRID.



5. Wenn Sie sich bei einem anderen Admin-Knoten anmelden möchten:

Option	Schritte
SSO ist nicht aktiviert	a. Geben Sie in der Adressleiste des Browsers den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens ein. Geben Sie die Portnummer nach Bedarf an. b. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein. c. Klicken Sie Auf **Anmelden**.

Option	Schritte
SSO aktiviert	Geben Sie in der Adressleiste des Browsers den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens ein. Wenn Sie sich bei einem Admin-Knoten angemeldet haben, können Sie auf andere Admin-Knoten zugreifen, ohne sich erneut anmelden zu müssen. Wenn Ihre SSO-Sitzung jedoch abläuft, werden Sie erneut zur Eingabe Ihrer Anmeldedaten aufgefordert. **Hinweis:** SSO ist auf dem Port des eingeschränkten Grid Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"Zugriffskontrolle durch Firewalls"

"Serverzertifikate werden konfiguriert"

"Konfigurieren der Single Sign-On-Konfiguration"

"Verwalten von Admin-Gruppen"

"Verwalten von Hochverfügbarkeitsgruppen"

"Verwenden Sie ein Mandantenkonto"

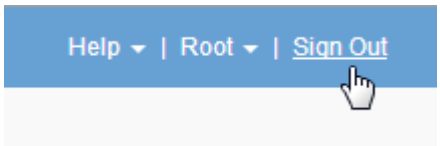
"Monitor Fehlerbehebung"

Vom Grid Manager abmelden

Wenn Sie mit dem Grid-Manager arbeiten, müssen Sie sich anmelden, 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. Klicken Sie oben rechts auf der Benutzeroberfläche auf den Link **Abmelden**.



2. Klicken Sie Auf **Abmelden**.

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

Verwandte Informationen

"Konfigurieren der Single Sign-On-Konfiguration"

"Verwenden Sie ein Mandantenkonto"

Ihr Passwort wird geändert

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

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn Sie sich bei StorageGRID als föderierten Benutzer anmelden oder SSO (Single Sign On) aktiviert ist, können Sie Ihr Kennwort 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**.
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. Klicken Sie Auf **Speichern**.

Ändern der 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 und Verschlüsselungen für das StorageGRID-System enthalten.

Was Sie benötigen

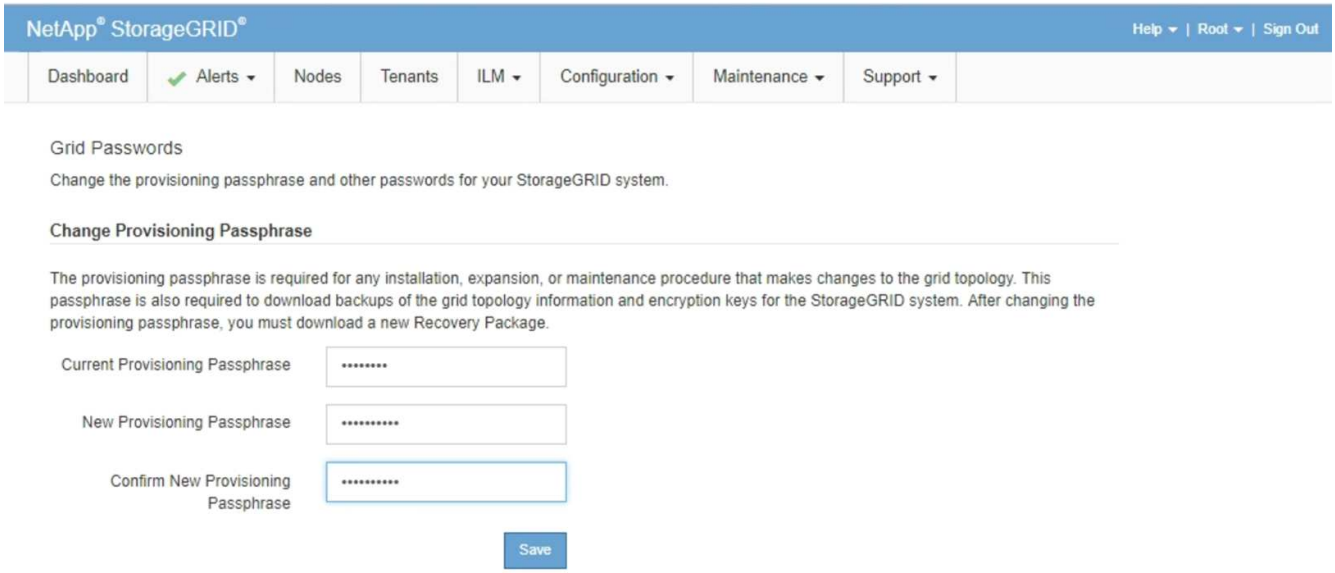
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über Wartungs- oder Root-Zugriffsberechtigungen verfügen.
- Sie müssen über die aktuelle Passphrase für die Bereitstellung verfügen.

Über diese Aufgabe

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

Schritte

1. Wählen Sie **Konfiguration** > **Zugangskontrolle** > **Grid-Passwörter**.

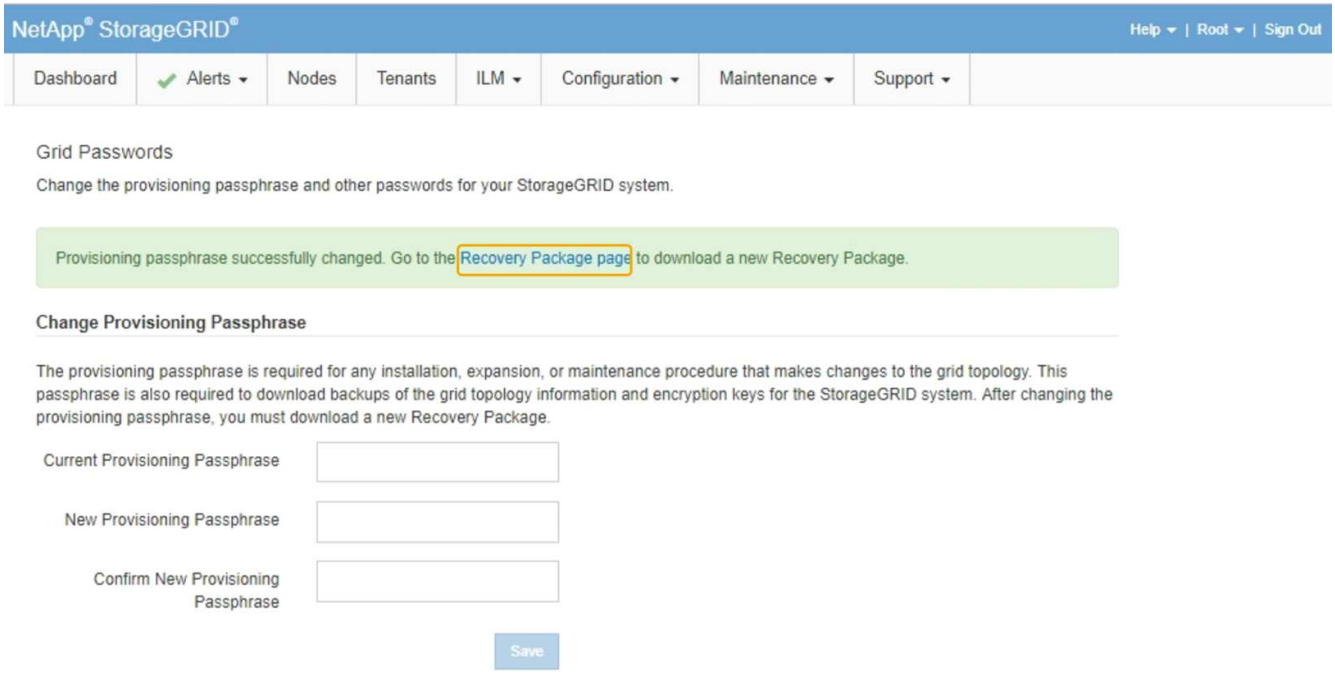


2. Geben Sie Ihre aktuelle Provisionierungs-Passphrase ein.
3. Geben Sie die neue Passphrase ein.die Passphrase muss mindestens 8 und nicht mehr als 32 Zeichen enthalten. Passphrases sind Groß-/Kleinschreibung.

> Speichern Sie die neue Provisionierungs-Passphrase an einem sicheren Ort. Sie ist für Installations-, Erweiterungs- und Wartungsverfahren erforderlich.

4. Geben Sie die neue Passphrase erneut ein, und klicken Sie auf **Speichern**.

   Das System zeigt ein grünes Erfolgsbanner an, wenn die Änderung der Provisionierungs-Passphrase abgeschlossen ist. Die Änderung sollte weniger als eine Minute dauern.



5. Wählen Sie den Link * Wiederherstellungspaket Seite* im Erfolgsbanner aus.
6. Laden Sie das neue Wiederherstellungspaket aus dem Grid Manager herunter. Wählen Sie **Wartung** > **Wiederherstellungspaket** und geben Sie die neue Provisioning-Passphrase ein.

> 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 Zeitüberschreitung der Browser-Sitzung

Sie können steuern, ob Grid Manager und Tenant Manager-Benutzer abgemeldet werden, wenn sie länger als eine bestimmte Zeit inaktiv sind.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Das Timeout für die GUI-Inaktivität ist standardmäßig auf 900 Sekunden (15 Minuten) eingestellt. Wenn die Browser-Sitzung eines Benutzers für diesen Zeitraum nicht aktiv ist, wird die Sitzung beendet.

Nach Bedarf können Sie den Timeout-Zeitraum vergrößern oder verkleinern, indem Sie die Anzeigeoption GUI Inaktivität Timeout einstellen.

Wenn Single Sign-On (SSO) aktiviert ist und die Browsersitzung eines Benutzers beendet wird, verhält sich das System so, als ob der Benutzer manuell auf **Abmelden** geklickt hat. Der Benutzer muss seine SSO-Anmeldedaten erneut eingeben, um wieder auf StorageGRID zugreifen zu können.

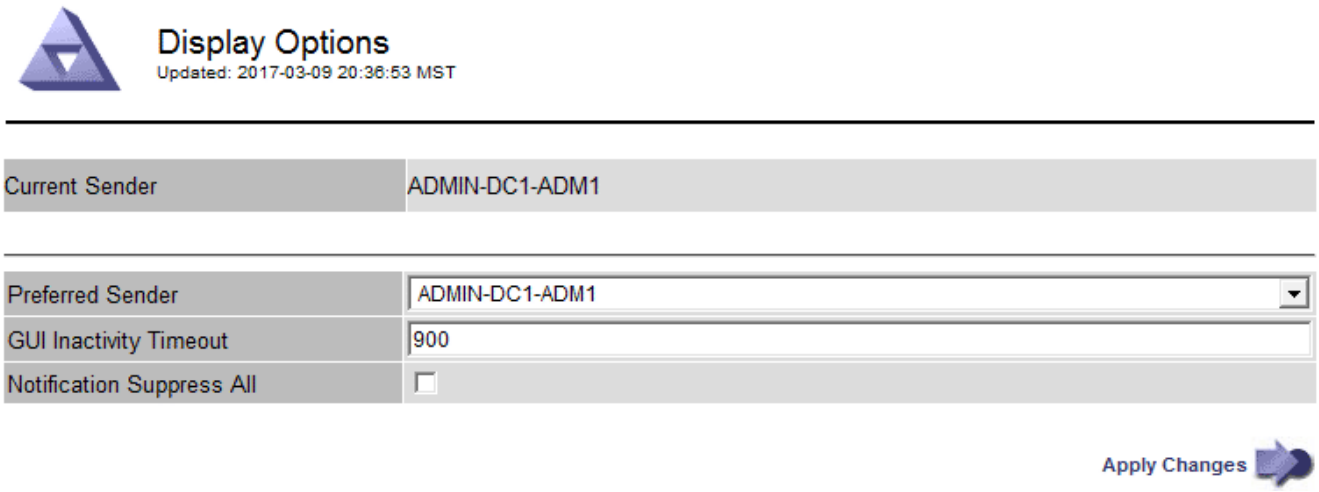
Das Timeout der Benutzersitzung kann auch durch Folgendes gesteuert werden:

- 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 der Wert für das Timeout der GUI nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.
- Zeitüberschreitungseinstellungen für den Identitäts-Provider, vorausgesetzt, SSO ist für StorageGRID aktiviert.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Geben Sie für **GUI Inaktivität Timeout** einen Timeout-Zeitraum von mindestens 60 Sekunden ein.

   Setzen Sie dieses Feld auf 0, wenn Sie diese Funktion nicht verwenden möchten. Benutzer werden 16 Stunden nach ihrer Anmeldung bei Ablauf ihrer Authentifizierungs-Tokens abgemeldet.



3. Klicken Sie Auf **Änderungen Übernehmen**.

   Die neue Einstellung hat keine Auswirkung auf die derzeit angemeldenen Benutzer. Benutzer müssen sich erneut anmelden oder ihre Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

Verwandte Informationen

"Funktionsweise von Single Sign-On"

"Verwenden Sie ein Mandantenkonto"

Anzeigen von StorageGRID-Lizenzinformationen

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn ein Problem mit der Softwarelizenz für dieses StorageGRID-System vorliegt, enthält das Bedienfeld „Systemzustand“ auf dem Dashboard ein Symbol für den Lizenzstatus und einen Link mit **Lizenz**. Die Nummer gibt an, wie viele Probleme mit Lizenzen es gibt.

Schritt

Um die Lizenz anzuzeigen, führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Bedienfeld „Systemzustand“ des Dashboards auf das Symbol Lizenzstatus oder den Link **Lizenz**. Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.
- Wählen Sie **Wartung** > **System** > **Lizenz**.

Die Lizenzseite wird angezeigt und enthält die folgenden, schreibgeschützten Informationen zur aktuellen Lizenz:

- StorageGRID System-ID. Hierbei handelt es sich um die eindeutige Identifikationsnummer für diese StorageGRID Installation
- Seriennummer der Lizenz
- Lizenzierte Storage-Kapazität des Grid
- Enddatum der Softwarelizenz
- Enddatum des Support-Servicevertrags
- 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.

Die StorageGRID-Lizenzinformationen werden aktualisiert

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.

Was Sie benötigen

- Sie müssen über eine neue Lizenzdatei verfügen, um sich auf Ihr StorageGRID-System bewerben zu können.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Schritte

1. Wählen Sie **Wartung** > **System** > **Lizenz**.
2. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
3. Klicken Sie Auf **Durchsuchen**.
4. Suchen Sie im Dialogfeld Öffnen die neue Lizenzdatei, und wählen Sie sie aus (`.txt`Und klicken Sie auf **Öffnen**.

   Die neue Lizenzdatei wird validiert und angezeigt.

5. Klicken Sie Auf **Speichern**.

Verwenden der 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.

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.

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. Details finden Sie in den Informationen zur Verwendung von Mandantenkonten.
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Diese APIs sind nur zur internen Verwendung bestimmt und nicht öffentlich dokumentiert. Diese APIs können auch ohne vorherige Ankündigung geändert werden.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Prometheus: Grundlagen der Abfrage"

Grid-Management-API-Vorgänge

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

- **Accounts** — Operationen für das Management von Speicher-Mandantenkonten, einschließlich der Erstellung neuer Konten und der Abruf der Speichernutzung für ein bestimmtes Konto.
- **Alarms** — Operationen zur Auflistung aktueller Alarme (Legacy-System) und zur Ausgabe von Informationen über den Systemzustand des Rasters, einschließlich der aktuellen Warnungen und einer Zusammenfassung der Knoten Verbindungsstatus.
- **Alarmverlauf** — Betrieb bei gelösten Warnmeldungen.
- **Alarm-Empfänger** — Betrieb bei Alarmbenachrichtigungen Empfänger (E-Mail).
- **Alert-rules** — Operationen für Alarmregeln.
- **Alarm-Stille** — Operationen bei Alarmgeräuschen.
- **Alerts** — Betrieb bei Warnungen.
- **Audit** — Operationen zur Auflistung und Aktualisierung der Audit-Konfiguration.
- **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 „`Protecting Against Cross-Site Request Forgery`“.

- **Client-Zertifikate** — Betrieb zum Konfigurieren von Client-Zertifikaten, sodass mit externen Monitoring-Tools sicher auf StorageGRID zugegriffen werden kann.
- **Config** — Operationen bezogen auf die Produktversion und 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.
- **Deaktivierte Funktionen** — Funktionen zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **dns-Server** — Operationen, um konfigurierte externe DNS-Server aufzulisten und zu ändern.
- **Endpunkt-Domain-Namen** — Operationen zum Auflisten und Ändern von Endpunkt-Domain-Namen.
- **Erasure-Coding** — Operationen auf Erasure Coding-Profilen.
- **Erweiterung** — Betrieb bei Erweiterung (Verfahrensebene).
- **Erweiterungsknoten** — Betrieb auf Erweiterung (Knotenebene).
- **Erweiterungsstandorte** — Betrieb auf Erweiterungsebene (Standort-Ebene).
- **Grid-Networks** — Operationen zur Auflistung und Änderung der Grid-Netzwerkliste.
- **Grid-passwords** — Operationen für das Grid-Passwort-Management.
- **Groups** — Operationen zur Verwaltung lokaler Grid-Administratorgruppen und zum Abrufen von föderierten Grid-Administratorgruppen von einem externen LDAP-Server.

- **Identity-Source** — Operationen, um eine externe Identitätsquelle zu konfigurieren und föderierte Gruppen- und Benutzerinformationen manuell zu synchronisieren.
- **ilm** — Operationen zum Information Lifecycle Management (ILM).
- **Lizenz** — Operationen zum Abrufen und Aktualisieren der StorageGRID-Lizenz.
- **Logs** — Operationen zum Sammeln und Herunterladen von Protokolldateien.
- **Metriken** — Betrieb auf StorageGRID-Kennzahlen einschließlich sofortiger metrischer Abfragen zu einem einzelnen Zeitpunkt und metrischen Bereichsabfragen 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-Health** — Operationen auf Node-Status.
- **ntp-Server** — Operationen zum Auflisten oder Aktualisieren von NTP-Servern (External Network Time Protocol).
- **Objects** — Operationen an Objekten und Objektmetadaten.
- **Recovery** — Operationen für den Wiederherstellungsvorgang.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **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** — Betrieb auf der aktuellen SNMP-Konfiguration.
- **Verkehrsklassen** — Operationen für Verkehrsklassifizierungen.
- **UnTrusted-Client-Netzwerk** — Operationen auf der nicht vertrauenswürdigen Client-Netzwerk-Konfiguration.
- **Benutzer** — Operationen zum Anzeigen und Verwalten von Grid Manager-Benutzern.

API-Anforderungen werden ausgegeben

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

> 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.

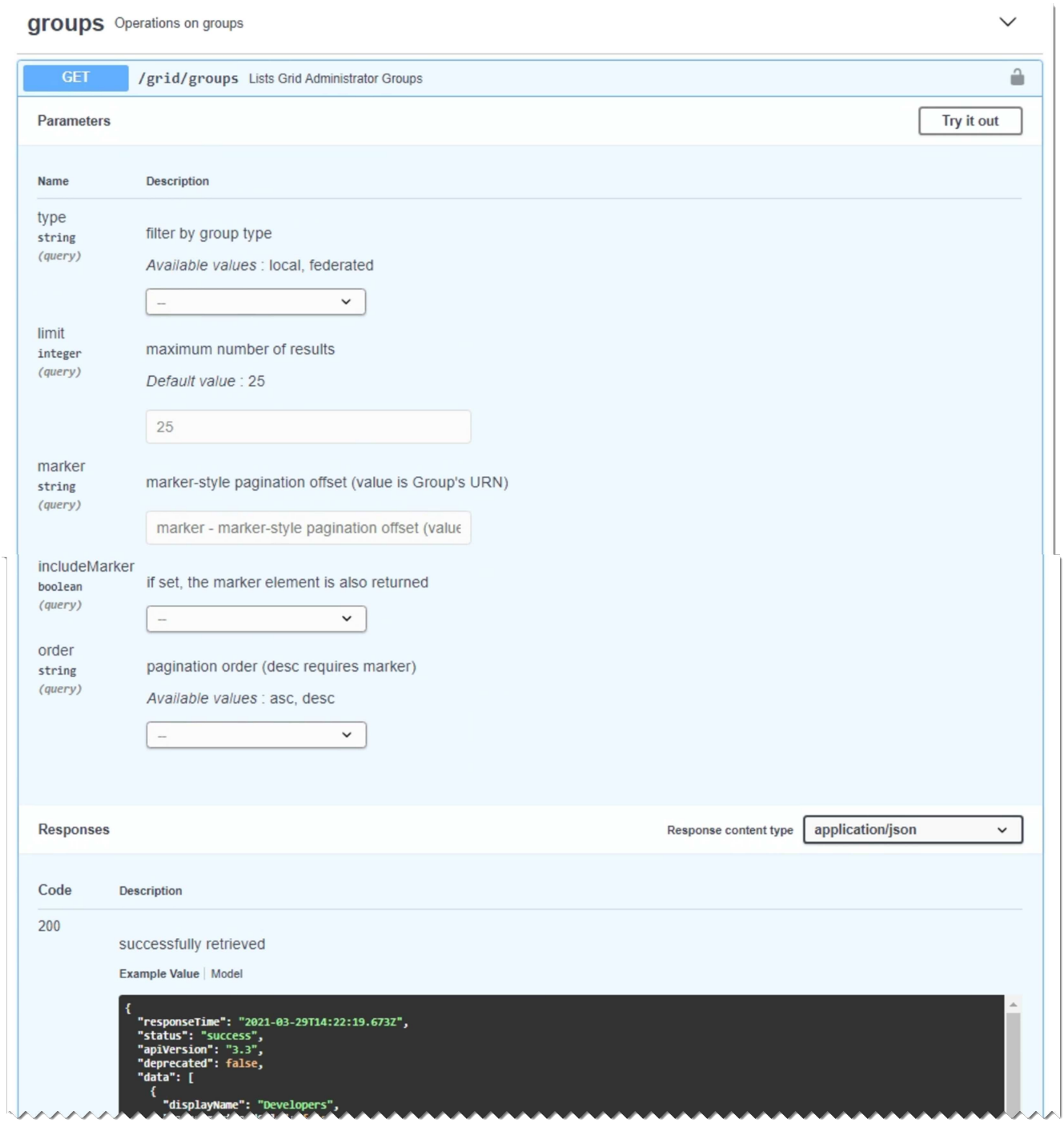
Schritte

1. Wählen Sie in der Kopfzeile des Grid Managers die Option **Hilfe** > **API-Dokumentation** aus.

2. 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.

3. 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.



4. 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.

5. Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie auf **Modell** klicken, um die Anforderungen für jedes Feld zu erfahren.
6. Klicken Sie auf **Probieren Sie es aus**.
7. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
8. Klicken Sie Auf **Ausführen**.
9. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Die Grid Management API-Versionierung

Die Grid Management API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

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

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

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

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

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

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

Veraltete Anfragen werden wie folgt als veraltet markiert:

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

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

Ermitteln, 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
  ]
}
```

Angeben einer API-Version für eine Anforderung

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

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

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

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

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

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

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

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

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

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

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

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

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

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

Verwenden der API, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert wurde, können Sie sich nicht mit den Standard-Authenticate-API-Anforderungen bei der Grid-Management-API oder der Mandantenmanagement-API anmelden und diese abzeichnen.

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

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen ausstellen, um ein Authentifizierungs-Token von AD FS zu erhalten, das für die Grid Management API oder die Mandantenmanagement-API gültig ist.

Was Sie benötigen

- 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: Eine gültige SubjectConfirmation wurde bei dieser Antwort nicht gefunden.

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

Falls Sie ein Problem mit der URL-Codierung haben, sehen Sie möglicherweise den Fehler: Nicht unterstützte 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:

   - Der SSO-Benutzername
   - Die Domäne, in der StorageGRID installiert ist
   - Die Adresse für StorageGRID
   - Wenn Sie auf die Mandantenmanagement-API zugreifen möchten, geben Sie die Mandantenkontokennung ein.

   +

   ```
   python3 /tmp/storagegrid-ssoauth.py
   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 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://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

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

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

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

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

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

Die Antwort umfasst die Client-Anforderungs-ID:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Die Antwort umfasst das Authentifizierungs-Token.

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

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

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

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

Wenn Single Sign-On aktiviert ist, wird die API von der API absigniert

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.

Über diese Aufgabe

Bei Bedarf können Sie sich einfach von der StorageGRID-API abmelden, indem Sie sich einfach von der Seite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

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

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

Es wird eine Abmeldung-URL zurückgegeben:

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

2. Speichern Sie die Abmeldung-URL.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...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
```

StorageGRID-Sicherheitszertifikate werden verwendet

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).

Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig den Informationssicherheitsrichtlinien Ihres Unternehmens entsprechen. StorageGRID umfasst außerdem eine integrierte Zertifizierungsstelle (Certificate Authority, CA), die während der Systeminstallation interne CA-Zertifikate generiert. Diese internen CA-Zertifikate werden standardmäßig zum Schutz des internen StorageGRID-Datenverkehrs verwendet. Obwohl Sie die internen CA-Zertifikate für eine nicht-Produktionsumgebungen verwenden können, empfiehlt es sich, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert sind. Ungesicherte Verbindungen ohne Zertifikat werden ebenfalls unterstützt, werden jedoch nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht. Die benutzerdefinierten Zertifikate sollten jedoch die für die Überprüfung der Serververbindungen angegebenen Zertifikate sein.
- Alle benutzerdefinierten Zertifikate müssen den Richtlinien zur Systemhärtung für Serverzertifikate entsprechen.

  "Systemhärtung"

- 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.

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Administrator-Client-Zertifikat	Client	Wird auf jedem Client installiert, sodass StorageGRID den externen Client-Zugriff authentifizieren kann. • Ermöglicht autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank. • Ermöglicht die sichere Überwachung von StorageGRID mit externen Tools.	**Konfiguration** > **Zugangskontrolle** > **Client-Zertifikate**	"Administrator-Client-Zertifikate werden konfiguriert"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Zertifikat für Identitätsföderation	Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Active Directory-, OpenLDAP- oder Oracle Directory-Server.wird für die Identitätsföderation verwendet, sodass Administratorgruppen und Benutzer von einem externen System gemanagt werden können.	**Konfiguration** > **Zugangskontrolle** > **Identitätsföderation**	"Identitätsföderation verwenden"
SSO-Zertifikat (Single Sign On)	Server	Authentifiziert die Verbindung zwischen Active Directory Federation Services (AD FS) und StorageGRID, die für SSO-Anfragen (Single Sign On) verwendet werden.	**Konfiguration** > **Zugangskontrolle** > **Single Sign-On**	"Konfigurieren der Single Sign-On-Konfiguration"
KMS-Zertifikat (Key Management Server)	Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Verschlüsselungsmanagement-Server (KMS), der Verschlüsselungsschlüssel für die StorageGRID Appliance-Nodes bereitstellt.	**Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver**	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Zertifikat für eine E-Mail-Benachrichtigung	Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, die für Benachrichtigungen verwendet werden. • Wenn die Kommunikation mit dem SMTP-Server TLS (Transport Layer Security) erfordert, müssen Sie das CA-Zertifikat für den E-Mail-Server angeben. • Geben Sie ein Clientzertifikat nur an, wenn für den SMTP-E-Mail-Server Clientzertifikate zur Authentifizierung erforderlich sind.	**Alarme** > **E-Mail-Einrichtung**	"Monitor Fehlerbehebung"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Endpunkt-Zertifikat für Load Balancer	Server	Authentifiziert die Verbindung zwischen S3- oder Swift-Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes oder Admin-Nodes. Sie laden ein Load Balancer-Zertifikat hoch oder generieren ein Load Balancer-Zertifikat, wenn Sie einen Load Balancer-Endpunkt konfigurieren.Client-Anwendungen verwenden das Load Balancer-Zertifikat bei der Verbindung zu StorageGRID zum Speichern und Abrufen von Objektdaten. **Hinweis:** das Load Balancer-Zertifikat ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID-Betriebs.	**Konfiguration** > **Netzwerkeinstellungen** > **Load Balancer Endpoints**	• "Konfigurieren von Load Balancer-Endpunkten" • Erstellen eines Endpunkts für den Load Balancer für FabricPool "Konfigurieren Sie StorageGRID für FabricPool"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Zertifikat Für Den Management Interface Server	Server	Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID-Managementoberfläche, sodass Benutzer ohne Sicherheitswarnungen auf Grid-Manager und Mandantenmanager zugreifen können. Dieses Zertifikat authentifiziert auch Grid Management-API- und Mandantenmanagement-API-Verbindungen. Sie können das interne CA-Zertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.	**Konfiguration** > **Netzwerkeinstellungen** > **Serverzertifikate**	• "Serverzertifikate werden konfiguriert" • "Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"
Endpunkt-Zertifikat für Cloud Storage Pool	Server	Authentifiziert die Verbindung vom StorageGRID Cloud Storage Pool an einem externen Storage-Standort (z. B. S3 Glacier oder Microsoft Azure Blob Storage). Für jeden Cloud-Provider-Typ ist ein anderes Zertifikat erforderlich.	**ILM** > **Speicherpools**	"Objektmanagement mit ILM"
Endpoint-Zertifikat für Plattform-Services	Server	Authentifiziert die Verbindung vom StorageGRID Plattform-Service zu einer S3-Storage-Ressource.	**Tenant Manager** > **STORAGE (S3)** > **Plattform-Services-Endpunkte**	"Verwenden Sie ein Mandantenkonto"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Endpoint Server-Zertifikat für den Objekt-Storage-API-Service	Server	Authentifiziert sichere S3- oder Swift-Client-Verbindungen mit dem LDR-Service (Local Distribution Router) auf einem Storage-Node oder zum veralteten Connection Load Balancer (CLB)-Service auf einem Gateway-Node.	**Konfiguration** > **Netzwerkeinstellungen** > **Load Balancer Endpoints**	"Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst"

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.

Kontrolle des Administratorzugriffs auf StorageGRID

Sie können den Administratorzugriff auf das StorageGRID-System steuern, indem Sie Firewall-Ports öffnen oder schließen, Administratorgruppen und Benutzer verwalten, SSO konfigurieren und Client-Zertifikate für den sicheren externen Zugriff auf StorageGRID-Metriken bereitstellen.

- "Zugriffskontrolle durch Firewalls"
- "Identitätsföderation verwenden"
- "Verwalten von Admin-Gruppen"
- "Verwalten von lokalen Benutzern"
- "Verwenden von Single Sign On (SSO) für StorageGRID"
- "Administrator-Client-Zertifikate werden konfiguriert"

Zugriffskontrolle durch Firewalls

Wenn Sie den Zugriff über Firewalls steuern möchten, öffnen oder schließen Sie bestimmte Ports an der externen Firewall.

Kontrolle des Zugriffs an der externen Firewall

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.

Port	Beschreibung	Port offen…
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen. **Hinweis:** Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Mandanten-Manager oder die Mandanten-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.

Port	Beschreibung	Port offen…
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Mandanten-Manager und die Mandanten-Management-API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid Management API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.

Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

"Melden Sie sich beim Grid Manager an"

"Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet"

"Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen"

"Verwalten von nicht vertrauenswürdigen Client-Netzwerken"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

Identitätsföderation verwenden

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

Identitätsföderation wird konfiguriert

Sie können einen Identitätsverbund konfigurieren, wenn Administratorgruppen und Benutzer in einem anderen System wie Active Directory, OpenLDAP oder Oracle Directory Server verwaltet werden sollen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie Single Sign-On (SSO) aktivieren möchten, müssen Sie Active Directory als föderierte Identitätsquelle und AD FS als Identitäts-Provider verwenden. Siehe „`Anforderungen für die Verwendung von Single Sign-On.`“
- Sie müssen Active Directory, OpenLDAP oder Oracle Directory Server als Identitäts-Provider verwenden.

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

- 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.

Über diese Aufgabe

Sie müssen eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie die folgenden Typen von föderierten Gruppen importieren möchten:

- Verwaltungsgruppen. Die Benutzer in Admin-Gruppen können sich beim Grid Manager anmelden und anhand der Verwaltungsberechtigungen, die der Gruppe zugewiesen sind, Aufgaben ausführen.
- Mandanten-Benutzergruppen für Mandanten, die ihre eigene Identitätsquelle nicht 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.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Identitätsföderation**.
2. Wählen Sie **Identitätsföderation aktivieren**.

   Die Felder zum Konfigurieren des LDAP-Servers werden angezeigt.

3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.

   Sie können **Active Directory**, **OpenLDAP** oder **Other** auswählen.

   Wenn Sie **OpenLDAP** auswählen, müssen Sie den OpenLDAP-Server konfigurieren. Weitere Informationen zur Konfiguration eines OpenLDAP-Servers finden Sie in den Richtlinien.

   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.
   - **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 im Abschnitt LDAP-Server konfigurieren die erforderlichen Informationen zum LDAP-Server und zur Netzwerkverbindung ein.
   - **Hostname**: Der Server-Hostname 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`

   - **Passwort**: Das mit dem Benutzernamen verknüpfte Passwort.
   - **Gruppenbasis 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 der **Group-Basis-DN**, zu der 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 **User Unique Name**-Werte müssen innerhalb der **User Base DN**, zu der sie gehören, eindeutig sein.

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

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-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.
8. Wählen Sie optional **Verbindung testen**, um die Verbindungseinstellungen für den LDAP-Server zu validieren.

   Wenn die Verbindung gültig ist, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.
9. Wenn die Verbindung gültig ist, wählen Sie **Speichern**.

   Der folgende Screenshot zeigt Beispielkonfigurationswerte für einen LDAP-Server, der Active Directory verwendet.

Verwandte Informationen

"Unterstützte Chiffren für ausgehende TLS-Verbindungen"

"Anforderungen für die Nutzung von Single Sign On"

"Erstellen eines Mandantenkontos"

"Verwenden Sie ein Mandantenkonto"

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.

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie im Administratorhandbuch für OpenLDAP in den Anweisungen zur Wartung der Reverse-Group-Mitgliedschaft.

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 der Umkehrgruppenmitgliedschaft finden Sie im Administratorhandbuch für OpenLDAP.

Verwandte Informationen

"OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die Identitätsquelle muss aktiviert sein.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Identitätsföderation**.

   Die Seite Identity Federation wird angezeigt. Die Schaltfläche **Synchronisieren** befindet sich am unteren Rand der Seite.

2. Klicken Sie Auf **Synchronisieren**.

   Eine Bestätigungsmeldung gibt an, dass die Synchronisierung erfolgreich gestartet wurde. 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.

Identitätsföderation deaktivieren

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 **Identitätsföderation aktivieren** ist deaktiviert, wenn Single Sign-On (SSO) auf **Enabled** oder **Sandbox Mode** gesetzt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Identitätsföderation**.
2. Deaktivieren Sie das Kontrollkästchen * Identitätsföderation aktivieren*.
3. Klicken Sie Auf **Speichern**.

Verwandte Informationen

"Deaktivieren der Einzelanmeldung"

Verwalten 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.

Erstellen von Admin-Gruppen

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

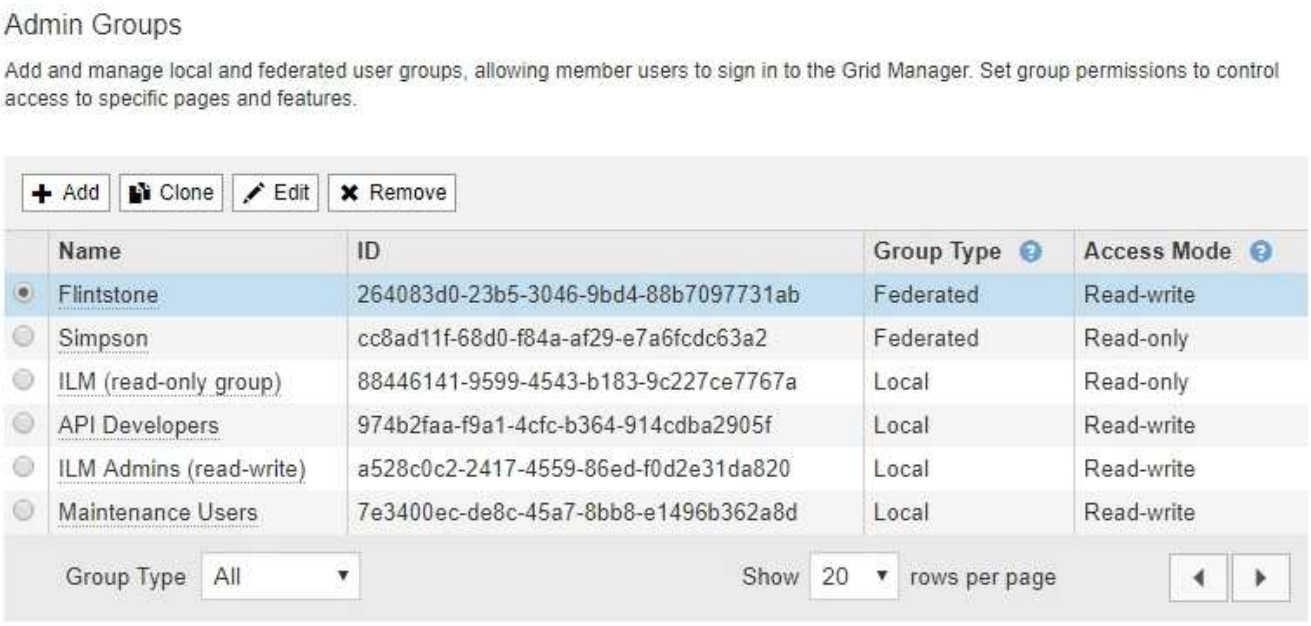
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie einen Identitätsverbund konfiguriert haben, und die föderierte Gruppe muss bereits in der konfigurierten Identitätsquelle vorhanden sein.

Schritte

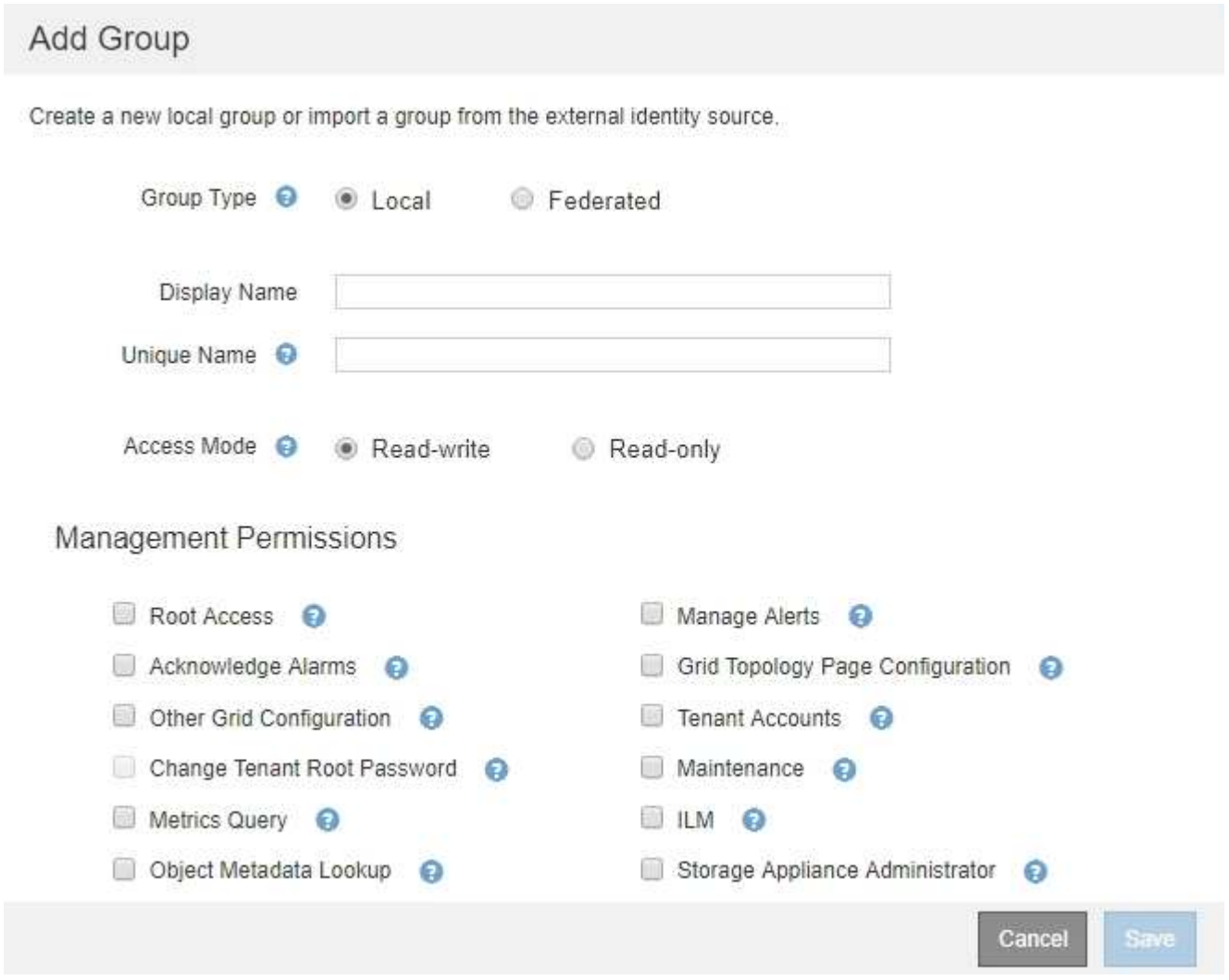
1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Gruppen**.

   Die Seite Admin Groups wird angezeigt und enthält alle vorhandenen Admin-Gruppen.



2. Wählen Sie **Hinzufügen**.

   Das Dialogfeld Gruppe hinzufügen wird angezeigt.



3. Wählen Sie für den Gruppentyp **Lokal** aus, wenn Sie eine Gruppe erstellen möchten, die nur innerhalb von StorageGRID verwendet werden soll, oder wählen Sie **föderiert** aus, wenn Sie eine Gruppe aus der Identitätsquelle importieren möchten.
4. Wenn Sie **Lokal** ausgewählt haben, geben Sie einen Anzeigenamen für die Gruppe ein. Der Anzeigename ist der Name, der im Grid Manager angezeigt wird. Zum Beispiel: „`MWartung Benutzer`“ oder „`ILM-Administratoren`“
5. Geben Sie einen eindeutigen Namen für die Gruppe ein.
   - **Lokal**: Geben Sie einen eindeutigen Namen ein. Beispiel: „`ILM-Administratoren`“
   - **Federated**: Geben Sie den Namen der Gruppe genau so ein, wie er in der konfigurierten Identitätsquelle angezeigt wird.
6. 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 vornehmen oder Vorgänge im Grid Manager oder der Grid Management API 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.
7. Wählen Sie eine oder mehrere Verwaltungsberechtigungen aus.

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

   Die neue Gruppe wird erstellt. Wenn es sich um eine lokale Gruppe handelt, können Sie jetzt einen oder mehrere Benutzer hinzufügen. Wenn es sich um eine föderierte Gruppe handelt, verwaltet die Identitätsquelle, welche Benutzer der Gruppe angehören.

Verwandte Informationen

"Verwalten von lokalen Benutzern"

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 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

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

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Admin-Gruppe zuweisen können. Für alle nicht explizit genannten Funktionen ist die Root-Zugriffsberechtigung erforderlich.

Root-Zugriff

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

Verwalten Von Warnmeldungen

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.

Quittierung von Alarmen (Altsystem)

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

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

Konfiguration Der Seite Grid Topology

Mit dieser Berechtigung haben Sie Zugriff auf die folgenden Menüoptionen:

- Konfigurationsregisterkarten auf den Seiten **Support** > **Tools** > **Grid Topology**.
- **Ereignisanzahl zurücksetzen**-Link auf der Registerkarte **Knoten** > **Ereignisse**.

Andere Grid-Konfiguration

Diese Berechtigung ermöglicht den Zugriff auf zusätzliche Grid-Konfigurationsoptionen.

> Um diese zusätzlichen Optionen zu sehen, müssen Benutzer auch über die Berechtigung für die Konfiguration der Grid Topology-Seite verfügen.

- **Alarme** (Altsystem):
  - Globale Alarme
  - Einrichtung Alter E-Mail-Adresse
- **ILM**:
  - Storage-Pools

    - Storage-Klasse
- **Konfiguration** > **Netzwerkeinstellungen**
    - Verbindungskosten
- **Konfiguration** > **Systemeinstellungen**:
    - Anzeigeoptionen
    - Grid-Optionen
    - Storage-Optionen
- **Konfiguration** > **Überwachung**:
    - Veranstaltungen
- * Support*:
    - AutoSupport

Mandantenkonten

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **Mieter** > **Mandantenkonten**.

> Version 1 der Grid Management API (die veraltet ist) verwendet diese Berechtigung, um Mandantengruppenrichtlinien zu managen, Swift-Admin-Passwörter zurückzusetzen und S3-Zugriffschlüssel für den Root-Benutzer zu verwalten.

Root-Passwort Des Mandanten Ändern

Mit dieser Berechtigung erhalten Sie Zugriff auf die Option **Root Passwort ändern** auf der Seite Mandantenkonten, mit der Sie steuern können, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern kann. Benutzer, die diese Berechtigung nicht besitzen, können die Option **Root Passwort ändern** nicht sehen.

> Sie müssen der Gruppe die Berechtigungen für Mandantenkonten zuweisen, bevor Sie diese Berechtigung zuweisen können.

Wartung

Mit dieser Berechtigung haben Sie Zugriff auf die folgenden Menüoptionen:

- **Konfiguration** > **Systemeinstellungen**:
    - Domain-Namen*
    - Server-Zertifikate*
- **Konfiguration** > **Überwachung**:
    - Audit*
- **Konfiguration** > **Zugangskontrolle**:
    - Grid-Passwörter
- **Wartung** > **Wartungsaufgaben**
    - Ausmustern
    - Erweiterung

    - Recovery
- **Wartung** > **Netzwerk**:
    - DNS-Server*
    - Grid-Netzwerk*
    - NTP-Server*
- **Wartung** > **System**:
    - Lizenz*
    - Wiederherstellungspaket
    - Software-Update
- **Support** > **Tools**:
    - Protokolle
- Benutzer, die nicht über die Wartungsberechtigung verfügen, können die mit einem Sternchen gekennzeichneten Seiten anzeigen, jedoch nicht bearbeiten.

Abfrage Von Kennzahlen

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **Support** > **Tools** > **Metriken**. Diese Berechtigung bietet auch Zugriff auf benutzerdefinierte Prometheus-metrische Abfragen unter Verwendung des Abschnitts **Metriken** der Grid Management API.

ILM

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

- * Erasure Coding*
- **Regeln**
- **Richtlinien**
- **Regionen**

> Der Zugriff auf die Menüoptionen **ILM** > **Storage Pools** und **ILM** > **Storage Klasse** wird über die anderen Berechtigungen für die Konfiguration der Grid-Konfiguration und Grid-Topologie-Seite gesteuert.

Lookup Von Objektmetadaten

Mit dieser Berechtigung haben Sie Zugriff auf das Menü **ILM** > **Object Metadaten Lookup**.

Storage Appliance Administrator

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

Interaktion zwischen Berechtigungen und Zugriffsmodus

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**

gesetzt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Features.

Deaktivieren von Funktionen über die Grid Management 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 die einzige Möglichkeit, zu verhindern, dass der Root-Benutzer oder Benutzer, die zu Administratorgruppen 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 Funktion **Ändern des Mandantenstammpassworts** im Grid Manager (sowohl der UI als auch der API) kann Unternehmen A sicherstellen, dass kein Admin-Benutzer - einschließlich des Stammbenutzers und der Benutzer, die zu Gruppen mit Root Access-Berechtigung gehören - das Passwort für den Root-Benutzer eines Mandantenkontos ändern kann.*

Deaktivieren von 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 **activateFeatures**-Funktion 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.

Details finden Sie in der Anleitung zur Implementierung von S3- oder Swift-Client-Applikationen.

Schritte

1. Rufen Sie die Swagger-Dokumentation für die Grid Management API auf.
2. Suchen Sie den Endpunkt zum Deaktivieren von Funktionen.
3. Um eine Funktion, wie z. B. **Ändern des Mandantenwurzelkennworts**, zu deaktivieren, senden Sie einen Text wie folgt an die API:

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

   Wenn die Anforderung abgeschlossen ist, ist die Funktion Mandantenstammpasswort ändern deaktiviert. Die Berechtigung zum Ändern des Stammkennworts für Mandanten erscheint nicht mehr in der Benutzeroberfläche, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu

ändern, schlägt mit „`403 Verbotenen`“ fehl.

4. Um alle Funktionen erneut zu aktivieren, senden Sie einen Text wie folgt an die API:

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

Wenn diese Anforderung abgeschlossen ist, werden alle Funktionen, einschließlich der Funktion „Mandantenstammpasswort ändern“, erneut aktiviert. Die Berechtigung zum Ändern des Root-Kennworts für Mandanten erscheint jetzt in der Benutzeroberfläche. Jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, wird erfolgreich sein, vorausgesetzt, der Benutzer hat die Berechtigung zum Verwalten des Root-Zugriffs oder zum Ändern des Root-Kennworts für Mandanten.

> 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. Wenn Sie beispielsweise die Funktion „Mandantenstammpasswort ändern“ erneut aktivieren und die Funktion „Alarm Acknowledgement“ deaktivieren möchten, senden Sie diese PUT-Anforderung:

```
{ "grid": { "alarmAcknowledgment": true } }
```

Verwandte Informationen

"Verwenden der Grid-Management-API"

Ändern einer Admin-Gruppe

Sie können eine Admin-Gruppe ändern, um die Berechtigungen zu ändern, die der Gruppe zugeordnet sind. Für lokale Admin-Gruppen können Sie auch den Anzeigenamen aktualisieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Gruppen**.
2. Wählen Sie die Gruppe aus.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Bearbeiten**.
4. Optional geben Sie für lokale Gruppen den Gruppennamen ein, der Benutzern angezeigt wird, z. B. „`Maintual users`“.

   Sie können den eindeutigen Namen, d. h. den internen Gruppennamen, nicht ändern.

5. Ändern Sie optional den Zugriffsmodus der Gruppe.

- **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 vornehmen oder Vorgänge im Grid Manager oder der Grid Management API 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.

6. Optional können Sie Gruppenberechtigungen hinzufügen oder entfernen.

   Weitere Informationen zu Administratorgruppenberechtigungen finden Sie unter.

7. Wählen Sie **Speichern**.

Verwandte Informationen

Berechtigungen für Admin-Gruppen

Löschen einer Admin-Gruppe

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 Admin-Benutzer aus der Gruppe entfernt, die Admin-Benutzer jedoch nicht gelöscht.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Wenn Sie eine Gruppe löschen, verlieren Benutzer, die dieser Gruppe zugewiesen sind, alle Zugriffsberechtigungen für den Grid Manager, es sei denn, sie werden von einer anderen Gruppe Berechtigungen erteilt.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Gruppen**.
2. Wählen Sie den Namen der Gruppe aus.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Wählen Sie **Entfernen**.
4. Wählen Sie **OK**.

Verwalten von lokalen Benutzern

Sie können lokale Benutzer erstellen und lokalen Admin-Gruppen zuweisen, um zu bestimmen, auf welche Grid Manager-Funktionen diese Benutzer zugreifen können.

Der Grid 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) aktiviert ist, können sich lokale Benutzer nicht bei StorageGRID anmelden.

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Erstellen eines lokalen Benutzers

Wenn Sie lokale Administratorgruppen erstellt haben, können Sie einen oder mehrere lokale Benutzer erstellen und jeden Benutzer einer oder mehreren Gruppen zuweisen. Die Berechtigungen der Gruppe steuern, auf welche Grid Manager den Benutzer zugreifen kann.

Über diese Aufgabe

Sie können nur lokale Benutzer erstellen und diese Benutzer nur lokalen Admin-Gruppen zuweisen. Verbundene Benutzer und Gruppen werden über die externe Identitätsquelle verwaltet.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Benutzer**.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie den Anzeigenamen, den eindeutigen Namen und das Kennwort des Benutzers ein.
4. Weisen Sie den Benutzer einer oder mehreren Gruppen zu, die die Zugriffsberechtigungen regeln.

   Die Liste der Gruppennamen wird aus der Tabelle Gruppen generiert.

5. Klicken Sie Auf **Speichern**.

Verwandte Informationen

"Verwalten von Admin-Gruppen"

Ändern des Kontos eines lokalen Benutzers

Sie können das Konto eines lokalen Administratorbenutzers ändern, um den Anzeigenamen oder die Gruppenmitgliedschaft des Benutzers zu aktualisieren. Sie können auch vorübergehend verhindern, dass ein Benutzer auf das System zugreift.

Über diese Aufgabe

Sie können nur lokale Benutzer bearbeiten. Verbundene Benutzerdetails werden automatisch mit der externen Identitätsquelle synchronisiert.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Benutzer**.
2. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Bearbeiten**.
4. Ändern Sie optional den Namen oder die Gruppenmitgliedschaft.

5. Um den Benutzer vorübergehend nicht auf das System zugreifen zu können, aktivieren Sie **Zugriff verweigern**.
6. Klicken Sie Auf **Speichern**.

   Die neuen Einstellungen werden angewendet, wenn sich der Benutzer beim nächsten Mal abmeldet und sich dann wieder beim Grid Manager anmeldet.

Löschen eines lokalen Benutzerkontos

Sie können Konten für lokale Benutzer löschen, die keinen Zugriff mehr auf den Grid Manager benötigen.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Benutzer**.
2. Wählen Sie den lokalen Benutzer aus, den Sie löschen möchten.

   Der vordefinierte lokale Root-Benutzer kann nicht gelöscht werden.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Entfernen**.
4. Klicken Sie auf **OK**.

Ändern des Kennworts eines lokalen Benutzers

Lokale Benutzer können ihre eigenen Passwörter mit der Option **Passwort ändern** im Banner Grid Manager ändern. Darüber hinaus können Benutzer, die Zugriff auf die Seite Admin-Benutzer haben, Passwörter für andere lokale Benutzer ändern.

Über diese Aufgabe

Sie können Passwörter nur für lokale Benutzer ändern. Verbundene Benutzer müssen ihre eigenen Passwörter in der externen Identitätsquelle ändern.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Benutzer**.
2. Wählen Sie auf der Seite Benutzer den Benutzer aus.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Sie können dann die Suchfunktion Ihres Browsers verwenden, um nach einem bestimmten Element in den aktuell angezeigten Zeilen zu suchen.

3. Klicken Sie Auf **Passwort Ändern**.
4. Geben Sie das Passwort ein und bestätigen Sie es, und klicken Sie auf **Speichern**.

Verwenden von Single Sign On (SSO) für StorageGRID

Das StorageGRID-System unterstützt Single Sign-On (SSO) unter Verwendung des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards. Wenn SSO aktiviert ist, müssen alle Benutzer von einem externen Identitäts-Provider authentifiziert werden,

bevor sie auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

- "Funktionsweise von Single Sign-On"
- "Anforderungen für die Nutzung von Single Sign On"
- "Konfigurieren der Single Sign-On-Konfiguration"

Funktionsweise von Single Sign-On

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

Anmeldung bei aktiviertem SSO

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

Schritte

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

   Die Seite StorageGRID-Anmeldung wird angezeigt.

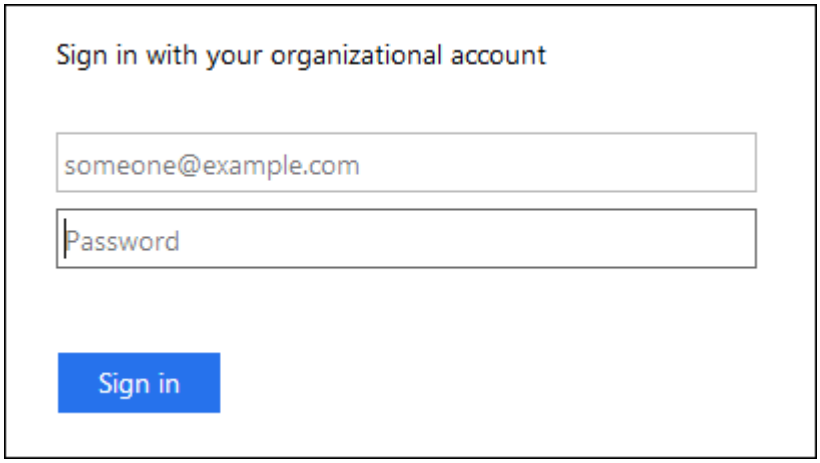
   - Wenn Sie in diesem Browser zum ersten Mal auf die URL zugegriffen haben, werden Sie aufgefordert, eine Konto-ID einzugeben:

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

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

2. Geben Sie an, ob Sie auf den Grid Manager oder den Tenant Manager zugreifen möchten:
   - Um auf den Grid Manager zuzugreifen, lassen Sie das Feld**Konto-ID** leer, geben Sie **0** als Konto-ID ein, oder wählen Sie **Grid-Manager**, 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. Klicken Sie auf **Anmelden**

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



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

   Falls Ihre SSO-Anmeldedaten korrekt sind:

   a. Der Identitäts-Provider (IdP) stellt eine Authentifizierungsantwort für StorageGRID bereit.
   b. StorageGRID validiert die Authentifizierungsantwort.
   c. Wenn die Antwort gültig ist und Sie einer Gruppe angehören, die über ausreichende Zugriffsberechtigungen verfügt, werden Sie je nach ausgewähltem Konto beim Grid Manager oder dem Tenant Manager angemeldet.
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. Klicken Sie oben rechts auf der Benutzeroberfläche auf den Link **Abmelden**.
2. Klicken Sie Auf **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
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.

Anforderungen für die Nutzung von Single Sign On

Bevor Sie Single Sign On (SSO) für ein StorageGRID-System aktivieren, überprüfen Sie die Anforderungen in diesem Abschnitt.

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.

Anforderungen an Identitätsanbieter

Der Identitäts-Provider (IdP) für SSO muss die folgenden Anforderungen erfüllen:

- Eine der folgenden Versionen des Active Directory Federation Service (AD FS):
  - AD FS 4.0, im Lieferumfang von Windows Server 2016 enthalten

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

Serverzertifikate-Anforderungen

StorageGRID verwendet auf jedem Admin-Node ein Zertifikat für die Managementschnittstelle, um den Zugriff auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandantenmanagement-API zu sichern. Wenn Sie SSO-Vertrauensstellen für StorageGRID in AD FS konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID-Anforderungen an AD FS.

Falls Sie noch kein benutzerdefiniertes Serverzertifikat für die Managementoberfläche installiert haben, sollten Sie dies jetzt tun. Wenn Sie ein benutzerdefiniertes Serverzertifikat installieren, wird es für alle Administratorknoten verwendet, und Sie können es in allen StorageGRID-Vertrauensstellungen verwenden.

Es wird nicht empfohlen, das Standardserverzertifikat eines Admin-Knotens im AD FS-Vertrauensverhältnis 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 betreffenden Partei in AD FS mit dem neuen Zertifikat aktualisieren.

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

Verwandte Informationen

"Zugriffskontrolle durch Firewalls"

"Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"

Konfigurieren der Single Sign-On-Konfiguration

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.

- "Bestätigung der föderierten Benutzer kann sich anmelden"
- "Sandbox-Modus verwenden"
- "Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS"
- "Testen von Vertrauen von Vertrauensstellen"
- "Aktivieren von Single Sign On"
- "Deaktivieren der Einzelanmeldung"
- "Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten"

Bestätigung der föderierten Benutzer kann sich anmelden

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie verwenden Active Directory als föderierte Identitätsquelle und AD FS als Identitätsanbieter.

  "Anforderungen für die Nutzung von Single Sign On"

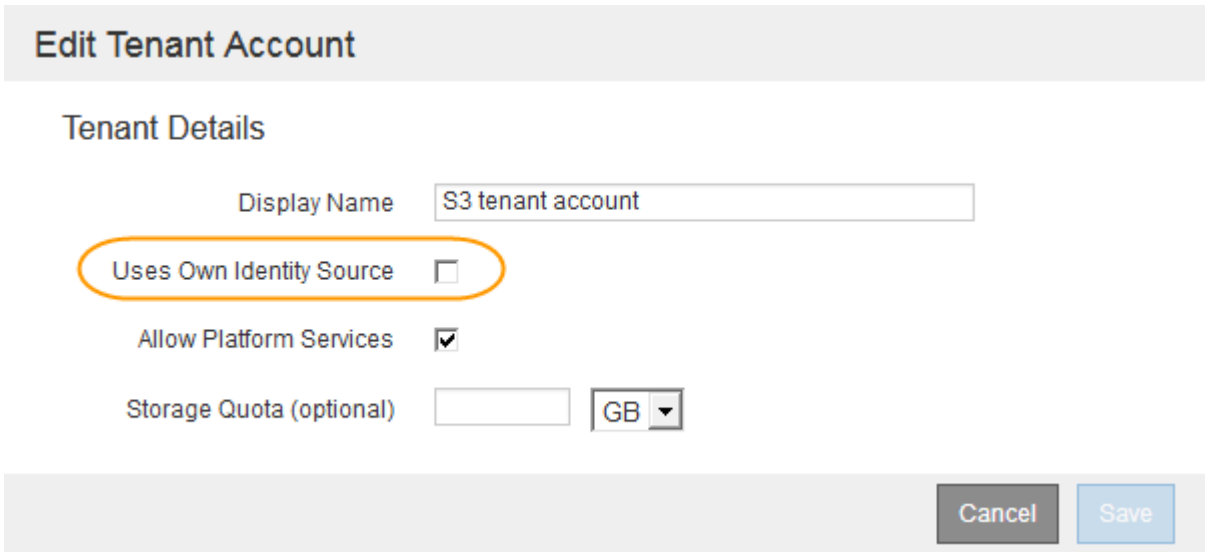
Schritte

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 **Zugriffskontrolle** > **Identitätsföderation**.
c. Bestätigen Sie, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht aktiviert ist.
d. Wenn dies der Fall ist, bestätigen Sie, dass alle föderierten Gruppen, die für dieses Mandantenkonto verwendet werden, nicht mehr erforderlich sind. Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **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 vorhandene Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root Access-Berechtigung anmelden kann:
   a. Wählen Sie im Grid Manager die Option **Miters** aus.
   b. Wählen Sie das Mandantenkonto aus und klicken Sie auf **Konto bearbeiten**.
   c. Wenn das Kontrollkästchen * verwendet eigene Identitätsquelle* aktiviert ist, deaktivieren Sie das Kontrollkästchen und klicken Sie auf **Speichern**.



Die Seite Mandantenkonten wird angezeigt.

a. Wählen Sie das Mandantenkonto aus, klicken Sie auf **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
b. Klicken Sie im Mandantenmanager auf **Zugriffskontrolle** > **Gruppen**.

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

d. Abmelden.

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

Verwandte Informationen

"Anforderungen für die Nutzung von Single Sign On"

"Verwalten von Admin-Gruppen"

"Verwenden Sie ein Mandantenkonto"

Sandbox-Modus verwenden

Sie können den Sandbox-Modus verwenden, um Active Directory Federation Services (AD FS) zu konfigurieren und zu testen, die auf Vertrauen von Parteien basieren, bevor Sie SSO für StorageGRID-Benutzer durchsetzen. Nachdem SSO aktiviert ist, können Sie den Sandbox-Modus erneut aktivieren, um neue und vorhandene Vertrauensstellen zu konfigurieren oder zu testen. Im Sandbox-Modus wird SSO für StorageGRID-Benutzer vorübergehend deaktiviert.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an AD FS. Wiederum sendet AD FS eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Autorisierungsanforderung erfolgreich war. Für erfolgreiche Anforderungen enthält die Antwort eine universell eindeutige Kennung (UUID) für den Benutzer.

Damit StorageGRID (der Service Provider) und AD FS (der Identitäts-Provider) sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, müssen Sie bestimmte Einstellungen in StorageGRID konfigurieren. Als Nächstes müssen Sie AD FS verwenden, um für jeden Admin-Knoten ein Vertrauensverhältnis zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, um SSO zu aktivieren.

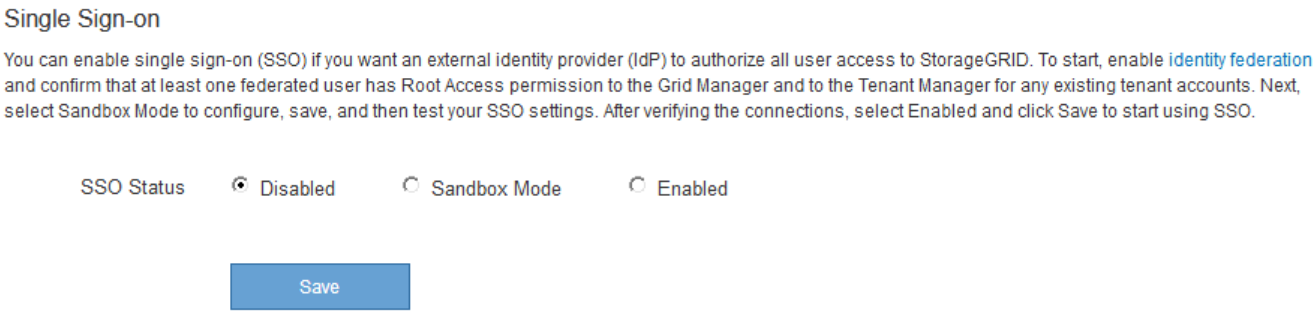
Im Sandbox-Modus ist es einfach, diese Rückkehrkonfiguration durchzuführen und alle Einstellungen zu testen, bevor Sie SSO aktivieren.

> Die Verwendung des Sandbox-Modus ist sehr empfehlenswert, aber nicht unbedingt erforderlich. Wenn Sie bereit sind, AD FS zu erstellen, auf denen die Teilnehmer vertrauen, unmittelbar nach der Konfiguration von SSO in StorageGRID, Und Sie müssen die SSO- und SLO-Prozesse (Single Logout) für jeden Admin-Knoten nicht testen, klicken Sie auf **aktiviert**, geben Sie die StorageGRID-Einstellungen ein, erstellen Sie für jeden Admin-Knoten in AD FS ein Vertrauensverhältnis, und klicken Sie dann auf **Speichern**, um SSO zu aktivieren.

Schritte

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

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



   Wenn die Optionen für den SSO-Status nicht angezeigt werden, bestätigen Sie, dass Sie Active Directory als föderierte Identitätsquelle konfiguriert haben. Siehe „`Anforderungen für die Verwendung von Single Sign-On.`“

2. Wählen Sie die Option **Sandbox Mode**.

   Die Einstellungen für Identitäts-Provider und vertrauende Partei werden angezeigt. Im Abschnitt „Identitätsanbieter“ wird das Feld **Diensttyp** schreibgeschützt angezeigt. Es zeigt den Typ des Services zur Identitätsföderation an, den Sie verwenden (z. B. Active Directory).

3. Im Abschnitt „Identitätsanbieter“:

   a. Geben Sie den Namen des Föderationsdienstes ein, genau wie er in AD FS angezeigt wird.

      Um den Federationsdienstnamen 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.

   b. Geben Sie an, ob Sie die Verbindung mit Transport Layer Security (TLS) sichern möchten, 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 das Zertifikat in das Textfeld **CA-Zertifikat** und fügen es ein.

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

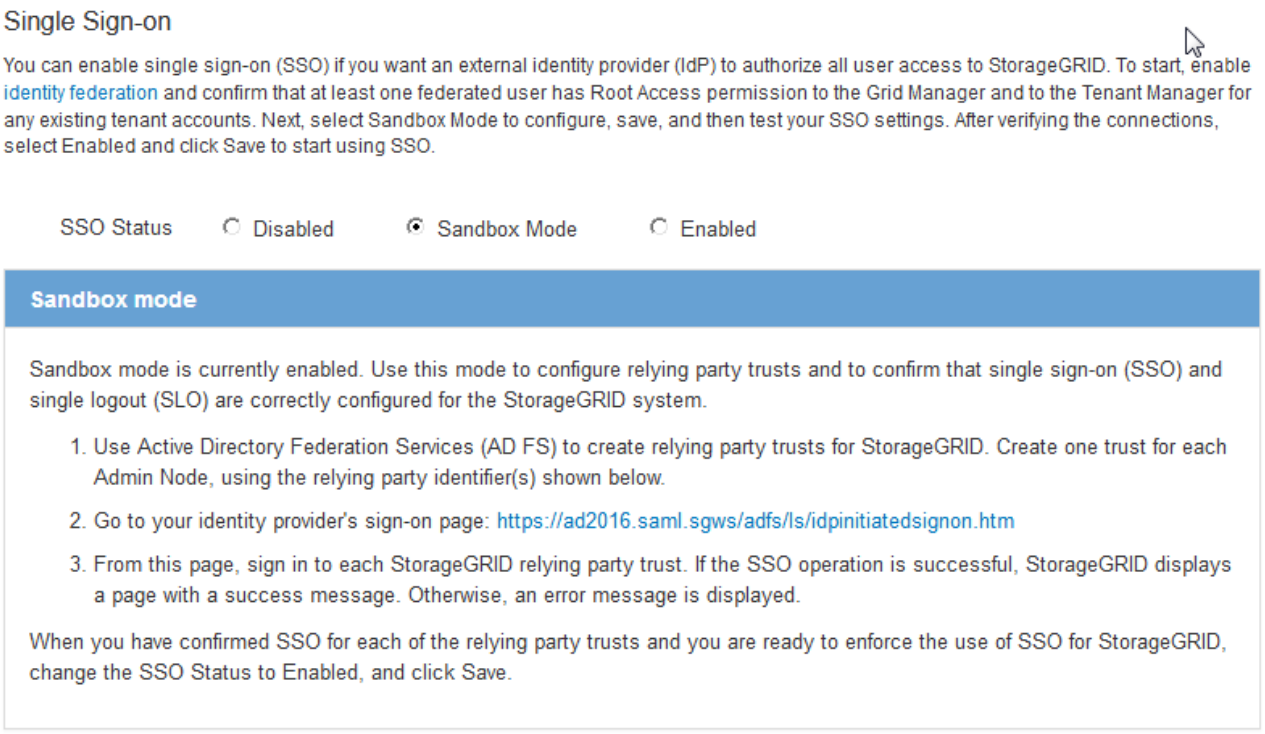
4. Geben Sie im Abschnitt „Vertrauenspartei“ die ID der betreffenden Partei an, die Sie für StorageGRID-Admin-Knoten verwenden, wenn Sie Vertrauensstellungen der betreffenden Partei konfigurieren.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Node hat und Sie nicht erwarten, dass künftig weitere Admin-Nodes hinzugefügt werden, 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 einer auf den Hostnamen des

Knotens beruhenden Partei-ID für jeden Admin-Node generiert. + HINWEIS: Sie müssen eine Vertrauensbasis für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

5. Klicken Sie Auf **Speichern**.
   - Ein grünes Häkchen wird für einige Sekunden auf der Schaltfläche **Speichern** angezeigt.

   - Der Bestätigungshinweis zum Sandbox-Modus wird angezeigt und bestätigt, dass der Sandbox-Modus nun aktiviert ist. Sie können diesen Modus verwenden, während Sie AD FS verwenden, um ein Vertrauensverhältnis von Vertrauensstellen für jeden Admin-Node zu konfigurieren und die Single Sign-in (SSO)- und SLO-Prozesse (Single Logout) zu testen.



Verwandte Informationen

"Anforderungen für die Nutzung von Single Sign On"

Erstellen von Vertrauensstellungen von Vertrauensstellen 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.

Erstellen eines Vertrauensverhältnisses mit Windows PowerShell

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

Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domänennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.

> 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.

Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Schritte

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

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

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

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

   Die Liste der Vertrauensstellen wird angezeigt.
5. Fügen Sie eine Zugriffskontrollrichtlinie zum neu erstellten Vertrauen der Vertrauensstellenden Partei hinzu:
   a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
   c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
   d. Klicken Sie auf **Anwenden** und klicken Sie auf **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. Klicken Sie auf **Regel hinzufügen**.

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

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

   Beispiel: **ObjectGUID 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. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.

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

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

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

      Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach 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 und zurück "Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen" Um sicherzustellen, dass sie richtig konfiguriert sind.

Schaffung eines Vertrauensverhältnisses durch den Import von Federationmetadaten

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

Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domänennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.

> ⓘ 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.

Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0

verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Schritte

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

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

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

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

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

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

      Beispiel: **ObjectGUID 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. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.
8. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.
   a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
   b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifier** und **Signatur** ausgefüllt sind.

      Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder

geben Sie einfach 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 und zurück "Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen" Um sicherzustellen, dass sie richtig konfiguriert sind.

Manuelles Erstellen eines Vertrauensverhältnisses mit einer Vertrauensbasis

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

Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domänennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.

> ⓘ 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 das benutzerdefinierte Zertifikat, das für die StorageGRID Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich von der Command Shell bei einem Admin-Node einloggen.
- 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.

Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Schritte

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

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

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

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

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

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

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

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

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

`*Admin_Node_Identifier*`

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

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

Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.

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

6. Um den Assistenten für die Antragsregel zu starten, klicken Sie auf **Regel hinzufügen**:
   a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
   b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

      Beispiel: **ObjectGUID 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. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **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. Klicken Sie auf **SAML hinzufügen**.
   b. Wählen Sie **Endpunkttyp** > **SAML Logout**.
   c. Wählen Sie **Bindung** > **Umleiten**.
   d. Geben Sie im Feld **Trusted URL** die URL ein, die für Single Logout (SLO) von diesem Admin-Node verwendet wird:

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

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

a. Klicken Sie auf **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, gehen Sie zu `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie das hinzu `custom-server.crt` Zertifikatdatei.

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

   b. Klicken Sie auf **Anwenden** und klicken Sie auf **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 und zurück "Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen" Um sicherzustellen, dass sie richtig konfiguriert sind.

Testen von Vertrauen von Vertrauensstellen

Bevor Sie die Verwendung von Single Sign On (SSO) für StorageGRID durchsetzen, müssen Sie sicherstellen, dass Single Sign On und Single Logout (SLO) korrekt konfiguriert sind. Wenn Sie für jeden Admin-Node eine Vertrauensbasis erstellt haben, bestätigen Sie, dass Sie SSO und SLO für jeden Admin-Node verwenden können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie haben eine oder mehrere Vertrauensstellen in AD FS konfiguriert.

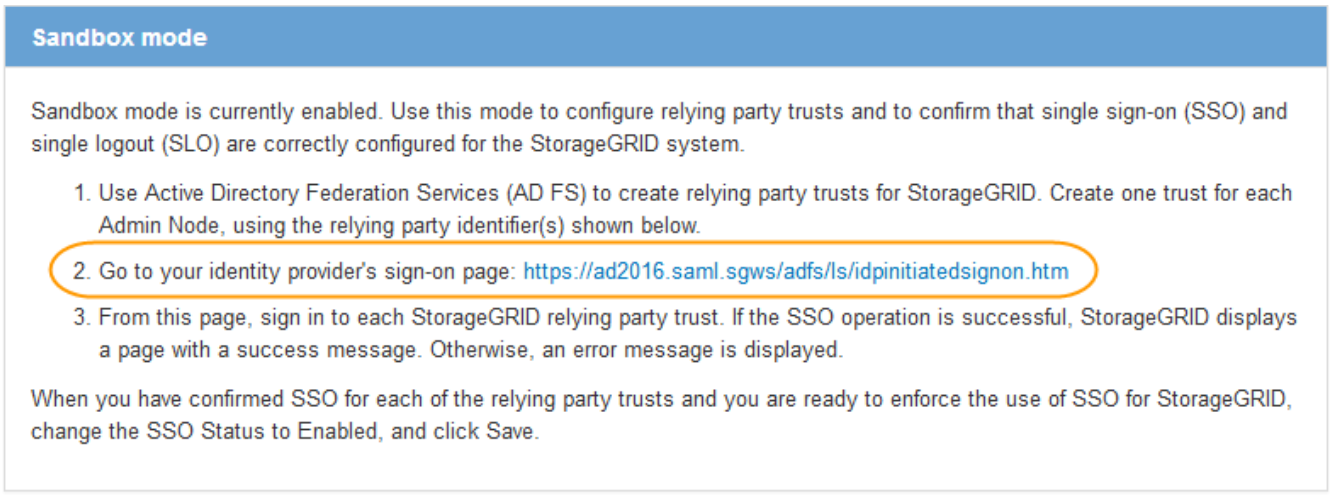
Schritte

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

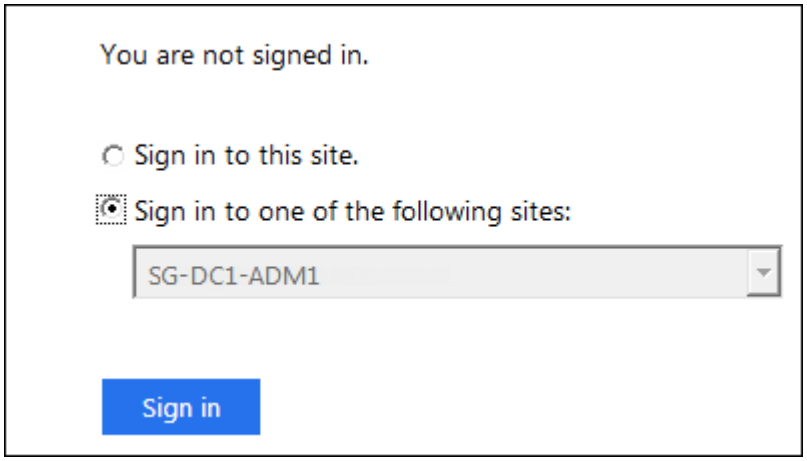
   Die Seite Single Sign-On wird angezeigt, wobei die Option **Sandbox Mode** ausgewählt ist.

2. Suchen Sie in den Anweisungen für den Sandbox-Modus den Link zur Anmeldeseite Ihres Identitätsanbieters.

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

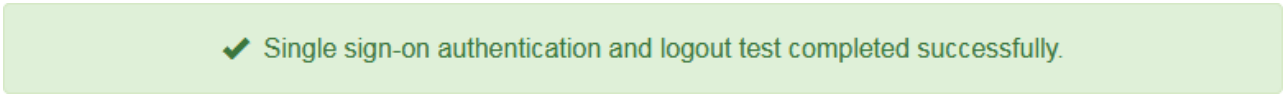


3. Klicken Sie auf den Link oder kopieren Sie die URL in einen Browser, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
4. Um zu bestätigen, dass Sie SSO zur Anmeldung bei StorageGRID verwenden können, wählen Sie **Anmelden bei einer der folgenden Sites**, wählen Sie die bevertrauende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



Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben.

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



   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.
6. Wiederholen Sie die vorherigen Schritte, um zu bestätigen, dass Sie sich bei anderen Admin-Nodes anmelden können.

Wenn alle SSO-Anmelde- und Abmeldevorgänge erfolgreich sind, können Sie SSO aktivieren.

Aktivieren von Single Sign On

Nachdem Sie den Sandbox-Modus verwendet haben, um alle Trusts von StorageGRID-Kunden zu testen, sind Sie bereit, Single Sign-On (SSO) zu aktivieren.

Was Sie benötigen

- Sie müssen mindestens eine föderierte Gruppe aus der Identitätsquelle importiert und der Gruppe Root Access Management-Berechtigungen zugewiesen haben. Sie müssen bestätigen, dass mindestens ein verbundener Benutzer Root Access-Berechtigung für den Grid Manager und den Tenant Manager für alle bestehenden Mandantenkonten hat.
- Sie müssen alle Vertrauensstellen der Vertrauensbesteller mit Sandbox-Modus getestet haben.

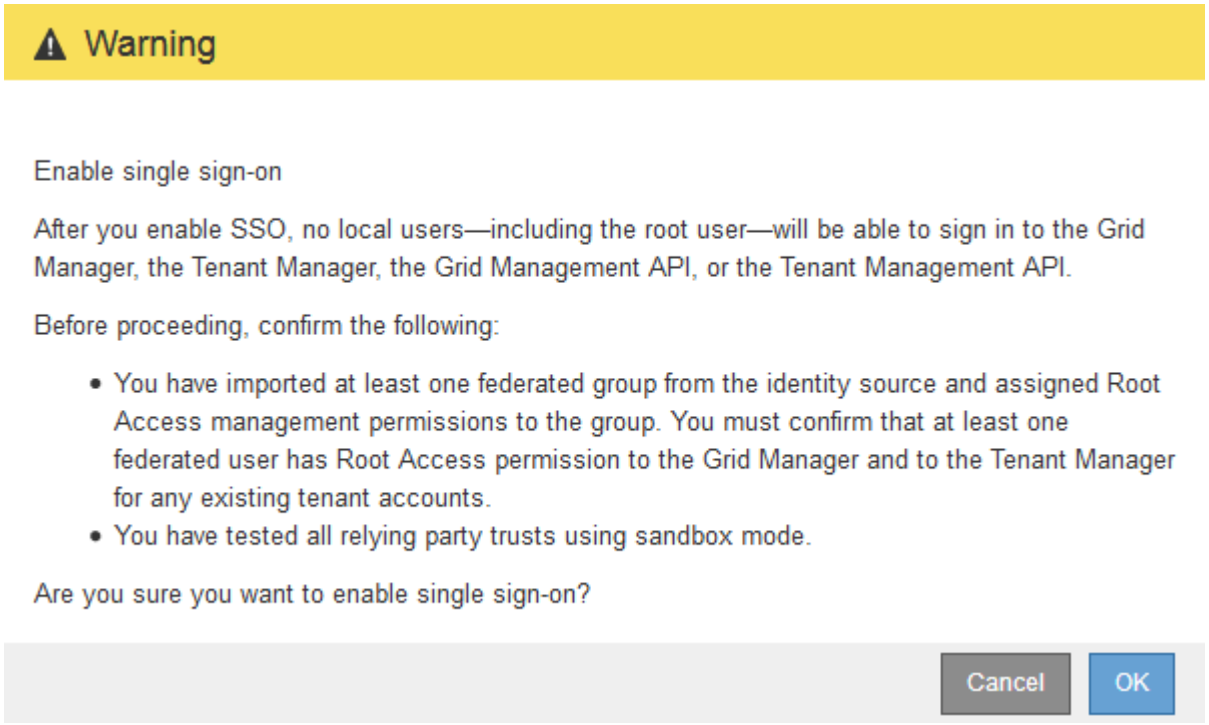
Schritte

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

   Die Seite Single Sign-On wird angezeigt, wobei **Sandbox-Modus** ausgewählt ist.

2. Ändern Sie den SSO-Status in **aktiviert**.
3. Klicken Sie Auf **Speichern**.

   Es wird eine Warnmeldung angezeigt.



4. Überprüfen Sie die Warnung und klicken Sie auf **OK**.

   Single Sign-On ist jetzt aktiviert.

> Alle Benutzer müssen 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.

Deaktivieren der Einzelanmeldung

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

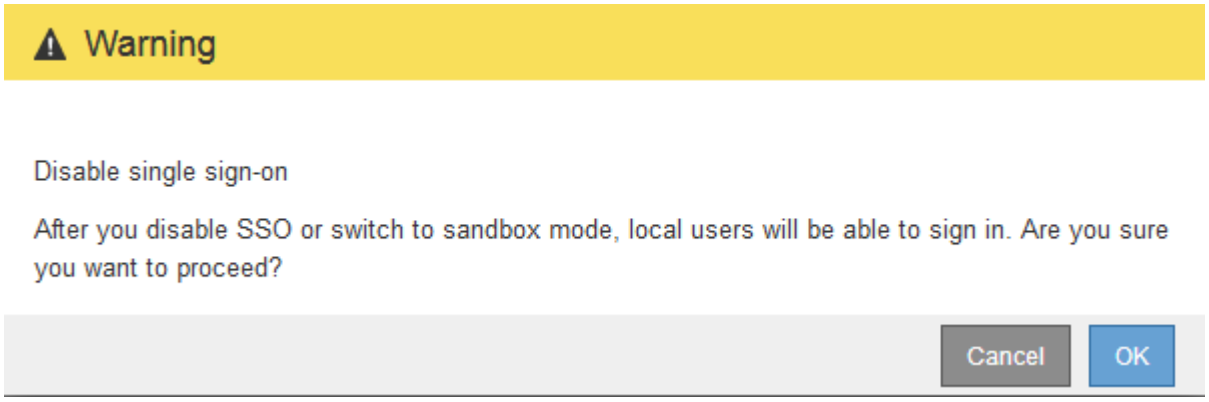
Schritte

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

   Die Seite Single Sign-On wird angezeigt.

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

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



4. Klicken Sie auf **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.

Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten

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.

Was Sie benötigen

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

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 bleiben erhalten, wenn 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. Klicken Sie Auf **Speichern**.

      Wenn Sie auf der Seite Single Sign-On auf **Save** klicken, 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. Klicken Sie auf **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.

Verwandte Informationen

"Konfigurieren der Single Sign-On-Konfiguration"

Administrator-Client-Zertifikate werden konfiguriert

Sie können Clientzertifikate verwenden, um autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank zu ermöglichen. Clientzertifikate bieten eine sichere Möglichkeit zur Verwendung externer Tools zur Überwachung von StorageGRID.

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.

Hinzufügen von Administrator-Client-Zertifikaten

Zum Hinzufügen eines Clientzertifikats können Sie Ihr eigenes Zertifikat bereitstellen oder mit dem Grid Manager ein Zertifikat erstellen.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen die IP-Adresse oder den Domänennamen des Admin-Knotens kennen.
- Sie müssen das Zertifikat für den StorageGRID-Verwaltungsserver konfiguriert haben und über das entsprechende CA-Paket verfügen
- Wenn Sie Ihr eigenes Zertifikat hochladen möchten, müssen der öffentliche Schlüssel und der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer verfügbar sein.

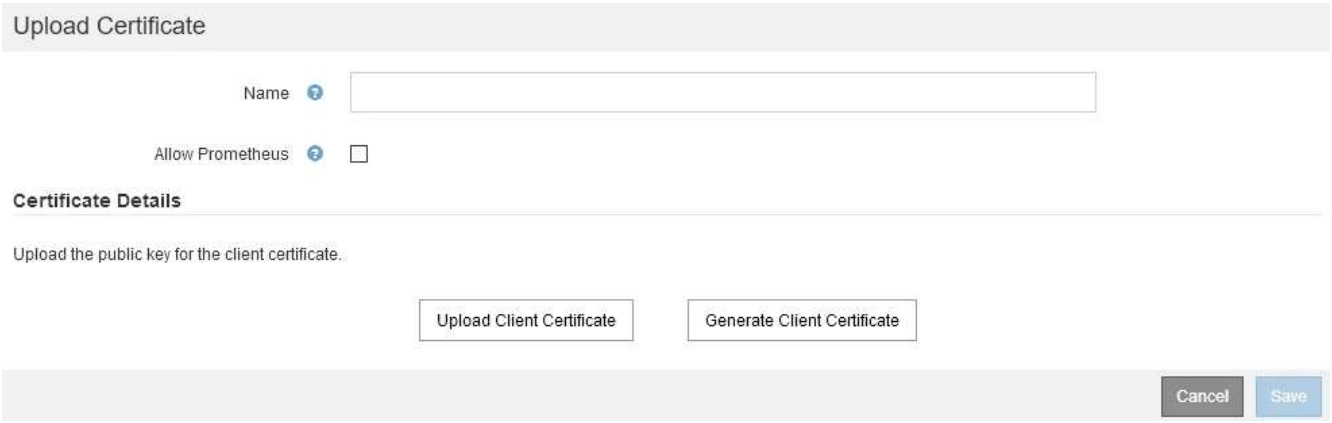
Schritte

1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Zugriffskontrolle** > **Clientzertifikate** aus.

   Die Seite Clientzertifikate wird angezeigt.

2. Wählen Sie **Hinzufügen**.

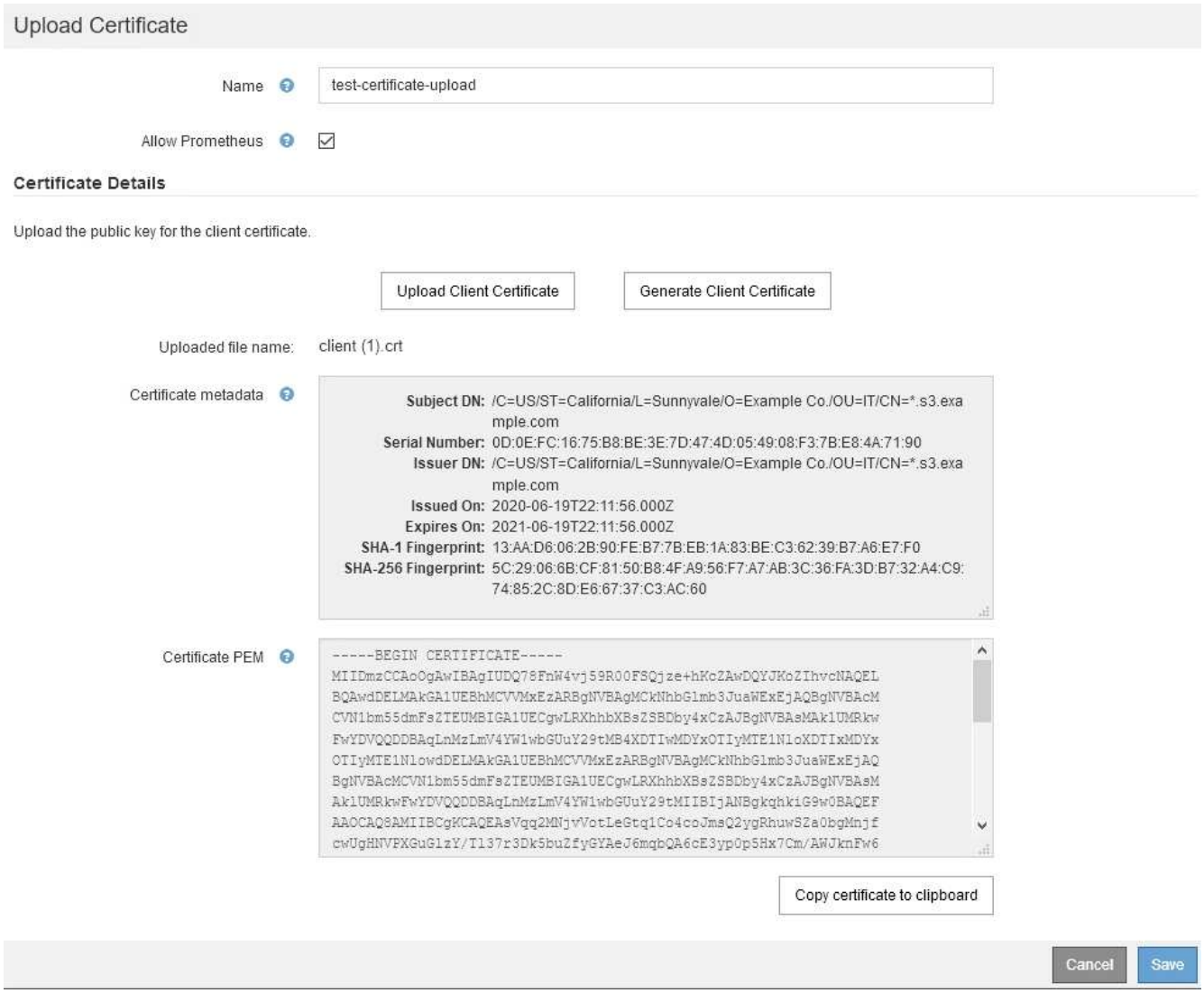
   Die Seite Zertifikat hochladen wird angezeigt.



3. Geben Sie einen Namen zwischen 1 und 32 Zeichen für das Zertifikat ein.
4. Um über Ihr externes Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, aktivieren Sie das Kontrollkästchen **Prometheus erlauben**.
5. Hochladen oder Generieren eines Zertifikats:
   a. Um ein Zertifikat hochzuladen, gehen Sie Hier.
   b. Gehen Sie zum Generieren eines Zertifikats Hier.
6.] zum Hochladen eines Zertifikats:

   a. Wählen Sie **Client-Zertifikat Hochladen**.
   b. Suchen Sie nach dem öffentlichen Schlüssel für das Zertifikat.

      Nachdem Sie den öffentlichen Schlüssel für das Zertifikat hochgeladen haben, werden die Felder **Certificate Metadaten** und **Certificate PEM** ausgefüllt.



a. Wählen Sie **Zertifikat in Zwischenablage kopieren** und fügen Sie das Zertifikat in Ihr externes Überwachungstool ein.

b. Verwenden Sie ein Bearbeitungswerkzeug, um den privaten Schlüssel in Ihr externes Überwachungstool zu kopieren und einzufügen.

c. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.

7.] zum Generieren eines Zertifikats:

a. Wählen Sie **Client-Zertifikat Erstellen**.

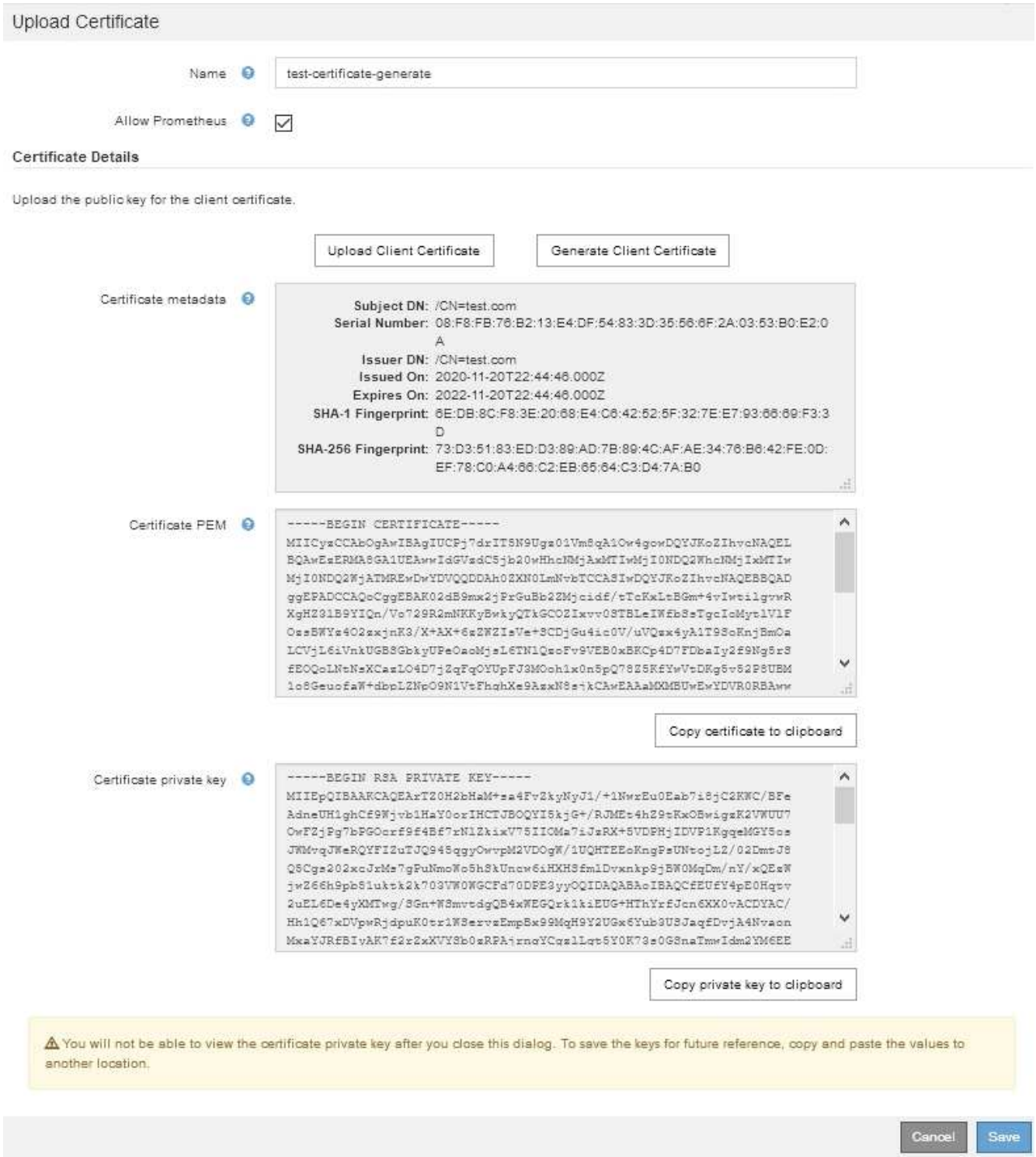
b. Geben Sie den Domänennamen oder die IP-Adresse des Admin-Knotens ein.

c. Geben Sie optional einen X.509-Studienteilnehmer ein, der auch als Distinguished Name (DN) bezeichnet wird, um den Administrator zu identifizieren, der das Zertifikat besitzt.

d. Wählen Sie optional die Anzahl der Tage aus, an denen das Zertifikat gültig ist. Der Standardwert ist 730 Tage.

e. Wählen Sie **Erzeugen**.

Die Felder **Certificate Metadaten**, **Certificate PEM** und **Certificate Private Key** sind ausgefüllt.



a. Wählen Sie **Zertifikat in Zwischenablage kopieren** und fügen Sie das Zertifikat in Ihr externes Überwachungstool ein.

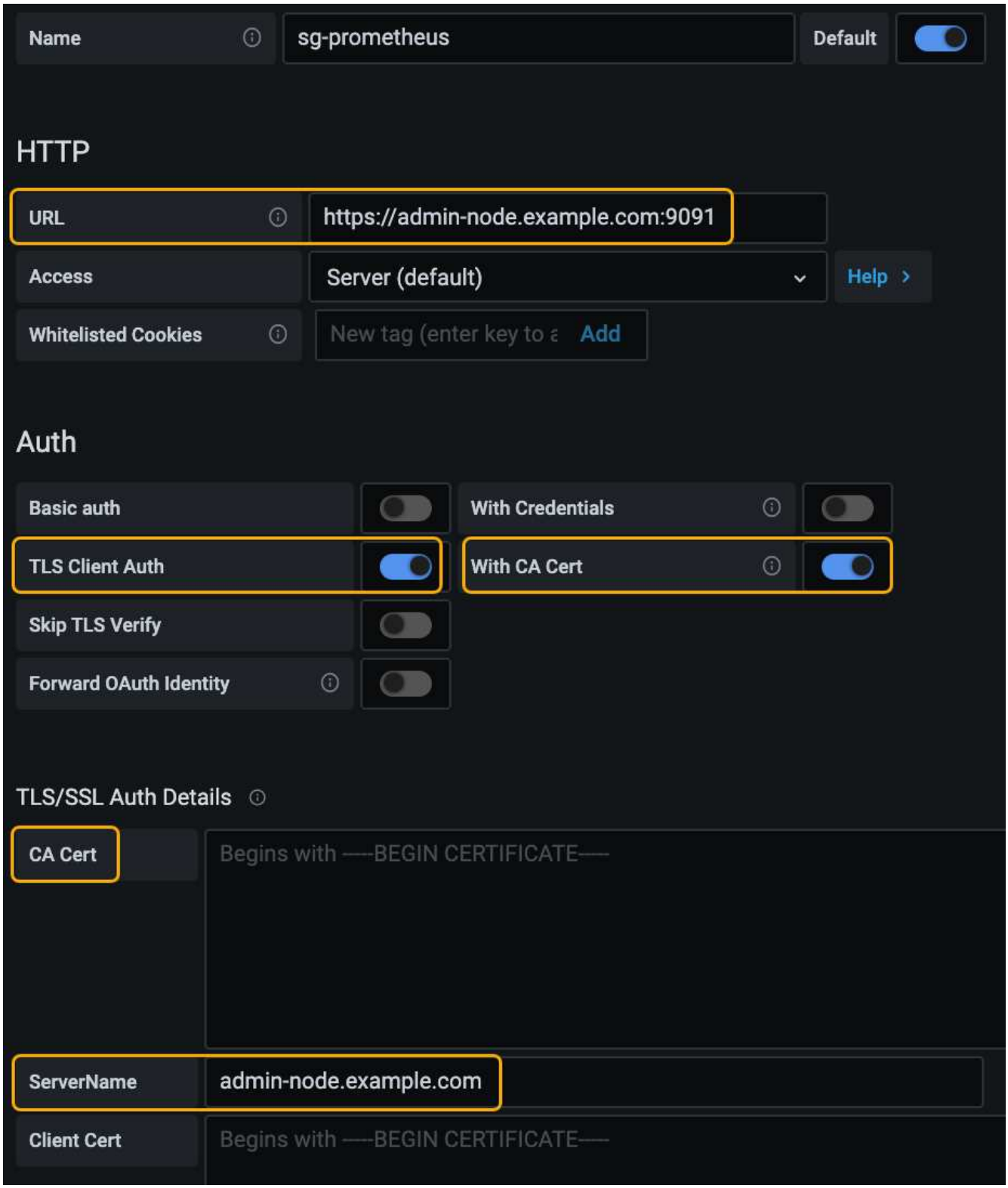
b. Wählen Sie **Privatschlüssel in Zwischenablage kopieren** und fügen Sie den Schlüssel in Ihr externes Überwachungstool ein.

> Nach dem Schließen des Dialogfelds können Sie den privaten Schlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einen sicheren Ort.

c. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.

8. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.

   Ein Grafana-Beispiel ist im folgenden Screenshot dargestellt:



   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 Authorization** und **mit CA Cert**.

d. Kopieren Sie das Zertifikat des Management Interface Server oder CA-Pakets unter TLS/SSL-Auth-Details auf das**CA-Zertifikat**.

e. **ServerName**: Geben Sie den Domainnamen des Admin-Knotens ein.

   Servername muss mit dem Domänennamen übereinstimmen, wie er im Management Interface Server Certificate angezeigt wird.

f. 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 in den Anweisungen für das Monitoring und die Fehlerbehebung von StorageGRID.

Verwandte Informationen

"StorageGRID-Sicherheitszertifikate werden verwendet"

"Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"

"Monitor Fehlerbehebung"

Bearbeiten von Administrator-Clientzertifikaten

Sie können ein Zertifikat bearbeiten, um seinen Namen zu ändern, Prometheus-Zugriff zu aktivieren oder zu deaktivieren oder ein neues Zertifikat hochzuladen, wenn das aktuelle abgelaufen ist.

Was Sie benötigen

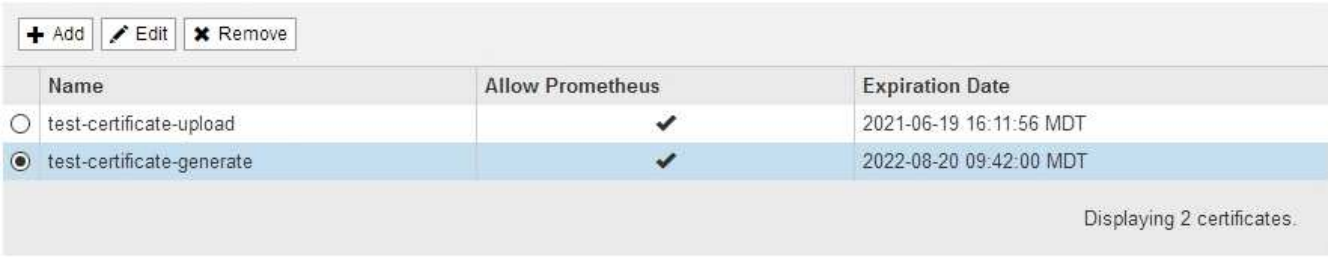
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen die IP-Adresse oder den Domänennamen des Admin-Knotens kennen.
- Wenn Sie ein neues Zertifikat und einen privaten Schlüssel hochladen möchten, müssen diese auf Ihrem lokalen Computer verfügbar sein.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Client-Zertifikate**.

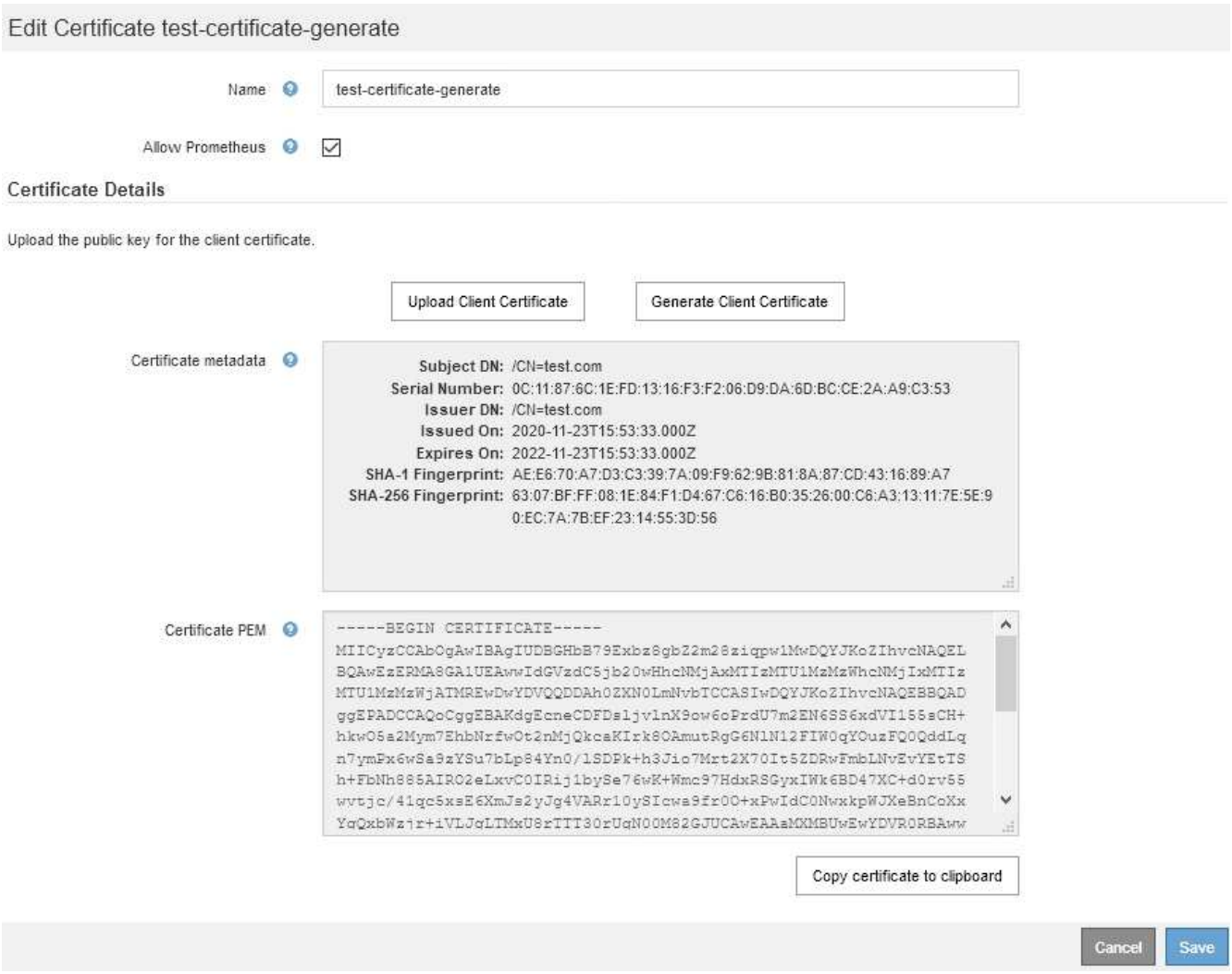
   Die Seite Clientzertifikate wird angezeigt. Die vorhandenen Zertifikate sind aufgelistet.

   In der Tabelle sind die Daten zum Ablauf des Zertifikats 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 Optionsfeld links neben dem Zertifikat, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten**.

   Das Dialogfeld Zertifikat bearbeiten wird angezeigt.



4. Nehmen Sie die gewünschten Änderungen am Zertifikat vor.
5. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.
6. Wenn Sie ein neues Zertifikat hochgeladen haben:
   a. Wählen Sie **Zertifikat in Zwischenablage kopieren** aus, um das Zertifikat in Ihr externes Überwachungstool einzufügen.
   b. Verwenden Sie ein Bearbeitungswerkzeug, um den neuen privaten Schlüssel in Ihr externes Überwachungstool zu kopieren und einzufügen.

c. Speichern und testen Sie das Zertifikat und den privaten Schlüssel in Ihrem externen Monitoring-Tool.

7. Wenn Sie ein neues Zertifikat generiert haben:
   a. Wählen Sie **Zertifikat in Zwischenablage kopieren** aus, um das Zertifikat in Ihr externes Überwachungstool einzufügen.
   b. Wählen Sie **Privatschlüssel in Zwischenablage kopieren**, um das Zertifikat in Ihr externes Überwachungstool einzufügen.

      Nach dem Schließen des Dialogfelds können Sie den privaten Schlüssel nicht anzeigen oder kopieren. Kopieren Sie den Schlüssel an einen sicheren Ort.

   c. Speichern und testen Sie das Zertifikat und den privaten Schlüssel in Ihrem externen Monitoring-Tool.

Entfernen von Administrator-Client-Zertifikaten

Wenn Sie kein Zertifikat mehr benötigen, können Sie es entfernen.

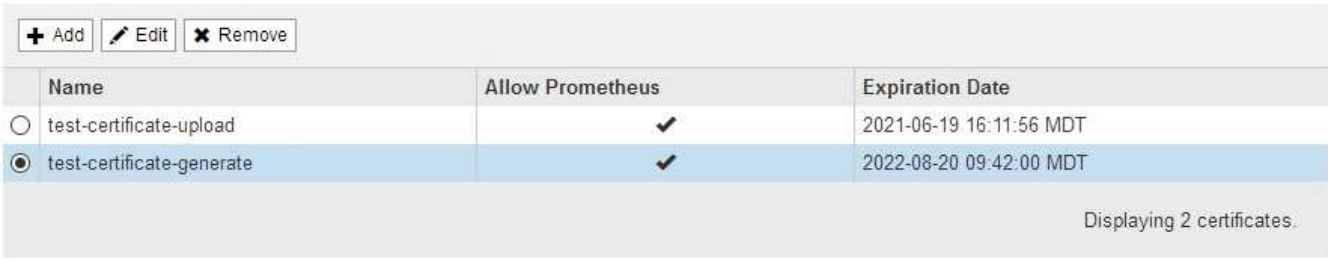
Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

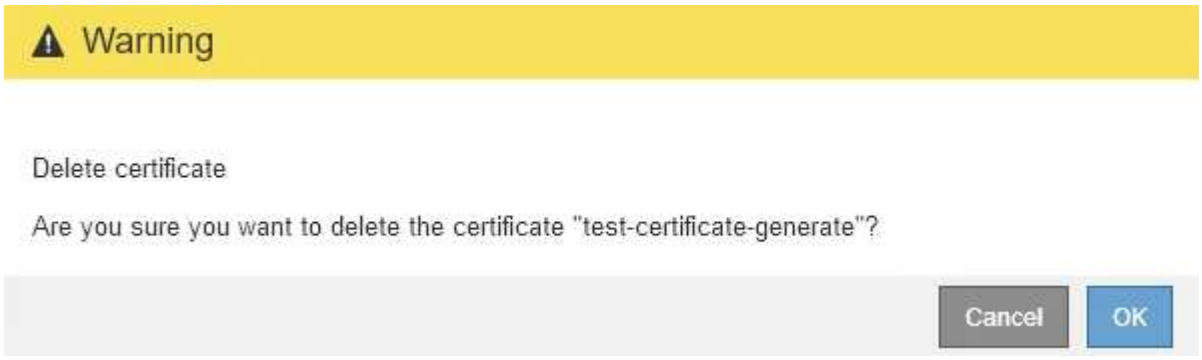
1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Client-Zertifikate**.

   Die Seite Clientzertifikate wird angezeigt. Die vorhandenen Zertifikate sind aufgelistet.



2. Wählen Sie das Optionsfeld links neben dem Zertifikat, das Sie entfernen möchten.
3. Wählen Sie **Entfernen**.

   Ein Bestätigungsdialogfeld wird angezeigt.



4. Wählen Sie **OK**.

Das Zertifikat wird entfernt.

Konfigurieren von Verschlüsselungsmanagement-Servern

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 sind, können Sie erst auf sämtliche 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.

Überprüfen von 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	Sie konfigurieren einen Schlüsselverwaltungsserver für den StorageGRID-Standort (**Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver**) und aktivieren die Knotenverschlüsselung 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. Kann mit einigen StorageGRID Storage und Service Appliances verwendet werden.
Laufwerkssicherheit in SANtricity System Manager	Wenn die Laufwerkssicherheitsfunktion für eine Speicher-Appliance aktiviert ist, können Sie den Sicherheitsschlüssel mit SANtricity System Manager erstellen und verwalten. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Storage-Applikationen mit Full Disk Encryption-Laufwerken (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard) Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Nicht bei einigen Storage-Appliances oder Service-Appliances verwendet werden können. "SG6000 Storage-Appliances" "SG5700 Storage-Appliances" "SG5600 Storage Appliances"
Grid-Option „gespeicherte Objektverschlüsselung“	Die Option **gespeicherte Objektverschlüsselung** kann im Grid Manager aktiviert werden (**Konfiguration** > **Systemeinstellungen** > **Grid-Optionen**). Bei Aktivierung werden alle neuen Objekte, die nicht auf Bucket-Ebene oder auf Objektebene verschlüsselt sind, während der Aufnahme verschlüsselt.	Neu aufgenommene S3- und Swift-Objektdaten vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. "Konfigurieren der gespeicherten Objektverschlüsselung"

Verschlüsselungsoption	So funktioniert es	Gilt für
S3-Bucket-Verschlüsselung	Sie stellen eine PUT-Bucket-Verschlüsselungsanforderung bereit, um die Verschlüsselung für den Bucket zu aktivieren. Neue Objekte, die nicht auf Objektebene verschlüsselt sind, werden bei der Aufnahme verschlüsselt.	Nur neu aufgenommene S3-Objektdaten.Verschlüsselung muss für den Bucket angegeben werden. Vorhandene Bucket-Objekte sind nicht verschlüsselt. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. "S3 verwenden"
S3-Objektserverseitige Verschlüsselung (SSE)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und schließen das ein `x-amz-server-side-encryption` Kopfzeile der Anfrage.	Nur neu aufgenommene S3-Objektdaten.Verschlüsselung muss für das Objekt angegeben werden. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. StorageGRID verwaltet die Schlüssel. "S3 verwenden"
S3 Objektserverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und enthalten drei Anfrageheader. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Nur neu aufgenommene S3-Objektdaten.Verschlüsselung muss für das Objekt angegeben werden. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. Schlüssel werden außerhalb von StorageGRID gemanagt. "S3 verwenden"
Externe Volume- oder Datastore-Verschlüsselung	Sofern die Implementierungsplattform sie unterstützt, verwenden Sie eine Verschlüsselungsmethode außerhalb von StorageGRID, um ein gesamtes Volume oder Datastore zu verschlüsseln.	Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, wobei jedes Volume oder jeder Datastore verschlüsselt ist Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.

Verschlüsselungsoption	So funktioniert es	Gilt für
Objektverschlüsselung außerhalb von StorageGRID	Dabei kommt eine Verschlüsselungsmethode außerhalb von StorageGRID zum Einsatz, um Objektdaten und Metadaten zu verschlüsseln, bevor sie in StorageGRID aufgenommen werden.	Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt). Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden. "Amazon Simple Storage Service – Developer Guide: Schutz von Daten mit Client-seitiger Verschlüsselung"

Verwendung mehrerer Verschlüsselungsmethoden

Je nach Ihren Anforderungen können Sie mehrere Verschlüsselungsmethoden gleichzeitig verwenden. Beispiel:

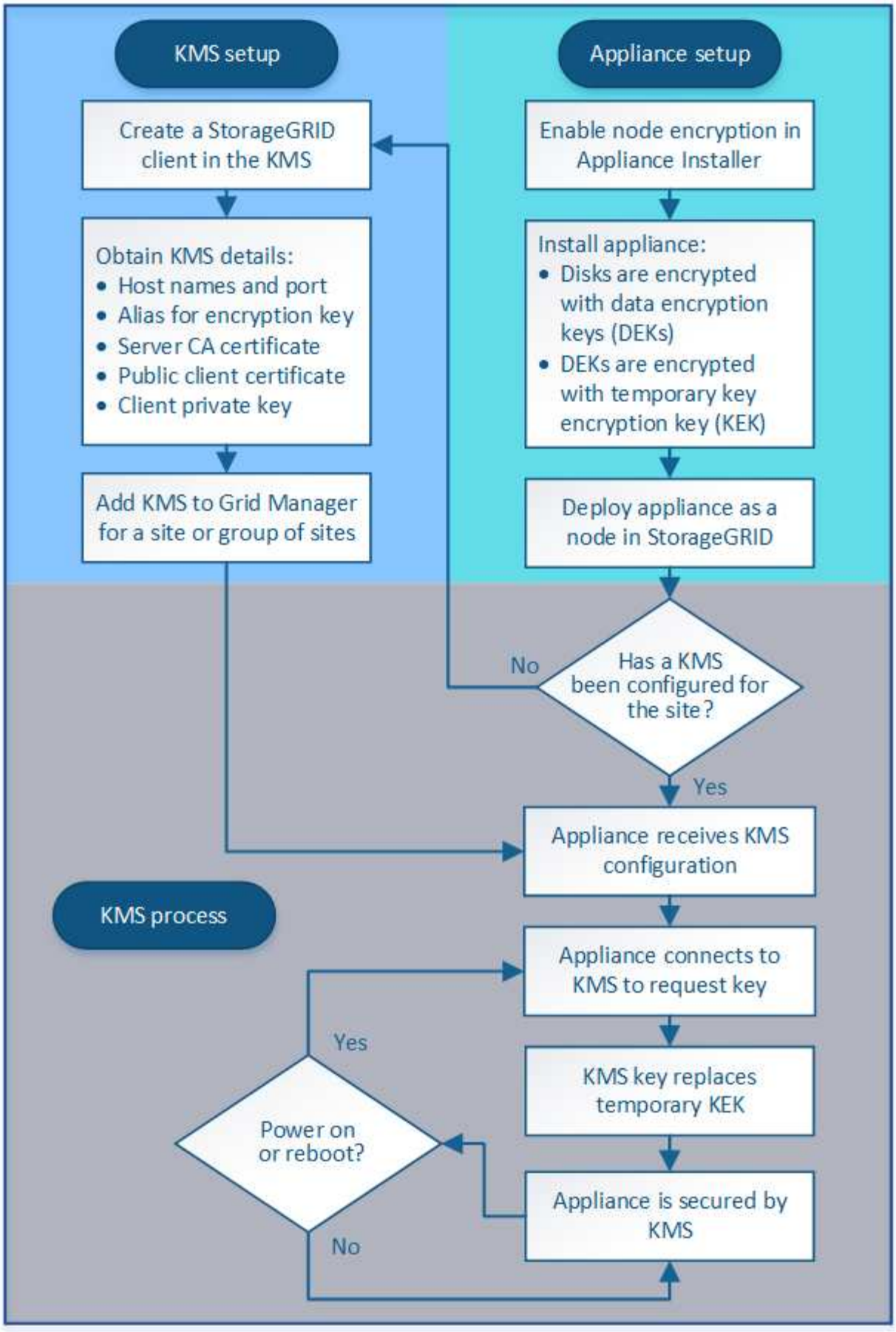
- Mit einem KMS können Appliance-Nodes geschützt werden. Außerdem kann mithilfe der Laufwerksicherheitsfunktion in SANtricity System Manager die Daten „`double verschlüsselte`“ auf den Self-Encrypting Drives in denselben Appliances verschlüsselt werden.
- Mit einem KMS lassen sich Daten auf Appliance-Nodes sichern. Zudem kann die Grid-Option „Speichered Object Encryption“ verwendet werden, 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.

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 von StorageGRID als Client im KMS"
Erhalten Sie die erforderlichen Informationen für den StorageGRID-Client auf dem KMS.	"Konfigurieren von 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)"

Einrichten des Geräts

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 ein Gerät zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, bei denen die Node-Verschlüsselung nicht 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 GerätebOS 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.

Weitere Informationen finden Sie unter:

- "SG100 SG1000 Services-Appliances"
- "SG6000 Storage-Appliances"
- "SG5700 Storage-Appliances"

- "SG5600 Storage Appliances"

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 wird, kann keinen Stromausfall oder Neustart überstehen.

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 können Sie die Node-Verschlüsselung nicht aktivieren. Appliances, bei denen die Node-Verschlüsselung nicht aktiviert ist, können externes Verschlüsselungsmanagement nicht verwenden.

Der konfigurierte KMS kann für die folgenden StorageGRID Appliances und Appliance-Nodes verwendet werden:

Appliance	Node-Typ
SG1000 Services-Appliance	Admin-Node oder Gateway-Node
SG100 Services-Appliance	Admin-Node oder Gateway-Node
SG6000 Storage Appliance	Storage-Node
SG5700 Storage-Appliance	Storage-Node
SG5600 Storage-Appliance	Storage-Node

Der konfigurierte KMS kann nicht für softwarebasierte (nicht-Appliance-) Nodes verwendet werden, einschließlich folgender Elemente:

- Als Virtual Machines (VMs) implementierte Nodes
- In Docker Containern auf Linux-Hosts implementierte Nodes

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?

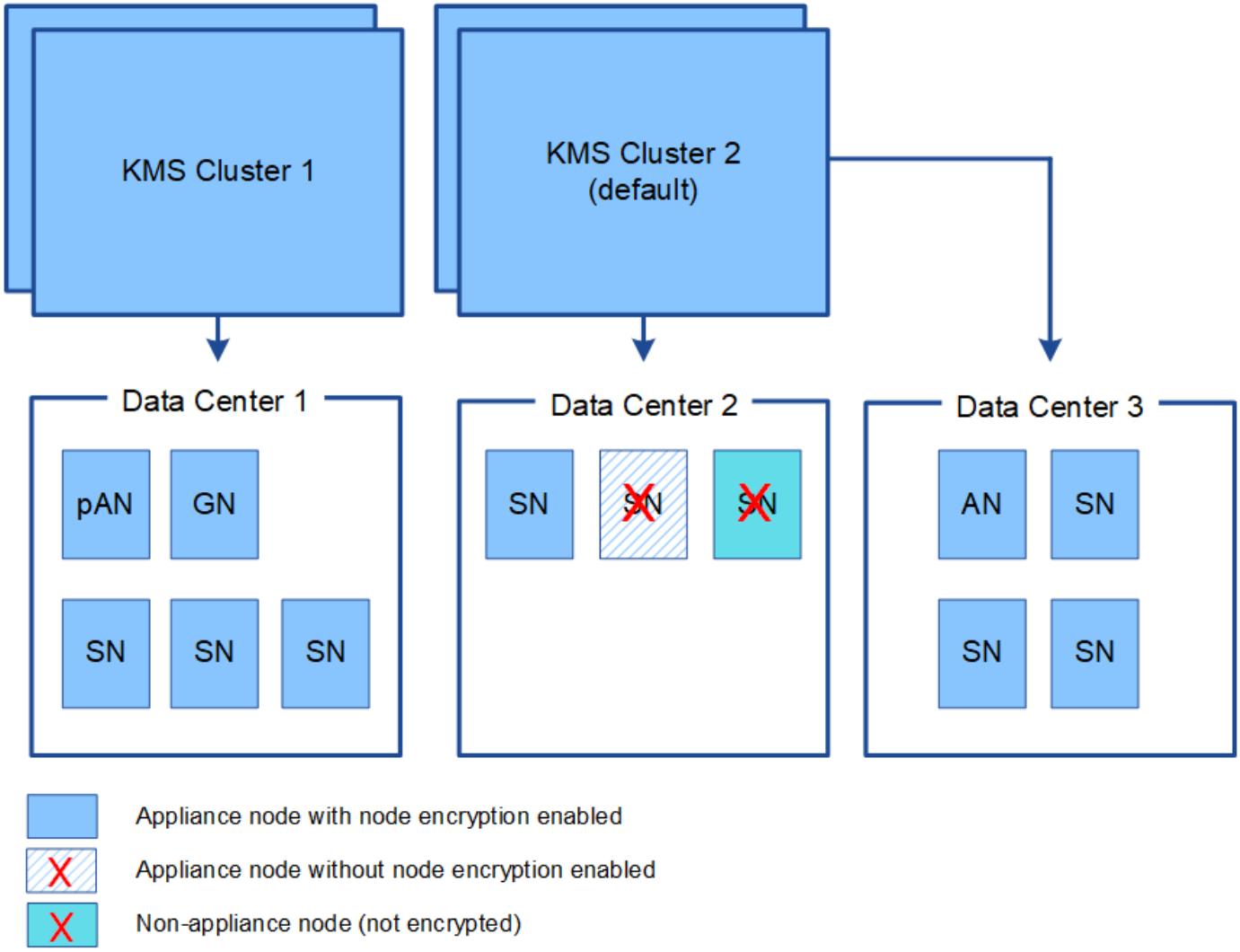
Sie können einen oder mehrere externe Verschlüsselungsmanagementserver konfigurieren, um die Appliance-Nodes in Ihrem StorageGRID-System Verschlüsselungen bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel 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 keinen KMS für nicht-Appliance-Knoten oder für Appliance-Knoten verwenden können, bei denen die **Node Encryption**-Einstellung 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 auf einen ganz anderen Schlüssel.

> 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 nicht zur Verschlüsselung von Appliance-Volumes aus irgendeinem Grund verwendet werden kann, wird für den Appliance-Node die Warnung **KMS-Verschlüsselungsschlüsseldrehung fehlgeschlagen** 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 die KMS-Konfiguration mit dem Installationsprogramm der StorageGRID-Appliance löschen. 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.

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Überlegungen für das Ändern des KMS für einen Standort

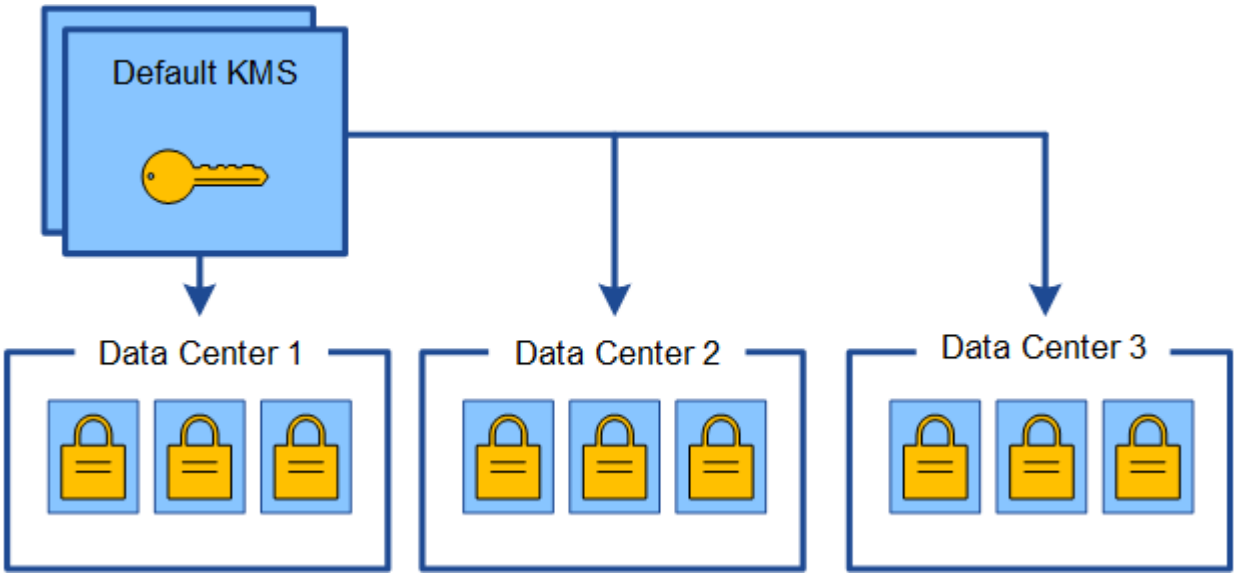
Jeder Verschlüsselungsmanagement-Server (KMS) oder KMS-Cluster gewährt allen Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel. Wenn Sie ändern müssen, welcher KMS für einen Standort verwendet wird, müssen Sie den Verschlüsselungsschlüssel möglicherweise 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

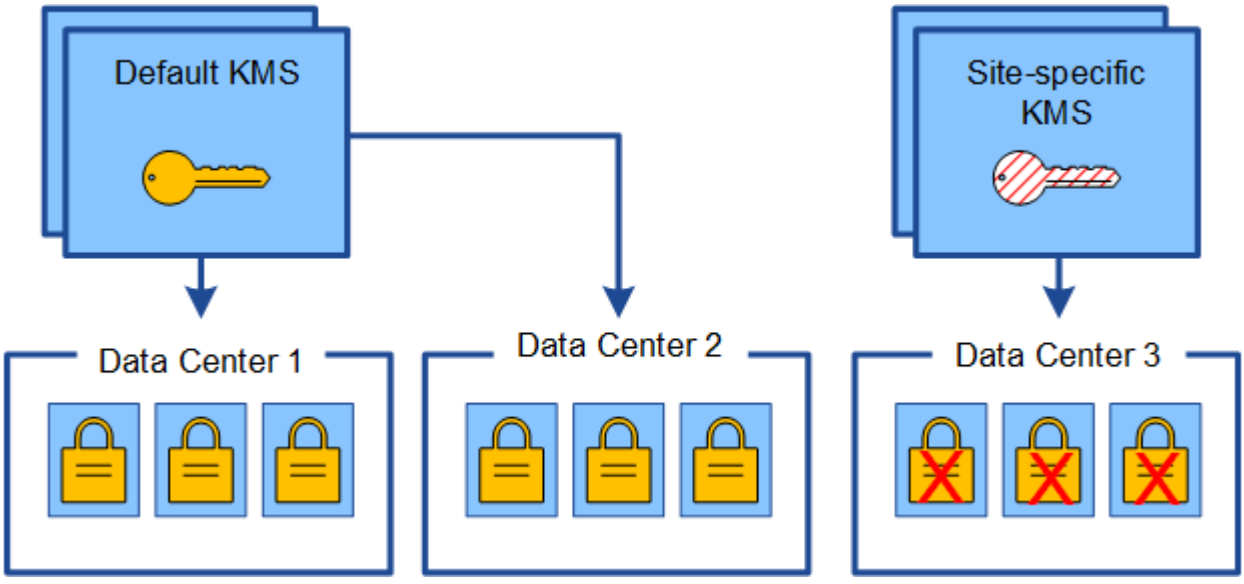
entschlüsseln.

Beispiel:

1. Sie konfigurieren zunächst einen Standard-KMS, der für alle Standorte gilt, die keinen dedizierten KMS besitzen.
2. Wenn der KMS gespeichert wird, stellen alle Appliance-Nodes, deren **Node Encryption**-Einstellung aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird verwendet, um die Appliance-Nodes an allen Standorten zu verschlüsseln. Dieser Schlüssel muss auch verwendet werden, um diese Geräte zu entschlüsseln.

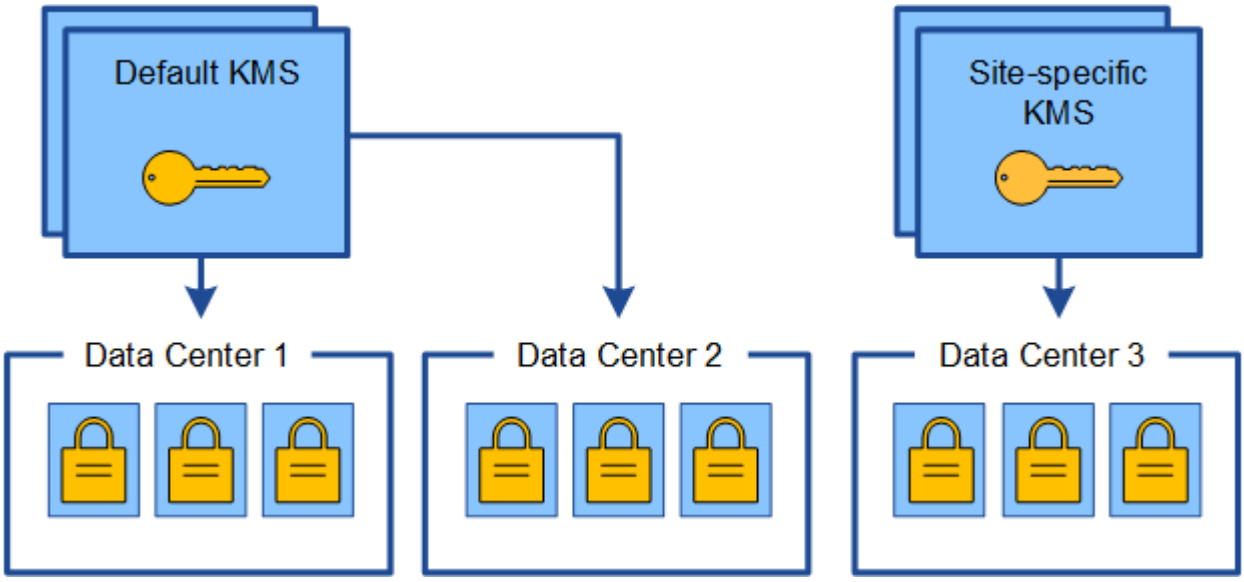


3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler tritt auf, weil der standortspezifische KMS nicht über den korrekten Schlüssel verfügt, um die Knoten an diesem Standort zu entschlüsseln.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS. (Technisch kopieren Sie den Originalschlüssel in einen neuen

Schlüssel mit dem gleichen Alias. Der ursprüngliche Schlüssel wird zu einer früheren Version des neuen Schlüssels.) Der standortspezifische KMS hat jetzt den richtigen Schlüssel zur Entschlüsselung der Appliance-Nodes in Datacenter 3, sodass er in StorageGRID gespeichert werden kann.



Anwendungsfälle für die Änderung, welcher KMS für eine Site verwendet wird

Die Tabelle fasst die erforderlichen Schritte für die häufigsten Fälle zur Änderung des KMS für einen Standort zusammen.

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie haben einen oder mehrere Site-spezifische KMS-Einträge, und Sie möchten einen von ihnen als Standard-KMS verwenden.	Bearbeiten Sie den Site-spezifischen KMS. Wählen Sie im Feld **verwaltet Schlüssel für** die Option **Sites, die nicht von einem anderen KMS verwaltet werden (Standard KMS)**. Der Site-spezifische KMS wird jetzt als Standard-KMS verwendet. Er gilt für alle Websites, die keinen dedizierten KMS haben. "Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)"
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten den Standard-KMS für die neue Site nicht verwenden.	1. Wenn die Appliance-Nodes auf dem neuen Standort bereits durch den Standard-KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf einen neuen KMS. 2. Fügen Sie mithilfe des Grid-Managers den neuen KMS hinzu und wählen Sie die Site aus. "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie möchten, dass der KMS für eine Site einen anderen Server verwendet.	1. Wenn die Appliance-Nodes am Standort bereits durch den vorhandenen KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom bestehenden KMS auf den neuen KMS. 2. Bearbeiten Sie mithilfe des Grid Manager die bestehende KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Konfigurieren von 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 k170v, Versionen 2.0, 2.1 und 2.2. Wenn Sie Fragen zur Verwendung eines anderen Verschlüsselungsmanagementservers mit StorageGRID haben, wenden Sie sich an den technischen Support.

"Thales CipherTrust Manager"

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.

   Die Verschlüsselung muss 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.

Was Sie benötigen

- Sie müssen den geprüft haben "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Dieser muss unbedingt vorhanden sein "StorageGRID wurde als Client im KMS konfiguriert", Und Sie müssen die erforderlichen Informationen für jeden KMS- oder KMS-Cluster haben
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

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.

"Überlegungen für das Ändern des KMS für einen Standort"

Schritte

1. "Schritt 1: Geben Sie KMS-Details ein"
2. "Schritt: Serverzertifikat Hochladen"
3. "Schritt 3: Laden Sie Client-Zertifikate Hoch"

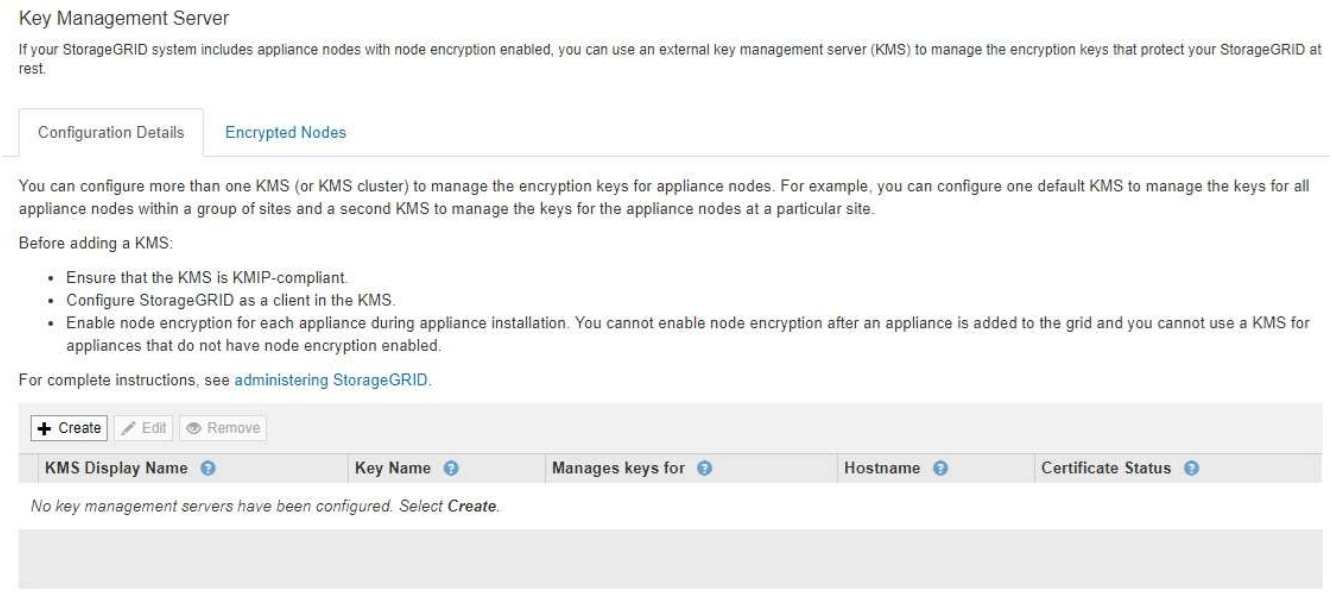
Schritt 1: Geben Sie KMS-Details ein

In Schritt 1 (KMS-Details eingeben) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers geben Sie Details zum KMS- oder KMS-Cluster an.

Schritte

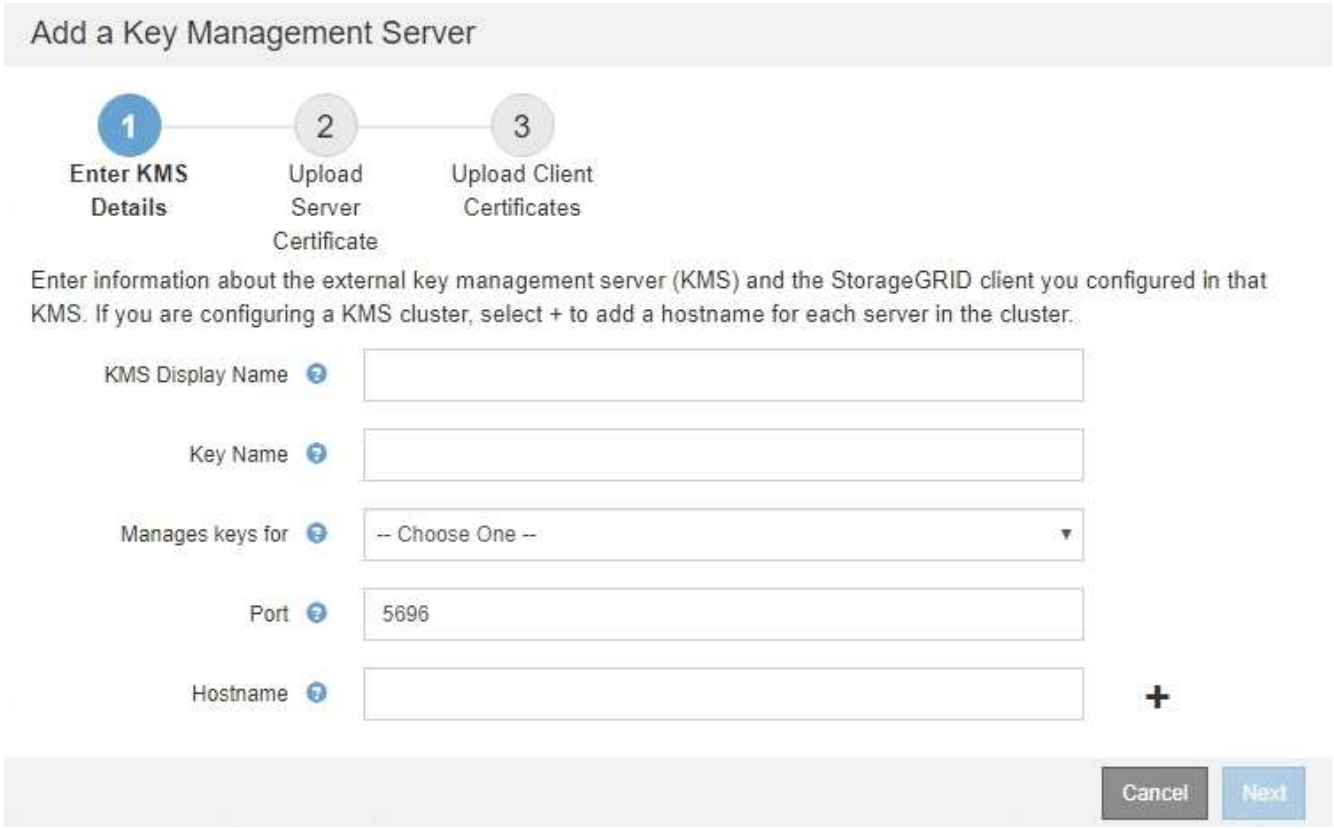
1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt, wobei die Registerkarte Konfigurationsdetails ausgewählt ist.



2. Wählen Sie **Erstellen**.

   Schritt 1 (KMS-Details eingeben) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.



3. Geben Sie die folgenden Informationen für den KMS und den StorageGRID-Client ein, den Sie in diesem KMS konfiguriert haben.

Feld	Beschreibung
KMS-Anzeigename	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.

Feld	Beschreibung
Verwaltet Schlüssel für	Der StorageGRID-Site, die diesem KMS zugeordnet wird. Wenn möglich, sollten Sie alle standortspezifischen Verschlüsselungsmanagement-Server konfigurieren, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. • Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt. • Wählen Sie **Sites, die nicht von einem anderen KMS (Standard KMS)** verwaltet werden, um einen Standard-KMS zu konfigurieren, der für alle Sites gilt, die keinen dedizierten KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. **Hinweis:** beim Speichern der KMS-Konfiguration Tritt Ein Validierungsfehler auf, wenn Sie eine Site auswählen, die zuvor durch den Standard-KMS verschlüsselt wurde, aber Sie haben die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels nicht dem neuen KMS zur Verfügung gestellt.
Port	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das SAN-Feld des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.

4. Wenn Sie einen KMS-Cluster verwenden, wählen Sie das Pluszeichen aus + Um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

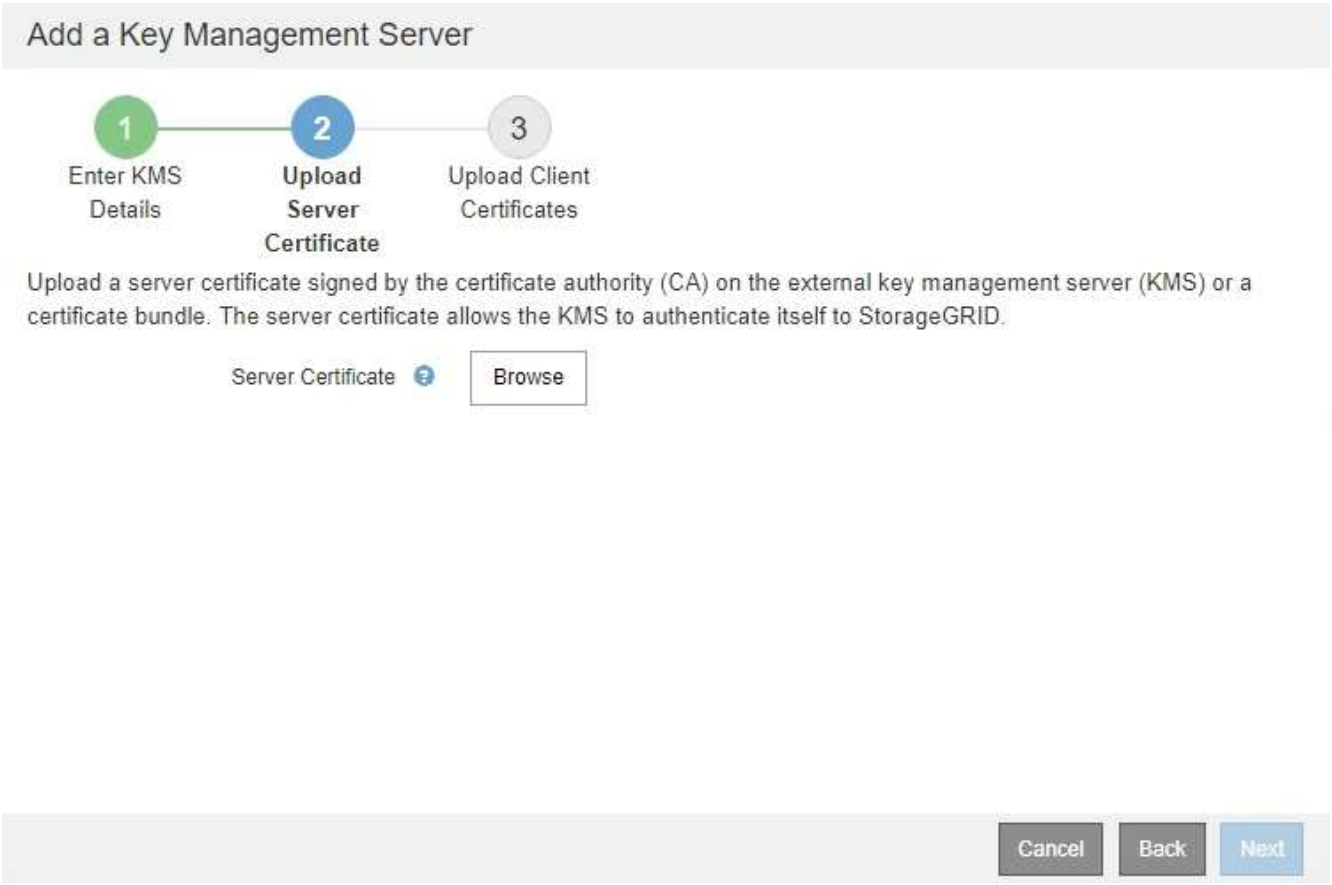
   Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.

Schritt: Serverzertifikat Hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Serverzertifikat (oder das Zertifikatspaket) für den KMS hoch. Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

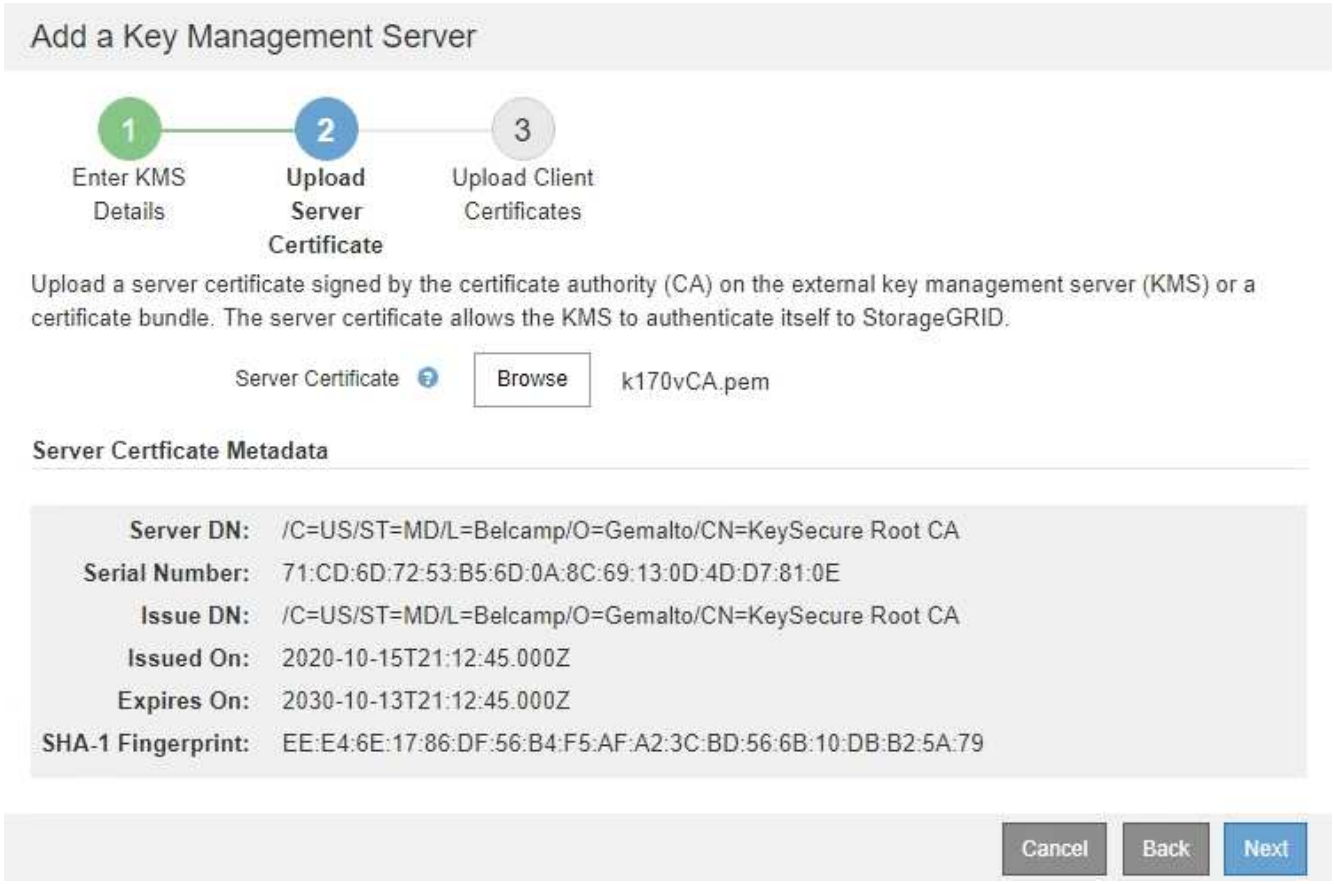
Schritte

1. Navigieren Sie ab **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatpakets.



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**.

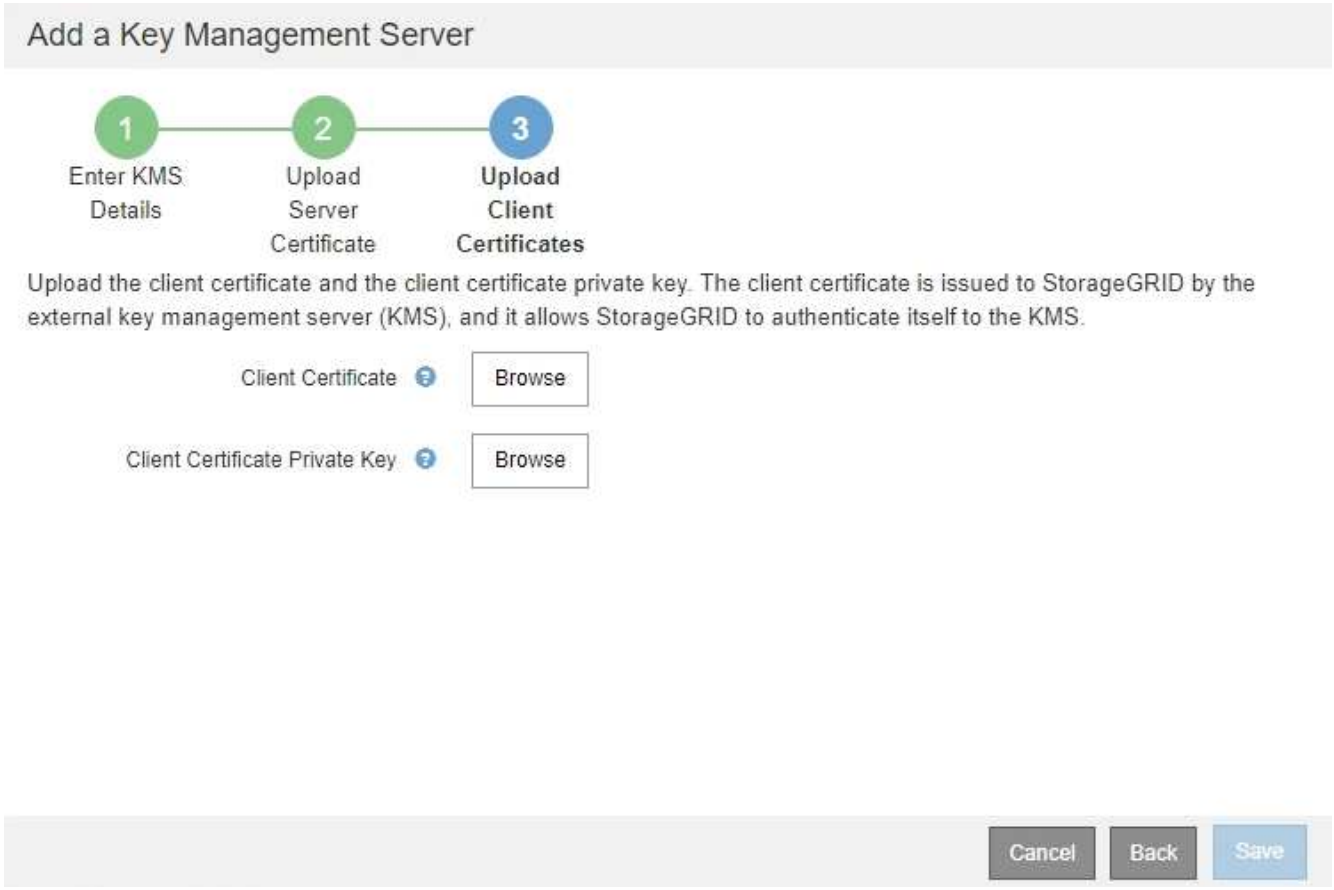
   Schritt 3 (Upload Client Certificates) des Assistenten Add a Key Management Server wird angezeigt.

Schritt 3: Laden Sie Client-Zertifikate Hoch

In Schritt 3 (Upload Client Certificates) des Assistenten Add a Key Management Server laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Schritte

1. Ab **Schritt 3 (Upload Client Certificates)** navigieren Sie zum Speicherort des Clientzertifikats.

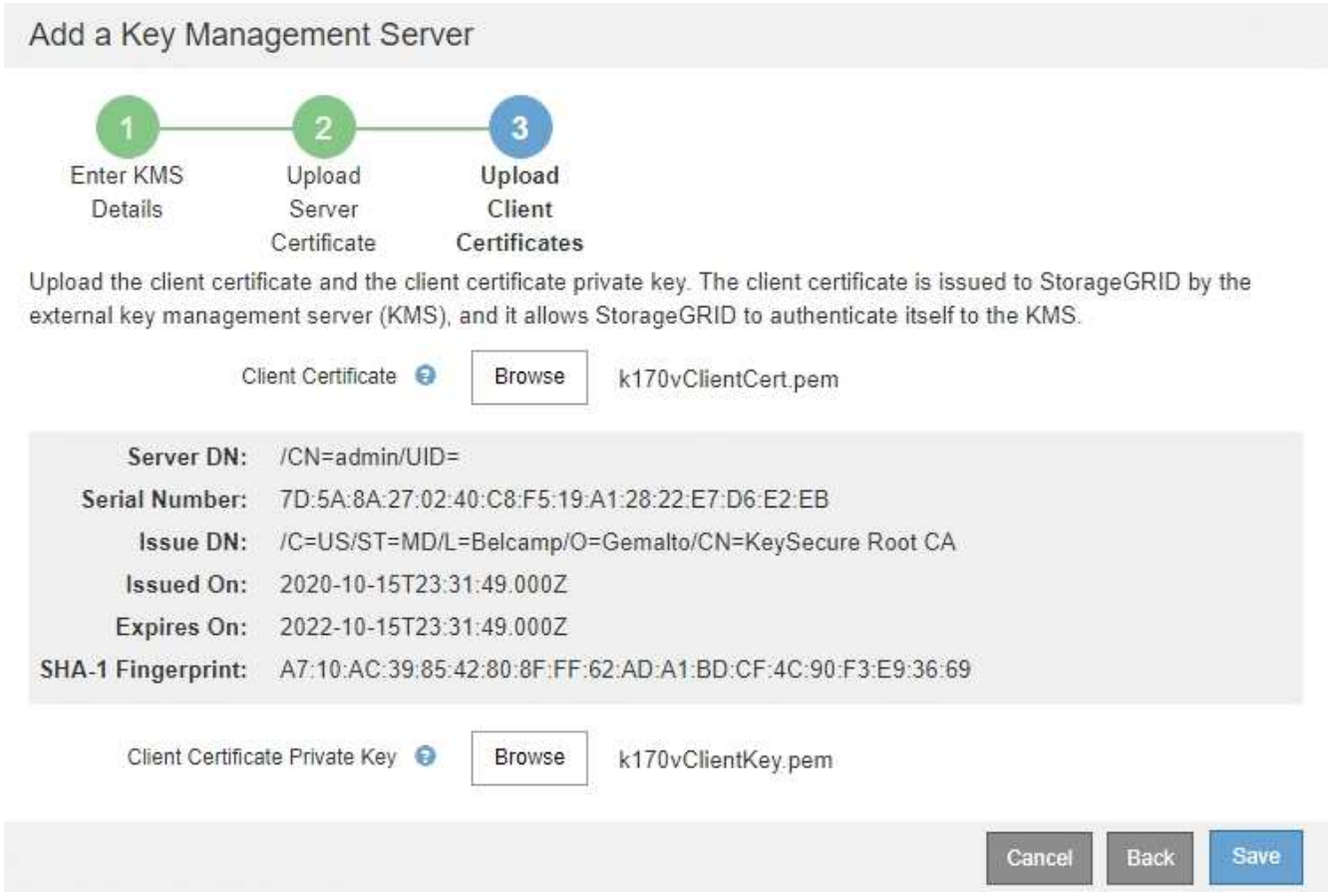


2. Laden Sie die Clientzertifikatdatei hoch.

   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.

   Die Metadaten für das Clientzertifikat und der private Schlüssel für das Clientzertifikat werden angezeigt.



5. Wählen Sie **Speichern**.

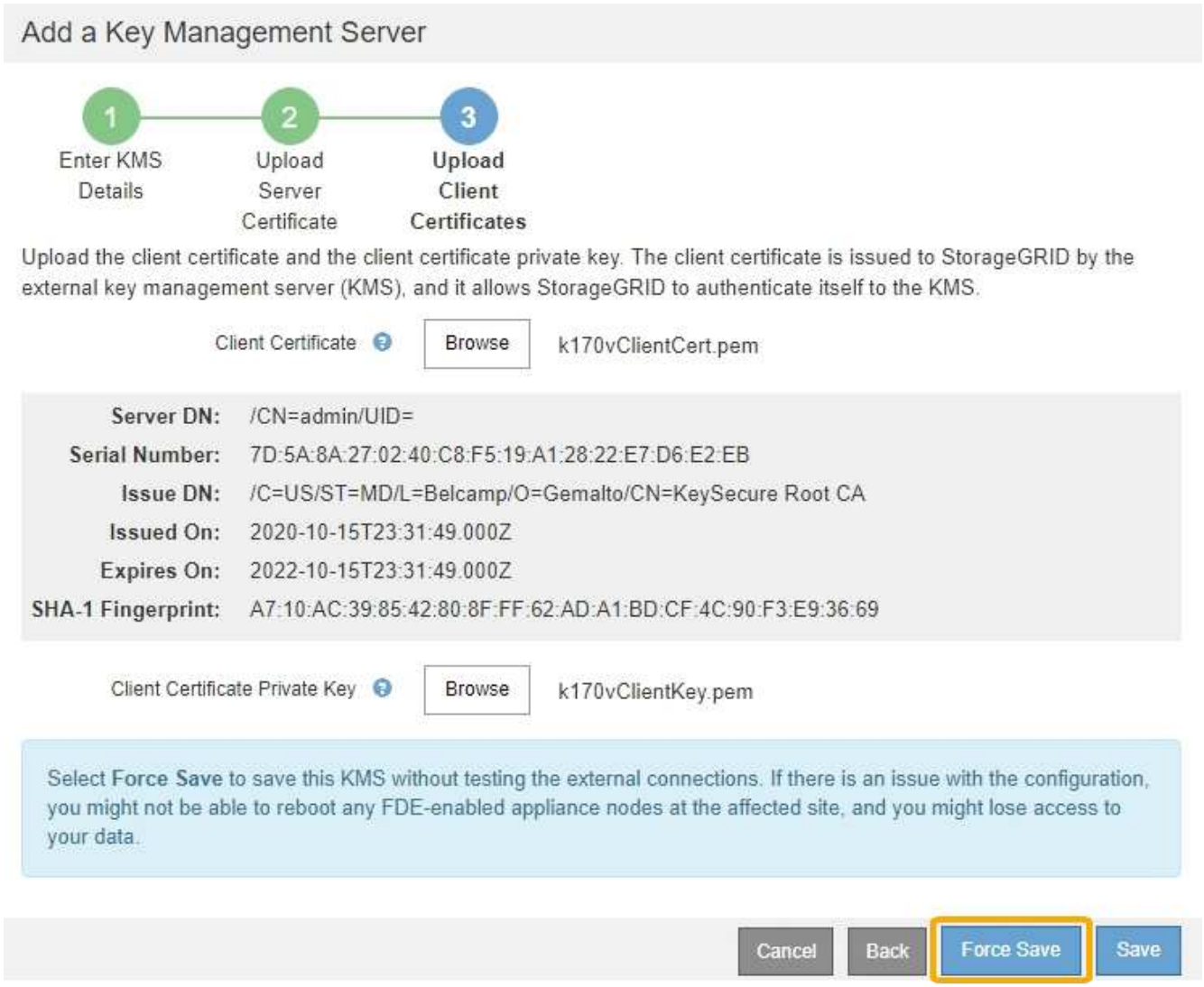
   Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und den Appliance-Nodes werden getestet. Wenn alle Verbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

   > 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 beim Auswählen von **Speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK** aus.

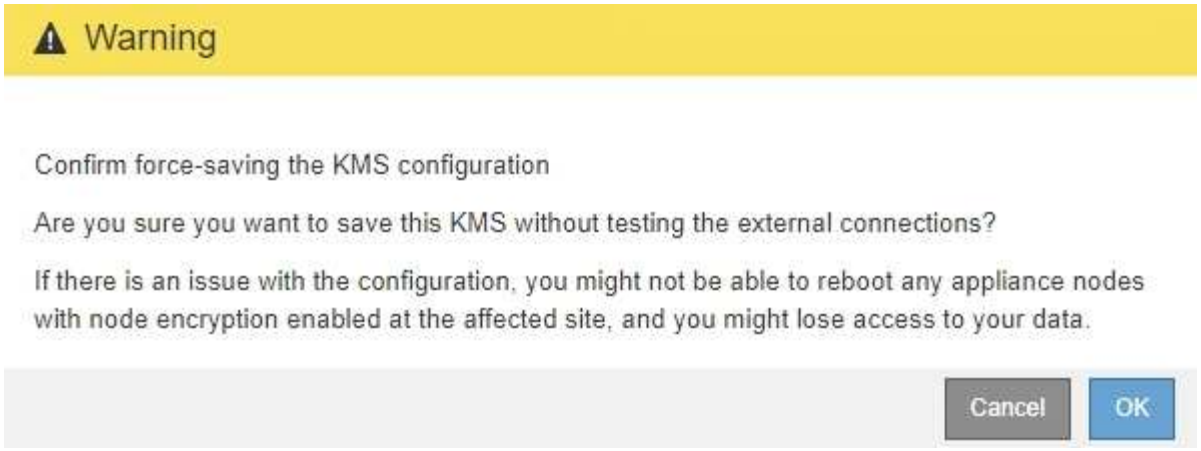
   Beispiel: Wenn ein Verbindungstest fehlgeschlagen ist, können Sie einen Fehler bei unbearbeitbarer Einheit mit 422: Nicht verarbeitbarer Einheit erhalten.

7. Wenn Sie die aktuelle Konfiguration speichern müssen, ohne die externe Verbindung zu testen, wählen Sie **Erzwingen Sie Speichern**.



Durch die Auswahl von **Erzwingen speichern** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

8. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.



Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

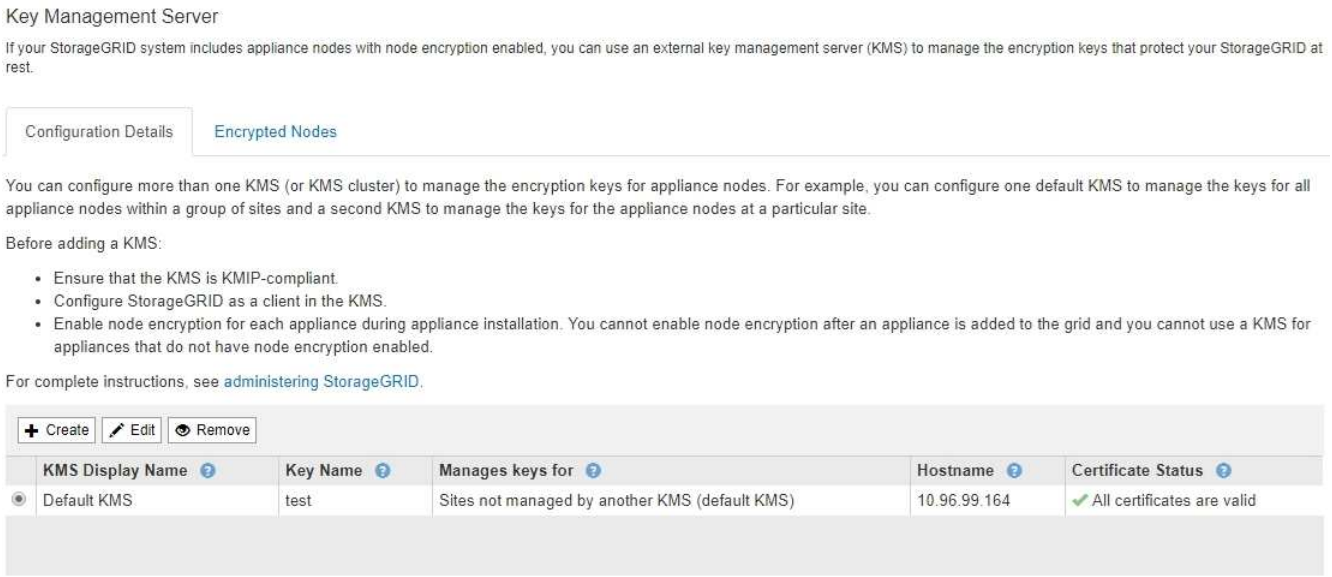
Anzeigen von KMS-Details

Sie können Informationen zu jedem Schlüsselverwaltungsserver (KMS) in Ihrem StorageGRID-System anzeigen, einschließlich des aktuellen Status des Servers und der Clientzertifikate.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.



2. Überprüfen Sie die Informationen in der Tabelle für jeden KMS.

Feld	Beschreibung
KMS-Anzeigename	Der beschreibende Name des KMS.

Feld	Beschreibung
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).**
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS. Wenn ein Cluster von zwei Schlüsselverwaltungsservern vorhanden ist, werden der vollständig qualifizierte Domänenname oder die IP-Adresse beider Server aufgelistet. Wenn mehr als zwei Schlüsselverwaltungsserver in einem Cluster vorhanden sind, wird der vollständig qualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet. Beispiel: `10.10.10.10 and 10.10.10.11` Oder `10.10.10.10 and 2 others`. Um alle Hostnamen in einem Cluster anzuzeigen, wählen Sie einen KMS aus, und wählen Sie dann **Bearbeiten** aus.
Zertifikatsstatus	Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt. **Hinweis:** möglicherweise dauert StorageGRID bis zu 30 Minuten, um Updates zum Zertifikatsstatus zu erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen.

3. Wenn der Zertifikatsstatus unbekannt ist, warten Sie bis zu 30 Minuten, und aktualisieren Sie dann Ihren Webbrowser.

> 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.

4. Wenn in der Spalte „Zertifikatsstatus“ angegeben ist, dass ein Zertifikat abgelaufen ist oder sich dem

Ablauf nähert, beheben Sie das Problem so schnell wie möglich.

Lesen Sie die empfohlenen Aktionen für den Ablauf des **KMS CA-Zertifikats**, **KMS-Clientzertifikats-Ablauf** und **KMS-Serverzertifikate-Ablauf**-Alarme in den Anweisungen zur Überwachung und Fehlerbehebung von StorageGRID.

> ⓘ Sie müssen Probleme mit dem Zertifikat so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

Verwandte Informationen

"Monitor Fehlerbehebung"

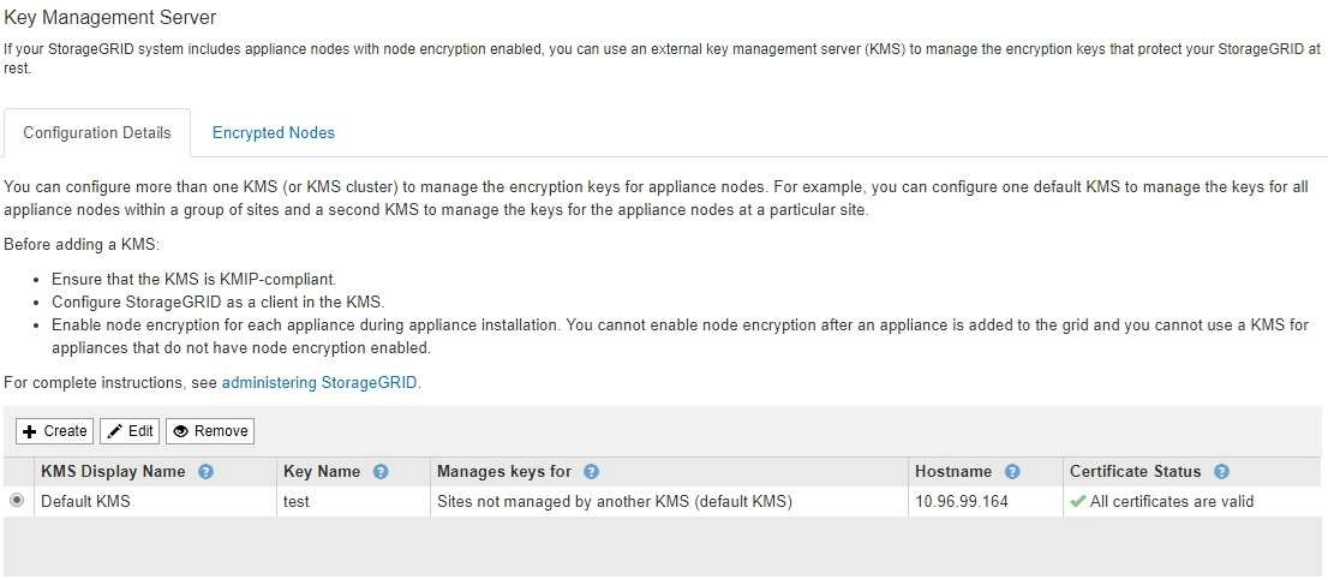
Anzeigen verschlüsselter Nodes

Sie können Informationen zu den Appliance-Knoten in Ihrem StorageGRID-System anzeigen, bei denen die Einstellung **Node-Verschlüsselung** aktiviert ist.

Schritte

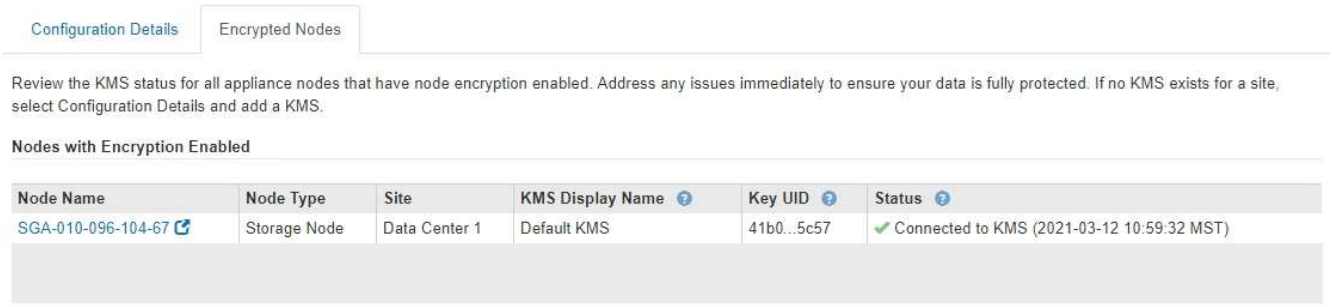
1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   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, bei denen 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-Anzeigename	Der beschreibende Name des für den Knoten verwendeten KMS. Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um einen 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. Wenn Sie eine vollständige Schlüssel-UID anzeigen möchten, bewegen Sie den Mauszeiger 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
- KMS ist nicht konfiguriert Siehe die empfohlenen Aktionen für diese Warnmeldungen in den Anweisungen für Monitoring und Fehlerbehebung StorageGRID.

> Sämtliche Probleme müssen sofort behoben werden, um einen vollständigen Schutz Ihrer Daten zu gewährleisten.

Verwandte Informationen

"Monitor Fehlerbehebung"

Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, z. B. wenn ein Zertifikat kurz vor dem Ablauf steht.

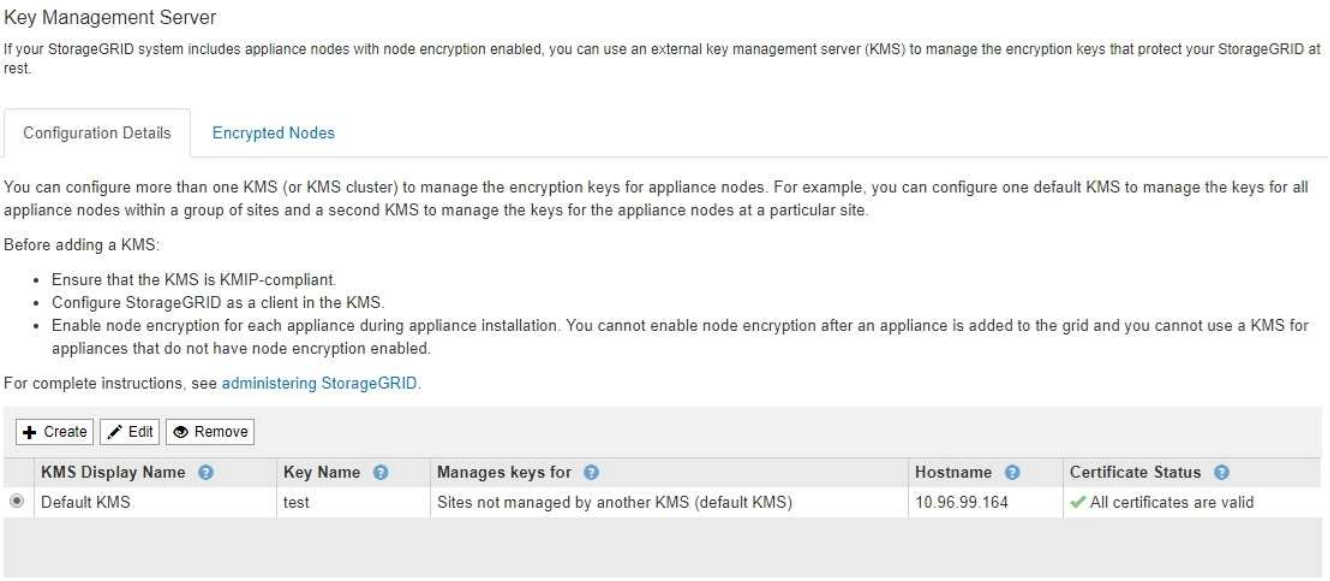
Was Sie benötigen

- Sie müssen den geprüft haben "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Wenn Sie planen, die für einen KMS ausgewählte Site zu aktualisieren, müssen Sie den geprüft haben "Überlegungen für das Ändern des KMS für einen Standort".
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver an.



2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **Bearbeiten**.
3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details eingeben)** des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers.

Feld	Beschreibung
KMS-Anzeigename	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. In seltenen Fällen müssen Sie nur den Schlüsselnamen bearbeiten. Sie müssen beispielsweise den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder alle Versionen des vorherigen Schlüssels in die Versionsgeschichte des neuen Alias kopiert wurden. Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Für StorageGRID müssen alle zuvor verwendeten Schlüsselversionen (sowie zukünftige Versionen) vom KMS mit demselben Schlüsselalias zugänglich sein. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln. "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"

Feld	Beschreibung
Verwaltet Schlüssel für	Wenn Sie einen Site-spezifischen KMS bearbeiten und noch keinen Standard-KMS haben, wählen Sie optional **Sites, die nicht von einem anderen KMS (Standard KMS)** verwaltet werden. Diese Auswahl konvertiert einen standortspezifischen KMS in den Standard-KMS, der für alle Sites gilt, die keinen dedizierten KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden. **Hinweis:** Wenn Sie einen Site-spezifischen KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie den Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.
Port	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das SAN-Feld des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie das Pluszeichen aus ➕ Um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

   Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüssel-Management-Server bearbeiten“ wird angezeigt.

6. Wenn Sie das Serverzertifikat ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neue Datei hoch.
7. Wählen Sie **Weiter**.

   Schritt 3 (Upload Client Certificates) des Assistenten Edit a Key Management Server 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 **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**.

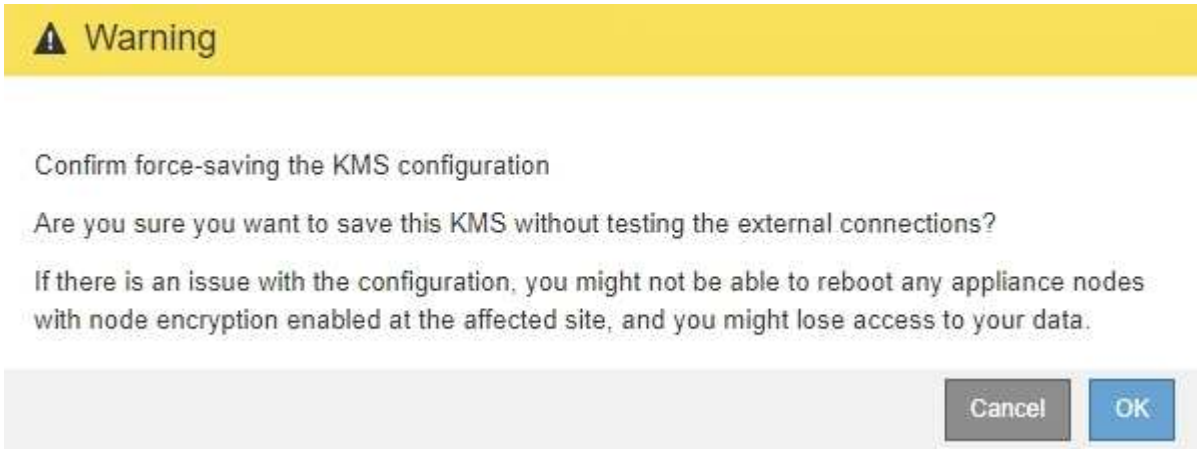
    Sie können beispielsweise einen Fehler bei der nicht verarbeitbaren Einheit von 422 erhalten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

11. Wenn Sie die aktuelle Konfiguration speichern müssen, bevor Sie die Verbindungsfehler beheben, wählen Sie **Erzwingen Sie Speichern**.

> Durch die Auswahl von **Erzwingen speichern** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch 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.

Was Sie benötigen

- Sie müssen den geprüft haben "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

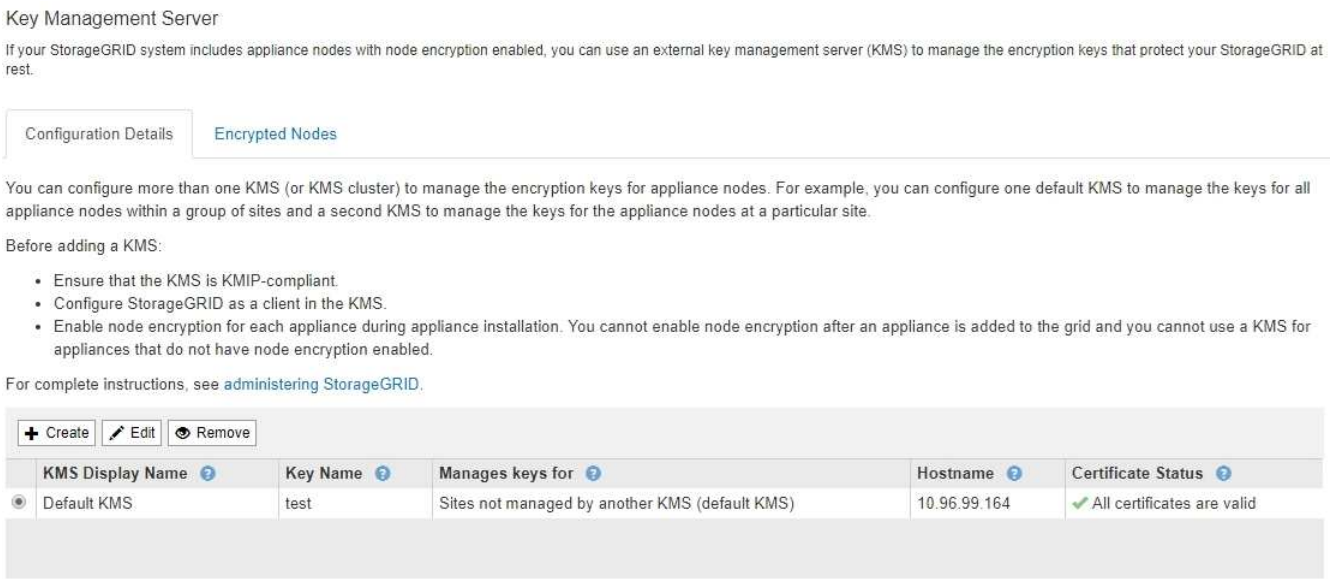
In diesen Fällen können Sie einen KMS entfernen:

- 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.

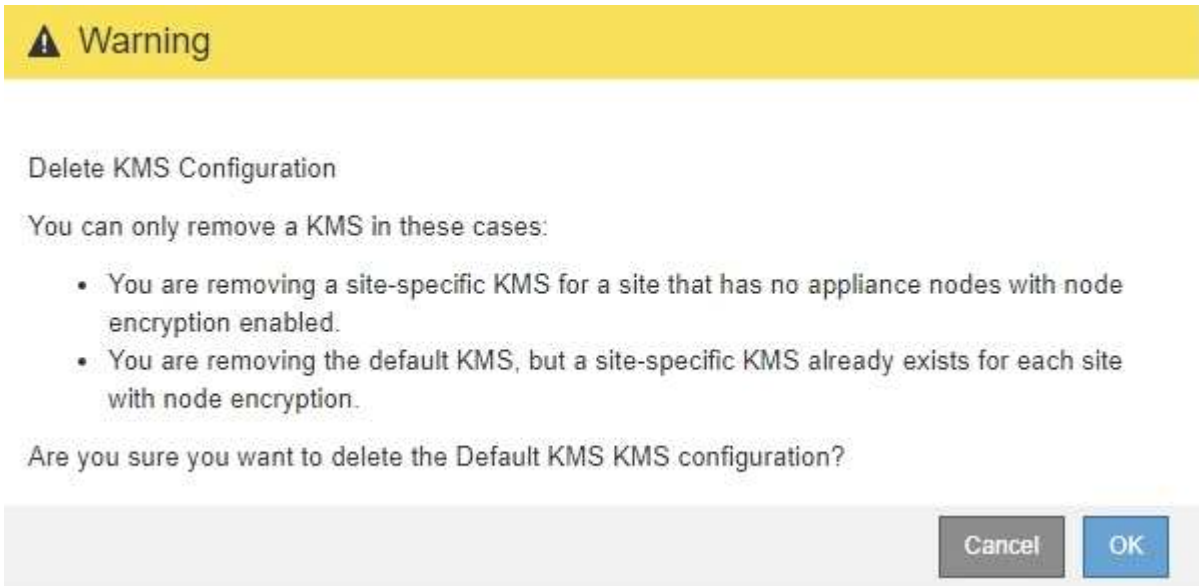
Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver an.



2. Wählen Sie das Optionsfeld für den KMS, den Sie entfernen möchten, und wählen Sie **Entfernen**.
3. Prüfen Sie die Überlegungen im Warndialogfeld.



4. Wählen Sie **OK**.

   Die KMS-Konfiguration wurde entfernt.

Management von Mandanten

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift-Clients verwenden, um Objekte zu speichern und abzurufen, die Storage-Nutzung

zu überwachen und die Aktionen zu managen, die Clients mit Ihrem StorageGRID System durchführen können.

Was Mandantenkonten sind

Mandantenkonten ermöglichen Client-Applikationen, die die Simple Storage Service (S3) REST-API oder die Swift REST API verwenden, um Objekte auf StorageGRID zu speichern und abzurufen.

Jedes Mandantenkonto unterstützt die Verwendung eines einzelnen Protokolls, das Sie beim Erstellen des Kontos angeben. Zum Speichern und Abrufen von Objekten in einem StorageGRID System mit beiden Protokollen müssen Sie zwei Mandantenkonten erstellen: Eine für S3 Buckets und Objekte, eine für Swift Container und Objekte. Jedes Mandantenkonto hat seine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets oder Container und Objekte.

Optional können Sie zusätzliche Mandantenkonten erstellen, wenn Sie die auf Ihrem System gespeicherten Objekte durch verschiedene Einheiten trennen möchten. Beispielsweise können Sie in einem der folgenden Anwendungsfälle mehrere Mandantenkonten einrichten:

- **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 mithilfe von S3-Buckets und Bucket-Richtlinien Objekte zwischen den Abteilungen eines Unternehmens trennen. Sie müssen keine Mandantenkonten verwenden. Weitere Informationen finden Sie in den Anweisungen zur Implementierung von S3-Client-Applikationen.

- **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.

Erstellen und Konfigurieren von Mandantenkonten

Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Zeigt den Namen des Mandantenkontos an.
- Welches Client-Protokoll wird vom Mandantenkonto verwendet (S3 oder Swift).
- Bei S3-Mandantenkonten: Unabhängig davon, ob das Mandantenkonto die Berechtigung hat, Plattform-Services mit S3 Buckets zu verwenden. Wenn Sie Mandantenkonten für die Nutzung von Plattformdiensten zulassen, müssen Sie sicherstellen, dass das Grid für seine Nutzung konfiguriert ist. Siehe „`MAnaging Platform Services`“.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte verfügbar sind. Wenn das Kontingent überschritten wird, kann der Mandant keine neuen Objekte erstellen.

  > Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.

- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.

- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Nachdem ein Mandantenkonto erstellt wurde, können Sie die folgenden Aufgaben durchführen:

- **Plattformdienste für das Grid verwalten**: Wenn Sie Plattformdienste für Mandantenkonten aktivieren, sollten Sie wissen, wie Plattform-Services-Nachrichten bereitgestellt werden und welche Netzwerkanforderungen die Verwendung von Plattformservices für Ihre StorageGRID-Bereitstellung stellen.
- **Überwachen der Storage-Nutzung eines Mandantenkontos**: Nachdem Mandanten ihre Konten verwenden, können Sie mithilfe von Grid Manager überwachen, wie viel Storage die einzelnen Mandanten verbrauchen.

  Wenn Sie Quoten für Mieter festgelegt haben, können Sie die Warnung **Tenant Quotenverbrauch hoch** aktivieren, um festzustellen, ob Mieter ihre Quoten verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Weitere Informationen finden Sie unter Alerts Referenz in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

- **Client-Vorgänge konfigurieren**: Sie können konfigurieren, wenn einige Arten von Client-Operationen verboten sind.

Konfigurieren von S3-Mandanten

Nachdem ein S3-Mandantenkonto erstellt wurde, können Mandantenbenutzer auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Verwalten von S3-Zugriffsschlüsseln
- Erstellen und Managen von S3 Buckets
- Monitoring der Storage-Auslastung
- Verwenden von Plattform-Services (falls aktiviert)

> Mandantenbenutzer von S3 können mit Mandanten-Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen. Sie müssen jedoch eine S3-Client-Applikation verwenden, um Objekte aufzunehmen und zu managen.

Konfiguration von Swift Mandanten

Nach der Erstellung eines Swift-Mandantenkontos kann der Root-Benutzer des Mandanten auf den Mandanten Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- 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 den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht 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.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Erstellen eines Mandantenkontos

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Storage in Ihrem StorageGRID-System zu kontrollieren.

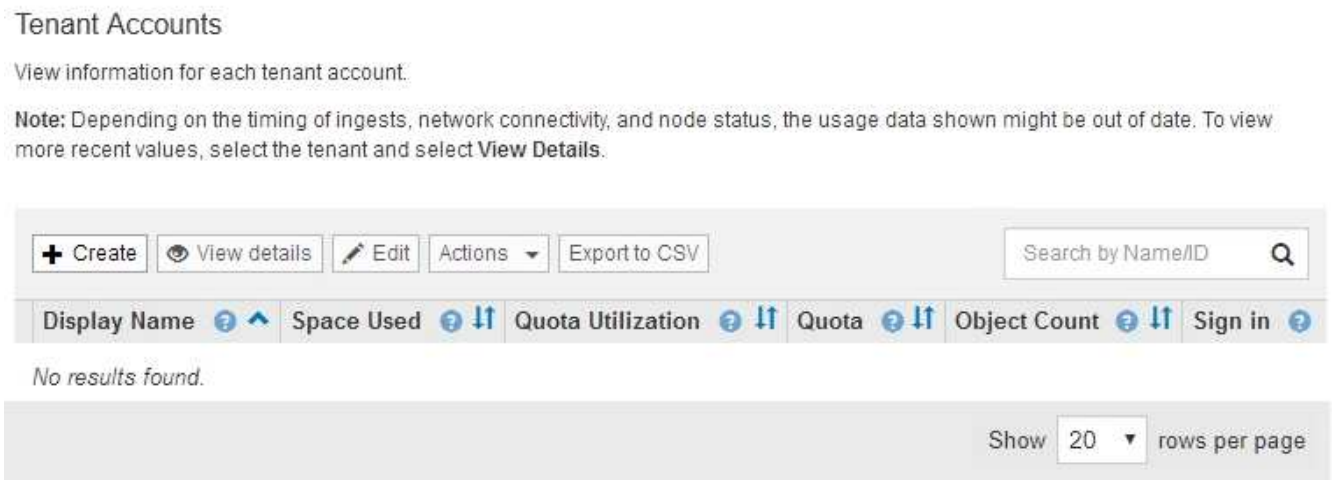
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Mieter**.

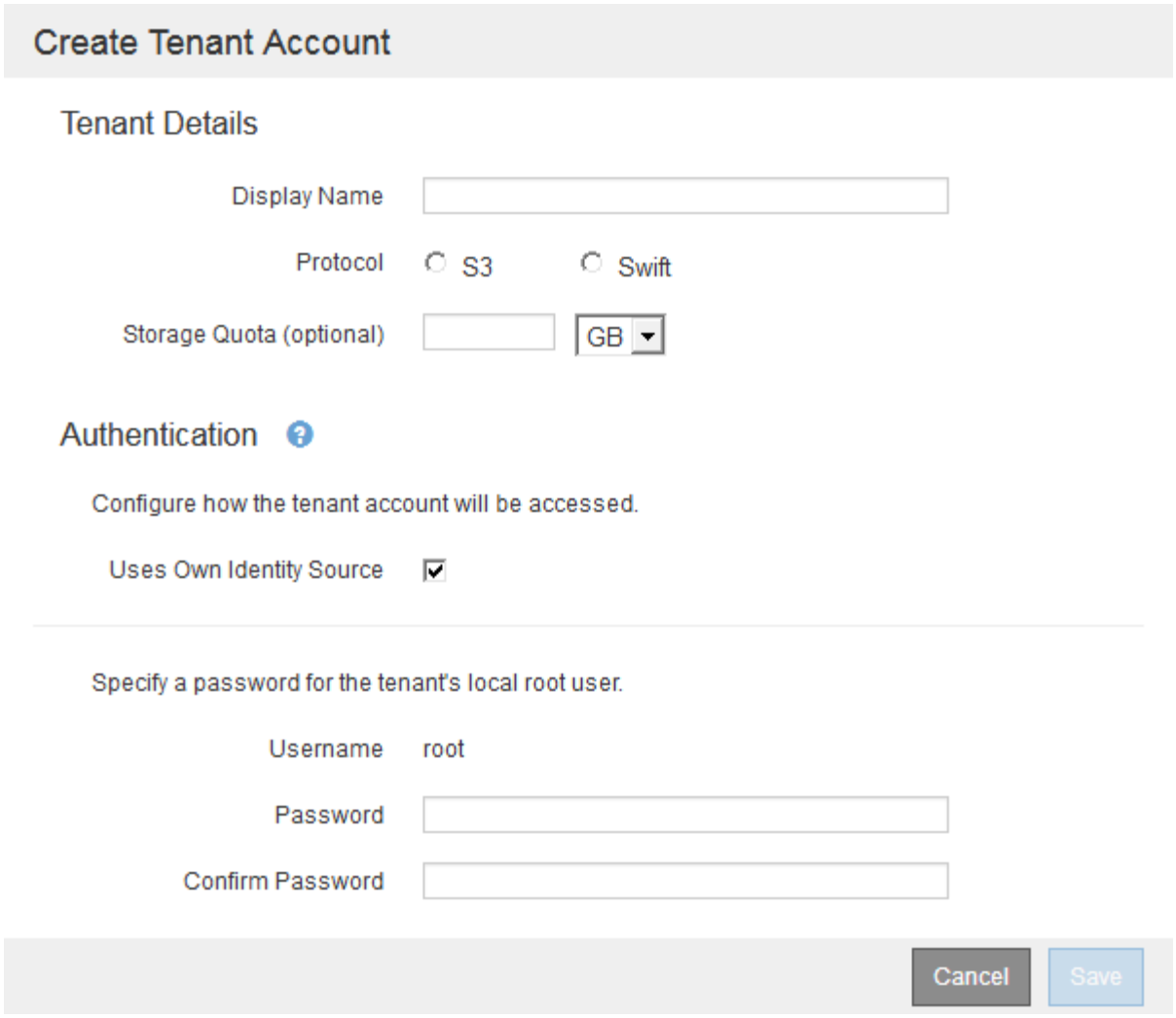
   Die Seite „Mandantenkonten“ wird angezeigt und enthält alle vorhandenen Mandantenkonten.



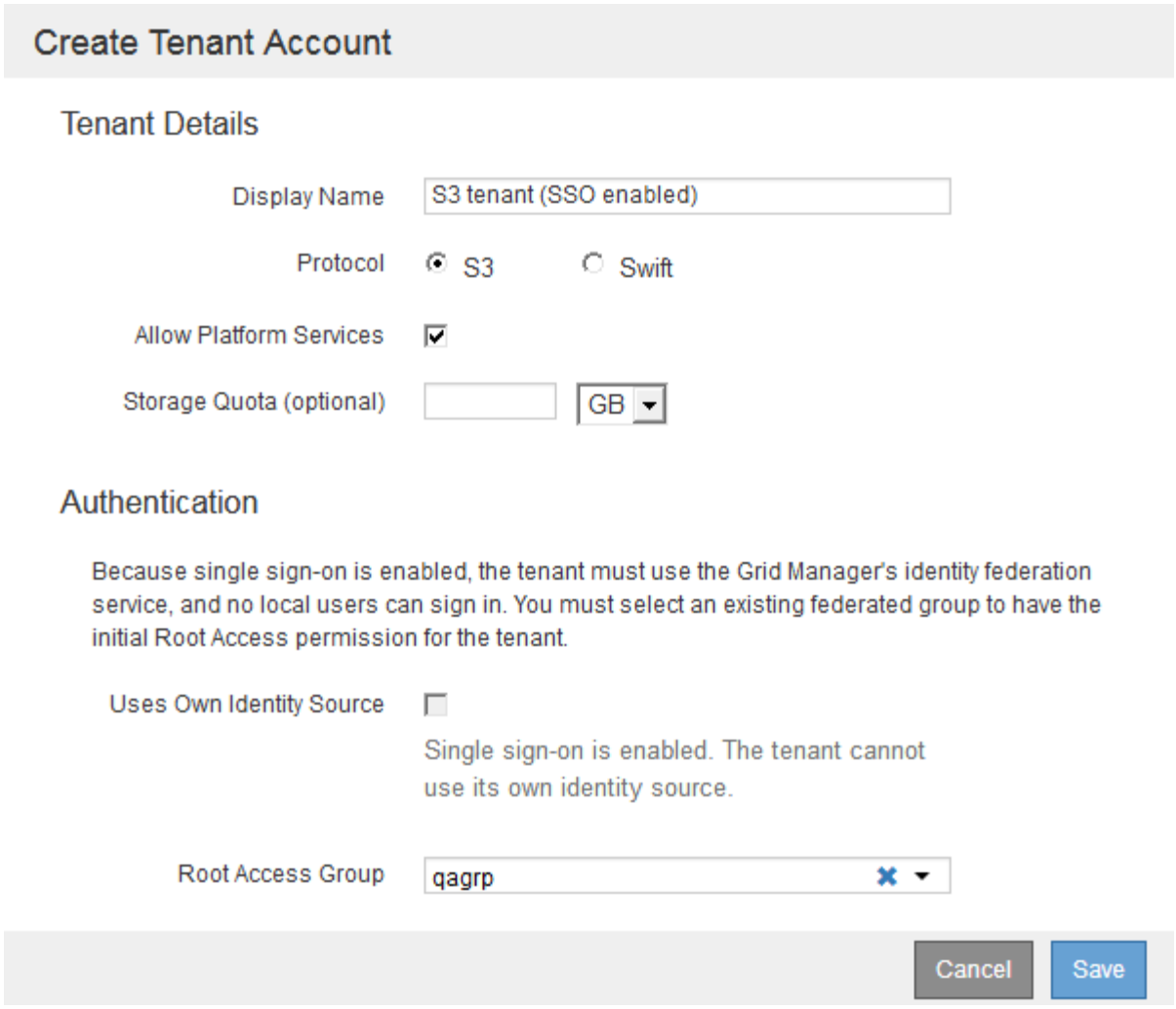
2. Wählen Sie **Erstellen**.

   Die Seite Mandantenkonto erstellen wird angezeigt. Die auf der Seite enthaltenen Felder hängen davon ab, ob Single Sign-On (SSO) für das StorageGRID-System aktiviert wurde.

   - Wenn SSO nicht verwendet wird, sieht die Seite Mandantenkonto erstellen so aus.



◦ Wenn SSO aktiviert ist, sieht die Seite Mandantenkonto erstellen so aus.



Verwandte Informationen

"Identitätsföderation verwenden"

"Konfigurieren der Single Sign-On-Konfiguration"

Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet

Wenn Sie ein Mandantenkonto erstellen, geben Sie einen Namen, ein Client-Protokoll und optional ein Storage-Kontingent an. Wenn StorageGRID keine Single Sign On (SSO) verwendet, müssen Sie außerdem angeben, ob das Mandantenkonto seine eigene Identitätsquelle verwendet und das ursprüngliche Passwort für den lokalen Root-Benutzer des Mandanten konfiguriert.

Über diese Aufgabe

Wenn das Mandantenkonto die Identitätsquelle verwendet, die für den Grid Manager konfiguriert wurde, und Sie eine föderierte Gruppe mit Root Access-Berechtigungen für das Mandantenkonto gewähren möchten, müssen Sie diese föderierte Gruppe in den Grid Manager importiert haben. Sie müssen dieser Admin-Gruppe keine Grid Manager-Berechtigungen zuweisen. Siehe Anweisungen für "Verwalten von Admin-Gruppen".

Schritte

1. Geben Sie im Textfeld **Anzeigename** einen Anzeigenamen für dieses Mandantenkonto ein.

Anzeigenamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.

2. Wählen Sie das Client-Protokoll aus, das von diesem Mandantenkonto verwendet wird, entweder **S3** oder **Swift**.
3. Aktivieren Sie für S3-Mandantenkonten das Kontrollkästchen **Platform Services zulassen**, es sei denn, dass dieser Mandant Plattformdienste für S3-Buckets verwendet.

   Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen. Vielleicht möchten Sie die Verwendung dieser Funktionen deaktivieren, um die Netzwerkbandbreite oder andere Ressourcen einzuschränken, die von einem Mandanten verbraucht werden. Siehe „`MAnaging Platform Services`“.

4. Geben Sie im Textfeld **Speicherkontingent** optional die maximale Anzahl von Gigabyte, Terabyte oder Petabytes ein, die Sie für die Objekte dieses Mandanten bereitstellen möchten. Wählen Sie dann die Einheiten aus der Dropdown-Liste aus.

   Lassen Sie dieses Feld leer, wenn dieser Mieter eine unbegrenzte Quote haben soll.

   > Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar. ILM-Kopien und Erasure Coding tragen nicht zum Umfang des verwendeten Kontingents bei. Wenn das Kontingent überschritten wird, kann das Mandantenkonto keine neuen Objekte erstellen.

   > Um die Storage-Nutzung jedes Mandantenkontos zu überwachen, wählen Sie **Nutzung**. Mandantenkonten können auch ihre eigene Storage-Auslastung von der Konsole im Mandantenmanager oder mit der Mandantenmanagement-API überwachen. Beachten Sie, dass die Storage-Nutzungswerte eines Mandanten möglicherweise nicht mehr aktuell sind, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

5. Wenn der Mandant seine eigenen Gruppen und Benutzer verwaltet, führen Sie diese Schritte aus.
   a. Aktivieren Sie das Kontrollkästchen * verwendet eigene Identitätsquelle* (Standard).

      > Wenn dieses Kontrollkästchen aktiviert ist und Sie einen Identitätsverbund für Mandanten und Benutzer verwenden möchten, muss der Mandant seine eigene Identitätsquelle konfigurieren. Siehe die Anweisungen zur Verwendung von Mandantenkonten.

   b. Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an.
6. Wenn der Mandant die für den Grid Manager konfigurierten Gruppen und Benutzer verwendet, führen Sie die folgenden Schritte aus.
   a. Deaktivieren Sie das Kontrollkästchen * verwendet eigene Identitätsquelle*.
   b. Führen Sie einen oder beide der folgenden Schritte aus:
      - Wählen Sie im Feld Root Access Group eine vorhandene föderierte Gruppe aus dem Grid Manager aus, die über die ursprüngliche Root Access-Berechtigung für den Mandanten verfügen soll.

        > Wenn Sie über ausreichende Berechtigungen verfügen, werden die vorhandenen föderierten Gruppen aus dem Grid Manager aufgelistet, wenn Sie auf das Feld klicken. Geben Sie andernfalls den eindeutigen Namen der Gruppe ein.

- Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an.

7. Klicken Sie Auf **Speichern**.

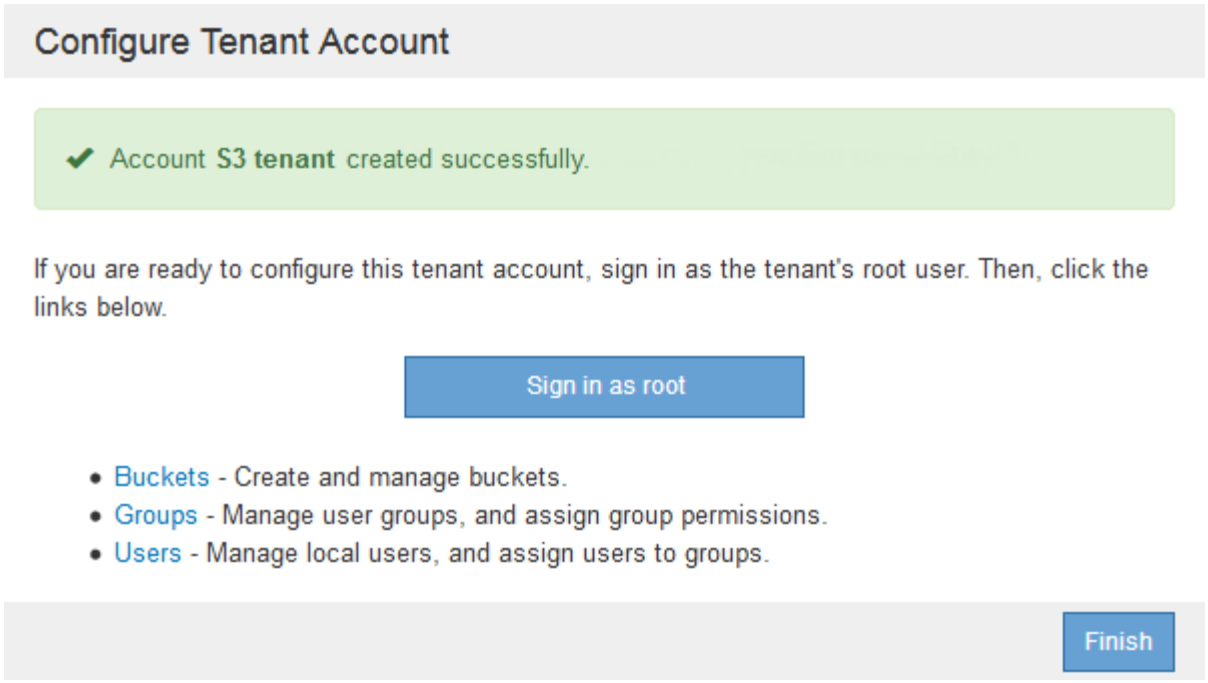
   Das Mandantenkonto wird erstellt.

8. Optional können Sie auf den neuen Mandanten zugreifen. Andernfalls fahren Sie mit dem Schritt für fort Später Zugriff auf den Mandanten.

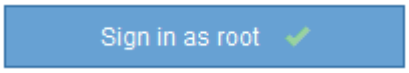
Ihr Unternehmen	Tun Sie das…
Zugriff auf den Grid Manager über einen eingeschränkten Port	Klicken Sie auf **eingeschränkt**, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. Die URL für den Tenant Manager weist folgendes Format auf: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens • *`port`* Ist der reine Mandantenport • *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten
Zugriff auf den Grid Manager auf Port 443, Sie haben jedoch kein Passwort für den lokalen Root-Benutzer festgelegt	Klicken Sie auf **Anmelden**, und geben Sie die Anmeldeinformationen für einen Benutzer in die Gruppe Stammzugriff ein.
Zugriff auf den Grid Manager auf Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	Fahren Sie mit dem nächsten Schritt fort melden Sie sich als Root an.

9. Melden Sie sich als Root beim Mandanten an:

   a. Klicken Sie im Dialogfeld Mandantenkonto konfigurieren auf die Schaltfläche **als root** anmelden.



Auf der Schaltfläche wird ein grünes Häkchen angezeigt, das angibt, dass Sie jetzt als Root-Benutzer beim Mandantenkonto angemeldet sind.



a. Klicken Sie auf die Links, um das Mandantenkonto zu konfigurieren.

   Jeder Link öffnet die entsprechende Seite im Tenant Manager. Zum Ausfüllen der Seite lesen Sie die Anweisungen zur Verwendung von Mandantenkonten.

b. Klicken Sie Auf **Fertig Stellen**.

10. um später auf den Mandanten zuzugreifen:

Sie verwenden…	Führen Sie eine dieser…
Port 443	• Wählen Sie im Grid Manager **Mieters** aus und klicken Sie rechts neben dem Mieternamen auf **Anmelden**. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *20-digit-account-id* Die eindeutige Account-ID des Mandanten

Sie verwenden…	Führen Sie eine dieser…
Ein eingeschränkter Port	• Wählen Sie im Grid Manager die Option **Miters** aus, und klicken Sie auf **eingeschränkt**. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *port* Ist der ausschließlich auf Mandanten beschränkte Port ◦ *20-digit-account-id* Die eindeutige Account-ID des Mandanten

Verwandte Informationen

"Zugriffskontrolle durch Firewalls"

"Management von Plattform-Services für S3-Mandantenkonten"

"Verwenden Sie ein Mandantenkonto"

Erstellen eines Mandantenkontos, wenn SSO aktiviert ist

Wenn Sie ein Mandantenkonto erstellen, geben Sie einen Namen, ein Client-Protokoll und optional ein Storage-Kontingent an. Wenn Single Sign-On (SSO) für StorageGRID aktiviert ist, geben Sie außerdem an, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren.

Schritte

1. Geben Sie im Textfeld **Anzeigename** einen Anzeigenamen für dieses Mandantenkonto ein.

   Anzeigenamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.

2. Wählen Sie das Client-Protokoll aus, das von diesem Mandantenkonto verwendet wird, entweder **S3** oder **Swift**.
3. Aktivieren Sie für S3-Mandantenkonten das Kontrollkästchen **Platform Services zulassen**, es sei denn, dass dieser Mandant Plattformdienste für S3-Buckets verwendet.

   Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen. Vielleicht möchten Sie die Verwendung dieser Funktionen deaktivieren, um die Netzwerkbandbreite oder andere Ressourcen einzuschränken, die von einem Mandanten verbraucht werden. Siehe „`MAnaging Platform Services`“.

4. Geben Sie im Textfeld **Speicherkontingent** optional die maximale Anzahl von Gigabyte, Terabyte oder Petabytes ein, die Sie für die Objekte dieses Mandanten bereitstellen möchten. Wählen Sie dann die Einheiten aus der Dropdown-Liste aus.

   Lassen Sie dieses Feld leer, wenn dieser Mieter eine unbegrenzte Quote haben soll.

Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar. ILM-Kopien und Erasure Coding tragen nicht zum Umfang des verwendeten Kontingents bei. Wenn das Kontingent überschritten wird, kann das Mandantenkonto keine neuen Objekte erstellen.

Um die Storage-Nutzung jedes Mandantenkontos zu überwachen, wählen Sie **Nutzung**. Mandantenkonten können auch ihre eigene Storage-Auslastung von der Konsole im Mandantenmanager oder mit der Mandantenmanagement-API überwachen. Beachten Sie, dass die Storage-Nutzungswerte eines Mandanten möglicherweise nicht mehr aktuell sind, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

5. Beachten Sie, dass das Kontrollkästchen * verwendet eigene Identitätsquelle* deaktiviert ist.

   Da SSO aktiviert ist, muss der Mandant die für den Grid Manager konfigurierte Identitätsquelle verwenden. Keine lokalen Benutzer können sich anmelden.

6. Wählen Sie im Feld **Root Access Group** eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root Access-Berechtigung für den Mandanten zu erhalten.

   Wenn Sie über ausreichende Berechtigungen verfügen, werden die vorhandenen föderierten Gruppen aus dem Grid Manager aufgelistet, wenn Sie auf das Feld klicken. Geben Sie andernfalls den eindeutigen Namen der Gruppe ein.

7. Klicken Sie Auf **Speichern**.

   Das Mandantenkonto wird erstellt. Die Seite Mandantenkonten wird angezeigt, und es enthält eine Zeile für den neuen Mandanten.

8. Wenn Sie ein Benutzer in der Root Access-Gruppe sind, klicken Sie optional auf den Link **Anmelden**, damit der neue Mandant sofort auf den Tenant Manager zugreift, wo Sie den Mandanten konfigurieren können. Geben Sie andernfalls die URL für den Link **Anmelden** an den Administrator des Mandantenkontos. (Die URL für einen Mandanten ist der vollständig qualifizierte Domain-Name oder die IP-Adresse eines Admin-Knotens, gefolgt von `/?accountId=`*`20-digit-account-id`*.)

   Wenn Sie auf **Anmelden** klicken, jedoch nicht zur Root Access-Gruppe für das Mandantenkonto gehören, wird eine Meldung angezeigt, die Zugriff verweigert.

Verwandte Informationen

"Konfigurieren der Single Sign-On-Konfiguration"

"Management von Plattform-Services für S3-Mandantenkonten"

"Verwenden Sie ein Mandantenkonto"

Ändern des Kennworts für den lokalen Root-Benutzer eines Mandanten

Möglicherweise müssen Sie das Passwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer aus dem Konto gesperrt ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

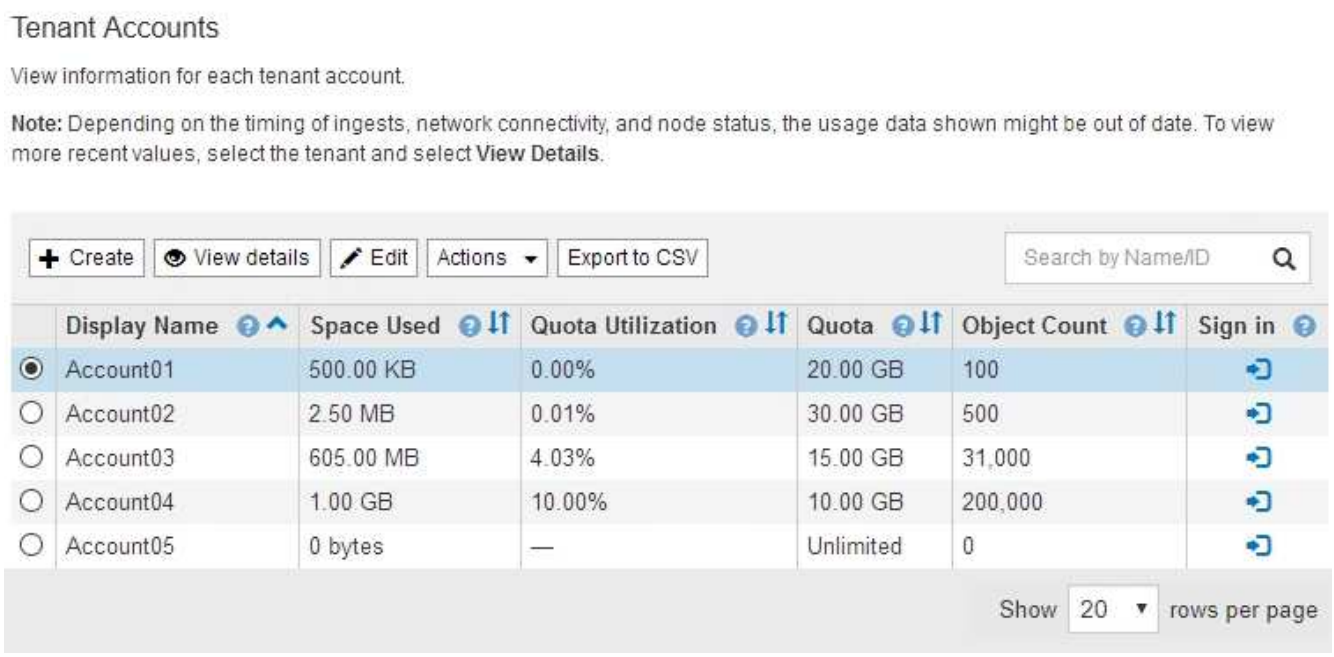
Über diese Aufgabe

Wenn Single Sign On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandantenkonto anmelden. Um Root-Benutzeraufgaben auszuführen, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **Mieter**.

   Die Seite „Mandantenkonten“ wird angezeigt und enthält alle vorhandenen Mandantenkonten.

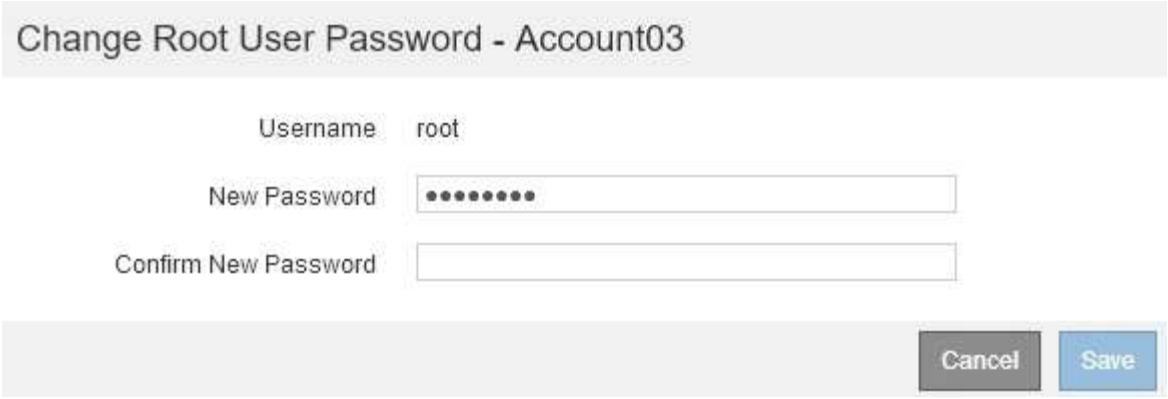


2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

   Die Schaltflächen „Details anzeigen“, „Bearbeiten“ und „Aktionen“ werden aktiviert.

3. Wählen Sie im Dropdown-Menü **Aktionen** die Option **Root Passwort ändern** aus.



4. Geben Sie das neue Kennwort für das Mandantenkonto ein.
5. Wählen Sie **Speichern**.

Verwandte Informationen

"Kontrolle des Administratorzugriffs auf StorageGRID"

Bearbeiten eines Mandantenkontos

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen zu ändern, die Einstellung für die Identitätsquelle zu ändern, Plattformservices zu ermöglichen oder zu verlassen oder ein Speicherkontingent einzugeben.

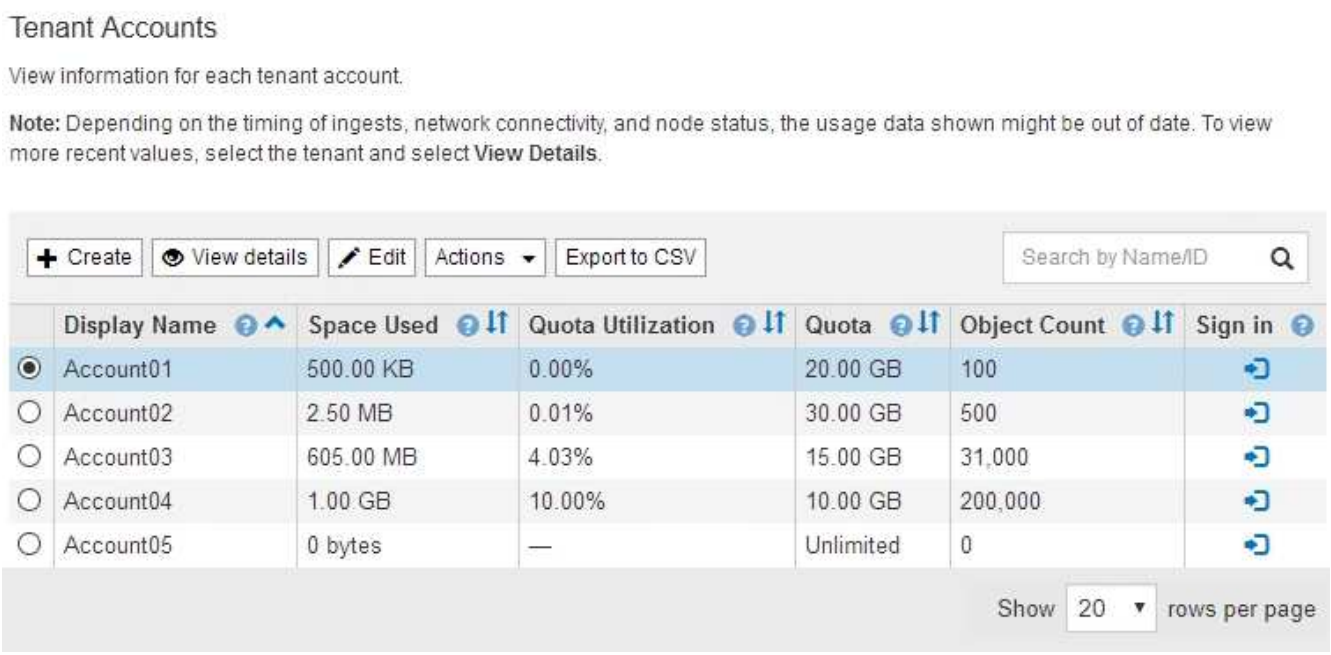
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Mieter**.

   Die Seite „Mandantenkonten“ wird angezeigt und enthält alle vorhandenen Mandantenkonten.

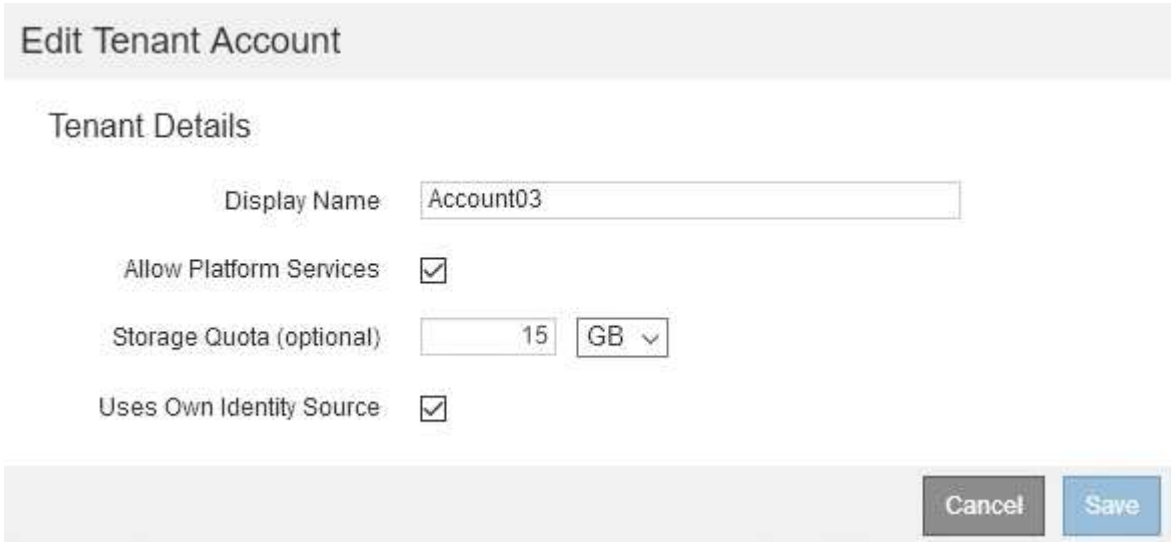


2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

3. Wählen Sie **Bearbeiten**.

   Die Seite Mandantenkonto bearbeiten wird angezeigt. Dieses Beispiel gilt für ein Raster, in dem keine SSO (Single Sign On) verwendet wird. Dieses Mandantenkonto hat keine eigene Identitätsquelle konfiguriert.



4. Ändern Sie die Werte für die Felder nach Bedarf.
   a. Ändern Sie den Anzeigenamen für dieses Mandantenkonto.
   b. Ändern Sie die Einstellung des Kontrollkästchen **Plattformdienste zulassen**, um festzustellen, ob das Mandantenkonto Plattformdienste für ihre S3-Buckets verwenden kann.

      Wenn Sie Plattform-Services für einen Mandanten deaktivieren, der sie bereits nutzt, funktionieren die Services, die er für seine S3-Buckets konfiguriert hat, nicht mehr. 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.

   c. Ändern Sie für **Speicherkontingent** die Anzahl der für die Objekte dieses Mandanten verfügbaren maximalen Gigabytes, Terabyte oder Petabytes, oder lassen Sie das Feld leer, wenn Sie möchten, dass dieser Mieter eine unbegrenzte Quote hat.

      Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar. ILM-Kopien und Erasure Coding tragen nicht zum Umfang des verwendeten Kontingents bei.

Um die Storage-Nutzung jedes Mandantenkontos zu überwachen, wählen Sie **Nutzung**. Mandantenkonten können auch ihre eigene Nutzung von der Konsole im Mandantenmanager oder mit der Mandantenmanagement-API überwachen. Beachten Sie, dass die Storage-Nutzungswerte eines Mandanten möglicherweise nicht mehr aktuell sind, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

d. Ändern Sie die Einstellung des Checkbox **uses own Identity Source**, um festzustellen, ob das Mandantenkonto eine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

Wenn das Kontrollkästchen * verwendet eigene Identitätsquelle*:

- Deaktiviert und überprüft, 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 deaktiviert ist, ist SSO für das StorageGRID System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.

5. Wählen Sie **Speichern**.

Verwandte Informationen

"Management von Plattform-Services für S3-Mandantenkonten"

"Verwenden Sie ein Mandantenkonto"

Löschen eines Mandantenkontos

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen alle Buckets (S3), Container (Swift) und Objekte, die mit dem Mandantenkonto verknüpft sind, entfernt haben.

Schritte

1. Wählen Sie **Mieter**.
2. Wählen Sie das Mandantenkonto aus, das gelöscht werden soll.

   Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

3. Wählen Sie im Dropdown-Menü **Aktionen** die Option **Entfernen** aus.
4. Wählen Sie **OK**.

Verwandte Informationen

"Kontrolle des Administratorzugriffs auf StorageGRID"

Management von Plattform-Services für S3-Mandantenkonten

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.

- "Um welche Plattform-Services geht es"
- "Networking und Ports für Plattform-Services"
- "Bereitstellung von Plattform-Services am Standort"
- "Plattform-Services zur Fehlerbehebung"

Um welche Plattform-Services geht es

Zu den Plattform-Services zählen die CloudMirror-Replizierung, Ereignisbenachrichtigungen und der Such-Integrationsservice.

Dank dieser Services können Mandanten die folgenden Funktionen mit ihren S3 Buckets nutzen:

- **CloudMirror Replikation**: Der StorageGRID CloudMirror Replikationsservice wird verwendet, um bestimmte Objekte von einem StorageGRID-Bucket auf ein bestimmtes externes Ziel zu spiegeln.

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

  > Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen**: Per Bucket-Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen über bestimmte Aktionen, die an Objekten ausgeführt werden, an einen bestimmten externen Amazon Simple Notification Service™ (SNS) zu senden.

  Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.

  > Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationsdienst**: Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

  Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.

Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperrmetadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Dank Plattform-Services können Mandanten externe Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für ihre Daten nutzen. Da sich der Zielstandort für Plattformservices in der Regel außerhalb Ihrer StorageGRID-Implementierung befindet, müssen Sie entscheiden, ob die Nutzung dieser Services durch Mandanten gestattet werden soll. Wenn Sie dies tun, müssen Sie die Verwendung von Plattform-Services aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen auch Ihr Netzwerk so konfigurieren, dass die von Mandanten generierten Plattformservices Meldungen ihre Ziele erreichen können.

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services müssen Sie die folgenden Empfehlungen beachten:

- 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.
- 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.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Konfigurieren von Speicher-Proxy-Einstellungen"

"Monitor Fehlerbehebung"

Networking und Ports für Plattform-Services

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 SNS-Meldungen (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 Storage Proxy-Einstellungen konfigurieren, damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einen Endpunkt im Internet.

Verwandte Informationen

"Konfigurieren von Speicher-Proxy-Einstellungen"

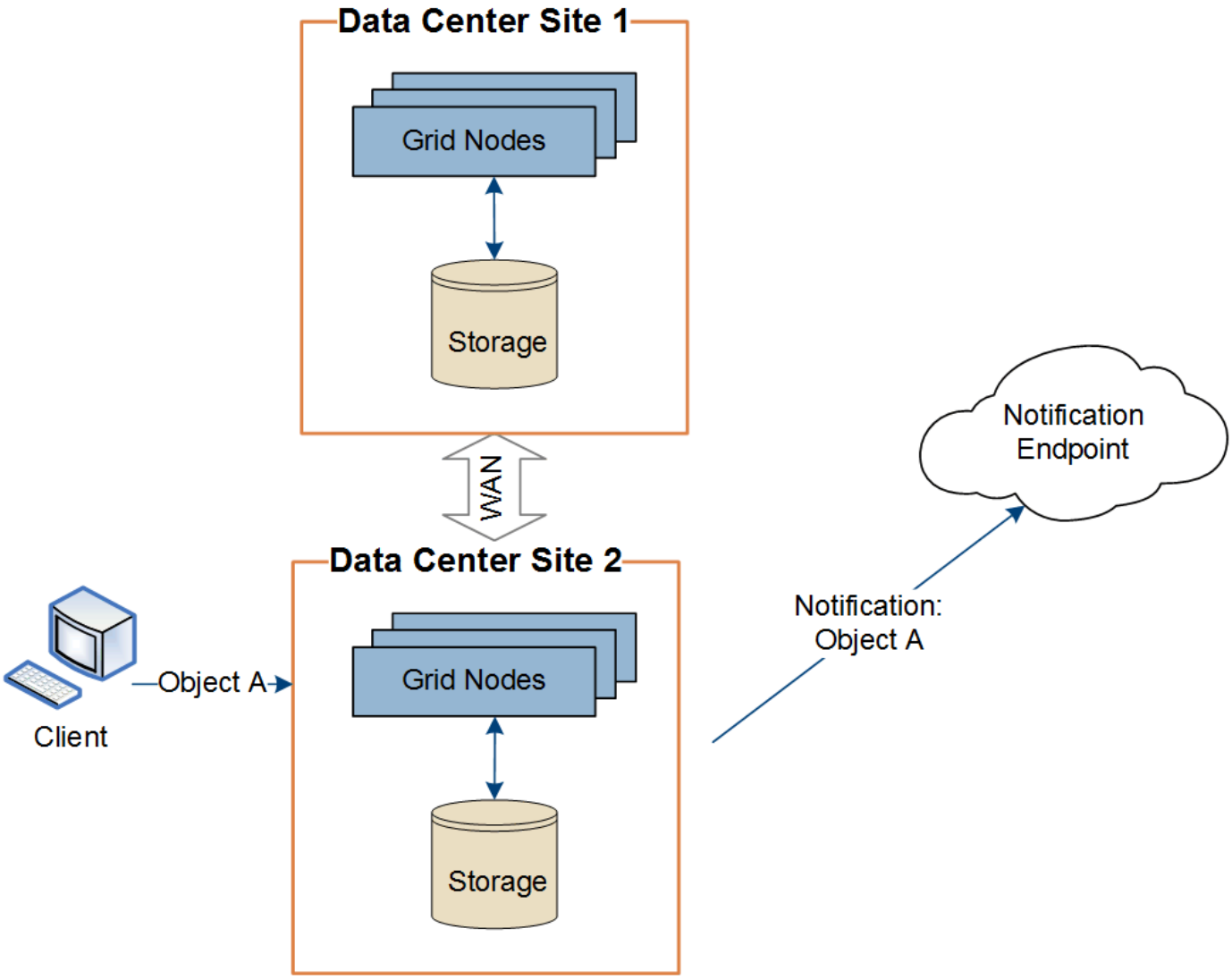
"Verwenden Sie ein Mandantenkonto"

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.

Plattform-Services zur Fehlerbehebung

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.

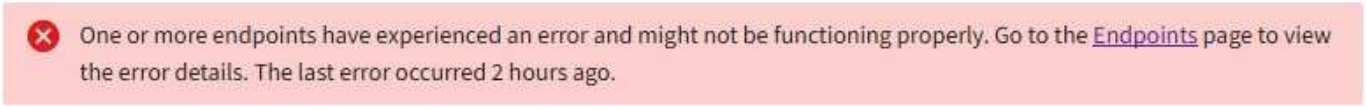
Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID System, ob der Endpunkt vorhanden ist und ob er mit den angegebenen Zugangsdaten erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

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.

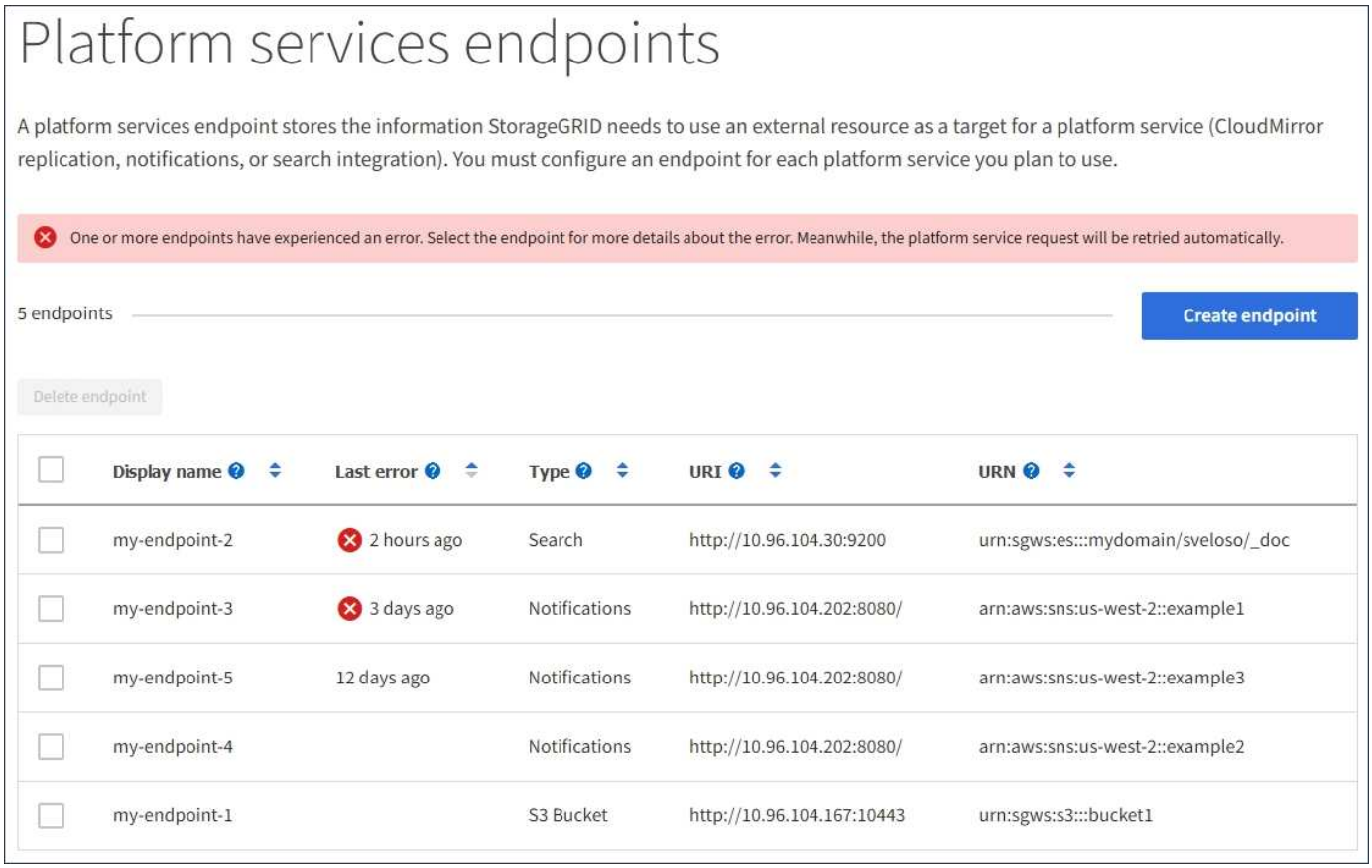
Die Erstellung von Endgeräten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn StorageGRID versucht, einen vorhandenen Endpunkt zu erreichen, tritt ein Fehler auf, wird im Mandantenmanager auf dem Dashboard eine Meldung angezeigt.



Mandantenbenutzer können auf der Seite Endpunkte die aktuellste Fehlermeldung für jeden Endpunkt lesen und herausfinden, wie lange der Fehler bereits aufgetreten ist. Die Spalte **Letzter Fehler** zeigt die aktuellste Fehlermeldung für jeden Endpunkt an und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das enthalten Das Symbol trat innerhalb der letzten 7 Tage auf.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** können eine LOGID in Klammern enthalten. Ein Grid-Administrator oder technischer Support kann diese ID verwenden, um ausführlichere Informationen über den Fehler im bycast.log zu finden.

Probleme im Zusammenhang mit Proxy-Servern

Wenn Sie einen Speicher-Proxy zwischen Speicherknoten und Plattform-Service-Endpunkten konfiguriert haben, treten möglicherweise Fehler auf, wenn Ihr Proxydienst keine Meldungen von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass die Nachrichten für den Plattformdienst nicht blockiert sind.

Ermitteln, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Endpoint-Fehler aufgetreten sind, wird im Dashboard im Tenant Manager eine Warnmeldung angezeigt. 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 Topology** Aus.
2. Wählen Sie ***site*** > ***Storage Node*** > **SSM** > **Services** aus.

Behebbare und nicht wiederherstellbare Endpunktfehler

Nach der Erstellung von Endpunkten können Fehler bei Plattformservice-Anfragen aus verschiedenen Gründen auftreten. Einige Fehler lassen sich durch Benutzereingriffe wiederherstellen. Beispielsweise können behebbare Fehler aus den folgenden Gründen auftreten:

- Die Anmeldedaten des Benutzers wurden gelöscht oder abgelaufen.
- Der Ziel-Bucket ist nicht vorhanden.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn bei StorageGRID ein wiederherstellbarer Fehler auftritt, wird die Serviceanfrage für die Plattform erneut versucht, bis sie erfolgreich ist.

Andere Fehler können nicht behoben werden. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn StorageGRID einen nicht behebbaren Endpunktfehler feststellt, wird der SMTT-Alarm (Total Events) im Grid Manager ausgelöst. So zeigen Sie den Alarm „Ereignisse insgesamt“ an:

1. Wählen Sie **Knoten**.
2. Wählen Sie ***site*** > ***GRID Node*** > **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. Klicken Sie auf **Ereignisanzahl zurücksetzen**.
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.

Plattform-Services-Meldungen 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 Plattformdienste-Meldungen aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der SMTT-Alarm (Total Events) im Grid Manager ausgelöst.

Langsamere Performance für Plattform-Service-Anfragen

StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.

Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.

CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanfragen schlagen fehl

So zeigen Sie die Ausfallrate der Anfrage für Plattformdienste an:

1. Wählen Sie **Knoten**.
2. Wählen Sie ***site*** > **Platform Services**.
3. Das Diagramm Fehlerrate anfordern anzeigen.

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 zur Fehlerbehebung bei Endpunkten für Plattformservices finden Sie in den Anweisungen für die Verwendung von Mandantenkonten.

"Verwenden Sie ein Mandantenkonto"

Verwandte Informationen

"Monitor Fehlerbehebung"

"Konfigurieren von Speicher-Proxy-Einstellungen"

Konfigurieren von S3- und Swift-Client-Verbindungen

Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie S3- und Swift-Mandanten Client-Applikationen mit Ihrem StorageGRID-System verbinden können, um Daten zu speichern und abzurufen. Es stehen verschiedene Optionen zur Verfügung, um verschiedene Anforderungen von Kunden und Mandanten zu erfüllen.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten

  Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- Storage-Nodes mit oder ohne externen Load Balancer

Auf dem StorageGRID-System können Sie optional die folgenden Funktionen konfigurieren:

- **Load Balancer Service**: Sie ermöglichen Clients die Verwendung des Load Balancer Service durch die Erstellung von Load Balancer Endpunkten für Client-Verbindungen. Beim Erstellen eines Load Balancer-Endpunkts geben Sie eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das Zertifikat, das für HTTPS-Verbindungen verwendet werden soll (falls zutreffend).
- **UnTrusted Client Network**: Sie können das Client-Netzwerk sicherer machen, indem Sie es als unvertrauenswürdig konfigurieren. Wenn das Client-Netzwerk nicht vertrauenswürdig ist, können Clients nur über Load Balancer-Endpunkte eine Verbindung herstellen.
- **Hochverfügbarkeitsgruppen**: Sie können eine HA-Gruppe von Gateway-Knoten oder Admin-Nodes erstellen, um eine aktiv-Backup-Konfiguration zu erstellen, oder Round-Robin-DNS oder einen Load Balancer eines Drittanbieters und mehrere HA-Gruppen verwenden, um eine aktiv/aktiv-Konfiguration zu erreichen. Client-Verbindungen werden mithilfe der virtuellen IP-Adressen der HA-Gruppen hergestellt.

Sie können auch die Verwendung von HTTP für Clients aktivieren, die eine Verbindung zu StorageGRID entweder direkt zu Storage-Nodes oder über den CLB-Dienst (veraltet) herstellen, und Sie können S3-API-Endpunktdomänennamen für S3-Clients konfigurieren.

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Client-Applikationen können sich mithilfe der IP-Adresse eines Grid-Node und der Port-Nummer eines Service auf diesem Node mit StorageGRID verbinden. Bei Konfiguration von Hochverfügbarkeitsgruppen (High Availability, HA) können Client-Applikationen eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe herstellen.

Über diese Aufgabe

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. Die Anleitung beschreibt das Auffinden dieser Informationen im Grid Manager, wenn die Endpunkte des Load Balancer und Gruppen für Hochverfügbarkeit (HA) bereits konfiguriert sind.

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
HA-Gruppe	CLB **Hinweis:** der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084 Swift-Standardports: • HTTPS:8083 • HTTP:8085
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
Gateway-Node	CLB **Hinweis:** der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node **Hinweis:** standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084 Swift-Standardports: • HTTPS:8083 • HTTP:8085

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: • HTTPS: 18082 • HTTP: 18084 Swift-Standardports: • HTTPS: 18083 • HTTP:18085

Beispiele

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen S3-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 192.0.2.5 lautet und die Portnummer eines S3 Load Balancer Endpunkts 10443 ist, kann ein S3-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.5:10443`

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.

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
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. Klicken Sie auf **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 **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen**.
   b. Notieren Sie in der Tabelle die virtuelle IP-Adresse der HA-Gruppe.
4. So finden Sie die Portnummer eines Load Balancer-Endpunkts:
   a. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**.

      Die Seite Load Balancer Endpoints wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte an.

   b. Wählen Sie einen Endpunkt aus, und klicken Sie auf **Endpunkt bearbeiten**.

      Das Fenster Endpunkt bearbeiten wird geöffnet und zeigt weitere Details zum Endpunkt an.

   c. Bestätigen Sie, dass der ausgewählte Endpunkt für die Verwendung mit dem korrekten Protokoll konfiguriert ist (S3 oder Swift), und klicken Sie dann auf **Abbrechen**.
   d. Notieren Sie sich die Portnummer für den Endpunkt, den Sie für eine Clientverbindung verwenden möchten.

> Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Alle anderen Ports werden sowohl an Gateway-Knoten als auch an Admin-Nodes konfiguriert.

Managen des Lastausgleichs

Die StorageGRID Lastausgleichfunktionen verarbeiten Aufnahme- und Abruf-Workloads von S3 und Swift Clients. Durch Verteilung der Workloads und Verbindungen auf mehrere Storage-Nodes maximiert der Lastausgleich die Geschwindigkeit und die Kapazität der Verbindungen.

Es gibt folgende Möglichkeiten für den Lastausgleich in Ihrem StorageGRID System:

- Verwenden Sie den Lastverteilungsservice, der auf Admin Nodes und Gateway Nodes installiert ist. Der Lastverteilungsservice bietet Layer 7 Load Balancing und führt TLS-Terminierung von Client-Anfragen durch, prüft die Anfragen und stellt neue sichere Verbindungen zu den Storage Nodes her. Dies ist der empfohlene Lastausgleichmechanismus.
- Verwenden Sie den Service Connection Load Balancer (CLB), der nur auf Gateway Nodes installiert ist. Der CLB-Service bietet Layer 4-Lastenausgleich und unterstützt Verbindungskosten.

Der CLB-Service ist veraltet.

- Integration eines Load Balancer eines Drittanbieters: Genaue Informationen erhalten Sie bei Ihrem NetApp Ansprechpartner.

Wie funktioniert der Lastausgleich? Load Balancer Service

Der Load Balancer Service verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage Nodes. Um den Lastenausgleich zu aktivieren, müssen Sie Load Balancer-Endpunkte mithilfe des Grid-Managers konfigurieren.

Sie können Load Balancer-Endpunkte nur für Admin-Nodes oder Gateway-Nodes konfigurieren, da diese Node-Typen den Load Balancer Service enthalten. Sie können keine Endpunkte für Speicherknoten oder Knoten archivieren konfigurieren.

Jeder Load Balancer-Endpunkt legt einen Port, ein Protokoll (HTTP oder HTTPS), einen Servicetyp (S3 oder Swift) und einen Bindungsmodus fest. HTTPS-Endpunkte erfordern ein Serverzertifikat. Bindungsmodi ermöglichen es Ihnen, die Zugriffsmöglichkeiten von Endpunktports auf folgende Arten zu beschränken:

- Spezifische virtuelle Hochverfügbarkeits-IP-Adressen (VIPs)
- Spezielle Netzwerkschnittstellen bestimmter Nodes

Überlegungen zu Ports

Clients können auf alle Endpunkte zugreifen, die Sie auf jedem Node konfigurieren, auf dem der Load Balancer Service ausgeführt wird. Es gibt zwei Ausnahmen: Die Ports 80 und 443 sind auf Admin-Nodes reserviert, sodass auf diesen Ports konfigurierte Endpunkte nur auf Gateway-Knoten Lastverteilungsvorgänge unterstützen.

Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte in der Recovery- und Wartungsanleitung zum Entfernen von Port-Remaps.

Der CLB-Service ist veraltet.

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.

Verwandte Informationen

"Verwalten Sie erholen"

Sie können Load Balancer-Endpunkte erstellen, bearbeiten und entfernen.

Erstellen von Load Balancer-Endpunkten

Jeder Load Balancer-Endpunkt legt einen Port, ein Netzwerkprotokoll (HTTP oder HTTPS) und einen Servicetyp (S3 oder Swift) fest. Wenn Sie einen HTTPS-Endpunkt erstellen, müssen Sie ein Serverzertifikat hochladen oder erstellen.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Wenn Sie zuvor Ports neu zugeordnet haben, die Sie für den Load Balancer-Dienst verwenden möchten, müssen Sie die Neuzuordnungen entfernt haben.

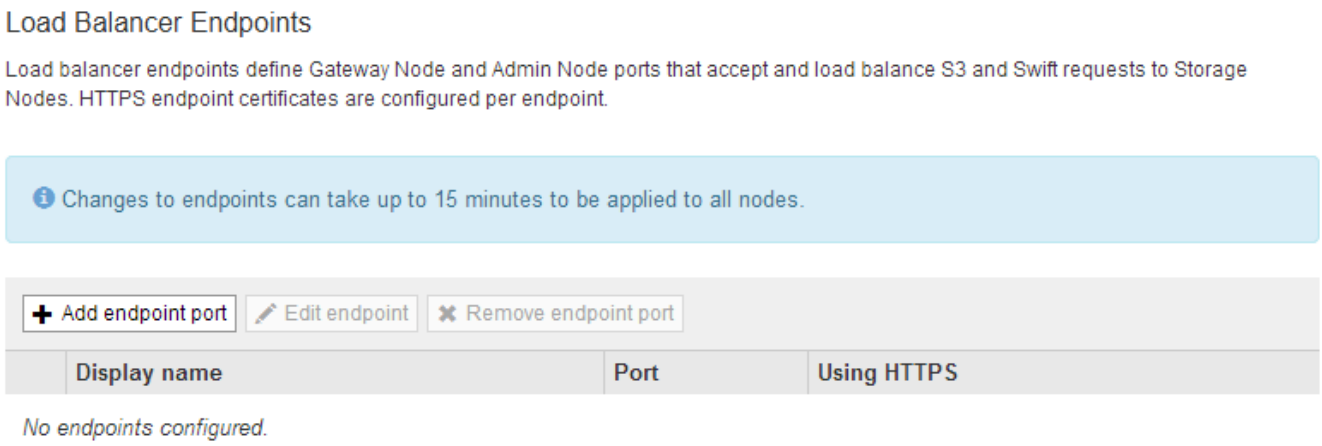
> Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte in der Recovery- und Wartungsanleitung zum Entfernen von Port-Remaps.

> Der CLB-Service ist veraltet.

Schritte

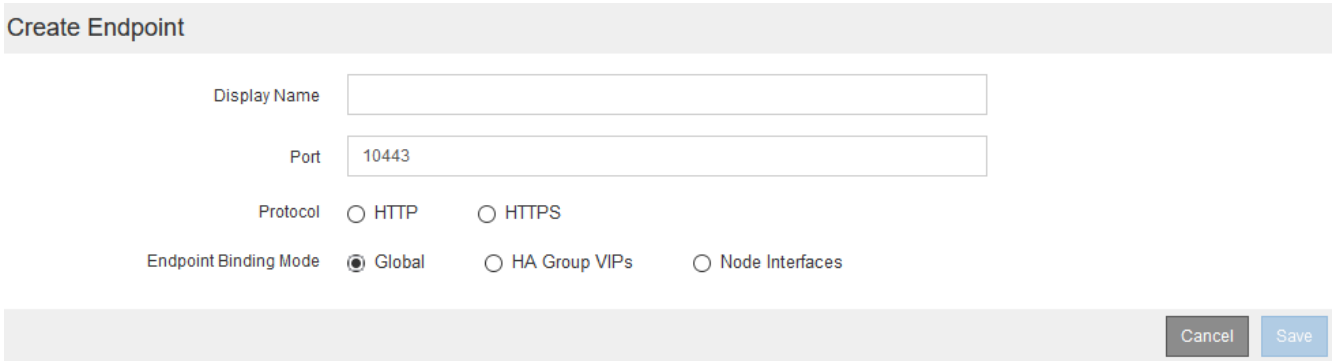
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**.

   Die Seite Load Balancer Endpoints wird angezeigt.



2. Wählen Sie **Endpunkt hinzufügen**.

   Das Dialogfeld Endpunkt erstellen wird angezeigt.



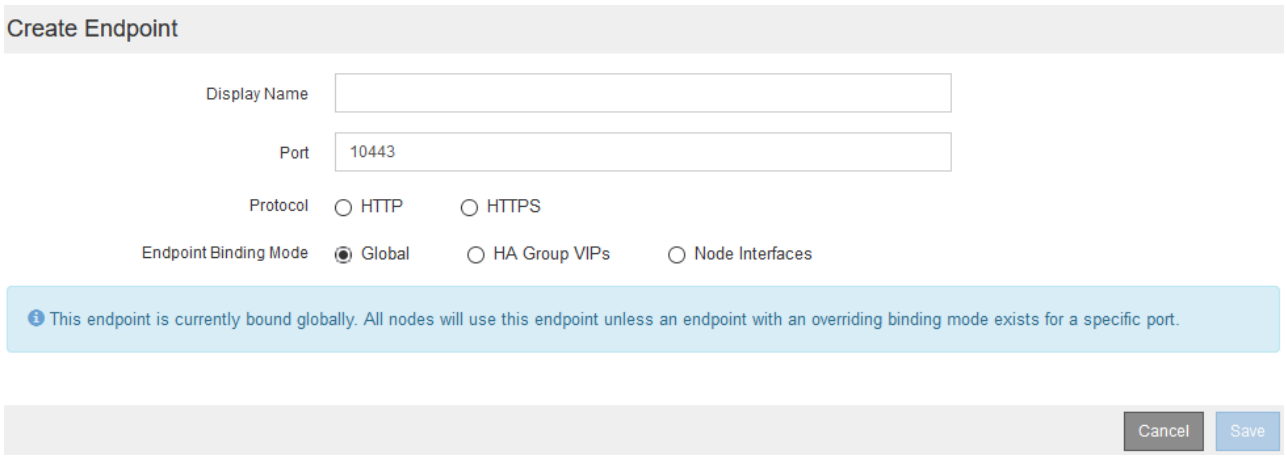
3. Geben Sie einen Anzeigenamen für den Endpunkt ein, der in der Liste auf der Seite Load Balancer Endpoints angezeigt wird.
4. Geben Sie eine Portnummer ein, oder lassen Sie die vorausgefüllte Portnummer unverändert.

   Wenn Sie die Portnummer 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind.

   > Von anderen Grid-Services verwendete Ports sind nicht zulässig. In den Netzwerkrichtlinien finden Sie eine Liste der Ports, die für die interne und externe Kommunikation verwendet werden.

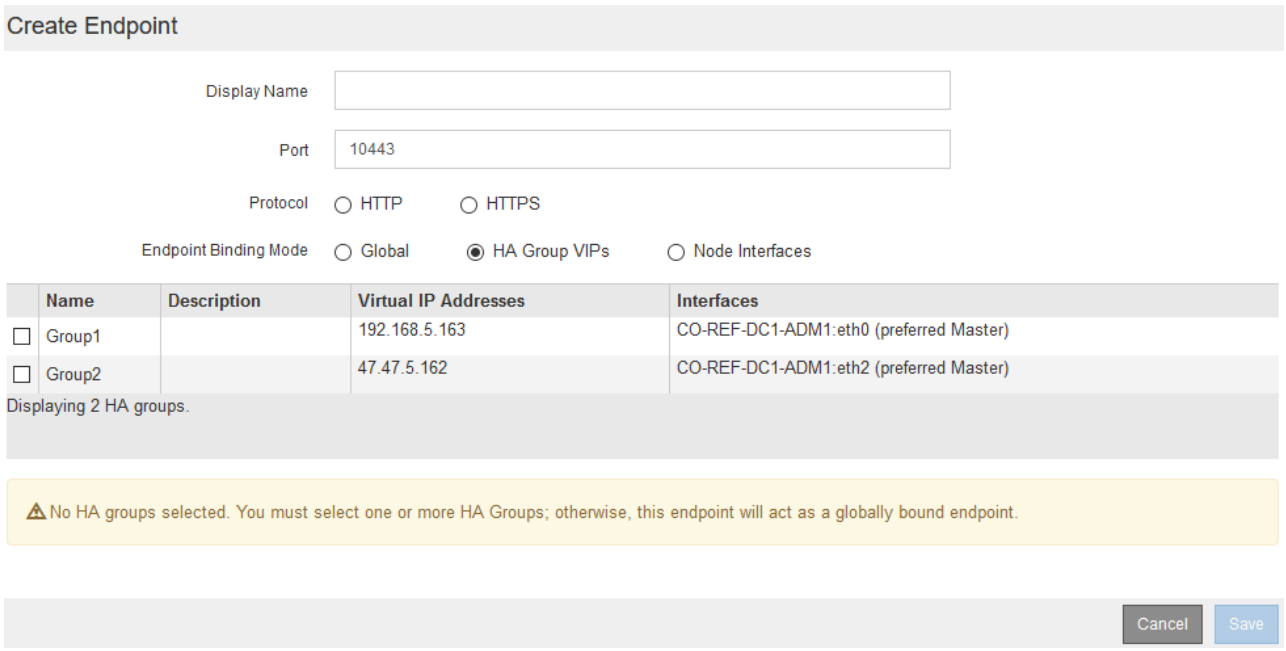
5. Wählen Sie **HTTP** oder **HTTPS** aus, um das Netzwerkprotokoll für diesen Endpunkt festzulegen.
6. Wählen Sie einen Endpunktbindungsmodus aus.

   - **Global** (Standard): Der Endpunkt ist auf allen Gateway Nodes und Admin Nodes auf der angegebenen Portnummer zugänglich.



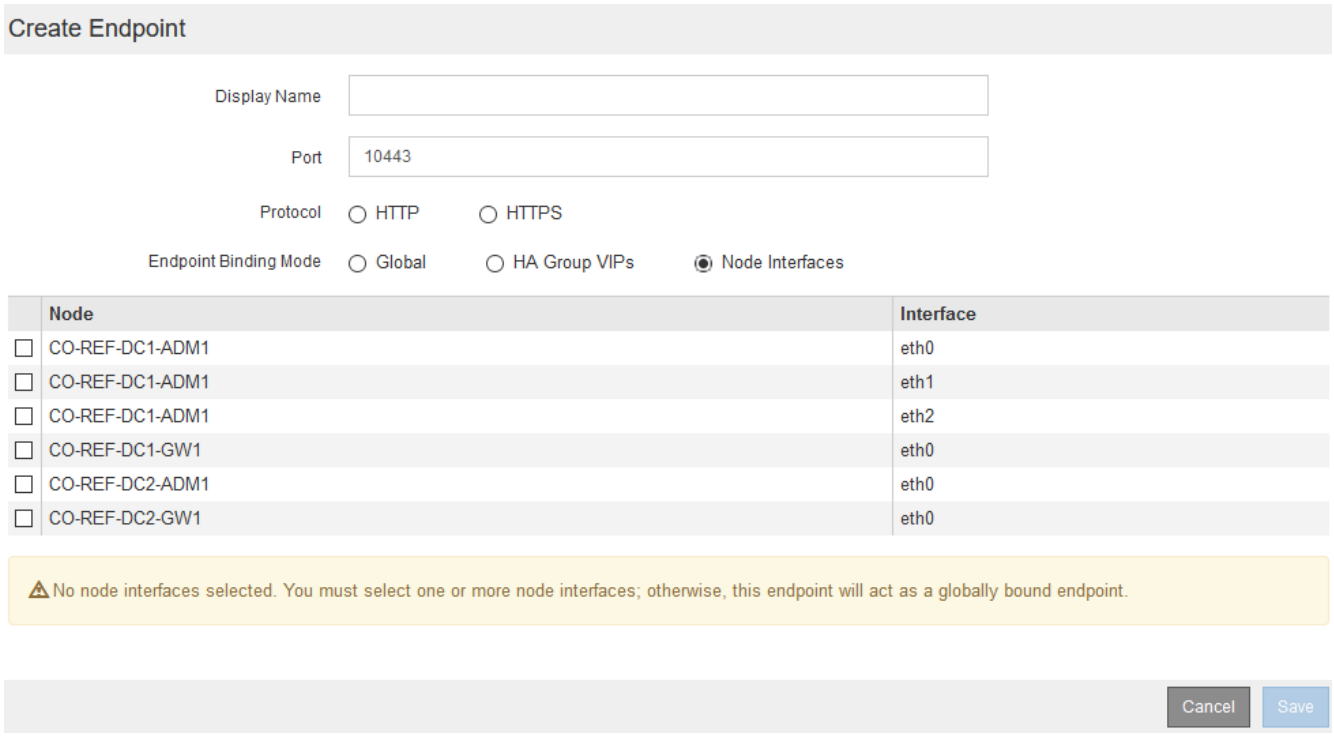
   - **HA Group VIPs**: Der Endpunkt ist nur über die für die ausgewählten HA-Gruppen definierten virtuellen IP-Adressen zugänglich. In diesem Modus definierte Endpunkte können die gleiche Port-Nummer wiederverwenden, solange die von diesen Endpunkten definierten HA-Gruppen nicht miteinander überlappen.

     Wählen Sie die HA-Gruppen mit den virtuellen IP-Adressen aus, auf denen der Endpunkt angezeigt werden soll.



- **Node-Schnittstellen**: Der Endpunkt ist nur auf den angegebenen Knoten und den Netzwerkschnittstellen zugänglich. In diesem Modus definierte Endpunkte können dieselbe Portnummer wiederverwenden, solange sich diese Schnittstellen nicht gegenseitig überschneiden.

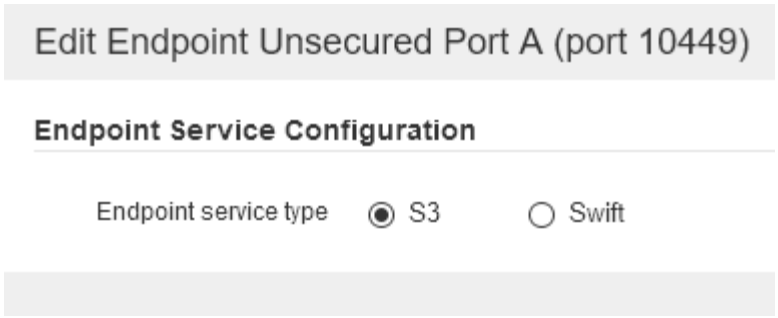
  Wählen Sie die Knotenschnittstellen aus, auf denen der Endpunkt angezeigt werden soll.



7. Wählen Sie **Speichern**.

   Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

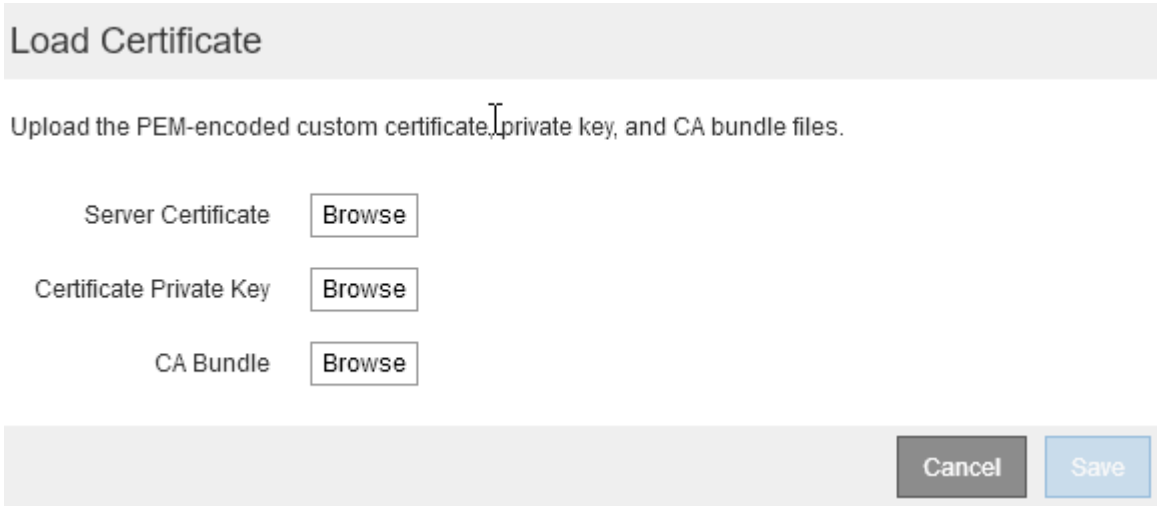
8. Wählen Sie **S3** oder **Swift** aus, um den Verkehrstyp festzulegen, den dieser Endpunkt bedienen wird.



9. Wenn Sie **HTTP** ausgewählt haben, wählen Sie **Speichern**.

   Der ungesicherte Endpunkt wird erstellt. In der Tabelle auf der Seite Load Balancer Endpoints werden der Anzeigename, die Portnummer, das Protokoll und die Endpunkt-ID des Endpunkts aufgeführt.

10. Wenn Sie **HTTPS** ausgewählt haben und ein Zertifikat hochladen möchten, wählen Sie **Zertifikat hochladen**.



   a. Suchen Sie nach dem Serverzertifikat und dem privaten Zertifikatschlüssel.

      Damit S3-Clients eine Verbindung über einen S3-API-Endpunkt-Domain-Namen herstellen können, verwenden Sie ein Multi-Domain- oder Platzhalterzertifikat, das mit allen Domänennamen übereinstimmt, die der Client zum Herstellen der Verbindung zum Grid verwenden kann. Beispielsweise kann das Serverzertifikat den Domänennamen verwenden `*.example.com`.

   "Konfigurieren von S3-API-Endpunkt-Domain-Namen"

   a. Optional können Sie nach einem CA-Bundle suchen.
   b. Wählen Sie **Speichern**.

      Die PEM-kodierten Zertifikatdaten für den Endpunkt werden angezeigt.

11. Wenn Sie **HTTPS** ausgewählt haben und ein Zertifikat erstellen möchten, wählen Sie **Zertifikat erstellen**.

a. Geben Sie einen Domain-Namen oder eine IP-Adresse ein.

   Sie können Platzhalter verwenden, um die vollständig qualifizierten Domänennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer Service ausgeführt wird. Beispiel: `*.sgws.foo.com` Verwendet den Platzhalter * für die Darstellung `gn1.sgws.foo.com` Und `gn2.sgws.foo.com`.

"Konfigurieren von S3-API-Endpunkt-Domain-Namen"

a. Wählen Sie + So fügen Sie weitere Domain-Namen oder IP-Adressen hinzu:

   Wenn Sie Hochverfügbarkeitsgruppen (HA-Gruppen) verwenden, fügen Sie die Domain-Namen und IP-Adressen der virtuellen HA-IPs hinzu.

b. Geben Sie optional einen X.509-Studienteilnehmer ein, der auch als Distinguished Name (DN) bezeichnet wird, um zu ermitteln, wer das Zertifikat besitzt.

c. Wählen Sie optional die Anzahl der Tage aus, an denen das Zertifikat gültig ist. Der Standardwert ist 730 Tage.

d. Wählen Sie **Erzeugen**.

   Die Zertifikatmetadaten und die PEM-kodierten Zertifikatdaten für den Endpunkt werden angezeigt.

12. Klicken Sie Auf **Speichern**.

    Der Endpunkt wird erstellt. In der Tabelle auf der Seite Load Balancer Endpoints werden der Anzeigename, die Portnummer, das Protokoll und die Endpunkt-ID des Endpunkts aufgeführt.

Verwandte Informationen

"Verwalten Sie erholen"

"Netzwerkrichtlinien"

"Verwalten von Hochverfügbarkeitsgruppen"

"Verwalten von nicht vertrauenswürdigen Client-Netzwerken"

Bearbeiten von Load Balancer-Endpunkten

Für einen ungesicherten (HTTP) Endpunkt können Sie den Diensttyp des Endpunkts zwischen S3 und Swift ändern. Für einen gesicherten Endpunkt (HTTPS) können Sie den Diensttyp des Endpunkts bearbeiten und das Sicherheitszertifikat anzeigen oder ändern.

Was Sie benötigen

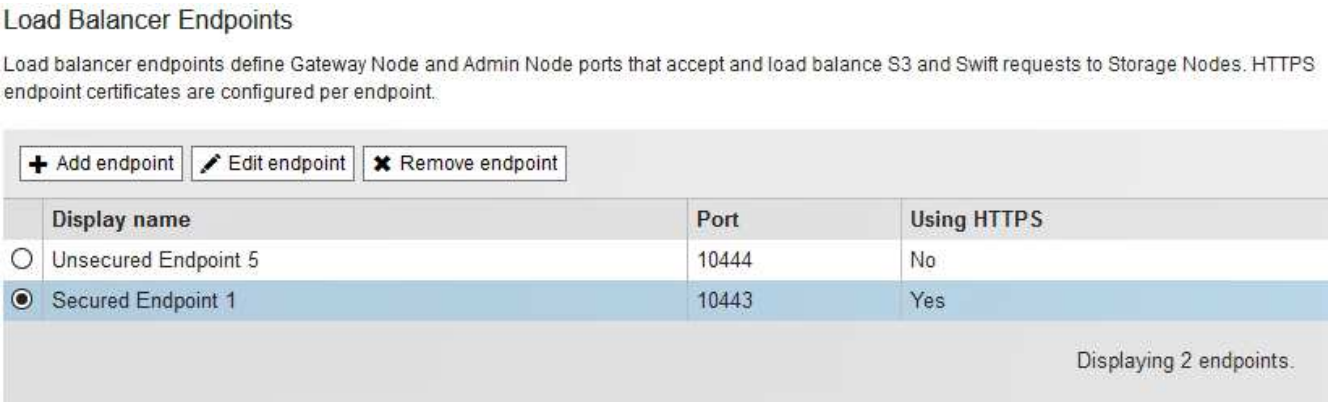
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**.

   Die Seite Load Balancer Endpoints wird angezeigt. Die vorhandenen Endpunkte sind in der Tabelle aufgeführt.

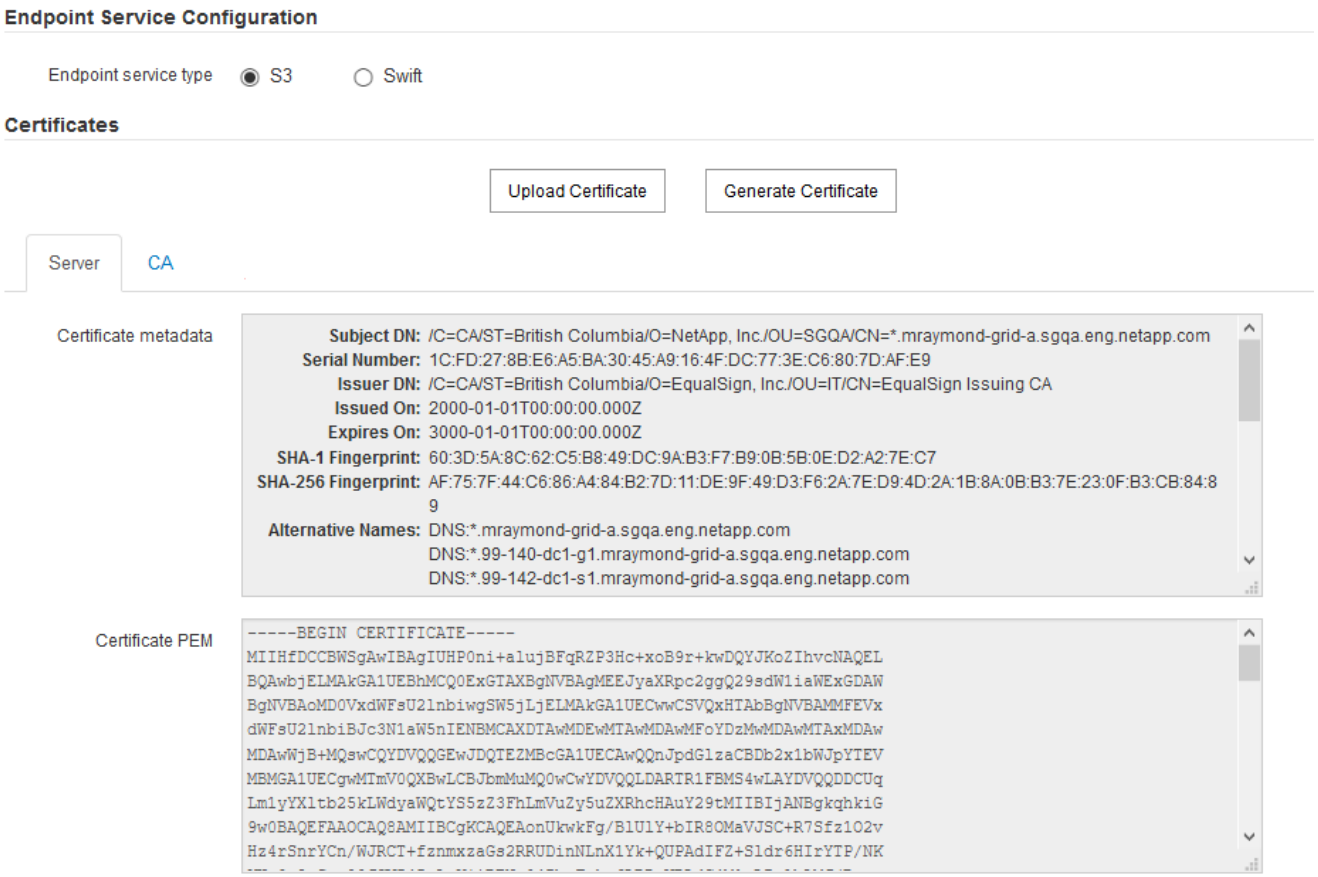
   Endpunkte mit bald auslaufenden Zertifikaten sind in der Tabelle aufgeführt.



2. Wählen Sie den Endpunkt aus, den Sie bearbeiten möchten.
3. Klicken Sie auf **Endpunkt bearbeiten**.

   Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

   Für einen ungesicherten (HTTP) Endpunkt wird nur der Abschnitt Konfiguration des Endpoint Service des Dialogfelds angezeigt. Für einen gesicherten Endpunkt (HTTPS) werden die Abschnitte Endpoint Service Configuration und die Zertifikate des Dialogfelds angezeigt, wie im folgenden Beispiel dargestellt.



4. Nehmen Sie die gewünschten Änderungen am Endpunkt vor.

   Für einen ungesicherten (HTTP-)Endpunkt können Sie:

   - Ändern Sie den Endpunkt-Servicetyp zwischen S3 und Swift.
   - Ändern Sie den Endpunktbindungsmodus. Für einen gesicherten Endpunkt (HTTPS) können Sie:
   - Ändern Sie den Endpunkt-Servicetyp zwischen S3 und Swift.
   - Ändern Sie den Endpunktbindungsmodus.
   - Zeigen Sie das Sicherheitszertifikat an.
   - Hochladen oder Generieren eines neuen Sicherheitszertifikats, wenn das aktuelle Zertifikat abgelaufen ist oder kurz vor Ablauf steht.

     Wählen Sie eine Registerkarte aus, um detaillierte Informationen zum StorageGRID-Standardserverzertifikat oder zum hochgeladenen Zertifikat einer Zertifizierungsstelle anzuzeigen.

   > Um das Protokoll für einen vorhandenen Endpunkt, zum Beispiel von HTTP zu HTTPS, zu ändern, müssen Sie einen neuen Endpunkt erstellen. Befolgen Sie die Anweisungen zum Erstellen von Load Balancer-Endpunkten, und wählen Sie das gewünschte Protokoll aus.

5. Klicken Sie Auf **Speichern**.

Verwandte Informationen

Erstellen von Load Balancer-Endpunkten

Entfernen von Load Balancer-Endpunkten

Wenn Sie keinen Endpunkt mehr für den Load Balancer benötigen, können Sie ihn entfernen.

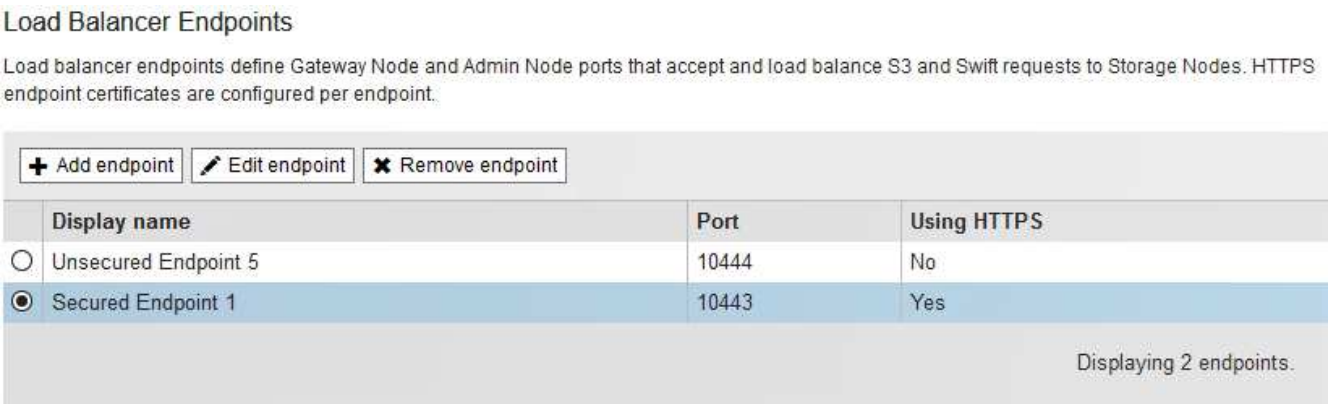
Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**.

   Die Seite Load Balancer Endpoints wird angezeigt. Die vorhandenen Endpunkte sind in der Tabelle aufgeführt.



2. Wählen Sie das Optionsfeld links neben dem Endpunkt, den Sie entfernen möchten.
3. Klicken Sie auf **Endpunkt entfernen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf **OK**.

   Der Endpunkt wird entfernt.

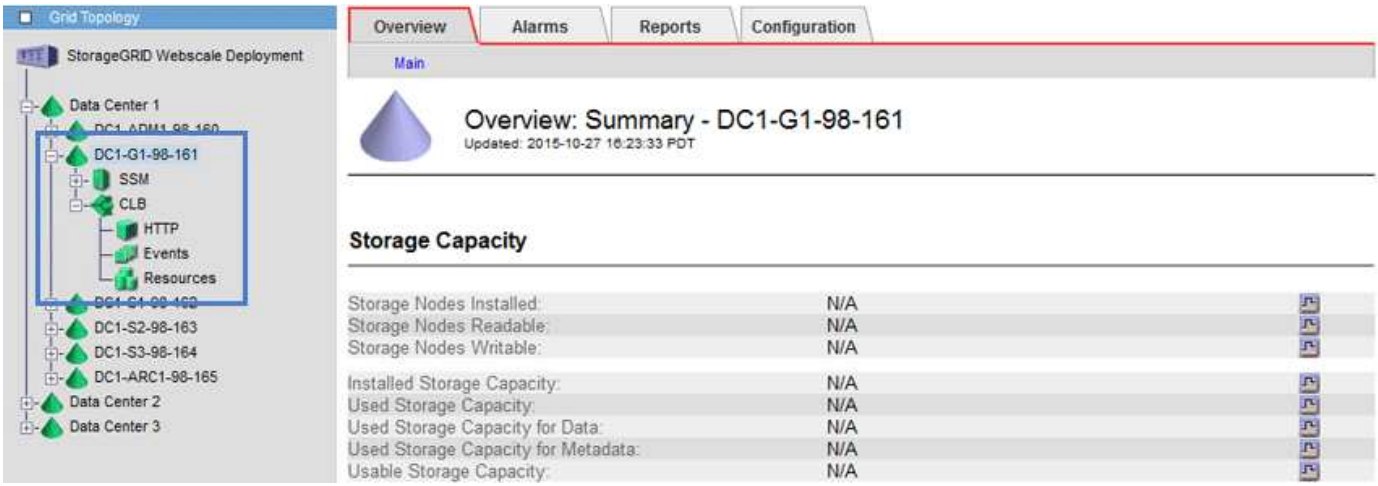
Wie der Lastenausgleich funktioniert - CLB-Service

Der CLB-Dienst (Connection Load Balancer) auf Gateway-Nodes ist veraltet. Der Lastausgleichsdienst ist jetzt der empfohlene Lastausgleichmechanismus.

Der CLB-Service nutzt Layer 4 Load Balancing zur Verteilung eingehender TCP-Netzwerkverbindungen von

Client-Anwendungen auf den optimalen Storage Node basierend auf Verfügbarkeit, Systemlast und den vom Administrator konfigurierten Verbindungskosten. Wenn der optimale Speicherknoten ausgewählt wird, baut der CLB-Dienst eine zweiseitige Netzwerkverbindung auf und leitet den Datenverkehr vom und zum ausgewählten Knoten weiter. Beim CLB wird die Konfiguration des Grid-Netzwerks nicht berücksichtigt, wenn eingehende Netzwerkverbindungen geleitet werden.

Um Informationen zum CLB-Dienst anzuzeigen, wählen Sie **Support** > **Tools** > **Grid Topology** und erweitern Sie dann einen Gateway-Knoten, bis Sie **CLB** und die darunter stehenden Optionen auswählen können.



Wenn Sie den CLB-Service nutzen möchten, sollten Sie die Verbindungskosten für Ihr StorageGRID-System in Betracht ziehen.

Verwandte Informationen

"Was sind Verbindungskosten"

"Verbindungskosten werden aktualisiert"

Verwalten von nicht vertrauenswürdigen Client-Netzwerken

Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Endpunkten akzeptieren.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, StorageGRID vertraut standardmäßig eingehende Verbindungen zu jedem Grid-Knoten auf allen verfügbaren externen Ports (siehe Informationen über externe Kommunikation in den Netzwerkrichtlinien).

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 Node nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

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. Konfigurieren Sie auf der Seite Load Balancer Endpoints einen Endpunkt für den Load Balancer für S3 über HTTPS am Port 443.

2. Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Gateway-Node 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 Datenverkehr des Outbound-S3-Plattformdienstes von einem Speicherknoten aktivieren, jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Speicherknoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, akzeptiert der Speicherknoten keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen an Amazon Web Services.

Verwandte Informationen

"Netzwerkrichtlinien"

"Konfigurieren von Load Balancer-Endpunkten"

Das Festlegen des Client-Netzwerks eines Knotens ist nicht vertrauenswürdig

Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob das Client-Netzwerk jedes Node vertrauenswürdig oder nicht vertrauenswürdig ist. Sie können auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.

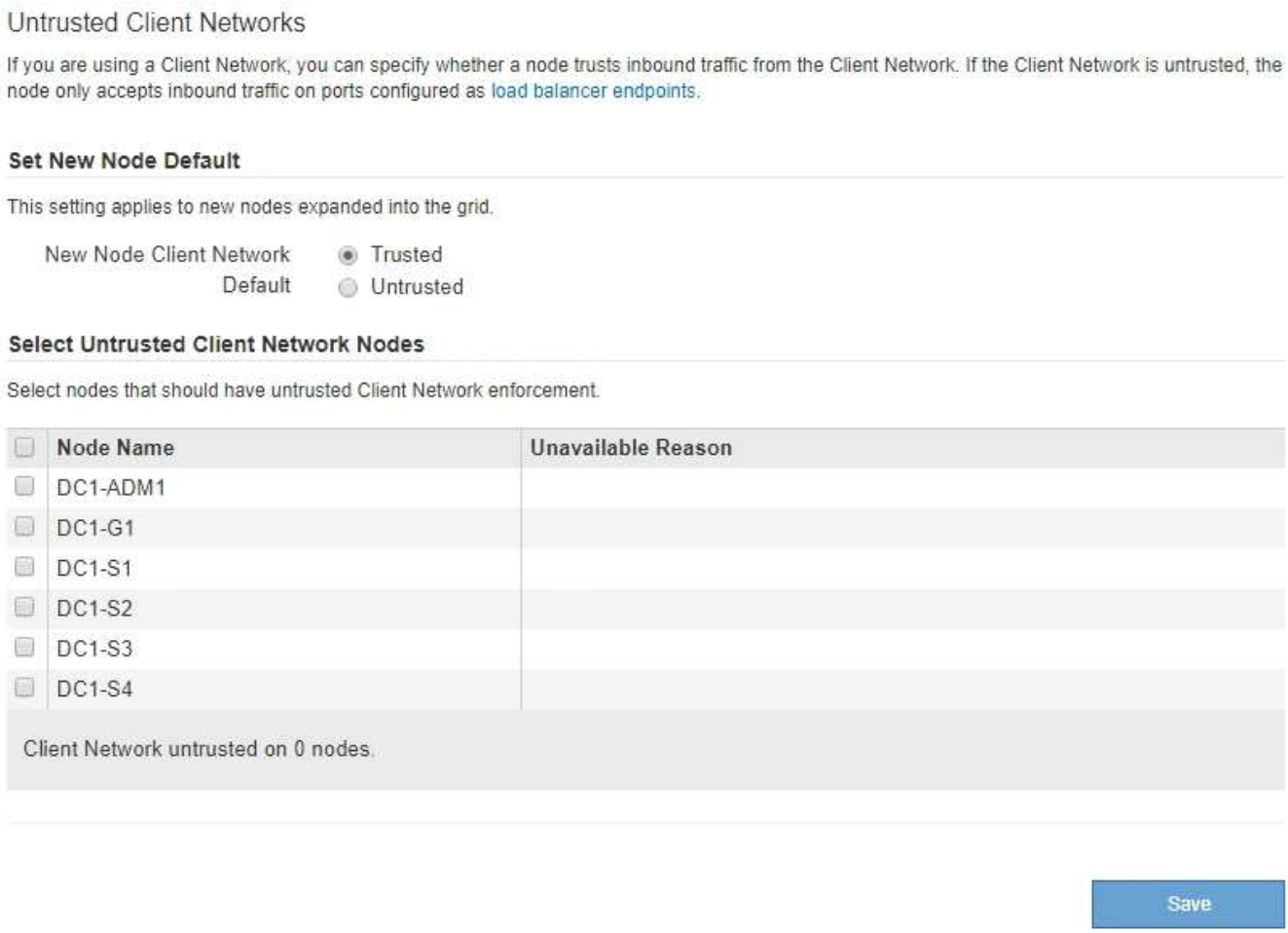
> Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Nicht Vertrauenswürdiges Clientnetzwerk**.

   Die Seite nicht vertrauenswürdige Clientnetzwerke wird angezeigt.

   Auf dieser Seite werden alle Knoten in Ihrem StorageGRID-System aufgelistet. Die Spalte „nicht verfügbar“ enthält einen Eintrag, wenn das Client-Netzwerk auf dem Knoten vertrauenswürdig sein muss.



2. Geben Sie im Abschnitt **Neue Knoten Standard** festlegen an, was die Standardeinstellung sein soll, wenn neue Knoten in einem Erweiterungsvorgang zum Raster hinzugefügt werden.
   - **Trusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird seinem Client-Netzwerk vertraut.
   - **UnTrusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig. Sie können bei Bedarf zu dieser Seite zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.

   Diese Einstellung hat keine Auswirkung auf die vorhandenen Nodes im StorageGRID System.

3. Wählen Sie im Abschnitt **nicht vertrauenswürdige Client-Netzwerkknoten auswählen** die Knoten aus, die Clientverbindungen nur auf explizit konfigurierten Load-Balancer-Endpunkten zulassen sollen.

   Sie können das Kontrollkästchen im Titel auswählen oder deaktivieren, um alle Knoten auszuwählen oder zu deaktivieren.

4. Klicken Sie Auf **Speichern**.

   Die neuen Firewall-Regeln werden sofort hinzugefügt und durchgesetzt. Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Verwandte Informationen

"Konfigurieren von Load Balancer-Endpunkten"

Verwalten von Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) sorgen für hochverfügbare Datenverbindungen für S3 und Swift Clients. HA-Gruppen können auch für hochverfügbare Verbindungen mit dem Grid Manager und dem Tenant Manager verwendet werden.

- "Eine HA-Gruppe"
- "Verwendung von HA-Gruppen"
- "Konfigurationsoptionen für HA-Gruppen"
- "Erstellen einer Hochverfügbarkeitsgruppe"
- "Bearbeiten einer Hochverfügbarkeitsgruppe"
- "Entfernen einer Hochverfügbarkeitsgruppe"

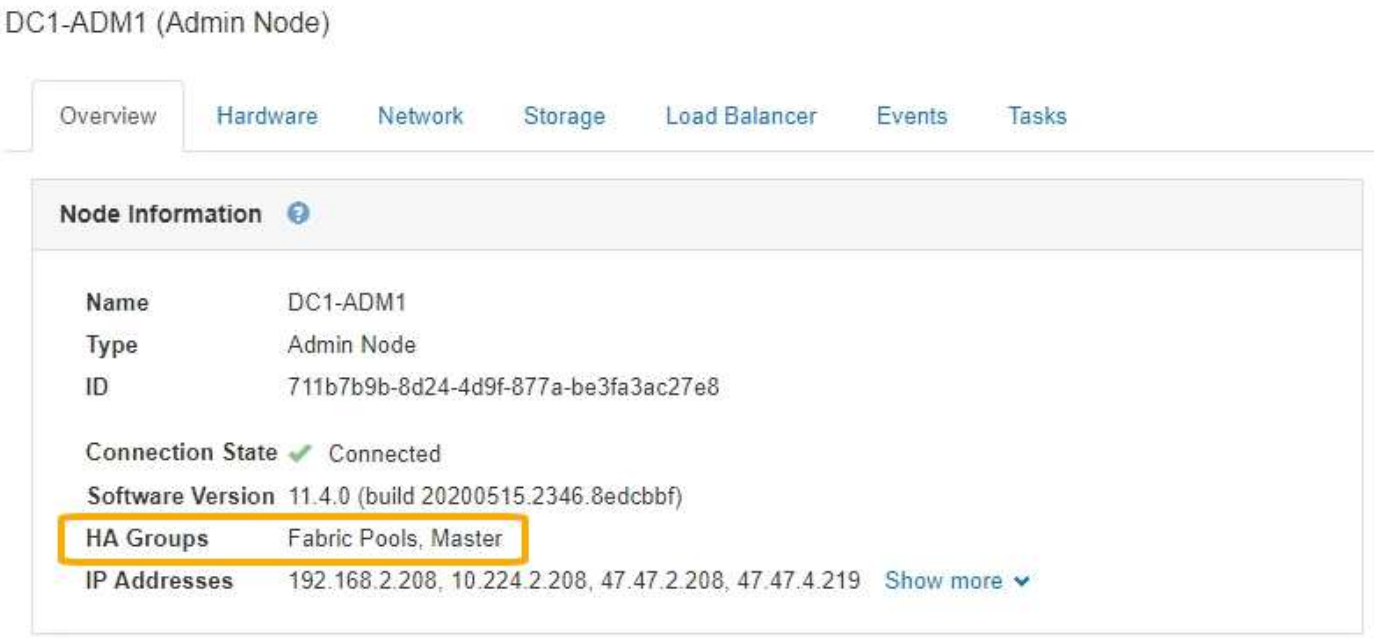
Eine HA-Gruppe

Hochverfügbarkeitsgruppen verwenden virtuelle IP-Adressen (VIPs), um aktiv-Backup-Zugriff auf Gateway Node- oder Admin-Node-Services bereitzustellen.

Eine HA-Gruppe besteht aus mindestens einer Netzwerkschnittstellen an Admin-Nodes und Gateway-Nodes. Beim Erstellen einer HA-Gruppe wählen Sie Netzwerkschnittstellen aus, die zum Grid Network (eth0) oder dem Client-Netzwerk (eth2) gehören. Alle Schnittstellen in einer HA-Gruppe müssen sich im selben Netzwerk-Subnetz befinden.

Eine HA-Gruppe behält eine oder mehrere virtuelle IP-Adressen bei, die der aktiven Schnittstelle in der Gruppe hinzugefügt werden. Wenn die aktive Schnittstelle nicht mehr verfügbar ist, werden die virtuellen IP-Adressen in eine andere Schnittstelle verschoben. Dieser 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.

Die aktive Schnittstelle in einer HA-Gruppe wird als Master bezeichnet. Alle anderen Schnittstellen werden als Backup bezeichnet. Um diese Bezeichnungen anzuzeigen, wählen Sie **Knoten** > ***Node*** > **Übersicht**.



Beim Erstellen einer HA-Gruppe geben Sie eine Schnittstelle an, die der bevorzugte Master sein soll. Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden. Wenn der Fehler behoben ist, werden die VIP-Adressen automatisch zurück zum bevorzugten Master verschoben.

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 der Failover nicht durch den Ausfall des CLB-Dienstes (veraltet) oder der Dienste für den Grid-Manager oder den Mandanten-Manager ausgelöst.

Wenn die HA-Gruppe Schnittstellen von mehr als zwei Nodes enthält, kann während des Failover die aktive Schnittstelle zu einer anderen Node verschoben werden.

Verwendung von HA-Gruppen

Es empfiehlt sich, aus mehreren Gründen Gruppen für Hochverfügbarkeit (HA) zu verwenden.

- 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-Knoten**: Schließen Sie den Load Balancer Service und den CLB-Dienst (veraltet) ein.

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
Zugriff auf Grid Manager	• Primärer Admin-Node (**bevorzugter Master**) • Nicht primäre Admin-Nodes **Hinweis:** der primäre Admin-Knoten muss der bevorzugte Master sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.
Zugriff nur auf Tenant Manager	• Primäre oder nicht primäre Admin-Nodes
S3- oder Swift-Client-Zugriff – Load Balancer Service	• Admin-Nodes • Gateway-Nodes
S3- oder Swift-Client-Zugriff — CLB-Service **Hinweis:** der CLB-Service ist veraltet.	• Gateway-Nodes

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Der Ausfall von Services für den Grid Manager oder den Mandanten-Manager löst nicht ein Failover innerhalb der HA-Gruppe aus.

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 Wartungsvorgänge können nicht ausgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager überwachen.

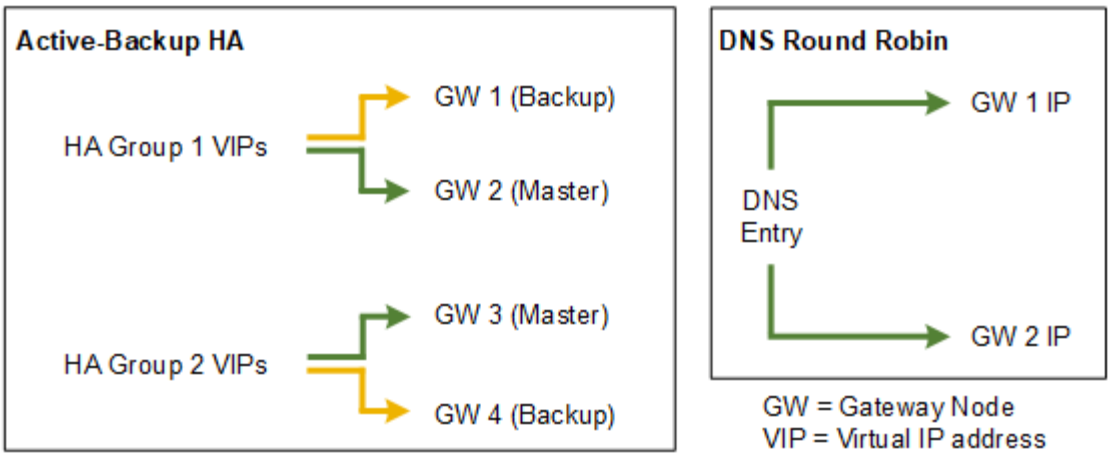
Einschränkungen bei der Verwendung von HA-Gruppen mit dem CLB-Service

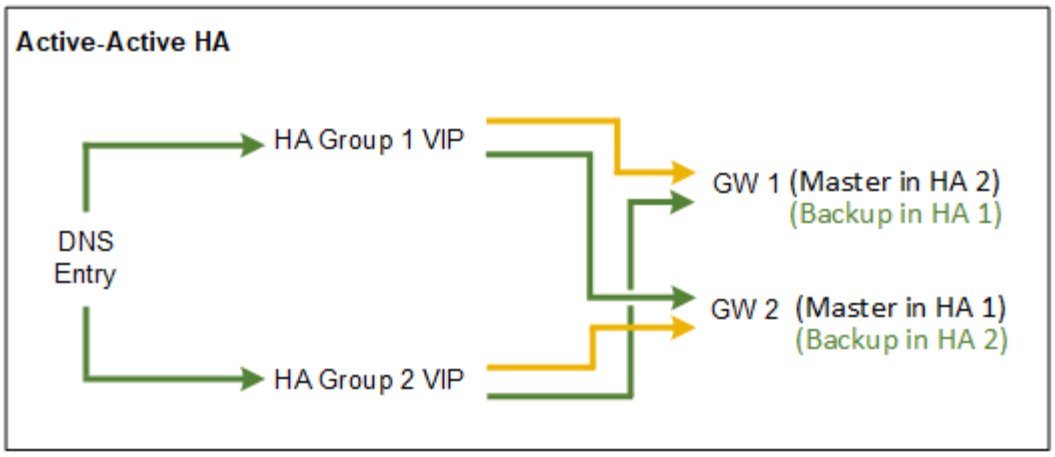
Der Ausfall des CLB-Dienstes löst nicht ein Failover innerhalb der HA-Gruppe aus.

Der CLB-Service ist veraltet.

Konfigurationsoptionen für HA-Gruppen

Die folgenden Diagramme bieten Beispiele für verschiedene Möglichkeiten zum Konfigurieren von HA-Gruppen. Jede Option hat vor- und Nachteile.





Wenn mehrere sich überschneidende HA-Gruppen erstellt werden, wie im „aktiv/aktiv-HA-Beispiel“ dargestellt, wird der Gesamtdurchsatz mit der Anzahl der Nodes und HA-Gruppen skaliert. Mit drei oder mehr Nodes und drei oder mehr HA-Gruppen können außerdem Vorgänge mithilfe einer der VIPs fortgesetzt werden – selbst bei Wartungsarbeiten, bei denen ein Node offline geschaltet werden muss.

Die Tabelle enthält eine Zusammenfassung der Vorteile der einzelnen HA-Konfigurationen, die in der Abbildung dargestellt sind.

Konfiguration	Vorteile	Nachteile
Aktiv/Backup HA	• Management über StorageGRID ohne externe Abhängigkeiten • Schnelles Failover.	• In einer HA-Gruppe ist nur ein Node aktiv. Mindestens ein Node pro HA-Gruppe bleibt im Ruhezustand.

Konfiguration	Vorteile	Nachteile
DNS Round Robin	• Erhöhter Aggregatdurchsatz: • Keine leerlaufenden Hosts	• Langsamer Failover, der vom Client-Verhalten abhängen kann. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.
Aktiv/Aktiv	• Der Datenverkehr wird über mehrere HA-Gruppen verteilt. • Hoher Aggregatdurchsatz, der mit der Anzahl der HA-Gruppen skaliert werden kann • Schnelles Failover.	• Komplexer zu konfigurieren. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.

Erstellen einer Hochverfügbarkeitsgruppe

Sie können eine oder mehrere Hochverfügbarkeitsgruppen (HA-Gruppen) erstellen, die für hochverfügbaren Zugriff auf die Services in Admin-Nodes oder Gateway-Nodes sorgen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Eine Schnittstelle muss die folgenden Bedingungen erfüllen, die in einer HA-Gruppe enthalten sein sollen:

- Die Schnittstelle muss für einen Gateway-Node oder einen Admin-Node verwendet werden.
- Die Schnittstelle muss zum Grid Network (eth0) oder dem Client Network (eth2) gehören.
- Die Schnittstelle muss mit fester oder statischer IP-Adresse konfiguriert werden, nicht mit DHCP.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen**.

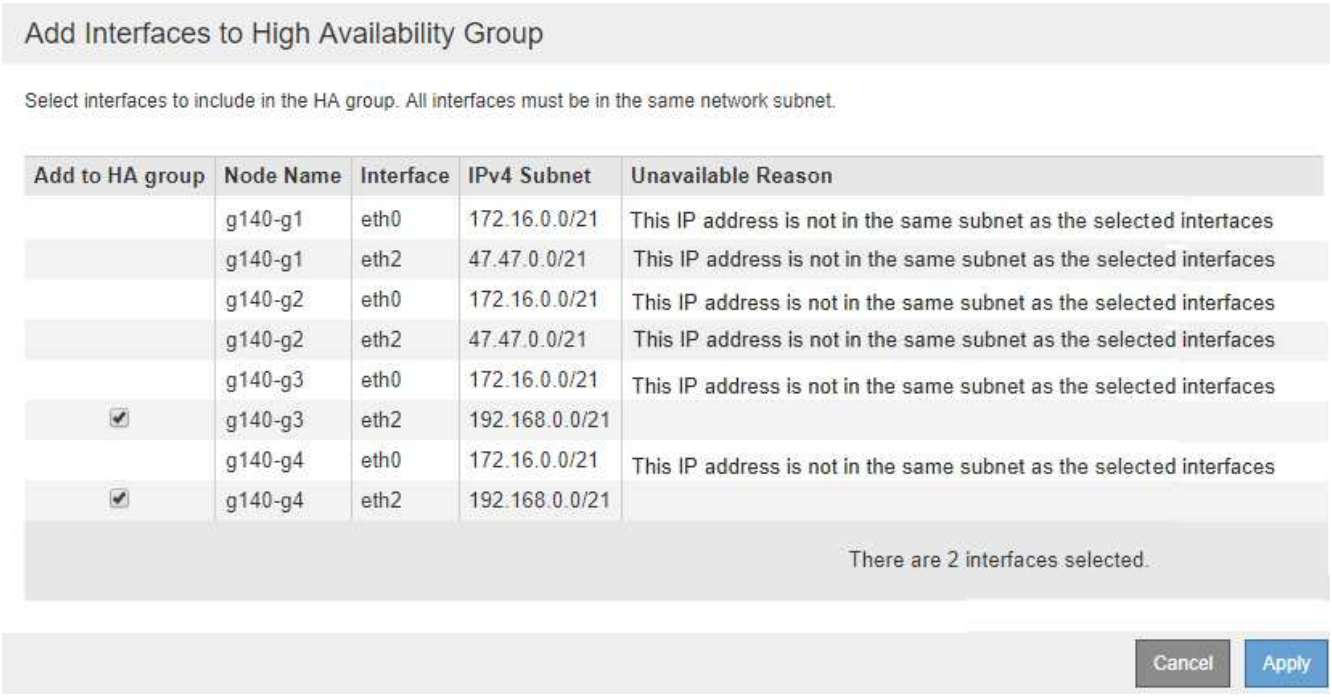
   Die Seite „Hochverfügbarkeitsgruppen“ wird angezeigt.

2. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld Gruppe für hohe Verfügbarkeit erstellen wird angezeigt.

3. Geben Sie einen Namen und, falls gewünscht, eine Beschreibung für die HA-Gruppe ein.
4. Klicken Sie Auf **Schnittstellen Auswählen**.

   Das Dialogfeld Schnittstellen zu Hochverfügbarkeitsgruppe hinzufügen wird angezeigt. In der Tabelle werden die infrage kommenden Nodes, Schnittstellen und IPv4-Subnetze aufgeführt.



   Eine Schnittstelle wird in der Liste nicht angezeigt, wenn ihre IP-Adresse durch DHCP zugewiesen wird.

5. Aktivieren Sie in der Spalte **zur HA-Gruppe** das Kontrollkästchen für die Schnittstelle, die zur HA-Gruppe hinzugefügt werden soll.

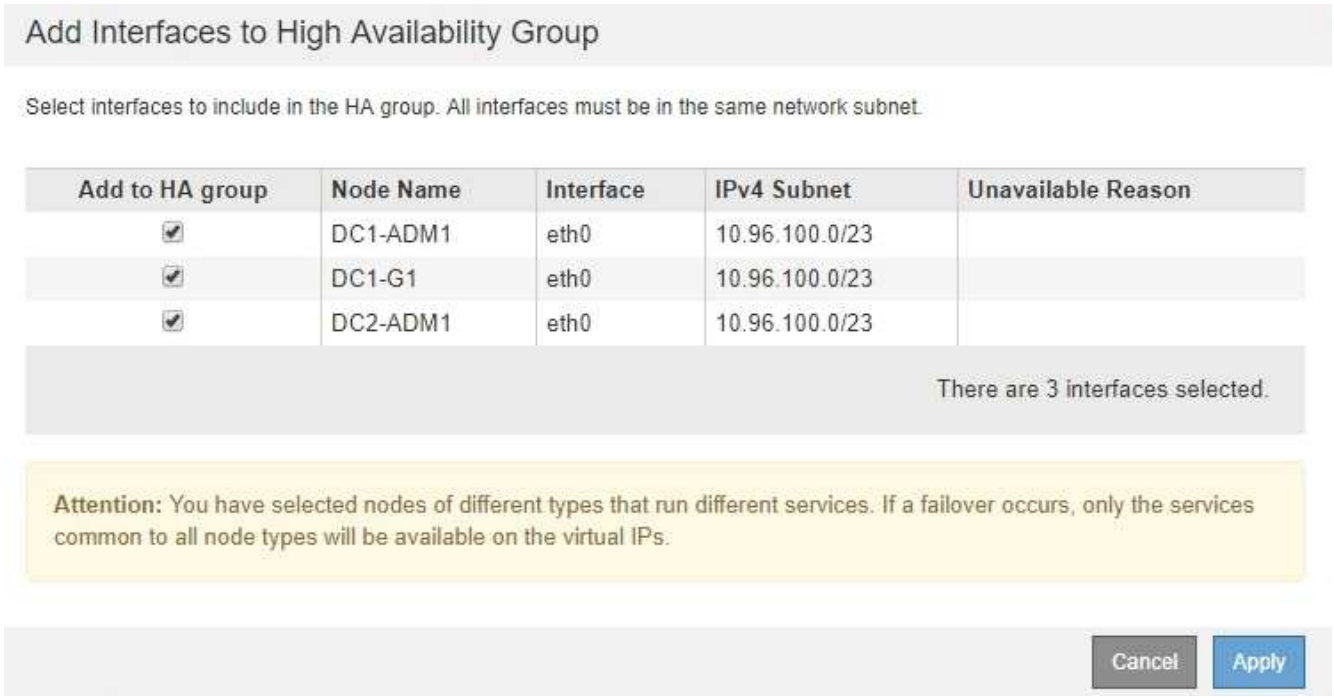
   Beachten Sie die folgenden Richtlinien für die Auswahl von Schnittstellen:

   - Sie müssen mindestens eine Schnittstelle auswählen.
   - Wenn Sie mehrere Schnittstellen auswählen, müssen sich alle Schnittstellen entweder im Grid Network (eth0) oder im Client Network (eth2) befinden.
   - Alle Schnittstellen müssen sich im gleichen Subnetz oder in Subnetzen mit einem gemeinsamen Präfix befinden.

IP-Adressen werden auf das kleinste Subnetz beschränkt (das mit dem größten Präfix).

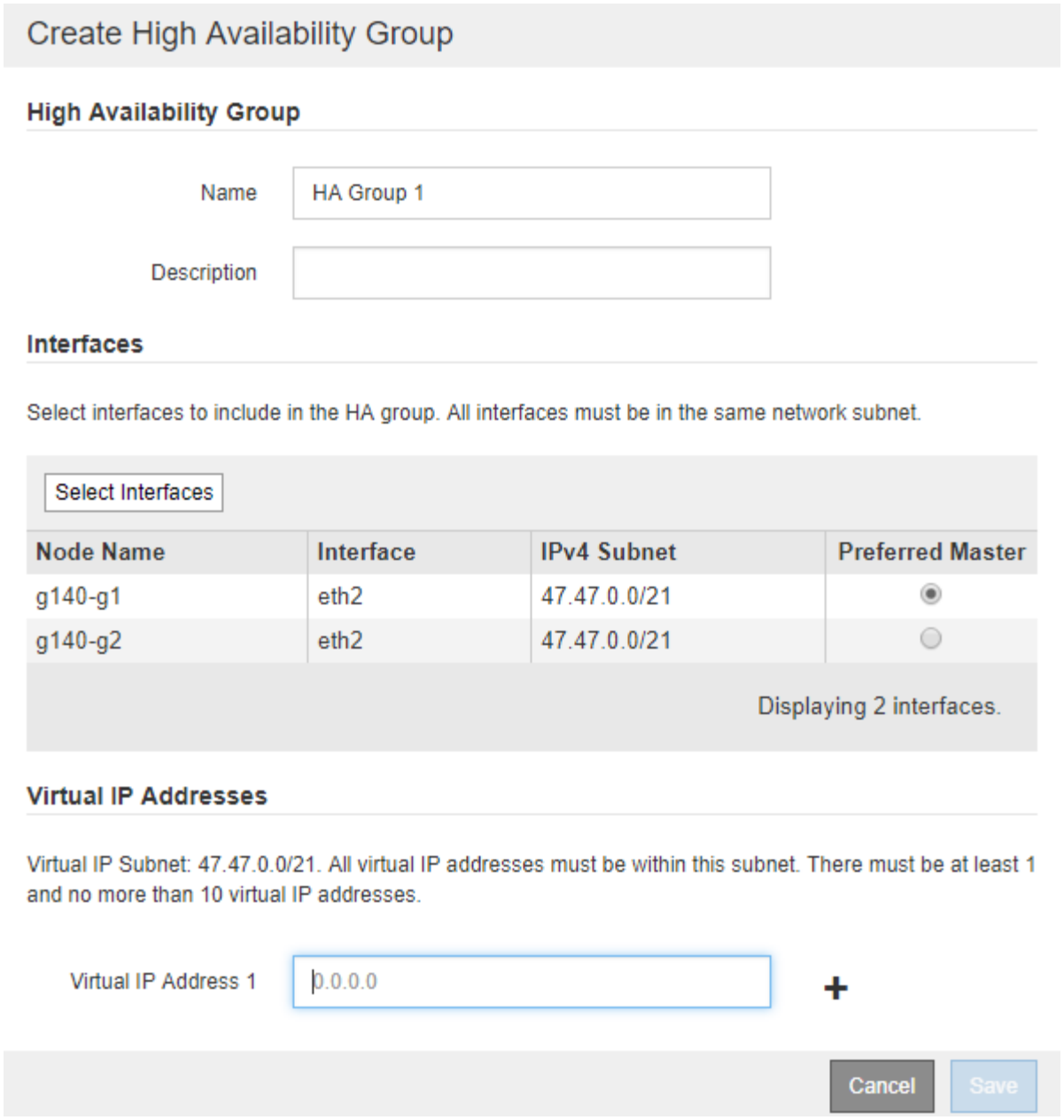
- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen und ein Failover auftritt, sind nur die Dienste verfügbar, die für die ausgewählten Knoten gemeinsam sind.
  - Wählen Sie mindestens zwei Admin-Nodes aus, um den HA-Schutz des Grid Manager oder des Mandanten-Manager zu erhalten.
  - Wählen Sie zwei oder mehr Admin-Nodes, Gateway-Nodes oder beide aus, um den HA-Schutz des Load Balancer Service zu gewährleisten.
  - Wählen Sie mindestens zwei Gateway-Nodes aus, um den HA-Schutz des CLB-Service zu gewährleisten.

    Der CLB-Service ist veraltet.



6. Klicken Sie Auf **Anwenden**.

   Die ausgewählten Schnittstellen werden auf der Seite Hochverfügbarkeitgruppe erstellen im Abschnitt Schnittstellen aufgeführt. Standardmäßig wird die erste Schnittstelle in der Liste als bevorzugter Master ausgewählt.



7. Wenn Sie eine andere Schnittstelle als bevorzugten Master auswählen möchten, wählen Sie diese Schnittstelle in der Spalte **bevorzugter Master** aus.

   Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden.

   > Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node auswählen, um der bevorzugte Master-Typ zu sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

8. Geben Sie im Abschnitt virtuelle IP-Adressen der Seite eine bis 10 virtuelle IP-Adressen für die HA-Gruppe ein. Klicken Sie auf das Pluszeichen (+) Um mehrere IP-Adressen hinzuzufügen.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

   IPv4-Adressen müssen sich im IPv4-Subnetz befinden, das von allen Mitgliedschnittstellen gemeinsam

genutzt wird.

9. Klicken Sie Auf **Speichern**.

   Die HA-Gruppe wird erstellt. Sie können jetzt die konfigurierten virtuellen IP-Adressen verwenden.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"VMware installieren"

"Installieren Sie Ubuntu oder Debian"

"Managen des Lastausgleichs"

Bearbeiten einer Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) bearbeiten, um ihren Namen und ihre Beschreibung zu ändern, Schnittstellen hinzuzufügen oder zu entfernen oder eine virtuelle IP-Adresse hinzuzufügen oder zu aktualisieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

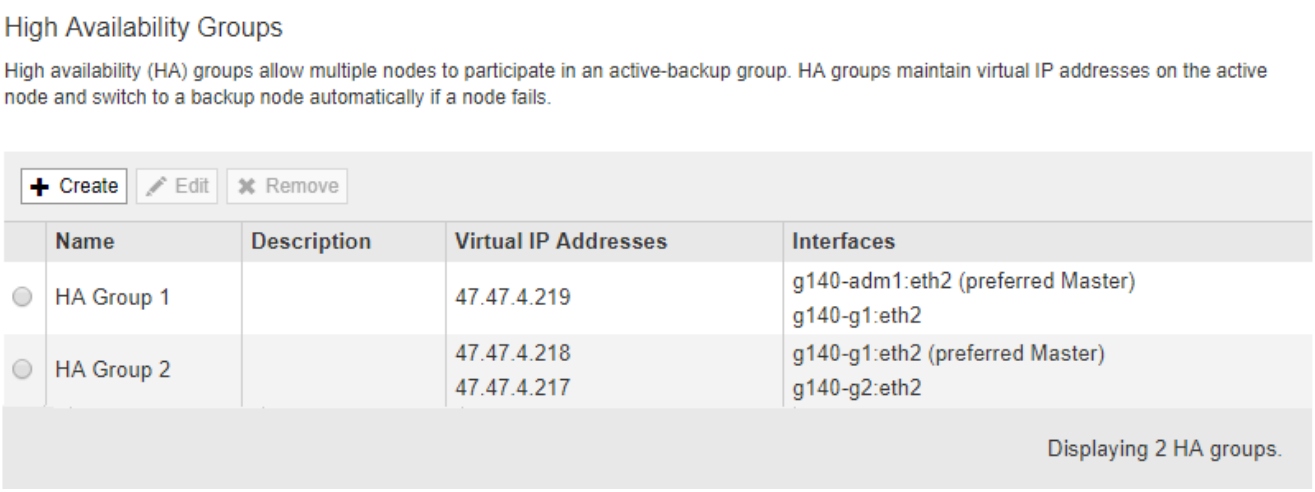
Das Bearbeiten einer HA-Gruppe hat einige der Gründe:

- Hinzufügen einer Schnittstelle zu einer vorhandenen Gruppe Die Schnittstellen-IP-Adresse muss sich innerhalb desselben Subnetzes befinden wie andere Schnittstellen, die der Gruppe bereits zugewiesen sind.
- Entfernen einer Schnittstelle aus einer HA-Gruppe. Sie können beispielsweise keine Deaktivierung eines Standorts oder Nodes starten, wenn die Schnittstelle eines Node für das Grid Network oder das Client Network in einer HA-Gruppe verwendet wird.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen**.

   Die Seite „Hochverfügbarkeitsgruppen“ wird angezeigt.

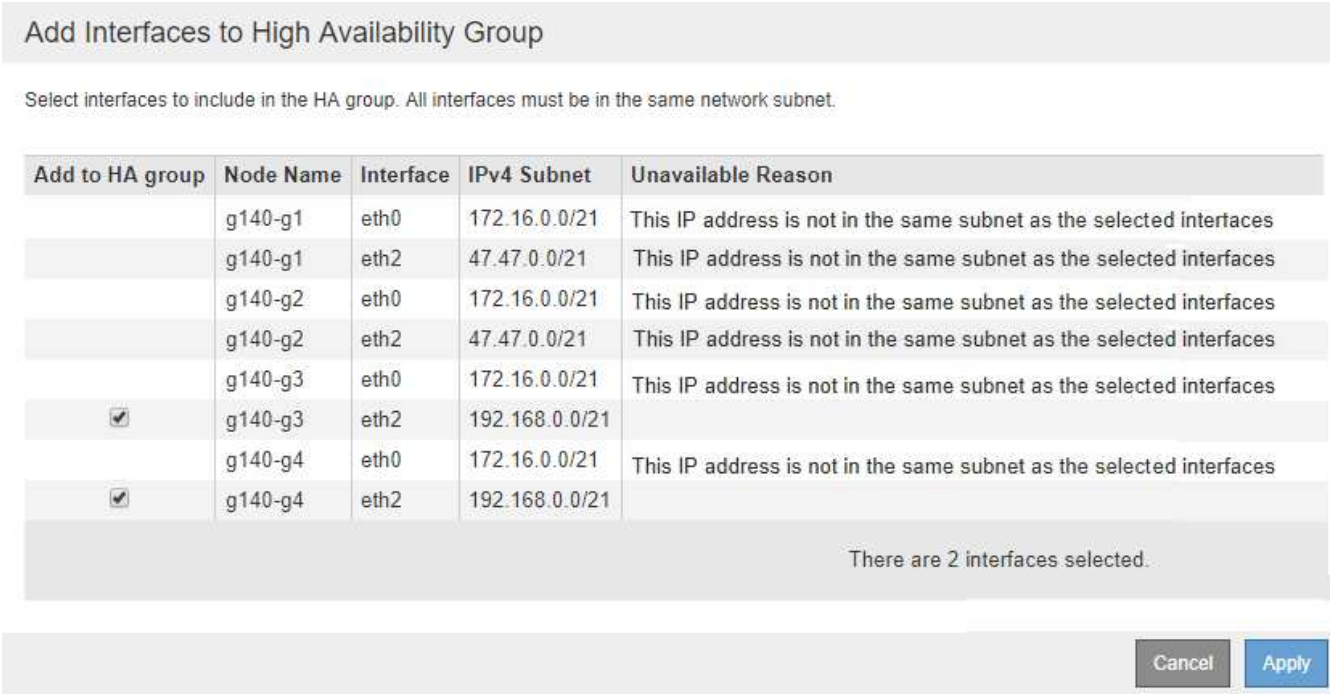


2. Wählen Sie die HA-Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

   Das Dialogfeld „High Availability Group bearbeiten“ wird angezeigt.

3. Optional können Sie den Namen oder die Beschreibung der Gruppe aktualisieren.
4. Klicken Sie optional auf **Schnittstellen auswählen**, um die Schnittstellen für die HA-Gruppe zu ändern.

   Das Dialogfeld Schnittstellen zu Hochverfügbarkeitsgruppe hinzufügen wird angezeigt.



   Eine Schnittstelle wird in der Liste nicht angezeigt, wenn ihre IP-Adresse durch DHCP zugewiesen wird.

5. Aktivieren oder deaktivieren Sie die Kontrollkästchen, um Schnittstellen hinzuzufügen oder zu entfernen.

   Beachten Sie die folgenden Richtlinien für die Auswahl von Schnittstellen:

   - Sie müssen mindestens eine Schnittstelle auswählen.
   - Wenn Sie mehrere Schnittstellen auswählen, müssen sich alle Schnittstellen entweder im Grid Network (eth0) oder im Client Network (eth2) befinden.

- Alle Schnittstellen müssen sich im gleichen Subnetz oder in Subnetzen mit einem gemeinsamen Präfix befinden.

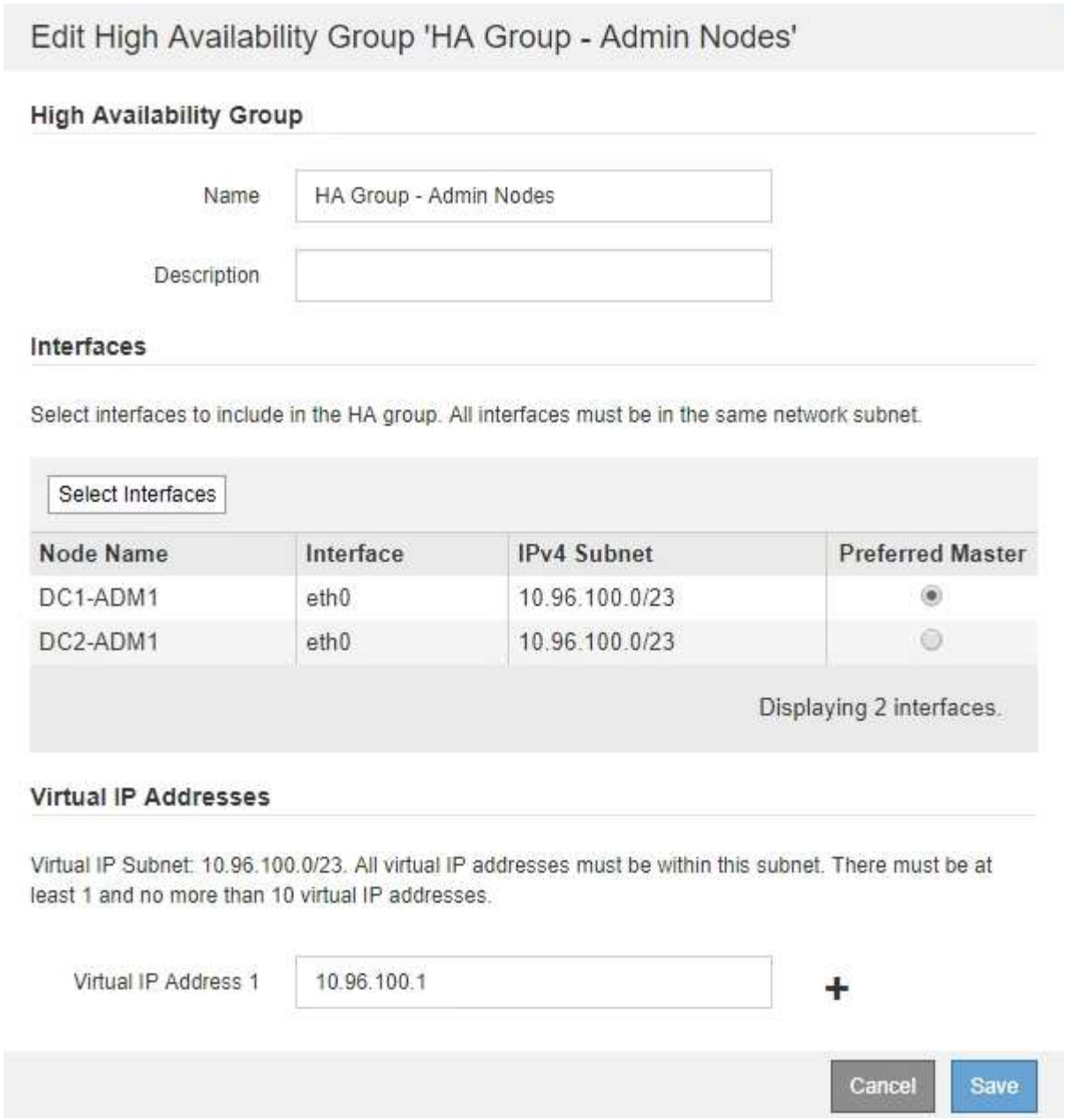
  IP-Adressen werden auf das kleinste Subnetz beschränkt (das mit dem größten Präfix).

- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen und ein Failover auftritt, sind nur die Dienste verfügbar, die für die ausgewählten Knoten gemeinsam sind.
  - Wählen Sie mindestens zwei Admin-Nodes aus, um den HA-Schutz des Grid Manager oder des Mandanten-Manager zu erhalten.
  - Wählen Sie zwei oder mehr Admin-Nodes, Gateway-Nodes oder beide aus, um den HA-Schutz des Load Balancer Service zu gewährleisten.
  - Wählen Sie mindestens zwei Gateway-Nodes aus, um den HA-Schutz des CLB-Service zu gewährleisten.

    Der CLB-Service ist veraltet.

6. Klicken Sie Auf **Anwenden**.

   Die ausgewählten Schnittstellen werden im Abschnitt Schnittstellen der Seite aufgeführt. Standardmäßig wird die erste Schnittstelle in der Liste als bevorzugter Master ausgewählt.



7. Wenn Sie eine andere Schnittstelle als bevorzugten Master auswählen möchten, wählen Sie diese Schnittstelle in der Spalte **bevorzugter Master** aus.

   Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden.

   > Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node auswählen, um der bevorzugte Master-Typ zu sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

8. Optional können Sie die virtuellen IP-Adressen für die HA-Gruppe aktualisieren.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

   IPv4-Adressen müssen sich im IPv4-Subnetz befinden, das von allen Mitgliedschnittstellen gemeinsam genutzt wird.

9. Klicken Sie Auf **Speichern**.

   Die HA-Gruppe wird aktualisiert.

Entfernen einer Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) entfernen, die Sie nicht mehr verwenden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

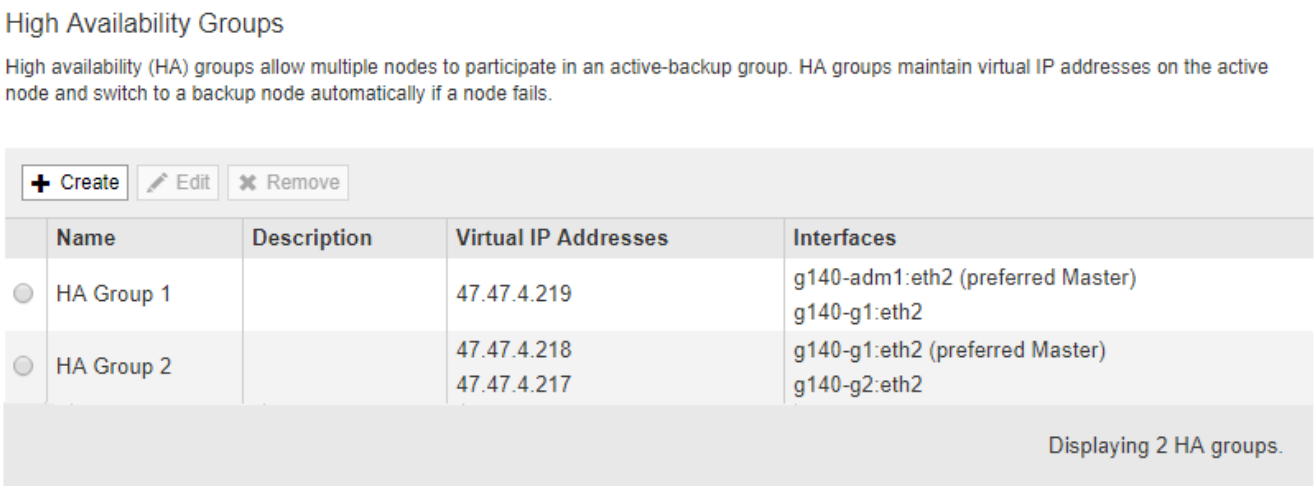
Diese Aufgabe auslassen

Wenn Sie eine HA-Gruppe entfernen, können alle S3- oder Swift-Clients, die für die Verwendung einer der virtuellen IP-Adressen der Gruppe konfiguriert sind, keine Verbindung zu StorageGRID mehr herstellen. Um Client-Unterbrechungen zu vermeiden, sollten Sie alle betroffenen S3 oder Swift Client-Applikationen aktualisieren, 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 oder bei der Verwendung von DHCP für eine Schnittstelle konfiguriert wurde.

Schritte

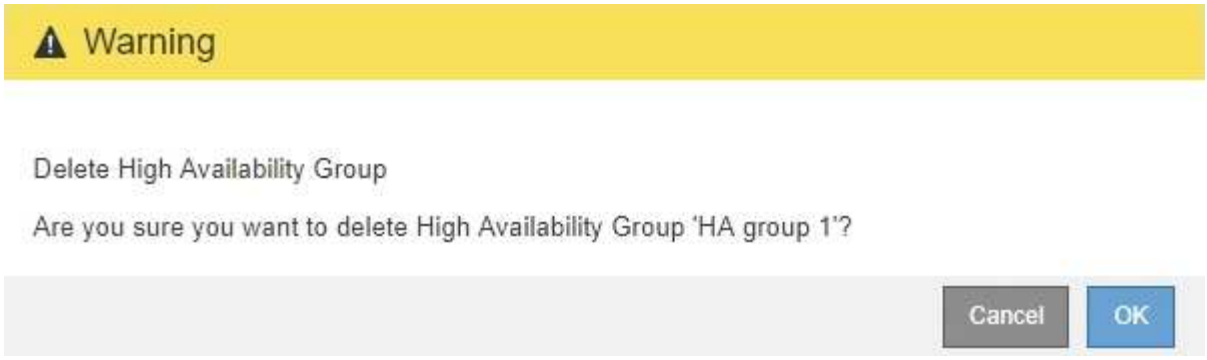
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen**.

   Die Seite „Hochverfügbarkeitsgruppen“ wird angezeigt.



2. Wählen Sie die HA-Gruppe aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.

   Die Warnung „Gruppe mit hoher Verfügbarkeit löschen“ wird angezeigt.



3. Klicken Sie auf **OK**.

   Die HA-Gruppe wird entfernt.

Konfigurieren von S3-API-Endpunkt-Domain-Namen

Um virtuelle S3-Hosted-Style-Anforderungen zu unterstützen, müssen Sie die Liste der Endpunkt-Domain-Namen, mit denen S3-Clients verbunden werden, mit konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen bestätigt haben, dass ein Grid-Upgrade nicht ausgeführt wird.

> Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, wenn ein Grid-Upgrade ausgeführt wird.

Über diese Aufgabe

Damit Clients S3-Endpunkt-Domain-Namen verwenden können, müssen Sie alle der folgenden Aufgaben ausführen:

- 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 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 von Clients zum Herstellen von Verbindungen verwendet werden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen Endpunkt-Domänennamen verweisen, einschließlich 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.

Das Zertifikat, das ein Client für HTTPS-Verbindungen verwendet, hängt davon ab, wie der Client mit dem Grid verbindet:

- Wenn ein Client eine Verbindung über den Load Balancer-Service herstellt, verwendet er das Zertifikat für einen bestimmten Load Balancer-Endpunkt.

  Jeder Load Balancer-Endpunkt verfügt über ein eigenes Zertifikat, und jeder Endpunkt kann so konfiguriert werden, dass verschiedene Endpunkt-Domain-Namen erkannt werden.

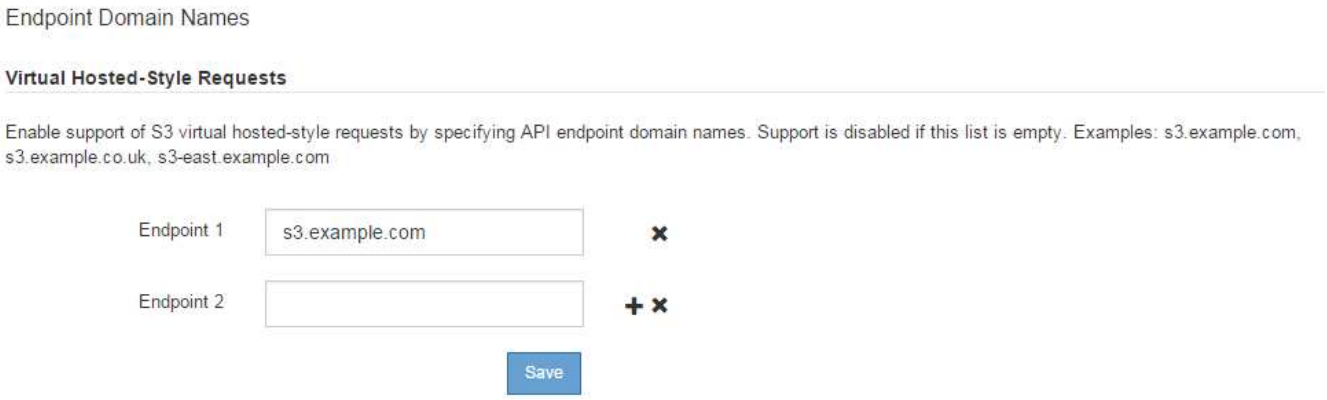
- Wenn der Client eine Verbindung zu einem Storage-Node oder zum CLB-Dienst auf einem Gateway-Node herstellt, verwendet der Client ein benutzerdefiniertes Grid-Serverzertifikat, das aktualisiert wurde, um alle erforderlichen Endpoint-Domänennamen einzuschließen.

  Der CLB-Service ist veraltet.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Domänennamen**.

   Die Seite „Endpoint Domain-Namen“ wird angezeigt.



2. Geben Sie mit dem (+)-Symbol die Liste der S3-API-Endpunktdomänennamen in die Felder **Endpunkt** ein.

   Wenn diese Liste leer ist, ist die Unterstützung für virtuelle S3-Hosted-Style-Anforderungen deaktiviert.

3. Klicken Sie Auf **Speichern**.
4. Stellen Sie sicher, dass die Serverzertifikate, die Clients verwenden, mit den erforderlichen Endpunktdomänennamen übereinstimmen.
   - Aktualisieren Sie für Clients, die den Lastverteilungsdienst verwenden, das Zertifikat, das dem Lastausgleichsendpunkt zugeordnet ist, mit dem der Client verbunden ist.
   - Aktualisieren Sie für Clients, die eine direkte Verbindung zu Speicherknoten herstellen oder den CLB-Dienst auf Gateway-Knoten verwenden, das benutzerdefinierte Serverzertifikat für das Grid.

5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass die Anforderungen für den Domänennamen des Endpunkts aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt verwenden `bucket.s3.company.com`, Der DNS-Server löst sich auf den richtigen Endpunkt und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Verwandte Informationen

"S3 verwenden"

"Anzeigen von IP-Adressen"

"Erstellen einer Hochverfügbarkeitsgruppe"

"Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst"

"Konfigurieren von Load Balancer-Endpunkten"

Aktivieren von HTTP für die Clientkommunikation

Standardmäßig verwenden Client-Anwendungen das HTTPS-Netzwerkprotokoll für alle Verbindungen zu Storage-Nodes oder zum veralteten CLB-Dienst auf Gateway-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Führen Sie diese Aufgabe nur aus, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes oder zum veralteten CLB-Service auf Gateway-Nodes herstellen müssen.

Sie müssen diese Aufgabe nicht für Clients abschließen, die nur HTTPS-Verbindungen verwenden oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (da Sie jeden Load Balancer-Endpunkt so konfigurieren können, dass entweder HTTP oder HTTPS verwendet werden). Weitere Informationen finden Sie in den Informationen zum Konfigurieren von Load Balancer-Endpunkten.

Siehe "Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen" Um zu erfahren, welche S3- und Swift-Clients beim Herstellen einer Verbindung zu Storage-Nodes oder zum veralteten CLB-Dienst über HTTP oder HTTPS verwenden

> Gehen Sie vorsichtig vor, wenn Sie HTTP für ein Produktions-Grid aktivieren, da die Anforderungen unverschlüsselt gesendet werden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Netzwerkoptionen das Kontrollkästchen **HTTP-Verbindung aktivieren**.

3. Klicken Sie Auf **Speichern**.

Verwandte Informationen

"Konfigurieren von Load Balancer-Endpunkten"

"S3 verwenden"

"Verwenden Sie Swift"

Steuern, welche Client-Operationen zulässig sind

Sie können die Option „Client Modification Grid verhindern“ auswählen, um bestimmte HTTP-Client-Vorgänge zu verweigern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

„Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option „Client-Änderung verhindern“ ausgewählt ist, werden die folgenden Anfragen verweigert:

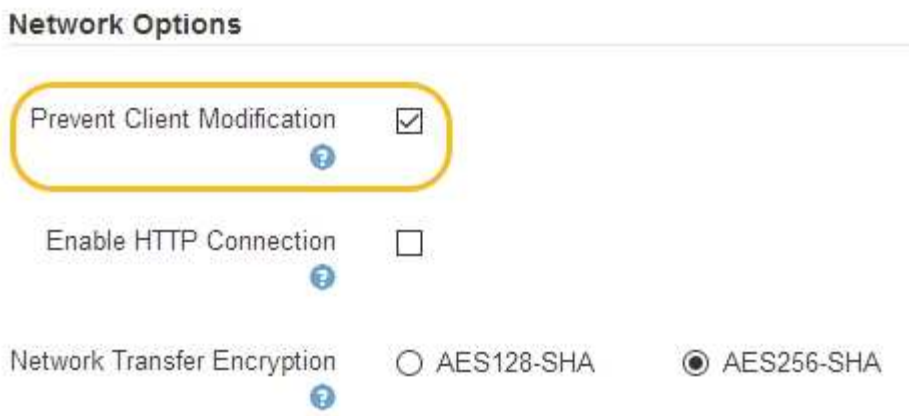
- **S3 REST API**
  - Bucket-Anforderungen löschen
  - Alle Anforderungen, die das Ändern von Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging zum Einsatz kommen

> Diese Einstellung gilt nicht für Buckets mit aktivierter Versionierung. Bei der Versionierung werden bereits Änderungen an Objektdaten, benutzerdefinierten Metadaten und Objekt-Tagging verhindert.

- **Swift REST API**
  - Container-Anforderungen löschen
  - Anträge zum Ändern vorhandener Objekte. Beispielsweise werden folgende Vorgänge verweigert: Put Overwrite, Delete, Metadata Update usw.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Netzwerkoptionen das Kontrollkästchen **Client-Änderung verhindern**.



3. Klicken Sie Auf **Speichern**.

Verwalten von StorageGRID-Netzwerken und -Verbindungen

Mit dem Grid Manager können Sie StorageGRID-Netzwerke und -Verbindungen konfigurieren und verwalten.

Siehe "Konfigurieren von S3- und Swift-Client-Verbindungen" Informationen zum Verbinden von S3 oder Swift Clients

- "Richtlinien für StorageGRID-Netzwerke"
- "Anzeigen von IP-Adressen"
- "Unterstützte Chiffren für ausgehende TLS-Verbindungen"
- "Die Netzwerkübertragungsverschlüsselung wird geändert"
- "Serverzertifikate werden konfiguriert"
- "Konfigurieren von Speicher-Proxy-Einstellungen"
- "Konfigurieren von Administrator-Proxy-Einstellungen"
- "Verwalten von Richtlinien für die Verkehrsklassifizierung"
- "Was sind Verbindungskosten"

Richtlinien für StorageGRID-Netzwerke

StorageGRID unterstützt bis zu drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass die Sicherheits- und Zugriffsanforderungen erfüllt werden.

> Informationen zum Ändern oder Hinzufügen eines Netzwerks für einen Grid-Node finden Sie in den Recovery- und Wartungsanweisungen. Weitere Informationen zur Netzwerktopologie finden Sie in den Netzwerkanweisungen.

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-Node kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Es wird ein einzelnes Gateway pro Netzwerk und pro Grid-Node unterstützt, das sich im gleichen Subnetz wie der Node befindet. Sie können bei Bedarf komplexere Routing-Lösungen im Gateway implementieren.
- Auf jedem Node ist jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

Netzwerk	Schnittstellenname
Raster	Eth0
Admin (optional)	Eth1
Client (optional)	Eth2

- Wenn der Node mit einer StorageGRID Appliance verbunden ist, werden für jedes Netzwerk bestimmte Ports verwendet. Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerät.
- Die Standardroute wird automatisch pro Knoten generiert. Wenn eth2 aktiviert ist, verwendet 0.0.0.0/0 das Client-Netzwerk auf eth2. Wenn eth2 nicht aktiviert ist, verwendet 0.0.0.0/0 das Grid-Netzwerk auf eth0.
- Das Client-Netzwerk ist erst betriebsbereit, wenn der Grid-Node dem Grid beigetreten ist
- Das Admin-Netzwerk kann während der Bereitstellung des Grid-Knotens konfiguriert werden, um den Zugriff auf die Installations-Benutzeroberfläche zu ermöglichen, bevor das Grid vollständig installiert ist.

Verwandte Informationen

"Verwalten Sie erholen"

"Netzwerkrichtlinien"

Anzeigen von IP-Adressen

Sie können die IP-Adresse für jeden Grid-Node im StorageGRID System anzeigen. Sie können diese IP-Adresse dann verwenden, um sich bei dem Grid-Node über die Befehlszeile anzumelden und verschiedene Wartungsvorgänge auszuführen.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

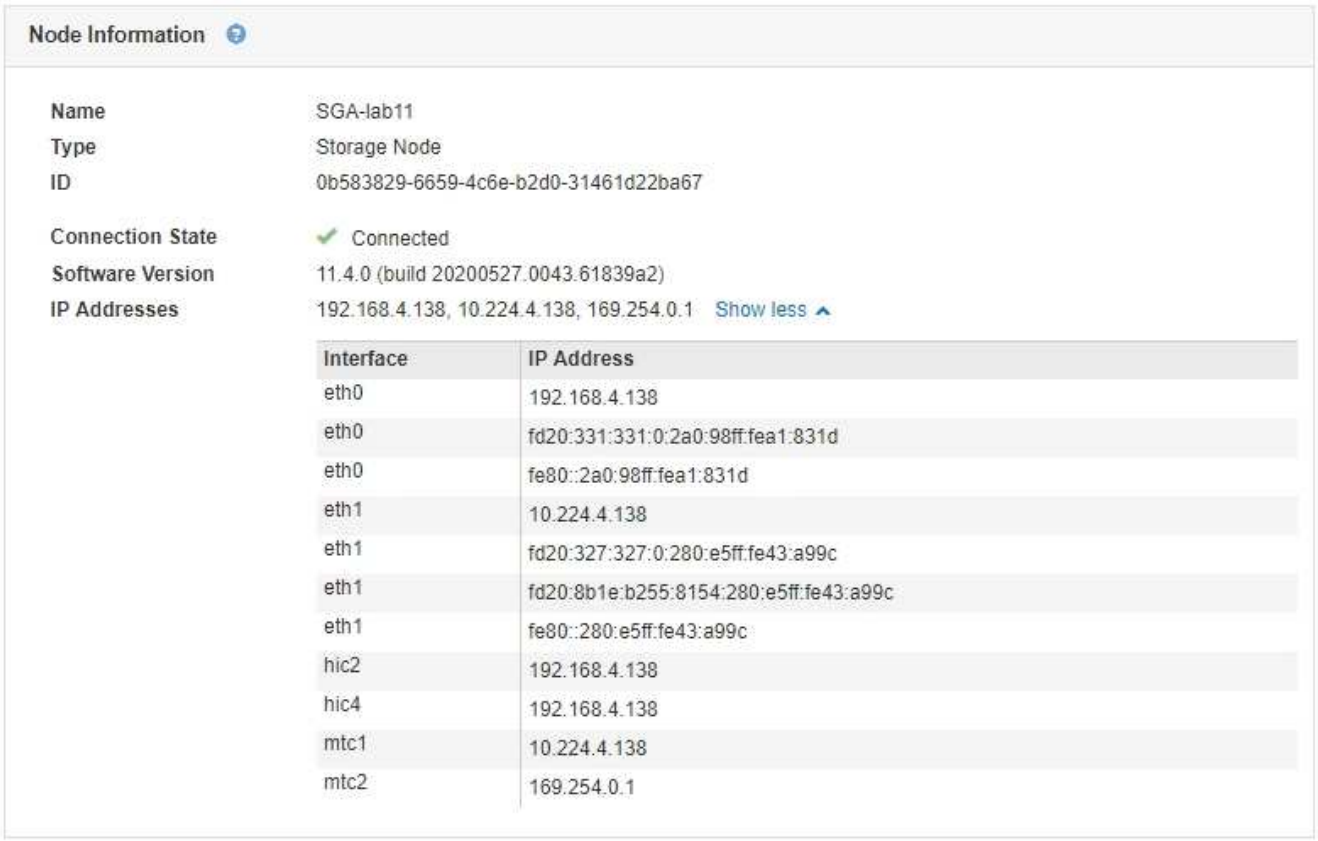
Über diese Aufgabe

Informationen zum Ändern von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.

Schritte

1. Wählen Sie **Nodes** > ***Grid Node*** > **Übersicht**.
2. Klicken Sie rechts neben dem Titel der IP-Adressen auf **Mehr anzeigen**.

   Die IP-Adressen für diesen Grid-Node werden in einer Tabelle aufgeführt.



Verwandte Informationen

"Verwalten Sie erholen"

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.

TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustausch-Algorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie spezifische Anfragen zu diesen Einstellungen haben.

Unterstützte TLS 1.2-Cipher-Suiten

Die folgenden TLS 1.2-Chiffre-Suiten werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Unterstützte TLS 1.3-Cipher-Suiten

Die folgenden TLS 1.3-Chiffre-Suiten werden unterstützt:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Die Netzwerkübertragungsverschlüsselung wird geändert

Das StorageGRID System verwendet Transport Layer Security (TLS) zum Schutz des internen Kontrolldatenverkehrs zwischen den Grid-Nodes. Die Option „Netzwerkübertragungsverschlüsselung“ legt den von TLS verwendeten Algorithmus zur Verschlüsselung der Datenverkehrskontrolle zwischen den Grid-Nodes fest. Diese Einstellung hat keine Auswirkung auf die Datenverschlüsselung.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Standardmäßig verwendet die Netzwerkübertragungsverschlüsselung den AES256-SHA-Algorithmus. Der Kontrolldatenverkehr kann auch mit dem AES128-SHA-Algorithmus verschlüsselt werden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.
2. Ändern Sie im Abschnitt Netzwerkoptionen die Netzwerkübertragungsverschlüsselung in **AES128-SHA** oder **AES256-SHA** (Standardeinstellung).

3. Klicken Sie Auf **Speichern**.

Serverzertifikate werden konfiguriert

Sie können die vom StorageGRID-System verwendeten Serverzertifikate anpassen.

Das StorageGRID System verwendet Sicherheitszertifikate für mehrere unterschiedliche Zwecke:

- Management Interface Server Certificates: Dient zum sicheren Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- Storage API Server Certificates: Dient zum sicheren Zugriff auf die Storage Nodes und Gateway Nodes, welche API-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Sie können die während der Installation erstellten Standardzertifikate verwenden oder diese Standardtypen durch Ihre eigenen benutzerdefinierten Zertifikate ersetzen.

Unterstützte Arten von benutzerdefiniertem Serverzertifikat

Das StorageGRID-System unterstützt benutzerdefinierte Serverzertifikate, die mit RSA oder ECDSA (Algorithmus für digitale Signaturen der Elliptischen Kurve) verschlüsselt sind.

Weitere Informationen dazu, wie StorageGRID Client-Verbindungen für DIE REST-API sichert, finden Sie in den S3 oder Swift-Implementierungsleitfäden.

Zertifikate für Load Balancer-Endpunkte

StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie in den Anweisungen zum Konfigurieren von Load Balancer-Endpunkten.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie Swift"

"Konfigurieren von Load Balancer-Endpunkten"

Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager

Sie können das standardmäßige StorageGRID-Serverzertifikat durch ein einzelnes benutzerdefiniertes Serverzertifikat ersetzen, das Benutzern den Zugriff auf den Grid-Manager und den Tenant-Manager ermöglicht, ohne dass Sicherheitswarnungen ausgegeben werden.

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 benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Da ein einzelnes benutzerdefiniertes Serverzertifikat für alle Administratorknoten verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients bei der Verbindung mit Grid Manager und Tenant Manager den Hostnamen 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, und je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Root CA-Zertifikat im Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen.

> Um sicherzustellen, dass die Vorgänge nicht durch ein Serverzertifikat unterbrochen werden, werden die Warnung **Ablauf des Serverzertifikats für die Managementoberfläche** und der Alarm Legacy Management Interface Certificate Expiry (MCEP) ausgelöst, wenn dieses Serverzertifikat abläuft. Nach Bedarf können Sie die Anzahl der Tage anzeigen, bis das aktuelle Service-Zertifikat abläuft, indem Sie **Support** > **Tools** > **Grid Topology** auswählen. Wählen Sie dann ***primary Admin Node*** > **CMN** > **Ressourcen** aus.

> Wenn Sie mit einem Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:
>
> - Ihr Zertifikat für den benutzerdefinierten Verwaltungsserver läuft ab.
> - Sie werden von einem Server-Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Management Interface Server Certificate auf **Benutzerdefiniertes Zertifikat installieren**.
3. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
   - **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (`.crt`).
   - **Server Certificate Private Key**: 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 Bundle**: Eine einzelne Datei, die die Zertifikate jeder Intermediate Emission Certificate Authority (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
4. Klicken Sie Auf **Speichern**.

   Die benutzerdefinierten Serverzertifikate werden für alle nachfolgenden neuen Clientverbindungen verwendet.

   Wählen Sie eine Registerkarte aus, um detaillierte Informationen zum StorageGRID-

Standardserverzertifikat oder zum hochgeladenen Zertifikat einer Zertifizierungsstelle anzuzeigen.

> Nachdem Sie ein neues Zertifikat hochgeladen haben, lassen Sie bis zu einem Tag, bis alle zugehörigen Alarme zum Ablauf des Zertifikats (oder ältere Alarme) gelöscht werden können.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Wiederherstellen der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager

Sie können auf die Verwendung der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager zurücksetzen.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Schnittstellenserverzertifikat verwalten auf **Standardzertifikate verwenden**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Wenn Sie die Standardserverzertifikate wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Die Standard-Serverzertifikate werden für alle nachfolgenden neuen Clientverbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst

Sie können das Serverzertifikat, das für S3- oder Swift-Client-Verbindungen zum Storage-Node oder zum CLB-Service (veraltet) auf Gateway-Node verwendet wird, ersetzen. 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 Benutzer möglicherweise auch das Root-CA-Zertifikat im S3- oder Swift-API-Client installieren, den sie für den Zugriff auf das System verwenden, abhängig von der Root Certificate Authority (CA), die Sie verwenden.

Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird der Alarm **Ablauf des Serverzertifikats für Storage API Endpunkte** und der Alarm Legacy Storage API Service Endpoints Certificate Expiry (SCEP) ausgelöst, wenn das Root-Server-Zertifikat abläuft. Nach Bedarf können Sie die Anzahl der Tage anzeigen, bis das aktuelle Service-Zertifikat abläuft, indem Sie **Support** > **Tools** > **Grid Topology** auswählen. Wählen Sie dann ***primary Admin Node*** > **CMN** > **Ressourcen** aus.

Die benutzerdefinierten Zertifikate werden nur verwendet, wenn Clients über den veralteten CLB-Dienst auf Gateway-Nodes eine Verbindung zu StorageGRID herstellen oder eine direkte Verbindung zu Storage-Nodes herstellen. S3- oder Swift-Clients, die über den Load Balancer Service am Admin-Nodes oder Gateway-Nodes eine Verbindung zu StorageGRID herstellen, verwenden das für den Load Balancer-Endpunkt konfigurierte Zertifikat.

Die Warnung **Ablauf des Load Balancer-Endpunktzertifikats** wird für Load Balancer-Endpunkte ausgelöst, die bald ablaufen.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte auf **Benutzerdefiniertes Zertifikat installieren**.
3. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
   - **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (`.crt`).
   - **Server Certificate Private Key**: 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 Bundle**: Eine einzelne Datei, die die Zertifikate jeder Intermediate Emission Certificate Authority (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
4. Klicken Sie Auf **Speichern**.

   Das benutzerdefinierte Serverzertifikat wird für alle nachfolgenden neuen API-Client-Verbindungen verwendet.

   Wählen Sie eine Registerkarte aus, um detaillierte Informationen zum StorageGRID-Standardserverzertifikat oder zum hochgeladenen Zertifikat einer Zertifizierungsstelle anzuzeigen.

   Nachdem Sie ein neues Zertifikat hochgeladen haben, lassen Sie bis zu einem Tag, bis alle zugehörigen Alarme zum Ablauf des Zertifikats (oder ältere Alarme) gelöscht werden können.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie Swift"

"Konfigurieren von S3-API-Endpunkt-Domain-Namen"

Wiederherstellen der Standard-Serverzertifikate für die S3- und Swift-REST-API-Endpunkte

Sie können die Standardeinstellungen für die S3- und Swift-REST-API-Endpunkte verwenden.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte auf **Standardzertifikate verwenden**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Wenn Sie die Standard-Serverzertifikate für die Endpunkte der Objekt-Storage-API wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Die Standard-Serverzertifikate werden für alle nachfolgenden neuen API-Client-Verbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Das CA-Zertifikat des StorageGRID-Systems wird kopiert

StorageGRID verwendet eine interne Zertifizierungsstelle (Certificate Authority, CA) zur Sicherung des internen Datenverkehrs. Dieses Zertifikat ändert sich nicht, wenn Sie Ihre eigenen Zertifikate hochladen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

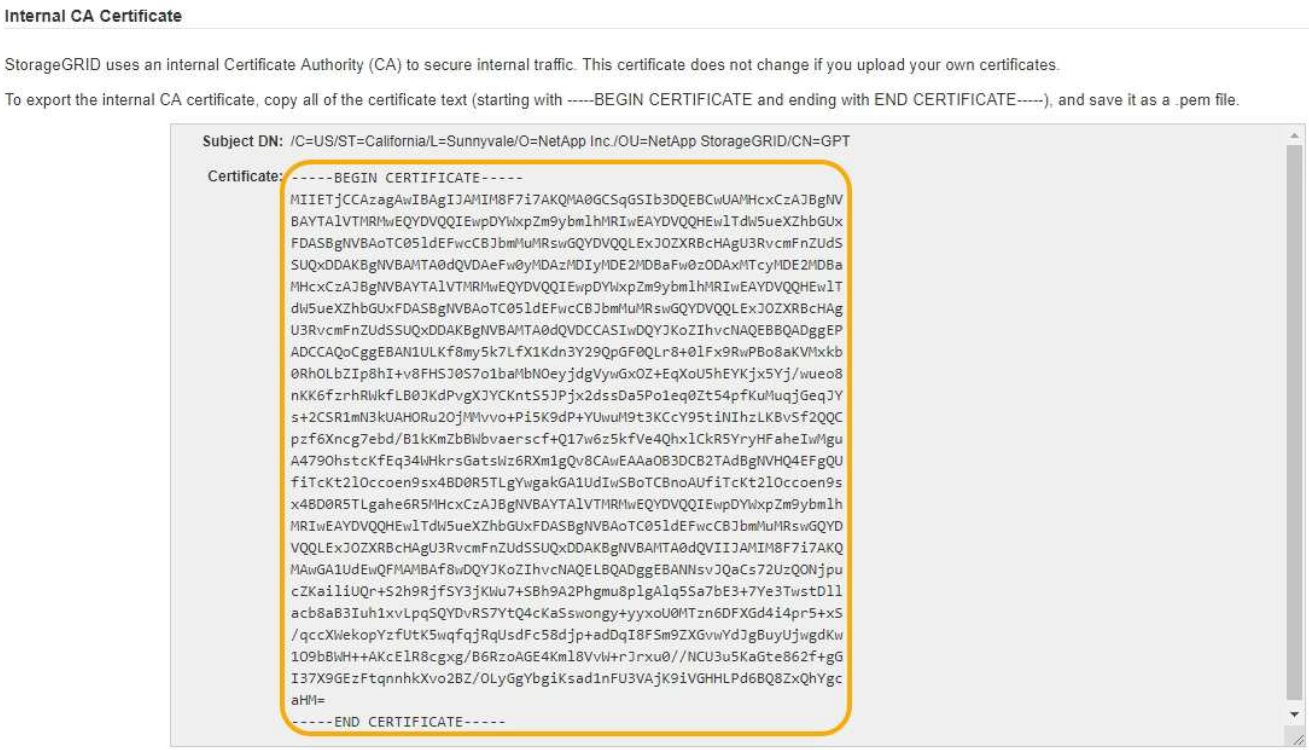
Über diese Aufgabe

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** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Wählen Sie im Abschnitt * Internes CA-Zertifikat* den gesamten Zertifikatstext aus.

   Sie müssen Folgendes einschließen `-----BEGIN CERTIFICATE-----` Und `-----END CERTIFICATE-----` Wählen Sie aus.



3. Klicken Sie mit der rechten Maustaste auf den ausgewählten Text, und wählen Sie **Kopieren**.
4. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
5. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren von StorageGRID-Zertifikaten für FabricPool

Bei S3-Clients, die eine strenge Hostname-Validierung durchführen und keine strenge Hostname-Validierung deaktivieren, z. B. ONTAP-Clients, die FabricPool verwenden, können Sie ein Serverzertifikat generieren oder hochladen, wenn Sie den Load Balancer-Endpunkt konfigurieren.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn Sie einen Load Balancer-Endpunkt erstellen, können Sie ein selbstsigniertes Serverzertifikat generieren oder ein Zertifikat hochladen, das von einer bekannten Zertifizierungsstelle (CA) signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten 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 in den Anweisungen zum Konfigurieren von StorageGRID für FabricPool.

Der separate Connection Load Balancer (CLB)-Service auf Gateway-Nodes ist veraltet und wird nicht mehr für die Verwendung mit FabricPool empfohlen.

Schritte

1. Konfigurieren Sie optional eine HA-Gruppe (High Availability, Hochverfügbarkeit) für die Verwendung von FabricPool.
2. Einen S3-Load-Balancer-Endpunkt für FabricPool erstellen.

   Wenn Sie einen HTTPS-Load-Balancer-Endpunkt erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, den privaten Zertifikatschlüssel und das CA-Bundle hochzuladen.

3. Fügen Sie StorageGRID als Cloud-Tier in ONTAP bei.

   Geben Sie den Endpunkt-Port des Load Balancer und den vollständig qualifizierten Domänennamen an, der im hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat ein.

   Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zertifikat der Zwischenzertifizierungsstelle vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.

Verwandte Informationen

"Konfigurieren Sie StorageGRID für FabricPool"

Erstellen eines selbstsignierten Serverzertifikats für die Managementoberfläche

Sie können ein Skript verwenden, um ein selbstsigniertes Serverzertifikat für Management-API-Clients zu generieren, die eine strenge Hostnamen-Validierung erfordern.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle (CA) 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.

Schritte

1. Ermitteln Sie den vollständig qualifizierten Domänennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

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

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

   - Für `--domains`, Verwenden Sie Platzhalter, um die vollständig qualifizierten Domänennamen aller Admin-Knoten darzustellen. Beispiel: `*.ui.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com`.
   - Einstellen `--type` Bis `management` Zum Konfigurieren des Zertifikats, 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-API-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 365
```

   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** > **Server Certificates** > **Management Interface Server Certificate** Aus.
7. Konfigurieren Sie den Management-API-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.

Konfigurieren von 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.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

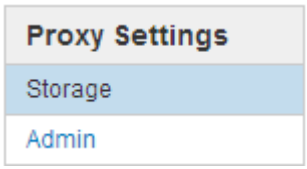
Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

Schritte

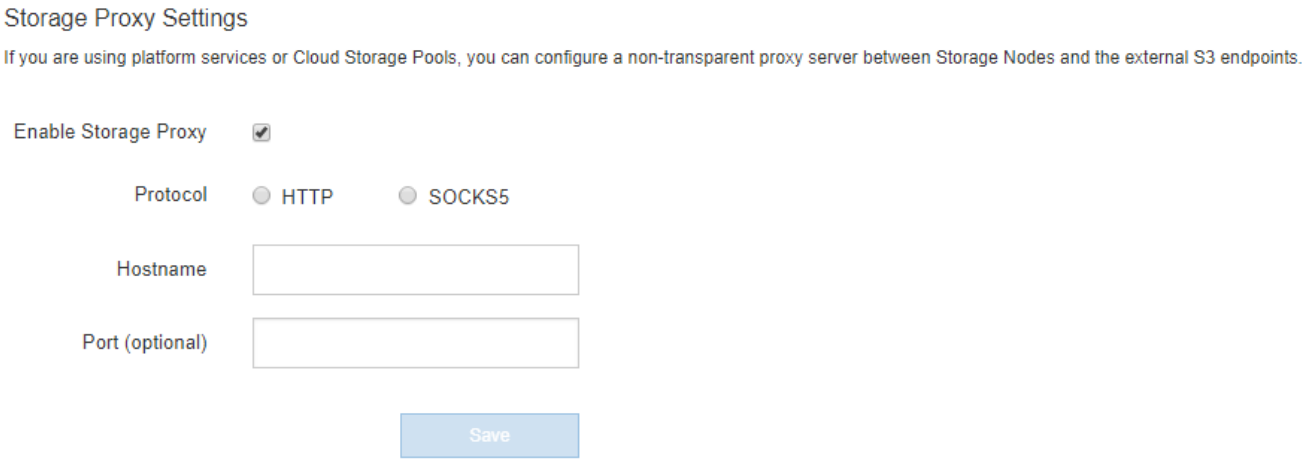
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Proxy-Einstellungen**.

   Die Seite Speicher-Proxy-Einstellungen wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.



2. Aktivieren Sie das Kontrollkästchen * Storage Proxy aktivieren*.

   Die Felder zum Konfigurieren eines Speicher-Proxys werden angezeigt.



3. Wählen Sie das Protokoll für den nicht-transparenten Speicher-Proxy aus.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie optional den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.

   Sie können dieses Feld leer lassen, wenn Sie den Standardport für das Protokoll verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Klicken Sie Auf **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 möchten, deaktivieren Sie das Kontrollkästchen **Storage Proxy aktivieren** und klicken Sie auf **Speichern**.

Verwandte Informationen

"Networking und Ports für Plattform-Services"

"Objektmanagement mit ILM"

Konfigurieren von Administrator-Proxy-Einstellungen

Wenn Sie AutoSupport-Meldungen über HTTP oder HTTPS senden, können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und dem technischen Support (AutoSupport) konfigurieren.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

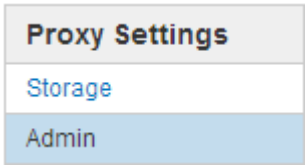
Sie können die Einstellungen für einen einzigen Admin-Proxy konfigurieren.

Schritte

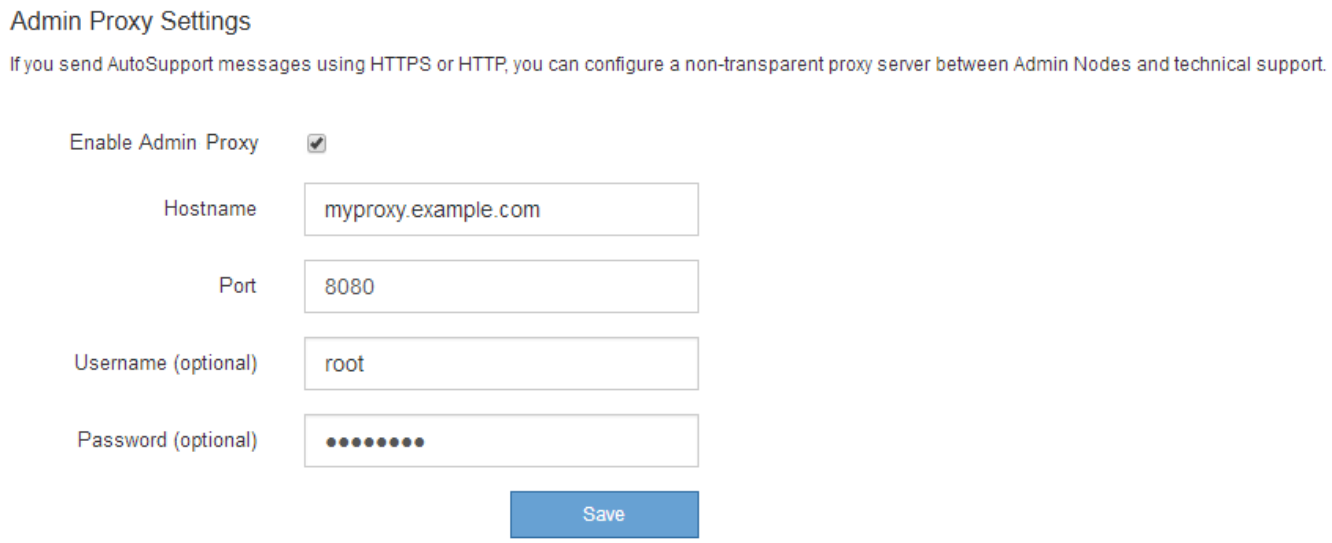
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Proxy-Einstellungen**.

   Die Seite Admin Proxy Settings wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.

2. Wählen Sie im Sidebar-Menü die Option **Admin**.



3. Aktivieren Sie das Kontrollkästchen * Admin Proxy aktivieren*.



4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie den Port ein, der für die Verbindung mit dem Proxy-Server verwendet wird.
6. Geben Sie optional den Proxy-Benutzernamen ein.

   Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server keinen Benutzernamen benötigt.

7. Geben Sie optional das Proxy-Kennwort ein.

   Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server kein Passwort benötigt.

8. Klicken Sie Auf **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 klicken Sie auf **Speichern**.

Verwandte Informationen

"Angeben des Protokolls für AutoSupport Meldungen"

Verwalten von Richtlinien für die Verkehrsklassifizierung

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.

Passende Regeln und optionale Grenzen

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
- Mandanten
- Subnetze (IPv4-Subnetze, in denen der Client enthalten ist)
- Endpunkte (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.

Optional können Sie Obergrenzen für eine Richtlinie auf Basis der folgenden Parameter festlegen:

- Aggregat-Bandbreite In
- Horizontale Aggregatbandbreite
- Gleichzeitige Leseanforderungen
- Anforderungen Für Gleichzeitige Schreibvorgänge
- Bandbreite Pro Anfrage In
- Bandbreitenausforderung Pro Anfrage
- Leseanforderungsrate
- Schreibanforderungen-Rate

> 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.

Traffic-Beschränkung

Wenn Sie Traffic-Klassifizierungsrichtlinien erstellt haben, ist der Datenverkehr entsprechend der von Ihnen festgelegten Regeln und Grenzen begrenzt. 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. 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.

Verwendung von 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.

Pro Load Balancer werden Einschränkungen für die Verkehrsklassifizierung implementiert. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.

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	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

Erstellen von Richtlinien zur Verkehrsklassifizierung

Sie erstellen Traffic-Klassifizierungsrichtlinien, wenn Sie den Netzwerkverkehr nach Bucket, Mandanten, IP-Subnetz oder Load Balancer-Endpunkt überwachen und optional begrenzen möchten. Optional können Sie Obergrenzen für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anfragen oder der Anfragerate festlegen.

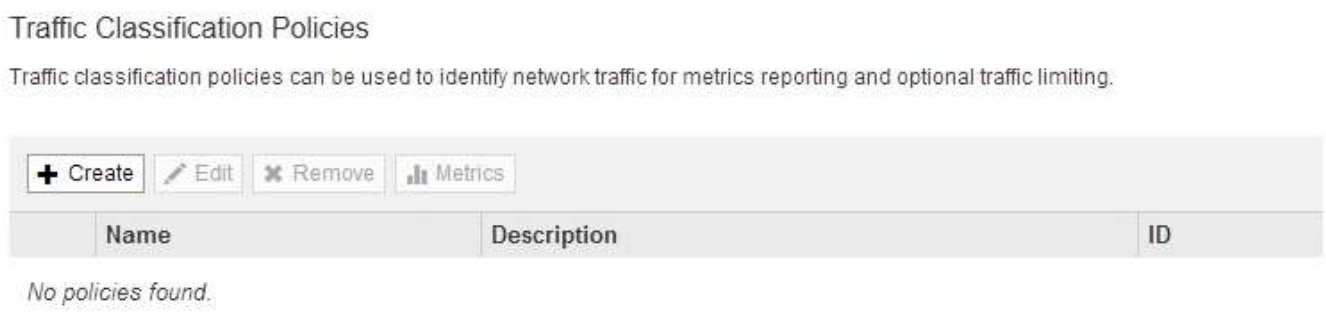
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen alle Load Balancer-Endpunkte erstellt haben, die übereinstimmen sollen.
- Sie müssen alle Mandanten erstellt haben, denen Sie entsprechen möchten.

Schritte

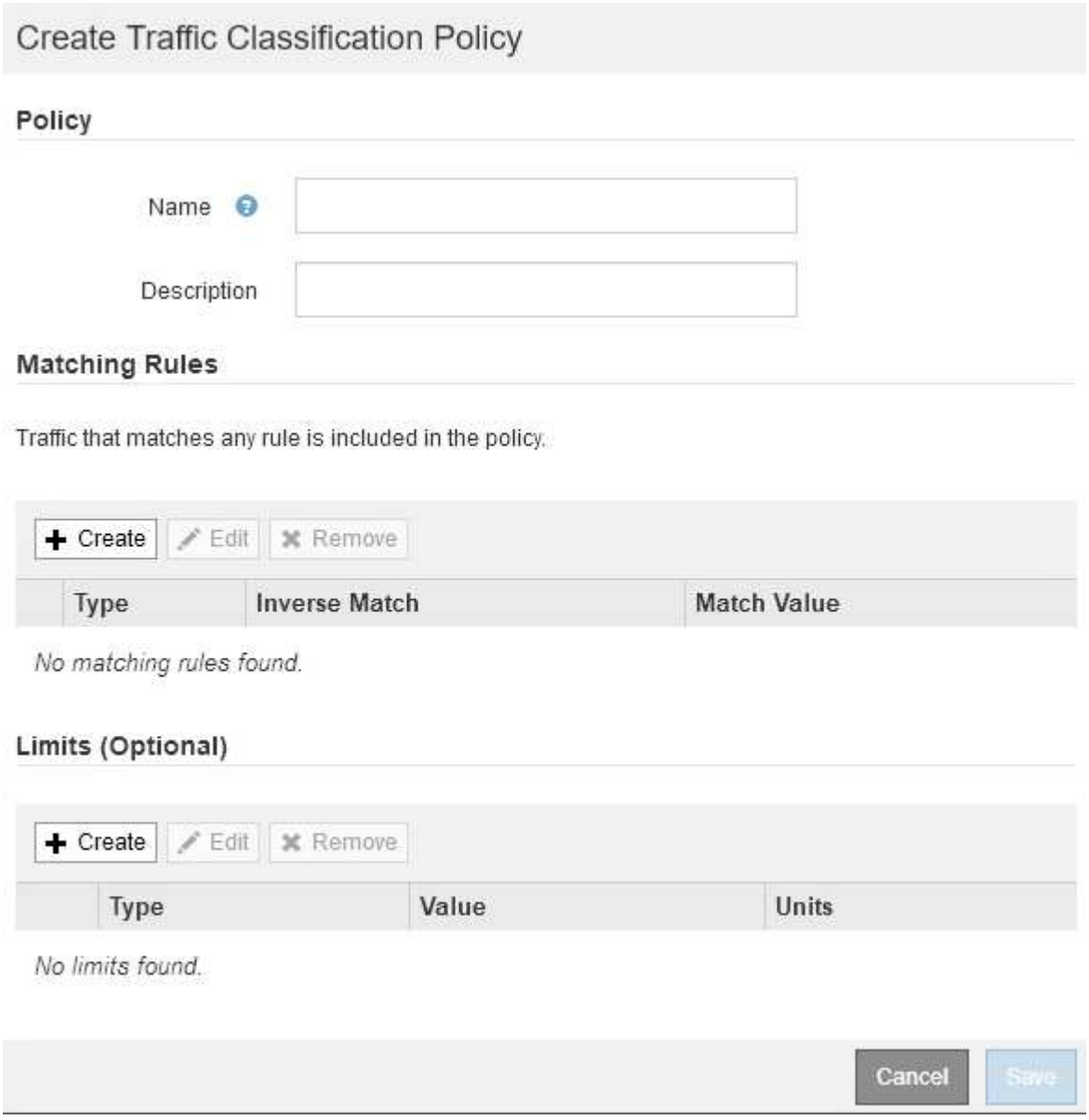
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt.



2. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld Richtlinie zur Verkehrsklassifizierung erstellen wird angezeigt.



3. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.

   Geben Sie einen beschreibenden Namen ein, damit Sie die Richtlinie erkennen können.

4. Fügen Sie optional eine Beschreibung für die Richtlinie im Feld **Beschreibung** hinzu.

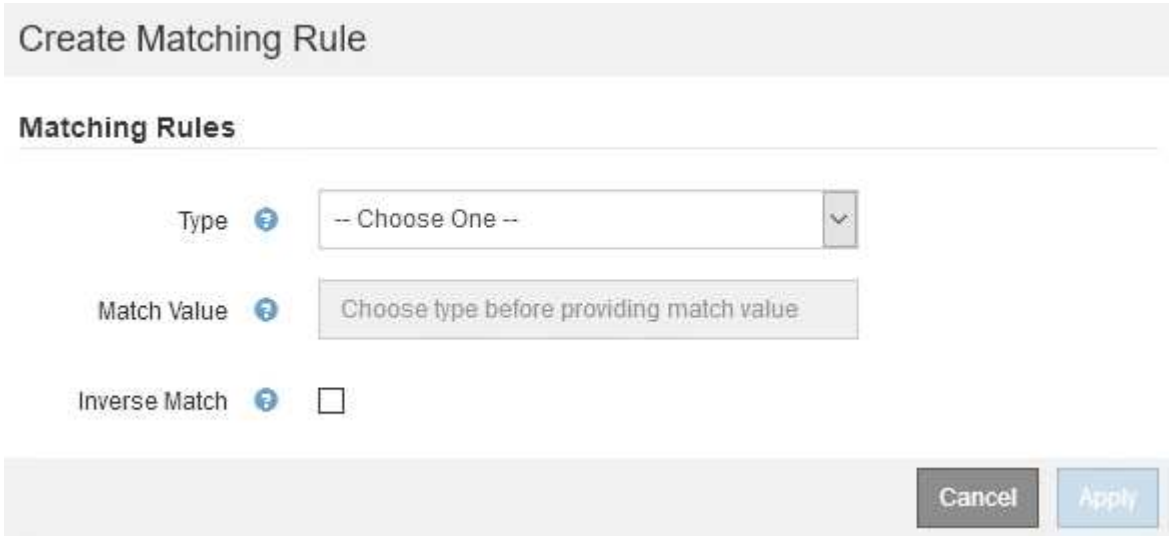
   Beschreiben Sie beispielsweise, auf welche Weise diese Richtlinie zur Klassifizierung von Verkehrsdaten zutrifft und welche Begrenzung sie hat.

5. Erstellen Sie eine oder mehrere passende Regeln für die Richtlinie.

   Die übereinstimmenden Regeln steuern, welche Einheiten von dieser Traffic-Klassifizierungsrichtlinie betroffen sein werden. Wählen Sie beispielsweise Tenant aus, wenn diese Richtlinie auf den Netzwerkverkehr für einen bestimmten Mandanten angewendet werden soll. Oder wählen Sie Endpunkt aus, wenn diese Richtlinie auf den Netzwerkverkehr auf einem bestimmten Load Balancer-Endpunkt angewendet werden soll.

   a. Klicken Sie im Abschnitt **passende Regeln** auf **Erstellen**.

      Das Dialogfeld „passende Regel erstellen“ wird angezeigt.



   b. Wählen Sie im Dropdown-Menü **Typ** den Typ der Entität aus, die in die übereinstimmende Regel aufgenommen werden soll.
   c. Geben Sie im Feld **Match-Wert** einen Match-Wert basierend auf dem gewählten Entitätstyp ein.
      - Bucket: Geben Sie einen Bucket-Namen ein.
      - Bucket-Regex: Geben Sie einen regulären Ausdruck ein, der für eine Reihe von Bucket-Namen verwendet wird.

        Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den ^-Anker, um am Anfang des Bucket-Namens zu entsprechen, und verwenden Sie den €-Anker, um am Ende des Namens zu entsprechen.

      - CIDR: Geben Sie ein IPv4-Subnetz in CIDR-Notation ein, das dem gewünschten Subnetz entspricht.
      - Endpunkt: Wählen Sie einen Endpunkt aus der Liste der vorhandenen Endpunkte aus. Dies sind die Load Balancer Endpunkte, die Sie auf der Seite Load Balancer Endpoints definiert haben.
      - Mandant: Wählen Sie einen Mandanten aus der Liste der bestehenden Mandanten aus. Die Zuordnung von Mandanten basiert auf dem Besitz des Buckets, auf dem zugegriffen wird. Der anonyme Zugriff auf einen Bucket entspricht dem Mandanten, der den Bucket besitzt.

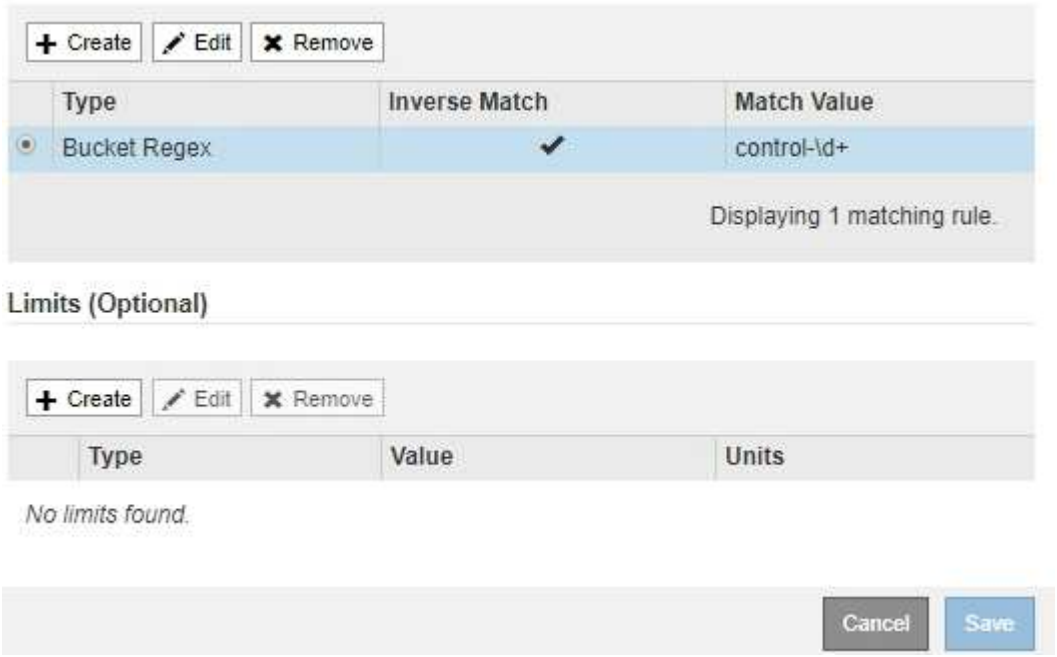
d. Wenn Sie dem gesamten Netzwerkverkehr *außer* Traffic entsprechen möchten, der mit dem gerade definierten Typ- und Vergleichswert übereinstimmt, aktivieren Sie das Kontrollkästchen **inverse**. Lassen Sie andernfalls das Kontrollkästchen nicht ausgewählt.

   Wenn diese Richtlinie beispielsweise auf alle Endpunkte des Load Balancer angewendet werden soll, geben Sie den zu ausgeschlossenen Endpunkt für den Load Balancer an und wählen Sie **Inverse** aus.

   Bei einer Richtlinie, die mehrere Matriken enthält, bei denen mindestens eine inverse Matrix ist, sollten Sie darauf achten, keine Richtlinie zu erstellen, die allen Anforderungen entspricht.

e. Klicken Sie Auf **Anwenden**.

   Die Regel wird erstellt und in der Tabelle Abpassende Regeln aufgeführt.



a. Wiederholen Sie diese Schritte für jede Regel, die Sie für die Richtlinie erstellen möchten.

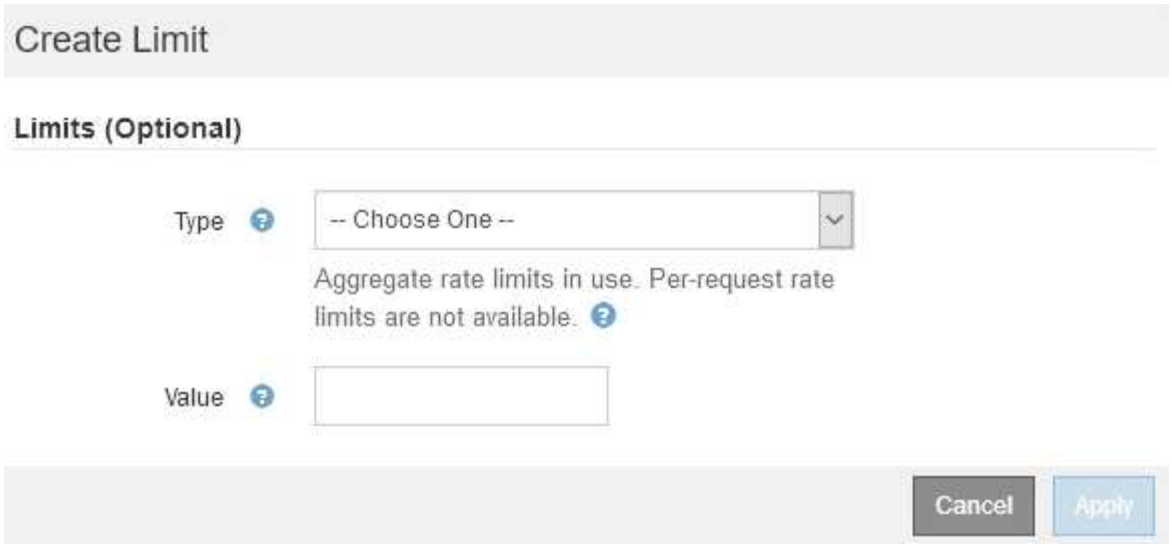
   Datenverkehr, der einer Regel entspricht, wird von der Richtlinie übernommen.

6. Optional können Grenzen für die Richtlinie erstellt werden.

   Selbst wenn Sie keine Grenzen erstellen, sammelt StorageGRID Metriken, sodass Sie den Netzwerk-Traffic, der der Richtlinie entspricht, überwachen können.

a. Klicken Sie im Abschnitt **Limits** auf **Erstellen**.

   Das Dialogfeld Limit erstellen wird angezeigt.



b. Wählen Sie im Dropdown-Menü **Typ** den Grenzwert aus, den Sie auf die Richtlinie anwenden möchten.

   In der folgenden Liste bezieht sich **in** auf Datenverkehr von S3- oder Swift-Clients auf den StorageGRID-Load-Balancer, und **out** bezieht sich auf den Datenverkehr vom Load Balancer auf S3- oder Swift-Clients.

   - Aggregat-Bandbreite In
   - Horizontale Aggregatbandbreite
   - Gleichzeitige Leseanforderungen
   - Anforderungen Für Gleichzeitige Schreibvorgänge
   - Bandbreite Pro Anfrage In
   - Bandbreitenausforderung Pro Anfrage
   - Leseanforderungsrate
   - Schreibanforderungen-Rate

   > 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 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 „`Best`"-Übereinstimmungen für Bandbreiteneinschränkungen in der folgenden Reihenfolge:

   - Exakte IP-Adresse (/32-Maske)
   - Exakter Bucket-Name
   - Eimer-Regex
   - Mandant

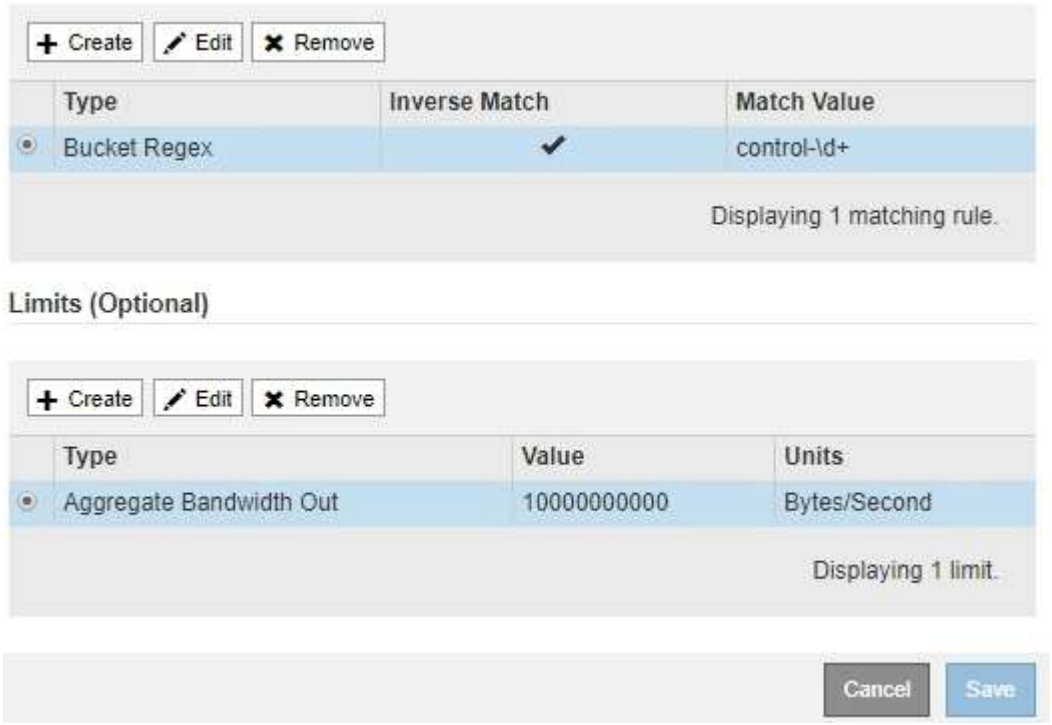
- Endpunkt
- Nicht exakte CIDR-Übereinstimmungen (nicht /32)
- Umgekehrte Übereinstimmungen

c. Geben Sie im Feld **Wert** einen numerischen Wert für den gewählten Grenzwert ein.

   Die erwarteten Einheiten werden angezeigt, wenn Sie ein Limit auswählen.

d. Klicken Sie Auf **Anwenden**.

   Die Begrenzung wird erstellt und in der Grenzwertetabelle aufgelistet.



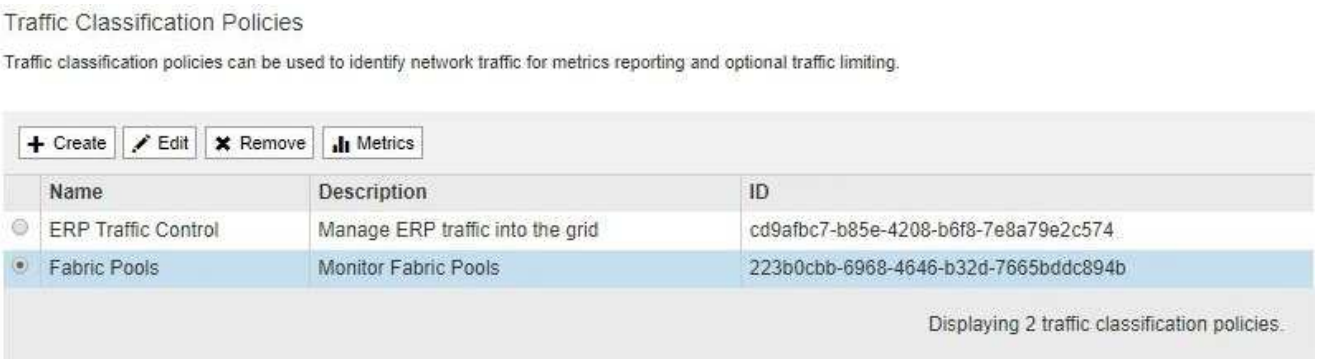
e. Wiederholen Sie diese Schritte für jedes Limit, das Sie der Richtlinie hinzufügen möchten.

   Wenn Sie beispielsweise ein Bandbreitenlimit von 40 Gbit/s für eine SLA-Ebene erstellen möchten, erstellen Sie eine aggregierte Bandbreitennutzung und ein Bandbreitenlimit und legen Sie jede auf 40 Gbit/s fest.

> Um Megabyte pro Sekunde in Gigabit pro Sekunde zu konvertieren, multiplizieren Sie mit acht. Beispielsweise entspricht 125 MB/s 1,000 Mbit/s oder 1 Gbit/s.

7. Wenn Sie mit dem Erstellen von Regeln und Grenzen fertig sind, klicken Sie auf **Speichern**.

   Die Richtlinie wird gespeichert und in der Tabelle „Richtlinien zur Klassifizierung von Verkehrsdaten“ aufgeführt.



Der S3- und Swift-Client-Traffic wird nun gemäß den Traffic-Klassifizierungsrichtlinien gehandhabt. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Verwandte Informationen

"Managen des Lastausgleichs"

"Anzeigen von Metriken zum Netzwerkverkehr"

Bearbeiten einer Traffic-Klassifizierungsrichtlinie

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.

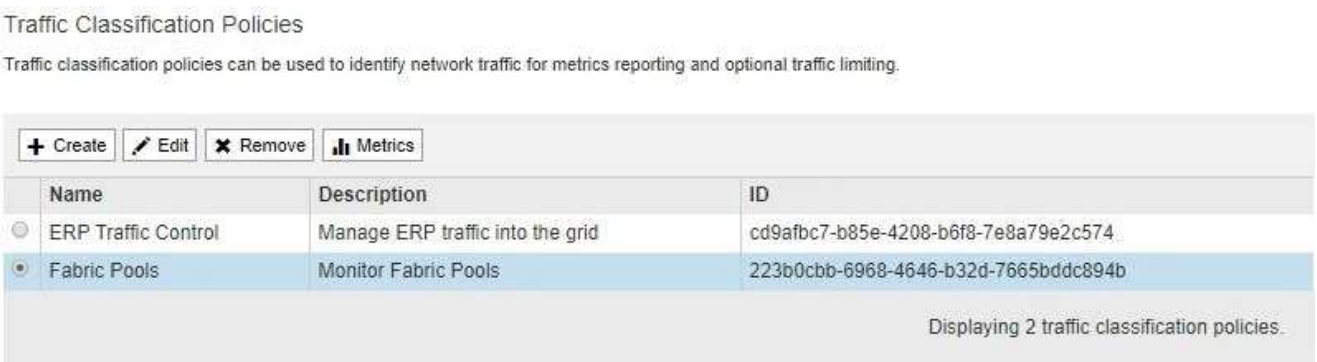
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Schritte

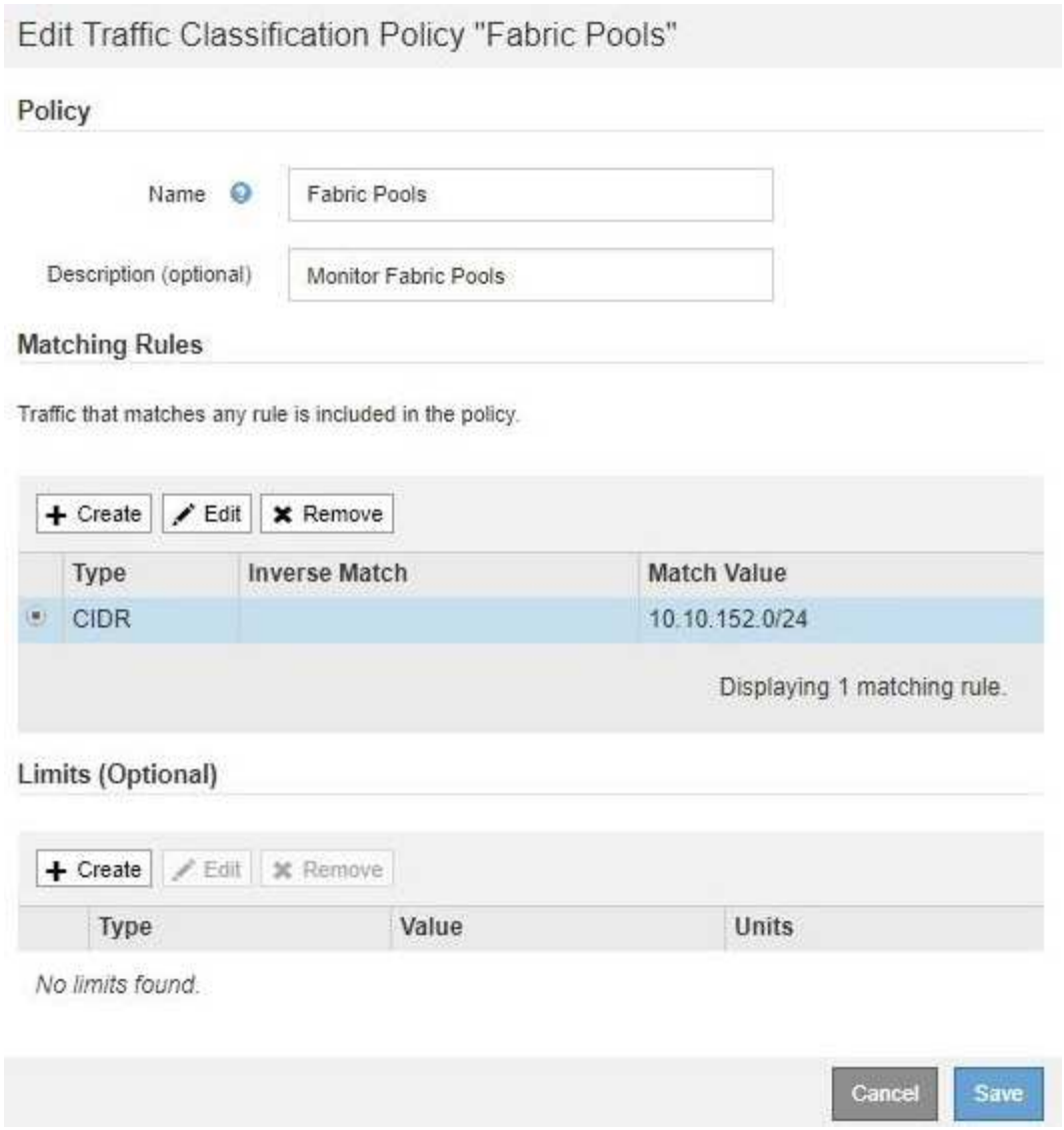
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



2. Wählen Sie das Optionsfeld links neben der Richtlinie, die Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.

   Das Dialogfeld Richtlinie zur Klassifizierung von Datenverkehr bearbeiten wird angezeigt.



4. Erstellen, Bearbeiten oder Entfernen übereinstimmender Regeln und Grenzen nach Bedarf.
   a. Um eine übereinstimmende Regel oder ein entsprechendes Limit zu erstellen, klicken Sie auf **Erstellen** und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
   b. Um eine passende Regel oder Grenze zu bearbeiten, wählen Sie die Optionsschaltfläche für die Regel oder das Limit aus, klicken Sie im Abschnitt **passende Regeln** oder im Abschnitt **Grenzen** auf **Bearbeiten** und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
   c. Um eine passende Regel oder Begrenzung zu entfernen, wählen Sie die Optionsschaltfläche für die Regel oder die Begrenzung aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie die Regel oder das Limit entfernen möchten.
5. Wenn Sie mit dem Erstellen oder Bearbeiten einer Regel oder eines Limits fertig sind, klicken Sie auf **Anwenden**.
6. Wenn Sie mit der Bearbeitung der Richtlinie fertig sind, klicken Sie auf **Speichern**.

   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

Wenn Sie keine Traffic-Klassifizierungsrichtlinie mehr benötigen, können Sie sie löschen.

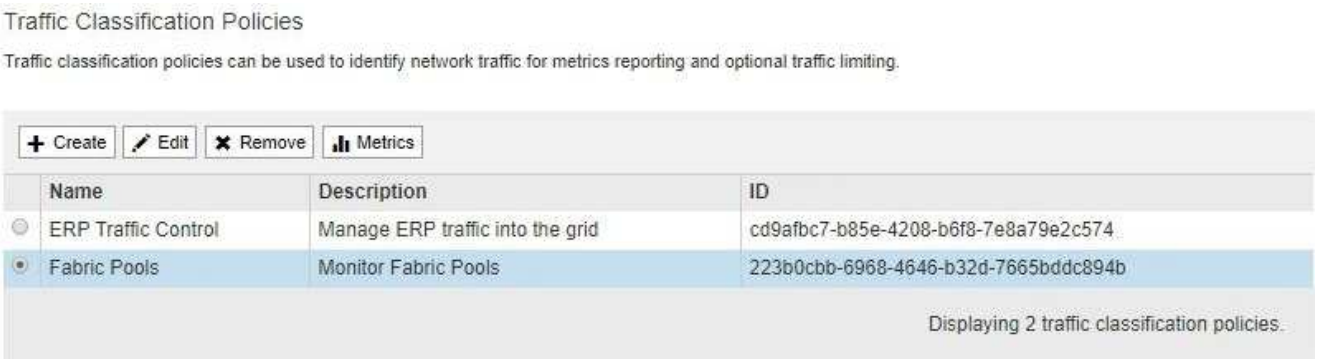
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



2. Wählen Sie das Optionsfeld links neben der Richtlinie, die Sie löschen möchten.
3. Klicken Sie Auf **Entfernen**.

   Ein Warndialogfeld wird angezeigt.

4. Klicken Sie auf **OK**, um zu bestätigen, dass Sie die Richtlinie löschen möchten.

   Die Richtlinie wird gelöscht.

Anzeigen von Metriken zum Netzwerkverkehr

Sie können den Netzwerkverkehr überwachen, indem Sie die Diagramme aufrufen, die auf der Seite Richtlinien zur Klassifizierung von Verkehrsmeldungen verfügbar sind.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

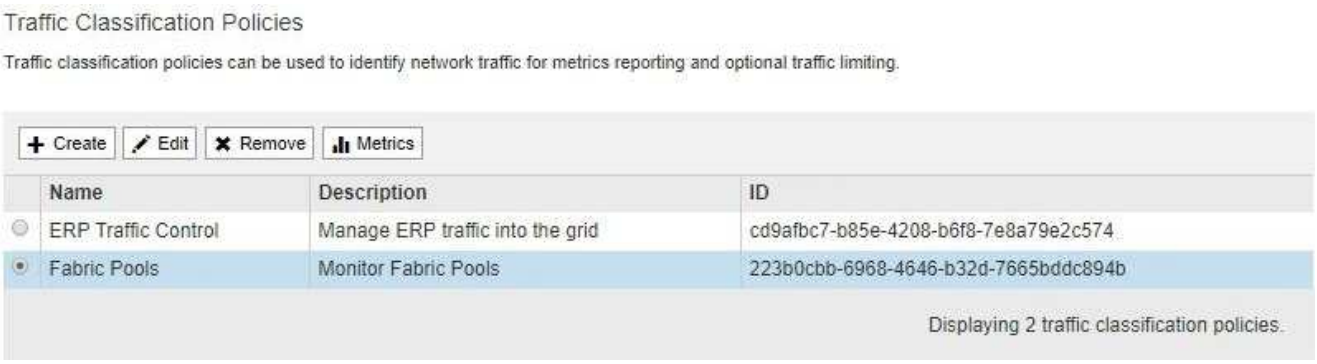
Für alle vorhandenen Traffic-Klassifizierungsrichtlinien können Sie Kennzahlen für den Load Balancer-Service anzeigen, um festzustellen, ob die Richtlinie den Datenverkehr im Netzwerk erfolgreich einschränkt. Anhand der Daten in den Diagrammen können Sie bestimmen, ob Sie die Richtlinie anpassen müssen.

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 **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



2. Wählen Sie das Optionsfeld links neben der Richtlinie, für die Sie Metriken anzeigen möchten.
3. Klicken Sie Auf **Metriken**.

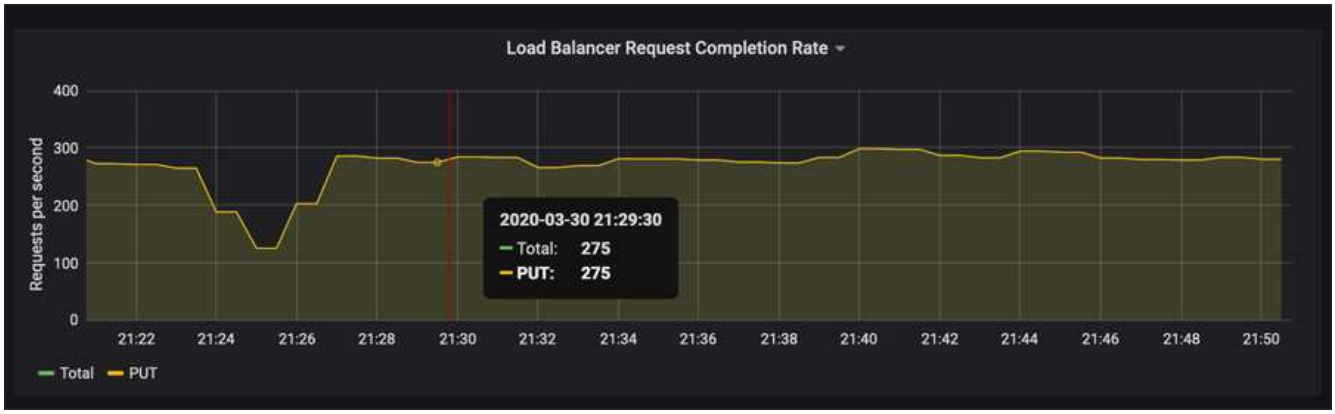
   Es wird ein neues Browserfenster geöffnet, und die Diagramme der Richtlinie zur Klassifizierung von Datenverkehr werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

   Sie können andere Richtlinien auswählen, die Sie anzeigen möchten, indem Sie das Pulldown-Menü **Policy** verwenden.

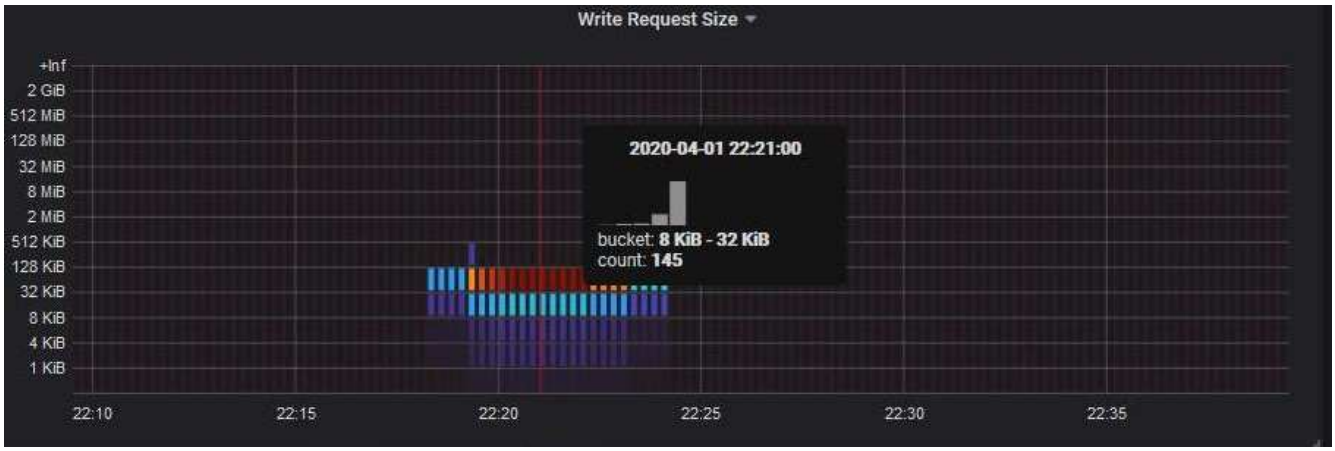
Die folgenden Diagramme sind auf der Webseite enthalten.

- Load Balancer Request Traffic: Dieses Diagramm liefert einen 3-minütigen Moving Average des Durchsatzes von Daten, die zwischen Load Balancer Endpunkten und den Clients, die die Anforderungen bearbeiten, in Bits pro Sekunde übertragen werden.
- Abschlusssatz für Lastbalancer-Anfragen: Dieses Diagramm bietet einen 3-minütigen Moving-Durchschnitt der Anzahl der abgeschlossenen Anfragen pro Sekunde, aufgeschlüsselt nach Anforderungstyp (GET, PUT, HEAD, DELETE). Dieser Wert wird aktualisiert, wenn die Kopfzeilen einer neuen Anfrage validiert wurden.
- Fehlerantwortzrate: Dieses Diagramm zeigt einen 3-minütigen Moving Average der Anzahl der an Kunden pro Sekunde zurückgegebenen Fehlerantworten, aufgeschlüsselt nach dem Fehlercode.
- Durchschnittliche Anfragedauer (nicht-Fehler): Dieses Diagramm bietet einen 3-minütigen Moving Average of Request durations, aufgeschlüsselt nach Anforderungstyp (GET, PUT, HEAD, DELETE). Jede Anforderungsdauer beginnt, wenn eine Anforderungs-Kopfzeile vom Lastbalancer-Dienst analysiert wird und endet, wenn der vollständige Antwortkörper an den Client zurückgesendet wird.
- Schreibanforderungsrate nach Objektgröße: Diese Heatmap bietet einen Moving Average von 3 Minuten für die Geschwindigkeit, mit der Schreibanforderungen basierend auf Objektgröße abgeschlossen werden. In diesem Zusammenhang beziehen sich Schreibanforderungen nur auf PUT-Anforderungen.
- Leseanforderungsrate nach Objektgröße: Dieser Heatmap bietet einen 3-minütigen Moving-Durchschnitt der Rate, mit der Leseanforderungen anhand der Objektgröße abgeschlossen werden. In diesem Zusammenhang beziehen sich Leseanforderungen nur auf ANFORDERUNGEN, DIE ABGERUFEN werden sollen. Die Farben in der Heatmap zeigen die relative Frequenz einer Objektgröße innerhalb eines einzelnen Diagramms an. Die kühleren Farben (z. B. violett und blau) zeigen niedrigere relative Raten an, und die wärmeren Farben (z. B. Orange und Rot) zeigen höhere relative Raten an.

4. Bewegen Sie den Cursor über ein Liniendiagramm, um ein Popup-Fenster mit Werten auf einem bestimmten Teil des Diagramms anzuzeigen.



5. Bewegen Sie den Mauszeiger über eine Heatmap, um ein Popup-Fenster mit Datum und Uhrzeit der Probe, Objektgrößen, die in die Anzahl aggregiert werden, und die Anzahl der Anfragen pro Sekunde in diesem Zeitraum anzuzeigen.



6. Verwenden Sie das Pull-down-Menü **Policy** oben links, um eine andere Richtlinie auszuwählen.

   Die Diagramme für die ausgewählte Richtlinie werden angezeigt.

7. Alternativ können Sie über das Menü * Support* auf die Diagramme zugreifen.
   a. Wählen Sie **Support** > **Tools** > **Metriken**.
   b. Wählen Sie im Abschnitt **Grafana** der Seite die Option **Traffic Classification Policy** aus.
   c. Wählen Sie die Richtlinie aus der Dropdown-Liste oben links auf der Seite aus.

      Richtlinien für die Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs sind auf der Seite Richtlinien zur Klassifizierung von Verkehrsdaten aufgeführt.

8. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

Verwandte Informationen

"Monitor Fehlerbehebung"

Was sind Verbindungskosten

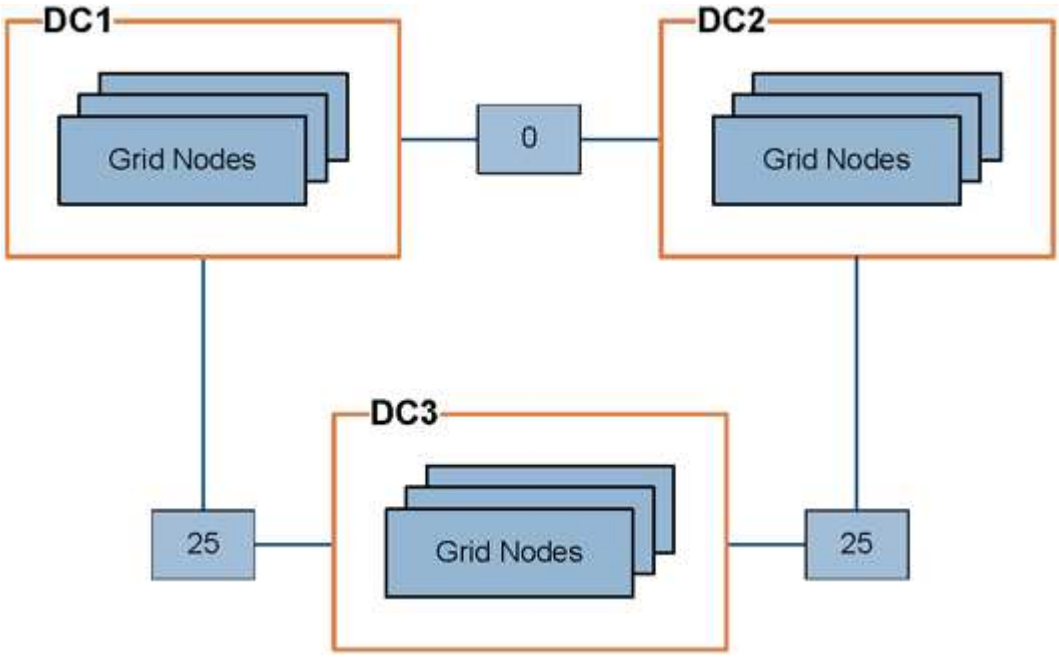
Durch die Verbindungskosten können Sie festlegen, welcher Datacenter-Standort einen angeforderten Service bereitstellt, wenn zwei oder mehr Datacenter-Standorte vorhanden

sind. Sie können die Verbindungskosten anpassen, um die Latenz zwischen Standorten reflektieren.

- 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.
- Die Verbindungskosten werden vom CLB-Service auf Gateway-Knoten zur direkten Verbindung von Clients genutzt.

> Der CLB-Service ist veraltet.

Das Diagramm zeigt ein drei Standortraster mit Verbindungskosten, die zwischen Standorten konfiguriert sind:



- Der CLB-Service auf Gateway-Knoten verteilt Client-Verbindungen gleichermaßen auf alle Storage-Nodes am selben Datacenter-Standort und an beliebige Datacenter-Standorte mit einem Linkskosten von 0.

  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 eine Client-Anwendung an DC2 ein Objekt abruft, das sowohl an DC1 als auch an DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 bis D2 0 sind, was niedriger ist als die Verbindungskosten von DC3 nach 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.

Verwandte Informationen

"Wie der Lastenausgleich funktioniert - CLB-Service"

Verbindungskosten werden aktualisiert

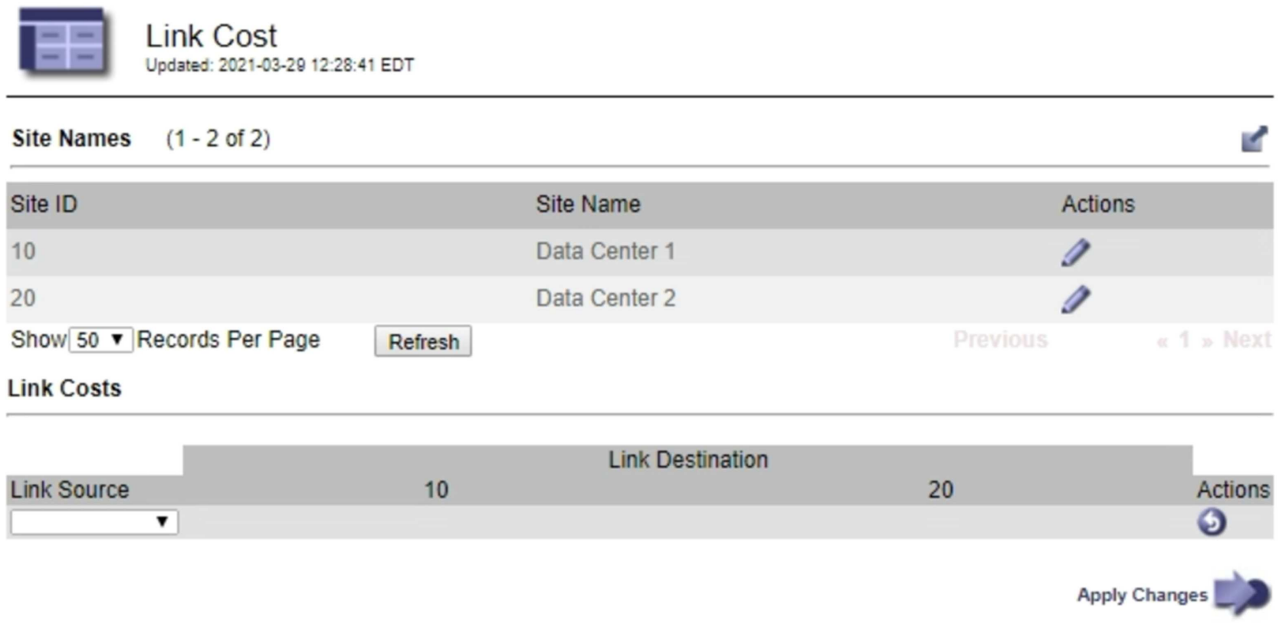
Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen Standorten wiederzugeben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung für die Konfiguration der Seite für die Grid-Topologie verfügen.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verbindungskosten**.



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, klicken Sie auf **Zurücksetzen**.

3. Klicken Sie Auf **Änderungen Übernehmen**.

AutoSupport wird konfiguriert

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.

Informationen, die in AutoSupport Meldungen enthalten sind

AutoSupport Meldungen enthalten Informationen, z. B. die folgenden:

- StorageGRID Softwareversion
- Betriebssystemversion
- Attributinformationen auf System- und Standortebene
- Aktuelle Warnmeldungen und Alarme (Altsystem)
- Aktueller Status aller Grid-Aufgaben, einschließlich historischer Daten
- Informationen zu Ereignissen, die auf der Seite **Nodes** > ***Grid Node*** > **Events** aufgeführt sind
- 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 ManagerDashboard eine Meldung angezeigt. Die Meldung enthält einen Link zur AutoSupport-Konfigurationsseite.

Sie können das Symbol „x“ auswählen Um die Meldung zu schließen. Die Nachricht wird erst wieder angezeigt, wenn Ihr Browser-Cache gelöscht wird, auch wenn AutoSupport deaktiviert bleibt.

Verwenden von Active IQ

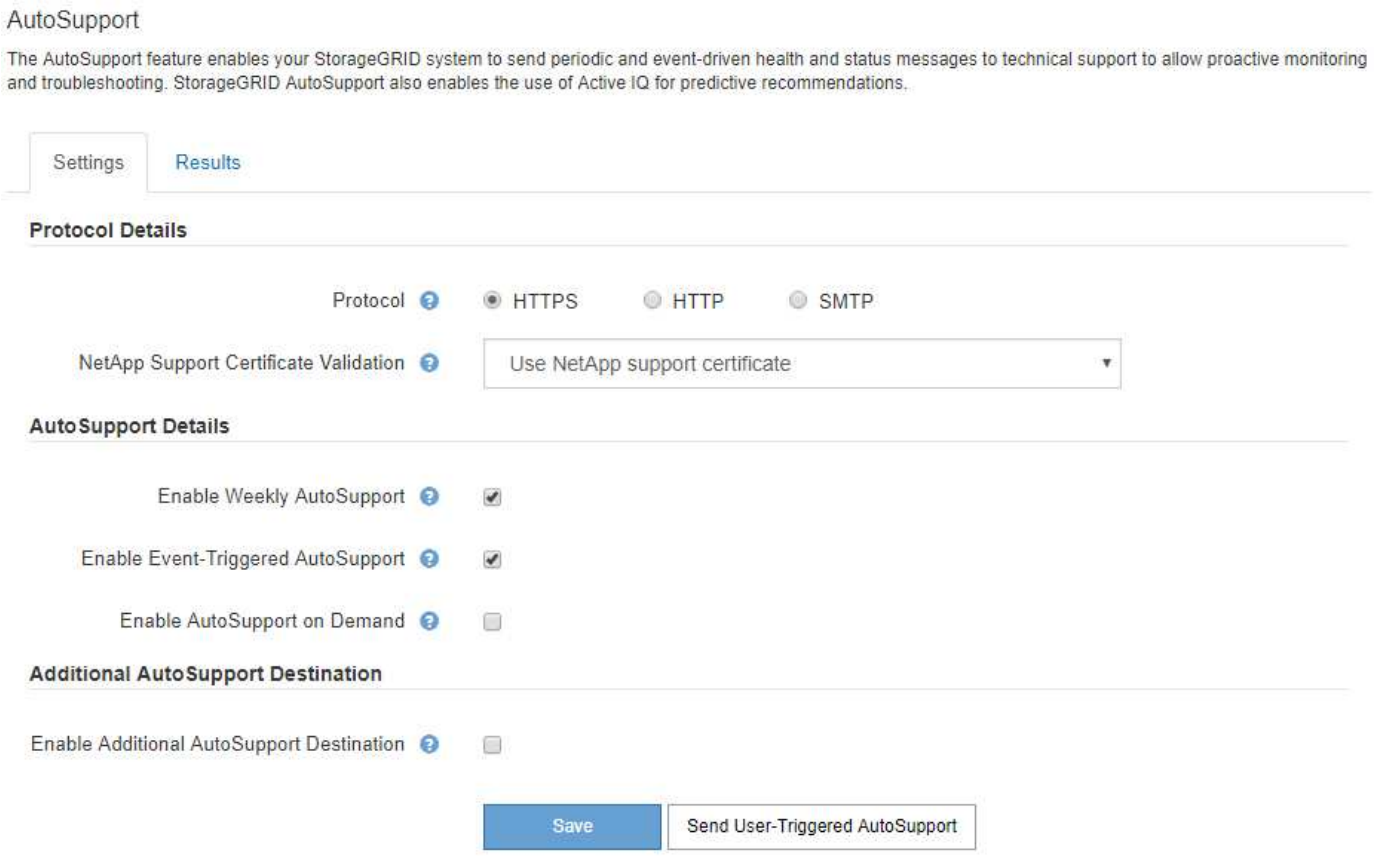
Active IQ ist ein Cloud-basierter digitaler Berater, der prädiktive Analysen und Community-Wissen aus der installierten Basis von NetApp nutzt. Kontinuierliche Risikobewertungen, prädiktive Warnungen, beschreibende Tipps und automatisierte Aktionen helfen Ihnen, Probleme zu vermeiden, bevor sie auftreten. Dies führt zu verbesserter Systemintegrität und höherer Systemverfügbarkeit.

Sie müssen AutoSupport aktivieren, wenn Sie die Active IQ Dashboards und Funktionen auf der NetApp Support-Website nutzen möchten.

"Active IQ Digital Advisor Dokumentation"

Zugriff auf AutoSupport-Einstellungen

Sie konfigurieren AutoSupport mit dem Grid Manager (**Support Tools AutoSupport**). Die **AutoSupport** Seite hat zwei Registerkarten: **Einstellungen** und **Ergebnisse**.



Protokolle zum Senden von AutoSupport Meldungen

Sie können eines von drei Protokollen zum Senden von AutoSupport Meldungen wählen:

- HTTPS
- HTTP
- SMTP

Wenn Sie AutoSupport-Meldungen über HTTPS oder HTTP senden, können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und dem technischen Support konfigurieren.

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.

Verwandte Informationen

"NetApp Support"

Angeben des Protokolls für AutoSupport Meldungen

Sie können eines von drei Protokollen zum Senden von AutoSupport Meldungen verwenden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.
- Wenn Sie das HTTPS- oder HTTP-Protokoll für das Senden von AutoSupport-Meldungen verwenden, müssen Sie Outbound-Internetzugang für den primären Admin-Node entweder direkt oder über einen Proxy-Server bereitgestellt haben (eingehende Verbindungen sind nicht erforderlich).
- Wenn Sie das HTTPS- oder HTTP-Protokoll verwenden und einen Proxy-Server verwenden möchten, müssen Sie einen Administrator-Proxy-Server konfiguriert haben.
- Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie einen SMTP-Mail-Server konfiguriert haben. Die gleiche E-Mail-Serverkonfiguration wird für Benachrichtigungen über Alarm E-Mails verwendet (altes System).

Über diese Aufgabe

AutoSupport Meldungen können mit einem der folgenden Protokolle gesendet werden:

- **HTTPS**: Dies ist die Standard-Einstellung und wird für Neuinstallationen empfohlen. Das HTTPS-Protokoll verwendet Port 443. Wenn Sie die Funktion AutoSupport On Demand aktivieren möchten, müssen Sie das HTTPS-Protokoll verwenden.
- **HTTP**: Dieses Protokoll ist nicht sicher, es sei denn, es wird in einer vertrauenswürdigen Umgebung verwendet, in der der Proxyserver beim Senden von Daten über das Internet in HTTPS konvertiert. Das HTTP-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.

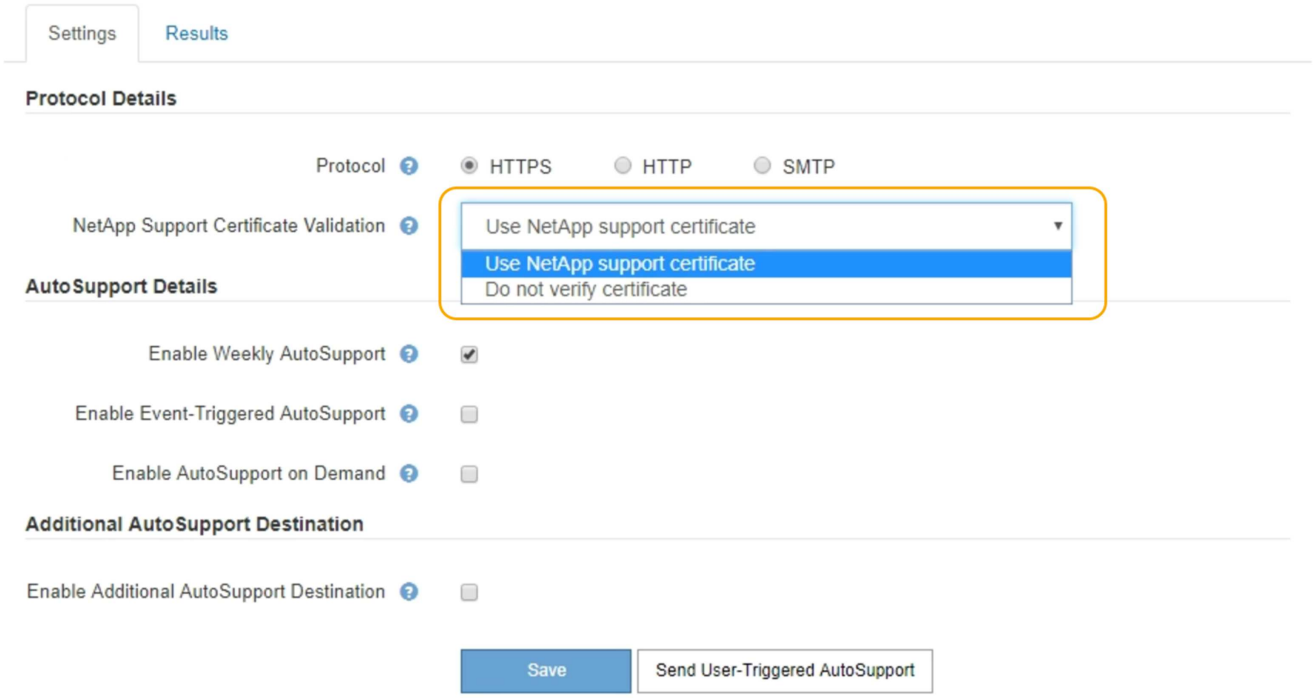
Das von Ihnen festgelegte Protokoll wird für das Senden aller Typen von AutoSupport Meldungen verwendet.

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, und die Registerkarte **Einstellungen** ist ausgewählt.

2. Wählen Sie das Protokoll aus, das Sie zum Senden von AutoSupport Meldungen verwenden möchten.



3. Wählen Sie Ihre Wahl für **NetApp Support Certificate Validation**.
   - Verwenden Sie ein NetApp Support-Zertifikat (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 ein vorübergehendes Problem mit einem Zertifikat vorliegt.
4. Wählen Sie **Speichern**.

   Alle wöchentlichen, vom Benutzer ausgelösten und von Ereignissen ausgelösten Meldungen werden über das ausgewählte Protokoll gesendet.

Verwandte Informationen

"Konfigurieren von Administrator-Proxy-Einstellungen"

Aktivieren von AutoSupport-on-Demand

AutoSupport On Demand kann Ihnen bei der Lösung von Problemen helfen, an denen der technische Support aktiv arbeitet. Wenn Sie AutoSupport on Demand aktivieren, kann der technische Support anfordern, dass AutoSupport Meldungen ohne Ihr Eingreifen gesendet werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.
- Sie müssen wöchentliche AutoSupport-Meldungen aktiviert haben.
- Sie müssen das Transportprotokoll auf HTTPS einstellen.

Über diese Aufgabe

Wenn Sie diese Funktion aktivieren, kann der technische Support von Ihrem StorageGRID System anfordern, dass AutoSupport Meldungen automatisch gesendet werden. Der technische Support kann auch das Abfrageintervall für AutoSupport-on-Demand-Abfragen festlegen.

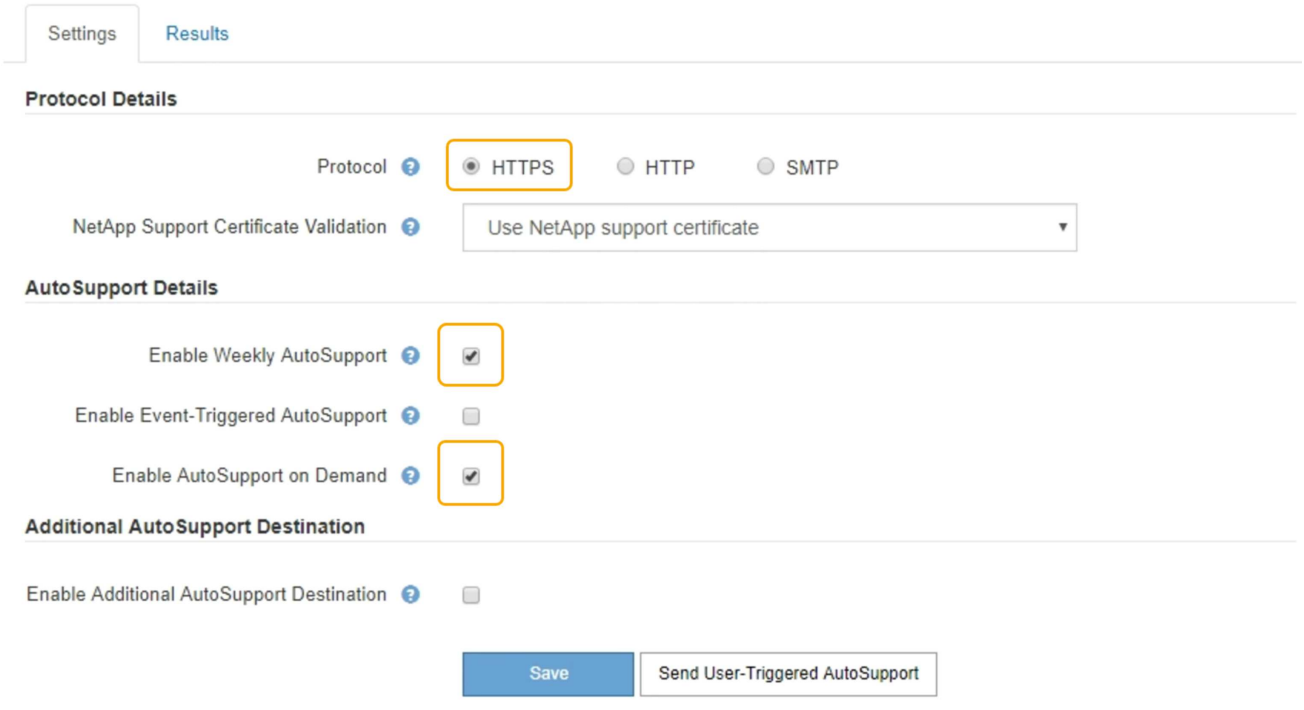
Der technische Support kann AutoSupport bei Bedarf nicht aktivieren oder deaktivieren.

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Aktivieren Sie das Optionsfeld HTTPS im Abschnitt **Protokolldetails** der Seite.



3. Aktivieren Sie das Kontrollkästchen **Wochenendfach-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 von wöchentlichen AutoSupport Meldungen

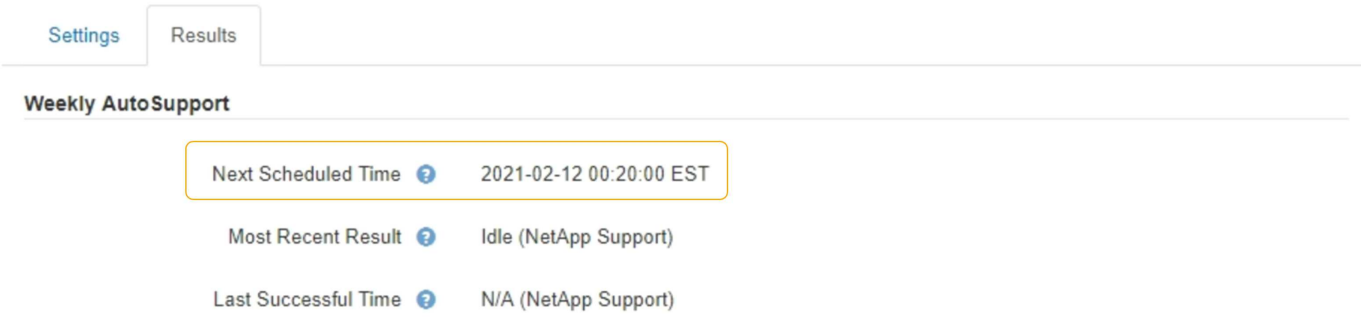
Standardmäßig wird das StorageGRID System so konfiguriert, dass einmal pro Woche eine AutoSupport Meldung an den NetApp Support gesendet wird.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Über diese Aufgabe

Um zu bestimmen, wann die wöchentliche AutoSupport-Nachricht gesendet wird, lesen Sie auf der Seite **AutoSupport** > **Results** die **nächste geplante Zeit** unter **wöchentlicher AutoSupport**.



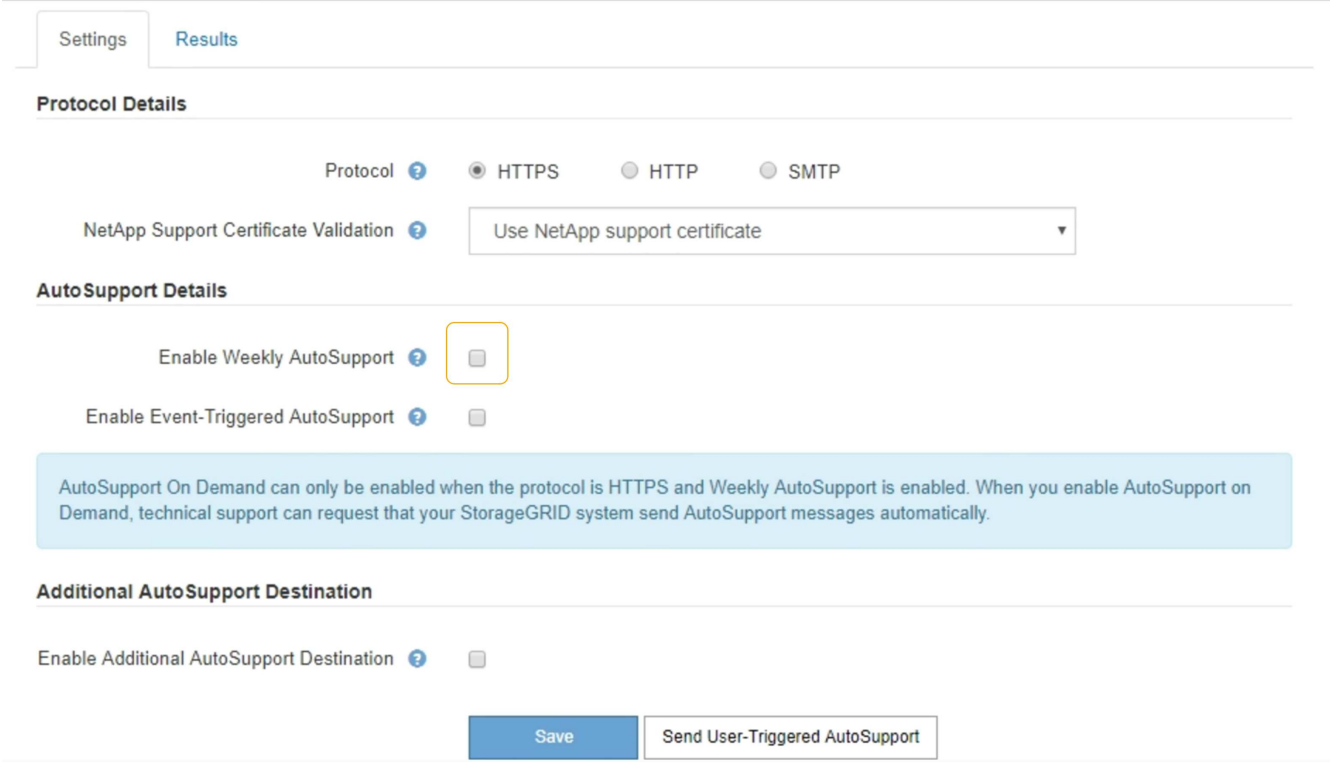
Sie können das automatische Senden einer AutoSupport Meldung jederzeit deaktivieren.

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Deaktivieren Sie das Kontrollkästchen **Wochenendfach-AutoSupport aktivieren**.



3. Wählen Sie **Speichern**.

Deaktivieren von AutoSupport-Meldungen, die durch Ereignisse ausgelöst wurden

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Über diese Aufgabe

Sie können AutoSupport Meldungen, bei denen Ereignisse ausgelöst wurden, jederzeit deaktivieren.

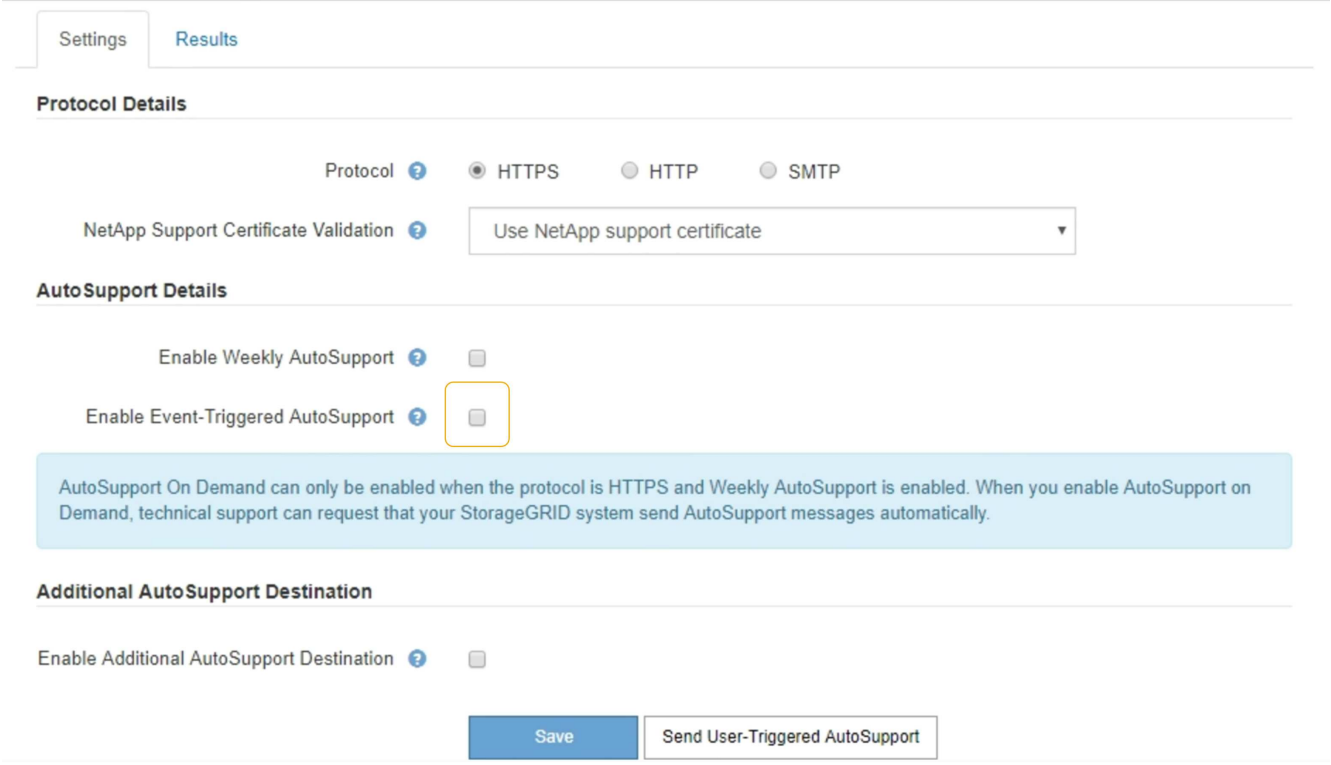
> Auch bei Event-ausgelösten AutoSupport-Meldungen werden diese unterdrückt, wenn Sie E-Mail-Benachrichtigungen systemweit unterdrücken. (Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**. Wählen Sie dann **Benachrichtigung Alle unterdrücken**.)

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Deaktivieren Sie das Kontrollkästchen * Event-Trigger AutoSupport* aktivieren.



3. Wählen Sie **Speichern**.

Manuelles Auslösen einer AutoSupport-Meldung

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Wählen Sie **vom Benutzer ausgelöste AutoSupport senden** aus.

   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.

Hinzufügen eines weiteren AutoSupport Ziels

Wenn Sie AutoSupport aktivieren, werden Zustandsmeldungen und Statusmeldungen an den NetApp Support gesendet. Sie können ein zusätzliches Ziel für alle AutoSupport Meldungen angeben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Über diese Aufgabe

Zum Überprüfen oder Ändern des Protokolls zum Senden von AutoSupport Meldungen finden Sie in den Anweisungen zur Angabe eines AutoSupport-Protokolls.

Sie können das SMTP-Protokoll nicht zum Senden von AutoSupport Meldungen an ein zusätzliches Ziel verwenden.

"Angeben des Protokolls für AutoSupport Meldungen"

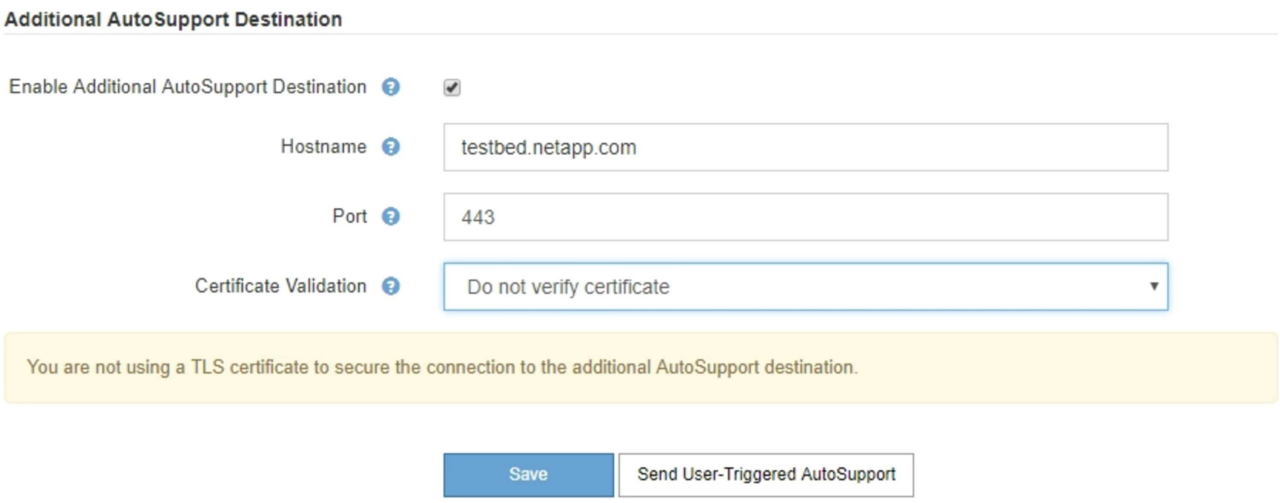
Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Wählen Sie **zusätzliches AutoSupport-Ziel aktivieren**.

   Die Felder „zusätzliche AutoSupport-Zieladresse“ werden angezeigt.



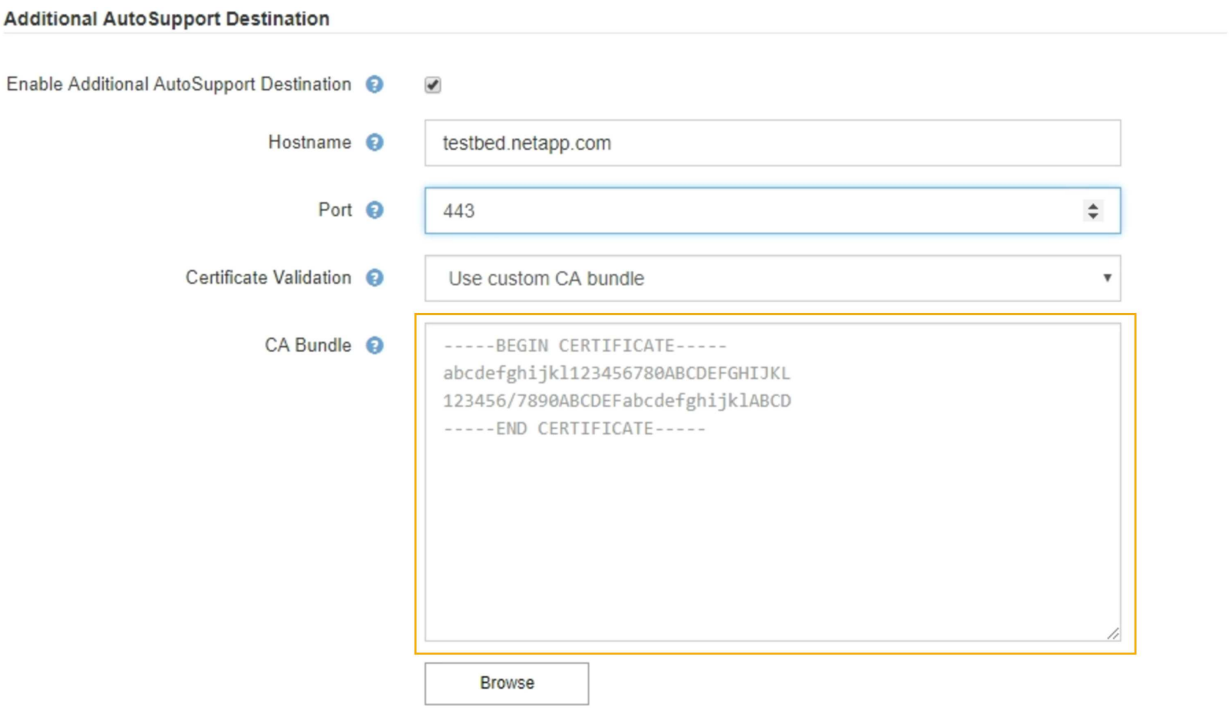
3. Geben Sie den Hostnamen oder die IP-Adresse des Servers eines zusätzlichen AutoSupport-Zielservers ein.

   Sie können nur ein weiteres Ziel eingeben.

4. Geben Sie den Port ein, der für die Verbindung zu einem zusätzlichen AutoSupport-Zielserver verwendet wird (standardmäßig ist Port 80 für HTTP oder Port 443 für HTTPS).
5. Um Ihre AutoSupport-Nachrichten mit Zertifikatvalidierung zu senden, wählen Sie im Dropdown-Menü

Zertifikatvalidierung Custom CA-Bundle verwenden aus. Führen Sie dann einen der folgenden Schritte aus:

- Verwenden Sie ein Bearbeitungswerkzeug, um alle Inhalte jeder PEM-kodierten CA-Zertifikatdatei in das Feld **CA Bundle** zu kopieren und einzufügen, das in der Reihenfolge der Zertifikatskette verkettet ist. Sie müssen Folgendes einschließen `----BEGIN CERTIFICATE----` Und `----END CERTIFICATE----` Wählen Sie aus.



- Wählen Sie **Durchsuchen**, navigieren Sie zu der Datei mit den Zertifikaten und wählen Sie dann **Öffnen**, um die Datei hochzuladen. Die Zertifikatvalidierung stellt sicher, dass die Übertragung von AutoSupport Meldungen sicher ist.

6. Um Ihre AutoSupport-Nachrichten ohne Zertifikatvalidierung zu senden, wählen Sie im Dropdown-Menü * Zertifikatvalidierung* * * * nicht verifizieren aus.

   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.

   Eine Warnung: "Sie verwenden kein TLS-Zertifikat, um die Verbindung zum zusätzlichen AutoSupport-Ziel zu sichern."

7. Wählen Sie **Speichern**.

   Alle zukünftigen wöchentlichen, ereignisgesteuert und vom Benutzer ausgelösten AutoSupport Meldungen werden an das zusätzliche Ziel gesendet.

E-Series AutoSupport Nachrichten über StorageGRID senden

Sie können AutoSupport Meldungen zu E-Series SANtricity System Manager über einen StorageGRID Admin-Node an den technischen Support senden und nicht über den Management-Port der Storage Appliance.

Was Sie benötigen

- Sie sind über einen unterstützten Webbrowser beim Grid Manager angemeldet.
- Sie verfügen über die Berechtigung zum Administrator oder Stammzugriff der Speicheranwendung.

> 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.

Konfigurieren Sie eine spezielle Proxy-Server-Adresse in SANtricity System Manager, damit die AutoSupport-Meldungen ohne Verwendung des Managementports der Appliance über einen StorageGRID-Admin-Node übertragen werden. Auf diese Weise übertragene AutoSupport-Nachrichten gelten für die Proxyeinstellungen für bevorzugte Sender und Admin, die möglicherweise im Grid Manager konfiguriert wurden.

Wenn Sie den Admin-Proxyserver in Grid Manager konfigurieren möchten, lesen Sie die Anweisungen zum Konfigurieren von Administrator-Proxy-Einstellungen.

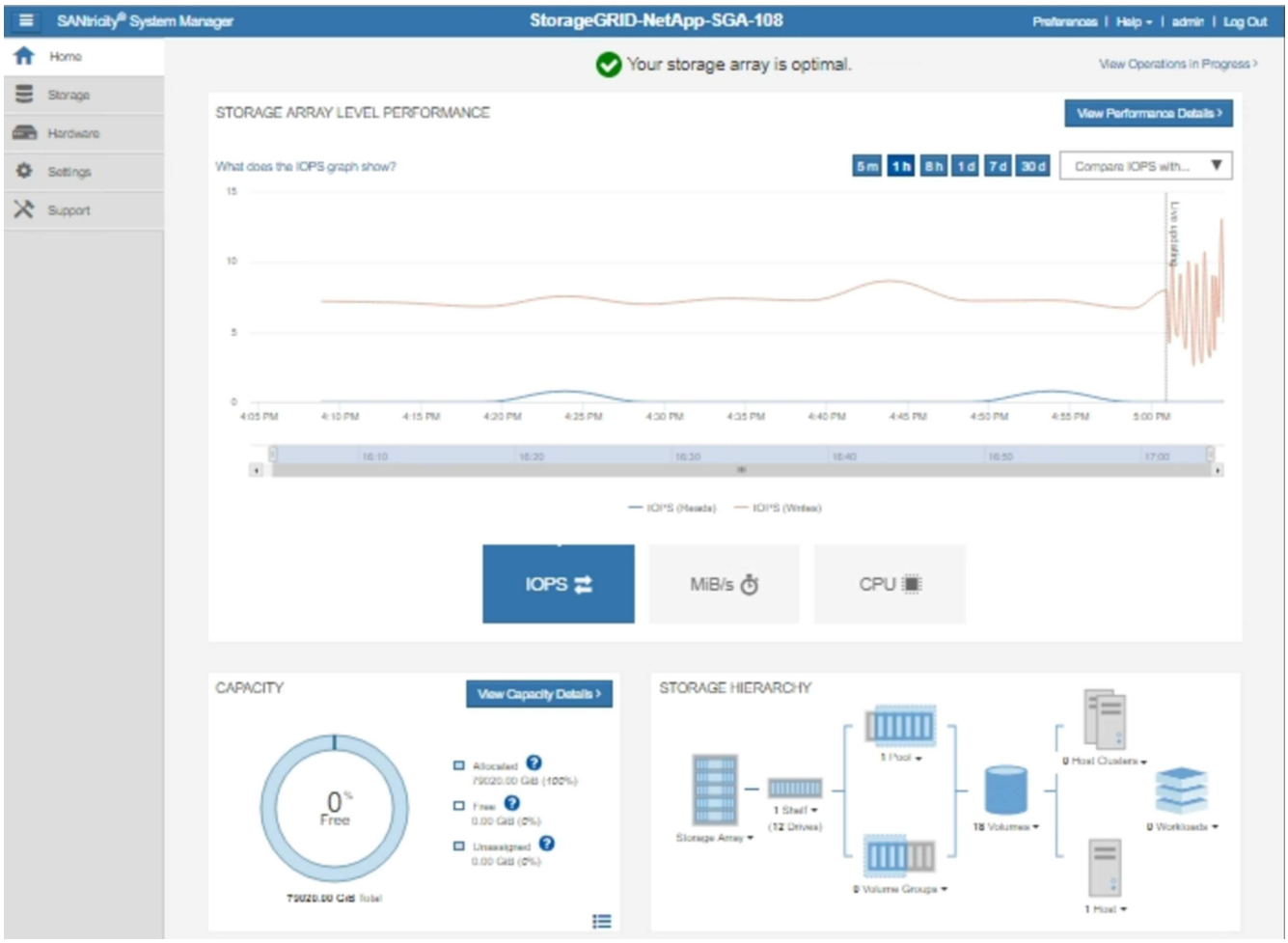
"Konfigurieren von Administrator-Proxy-Einstellungen"

> 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 im Dokumentationszentrum zur E-Series.
>
> "NetApp E-Series Systems Documentation Center"

Schritte

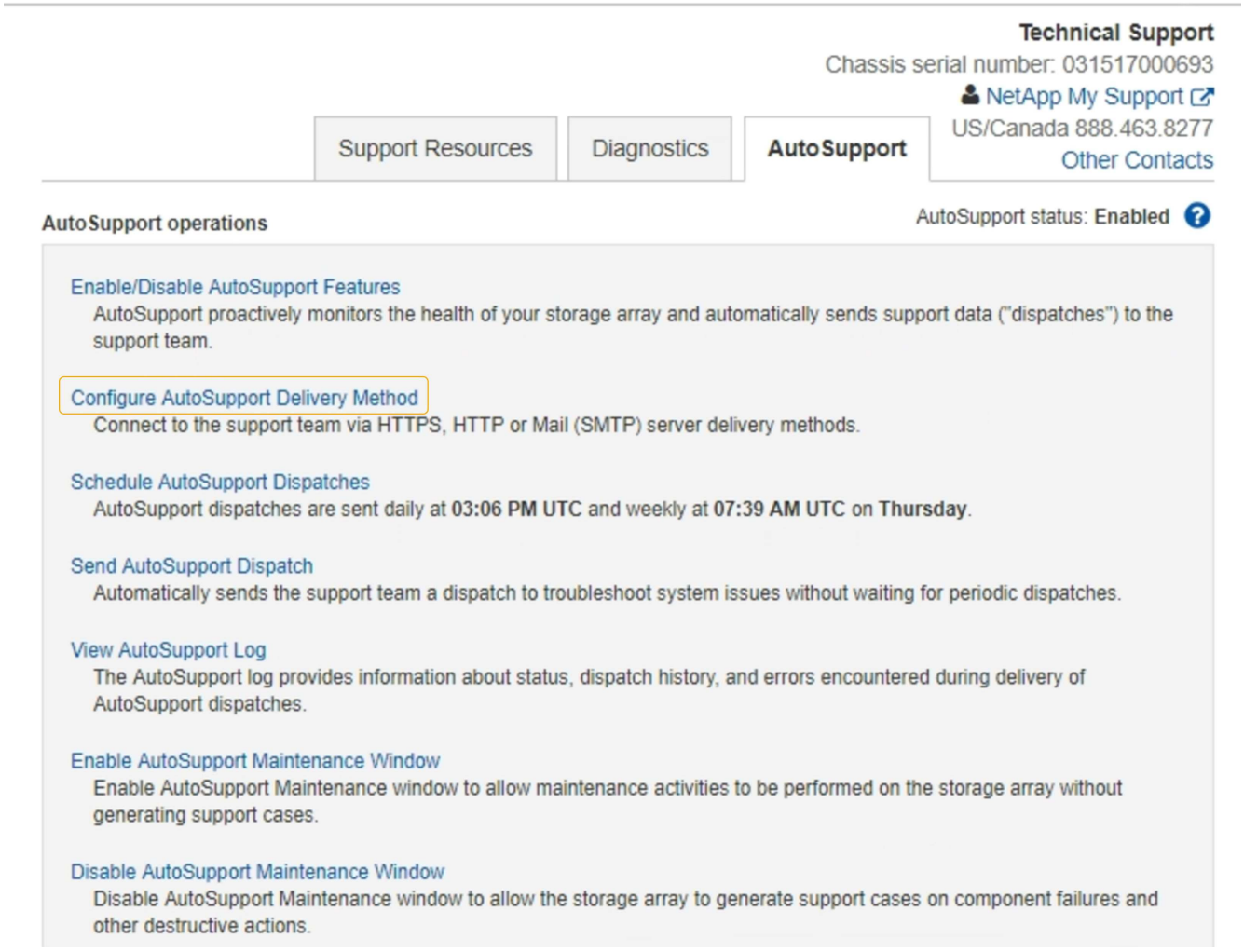
1. Wählen Sie im Grid Manager die Option **Nodes** aus.
2. Wählen Sie in der Liste der Knoten links den Speicher-Appliance-Node aus, den Sie konfigurieren möchten.
3. Wählen Sie **SANtricity System Manager**.

   Die Startseite von SANtricity System Manager wird angezeigt.



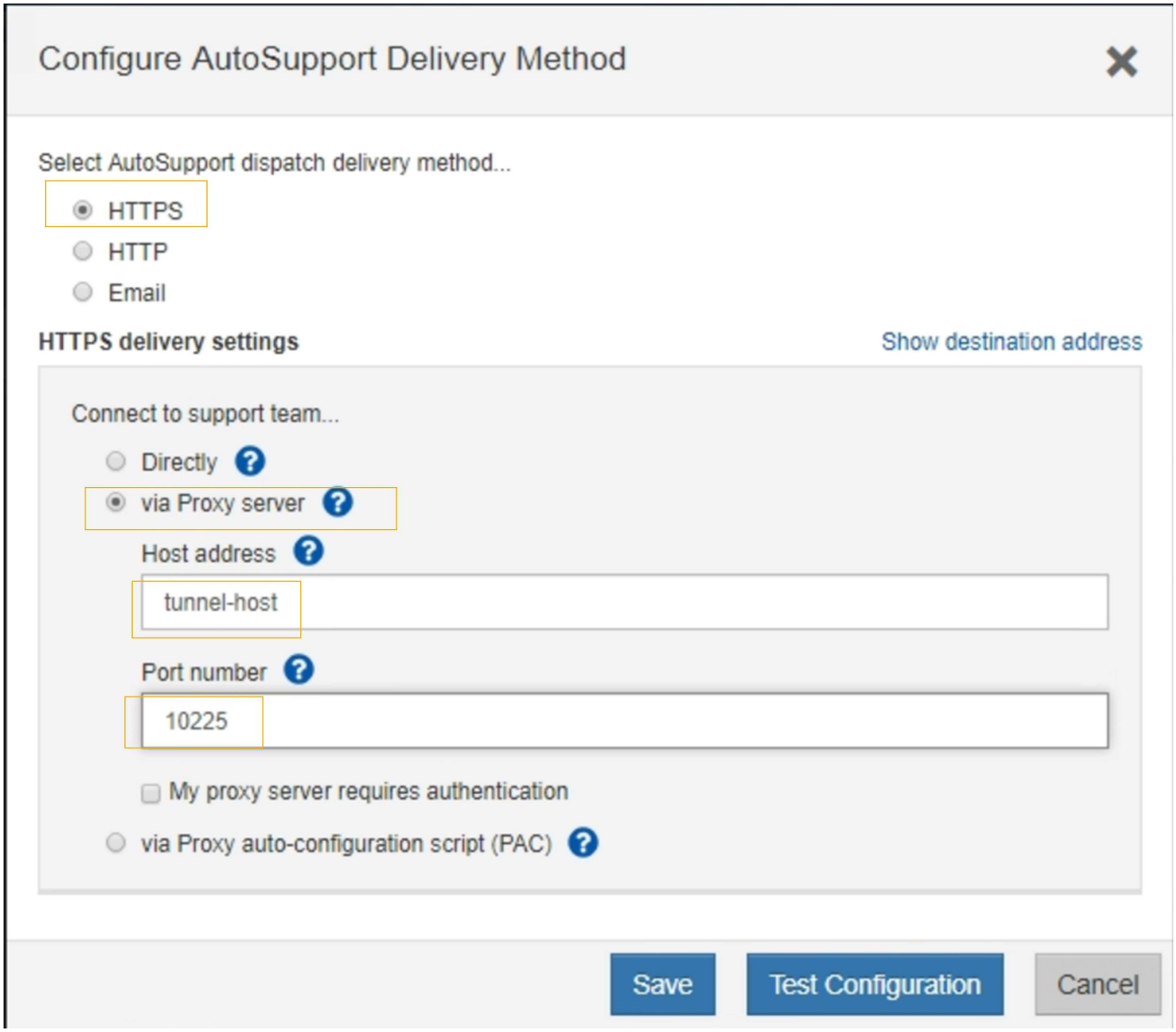
4. Wählen Sie **Support** > **Support Center** > **AutoSupport**.

   Die Seite AutoSupport-Vorgänge wird angezeigt.



5. Wählen Sie **AutoSupport-Bereitstellungsmethode konfigurieren**.

   Die Seite AutoSupport-Bereitstellungsmethode konfigurieren wird angezeigt.



6. Wählen Sie **HTTPS** für die Liefermethode aus.

   Das Zertifikat, das das HTTPS-Protokoll 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 Netzwerke. Stellen Sie sicher, dass der bevorzugte Sender Admin-Node eine Verbindung zur NetApp Support-Website herstellen kann, und versuchen Sie es erneut.

11. Wählen Sie **Speichern**.

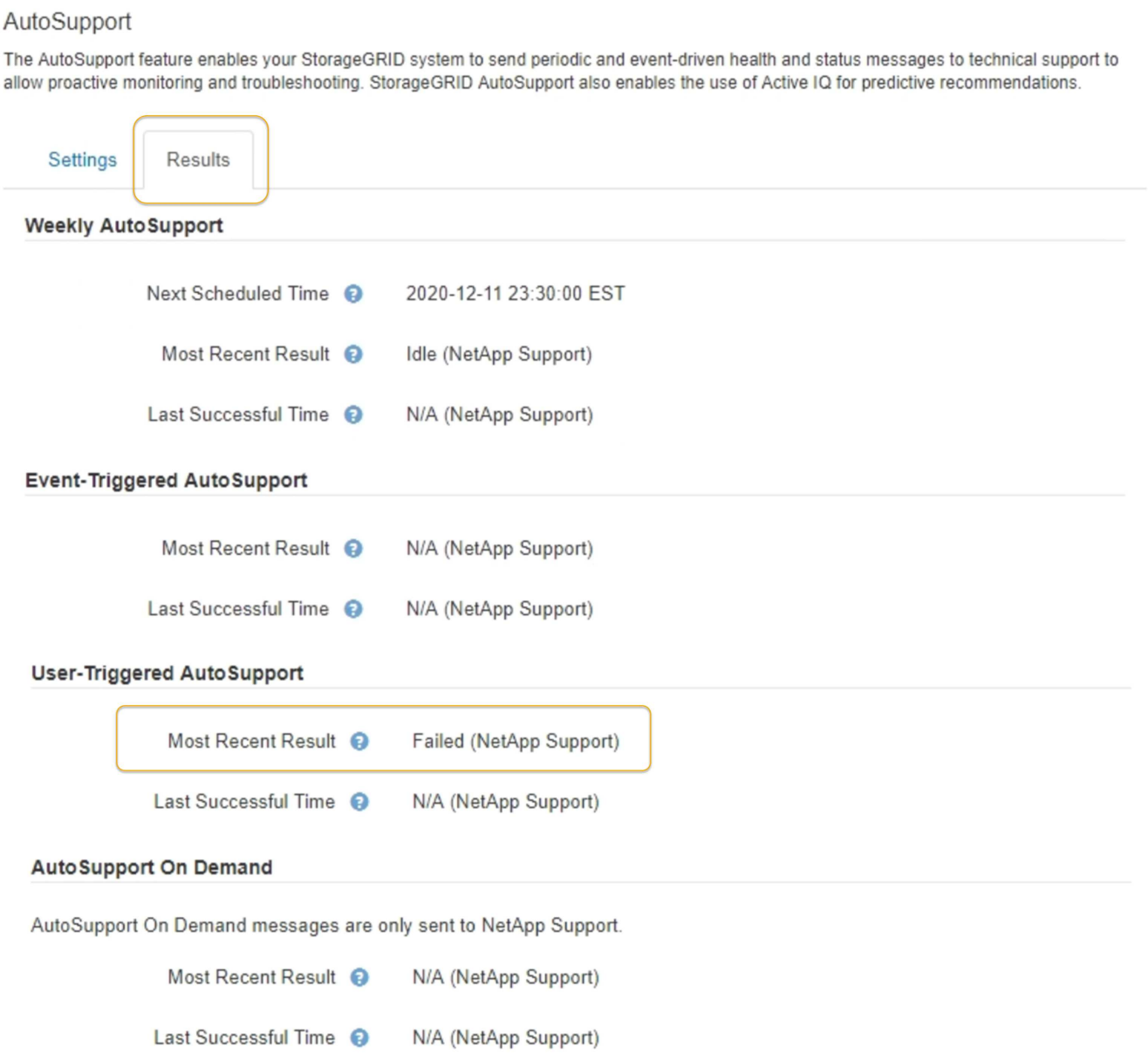
    Die Konfiguration wird gespeichert, und es wird eine Bestätigungsmeldung angezeigt: „`AutoSupport-Bereitstellungsmethode wurde konfiguriert.`“

Fehlerbehebung bei 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 **Unterstützung** > **Werkzeuge** > **AutoSupport** > **Ergebnisse** auswählen.

> Wenn Sie E-Mail-Benachrichtigungen im gesamten System unterdrücken, werden ereignisgesteuerte AutoSupport Meldungen unterdrückt. (Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**. Wählen Sie dann **Benachrichtigung Alle unterdrücken**.)

Wenn die AutoSupport-Meldung nicht gesendet wird, wird „`failed`“ auf der Registerkarte **Results** der Seite **AutoSupport** angezeigt.



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 die Einstellungen für E-Mail-Server im konfigurieren "Monitor Anweisungen zur Fehlerbehebung".

Korrigieren eines Fehlers bei AutoSupport-Meldungen

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.`

Verwandte Informationen

"Monitor Fehlerbehebung"

Verwalten Von Storage-Nodes

Storage-Nodes stellen Festplattenkapazität und Services zur Verfügung. Das Verwalten von Storage-Nodes umfasst die Überwachung des nutzbaren Speicherplatzes auf jedem Node mithilfe von Wasserzeichen-Einstellungen und das Anwenden der Konfigurationseinstellungen von Storage-Nodes.

- "Was ist ein Storage-Node"
- "Verwalten Von Storage-Optionen"
- "Management von Objekt-Metadaten-Storage"
- "Globale Einstellungen für gespeicherte Objekte konfigurieren"
- "Konfigurationseinstellungen für Storage-Nodes"
- "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 der ADC-Dienst ist

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.

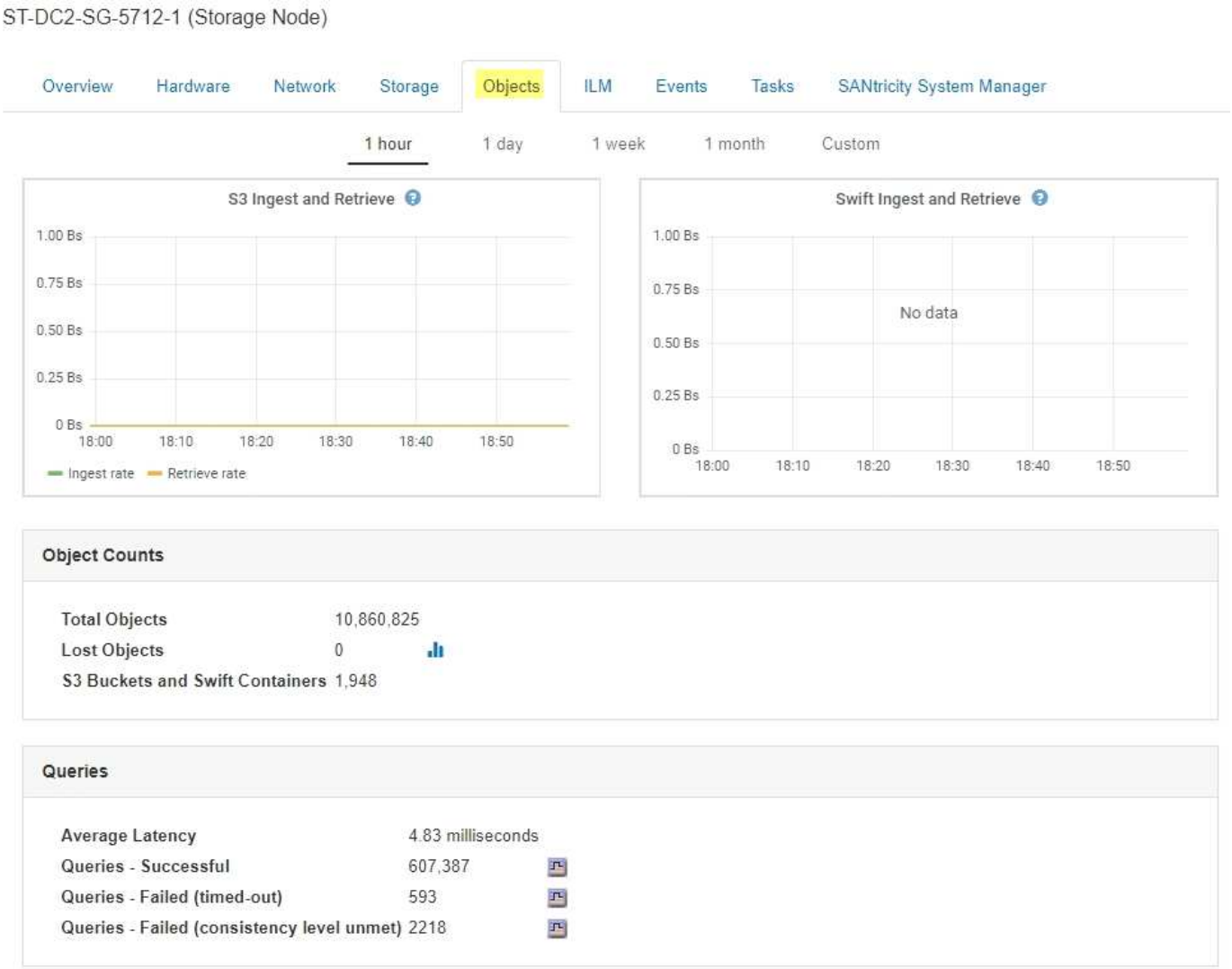
Was der DDS-Dienst ist

Der DDS-Service (Distributed Data Store) wird von einem Storage-Node gehostet und führt Hintergrundaufgaben zu den im StorageGRID-System gespeicherten Objektmetadaten durch.

Anzahl der Objekte

Der DDS-Dienst verfolgt die Gesamtzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtzahl der über die unterstützten Schnittstellen (S3 oder Swift) des Systems aufgenommenen Objekte.

Die Anzahl der Objekte insgesamt wird auf der Seite Nodes > Registerkarte Objekte für jeden Storage Node angezeigt.



Abfragen

Sie können die durchschnittliche Zeit für die Ausführung einer Abfrage zum Metadatenspeicher durch den spezifischen DDS-Dienst, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtanzahl der fehlgeschlagenen Abfragen für ein Timeout-Problem identifizieren.

Vielleicht möchten Sie nach Abfrageinformationen suchen, um den Zustand des Metadatenspeichers, Cassandra, zu überwachen. Dies hat Auswirkungen auf die Aufnahme- und Abrufleistung des Systems. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl von verfügbaren Metadatenspeichern zum Zeitpunkt der Durchführung einer Abfrage durch den spezifischen DDS-Service.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen. Siehe "Diagnose wird ausgeführt".

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.

Das 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-Service erledigt den Großteil der harten Arbeit des StorageGRID-Systems durch die Handhabung von Datenübertragungslasten und Datenverkehrsfunktionen.

Der LDR-Service übernimmt folgende Aufgaben:

- Abfragen
- Information Lifecycle Management-Aktivitäten (ILM
- Löschen von Objekten
- Objekt-Storage
- Objektdatenübertragung von einem anderen LDR-Service (Storage Node)
- Datenspeicher-Management
- Protokollschnittstellen (S3 und Swift)

Der LDR-Service managt auch die Zuordnung von S3- und Swift-Objekten zu den eindeutigen „`Content Handles`“ (UUIDs), die das StorageGRID System jedem aufgenommene Objekt zuweist.

Abfragen

LDR-Abfragen umfassen Abfragen zum Objektspeicherort während Abruf- und Archivierungsvorgängen. Sie können die durchschnittliche Zeit zum Ausführen einer Abfrage, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtzahl der Abfragen, die aufgrund eines Timeout-Problems fehlgeschlagen sind, identifizieren.

Sie können Abfrageinformationen prüfen, um den Zustand des Metadatenspeichers zu überwachen und die Aufnahme- und Abrufleistung des Systems zu beeinträchtigen. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl an verfügbaren Metadatenspeichern zum Zeitpunkt einer Abfrage durch den spezifischen LDR-Service.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen. Siehe "Diagnose wird ausgeführt".

ILM-Aktivität

Mithilfe der ILM-Metriken (Information Lifecycle Management) können Sie die Bewertung von Objekten für die ILM-Implementierung durchführen. Sie können diese Metriken auf dem Dashboard oder auf der Seite Nodes > ILM für jeden Storage Node 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	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	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. Die Kopien werden gleichmäßig auf alle Storage-Nodes an jedem Standort verteilt. Diese Replikation ist nicht konfigurierbar und wird automatisch ausgeführt.

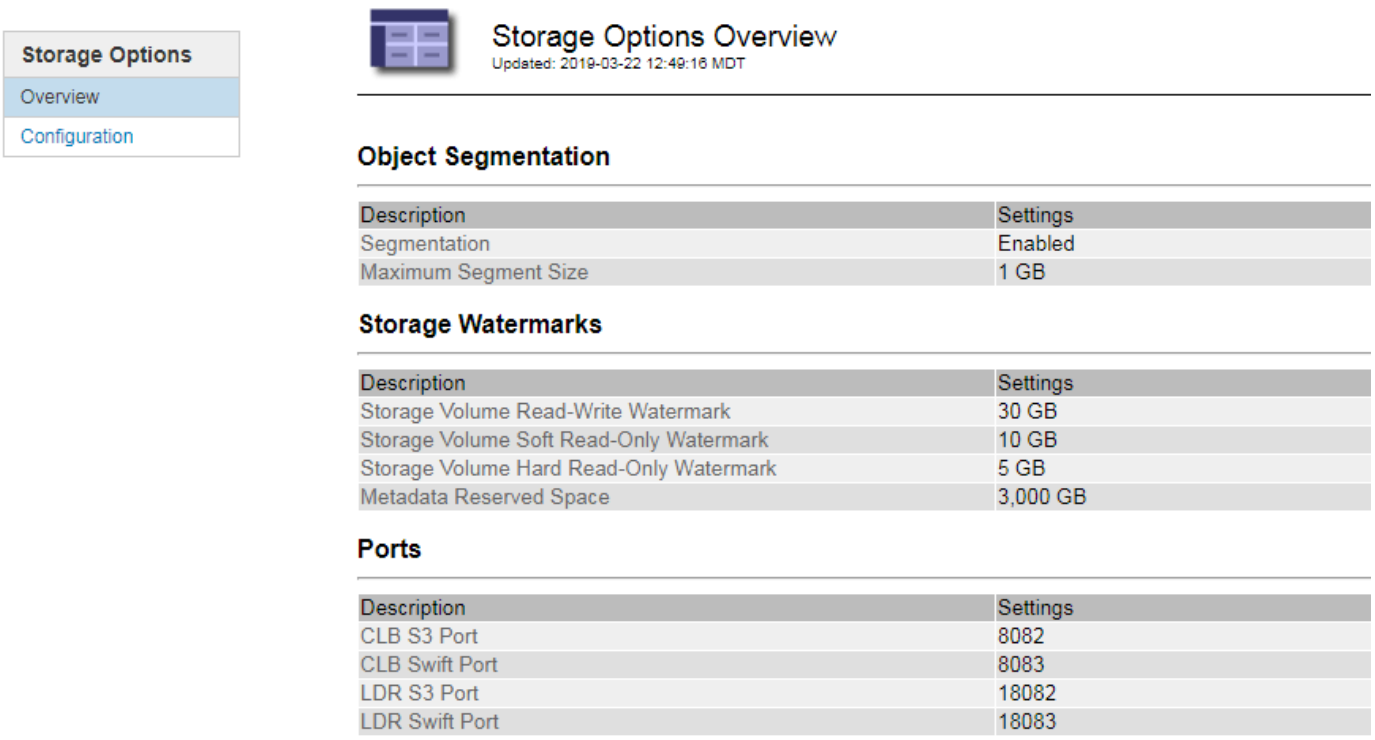
"Management von Objekt-Metadaten-Storage"

Verwalten Von Storage-Optionen

Sie können Speicheroptionen über das Menü Konfiguration im Grid Manager anzeigen

und konfigurieren. Storage-Optionen enthalten die Einstellungen für die Objektsegmentierung und die aktuellen Werte für Storage-Wasserzeichen. Sie können auch die S3- und Swift-Ports anzeigen, die vom veralteten CLB-Dienst auf Gateway-Nodes und vom LDR-Service auf Storage-Nodes verwendet werden.

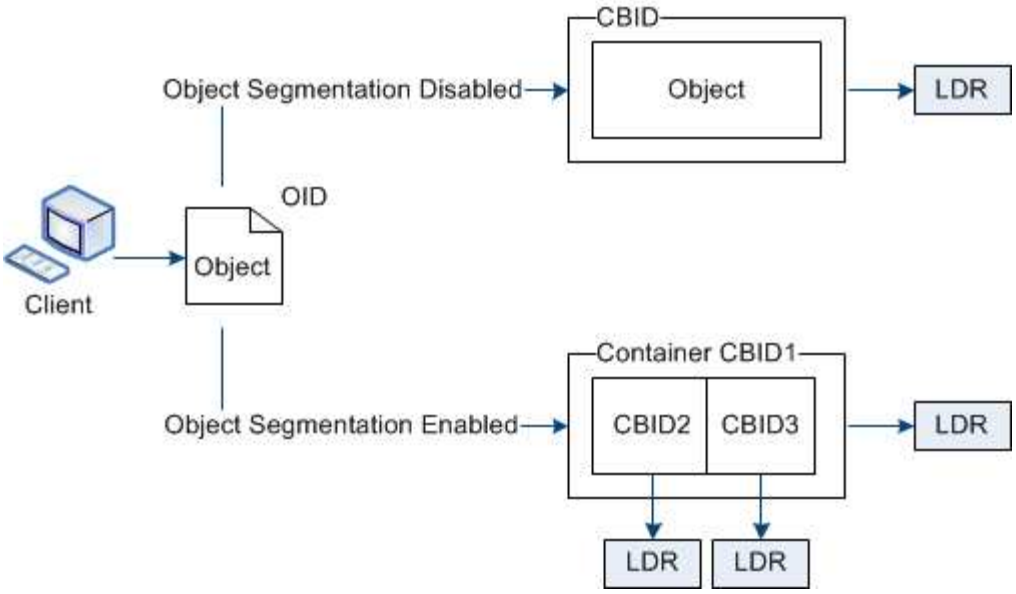
Informationen zu Port-Zuweisungen finden Sie unter "Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen".



Objektsegmentierung

Objektsegmentierung ist der Vorgang, ein Objekt in eine Sammlung kleinerer Objekte mit fester Größe aufzuteilen, um die Speicherung 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.



Wenn Ihr StorageGRID-System einen Archiv-Node enthält, dessen Zieltyp Cloud Tiering — einfacher Speicherdienst ist und das Zielspeichersystem Amazon Web Services (AWS) ist, muss die maximale Segmentgröße kleiner als oder gleich 4.5 gib (4,831,838,208 Byte) sein. Diese Obergrenze stellt sicher, dass die Put-Beschränkung von fünf GB bei AWS nicht überschritten wird. Anträge an AWS, die diesen Wert überschreiten, fallen nicht an.

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 notwendigerweise auf demselben Storage-Node gespeichert. Container und Segmente können auf jedem beliebigen Speicherknoten 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:

Segmentcontainer + Segment 1 + Segment 2 = drei gespeicherte Objekte

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.

Welche Wasserzeichen für Storage Volume sind

StorageGRID verwendet Wasserzeichen für Speichervolumen, damit Sie die Menge an nutzbarem Speicherplatz auf Speicherknoten überwachen können. Wenn der verfügbare Speicherplatz eines Knotens kleiner als eine konfigurierte Wasserzeicheneinstellung ist, wird der Speicherstatus (SSTS)-Alarm ausgelöst, damit Sie feststellen können, ob Sie

Storage-Nodes hinzufügen müssen.

Um die aktuellen Einstellungen für die Speichervolumen-Wasserzeichen anzuzeigen, wählen Sie **Konfiguration** > **Speicheroptionen** > **Übersicht**.

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

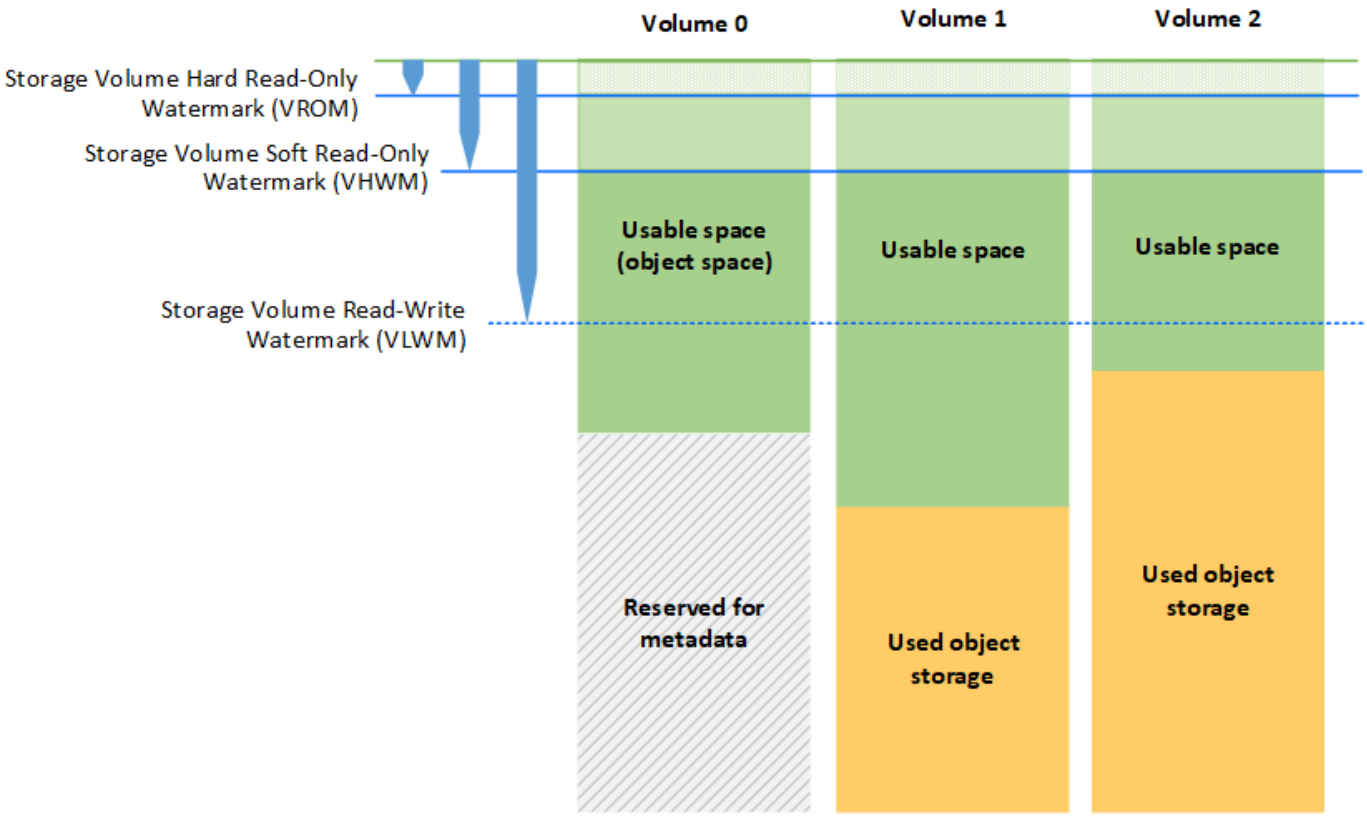
Object Segmentation

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

Die folgende Abbildung zeigt einen Storage-Node mit drei Volumes und zeigt die relative Position der drei Storage Volume-Wasserzeichen. Innerhalb jedes Storage-Nodes reserviert StorageGRID auf Volume 0 Platz für Objekt-Metadaten. Der restliche Speicherplatz auf diesem Volume wird für Objektdaten verwendet. Alle anderen Volumes werden ausschließlich für Objektdaten verwendet, zu denen replizierte Kopien und nach dem Erasure-Coding-Verfahren gehören.



Die Wasserzeichen für das Speichervolumen sind systemweite Standardwerte, die die Mindestmenge an freiem Speicherplatz angeben, die für jedes Volume im Speicherknoten benötigt wird, um zu verhindern, dass StorageGRID das Schreibverhalten des Knotens ändert oder einen Alarm auslöst. Beachten Sie, dass alle Volumes das entsprechende Wasserzeichen erreichen müssen, bevor StorageGRID entsprechende Maßnahmen ergreift. Wenn einige Volumes mehr als den mindestens erforderlichen freien Speicherplatz haben, wird der Alarm nicht ausgelöst, und das Lesen-Schreiben-Verhalten des Knotens ändert sich nicht.

Speichervolumen Soft Read-Only-Wasserzeichen (VHWM)

Das Speichervolumen Soft Read-Only Watermark ist das erste Wasserzeichen, das angibt, dass der für Objektdaten nutzbare Speicherplatz eines Node voll wird. Dieses Wasserzeichen gibt an, wie viel freier Speicherplatz auf jedem Volume in einem Storage Node vorhanden sein muss, um zu verhindern, dass der Node in den „`soft schreibgeschützten Modus" wechselt.` „Soft Read-Only"-Modus bedeutet, dass der Storage-Node mit Read-Only-Diensten für den Rest des StorageGRID Systems wirbt, aber alle ausstehenden Schreibanforderungen erfüllt.

Wenn die Menge an freiem Speicherplatz auf jedem Volume kleiner als die Einstellung dieses Wasserzeichens ist, wird der Alarm „Speicherstatus" (SSTS) auf der Ebene „Hinweis" ausgelöst und der Speicherknoten wechselt in den Modus „Soft Read-Only".

Angenommen, das Speichervolumen-Soft-Read-Only-Wasserzeichen ist auf 10 GB gesetzt, das ist der Standardwert. Wenn weniger als 10 GB freier Speicherplatz auf jedem Volume im Speicherknoten verbleibt, wird der SSTS-Alarm auf der Ebene Notice ausgelöst und der Speicherknoten wechselt in den Modus Soft Read.

Hard Read-Only-Wasserzeichen (VROM) für Speichervolumen

Das Hard Read-Only-Wasserzeichen für Speichervolumen ist das nächste Wasserzeichen, das angibt, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird. Dieses Wasserzeichen gibt an, wie viel freier Speicherplatz auf jedem Volume in einem Storage Node vorhanden sein muss, um zu verhindern, dass der Knoten in den „`Hard Read-Only Mode`“ wechselt. Der Festplatten-Lesemodus bedeutet, dass der Speicherknoten schreibgeschützt ist und keine Schreibanforderungen mehr akzeptiert.

Wenn die Menge an freiem Speicherplatz auf jedem Volume in einem Speicherknoten kleiner als die Einstellung dieses Wasserzeichens ist, wird der Alarm Speicherstatus (SSTS) auf der Hauptebene ausgelöst, und der Speicherknoten wechselt in den Modus für den reinen Lesezugriff.

Beispiel: Angenommen, der Hard Read-Only-Wasserzeichen des Speichervolumens ist auf 5 GB gesetzt, was der Standardwert ist. Wenn weniger als 5 GB freier Speicherplatz auf jedem Speicher-Volume im Storage-Node verbleibt, wird der SSTS-Alarm auf der Hauptebene ausgelöst und der Storage-Node wechselt in den reinen Schreibmodus.

Der Wert des Hard Read-Only-Wasserzeichens für Speichervolumen muss kleiner sein als der Wert des Speichervolumes Soft Read-Only-Wasserzeichens.

Storage-Volume-Lese-/Schreibmarke (VLWM)

Die Wasserzeichen Storage Volume für Lese- und Schreibvorgänge gilt nur für Storage-Nodes, die in den schreibgeschützten Modus versetzt wurden. Dieses Wasserzeichen bestimmt, wann der Speicherknoten wieder Lese- und Schreibzugriff erhalten darf.

Angenommen, ein Storage-Node ist in den reinen Lesemodus verschoben. Wenn das Speichervolume-Lese-Schreib-Wasserzeichen auf 30 GB (Standard) gesetzt ist, muss der freie Speicherplatz auf jedem Speichervolumen im Speicherknoten von 5 GB auf 30 GB ansteigen, bevor der Knoten wieder Lese-/Schreibzugriff erhalten kann.

Der Wert des Speichervolumes-Wasserzeichens für Lesen und Schreiben muss größer sein als der Wert des Speichervolumes Soft-Read-Only-Wasserzeichens.

Verwandte Informationen

"Verwalten vollständiger Speicherknoten"

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

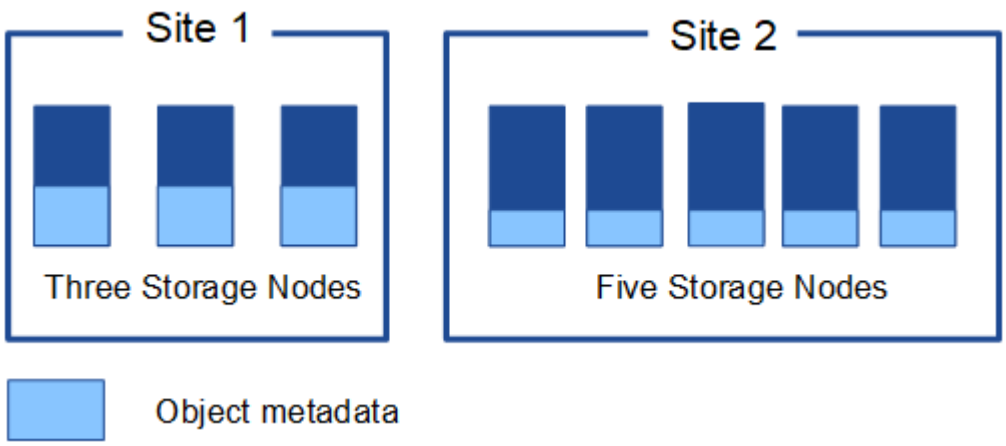
Namen des S3-Buckets oder Swift-Containers, dem Mandanten-Kontonamen oder -ID, der logischen Größe des Objekts, dem Datum und der Uhrzeit der ersten Erstellung des Objekts Und Datum und Uhrzeit der letzten Änderung des Objekts.

- 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?

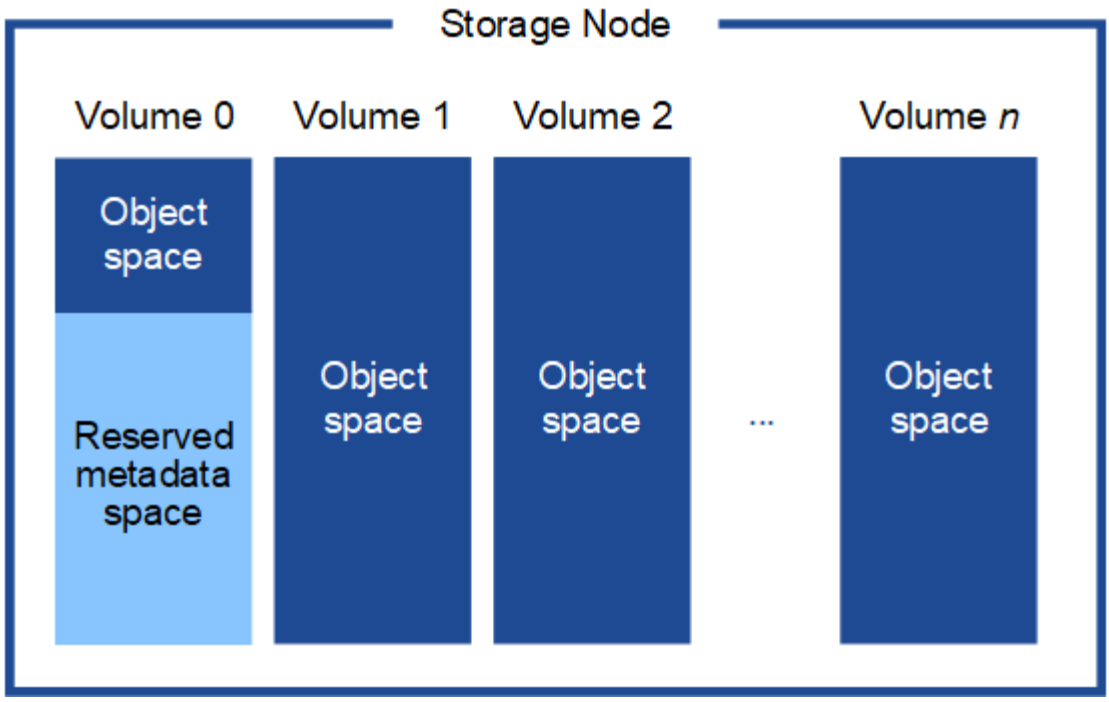
StorageGRID speichert Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert werden. Um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen, speichert StorageGRID drei Kopien der Metadaten für alle Objekte im System an jedem Standort. Die drei Kopien der Objektmetadaten werden gleichmäßig auf alle Storage-Nodes an jedem Standort verteilt.

Diese Abbildung zeigt die Speicherknoten an zwei Standorten. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten, die auf die Storage-Nodes an diesem Standort verteilt werden.



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.

Die Menge an Speicherplatz, die für Objektmetadaten auf einem bestimmten Storage-Node reserviert ist, hängt von einer Reihe von 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 dargestellt, basiert der Standardwert dieser Einstellung für StorageGRID 11.5 auf dem folgenden:

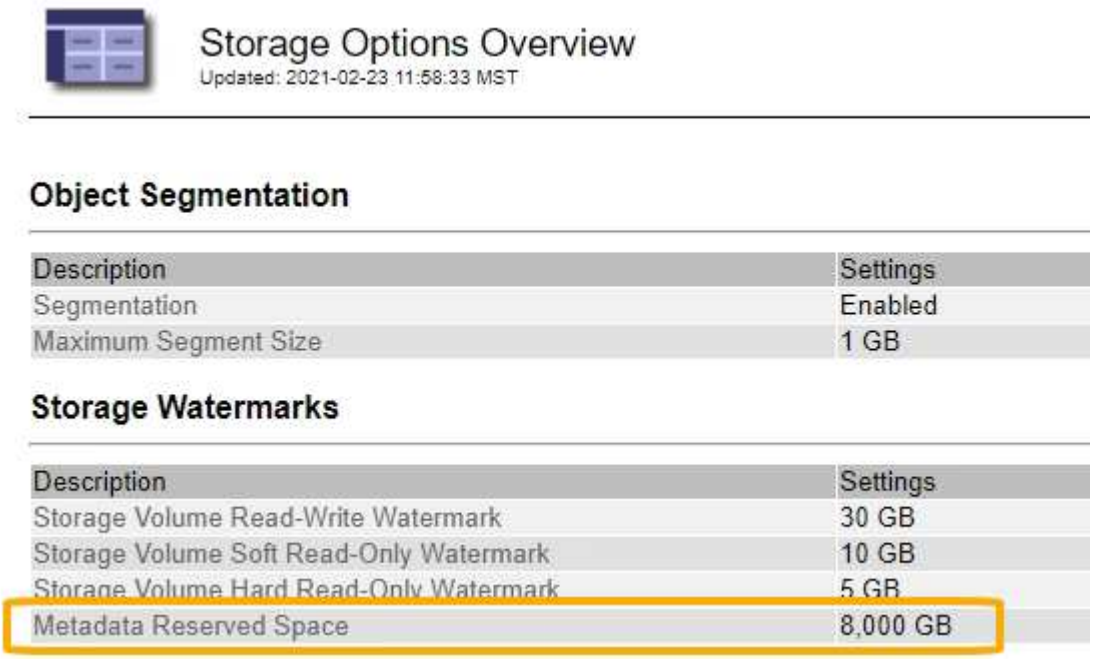
- Die Softwareversion, die Sie bei der Erstinstallation von StorageGRID verwendet haben.
- Die RAM-Menge auf jedem Storage-Node.

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz bei Metadaten für StorageGRID 11.5
11.5	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)

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz bei Metadaten für StorageGRID 11.5
	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)

So zeigen Sie die Einstellung für den reservierten Metadatenspeicherplatz für Ihr StorageGRID-System an:

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Speicheroptionen**.
2. Suchen Sie in der Tabelle Speicherwasserzeichen **Metadatenreservierter Speicherplatz**.



Im Screenshot beträgt der Wert **Metadaten reservierter Speicherplatz** 8,000 GB (8 TB). Dies ist die Standardeinstellung für eine neue StorageGRID 11.5-Installation, bei der jeder Speicherknoten 128 GB oder mehr RAM hat.

Tatsächlich reservierter Speicherplatz für Metadaten

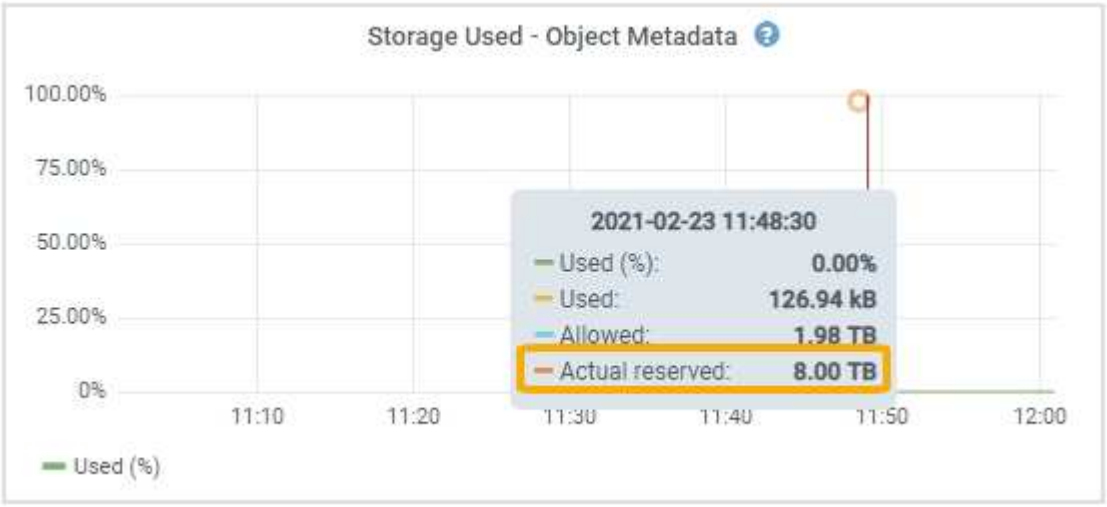
Im Gegensatz zur Einstellung „systemweiter reservierter Speicherplatz für Metadaten“ wird für jeden Storage-Node der_tatsächlich reservierte Speicherplatz_ für Objektmetadaten ermittelt. Für jeden bestimmten Storage-Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des 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

Größe von Volume 0 für den Node	Tatsächlich reservierter Speicherplatz für Metadaten
500 GB oder mehr	Die kleineren Werte: • Lautstärke 0 • Einstellung für reservierten Speicherplatz für Metadaten

So zeigen Sie den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Speicherknoten an:

1. Wählen Sie im Grid Manager die Option **Nodes** > ***Storage Node*** aus.
2. Wählen Sie die Registerkarte **Storage** aus.
3. Bewegen Sie den Cursor über das Diagramm verwendete Speicherdaten — Objektmetadaten 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 11.5 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.

Der **ist-reservierte**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

Beispiel für den tatsächlich reservierten Metadatenspeicherplatz

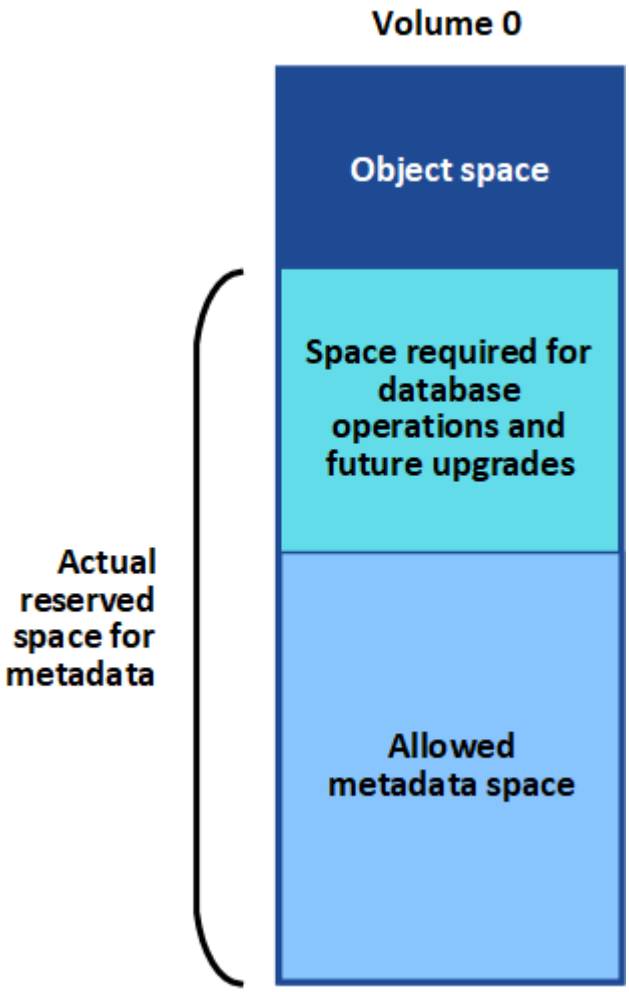
Angenommen, Sie installieren ein neues StorageGRID System unter Verwendung der Version 11.5. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für eine neue StorageGRID 11.5-Installation, wenn jeder Speicherknoten über mehr als 128 GB RAM verfügt.)

- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)

Zulässiger Metadatenspeicherplatz

Der tatsächlich reservierte Speicherplatz jedes Storage-Node für Metadaten wird in den Speicherplatz für Objekt-Metadaten (den „ *zulässigen Metadatenspeicherplatz*“) und den Platzbedarf für wichtige Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.



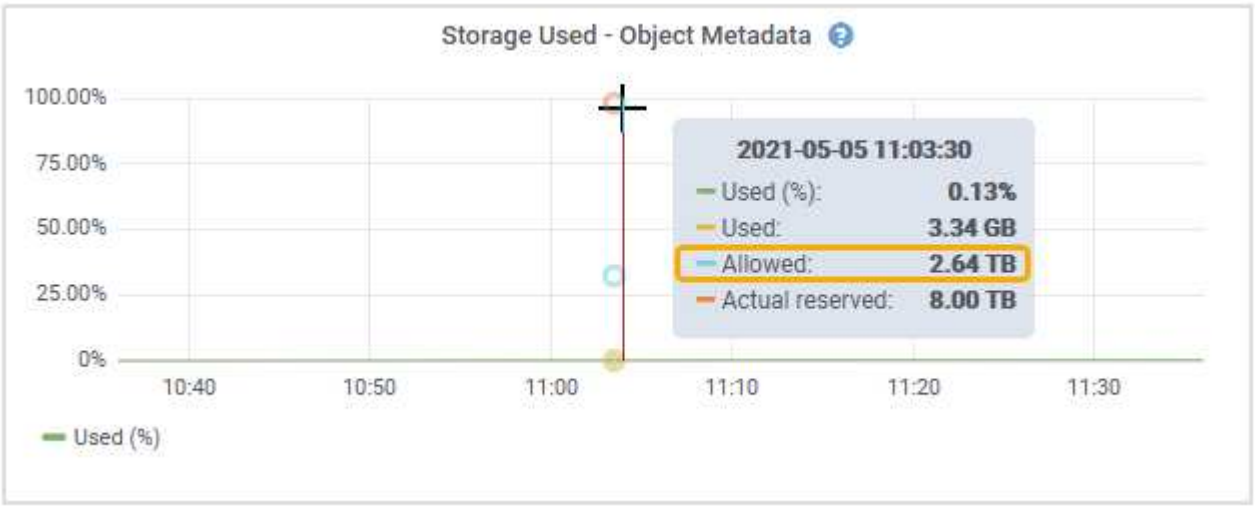
Die folgende Tabelle fasst zusammen, wie StorageGRID den zulässigen Metadatenspeicherplatz für einen Storage-Node bestimmt.

Tatsächlich reservierter Speicherplatz für Metadaten	Zulässiger Metadatenspeicherplatz
4 TB oder weniger	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.98 TB
Mehr als 4 TB	(Tatsächlicher reservierter Speicherplatz für Metadaten − 1 TB) × 60 %, bis zu einem Maximum von 2.64 TB

Wenn Ihr StorageGRID System mehr als 2.64 TB Metadaten auf jedem Storage-Node speichert (oder voraussichtlich gespeichert werden), kann der zulässige Metadatenspeicherplatz in einigen Fällen erhöht werden. Wenn jeweils Ihre Storage-Nodes mehr als 128 GB RAM und freier Speicherplatz auf dem Storage-Volume 0 haben, wenden Sie sich an Ihren NetApp Ansprechpartner. NetApp überprüft ggf. die Anforderungen und erhöht den zulässigen Metadatenspeicherplatz für jeden Storage-Node.

So zeigen Sie den zulässigen Metadatenspeicherplatz für einen Speicherknoten an:

1. Wählen Sie im Grid Manager **Node** > ***Storage Node*** aus.
2. Wählen Sie die Registerkarte **Storage** aus.
3. Bewegen Sie den Cursor über das Diagramm verwendete Speicherdaten — Objektmetadaten und suchen Sie den Wert **zulässig**.



Im Screenshot beträgt der **zulässige**-Wert 2.64 TB, was der maximale Wert für einen Storage Node ist, dessen tatsächlicher reservierter Speicherplatz für Metadaten mehr als 4 TB beträgt.

Der **zulässige**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Beispiel für zulässigen Metadatenspeicherplatz

Angenommen, Sie installieren ein StorageGRID System mit Version 11.5. 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 11.5, 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**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 2.64 TB. (Dies ist der höchste Wert für den tatsächlich reservierten Speicherplatz.)

Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität

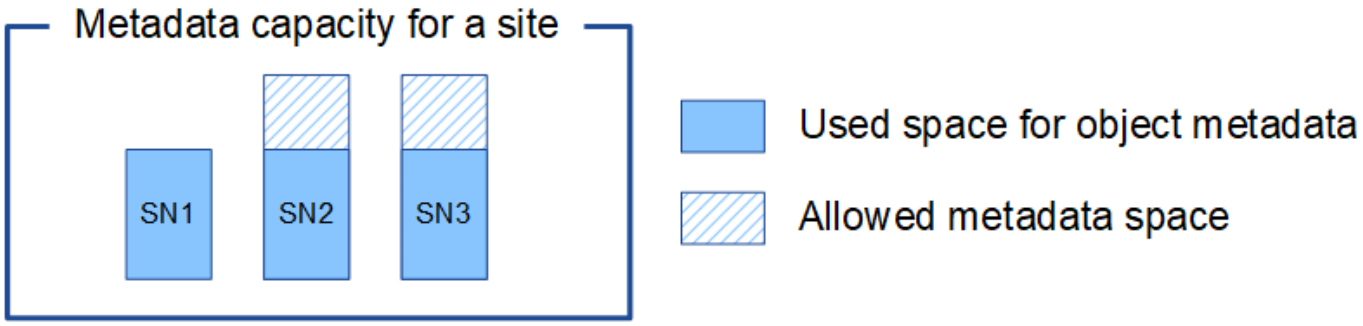
Wie oben beschrieben, verteilt StorageGRID Objektmetadaten gleichmäßig über Storage-Nodes an jedem Standort. Wenn ein Standort Storage-Nodes unterschiedlicher Größen enthält, bestimmt der kleinste Node am Standort die Metadaten-Kapazität des Standorts.

Beispiel:

- Sie haben ein Raster mit drei Storage Nodes unterschiedlicher Größe an einem einzigen Standort.
- Die Einstellung **Metadaten reservierter Platz** beträgt 4 TB.
- Die Storage-Nodes haben die folgenden Werte für den tatsächlich reservierten Metadatenspeicherplatz und den zulässigen Metadatenspeicherplatz.

Storage-Node	Größe von Volumen 0	Tatsächlich reservierter Metadatenspeicherplatz	Zulässiger Metadatenspeicherplatz
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Da Objektmetadaten gleichmäßig auf die Storage-Nodes an einem Standort verteilt werden, kann jeder Node in diesem Beispiel nur 1.32 TB Metadaten enthalten. Der zusätzlich zulässige Metadatenspeicherplatz von 0.66 TB für SN2 und SN3 kann 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

- So überwachen Sie die Objektmetadaten für jeden Storage-Node und -Konfiguration:

  "Monitor Fehlerbehebung"

- Um die Kapazität der Objektmetadaten für Ihr System zu erhöhen, müssen Sie neue Storage-Nodes hinzufügen:

  "Erweitern Sie Ihr Raster"

Globale Einstellungen für gespeicherte Objekte konfigurieren

Mit den Grid-Optionen können Sie die Einstellungen für alle Objekte konfigurieren, die in Ihrem StorageGRID-System gespeichert sind, einschließlich gespeicherter Objektkomprimierung und gespeicherter Objektverschlüsselung. Und gespeichertes Objekt-Hashing.

- "Konfigurieren der gespeicherten Objektkomprimierung"
- "Konfigurieren der gespeicherten Objektverschlüsselung"
- "Konfigurieren von gespeichertes Objekt-Hashing"

Konfigurieren der gespeicherten Objektkomprimierung

Über die Grid-Option „gespeicherte Objekte komprimieren“ lässt sich die Größe der in StorageGRID gespeicherten Objekte reduzieren, sodass Objekte weniger Storage belegen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die Grid-Option „gespeicherte Objekte komprimieren“ ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, versucht StorageGRID, jedes Objekt beim Speichern mit verlustfreier 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 diese Option aktivieren, beachten Sie Folgendes:

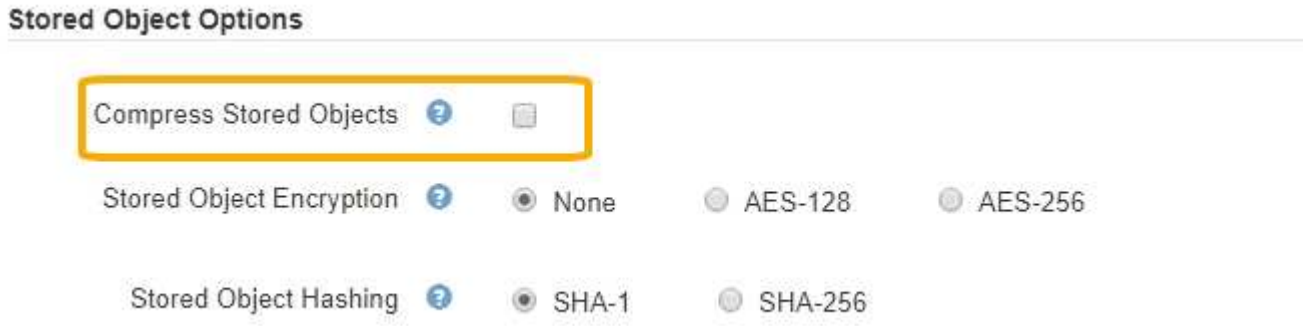
- Die Komprimierung sollte nur aktiviert werden, wenn die gespeicherten Daten komprimierbar sind.
- Applikationen, die Objekte in StorageGRID speichern, komprimieren möglicherweise Objekte, bevor sie gespeichert werden. Wenn bereits eine Client-Applikation ein Objekt komprimiert hat, bevor sie in StorageGRID gespeichert wird, wird die Komprimierung gespeicherter Objekte die Größe eines Objekts nicht weiter verringert.
- Aktivieren Sie die Komprimierung nicht, wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn die Grid-Option „gespeicherte Objekte komprimieren“ aktiviert ist, sollten S3- und Swift-Client-Applikationen die AUSFÜHRUNG VON GET-Objektoperationen vermeiden, die einen Bereich von 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.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Optionen für gespeicherte Objekte das Kontrollkästchen **gespeicherte Objekte komprimieren**.



3. Klicken Sie Auf **Speichern**.

Konfigurieren der gespeicherten Objektverschlüsselung

Sie können gespeicherte Objekte verschlüsseln, wenn Sie sicherstellen möchten, dass die Daten bei einer Gefährdung eines Objektspeichers nicht in lesbarer Form abgerufen werden können. Objekte sind standardmäßig nicht verschlüsselt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme durch S3 oder Swift. 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 aktuell verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

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.

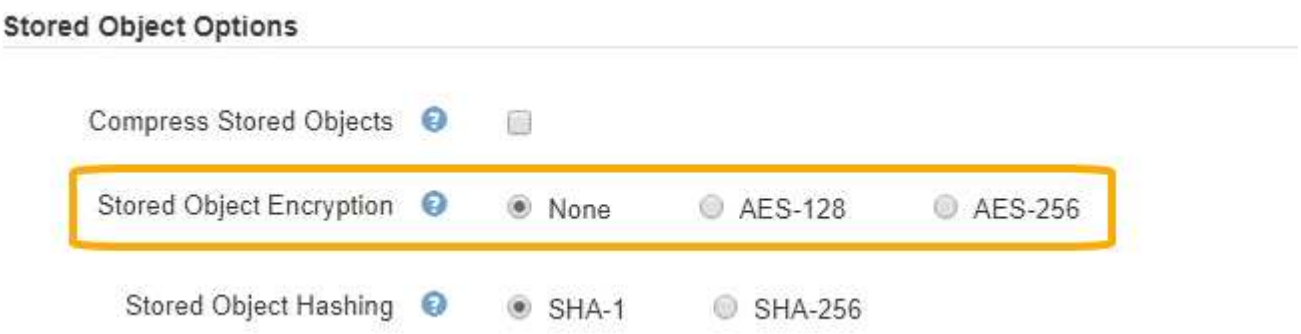
Gespeicherte Objekte können mit dem Verschlüsselungsalgorithmus AES-128 oder AES-256 verschlüsselt werden.

Die Einstellung „gespeicherte Objektverschlüsselung“ gilt nur für S3 Objekte, die nicht durch Verschlüsselung auf Bucket- oder Objektebene verschlüsselt wurden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.

2. Ändern Sie im Abschnitt Speicherte Objektoptionen die gespeicherte Objektverschlüsselung in **Keine** (Standard), **AES-128** oder **AES-256**.



3. Klicken Sie Auf **Speichern**.

Konfigurieren von gespeichertes Objekt-Hashing

Die Option „Speichertes Objekt-Hashing“ gibt den Hash-Algorithmus an, der zur Überprüfung der Objektintegrität verwendet wird.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

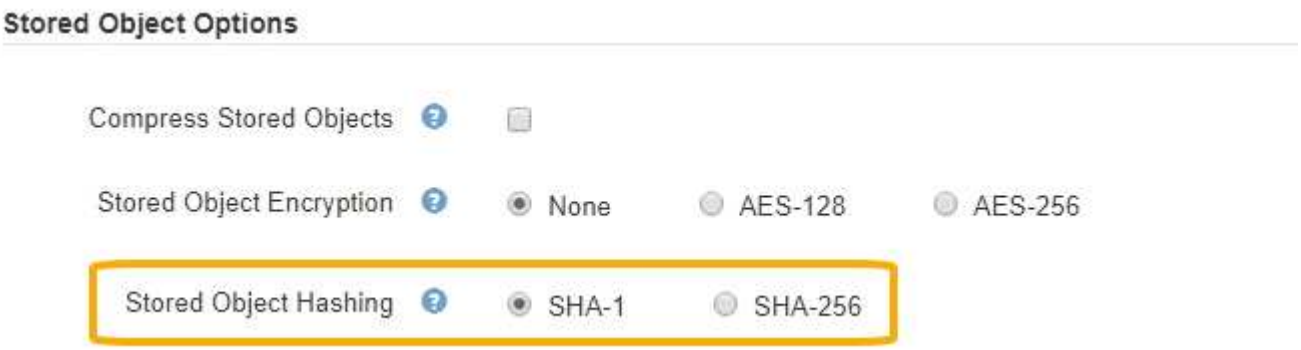
Über diese Aufgabe

Standardmäßig werden Objektdaten mit dem SHA-1-Algorithmus gehasht. Der SHA-256-Algorithmus erfordert zusätzliche CPU-Ressourcen und wird im Allgemeinen nicht für die Integritätsprüfung empfohlen.

> 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.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.
2. Ändern Sie im Abschnitt „Optionen für gespeicherte Objekte“ die Option „gespeicherte Objekt-Hashing“ in **SHA-1** (Standardeinstellung) oder **SHA-256**.



3. Klicken Sie Auf **Speichern**.

Konfigurationseinstellungen für Storage-Nodes

Jeder Storage Node verwendet eine Reihe von Konfigurationseinstellungen und Zählern. 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.

So greifen Sie auf die Konfigurationseinstellungen und Zähler eines Speicherknotens zu:

1. Wählen Sie **Support** > **Tools** > **Grid Topology** 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 des HTTP-Protokolls für S3, Swift und andere interne StorageGRID-Zugriffe: • Offline: Es sind keine Vorgänge zulässig. Jede Client-Anwendung, die versucht, eine HTTP-Sitzung für den LDR-Dienst zu öffnen, erhält eine Fehlermeldung. Aktive Sitzungen werden ordnungsgemäß geschlossen. • Online: Der Vorgang wird normal fortgesetzt
Automatisches Starten von HTTP	HTAS	• Wenn diese Option ausgewählt ist, hängt der Zustand des Systems beim Neustart vom Status der Komponente **LDR** > **Storage** ab. Wenn die Komponente **LDR** > **Storage** beim Neustart schreibgeschützt ist, ist auch die HTTP-Schnittstelle schreibgeschützt. Wenn die Komponente **LDR** > **Speicherung** Online ist, ist HTTP auch Online. Andernfalls bleibt die HTTP-Schnittstelle im Status Offline. • Wenn diese Option nicht aktiviert ist, bleibt die HTTP-Schnittstelle offline, bis sie explizit aktiviert ist.

LDR > Datenspeicher

Attributname	Codieren	Beschreibung
Anzahl Verlorener Objekte Zurücksetzen	RCOR	Setzen Sie den Zähler für die Anzahl der verlorenen Objekte dieses Dienstes zurück.

LDR > Storage

Attributname	Codieren	Beschreibung
Storage-Zustand - Gewünscht	SSDS	Eine vom Benutzer konfigurierbare Einstellung für den gewünschten Status der Speicherkomponente. Der LDR-Dienst liest diesen Wert und versucht, den durch dieses Attribut angegebenen Status zu entsprechen. Der Wert wird bei Neustarts dauerhaft verwendet. Mit dieser Einstellung können Sie beispielsweise dazu zwingen, dass Speicher schreibgeschützt wird, selbst wenn genügend Speicherplatz vorhanden ist. Dies kann bei der Fehlerbehebung hilfreich sein. Das Attribut kann einen der folgenden Werte annehmen: • Offline: Wenn der gewünschte Status Offline ist, schaltet der LDR-Dienst die **LDR** > **Storage** -Komponente offline. • Schreibgeschützt: Wenn der gewünschte Status schreibgeschützt ist, verschiebt der LDR-Service den Speicherstatus auf schreibgeschützt und hört auf, neue Inhalte zu akzeptieren. Beachten Sie, dass Inhalte möglicherweise noch für kurze Zeit im Speicherknoten gespeichert werden, bis offene Sitzungen geschlossen sind. • Online: Den Wert bei Online während des normalen Systembetriebs belassen. Der Speicherstatus – der aktuelle Status der Speicherkomponente wird durch den Service dynamisch festgelegt, basierend auf dem Zustand des LDR-Service, z. B. der Menge des verfügbaren Objektspeicherspeichers. Wenn der Speicherplatz knapp ist, ist die Komponente schreibgeschützt.
Zeitüberschreitung Bei Der Integritätsprüfung	SHCT	Die Zeitgrenze in Sekunden, innerhalb derer ein Integritätstest abgeschlossen werden muss, damit ein Speichervolumen als ordnungsgemäß angesehen wird. Ändern Sie diesen Wert nur, wenn Sie dazu vom Support aufgefordert werden.

LDR > Verifizierung

Attributname	Codieren	Beschreibung
Fehlende Objekte Zurücksetzen Anzahl	VCMI	Setzt die Anzahl der erkannten fehlenden Objekte zurück (OMIS). Erst nach Abschluss der Vordergrundüberprüfung verwenden. Fehlende replizierte Objektdaten werden vom StorageGRID System automatisch wiederhergestellt.
Verifizieren	FVOV	Wählen Sie Objektspeichern aus, bei denen die Vordergrundüberprüfung durchgeführt werden soll.
Verifizierungsrate	VPRI	Legen Sie die Geschwindigkeit fest, mit der die Hintergrundüberprüfung durchgeführt wird. Weitere Informationen zur Konfiguration der Hintergrundverifizierungsrate 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). Weitere Informationen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.
Objekte In Quarantäne Löschen	OQRT	Löschen Sie beschädigte Objekte aus dem Quarantäneverzeichnis, setzen Sie die Anzahl der isolierten Objekte auf Null zurück und löschen Sie den Alarm „Quarantäne Objekte erkannt“ (OQRT). Diese Option wird verwendet, nachdem beschädigte Objekte vom StorageGRID-System automatisch wiederhergestellt wurden. Wenn ein Alarm „Lost Objects“ ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen. In manchen Fällen können isolierte Objekte für die Datenwiederherstellung oder das Debuggen der zugrunde liegenden Probleme, die die beschädigten Objektkopien verursacht haben, nützlich sein.

LDR > Erasure Coding

Attributname	Codieren	Beschreibung
Zurücksetzen Der Fehleranzahl Für Schreibvorgänge	RWF.	Setzen Sie den Zähler auf Schreibfehler von Objektdaten mit Erasure-Coding-Verfahren auf den Storage-Node zurück.

Attributname	Codieren	Beschreibung
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 Löschfehler von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.
Beschädigte Kopien Erkannte Anzahl Zurücksetzen	RSCC	Setzen Sie den Zähler für die Anzahl beschädigter Kopien von Objektdaten, die nach dem Erasure-Coding-Verfahren codiert wurden, auf dem Storage-Node zurück.
Beschädigte Fragmente Erkannte Anzahl Zurücksetzen	RCD	Setzen Sie den Zähler auf beschädigte Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage-Node zurück.
Fehlende Fragmente Erkannt Anzahl Zurücksetzen	RSMD	Setzen Sie den Zähler auf fehlende Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage Node zurück. Erst nach Abschluss der Vordergrundüberprüfung 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.

Attributname	Codieren	Beschreibung
Deaktivieren Sie Inbound Replication	DSIR	Wählen Sie diese Option aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen. Wenn die eingehende Replikation deaktiviert ist, können Objekte vom Speicherknoten zum Kopieren an andere Speicherorte im StorageGRID-System abgerufen werden, Objekte können jedoch nicht von anderen Speicherorten aus zu diesem Speicherknoten kopiert werden: Der LDR-Dienst ist schreibgeschützt.
Deaktivieren Sie Ausgehende Replikation	DSOR	Wählen Sie diese Option aus, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abrufvorgänge) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen. Wenn die ausgehende Replikation deaktiviert ist, können Objekte auf diesen Speicherknoten kopiert werden. Objekte können jedoch nicht vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der LDR-Service ist schreibgeschützt.

Verwandte Informationen

"Monitor Fehlerbehebung"

Verwalten vollständiger Speicherknoten

Wenn Storage-Nodes die Kapazität erreichen, müssen Sie das StorageGRID System durch Hinzufügen eines neuen Storage erweitern. Es sind drei Optionen verfügbar: Das Hinzufügen von Storage Volumes, das Hinzufügen von Shelfs zur Storage-Erweiterung und das Hinzufügen von Storage-Nodes.

Hinzufügen von Storage-Volumes

Jeder Storage-Node unterstützt eine maximale Anzahl an Storage-Volumes. Der definierte Höchstwert variiert je nach Plattform. Wenn ein Storage-Node weniger als die maximale Anzahl an Storage-Volumes enthält, können Sie Volumes hinzufügen, um seine Kapazität zu erhöhen. Anweisungen zum erweitern eines StorageGRID-Systems finden Sie in den Anweisungen.

Hinzufügen von Shelfs zur Storage-Erweiterung

Einige Storage-Nodes von StorageGRID Appliances, z. B. SG6060, können zusätzliche Storage-Shelfs unterstützen. Bei StorageGRID Appliances mit Erweiterungsfunktionen, die nicht bereits auf die maximale Kapazität erweitert wurden, können Sie Storage-Shelfs zur Steigerung der Kapazität hinzufügen. Anweisungen zum erweitern eines StorageGRID-Systems finden Sie in den Anweisungen.

Speicherknoten Werden Hinzugefügt

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. Anweisungen zum erweitern eines StorageGRID-Systems finden Sie in den Anweisungen.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

Verwalten Von Admin-Nodes

Jeder Standort in einer StorageGRID Implementierung kann einen oder mehrere Admin-Nodes enthalten.

- "Was ist ein Admin-Node"
- "Mehrere Admin-Nodes werden verwendet"
- "Identifizieren des primären Admin-Knotens"
- "Auswählen eines bevorzugten Senders"
- "Anzeigen von Benachrichtigungsstatus und -Warteschlangen"
- "So zeigen Admin-Knoten bestätigte Alarme an (Legacy-System)"
- "Konfigurieren des Zugriffs auf Audit-Clients"

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.

Admin-Nodes hosten die folgenden Services:

- AMS-Service
- CMN-Service
- NMS-Service
- Prometheus Service
- Load Balancer- und High Availability-Services (zur Unterstützung von S3- und Swift-Client-Datenverkehr)

Admin-Nodes unterstützen außerdem die Management Application Program Interface (Management-API) zur Verarbeitung von Anfragen aus der Grid Management API und der Mandanten-Management-API.

Was ist der AMS-Service

Der Audit Management System (AMS)-Dienst verfolgt Systemaktivität und -Ereignisse.

Was der CMN-Service ist

Der Configuration Management Node (CMN)-Dienst verwaltet systemweite Konfigurationen von Konnektivität und Protokollfunktionen, die von allen Diensten benötigt werden. Darüber hinaus wird der CMN-Dienst zur Ausführung und Überwachung von Grid-Aufgaben verwendet. Es gibt nur einen CMN-Service pro StorageGRID-Implementierung. Der Admin-Node, der den CMN-Service hostet, wird als primärer Admin-Node bezeichnet.

Was ist der NMS-Service

Der NMS-Dienst (Network Management System) steuert die Überwachungs-, Reporting- und Konfigurationsoptionen, die über den Grid Manager, die browserbasierte Schnittstelle des StorageGRID-Systems, angezeigt werden.

Was der Prometheus Service ist

Der Prometheus Service sammelt Zeitreihungsmetriken aus den Services auf allen Knoten.

Verwandte Informationen

"Verwenden der Grid-Management-API"

"Verwenden Sie ein Mandantenkonto"

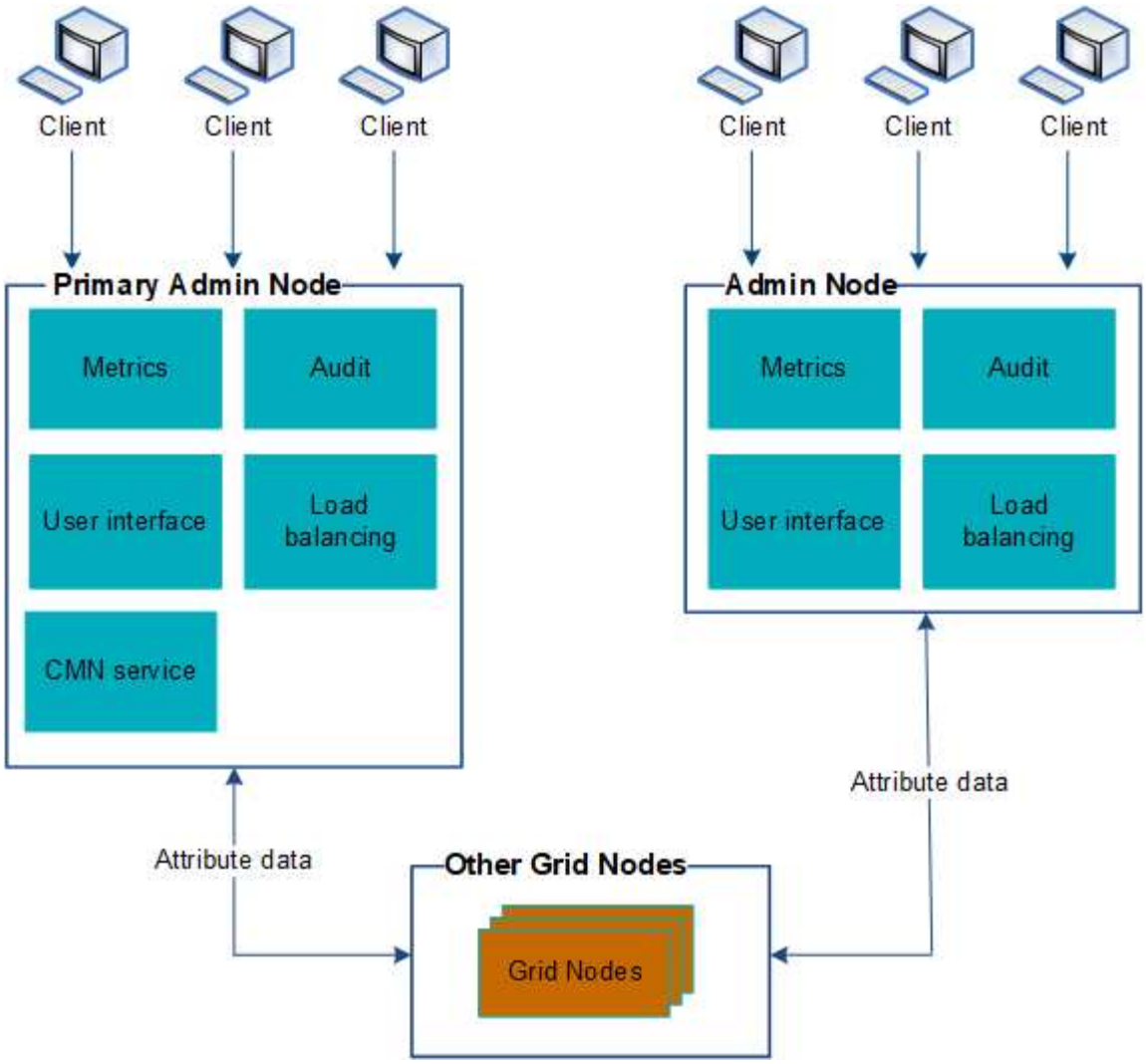
"Managen des Lastausgleichs"

"Verwalten von Hochverfügbarkeitsgruppen"

Mehrere Admin-Nodes werden verwendet

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 die von einem Admin-Knoten ausgemachten Alarmbestätigungen nicht auf 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.

> Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der Master 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.

Verwandte Informationen

"Verwalten von Hochverfügbarkeitsgruppen"

Identifizieren des primären Admin-Knotens

Der primäre Admin-Node hostet den CMN-Service. Einige Wartungsarbeiten können nur mit dem primären Admin-Node durchgeführt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > **Admin Node** und klicken Sie dann auf ➕ 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.

Auswählen eines bevorzugten Senders

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten enthält, können Sie auswählen, welcher Admin-Knoten der bevorzugte Absender von Benachrichtigungen sein soll. Standardmäßig ist der primäre Admin-Node ausgewählt, aber jeder Admin-Node kann der bevorzugte Absender sein.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Auf der Seite **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen** wird angezeigt, welcher Admin-Node derzeit als bevorzugter Absender ausgewählt wurde. Der primäre Admin-Node ist standardmäßig ausgewählt.

Bei normalen Systemvorgängen sendet nur der bevorzugte Absender folgende Benachrichtigungen:

- AutoSupport Nachrichten
- SNMP-Benachrichtigungen
- E-Mails benachrichtigen
- Alarm-E-Mails (älteres System)

Alle anderen Admin-Knoten (Standby-Sender) überwachen jedoch den bevorzugten Sender. Wenn ein Problem erkannt wird, kann ein Standby-Sender diese Benachrichtigungen auch senden.

In diesen Fällen können sowohl der bevorzugte Sender als auch ein Standby-Sender Benachrichtigungen senden:

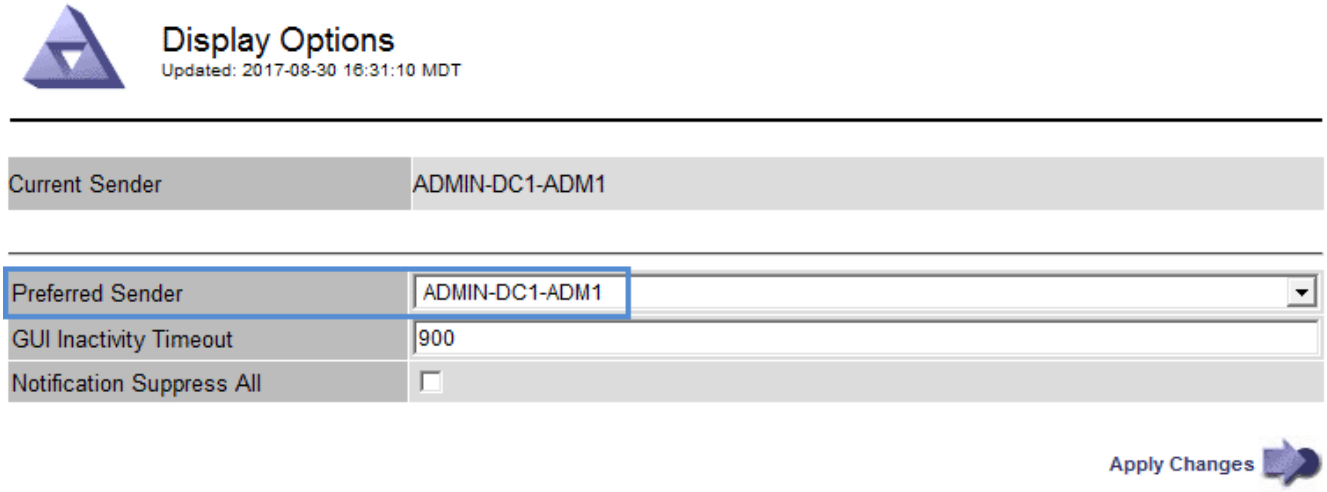
- Wenn Admin-Knoten von einander “islanded” werden, werden sowohl der bevorzugte Sender als auch die Standby-Sender versuchen, Benachrichtigungen zu senden, und mehrere Kopien von Benachrichtigungen können empfangen werden.

- Nachdem ein Standby-Sender Probleme mit dem bevorzugten Sender erkannt hat und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Sender seine Fähigkeit zum Senden von Benachrichtigungen wiederherstellen. 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 Alarmbenachrichtigungen und AutoSupport-Meldungen testen, senden alle Admin-Knoten die Test-E-Mail. Wenn Sie die Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Verbindung zu überprüfen.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie im Menü Anzeigeoptionen die Option **Optionen**.
3. Wählen Sie in der Dropdown-Liste den Admin-Knoten aus, den Sie als bevorzugten Sender festlegen möchten.



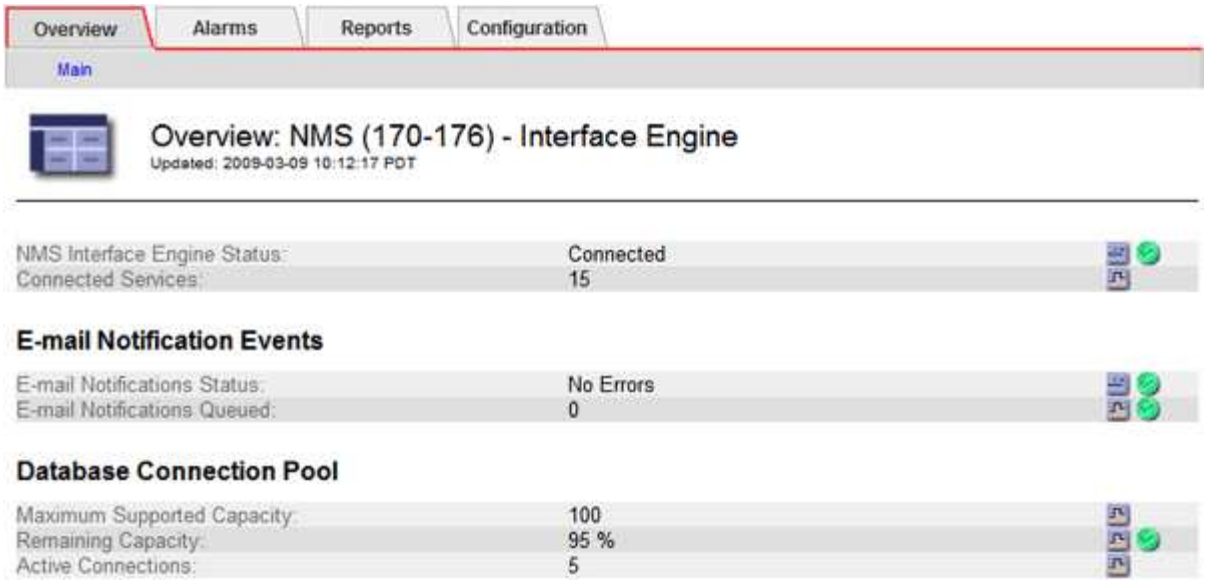
4. Klicken Sie Auf **Änderungen Übernehmen**.

   Der Admin-Node wird als bevorzugter Absender von Benachrichtigungen festgelegt.

Anzeigen von Benachrichtigungsstatus und -Warteschlangen

Der NMS-Dienst 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 Topology**. Wählen Sie schließlich ***site*** > ***Admin Node*** > **NMS** > **Interface Engine** aus.

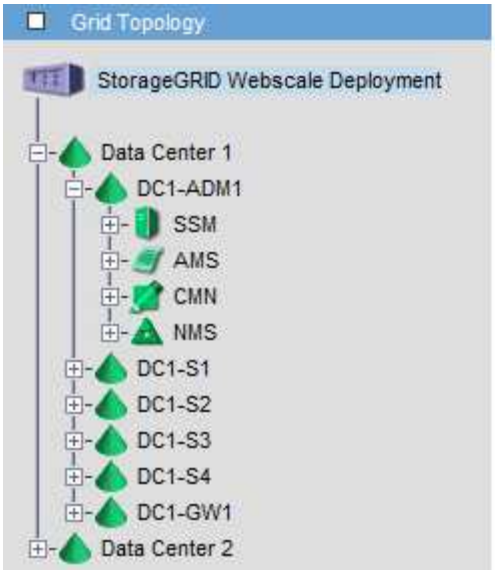


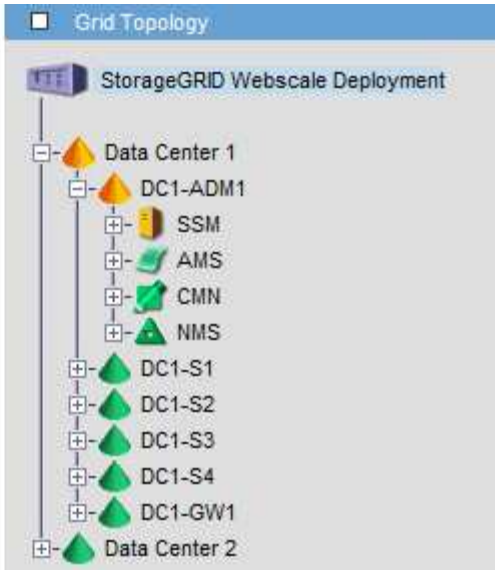
Benachrichtigungen werden über die E-Mail-Benachrichtigungswarteschlange verarbeitet und an den Mail-Server gesendet, einer nach dem anderen in der Reihenfolge, in der sie ausgelöst werden. Wenn ein Problem auftritt (z. B. ein Netzwerkverbindungsfehler) und der Mail-Server nicht verfügbar ist, wenn versucht wird, die Benachrichtigung zu senden, wird der Versuch unternommen, die Benachrichtigung an den Mailserver erneut zu senden, 60 Sekunden lang fortgesetzt. Wenn die Benachrichtigung nach 60 Sekunden nicht an den Mailserver gesendet wird, wird die Benachrichtigung aus der Benachrichtigungswarteschlange gelöscht und es wird versucht, die nächste Benachrichtigung in der Warteschlange zu senden. Da Benachrichtigungen aus der Benachrichtigungswarteschlange gelöscht werden können, ohne gesendet zu werden, ist es möglich, dass ein Alarm ausgelöst werden kann, ohne dass eine Benachrichtigung gesendet wird. Wenn eine Benachrichtigung aus der Warteschlange gelöscht wird, ohne gesendet zu werden, wird der Minor-Alarm FÜR MINUTEN (E-Mail-Benachrichtigungsstatus) ausgelöst.

So zeigen Admin-Knoten bestätigte Alarme an (Legacy-System)

Wenn Sie einen Alarm an einem Admin-Knoten bestätigen, wird der bestätigte Alarm nicht auf einen anderen Admin-Knoten kopiert. Da Danksagungen nicht auf andere Admin-Knoten kopiert werden, sieht die Struktur der Grid Topology 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

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. Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, lässt sich der Client-Zugriff auf Audit-Freigaben für CIFS und NFS konfigurieren.

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 in den Anweisungen zum Verständnis von Überwachungsmeldungen.

Wenn Sie CIFS oder NFS verwenden möchten, wählen Sie NFS.

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Verwandte Informationen

"Was ist ein Admin-Node"

"Prüfung von Audit-Protokollen"

"Software-Upgrade"

Konfigurieren von Audit-Clients für CIFS

Das Verfahren zum Konfigurieren eines Audit-Clients hängt von der Authentifizierungsmethode ab: Windows Workgroup oder Windows Active Directory (AD). Wenn diese Option hinzugefügt wird, wird die Revisionsfreigabe automatisch als schreibgeschützte Freigabe aktiviert.

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Verwandte Informationen

"Software-Upgrade"

Konfigurieren von Audit-Clients für Workgroup

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

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

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

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „geprüft“ aufweisen: `storagegrid-status`

   Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
-------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------
```

5. Legen Sie die Authentifizierung für die Windows Workgroup fest:

   Wenn die Authentifizierung bereits festgelegt wurde, wird eine Beratungsmeldung angezeigt. Wenn die Authentifizierung bereits festgelegt wurde, fahren Sie mit dem nächsten Schritt fort.

   a. Geben Sie Ein: `set-authentication`
   b. Wenn Sie zur Installation von Windows Workgroup oder Active Directory aufgefordert werden, geben Sie Folgendes ein: `workgroup`
   c. Geben Sie bei der entsprechenden Aufforderung einen Namen für die Arbeitsgruppe ein: *`workgroup_name`*
   d. Erstellen Sie bei Aufforderung einen aussagekräftigen NetBIOS-Namen: *`netbios_name`*

      Oder

      Drücken Sie **Enter**, um den Hostnamen des Admin-Knotens als NetBIOS-Name zu verwenden.

   Das Skript startet den Samba-Server neu und es werden Änderungen vorgenommen. Dies sollte weniger als eine Minute dauern. Fügen Sie nach dem Festlegen der Authentifizierung einen Audit-Client hinzu.

   a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Hinzufügen eines Audit-Clients:

   a. Geben Sie Ein: `add-audit-share`

      Die Freigabe wird automatisch als schreibgeschützt hinzugefügt.

   b. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: *`user`*
   c. Geben Sie bei der entsprechenden Aufforderung den Benutzernamen für die Prüfung ein: *`audit_user_name`*
   d. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den Benutzer der Prüfung ein: *`password`*
   e. Geben Sie bei der entsprechenden Aufforderung dasselbe Passwort erneut ein, um es zu bestätigen:

password

f. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

> Es ist nicht erforderlich, ein Verzeichnis einzugeben. Der Name des Überwachungsverzeichnisses ist vordefiniert.

7. Wenn mehr als ein Benutzer oder eine Gruppe auf die Revisionsfreigabe zugreifen darf, fügen Sie die zusätzlichen Benutzer hinzu:

a. Geben Sie Ein: `add-user-to-share`

Es wird eine nummerierte Liste mit aktivierten Freigaben angezeigt.

b. Geben Sie bei der entsprechenden Aufforderung die Nummer der Freigabe für den Audit-Export ein: *share_number*

c. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user`

Oder `group`

d. Geben Sie bei Aufforderung den Namen des Audit-Benutzers oder der Gruppe ein: *audit_user or audit_group*

e. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

f. Wiederholen Sie diese Teilschritte für jeden weiteren Benutzer oder jede Gruppe, die Zugriff auf die Revisionsfreigabe hat.

8. Überprüfen Sie optional die Konfiguration: `validate-config`

Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Die Konfiguration des Audit-Clients wird angezeigt.

b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`

10. Starten Sie den Samba-Dienst: `service smbd start`
11. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

    Oder

    Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten enthält, aktivieren Sie diese Revisionsfreigabe 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 die Schritte, um die Revisionsfreigabe für jeden zusätzlichen Admin-Knoten zu konfigurieren.
    c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
12. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

"Software-Upgrade"

Konfigurieren von Audit-Clients für Active Directory

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen über den Benutzernamen und das Kennwort für das CIFS Active Directory verfügen.
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

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

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

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „geprüft“ aufweisen: `storagegrid-status`

   Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg**+**C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Legen Sie die Authentifizierung für Active Directory fest: `set-authentication`

   In den meisten Bereitstellungen müssen Sie die Authentifizierung festlegen, bevor Sie den Audit-Client hinzufügen. Wenn die Authentifizierung bereits festgelegt wurde, wird eine Beratungsmeldung angezeigt. Wenn die Authentifizierung bereits festgelegt wurde, fahren Sie mit dem nächsten Schritt fort.

   a. Bei Aufforderung zur Workgroup- oder Active Directory-Installation: `ad`
   b. Geben Sie bei der entsprechenden Aufforderung den Namen der AD-Domäne ein (kurzer Domain-Name).
   c. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den DNS-Hostnamen des Domänencontrollers ein.
   d. Geben Sie bei entsprechender Aufforderung den vollständigen Domänennamen ein.

      Verwenden Sie Großbuchstaben.

   e. Geben Sie bei Aufforderung zur Aktivierung der Winbindunterstützung **y** ein.

      Winbind wird verwendet, um Benutzer- und Gruppeninformationen von AD-Servern zu lösen.

   f. Geben Sie bei entsprechender Aufforderung den NetBIOS-Namen ein.
   g. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Treten Sie der Domäne bei:

   a. Wenn noch nicht gestartet, starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`
   b. Treten Sie der Domäne bei: `join-domain`

c. Sie werden aufgefordert zu testen, ob der Admin-Knoten derzeit ein gültiges Mitglied der Domain ist. Wenn dieser Admin-Node der Domäne noch nicht beigetreten ist, geben Sie Folgendes ein: `no`

d. Geben Sie bei entsprechender Aufforderung den Benutzernamen des Administrators an: *`administrator_username`*

   Wo *`administrator_username`* Ist der Benutzername für das CIFS Active Directory, nicht der StorageGRID-Benutzername.

e. Geben Sie bei entsprechender Aufforderung das Administratorpasswort an: *`administrator_password`*

   Waren *`administrator_password`* Ist der Benutzername für das CIFS-Active-Verzeichnis und nicht das StorageGRID-Kennwort.

f. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

7. Vergewissern Sie sich, dass Sie der Domäne ordnungsgemäß beigetreten sind:

   a. Treten Sie der Domäne bei: `join-domain`

   b. Wenn Sie aufgefordert werden, zu testen, ob der Server derzeit ein gültiges Mitglied der Domäne ist, geben Sie Folgendes ein: `y`

      Wenn Sie die Meldung „`Join is OK,`“ erhalten, haben Sie sich erfolgreich der Domäne angeschlossen. Wenn diese Antwort nicht angezeigt wird, versuchen Sie, die Authentifizierung zu aktivieren und die Domain erneut anzuschließen.

   c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

8. Hinzufügen eines Audit-Clients: `add-audit-share`

   a. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe hinzuzufügen, geben Sie Folgendes ein: `user`

   b. Wenn Sie zur Eingabe des Benutzernamens für die Prüfung aufgefordert werden, geben Sie den Benutzernamen für die Prüfung ein.

   c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

9. Wenn mehr als ein Benutzer oder eine Gruppe auf die Revisionsfreigabe zugreifen darf, fügen Sie weitere Benutzer hinzu: `add-user-to-share`

   Es wird eine nummerierte Liste mit aktivierten Freigaben angezeigt.

   a. Geben Sie die Nummer der Freigabe für den Audit-Export ein.

   b. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe hinzuzufügen, geben Sie Folgendes ein: `group`

      Sie werden aufgefordert, den Namen der Überwachungsgruppe anzugeben.

c. Wenn Sie zur Eingabe des Namens der Überwachungsgruppe aufgefordert werden, geben Sie den Namen der Benutzergruppe für die Prüfung ein.

d. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

e. Wiederholen Sie diesen Schritt für jeden weiteren Benutzer oder jede Gruppe, der Zugriff auf die Revisionsfreigabe hat.

10. Überprüfen Sie optional die Konfiguration: `validate-config`

    Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-interfaces.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-filesystem.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-interfaces.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-custom-config.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-shares.inc`
    - Rlimit_max: Anstieg von rlimit_max (1024) auf Windows-Minimum (16384)

    > Kombinieren Sie die Einstellung 'security=ads' nicht mit dem Parameter 'Password Server'. (Standardmäßig erkennt Samba das korrekte DC, um automatisch Kontakt aufzunehmen).

    i. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um die Konfiguration des Audit-Clients anzuzeigen.

    ii. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

        Das CIFS-Konfigurationsprogramm wird angezeigt.

11. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`

12. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

    Oder

    Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten enthält, aktivieren Sie optional die folgenden 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 beim Admin-Node: `exit`

13. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

"Software-Upgrade"

Hinzufügen eines Benutzers oder einer Gruppe zu einer CIFS-Revisionsfreigabe

Sie können einen Benutzer oder eine Gruppe zu einer CIFS-Revisionsfreigabe hinzufügen, die in die AD-Authentifizierung integriert ist.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Das folgende Verfahren gilt für eine mit AD-Authentifizierung integrierte Audit-Freigabe.

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

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

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

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

   Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
-------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------------
```

5. Beginnen Sie mit dem Hinzufügen eines Benutzers oder einer Gruppe: `add-user-to-share`

   Eine nummerierte Liste der konfigurierten Audit-Shares wird angezeigt.

6. Wenn Sie dazu aufgefordert werden, geben Sie die Nummer für die Revisionsfreigabe ein (Audit-Export): *`audit_share_number`*

   Sie werden gefragt, ob Sie einem Benutzer oder einer Gruppe Zugriff auf diese Revisionsfreigabe gewähren möchten.

7. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user` Oder `group`
8. Wenn Sie zur Eingabe des Benutzer- oder Gruppennamens für diese AD-Revisionsfreigabe aufgefordert werden, geben Sie den Namen ein.

   Der Benutzer oder die Gruppe wird als schreibgeschützt für die Revisionsfreigabe sowohl im Betriebssystem des Servers als auch im CIFS-Dienst hinzugefügt. Die Samba-Konfiguration wird neu geladen, damit der Benutzer oder die Gruppe auf die Audit-Client-Freigabe zugreifen können.

9. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

10. Wiederholen Sie diese Schritte für jeden Benutzer oder jede Gruppe, der Zugriff auf die Revisionsfreigabe hat.
11. Überprüfen Sie optional die Konfiguration: `validate-config`

    Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

    - Kann die Datei /etc/samba/includes/cifs-interfaces.inc nicht finden
    - Kann die Datei /etc/samba/includes/cifs-filesystem.inc nicht finden
    - Kann die Datei /etc/samba/includes/cifs-custom-config.inc nicht finden
    - Kann die Datei /etc/samba/includes/cifs-shares.inc nicht finden

      i. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um die Konfiguration des Audit-Clients anzuzeigen.

ii. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

12. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
13. Ermitteln Sie wie folgt, ob zusätzliche Audit-Shares 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 eines 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 Admin-Knoten zu konfigurieren.
      iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
14. Melden Sie sich aus der Befehlsshell ab: `exit`

Entfernen eines Benutzers oder einer Gruppe aus einer CIFS-Revisionsfreigabe

Sie können den letzten Benutzer oder die letzte Gruppe, der Zugriff auf die Revisionsfreigabe hat, nicht entfernen.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit den Passwörtern des Root-Kontos (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

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 CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

3. Starten Sie das Entfernen eines Benutzers oder einer Gruppe: `remove-user-from-share`

   Eine nummerierte Liste der verfügbaren Audit-Shares für den Admin-Knoten wird angezeigt. Die Revisionsfreigabe wird als Audit-Export bezeichnet.

4. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*
5. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe zu entfernen: `user` Oder `group`

   Eine nummerierte Liste von Benutzern oder Gruppen für die Revisionsfreigabe wird angezeigt.

6. Geben Sie die Nummer für den Benutzer oder die Gruppe ein, die Sie entfernen möchten: *`number`*

   Die Revisionsfreigabe wird aktualisiert, und der Benutzer oder die Gruppe ist nicht mehr berechtigt, auf die Revisionsfreigabe zuzugreifen. Beispiel:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
8. Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, deaktivieren Sie die Revisionsfreigabe an jedem Standort nach Bedarf.
9. Melden Sie sich bei Abschluss der Konfiguration von jeder Befehlshaber ab: `exit`

Verwandte Informationen

"Software-Upgrade"

Ändern eines CIFS-Revisionsfreigabe-Benutzers oder Gruppennamens

Sie können den Namen eines Benutzers oder einer Gruppe für eine CIFS-Revisionsfreigabe ändern, indem Sie einen neuen Benutzer oder eine neue Gruppe hinzufügen und dann den alten löschen.

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Fügen Sie einen neuen Benutzer oder eine neue Gruppe mit dem aktualisierten Namen zur Revisionsfreigabe hinzu.
2. Löschen Sie den alten Benutzer- oder Gruppennamen.

Verwandte Informationen

"Software-Upgrade"

"Hinzufügen eines Benutzers oder einer Gruppe zu einer CIFS-Revisionsfreigabe"

"Entfernen eines Benutzers oder einer Gruppe aus einer CIFS-Revisionsfreigabe"

Überprüfung der Integration von CIFS-Audits

Die Revisionsfreigabe ist schreibgeschützt. Die Protokolldateien sind für Computeranwendungen gedacht, und die Überprüfung beinhaltet nicht das Öffnen einer Datei. Es wird als ausreichend überprüft, ob die Audit-Log-Dateien in einem Windows Explorer-Fenster angezeigt werden. Schließen Sie nach der Verbindungsüberprüfung alle Fenster.

Konfigurieren des Audit-Clients für NFS

Die Revisionsfreigabe wird automatisch als schreibgeschützte Freigabe aktiviert.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).
- Der Audit-Client muss NFS-Version 3 (NFSv3) verwenden.

Über diese Aufgabe

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`

b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

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

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

Wenn Dienste nicht als aktiv oder verifiziert 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.

Hinzufügen eines NFS-Audit-Clients zu einer Revisionsfreigabe

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.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).
- Der Audit-Client muss NFS-Version 3 (NFSv3) verwenden.

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 eines NFS-Audit-Clients 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.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie müssen die haben `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Sie können die letzte IP-Adresse, die für den Zugriff auf die Revisionsfreigabe 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

1. Fügen Sie einer vorhandenen NFS-Revisionsfreigabe eine neue IP-Adresse hinzu.
2. Entfernen Sie die ursprüngliche IP-Adresse.

Verwandte Informationen

"Hinzufügen eines NFS-Audit-Clients zu einer Revisionsfreigabe"

"Entfernen eines NFS-Audit-Clients aus der Revisionsfreigabe"

Verwalten Von Archivierungs-Knoten

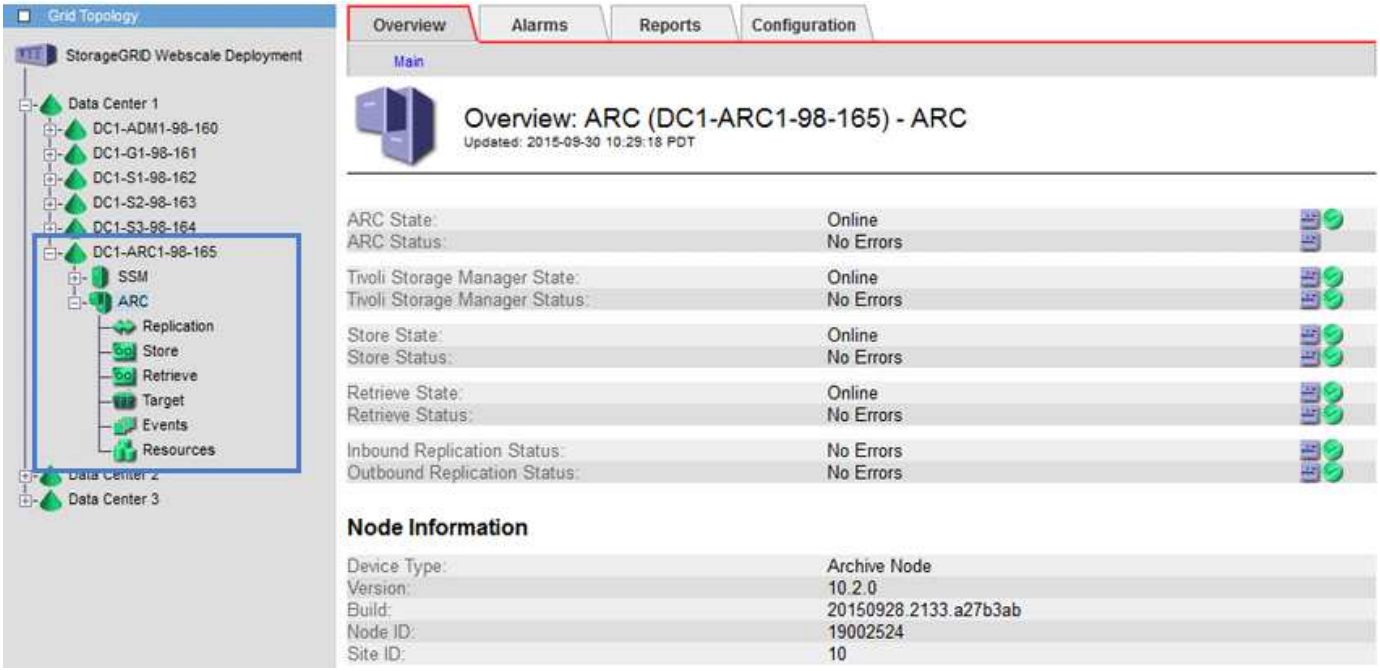
Optional können die Datacenter-Standorte des StorageGRID Systems über einen Archive Node bereitgestellt werden, wodurch eine Verbindung zu einem speziell externen Archiv-Storage-System wie Tivoli Storage Manager (TSM) hergestellt werden kann.

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.

- "Was ist ein Archivknoten"
- "Konfigurieren von Archivierungs-Node-Verbindungen mit Archiv-Storage"
- "Einstellen benutzerdefinierter Alarme für den Knoten „Archiv“"
- "Integration Von Tivoli Storage Manager"

Was ist ein Archivknoten

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.



Objektdaten, die nicht gelöscht, aber nicht regelmäßig abgerufen werden können, können jederzeit von den rotierenden Festplatten eines Storage Node auf einen 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 Archiv-Node (ARC)-Service stellt die Managementoberfläche bereit, über die Sie Verbindungen zu externen Archivspeichern konfigurieren können, z. B. Bandmedien über TSM Middleware.

Der ARC-Service interagiert mit einem externen Archivspeichersystem, sendet Objektdaten für Nearline-Speicherung und führt Abrufvorgänge durch, wenn eine Client-Anwendung ein archiviertes Objekt anfordert. Wenn eine Client-Anwendung ein archiviertes Objekt anfordert, fordert ein Storage Node die Objektdaten vom ARC-Service an. Der ARC-Dienst stellt eine Anfrage an das externe Archiv-Speichersystem, das die angeforderten Objektdaten abruft und diese an den ARC-Dienst sendet. Der ARC-Dienst überprüft die Objektdaten und leitet sie an den Speicherknoten weiter, der wiederum das Objekt an die anfordernde Client-Anwendung zurückgibt.

Anfragen nach über TSM Middleware auf Tape archivierten Objektdaten werden für eine effiziente Abrufvorgänge verwaltet. Anfragen können so bestellt werden, dass Objekte, die nacheinander auf Band gespeichert sind, in derselben sequenziellen Reihenfolge angefordert werden. Anforderungen werden dann in die Warteschlange gestellt, um sie an das Speichergerät zu übertragen. Je nach Archivgerät können mehrere Anfragen für Objekte auf verschiedenen Volumes gleichzeitig verarbeitet werden.

Konfigurieren von Archivierungs-Node-Verbindungen mit Archiv-Storage

Wenn Sie einen Archivknoten für die Verbindung mit einem externen Archiv konfigurieren, müssen Sie den Zieltyp auswählen.

Das StorageGRID System unterstützt die Archivierung von Objektdaten in der Cloud über eine S3-Schnittstelle oder auf Tape über Tivoli Storage Manager (TSM) Middleware.

Wenn der Typ des Archivziels für einen Archiv-Knoten konfiguriert ist, kann der Zieltyp nicht mehr geändert werden.

- "Archivierung in der Cloud über die S3-API"
- "Archivierung auf Band über TSM Middleware"
- "Konfigurieren von Einstellungen für den Abruf von Archivknoten"
- "Konfiguration der Replikation von Archivierungs-Knoten"

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.

Das Verschieben von Objekten vom Archiv-Node auf ein externes Archiv-Storage-System über die S3-API wurde durch ILM Cloud Storage-Pools ersetzt, die mehr Funktionen bieten. Die **Cloud Tiering - Simple Storage Service (S3)** Option wird weiterhin unterstützt, aber Sie könnten stattdessen Cloud Storage Pools implementieren.

Wenn Sie derzeit einen Archiv-Node mit der Option **Cloud Tiering - Simple Storage Service (S3)** verwenden, sollten Sie Ihre Objekte in einen Cloud-Storage-Pool migrieren. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Verwandte Informationen

"Objektmanagement mit ILM"

Verbindungseinstellungen für die S3-API werden konfiguriert

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.

Das Verschieben von Objekten vom Archiv-Node auf ein externes Archiv-Storage-System über die S3-API wurde durch ILM Cloud Storage-Pools ersetzt, die mehr Funktionen bieten. Die **Cloud Tiering - Simple Storage Service (S3)** Option wird weiterhin unterstützt, aber Sie könnten stattdessen Cloud Storage Pools implementieren.

Wenn Sie derzeit einen Archiv-Node mit der Option **Cloud Tiering - Simple Storage Service (S3)** verwenden, sollten Sie Ihre Objekte in einen Cloud-Storage-Pool migrieren. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

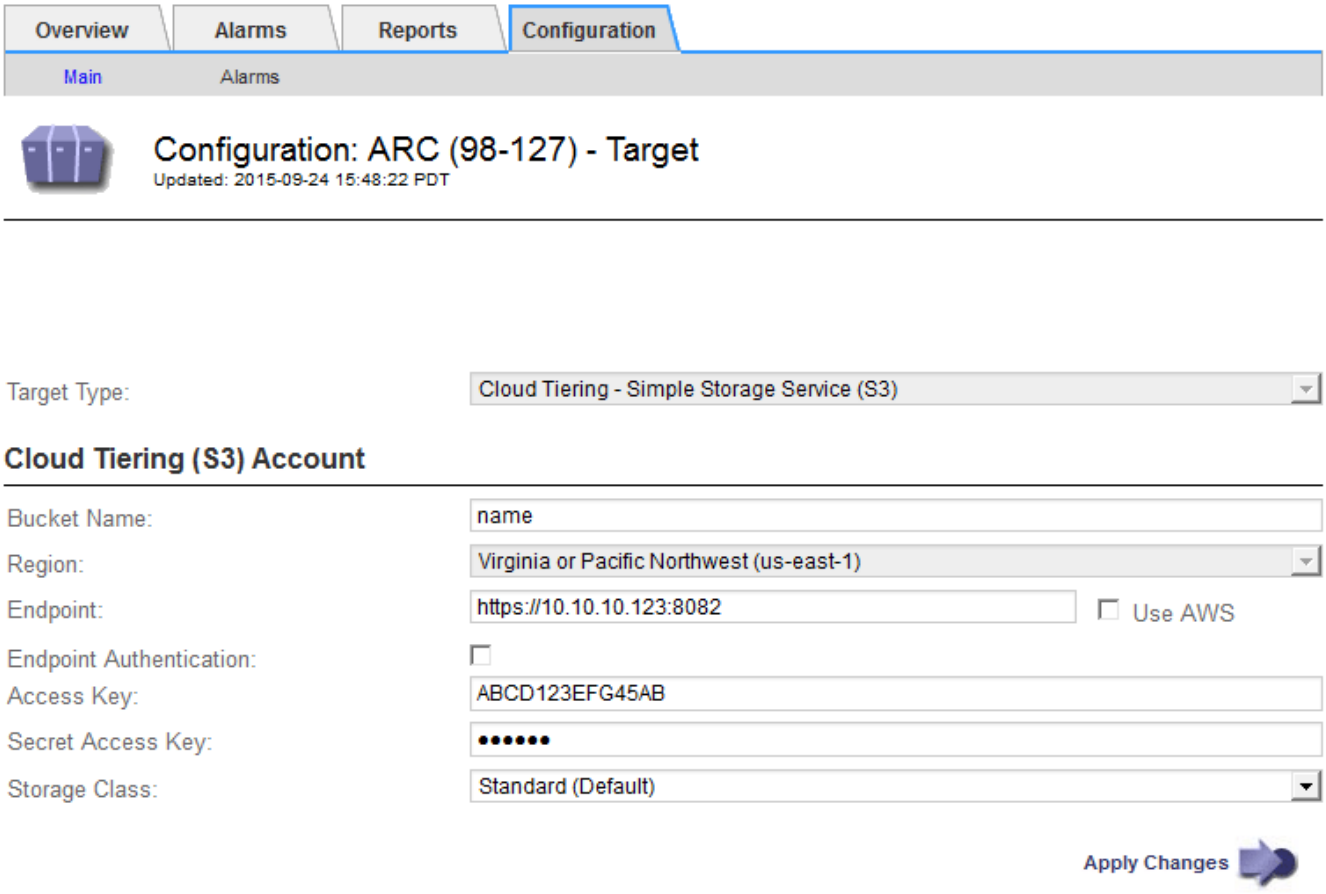
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

- Sie müssen einen Bucket auf dem Ziel-Archiv-Storage-System erstellt haben:
  - Der Bucket muss einem einzelnen Archivierungs-Node zugewiesen sein. Sie kann nicht von anderen Archiv-Nodes oder anderen Anwendungen verwendet werden.
  - Der Bucket muss die für Ihren Standort passende Region ausgewählt haben.
  - Der Bucket sollte mit der Versionierung als ausgesetzt konfiguriert werden.
- Objektsegmentierung muss aktiviert sein, und die maximale Segmentgröße muss kleiner oder gleich 4.5 gib (4,831,838,208 Byte) sein. 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 Topology** Aus.
2. Wählen Sie **Archivknoten** > **ARC** > **Ziel**.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie in der Dropdown-Liste Zieltyp * Cloud Tiering - Simple Storage Service (S3)* aus.

   Konfigurationseinstellungen sind erst verfügbar, wenn Sie einen Zieltyp auswählen.

5. Konfigurieren Sie das Cloud-Tiering-Konto (S3), über das der Archive-Node eine Verbindung zum externen S3-fähigen Archiv-Storage-System herstellen soll.

   Die meisten Felder auf dieser Seite sind selbsterklärend. Im folgenden werden die Felder beschrieben, für die Sie möglicherweise Hinweise benötigen.

- **Region**: Nur verfügbar, wenn **AWS verwenden** ausgewählt ist. Die ausgewählte Region muss mit der Region des Buckets übereinstimmen.
- **Endpunkt** und **AWS verwenden**: Für Amazon Web Services (AWS) wählen Sie **AWS verwenden**. **Endpunkt** wird dann automatisch mit einer Endpunkt-URL auf der Grundlage der Attribute Bucket-Name und Region ausgefüllt. Beispiel:

  ```
  https://bucket.region.amazonaws.com
  ```

  Geben Sie bei einem nicht von AWS stammenden Ziel die URL des Systems ein, das den Bucket hostet, einschließlich der Portnummer. Beispiel:

```
https://system.com:1080
```

- **Endpunktauthentifizierung**: Standardmäßig aktiviert. Wenn das Netzwerk dem externen Archivspeichersystem vertraut ist, können Sie das Kontrollkästchen deaktivieren, um das SSL-Zertifikat und die hostname-Überprüfung des Zielsystems für die externe Archivierung zu deaktivieren. Wenn eine andere Instanz eines StorageGRID-Systems das Zielspeichergerät für die Archivierung 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. Klicken Sie Auf **Änderungen Übernehmen**.

   Die angegebenen Konfigurationseinstellungen werden validiert und auf Ihr StorageGRID System angewendet. Nach der Konfiguration kann das Ziel nicht mehr geändert werden.

Verwandte Informationen

"Objektmanagement mit ILM"

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

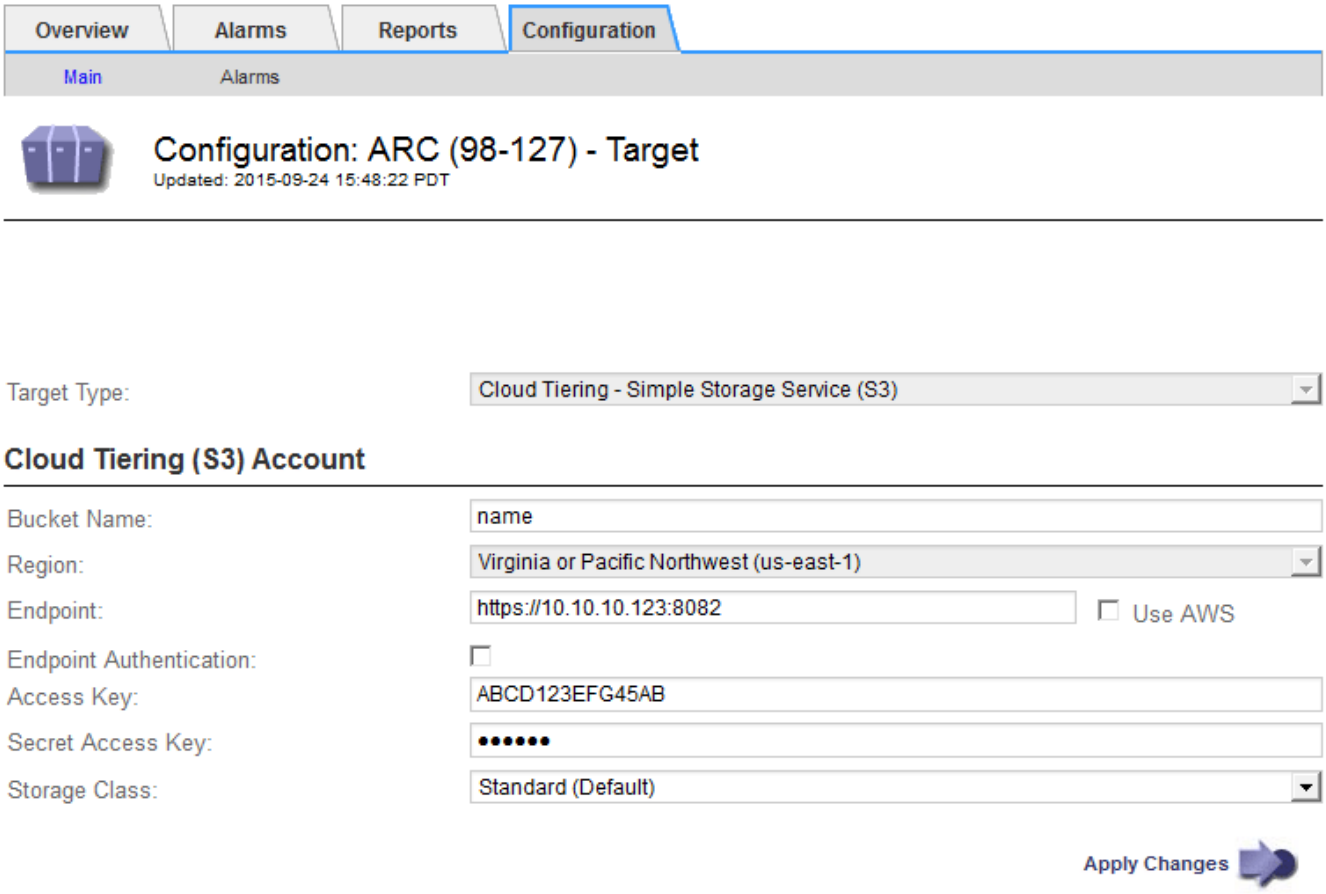
Über diese Aufgabe

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 Topology** Aus.

2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie ggf. die Kontoinformationen.

   Wenn Sie die Storage-Klasse ändern, werden neue Objektdaten mit der neuen Storage-Klasse gespeichert. Vorhandene Objekte werden bei der Aufnahme weiterhin unter dem Storage-Klassensatz gespeichert.

   Bucket-Name, -Region und -Endpunkt verwenden AWS-Werte und können nicht geändert werden.

5. Klicken Sie Auf **Änderungen Übernehmen**.

Ändern des Cloud Tiering Service-Status

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.

Was Sie benötigen

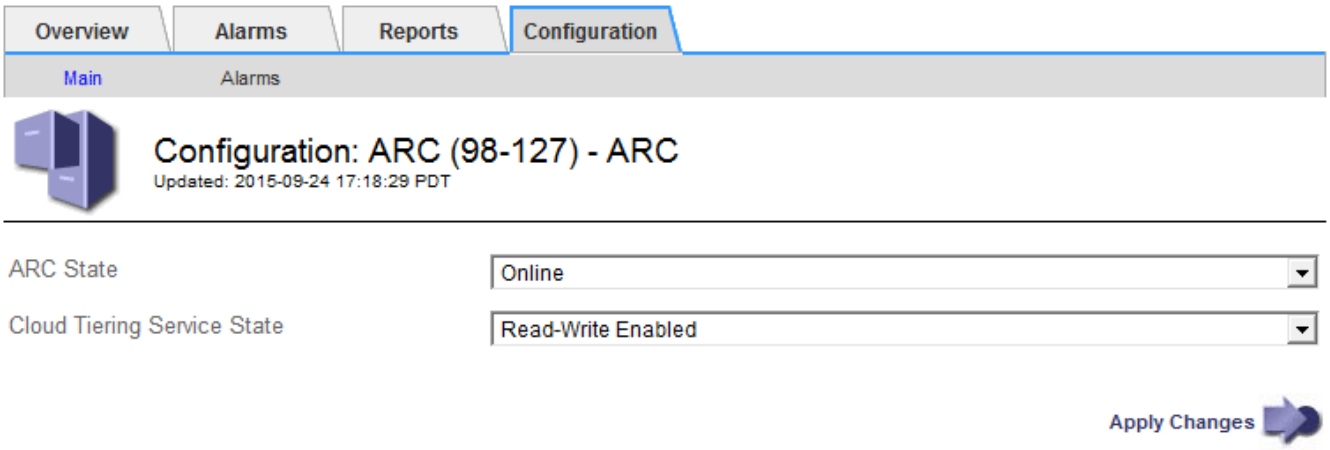
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der Archivknoten muss konfiguriert sein.

Über diese Aufgabe

Sie können den Archiv-Knoten effektiv offline setzen, indem Sie den Cloud-Tiering-Servicenstatus in **Lesen-Schreiben deaktiviert** ändern.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Archivknoten*** > **ARC** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie einen **Cloud Tiering Service-Status** aus.
5. Klicken Sie Auf **Änderungen Übernehmen**.

Zurücksetzen der Speicherfehler-Anzahl für S3-API-Verbindung

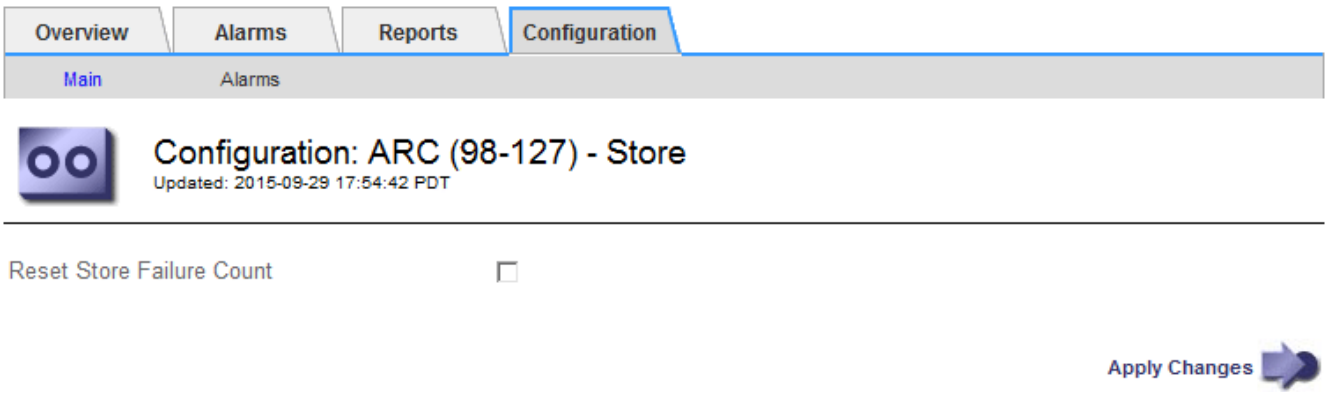
Wenn Ihr Archiv-Node über die S3-API eine Verbindung zu einem Archivspeichersystem herstellt, können Sie die Anzahl der Speicherfehler zurücksetzen, die zum Löschen des ARVF-Alarms (Store Failures) verwendet werden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Store** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie **Anzahl Der Fehler Im Store Zurücksetzen** Aus.
5. Klicken Sie Auf **Änderungen Übernehmen**.

   Das Attribut Fehler speichern wird auf Null zurückgesetzt.

Migration von Objekten aus Cloud Tiering – S3 in einen Cloud-Storage-Pool

Wenn Sie derzeit die Funktion **Cloud Tiering - Simple Storage Service (S3)** verwenden, um Objektdaten auf 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- 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 werden, können im StorageGRID keine Kopien dieser Objekte 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 Tape 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.

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 von Verbindungen zur TSM Middleware

Bevor der Archivknoten mit der Tivoli Storage Manager (TSM) Middleware kommunizieren kann, müssen Sie eine Reihe von Einstellungen konfigurieren.

Was Sie benötigen

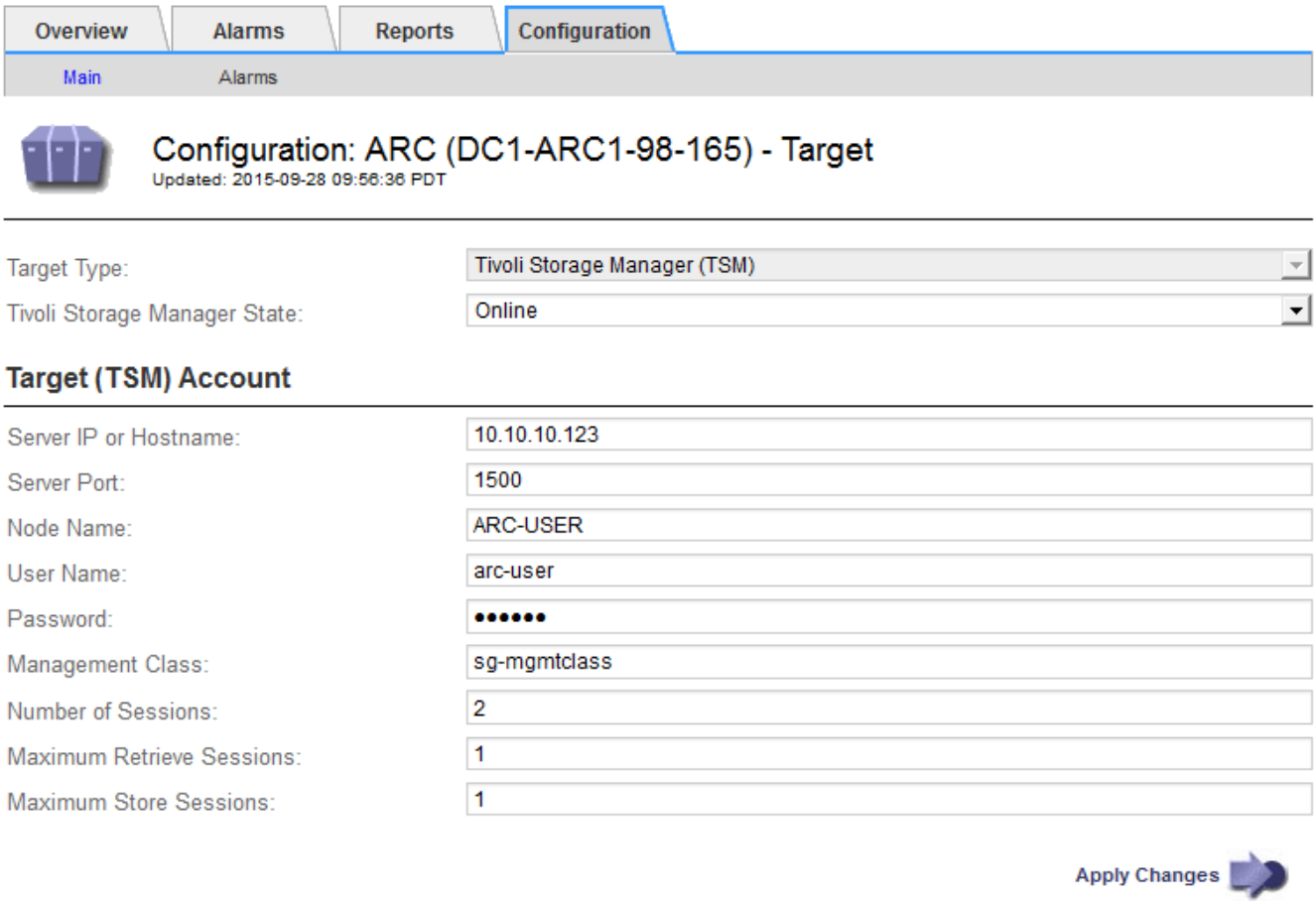
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 Topology** Aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie aus der Dropdown-Liste **Zieltyp** die Option **Tivoli Storage Manager (TSM)** aus.
5. Wählen Sie für den **Tivoli Storage Manager State Offline** aus, um Rückrufe vom TSM Middleware-Server zu verhindern.

   Standardmäßig ist der Status von Tivoli Storage Manager auf Online eingestellt, was bedeutet, dass der Archive Node Objektdaten vom TSM Middleware-Server abrufen kann.

6. Geben Sie die folgenden Informationen an:

   - **Server IP oder Hostname**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen des TSM Middleware-Servers an, der vom ARC-Dienst verwendet wird. Die Standard-IP-Adresse ist 127.0.0.1.
   - **Server-Port**: Geben Sie die Portnummer auf dem TSM Middleware-Server an, mit dem der ARC-Dienst eine Verbindung herstellen wird. Der Standardwert ist 1500.
   - **Knotenname**: Geben Sie den Namen des Archiv-Knotens an. Sie müssen den Namen (Arc-user) eingeben, den Sie auf dem TSM Middleware-Server registriert haben.
   - **Benutzername**: Geben Sie den Benutzernamen an, den der ARC-Dienst zur Anmeldung am TSM-Server verwendet. Geben Sie den Standardbenutzernamen (Arc-user) oder den administrativen Benutzer ein, den Sie für den Archiv-Node angegeben haben.
   - **Passwort**: Geben Sie das Passwort an, das der ARC-Dienst zur Anmeldung am TSM-Server verwendet.
   - **Managementklasse**: Geben Sie die Standardverwaltungsklasse an, die verwendet werden soll, wenn beim Speichern des Objekts auf dem StorageGRID-System keine Managementklasse angegeben ist oder die angegebene Managementklasse nicht auf dem TSM Middleware-Server definiert ist.
   - **Anzahl der Sitzungen**: Geben Sie die Anzahl der Bandlaufwerke auf dem TSM Middleware-Server an, die dem Archiv-Knoten gewidmet sind. Der Archivknoten erstellt gleichzeitig maximal eine Sitzung pro Bereitstellungspunkt plus eine kleine Anzahl zusätzlicher Sitzungen (weniger als fünf).

     Sie müssen diesen Wert ändern, um den für MAXNUMMP festgelegten Wert (maximale Anzahl von Mount-Punkten) zu erhalten, wenn der Archivknoten registriert oder aktualisiert wurde. (Im Register-Befehl ist der Standardwert von MAXNUMMP verwendet 1, wenn kein Wert festgelegt ist.)

   Außerdem müssen Sie den Wert von MAXSESSIONS für den TSM-Server auf eine Zahl ändern, die mindestens so groß ist wie die Anzahl der Sitzungen, die für den ARC-Dienst festgelegt wurden. Der Standardwert von MAXSESSIONS auf dem TSM-Server ist 25.

   - **Maximum Retrieve Sessions**: Geben Sie die maximale Anzahl von Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Abrufvorgänge öffnen kann. In den meisten Fällen ist der entsprechende Wert die Anzahl der Sitzungen abzüglich der maximalen Speichersitzungen. Wenn Sie ein Bandlaufwerk für die Speicherung und den Abruf freigeben möchten, geben Sie einen Wert an, der der Anzahl der Sitzungen entspricht.
   - **Maximum Store Sessions**: Geben Sie die maximale Anzahl gleichzeitiger Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Archivierungsvorgänge öffnen kann.

     Dieser Wert sollte auf eins gesetzt werden, außer wenn das gezielte Archivspeichersystem voll ist und nur Abrufvorgänge durchgeführt werden können. Setzen Sie diesen Wert auf Null, um alle Sitzungen für Abrufvorgänge zu verwenden.

7. Klicken Sie Auf **Änderungen Übernehmen**.

Optimierung eines Archivknotes 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.

Was Sie benötigen

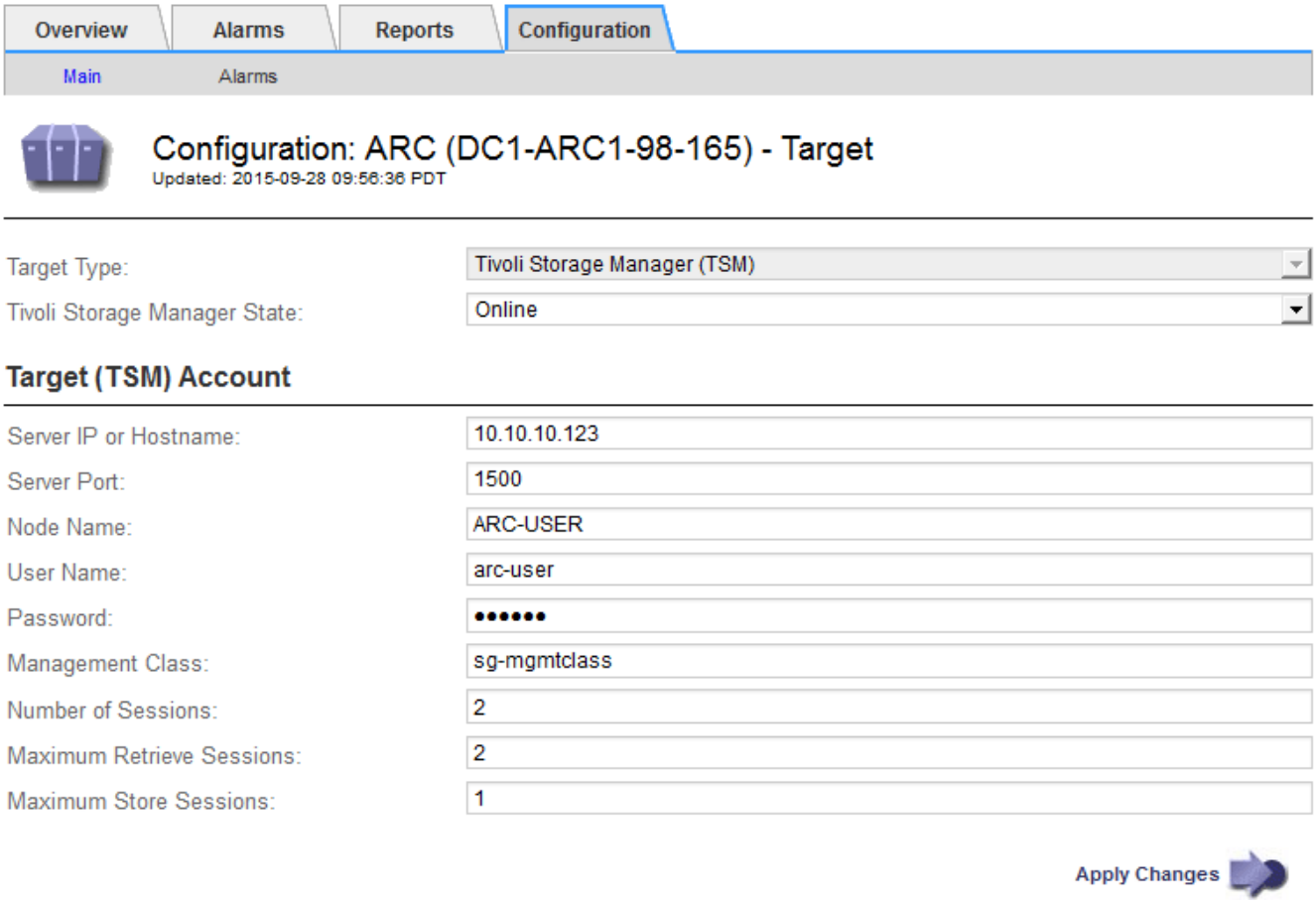
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 Topology** Aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.
4. Ändern Sie **Maximum Retrieve Sessions** als **Anzahl der Sitzungen**.



5. Klicken Sie Auf **Änderungen Übernehmen**.

Konfigurieren des Archivierungsstatus und der 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

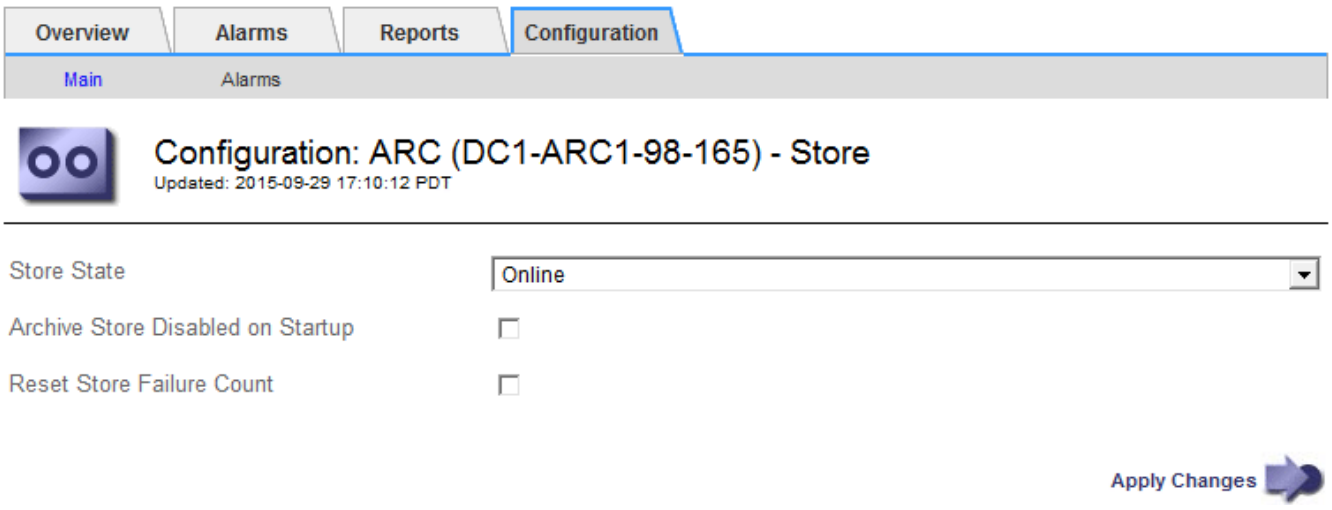
konfigurieren. Sie können den Archivspeicher auch deaktivieren, wenn der Archivknoten zum ersten Mal gestartet wird, oder die Fehleranzahl, die für den zugehörigen Alarm nachverfolgt wird, zurücksetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Store** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - Speicherstatus: Legen Sie den Komponentenstatus auf entweder:
     - Online: Der Archiv-Node ist zur Verarbeitung von Objektdaten zum Speichern im Archiv-Storage-System verfügbar.
     - Offline: Der Archiv-Node ist nicht verfügbar, um Objektdaten zum Speichern im Archiv-Storage-System zu verarbeiten.
   - Archivspeicher beim Start deaktiviert: Wenn diese Option ausgewählt ist, bleibt die Komponente Archivspeicher beim Neustart im schreibgeschützten Zustand. Wird verwendet, um Speicher dauerhaft für das Zielspeichersystem zu deaktivieren. Nützlich, wenn das ausgewählte Archiv-Speichersystem 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. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

"Verwalten eines Archiv-Knotens, wenn TSM-Server die Kapazität erreicht"

Verwalten eines Archiv-Knotens, wenn 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. 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. Dies kann durch proaktive Überwachung des TSM-Servers vermieden werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Um zu verhindern, dass der ARC-Service weitere Inhalte an den TSM-Server sendet, können Sie den Archiv-Node offline schalten, indem Sie die **ARC** > **Store**-Komponente offline schalten. Dieses Verfahren kann auch nützlich sein, um Alarme zu vermeiden, wenn der TSM-Server nicht zur Wartung verfügbar ist.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** 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. Klicken Sie Auf **Änderungen Übernehmen**.

Einrichten des Archivierungs-Nodes auf „schreibgeschützt“, 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** 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. Klicken Sie Auf **Änderungen Übernehmen**.

Konfigurieren von Einstellungen für den Abruf von Archivknoten

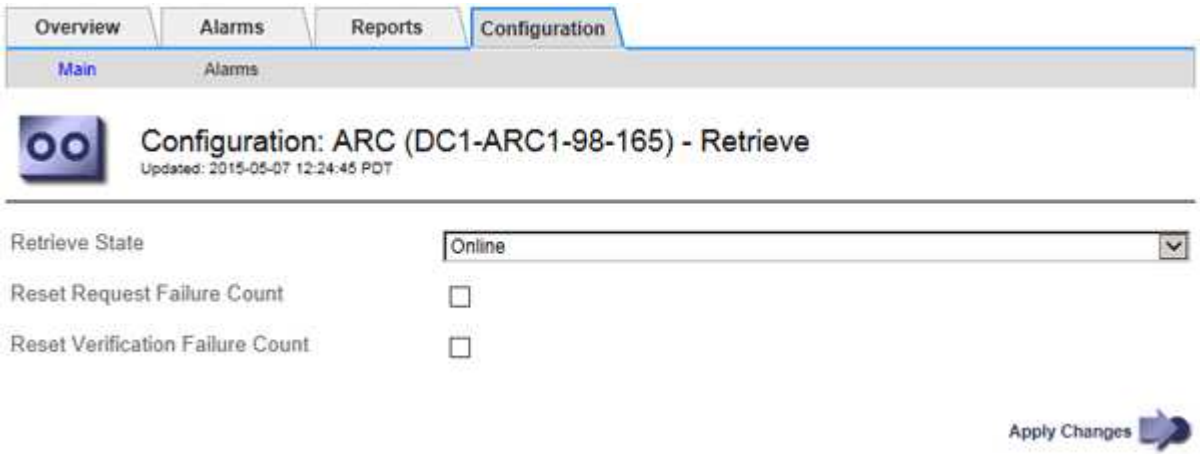
Sie können die Einstellungen für den Abruf eines Archiv-Knotens so konfigurieren, dass der Status auf Online oder Offline gesetzt wird, oder die Fehleranzahl, die für die zugehörigen Alarme nachverfolgt wird, zurücksetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie **Archivknoten** > **ARC** > **Abruf**.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - **Retrieve Status**: Den Komponentenzustand auf entweder einstellen:
     - Online: Der Grid-Node ist verfügbar, um Objektdaten vom Archivierungsmedium abzurufen.
     - Offline: Der Grid-Node ist zum Abrufen von Objektdaten nicht verfügbar.
   - Reset Request Failures Count: Aktivieren Sie das Kontrollkästchen, um den Zähler für Anforderungsfehler zurückzusetzen. Dieser kann verwendet werden, um den ARRF-Alarm (Request

Failures) zu löschen.

- Zurücksetzen Fehleranzahl der Überprüfung: Aktivieren Sie das Kontrollkästchen, um den Zähler auf Überprüfungsfehler bei abgerufenen Objektdaten zurückzusetzen. Dies kann verwendet werden, um den ARRV-Alarm (Verifizierungsfehler) zu löschen.

5. Klicken Sie Auf **Änderungen Übernehmen**.

Konfiguration der Replikation von Archivierungs-Knoten

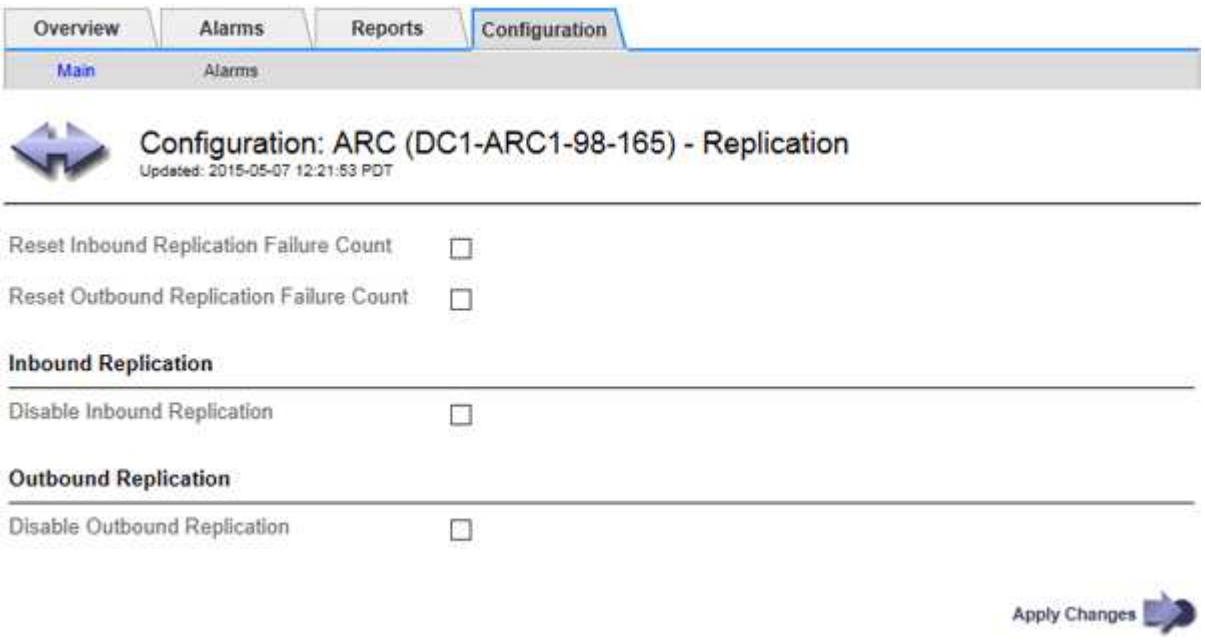
Sie können die Replikationseinstellungen für einen Archivknoten konfigurieren und die ein- und ausgehende Replikation deaktivieren oder die für die zugehörigen Alarme zu protokollierenden Fehlerzählungen zurücksetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Replikation** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - **Fehleranzahl Inbound Replication zurücksetzen**: Wählen Sie, um den Zähler für eingehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RIRF-Alarm (eingehende Replikationen — fehlgeschlagen) zu löschen.
   - **Fehleranzahl bei ausgehenden Replikationsfehlern zurücksetzen**: Wählen Sie, um den Zähler für ausgehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
   - **Inbound Replication** deaktivieren: Wählen Sie aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs löschen lassen.

Wenn die eingehende Replikation deaktiviert ist, können Objektdaten vom ARC-Dienst zur Replikation an andere Standorte im StorageGRID-System abgerufen werden. Objekte können jedoch von anderen Systemstandorten nicht zu diesem 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-Abruf) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.

  Wenn die ausgehende Replikation deaktiviert ist, können Objektdaten in diesen ARC-Dienst kopiert werden, um ILM-Regeln zu erfüllen. Objektdaten können jedoch nicht vom ARC-Dienst abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der ARC-Dienst ist nur schreiben-.

5. Klicken Sie Auf **Änderungen Übernehmen**.

Einstellen benutzerdefinierter Alarme für den Knoten „Archiv“

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.

Verwandte Informationen

"Monitor Fehlerbehebung"

Integration Von Tivoli Storage Manager

Dieser Abschnitt enthält Best Practices und Setup-Informationen für die Integration eines Archiv-Knotens mit einem Tivoli Storage Manager (TSM)-Server, einschließlich Betriebsdetails zu Archive Node, die sich auf die Konfiguration des TSM-Servers auswirken.

- "Konfiguration und Betrieb des Archivierungs-Node"
- "Best Practices für die Konfiguration"
- "Abschluss der Konfiguration des Archivierungs-Knotens"

Konfiguration und Betrieb des Archivierungs-Node

Ihr StorageGRID-System managt den Archiv-Node als Speicherort, an dem Objekte unendlich gespeichert werden und stets zugänglich sind.

Bei der Aufnahme eines Objekts werden auf Basis der für das StorageGRID System definierten Regeln für das Information Lifecycle Management Kopien an allen erforderlichen Speicherorten, einschließlich Archiv-Nodes, erstellt. Der Archivknoten fungiert als Client auf einem TSM-Server, und die TSM-Clientbibliotheken sind auf dem Archiv-Knoten durch den Installationsvorgang der StorageGRID-Software installiert. Objektdaten, die zum Archiv-Node für Speicher geleitet werden, werden beim Empfang direkt auf dem TSM-Server gespeichert. Der Archivknoten stellt keine Objektdaten vor dem Speichern auf dem TSM-Server dar und führt auch keine Objektaggregation durch. Der Archivknoten kann jedoch in einer einzigen Transaktion mehrere Kopien an den TSM-Server senden, wenn die Datenraten dies erfordern.

Nachdem der Archivknoten Objektdaten auf dem TSM-Server speichert, werden die Objektdaten unter Anwendung der Lifecycle-/Aufbewahrungsrichtlinien vom TSM-Server gemanagt. Diese Aufbewahrungsrichtlinien müssen definiert werden, damit sie mit dem Vorgang des Archivierungs-Nodes kompatibel sind. Das bedeutet, dass vom Archiv-Node gespeicherte Objektdaten unbegrenzt gespeichert werden müssen und vom Archiv-Node immer darauf zugegriffen werden muss, es sei denn, sie werden vom Archiv-Node gelöscht.

Es besteht keine Verbindung zwischen den ILM-Regeln des StorageGRID Systems und den Lifecycle-/Aufbewahrungsrichtlinien des TSM Servers. Jeder arbeitet unabhängig voneinander. Wenn jedoch jedes Objekt in das StorageGRID System aufgenommen wird, kann ihm eine TSM Management-Klasse zugewiesen werden. Diese Managementklasse wird gemeinsam mit Objektdaten an den TSM Server übergeben. Durch das Zuweisen verschiedener Managementklassen zu unterschiedlichen Objekttypen können Sie den TSM-Server so konfigurieren, dass Objektdaten in verschiedenen Storage-Pools gespeichert werden, oder unterschiedliche Migrations- oder Aufbewahrungsrichtlinien anwenden. Beispielsweise können als Datenbank-Backups identifizierte Objekte (temporärer Content als mit neueren Daten überschrieben werden kann) anders als Applikationsdaten behandelt werden (unveränderlicher Inhalt, der für unbegrenzte Zeit aufbewahrt werden muss).

Der Archivknoten kann in einen neuen oder vorhandenen TSM-Server integriert werden; es ist kein dedizierter TSM-Server erforderlich. TSM-Server können mit anderen Clients gemeinsam genutzt werden, vorausgesetzt, der TSM-Server ist für die erwartete maximale Last angemessen dimensioniert. TSM muss auf einem vom Archiv-Node getrennten Server oder einer virtuellen Maschine installiert sein.

Es ist möglich, mehr als einen Archivknoten zu konfigurieren, um auf denselben TSM-Server zu schreiben; diese Konfiguration wird jedoch nur empfohlen, wenn die Archiv-Knoten unterschiedliche Datensätze auf den TSM-Server schreiben. Die Konfiguration von mehr als einem Archiv-Node zum Schreiben auf denselben TSM-Server wird nicht empfohlen, wenn jeder Archiv-Node Kopien derselben Objektdaten in das Archiv schreibt. Bei einem letzteren Szenario unterliegen beide Kopien einem Single Point of Failure (dem TSM-Server), da sie unabhängige, redundante Kopien von Objektdaten sind.

Archive Nodes nutzen die hierarchische Storage Management (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.

- Die Archivierungs-Node-Software kann die Latenz beim Schreiben von Objekten direkt auf Tapes oder andere Wechseldatenträger 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 Copy-Pool des Disk-Pools konfiguriert werden, wobei gleichzeitig in beide Pools geschrieben wird (das heißt, der Bandpool kann kein COPYSTGPOL für den Laufwerk-Pool 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.

Abschluss der Konfiguration des Archivierungs-Knotens

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.

Weitere Informationen zur Optimierung von TSM-Abruf- und Speichersitzungen finden Sie unter Informationen zum Management von Archivspeicher.

- "Verwalten Von Archivierungs-Knoten"

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 eines neuen TSM-Servers

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 Archivknoten kann nicht mit einem TSM-Server Co-gehostet werden.

Konfigurieren des TSM-Servers

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 dienen nicht als Ersatz für die TSM Dokumentation oder zur Bereitstellung der vollständigen und umfassenden Anweisungen für alle Konfigurationen. 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.

Definition von 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 eine Reihe von Schritten auf Ihrem TSM-Server durchführen, bevor Sie einen Bandspeicher-Pool 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 mit Administratorrechten auf dem Server anmelden und das dsmadmc-Tool verwenden, um die folgenden Befehle auszuführen.

Schritte

1. Erstellen einer Tape Library

   `define library` *`tapelibrary`* `libtype=`*`scsi`*

   Wo *`tapelibrary`* Ist ein willkürlicher Name, der für die Bandbibliothek und den Wert von ausgewählt wurde `libtype` Je nach Art der Tape Library kann es variieren.

2. Definieren Sie einen Pfad vom Server zur Bandbibliothek.

   `define path` *`servername tapelibrary`* `srctype=server desttype=library device=`*`lib-devicename`*

   - *`servername`* Ist der Name des TSM-Servers

- `tapelibrary` Ist der von Ihnen definierte Bandbibliothek
- `lib-devicename` Ist der Gerätename für die Bandbibliothek

3. Legen Sie ein Laufwerk für die Bibliothek fest.

   ```
   define drive tapelibrary drivename
   ```

   - `drivename` Ist der Name, den Sie für das Laufwerk angeben möchten
   - `tapelibrary` Ist der von Ihnen definierte Bandbibliothek

     Je nach Hardwarekonfiguration möchten Sie möglicherweise ein zusätzliches Laufwerk oder weitere Laufwerke konfigurieren. (Wenn beispielsweise der TSM-Server mit einem Fibre Channel-Switch verbunden ist, der über zwei Eingaben aus einer Bandbibliothek verfügt, sollten Sie für jede Eingabe möglicherweise ein Laufwerk definieren.)

4. Definieren Sie einen Pfad vom Server zum Laufwerk, das Sie definiert haben.

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - `drive-dname` Ist der Gerätename für das Laufwerk
   - `tapelibrary` Ist der von Ihnen definierte Bandbibliothek

     Wiederholen Sie diesen Vorgang für jedes Laufwerk, das Sie für die Bandbibliothek definiert haben, mit einem separaten Laufwerk `drivename` Und `drive-dname` Für jedes Laufwerk.

5. Definieren Sie eine Geräteklasse für die Laufwerke.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - `DeviceClassName` Ist der Name der Geräteklasse
   - `lto` Ist der Laufwerkstyp, der mit dem Server verbunden ist
   - `tapelibrary` Ist der von Ihnen definierte Bandbibliothek
   - `tapetype` Ist der Tape-Typ, z. B. ultrium3

6. Fügen Sie dem Bestand der Bibliothek Bandvolumen hinzu.

   ```
   checkin libvolume tapelibrary
   ```

   `tapelibrary` Ist der von Ihnen definierte Bandbibliothek.

7. Erstellen Sie den primären Bandspeicherpool.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - `SGWSTapePool` Ist der Name des Bandspeicherpools des Archiv-Nodes. Sie können einen beliebigen Namen für den Bandspeicher-Pool auswählen (sofern der Name die vom TSM-Server erwarteten Syntaxkonventionen verwendet).

- *DeviceClassName* Ist der Name des Klassennamens für die Bandbibliothek.
- *description* Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „`Bandspeicher-Pool für den Archiv-Node`“
- *collocate=filespace* Gibt an, dass der TSM-Server Objekte aus demselben Dateispeicher auf ein einzelnes Band schreiben soll.
- `XX` Ist eine der folgenden Optionen:
  - Die Anzahl der leeren Bänder in der Bandbibliothek (falls der Archivknoten die einzige Anwendung ist, die die Bibliothek verwendet).
  - Die Anzahl der vom StorageGRID System zugewiesenen Tapes (in Fällen, in denen die Tape-Bibliothek gemeinsam genutzt wird).

8. Erstellen Sie auf einem TSM-Server einen Festplatten-Speicherpool. Geben Sie an der Administrationskonsole des TSM-Servers ein

   `define stgpool SGWSDiskPool disk description=description maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high lowmig=percent_low`

   - *SGWSDiskPool* Ist der Name des Festplatten-Pools des Archiv-Nodes. Sie können einen beliebigen Namen für den Festplatten-Speicherpool auswählen (sofern der Name die vom TSM erwarteten Syntaxkonventionen verwendet).
   - *description* Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „`DFestplatten-Storage-Pool für den Archiv-Node`“
   - *maximum_file_size* Zwingt das Schreiben von Objekten, die größer sind als diese Größe, direkt auf Tape, statt im Festplatten-Pool gespeichert zu werden. Es wird empfohlen, die Einstellung festzulegen *maximum_file_size* Bis 10 GB.
   - *nextstgpool=SGWSTapePool* Bezeichnet den Festplatten-Speicherpool auf den für den Archiv-Node definierten Bandspeicher-Pool.
   - *percent_high* Legt den Wert fest, mit dem der Laufwerk-Pool seine Inhalte in den Bandpool migriert. Es wird empfohlen, die Einstellung festzulegen *percent_high* Zu 0, sodass sofort die Datenmigration beginnt
   - *percent_low* Legt den Wert fest, mit dem die Migration zum Bandpool angehalten wird. Es wird empfohlen, die Einstellung festzulegen *percent_low* Zu 0, um den Laufwerk-Pool zu löschen.

9. Erstellen Sie auf einem TSM-Server ein Festplatten-Volume (oder Volumes) und weisen Sie es dem Festplatten-Pool zu.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* Ist der Name des Disk-Pools.
   - *volume_name* Ist der vollständige Pfad zum Speicherort des Volumes (z. B. `/var/local/arc/stage6.dsm`) Auf dem TSM-Server, wo er den Inhalt des Laufwerk-Pools in Vorbereitung für die Übertragung auf Band schreibt.
   - *size* Ist die Größe des Datenträgers in MB.

     Wenn Sie beispielsweise ein einzelnes Laufwerk-Volume so erstellen möchten, dass der Inhalt eines

Festplattenpools ein einzelnes Band enthält, setzen Sie den Wert der Größe auf 200000, wenn das Bandvolumen 200 GB hat.

Es könnte jedoch wünschenswert sein, mehrere Festplatten-Volumes einer kleineren Größe zu erstellen, da der TSM-Server auf jedes Volume im Festplatten-Pool schreiben kann. Wenn die Bandgröße beispielsweise 250 GB beträgt, erstellen Sie 25 Festplatten-Volumes mit jeweils 10 GB (10000).

Der TSM-Server weist im Verzeichnis für das Festplatten-Volume vorab Speicherplatz zu. Dies kann einige Zeit in Anspruch nehmen (mehr als drei Stunden für ein 200-GB-Laufwerk).

Definieren einer Domänenrichtlinie und Registrieren eines Knotens

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 Nummer muss mindestens so groß sein wie der Wert für die **ARC** > **Ziel** > **Konfiguration** > **Main** > **Maximum Store Sessions** für den Archiv-Node, Der auf den Wert 0 oder 1 gesetzt ist, da gleichzeitige Speichersitzungen vom Archiv-Node nicht unterstützt werden.

Der Wert des MAXSESSIONS-Satzes für den TSM-Server steuert die maximale Anzahl von Sitzungen, die für den TSM-Server von allen Client-Anwendungen geöffnet werden können. Der auf dem TSM angegebene MAXSESSIONS-Wert muss mindestens so groß sein wie der für **ARC** > **Ziel** > **Konfiguration** > **Main** > **Anzahl Sitzungen** im Grid Manager für den Archiv-Node angegebene Wert. Der Archivknoten erstellt gleichzeitig höchstens eine Sitzung pro Bereitstellungspunkt plus eine kleine Zahl (< 5) zusätzlicher Sitzungen.

Der dem Archiv-Node zugewiesene TSM-Node verwendet eine benutzerdefinierte Domänenrichtlinie `tsm-domain`. Der `tsm-domain` Die Domänenrichtlinie ist eine geänderte Version der Domänenrichtlinie „`standard`“, die auf Band geschrieben und als Speicherpool des StorageGRID Systems das Archivziel festgelegt wurde (*`SGWSDiskPool`*).

> Sie müssen sich am TSM-Server mit Administratorrechten anmelden und das dsmadmc-Tool verwenden, um die Domänenrichtlinie zu erstellen und zu aktivieren.

Die Domänenrichtlinie wird erstellt und aktiviert

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 Managementklasse verwenden, geben Sie eine der folgenden Werte 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 den Archiv-Knoten vom Löschen von Inhalten, da Aufbewahrungsereignisse verwendet werden, um Inhalte vom TSM-Server zu entfernen.

4. Weisen Sie die Managementklasse als Standard zu.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Legen Sie den neuen Richtliniensatz als aktiv fest.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorieren Sie die Warnung „`no Backup copy Group`“, die beim Eingeben des Befehls activate angezeigt wird.

6. Registrieren Sie einen Knoten, um den neuen Richtliniensatz auf dem TSM-Server zu verwenden. Geben Sie auf dem TSM-Server (in einer Zeile) Folgendes ein:

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user und Arc-password sind der Name und das Kennwort des Client-Knotens, den Sie auf dem Archiv-Node definieren, und der Wert von MAXNUMMP ist auf die Anzahl der Bandlaufwerke festgelegt, die für Archive Node Store-Sessions reserviert sind.

   > Durch die Registrierung eines Knotens wird standardmäßig eine Administrator-Benutzer-ID mit der Berechtigung des Clienteigentümers erstellt, wobei das für den Knoten definierte Passwort angegeben ist.

Datenmigration zu StorageGRID

Sie können große Datenmengen bei gleichzeitigem Einsatz des StorageGRID Systems auf das StorageGRID System migrieren.

Der folgende Abschnitt enthält einen Leitfaden zu verstehen und zu planen, eine Migration großer Datenmengen in das StorageGRID System durchzuführen. 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 der Kapazität des StorageGRID Systems"
- "Ermitteln der ILM-Richtlinie für migrierte Daten"
- "Auswirkungen der Migration auf den Betrieb"
- "Planen der Datenmigration"
- "Monitoring der Datenmigration"
- "Erstellen benutzerdefinierter Benachrichtigungen für Migrationsalarme"

Bestätigen der 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 umfasst und eine Kopie migriertes Objekt in Nearline-Speicher (z. B. Band) gespeichert wurde, stellen Sie sicher, dass der Speicher des Archivknotens über ausreichende Kapazität für das erwartete Volumen migriertes Datenvolumen 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 in den Anweisungen für das Monitoring und die Fehlerbehebung von StorageGRID.

Verwandte Informationen

"Monitor Fehlerbehebung"

"Verwalten Von Storage-Nodes"

Ermitteln der ILM-Richtlinie für migrierte Daten

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.

> 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.

Verwandte Informationen

"Objektmanagement mit ILM"

Auswirkungen 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 Kapitel sorgfältig gemanagt werden, um die alltäglichen Systemvorgänge zu vermeiden oder im Extremfall das Risiko eines Datenverlusts bei einem Ausfall im StorageGRID System zu gefährden.

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. Anschließend überwacht das StorageGRID System fortlaufend, um sicherzustellen, dass verschiedene Attributwerte nicht überschritten werden.

Planen der 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 die Datenmigration nach Möglichkeit nicht für Zeiten 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.

Verwandte Informationen

"Monitoring der Datenmigration"

Monitoring der Datenmigration

Die Datenmigration muss bei Bedarf überwacht und angepasst werden, um sicherzustellen, dass die Daten gemäß der ILM-Richtlinie innerhalb des erforderlichen Zeitrahmens platziert werden.

In dieser Tabelle sind die Attribute aufgeführt, die während der Datenmigration überwacht werden müssen, und die jeweiligen Probleme aufgeführt.

Wenn Sie Traffic-Klassifizierungsrichtlinien mit Geschwindigkeitsbegrenzungen zur Drosselung verwenden, können Sie die beobachtete Rate in Verbindung mit den in der folgenden Tabelle beschriebenen Statistiken überwachen und die Grenzwerte bei Bedarf reduzieren.

Überwachen	Beschreibung
Anzahl an Objekten, die auf die ILM-Bewertung warten	1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 2. Wählen Sie ***Deployment*** > **Übersicht** > **Main**. 3. Überwachen Sie im Abschnitt ILM-Aktivität die Anzahl der für die folgenden Attribute angezeigten Objekte: ◦ **Ausstehend - alles (XQUZ)**: Die Gesamtzahl der Objekte, die auf die ILM-Bewertung warten. ◦ **Ausstehend - Client (XCQZ)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aus Client-Operationen warten (zum Beispiel Aufnahme). 4. Wenn die Anzahl der für eines dieser Attribute angezeigten Objekte 100,000 überschreitet, drosseln Sie die Aufnahmegeschwindigkeit von Objekten, um die Last auf dem StorageGRID-System zu verringern.
Storage-Kapazität eines Targeted Archivsystems	Wenn durch die ILM-Richtlinie eine Kopie der migrierten Daten auf ein zielgerichtetes Storage-System (Band oder Cloud) gespeichert wird, überwachen Sie die Kapazität des Zielspeichersystems, um sicherzustellen, dass genügend Kapazität für die migrierten Daten vorhanden ist.

Überwachen	Beschreibung
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.

Erstellen benutzerdefinierter Benachrichtigungen für Migrationsalarme

Möglicherweise soll StorageGRID Alarmbenachrichtigungen oder Warnmeldungen an den Systemadministrator senden, der für das Monitoring der Migration verantwortlich ist, falls bestimmte Werte die empfohlenen Schwellenwerte überschreiten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen E-Mail-Einstellungen für Alarm- (oder Alarm-) Benachrichtigungen konfiguriert haben.

Schritte

1. Erstellen Sie für jede Prometheus-Metrik oder jedes StorageGRID-Attribut, das Sie während der Datenmigration überwachen möchten, eine benutzerdefinierte Alarmregel oder einen globalen benutzerdefinierten Alarm.

   Warnmeldungen werden auf Basis der Prometheus-Messwerte ausgelöst. Alarme werden basierend auf Attributwerten ausgelöst. Weitere Informationen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

2. Deaktivieren Sie die benutzerdefinierte Alarmregel oder den globalen benutzerdefinierten Alarm, nachdem die Datenmigration abgeschlossen ist.

   Beachten Sie, dass globale benutzerdefinierte Alarme Standardalarme überschreiben.

Verwandte Informationen

"Monitor Fehlerbehebung"

Objektmanagement mit ILM

Erfahren Sie, wie Sie Objekte mithilfe von Richtlinien und Regeln für den Informationslebenszyklus managen und S3 Object Lock verwenden, um gesetzliche Vorgaben für die Objektaufbewahrung zu erfüllen.

- "Verwalten von Objekten mit Information Lifecycle Management"
- "Verwalten von Objekten mit S3 Object Lock"
- "Beispiele für ILM-Regeln und -Richtlinien"

Verwalten von Objekten mit Information Lifecycle Management

Sie managen die Objekte in einem StorageGRID-System durch die Konfiguration von Regeln und Richtlinien für das Information Lifecycle Management (ILM). Die ILM-Regeln und Richtlinien erläutern StorageGRID, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien im Laufe der Zeit gemanagt werden.

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.

- "Funktionsweise von ILM während der gesamten Nutzungsdauer eines Objekts"
- "Was ist eine ILM-Richtlinie"
- "Was ist eine ILM-Regel"
- "Erstellung von Speicherklassen, Speicherpools, EC-Profilen und Regionen"
- "Erstellen einer ILM-Regel"
- "ILM-Richtlinie erstellen"
- "Arbeiten mit ILM-Regeln und ILM-Richtlinien"

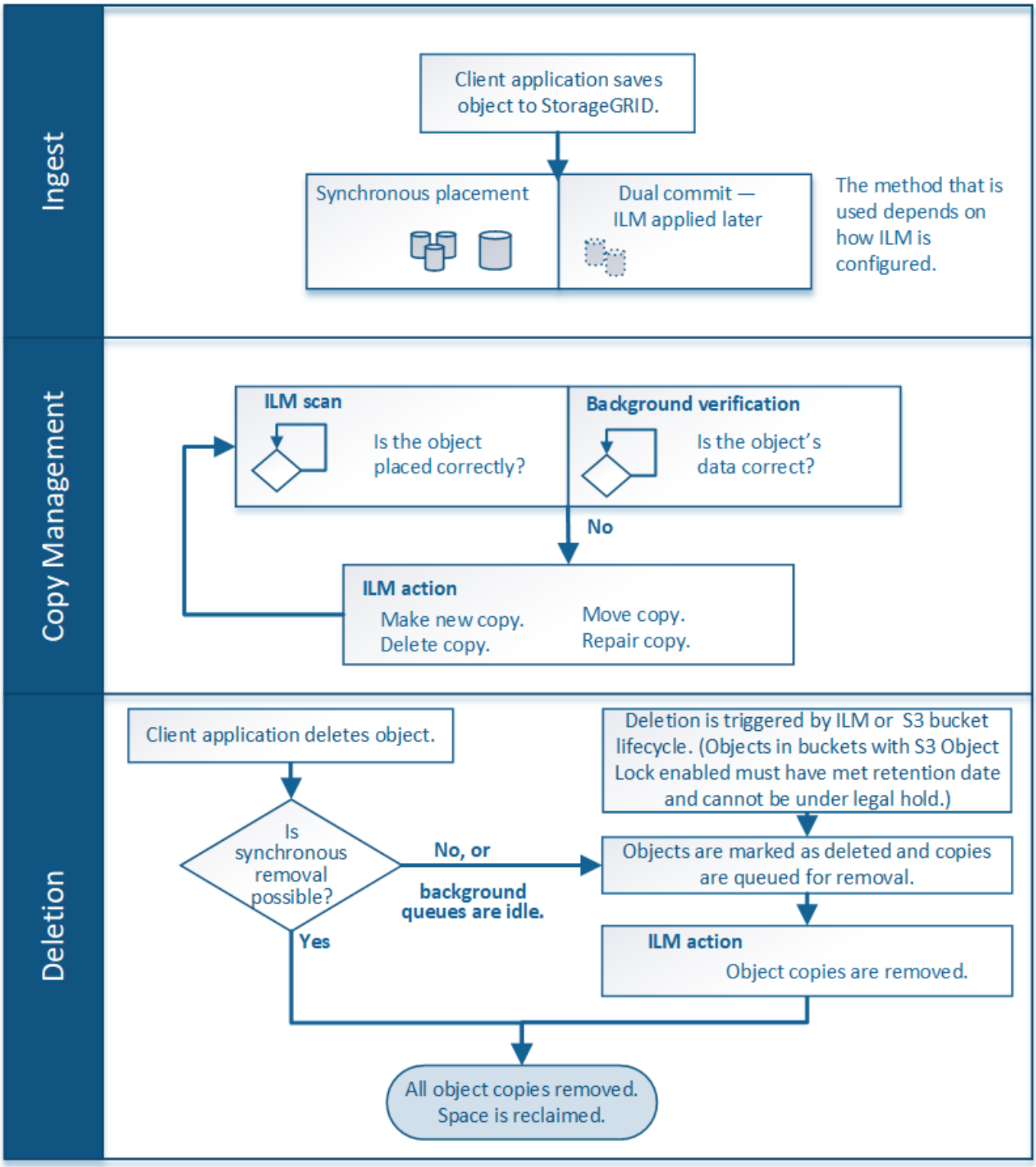
Wie ILM im gesamten Leben eines Objekts funktioniert

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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.
- **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-Objektsperre aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einer gesetzlichen Aufbewahrungspflichten befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.

Das Diagramm fasst die Funktionsweise von ILM im gesamten Lebenszyklus eines Objekts zusammen.



Verwandte Informationen

"Monitor Fehlerbehebung"

Aufnahme von Objekten

StorageGRID schützt Objekte bei der Aufnahme, entweder durch synchrones Platzieren oder durch Dual-Commit, wie in der ILM-Regel, die den Objekten entspricht.

Wenn ein S3- oder Swift-Client ein Objekt im Grid speichert, führt StorageGRID das Objekt mithilfe einer der folgenden beiden Methoden ein:

- **Synchronous Placement**: StorageGRID erstellt sofort alle Objektkopien, die zur Erfüllung der ILM-Anforderungen benötigt werden. StorageGRID sendet eine Nachricht „`Aufnahme erfolgreich`“ an den Client, wenn alle Kopien erstellt werden.

  Wenn StorageGRID nicht sofort alle Objektkopien erstellen kann (z. B. weil ein erforderlicher Standort vorübergehend nicht verfügbar ist), sendet er entweder eine „`Aufnahme fehlgeschlagen`“-Nachricht an den Client, Es ist aber auch möglich, vorläufige Objektkopien zu erstellen und ILM später zu evaluieren. Dies hängt davon ab, welche Auswahl Sie bei der Erstellung der ILM-Regel getroffen haben.

- **Dual Commit**: StorageGRID erstellt sofort zwei Zwischenkopien des Objekts, jedes auf einem anderen Speicherknoten und sendet eine „`Aufnahme erfolgreich`“-Nachricht an den Client. StorageGRID Warteschlangen für die ILM-Bewertung.

  Wenn StorageGRID die ILM-Bewertung durchführt, wird zunächst geprüft, ob die übergangsweisen Kopien die Anweisungen zur Platzierung in der ILM-Regel erfüllen. So könnten die beiden vorläufigen Kopien beispielsweise die Anweisungen in einer ILM-Regel mit zwei Kopien erfüllen, doch würden sie die Anweisungen in einer Regel für das Erasure Coding nicht erfüllen. Wenn die Zwischenkopien die ILM-Anweisungen nicht erfüllen, erstellt StorageGRID neue Objektkopien und löscht alle nicht benötigten Zwischenkopien.

  Wenn StorageGRID nicht zwei Übergangskopien erstellen kann (z. B. wenn ein Netzwerkproblem die Erstellung der zweiten Kopie verhindert), wird StorageGRID nicht erneut versuchen. Aufnahme schlägt fehl.

> ⓘ S3- oder Swift-Clients können angeben, dass StorageGRID bei der Aufnahme eine einzelne Interimskopie erstellt `REDUCED_REDUNDANCY` Für die Speicherklasse. Weitere Informationen finden Sie in der Anleitung zur Implementierung eines S3- oder Swift-Clients.

StorageGRID verwendet standardmäßig die synchrone Platzierung, um Objekte bei der Aufnahme zu schützen.

Verwandte Informationen

"Datensicherungsoptionen für die Aufnahme"

"S3 verwenden"

"Verwenden Sie Swift"

Datensicherungsoptionen für die Aufnahme

Bei der Erstellung einer ILM-Regel geben Sie eine von drei Optionen zum Schutz von Objekten bei ihrer Aufnahme an: Doppelte Provisionierung, Balance oder strikte. 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.

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. Bei der Verwendung von Dual-Commit müssen Sie sicherstellen, dass das Grid zusätzliche Aufgaben zur Erstellung und Entfernung der Dual-Commit-Kopien ausführen kann, wenn sie ILM nicht erfüllen. Im Detail:
  - Die Last am Grid muss so gering sein, dass kein ILM-Rückstand mehr vorhanden ist.
  - Das Grid muss über überschüssige Hardware-Ressourcen verfügen (IOPS, CPU, Arbeitsspeicher, Netzwerkbandbreite usw.).
- Sie verwenden ILM-Regeln für mehrere Standorte und die WAN-Verbindung zwischen den Standorten weist normalerweise eine hohe Latenz oder eine begrenzte Bandbreite auf. In diesem Szenario kann die Verwendung der Dual-Commit-Option dazu beitragen, Client-Timeouts zu verhindern. Bevor Sie sich für die Dual Commit-Option entscheiden, sollten Sie die Client-Applikation mit realistischen Workloads testen.

Streng

Wenn Sie die strenge Option auswählen, verwendet StorageGRID bei der Aufnahme eine synchrone Platzierung und erstellt sofort alle Objektkopien, die in der Plazierung der Regel angegeben sind. Die Aufnahme schlägt fehl, wenn StorageGRID beispielsweise nicht alle Kopien erstellen kann, da ein benötigter Speicherplatz 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. Beispielsweise müssen Sie zur Einhaltung gesetzlicher Vorgaben unter Umständen die strenge Option und einen erweiterten Filter für Speicherortbeschränkungen verwenden, um zu gewährleisten, dass Objekte nie in einem bestimmten Rechenzentrum gespeichert werden.

"Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"

Ausgeglichen

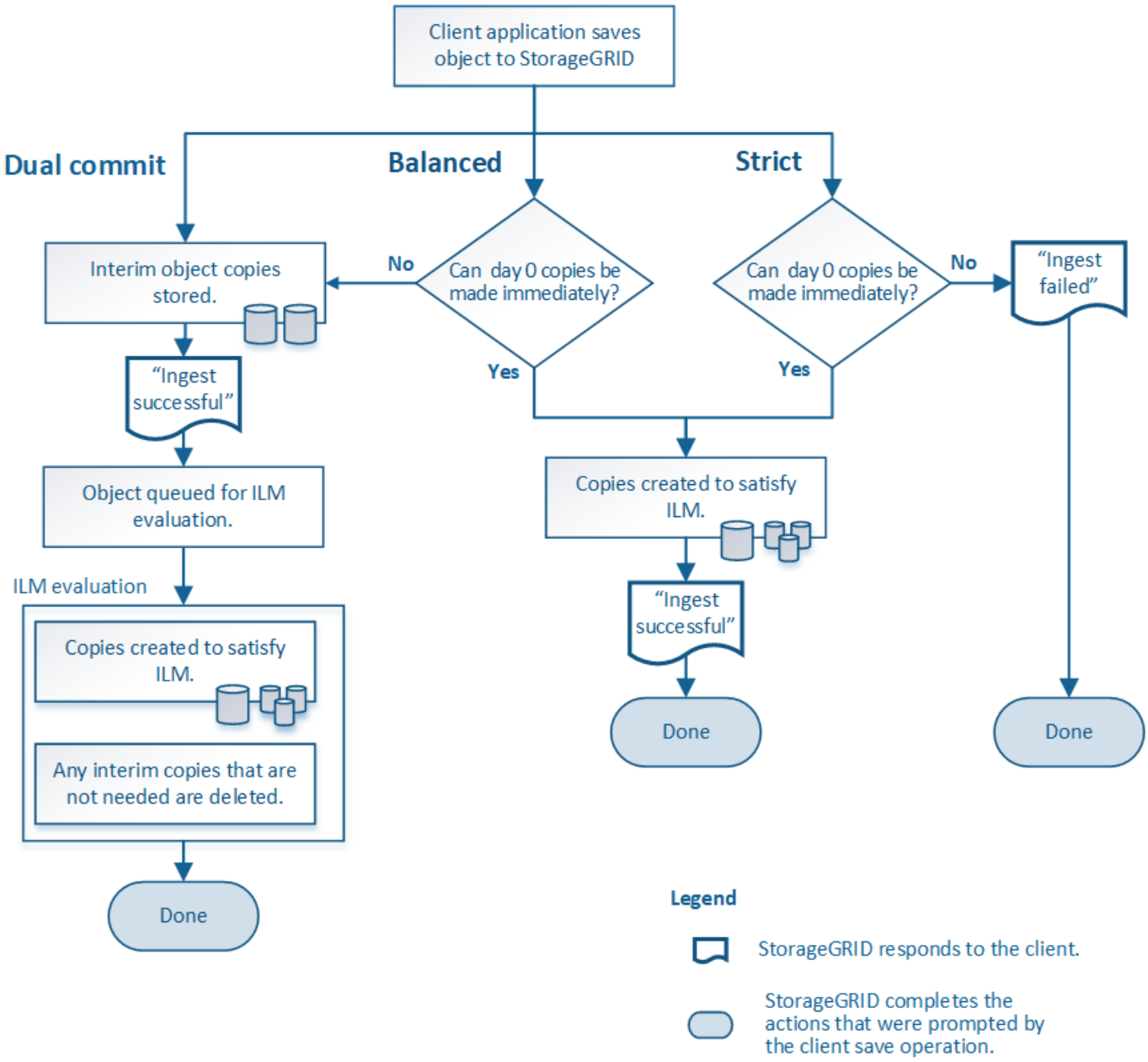
Wenn Sie die Option „Ausgleich“ auswählen, verwendet StorageGRID bei der Aufnahme auch die synchrone Platzierung und erstellt sofort alle Kopien, die in den Anweisungen zur Platzierung der Regel angegeben sind. Falls StorageGRID nicht sofort alle Kopien erstellen kann, verwendet er dagegen die doppelte Provisionierung.

Wann sollte die Option „Balance“ verwendet werden

Die ausgewogene Option erzielt die beste Kombination aus Datensicherung, Grid-Performance und Aufnahme-Erfolg. Balance ist die Standardoption im ILM-Regelassistenten.

Flussdiagramm mit drei Aufnahmeoptionen

Das Flussdiagramm zeigt, was passiert, wenn Objekte mit einer ILM-Regel abgeglichen werden, die eine dieser Aufnahmeoptionen verwendet.



Verwandte Informationen

"Aufnahme von Objekten"

Vor- und Nachteile sowie Einschränkungen der Datensicherungsoptionen

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.

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 Option „Balanced“ wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Grid erfüllt alle Kriterien für die Verwendung von Dual-Commit.
- **(striktes) Gewissheit über Objektstandorte**: Die strenge Option garantiert, dass Objekte sofort nach den Platzierungsanweisungen in der ILM-Regel gespeichert werden.

Nachteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual Commit haben die ausgewogenen und strengen Optionen einige Nachteile:

- **Längere Client-Ingest**: Client-Ingest-Latenzen können länger sein. Wenn Sie die ausgeglichenen und strengen Optionen verwenden, wird eine „`Aufnahme erfolgreich`“-Meldung erst an den Client zurückgegeben, wenn alle mit Erasure Coding verschlüsselten Fragmente oder replizierte Kopien erstellt und gespeichert werden. Objektdaten werden allerdings sehr wahrscheinlich die endgültige Platzierung viel schneller erreichen.
- **(strenge) höhere Aufnahmeraten**: Bei der strikten Option schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle Kopien erstellen kann, die in der ILM-Regel angegeben sind. 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 jedoch für jeden Teil des Objekts während der Aufnahme und für das Objekt als Ganzes bewertet, 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 werden alle Teile, die nicht korrekt platziert werden, zur ILM-Neubewertung in eine Warteschlange eingereiht und zu einem späteren Zeitpunkt an den richtigen Ort 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 Standorten gespeichert werden können, die die ILM-Anforderungen für das Objekt als Ganzes 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. Falls erforderliche Platzierungsänderungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Standort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung vor, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei der Platzierung von Objekten mit den ausgewogenen oder strengen Optionen

Die ausgewogenen oder strengen Optionen können nicht für ILM-Regeln verwendet werden, die eine der folgenden Anweisungen zur Platzierung haben:

- Platzierung in einem Cloud-Storage-Pool am Tag 0
- Platzierung in einem Archiv-Knoten an Tag 0.
- Platzierungen in einem Cloud-Speicherpool oder einem Archivknoten, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit hat.

Diese Einschränkungen sind vorhanden, da StorageGRID keine synchronen Kopien in einen Cloud-Speicherpool oder einen Archiv-Node erstellen kann und eine benutzerdefinierte Erstellungszeit auf die vorhandene auflösen 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. 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.

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
- **Verfügbar** (eventuelle Konsistenz für KOPFOPERATIONEN): Verhält sich wie das “read-after-New-write” Konsistenzniveau, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB.

Lesen Sie vor Auswahl einer Konsistenzstufe die vollständige Beschreibung dieser Einstellungen in den Anweisungen zur Erstellung einer S3- oder Swift-Client-Applikation. 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

"Was ist Replizierung"

"Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding"

"Was sind die Erasure Coding-Schemata"

"Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"

"S3 verwenden"

"Verwenden Sie Swift"

Speicherung von Objekten (Replizierung oder Erasure Coding)

StorageGRID schützt Objekte vor Verlust, indem replizierte Kopien gespeichert oder nach dem Erasure Coding Kopien gespeichert werden. Sie geben den Typ der Kopien an, die in den Anweisungen zur Platzierung von ILM-Regeln erstellt werden sollen.

- "Was ist Replizierung"
- "Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden"
- "Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding"

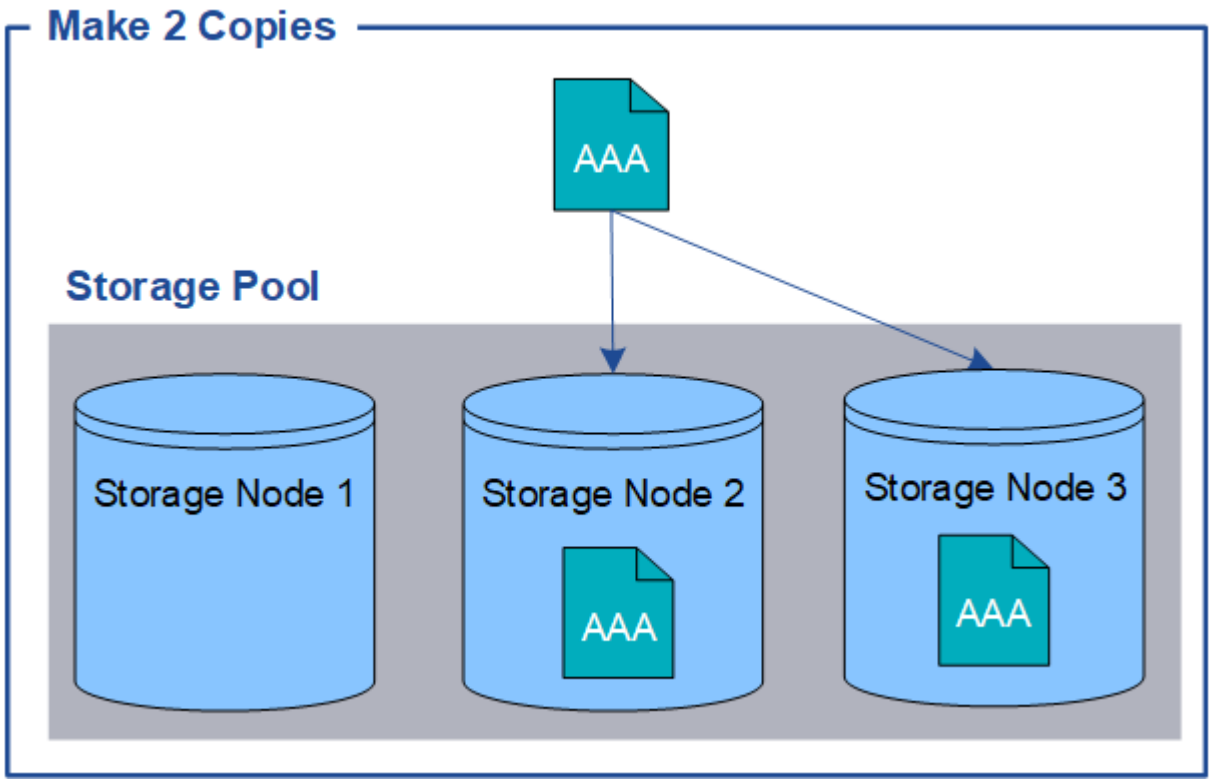
- "Was sind die Erasure Coding-Schemata"
- "Vor- und Nachteile sowie Anforderungen für Erasure Coding"

Was ist Replizierung

Die Replizierung ist eine von zwei Methoden, die von StorageGRID zum Speichern von Objektdaten verwendet werden. Wenn Objekte mit einer ILM-Regel übereinstimmen, die Replizierung verwendet, erstellt das System exakte Kopien von Objektdaten und speichert die Kopien auf Storage-Nodes oder Archiv-Nodes.

Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien konfigurieren, geben Sie an, wie viele Kopien erstellt werden sollen, wo diese Kopien erstellt werden sollen und wie lange die Kopien an jedem Standort gespeichert werden sollen.

Im folgenden Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts in einem Storage-Pool mit drei Storage-Nodes platziert werden.



Wenn StorageGRID Objekte mit dieser Regel übereinstimmt, werden zwei Kopien des Objekts erstellt, wobei jede Kopie auf einem anderen Storage-Node im Storage-Pool platziert wird. Die beiden Kopien können auf zwei der drei verfügbaren Storage-Nodes platziert werden. In diesem Fall wurden in der Regel Objektkopien auf Speicherknoten 2 und 3 platziert. Da es zwei Kopien gibt, kann das Objekt abgerufen werden, wenn einer der Nodes im Speicherpool ausfällt.

> StorageGRID kann nur eine replizierte Kopie eines Objekts auf einem beliebigen Storage Node speichern. Wenn Ihr Grid drei Storage-Nodes enthält und Sie eine ILM-Regel mit 4 Kopien erstellen, werden nur drei Kopien erstellt: Eine Kopie für jeden Storage-Node. Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Verwandte Informationen

"Was ist ein Speicherpool"

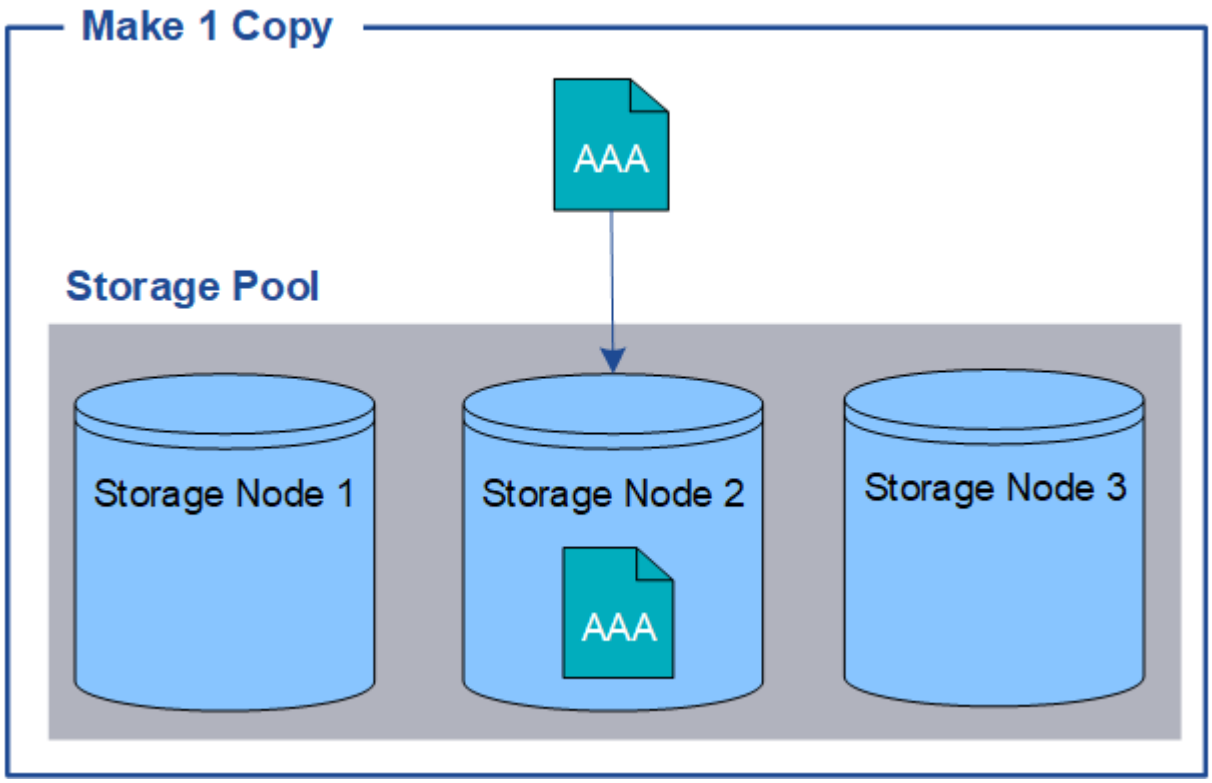
"Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung"

Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden

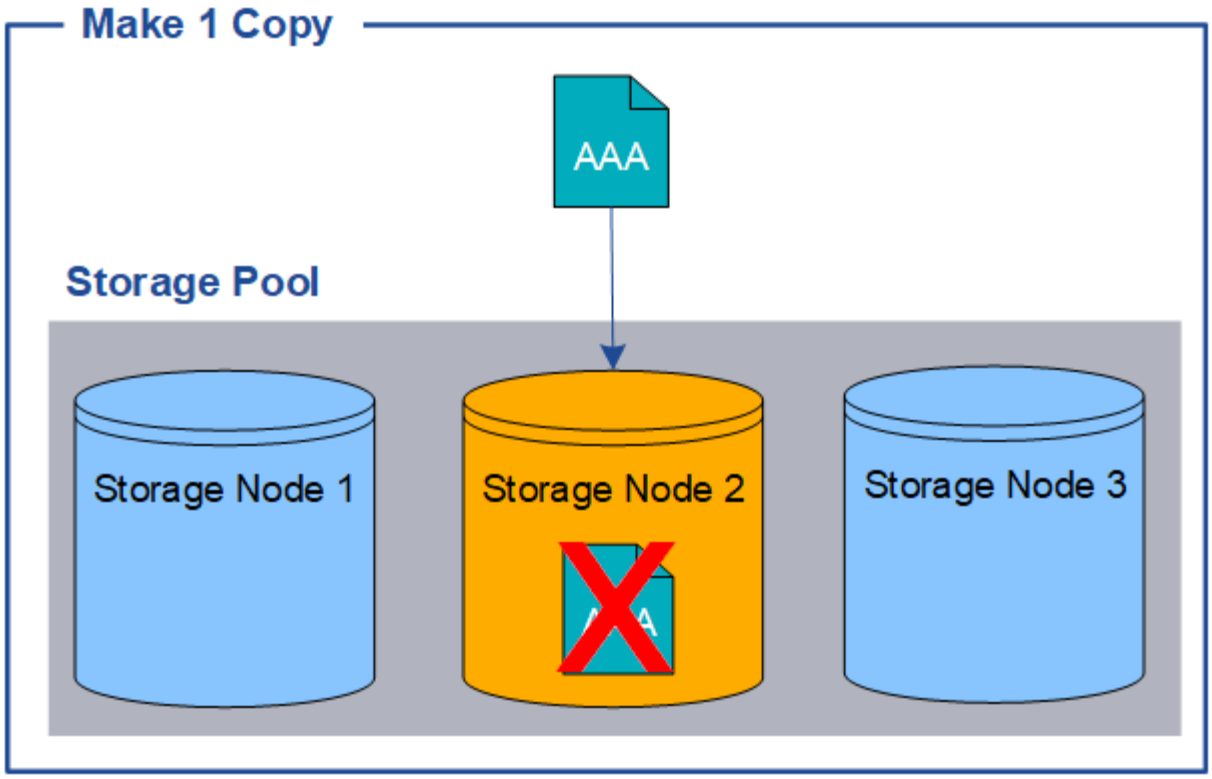
Beim Erstellen einer ILM-Regel zum Erstellen replizierter Kopien sollten Sie immer mindestens zwei Kopien für einen beliebigen Zeitraum in den Anweisungen zur Platzierung angeben.

> Verwenden Sie keine ILM-Regel, die immer nur eine replizierte Kopie 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.

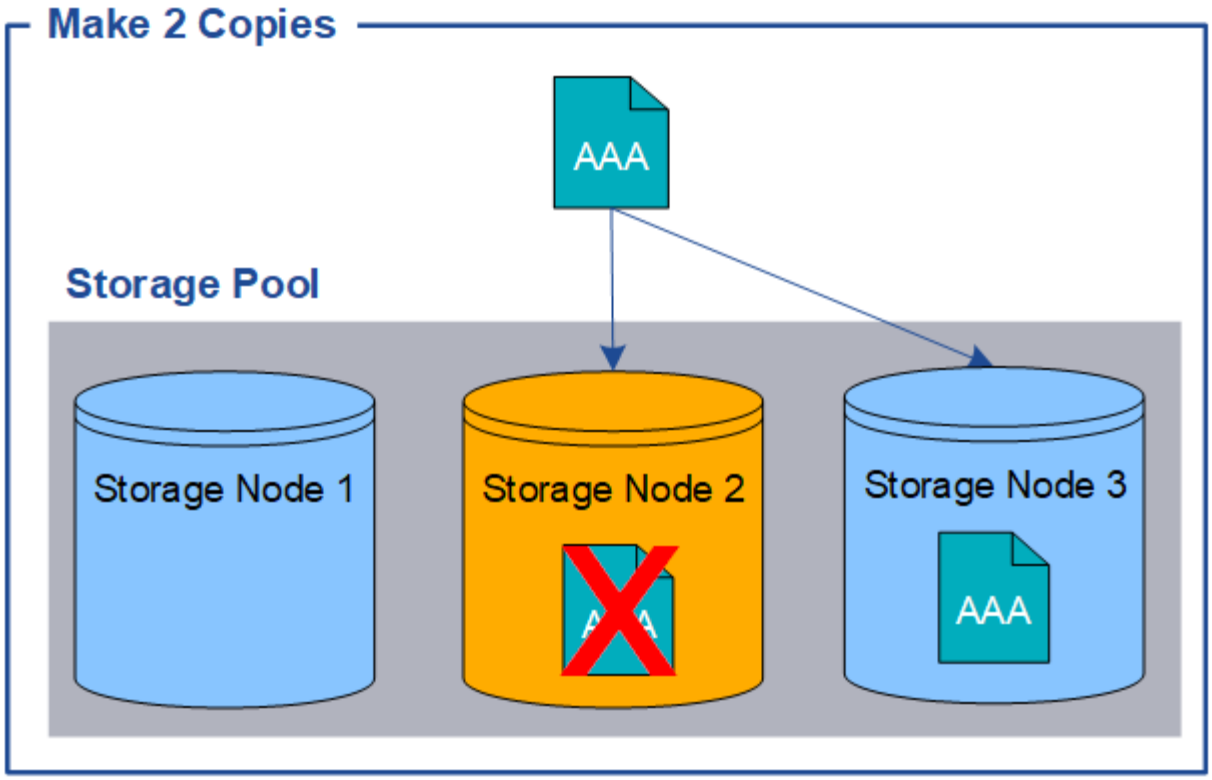
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool platziert wird, der drei Storage-Nodes enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Storage-Node.



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.



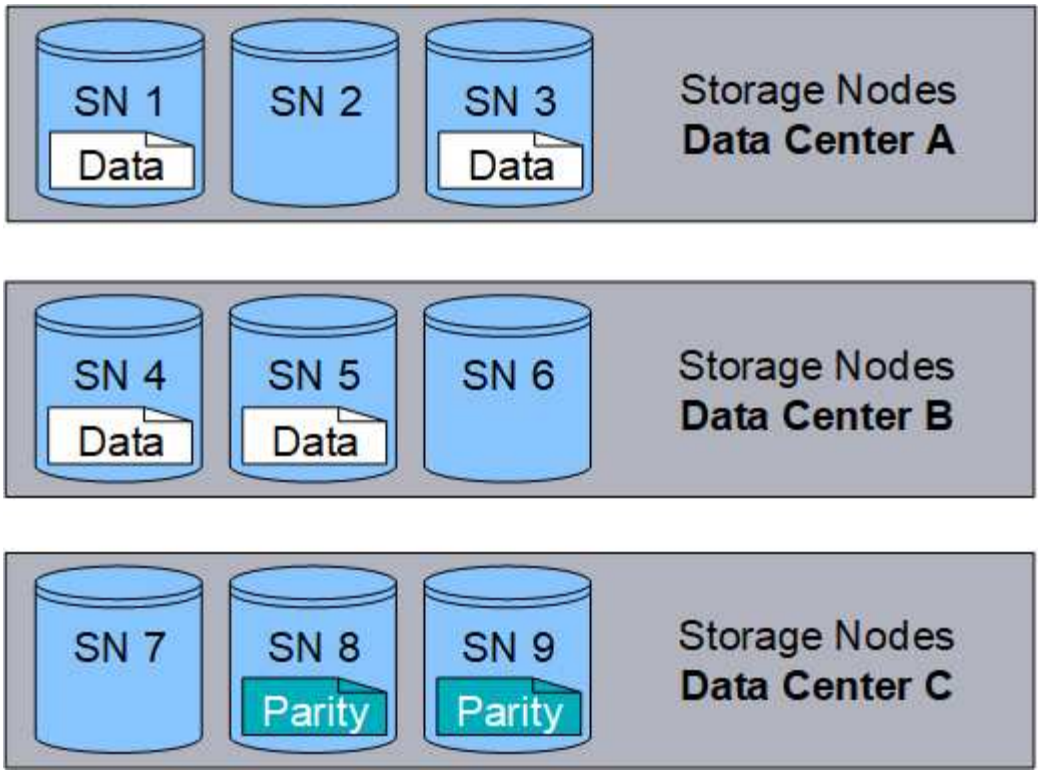
Um den Verlust von Objektdaten zu vermeiden, sollten immer mindestens zwei Kopien aller Objekte erstellt werden, die durch die Replizierung gesichert werden sollen. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Storage-Node ausfällt oder offline geht.



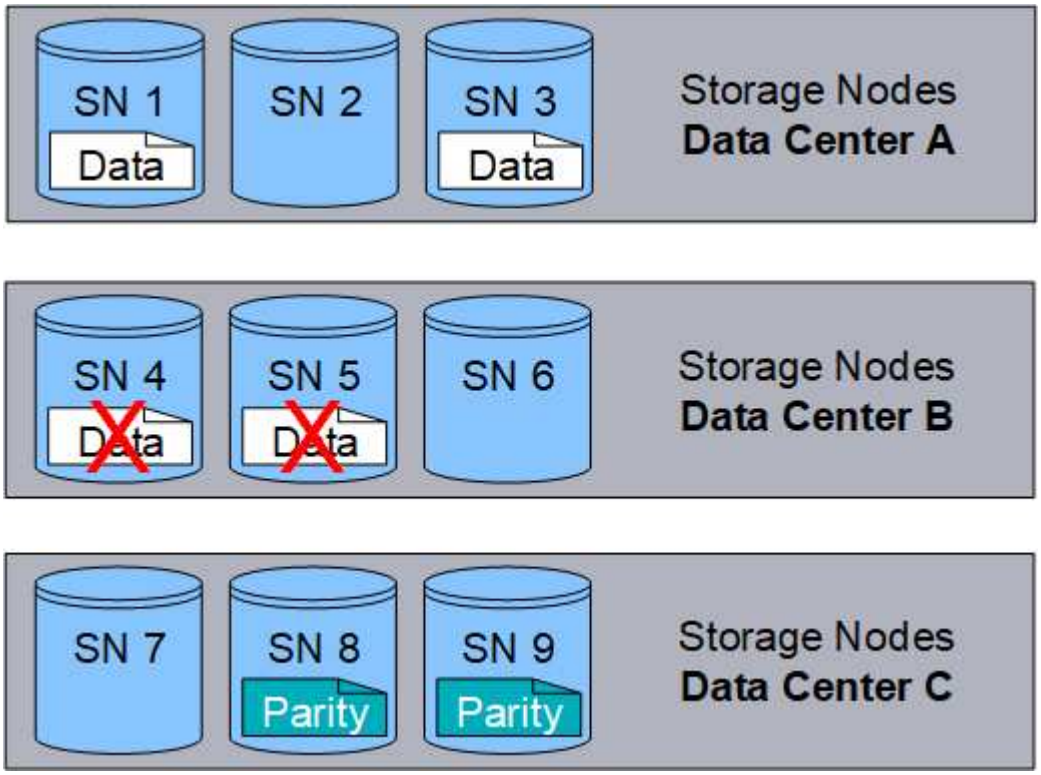
Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding

Das Verfahren zur Einhaltung von Datenkonsistenz ist die zweite Methode, die von StorageGRID zum Speichern von Objektdaten verwendet wird. 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 zur Fehlerkorrektur dieses Fragment mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente neu erstellen.

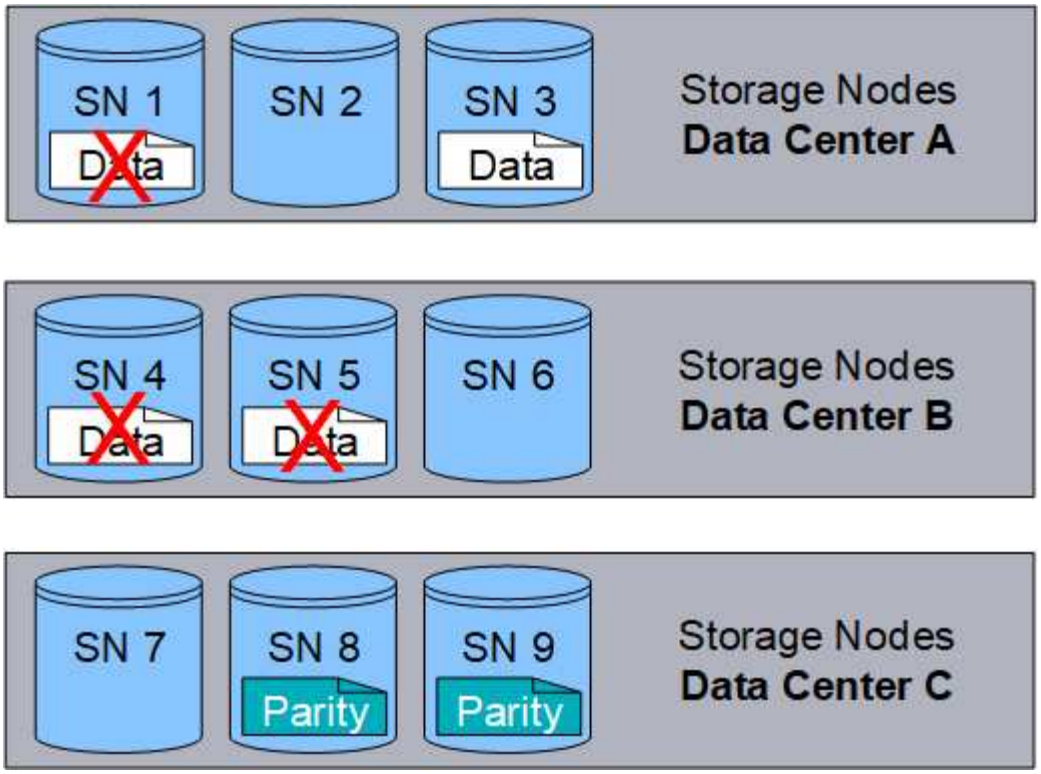
Im folgenden Beispiel wird der Algorithmus zur Einhaltung von Datenkonsistenz (Erasure Coding) für Objektdaten dargestellt. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden 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 Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) in 4+2 erfordert mindestens neun Storage-Nodes mit drei Storage-Nodes an jedem der drei Standorte. 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. Bei einem Ausfall eines gesamten Datacenter-Standorts kann das Objekt weiterhin abgerufen oder repariert werden, solange alle anderen Fragmente verfügbar sind.



Wenn mehr als zwei Speicherknoten verloren gehen, kann das Objekt nicht abgerufen werden.



Verwandte Informationen

"Was ist ein Speicherpool"

"Was sind die Erasure Coding-Schemata"

"Konfigurieren von Erasure Coding-Profilen"

Was sind die Erasure Coding-Schemata

Wenn Sie das Erasure Coding-Profil für eine ILM-Regel konfigurieren, wählen Sie ein verfügbares Codierungsschema zur Fehlerkorrektur aus, basierend darauf, wie viele Storage-Nodes und -Standorte den zu verwendenden Speicherpool bilden. Erasure Coding steuert die Anzahl von Datenfragmenten und die Anzahl der Parity-Fragmente für jedes Objekt.

Das StorageGRID-System verwendet den Reed-Solomon-Erasure-Coding-Algorithmus. Der Algorithmus schneidet ein Objekt in k Datenfragmente auf und berechnet m Paritätsfragmente. Die k + m = n Fragmente sind auf n Speicherknoten verteilt, um die Datensicherung zu gewährleisten. Ein Objekt kann bis zu m verlorene oder beschädigte Fragmente erhalten. k Fragmente sind erforderlich, um ein Objekt abzurufen oder zu reparieren.

Verwenden Sie bei der Konfiguration eines Erasure Coding-Profils die folgenden Richtlinien für Speicherpools:

- Der Speicherpool muss drei oder mehr Standorte oder exakt einen Standort umfassen.

  Sie können kein Erasure Coding-Profil konfigurieren, wenn der Speicherpool 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 nicht den Standardspeicherpool, alle Speicherknoten oder einen Speicherpool, der den Standardstandort, Alle Standorte, enthält.
- Der Speicherpool sollte mindestens *k*+*m* +1 Storage-Nodes enthalten.

  Die Mindestanzahl der benötigten Storage-Nodes beträgt *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 berechnet, indem die Anzahl der Paritäts-Fragmente (*m*) durch die Anzahl der Datenfragmente (*k*) geteilt wird. Der Storage Overhead lässt sich ermitteln, wie viel Festplattenspeicher jedes mit Erasure-Coding-Objekt benötigt:

```
disk space = object size + (object size * storage overhead)
```

Wenn Sie beispielsweise ein Objekt mit 10 MB unter Verwendung des Schemas von 4+2 speichern (mit einem Mehraufwand von 50 %), verbraucht das Objekt 15 MB Grid Storage. Wenn Sie dasselbe 10 MB große Objekt mit dem Schema 6+2 speichern (mit einem Mehraufwand von 33 %), verbraucht das Objekt etwa 13.3 MB.

Wählen Sie das Erasure-Coding-Schema mit dem niedrigsten Gesamtwert von *k*+*m* aus, das Ihren Anforderungen entspricht. Erasure Coding-Schemata mit einer geringeren Anzahl von Fragmenten werden insgesamt recheneffizienter, da weniger Fragmente pro Objekt erstellt und verteilt (oder abgerufen) werden. Je größer die Fragmentgröße ist, desto weniger Nodes können bei einer Erweiterung hinzugefügt werden, wenn mehr Storage benötigt wird. (Informationen zur Planung einer Speichererweiterung finden Sie in den Anweisungen zum erweitern 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 Systeme bieten einen Schutz vor Schäden an den Standorten. Ein Standort kann verloren gehen, und das Objekt ist weiterhin verfügbar.

Für Erasure-Coding-Schemata, die Site-Loss-Schutz bieten, übersteigt die empfohlene Anzahl von Storage-Nodes im Speicherpool die Anzahl *k*+*m*+1, da für jeden Standort mindestens drei Storage-Nodes erforderlich sind.

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
6 + 3	3	4	12	Ja.	50 % erzielt
9 + 3	4	4	16	Ja.	33 % 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
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 durch mehr Paritäts-Segmente erhöht (d. h. wenn *m* einen höheren Wert hat).
- **Netzverkehr**: Bei der Wiederherstellung nach Ausfällen erzeugt ein Schema mit mehr Fragmenten (das heißt, eine höhere Summe für *k*+*m*) 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 erforderliche Mindestanzahl an Storage-Nodes beträgt *k*+*m*, es wird jedoch ein Speicherpool mit *k*+*m*+1 Storage-Nodes 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

Verwandte Informationen

"Erweitern Sie Ihr Raster"

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:

- Es ist eine größere Anzahl von Speicherknoten und Standorten erforderlich. Wenn Sie beispielsweise ein Erasure-Coding-Schema von 6+3 verwenden, müssen Sie mindestens drei Storage-Nodes an drei verschiedenen Standorten haben. Wenn Sie dagegen nur Objektdaten replizieren, benötigen Sie nur einen Storage Node für jede Kopie.
- Höhere Kosten und Komplexität der Storage-Erweiterungen. Um eine Implementierung mit Replizierung zu erweitern, fügen Sie einfach Storage-Kapazität an jedem Speicherort hinzu, an dem Objektkopien erstellt werden. 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 vorhandene Nodes zu 100 % voll sind, müssen Sie mindestens *k*+*m* Storage-Nodes hinzufügen. Wenn jedoch vorhandene Nodes zu 70 % voll sind, können Sie zwei Nodes pro Standort hinzufügen und dennoch die nutzbare Storage-Kapazität maximieren. Weitere Informationen finden Sie in den Anweisungen zum erweitern von StorageGRID.
- 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.

> Aufgrund des Overhead zum Managen der Anzahl von Fragmenten, die mit einer mit Erasure Coding verschlüsselten Kopie verbunden sind, sollten Sie für Objekte, die mindestens 200 KB groß sind, kein Erasure Coding verwenden.

- 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

Verwandte Informationen

"Erweitern Sie Ihr Raster"

Wie die Aufbewahrung von Objekten bestimmt wird

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzer Optionen, um die Speicherdauer von Objekten festzulegen. Im Allgemeinen haben alle von einem Mandantenbenutzer bereitgestellten Aufbewahrungsanweisungen Vorrang vor den Aufbewahrungsanweisungen, die vom Grid-Administrator bereitgestellt werden.

Wie Mandantenbenutzer die Aufbewahrung von Objekten steuern

Mandantenbenutzer haben drei primäre Möglichkeiten, um zu steuern, wie lange ihre Objekte in StorageGRID gespeichert sind:

- Wenn die globale S3-Objektsperreneinstellung für das Grid aktiviert ist, können Nutzer von S3-Mandanten Buckets erstellen, deren S3-Objektsperre aktiviert ist. Anschließend können sie über die S3-REST-API Aufbewahrungseinstellungen für jede zu diesem Bucket hinzugefügte Objektversion festlegen.
  - Eine Objektversion, die sich unter einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht mit irgendeiner 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.

    "Verwalten von Objekten 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.
- 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.

Verwandte Informationen

"Verwalten von Objekten mit S3 Object Lock"

"S3 verwenden"

"Welche Anweisungen zur Platzierung der ILM-Regeln gibt es"

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Antwort auf eine Client-Anfrage oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der Anforderungen der ILM-Richtlinie löschen. Wenn Sie verstehen, auf welche Weise Objekte gelöscht werden können und wie StorageGRID Löschanfragen verarbeitet, können Sie Objekte effizienter managen.

StorageGRID kann Objekte auf eine von zwei Methoden löschen:

- Synchrones Löschen: Erhält StorageGRID eine Client-Löschanforderung, werden alle Objektkopien sofort entfernt. Der Client wird informiert, dass das Löschen nach dem Entfernen der Kopien erfolgreich war.
- Objekte werden zum Löschen in die Warteschlange eingereiht: Wenn StorageGRID eine Löschanforderung empfängt, wird das Objekt zum Löschen in die Warteschlange verschoben. Der Client wird umgehend darüber informiert, dass das Löschen erfolgreich war. Objektkopien werden später durch ILM-Verarbeitung im Hintergrund entfernt.

Beim Löschen von Objekten verwendet StorageGRID die Methode, die das Löschen der Performance optimiert, mögliche Rückprotokolle für das Löschen minimiert und Speicherplatz am schnellsten freigegeben wird.

Die Tabelle fasst zusammen, wann StorageGRID die einzelnen Methoden verwendet.

Löschmethode	Wenn verwendet
Objekte werden zum Löschen in eine Warteschlange eingereiht	Wenn **eine** der folgenden Bedingungen zutrifft: • Das automatische Löschen von Objekten wurde von einem der folgenden Ereignisse ausgelöst: ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket erreicht ist. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. **Hinweis:** Objekte in einem Bucket mit aktivierter S3-Objektsperre können nicht gelöscht werden, wenn sie sich unter einer gesetzlichen Sperre befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde. • Ein S3- oder Swift-Client fordert eine Löschung an. Eine oder mehrere der folgenden Bedingungen gilt: ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, da z. B. ein Objektverzeichnis vorübergehend nicht verfügbar ist. ◦ Löschwarteschlangen im Hintergrund sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	Wenn ein S3- oder Swift-Client eine Löschanfrage erstellt und **alle** der folgenden Bedingungen erfüllt sind: • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Warteschlangen zum Löschen im Hintergrund enthalten Objekte, die verarbeitet werden sollen.

Wenn S3- oder Swift-Clients Anforderungen löschen, beginnt StorageGRID mit dem Hinzufügen einer Reihe von Objekten zur Löschwarteschlange. 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.

Allgemeines zum Löschen von Objekten in StorageGRID

Die Art und Weise, wie StorageGRID Objekte löscht, kann sich auf die Ausführung des Systems auswirken:

- Wenn StorageGRID das synchrone Löschen durchführt, kann StorageGRID bis zu 30 Sekunden dauern, bis ein Ergebnis an den Client zurückgegeben wird. Das heißt, das Löschen kann scheinbar langsamer erfolgen, auch wenn Kopien tatsächlich schneller entfernt werden als wenn StorageGRID Objekte zum Löschen Warteschlangen.
- Falls Sie die Löschleistung während eines Massenlöschs genau überwachen, kann es vorkommen, dass sich die Löschrate nach dem Löschen einer bestimmten Anzahl von Objekten verlangsamt. Diese Änderung tritt auf, wenn StorageGRID von Objekten aus der Warteschlange zum Löschen auf das synchrone Löschen verschiebt. Die offensichtliche Reduzierung der Löschrate bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil: Er zeigt an, dass durchschnittlich Speicherplatz schneller freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, Speicherplatz schnell freizugeben, ziehen Sie in Betracht, Objekte mithilfe einer Client-Anfrage zu löschen, anstatt sie mit ILM oder anderen Methoden zu löschen. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn das Löschen durch Clients durchgeführt wird, da StorageGRID das synchrone Löschen verwenden kann.

Beachten Sie, dass die zur Freigabe von Speicherplatz nach dem Löschen eines Objekts benötigte Zeit von mehreren Faktoren abhängt:

- Gibt an, ob Objektkopien synchron entfernt werden oder später zur Entfernung in die Warteschlange verschoben werden (für Client-Löschanfragen).
- Weitere Faktoren wie die Anzahl der Objekte im Grid oder die Verfügbarkeit von Grid-Ressourcen, wenn Objektkopien zur Entfernung in eine Warteschlange verschoben werden (für Clientlöschungen und andere Methoden).

Löschen von S3-versionierten Objekten

Wenn die Versionierung für einen S3-Bucket aktiviert ist, befolgt StorageGRID das Verhalten von Amazon S3, wenn es auf Löschanfragen reagiert, unabhängig davon, ob diese Anfragen von einem S3-Client, dem Ablauf eines S3-Bucket-Lebenszyklus oder den Anforderungen der ILM-Richtlinie stammen.

Wenn Objekte versioniert sind, löschen Anforderungen zum Löschen von Objekten nicht die aktuelle Version des Objekts und geben keinen freien Speicherplatz frei. Stattdessen erstellt eine Anforderung zum Löschen eines Objekts einfach eine Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „`non-current.`“

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 freien Speicherplatz zu erhalten, müssen Sie einen der folgenden Schritte ausführen:

- **S3-Clientanforderung**: Geben Sie die Objektversionsnummer in der S3-LÖSCHOBJEKTANFORDERUNG 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.
- **ILM**: Fügen Sie zwei ILM-Regeln zu Ihrer ILM-Richtlinie hinzu. Verwenden Sie **nicht aktuelle Zeit** als Referenzzeit in der ersten Regel, um die nicht aktuellen Versionen des Objekts zu entsprechen. Verwenden Sie **Aufnahmezeit** in der zweiten Regel, um mit der aktuellen Version zu übereinstimmen. Die **nicht aktuelle Zeit**-Regel muss in der Regel über der **Aufnahmezeit**-Regel erscheinen.

Verwandte Informationen

"S3 verwenden"

"Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"

Was ist eine ILM-Richtlinie

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.

Bewertung von Objekten durch eine ILM-Richtlinie

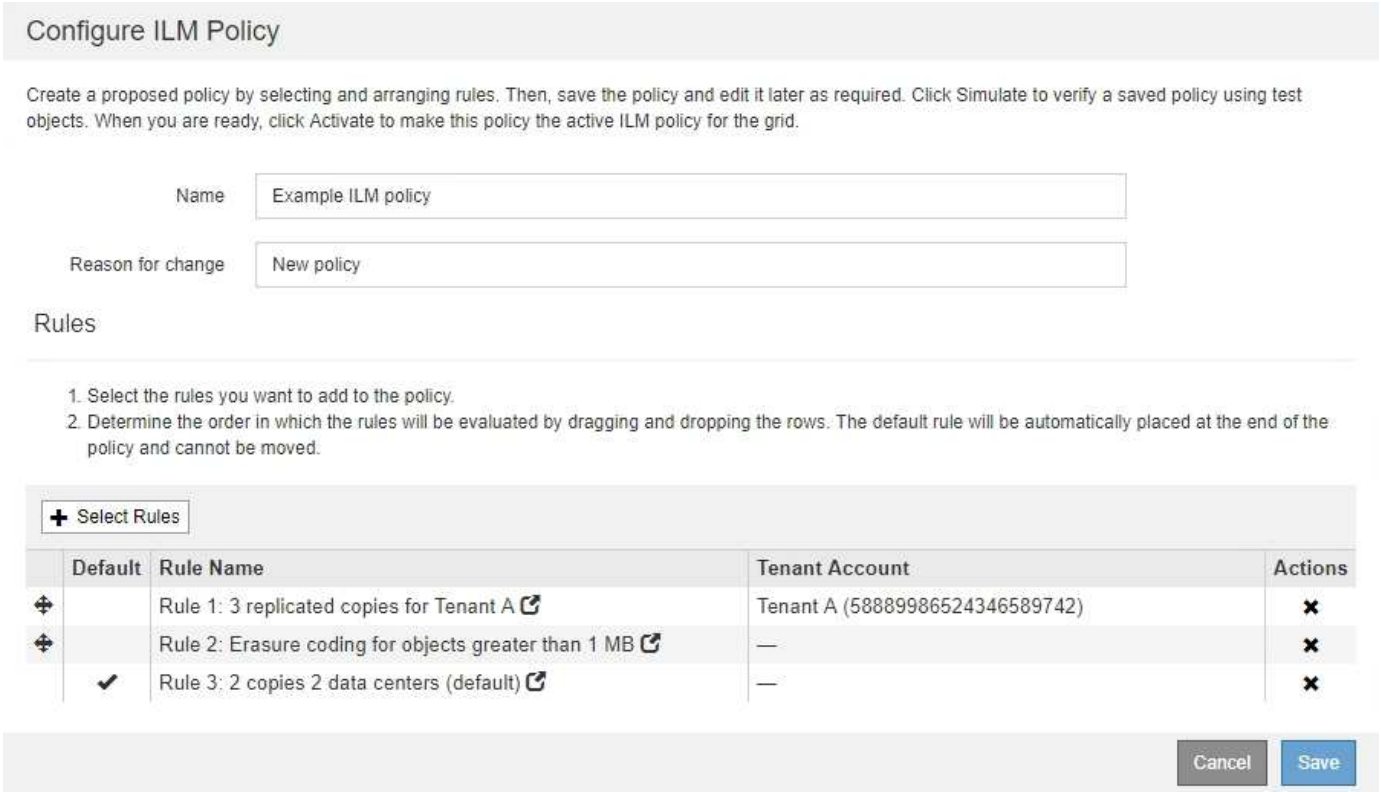
Die aktive ILM-Richtlinie für Ihr StorageGRID System steuert die Platzierung, Dauer und Datensicherung aller Objekte.

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 ausgewertet, bis eine Übereinstimmung erfolgt.
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.

Beispiel für eine ILM-Richtlinie

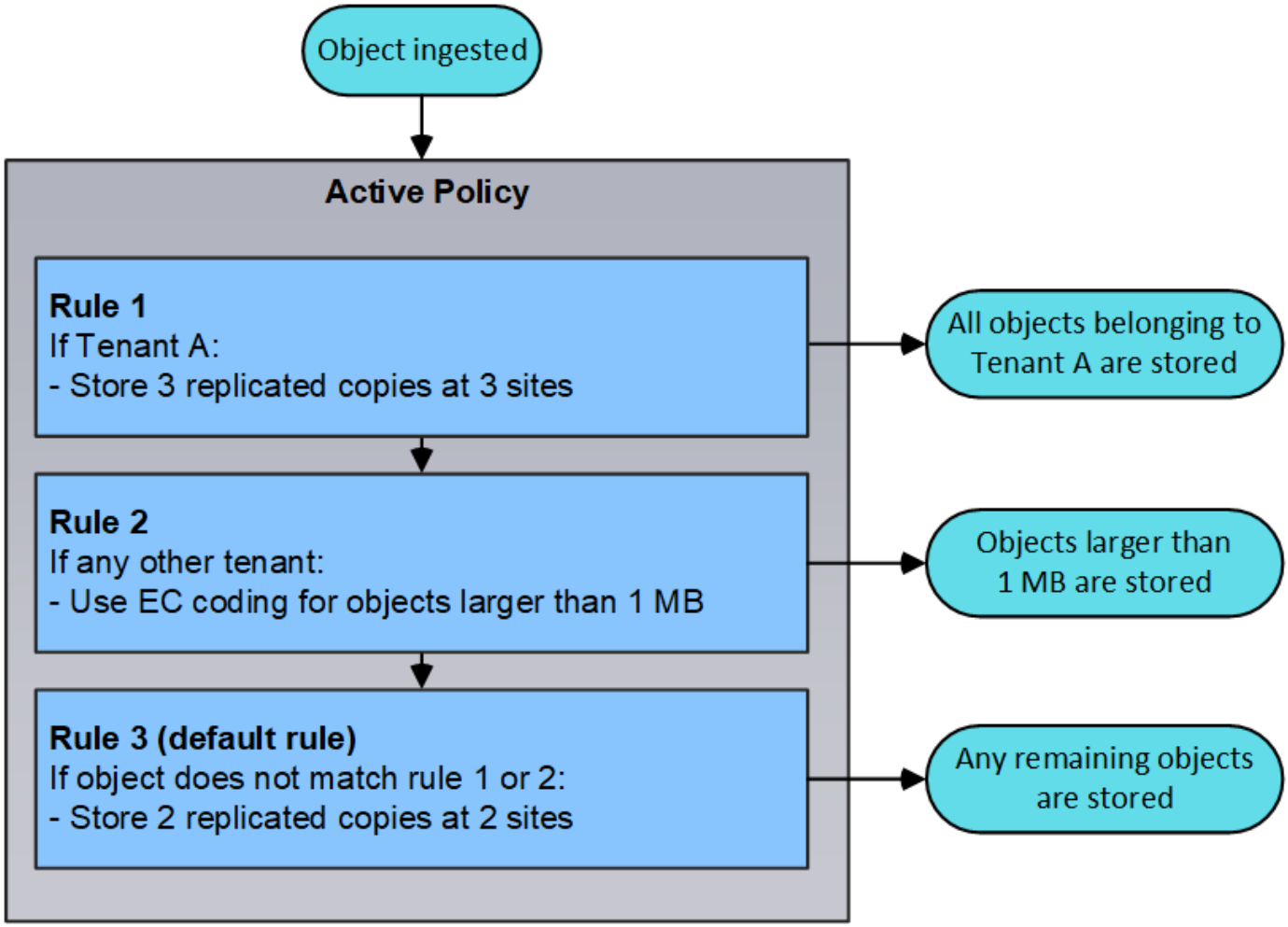
In diesem Beispiel verwendet die ILM-Richtlinie drei ILM-Regeln.



In diesem Beispiel stimmt Regel 1 mit allen Objekten überein, die zu Mandant A gehören Diese Objekte werden als drei replizierte Kopien an drei Standorten gespeichert. Objekte, die zu anderen Mietern gehören, werden von Regel 1 nicht abgeglichen, so dass sie gegen Regel 2 ausgewertet werden.

Regel 2 entspricht allen Objekten anderer Mandanten, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert. Regel 2 stimmt nicht mit Objekten 1 MB oder kleiner überein, daher werden diese Objekte gegen Regel 3 ausgewertet.

Regel 3 ist die letzte und Standardregel in der Richtlinie und verwendet keine Filter. Regel 3 erstellt zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmt (Objekte, die nicht zu Mandant A gehören, die 1 MB oder kleiner sind).



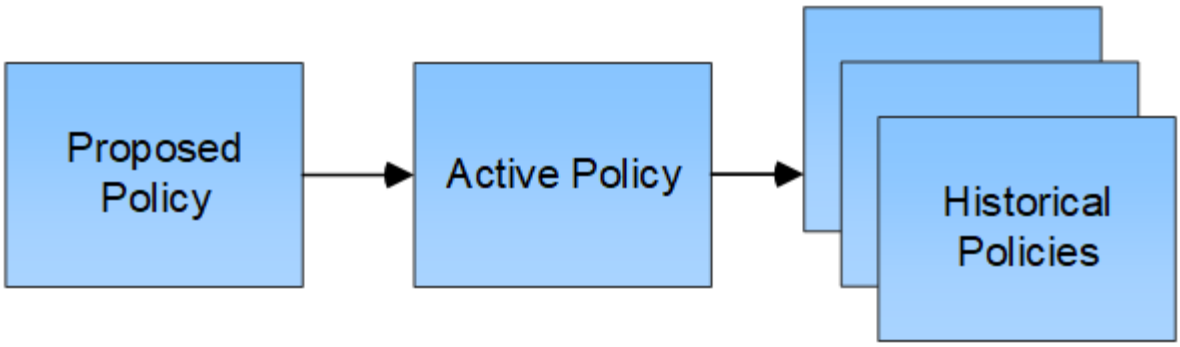
Welche vorgeschlagenen, aktiven und historischen Politiken sind

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.



Verwandte Informationen

"ILM-Richtlinie erstellen"

Was ist eine ILM-Regel

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 den Metadaten eines Objekts entspricht, legen die Anweisungen in der Regel fest, welche Aktionen StorageGRID zum Kopieren und Speichern des Objekts ergreift.

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 Koprottypen 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. Die Kopien werden gleichmäßig auf alle Storage Nodes verteilt.

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.

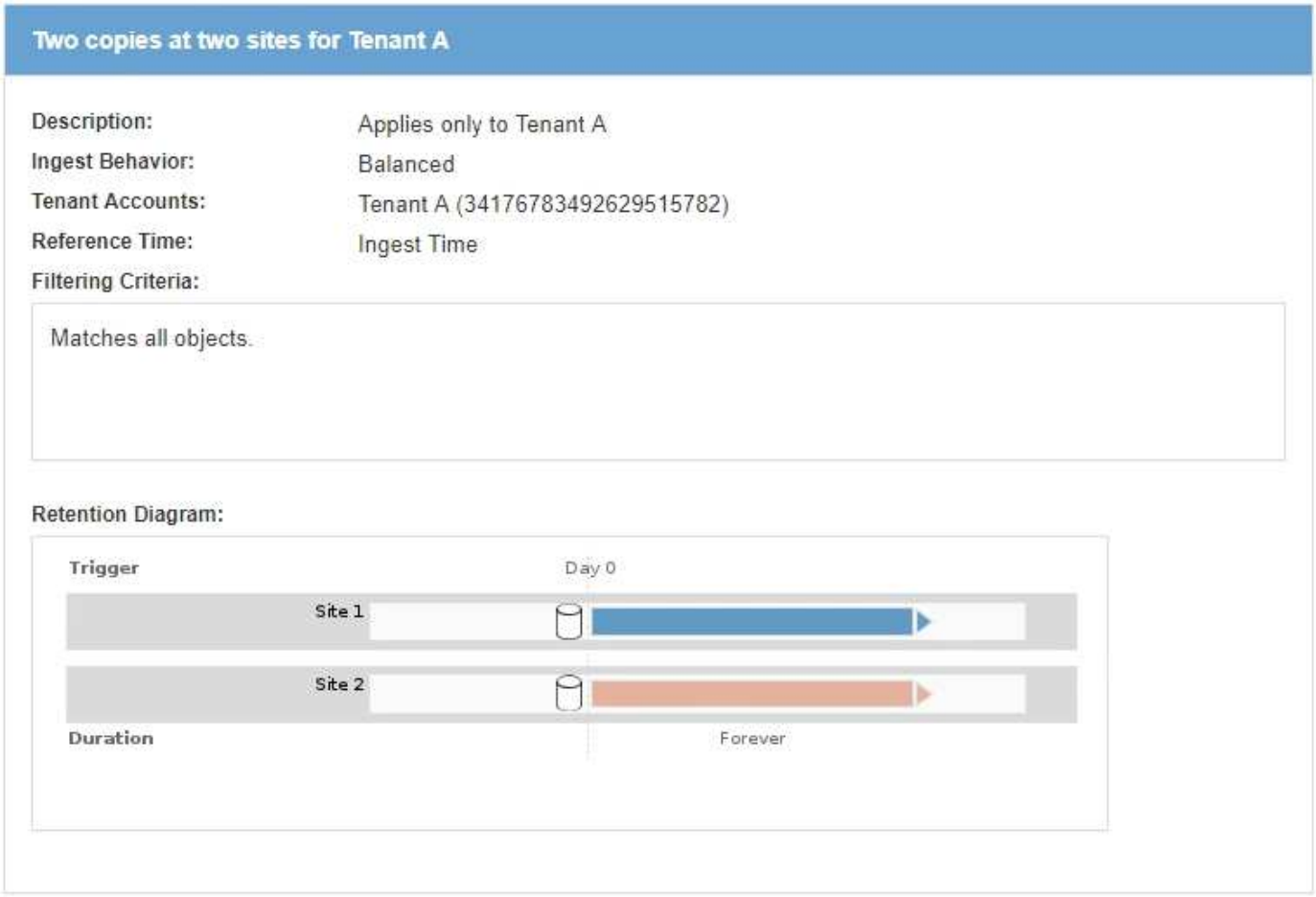
Wenn ein Objekt allen Filtern entspricht, wendet StorageGRID die Regel an und erstellt die Objektkopien, die in den Platzierungsanweisungen der Regel angegeben sind.

- **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.
- **Aufnahmeverhalten**: Das Aufnahmeverhalten einer Regel definiert, was passiert, wenn ein S3- oder Swift-Client ein Objekt im Grid speichert. 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.

Beispiel für eine ILM-Regel

Diese Beispiel-ILM-Regel gilt für die Objekte, die zu Mandant A gehören Es erstellt zwei replizierte Kopien dieser Objekte und speichert jede Kopie an einem anderen Standort. Die beiden Kopien werden „`forever`,“ aufbewahrt. Das 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.

Diese Regel verwendet die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung an zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, 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

"Datensicherungsoptionen für die Aufnahme"

"Was ist ein Speicherpool"

"Was ist ein Cloud-Storage-Pool"

"Speicherung von Objekten (Replizierung oder Erasure Coding)"

"Was ist die ILM-Regelfilterung"

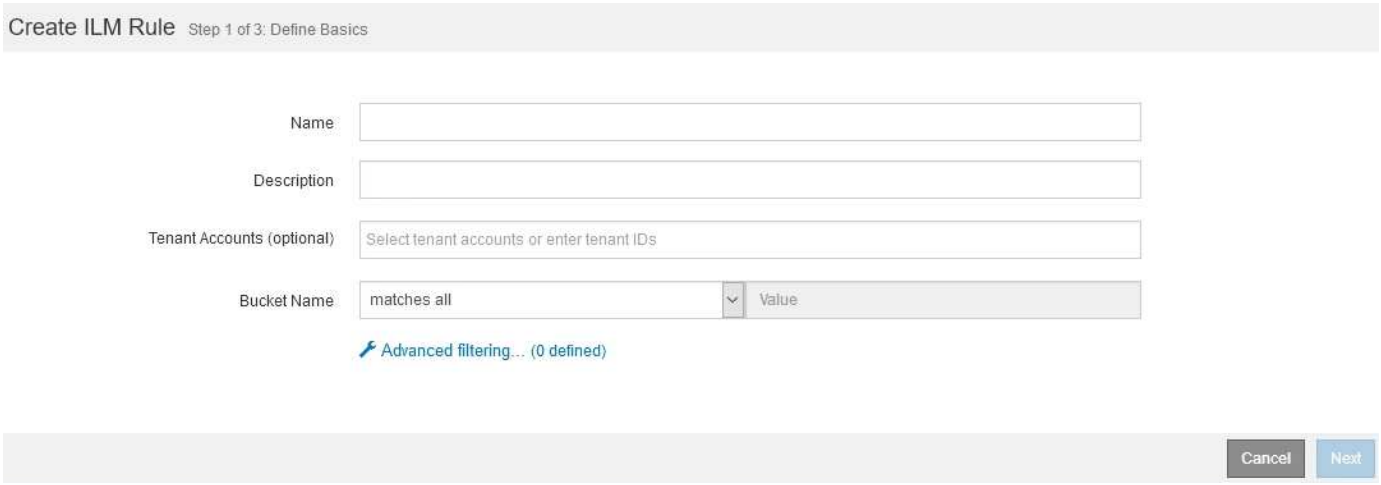
"Welche Anweisungen zur Platzierung der ILM-Regeln gibt es"

Was ist die ILM-Regelfilterung

Wenn Sie eine ILM-Regel erstellen, geben Sie Filter an, um zu identifizieren, für welche Objekte die Regel gilt.

Im einfachsten Fall verwendet eine Regel möglicherweise keine Filter. Alle Regeln, die keine Filter verwenden, gelten für alle Objekte. Daher muss es sich um die letzte (standardmäßige) Regel in einer ILM-Richtlinie handelt. Die Standardregel enthält Speicheranweisungen für Objekte, die nicht mit den Filtern in einer anderen Regel übereinstimmen.

Grundlegende Filter ermöglichen es Ihnen, unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anzuwenden. Mit den grundlegenden Filtern auf der Seite „Grundlagen definieren“ des Assistenten zur Erstellung von ILM-Regeln können Sie eine Regel auf spezifische Mandantenkonten, bestimmte S3-Buckets oder Swift-Container oder beides anwenden.



Diese Grundfilter bieten 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.

Die Seite **Advanced Filtering** des Create ILM Rule Wizard gibt Ihnen granulare Kontrolle. Sie können Filter erstellen, um Objekte anhand der folgenden Objekteigenschaften auszuwählen:

- Aufnahmezeit

- Zeitpunkt des letzten Zugriffs
- Der Objektname (Schlüssel) ganz oder teilweise
- S3-Bucket-Region (Speicherortbeschränkung)
- Objektgröße
- Benutzer-Metadaten
- S3-Objekt-Tags

Sie können Objekte nach sehr spezifischen Kriterien filtern. So können beispielsweise Objekte, die von der Bildgebungsabteilung eines Krankenhauses gespeichert sind, häufig verwendet werden, wenn sie weniger als 30 Tage alt und selten danach sind, während Objekte, die Angaben zu Patientenbesuchen enthalten, möglicherweise in die Rechnungsabteilung des Gesundheitsnetzwerks kopiert werden müssen. Sie können Filter erstellen, die jeden Objekttyp anhand von Objektnamen, -Größe, S3-Objekt-Tags oder anderen relevanten Kriterien identifizieren. Anschließend können separate Regeln erstellt werden, um jeden Objektsatz entsprechend zu speichern.

Sie können auch einfache und erweiterte 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 erweiterte Filter verwenden, um den spezifischen Objekttyp zu identifizieren, für den die Regel gilt.

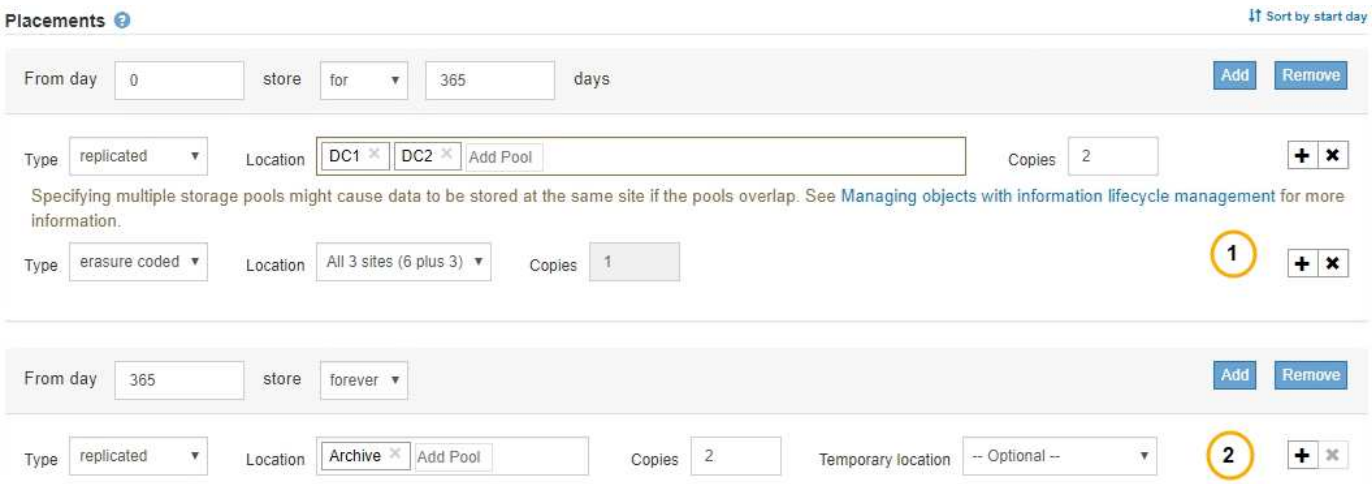
Welche Anweisungen zur Platzierung der ILM-Regeln gibt es

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.

Beim Erstellen einer Speicheranweisung geben Sie an, wann die Platzierung zutrifft (der Zeitraum), welche Art von Kopien erstellt werden sollen (repliziert oder Erasure Coding) und wo die Kopien gespeichert werden (ein oder mehrere Speicherorte). Innerhalb einer einzigen Regel können Sie mehrere Platzierungen für einen Zeitraum festlegen und Anweisungen zur Platzierung für mehr als einen Zeitraum:

- Klicken Sie auf das Pluszeichen-Symbol, um mehr als eine Objektplatzierung während eines einzelnen Zeitraums festzulegen ➕ Hinzufügen von mehr als einer Zeile für diesen Zeitraum.
- Wenn Sie für mehr als einen Zeitraum Objektplatzierungen angeben möchten, klicken Sie auf die Schaltfläche **Hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt die Seite Platzierungen definieren im Assistenten „ILM-Regel erstellen“.



1	Die erste Einstufungsanweisung hat zwei Linien für das erste Jahr: 1. In der ersten Zeile werden zwei replizierte Objektkopien an zwei Datacenter-Standorten erstellt. 2. Die zweite Zeile erstellt eine Kopie mit 6 und 3 zur Fehlerkorrektur codierten Kopien unter Verwendung von drei Datacenter-Standorten.
2	Die zweite Anleitung zur Platzierung 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.

Erstellung von Speicherklassen, Speicherpools, EC-Profilen und Regionen

Bevor Sie die ILM-Regeln für Ihr StorageGRID System erstellen können, müssen Sie Objekt-Storage-Standorte definieren, die gewünschten Kopftypen festlegen und optional S3-Bereiche konfigurieren.

- "Speicherklassen werden erstellt und zugewiesen"
- "Konfigurieren von Speicherpools"
- "Verwendung Von Cloud Storage Pools"
- "Konfigurieren von Erasure Coding-Profilen"
- "Regionen konfigurieren (nur optional und S3)"

Speicherklassen werden erstellt und zugewiesen

Speicherklassen identifizieren den Speichertyp, der von einem Speicherknoten verwendet wird. Sie können Storage-Klassen erstellen, wenn ILM-Regeln bestimmte

Objekte auf bestimmten Storage-Nodes anstatt auf allen Nodes am Standort platzieren sollen. Möglicherweise möchten Sie beispielsweise bestimmte Objekte auf Ihren schnellsten Storage-Nodes wie z. B. StorageGRID All-Flash Storage Appliances speichern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Wenn Sie mehr als einen Storage-Typ verwenden, können Sie optional eine Storage-Klasse erstellen, um jeden Typ zu identifizieren. Beim Erstellen von Speicherklassen können Sie bei der Konfiguration von Speicherpools einen bestimmten Typ von Speicherknoten auswählen.

Wenn die Speicherklasse kein Problem ist (beispielsweise sind alle Speicherknoten identisch), können Sie dieses Verfahren überspringen und bei der Konfiguration von Speicherpools die Standardspeicherklasse Alle Speicherknoten verwenden.

Wenn Sie in einer Erweiterung einen neuen Storage-Node hinzufügen, wird dieser Node zur Standardspeicherklasse Alle Storage-Nodes hinzugefügt. Das Ergebnis:

- Wenn eine ILM-Regel einen Storage-Pool mit der Klasse „Alle Storage-Nodes“ verwendet, kann der neue Node unmittelbar nach Abschluss der Erweiterung verwendet werden.
- Wenn eine ILM-Regel einen Storage-Pool mit einer benutzerdefinierten Storage-Klasse verwendet, wird der neue Node erst verwendet, nachdem Sie den Node wie unten beschrieben manuell die benutzerdefinierte Storage-Klasse zugewiesen haben.

> Beim Erstellen von Lagergüten nicht mehr als erforderlich Speicherklassen erstellen. Erstellen Sie beispielsweise nicht für jeden Storage-Node eine Storage-Klasse. 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** > **Storage-Klasse** aus.
2. Speicherklasse erstellen:

   a. Klicken Sie für jede Speicherklasse, die Sie definieren möchten, auf **Einfügen** Um eine Zeile hinzuzufügen und eine Bezeichnung für die Speicherklasse einzugeben.

      Die Standard-Speicherstufe kann nicht geändert werden. Es ist für neue, während einer StorageGRID Systemerweiterung hinzugefügte Storage Nodes reserviert.

Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	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

a. Klicken Sie zum Bearbeiten einer vorhandenen Speicherklasse auf **Bearbeiten** Und ändern Sie die Beschriftung nach Bedarf.

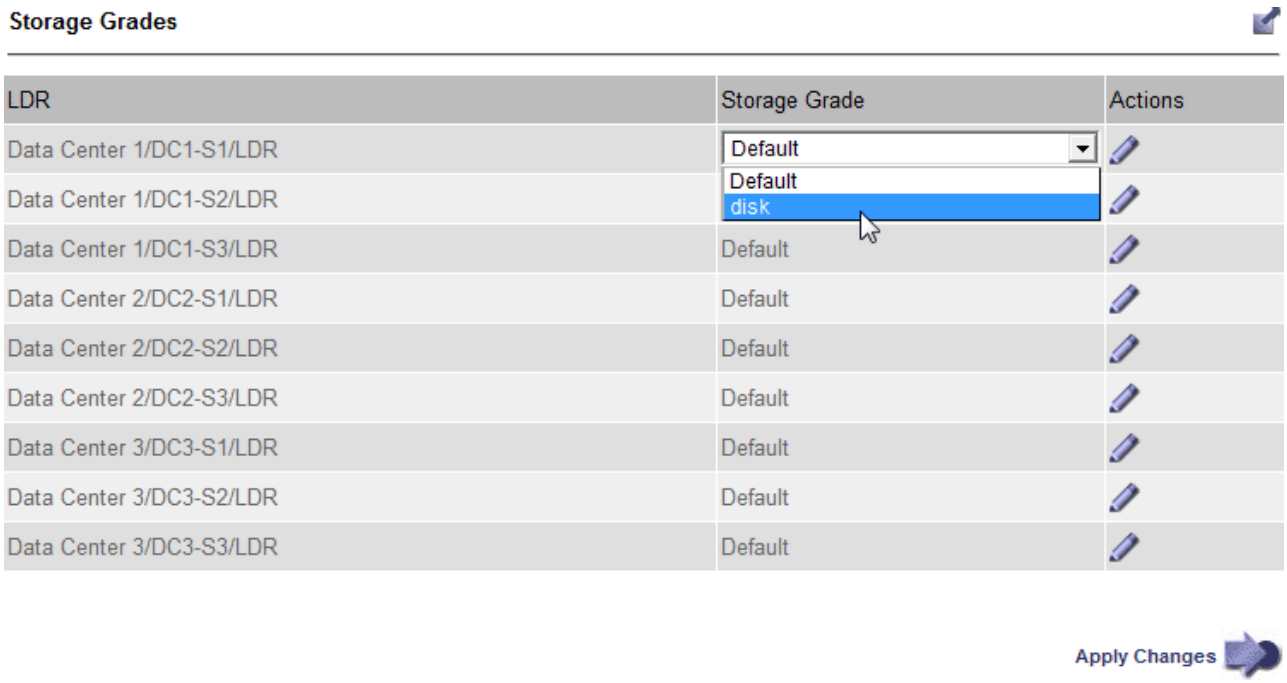
   Speicherklassen können nicht gelöscht werden.

b. Klicken Sie Auf **Änderungen Übernehmen**.

   Diese Speicherklassen sind jetzt für die Zuordnung zu Speicherknoten verfügbar.

3. Weisen Sie einem Storage-Node eine Storage-Klasse zu:

   a. Klicken Sie für den LDR-Service jedes Speicherknotens auf **Bearbeiten** Und wählen Sie eine Speicherklasse aus der Liste aus.



Weisen Sie einem bestimmten Speicherknoten nur einmal eine Speicherklasse zu. Bei einem nach einem Ausfall wiederhergestellten Storage-Node wird die zuvor zugewiesene Storage-Klasse erhalten. Ändern Sie diese Zuweisung nicht, wenn die ILM-Richtlinie aktiviert ist. Wenn die Zuweisung geändert wird, werden die Daten auf Basis der neuen Speicherklasse gespeichert.

a. Klicken Sie Auf **Änderungen Übernehmen**.

Konfigurieren von Speicherpools

Wenn Sie eine ILM-Regel definieren, verwenden Sie Speicherpools, um anzugeben, wo Objekte gespeichert werden. Bevor Sie einen Speicherpool erstellen, müssen Sie die Richtlinien für den Speicherpool überprüfen.

- "Was ist ein Speicherpool"
- "Richtlinien zur Erstellung von Speicherpools"
- "Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung"
- "Verwenden eines Speicherpools als temporärer Speicherort (veraltet)"
- "Erstellen eines Speicherpools"
- "Anzeigen von Details zum Speicherpool"
- "Bearbeiten eines Speicherpools"
- "Entfernen eines Speicherpools"

Was ist ein Speicherpool

Ein Speicherpool ist eine logische Gruppierung von Storage-Nodes oder Archiv-Nodes. Sie konfigurieren Speicherpools, um zu bestimmen, wo das StorageGRID-System Objektdaten und den verwendeten Storage-Typ speichert.

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. 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 Erasure Coding-Profile erstellen, wählen Sie einen Speicherpool aus, der Storage-Nodes enthält.

Richtlinien zur Erstellung von Speicherpools

Befolgen Sie bei der Konfiguration und Verwendung von Speicherpools die folgenden Richtlinien.

Richtlinien für alle Speicherpools

- StorageGRID enthält einen Standard-Speicherpool, alle Storage-Nodes, der den Standardstandort, Alle Standorte und die Standard-Storage-Klasse, alle Storage-Nodes verwendet. Der Speicherpool Alle Storage-Nodes wird automatisch aktualisiert, wenn Sie neue Datacenter-Standorte hinzufügen.

> ⓘ Es wird nicht empfohlen, den Speicherpool für alle Storage-Nodes oder den Standort Alle Standorte zu verwenden, da diese Elemente automatisch aktualisiert werden, um neue Sites, die Sie in eine Erweiterung einfügen, einzubeziehen. Dies ist möglicherweise nicht das gewünschte Verhalten. Bevor Sie den Storage-Pool aller Storage-Nodes oder den Standardstandort verwenden, prüfen Sie sorgfältig die Richtlinien für replizierte und mit Erasure Coding gekennzeichnete Kopien.

- Halten Sie Storage-Pool-Konfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Storage Pools 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.

Richtlinien für Storage-Pools, die für replizierte Kopien verwendet werden

- Erstellen Sie für jeden Standort einen anderen Speicherpool. Geben Sie dann in den Anweisungen zur Platzierung für jede Regel einen oder mehrere standortspezifische Speicherpools an. 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 für den neuen Standort. Aktualisieren Sie dann ILM-Regeln, um zu steuern, welche Objekte auf der neuen Site gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Standard-Speicherpool, alle Speicherknoten oder einen beliebigen Speicherpool, der den Standardstandort, Alle Standorte enthält.

Richtlinien für Storage-Pools, die für Kopien mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verwendet werden

- Sie können Archiv-Knoten nicht zum Löschen codierter Daten verwenden.
- Die Anzahl der im Storage-Pool enthaltenen Storage-Nodes und -Standorte bestimmen, welche Erasure Coding-Schemata zur Verfügung stehen.
- Wenn ein Speicherpool nur zwei Standorte umfasst, können Sie diesen Speicherpool nicht für Erasure Coding verwenden. Für einen Speicherpool mit zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.
- Verwenden Sie im Allgemeinen nicht den Standardspeicherpool, alle Speicherknoten oder einen beliebigen Speicherpool, der den Standardstandort, Alle Standorte in einem beliebigen Erasure-Coding-Profil enthält.

> Wenn in Ihrem Grid nur ein Standort enthalten ist, können Sie den Speicherpool „Alle Speicherknoten“ oder den Standardstandort „Alle Standorte“ in einem Erasure-Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Erasure Coding-Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

- Bei hohen Durchsatzanforderungen wird die Erstellung eines Storage-Pools mit mehreren Standorten nicht empfohlen, wenn die Netzwerklatenz zwischen Standorten größer als 100 ms ist. Mit steigender Latenz sinkt auch die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes erheblich. Die Abnahme des Durchsatzes wirkt sich auf die maximal erreichbaren Raten für Objekteinspeisung und -Abruf aus (wenn strenge oder ausgewogene als Aufnahmeverhalten ausgewählt werden) oder kann zu Backlogs in der ILM-Warteschlange führen (wenn Dual-Commit als Aufnahmeverhalten ausgewählt wird).
- Wenn möglich, sollte ein Speicherpool mehr als die Mindestanzahl an Speicherknoten enthalten, die für das ausgewählte Erasure-Coding-Schema erforderlich ist. Wenn Sie beispielsweise ein 6+3-Schema zur Codierung von Löschverfahren verwenden, müssen Sie mindestens neun Storage-Nodes haben. Es wird jedoch empfohlen, mindestens einen zusätzlichen Storage-Node pro Standort zu haben.
- Verteilen Sie Storage Nodes so gleichmäßig wie möglich auf Standorte. Um beispielsweise ein 6+3 Erasure Coding-Schema zu unterstützen, konfigurieren Sie einen Storage-Pool, der mindestens drei Storage-Nodes an drei Standorten enthält.

Richtlinien für Speicherpools, die für archivierte Kopien verwendet werden

- Es kann kein Speicherpool erstellt werden, der sowohl Speicherknoten als auch Archivknoten enthält. 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 auch Archiv-Nodes enthält. 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. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"Was ist Replizierung"

"Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding"

"Was sind die Erasure Coding-Schemata"

"Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung"

"Verwenden eines Speicherpools als temporärer Speicherort (veraltet)"

"Verwalten von Objekten mit S3 Object Lock"

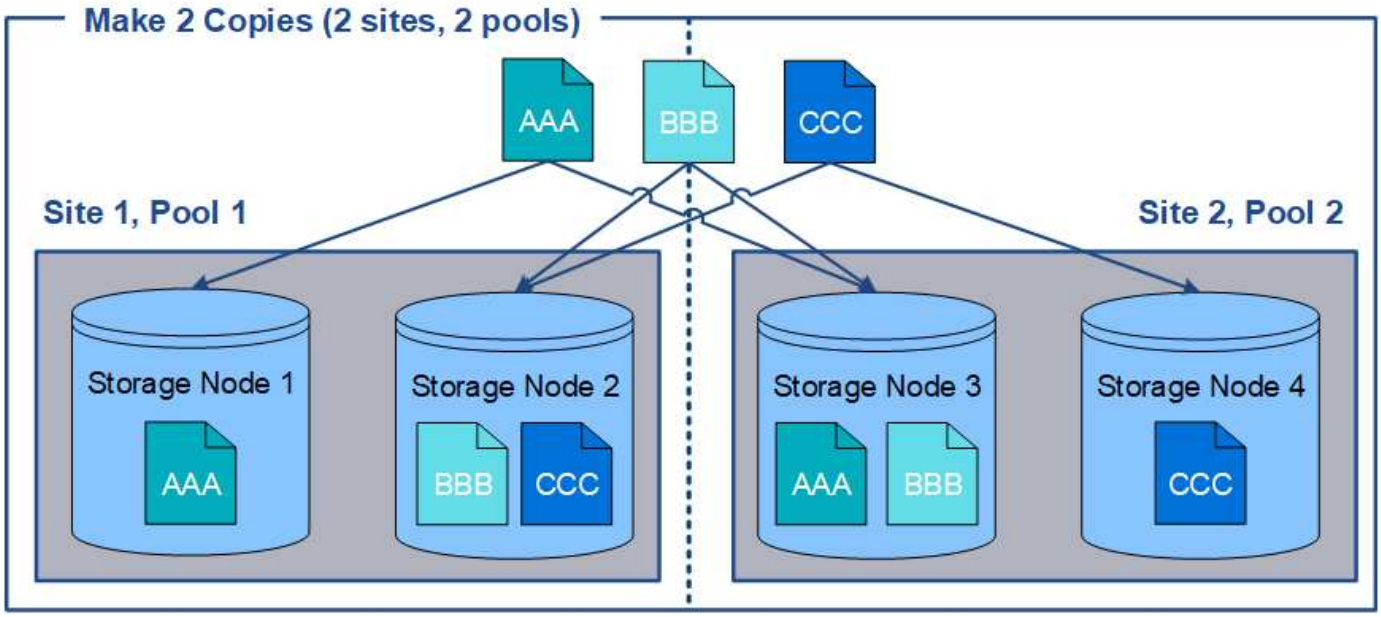
"StorageGRID verwalten"

Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung

Wenn Ihre StorageGRID-Implementierung mehr als einen Standort umfasst, können Sie den Site-Loss-Schutz durch die Erstellung eines Storage-Pools für jeden Standort aktivieren und in den Anweisungen zur Platzierung der Regeln beide Storage Pools angeben. Wenn Sie beispielsweise eine ILM-Regel konfigurieren, um zwei replizierte Kopien zu erstellen und Storage-Pools an zwei Standorten festzulegen, wird an jedem Standort eine Kopie jedes Objekts erstellt. Wenn Sie eine Regel für die Erstellung von zwei Kopien konfigurieren und drei Speicherpools festlegen, werden die Kopien verteilt, um die Festplattennutzung in den Speicherpools auszugleichen, während gleichzeitig sichergestellt wird, dass die beiden Kopien an unterschiedlichen Standorten gespeichert werden.

Das folgende Beispiel zeigt, was passieren kann, wenn eine ILM-Regel replizierte Objektkopien in einen einzelnen Storage-Pool mit Storage Nodes von zwei Standorten platziert. Da das System alle verfügbaren Nodes im Storage-Pool zum Speichern der replizierten Kopien verwendet, kann es alle Kopien von einigen Objekten innerhalb eines der Standorte platzieren. In diesem Beispiel speicherte das System zwei Kopien von Objekt AAA auf Storage Nodes an Standort 1 und zwei Kopien von Objekt CCC auf Storage Nodes an Standort 2. Nur Objekt BBB ist geschützt, wenn eine der Standorte ausfällt oder nicht mehr zugänglich ist.

Im Gegensatz dazu zeigt dieses Beispiel, wie Objekte gespeichert werden, wenn Sie mehrere Speicherpools verwenden. Im Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts erstellt und die Kopien auf zwei Storage-Pools verteilt werden. Jeder Speicherpool enthält alle Storage-Nodes an einem Standort. Da an jedem Standort eine Kopie jedes Objekts gespeichert wird, werden Objektdaten gegen Standortausfall oder Nichtverfügbarkeit geschützt.



Beachten Sie bei der Verwendung mehrerer Speicherpools die folgenden Regeln:

- Wenn Sie n Kopien erstellen, müssen Sie n oder mehr Speicherpools hinzufügen. Wenn eine Regel beispielsweise für die Erstellung von drei Kopien konfiguriert ist, müssen Sie drei oder mehr Speicherpools angeben.
- 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 kleiner als die Anzahl der Storage-Pools ist, verteilt das System die Kopien, um die Festplattennutzung auf den ausgeglichenen Pools zu halten, und um sicherzustellen, dass mindestens zwei Kopien nicht im selben Storage-Pool gespeichert werden.
- 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 die gleichen Speicherknoten enthalten.

Verwenden eines Speicherpools als temporärer Speicherort (veraltet)

Wenn Sie eine ILM-Regel mit einer Objektplatzierung erstellen, die einen einzelnen Storage-Pool umfasst, werden Sie aufgefordert, einen zweiten Storage-Pool anzugeben, der als temporärer Speicherort verwendet werden soll.

Temporäre Speicherorte wurden veraltet und werden in einer zukünftigen Version entfernt. Sie sollten einen Speicherpool nicht als temporären Speicherort für eine neue ILM-Regel auswählen.

> Wenn Sie das strikte Aufnahmeverhalten auswählen (Schritt 3 des Assistenten zur Erstellung von ILM-Regeln), wird der temporäre Speicherort ignoriert.

Verwandte Informationen

"Datensicherungsoptionen für die Aufnahme"

Erstellen eines Speicherpools

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Erstellen von Speicherpools überprüft haben.

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. Wählen Sie das Plus-Symbol ➕ So fügen Sie für jede Site einen Eintrag hinzu:

> ⓘ Schließen Sie den standardmäßigen 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:

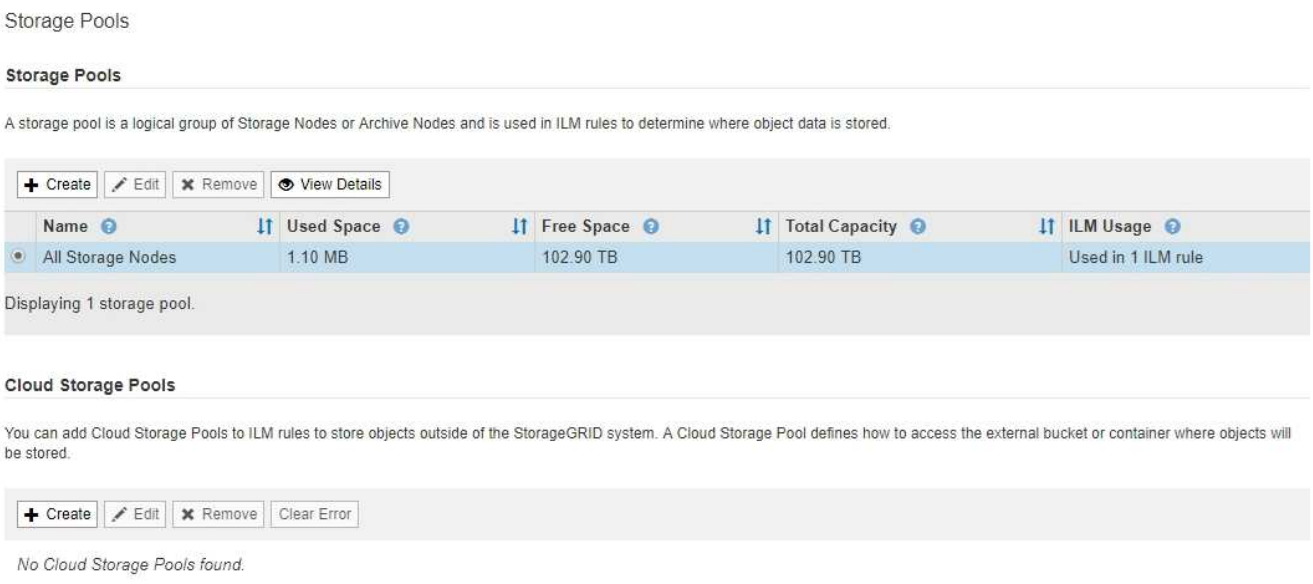
- Wenn Sie über mehrere Speicherklassen verfügen, erstellen Sie keinen Speicherpool, der unterschiedliche Speicherklassen an einem einzelnen Standort enthält.

  "Richtlinien zur Erstellung von Speicherpools"

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt und listet alle definierten Speicherpools auf.

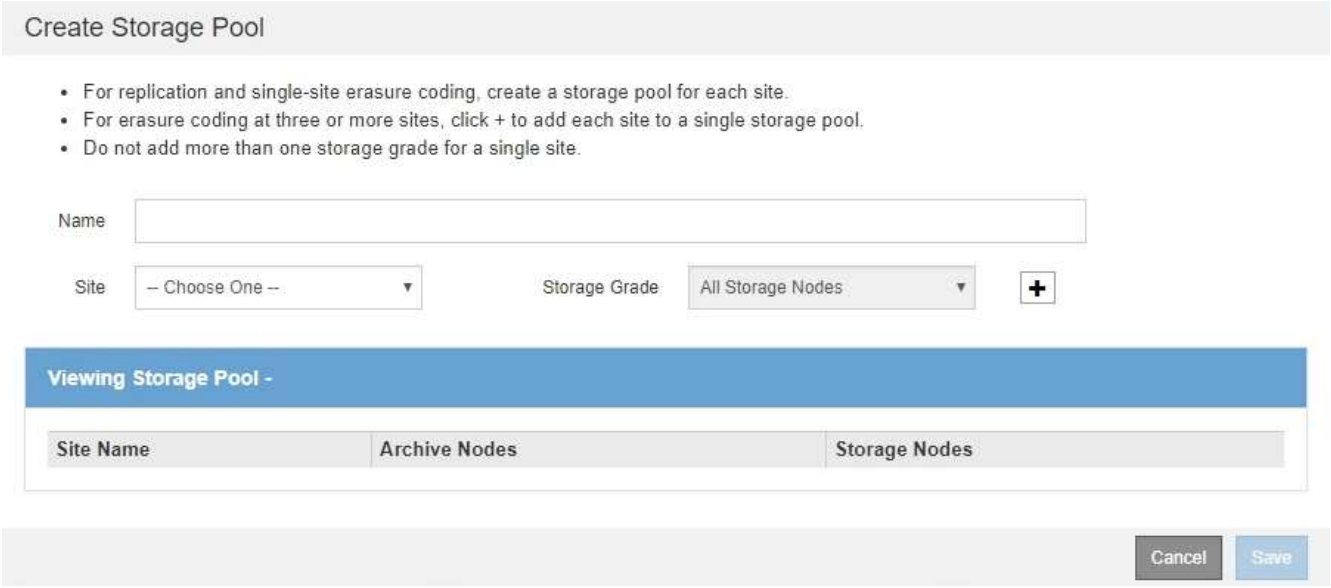


Die Liste umfasst den systemstandardmäßigen Speicherpool, alle Speicherknoten, der den systemstandardmäßigen Standort, Alle Standorte und die Standard-Speicherklasse Alle Speicherknoten verwendet.

> Da der Speicherpool für alle Storage-Nodes beim Hinzufügen neuer Datacenter-Standorte automatisch aktualisiert wird, wird die Verwendung dieses Speicherpools in ILM-Regeln nicht empfohlen.

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.

   Das Dialogfeld Speicherpool erstellen wird angezeigt.



3. Geben Sie einen eindeutigen Namen für den Speicherpool ein.

   Verwenden Sie einen Namen, der bei der Konfiguration von Erasure Coding-Profilen und ILM-Regeln leicht zu identifizieren ist.

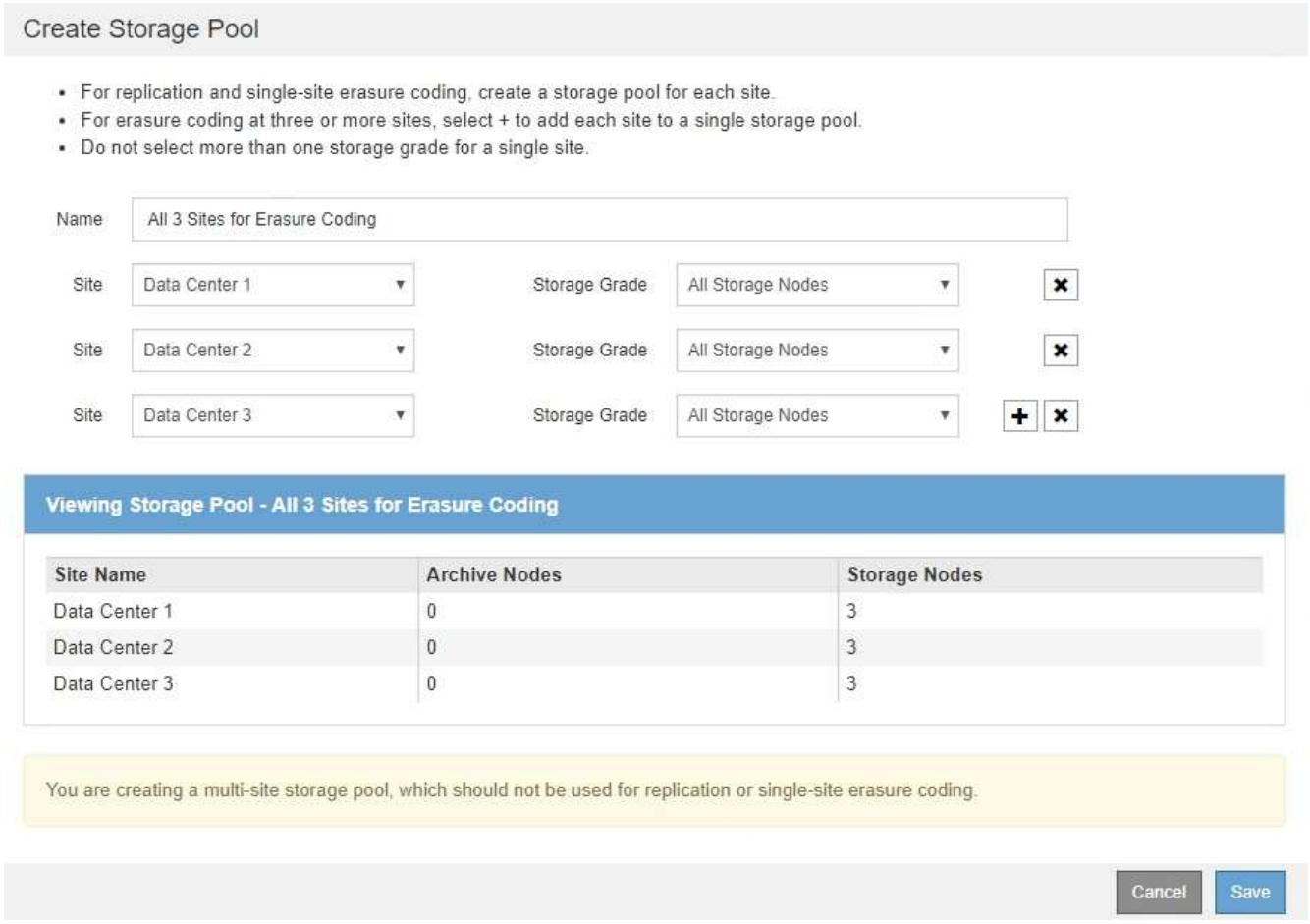
4. Wählen Sie aus der Dropdown-Liste **Standort** einen Standort für diesen Speicherpool aus.

   Wenn Sie einen Standort auswählen, wird die Anzahl der Speicherknoten und Archivknoten in der Tabelle automatisch aktualisiert.

5. Wählen Sie aus der Dropdown-Liste **Storage Grade** den Storage-Typ aus, der verwendet werden soll, wenn eine ILM-Regel diesen Speicherpool verwendet.

   Die standardmäßige Speicherklasse „Alle Speicherknoten“ enthält alle Speicherknoten 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 Erasure Coding-Profil für mehrere Standorte verwenden möchten, wählen Sie ➕ So fügen Sie dem Speicherpool einen Eintrag für jeden Standort hinzu.



Sie können keine doppelten Einträge erstellen oder einen Speicherpool erstellen, der sowohl die Speicherklasse **Archivknoten** als auch jede Speicherklasse enthält, die Speicherknoten enthält.

Sie sind gewarnt, wenn Sie mehr als einen Eintrag für einen Standort, aber mit verschiedenen Speicherklassen hinzufügen.

Um einen Eintrag zu entfernen, wählen Sie ✖.

7. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie **Speichern**.

   Der neue Speicherpool wird der Liste hinzugefügt.

Verwandte Informationen

"Richtlinien zur Erstellung von Speicherpools"

Anzeigen von Details zum Speicherpool

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.

Was Sie benötigen

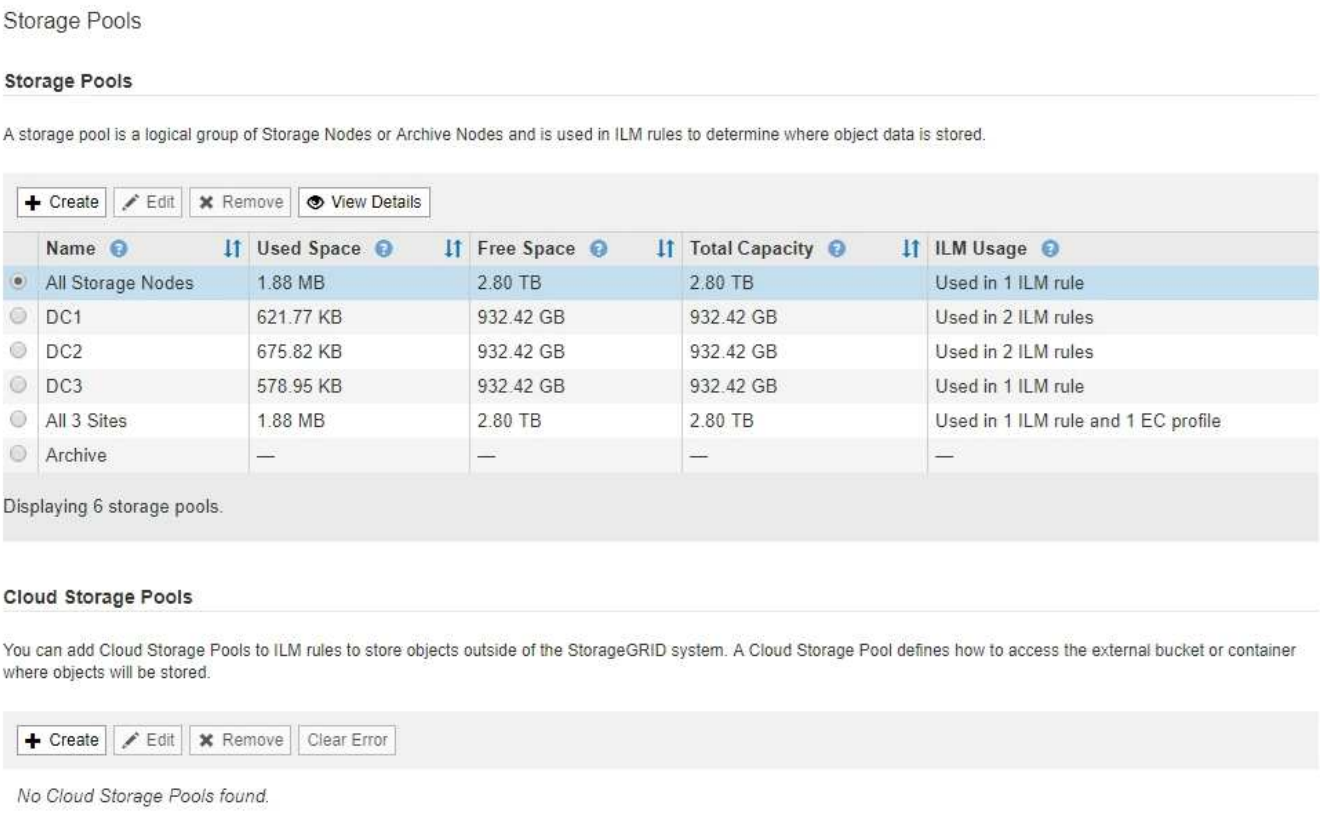
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt. Auf dieser Seite werden alle definierten Speicherpools aufgelistet.



   Die Tabelle enthält die folgenden Informationen zu den einzelnen Storage-Pools, einschließlich Storage-Nodes:

   - **Name**: Der eindeutige Anzeigename des Speicherpools.
   - **Verwendeter Platz**: Die Menge an Speicherplatz, die derzeit zum Speichern von Objekten im Speicherpool verwendet wird.
   - **Freier Raum**: Der Speicherplatz, der zur Speicherung von Objekten im Speicherpool verfügbar bleibt.
   - **Gesamtkapazität**: Die Größe des Speicherpools, die der gesamten nutzbaren Menge an Objektdaten für alle Knoten im Speicherpool entspricht.
   - **ILM-Nutzung**: Wie der Speicherpool derzeit genutzt wird. Ein Storage-Pool kann ungenutzt sein oder auch in einem oder mehreren ILM-Regeln, Erasure Coding-Profilen oder beidem verwendet werden.

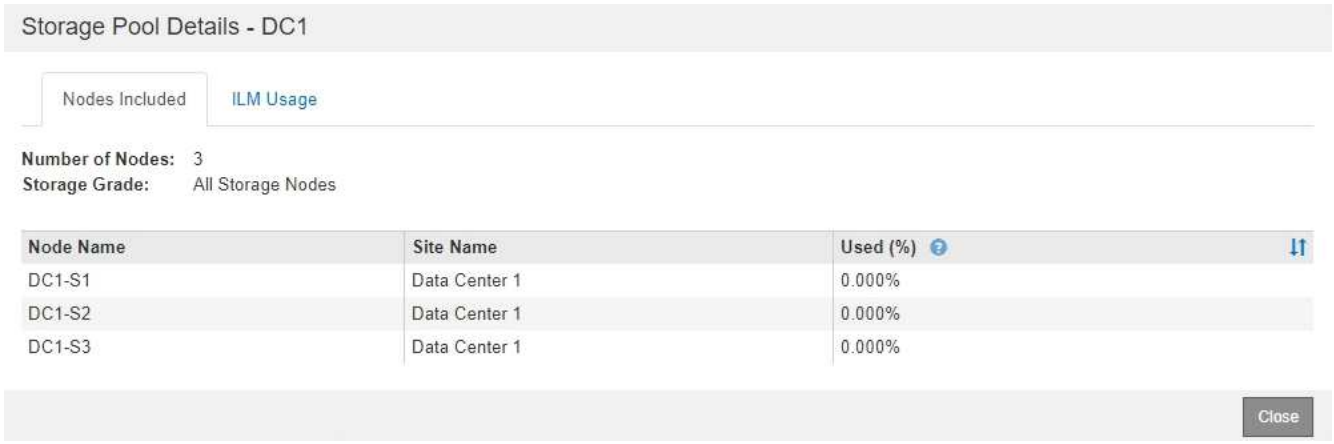
     Ein Speicherpool kann nicht entfernt werden, wenn er verwendet wird.

2. Um Details zu einem bestimmten Speicherpool anzuzeigen, wählen Sie das entsprechende Optionsfeld aus, und wählen Sie **Details anzeigen**.

   Der Storage Pool Details Modal wird angezeigt.

3. Auf der Registerkarte **enthaltene Knoten** erfahren Sie mehr über die Speicherknoten oder Archivknoten,

die im Speicherpool enthalten sind.



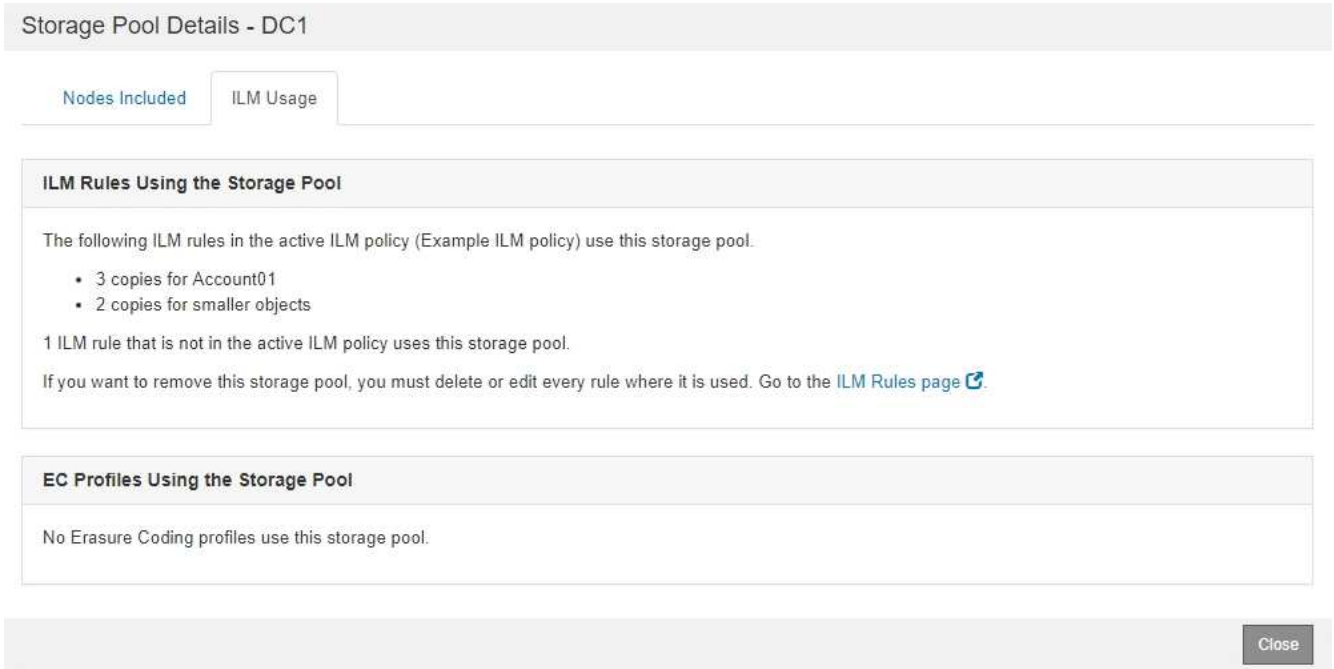
Die Tabelle enthält die folgenden Informationen für jeden Node:

- Node-Name
- Standortname
- Genutzt (%): Für Storage-Nodes, der Prozentsatz des insgesamt nutzbaren Speicherplatzes für Objektdaten, der verwendet wurde. Dieser Wert enthält keine Objektmetadaten.

> Der gleiche verwendete (%) Wert wird auch im Diagramm Speicher verwendet - Objektdaten für jeden Speicherknoten angezeigt (wählen Sie **Knoten** > ***Speicherknoten*** > **Speicher**).

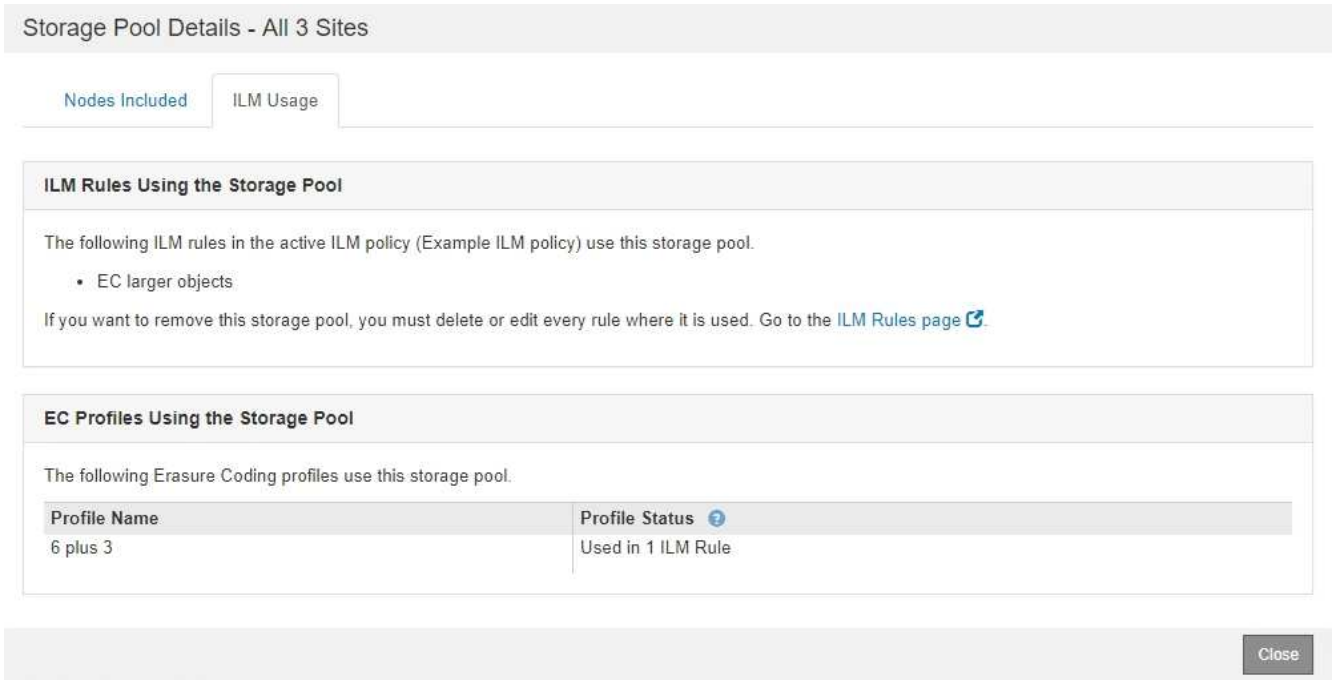
4. Wählen Sie die Registerkarte **ILM-Nutzung** aus, um festzustellen, ob der Speicherpool derzeit in ILM-Regeln oder Erasure Coding-Profilen verwendet wird.

   In diesem Beispiel wird der DC1-Speicherpool in drei ILM-Regeln verwendet: Zwei Regeln, die sich in der aktiven ILM-Richtlinie befinden, und eine Regel, die nicht in der aktiven Richtlinie ist.



Sie können einen Speicherpool nicht entfernen, wenn er in einer ILM-Regel verwendet wird.

In diesem Beispiel wird der Speicherpool „Alle 3 Standorte“ in einem Erasure Coding-Profil verwendet. Dieses Erasure Coding-Profil wird wiederum von einer ILM-Regel in der aktiven ILM-Richtlinie verwendet.



Ein Speicherpool kann nicht entfernt werden, wenn er in einem Erasure Coding-Profil verwendet wird.

5. Klicken Sie optional auf die Seite **ILM-Regeln**, um mehr über die Regeln zu erfahren und diese zu verwalten, die den Speicherpool verwenden.

   Anweisungen zum Arbeiten mit ILM-Regeln finden Sie in der Anleitung.

6. Wenn Sie die Details des Speicherpools anzeigen, wählen Sie **Schließen**.

Verwandte Informationen

"Arbeiten mit ILM-Regeln und ILM-Richtlinien"

Bearbeiten eines Speicherpools

Sie können einen Speicherpool bearbeiten, um seinen Namen zu ändern oder Standorte und Speicherklassen zu aktualisieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Erstellen von Speicherpools überprüft haben.
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, müssen Sie prüfen, wie sich Ihre Änderungen auf die Platzierung der Objektdaten auswirken.

Über diese Aufgabe

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, eine neue Speicherklasse hinzufügen, beachten Sie, dass die Speicherknoten in der neuen Speicherklasse nicht automatisch verwendet werden. Damit StorageGRID die Verwendung einer neuen Storage-Klasse erzwingen kann, müssen Sie eine neue ILM-Richtlinie aktivieren, nachdem Sie den bearbeiteten Speicherpool gespeichert haben.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt.

2. Wählen Sie das Optionsfeld für den Speicherpool aus, den Sie bearbeiten möchten.

   Der Speicherpool Alle Speicherknoten 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 die Standort- oder Speicherklasse nicht ändern, wenn der Speicherpool in einem Erasure-Coding-Profil verwendet wird und die Änderung das Erasure-Coding-Schema ungültig machen würde. Wenn beispielsweise ein Speicherpool, der in einem Erasure-Coding-Profil verwendet wird, derzeit eine Speicherklasse mit nur einem Standort enthält, können Sie eine Speicherklasse 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 Storage-Pool, der in der aktiven ILM-Richtlinie verwendet wird, eine neue Storage-Klasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um die Verwendung der neuen Storage-Klasse durch StorageGRID zu erzwingen. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon.

Entfernen eines Speicherpools

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt.

2. Sehen Sie sich die Spalte ILM-Nutzung in der Tabelle an, um zu bestimmen, ob Sie den Speicherpool entfernen können.

   Ein Speicherpool kann nicht entfernt werden, wenn er in einer ILM-Regel oder in einem Erasure Coding-Profil verwendet wird. Wählen Sie nach Bedarf **Details anzeigen** > **ILM-Nutzung** aus, um festzustellen,

wo ein Speicherpool verwendet wird.

3. Wenn der Speicherpool, den Sie entfernen möchten, nicht verwendet wird, aktivieren Sie das Optionsfeld.
4. Wählen Sie **Entfernen**.
5. Wählen Sie **OK**.

Verwendung Von Cloud Storage Pools

Mithilfe von Cloud-Storage-Pools können StorageGRID Objekte an einen externen Storage-Standort wie S3 Glacier oder Microsoft Azure Blob Storage verschoben werden. Durch das Verschieben von Objekten außerhalb des Grid können Sie von einem kostengünstigen Storage Tier für die Langzeitarchivierung profitieren.

- "Was ist ein Cloud-Storage-Pool"
- "Lebenszyklus eines Cloud-Storage-Pool-Objekts"
- "Wann sollten Sie Cloud Storage Pools nutzen"
- "Überlegungen zu Cloud-Storage-Pools"
- "Vergleich von Cloud Storage Pools und CloudMirror Replizierung"
- "Erstellen eines Cloud-Speicherpools"
- "Bearbeiten eines Cloud-Speicherpools"
- "Entfernen eines Cloud-Speicherpools"
- "Fehlerbehebung Bei 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 möchten Sie selten genutzte Objekte in kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive oder die Archive Access 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).

Die folgende Tabelle vergleicht Storage-Pools mit Cloud Storage Pools 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. Sie müssen Speicherklassen einrichten, bevor Sie den Speicherpool erstellen können.	Verwenden der Option **ILM** > **Storage Pools** 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 einem Amazon S3-Bucket oder Azure Blob-Storage-Container, der nicht zum StorageGRID System integriert ist Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: • Optional kann ein Bucket-Lebenszyklus konfiguriert werden, um Objekte auf kostengünstigen Langzeit-Storage wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu verschieben. Das externe Storage-System muss die Glacier Storage-Klasse und die S3 POST Object Restore API unterstützen. • Sie können Cloud-Storage-Pools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. Wenn der Cloud-Storage-Pool ein Azure Blob-Storage-Container ist, überträgt StorageGRID das Objekt auf die Archiv-Tier. **Hinweis:** Konfigurieren Sie generell nicht das Lifecycle-Management für Azure Blob Storage für den Container, der für einen Cloud-Storage-Pool 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 Datensicherungsmethode 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:** Sie können ein Objekt nicht in mehr als einem Cloud-Speicherpool speichern.
Worin liegen die Vorteile?	Objekte sind jederzeit schnell abrufbar.	Kostengünstiger Storage:

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.

Verwandte Informationen

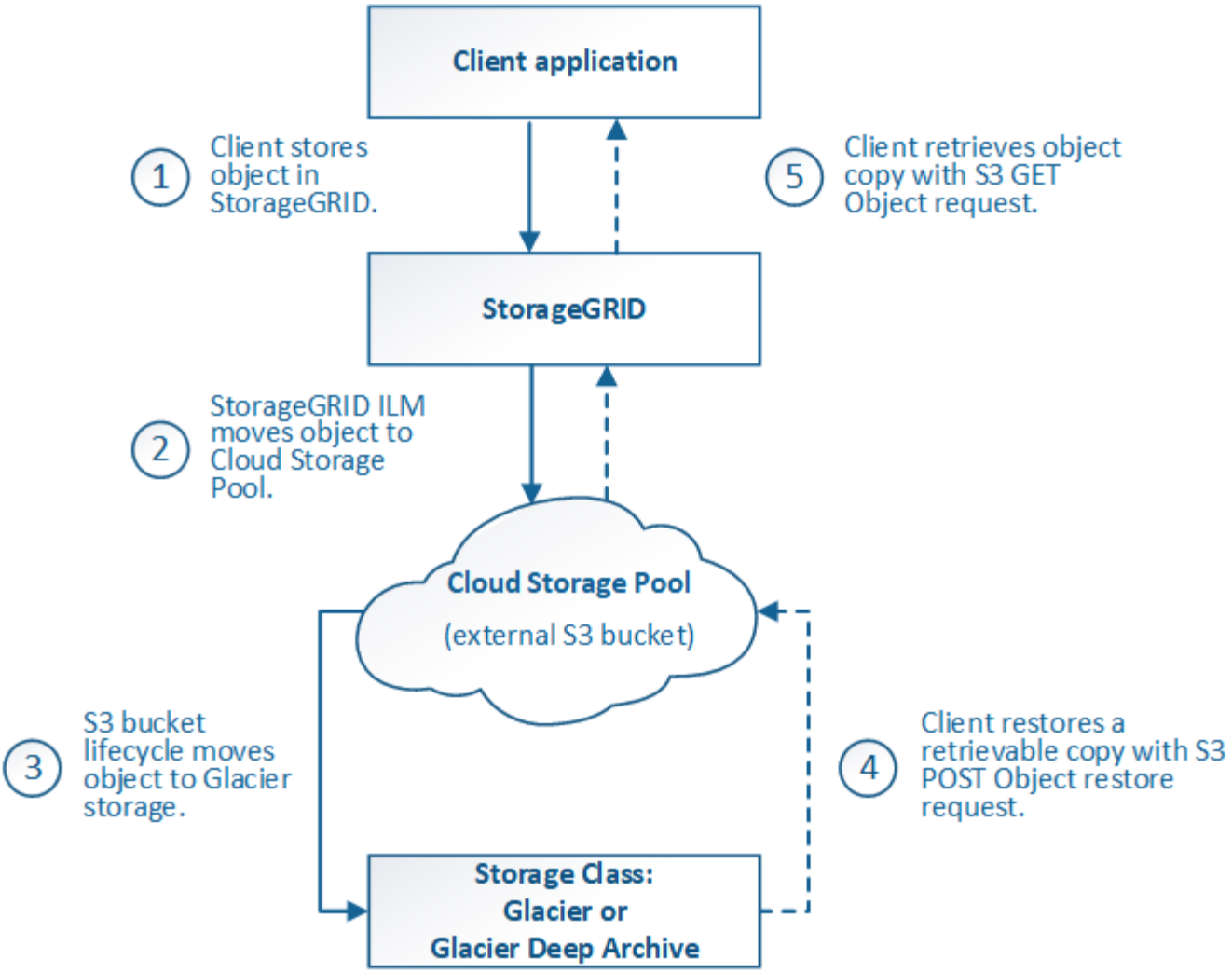
S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts

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.



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**

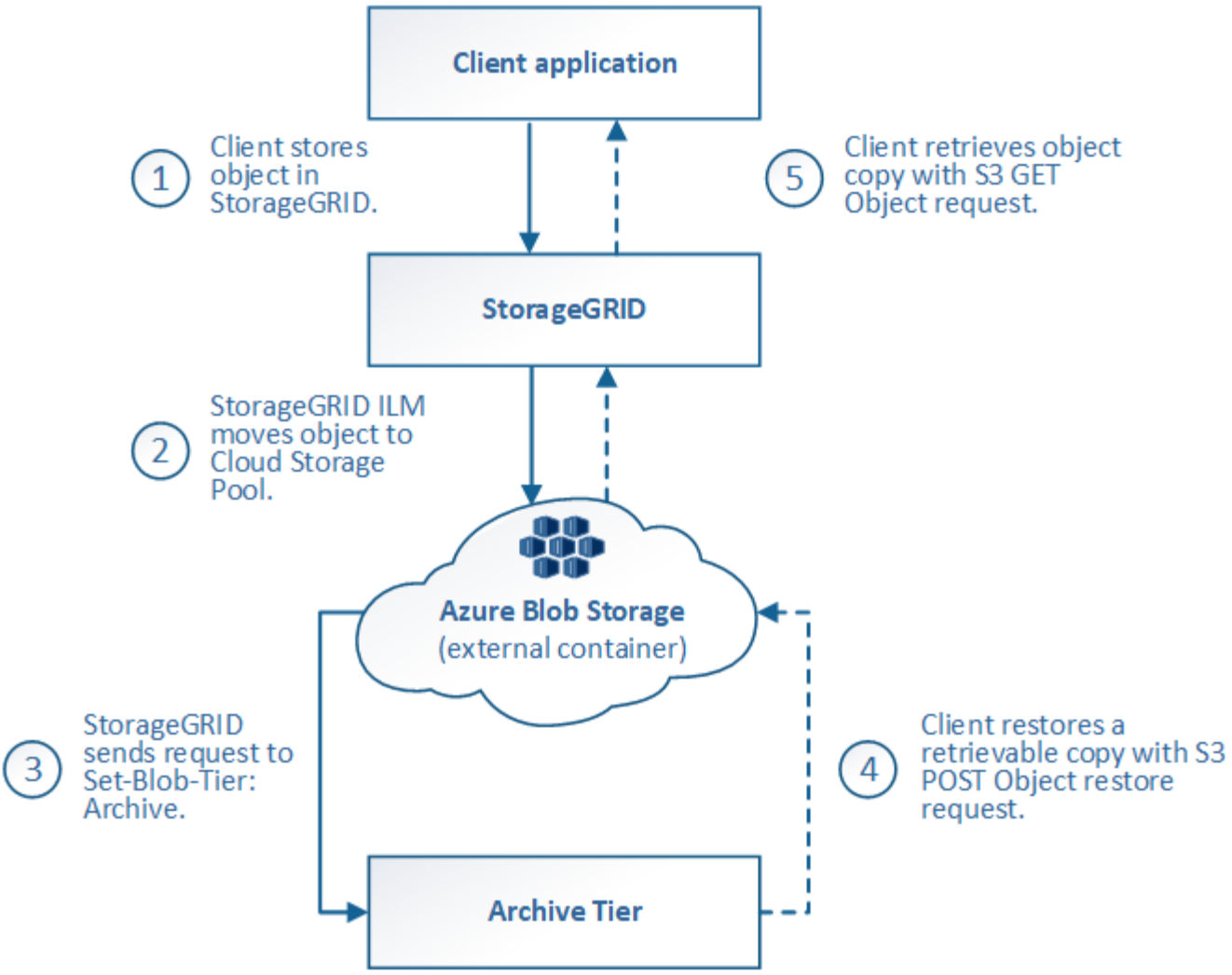
   Sobald ein Objekt wiederhergestellt ist, kann die Client-Applikation eine GET Object-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Verwandte Informationen

"S3 verwenden"

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.

Wann sollten Sie Cloud Storage Pools nutzen

Cloud Storage Pools können in verschiedenen Anwendungsfällen deutliche Vorteile bieten.

Sichern von StorageGRID Daten an einem externen Standort

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.

Tiering von Daten von StorageGRID an externen Speicherort

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 mehrere Cloud-Storage-Pools konfigurieren, wenn Sie Objektdaten auf mehreren Clouds abstufen oder sichern möchten. Mit den Filtern Ihrer ILM-Regeln können Sie festlegen, welche Objekte in den einzelnen Cloud Storage-Pools gespeichert werden. Beispielsweise möchten Sie Objekte von einigen Mandanten oder Buckets in Amazon S3 Glacier und Objekten von anderen Mandanten oder Buckets im Azure Blob Storage speichern. Alternativ können Sie Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben. Bei dem Einsatz mehrerer Cloud-Storage-Pools ist zu beachten, dass ein Objekt immer nur in einem Cloud-Storage-Pool 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.

Zum Erstellen eines Cloud-Storage-Pools erforderliche Informationen

Bevor Sie einen Cloud Storage Pool erstellen können, müssen Sie den externen S3-Bucket oder den externen

Azure Blob-Storage-Container erstellen, den Sie für den Cloud Storage Pool verwenden werden. Wenn Sie dann den Cloud-Speicherpool in StorageGRID erstellen, müssen Sie die folgenden Informationen angeben:

- Der Provider-Typ: Amazon S3 oder Azure Blob Storage
- Wenn Sie Amazon S3 auswählen, ob der Cloud-Storage-Pool für die Verwendung mit der AWS Secret Region (**CAP (C2S Access Portal)**) verwendet werden soll.
- Der genaue Name des Buckets oder Containers.
- Der Service-Endpunkt für den Zugriff auf den Bucket oder Container
- Die für den Zugriff auf den Bucket oder Container erforderliche Authentifizierung:
  - **S3**: Optional eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel.
  - **C2S**: Die vollständige URL zum Abrufen temporärer Anmeldeinformationen vom CAP-Server; ein Server-CA-Zertifikat, ein Clientzertifikat, ein privater Schlüssel für das Clientzertifikat und, wenn der private Schlüssel verschlüsselt ist, die Passphrase zum Entschlüsseln.
  - **Azure Blob Storage**: Ein Kontoname und Kontokschlüssel. Diese Anmeldedaten müssen über vollständige Berechtigungen für den Container verfügen.
- Optional kann ein individuelles CA-Zertifikat zum Überprüfen der TLS-Verbindungen mit dem Bucket oder Container genutzt werden.

Überlegungen zu den Ports, die für Cloud-Storage-Pools verwendet werden

Um sicherzustellen, dass die ILM-Regeln Objekte in den und aus dem angegebenen Cloud Storage-Pool verschieben können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die Storage-Nodes Ihres Systems enthalten. Sie müssen sicherstellen, dass die folgenden Ports mit dem Cloud-Speicherpool kommunizieren können.

Standardmäßig verwenden Cloud-Speicherpools die folgenden Ports:

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

Sie können einen anderen Port angeben, wenn Sie einen Cloud-Speicherpool erstellen oder bearbeiten.

Wenn Sie einen nicht transparenten Proxyserver verwenden, müssen Sie auch einen Speicher-Proxy konfigurieren, damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einen 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 müssen Sie einfach Ihre ILM-Regeln und -Richtlinien neu konfigurieren. 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 das 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 kein Lifecycle-Management für Azure Blob Storage für den Container, der mit einem Cloud-Storage-Pool verwendet wird. Lifecycle-Operationen beeinträchtigen möglicherweise Cloud-Storage-Pool-Vorgänge.

Verwandte Informationen

"Erstellen eines Cloud-Speicherpools"

"S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"

"C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool"

"Azure: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"

"StorageGRID verwalten"

Vergleich von Cloud Storage Pools und CloudMirror Replizierung

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?	Ein Cloud-Storage-Pool fungiert als Archivziel. Die Objektkopie im Cloud-Storage-Pool kann die einzige Kopie des Objekts sein oder es kann eine zusätzliche Kopie sein. Das bedeutet, dass Sie nicht mehr zwei Kopien lokal aufbewahren müssen, sondern nur eine Kopie innerhalb von StorageGRID aufbewahren und eine Kopie an den Cloud-Storage-Pool senden können.	Der CloudMirror Replikationsservice ermöglicht einem Mandanten, Objekte automatisch von einem Bucket in StorageGRID (Quelle) auf einen externen S3 Bucket (Ziel) zu replizieren. Bei der CloudMirror-Replizierung wird eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur erstellt.
Wie ist es eingerichtet?	Cloud-Storage-Pools werden mit Grid Manager oder Grid-Management-API auf dieselbe Weise wie Storage-Pools definiert. Sie können einen Cloud-Storage-Pool als Speicherort in einer ILM-Regel auswählen. 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 konfiguriert die CloudMirror-Replizierung mithilfe des Tenant Manager oder der S3-API durch Definition eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.). Nachdem der CloudMirror Endpunkt eingerichtet wurde, können alle Buckets dieses Mandantenkontos so konfiguriert werden, dass sie auf den CloudMirror Endpunkt verweisen.
Wer ist für die Einrichtung zuständig?	In der Regel ist ein Grid-Administrator erforderlich	In der Regel ein Mandantenbenutzer
Was ist das Ziel?	• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Azure Blob Archivebene	• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3)
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.	Das Einspeisen eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror-Endpunkt konfiguriert wurde.Objekte, die sich vor der Konfiguration mit dem CloudMirror-Endpunkt im Quell-Bucket befanden, werden nicht repliziert, es sei denn, sie werden modifiziert.

	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 im Cloud-Speicherpool gelöscht.	Die Löschaktion wird nicht repliziert. Ein gelöschtes Objekt ist nicht mehr im StorageGRID-Bucket vorhanden, ist jedoch weiterhin im Ziel-Bucket vorhanden. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.
Wie greifen Sie nach einem Ausfall auf Objekte zu (StorageGRID System nicht betriebsbereit)?	Fehlerhafte StorageGRID-Knoten müssen wiederhergestellt werden. Während dieses Prozesses können Kopien replizierter Objekte mithilfe der Kopien im Cloud Storage Pool wiederhergestellt werden.	Die Objektkopien im CloudMirror Zielsystem sind unabhängig von StorageGRID, sodass sie direkt vor dem Recovery der StorageGRID-Nodes zugänglich sind.

Verwandte Informationen

"StorageGRID verwalten"

Erstellen eines Cloud-Speicherpools

Wenn Sie einen Cloud-Storage-Pool erstellen, geben Sie den Namen und den Standort des externen Buckets oder Containers an, den StorageGRID zum Speichern von Objekten, dem Cloud-Provider-Typ (Amazon S3 oder Azure Blob Storage) und den Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Konfigurieren von Cloud-Speicherpools überprüft haben.
- Der externe Bucket oder Container, auf den der Cloud-Storage-Pool verweist, muss vorhanden sein.
- Für den Zugriff auf den Bucket oder Container müssen alle Authentifizierungsinformationen vorhanden sein.

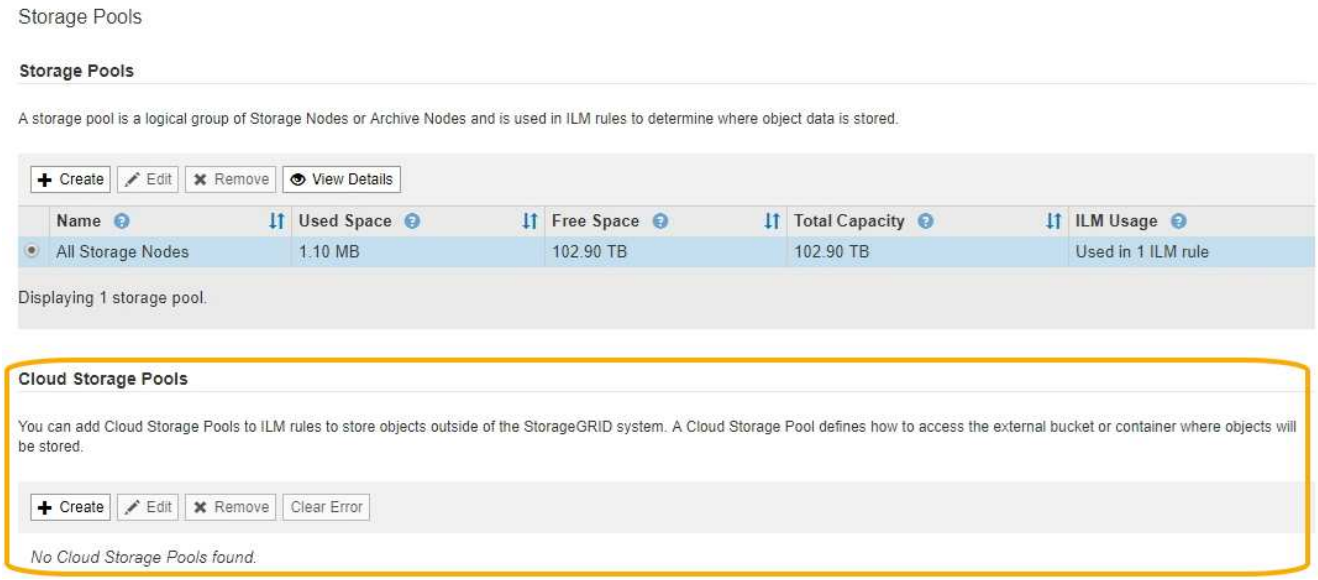
Über diese Aufgabe

Ein Cloud-Storage-Pool gibt einen einzelnen externen S3-Bucket oder Azure Blob-Storage-Container an. 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.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt. Diese Seite enthält zwei Abschnitte: Speicherpools und Cloud-Speicherpools.



2. Klicken Sie im Abschnitt Cloud-Speicherpools auf der Seite auf **Erstellen**.

   Das Dialogfeld Cloud-Speicherpool erstellen wird angezeigt.

3. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Anzeigename	Ein Name, der kurz den Cloud Storage Pool und dessen Zweck beschreibt. Verwenden Sie einen Namen, der leicht zu erkennen ist, wann Sie ILM-Regeln konfigurieren.
Art Des Anbieters	Welcher Cloud-Provider nutzen Sie für diesen Cloud-Storage-Pool? • Amazon S3 (wählen Sie diese Option für einen S3- oder C2S S3-Cloud-Storage-Pool) • Azure Blob Storage **Hinweis:** Wenn Sie einen Provider-Typ auswählen, werden unten auf der Seite die Abschnitte „Service Endpoint“, „Authentifizierung“ und „Server-Überprüfung“ angezeigt.
Bucket oder Container	Der Name des externen S3-Buckets oder Azure-Containers, der für den Cloud-Storage-Pool erstellt wurde. Der hier angegebene Name muss exakt mit dem Bucket oder Container-Namen übereinstimmen, oder die Erstellung von Cloud-Storage-Pool schlägt fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

4. Schließen Sie die Abschnitte „Service Endpoint“, „Authentifizierung“ und „Server-Verifizierung“ der Seite basierend auf dem ausgewählten Provider-Typ ab.
   - "S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"
   - "C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool"
   - "Azure: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"

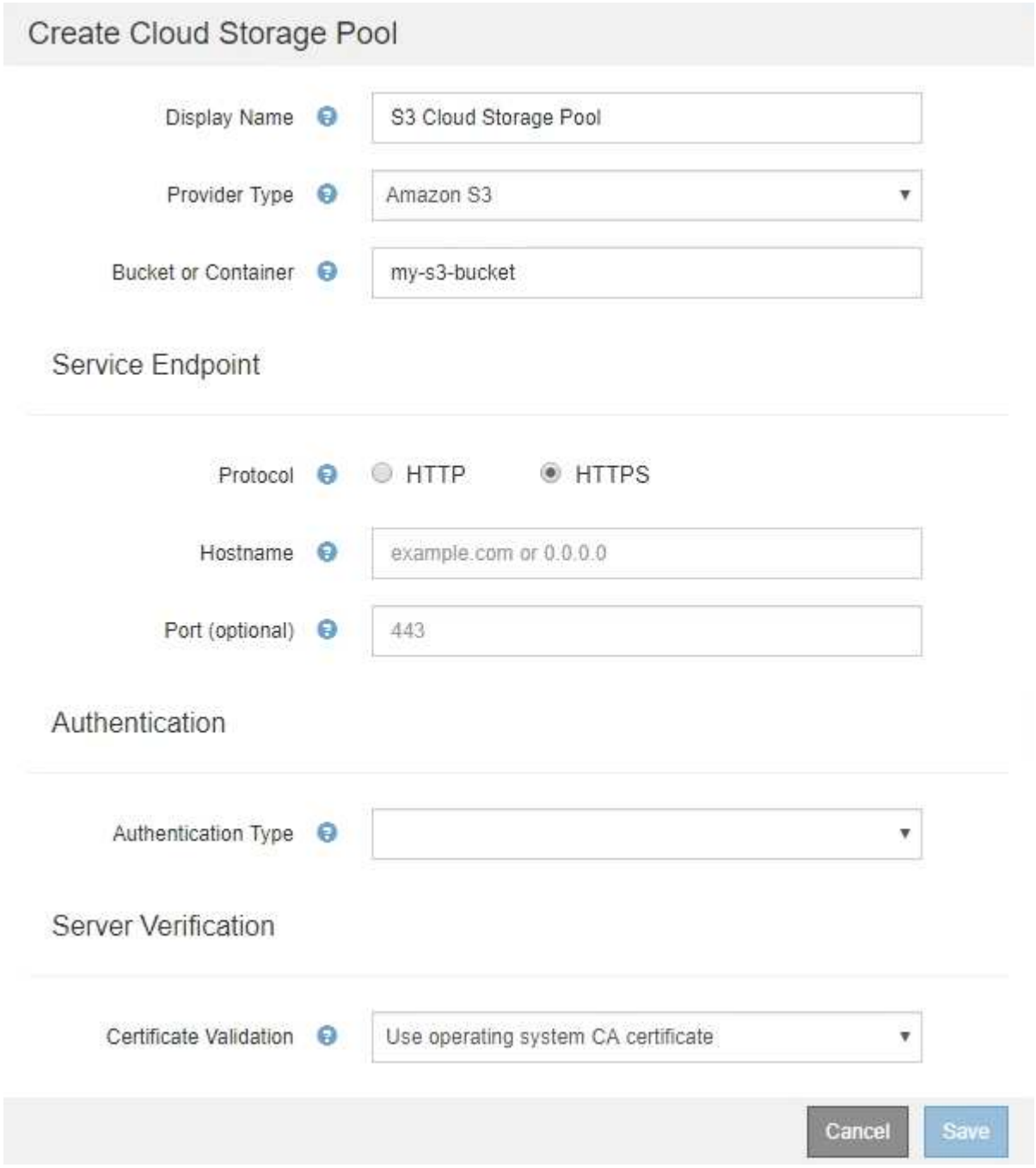
S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool

Wenn Sie einen Cloud Storage Pool für S3 erstellen, müssen Sie den Authentifizierungstyp für den Cloud Storage Pool-Endpunkt auswählen. Sie können Anonymous angeben oder eine Zugriffsschlüssel-ID und einen geheimen

Zugriffsschlüssel eingeben.

Was Sie benötigen

- Sie müssen die Basisinformationen für den Cloud-Speicherpool eingegeben und **Amazon S3** als Provider-Typ angegeben haben.



- Wenn Sie die Authentifizierung für Zugriffsschlüssel verwenden, müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den externen S3-Bucket kennen.

Schritte

1. Geben Sie im Abschnitt * Service Endpoint* folgende Informationen an:

   a. Wählen Sie das Protokoll aus, das bei der Verbindung mit dem Cloud-Storage-Pool verwendet werden soll.

Das Standardprotokoll ist HTTPS.

b. Geben Sie den Serverhostnamen oder die IP-Adresse des Cloud-Speicherpools ein.

Beispiel:

`s3-aws-region.amazonaws.com`

> Geben Sie den Bucket-Namen nicht in dieses Feld ein. Sie fügen den Bucket-Namen in das Feld **Bucket oder Container** ein.

a. Geben Sie optional den Port an, der bei der Verbindung mit dem Cloud Storage Pool verwendet werden soll.

Lassen Sie dieses Feld leer, um den Standardport Port 443 für HTTPS oder Port 80 für HTTP zu verwenden.

2. Wählen Sie im Abschnitt **Authentifizierung** den Authentifizierungstyp aus, der für den Cloud-Storage-Pool-Endpunkt erforderlich ist.

Option	Beschreibung
Zugriffsschlüssel	Für den Zugriff auf den Cloud Storage Pool-Bucket sind eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel erforderlich.
Anonym	Jeder hat Zugriff auf den Cloud-Storage-Pool-Bucket. Eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel sind nicht erforderlich.
KAPPE (C2S-Zugangsportal)	Wird nur für C2S S3 verwendet. Gehen Sie zu "C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool".

3. Wenn Sie den Zugriffsschlüssel ausgewählt haben, geben Sie die folgenden Informationen ein:

Option	Beschreibung
Zugriffsschlüssel-ID	Zugriffsschlüssel-ID für das Konto, das den externen Bucket besitzt
Geheimer Zugriffsschlüssel	Der zugehörige Schlüssel für den geheimen Zugriff.

4. Wählen Sie im Abschnitt Server Verification die Methode aus, mit der das Zertifikat für TLS-Verbindungen zum Cloud Storage Pool validiert werden soll:

Option	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie die auf dem Betriebssystem installierten Standard-CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Klicken Sie auf **Neu auswählen**, und laden Sie das PEM-codierte CA-Zertifikat hoch.

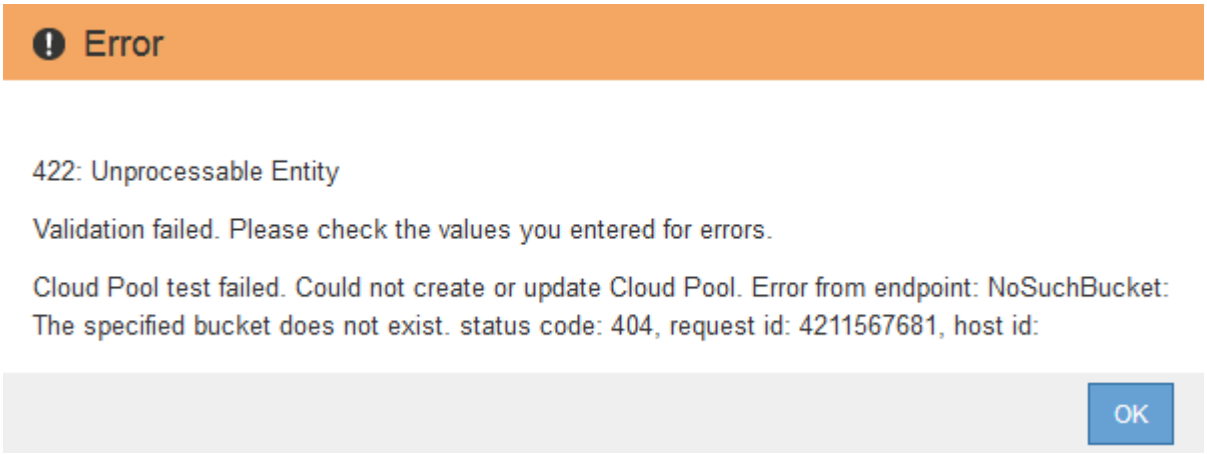
Option	Beschreibung
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

5. Klicken Sie Auf **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Bucket und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Bucket, um den Bucket 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. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Bucket nicht bereits vorhanden ist.



Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

"Fehlerbehebung Bei Cloud Storage Pools"

C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool

Wenn Sie den S3-Service (Commercial Cloud Services, C2S) als Cloud-Storage-Pool verwenden möchten, müssen Sie C2S Access Portal (CAP) als Authentifizierungstyp konfigurieren, damit StorageGRID temporäre Anmeldedaten für den Zugriff auf den S3-Bucket in Ihrem C2S-Konto anfordern kann.

Was Sie benötigen

- Sie müssen die Basisinformationen für einen Amazon S3 Cloud-Storage-Pool, einschließlich des Service-Endpunkts, eingegeben haben.
- Sie müssen die vollständige URL kennen, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
- Sie müssen über ein Server-CA-Zertifikat verfügen, das von einer entsprechenden Behörde ausgestellt

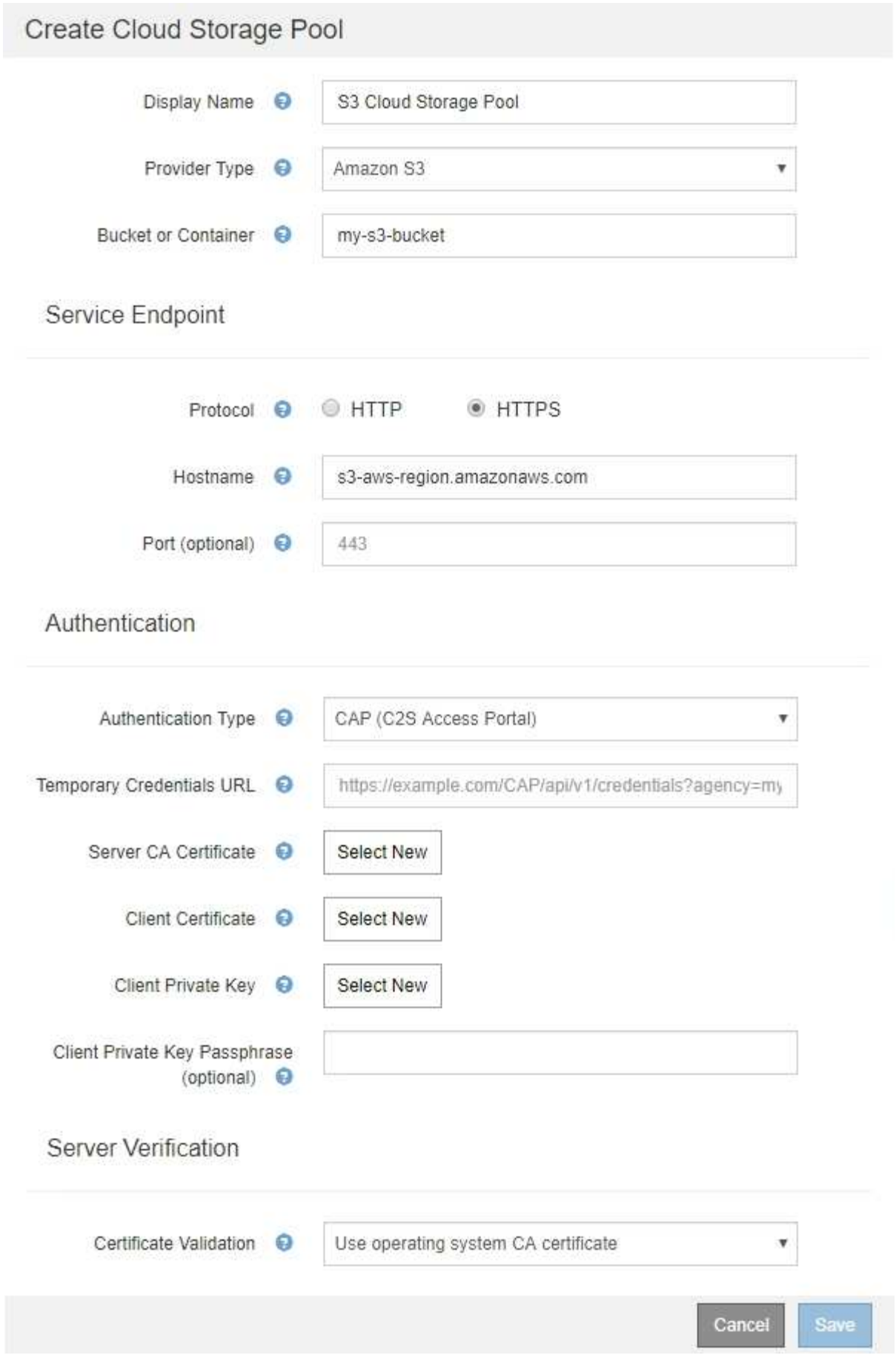
wurde. StorageGRID verwendet dieses Zertifikat, um die Identität des CAP-Servers zu überprüfen. Das Server-CA-Zertifikat muss die PEM-Kodierung verwenden.

- Sie müssen über ein Clientzertifikat verfügen, das von einer entsprechenden Behörde ausgestellt wurde. StorageGRID verwendet dieses Zertifikat zur Identität des CAP-Servers. Das Clientzertifikat muss PEM-Kodierung verwenden und Zugriff auf Ihr C2S-Konto haben.
- Sie benötigen einen PEM-kodierten privaten Schlüssel für das Clientzertifikat.
- Wenn der private Schlüssel für das Clientzertifikat verschlüsselt ist, müssen Sie die Passphrase zum Entschlüsseln besitzen.

Schritte

1. Wählen Sie im Abschnitt **Authentifizierung** im Dropdown-Menü **Authentifizierungstyp** die Option **CAP (C2S Access Portal)** aus.

   Die C2S-Authentifizierungsfelder werden angezeigt.


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. Geben Sie die folgenden Informationen an:
   a. Geben Sie unter **URL für temporäre Anmeldeinformationen** die vollständige URL ein, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
   b. Klicken Sie für **Server-CA-Zertifikat** auf **Neu auswählen** und laden Sie das PEM-codierte CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwendet.
   c. Klicken Sie für **Clientzertifikat** auf **Neu auswählen** und laden Sie das PEM-kodierte Zertifikat, das StorageGRID zur Identifizierung auf den CAP-Server verwendet.
   d. Klicken Sie für **Client Private Key** auf **Select New** und laden Sie den PEM-kodierten privaten Schlüssel für das Clientzertifikat hoch.

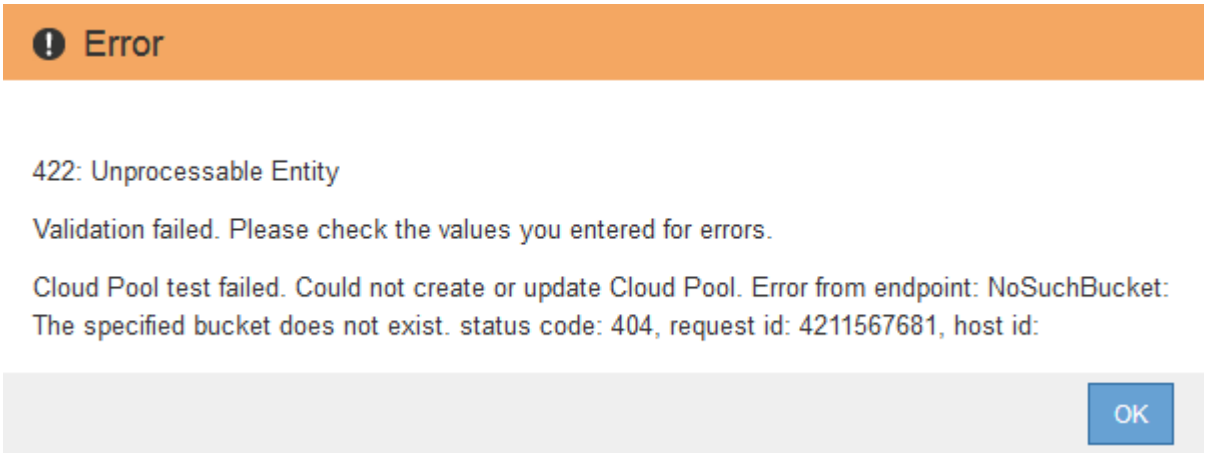
      Wenn der private Schlüssel verschlüsselt ist, muss das traditionelle Format verwendet werden. (Das verschlüsselte PKCS #8-Format wird nicht unterstützt.)

   e. Wenn der private Clientschlüssel verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Clientschlüssels ein. Andernfalls lassen Sie das Feld **Client Private Key Passphrase** leer.
3. Geben Sie im Abschnitt Server-Überprüfung folgende Informationen an:
   a. Wählen Sie für **Zertifikatvalidierung** * Benutzerdefiniertes CA-Zertifikat verwenden* aus.
   b. Klicken Sie auf **Neu auswählen**, und laden Sie das PEM-codierte CA-Zertifikat hoch.
4. Klicken Sie Auf **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Bucket und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Bucket, um den Bucket 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. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Bucket nicht bereits vorhanden ist.



Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

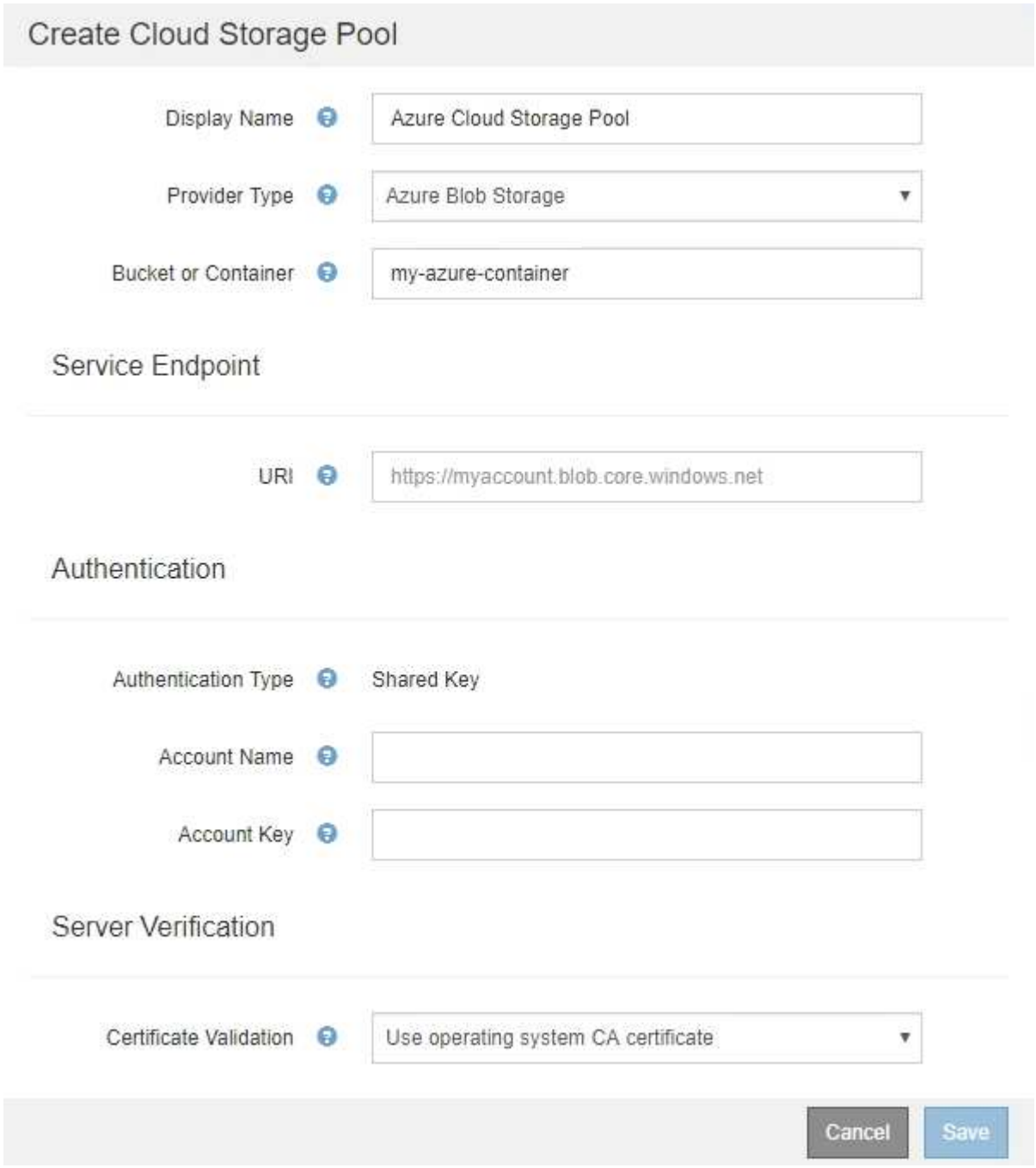
"Fehlerbehebung Bei Cloud Storage Pools"

Azure: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool

Wenn Sie einen Cloud Storage Pool für Azure Blob Storage erstellen, müssen Sie einen Kontonamen und Kontoschlüssel für den externen Container angeben, den StorageGRID zum Speichern von Objekten verwendet.

Was Sie benötigen

- Sie müssen die Basisinformationen für den Cloud Storage Pool eingegeben und **Azure Blob Storage** als Provider-Typ angegeben haben. **Gemeinsamer Schlüssel** wird im Feld **Authentifizierungstyp** angezeigt.



- Sie müssen den URI (Unified Resource Identifier) kennen, der für den Zugriff auf den Blob-Storage-

Container verwendet wird, der für den Cloud Storage-Pool verwendet wird.

- Sie müssen den Namen des Speicherkontos und den geheimen Schlüssel kennen. Im Azure-Portal finden Sie diese Werte.

Schritte

1. Geben Sie im Abschnitt **Service Endpoint** den Uniform Resource Identifier (URI) ein, der für den Zugriff auf den Blob-Storage-Container verwendet wird, der für den Cloud-Storage-Pool verwendet wird.

   Geben Sie den URI in einem der folgenden Formate an:

   - `https://host:port`
   - `http://host:port`

   Wenn Sie keinen Port angeben, wird standardmäßig der Port 443 für HTTPS-URIs verwendet, und Port 80 wird für HTTP-URIs verwendet. + * Beispiel-URI für Azure Blob Storage-Container*: `https://myaccount.blob.core.windows.net`

2. Geben Sie im Abschnitt **Authentifizierung** folgende Informationen an:

   a. Geben Sie für **Kontoname** den Namen des Blob-Speicherkontos ein, der den externen Service-Container besitzt.

   b. Geben Sie für **Kontenschlüssel** den geheimen Schlüssel für das Blob-Speicherkonto ein.

   Für Azure-Endpunkte ist die Authentifizierung mit gemeinsamem Schlüssel erforderlich.

3. Wählen Sie im Abschnitt **Server Verification** die Methode aus, mit der das Zertifikat für TLS-Verbindungen zum Cloud-Speicherpool validiert werden soll:

Option	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie die auf dem Betriebssystem installierten Standard-CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Klicken Sie auf **Neu auswählen**, und laden Sie das PEM-kodierte Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

4. Klicken Sie Auf **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Container und die URI vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den 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. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Container nicht bereits vorhanden ist.

Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

"Fehlerbehebung Bei Cloud Storage Pools"

Bearbeiten eines Cloud-Speicherpools

Sie können einen Cloud Storage Pool bearbeiten, um seinen Namen, seinen Service-Endpunkt oder andere Details zu ändern. Es ist jedoch nicht möglich, den S3-Bucket oder den Azure-Container für einen Cloud-Storage-Pool zu ändern.

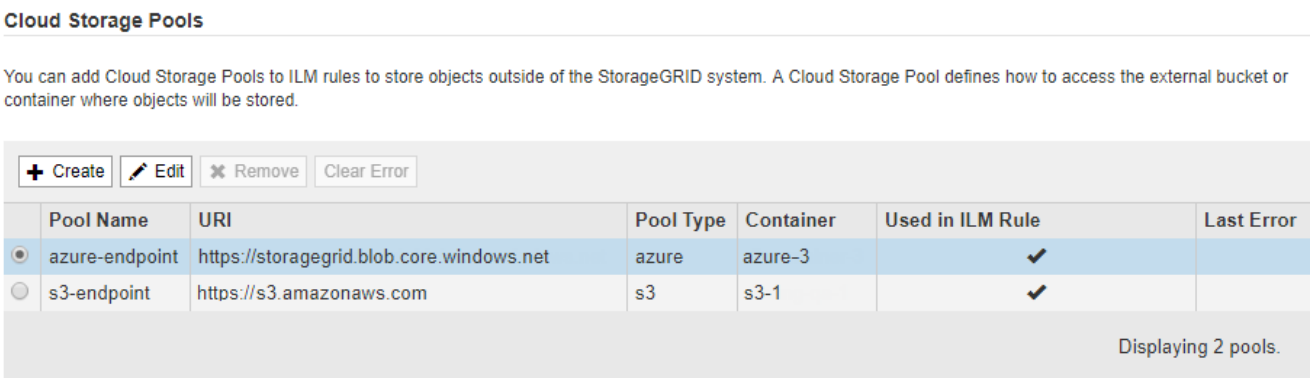
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Konfigurieren von Cloud-Speicherpools überprüft haben.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt. In der Tabelle Cloud-Storage-Pools werden die vorhandenen Cloud-Storage-Pools aufgeführt.



2. Wählen Sie das Optionsfeld für den Cloud-Storage-Pool, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
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 Clientzertifikat hochgeladen haben, können Sie **Aktuell anzeigen** auswählen, um das aktuell verwendete Zertifikat zu überprüfen.

5. Klicken Sie Auf **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.

Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

"Überlegungen zu Cloud-Storage-Pools"

"Fehlerbehebung Bei Cloud Storage Pools"

Entfernen eines Cloud-Speicherpools

Sie können einen Cloud-Storage-Pool entfernen, der nicht in einer ILM-Regel verwendet wird und der keine Objektdaten enthält.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- 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 nicht, die den Namen trägt `x-ntap-sgws-cloud-pool-uuid`.

- Sie haben bereits alle ILM-Regeln entfernt, die den Pool möglicherweise verwendet haben.

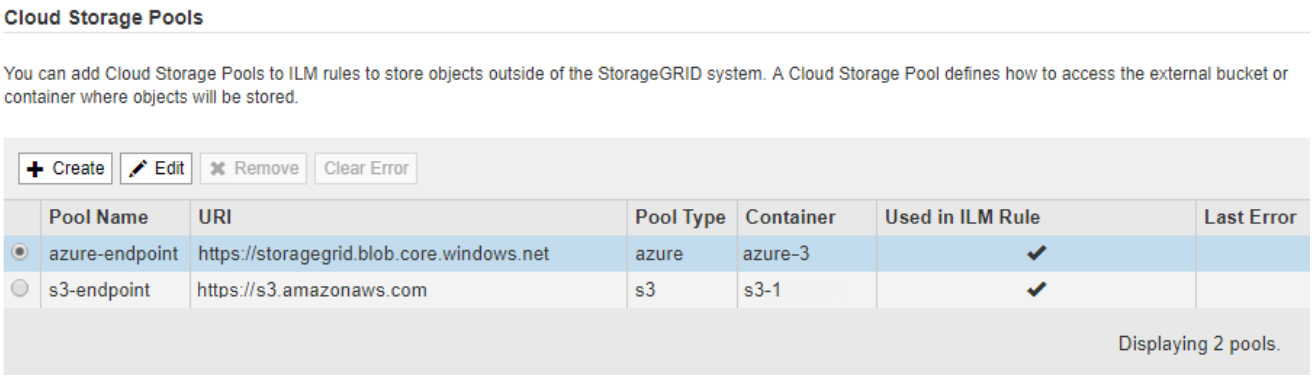
Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt.

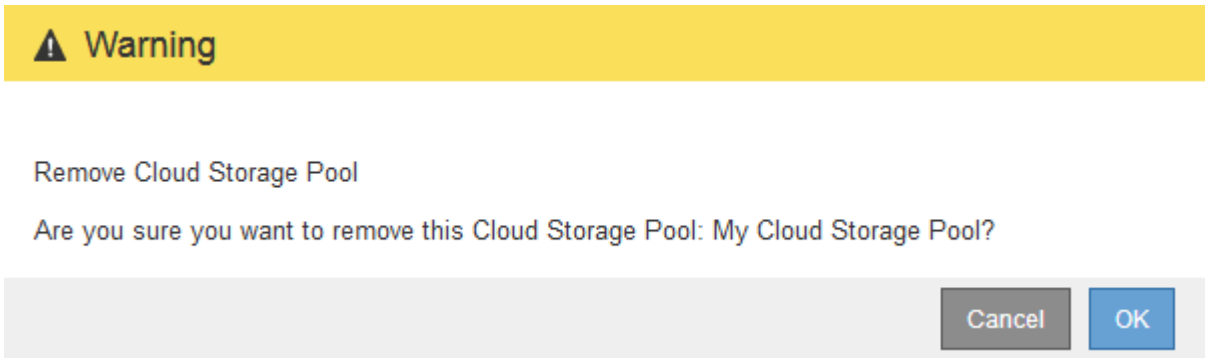
2. Wählen Sie das Optionsfeld für einen Cloud-Storage-Pool aus, der derzeit nicht in einer ILM-Regel verwendet wird.

   Sie können einen Cloud-Storage-Pool nicht entfernen, wenn er in einer ILM-Regel verwendet wird. Die Schaltfläche **Entfernen** ist deaktiviert.



3. Klicken Sie Auf **Entfernen**.

   Eine Bestätigungsmeldung wird angezeigt.



4. Klicken Sie auf **OK**.

   Der Cloud-Speicherpool wird entfernt.

Verwandte Informationen

"Fehlerbehebung Bei Cloud Storage Pools"

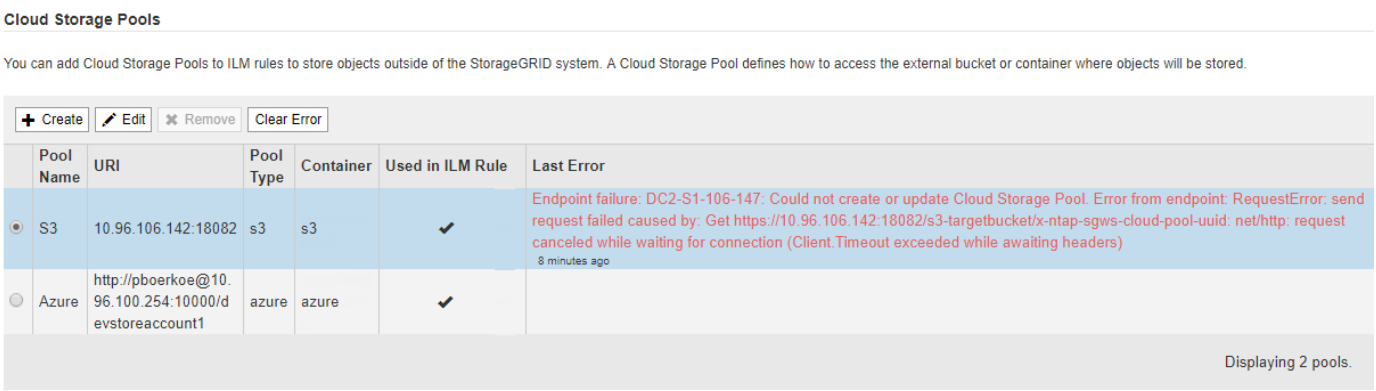
Fehlerbehebung Bei Cloud Storage Pools

Wenn beim Erstellen, Bearbeiten oder Löschen eines Cloud-Speicherpools Fehler auftreten, führen Sie diese Schritte zur Fehlerbehebung durch.

Ermitteln, 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 die Zustandsprüfung ein Problem feststellt, wird in der Spalte „Letzter Fehler“ der Tabelle „Cloud Storage Pools“ auf der Seite „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.

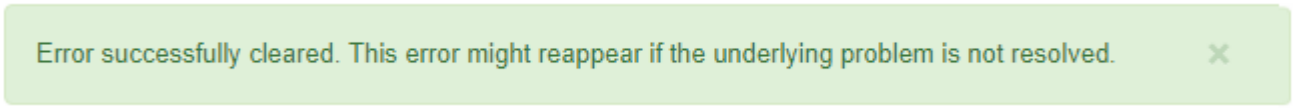


Zusätzlich wird eine Meldung mit * Cloud Storage Pool Verbindungsfehler* ausgelöst, wenn die Systemprüfung feststellt, dass innerhalb der letzten 5 Minuten ein oder mehrere neue Cloud Storage Pool-Fehler aufgetreten sind. Wenn Sie eine E-Mail-Benachrichtigung für diese Warnmeldung erhalten, gehen Sie auf die Seite Storage Pool (wählen Sie **ILM** > **Storage Pools**), überprüfen Sie die Fehlermeldungen in der Spalte Letzter

Fehler und lesen Sie die nachfolgenden Hinweise zur Fehlerbehebung.

Überprüfen, 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 das Optionsfeld für den Endpunkt aus, und klicken Sie auf **Fehler löschen**. 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 jedoch das zugrunde liegende Problem 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 Service-Endpunkt für den Cloud Storage Pool das HTTP-Protokoll 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 Anmeldedaten besitzen 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. Ein Cloud-Storage-Pool kann nicht gelöscht werden, wenn er Daten enthält, die durch ILM verschoben wurden, Daten, die sich vor dem Konfigurieren des Cloud-Storage-Pools im Bucket befand, oder Daten, die nach der Erstellung des Cloud-Storage-Pools von einer anderen Quelle in den Bucket verschoben wurden.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Folgen Sie den Anweisungen, um Objekte in „`Lifecycle eines Cloud-Storage-Pool-Objekts zurück in StorageGRID zu verschieben.`“
- Wenn Sie sicher sind, dass die verbleibenden Objekte nicht durch ILM im Cloud-Storage-Pool platziert wurden, löschen Sie die Objekte manuell aus dem Bucket.

> Löschen Sie nie Objekte manuell aus einem Cloud-Storage-Pool, der eventuell durch ILM gespeichert wurde. Wenn Sie später versuchen, auf ein manuell gelöschtes Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Fehler: Beim Versuch, den Cloud-Speicherpool zu erreichen, ist ein externer Fehler aufgetreten

Dieser Fehler kann auftreten, wenn Sie zwischen Storage-Nodes einen nicht transparenten Storage Proxy und den externen S3-Endpunkt konfiguriert haben, der für den Cloud Storage-Pool verwendet wird. Dieser Fehler tritt auf, wenn der externe Proxyserver den Endpunkt des Cloud-Storage-Pools 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"

Konfigurieren von Erasure Coding-Profilen

Sie konfigurieren Erasure Coding-Profile, indem Sie einen Storage Pool mit einem Erasure Coding-Schema wie 6+3 verknüpfen. Wenn Sie dann die Anweisungen zur Platzierung einer ILM-Regel konfigurieren, können Sie das Erasure Coding-Profil auswählen. Entspricht ein Objekt der Regel, werden Daten- und Paritätsfragmente erstellt und gemäß dem Erasure Coding-Schema an die Storage-Standorte im Storage Pool verteilt.

- "Erstellen eines Erasure Coding-Profils"
- "Umbenennen eines Erasure Coding-Profils"
- "Deaktivieren eines Erasure Coding-Profils"

Erstellen eines Erasure Coding-Profils

Um ein Erasure Coding-Profil zu erstellen, verknüpfen Sie einen Speicherpool mit Storage-Nodes mit einem Codierungsschema zur Fehlerkorrektur. Diese Verknüpfung bestimmt die Anzahl der erstellten Daten und Paritäts-Fragmente und wo das System diese Fragmente verteilt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen einen Speicherpool erstellt haben, der genau einen Standort oder einen Speicherpool umfasst, der drei oder mehr Standorte umfasst. Für einen Storage Pool mit nur zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.

Über diese Aufgabe

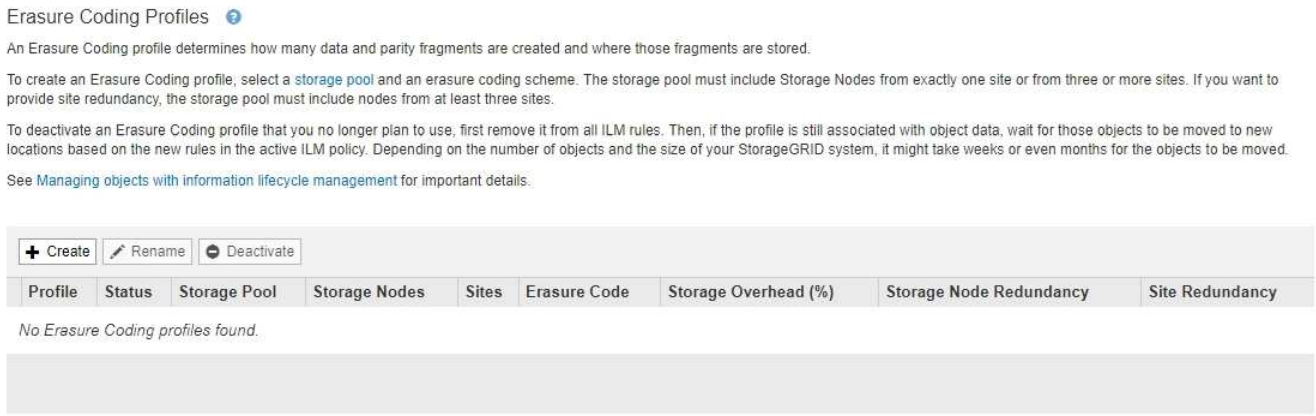
Die in Erasure Coding-Profilen verwendeten Storage-Pools müssen exakt einen oder drei oder mehr Standorte umfassen. Wenn Sie Standortredundanz bereitstellen möchten, muss der Speicherpool mindestens drei Standorte aufweisen.

Sie müssen einen Speicherpool auswählen, der Speicherknoten enthält. Sie können Archiv-Knoten nicht zum Löschen codierter Daten verwenden.

Schritte

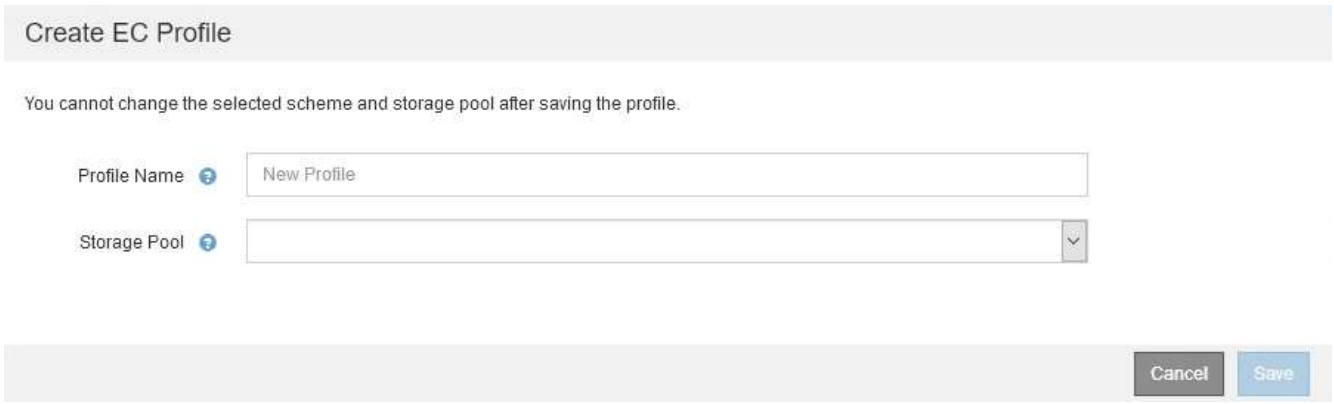
1. Wählen Sie **ILM** > **Erasure Coding** aus.

   Die Seite Erasure Coding Profiles wird angezeigt.



2. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld EC-Profil erstellen wird angezeigt.



3. Geben Sie einen eindeutigen Namen für das Erasure Coding-Profil ein.

   Profilnamen müssen eindeutig sein. Ein Validierungsfehler tritt auf, wenn Sie den Namen eines vorhandenen Profils verwenden, auch wenn dieses Profil deaktiviert wurde.

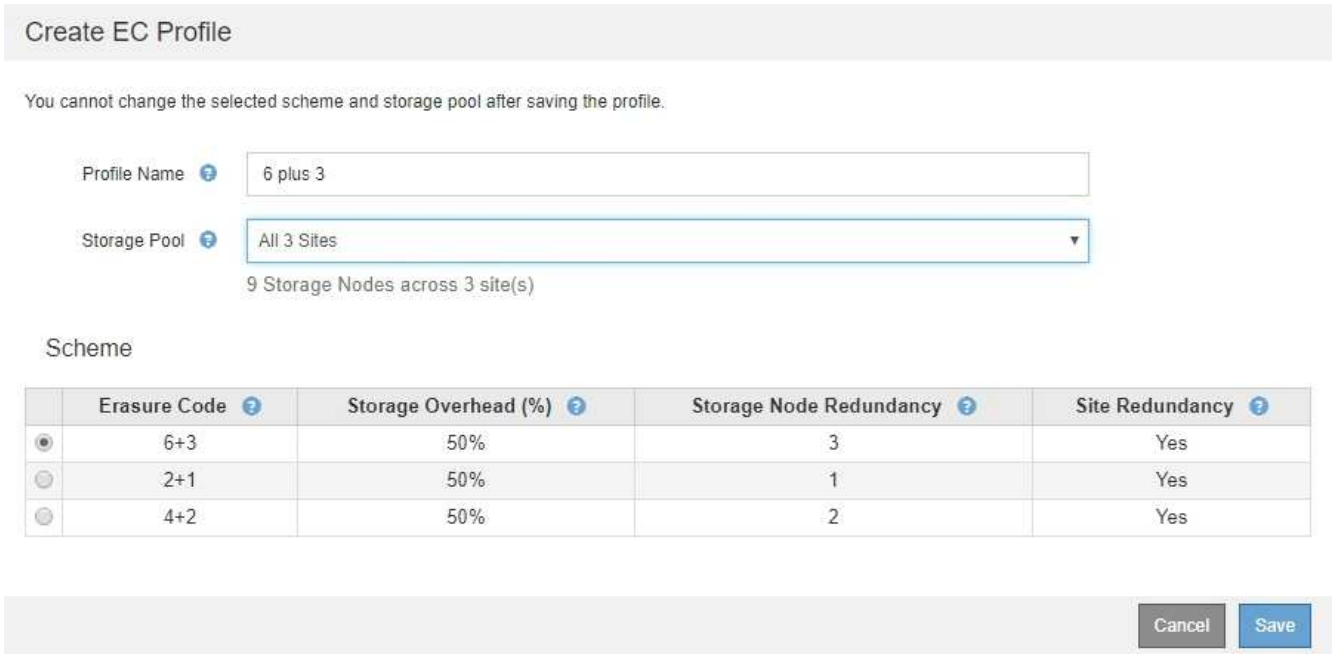
   Der Name des Erasure Coding-Profils wird an den Namen des Speicherpools in der Platzierungsanweisung für eine ILM-Regel angehängt.

4. Wählen Sie den Speicherpool aus, den Sie für dieses Erasure Coding-Profil erstellt haben.

Wenn Ihr Grid derzeit nur einen Standort enthält, können Sie den Standardspeicherpool, alle Speicherknoten oder einen beliebigen Speicherpool, der den Standardstandort, Alle Standorte enthält, nicht verwenden. Dieses Verhalten verhindert, dass das Erasure Coding-Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

Wenn ein Speicherpool genau zwei Standorte umfasst, kann er nicht für Erasure Coding verwendet werden. Für einen Speicherpool mit zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.

Wenn Sie einen Speicherpool auswählen, wird die Liste der verfügbaren Erasure-Coding-Schemata angezeigt, basierend auf der Anzahl der Speicherknoten und Standorte im Pool.



Die folgenden Informationen sind für jedes verfügbare Erasure Coding-Schema aufgeführt:

- **Erasure Code**: Der Name des Erasure-Codierungsschemas im folgenden Format: Datenfragmente + Paritätsfragmente.
- **Storage Overhead (%)**: Der zusätzliche Speicher, der für Paritäts-Fragmente im Verhältnis zur Datengröße des Objekts benötigt wird. Storage Overhead = Gesamtzahl der Parity-Fragmente / Gesamtzahl an Datenfragmenten
- **Speicherknoten-Redundanz**: Die Anzahl der Speicherknoten, die verloren gehen können, während weiterhin die Fähigkeit, Objektdaten abzurufen.
- **Standortredundanz**: Ob der ausgewählte Löschcode die Objektdaten bei Verlust eines Standorts abrufen lässt.

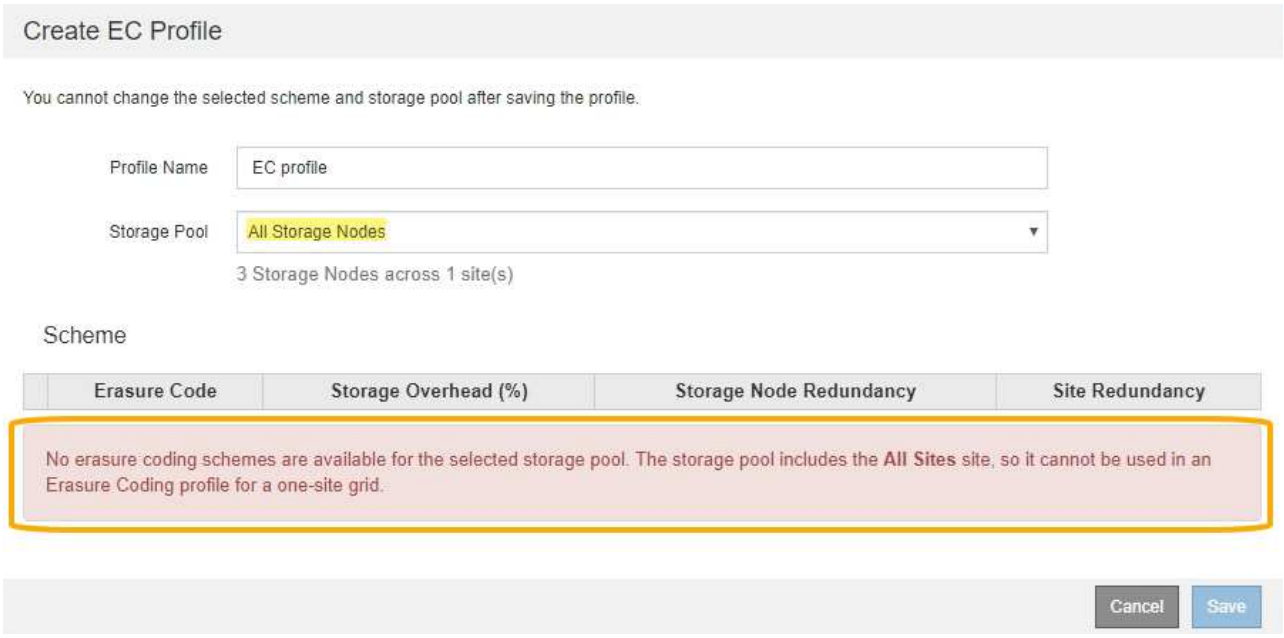
  Um Standortredundanz zu unterstützen, muss der ausgewählte Speicherpool mehrere Standorte umfassen, von denen jeder über genügend Storage-Nodes verfügt, damit jeder Standort verloren geht. Beispielsweise muss der ausgewählte Speicherpool mindestens drei Standorte mit mindestens drei Storage-Nodes an jedem Standort enthalten, um die Standortredundanz mithilfe eines Erasure Coding-Schemas von 6+3 zu unterstützen.

  In den folgenden Fällen werden Meldungen angezeigt:

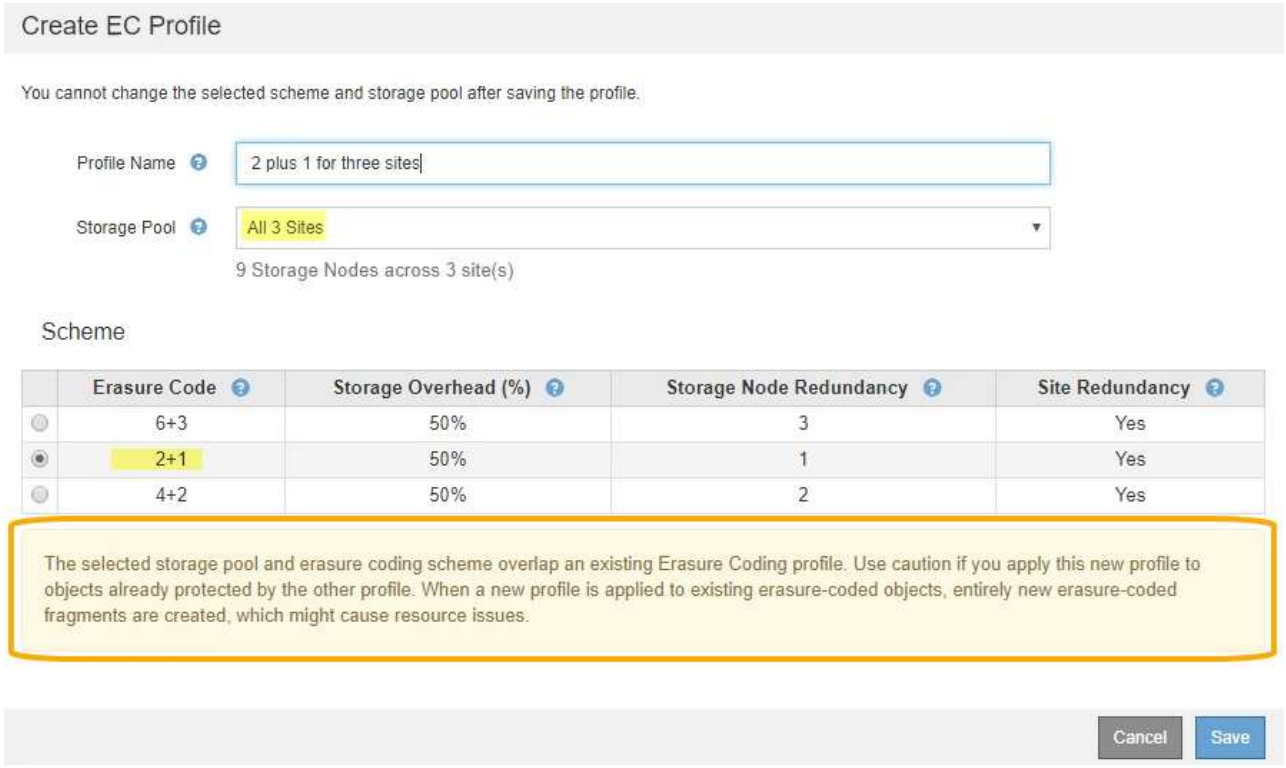
- Der ausgewählte Speicherpool bietet keine Standortredundanz. Die folgende Meldung wird erwartet, wenn der ausgewählte Speicherpool nur einen Standort umfasst. Sie können dieses Erasure Coding-Profil in ILM-Regeln verwenden, um sich vor Node-Ausfällen zu schützen.

- Der ausgewählte Speicherpool erfüllt nicht die Anforderungen für ein Erasure Coding-Schema. Zum Beispiel wird die folgende Meldung erwartet, wenn der ausgewählte Speicherpool genau zwei Standorte umfasst. Um Objektdaten mit Erasure Coding zu sichern, müssen Sie einen Storage-Pool mit genau einem Standort oder einem Storage-Pool mit drei oder mehr Standorten auswählen.

- Das Grid enthält nur einen Standort, und Sie haben den Standardspeicherpool, alle Speicherknoten oder einen beliebigen Speicherpool ausgewählt, der den Standardstandort, Alle Standorte enthält.



- Das von Ihnen ausgewählte Erasure Coding-Schema und der ausgewählte Speicherpool überschneiden sich mit einem anderen Erasure Coding-Profil.



In diesem Beispiel wird eine Warnmeldung angezeigt, weil ein anderes Erasure Coding-Profil das 2+1-Schema verwendet und der Speicherpool für das andere Profil auch einen der Standorte im Speicherpool Alle 3 Standorte verwendet.

Obwohl Sie nicht daran gehindert werden, dieses neue Profil zu erstellen, müssen Sie sehr vorsichtig sein, wenn Sie es in der ILM-Richtlinie verwenden. Wird dieses neue Profil auf vorhandene Objekte angewendet, die mit Erasure-Coding-Verfahren versehen sind und bereits durch das andere Profil geschützt sind, erstellt StorageGRID einen völlig neuen Satz von Objektfragmenten. Die vorhandenen 2+1-Fragmente werden nicht wiederverwendet. Bei der Migration von einem Erasure Coding-Profil zum anderen können Ressourcenprobleme auftreten, auch wenn die Erasure Coding-Schemata identisch sind.

5. Wenn mehr als ein Erasure-Coding-Schema aufgeführt ist, wählen Sie das gewünschte Schema aus.

   Bei der Entscheidung, welches Erasure-Coding-Schema verwendet werden soll, sollten Sie die Fehlertoleranz (die durch mehr Paritätssegmente erzielt wird) mit den Anforderungen des Netzwerkverkehrs für Reparaturen abgleichen (mehr Fragmente entsprechen mehr Netzwerkverkehr). Wenn Sie beispielsweise zwischen einem Schema 4+2 und 6+3 entscheiden, wählen Sie das Schema 6+3 aus, wenn zusätzliche Parität und Fehlertoleranz erforderlich sind. Wählen Sie das Schema 4+2 aus, wenn die Netzwerkressourcen eingeschränkt sind, um den Netzwerkverbrauch bei Node-Reparaturen zu reduzieren.

6. Klicken Sie Auf **Speichern**.

Umbenennen eines Erasure Coding-Profils

Vielleicht möchten Sie ein Erasure Coding-Profil umbenennen, um es offensichtlicher zu machen, was das Profil tut.

Was Sie benötigen

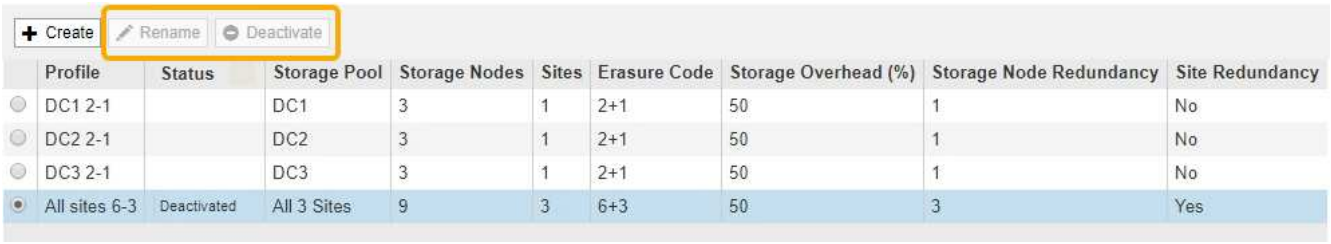
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **ILM** > **Erasure Coding** aus.

   Die Seite Erasure Coding Profiles wird angezeigt. Die Schaltflächen **Umbenennen** und **Deaktivieren** sind beide deaktiviert.



2. Wählen Sie das Profil aus, das Sie umbenennen möchten.

   Die Schaltflächen **Umbenennen** und **Deaktivieren** werden aktiviert.

3. Klicken Sie Auf **Umbenennen**.

   Das Dialogfeld EC-Profil umbenennen wird angezeigt.

4. Geben Sie einen eindeutigen Namen für das Erasure Coding-Profil ein.

   Der Name des Erasure Coding-Profils wird an den Namen des Speicherpools in der Platzierungsanweisung für eine ILM-Regel angehängt.

> Profilnamen müssen eindeutig sein. Ein Validierungsfehler tritt auf, wenn Sie den Namen eines vorhandenen Profils verwenden, auch wenn dieses Profil deaktiviert wurde.

5. Klicken Sie Auf **Speichern**.

Deaktivieren eines Erasure Coding-Profils

Sie können ein Erasure Coding-Profil deaktivieren, wenn Sie es nicht mehr verwenden

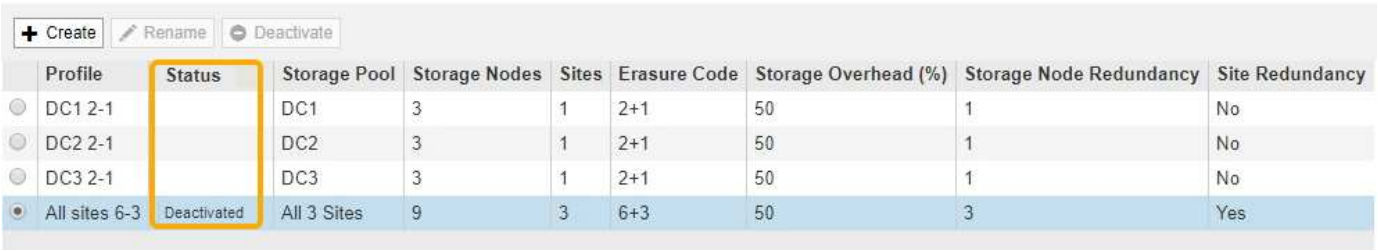
möchten und wenn das Profil derzeit in keiner ILM-Regel verwendet wird.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen bestätigt haben, dass keine entsprechend dem Erasure-Coding-Verfahren zur Reparatur von Daten oder zur Ausmusterung durchgeführten Verfahren ausgeführt werden. Wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren, während einer dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung zurückgegeben.

Über diese Aufgabe

Wenn Sie ein Erasure Coding-Profil deaktivieren, wird das Profil auf der Seite Erasure Coding Profiles weiterhin angezeigt, der Status ist jedoch **deactivated**.



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 können, 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. Objektdaten und Paritätsfragmente für das Profil sind jedoch weiterhin vorhanden.

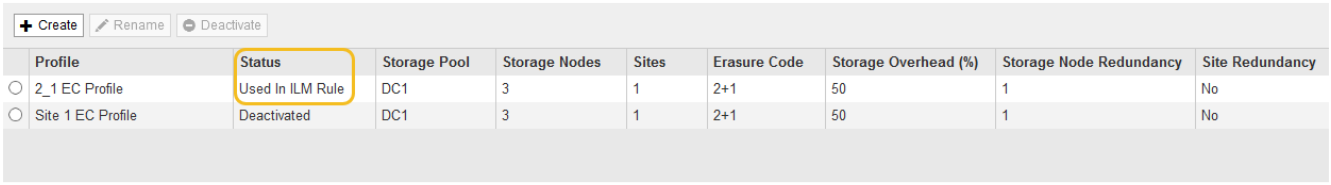
Schritte

1. Wählen Sie **ILM** > **Erasure Coding** aus.

   Die Seite Erasure Coding Profiles wird angezeigt. Die Schaltflächen **Umbenennen** und **Deaktivieren** sind beide deaktiviert.

2. Überprüfen Sie in der Spalte **Status**, ob das zu deaktivierungssyquente Erasure-Coding-Profil nicht in ILM-Regeln verwendet wird.

   Ein Erasure Coding-Profil kann nicht deaktiviert werden, wenn es in einer ILM-Regel verwendet wird. Im Beispiel wird das **2_1 EC-Profil** in mindestens einer ILM-Regel verwendet.

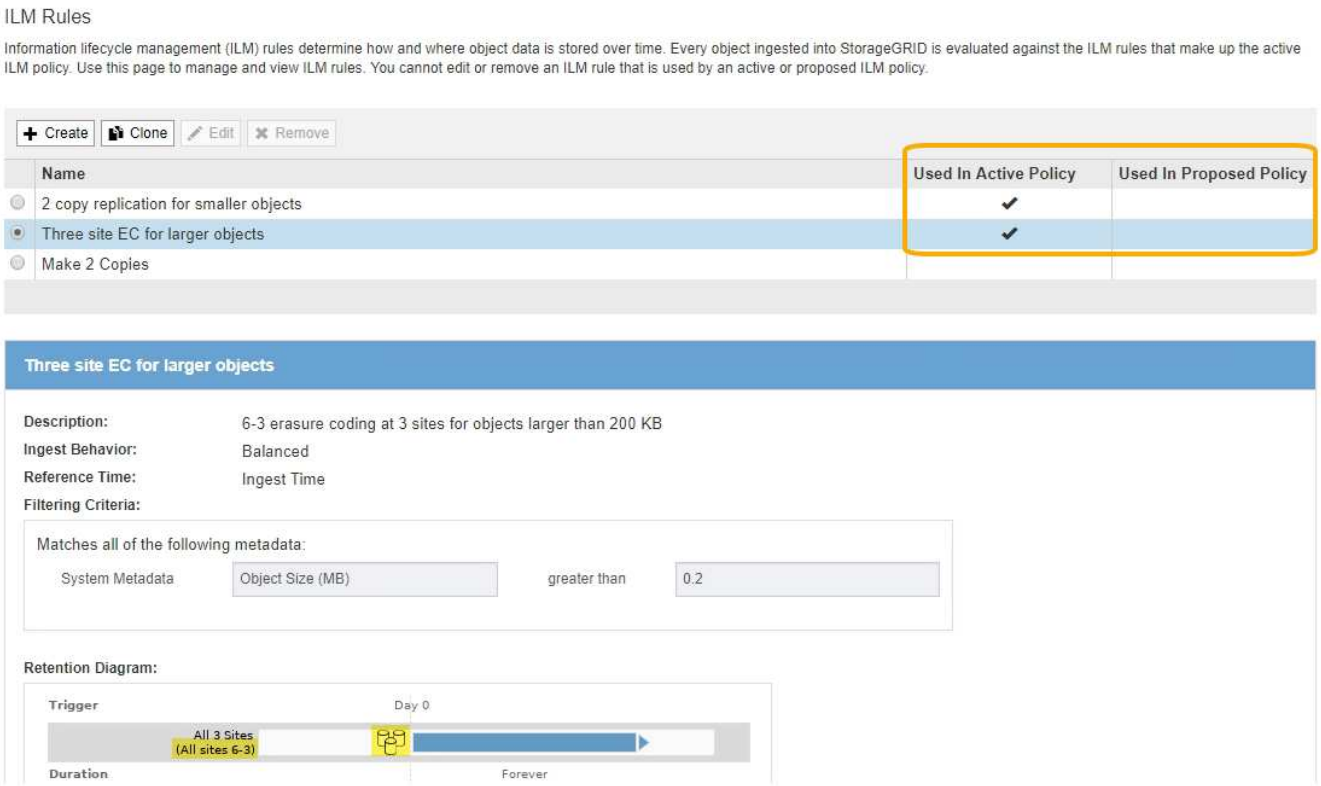


3. Wenn das Profil in einer ILM-Regel verwendet wird, führen Sie die folgenden Schritte aus:

   a. Wählen Sie **ILM** > **Regeln**.

   b. Wählen Sie für jede der aufgeführten Regeln das Optionsfeld aus, und überprüfen Sie das Aufbewahrungsdiagramm, um festzustellen, ob die Regel das Erasure-Coding-Profil verwendet, das Sie deaktivieren möchten.

      Im Beispiel verwendet die Regel **drei Seiten-EC für größere Objekte** einen Speicherpool mit dem Namen **Alle 3 Standorte** und das Profil **Alle Standorte 6-3** Erasure Coding. Dieses Symbol repräsentiert die Profile von Erasure Coding:



   a. Wenn die ILM-Regel das Erasure Coding-Profil verwendet, das Sie deaktivieren möchten, stellen Sie fest, ob die Regel entweder in der aktiven ILM-Richtlinie oder in einer vorgeschlagenen Richtlinie verwendet wird.

      Im Beispiel wird die Regel **drei Standorte EC für größere Objekte** in der aktiven ILM-Richtlinie verwendet.

   b. Führen Sie die zusätzlichen Schritte in der Tabelle aus, wobei 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.	*None*

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 noch nie in einer ILM-Richtlinie verwendet wurde	i. Alle betroffenen ILM-Regeln bearbeiten oder löschen. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. ii. Fahren Sie mit diesem Verfahren fort.	"Arbeiten mit ILM-Regeln und ILM-Richtlinien"
In einer ILM-Regel, die sich derzeit in der aktiven ILM-Richtlinie befindet	i. Klonen der aktiven Richtlinie ii. Entfernen Sie die ILM-Regel, die das Erasure Coding-Profil verwendet. iii. Fügen Sie mindestens eine neue ILM-Regel hinzu, um die Sicherheit von Objekten zu gewährleisten. iv. Speichern, simulieren und aktivieren Sie die neue Richtlinie. v. Warten Sie, bis die neue Richtlinie angewendet wird und vorhandene Objekte basierend auf den neuen Regeln, die Sie hinzugefügt haben, an neue Orte verschoben werden. **Hinweis:** abhängig von der Anzahl der Objekte und der Größe Ihres StorageGRID-Systems kann es Wochen oder sogar Monate dauern, bis ILM-Vorgänge die Objekte auf der Grundlage der neuen ILM-Regeln an neue Orte verschieben. Während Sie sicher versuchen können, ein Erasure-Coding-Profil zu deaktivieren, während es noch mit Daten verknüpft ist, schlägt die Deaktivierung fehl. Eine Fehlermeldung informiert Sie darüber, ob das Profil noch nicht deaktiviert werden kann. vi. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. vii. Fahren Sie mit diesem Verfahren fort.	• "ILM-Richtlinie erstellen" • "Arbeiten 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 einer vorgeschlagenen ILM-Richtlinie befindet	i. Bearbeiten Sie die vorgeschlagene Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Erasure Coding-Profil verwendet. iii. Fügen Sie ein oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass alle Objekte geschützt sind. iv. Speichern Sie die vorgeschlagene Richtlinie. v. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. vi. Fahren Sie mit diesem Verfahren fort.	• "ILM-Richtlinie erstellen" • "Arbeiten mit ILM-Regeln und ILM-Richtlinien"
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 mit ILM-Regeln und ILM-Richtlinien"

c. 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, lautet sein Status **deaktiviert**. 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Beim Erstellen eines S3-Buckets können Sie angeben, dass er in einer bestimmten Region erstellt wird. Wenn Sie eine Region angeben, kann der Bucket sich in geografischer Nähe zu seinen Benutzern befinden, um die Latenz zu optimieren, Kosten zu minimieren und gesetzliche Anforderungen zu erfüllen.

Wenn Sie eine ILM-Regel erstellen, möchten Sie die Region, die einem S3-Bucket zugeordnet ist, möglicherweise als erweiterten Filter verwenden. Sie können zum Beispiel eine Regel entwerfen, die sich nur auf Objekte bezieht, die in den in uns-West-2 erstellten S3-Buckets gelten. Sie können dann angeben, die Kopien dieser Objekte an Storage-Nodes an einem Datacenter-Standort innerhalb dieser Region platziert werden, um die Latenz zu optimieren.

Befolgen Sie bei der Konfiguration von Regionen die folgenden Richtlinien:

- Standardmäßig gehören alle Buckets zu US-East-1-Region.
- Sie müssen die Regionen mit dem Grid Manager erstellen, bevor Sie beim Erstellen von Buckets mithilfe der Mandanten-Manager- oder Mandantenmanagement-API oder mit dem LocationConstraint-Anforderungselement für S3 PUT-Bucket-API-Anforderungen eine nicht standardmäßige Region angeben können. Ein Fehler tritt auf, wenn eine PUT-Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.
- Sie müssen beim Erstellen des S3-Buckets den genauen Regionalnamen verwenden. Bei regionalen Namen wird zwischen Groß- und Kleinschreibung unterschieden. Das Unternehmen muss mindestens 2 und nicht mehr als 32 Zeichen enthalten. 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.

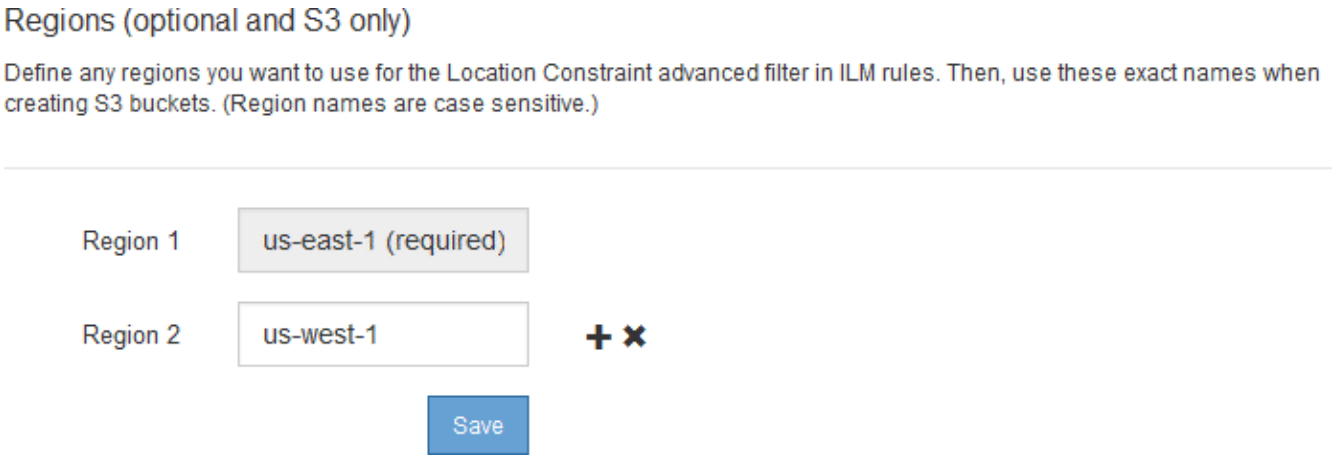
- Eine Region kann nicht gelöscht oder geändert werden, wenn sie derzeit in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.
- Wenn die Region, die als erweiterter Filter in einer ILM-Regel verwendet wird, ungültig ist, kann diese Regel noch zur vorgeschlagenen Richtlinie hinzugefügt werden. Es tritt jedoch ein Fehler auf, wenn Sie versuchen, die vorgeschlagene Richtlinie zu speichern oder zu aktivieren. (Eine ungültige Region kann dazu führen, dass Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region später jedoch löschen oder wenn Sie die Grid Management API verwenden, um eine Regel zu erstellen und eine Region anzugeben, 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 kann.

2. So fügen Sie eine Region hinzu:
   a. Klicken Sie auf das INSERT-Symbol ➕ 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, klicken Sie auf das Löschsymbol ✖.

   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, klicken Sie auf **Speichern**.

   Sie können diese Regionen nun aus der Liste **Location Constraint** auf der Seite Advanced Filtering des Assistenten Create ILM rule auswählen.

Verwandte Informationen

"Verwendung erweiterter Filter in ILM-Regeln"

Erstellen einer ILM-Regel

ILM-Regeln ermöglichen es Ihnen, die Platzierung von Objektdaten im Laufe der Zeit zu managen. Zum Erstellen einer ILM-Regel verwenden Sie den Assistenten zur Erstellung von ILM-Regeln.

Bevor Sie beginnen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie angeben möchten, für welche Mandantenkonten diese Regel gilt, müssen Sie über die Berechtigung für Mandantenkonten verfügen, oder Sie müssen die Konto-ID für jedes Konto kennen.
- Wenn die Regel Objekte nach Metadaten der letzten Zugriffszeit filtern soll, müssen Updates der letzten Zugriffszeit für S3 oder für Swift nach Container aktiviert werden.
- Falls Sie replizierte Kopien erstellen, müssen Sie alle Storage-Pools oder Cloud-Storage-Pools konfiguriert haben, die Sie verwenden möchten.
- Wenn Sie Kopien mit Erasure Coding erstellen, müssen Sie ein Erasure Coding-Profil konfiguriert haben.
- Sie müssen mit dem vertraut sein "Datensicherungsoptionen für die Aufnahme".
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, müssen Sie mit dem vertraut sein "Anforderungen für die S3-Objektsperre".

> Verwenden Sie stattdessen dieses Verfahren, um die ILM-Standardregel für eine Richtlinie zu erstellen: "Erstellen einer Standard-ILM-Regel".

Über diese Aufgabe

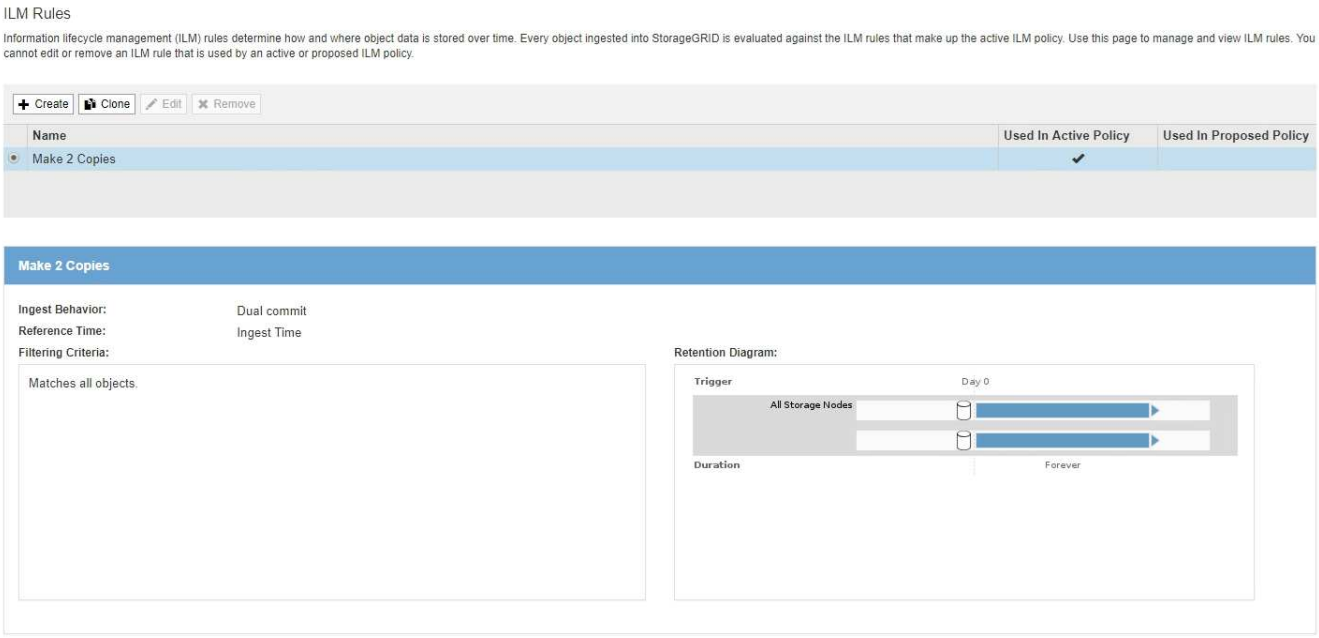
Wenn ILM-Regeln erstellt werden:

- 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, welche Option für die Datensicherungsoption bei Aufnahme verwendet werden soll (ausgewogen, streng oder Dual-Commit)

Schritte

1. Wählen Sie **ILM** > **Regeln**.

   Die Seite ILM-Regeln wird angezeigt, wobei die Bestandsregel 2 Kopien erstellen soll, ausgewählt.



Die Seite ILM-Regeln sieht etwas anders aus, wenn die globale S3-Objektsperre für das StorageGRID System aktiviert wurde. Die Übersichtstabelle enthält eine **Compliant**-Spalte, und die Details für die ausgewählte Regel enthalten ein **Compliant**-Feld.

2. Wählen Sie **Erstellen**.

   Schritt 1 (Grundlagen definieren) des Assistenten „ILM-Regel erstellen“ wird angezeigt. Auf der Seite Grundlagen definieren können Sie definieren, für welche Objekte die Regel gilt.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie Swift"

"Konfigurieren von Erasure Coding-Profilen"

"Konfigurieren von Speicherpools"

"Verwendung Von Cloud Storage Pools"

"Datensicherungsoptionen für die Aufnahme"

"Verwalten von Objekten mit S3 Object Lock"

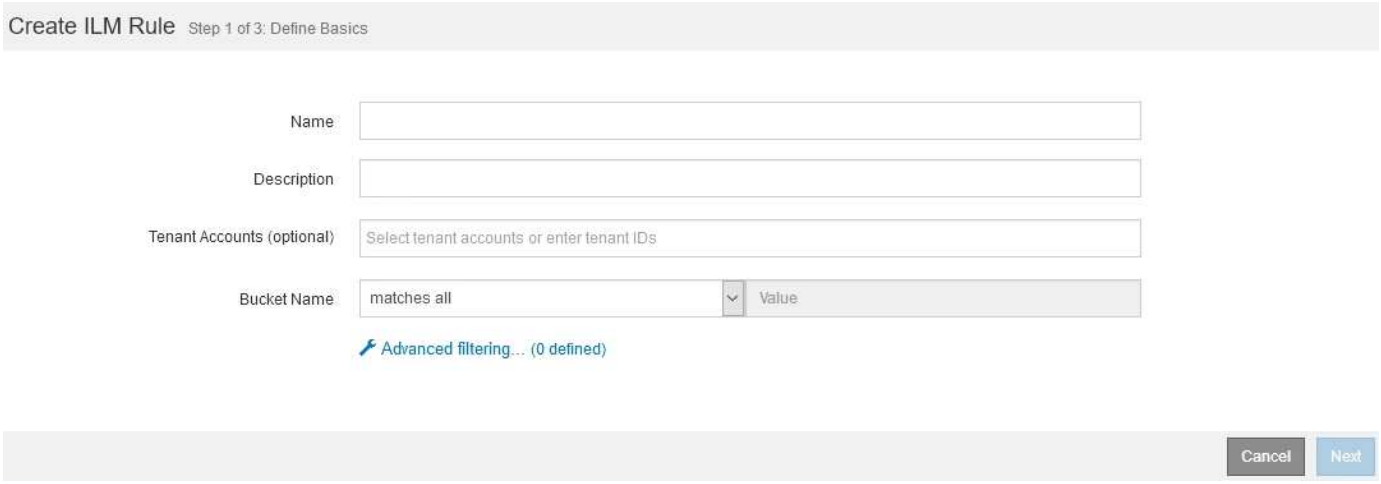
Schritt 1 von 3: Grundlagen definieren

Schritt 1 (Grundlagen definieren) des Assistenten „ILM-Regel erstellen“ ermöglicht es Ihnen, die grundlegenden und erweiterten Filter der Regel zu definieren.

Über diese Aufgabe

Bei der Bewertung eines Objekts mit einer ILM-Regel vergleicht StorageGRID die Objekt-Metadaten 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.

   Sie müssen 1 bis 64 Zeichen eingeben.

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 nicht über die Berechtigung Stammzugriff oder 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 optional **Erweiterte Filterung**, um zusätzliche Filter festzulegen.

   Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den grundlegenden Filtern entsprechen.

   > Wenn diese Regel mit dem Löschen kodierte Kopien erstellt, wählen Sie **Erweiterte Filterung**. Fügen Sie dann den erweiterten Filter **Objektgröße (MB)** hinzu und setzen Sie ihn auf **größer als 0.2**. Der Größenfilter stellt sicher, dass Objekte, die 2 MB oder kleiner sind, nicht gelöscht werden.

6. Wählen Sie **Weiter**.

Schritt 2 (Platzierungen definieren) wird angezeigt.

Verwandte Informationen

"Was ist die ILM-Regelfilterung"

"Verwendung erweiterter Filter in ILM-Regeln"

"Schritt 2 von 3: Definieren von Platzierungen"

Verwendung erweiterter 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 (Mikrosekunden)	• Gleich • Ist nicht gleich • Kleiner als • Weniger als oder gleich • Größer als • Größer als oder gleich	Uhrzeit und Datum, an dem das Objekt aufgenommen wurde. **Hinweis:** um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter für die Aufnahmezeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie die Aufnahmezeit auf größer oder gleich der ungefähren Zeit fest, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.
Taste	• Gleich • Ist nicht gleich • Enthält • Enthält nicht • Beginnt mit • Startet nicht mit • Endet mit • Endet nicht mit	Der gesamte Objektschlüssel oder Teil eines eindeutigen S3- oder Swift-Objektschlüssels. Beispielsweise können Sie Objekte, die mit enden, aufeinander abstimmen `.txt` Oder beginnen Sie mit `test-object/`.

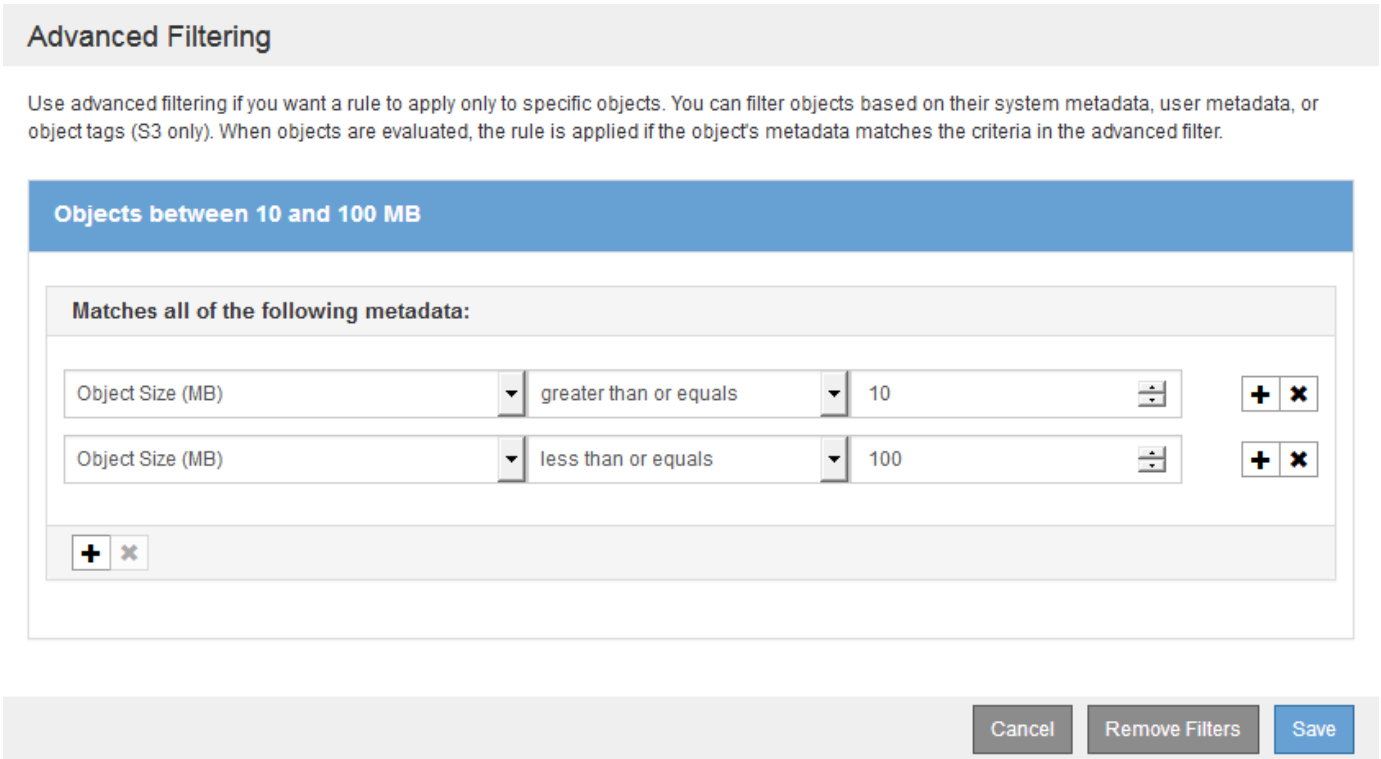
Metadatentyp	Unterstützte Operatoren	Metadatenwert
Zeitpunkt des letzten Zugriffs (Mikrosekunden)	• Gleich • Ist nicht gleich • Kleiner als • Weniger als oder gleich • Größer als • Größer als oder gleich • Vorhanden • Nicht vorhanden	Uhrzeit und Datum, an dem das Objekt zuletzt abgerufen wurde (gelesen oder angezeigt). **Hinweis:** Wenn Sie die letzte Zugriffszeit als erweiterten Filter verwenden möchten, müssen Updates der letzten Zugriffszeit für den S3-Bucket oder Swift-Container aktiviert sein. "Verwenden der Zeit für den letzten Zugriff in ILM-Regeln"
Speicherortbeschränkung (nur S3)	• Gleich • Ist nicht gleich	Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie **ILM** > **Regionen**, um die angezeigten Regionen zu definieren. **Hinweis:** Ein Wert von US-East-1 entspricht Objekten in Eimern, die in der Region US-East-1 erstellt wurden, sowie Objekten in Buckets, die keine Region angegeben haben. "Regionen konfigurieren (nur optional und S3)"
Objektgröße (MB)	• Gleich • Nicht gleich • Kleiner als • Weniger als oder gleich • Größer als • Größer als oder gleich	Die Größe des Objekts in MB. Um nach Objektgrößen kleiner als 1 MB zu filtern, geben Sie einen Dezimalwert ein. Stellen Sie beispielsweise den erweiterten Filter **Objektgröße (MB)** auf **größer als 0.2** für jede Regel ein, die eine Löschkopie erstellt. Mit dieser Einstellung wird sichergestellt, dass das Erasure Coding nicht für Objekte mit einer Größe von 200 KB verwendet wird. **Hinweis:** Ihr Browsertyp und die Gebietseinstellungen steuern, ob Sie einen Punkt oder ein Komma als Dezimaltrennzeichen verwenden müssen.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Benutzermetadaten	• Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit	Schlüssel-Wert-Paar, wobei **User Metadata Name** der Schlüssel ist und **User Metadata Value** der Wert ist. Zum Beispiel nach Objekten mit Benutzer-Metadaten von filtern `color=blue`, Spezifizieren `color` Für **User Metadata Name**, `equals` Für den Bediener, und `blue` Für **User Metadata Value**. **Hinweis:** Benutzer-Metadaten Namen sind nicht Groß-/Kleinschreibung; Benutzer-Metadaten-Werte sind Groß-/Kleinschreibung.
Objekt-Tag (nur S3)	• Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit	Schlüssel-Wert-Paar, wobei **Objekt-Tag-Name** der Schlüssel und **Objekt-Tag-Wert** der Wert ist. Zum Beispiel, um nach Objekten zu filtern, die ein Objekt-Tag von haben `Image=True`, Spezifizieren `Image` Für **Objekt-Tag-Name**, `equals` Für den Bediener, und `True` Für **Objekt-Tag-Wert**. **Hinweis:** Objekt-Tag-Namen und Objekt-Tag-Werte sind Groß- und Kleinschreibung. Sie müssen diese Elemente genau so eingeben, wie sie für das Objekt definiert wurden.

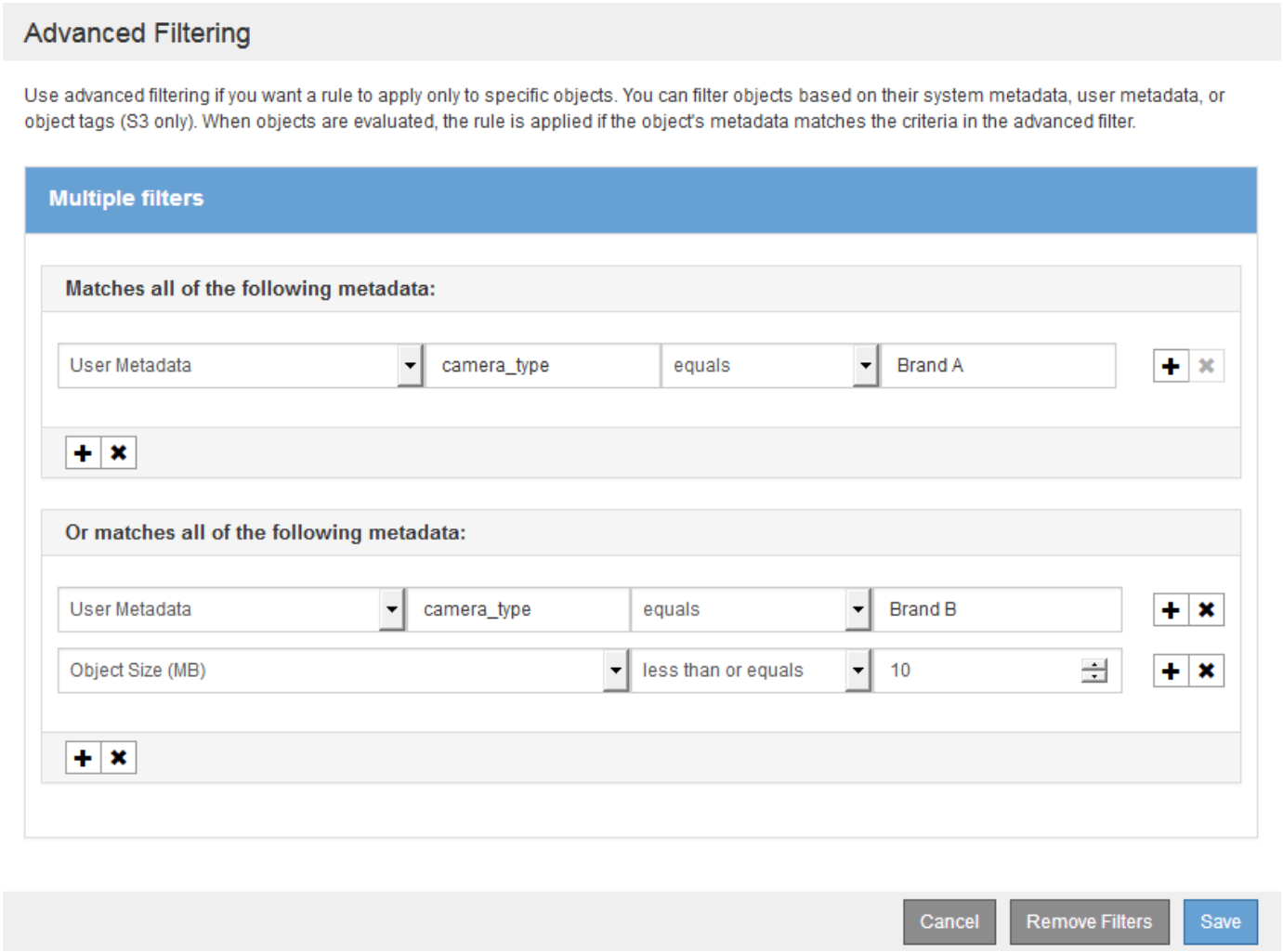
Angeben mehrerer Metadatentypen und -Werte

Wenn Sie die erweiterte Filterung definieren, können Sie mehrere Metadatentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise eine Regel für Objekte zwischen 10 MB und 100 MB Größe festlegen möchten, wählen Sie den Metadatentyp **Objektgröße** aus und geben zwei Metadaten an.

- Der erste Metadatenwert gibt Objekte an, die größer oder gleich 10 MB sind.
- Der zweite Metadatenwert gibt Objekte an, die kleiner als oder gleich 100 MB sind.



Durch die Verwendung mehrerer Einträge können Sie genau steuern, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, die einen Brand A oder eine Marke B als Wert der Camera_type-Benutzermetadaten haben. Die Regel gilt jedoch nur für Objekte der Marke B, die kleiner als 10 MB sind.



Verwandte Informationen

"Verwenden der Zeit für den letzten Zugriff in ILM-Regeln"

"Regionen konfigurieren (nur optional und S3)"

Schritt 2 von 3: Definieren von Platzierungen

Schritt 2 (Platzierungen definieren) des Assistenten zur Erstellung von ILM-Regeln können Sie die Anweisungen zur Platzierung festlegen, um festzulegen, wie lange Objekte gespeichert werden, wie viel Kopien (repliziert oder Erasure Coding), den Storage-Standort und die Anzahl der Kopien erstellt werden.

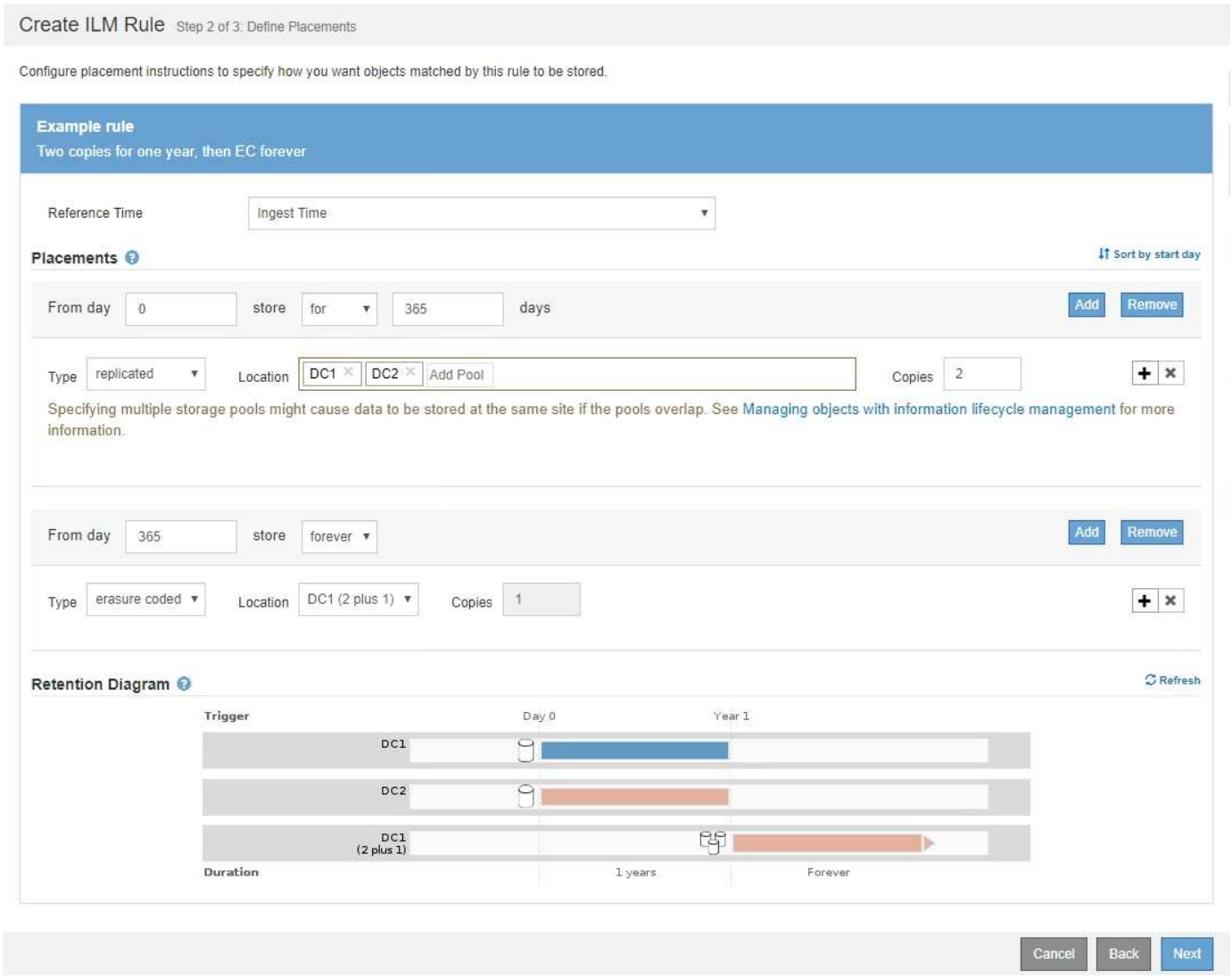
Über diese Aufgabe

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.

Diese Beispiel-ILM-Regel erstellt zwei replizierte Kopien für das erste Jahr. Jede Kopie wird in einem Speicherpool an einem anderen Standort gespeichert. Nach einem Jahr wird eine 2+1-Kopie mit Erasure-

Coding-Verfahren an nur einem Standort erstellt und gespeichert.



Schritte

1. Wählen Sie für **Referenzzeit** den Zeittyp aus, der bei der Berechnung der Startzeit für eine Platzierungsanweisung verwendet werden soll.

Option	Beschreibung
Aufnahmezeit	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 zu nutzen, müssen Updates zur letzten Zugriffszeit für den S3-Bucket oder Swift-Container aktiviert sein. "Verwenden der Zeit für den letzten Zugriff in ILM-Regeln"

Option	Beschreibung
Nicht Aktuelle Zeit	Die Zeit, in der eine Objektversion nicht mehr aktuell wurde, weil eine neue Version aufgenommen und als aktuelle Version ersetzt wurde. **Hinweis:** die nicht aktuelle Zeit gilt nur für S3-Objekte in Versionierungsfähigen Buckets. 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 S3-Objekte.`“
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.

Wenn Sie eine konforme Regel erstellen möchten, müssen Sie **Aufnahmezeit** auswählen.

2. Wählen Sie im Abschnitt **Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum aus.

   Sie können beispielsweise festlegen, wo Objekte für das erste Jahr gespeichert werden sollen („`day 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 **Typ** die Option **repliziert** aus.
   b. Wählen Sie im Feld **Standort** für jeden Speicherpool, den Sie hinzufügen möchten, **Pool hinzufügen** aus.

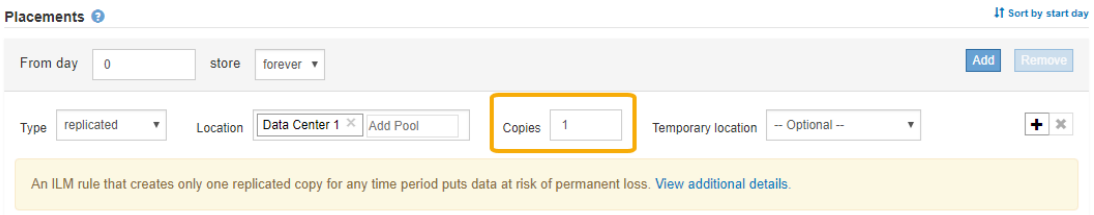
      Wenn Sie nur einen Speicherpool angeben, beachten Sie, dass StorageGRID nur eine replizierte Kopie eines Objekts auf einem beliebigen Speicherknoten speichern kann. Wenn Ihr Grid drei Storage-Nodes enthält und Sie 4 als Anzahl der Kopien auswählen, werden nur drei Kopien erstellt: Eine Kopie für jeden 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 kleiner als die Anzahl der Storage-Pools ist, verteilt das System die Kopien, damit die Festplattennutzung zwischen den Pools ausgeglichen bleibt. Gleichzeitig wird sichergestellt, dass an keinem Standort mehr als eine Kopie eines Objekts gespeichert wird.
      - Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Geben Sie aus diesem Grund nicht den Standardpool Alle Speicherknoten und einen anderen Speicherpool an.

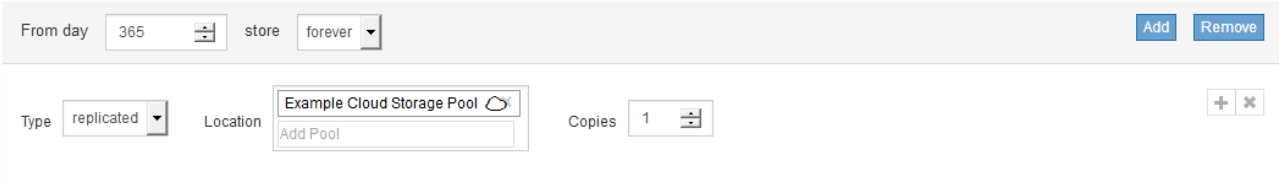
c. Wählen Sie die Anzahl der Kopien aus, die Sie erstellen möchten.

> 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. Wenn nur eine replizierte Kopie eines Objekts während eines Zeitraums vorhanden ist, geht dieses Objekt verloren, wenn ein Storage Node ausfällt oder einen beträchtlichen Fehler aufweist. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.
>
> 
>
>
> Um diese Risiken zu vermeiden, führen Sie einen oder mehrere der folgenden Schritte aus:
>
> - Erhöhen Sie die Anzahl der Kopien für den Zeitraum.
> - Klicken Sie auf das Pluszeichen-Symbol ➕ Um während des Zeitraums zusätzliche Kopien zu erstellen. Wählen Sie dann einen anderen Speicherpool oder einen Cloud-Speicherpool aus.
> - Wählen Sie **Erasure Coded** für Typ, statt **repliziert**. Sie können diese Warnung ohne Bedenken ignorieren, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

d. Wenn Sie nur einen Speicherpool angegeben haben, ignorieren Sie das Feld **temporärer Standort**.

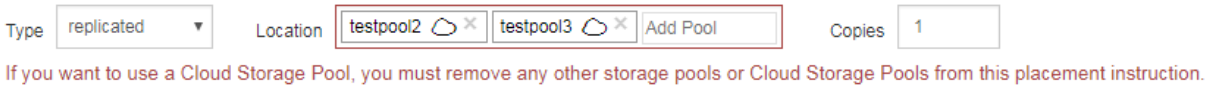
> Temporäre Speicherorte sind veraltet und werden in einer zukünftigen Version entfernt.

4. Wenn Sie Objekte in einem Cloud-Speicherpool speichern möchten:
   a. Wählen Sie aus der Dropdown-Liste **Typ** die Option **repliziert** aus.
   b. Wählen Sie im Feld **Ort** die Option **Pool hinzufügen** aus. Wählen Sie dann einen Cloud-Speicherpool aus.



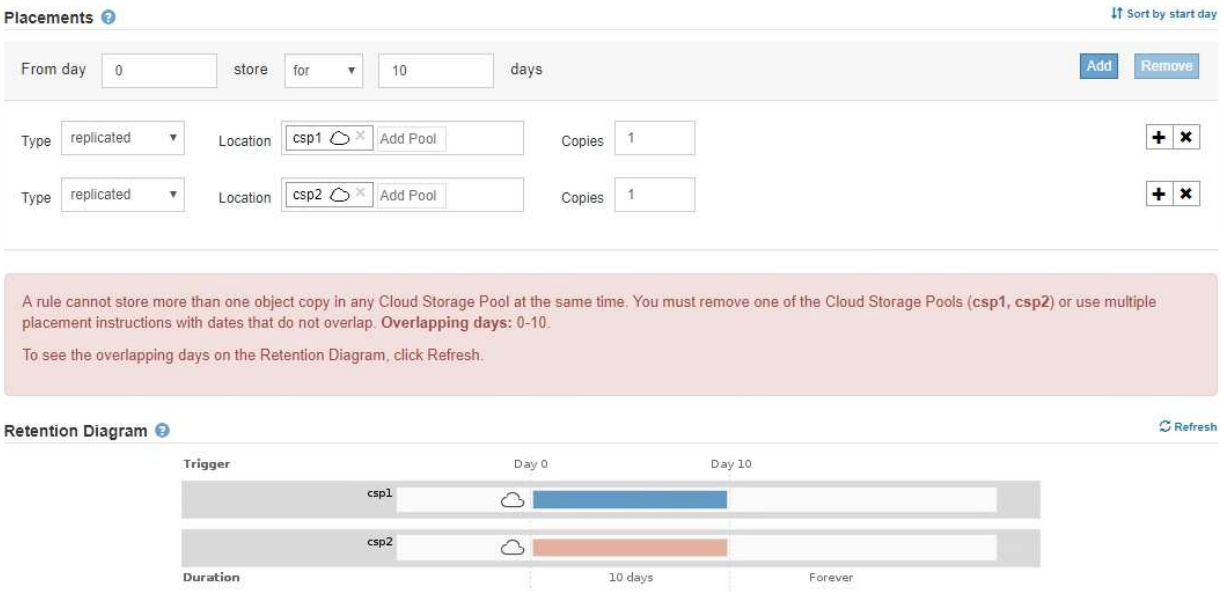
Beachten Sie bei der Verwendung von Cloud-Storage-Pools folgende Regeln:

- Sie können nicht mehr als einen Cloud-Storage-Pool in einer einzelnen Speicheranweisung auswählen. Auf ähnliche Weise können Sie keinen Cloud-Storage-Pool und einen Storage-Pool in derselben Speicheranweisung auswählen.

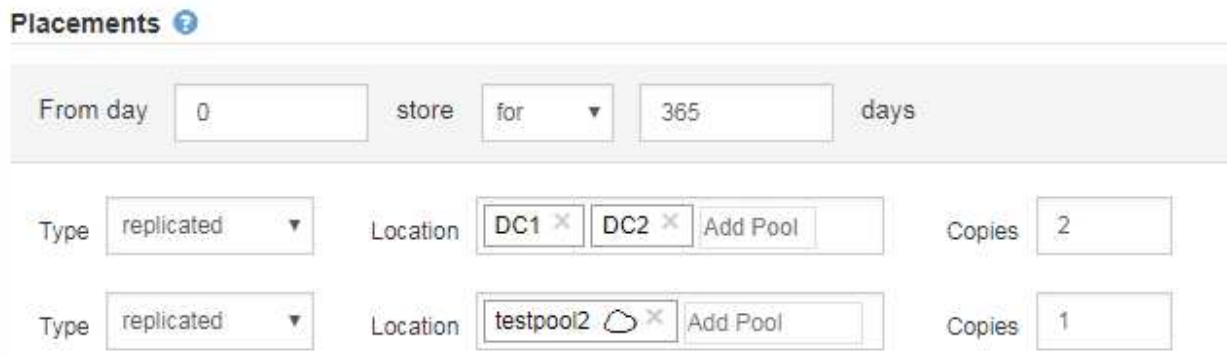


- Sie können nur eine Kopie eines Objekts in einem beliebigen Cloud Storage Pool speichern. Wenn Sie **Copies** auf 2 oder mehr setzen, wird eine Fehlermeldung angezeigt.

- Sie können nicht mehr als eine Objektkopie in einem Cloud-Speicherpool gleichzeitig speichern. 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. Wie in diesem Beispiel gezeigt wird, müssen Sie für den Zeitraum jedoch mehr als eine Zeile in die Platzierungsanweisung aufnehmen, damit Sie die Anzahl und die Art der Kopien für jeden Standort angeben können.



5. Wenn Sie eine Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) erstellen möchten:

a. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Löschvorgang codiert** aus.

   Die Anzahl der Kopien ändert sich in 1. Es wird eine Warnung angezeigt, wenn die Regel keinen erweiterten Filter besitzt, um Objekte zu ignorieren, die 200 KB oder kleiner sind.

   Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to "greater than 0.2".

   > Verwenden Sie kein Erasure Coding für Objekte mit einer Größe von mehr als 200 KB, um den Overhead zu vermeiden, der bei dem Management sehr kleiner, mit Erasure Coding codierter Fragmente verbunden ist.

b. Wenn die Warnung Objektgröße angezeigt wurde, führen Sie die folgenden Schritte aus, um sie zu löschen:

   i. Wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren.

   ii. Wählen Sie **Erweiterte Filterung**.

   iii. Setzen Sie den Filter Objektgröße (MB) auf „`größer als 0.2`“.

c. Wählen Sie den Speicherort aus.

   Der Speicherort für eine Kopie mit Erasure-Coding-Verfahren umfasst den Namen des Speicherpools, gefolgt vom Namen des Erasure Coding-Profils.

6. Optional können Sie verschiedene Zeiträume hinzufügen oder zusätzliche Kopien an verschiedenen Standorten erstellen:
   - Klicken Sie auf das Plus-Symbol, um während des gleichen Zeitraums zusätzliche Kopien an einem anderen Ort zu erstellen.
   - Klicken Sie auf **Hinzufügen**, um den Anweisungen zur Platzierung einen anderen Zeitraum hinzuzufügen.

   > Objekte werden am Ende des Endzeitzeitraums automatisch gelöscht, es sei denn, der Endzeitraum endet mit **forever**.

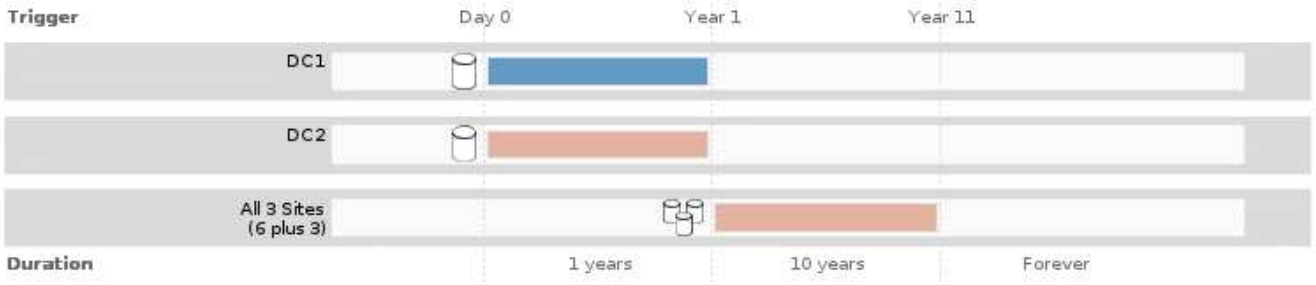
7. Klicken Sie auf **Aktualisieren**, um das Aufbewahrungsdiagramm zu aktualisieren und die Anweisungen zur Platzierung zu bestätigen.

   Jede Zeile im Diagramm zeigt an, wo und wann Objektkopien platziert werden. Der Kopiertyp wird durch eines der folgenden Symbole dargestellt:

	Replizierte Kopie
	Kopie mit Erasure Coding – eine Kopie

	Cloud-Storage-Pool-Kopie

In diesem Beispiel werden zwei replizierte Kopien für ein Jahr in zwei Speicherpools (DC1 und DC2) gespeichert. Anschließend wird eine Kopie mit Erasure Coding für weitere 10 Jahre gespeichert. Dabei wird ein 6+3 Erasure Coding-Schema an drei Standorten verwendet. Nach 11 Jahren werden die Objekte aus StorageGRID gelöscht.



8. Klicken Sie Auf **Weiter**.

   Schritt 3 (Ingest Behavior definieren) wird angezeigt.

Verwandte Informationen

"Welche Anweisungen zur Platzierung der ILM-Regeln gibt es"

"Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"

"Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden"

"Verwalten von Objekten mit S3 Object Lock"

"Verwenden eines Speicherpools als temporärer Speicherort (veraltet)"

"Schritt 3 von 3: Definieren des Aufnahmeverhaltens"

Verwenden der Zeit für den letzten Zugriff in ILM-Regeln

Sie können den Zeitpunkt 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 den Zeitpunkt des letzten Zugriffs auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur für Objekte gelten soll, auf die zuletzt an einem bestimmten Datum zugegriffen wurde.

Über diese Aufgabe

Bevor Sie den Zeitpunkt des letzten Zugriffs in einer ILM-Regel verwenden, prüfen Sie die folgenden Aspekte:

- Wenn Sie den Zeitpunkt des letzten Zugriffs als Referenzzeit verwenden, beachten Sie, dass durch das Ändern der Uhrzeit für den letzten Zugriff für ein Objekt keine sofortige ILM-Evaluierung ausgelöst wird. 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, die auf Last Access Time basieren, und vermeiden Sie Platzierungen, die kurze Zeiträume (weniger als einen Monat) nutzen.

- Wenn Sie den Zeitpunkt des letzten Zugriffs als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Updates der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können den Tenant Manager oder die Mandantenmanagement-API verwenden.

> 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.

Die folgende Tabelle fasst zusammen, ob die letzte Zugriffszeit für alle Objekte im Bucket für unterschiedliche Anträgen aktualisiert wird.

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn Updates der letzten Zugriffszeit deaktiviert sind	Ob die letzte Zugriffszeit aktualisiert wird, wenn Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Verwandte Informationen

"S3 verwenden"

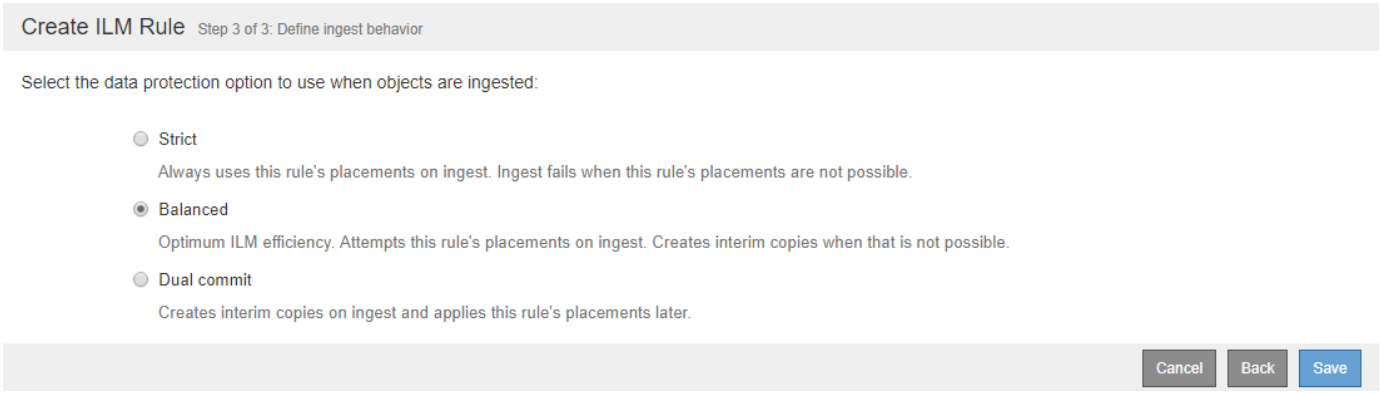
"Verwenden Sie ein Mandantenkonto"

Schritt 3 von 3: Definieren des Aufnahmeverhaltens

Schritt 3 (Ingest Behavior definieren) des Assistenten Create ILM Rule ermöglicht es Ihnen, festzulegen, wie die Objekte, die von dieser Regel gefiltert werden, beim Einnehmen 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 Datenschutzoption aus, die verwendet werden soll, wenn Objekte aufgenommen werden:

Option	Beschreibung
Streng	Verwendet bei der Aufnahme immer die Platzierungen dieser Regel. Einspeisung scheitert, wenn die Platzierungen dieser Regel nicht möglich sind.
Ausgeglichen	Optimale ILM-Effizienz: Versucht die Platzierungen dieser Regel bei der Aufnahme. Erstellt zwischenzeitliche Kopien, wenn dies nicht möglich ist.
Doppelte Provisionierung	Erstellt vorläufige Kopien bei der Aufnahme und wendet die Platzierung dieser Regel später an.

Balance bietet eine Kombination aus Datensicherheit und Effizienz, die in den meisten Fällen geeignet ist. Zur Erfüllung spezifischer Anforderungen wird in der Regel eine strenge oder doppelte Provisionierung verwendet.

Weitere Informationen finden Sie unter „`welche Datensicherungsoptionen für die Aufnahme`“ und „`vor- und Nachteile jeder Datensicherungsoption`“.

> Wenn Sie die Option streng oder ausgewogen auswählen und die Regel eine der folgenden Platzierungen verwendet, wird eine Fehlermeldung angezeigt:
>
> - Ein Cloud-Storage-Pool am Tag 0
> - Ein Archiv-Node am Tag 0
> - Ein Cloud-Speicherpool oder ein Archiv-Node, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit verwendet

2. Klicken Sie Auf **Speichern**.

   Die ILM-Regel wird gespeichert. Die Regel bleibt erst aktiv, wenn sie zu einer ILM-Richtlinie hinzugefügt und diese Richtlinie aktiviert wird.

Verwandte Informationen

"Datensicherungsoptionen für die Aufnahme"

"Vor- und Nachteile sowie Einschränkungen der Datensicherungsoptionen"

"Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"

"ILM-Richtlinie erstellen"

Erstellen einer Standard-ILM-Regel

Jede ILM-Richtlinie muss über eine Standardregel verfügen, die keine Objekte filtert. Vor dem Erstellen einer ILM-Richtlinie müssen Sie mindestens eine ILM-Regel erstellen, die als Standardregel für die Richtlinie verwendet werden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie ausgewertet werden muss. Daher kann sie keine Filter verwenden. Die Anweisungen zur Platzierung der Standardregel werden auf alle Objekte angewendet, die nicht mit einer anderen Regel in der Richtlinie abgeglichen werden.

In dieser Beispielrichtlinie gilt die erste Regel nur für Objekte, die zu Mandant A gehören Die letzte Standardregel gilt für Objekte, die zu allen anderen Mandantenkonten gehören.

Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel in der Richtlinie gesetzt.
- Die Standardregel kann keine einfachen oder erweiterten Filter verwenden.
- Die Standardregel sollte replizierte Kopien erstellen.

> Verwenden Sie keine Regel, die Kopien, die zur Fehlerkorrektur 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**.

Die Seite ILM-Regeln wird angezeigt.

2. Wählen Sie **Erstellen**.

   Schritt 1 (Grundlagen definieren) des Assistenten „ILM-Regel erstellen“ wird angezeigt.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.
4. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.
5. Lassen Sie das Feld **Mandantenkonten** leer.

   Die Standardregel muss auf alle Mandantenkonten angewendet werden.

6. Lassen Sie das Feld **Bucket Name** leer.

   Die Standardregel muss auf alle S3-Buckets und Swift-Container angewendet werden.

7. Wählen Sie nicht **Advanced Filtering** aus

   Die Standardregel kann keine Filter angeben.

8. Wählen Sie **Weiter**.

   Schritt 2 (Platzierungen definieren) wird angezeigt.

9. 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 zur Fehlerkorrektur codiert wurden, als Standardregel für eine Richtlinie erstellt. Erasure-Coding-Regeln sollten den erweiterten Filter **Objektgröße (MB) von mehr als 0.2** enthalten, um zu verhindern, dass kleinere Objekte gelöscht werden.

   - Wenn Sie die globale S3-Objektsperre verwenden (oder diese aktivieren möchten), muss die Standardregel konform sein:
     - Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
     - Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Plazierung vorhanden sein.
     - Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
     - Objektkopien können nicht auf Archiv-Knoten gespeichert werden.
     - Mindestens eine Zeile der Anweisungen für die Platzierung muss am Tag 0 beginnen, wobei die Aufnahmezeit als Referenzzeit verwendet wird.
     - Mindestens eine Zeile der Platzierungsanweisungen muss „`Forever`“ sein.
10. Klicken Sie auf **Aktualisieren**, um das Aufbewahrungsdiagramm zu aktualisieren und die Anweisungen zur Platzierung zu bestätigen.
11. Klicken Sie Auf **Weiter**.

Schritt 3 (Ingest Behavior definieren) wird angezeigt.

12. Wählen Sie die Datenschutzoption aus, die verwendet werden soll, wenn Objekte aufgenommen werden, und wählen Sie **Speichern**.

ILM-Richtlinie erstellen

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.

Überlegungen bei der Erstellung einer ILM-Richtlinie

- Verwenden Sie die integrierte Systemrichtlinie Basis-2-Kopien-Richtlinie nur in Testsystemen. Die Regel 2 Kopien erstellen in dieser Richtlinie verwendet 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.
- 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 einer Richtlinie mit einem Objekt übereinstimmt, wird diese Regel nicht durch eine andere Regel ausgewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die Standard-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.

Verwandte Informationen

"Was ist eine ILM-Richtlinie"

"Beispiel 6: Ändern einer ILM-Richtlinie"

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die ILM-Regeln erstellt haben, die Sie der vorgeschlagenen Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
- Sie müssen eine Standard-ILM-Regel für die Richtlinie erstellt haben, die keine Filter enthält.

  "Erstellen einer Standard-ILM-Regel"

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 außer Betrieb nehmen und alle Regeln, die sich auf den Standort beziehen, entfernen.
- Sie haben einen neuen Mandanten mit besonderen Anforderungen an die Datensicherheit hinzugefügt.
- Sie haben damit begonnen, einen Cloud-Storage-Pool zu verwenden.

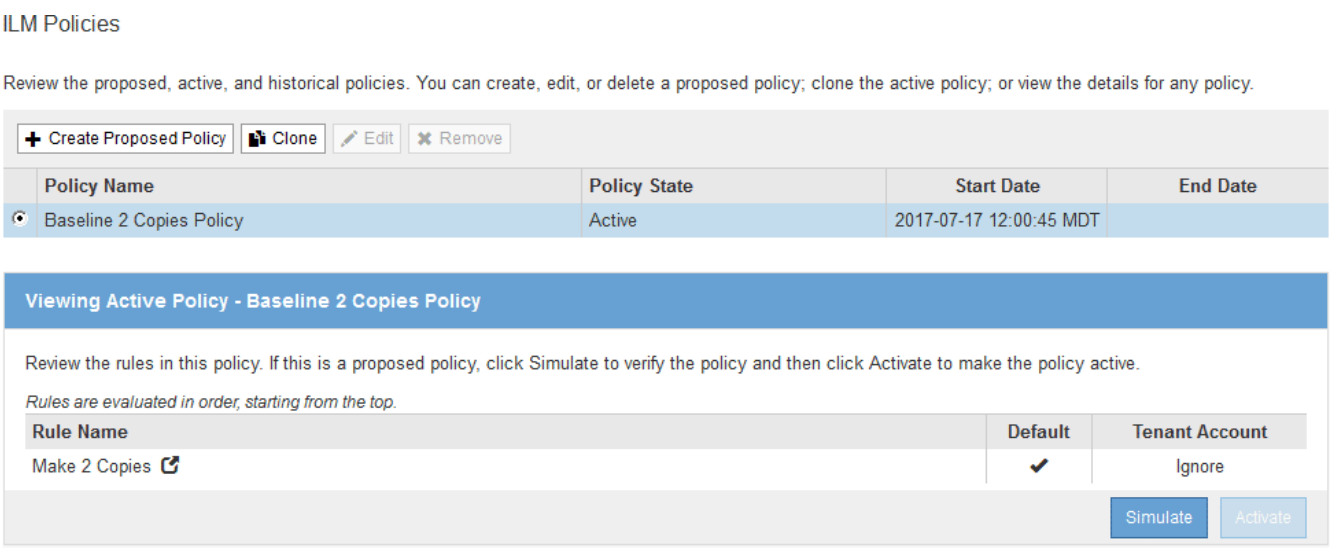
> Verwenden Sie die integrierte Systemrichtlinie Basis-2-Kopien-Richtlinie nur in Testsystemen. Die Regel 2 Kopien erstellen in dieser Richtlinie verwendet den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

> Wenn die globale S3-Objektsperre aktiviert wurde, sind die Schritte zum Erstellen einer Richtlinie etwas unterschiedlich. Sie müssen sicherstellen, dass die ILM-Richtlinie die Anforderungen von Buckets erfüllt, für die S3 Object Lock aktiviert ist.
>
> "Erstellen einer ILM-Richtlinie, nachdem S3 Object Lock aktiviert ist"

Schritte

1. Wählen Sie **ILM** > **Richtlinien**.

   Die Seite ILM-Richtlinien wird angezeigt. Auf dieser Seite können Sie die Liste der vorgeschlagenen, aktiven und historischen Richtlinien überprüfen; erstellen, bearbeiten, Oder entfernen Sie eine vorgeschlagene Richtlinie, klonen Sie die aktive Richtlinie oder lesen Sie die Details zu einer Richtlinie.

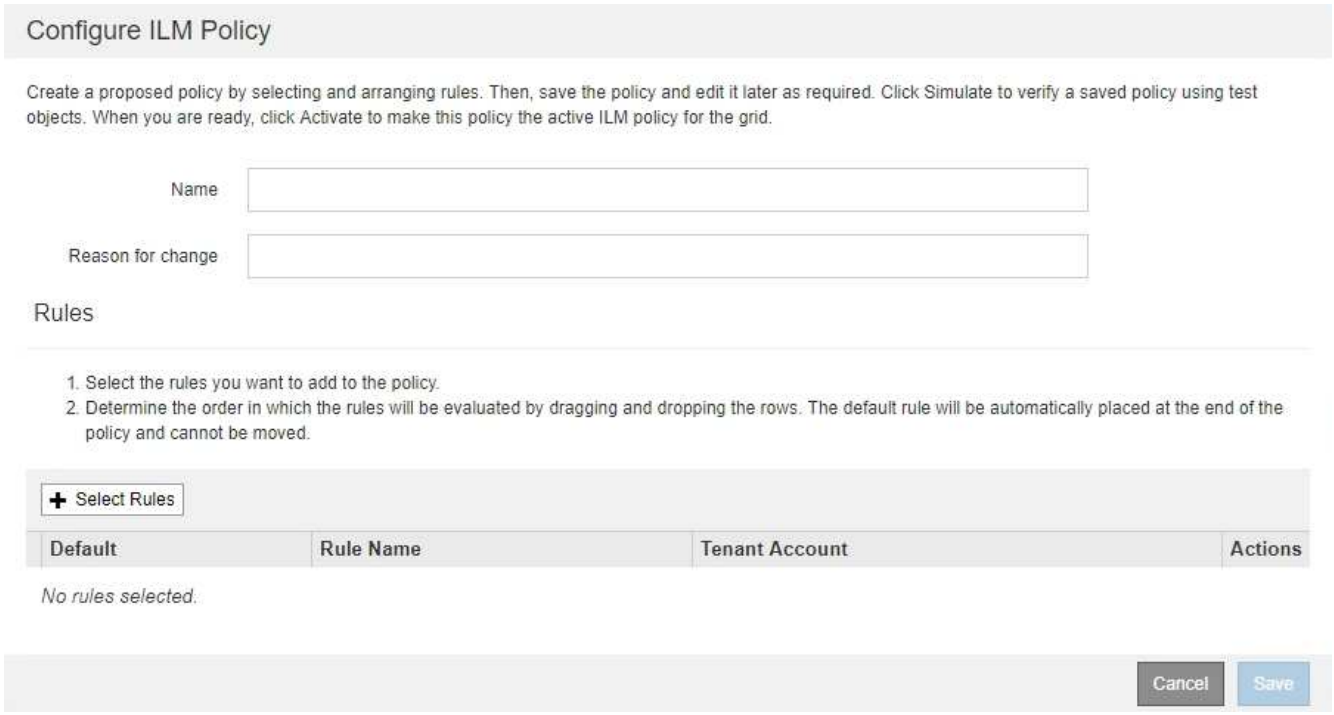


2. Legen Sie fest, wie Sie die vorgeschlagene ILM-Richtlinie erstellen möchten.

Option	Schritte
Erstellen Sie eine neue vorgeschlagene Richtlinie, für die keine Regeln bereits ausgewählt sind	a. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie diese Richtlinie aus, und klicken Sie auf **Entfernen**. Sie können keine neue vorgeschlagene Richtlinie erstellen, wenn eine vorgeschlagene Richtlinie bereits vorhanden ist. b. Klicken Sie Auf **Vorgeschlagene Richtlinie Erstellen**.
Erstellen Sie eine vorgeschlagene Richtlinie auf der Grundlage der aktiven Richtlinie	a. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie diese Richtlinie aus, und klicken Sie auf **Entfernen**. Sie können die aktive Richtlinie nicht klonen, wenn eine vorgeschlagene Richtlinie bereits vorhanden ist. b. Wählen Sie die aktive Richtlinie aus der Tabelle aus. c. Klicken Sie Auf **Clone**.
Bearbeiten Sie die vorhandene vorgeschlagene Richtlinie	a. Wählen Sie die vorgeschlagene Richtlinie aus der Tabelle aus. b. Klicken Sie Auf **Bearbeiten**.

Das Dialogfeld ILM-Richtlinie konfigurieren wird angezeigt.

Wenn Sie eine neue vorgeschlagene Richtlinie erstellen, sind alle Felder leer und es werden keine Regeln ausgewählt.



Wenn Sie die aktive Richtlinie klonen, zeigt das Feld **Name** den Namen der aktiven Richtlinie an, der durch eine Versionsnummer („`v2`" im Beispiel angehängt wird. Die in der aktiven Richtlinie verwendeten Regeln werden ausgewählt und in ihrer aktuellen Reihenfolge angezeigt.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die vorgeschlagene Richtlinie ein.

   Sie müssen mindestens 1 und nicht mehr als 64 Zeichen eingeben. Wenn Sie die aktive Richtlinie klonen, können Sie den aktuellen Namen mit der angehängerten Versionsnummer verwenden oder einen neuen Namen eingeben.

4. Geben Sie im Feld **Grund für Änderung** den Grund für die Erstellung einer neuen Policy ein.

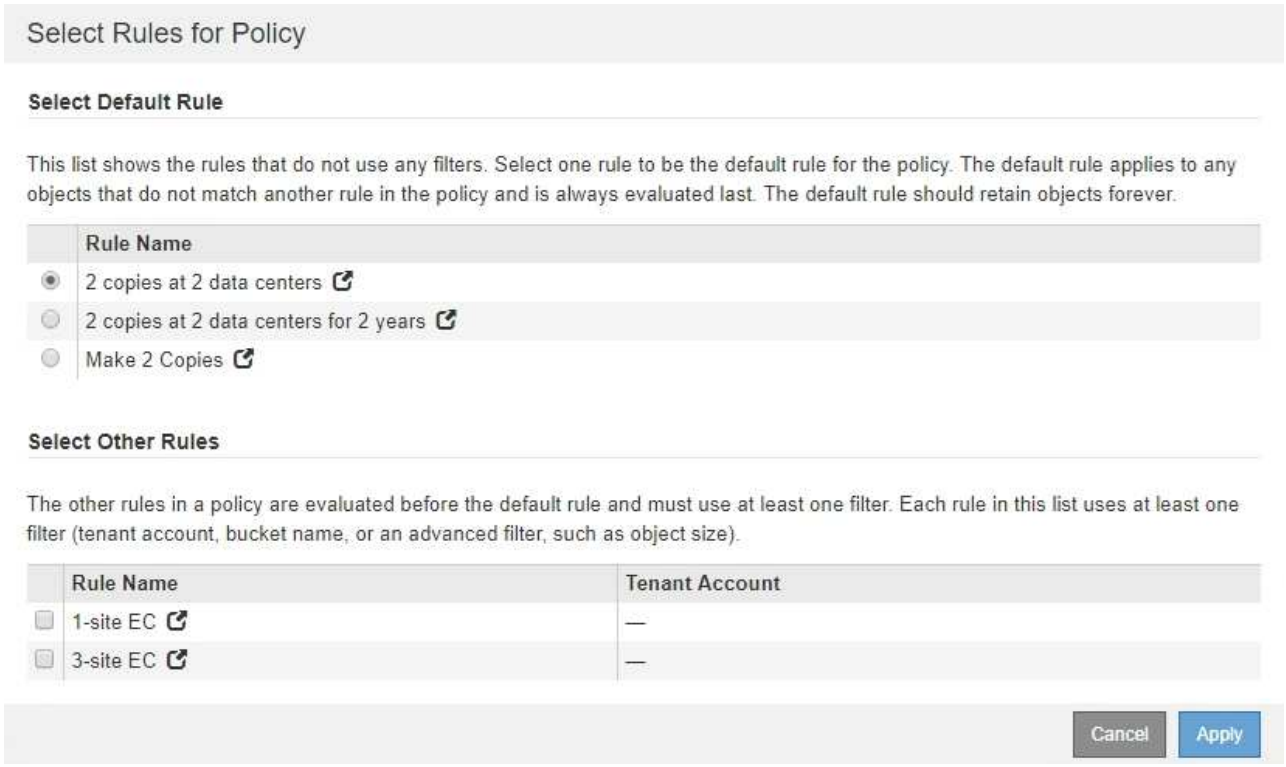
   Sie müssen mindestens 1 und nicht mehr als 128 Zeichen eingeben.

5. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**.

   Das Dialogfeld Regeln für Richtlinie auswählen wird angezeigt, in dem alle definierten Regeln aufgeführt sind. 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 mit einer Schaltfläche die Regel an das Ende der neuen Richtlinie

verschieben.



6. Wählen Sie einen Regelnamen oder das Symbol für weitere Details aus So zeigen Sie die Einstellungen für diese Regel an:

   Dieses Beispiel zeigt die Details einer ILM-Regel, die zwei Kopien an zwei Standorten erstellt.

7. Wählen Sie im Abschnitt **Standardregel auswählen** eine Standardregel für die vorgeschlagene Richtlinie aus.

   Die Standardregel gilt für alle Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen. Die Standardregel kann keinen Filter verwenden und wird immer zuletzt ausgewertet.

Wenn im Abschnitt Standardregel auswählen keine Regel aufgeführt wird, müssen Sie die Seite ILM-Richtlinie beenden und eine Standardregel erstellen.

"Erstellen einer Standard-ILM-Regel"

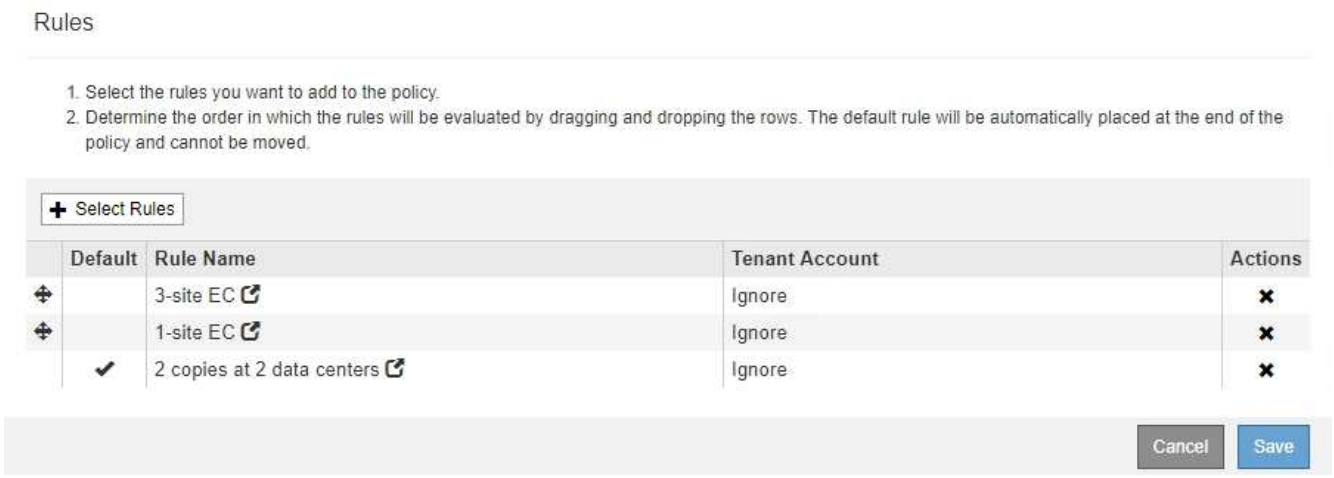
Verwenden Sie die Regel „2-Kopien-Bestand erstellen“ nicht als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

8. Wählen Sie im Abschnitt **Weitere Regeln** alle weiteren Regeln aus, die Sie in die Richtlinie aufnehmen möchten.

   Die anderen Regeln werden vor der Standardregel evaluiert und müssen mindestens einen Filter verwenden (Mandantenkonto, Bucket-Name oder erweiterten Filter, wie Objektgröße).

9. Wenn Sie die Auswahl von Regeln abgeschlossen haben, wählen Sie **Anwenden**.

   Die ausgewählten Regeln werden aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber.



Eine Warnung wird angezeigt, wenn die Standardregel Objekte nicht dauerhaft enthält. 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 länger).

10. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln per Drag-and-Drop, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

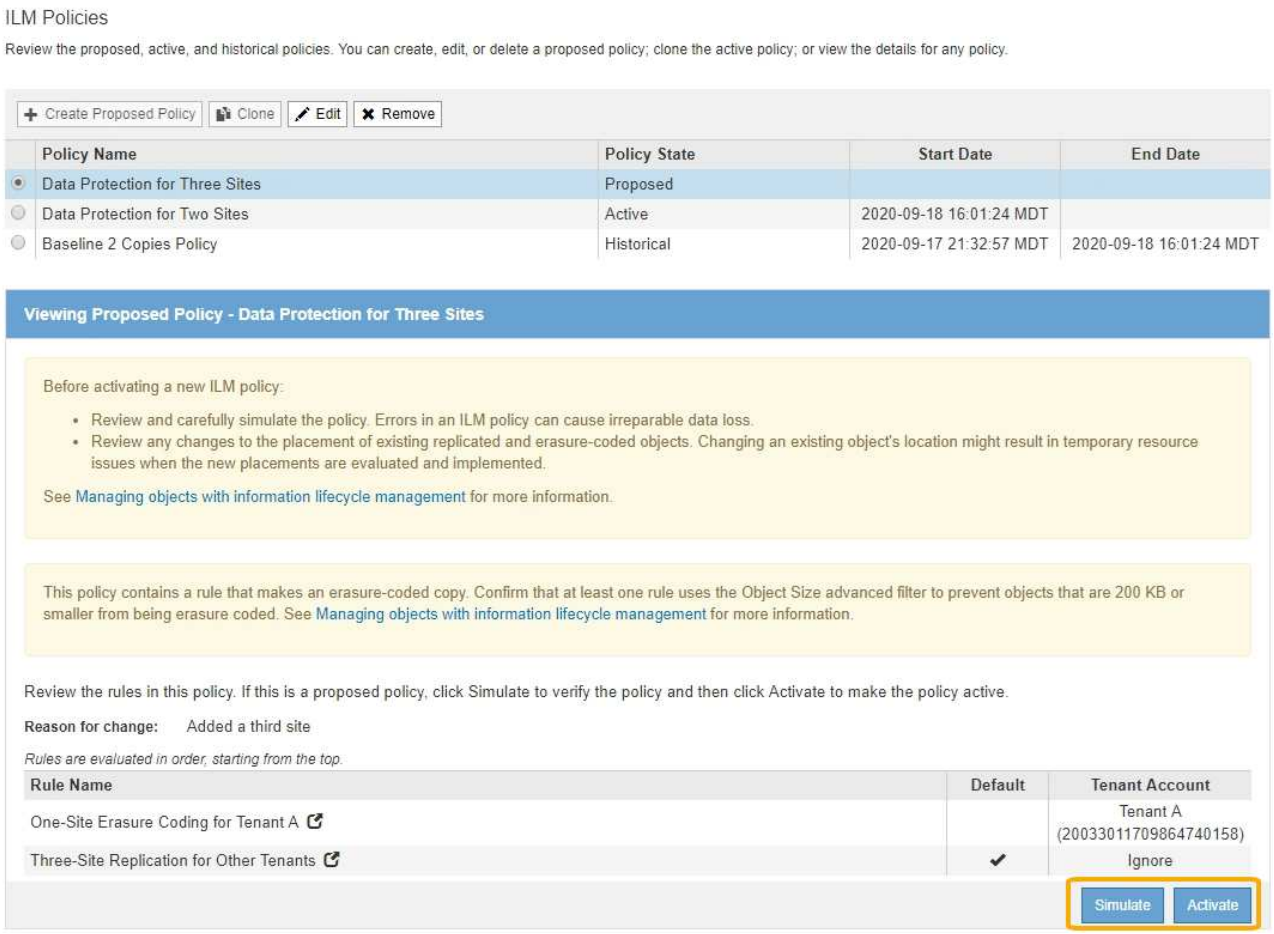
Sie können die Standardregel nicht verschieben.

> 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.

11. Klicken Sie bei Bedarf auf das Löschsymbol ✖ Wenn Sie Regeln löschen möchten, die in der Richtlinie nicht enthalten sein sollen, oder wählen Sie **Regeln auswählen**, um weitere Regeln hinzuzufügen.
12. Wenn Sie fertig sind, wählen Sie **Speichern**.

    Die Seite ILM-Richtlinien wird aktualisiert:

    - Die von Ihnen gespeicherte Richtlinie wird als Vorschlag angezeigt. Die vorgeschlagenen Richtlinien haben kein Start- und Enddatum.
    - Die Schaltflächen **Simulate** und **Activate** sind aktiviert.



13. Gehen Sie zu "Simulation einer ILM-Richtlinie".

Verwandte Informationen

"Was ist eine ILM-Richtlinie"

"Verwalten von Objekten mit S3 Object Lock"

Erstellen einer ILM-Richtlinie, nachdem S3 Object Lock aktiviert ist

Wenn die globale S3-Objektsperre aktiviert ist, unterscheiden sich die Schritte zum Erstellen einer Richtlinie geringfügig. Sie müssen sicherstellen, dass die ILM-Richtlinie die Anforderungen von Buckets erfüllt, für die S3 Object Lock aktiviert ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die globale S3-Objektsperre muss bereits für das StorageGRID-System aktiviert sein.

> Wenn die globale S3-Objektsperre nicht aktiviert wurde, verwenden Sie stattdessen die allgemeinen Anweisungen zum Erstellen einer vorgeschlagenen Richtlinie.
>
> "Erstellen einer vorgeschlagenen ILM-Richtlinie"

- Sie müssen die konformen und nicht konformen ILM-Regeln erstellt haben, die Sie der vorgeschlagenen Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.

  "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

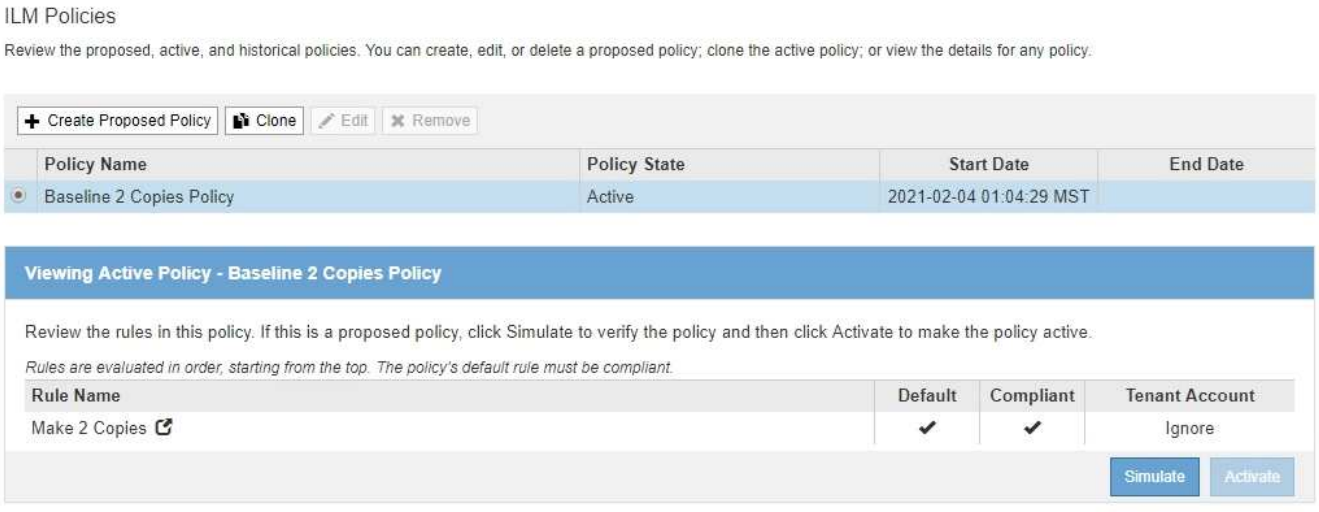
- Sie müssen eine konforme Standard-ILM-Regel für die Richtlinie erstellt haben.

  "Erstellen einer Standard-ILM-Regel"

Schritte

1. Wählen Sie **ILM** > **Richtlinien**.

   Die Seite ILM-Richtlinien wird angezeigt. Wenn die globale S3-Objektsperreneinstellung aktiviert ist, zeigt die Seite ILM-Richtlinien an, welche ILM-Regeln konform sind.



2. Geben Sie im Feld **Name** einen eindeutigen Namen für die vorgeschlagene Richtlinie ein.

   Sie müssen mindestens 1 und nicht mehr als 64 Zeichen eingeben.

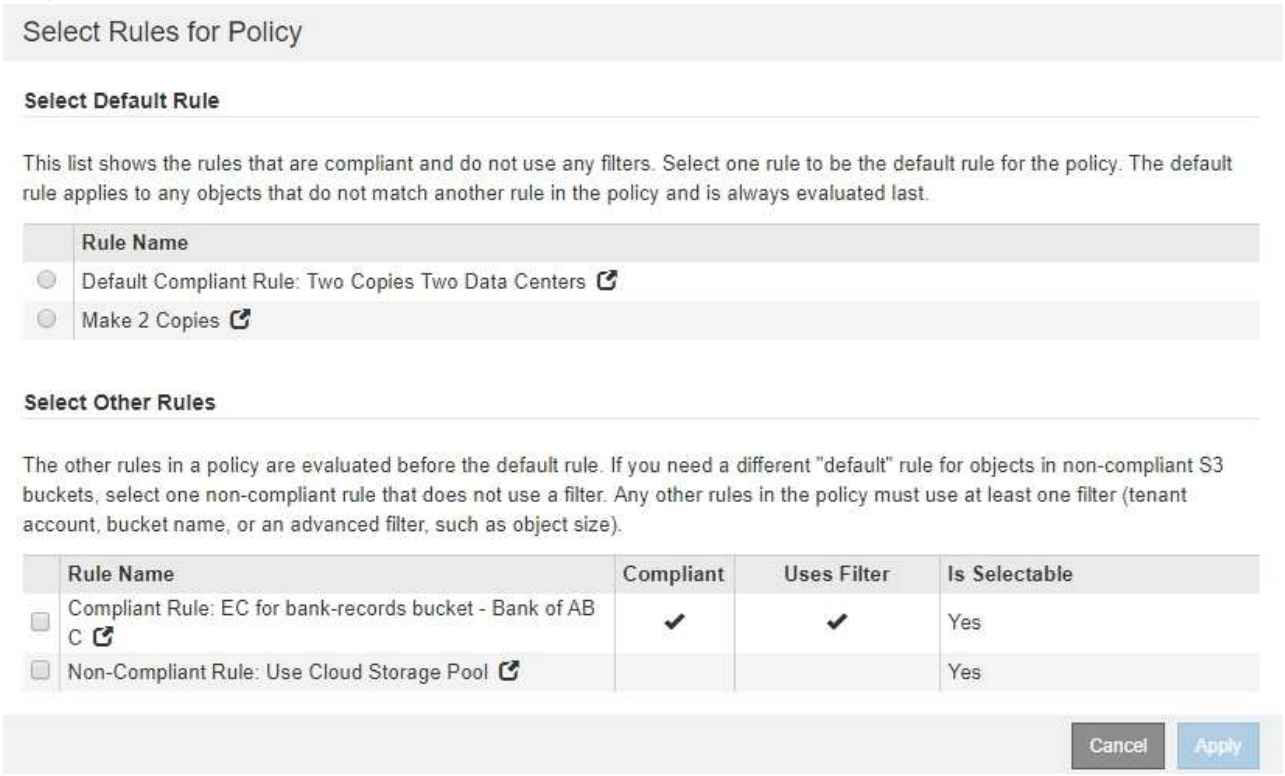
3. Geben Sie im Feld **Grund für Änderung** den Grund für die Erstellung einer neuen Policy ein.

   Sie müssen mindestens 1 und nicht mehr als 128 Zeichen eingeben.

4. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**.

   Das Dialogfeld Regeln für Richtlinie auswählen wird angezeigt, in dem alle definierten Regeln aufgeführt sind.

   - Im Abschnitt Standardregel auswählen werden die Regeln aufgeführt, die für eine konforme Richtlinie standardmäßig gelten können. Es enthält konforme Regeln, die keine Filter verwenden.
   - Im Abschnitt andere Regeln auswählen werden die anderen für diese Richtlinie ausgewählten Compliance- und nicht-konformen Regeln aufgeführt.



5. Wählen Sie einen Regelnamen oder das Symbol für weitere Details aus So zeigen Sie die Einstellungen für diese Regel an:
6. Wählen Sie im Abschnitt **Standardregel auswählen** eine Standardregel für die vorgeschlagene Richtlinie aus.

   In der Tabelle in diesem Abschnitt werden nur die Regeln aufgeführt, die kompatibel sind und keine Filter verwenden.

   > Wenn im Abschnitt Standardregel auswählen keine Regel aufgeführt wird, müssen Sie die Seite ILM-Richtlinie beenden und eine konforme Standardregel erstellen.
   >
   > "Erstellen einer Standard-ILM-Regel"

> Verwenden Sie die Regel „2-Kopien-Bestand erstellen“ nicht 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.

7. Wählen Sie im Abschnitt **Weitere Regeln** alle weiteren Regeln aus, die Sie in die Richtlinie aufnehmen möchten.

   a. Wenn Sie für Objekte in nicht-konformen S3-Buckets eine andere „`default`“-Regel benötigen, wählen Sie optional eine nicht konforme Regel aus, die keinen Filter verwendet.

      Beispielsweise möchten Sie einen Cloud-Storage-Pool oder einen Archiv-Node verwenden, um Objekte in Buckets zu speichern, in denen die S3-Objektsperre nicht aktiviert ist.

      > Sie können nur eine nicht kompatible Regel auswählen, die keinen Filter verwendet. Sobald Sie eine Regel auswählen, wird in der Spalte **ist wählbar Nein** für alle anderen nicht-konformen Regeln ohne Filter angezeigt.

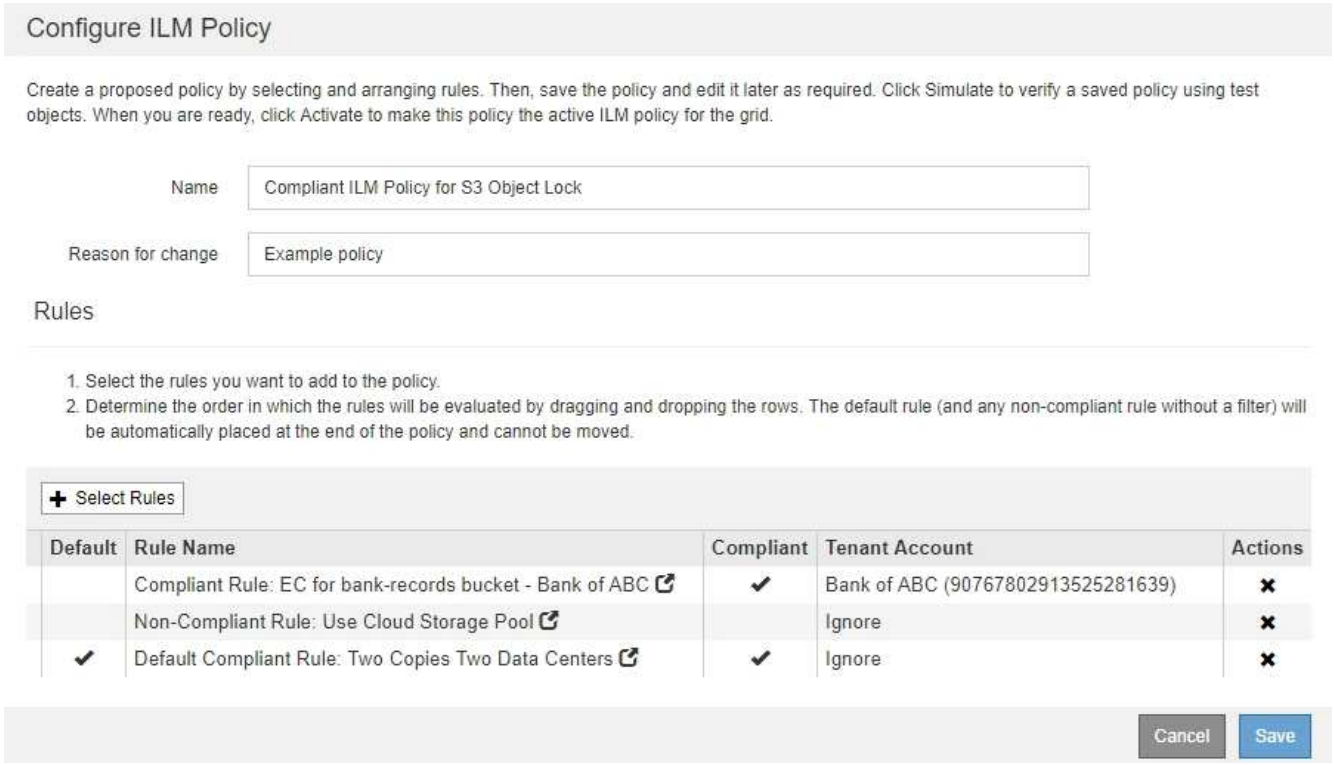
   a. Wählen Sie alle anderen konformen oder nicht konformen Regeln aus, die Sie in der Richtlinie verwenden möchten.

      Die anderen Regeln müssen mindestens einen Filter verwenden (Mandantenkonto, Bucket-Name oder erweiterte Filter, wie Objektgröße).

8. Wenn Sie die Regeln ausgewählt haben, wählen Sie **Anwenden**.

   Die ausgewählten Regeln werden aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber. Wenn Sie auch eine nicht-konforme Regel „`default`“ ausgewählt haben, wird diese Regel als zweite zu letzte Regel in der Richtlinie hinzugefügt.

   In diesem Beispiel ist die letzte Regel, 2 Kopien 2 Rechenzentren, die Standardregel: Sie ist kompatibel und hat keine Filter. Die zweite bis letzte Regel – Cloud Storage Pool – verfügt ebenfalls über keine Filter, ist aber nicht konform.



.

9. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln per Drag-and-Drop, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

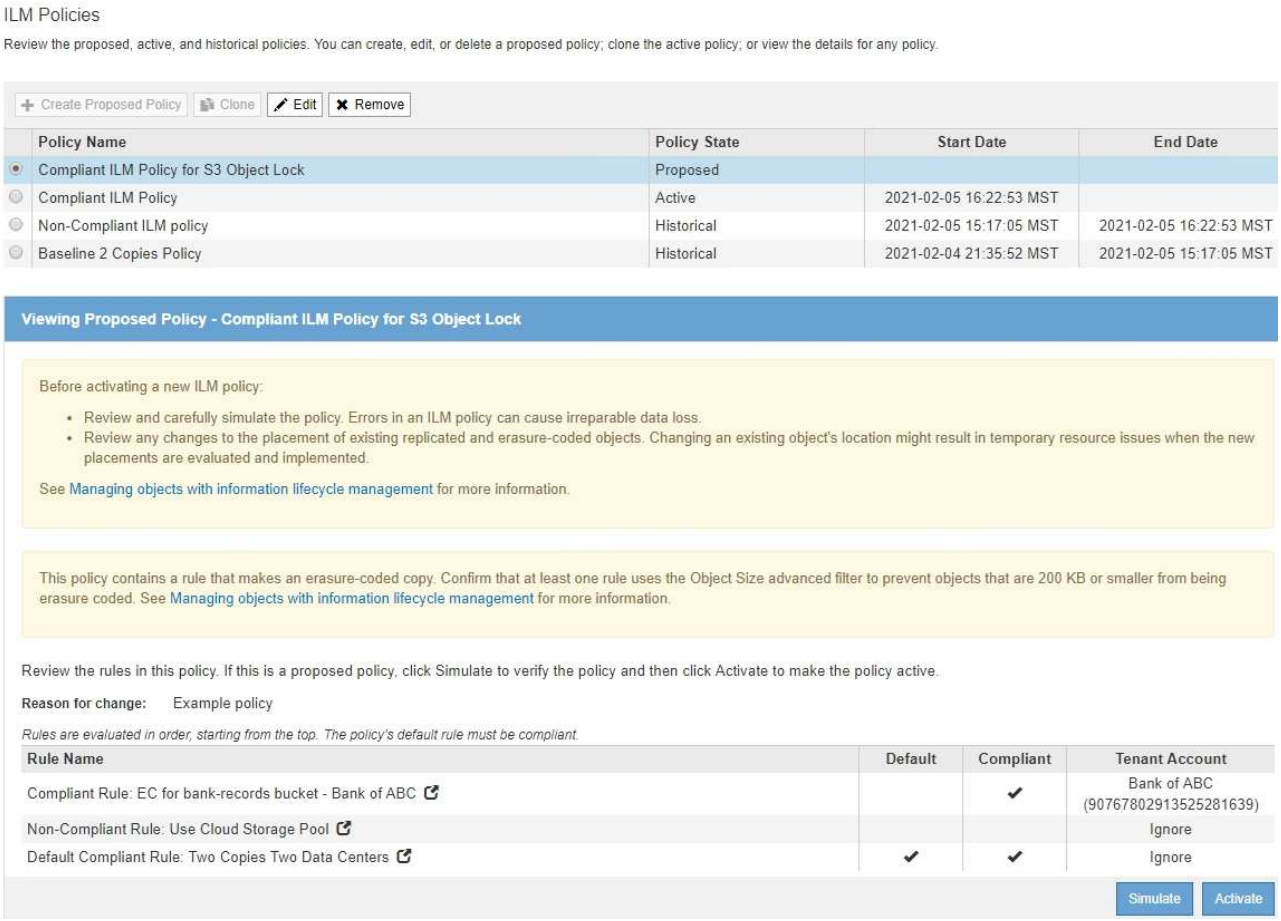
   Sie können die Standardregel oder die nicht-konforme Regel „`default`“ nicht verschieben.

   > 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.

10. Klicken Sie bei Bedarf auf das Löschsymbol ✖ Wenn Sie Regeln löschen möchten, die in der Richtlinie nicht enthalten sein sollen, oder wählen Sie **Regeln auswählen**, um weitere Regeln hinzuzufügen.
11. Wenn Sie fertig sind, wählen Sie **Speichern**.

    Die Seite ILM-Richtlinien wird aktualisiert:

    - Die von Ihnen gespeicherte Richtlinie wird als Vorschlag angezeigt. Die vorgeschlagenen Richtlinien haben kein Start- und Enddatum.
    - Die Schaltflächen **Simulate** und **Activate** sind aktiviert.



12. Gehen Sie zu "Simulation einer ILM-Richtlinie".

Simulation einer ILM-Richtlinie

Sie sollten eine vorgeschlagene Richtlinie für Testobjekte simulieren, 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen den S3-Bucket/Objektschlüssel oder den Swift-Container/Objektnamen für jedes Objekt, das Sie testen möchten, kennen und diese Objekte bereits aufgenommen haben.

Über diese Aufgabe

Sie müssen sorgfältig die Objekte auswählen, 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. Wenn die Richtlinie eine Standardregel zum Platzieren aller anderen Objekte enthält, müssen Sie mindestens ein Objekt aus einem anderen Bucket 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.
- Auf der Seite Simulation werden die von Ihnen getesteten Objekte gespeichert, bis Sie die Seite ILM-Richtlinien schließen, wegnavigieren oder aktualisieren.
- Simulation gibt den Namen der übereinstimmenden Regel zurück. Um festzustellen, welcher Speicherpool oder welches Erasure-Coding-Profil wirksam ist, können Sie das Aufbewahrungsdiagramm anzeigen, indem Sie auf den Regelnamen oder das Detailsymbol klicken .
- Wenn die S3-Versionierung aktiviert ist, wird die Richtlinie nur mit der aktuellen Objektversion simuliert.

Schritte

1. Wählen Sie die Regeln aus und ordnen Sie sie an, und speichern Sie die vorgeschlagene Richtlinie.

   Die Richtlinie in diesem Beispiel hat drei Regeln:

Regelname	Filtern	Kopentyp	Aufbewahrung
X-men	• Mandant A • Benutzer-Metadaten (Serie=x-men)	2 Kopien in zwei Rechenzentren	2 Jahre
PNGs	Die Schlüssel enden mit .png	2 Kopien in zwei Rechenzentren	5 Jahre
Zwei Kopien Zwei Datacenter	*Keine*	2 Kopien in zwei Rechenzentren	Für Immer

2. Klicken Sie Auf **Simulieren**.

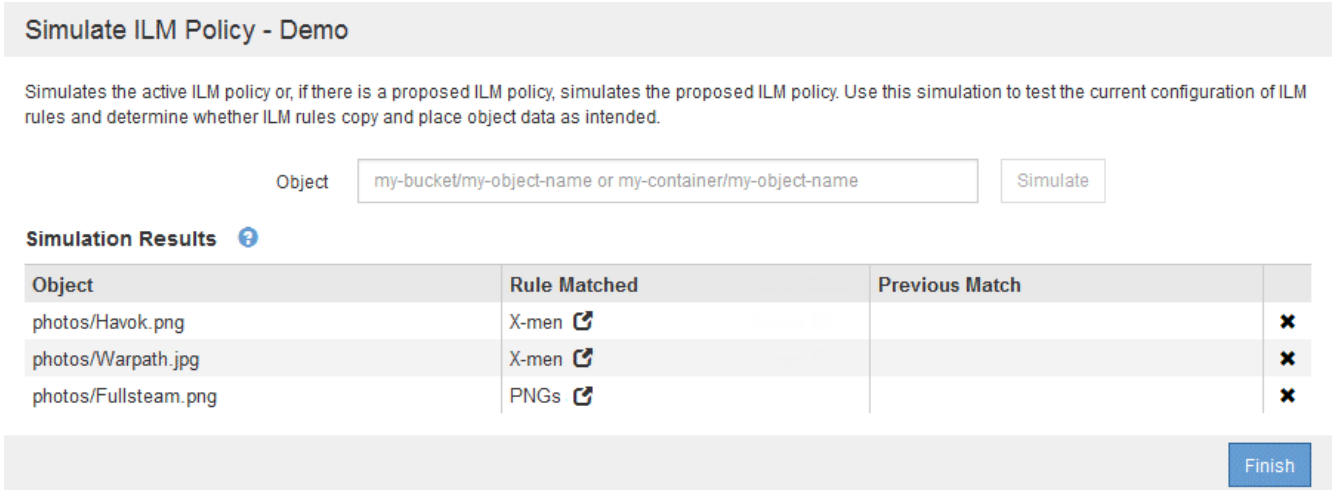
Das Dialogfeld Simulation ILM-Richtlinie wird angezeigt.

3. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und klicken Sie auf **Simulate**.

> Wenn Sie ein Objekt angeben, das nicht aufgenommen wurde, wird eine Meldung angezeigt.

4. Bestätigen Sie unter **Simulationsergebnisse**, dass jedes Objekt mit der richtigen Regel übereinstimmt.

   In dem Beispiel wird der verwendet `Havok.png` Und `Warpath.jpg` Objekte wurden durch die X-Men-Regel korrekt abgeglichen. Der `Fullsteam.png` Objekt, das nicht enthält `series=x-men` Benutzermetadaten, wurde nicht mit der X-Men-Regel abgeglichen, wurde aber von der PNGs-Regel korrekt abgeglichen. Die Standardregel wurde nicht verwendet, da alle drei Objekte mit anderen Regeln abgeglichen wurden.



Beispiele für die Simulation von ILM-Richtlinien

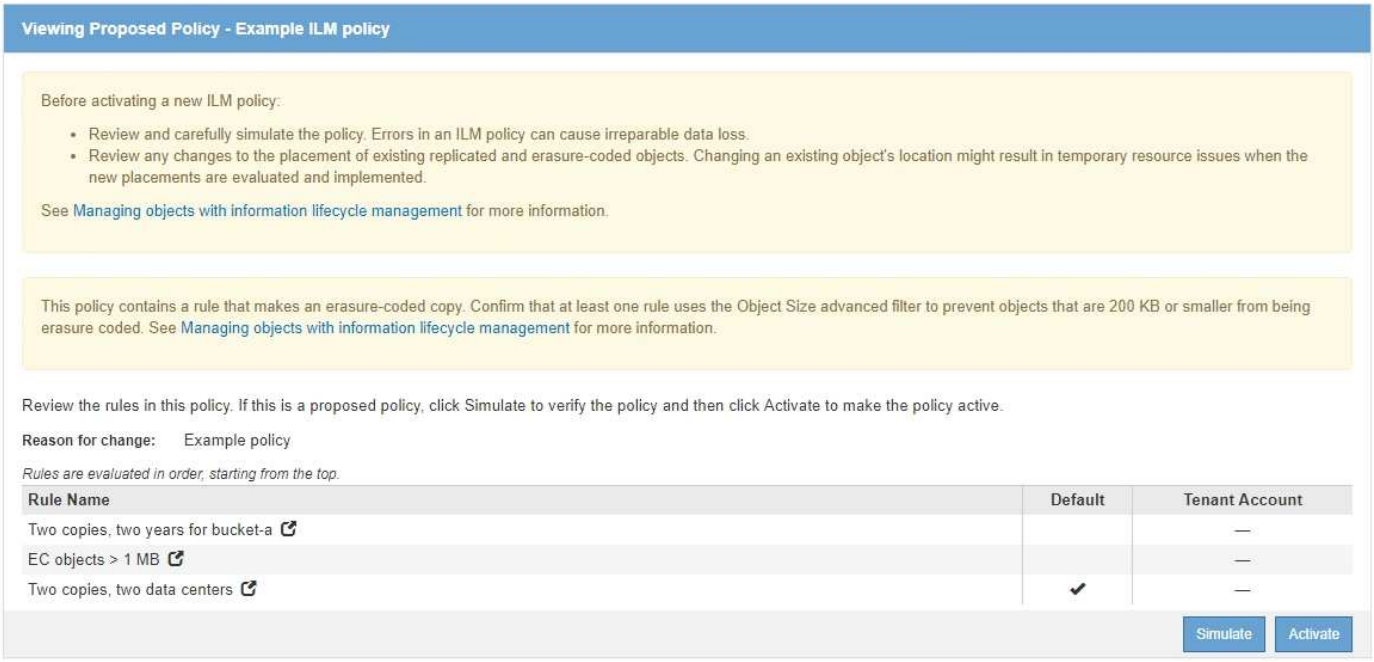
Diese Beispiele zeigen, wie Sie ILM-Regeln durch Simulation der ILM-Richtlinie vor der Aktivierung überprüfen können.

Beispiel 1: Überprüfung der Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, 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 Objects › 1 MB**, gilt für alle Buckets, aber für Filter auf Objekten größer als 1 MB.
- Die dritte Regel ist die Standardregel und enthält keine Filter.



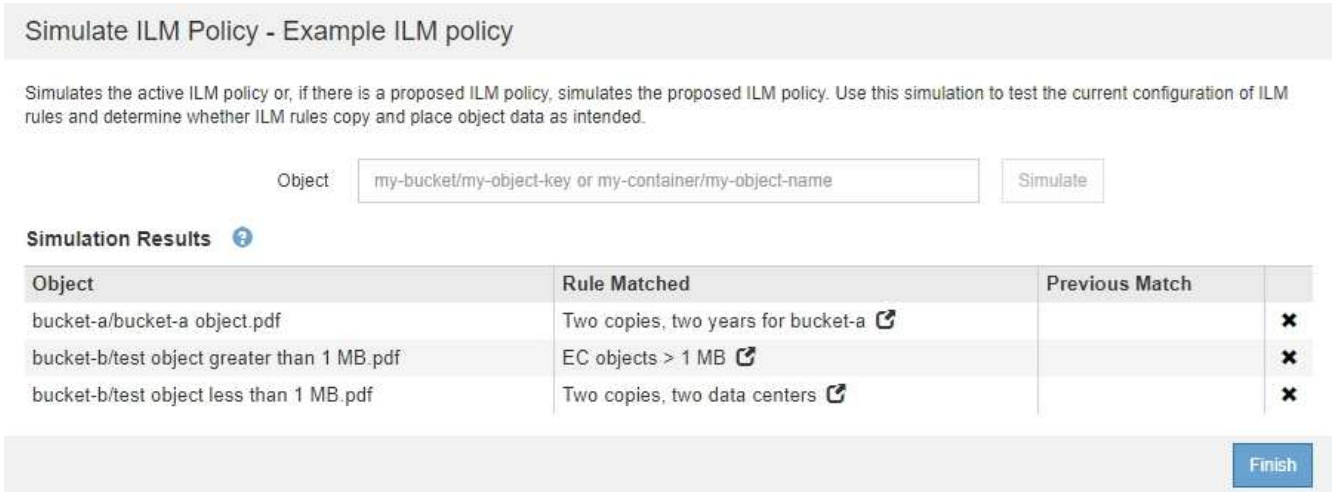
Schritte

1. Klicken Sie nach dem Hinzufügen der Regeln und dem Speichern der Richtlinie auf **Simulieren**.

   Das Dialogfeld ILM-Richtlinie simulieren wird angezeigt.

2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und klicken Sie auf **Simulate**.

   Die Simulationsergebnisse werden angezeigt und zeigen an, welche Regel in der Richtlinie zu jedem getesteten Objekt passt.



3. Vergewissern Sie sich, dass jedes Objekt mit der richtigen Regel übereinstimmt.

   In diesem Beispiel:

   a. `bucket-a/bucket-a object.pdf` Die erste Regel, die nach Objekten in filtert, wurde richtig zugeordnet `bucket-a`.

   b. `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.

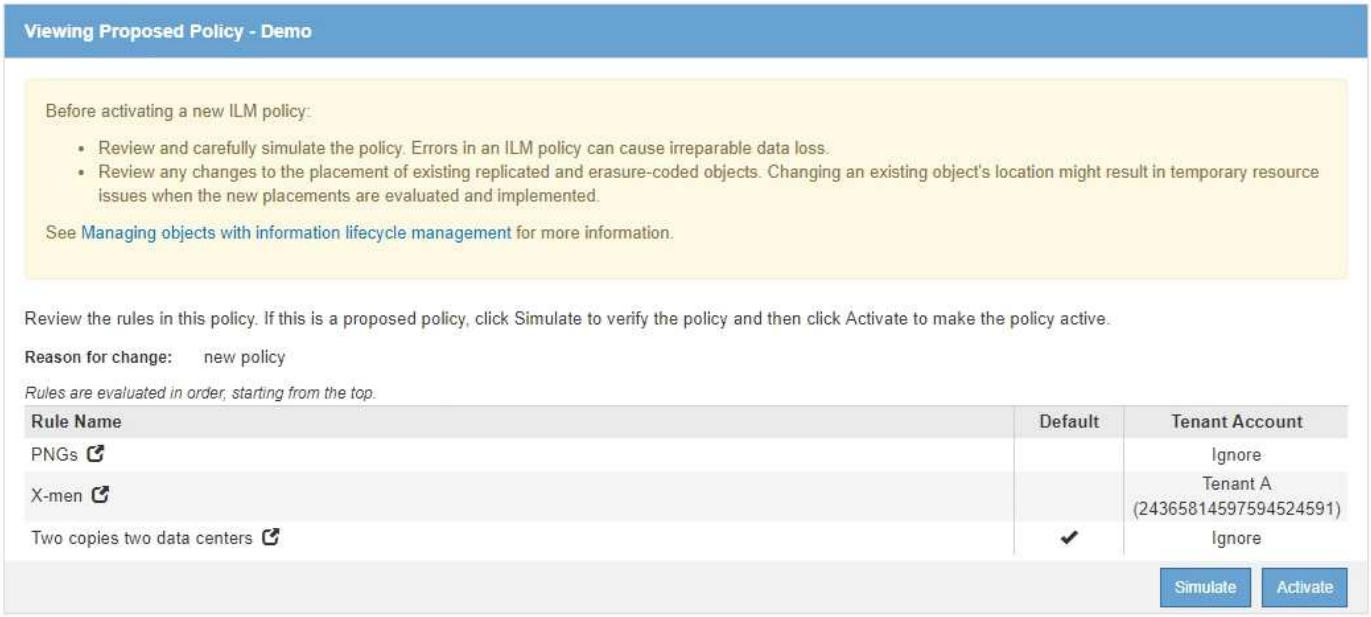
c. `bucket-b/test object less than 1 MB.pdf` Stimmt nicht mit den Filtern in den ersten beiden Regeln überein, so wird sie durch die Standardregel platziert, die keine Filter enthält.

Beispiel 2: Neuanordnung von Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, wie Sie Regeln neu anordnen können, um die Ergebnisse bei der Simulation einer Richtlinie zu ändern.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die zum Auffinden von Objekten mit Metadaten für Benutzer der Serie=x-men bestimmt ist, enthält drei Regeln:

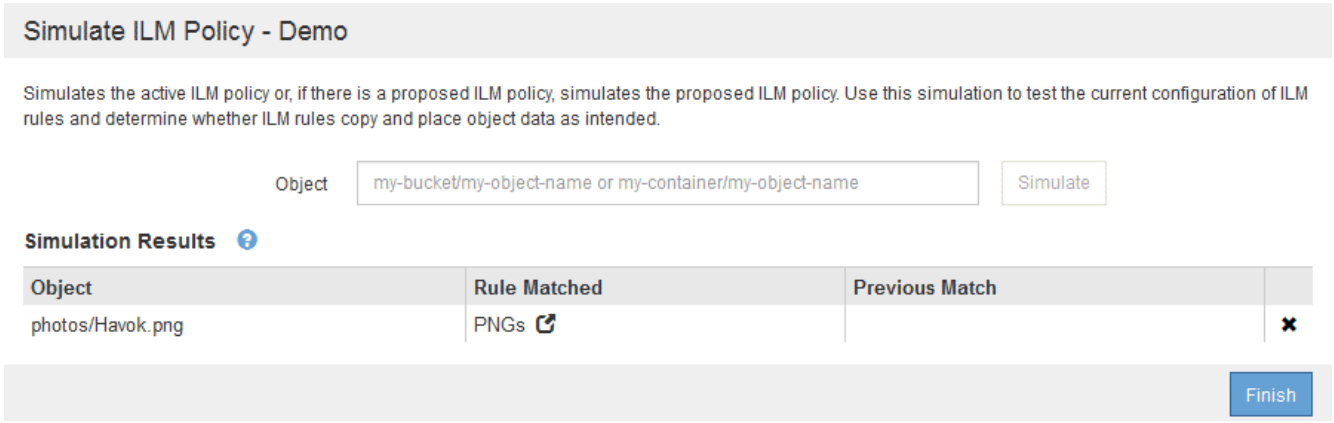
- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die enden `.png`.
- Die zweite Regel, **X-Men**, gilt nur für Objekte für Mieter A und Filter für `series=x-men` Benutzer-Metadaten:
- Die letzte Regel, **zwei Kopien zwei Rechenzentren**, ist die Standardregel, die alle Objekte, die nicht mit den ersten beiden Regeln übereinstimmen, übereinstimmt.



Schritte

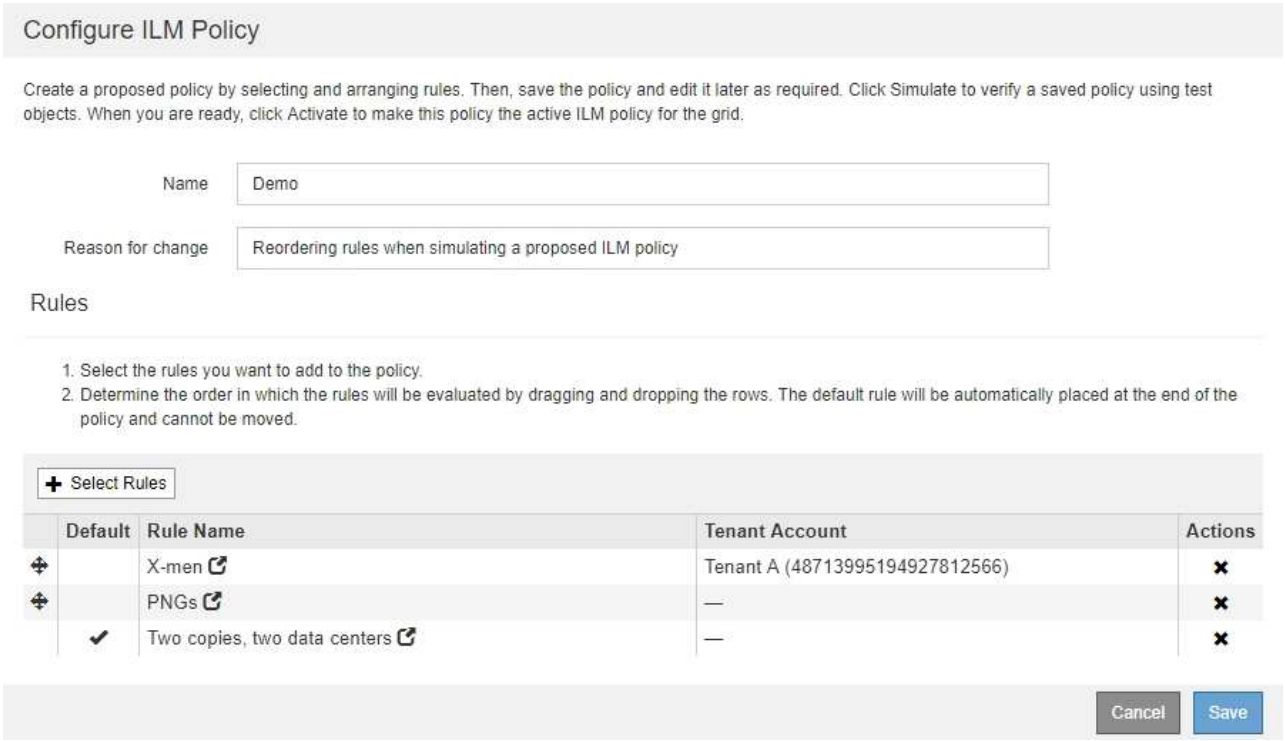
1. Klicken Sie nach dem Hinzufügen der Regeln und dem Speichern der Richtlinie auf **Simulieren**.
2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und klicken Sie auf **Simulate**.

   Die Simulationsergebnisse werden angezeigt, wobei das angezeigt wird `Havok.png` Das Objekt wurde durch die **PNGs**-Regel abgeglichen.



Allerdings die Regel, dass die `Havok.png` Das Objekt war für den Test die **X-Men**-Regel gedacht.

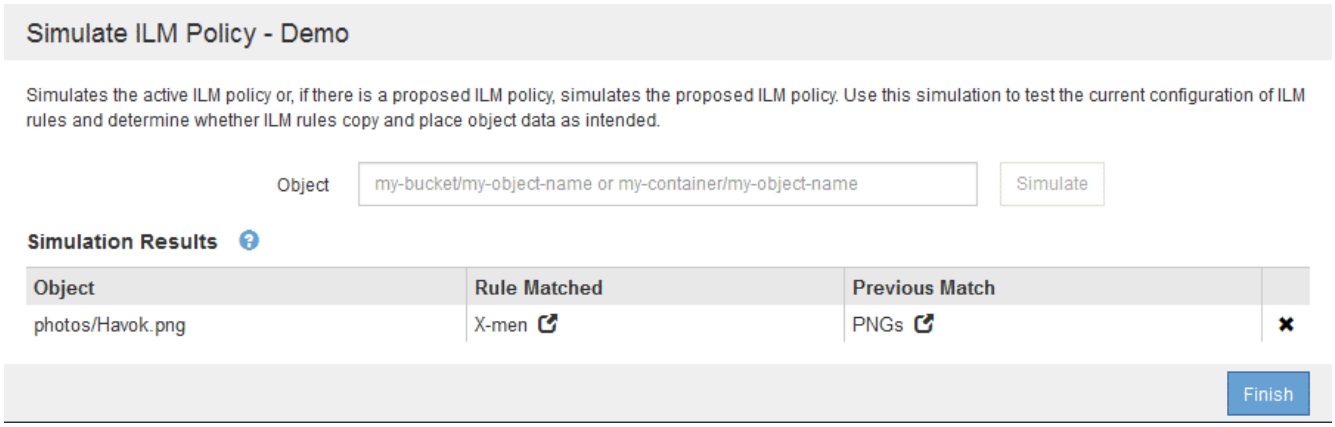
3. Um das Problem zu lösen, ordnen Sie die Regeln neu an.
   a. Klicken Sie auf **Fertig stellen**, um die Seite ILM-Richtlinie simulieren zu schließen.
   b. Klicken Sie auf **Bearbeiten**, um die Richtlinie zu bearbeiten.
   c. Ziehen Sie die **X-Men**-Regel an den Anfang der Liste.



   d. Klicken Sie Auf **Speichern**.

4. Klicken Sie Auf **Simulieren**.

   Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie neu bewertet und die neuen Simulationsergebnisse angezeigt. Im Beispiel wird in der Spalte Regel zugeordnet das angezeigt `Havok.png` Das Objekt entspricht jetzt wie erwartet der X-Men-Metadatenregel. Die Spalte Vorheriger Abgleich zeigt an, dass die PNGs-Regel mit dem Objekt in der vorherigen Simulation übereinstimmt.

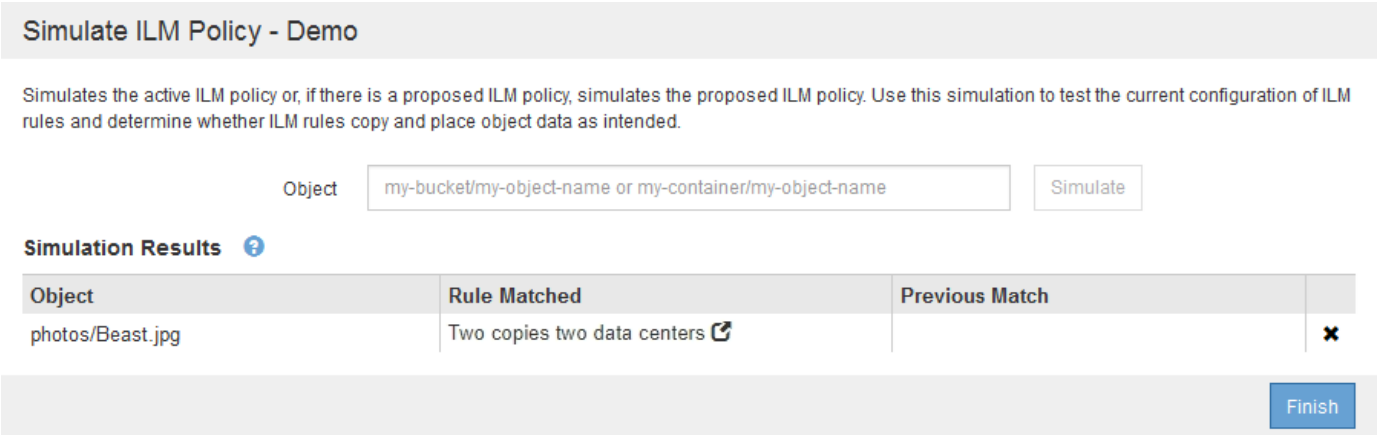


Wenn Sie auf der Seite Richtlinien konfigurieren bleiben, können Sie eine Richtlinie nach Änderungen erneut simulieren, ohne die Namen der Testobjekte erneut eingeben zu müssen.

Beispiel 3: Korrektur einer Regel bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, wie eine Richtlinie simuliert, eine Regel in der Richtlinie korrigiert und die Simulation fortgesetzt wird.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie dient zum Suchen von Objekten, die über solche verfügen `series=x-men` Benutzer-Metadaten: Bei der Simulation dieser Richtlinie gegen die traten jedoch unerwartete Ergebnisse auf `Beast.jpg` Objekt: Anstatt die X-Men-Metadatenregel zu entsprechen, kopiert das Objekt die Standardregel. Zwei Rechenzentren werden kopiert.

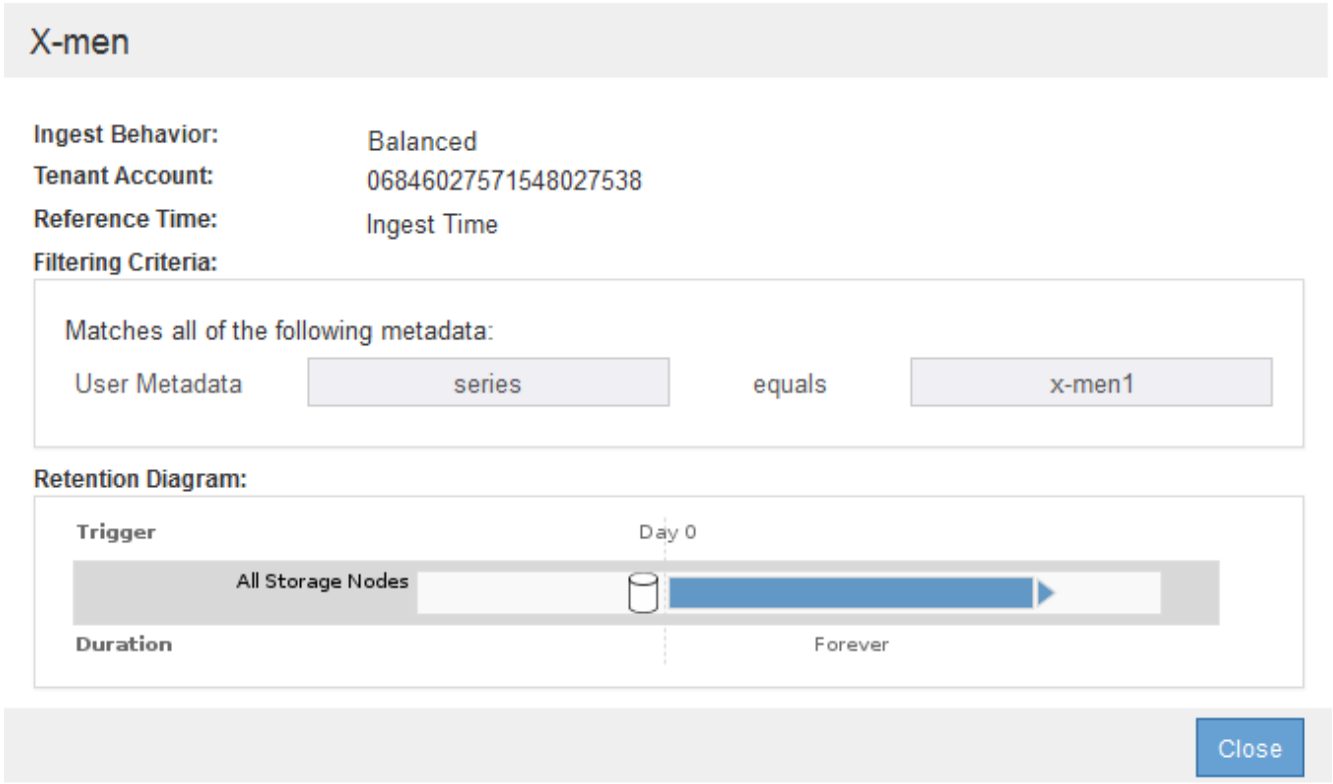


Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, müssen Sie jede Regel in der Richtlinie überprüfen und eventuelle Fehler korrigieren.

Schritte

1. Zeigen Sie für jede Regel in der Richtlinie die Regeleinstellungen an, indem Sie auf den Regelnamen oder das Symbol Weitere Details klicken In jedem Dialogfeld, in dem die Regel angezeigt wird.
2. Prüfen Sie das Mandantenkonto der Regel, die Referenzzeit und die Filterkriterien.

   In diesem Beispiel enthält die Metadaten für die X-Men-Regel einen Fehler. Der Metadatenwert wurde als „`x-men1`“ 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 eine Regel nicht bearbeiten oder aus der aktiven Richtlinie entfernen.

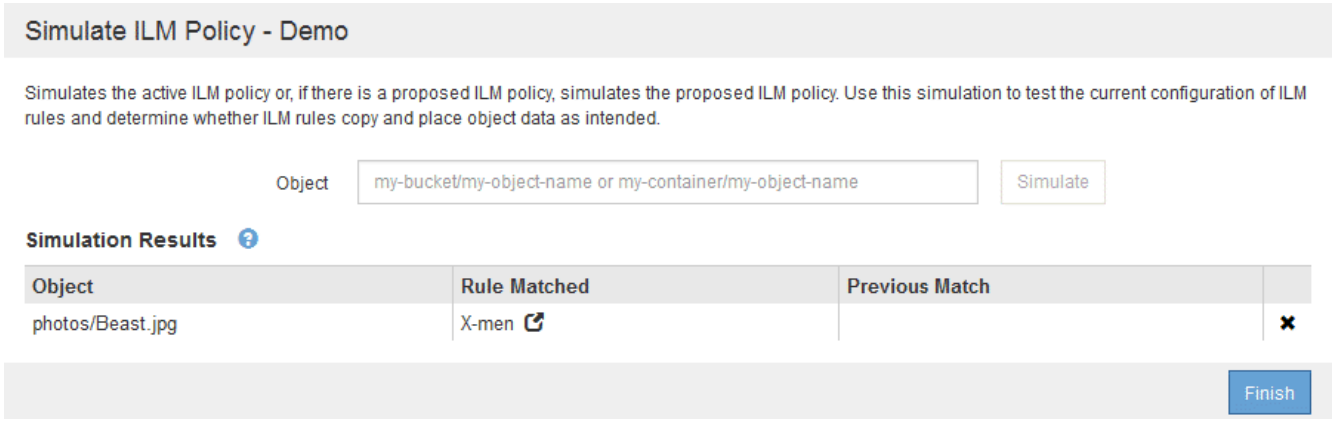
Option	Beschreibung
Klonen der Regel	i. Wählen Sie **ILM** > **Regeln**. ii. Wählen Sie die falsche Regel aus, und klicken Sie auf **Clone**. iii. Ändern Sie die falschen Informationen, und klicken Sie auf **Speichern**. iv. Wählen Sie **ILM** > **Richtlinien**. v. Wählen Sie die vorgeschlagene Richtlinie aus, und klicken Sie auf **Bearbeiten**. vi. Klicken Sie Auf **Regeln Auswählen**. vii. Aktivieren Sie das Kontrollkästchen für die neue Regel, deaktivieren Sie das Kontrollkästchen für die ursprüngliche Regel, und klicken Sie auf **Anwenden**. viii. Klicken Sie Auf **Speichern**.

Option	Beschreibung
Bearbeiten der Regel	i. Wählen Sie die vorgeschlagene Richtlinie aus, und klicken Sie auf **Bearbeiten**. ii. Klicken Sie auf das Löschsymbol ✖ Um die falsche Regel zu entfernen, und klicken Sie auf **Speichern**. iii. Wählen Sie **ILM** > **Regeln**. iv. Wählen Sie die falsche Regel aus, und klicken Sie auf **Bearbeiten**. v. Ändern Sie die falschen Informationen, und klicken Sie auf **Speichern**. vi. Wählen Sie **ILM** > **Richtlinien**. vii. Wählen Sie die vorgeschlagene Richtlinie aus, und klicken Sie auf **Bearbeiten**. viii. Wählen Sie die korrigierte Regel aus, klicken Sie auf **Anwenden** und klicken Sie auf **Speichern**.

4. Führen Sie die Simulation erneut aus.

> Da Sie zur Bearbeitung der Regel nicht mehr auf der Seite ILM-Richtlinien navigiert haben, werden die zuvor für die Simulation eingegebenen Objekte nicht mehr angezeigt. Sie müssen die Namen der Objekte erneut eingeben.

In diesem Beispiel entspricht die korrigierte X-Men-Regel nun dem `Beast.jpg` Objekt auf Grundlage des `series=x-men` Benutzer-Metadaten, wie erwartet.



Aktivieren der 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die vorgeschlagene ILM-Richtlinie gespeichert und simuliert haben.

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.

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.

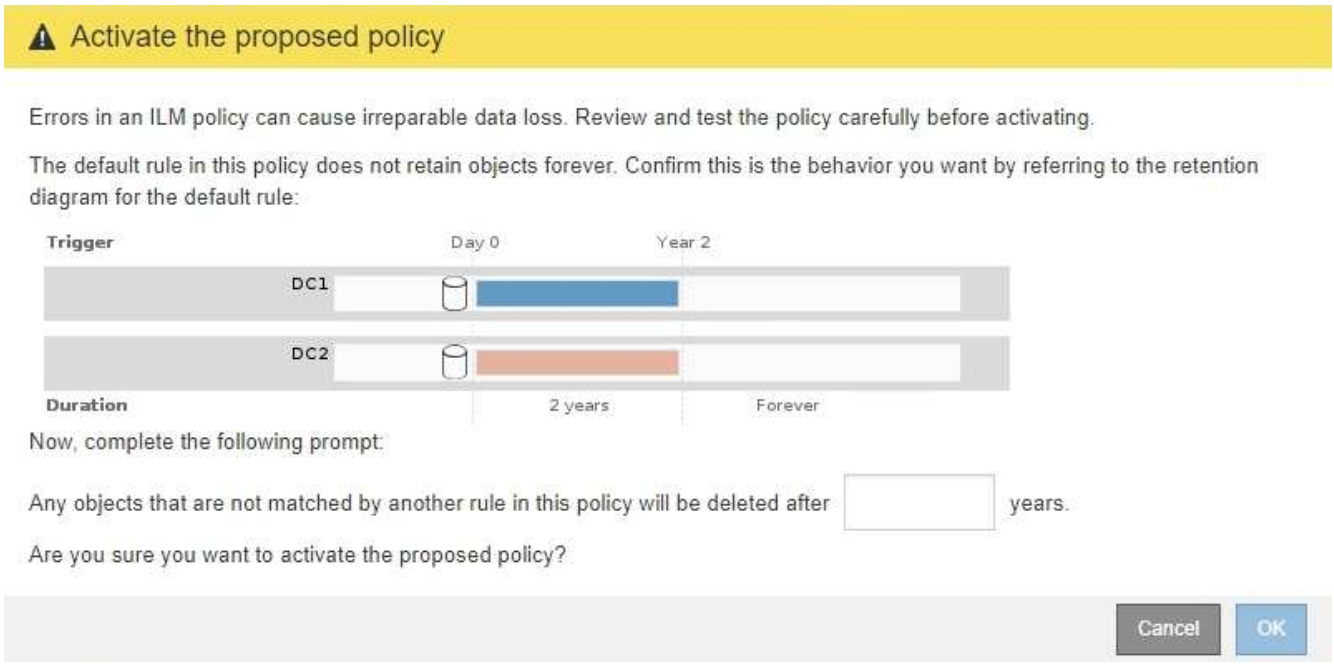
- Nehmen Richtlinienänderungen vor, die die Datenredundanz oder Aufbewahrungszeit verbessern, werden diese Änderungen sofort implementiert. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit drei Kopien anstelle einer Regel mit zwei Kopien enthält, wird diese Richtlinie sofort 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 als „`aktiv,`“ gekennzeichnet. Sie wird jedoch nicht wirksam, bis alle Knoten online und verfügbar sind.

Schritte

1. Wenn Sie bereit sind, eine vorgeschlagene Richtlinie zu aktivieren, wählen Sie die Richtlinie auf der Seite ILM-Richtlinien aus, und klicken Sie auf **Aktivieren**.

   Es wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, zu bestätigen, dass Sie die vorgeschlagene Richtlinie aktivieren möchten.

   Eine Eingabeaufforderung wird in der Warnmeldung angezeigt, wenn die Standardregel für die Richtlinie Objekte nicht für immer enthält. In diesem Beispiel zeigt das Aufbewahrungsdiagramm, dass die Standardregel Objekte nach 2 Jahren löscht. Sie müssen **2** in das Textfeld eingeben, um zu bestätigen, dass Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmt, nach 2 Jahren aus StorageGRID entfernt werden.

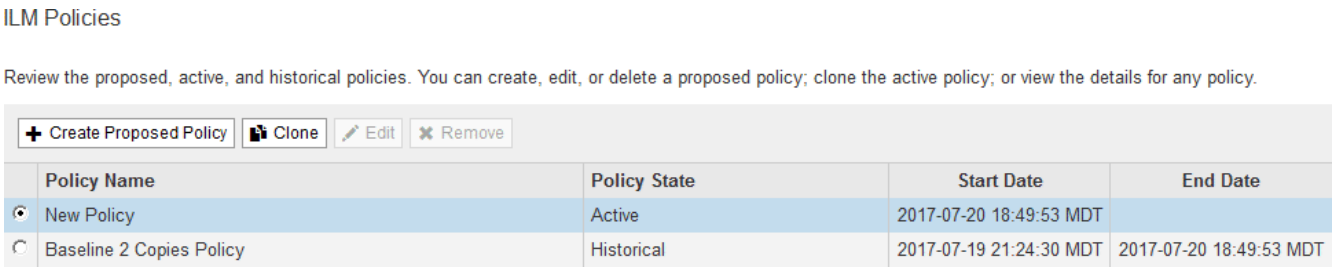


2. Klicken Sie auf **OK**.

Ergebnis

Wenn eine neue ILM-Richtlinie aktiviert wurde:

- Die Richtlinie wird in der Tabelle auf der Seite ILM-Richtlinien mit einem Status von „aktiv“ angezeigt. Der Eintrag Startdatum gibt das Datum und die Uhrzeit an, zu der die Richtlinie aktiviert wurde.



- Die zuvor aktive Richtlinie wird mit dem Status „Historische Richtlinien“ angezeigt. Die Einträge Startdatum und Enddatum geben an, wann die Richtlinie aktiv wurde und wann sie nicht mehr wirksam 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.

Was Sie benötigen

- 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**: Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
- **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** > **Objekt Metadaten Lookup** aus.
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. Klicken Sie Auf **Look Up**.

   Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

   - Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
   - Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
   - Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
   - Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
   - Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
   - Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
   - Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
   - Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

     Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


5. 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-Prüfmeldung kann Ihnen mehr Informationen über den Status des ILM-Auswertungsprozesses zur Verfügung stellen, jedoch kann sie Ihnen keine Informationen über die Richtigkeit der Platzierung der Objektdaten oder die Vollständigkeit der ILM-Richtlinie liefern. Das müssen Sie selbst beurteilen. Weitere Informationen finden Sie in den Informationen zum Verständnis von Überwachungsmeldungen.

Verwandte Informationen

"Prüfung von Audit-Protokollen"

"S3 verwenden"

"Verwenden Sie Swift"

Sobald Sie ILM-Regeln und eine ILM-Richtlinie erstellt haben, können Sie sie weiterhin verwenden und ihre Konfiguration an die sich ändernden Storage-Anforderungen anpassen.

Löschen einer ILM-Regel

Löschen Sie alle ILM-Regeln, die Sie wahrscheinlich nicht verwenden, um die Liste der aktuellen ILM-Regeln überschaubar zu halten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

> Eine ILM-Regel kann nicht gelöscht werden, wenn sie derzeit in der aktiven Richtlinie oder in der vorgeschlagenen Richtlinie verwendet wird. Wenn Sie eine ILM-Regel löschen müssen, die eine Richtlinie verwendet, müssen Sie zuerst die folgenden Schritte durchführen:
>
> 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.

Schritte

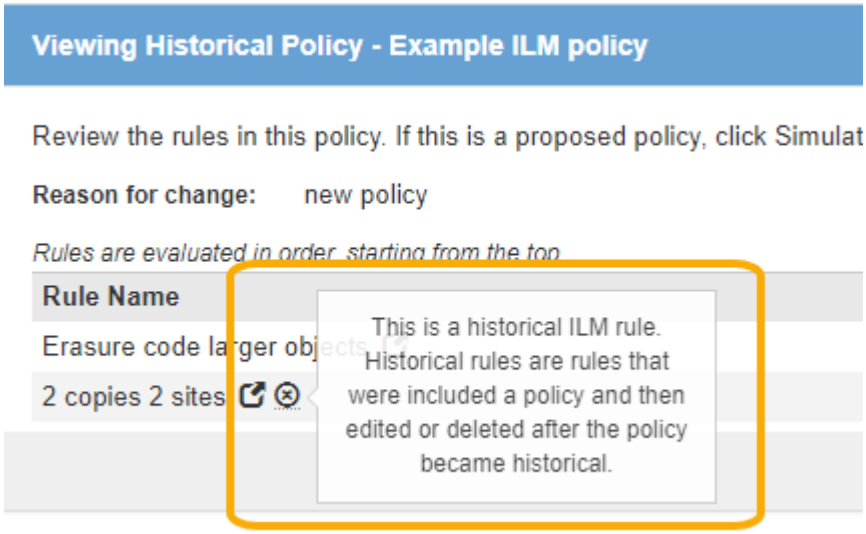
1. Wählen Sie **ILM** > **Regeln**.
2. Überprüfen Sie den Tabelleneintrag für die Regel, die Sie entfernen möchten.

   Vergewissern Sie sich, dass die Regel nicht in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.

3. Wenn die Regel, die Sie entfernen möchten, nicht verwendet wird, wählen Sie die Optionsschaltfläche und wählen Sie **Entfernen**.
4. Wählen Sie **OK** aus, um zu bestätigen, dass Sie die ILM-Regel löschen möchten.

   Die ILM-Regel wird gelöscht.

Wenn Sie eine Regel löschen, die in einer historischen Richtlinie verwendet wird, wird ein ⊗ Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.



Verwandte Informationen

"ILM-Richtlinie erstellen"

Bearbeiten einer ILM-Regel

Möglicherweise müssen Sie eine ILM-Regel bearbeiten, um einen Filter oder eine Platzierungsanweisung zu ändern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

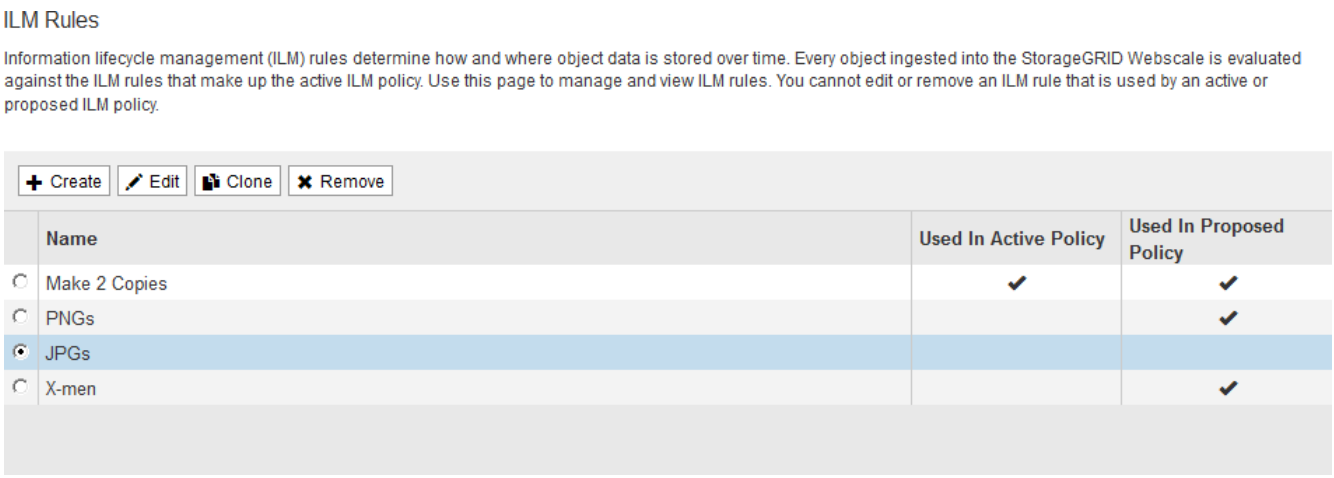
Eine Regel kann nicht bearbeitet werden, wenn sie in der vorgeschlagenen ILM-Richtlinie oder der aktiven ILM-Richtlinie verwendet wird. Stattdessen können Sie diese Regeln klonen und erforderliche Änderungen an der geklonten Kopie vornehmen. Sie können auch die ILM-Regel (2 Kopien erstellen) oder ILM-Regeln, die vor StorageGRID Version 10.3 erstellt wurden, nicht bearbeiten.

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**.

   Die Seite ILM-Regeln wird angezeigt. Diese Seite zeigt alle verfügbaren Regeln an und gibt an, welche Regeln in der aktiven Richtlinie oder in der vorgeschlagenen Richtlinie verwendet werden.



2. Wählen Sie eine Regel aus, die nicht verwendet wird, und klicken Sie auf **Bearbeiten**.

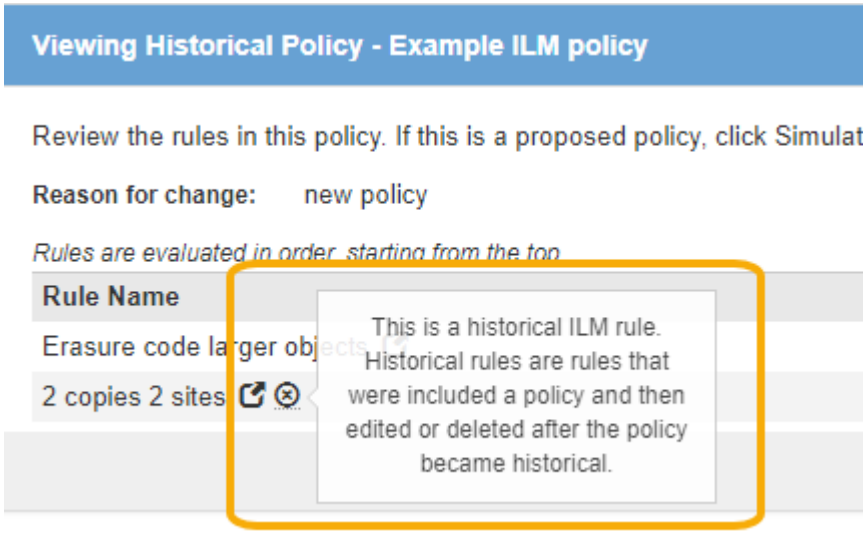
   Der Assistent zum Bearbeiten der ILM-Regel wird geöffnet.

3. Füllen Sie die Seiten des Assistenten zur Bearbeitung von ILM-Regeln aus und befolgen Sie die Schritte zum Erstellen einer ILM-Regel, und verwenden Sie gegebenenfalls erweiterte Filter.

   Beim Bearbeiten einer ILM-Regel können Sie ihren Namen nicht ändern.

4. Klicken Sie Auf **Speichern**.

Wenn Sie eine Regel bearbeiten, die in einer historischen Richtlinie verwendet wird, wird ein ⊗ Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.



Verwandte Informationen

"Erstellen einer ILM-Regel"

"Verwendung erweiterter Filter in ILM-Regeln"

Klonen einer ILM-Regel

Eine Regel kann nicht bearbeitet werden, 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 keine ILM-Regel klonen, wenn sie mit StorageGRID Version 10.2 oder früher erstellt wurde.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

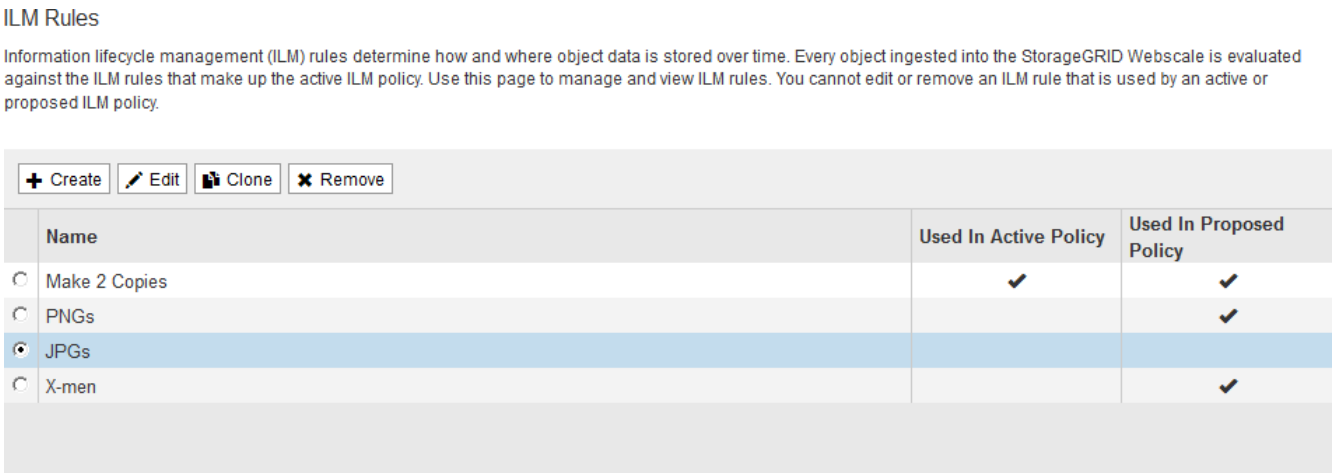
Über diese Aufgabe

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**.

   Die Seite ILM-Regeln wird angezeigt.



2. Wählen Sie die ILM-Regel aus, die Sie klonen möchten, und klicken Sie auf **Clone**.

   Der Assistent für die Erstellung von ILM-Regeln wird geöffnet.

3. Aktualisieren Sie die geklonte Regel, indem Sie die Schritte zum Bearbeiten einer ILM-Regel und Verwenden erweiterter Filter ausführen.

   Beim Klonen einer ILM-Regel müssen Sie einen neuen Namen eingeben.

4. Klicken Sie Auf **Speichern**.

   Die neue ILM-Regel wird erstellt.

Verwandte Informationen

"Arbeiten mit ILM-Regeln und ILM-Richtlinien"

"Verwendung erweiterter Filter in ILM-Regeln"

Anzeigen der Aktivitätswarteschlange für ILM-Richtlinien

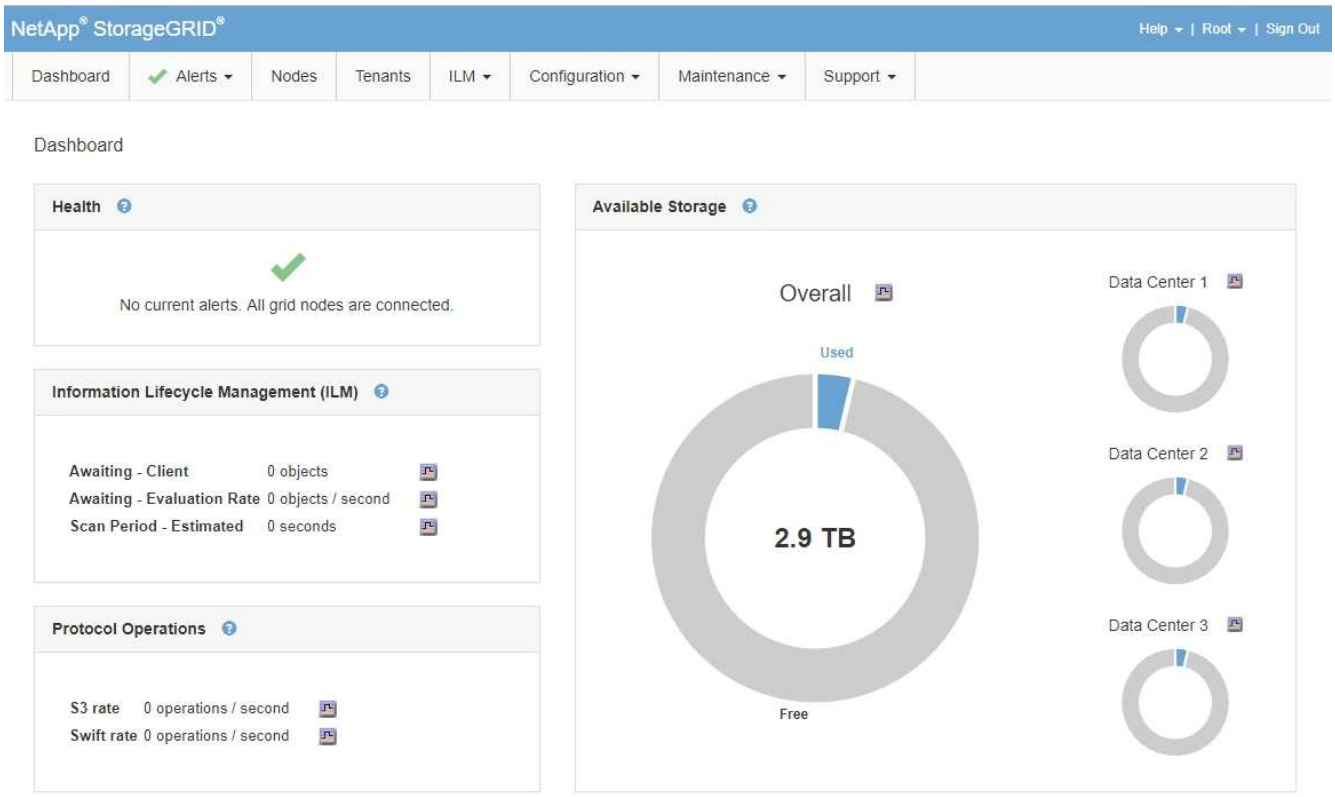
Sie können jederzeit die Anzahl der Objekte anzeigen, die sich in der Warteschlange befinden, die mit der ILM-Richtlinie bewertet werden sollen. Möglicherweise möchten Sie die ILM-Verarbeitungswarteschlange überwachen, um die System-Performance zu ermitteln. Eine große Warteschlange könnte darauf hindeuten, dass das System nicht mit der Aufnahmerate Schritt halten kann, dass die Last von den Client-Anwendungen zu groß ist oder dass ein anormaler Zustand vorhanden ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Dashboard**.



2. Überwachen Sie den Abschnitt Information Lifecycle Management (ILM).

   Sie können auf das Fragezeichen klicken Um eine Beschreibung der Elemente in diesem Abschnitt anzuzeigen.

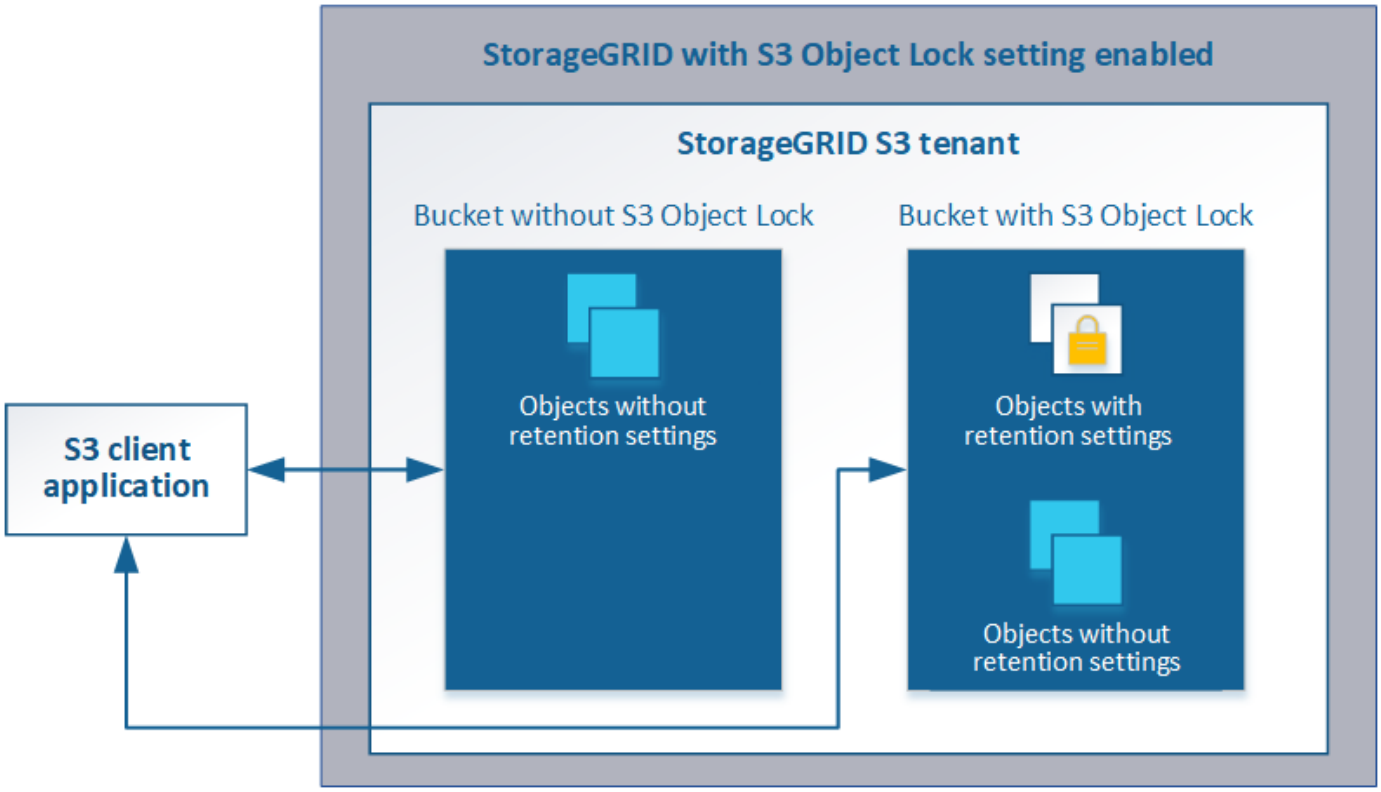
Verwalten von Objekten mit S3 Object Lock

Als Grid-Administrator können Sie die S3 Objektsperre für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren. So wird sichergestellt, dass Objekte in bestimmten S3-Buckets nicht für eine bestimmte Zeit 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 in einem Bucket S3-Objektsperre aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion in diesem Bucket angeben. Eine Objektversion muss über Aufbewahrungseinstellungen verfügen, die durch S3 Object Lock geschützt werden sollen.



Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

Wenn in einem Bucket S3-Objektsperre aktiviert ist, kann die S3-Client-Applikation beim Erstellen oder Aktualisieren eines Objekts optional eine oder beide der folgenden Aufbewahrungseinstellungen auf Objektebene angeben:

- **Bis-Datum aufbewahren**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Bei Bedarf kann das Aufbewahrungsdatum eines Objekts erhöht werden, dieses Datum kann jedoch nicht verringert werden.
- **Legal Hold**: Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflichten haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

Weitere Informationen zu diesen Einstellungen finden Sie unter „`Using S3 object Lock`“ in "Unterstützte Vorgänge und Einschränkungen durch S3-REST-API".

Vergleich der S3-Objektsperre mit älterer Compliance

Die S3-Objektsperrfunktion in StorageGRID 11.5 ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die neue S3-Objektsperrfunktion den Amazon S3-Anforderungen entspricht, depretiert sie die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „`` Legacy-Compliance“ bezeichnet wird.

Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, wird die neue globale S3-Objektsperre beim Upgrade auf StorageGRID 11.5 automatisch aktiviert. Mandantenbenutzer können keine neuen Buckets erstellen, für die in StorageGRID 11.5 die Compliance aktiviert ist. Mandantenbenutzer können jedoch nach Bedarf alle vorhandenen, Compliance-Buckets weiterhin verwenden und managen. Dazu gehören auch die Durchführung der folgenden Aufgaben:

- Einbinden neuer Objekte in einen vorhandenen Bucket, für den veraltete Compliance aktiviert ist
- Verlängern der Aufbewahrungsfrist für einen vorhandenen Bucket, für den die veraltete Compliance-Funktion aktiviert ist
- Ändern der Einstellung zum automatischen Löschen für einen vorhandenen Bucket, für den die alte Compliance aktiviert ist
- Wenn Sie einen gesetzlichen Aufbewahrungspflichten auf einem vorhandenen Bucket platzieren, für den die veraltete Compliance-Funktion aktiviert ist.
- Anheben eines gesetzlichen Haltes

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

Wenn Sie die ältere Compliance-Funktion in einer früheren Version von StorageGRID verwendet haben, lesen Sie die folgende Tabelle, um zu erfahren, wie sie mit der S3-Objektsperrfunktion in StorageGRID verglichen wird.

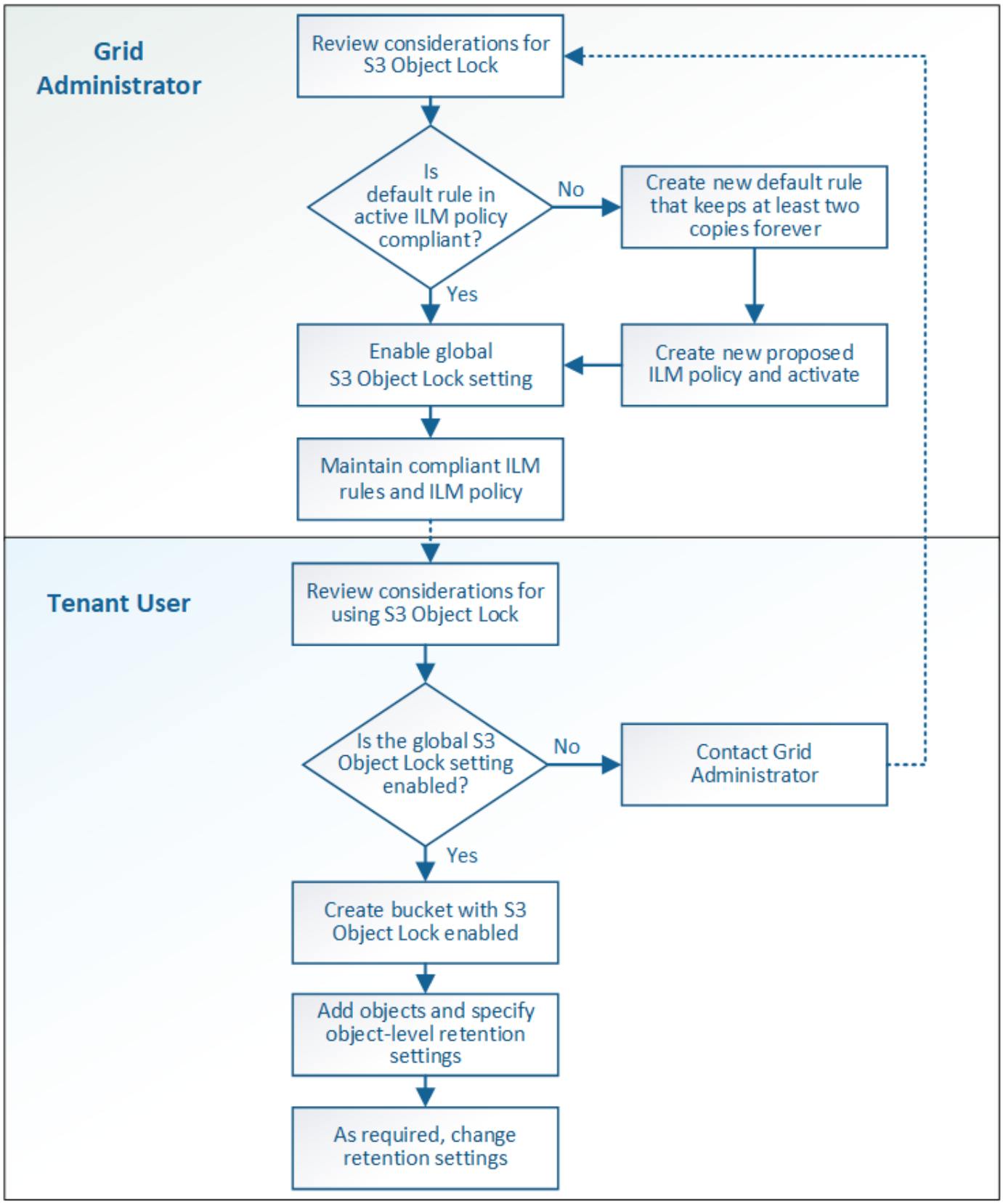
	S3-Objektsperre (neu)	**Compliance (alt)**
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **S3 Objektsperre**.	Wird nicht mehr unterstützt. **Hinweis:** Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, wird die globale S3-Objektsperre automatisch aktiviert, wenn Sie auf StorageGRID 11.5 aktualisieren.
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.	Benutzer können keine neuen Buckets mehr erstellen, für die Compliance aktiviert ist. Sie können jedoch auch weiterhin vorhandene konforme Buckets hinzufügen.
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 Die alte Compliance-Funktion ermöglicht keine Bucket-Versionierung.
Wie wird die Objektaufbewahrung festgelegt?	Benutzer können für jede Objektversion ein „bis-Datum beibehalten“ festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Der Aufbewahrungszeitraum gilt für alle Objekte im Bucket.

	S3-Objektsperre (neu)	Compliance (alt)
Kann ein Bucket Standardeinstellungen für Aufbewahrung und Aufbewahrung gesetzlicher Aufbewahrungspflichten haben?	Nein Für StorageGRID-Buckets, für die S3-Objektsperre aktiviert ist, ist kein Standardaufbewahrungszeitraum vorhanden. Stattdessen können Sie für jede Objektversion ein „bis-Aufbewahrung“-Datum angeben.	Ja.
Kann der Aufbewahrungszeitraum geändert werden?	Die Aufbewahrung bis zum Datum für eine Objektversion kann erhöht, aber nie verkleinert werden.	Die Aufbewahrungsfrist des 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?	Eine Objektversion kann nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt befindet sich nicht in der gesetzlichen Aufbewahrungspflichten.	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. Fügen Sie diesen Buckets Objekte hinzu, und legen Sie Aufbewahrungszeiträume auf Objektebene sowie Einstellungen für die Aufbewahrung rechtlicher Daten fest.
3. Aktualisieren Sie je nach Bedarf eine Aufbewahrungsfrist oder ändern Sie die Einstellung für die gesetzliche Aufbewahrungspflichten für ein einzelnes Objekt.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"S3 verwenden"

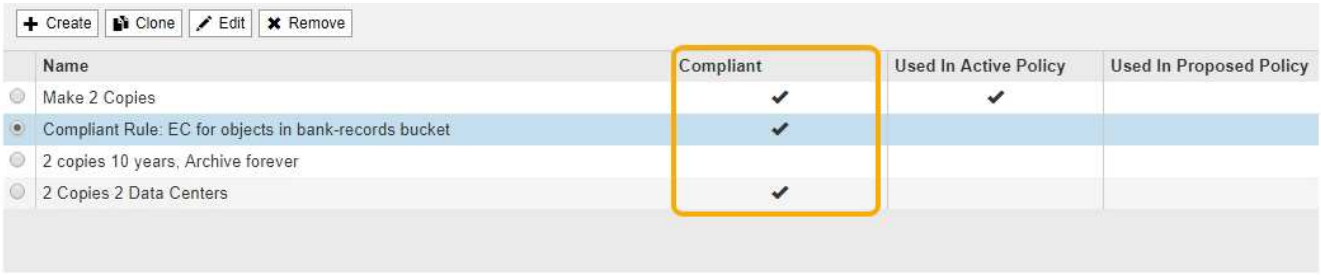
Anforderungen für die S3-Objektsperre

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-Objektsperre kann nur aktiviert werden, wenn die Standardregel in der aktiven ILM-Richtlinie*konform_* ist (das heißt, die Standardregel muss die Anforderungen von Buckets erfüllen, wenn S3 Object Lock aktiviert ist).
- Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können Sie keine neue vorgeschlagene ILM-Richtlinie erstellen oder eine vorhandene vorgeschlagene ILM-Richtlinie aktivieren, wenn die Standardregel in der Richtlinie nicht konform ist. Nachdem die globale S3 Object Lock-Einstellung aktiviert wurde, geben die Seiten ILM-Regeln und ILM-Richtlinien an, welche ILM-Regeln konform sind.

  Im folgenden Beispiel führt die Seite ILM-Regeln drei Regeln auf, die mit Buckets kompatibel sind, bei denen S3 Object Lock aktiviert ist.

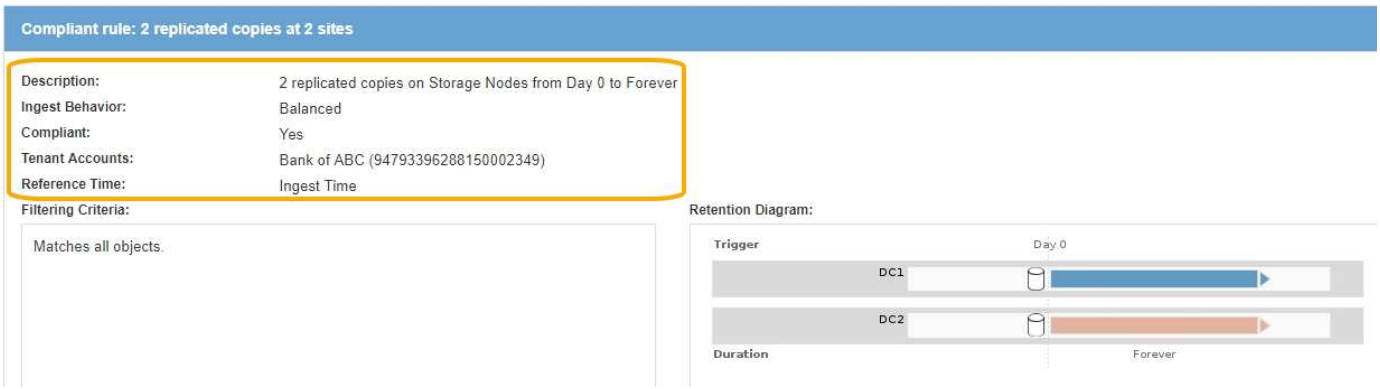


Anforderungen für konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperre aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in Ihrer aktiven ILM-Richtlinie konform ist. Eine konforme Regel erfüllt die Anforderungen beider Buckets durch aktivierte S3-Objektsperre und alle vorhandenen Buckets, für die Compliance aktiviert ist:

- Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
- Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Plazierung vorhanden sein.
- Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
- Objektkopien können nicht auf Archiv-Knoten gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen und als Referenzzeit **Aufnahmezeit** verwenden.
- Mindestens eine Zeile der Platzierungsanweisungen muss „`Forever`“ sein.

Diese Regel erfüllt beispielsweise die Anforderungen von Buckets, wenn die S3-Objektsperre aktiviert ist. Es werden zwei replizierte Objektkopien von der Aufnahmezeit (Tag 0) bis „`` für immer“ gespeichert. Die Objekte werden auf Storage-Nodes in zwei Datacentern gespeichert.



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, die die S3-Objektsperre nicht aktiviert haben oder die die ältere Compliance-Funktion nicht aktiviert haben.
- Konforme Regeln können auf Objekte in jedem Bucket angewendet werden; S3-Objektsperre oder vorhandene Compliance muss für den Bucket nicht aktiviert werden.

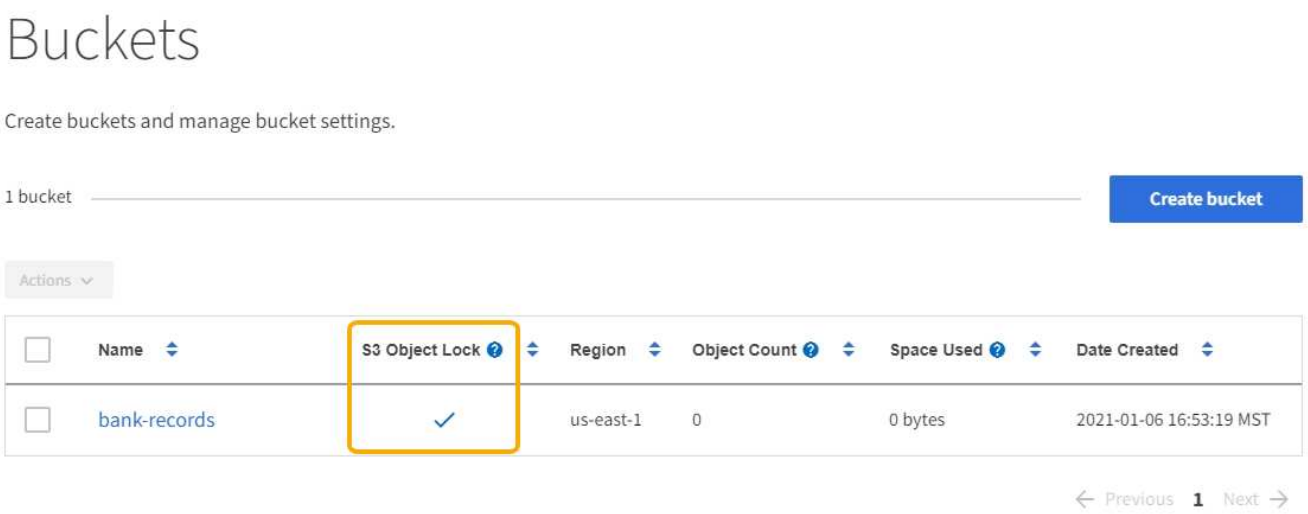
Eine ILM-konforme Richtlinie kann folgende drei Regeln umfassen:

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 die S3-Objektsperre oder ältere Compliance nicht aktiviert ist, da nur eine Objektkopie für immer gespeichert wird und Archiv-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.

  In diesem Beispiel aus dem Tenant Manager wird ein Bucket angezeigt, in dem S3 Object Lock aktiviert ist.



- 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.
- Bucket-Versionierung ist mit S3 Object Lock erforderlich. Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket.

- Nachdem Sie einen Bucket mit aktivierter S3-Objektsperre erstellt haben, können Sie die S3-Objektsperre oder die Versionierung für diesen Bucket nicht deaktivieren.
- Ein StorageGRID-Bucket mit aktivierter S3-Objektsperre hat keinen standardmäßigen Aufbewahrungszeitraum. Stattdessen kann die S3-Client-Applikation optional für jede Objektversion, die zu diesem Bucket hinzugefügt wird, ein Aufbewahrungsdatum und eine Einstellung für die Aufbewahrung gemäß den gesetzlichen Aufbewahrungspflichten festlegen.
- Bucket-Lifecycle-Konfiguration wird für S3-Objekt-Lifecycle-Buckets unterstützt.
- 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

- Die S3-Client-Applikation muss Aufbewahrungseinstellungen für jedes Objekt angeben, das durch die S3-Objektsperre geschützt werden muss.
- Sie können das Aufbewahrungsdatum für eine Objektversion erhöhen, diesen Wert jedoch nie reduzieren.
- Wenn Sie über eine ausstehende rechtliche oder behördliche Untersuchung informiert werden, können Sie relevante Informationen erhalten, indem Sie eine gesetzliche Aufbewahrungspflichten auf eine Objektversion setzen. Wenn eine Objektversion unter einer gesetzlichen Aufbewahrungspflichten liegt, kann das Objekt nicht aus StorageGRID gelöscht werden, auch wenn es seine Aufbewahrungsfrist bis zum letzten Tag erreicht hat. Sobald die gesetzliche Aufbewahrungspflichten aufgehoben sind, kann die Objektversion gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
- Für die S3-Objektsperre ist die Verwendung versionierter Buckets erforderlich. 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 Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft drei Phasen:

1. **Objektaufnahme**
   - Beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre kann die S3-Client-Applikation optional Aufbewahrungseinstellungen für das Objekt festlegen (bis dato, gesetzliche Aufbewahrungspflichten oder beides). StorageGRID generiert dann Metadaten für dieses Objekt, einschließlich einer eindeutigen Objekt-ID (UUID) sowie Datum und Uhrzeit der Aufnahme.
   - Nach der Aufnahme einer Objektversion mit Aufbewahrungseinstellungen können seine Daten und benutzerdefinierten S3-Metadaten nicht mehr geändert werden.
   - StorageGRID speichert die Objektmetadaten unabhängig von den Objektdaten. Es behält drei Kopien aller Objektmetadaten an jedem Standort.
2. **Aufbewahrung von Objekten**
   - StorageGRID speichert mehrere Kopien des Objekts. Die genaue Anzahl und Art der Kopien und der Speicherorte werden durch die konformen Regeln in der aktiven ILM-Richtlinie festgelegt.
3. **Löschen von Objekten**
   - Ein Objekt kann gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
   - Ein Objekt, das sich unter einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht gelöscht werden.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"S3 verwenden"

"Vergleich der S3-Objektsperre mit älterer Compliance"

"Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

"Prüfung von Audit-Protokollen"

Aktivieren der 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.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen den S3 Object Lock Workflow überprüft haben, und Sie müssen die Überlegungen verstehen.
- Die Standardregel in der aktiven ILM-Richtlinie muss konform sein.

  "Erstellen einer Standard-ILM-Regel"

  "ILM-Richtlinie erstellen"

Über diese Aufgabe

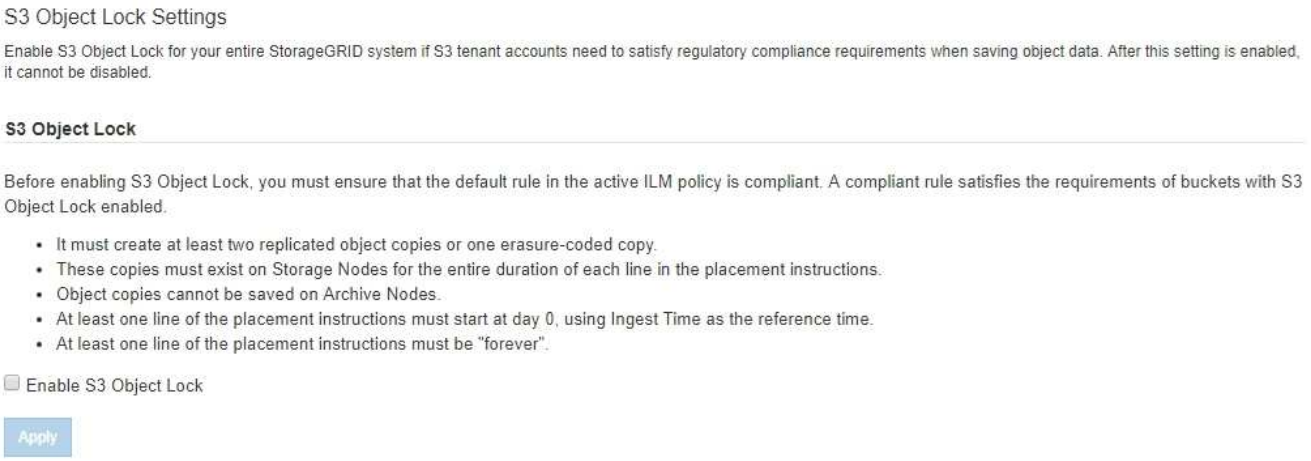
Ein Grid-Administrator muss die globale S3-Objektsperre aktivieren, damit Mandantenbenutzer neue Buckets erstellen können, für die S3-Objektsperre aktiviert ist. Nachdem diese Einstellung aktiviert ist, kann sie nicht deaktiviert werden.

> Wenn Sie die globale Compliance-Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die neue S3-Objektsperre automatisch aktiviert, wenn Sie auf StorageGRID Version 11.5 aktualisieren. Sie können StorageGRID weiterhin zum Management der Einstellungen vorhandener konformer Buckets verwenden. Es ist jedoch nicht mehr möglich, neue konforme Buckets zu erstellen.
>
> "NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

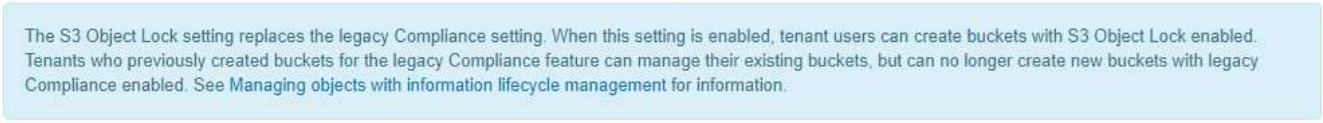
Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **S3 Objektsperre**.

   Die Seite Einstellungen für die S3-Objektsperre wird angezeigt.

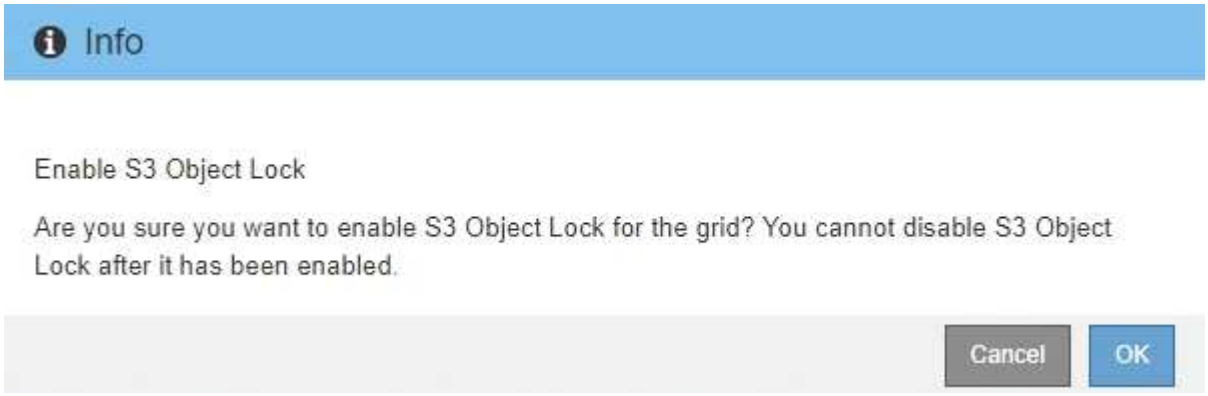


Wenn Sie die globale Compliance-Einstellung mit einer früheren Version von StorageGRID aktiviert haben, enthält die Seite den folgenden Hinweis:



2. Wählen Sie **S3-Objektsperre aktivieren**.
3. Wählen Sie **Anwenden**.

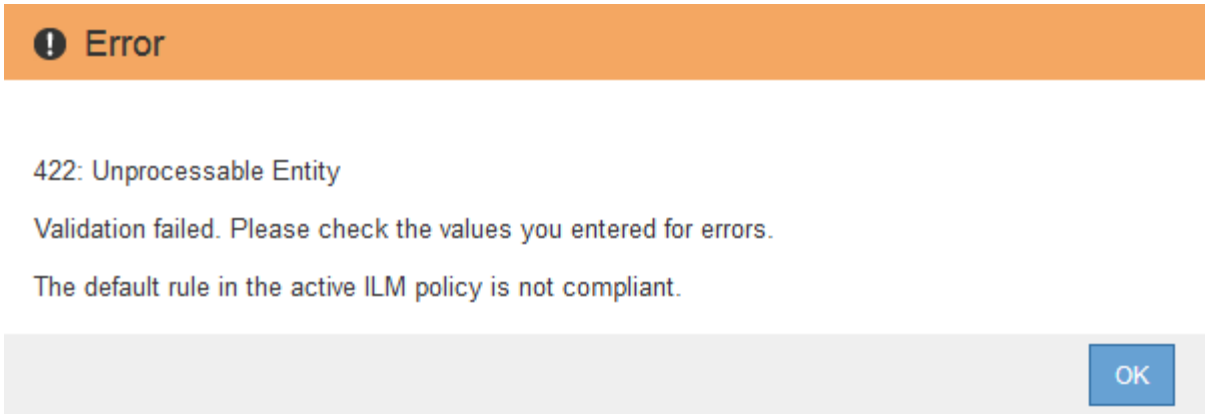
   Ein Bestätigungsdialogfeld wird angezeigt und Sie werden daran erinnert, dass Sie die S3-Objektsperre nach ihrer Aktivierung nicht deaktivieren können.



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 die S3-Objektsperre nun für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
   - Wenn die Standardregel nicht konform ist, erscheint ein Fehler, der angibt, dass Sie eine neue ILM-Richtlinie erstellen und aktivieren müssen, die eine konforme Regel als Standardregel enthält. Wählen Sie **OK**, und erstellen Sie eine neue vorgeschlagene Richtlinie, simulieren Sie sie und aktivieren Sie sie.



Nachdem Sie fertig sind

Nachdem Sie die globale S3 Object Lock-Einstellung aktiviert haben, sollten Sie möglicherweise eine 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 möchten Sie eine nicht-konforme Regel verwenden, die keine Filter für Objekte in Buckets enthält, für die die S3-Objektsperre nicht aktiviert ist.

Verwandte Informationen

"Erstellen einer ILM-Richtlinie, nachdem S3 Object Lock aktiviert ist"

"Erstellen einer ILM-Regel"

"ILM-Richtlinie erstellen"

"Vergleich der S3-Objektsperre mit älterer Compliance"

Beseitigung von Konsistenzfehlern bei der Aktualisierung 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, da ein Datacenter-Standort oder mehrere Speicherknoten nicht verfügbar sind, wird eine Fehlermeldung angezeigt. Im Detail:

- Mandantenmanager Benutzer sehen die folgende Fehlermeldung:

- Mandantenmanagement-API-Benutzer und S3-API-Benutzer erhalten einen Antwortcode von `503 Service Unavailable` Mit ähnlichem Nachrichtentext.

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 verwenden"

"Verwalten Sie erholen"

Beispiele für ILM-Regeln und -Richtlinien

Die Beispiele in diesem Abschnitt dienen als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien.

- "Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage"
- "Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung"
- "Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien"
- "Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"
- "Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"
- "Beispiel 6: Ändern einer ILM-Richtlinie"
- "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

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.

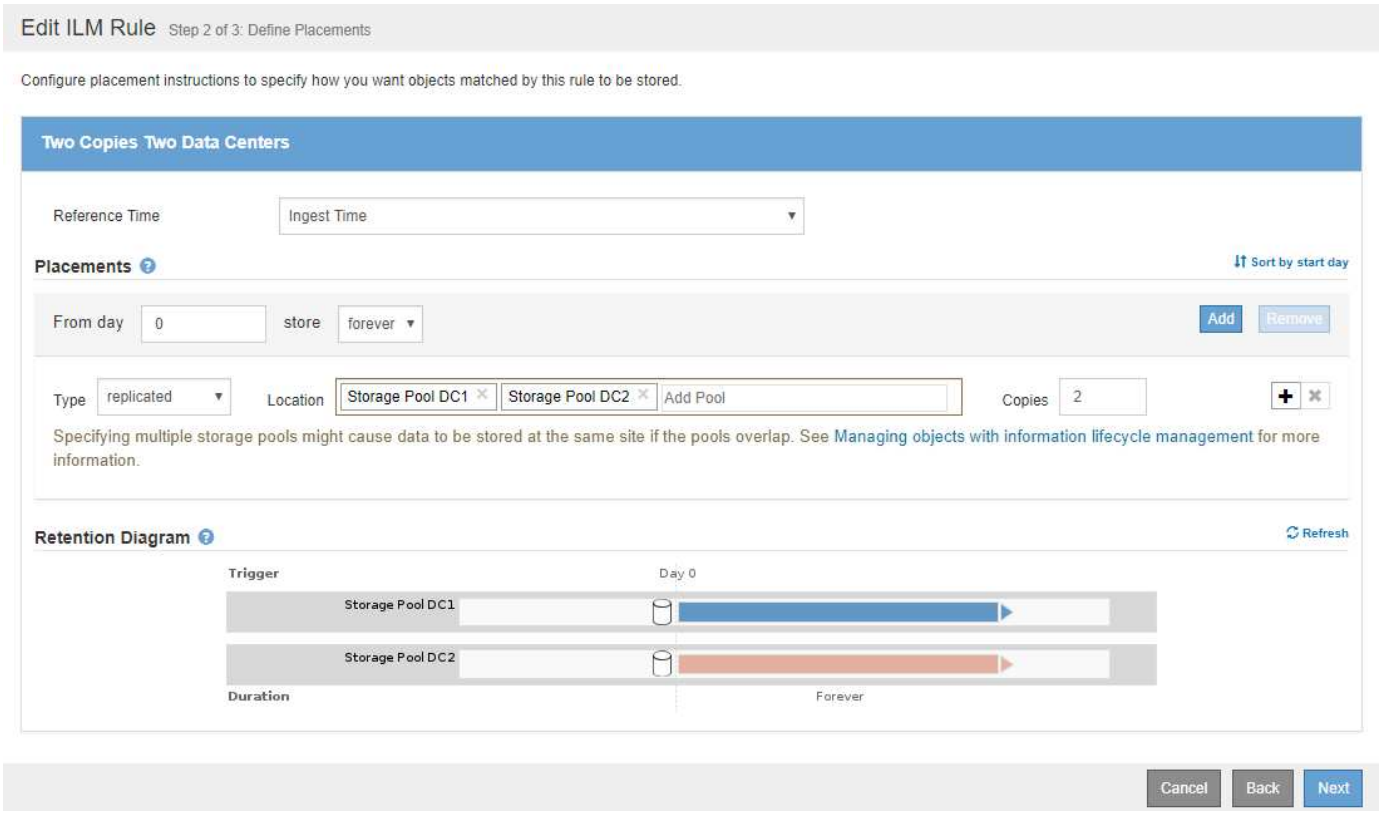
> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 1: Objektdaten in zwei Datacenter kopieren

Diese Beispiel-ILM-Regel kopiert Objektdaten in Storage-Pools in zwei Datacentern.

Regeldefinition	Beispielwert
Storage-Pools	Zwei Speicherpools, jeweils in verschiedenen Datacentern, genannt Storage Pool DC1 und Storage Pool DC2.

Regeldefinition	Beispielwert
Regelname	Zwei Kopien Zwei Datacenter
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0, behalten Sie zwei replizierte Kopien für immer - eins im Storage Pool DC1 und eine im Storage Pool DC2.

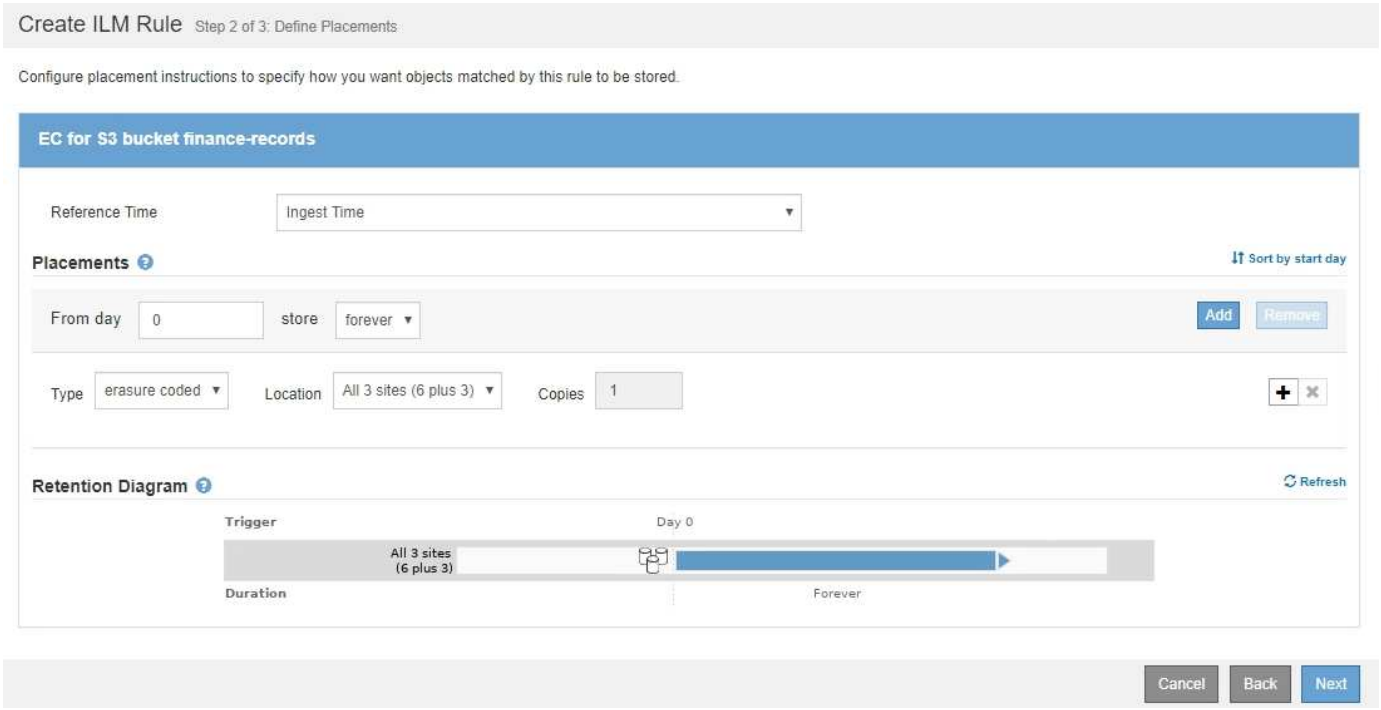


ILM-Regel 2 zum Beispiel 1: Erasure Coding-Profil mit Bucket-Übereinstimmung

In diesem Beispiel wird eine ILM-Regel verwendet ein Erasure Coding-Profil und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert wird.

Regeldefinition	Beispielwert
Verfahren Zur Einhaltung Von Datenkonsistenz	• Ein Storage-Pool für drei Datacenter (alle 3 Standorte) • Verwenden Sie das Erasure Coding-Schema für 6+3
Regelname	EC für S3-Bucket-Finanzdatensätze
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierung Von Inhalten	Erstellen Sie für Objekte im S3-Bucket mit Namen „Finance-Records“ eine Kopie mit Erasure-Coding-Verfahren im Pool, der durch das Erasure Coding-Profil festgelegt wird. Bewahren Sie diese Kopie für immer auf.

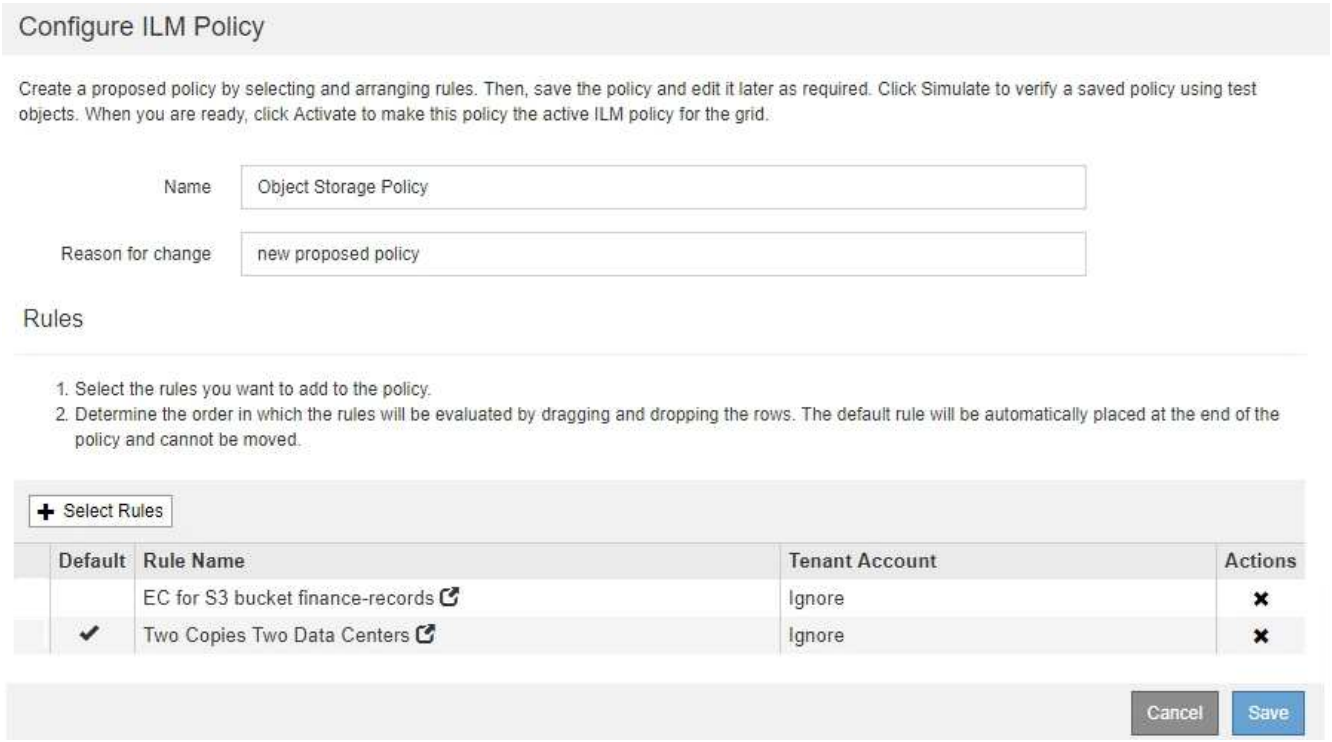


ILM-Richtlinie z. B. 1

Mit dem StorageGRID System entwickeln Sie ausgereifte und komplexe ILM-Richtlinien. In der Praxis sind jedoch die meisten ILM-Richtlinien einfach.

Eine typische ILM-Richtlinie für eine Topologie mit mehreren Standorten kann ILM-Regeln wie die folgenden umfassen:

- Bei der Aufnahme sollten Sie Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) in 6+3 verwenden, um alle Objekte zu speichern, die dem S3-Bucket mit dem Namen gehören `finance-records` Über drei Datacenter verteilt.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, verwenden Sie die Standard-ILM-Regel der Richtlinie, zwei Kopien von zwei Rechenzentren, um eine Kopie dieses Objekts in zwei Rechenzentren zu speichern, DC1 und DC2.



Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung

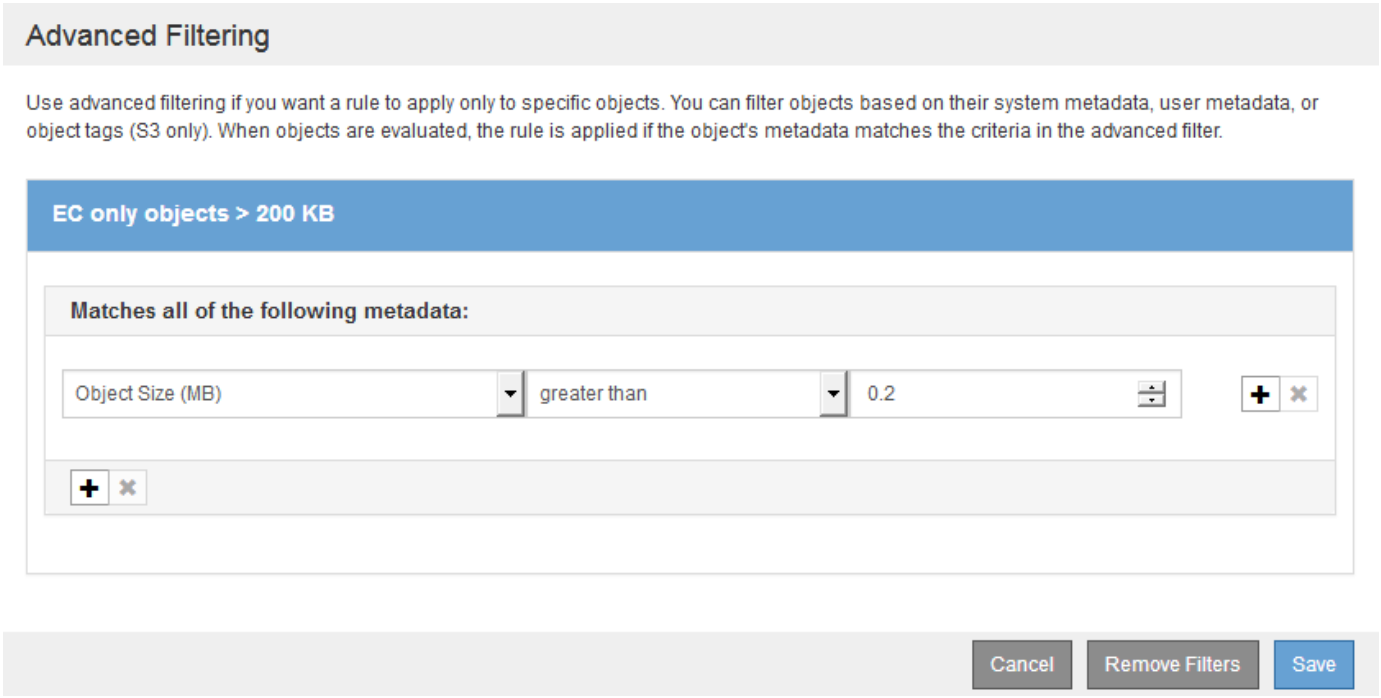
Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt für die Definition einer ILM-Richtlinie, die nach Objektgröße gefiltert wird, um empfohlene EC-Anforderungen zu erfüllen.

> 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 alle Objekte, die größer als 200 KB sind

In diesem Beispiel werden alle Objekte, die größer als 200 KB sind (0.20 MB), mit einer ILM-Regel gelöscht.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 200 KB
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Objektgröße	Objektgröße (MB) größer als 0.20
Platzierung Von Inhalten	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

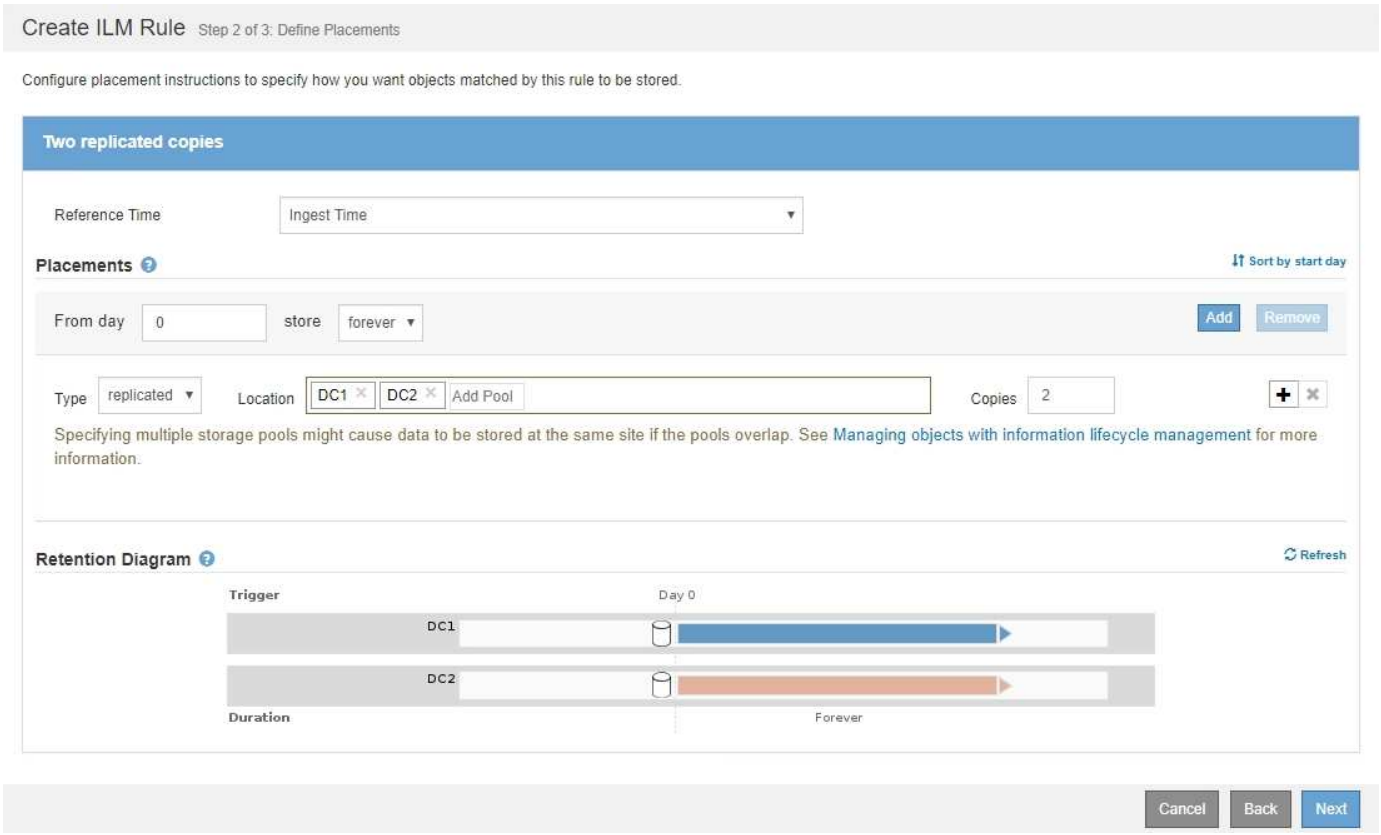


In den Anweisungen zur Platzierung wird angegeben, dass eine Kopie mit 2+1-Erasure-Coding-Verfahren unter Verwendung aller drei Standorte erstellt wird.

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 zweite Regel in der Richtlinie. Da ILM-Regel 1 beispielsweise 2 alle Objekte gefiltert, die größer als 200 KB sind, gilt ILM-Regel 2 beispielsweise nur für Objekte mit einer Größe von 200 KB.

Regeldefinition	Beispielwert
Regelname	Zwei Replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Objektgröße	Keine
Platzierung Von Inhalten	Erstellen Sie zwei replizierte Kopien, und speichern Sie sie in zwei Rechenzentren, DC1 und DC2



ILM-Richtlinie beispielsweise 2: Verwenden Sie EC für Objekte, die größer als 200 KB sind

In dieser Beispielrichtlinie werden Objekte mit einer Größe von mehr als 200 KB Erasure-Coding ausgeführt. Von allen anderen Objekten werden zwei replizierte Kopien erstellt.

Diese ILM-Richtlinie für das Beispiel umfasst die folgenden ILM-Regeln:

- Löschcode für alle Objekte, die größer als 200 KB sind.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, erstellen Sie zwei replizierte Kopien dieses Objekts mithilfe der Standard-ILM-Regel. Da Objekte mit einer Größe von mehr als 200 KB nach Regel 1 herausgefiltert wurden, gilt Regel 2 nur für Objekte, die 200 KB 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 einer Größe von mehr als 200 KB gelöscht werden und drei Kopien von kleineren Images erstellt werden.

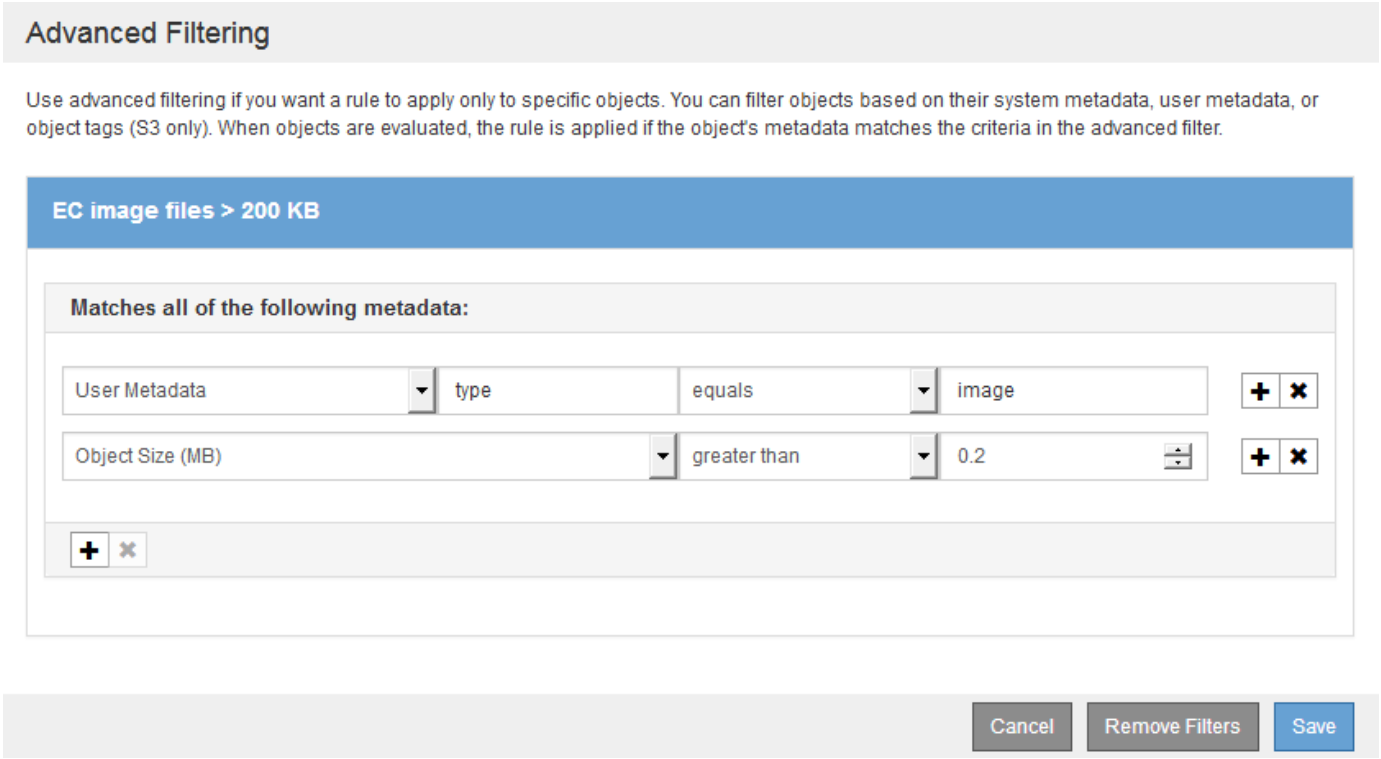
> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 3: Verwenden Sie EC für Bilddateien, die größer als 200 KB sind

Diese Beispiel ILM-Regel verwendet erweiterte Filterung zur Löschung von Code aller Bilddateien, die größer

als 200 KB sind.

Regeldefinition	Beispielwert
Regelname	EC-Bilddateien > 200 KB
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Benutzermetadaten	Der Metadatentyp des Benutzers entspricht den Bilddateien
Erweiterte Filterung für Objektgröße	Objektgröße (MB) größer als 0.2
Platzierung Von Inhalten	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten



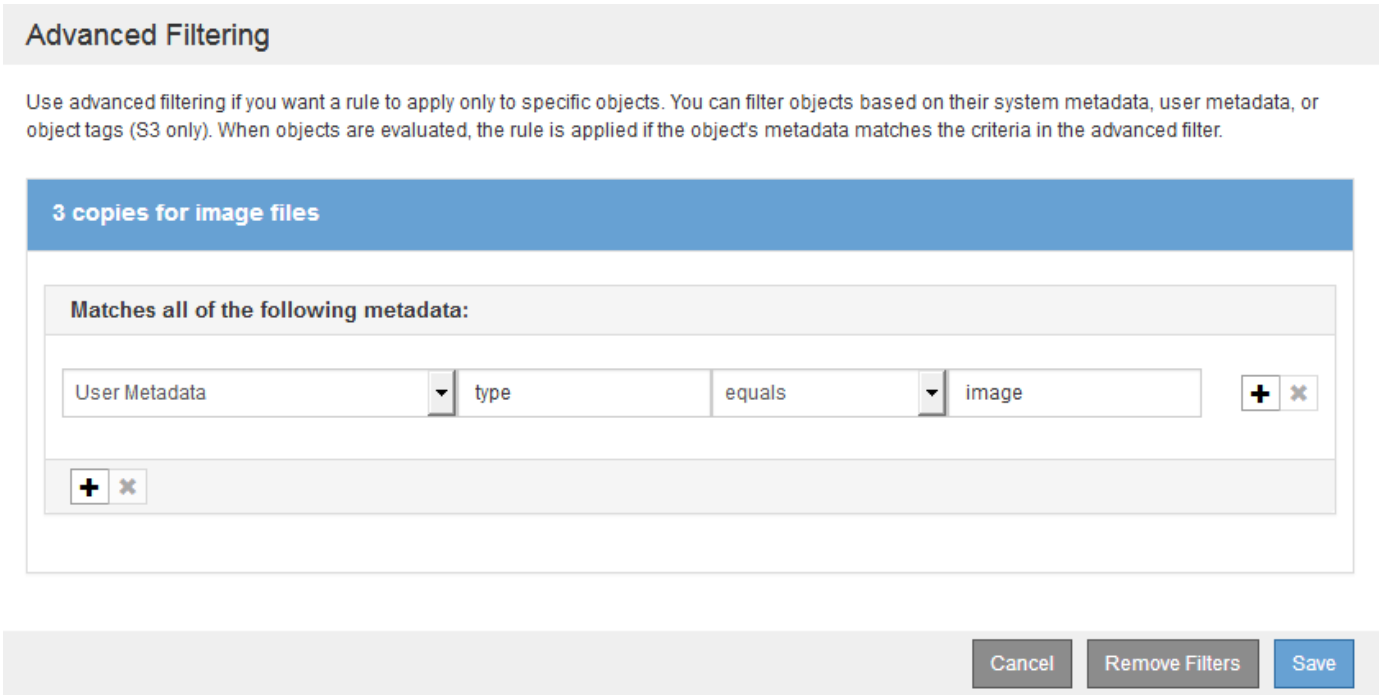
Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Anweisung zur Platzierung von Erasure Coding nur für Bilder, die größer als 200 KB sind.

ILM-Regel 2 beispielsweise 3: Replizieren Sie 3 Kopien für alle übrigen Image-Dateien

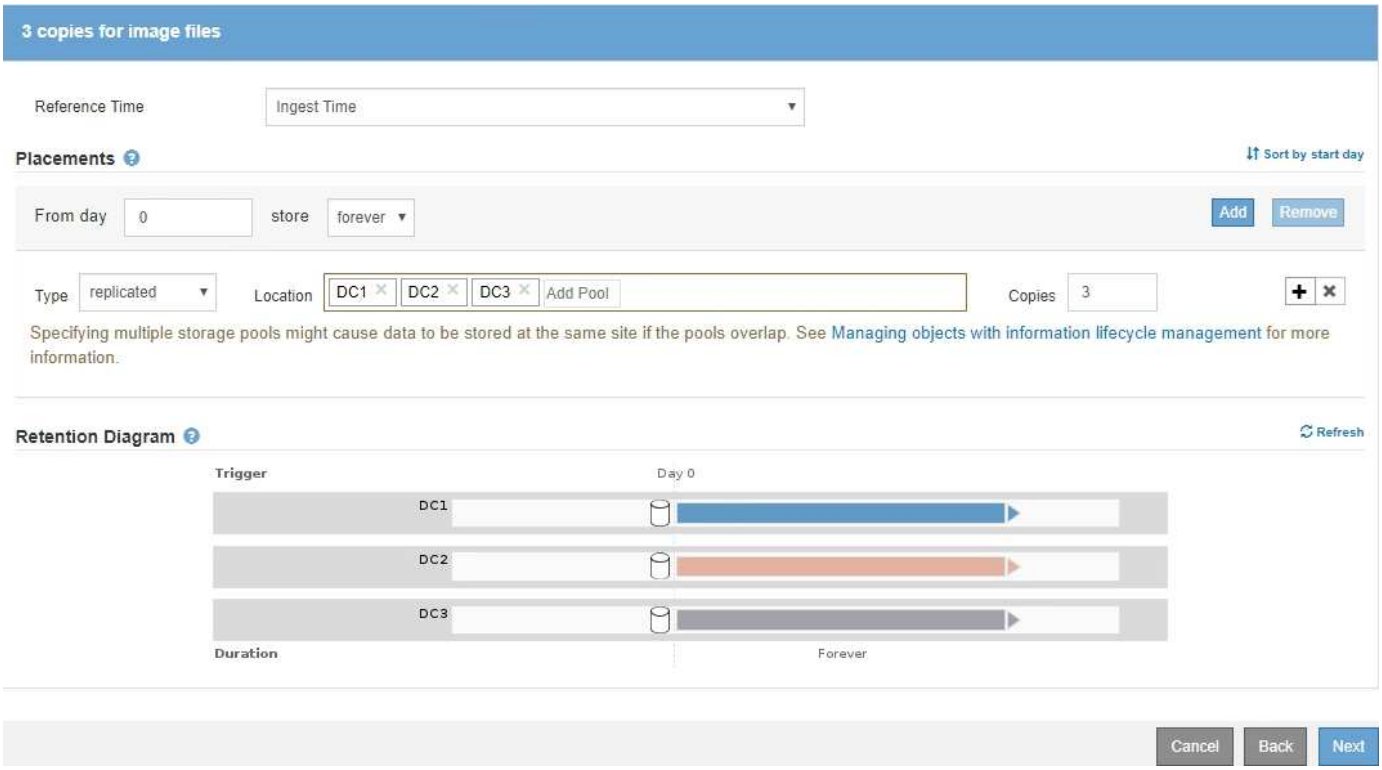
Diese Beispiel-ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass Bilddateien repliziert werden.

Regeldefinition	Beispielwert
Regelname	3 Kopien für Bilddateien

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Benutzermetadaten	Der Metadatentyp des Benutzers entspricht den Bilddateien
Platzierung Von Inhalten	Erstellen Sie 3 replizierte Kopien in allen Storage-Nodes



Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von mehr als 200 KB übereinstimmt, gelten diese Platzierungsanweisungen nur für Bilddateien mit einer Größe von 200 KB.

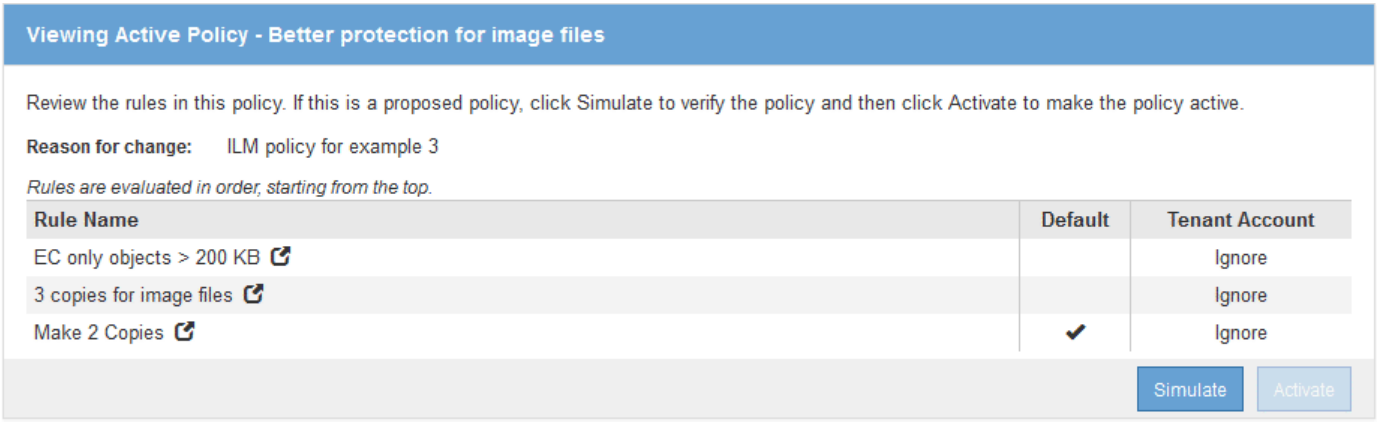


ILM-Richtlinie beispielsweise 3: Besserer Schutz für Image-Dateien

In diesem Beispiel erstellt die ILM-Richtlinie drei ILM-Regeln, die eine Richtlinie erstellen, die beim Löschen von Image-Dateien, die größer als 200 KB (0.2 MB) sind, replizierte Kopien für Image-Dateien erstellt, die mindestens 200 KB groß sind, und zwei replizierte Kopien für alle Dateien erstellt, die nicht mit dem Image verknüpft sind.

In diesem Beispiel enthält die ILM-Richtlinie folgende Regeln:

- Löschen Code alle Bilddateien größer als 200 KB.
- Erstellen Sie drei Kopien aller verbleibenden Bilddateien (d. h. Bilder, die 200 KB oder kleiner sind).
- Wenden Sie die Standardregel auf alle übrigen Objekte an (d. h. alle nicht-Image-Dateien).



Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3

Wenn Sie einen S3-Bucket mit aktivierter Versionierung haben, können Sie die nicht aktuellen Objektversionen verwalten, indem Sie Regeln in Ihre ILM-Richtlinie einarbeiten,

die **nicht aktuelle Zeit** als Referenzzeit verwenden.

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.

> Wenn Sie ILM-Richtlinien erstellen, um nicht aktuelle Objektversionen zu managen, beachten Sie, dass Sie zum Simulieren der Richtlinie die UUID oder CBID der Objektversion kennen müssen. Um die UUID und die CBID eines Objekts zu finden, verwenden Sie Object Metadata Lookup, während das Objekt noch aktuell ist.

Verwandte Informationen

"Löschen von S3-versionierten Objekten"

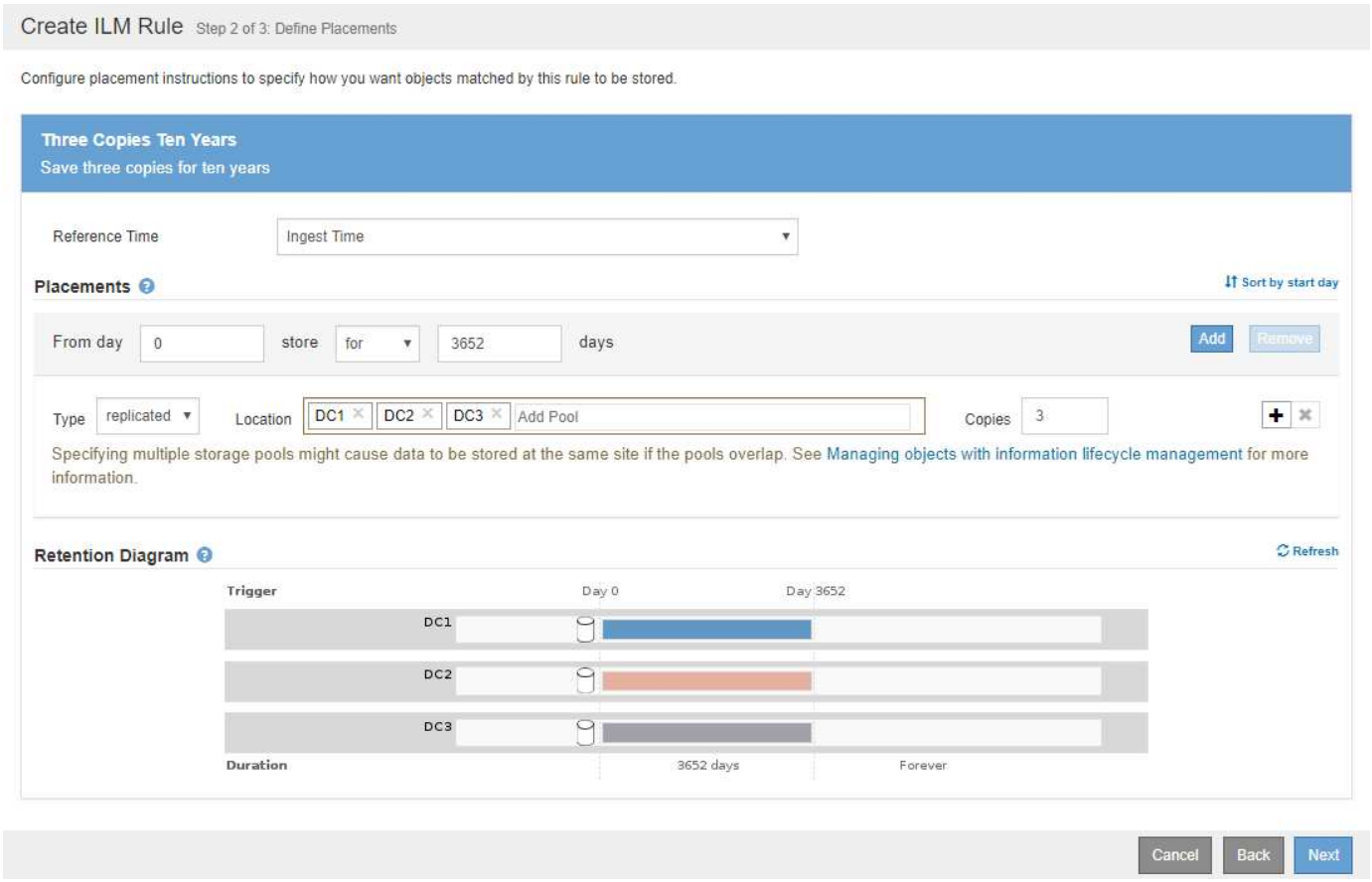
"Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup"

ILM-Regel 1 beispielsweise 4: Speichern Sie drei Kopien für 10 Jahre

In diesem Beispiel wird eine ILM-Regel für 10 Jahre eine Kopie jedes Objekts in drei Datacentern gespeichert.

Diese Regel gilt für alle Objekte, unabhängig davon, ob sie versioniert sind.

Regeldefinition	Beispielwert
Storage-Pools	Drei Storage-Pools mit den Namen DC1, DC2 und DC3.
Regelname	Drei Kopien Zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0 behalten Sie drei replizierte Kopien für 10 Jahre (3,652 Tage), eins in DC1, eins in DC2 und eins in DC3. Löschen Sie Ende 10 Jahre alle Kopien des Objekts.



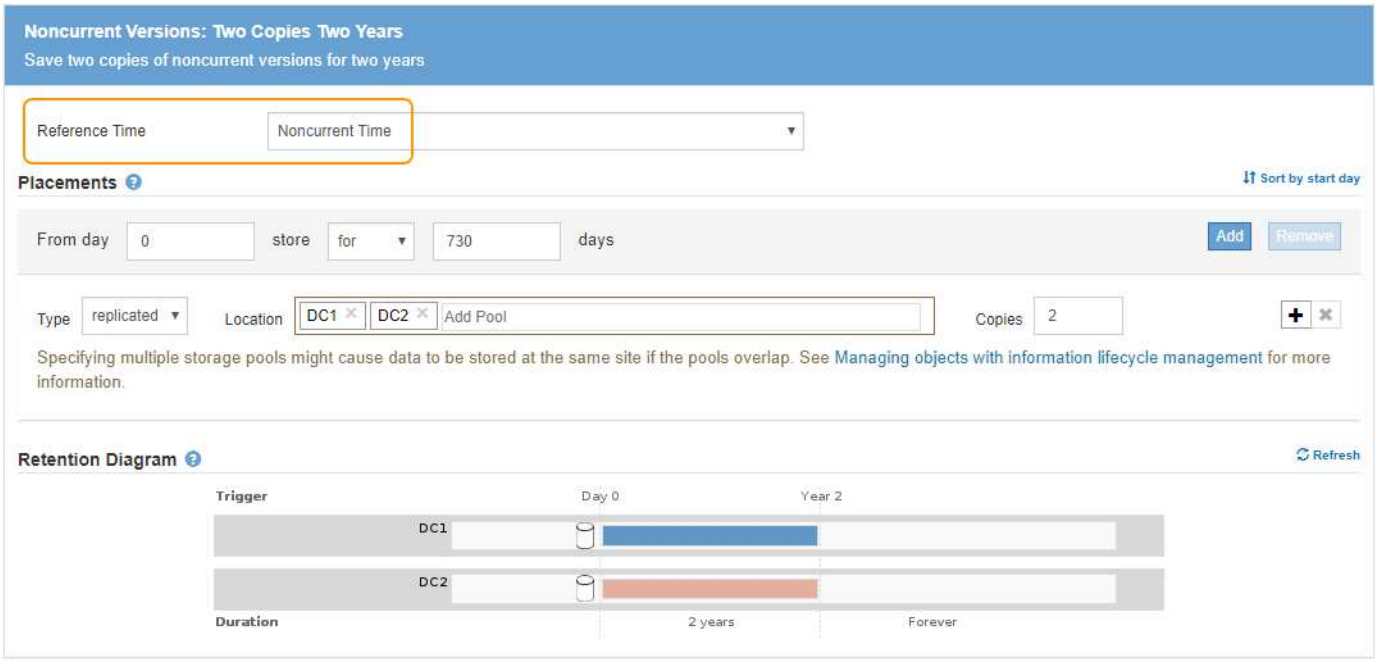
ILM-Regel 2 beispielsweise 4: Speichern Sie zwei Kopien nicht aktueller Versionen für zwei Jahre

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. Diese Regel verwendet die Option **nicht aktuelle Zeit** für Referenzzeit.

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 mit den Namen DC1 und DC2 an verschiedenen Rechenzentren.
Regelname	Nicht Aktuelle Versionen: Zwei Kopien Zwei Jahre
Referenzzeit	Nicht Aktuelle Zeit
Platzierung Von Inhalten	Am Tag 0 im Verhältnis zur nicht aktuellen Zeit (d.h. ab dem Tag, an dem die Objektversion zur nicht aktuellen Version wird) zwei replizierte Kopien der nicht aktuellen Objektversionen für 2 Jahre (730 Tage), eines in DC1 und eines in DC2. Löschen Sie Ende 2 Jahre die nicht aktuellen Versionen.



ILM-Richtlinie z. B. 4: S3-versionierte Objekte

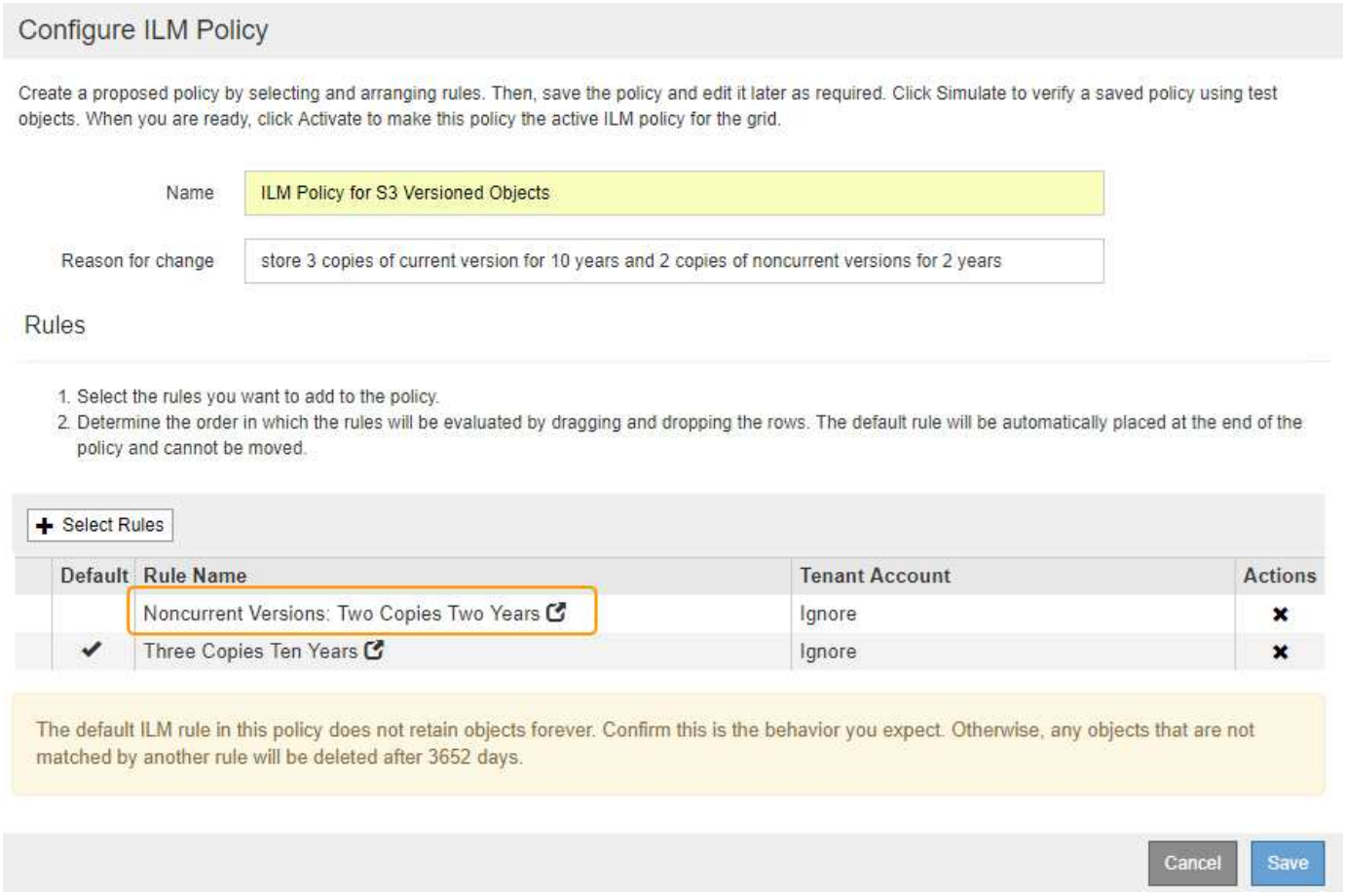
Wenn Sie ältere Versionen eines Objekts anders als die aktuelle Version verwalten möchten, müssen Regeln, die **nicht aktuelle Zeit** als Referenzzeit verwenden, in der ILM-Richtlinie vor Regeln erscheinen, die für die aktuelle Objektversion gelten.

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 nicht aktuellen Zeitregeln müssen in der Richtlinie vor den Regeln erscheinen, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht aktuellen Objektversionen niemals mit der nicht aktuellen Zeitregel abgeglichen.

- Bei Aufnahme der Daten werden drei replizierte Kopien erstellt und eine Kopie an jedem der drei Datacenter gespeichert. 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. Während das Objekt noch aktuell ist, können Sie Object Metadata Lookup verwenden, um seine UUID und CBID zu finden.

- Die aktuelle Objektversion würde mit der zweiten Regel abgeglichen. Wenn die aktuelle Objektversion 10 Jahre lang gespeichert wurde, fügt der ILM-Prozess als aktuelle Version des Objekts eine Löschmarkierung hinzu und macht die vorherige Objektversion „`non current`“. Bei der nächsten ILM-Bewertung wird diese nicht aktuelle Version der ersten Regel zugeordnet. Dadurch wird die Kopie bei DC3 gelöscht und die beiden Kopien bei DC1 und DC2 für weitere 2 Jahre gespeichert.

Verwandte Informationen

"Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup"

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

"Aufnahme von Objekten"

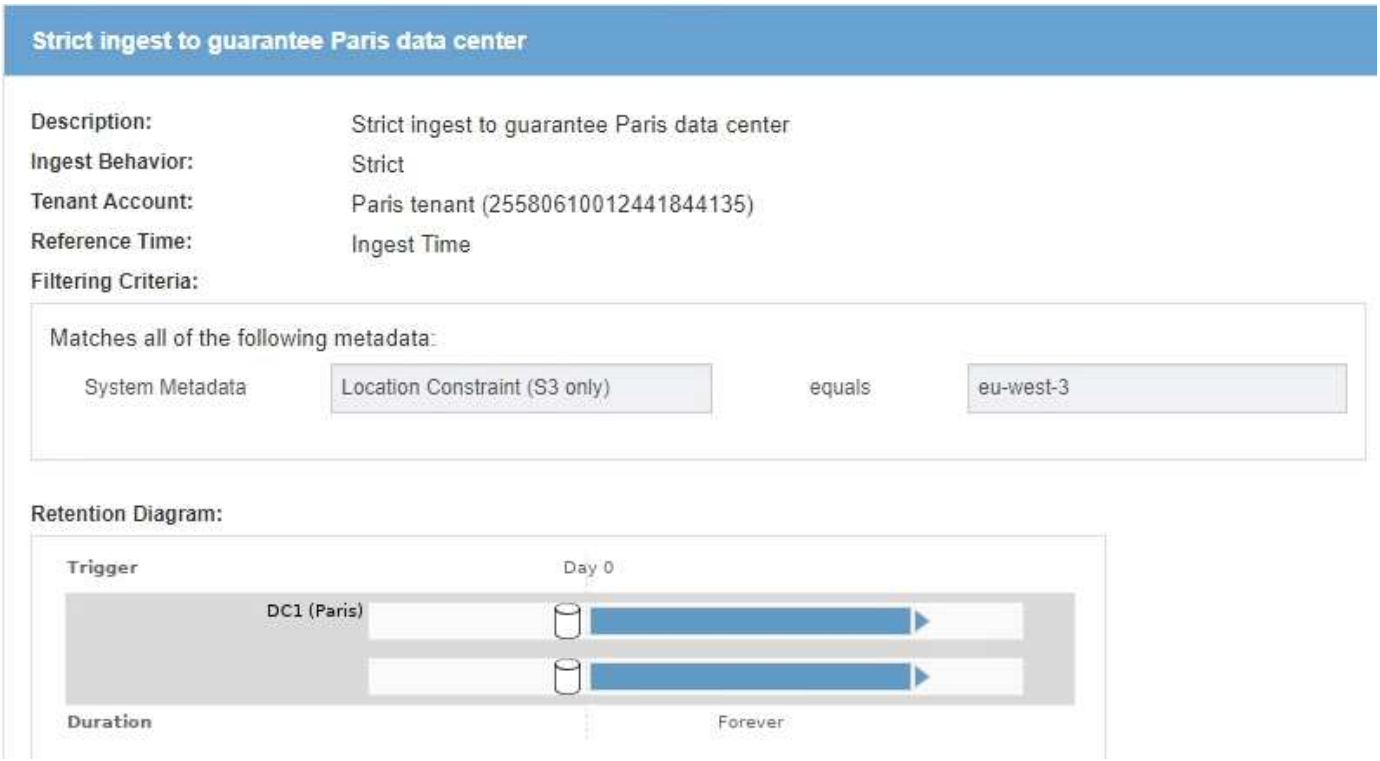
"Schritt 3 von 3: Definieren des Aufnahmeverhaltens"

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
Erweiterte Filterung	Standortbeschränkung entspricht eu-West-3
Storage-Pools	DC1 (Paris)
Regelname	Strenge Einspeisung für ein Pariser Rechenzentrum
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0, zwei replizierte Kopien für immer in DC1 (Paris)
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 an jedem verfügbaren Ort Zwischenkopien abgelegt.

Diese Regel gilt für Objekte, die einem beliebigen Mieter und einer beliebigen Region angehören.

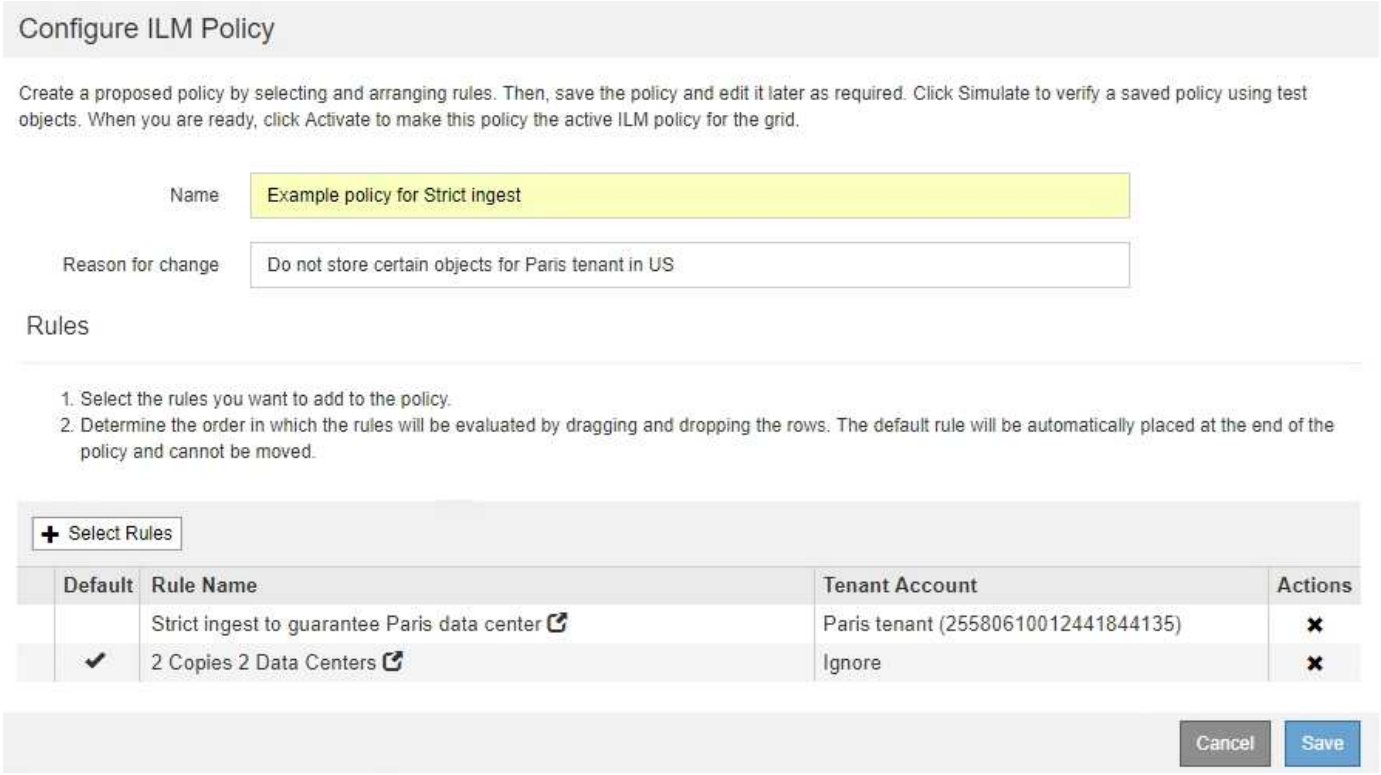
Regeldefinition	Beispielwert
Mandantenkonto	Ignorieren
Erweiterte Filterung	*Nicht angegeben*
Storage-Pools	DC1 (Paris) und DC2 (USA)
Regelname	2 Kopien 2 Datacenter
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0 werden zwei replizierte Kopien für immer in zwei Datacentern aufbewahrt
Aufnahmeverhalten	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 Ort, 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 Speicherknoten im Pariser Rechenzentrum nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle anderen Objekte werden mit der zweiten Regel abgeglichen, einschließlich Objekte, die zum Pariser Mieter gehören und die die S3-Bucket-Region nicht auf eu-West-3 gesetzt hat. 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

Möglicherweise müssen Sie eine neue ILM-Richtlinie erstellen und aktivieren, wenn sich Ihre Datensicherungsanforderungen ändern oder Sie neue Standorte hinzufügen.

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 in einer Erweiterung hinzugefügt. Die aktive ILM-Richtlinie muss überarbeitet werden, um Daten am neuen Standort zu speichern.

> 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 wirkt sich die Änderung einer ILM-Richtlinie auf die Performance aus

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.

Folgende Arten von ILM-Richtlinienänderungen, die vorübergehend Auswirkungen auf die StorageGRID Performance haben:

- Anwenden eines anderen Profils zur Einhaltung von Datenkonsistenz (Erasure Coding) auf vorhandene Objekte mit Verfahren zur Fehlerkorrektur.

  > StorageGRID hält jedes Erasure Coding-Profil für einzigartig und verwendet bei Verwendung eines neuen Profils keine Erasure Coding-Fragmente.

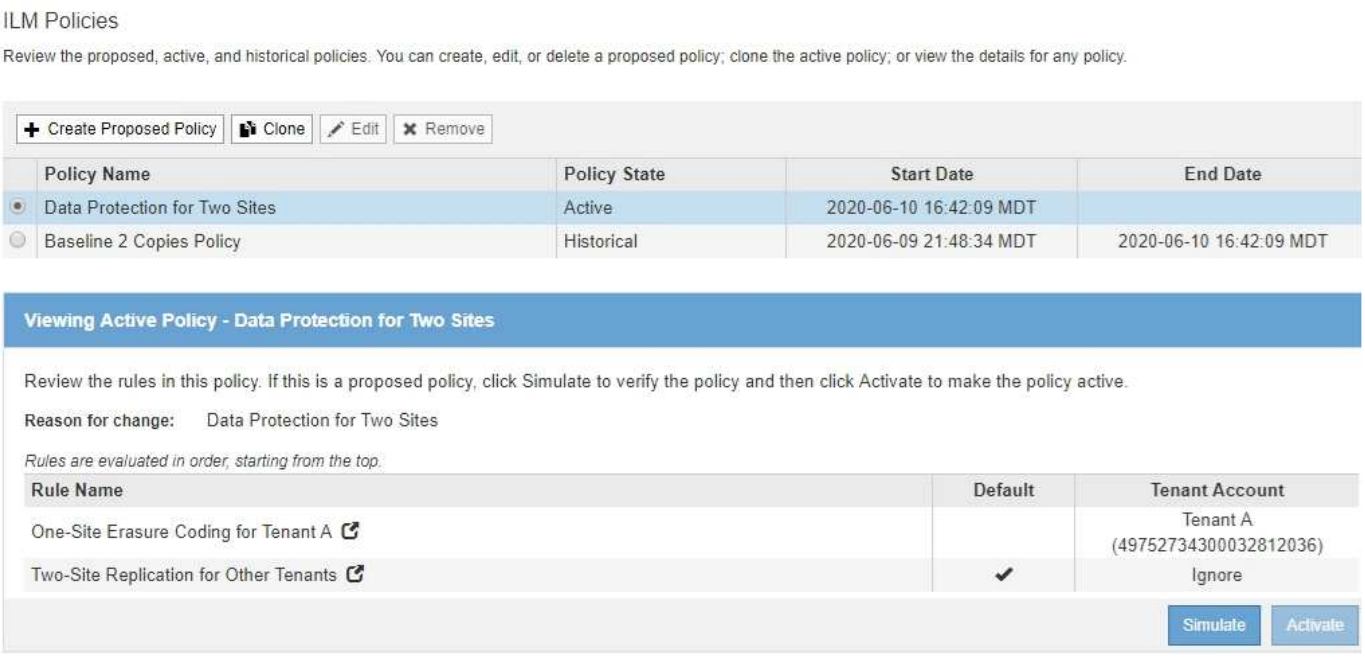
- Ändern des für vorhandene Objekte erforderlichen Kopientyps; z. B. Konvertieren eines großen Anteils replizierter Objekte in Objekte mit Erasure-Coding-Verfahren.
- Kopien vorhandener Objekte werden an einen völlig anderen Speicherort verschoben, z. B. um eine große Anzahl von Objekten in einen oder aus einem Cloud-Storage-Pool oder an einen Remote-Standort zu verschieben.

Verwandte Informationen

"ILM-Richtlinie erstellen"

Aktive ILM-Richtlinie z. B. 6: Datensicherung an zwei Standorten

In diesem Beispiel wurde die aktive ILM-Richtlinie ursprünglich für ein StorageGRID System mit zwei Standorten konzipiert und verwendet zwei ILM-Regeln.



In dieser ILM-Richtlinie werden Objekte, die von Mandanten A gehören, durch Erasure Coding von 2+1 an einem Standort geschützt, während Objekte, die zu allen anderen Mandanten gehören, durch die Replizierung mit zwei Kopien über zwei Standorte hinweg geschützt sind.

> Die erste Regel in diesem Beispiel verwendet einen erweiterten Filter, um sicherzustellen, dass das Erasure Coding nicht für kleine Objekte verwendet wird. Alle Objekte von Mandanten A, die kleiner als 200 KB sind, werden durch die zweite Regel 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	Datacenter 1
Platzierung Von Inhalten	2+1 Erasure Coding in Datacenter 1 – von Tag 0 bis für immer

Regel 2: Replizierung zwischen zwei Standorten für andere Mandanten

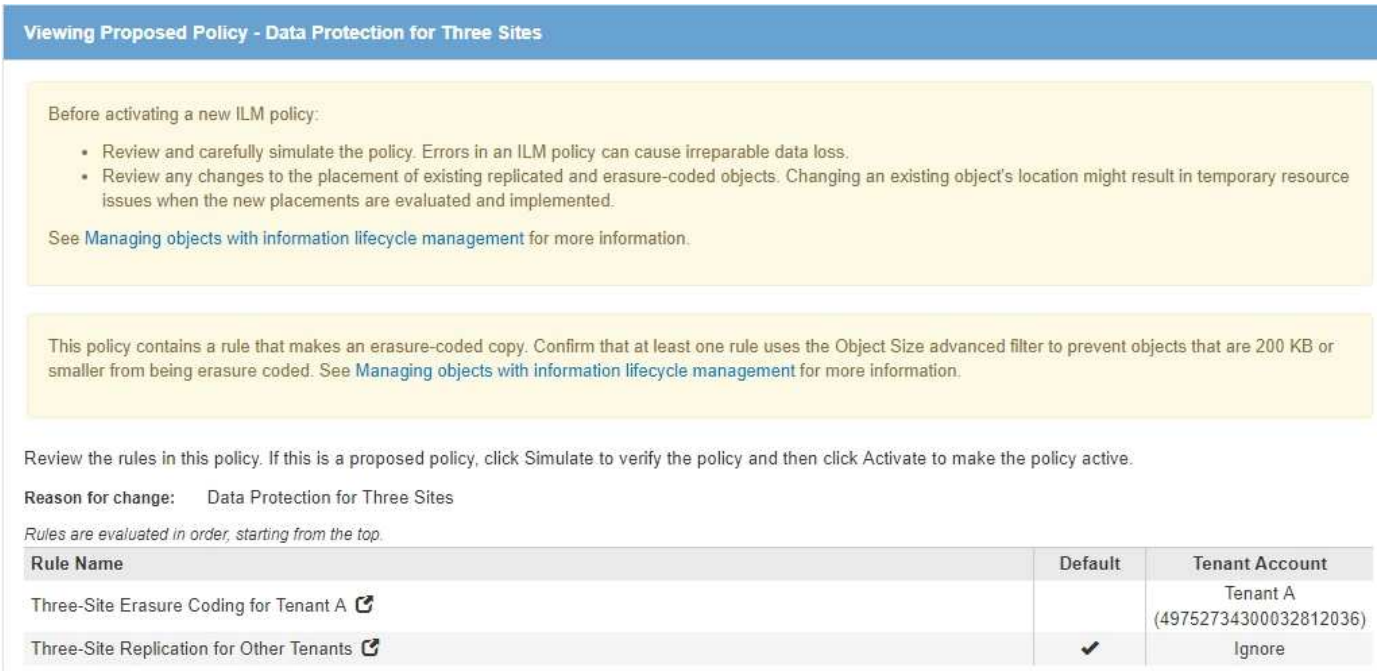
Regeldefinition	Beispielwert
Regelname	Replizierung an zwei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Datacenter 1 und Datacenter 2

Regeldefinition	Beispielwert
Platzierung Von Inhalten	Zwei replizierte Kopien von Tag 0 bis für immer: Eine Kopie im Datacenter 1 und eine Kopie im Datacenter 2.

Vorgeschlagene ILM-Richtlinie z. B. 6: Datensicherung an drei Standorten

In diesem Beispiel wird die ILM-Richtlinie für ein StorageGRID System mit drei Standorten aktualisiert.

Nach Durchführung einer Erweiterung zum Hinzufügen des neuen Standorts erstellte der Grid-Administrator zwei neue Speicherpools: Einen Speicherpool für Data Center 3 und einen Speicherpool mit allen drei Standorten (nicht identisch mit dem Standardspeicherpool für 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 Datacenter (einschließlich Datacenter 1, Datacenter 2 und Datacenter 3)
Platzierung Von Inhalten	2+1 Erasure Coding in allen 3 Datacentern von 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	Datacenter 1, Datacenter 2 und Datacenter 3
Platzierung Von Inhalten	Drei replizierte Kopien von Tag 0 bis für immer: Eine Kopie im Datacenter 1, eine Kopie im Datacenter 2 und eine Kopie im Datacenter 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 werden Objekte, die von Mandant A gehören, durch Erasure Coding von 2+1 in Datacenter 1 geschützt. In der neuen vorgeschlagenen ILM-Richtlinie werden Objekte, die von Mandant A gehören, durch Erasure Coding (2+1) in Datacentern 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. Anschließend wird jedes der drei Fragmente in einem anderen Rechenzentrum gespeichert.
- Die vorhandenen Objekte, die von Mandant A gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die ILM-Speicheranweisungen ein neues Erasure Coding-Profil verwenden, werden vollständig neue Fragmente mit Erasure-Coding-Verfahren erstellt und auf die drei Datacenter verteilt.

Die vorhandenen 2+1-Fragmente im Datacenter 1 werden nicht wiederverwendet. StorageGRID hält jedes Erasure Coding-Profil für einzigartig und verwendet bei Verwendung eines neuen Profils keine Erasure Coding-Fragmente.

Was geschieht, wenn sich Replikationsanweisungen ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte, die andere Mandanten gehören, durch zwei replizierte Kopien in Storage-Pools in Datacentern 1 und 2 geschützt. In der neuen ILM-Richtlinie werden Objekte, die zu anderen Mandanten gehören, durch drei replizierte Kopien in Storage-Pools in Datacentern 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Wenn ein Mandant außer Mandanten A ein neues Objekt in den Mittelpunkt stellt, erstellt StorageGRID drei Kopien und speichert eine Kopie in jedem Datacenter.
- Vorhandene Objekte, die zu diesen anderen Mandanten gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die vorhandenen Objektkopien von Datacenter 1 und Datacenter 2 die Replizierungsanforderungen der neuen ILM-Regel weiterhin erfüllen, muss StorageGRID nur eine neue Kopie des Objekts für Datacenter 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. Höher als die normalen Grid-Ressourcen sind erforderlich, um neue, mit Erasure Coding codierte Fragmente für vorhandene Objekte von Mandanten A und neue replizierte Kopien im Datacenter 3 für vorhandene Objekte anderer Mandanten zu erstellen.

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 die Aufnahmezeit auf größer oder gleich der ungefähren Zeit fest, 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

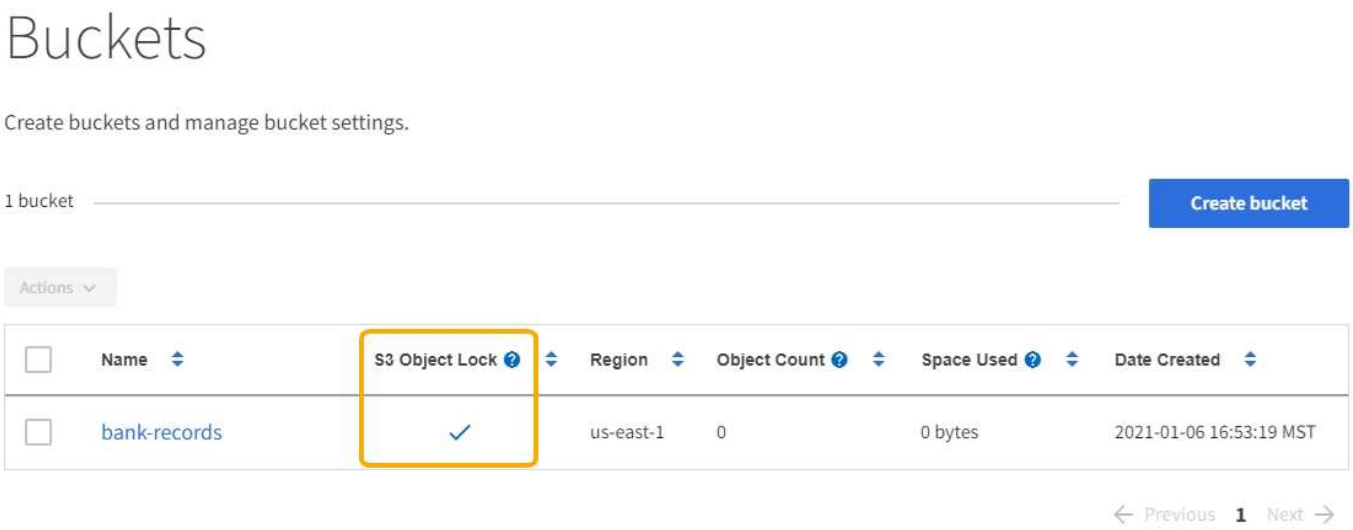
"Verwalten von Objekten mit S3 Object Lock"

"ILM-Richtlinie erstellen"

Bucket und Objekte für S3 Object Lock Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit der Bezeichnung „Bank of ABC“ durch den Mandanten-Manager einen Bucket erstellt, der mit S3-Objektsperre aktiviert wurde, um kritische Bankdatensätze zu speichern.

Bucket-Definition	Beispielwert
Name Des Mandantenkontos	Bank von ABC
Bucket-Name	bankaufzeichnungen
Bucket-Region	US-East-1 (Standard)



Jedes Objekt und jede Objektversion, die dem Bucket für die Bankdatensätze hinzugefügt wird, verwenden die folgenden Werte für `retain-until-date` Und `legal hold` Einstellungen.

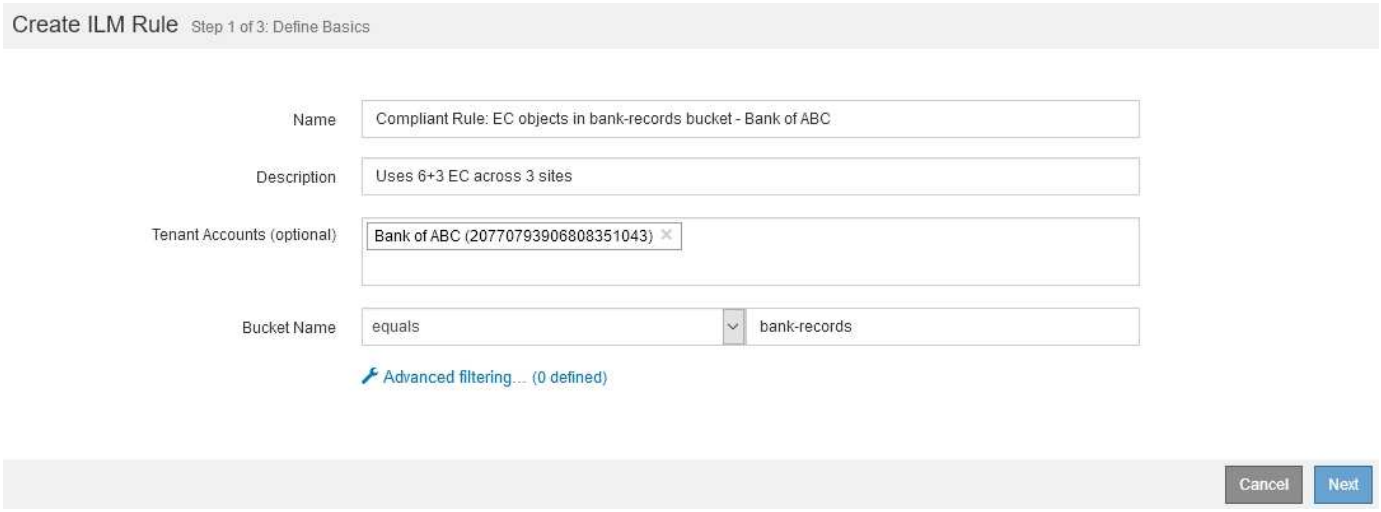
Einstellung für jedes Objekt	Beispielwert
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30. Dezember 2030) Jede Objektversion hat ihre eigene `retain-until-date` Einstellung. Diese Einstellung kann erhöht, aber nicht verringert werden.

Einstellung für jedes Objekt	Beispielwert
`legal hold`	`"OFF"` (Nicht wirksam) Eine gesetzliche Aufbewahrungsphase kann jederzeit während der Aufbewahrungsfrist auf jeder Objektversion platziert oder aufgehoben werden. Wenn ein Objekt unter einer gesetzlichen Aufbewahrungspflichten steht, kann das Objekt auch dann nicht gelöscht werden, wenn der `retain-until-date` Wurde erreicht.

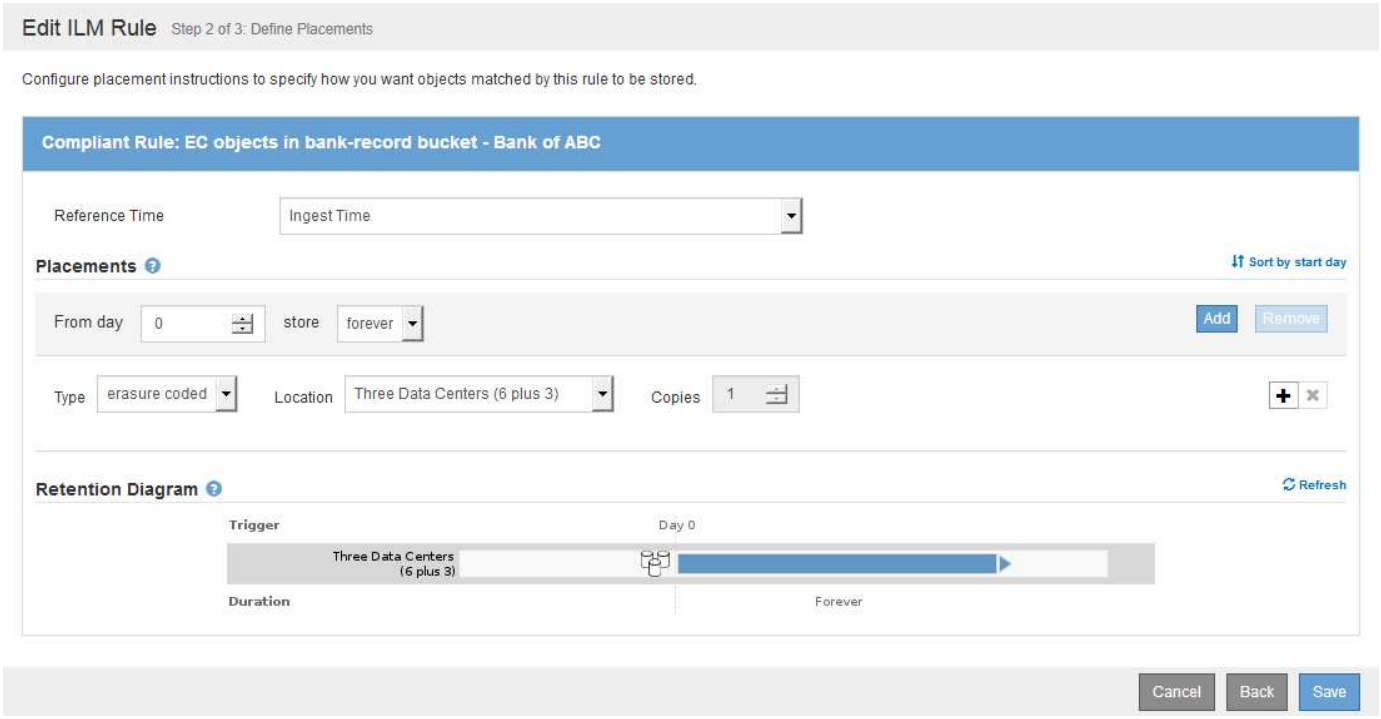
ILM-Regel 1 für S3 Object Lock Beispiel: Erasure Coding-Profil mit Bucket-Abgleich

Diese Beispiel-ILM-Regel gilt nur für das S3-Mandantenkonto namens Bank of ABC. Sie entspricht jedem Objekt im `bank-records` Bucket und verwendet dann Erasure Coding, um das Objekt mithilfe eines 6+3 Erasure Coding-Profils auf Storage Nodes an drei Datacenter-Standorten zu speichern. Diese Regel erfüllt die Anforderungen von Buckets bei aktivierter S3-Objektsperre: Eine Kopie, die gemäß Erasure-Coding-Verfahren in Storage-Nodes von Tag 0 bis für immer gespeichert wird, wobei die Aufnahmerzeit als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte in Bankaufzeichnungeimer - Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	`bank-records`
Erweiterte Filterung	Objektgröße (MB) größer als 0.20 **Hinweis:** dieser Filter sorgt dafür, dass das Erasure Coding nicht für Objekte mit einer Größe von 200 KB verwendet wird.



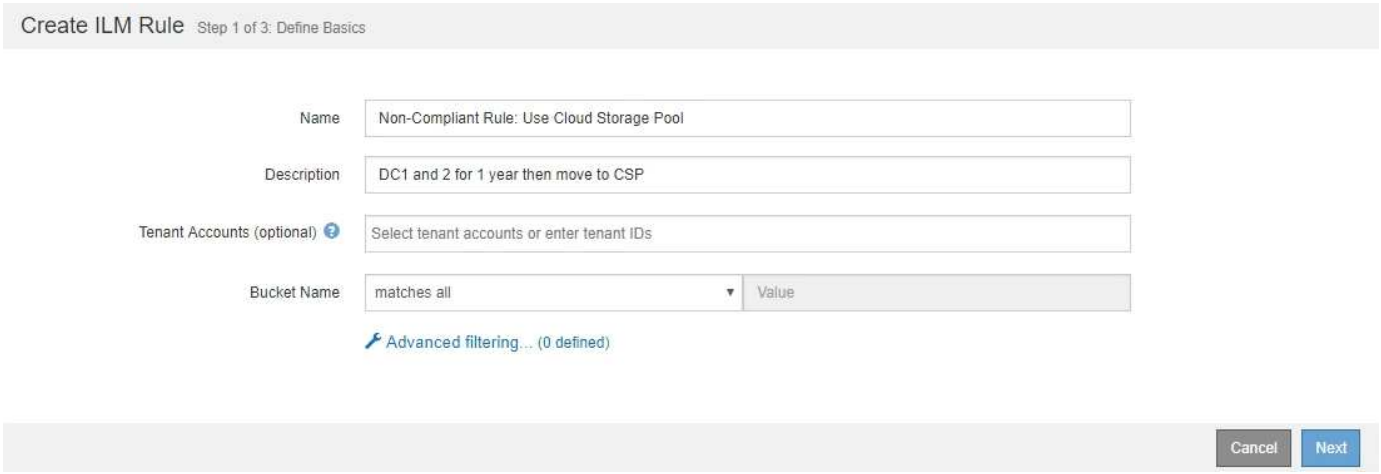
Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 dauerhaft speichern
Verfahren Zur Einhaltung Von Datenkonsistenz	• Erstellen einer mit Erasure Coding verschlüsselten Kopie auf Storage-Nodes an drei Datacenter-Standorten • Verwendet das Erasure Coding-Schema 6+3



ILM-Regel 2 für S3 Object Lock Beispiel: Nicht konforme Regel

Diese Beispiel-ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Storage Nodes. Nach einem Jahr wird für immer eine Kopie auf einem Cloud-Storage-Pool gespeichert. Da diese Regel einen Cloud-Storage-Pool verwendet, ist diese nicht konform und gilt nicht für Objekte in Buckets, deren S3-Objektsperre aktiviert ist.

Regeldefinition	Beispielwert
Regelname	Nicht Konforme Regel: Nutzung Von 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.
Erweiterte Filterung	Nicht angegeben

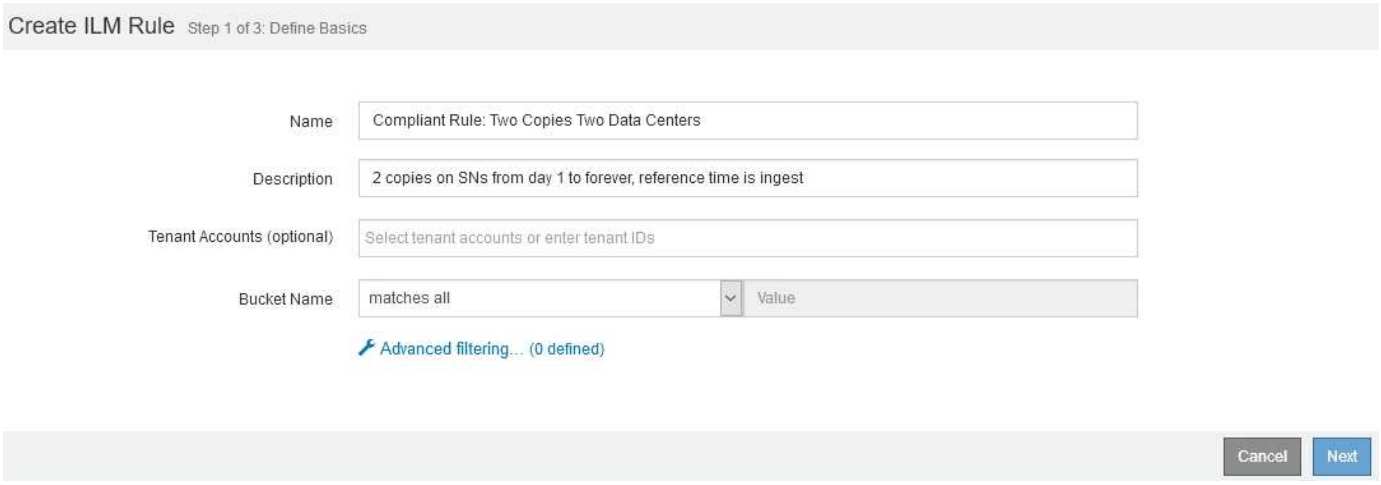


Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	• Halten Sie am Tag 0 zwei replizierte Kopien auf Storage Nodes in Datacenter 1 und Datacenter 2 für 365 Tage • Nach einem Jahr sollte eine replizierte Kopie immer in einem Cloud-Storage-Pool aufbewahrt werden

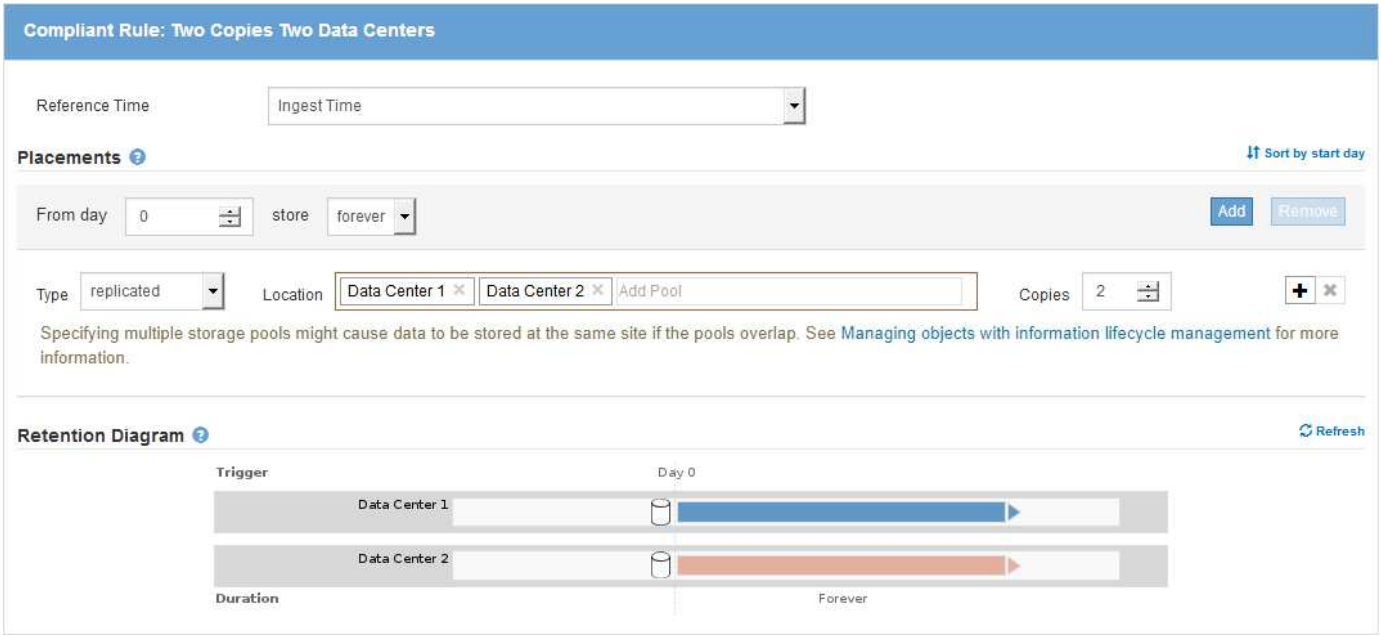
ILM-Regel 3 für S3 Object Lock Beispiel: Standardregel

Diese Beispiel-ILM-Regel kopiert Objektdaten in Storage-Pools in zwei Datacentern. Diese konforme Regel wurde als Standardregel in der ILM-Richtlinie konzipiert. Es enthält keine Filter und erfüllt die Anforderungen von Buckets mit aktivierter S3-Objektsperre: Es werden zwei Objektkopien auf Storage-Nodes von Tag 0 bis für immer aufbewahrt, wobei die Aufnahme als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Standard-Compliance-Regel: Zwei Kopien Zwei Datacenter
Mandantenkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterte Filterung	Nicht angegeben



Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
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.

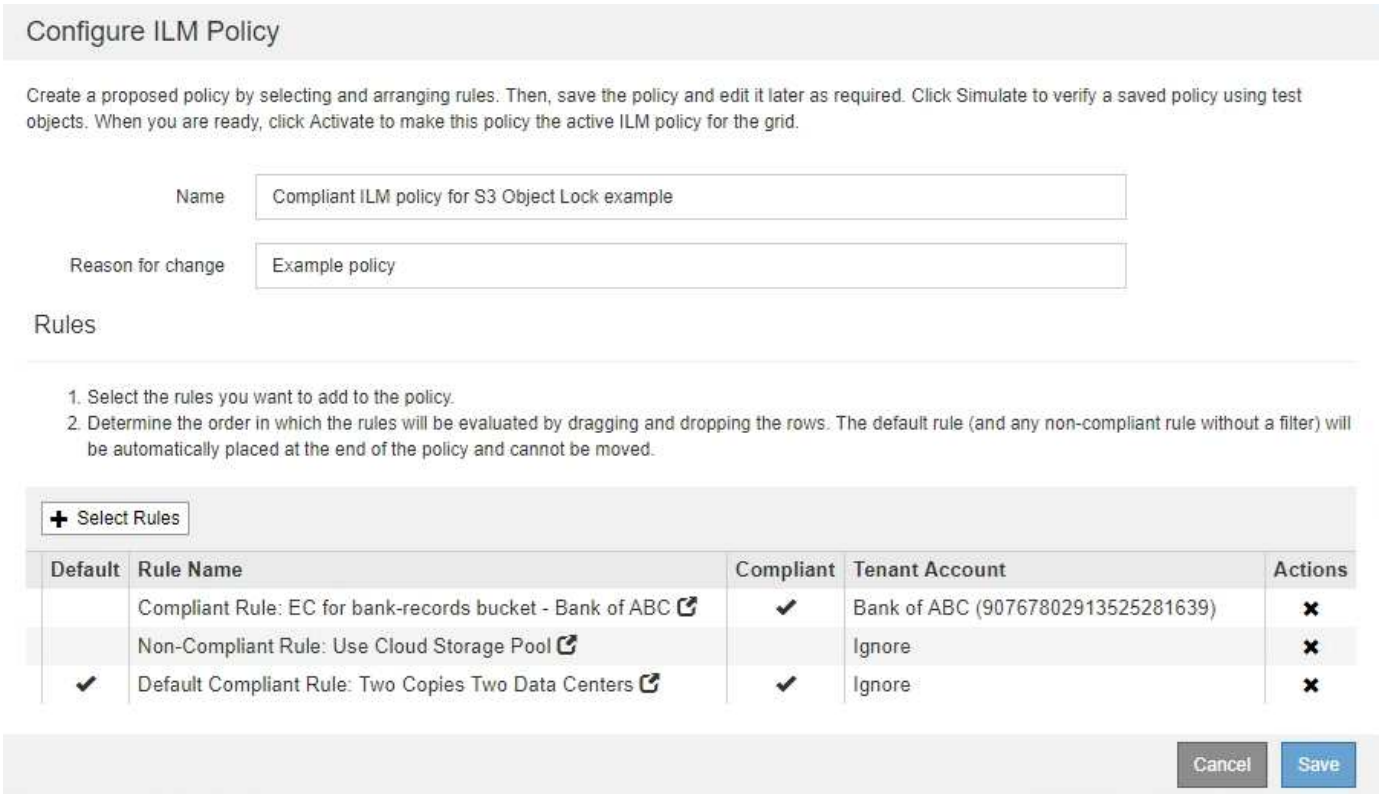
Hinzufügen von Regeln zu der Richtlinie

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 200 KB in

einem bestimmten Bucket zu schützen, wobei S3 Object Lock aktiviert ist. 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.



Simulation der vorgeschlagenen 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 in den Bucket-Bankdatensätzen für den Mandanten der Bank of ABC größer als 200 KB 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 mit einer Größe von 200 KB oder kleiner in den Bucket-Bankaufzeichnungen für den Mandanten der Bank of ABC
  - Objekte in jedem anderen Bucket, bei dem die S3-Objektsperre für alle anderen Mandantenkonten aktiviert ist

Richtlinie wird aktiviert

Wenn Sie mit der neuen Richtlinie zufrieden sind, dass Objektdaten wie erwartet geschützt werden, können

Sie sie aktivieren.

Systemhärtung

Informieren Sie sich über Systemeinstellungen, Best Practices und Empfehlungen zum Schutz eines StorageGRID-Systems vor Sicherheitsbedrohungen.

- "Sicherung eines StorageGRID Systems"
- "Hardening-Richtlinien für Software Upgrades"
- "Hardening Guidelines for StorageGRID Networks"
- "Hardening-Richtlinien für StorageGRID-Knoten"
- "Härtungsrichtlinien für Serverzertifikate"
- "Andere Hinweise zur Verhärtung"]

Sicherung eines StorageGRID Systems

Systemhärtung ist der Prozess, bei dem so viele Sicherheitsrisiken wie möglich durch ein StorageGRID System beseitigt werden.

Dieses Dokument bietet einen Überblick über die StorageGRID-spezifischen Härtungsrichtlinien. Diese Richtlinien sind eine Ergänzung zu branchenüblichen Best Practices zur Systemhärtung. In diesen Richtlinien wird beispielsweise davon ausgegangen, dass Sie für StorageGRID starke Passwörter verwenden, HTTPS statt HTTP verwenden und sofern verfügbar die zertifikatbasierte Authentifizierung aktivieren.

Bei der Installation und Konfiguration von StorageGRID können Sie diese Richtlinien nutzen, um alle vorgeschriebenen Sicherheitsziele bezüglich Vertraulichkeit, Integrität und Verfügbarkeit des Informationssystems zu erfüllen.

StorageGRID folgt *NetApp Richtlinie zur Handhabung von Schwachstellen*. Gemeldete Schwachstellen werden gemäß dem Prozess der Reaktion auf Produktsicherheitsvorfälle überprüft und behoben.

Allgemeine Überlegungen zur Erhöhung der Sicherheit eines StorageGRID-Systems

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 eines Docker Containers auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattformtyp verfügt über eigene Best Practices zur Härtung.
- Wie vertrauenswürdig sind die Mandantenkonten? Wenn Sie ein Service-Provider mit nicht vertrauenswürdigen Mandantenkonten sind, haben Sie andere Sicherheitsbedenken als, wenn Sie nur vertrauenswürdige interne Mandanten verwenden.
- Welche Sicherheitsanforderungen und -Konventionen von Ihrem Unternehmen erfüllt werden? Möglicherweise müssen Sie bestimmte gesetzliche oder unternehmensbezogene Anforderungen einhalten.

Verwandte Informationen

"Richtlinie Zum Umgang Mit Schwachstellen"

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 Versionen von StorageGRID oft Funktionen zur Erhöhung der Sicherheit, die in früheren Versionen nicht enthalten sind.

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 auf der StorageGRID Software Download-Seite herunterladen. Schritt-für-Schritt-Anleitungen zum Aktualisieren der StorageGRID-Software finden Sie in den Anweisungen zum Aktualisieren von StorageGRID. Anweisungen zum Anwenden eines Hotfix finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

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.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

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.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Upgrade 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.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Verwandte Informationen

"NetApp Downloads: StorageGRID"

"Software-Upgrade"

"Verwalten Sie erholen"

"NetApp Interoperabilitäts-Matrix-Tool"

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.

Richtlinien für das Grid-Netzwerk

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 das Admin-Netzwerk

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. Informationen zu Ihrer Plattform finden Sie in der Liste der internen Ports im Installationshandbuch.
- Wenn nicht vertrauenswürdige Clients auf das Admin-Netzwerk zugreifen können, blockieren Sie den Zugriff auf StorageGRID im Admin-Netzwerk mit einer externen Firewall.

Richtlinien für das Client-Netzwerk

Das Client-Netzwerk wird 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. Informationen zu Ihrer Plattform finden Sie in der Liste der internen Ports im Installationshandbuch.

- Eingehende Clientdatenverkehr nur an explizit konfigurierten Endpunkten akzeptieren. Informationen zum Verwalten von nicht vertrauenswürdigen Clientnetzwerken finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"Netzwerkrichtlinien"

"Gittergrundierung"

"StorageGRID verwalten"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

Hardening-Richtlinien für StorageGRID-Knoten

StorageGRID Nodes können auf VMware Virtual Machines, innerhalb eines Docker Containers auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattformtyp und jeder Node-Typ verfügt über eigene Best Practices zur Härtung.

Firewall-Konfiguration

Im Rahmen des System-Hardening-Prozesses müssen Sie externe Firewall-Konfigurationen überprüfen und ändern, damit der Datenverkehr nur von den IP-Adressen und den Ports akzeptiert wird, von denen er unbedingt benötigt wird.

Bei Nodes, die auf VMware Plattformen und StorageGRID Appliances ausgeführt werden, kommt eine interne Firewall zum Einsatz, die automatisch gemanagt wird. Diese interne Firewall bietet zwar eine zusätzliche Schutzschicht gegen häufig vorgängige Bedrohungen, sie macht aber keine externe Firewall erforderlich.

Eine Liste aller von StorageGRID verwendeten internen und externen Ports finden Sie im Installationsleitfaden für Ihre Plattform.

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. Gehen Sie nicht davon aus, dass der Hypervisor-Schutz Malware den Zugriff auf StorageGRID geschützte Daten verhindert, wenn sowohl StorageGRID als auch die Malware auf derselben physischen Hardware vorhanden sind. So nutzen beispielsweise die Meltdown- und Specter-Angriffe kritische Schwachstellen in modernen Prozessoren und ermöglichen Programmen, Daten im Arbeitsspeicher auf demselben Computer zu stehlen.

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 Client-Zugriff auf die Audit-Shares für CIFS oder NFS zu konfigurieren, blockieren oder deaktivieren Sie den Zugriff auf diese Dienste.

Schutz von Nodes während der Installation

Erlauben Sie nicht, nicht vertrauenswürdigen Benutzern über das Netzwerk auf StorageGRID-Knoten zuzugreifen, wenn die Knoten installiert werden. Nodes sind erst dann vollständig gesichert, 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 Mandanten nicht vertrauenswürdig sind, dürfen sie keinen direkten Zugriff auf den Mandantenmanager oder die Mandantenmanagement-API haben. Verwenden Sie stattdessen ein Mandantenportal oder ein externes Mandantenmanagement-System, das mit der Mandantenmanagement-API interagiert.
- Optional können Sie einen Admin-Proxy verwenden, um mehr Kontrolle über die AutoSupport Kommunikation von Admin Nodes zur NetApp Unterstützung zu erhalten. Lesen Sie die Schritte zum Erstellen eines Admin-Proxys in den Anweisungen zur Administration von StorageGRID.
- 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 zum Verwalten 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.

- Aktivieren Sie keine Outbound-Services für nicht vertrauenswürdige Mandanten. Wenn Sie beispielsweise das Konto für einen nicht vertrauenswürdigen Mandanten erstellen, dürfen Sie dem Mandanten nicht erlauben, seine eigene Identitätsquelle zu verwenden, und lassen Sie die Nutzung von Plattformdiensten nicht zu. Informationen zum Erstellen eines Mandantenkontos finden Sie in den Anweisungen für die Administration von StorageGRID.
- 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. Lesen

Sie die Schritte zum Erstellen eines Speicher-Proxy in den Anweisungen für die Administration von StorageGRID.

- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **Konfiguration** > **Netzwerkeinstellungen** > **nicht vertrauenswürdiges Clientnetzwerk** aus, und geben Sie an, dass das Client-Netzwerk auf dem Speicherknoten 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 anstatt den CLB-Service auf Gateway-Nodes zu verwenden. Lesen Sie in den Anweisungen zur Administration von StorageGRID die Schritte zum Verwalten des Lastausgleichs.

  Der CLB-Service ist veraltet.

- 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 **Konfiguration** > **Netzwerkeinstellungen** > **nicht vertrauenswürdiges Clientnetzwerk** aus, und geben Sie an, dass das Client-Netzwerk auf dem Gateway-Knoten 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.
- 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.

- Bei Appliances ohne FDE- oder FIPS-Laufwerke ermöglicht die Node-Verschlüsselung mithilfe eines Key Management Servers (KMS).

Hinweise zur Installation und Wartung Ihrer StorageGRID Hardware-Appliance finden Sie in der Installations- und Wartungsanleitung.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"SG100 SG1000 Services-Appliances"

"SG5600 Storage Appliances"

"SG5700 Storage-Appliances"

"SG6000 Storage-Appliances"

Härtungsrichtlinien für Serverzertifikate

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:

- **Management Interface Server Certificate**: Wird verwendet, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern.
- **Object Storage API Service Endpoints Serverzertifikat**: Wird verwendet, um den Zugriff auf Storage-Nodes und Gateway-Nodes zu sichern, die S3- und Swift-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

> StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie in den Schritten zum Konfigurieren von Load Balancer-Endpunkten in den Anweisungen zur Verwaltung von StorageGRID.

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 von dieser Richtlinie ist das Zertifikat für einen virtualisierten S3-Endpunkt im gehosteten Stil. Dazu ist die Verwendung eines Platzhalters erforderlich, wenn Bucket-Namen vorab nicht 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.

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.

Weitere Informationen zu StorageGRID-Protokollen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung. Weitere Informationen zu StorageGRID-Audit-Meldungen finden Sie in den Anweisungen für Audit-Meldungen.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID können Sie proaktiv den Systemzustand überwachen und automatisch Nachrichten und Details an den technischen Support von NetApp, das interne Support-Team Ihres Unternehmens oder einen Support-Partner senden. Standardmäßig sind AutoSupport Meldungen an den technischen Support von NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert ist.

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 sensible Natur von AutoSupport Meldungen empfiehlt NetApp dringend, HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an die NetApp Unterstützung zu verwenden.

Optional können Sie einen Admin-Proxy für mehr Kontrolle über die AutoSupport Kommunikation von Admin Nodes zum technischen Support von NetApp konfigurieren. Lesen Sie die Schritte zum Erstellen eines Admin-Proxys in den Anweisungen zur Administration von StorageGRID.

Cross-Origin Resource Sharing (CORS)

Die Cross-Origin Resource Sharing (CORS) kann für einen S3-Bucket konfiguriert werden, wenn für Web-Applikationen in anderen Domänen auf diesen Bucket und Objekte in diesem Bucket zugegriffen werden soll. Aktivieren Sie CORS im Allgemeinen nur, wenn dies erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Herkunft.

Lesen Sie die Schritte zum Konfigurieren der Cross-Origin Resource Sharing (CORS) in der Anleitung zur Verwendung von Mandantenkonten.

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.

Verwandte Informationen

"Monitor Fehlerbehebung"

"Prüfung von Audit-Protokollen"

"Verwenden Sie ein Mandantenkonto"

"StorageGRID verwalten"

Konfigurieren Sie StorageGRID für FabricPool

Erfahren Sie, wie Sie StorageGRID als NetApp FabricPool Cloud Tier konfigurieren.

- "StorageGRID für FabricPool wird konfiguriert"
- "Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier"
- "Informationslebenszyklus-Management von StorageGRID bei FabricPool-Daten ein"
- "Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool"
- "Weitere Best Practices für StorageGRID und FabricPool"

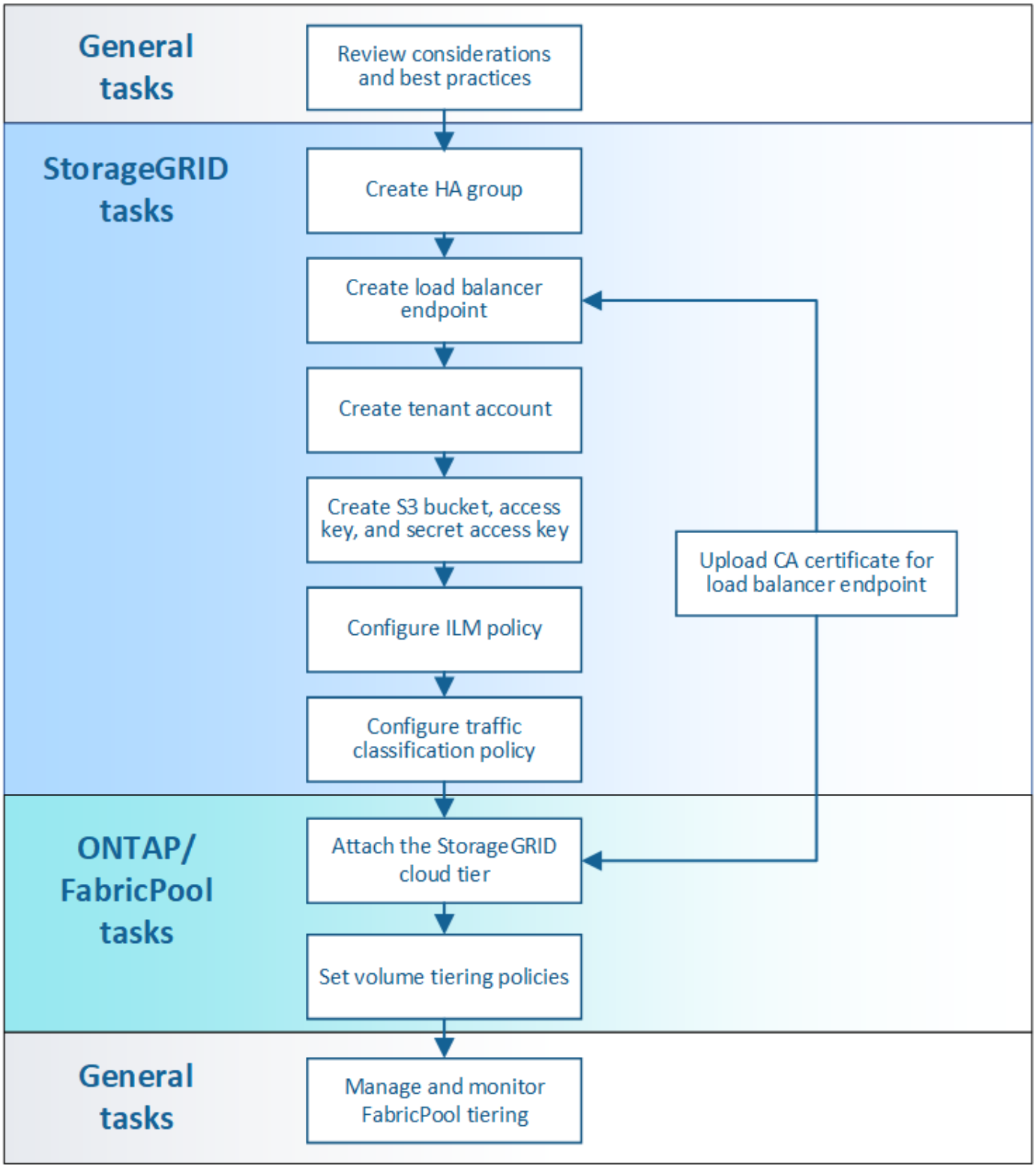
StorageGRID für FabricPool wird konfiguriert

Wenn Sie NetApp ONTAP verwenden, können Sie mit NetApp FabricPool inaktive oder kalte Daten auf einem NetApp StorageGRID Objekt-Storage-System verschieben.

Mithilfe dieser Anweisungen können Sie:

- Hier erhalten Sie einen Überblick über die Konfiguration eines StorageGRID Objekt-Storage-Systems zur Verwendung mit FabricPool.
- Informieren Sie sich, wie Sie ONTAP Informationen erhalten, wenn Sie StorageGRID als FabricPool Cloud-Tier hinzufügen.

- Best Practices für die Konfiguration der StorageGRID Information Lifecycle Management (ILM)-Richtlinie, einer StorageGRID Traffic-Klassifizierungsrichtlinie und weiterer StorageGRID-Optionen für einen FabricPool-Workload.



Was Sie benötigen

Bevor Sie folgende Anweisungen verwenden:

- 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 Systemsoftware vertraut, einschließlich Grid Manager und Tenant Manager.

Verwandte Informationen

- "TR-4598: FabricPool Best Practices für ONTAP 9.8"
- "ONTAP 9 Dokumentationszentrum"

Was ist FabricPool

FabricPool ist eine ONTAP Hybrid-Storage-Lösung mit einem hochperformanten Flash-Aggregat als Performance-Tier und einem Objektspeicher als Cloud-Tier. Die Daten in einer FabricPool werden in einer Tier gespeichert, basierend darauf, ob häufig darauf zugegriffen wird oder nicht. Mit einer FabricPool senken Sie die Storage-Kosten, ohne dabei Einbußen bei Performance, Effizienz oder Sicherung hinnehmen zu müssen.

Es sind keine Änderungen an der Architektur erforderlich und die Datenbank- und Applikationsumgebung lässt sich weiterhin über das zentrale ONTAP Storage-System managen.

Was ist Objekt-Storage

Objekt-Storage ist eine Storage-Architektur, die Daten als Objekte managt, anstatt anderer Storage-Architekturen wie Datei- oder Block-Storage. Objekte werden in einem einzelnen Container (z. B. in einem Bucket) aufbewahrt und sind 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 enthalten.

Nutzung von StorageGRID als Cloud-Tier von FabricPool

FabricPool kann ONTAP Daten zu verschiedenen Objektspeicher-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.

Verwendung mehrerer ONTAP Cluster mit StorageGRID

In diesen Anweisungen wird beschrieben, wie StorageGRID mit einem einzelnen ONTAP Cluster verbunden werden. Es empfiehlt sich jedoch, dasselbe StorageGRID System mit mehreren ONTAP Clustern zu verbinden.

Die einzige Voraussetzung für das Tiering von Daten zwischen mehreren ONTAP Clustern zu einem einzelnen StorageGRID System ist, dass Sie für jedes Cluster einen anderen S3 Bucket verwenden müssen. Je nach Ihren Anforderungen können Sie für alle Cluster dieselbe HA-Gruppe (High Availability, HA-Gruppe), einen Load Balancer-Endpunkt und ein Mandantenkonto verwenden. Alternativ können Sie jede dieser Elemente für jedes Cluster konfigurieren.

Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier

Bevor Sie StorageGRID als Cloud Tier für FabricPool hinzufügen können, müssen Sie einige Konfigurationsschritte in StorageGRID ausführen, um bestimmte Werte zu erhalten.

Über diese Aufgabe

In der folgenden Tabelle werden die Informationen aufgeführt, die Sie ONTAP bereitstellen müssen, wenn Sie StorageGRID als Cloud-Tier für FabricPool anhängen. In den Themen in diesem Abschnitt wird erläutert, wie Sie den StorageGRID Grid Manager und den Tenant Manager verwenden, um die Informationen zu erhalten, die Sie benötigen.

> Die genauen Feldnamen und der Prozess, den Sie zur Eingabe der erforderlichen Werte in ONTAP verwenden, hängen davon ab, ob Sie die ONTAP CLI (Storage Aggregate Object-Store config create) oder ONTAP System Manager (**Storage** > **Aggregate & Disks** > **Cloud Tier**) verwenden.

Weitere Informationen finden Sie im Folgenden:

- "TR-4598: FabricPool Best Practices für ONTAP 9.8"
- "ONTAP 9 Dokumentationszentrum"

ONTAP Field	Beschreibung
Objektspeichername	Jeder eindeutige und beschreibende Name. Beispiel: `StorageGRID_Cloud_Tier`.
Anbietertyp	StorageGRID (System Manager) oder `SGWS` (CLI).
Port	Der Port, den FabricPool verwenden wird, wenn er eine Verbindung zu StorageGRID herstellt. Sie legen fest, welche Portnummer beim Definieren des StorageGRID Load Balancer-Endpunkts verwendet werden soll. "Erstellen eines Endpunkts für den Load Balancer für FabricPool"
Servername	Der vollständig qualifizierte Domänenname (FQDN) für den StorageGRID Load Balancer-Endpunkt. Beispiel: `s3.storagegrid.company.com`. Beachten Sie Folgendes: • Der hier angegebene Domänenname muss mit dem Domänennamen auf dem CA-Zertifikat übereinstimmen, das Sie für den StorageGRID Load Balancer-Endpunkt hochladen. • Der DNS-Datensatz für diesen Domain-Namen muss jeder IP-Adresse zugeordnet werden, die Sie zum Herstellen einer Verbindung zu StorageGRID verwenden werden. "Konfigurieren des DNS-Servers für StorageGRID-IP-Adressen"

ONTAP Field	Beschreibung
Containername	Der Name des StorageGRID-Buckets, den Sie mit diesem ONTAP-Cluster verwenden werden. Beispiel: `fabricpool-bucket`. Sie erstellen diesen Bucket im Tenant Manager. Beachten Sie Folgendes: • Der Bucket-Name kann nach dem Erstellen der Konfiguration nicht mehr geändert werden. • Für den Bucket ist die Versionierung nicht aktiviert. • Sie müssen einen anderen Bucket für jedes ONTAP Cluster verwenden, für das Daten in StorageGRID verschoben werden sollen. "Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"
Zugriffsschlüssel und geheimes Passwort	Der Zugriffsschlüssel und der geheime Zugriffsschlüssel für das StorageGRID-Mandantenkonto. Diese Werte generieren Sie im Tenant Manager. "Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"
SSL	Muss aktiviert sein.
Objektspeicherzertifikat	Das CA-Zertifikat, das Sie beim Erstellen des StorageGRID Load Balancer-Endpunkts hochgeladen haben. **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. "Erstellen eines Endpunkts für den Load Balancer für FabricPool"

Nachdem Sie fertig sind

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, können Sie unter ONTAP StorageGRID als Cloud-Tier hinzufügen, die Cloud-Ebene als Aggregat hinzufügen und die Tiering-Richtlinien für Volumes festlegen.

Best Practices für den Lastausgleich

Bevor Sie StorageGRID als FabricPool-Cloud-Tier anhängen, verwenden Sie den StorageGRID Grid-Manager, um mindestens einen Load Balancer-Endpunkt zu konfigurieren.

Was ist die Lastverteilung

Wenn Daten vom FabricPool zu einem StorageGRID System verschoben werden, verwendet StorageGRID einen Load Balancer zum Managen des Aufnahme- und Abrufs-Workloads. Der Lastausgleich maximiert die

Geschwindigkeit und die Verbindungskapazität, indem der FabricPool 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 bei Ihrem NetApp Ansprechpartner oder in den folgenden technischen Berichten:

"Optionen zum StorageGRID Load Balancer"

> Der separate Connection Load Balancer (CLB)-Service auf Gateway-Nodes ist veraltet und wird nicht mehr für die Verwendung mit FabricPool empfohlen.

Best Practices für den StorageGRID-Lastausgleich

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 einen Admin-Node und einen Gateway-Node oder sogar zwei Admin-Nodes enthalten. 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.

Sie müssen einen StorageGRID Load Balancer-Endpunkt konfigurieren, um den Port zu definieren, den Gateway-Knoten und Admin-Knoten für eingehende und ausgehende FabricPool-Anforderungen verwenden werden.

Best Practices für das Endpoint-Zertifikat für Load Balancer

Beim Erstellen eines Endpunkts für den Lastausgleich für die Verwendung mit FabricPool müssen Sie HTTPS als Protokoll verwenden. Sie können dann entweder ein Zertifikat hochladen, das entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert ist, oder Sie können ein selbstsigniertes Zertifikat generieren. Mit dem Zertifikat kann ONTAP sich mit StorageGRID authentifizieren.

Als Best Practice sollten Sie ein CA-Serverzertifikat verwenden, um die Verbindung zu sichern. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden.

Wenn Sie ein CA-Zertifikat zur Verwendung mit dem Endpunkt des Load Balancer anfordern, stellen Sie sicher, dass der Domänenname auf dem Zertifikat mit dem in ONTAP eingegebenen Servernamen für diesen Load Balancer-Endpunkt übereinstimmt. Wenn möglich, verwenden Sie einen Platzhalter (*), um virtuelle URLs im Hoststil zu ermöglichen. Beispiel:

```
*.s3.storagegrid.company.com
```

Wenn Sie StorageGRID als FabricPool Cloud Tier hinzufügen, müssen Sie beim ONTAP Cluster dasselbe Zertifikat sowie die Zertifikate „Root“ und „untergeordnete Certificate Authority“ (CA) installieren.

StorageGRID verwendet Serverzertifikate aus verschiedenen Gründen. Wenn Sie eine Verbindung zum Load Balancer-Dienst herstellen, müssen Sie das Object Storage API Service Endpoints Server Certificate nicht hochladen.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- "Managen des Lastausgleichs"
- "Härtungsrichtlinien für Serverzertifikate"

Best Practices für Hochverfügbarkeitsgruppen

Bevor Sie StorageGRID als FabricPool Cloud-Tier anhängen, können Sie mithilfe von StorageGRID Grid Manager eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren.

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist das

Um sicherzustellen, dass der Load Balancer-Service zum Verwalten von FabricPool-Daten immer verfügbar ist, können Sie die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes zu einer einzigen Einheit gruppieren, die als HA-Gruppe (High Availability, Hochverfügbarkeit) bezeichnet wird. Wenn der aktive Node in der HA-Gruppe ausfällt, kann der Workload weiterhin von einem anderen Node in der Gruppe gemanagt werden.

Jede HA-Gruppe ermöglicht einen hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes. Beispielsweise bietet eine HA-Gruppe, die aus allen Admin-Nodes besteht, hochverfügbaren Zugriff auf einige Management-Services für Admin-Nodes und den Load-Balancer-Service. Eine HA-Gruppe, die aus nur Gateway-Nodes oder Admin-Nodes und Gateway-Nodes besteht, bietet hochverfügbaren Zugriff auf den Shared Load Balancer Service.

Beim Erstellen einer HA-Gruppe wählen Sie Netzwerkschnittstellen aus, die zum Grid Network (eth0) oder dem Client-Netzwerk (eth2) gehören. Alle Schnittstellen in einer HA-Gruppe müssen sich im selben Netzwerk-Subnetz befinden.

Eine HA-Gruppe behält eine oder mehrere virtuelle IP-Adressen bei, die der aktiven Schnittstelle in der Gruppe hinzugefügt werden. Wenn die aktive Schnittstelle nicht mehr verfügbar ist, werden die virtuellen IP-Adressen in eine andere Schnittstelle verschoben. Dieser 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 Sie eine HA-Gruppe mit Nodes für den Lastausgleich konfigurieren, stellt FabricPool eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.

Best Practices für Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen

Die Best Practices zum Erstellen einer StorageGRID HA-Gruppe für FabricPool hängen vom Workload ab:

- Wenn Sie FabricPool für Daten mit primären Workloads verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Load-Balancing-Nodes umfasst, um eine Unterbrechung beim Datenabruf zu vermeiden.
- 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".

Konfigurieren des DNS-Servers für StorageGRID-IP-Adressen

Nach der Konfiguration von Hochverfügbarkeitsgruppen und Endpunkten des Load Balancer müssen Sie sicherstellen, dass das DNS (Domain Name System) für das ONTAP-System einen Datensatz enthält, um den StorageGRID-Servernamen (vollständig qualifizierter Domänenname) der IP-Adresse zuzuordnen, die FabricPool zum Herstellen von Verbindungen verwendet.

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, stellt FabricPool eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, kann FabricPool eine Verbindung zum StorageGRID Load Balancer Service herstellen. Dabei wird die IP-Adresse eines Gateway Node oder eines Admin-Nodes verwendet.

Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

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 besteht aus mindestens einer Netzwerkschnittstellen auf Admin-Nodes, Gateway-Nodes oder beiden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Jede HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes zu ermöglichen.

Weitere Informationen zu dieser Aufgabe. Siehe "Verwalten von Hochverfügbarkeitsgruppen".

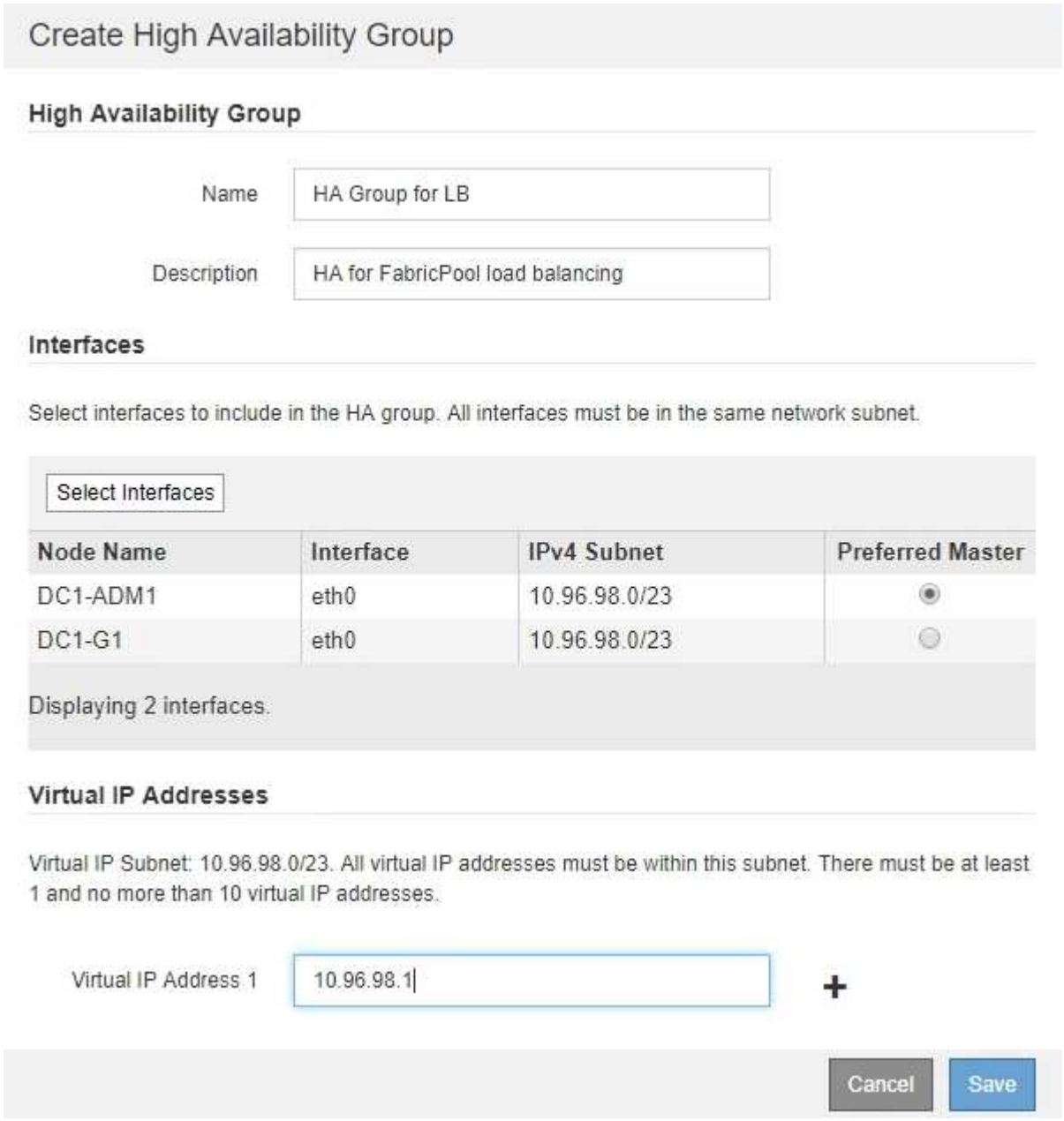
Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen**.
2. Wählen Sie eine oder mehrere der Netzwerkschnittstellen aus. Die Netzwerkschnittstellen müssen entweder im Grid Network (eth0) oder im Client Network (eth2) zum selben Subnetz gehören.
3. Weisen Sie einen Knoten als bevorzugter Master zu.

   Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden.

4. Geben Sie bis zu zehn IPv4-Adressen für die HA-Gruppe ein.

   Die Adressen müssen sich im IPv4-Subnetz befinden, das von allen Mitgliedschnittstellen gemeinsam genutzt wird.



Erstellen eines Endpunkts für den Load Balancer für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, konfigurieren Sie einen Endpunkt für den Load Balancer und laden das Endpoint-Zertifikat für den Load Balancer hoch, mit dem die Verbindung zwischen ONTAP und StorageGRID gesichert werden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

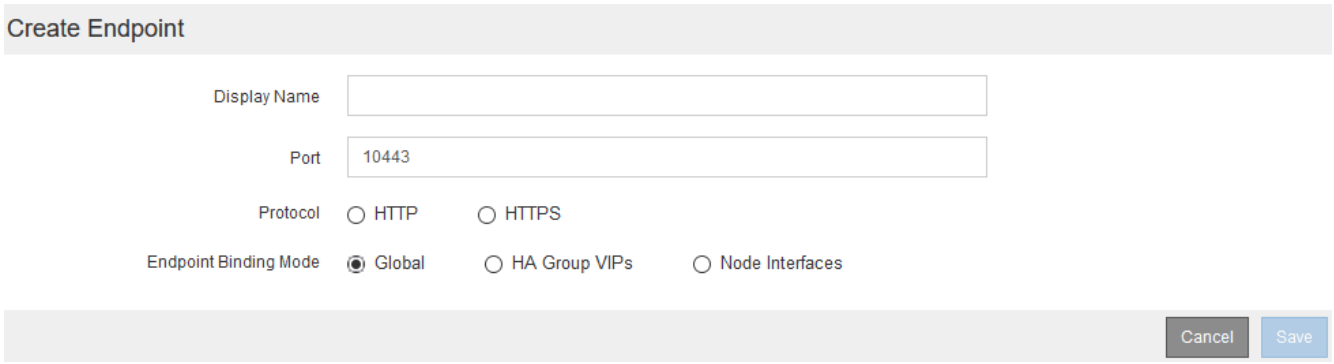
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie haben die folgenden Dateien:
  - Serverzertifikat: Die benutzerdefinierte Serverzertifikatdatei.
  - Server Certificate Private Key: Die private Schlüsseldatei des benutzerdefinierten Serverzertifikats.
  - CA-Paket: Eine einzelne Datei, die die Zertifikate jeder Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

Über diese Aufgabe

Weitere Informationen zu dieser Aufgabe finden Sie unter "Konfigurieren von Load Balancer-Endpunkten".

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**.



2. Wählen Sie **Endpunkt hinzufügen**.
3. Geben Sie die folgenden Informationen ein.

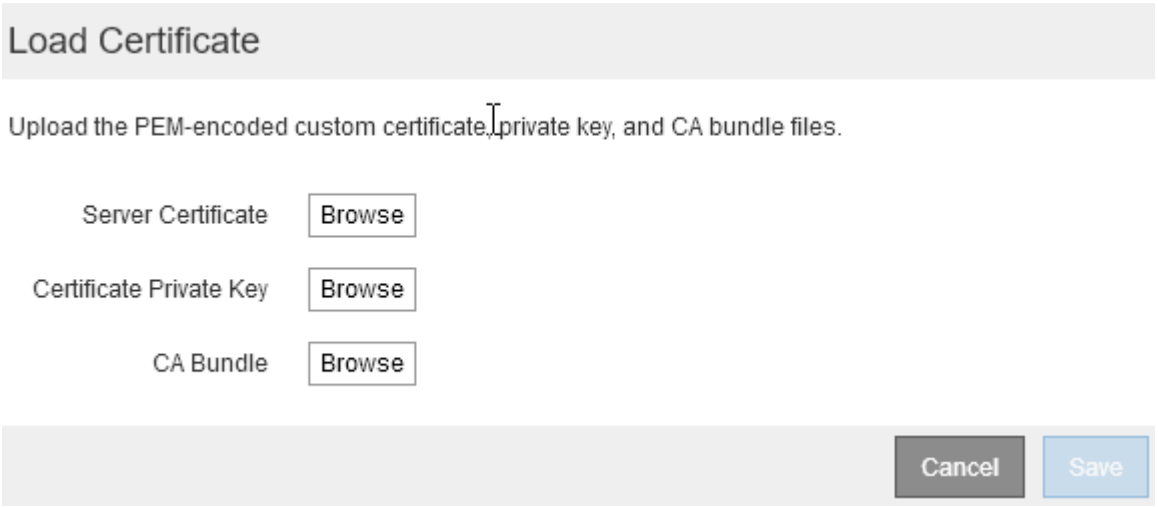
Feld	Beschreibung
Anzeigename	Einen beschreibenden Namen für den Endpunkt
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist standardmäßig auf 10433 eingestellt, Sie können jedoch alle nicht verwendeten externen Ports eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. **Hinweis:** Ports, die von anderen Netzdiensten verwendet werden, sind nicht zulässig. Siehe Liste der Anschlüsse, die für interne und externe Kommunikation verwendet werden: "Referenz für Netzwerk-Ports" Sie müssen diese Portnummer an ONTAP angeben, wenn Sie StorageGRID als FabricPool Cloud Tier anhängen.

Feld	Beschreibung
Protokoll	Muss **HTTPS** sein.
Endpunktbindungsmodus	Verwenden Sie die **Global**-Einstellung (empfohlen) oder beschränken Sie die Zugänglichkeit dieses Endpunkts auf einen der folgenden Elemente: • Spezifische virtuelle Hochverfügbarkeits-IP-Adressen (VIPs). Verwenden Sie diese Auswahl nur, wenn ein deutlich höheres Maß an Isolierung von Workloads erforderlich ist. • Spezielle Netzwerkschnittstellen bestimmter Nodes.

4. Wählen Sie **Speichern**.

   Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

5. Wählen Sie für * Endpoint Service Type* **S3** aus.
6. Wählen Sie **Zertifikat hochladen** (empfohlen) und navigieren Sie anschließend zu Ihrem Serverzertifikat, Ihrem privaten Zertifikatschlüssel und dem CA-Paket.



7. Wählen Sie **Speichern**.

Erstellen eines Mandantenkontos für FabricPool

Sie müssen ein Mandantenkonto im Grid Manager for FabricPool Use erstellen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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.

Sie können dasselbe Mandantenkonto für mehrere ONTAP Cluster verwenden. Oder Sie können bei Bedarf ein dediziertes Mandantenkonto für jedes ONTAP Cluster erstellen.

> Bei diesen Anweisungen wird davon ausgegangen, dass Sie Single Sign-On (SSO) für den Grid Manager konfiguriert haben. Wenn Sie kein SSO verwenden, befolgen Sie die Anweisungen für "Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet".

Schritte

1. Wählen Sie **Mieter**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Anzeigenamen für das FabricPool-Mandantenkonto ein.
4. Wählen Sie **S3**.
5. Lassen Sie das Kontrollkästchen **Plattformdienste zulassen** aktiviert, um die Nutzung von Plattformdiensten zu aktivieren.

   Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen.
6. Lassen Sie das Feld **Storage Quota** leer.
7. Wählen Sie im Feld **Root Access Group** eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root Access-Berechtigung für den Mandanten zu erhalten.
8. Wählen Sie **Speichern**.

Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels

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.

Was Sie benötigen

- Sie müssen ein Mandantenkonto für die Nutzung von FabricPool erstellt haben.

Über diese Aufgabe

In diesen Anweisungen wird die Verwendung von StorageGRID Mandanten-Manager zur Erstellung eines Buckets beschrieben und Zugriffschlüssel erhalten. Sie können diese Aufgaben auch mit der Mandantenmanagement-API oder der StorageGRID S3 REST-API ausführen.

Weitere Informationen:

- "Verwenden Sie ein Mandantenkonto"
- "S3 verwenden"

Schritte

1. Melden Sie sich beim Tenant Manager an.

   Sie können eine der folgenden Aktionen ausführen:

- Wählen Sie auf der Seite Mandantenkonten im Grid Manager den Link **Anmelden** für den Mieter aus, und geben Sie Ihre Anmeldedaten ein.
- Geben Sie die URL für das Mandantenkonto in einem Webbrowser ein, und geben Sie Ihre Anmeldedaten ein.

2. Erstellung eines S3-Buckets für FabricPool-Daten

   Sie müssen für jedes zu verwendende ONTAP Cluster einen eindeutigen Bucket erstellen.

   a. Wählen Sie **STORAGE (S3)** > **Buckets** aus.
   b. Wählen Sie **Eimer erstellen**.
   c. Geben Sie den Namen des StorageGRID-Buckets ein, den Sie mit FabricPool verwenden möchten. Beispiel: `fabricpool-bucket`.

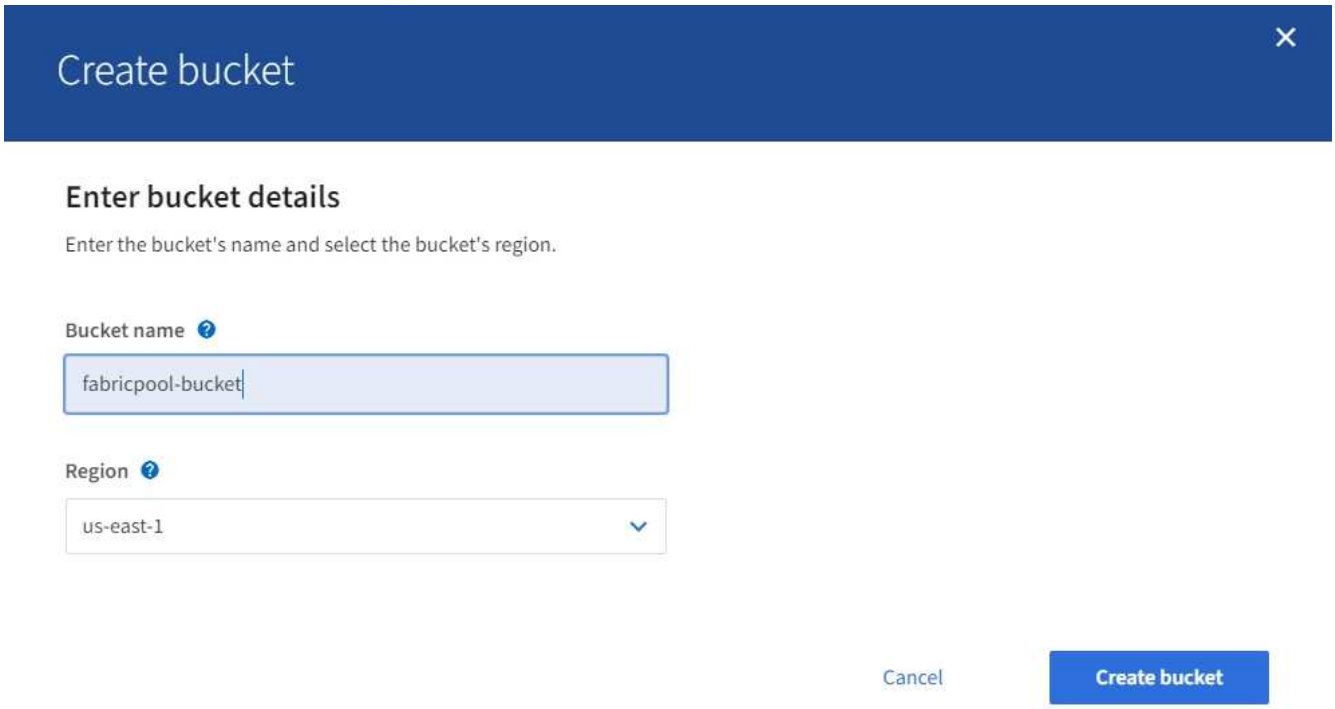
      Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

      Bucket-Namen müssen folgende Regeln einhalten:

      - 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.

   d. Wählen Sie die Region für diesen Bucket aus.

      Standardmäßig werden alle Buckets im erstellt `us-east-1` Werden.



a. Wählen Sie **Eimer erstellen**.

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 einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel erstellen, vergessen Sie nicht, die entsprechenden Werte in ONTAP sofort zu aktualisieren, um sicherzustellen, dass ONTAP Daten unterbrechungsfrei in StorageGRID speichern und abrufen kann.

Informationslebenszyklus-Management von StorageGRID bei FabricPool-Daten ein

Wenn Sie FabricPool für das Tiering von Daten zu StorageGRID verwenden, müssen Sie die Anforderungen für die Erstellung von StorageGRID Information Lifecycle Management (ILM)-Regeln und eine ILM-Richtlinie für das Management von FabricPool-Daten kennen. Sie müssen sicherstellen, dass die ILM-Regeln für FabricPool Daten nicht von Unterbrechungen geprägt sind.

FabricPool ist nicht mit den StorageGRID ILM-Regeln oder -Richtlinien bekannt. Wenn die StorageGRID ILM-Richtlinie falsch konfiguriert ist, kann es zu Datenverlusten kommen.

Weitere Informationen: "Objektmanagement mit ILM"

ILM-Richtlinien für FabricPool-Daten

Diese Richtlinien prüfen, um sicherzustellen, dass Ihre ILM-Regeln und ILM-Richtlinien für FabricPool Daten und Ihre geschäftlichen Anforderungen geeignet sind. Wenn Sie bereits StorageGRID ILM verwenden, müssen Sie möglicherweise 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. Bei Erasure Coding erfolgt eine höhere CPU-Auslastung, allerdings deutlich weniger Storage-Kapazität als mit Replizierung. Die Schemata 4+1 und 6+1 benötigen weniger Kapazität als 2+1, aber zu den Kosten eines niedrigeren Durchsatzes und weniger Flexibilität, wenn Sie Storage-Nodes während der Grid-Erweiterung hinzufügen.

- 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.

- Verwenden Sie keine ILM-Regel, die Daten des FabricPool Cloud-Tiers ablaufen oder löschen soll. Legen Sie die Aufbewahrungsdauer in jeder ILM-Regel auf „Forever“ fest, um zu gewährleisten, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.
- Erstellen Sie keine Regeln, nach denen FabricPool Cloud-Tiering-Daten aus dem Bucket in einen anderen Speicherort verschoben werden. Mit den ILM-Regeln können FabricPool-Daten nicht mithilfe eines Archivierungs-Nodes auf Band archiviert werden, oder es kann ein Cloud-Storage-Pool zum Verschieben von FabricPool-Daten auf Glacier verwendet werden.

  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.

Beispiel für eine ILM-Richtlinie für FabricPool-Daten

Nutzen Sie diese einfache Beispielrichtlinie als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien.

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: "Objektmanagement mit ILM"

Schritte

1. Erstellen Sie einen Speicherpool mit dem Namen **DEN**. Wählen Sie den Standort Denver aus.
2. Erstellen Sie ein Erasure-Coding-Profil mit dem Namen **2 plus 1**. Wählen Sie die 2+1-Löschcodierung und den **DEN**-Speicherpool aus.
3. 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 plus 1 Erasure Coding für FabricPool-Daten
Bucket-Name	`fabricpool-bucket` Sie könnten auch nach dem FabricPool-Mandantenkonto filtern.
Erweiterte Filterung	Objektgröße (MB) größer als 0.2 MB. **Hinweis:** FabricPool schreibt nur 4 MB Objekte, aber Sie müssen einen Filter für Objektgröße hinzufügen, da diese Regel das Erasure Coding verwendet.
Referenzzeit	Aufnahmezeit
Platzierung	Ab Tag 0 dauerhaft speichern
Typ	Erasure Coding
Standort	DEN (2 plus 1)
Aufnahmeverhalten	Ausgeglichen

4. Erstellen einer ILM-Regel, die zwei replizierte Kopien von Objekten erstellt, die nicht mit der ersten Regel übereinstimmt. Wählen Sie keinen grundlegenden Filter (Mandantenkonto oder Bucket-Name) oder erweiterte Filter aus.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket-Name	*None*
Erweiterte Filterung	*None*
Referenzzeit	Aufnahmezeit
Platzierung	Ab Tag 0 dauerhaft speichern
Typ	Datenreplizierung
Standort	DEN
Kopien	2
Aufnahmeverhalten	Ausgeglichen

5. Erstellen Sie eine vorgeschlagene ILM-Richtlinie und wählen Sie beide Regeln aus. Da die Replikationsregel keine Filter verwendet, kann es sich um die Standardregel (letzte) für die Richtlinie handelt.
6. Aufnahme von Testobjekten in das Raster
7. Simulieren Sie die Richtlinie mit den Testobjekten, um das Verhalten zu überprüfen.
8. 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 von Erasure Coding und replizierten Kopien werden in StorageGRID aufbewahrt, bis sie vom S3 Client gelöscht werden. StorageGRID ILM löscht diese Elemente nie.

Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool

Optional können Sie eine StorageGRID Traffic-Klassifizierungsrichtlinie entwerfen, um die Servicequalität für den FabricPool-Workload zu optimieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Die Best Practices für das Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool hängen vom Workload ab:

- Wenn Sie einen Tiering von primären FabricPool-Workload-Daten zu StorageGRID planen, sollten Sie sicherstellen, dass der FabricPool-Workload den Großteil 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 keine Grenzen für die Servicequalität für jeden FabricPool Workload gesetzt werden, sondern lediglich die anderen Workloads begrenzt werden.
- Die für andere Workloads gesetzten Grenzen müssen möglicherweise weit sein, um das unbekannte Verhalten dieser Workloads zu berücksichtigen. Die auferlegten Einschränkungen hängen auch von der Größe und den Funktionen des Grids und der erwarteten Auslastung ab.

Weitere Informationen: "Verwalten von Richtlinien für die Verkehrsklassifizierung"

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.
2. Geben Sie einen Namen und eine Beschreibung ein.
3. Erstellen Sie im Abschnitt Regeln für die Abgleich mindestens eine Regel.
   a. Wählen Sie **Erstellen**.
   b. Wählen Sie **Endpunkt** aus, und wählen Sie den für FabricPool erstellten Load Balancer-Endpunkt aus.

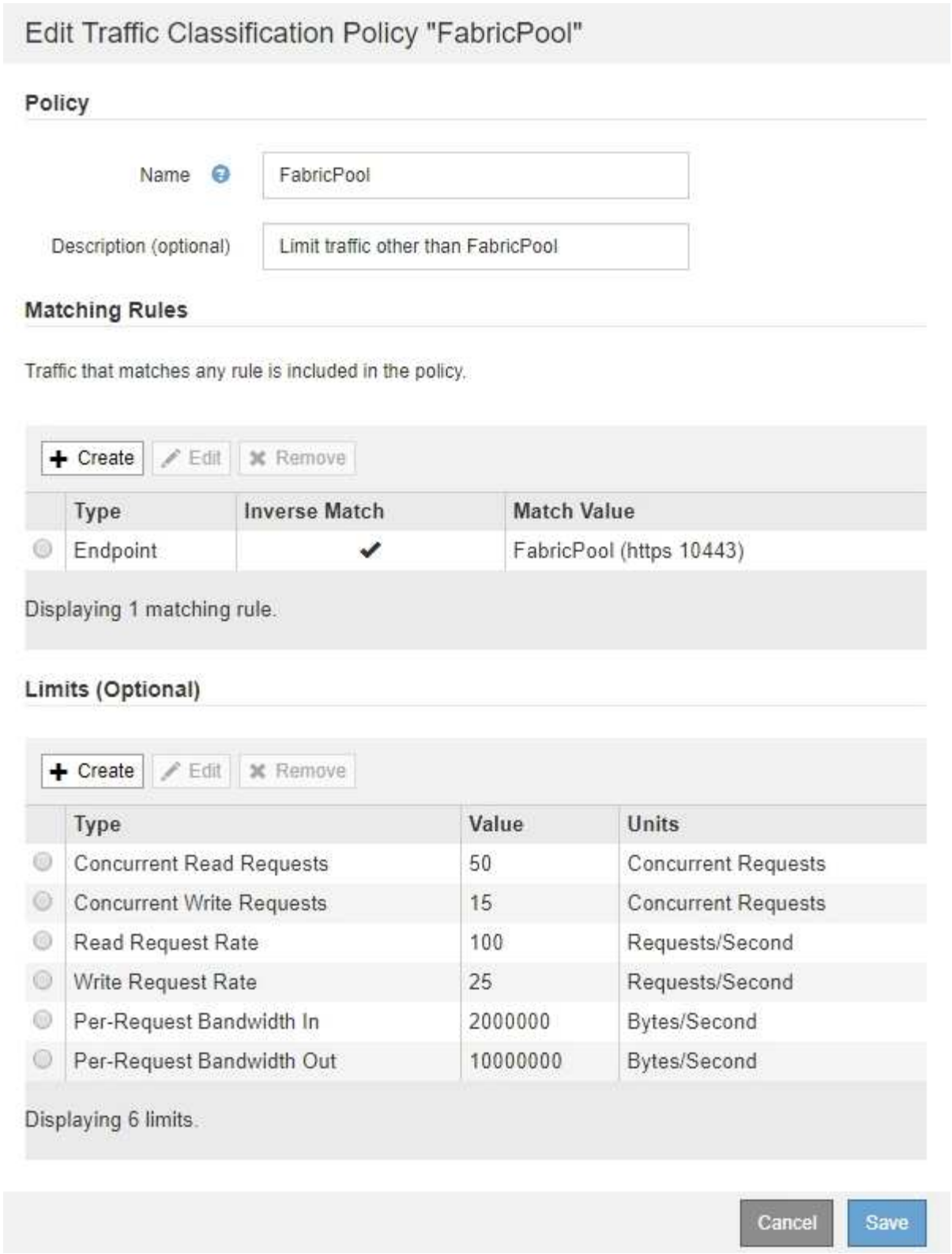
      Sie können auch das FabricPool-Mandantenkonto oder den Bucket auswählen.

   c. Wenn diese Verkehrsrichtlinie den Datenverkehr für die anderen Endpunkte einschränken soll, wählen Sie **Inverse Übereinstimmung**.
4. Optional können Sie eine oder mehrere Limits erstellen.

   Auch wenn für eine Traffic-Klassifizierungsrichtlinie keine Grenzen festgelegt sind, werden Kennzahlen erfasst, um Verkehrstrends zu verstehen.

   a. Wählen Sie **Erstellen**.
   b. Wählen Sie den zu begrenzenden Verkehrstyp und die anzuwählenden Grenzwerte aus.

      In diesem Beispiel FabricPool werden die Typen des Netzwerkdatenverkehrs, den Sie begrenzen können, sowie die Arten von Werten aufgeführt, die Sie auswählen können. Die Traffic-Typen und -Werte für eine tatsächliche Richtlinie basieren auf Ihren spezifischen Anforderungen.



5. Wählen Sie nach dem Erstellen der Traffic-Klassifizierungsrichtlinie die Richtlinie aus und wählen Sie dann **Metriken** aus, um festzustellen, ob die Richtlinie den Datenverkehr wie erwartet begrenzt.

Weitere Best Practices für StorageGRID und FabricPool

Wenn Sie ein StorageGRID-System für die Verwendung mit FabricPool konfigurieren, sollten Sie die Einstellung globaler Optionen vermeiden, die sich auf die Speicherung Ihrer Daten auswirken könnten.

Objektverschlüsselung

Bei der Konfiguration von StorageGRID können Sie optional die globale **gespeicherte Objektverschlüsselung**-Einstellung aktivieren, wenn für andere StorageGRID-Clients eine Datenverschlüsselung erforderlich ist (**Konfiguration** > **Systemeinstellungen** > **Rasteroptionen**). 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 bei der Konfiguration von StorageGRID nicht die globale **Komprimierung gespeicherter Objekte**-Einstellung (**Konfiguration** > **Systemeinstellungen** > **Rasteroptionen**). Die Daten, die von FabricPool zu StorageGRID verschoben werden, werden bereits komprimiert. Durch das Aktivieren von **compress gespeicherter Objekte** wird die Größe eines Objekts nicht weiter verringert.

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 **available** oder eine andere Konsistenzstufe zu verwenden.

FabricPool Tiering

Wenn der StorageGRID-Node Storage verwendet, der einem NetApp AFF System zugewiesen ist, 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.

Verwenden Sie StorageGRID

Verwenden Sie ein Mandantenkonto

StorageGRID-Mandantenkonto nutzen

- "Verwenden des Mandanten-Manager"
- "Managen des Systemzugriffs für Mandantenbenutzer"
- "Verwalten von S3-Mandantenkonten"
- "Verwalten von S3-Plattformservices"

Verwenden des Mandanten-Manager

Der Tenant Manager ermöglicht das Management aller Aspekte eines StorageGRID-Mandantenkontos.

Mit dem Mandanten-Manager lässt sich die Storage-Auslastung eines Mandantenkontos überwachen und Benutzer mit Identitätsföderation bzw. durch das Erstellen von lokalen Gruppen und Benutzern managen. Bei S3-Mandantenkonten können Sie auch S3-Schlüssel managen, S3-Buckets managen und Plattform-Services konfigurieren.

Verwenden eines StorageGRID-Mandantenkontos

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 eigene föderierte bzw. lokale Gruppen, Benutzer, S3 Buckets oder Swift Container und Objekte.

Optional können Mandantenkonten verwendet werden, um gespeicherte Objekte nach verschiedenen 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. Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie unter.

- **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 von Mandantenkonten

Mandantenkonten werden von einem StorageGRID Grid-Administrator mit dem Grid Manager erstellt. Beim Erstellen eines Mandantenkontos gibt der Grid-Administrator die folgenden Informationen an:

- Anzeigename für den Mandanten (die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden).
- Gibt an, ob das Mandantenkonto das S3 oder Swift verwenden wird
- Bei S3-Mandantenkonten: Unabhängig davon, ob das Mandantenkonto Plattform-Services nutzen darf. Wenn die Nutzung von Plattformdiensten zulässig ist, muss das Grid so konfiguriert werden, dass es seine Verwendung unterstützt.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte verfügbar sind. Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.
- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.
- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Grid-Administratoren können zudem die S3-Objektsperreneinstellung 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.

Konfigurieren von S3-Mandanten

Nachdem ein S3-Mandantenkonto erstellt wurde, können Sie auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) oder Erstellen lokaler Gruppen und Benutzer
- Verwalten von S3-Zugriffsschlüsseln
- Erstellung und Management von S3 Buckets, einschließlich konformer Buckets
- Verwenden von Plattform-Services (falls aktiviert)
- Monitoring der Storage-Auslastung

> Während Sie mit Mandanten-Manager S3-Buckets erstellen und managen können, müssen Sie über S3-Zugriffsschlüssel verfügen und die S3-REST-API verwenden, um Objekte aufzunehmen und zu managen.

Konfiguration von Swift Mandanten

Nach der Erstellung eines Swift-Mandantenkontos können Benutzer mit Root Access-Berechtigung auf den Mandanten-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 den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht 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.

Verwandte Informationen

"StorageGRID verwalten"

"S3 verwenden"

"Verwenden Sie Swift"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Tenant Manager an

Sie greifen auf den Tenant Manager zu, indem Sie die URL für den Mandanten in die Adressleiste eines unterstützten Webbrowsers eingeben.

Was Sie benötigen

- Sie müssen über Ihre Anmeldedaten verfügen.
- Sie müssen über eine URL auf den Tenant Manager zugreifen können, die von Ihrem 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 entweder den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse, die für den Zugriff auf einen Admin-Node verwendet wird, und kann optional auch eine Portnummer, die 20-stellige Mandantenkontokennung oder beide enthalten.

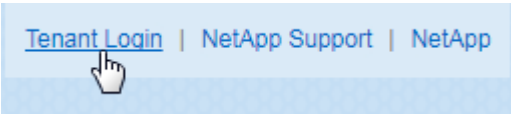
- Wenn die URL die 20-stellige Konto-ID des Mandanten nicht enthält, müssen Sie über diese Konto-ID verfügen.
- Sie müssen einen unterstützten Webbrowser verwenden.
- Cookies müssen in Ihrem Webbrowser aktiviert sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

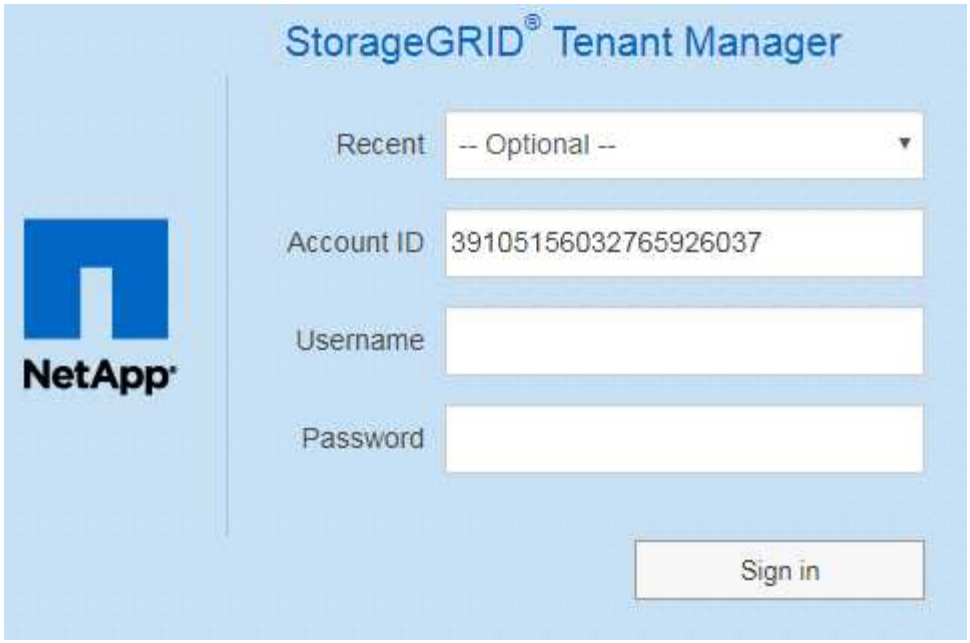
1. Starten Sie einen unterstützten Webbrowser.
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf Tenant Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie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

   Der Anmeldebildschirm, den Sie sehen, hängt von der eingegebenen URL ab und davon, ob Ihr Unternehmen Single Sign-On (SSO) verwendet. Sie sehen einen der folgenden Bildschirme:

   - Die Anmeldeseite des Grid Manager. Klicken Sie oben rechts auf den Link **Tenant Login**.

   - Die Anmeldeseite von Tenant Manager. Das Feld **Konto-ID** ist möglicherweise bereits ausgefüllt, wie unten gezeigt.



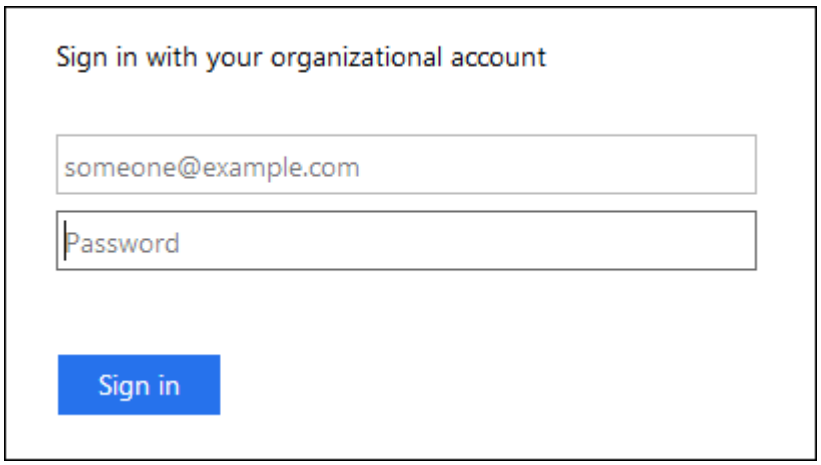
i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn er in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.

ii. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

iii. Klicken Sie auf **Anmelden**.

Das Tenant Manager Dashboard wird angezeigt.

◦ Falls SSO-Seite Ihres Unternehmens im Grid aktiviert ist, Beispiel:



Geben Sie Ihre Standard-SSO-Anmeldedaten ein, und klicken Sie auf **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. Klicken Sie auf **Anmelden**.

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

Das Tenant Manager Dashboard wird angezeigt.

5. Wenn Sie ein erstes Kennwort von einer anderen Person erhalten haben, ändern Sie Ihr Kennwort, um Ihr Konto zu sichern. Wählen Sie ***username*** > **Passwort ändern**.

> Wenn SSO für das StorageGRID-System aktiviert ist, können Sie Ihr Passwort nicht vom Mandanten-Manager ändern.

Verwandte Informationen

"StorageGRID verwalten"

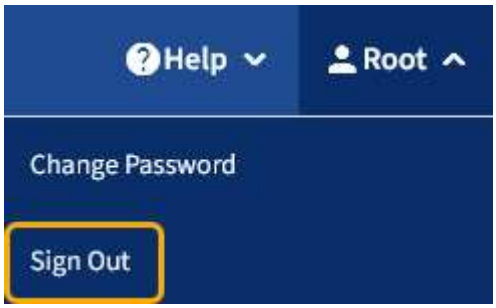
"Anforderungen an einen Webbrowser"

Sich vom Tenant Manager abmelden

Wenn Sie mit dem Mandanten-Manager arbeiten, müssen Sie sich anmelden, 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** aus.

Option	Beschreibung
SSO wird nicht verwendet	Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite für den Mandanten-Manager wird angezeigt. **Hinweis:** Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.

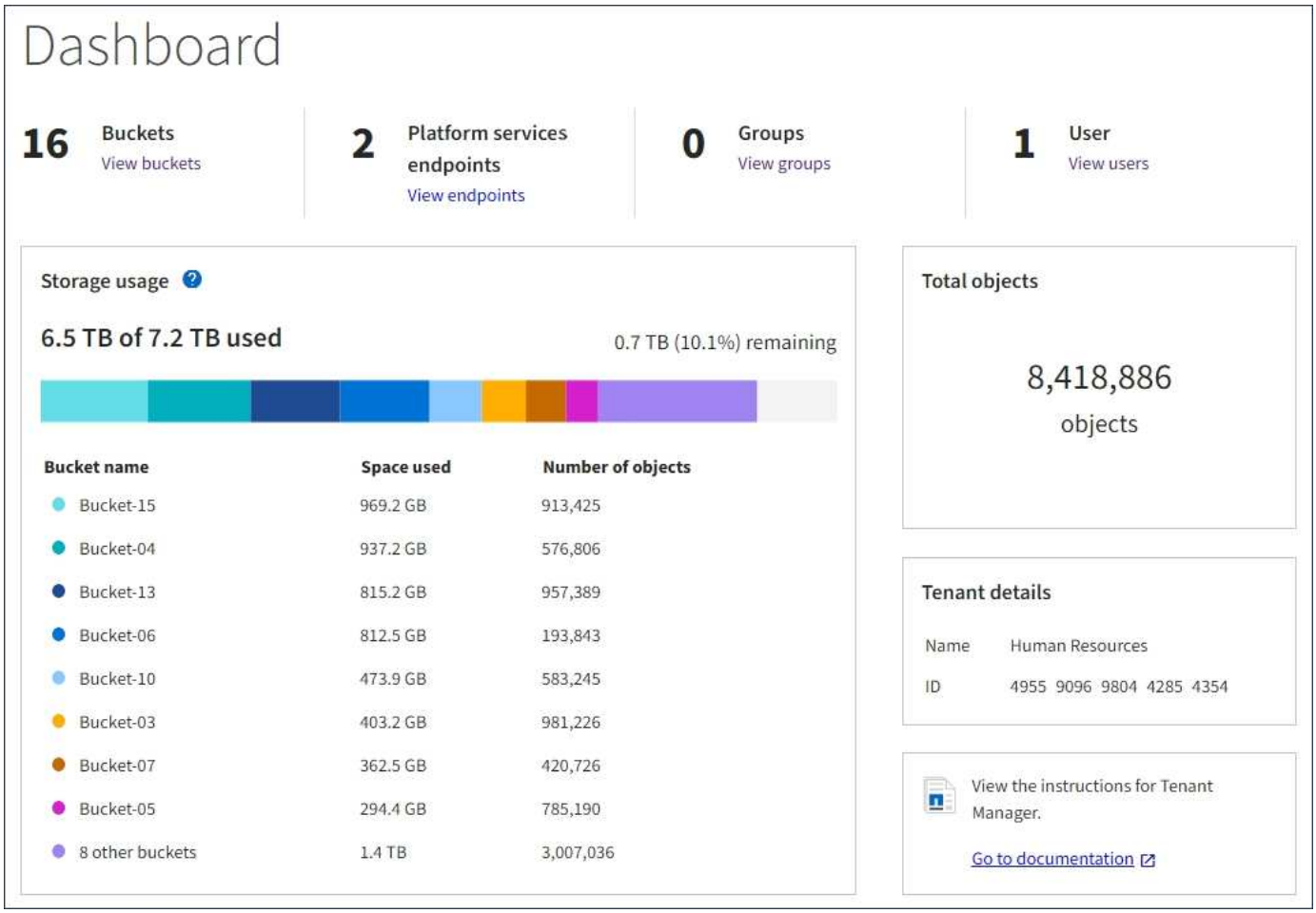
Option	Beschreibung
SSO aktiviert	Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. Der Name des Mietkontos, auf das Sie gerade zugegriffen haben, wird als Standard im Dropdown-Menü **Letzte Konten** angegeben, und die **Konto-ID** des Mieters wird angezeigt. **Hinweis:** Wenn SSO aktiviert ist und Sie auch beim Grid Manager angemeldet sind, müssen Sie sich auch vom Grid Manager abmelden, um SSO abzumelden.

Informationen zum Tenant Manager Dashboard

Das Mandanten-Manager-Dashboard bietet einen Überblick über die Konfiguration eines Mandanten-Accounts sowie den Speicherplatz, der von Objekten in Buckets (S3) oder Containern (Swift) verwendet wird. Wenn der Mandant ein Kontingent hat, zeigt das Dashboard an, wie viel des Kontingents verwendet wird und wie viel übrig ist. Wenn beim Mandantenkonto Fehler auftreten, werden die Fehler im 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:



Zusammenfassung des Mandantenkontos

Oben im Dashboard sind folgende 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 bei einem S3-Konto keine Objekte aufgenommen wurden und Sie über die Berechtigung Stammzugriff verfügen, werden Startrichtlinien anstelle der Gesamtzahl der Objekte angezeigt.

- Name und ID des Mandantenkontos
- Ein Link zur StorageGRID-Dokumentation.

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 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.

- 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.

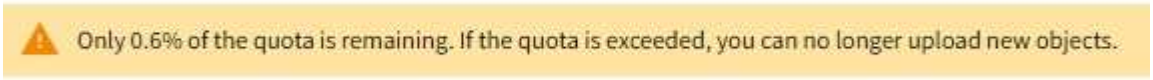
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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.

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. Weitere Informationen finden Sie unter Alerts Referenz in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

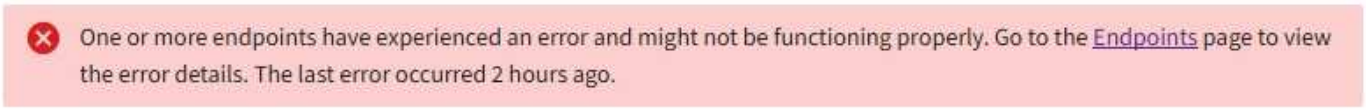


Wenn Sie Ihr Kontingent überschreiten, können Sie keine neuen Objekte hochladen.

Weitere Details sowie das Management von Regeln und Benachrichtigungen für Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

Endpunktfehler

Wenn Sie mithilfe des Grid Manager einen oder mehrere Endpunkte für die Verwendung mit Plattformdiensten konfiguriert haben, zeigt das Tenant Manager Dashboard eine Warnung an, wenn innerhalb der letzten sieben Tage Endpoint-Fehler aufgetreten sind.



Wenn Sie Details zu einem Endpunktfehler anzeigen möchten, wählen Sie Endpunkte aus, um die Seite Endpunkte anzuzeigen.

Verwandte Informationen

"Fehlerbehebung bei Endpoint-Fehlern bei Plattform-Services"

"Monitor Fehlerbehebung"

Das Mandantenmanagement-API von NetApp

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 Swagger Open Source API-Plattform. 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.

So greifen Sie auf die Swagger-Dokumentation für die Mandantenmanagement-API zu:

Schritte

1. Melden Sie sich beim Tenant Manager an.
2. Wählen Sie in der Kopfzeile des Mandanten-Managers die Option **Hilfe** > **API-Dokumentation** aus.

API-Betrieb

Die Mandantenmanagement-API organisiert die verfügbaren API-Vorgänge in die folgenden Abschnitte:

- **Account** — Betrieb auf dem aktuellen Mandantenkonto, einschließlich der Speicherung Informationen zur Nutzung.
- **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 „`Protecting Against Cross-Site Request Forgery`“.

  > Wenn Single Sign-On (SSO) für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Weitere Informationen finden Sie unter „`Authentifizierung bei Aktivierung der einmaligen Anmeldung bei der API`“ in den Anweisungen zum Verwalten von StorageGRID.

- **Config** — Operationen bezogen auf die Produktversion und Versionen der Mandantenmanagement-API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container** — Betrieb auf S3 Buckets oder Swift Containern, wie folgt:

Protokoll	Berechtigung erlaubt
S3	• Erstellen von konformen und nicht konformen Buckets • Ändern von Compliance-Einstellungen für ältere Versionen • Festlegen der Consistency Control für Vorgänge, die an Objekten ausgeführt werden • Erstellen, Aktualisieren und Löschen der CORS-Konfiguration eines Buckets • Aktivieren und Deaktivieren von Updates der letzten Zugriffszeit für Objekte • Verwalten der Konfigurationseinstellungen für Plattformservices, einschließlich CloudMirror-Replizierung, Benachrichtigungen und Suchintegration (Metadatenbenachrichtigung) • Leere Buckets werden gelöscht
Swift	Festlegen der für Container verwendeten Konsistenzstufe

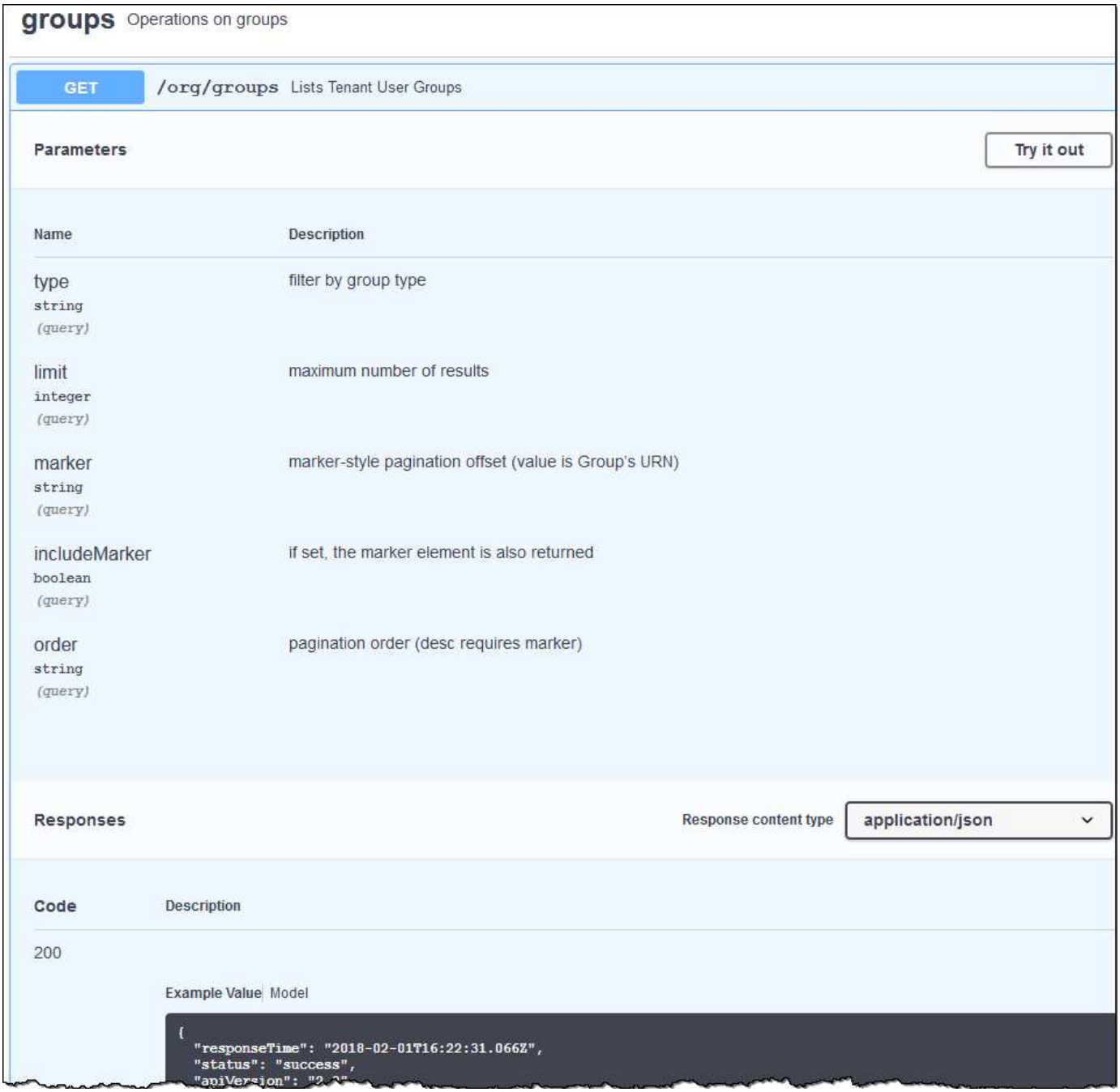
- **Deaktivierte Funktionen** — Funktionen zum Anzeigen von Funktionen, die möglicherweise deaktiviert

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.
- **Groups** — Operations zur Verwaltung lokaler Mandantengruppen und zum Abrufen von verbundenen Mandantengruppen aus einer externen Identitätsquelle.
- **Identity-Source** — Operationen, um eine externe Identitätsquelle zu konfigurieren und föderierte Gruppen- und Benutzerinformationen manuell zu synchronisieren.
- **Regionen** — Operationen zur Bestimmung, welche Regionen für das StorageGRID-System konfiguriert wurden.
- **s3** — Betrieb zum Managen von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-Object-Lock** — Operationen zur Bestimmung der globalen S3-Objektsperre (Compliance) für das StorageGRID-System.
- **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.



API-Anforderungen werden ausgegeben

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. Klicken Sie auf die HTTP-Aktion, 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 auf **Modell** klicken, um die Anforderungen für jedes Feld zu erfahren.

4. Klicken Sie auf **Probieren Sie es aus**.
5. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
6. Klicken Sie Auf **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Verwandte Informationen

"Schutz vor standortübergreifenden Anfrageschmieden (CSRF)"

"StorageGRID verwalten"

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

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

Wenn 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

Ermitteln, 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
  ]
}
```

Angeben einer API-Version für eine Anforderung

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

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

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

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

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

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

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

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

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

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

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

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

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

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

Managen des Systemzugriffs für Mandantenbenutzer

Sie gewähren Benutzern Zugriff auf ein Mandantenkonto, indem Sie Gruppen von einer föderierten Identitätsquelle importieren und Verwaltungsberechtigungen zuweisen. Außerdem können lokale Mandantengruppen und Benutzer erstellt werden, es sei denn, Single Sign On (SSO) gilt für das gesamte StorageGRID System.

- "Identitätsföderation verwenden"
- "Verwalten von Gruppen"
- "Verwalten von lokalen Benutzern"

Identitätsföderation verwenden

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 einer föderierten Identitätsquelle"
- "Synchronisierung mit der Identitätsquelle erzwingen"
- "Identitätsföderation deaktivieren"

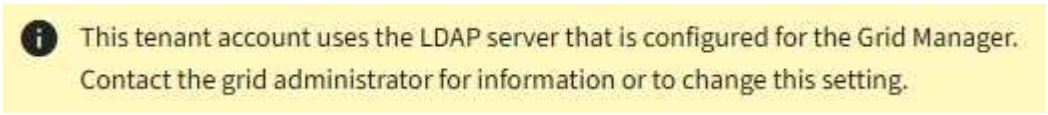
Sie können eine Identitätsföderation konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System wie Active Directory, OpenLDAP oder Oracle Directory Server verwaltet werden sollen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen Active Directory, OpenLDAP oder Oracle Directory Server als Identitäts-Provider verwenden. Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, müssen Sie sich an den technischen Support wenden.
- 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.

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 für diesen Mandanten keine separate föderierte Identitätsquelle konfigurieren.



Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Diensttyp **Active Directory**, **OpenLDAP** oder **Other** aus.

   Wenn Sie **OpenLDAP** wählen, konfigurieren Sie den OpenLDAP-Server. Weitere Informationen zur Konfiguration eines OpenLDAP-Servers finden Sie in den Richtlinien.

   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.
   - **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 im Abschnitt LDAP-Server konfigurieren die erforderlichen Informationen zum LDAP-Server und zur Netzwerkverbindung ein.
   - **Hostname**: Der Server-Hostname 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`
   - **Passwort**: Das mit dem Benutzernamen verknüpfte Passwort.
   - **Gruppenbasis 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 der **Group-Basis-DN**, zu der 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 **User Unique Name**-Werte müssen innerhalb der **User Base DN**, zu der sie gehören, eindeutig sein.

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

     Diese Option 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-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.
8. Wählen Sie **Verbindung testen**, um die Verbindungseinstellungen für den LDAP-Server zu validieren.

   Wenn die Verbindung gültig ist, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.
9. Wenn die Verbindung gültig ist, wählen Sie **Speichern**.

   Der folgende Screenshot zeigt Beispielkonfigurationswerte für einen LDAP-Server, der Active Directory verwendet.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

"Richtlinien für die Konfiguration eines OpenLDAP-Servers"

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.

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie im Administratorhandbuch für OpenLDAP in den Anweisungen zur Wartung der Reverse-Group-Mitgliedschaft.

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 der Umkehrgruppenmitgliedschaft finden Sie im Administratorhandbuch für OpenLDAP.

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die gespeicherte Identitätsquelle muss aktiviert sein.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.

   Die Seite Identitätsföderation wird angezeigt. Die Schaltfläche **Sync Server** befindet sich oben rechts auf der Seite.

   > Wenn die gespeicherte Identitätsquelle nicht aktiviert ist, ist die Schaltfläche **Sync Server** nicht aktiv.

2. Wählen Sie **Sync Server**.

   Eine Bestätigungsmeldung zeigt an, dass die Synchronisierung erfolgreich gestartet wurde.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Identitätsföderation deaktivieren

Wenn Sie einen Identitätsföderationsdienst für diesen Mandanten konfiguriert haben, können Sie die Identitätsföderation für Mandanten und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen dem StorageGRID-System und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die derzeit angemeldet sind, erhalten bis zum Ablauf ihrer Sitzung Zugriff auf das Mandantenkonto, können sich jedoch nach Ablauf ihrer Sitzung nicht anmelden.
- Es erfolgt keine Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
2. Deaktivieren Sie das Kontrollkästchen * Identitätsföderation aktivieren*.
3. Wählen Sie **Speichern**.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Verwalten von Gruppen

Sie weisen Benutzergruppen Berechtigungen zu, um zu steuern, welche Aufgaben Mandantenbenutzer durchführen können. Sie können föderierte Gruppen aus einer Identitätsquelle importieren, z. B. Active Directory oder OpenLDAP, oder Sie können lokale Gruppen erstellen.

> Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager anmelden, obwohl sie auf Basis der Gruppenberechtigungen auf S3- und Swift-Ressourcen zugreifen können.

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. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Berechtigung	Beschreibung
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API. **Hinweis:** Swift-Benutzer müssen Root Access-Berechtigung haben, 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 Credentials	Nur S3-Mandanten. Benutzer können ihre eigenen S3-Zugriffsschlüssel erstellen und entfernen. Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption **STORAGE (S3)** > **Meine S3-Zugriffstasten**.
Alle Buckets Verwalten	• 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. Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption **Buckets** nicht. • Swift Mandanten: Ermöglicht Swift Benutzern die Kontrolle der Konsistenzstufe für Swift Container mithilfe der Mandanten-Management-API. **Hinweis:** Sie können Swift-Gruppen nur die Berechtigung Alle Buckets verwalten aus der Mandantenmanagement-API zuweisen. Sie können diese Berechtigung nicht Swift-Gruppen mit dem Tenant Manager zuweisen.
Endpunkte Managen	Nur S3-Mandanten. Ermöglicht Benutzern, Endpunkte mithilfe des Mandanten-Managers oder der Mandanten-Management-API zu erstellen oder zu bearbeiten, die als Ziel für StorageGRID-Plattformservices verwendet werden. Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption **Platform Services Endpunkte**.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie Swift"

Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen managen, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.

2. Wählen Sie **Gruppe erstellen**.
3. 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.

4. 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.
5. Wählen Sie **Weiter**.
6. Wählen Sie einen Zugriffsmodus aus. 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.
   - **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.

- **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

7. Wählen Sie die Gruppenberechtigungen für diese Gruppe aus.

   Weitere Informationen zu Berechtigungen für die Mandantenverwaltung finden Sie unter.

8. Wählen Sie **Weiter**.
9. Wählen Sie eine Gruppenrichtlinie aus, um zu bestimmen, über welche S3-Zugriffsrechte die Mitglieder dieser Gruppe verfügen.
   - **Kein S3-Zugriff**: Standard. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat 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. Sie können diesen String nicht bearbeiten.
   - **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. Sie können diesen String nicht bearbeiten.
   - **Benutzerdefiniert**: Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben. Anweisungen zur Implementierung einer S3-Client-Applikation finden Sie in den detaillierten Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispielen.
10. 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.

    In diesem Beispiel dürfen Mitglieder der Gruppe nur einen Ordner auflisten und darauf zugreifen, der ihrem Benutzernamen (Schlüsselpräfix) im angegebenen Bucket entspricht. Beachten Sie, dass bei der Festlegung der Privatsphäre dieser Ordner Zugriffsberechtigungen aus anderen Gruppenrichtlinien und der Bucket-Richtlinie berücksichtigt werden sollten.

11. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:

    - Verbundgruppe: **Gruppe erstellen**
    - Lokale Gruppe: **Weiter**

    Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

12. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

    Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können der Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer hinzufügen.

13. Wählen Sie **Fertig**.

    Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

"S3 verwenden"

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.

2. Wählen Sie **Gruppe erstellen**.
3. 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.

4. 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.
5. Wählen Sie **Weiter**.

6. Wählen Sie einen Zugriffsmodus aus. 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.
   - **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.
   - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.
7. Legen Sie die Gruppenberechtigung fest.
   - Aktivieren Sie das Kontrollkästchen **Root Access**, wenn sich Benutzer bei der Tenant Manager- oder Mandantenmanagement-API anmelden müssen. (Standard)
   - Deaktivieren Sie das Kontrollkästchen **Root Access**, wenn Benutzer keinen Zugriff auf die Tenant Manager- oder Mandantenmanagement-API benötigen. Deaktivieren Sie beispielsweise das Kontrollkästchen für Anwendungen, die nicht auf den Mandanten zugreifen müssen. Weisen Sie dann die **Swift Administrator**-Berechtigung zu, damit diese Benutzer Container und Objekte verwalten können.
8. Wählen Sie **Weiter**.
9. Aktivieren Sie das Kontrollkästchen **Swift Administrator**, wenn der Benutzer die Swift REST API verwenden muss.

   Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht 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.

10. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:
    - Verbundgruppe: **Gruppe erstellen**
    - Lokale Gruppe: **Weiter**

      Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

11. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

    Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können die Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer erstellen.

12. Wählen Sie **Fertig**.

    Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

"Verwenden Sie Swift"

Anzeigen und Bearbeiten von Gruppendetails

Wenn Sie die Details für eine Gruppe anzeigen, können Sie den Anzeigenamen, Berechtigungen, Richtlinien und die Benutzer, die zu der Gruppe gehören, ändern.

Was Sie benötigen

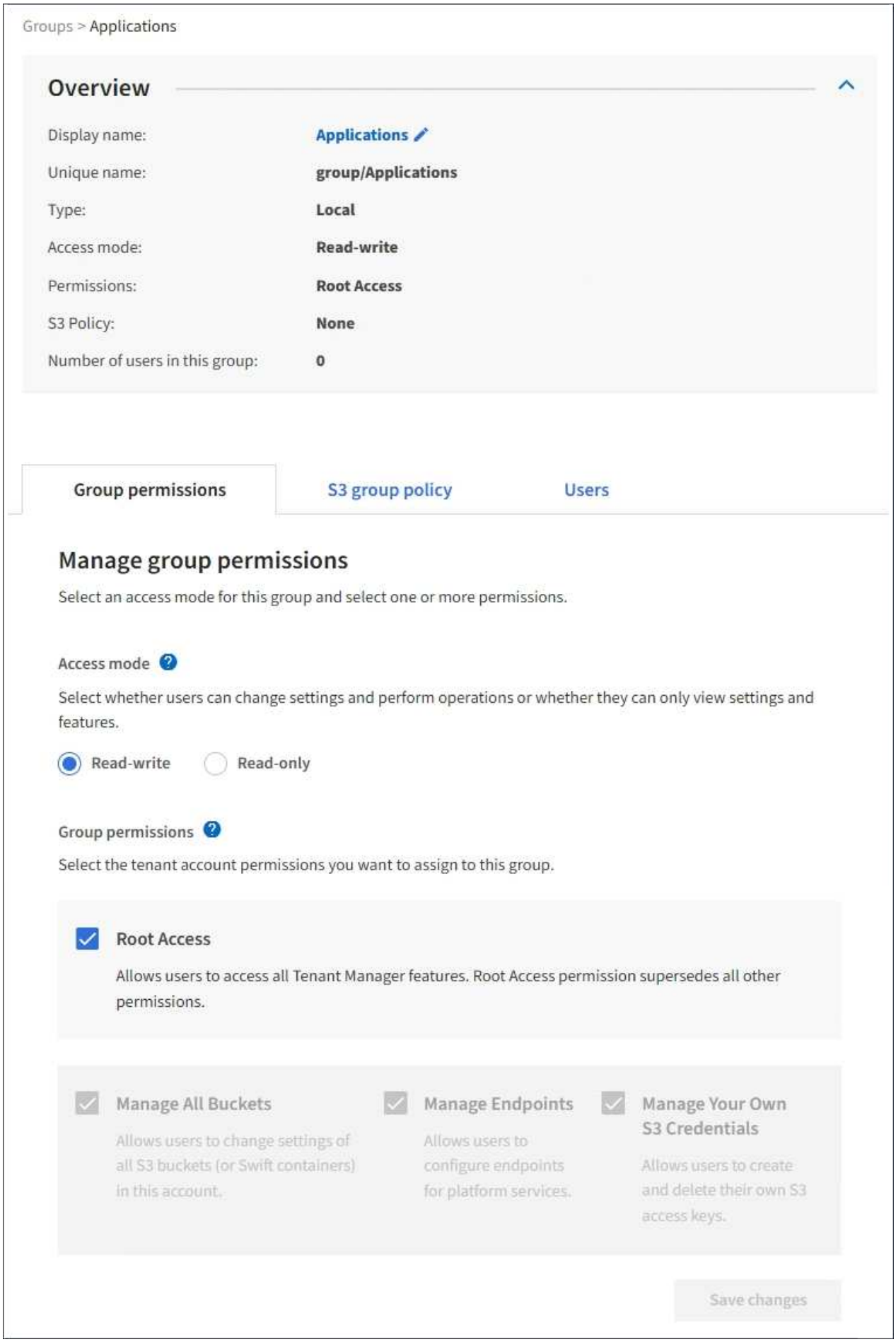
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wählen Sie den Namen der Gruppe aus, deren Details Sie anzeigen oder bearbeiten möchten.

   Alternativ können Sie **Aktionen** > **Gruppendetails anzeigen** wählen.

   Die Seite Gruppendetails wird angezeigt. Im folgenden Beispiel wird die Seite mit den S3-Gruppendetails angezeigt.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Nehmen Sie bei Bedarf Änderungen an den Gruppeneinstellungen vor.

> Um sicherzustellen, dass Ihre Änderungen gespeichert werden, wählen Sie **Änderungen speichern** aus, nachdem Sie Änderungen in jedem Abschnitt vorgenommen haben. Wenn Ihre Änderungen gespeichert sind, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.

   a. Wählen Sie optional den Anzeigenamen oder das Bearbeitungssymbol aus Um den Anzeigenamen zu aktualisieren.

      Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

   b. Optional können Sie die Berechtigungen aktualisieren.

   c. Nehmen Sie für die Gruppenrichtlinie die entsprechenden Änderungen für Ihren S3- oder Swift-Mandanten vor.

      - Wenn Sie eine Gruppe für einen S3-Mandanten bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus. Wenn Sie eine benutzerdefinierte S3-Richtlinie auswählen, aktualisieren Sie den JSON-String wie erforderlich.
      - Wenn Sie eine Gruppe für einen Swift-Mandanten bearbeiten, aktivieren oder deaktivieren Sie das Kontrollkästchen **Swift Administrator**.

        Weitere Informationen zum Swift Administrator erhalten Sie in den Anweisungen zum Erstellen von Gruppen für einen Swift-Mandanten.

   d. Optional können Benutzer hinzugefügt oder entfernt werden.

4. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

   Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Erstellen von Gruppen für einen S3-Mandanten"

"Erstellen von Gruppen für einen Swift Mandanten"

Hinzufügen von Benutzern zu einer lokalen Gruppe

Sie können bei Bedarf Benutzer zu einer lokalen Gruppe hinzufügen.

Was Sie benötigen

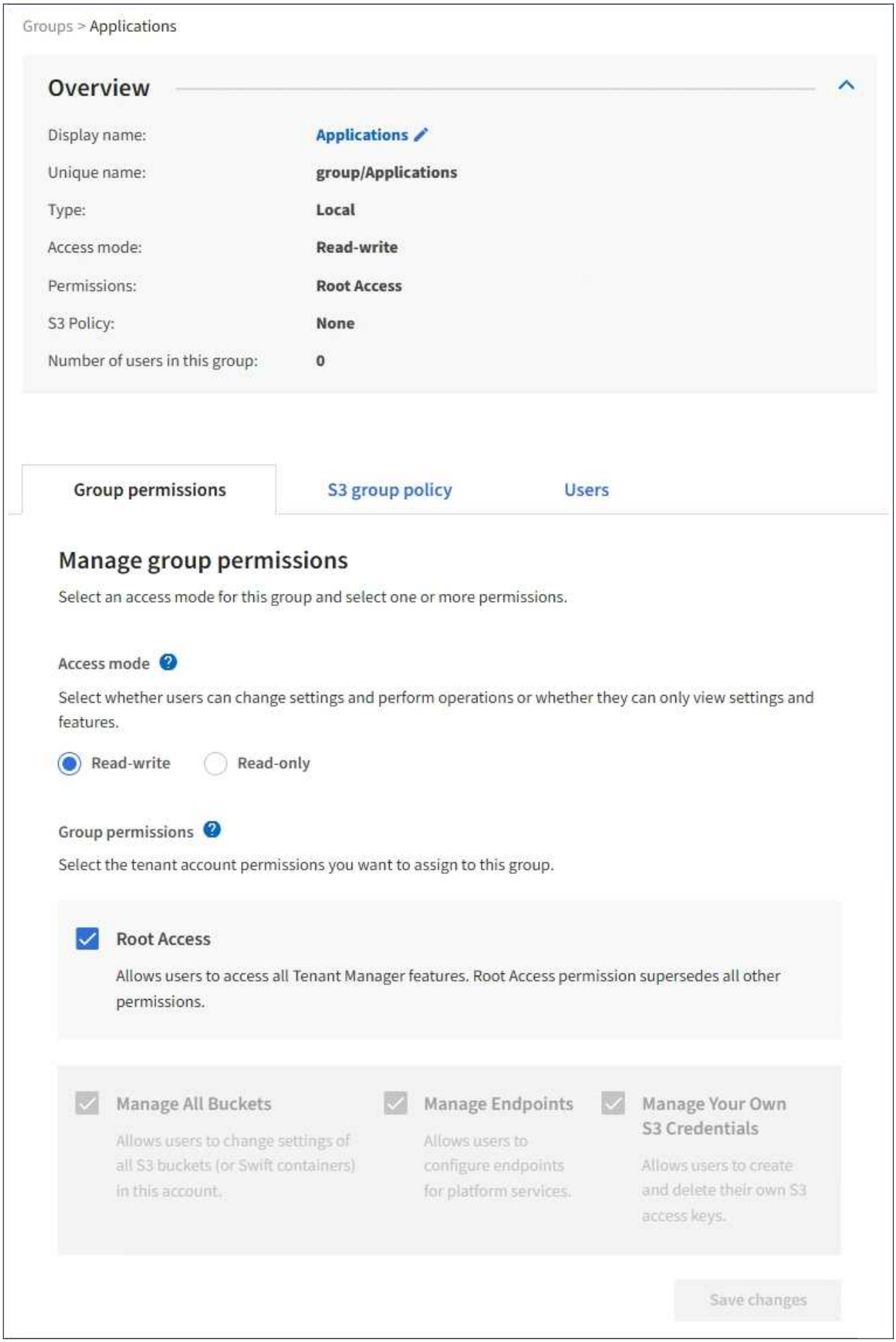
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

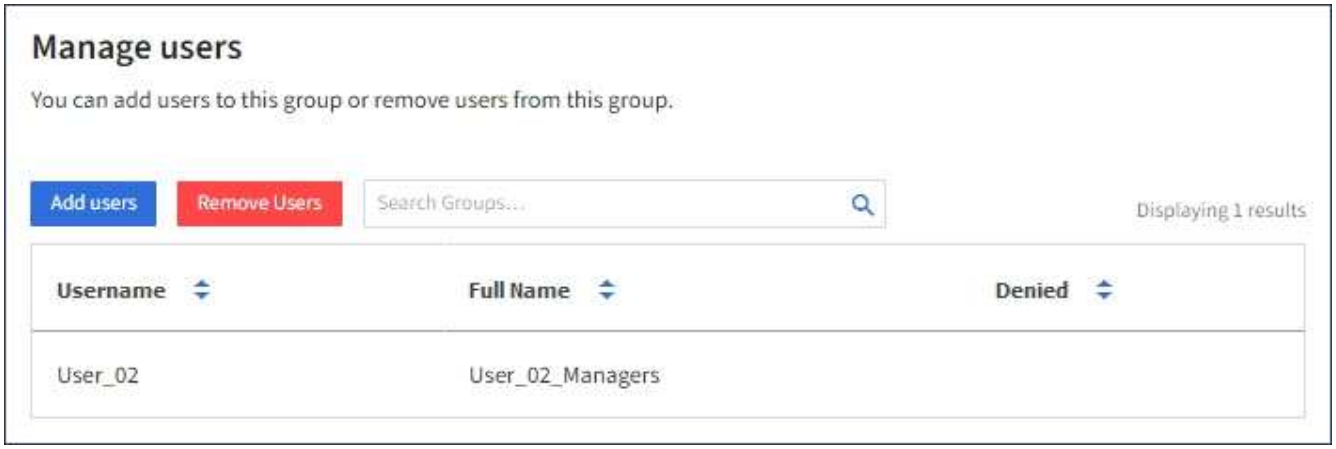
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wählen Sie den Namen der lokalen Gruppe aus, der Sie Benutzer hinzufügen möchten.

   Alternativ können Sie **Aktionen** > **Gruppendetails anzeigen** wählen.

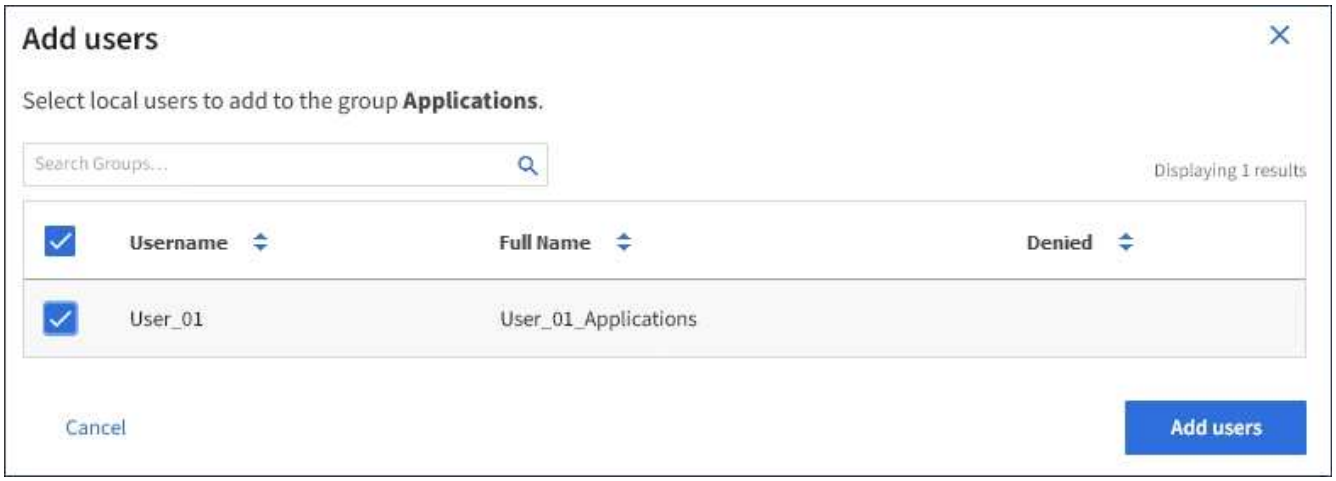
   Die Seite Gruppendetails wird angezeigt.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Wählen Sie **Benutzer verwalten** und dann **Benutzer hinzufügen**.



4. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Benutzer hinzufügen**.



In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Gruppennamen bearbeiten

Sie können den Anzeigenamen für eine Gruppe bearbeiten. Sie können den eindeutigen Namen für eine Gruppe nicht bearbeiten.

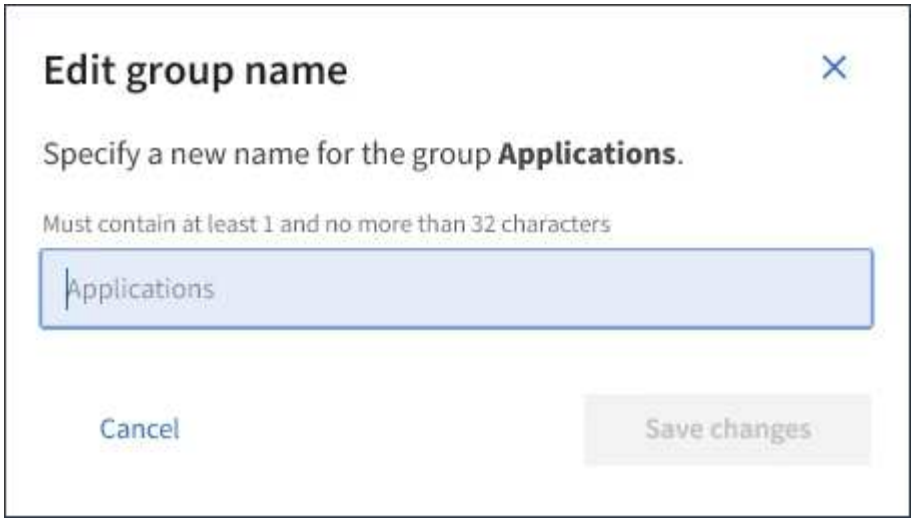
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, deren Anzeigename Sie bearbeiten möchten.
3. Wählen Sie **Aktionen** > **Gruppenname bearbeiten**.

   Das Dialogfeld Gruppenname bearbeiten wird angezeigt.



4. Wenn Sie eine lokale Gruppe bearbeiten, aktualisieren Sie den Anzeigenamen nach Bedarf.

   Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

5. Wählen Sie **Änderungen speichern**.

   In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Duplizieren einer Gruppe

Sie können neue Gruppen schneller erstellen, indem Sie eine vorhandene Gruppe duplizieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Gruppe duplizieren**. Weitere Details zum Erstellen einer Gruppe finden Sie in den Anweisungen zum Erstellen von Gruppen für einen S3-Mandanten oder für einen Swift-Mandanten.
4. 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.

5. 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.
6. Wählen Sie **Weiter**.
7. Ändern Sie bei Bedarf die Berechtigungen für diese Gruppe.
8. Wählen Sie **Weiter**.
9. Wenn Sie eine Gruppe für einen S3-Mandanten duplizieren, wählen Sie bei Bedarf aus den Optionsfeldern **S3-Richtlinie hinzufügen** eine andere Richtlinie aus. Wenn Sie eine benutzerdefinierte Richtlinie ausgewählt haben, aktualisieren Sie den JSON-String wie erforderlich.
10. Wählen Sie **Gruppe erstellen**.

Verwandte Informationen

"Erstellen von Gruppen für einen S3-Mandanten"

"Erstellen von Gruppen für einen Swift Mandanten"

"Mandantenmanagement-Berechtigungen"

Löschen einer Gruppe

Sie können eine Gruppe aus dem System löschen. Benutzer, die nur zu dieser Gruppe gehören, können sich nicht mehr beim Mandantenmanager anmelden oder das Mandantenkonto verwenden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.

2. Aktivieren Sie die Kontrollkästchen für die Gruppen, die Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Gruppe löschen**.

   Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie **Gruppe löschen**, um zu bestätigen, dass Sie die in der Bestätigungsmeldung angegebenen Gruppen löschen möchten.

   In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Verwalten von lokalen Benutzern

Sie können lokale Benutzer erstellen und lokalen Gruppen zuweisen, um zu bestimmen, auf welche Funktionen diese Benutzer zugreifen können. Der Mandantenmanager enthält einen vordefinierten lokalen Benutzer mit dem Namen „`root`“. Obwohl Sie lokale Benutzer hinzufügen und entfernen können, können Sie den Root-Benutzer nicht entfernen.

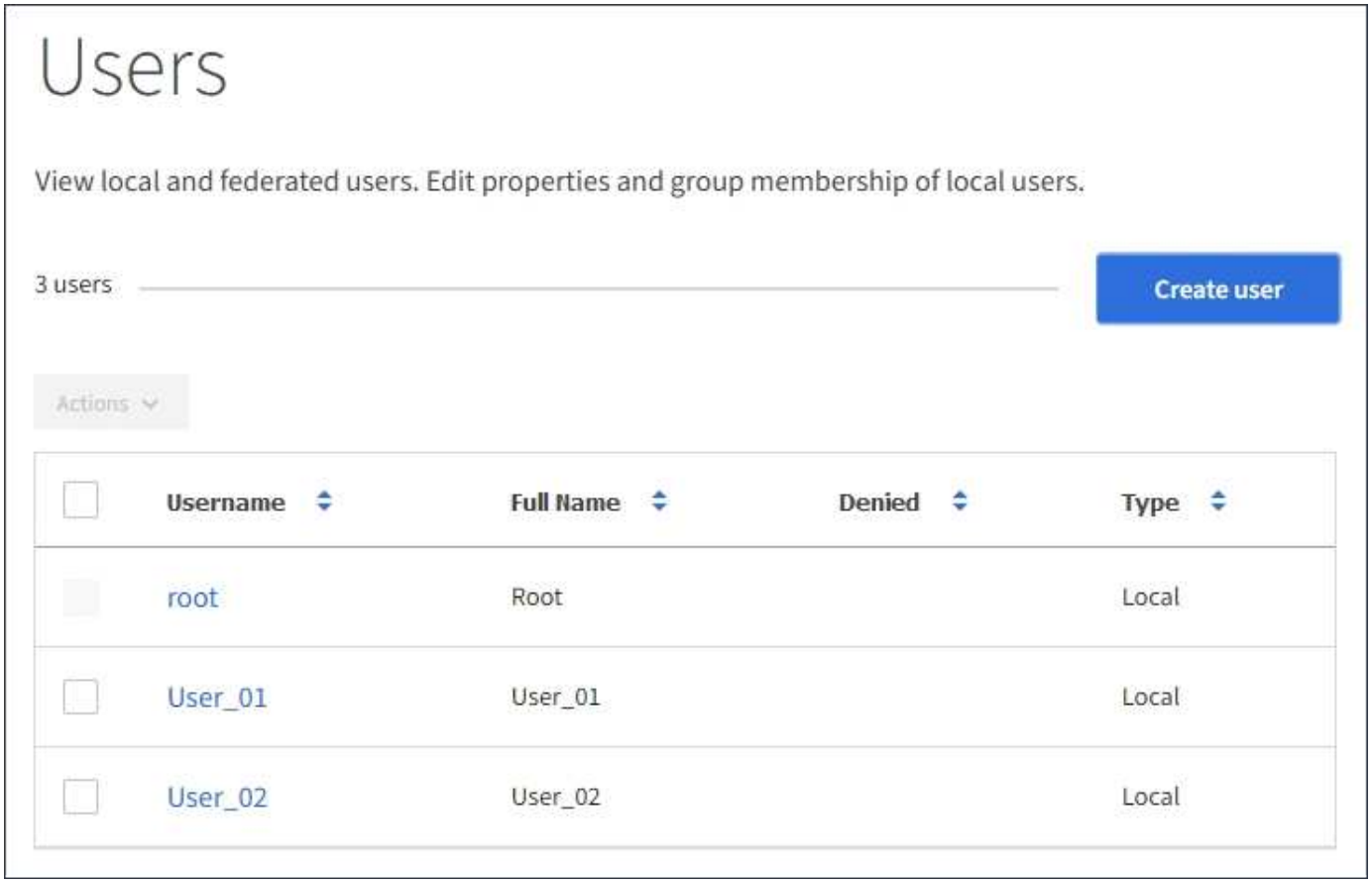
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen zu einer Lese-/Schreib-Benutzergruppe mit Root Access-Berechtigung gehören.

> Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager oder bei der Mandantenmanagement-API anmelden, auch wenn sie mithilfe von S3- oder Swift-Client-Applikationen auf die Ressourcen des Mandanten zugreifen können, basierend auf Gruppenberechtigungen.

Zugriff auf die Seite Benutzer

Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.



Erstellen lokaler Benutzer

Sie können lokale Benutzer erstellen und sie einer oder mehreren lokalen Gruppen zuweisen, um ihre Zugriffsberechtigungen zu steuern.

S3-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder S3-Gruppenrichtlinien auf sie angewendet. Diese Benutzer haben möglicherweise S3-Bucket-Zugriff, der über eine Bucket-Richtlinie gewährt wird.

Swift-Benutzer, die keiner Gruppe angehören, haben weder Managementberechtigungen noch Swift-Container-Zugriff.

Schritte

1. Wählen Sie **Benutzer erstellen**.
2. Füllen Sie die folgenden Felder aus.
   - **Vollständiger Name**: Der vollständige Name für diesen Benutzer, zum Beispiel 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.
   - **Passwort**: Ein Passwort, das bei der Anmeldung des Benutzers verwendet wird.
   - **Passwort bestätigen**: Geben Sie dasselbe Passwort ein, das Sie im Feld Passwort eingegeben haben.

- **Zugriff verweigern**: Wenn Sie **Ja** wählen, kann sich dieser Benutzer nicht beim Mandantenkonto anmelden, obwohl der Benutzer noch zu einer oder mehreren Gruppen gehört.

  Als Beispiel können Sie diese Funktion verwenden, um die Fähigkeit eines Benutzers, sich anzumelden, vorübergehend auszusetzen.

3. Wählen Sie **Weiter**.
4. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu.

   Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören.

5. Wählen Sie **Benutzer erstellen**.

   Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Benutzerdetails werden bearbeitet

Wenn Sie die Details für einen Benutzer bearbeiten, können Sie den vollständigen Namen und das Kennwort des Benutzers ändern, den Benutzer zu verschiedenen Gruppen hinzufügen und verhindern, dass der Benutzer auf den Mandanten zugreift.

Schritte

1. Wählen Sie in der Liste Benutzer den Namen des Benutzers aus, dessen Details Sie anzeigen oder bearbeiten möchten.

   Alternativ können Sie das Kontrollkästchen für den Benutzer aktivieren und dann **Aktionen** > **Benutzerdetails anzeigen** wählen.

2. Nehmen Sie bei Bedarf Änderungen an den Benutzereinstellungen vor.
   a. Ändern Sie den vollständigen Namen des Benutzers nach Bedarf, indem Sie den vollständigen Namen oder das Bearbeiten-Symbol auswählen Im Abschnitt Übersicht.

      Sie können den Benutzernamen nicht ändern.

   b. Ändern Sie auf der Registerkarte **Passwort** das Kennwort des Benutzers nach Bedarf.
   c. Auf der Registerkarte **Zugriff** können Sie sich anmelden (wählen Sie **Nein**) oder verhindern, dass sich der Benutzer bei Bedarf anmelden kann (wählen Sie **Ja**).
   d. Fügen Sie auf der Registerkarte **Groups** den Benutzer zu Gruppen hinzu, oder entfernen Sie den Benutzer aus Gruppen nach Bedarf.
   e. Wählen Sie nach Bedarf für jeden Abschnitt **Änderungen speichern**.

      Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Lokale Benutzer werden dupliziert

Sie können einen lokalen Benutzer duplizieren, um einen neuen Benutzer schneller zu erstellen.

Schritte

1. Wählen Sie in der Liste Benutzer den Benutzer aus, den Sie duplizieren möchten.
2. Wählen Sie **Benutzer duplizieren**.

3. Ändern Sie die folgenden Felder für den neuen Benutzer.
   - **Vollständiger Name**: Der vollständige Name für diesen Benutzer, zum Beispiel 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.
   - **Passwort**: Ein Passwort, das bei der Anmeldung des Benutzers verwendet wird.
   - **Passwort bestätigen**: Geben Sie dasselbe Passwort ein, das Sie im Feld Passwort eingegeben haben.
   - **Zugriff verweigern**: Wenn Sie **Ja** wählen, kann sich dieser Benutzer nicht beim Mandantenkonto anmelden, obwohl der Benutzer noch zu einer oder mehreren Gruppen gehört.

     Als Beispiel können Sie diese Funktion verwenden, um die Fähigkeit eines Benutzers, sich anzumelden, vorübergehend auszusetzen.
4. Wählen Sie **Weiter**.
5. Wählen Sie eine oder mehrere lokale Gruppen aus.

   Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören.
6. Wählen Sie **Benutzer erstellen**.

   Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Lokale Benutzer werden gelöscht

Sie können lokale Benutzer dauerhaft löschen, die nicht mehr auf das StorageGRID-Mandantenkonto zugreifen müssen.

Mit dem Tenant Manager können Sie lokale Benutzer löschen, aber keine föderierten Benutzer. Sie müssen die föderierte Identitätsquelle verwenden, um verbundene Benutzer zu löschen.

Schritte

1. Aktivieren Sie in der Liste Benutzer das Kontrollkästchen für den lokalen Benutzer, den Sie löschen möchten.
2. Wählen Sie **Aktionen** > **Benutzer löschen**.
3. Wählen Sie im Bestätigungsdialogfeld **Benutzer löschen** aus, um zu bestätigen, dass Sie den Benutzer aus dem System löschen möchten.

   Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Verwalten von S3-Mandantenkonten

Mandanten-Manager können S3-Zugriffsschlüssel managen und S3-Buckets erstellen und managen.

- "Verwalten von S3-Zugriffsschlüsseln"
- "Management von S3-Buckets"

Verwalten von S3-Zugriffsschlüsseln

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.

Über diese Aufgabe

S3-Zugriffsschlüssel können wie folgt gemanagt werden:

- Benutzer, die über die **Verwalten Ihrer eigenen S3-Anmeldeinformationen**-Berechtigung verfügen, können eigene S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung * Root Access* können die Zugriffsschlüssel für das S3-Stammkonto 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. Für den Zugriff auf Buckets und Objekte im S3-Mandantenkonto ist ein Zugriffsschlüssel erforderlich.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.

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. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel, als Sie benötigen, und löschen Sie die nicht verwendeten Schlüssel. 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 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 keine regelmäßigen neuen 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.

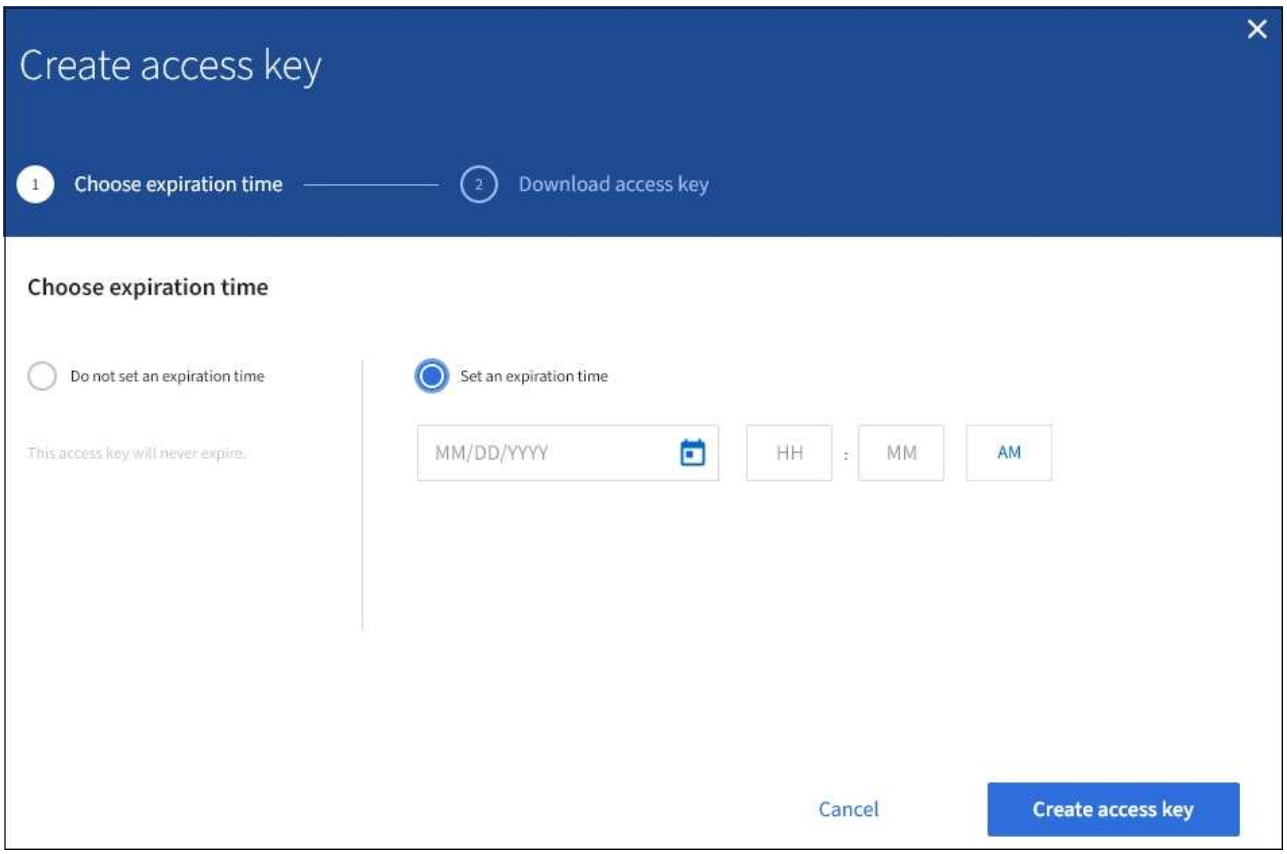
Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, 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.

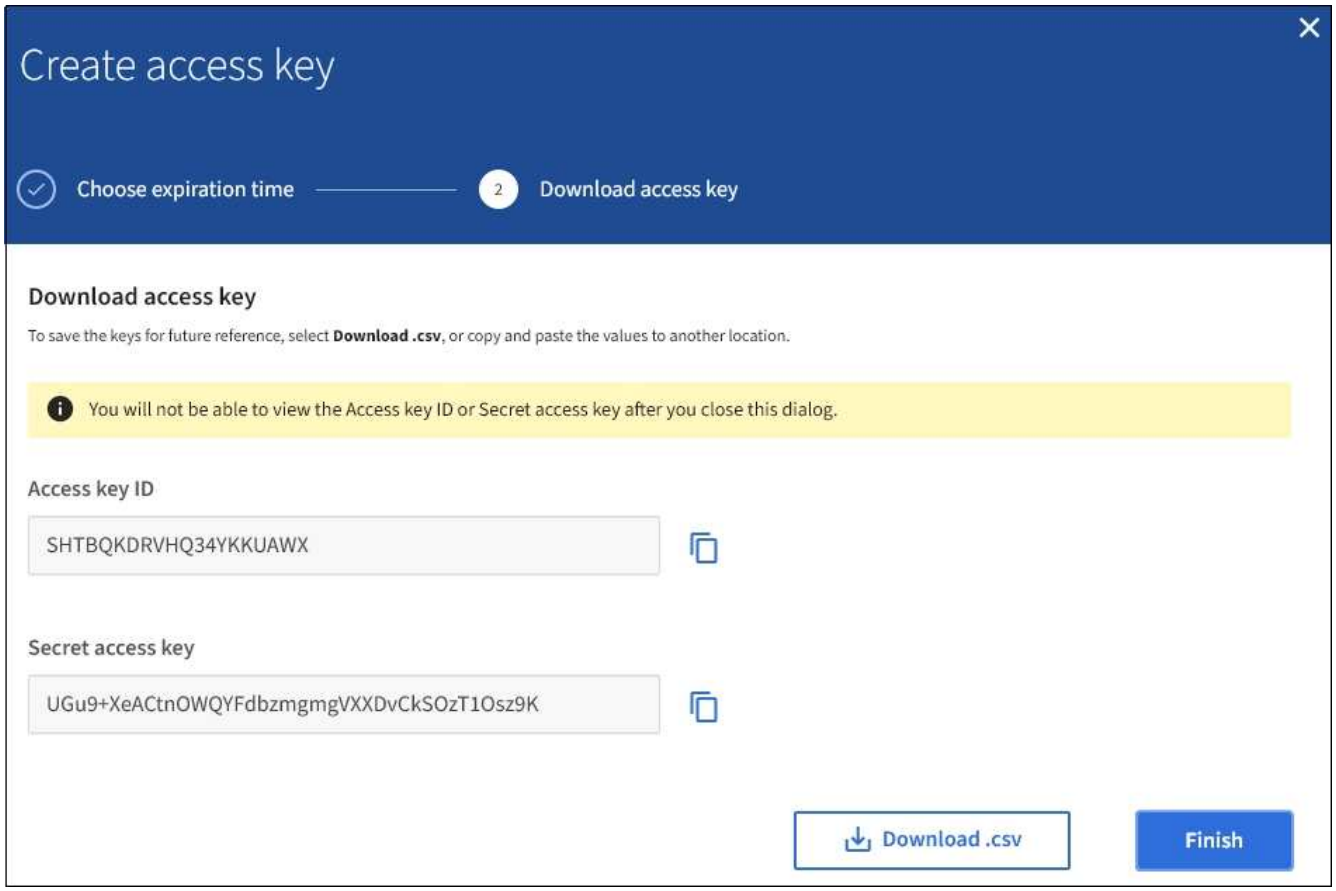


4. Wählen Sie **Zugriffsschlüssel erstellen**.

   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.



6. Wählen Sie **Fertig**.

   Die neue Taste wird auf der Seite eigene Zugriffsschlüssel angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Anzeigen der S3-Zugriffsschlüssel

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 neue Schlüssel erstellen oder Schlüssel löschen, die Sie nicht mehr verwenden.

Was Sie benötigen

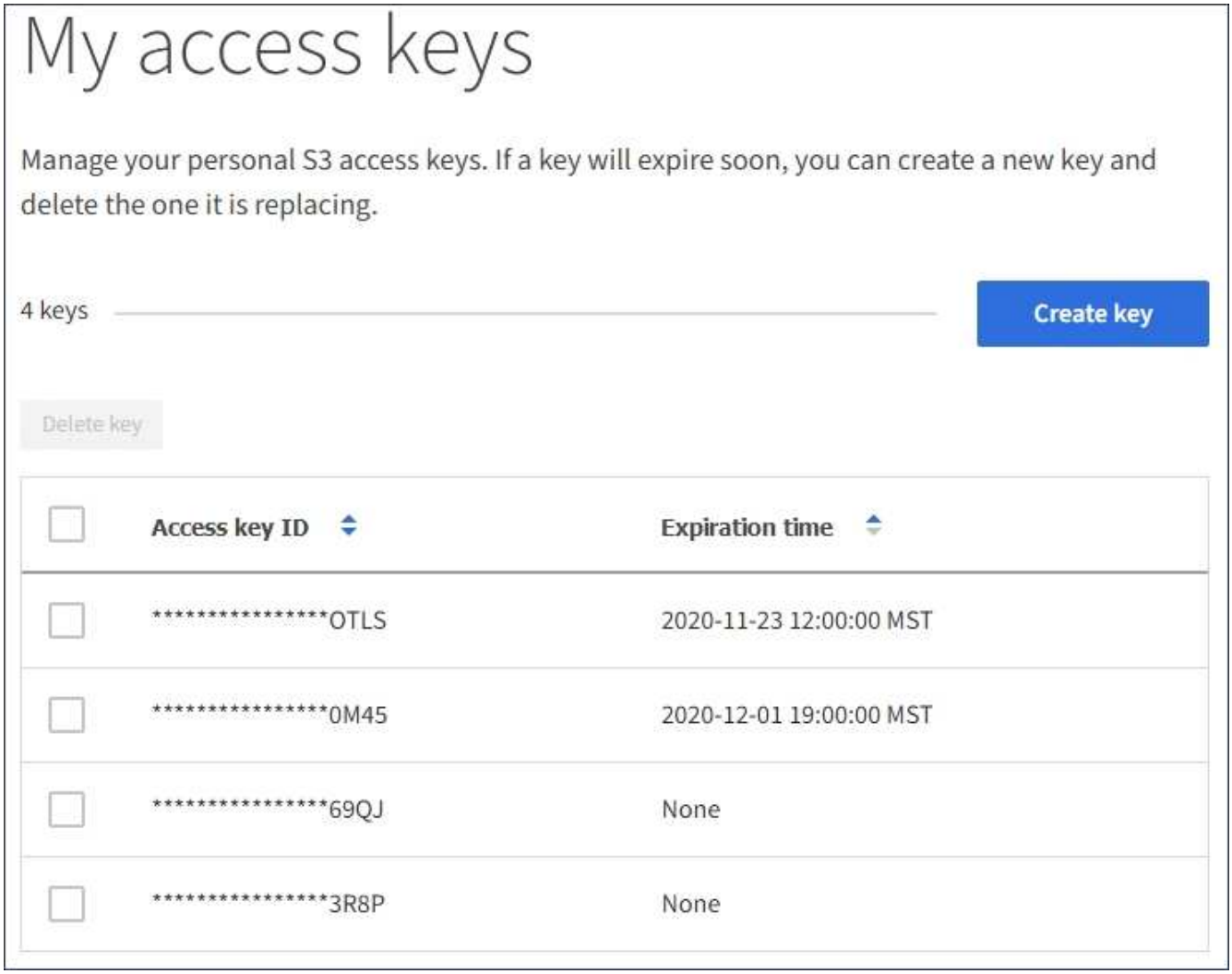
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.

> 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. Sortieren Sie die Tasten nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie nach Bedarf neue Schlüssel und löschen Sie manuell nicht mehr verwendete Schlüssel.

   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.

Verwandte Informationen

"Erstellen Ihrer eigenen S3-Zugriffsschlüssel"

"Löschen Ihrer eigenen S3-Zugriffsschlüssel"

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.

> 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.

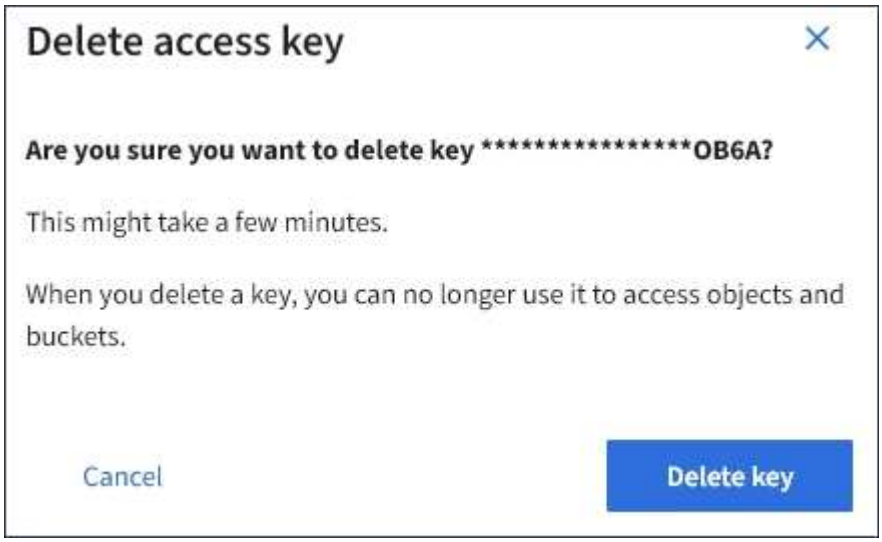
Schritte

1. Wählen Sie **STORAGE (S3)** > **Meine Zugriffsschlüssel** aus.

   Die Seite Meine Zugriffsschlüssel wird angezeigt und enthält alle vorhandenen Zugriffsschlüssel.

2. Aktivieren Sie das Kontrollkästchen für jeden Zugriffschlüssel, den Sie entfernen möchten.
3. Wählen Sie * Taste löschen*.

   Ein Bestätigungsdialogfeld wird angezeigt.



4. Wählen Sie * Taste löschen*.

   In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Erstellen von S3-Zugriffsschlüsseln 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

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 nicht verwendeten Schlüssel. 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 regelmäßigen 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.

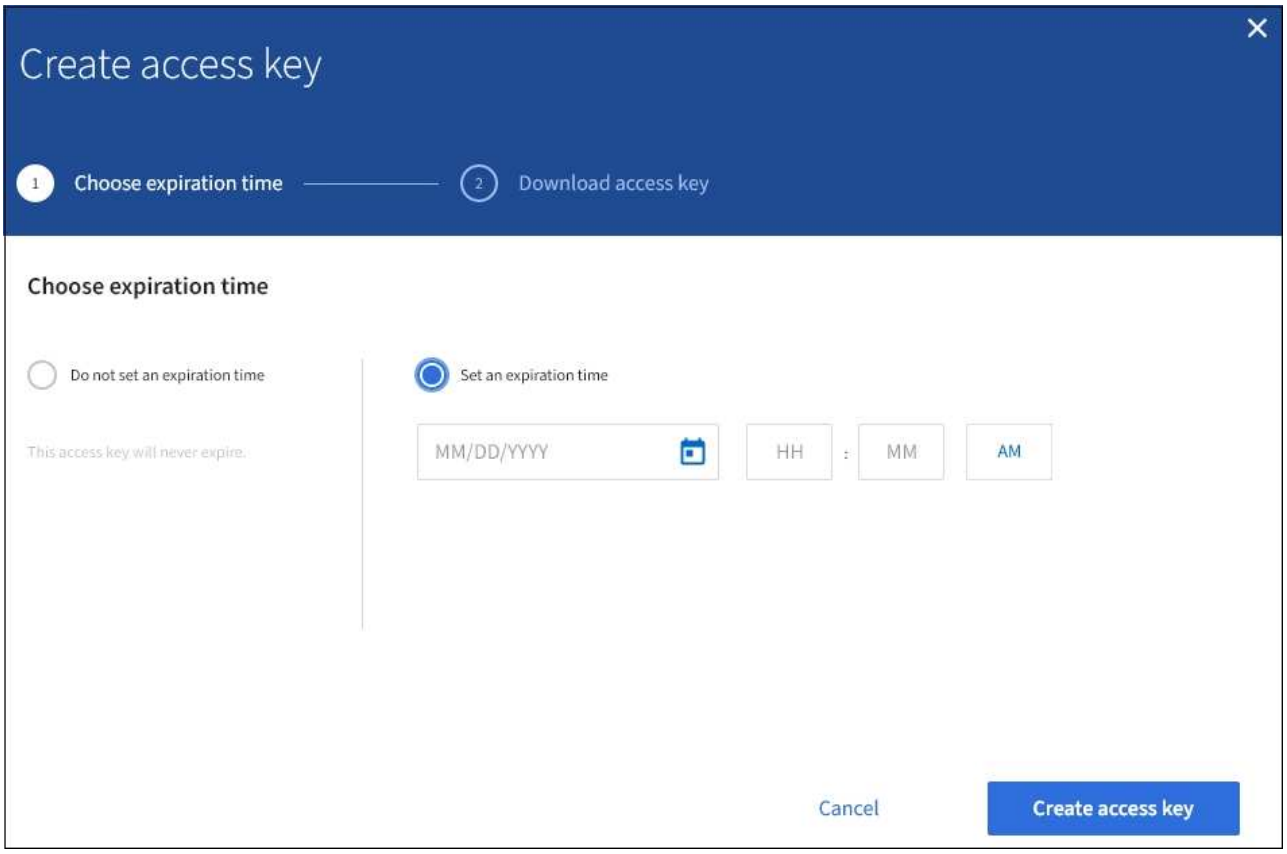
> Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten 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 **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.

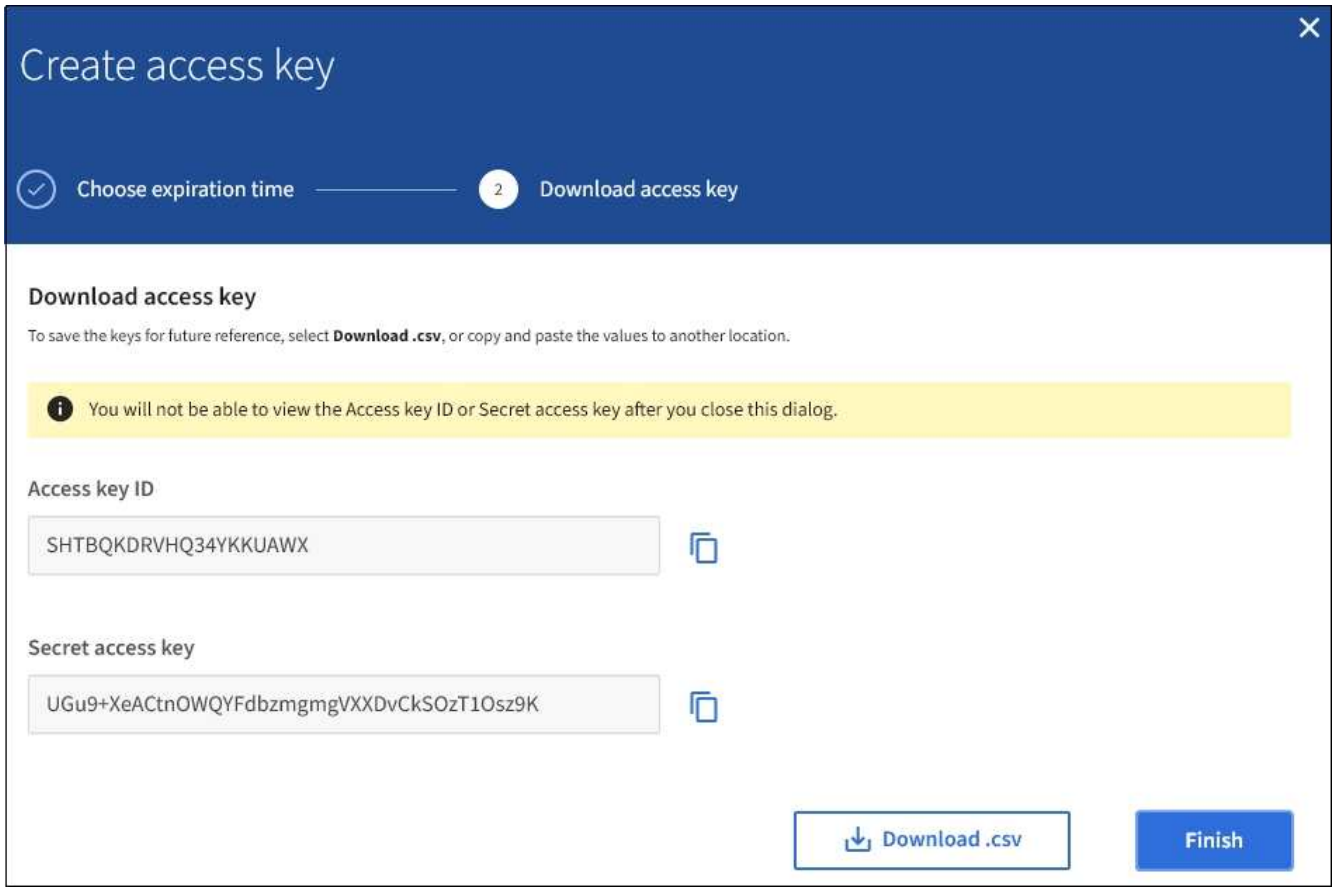


5. Wählen Sie **Zugriffsschlüssel erstellen**.

   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.



7. Wählen Sie **Fertig**.

   Der neue Schlüssel wird auf der Registerkarte Zugriffsschlüssel der Seite mit den Benutzerdetails angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Anzeigen der 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 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

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

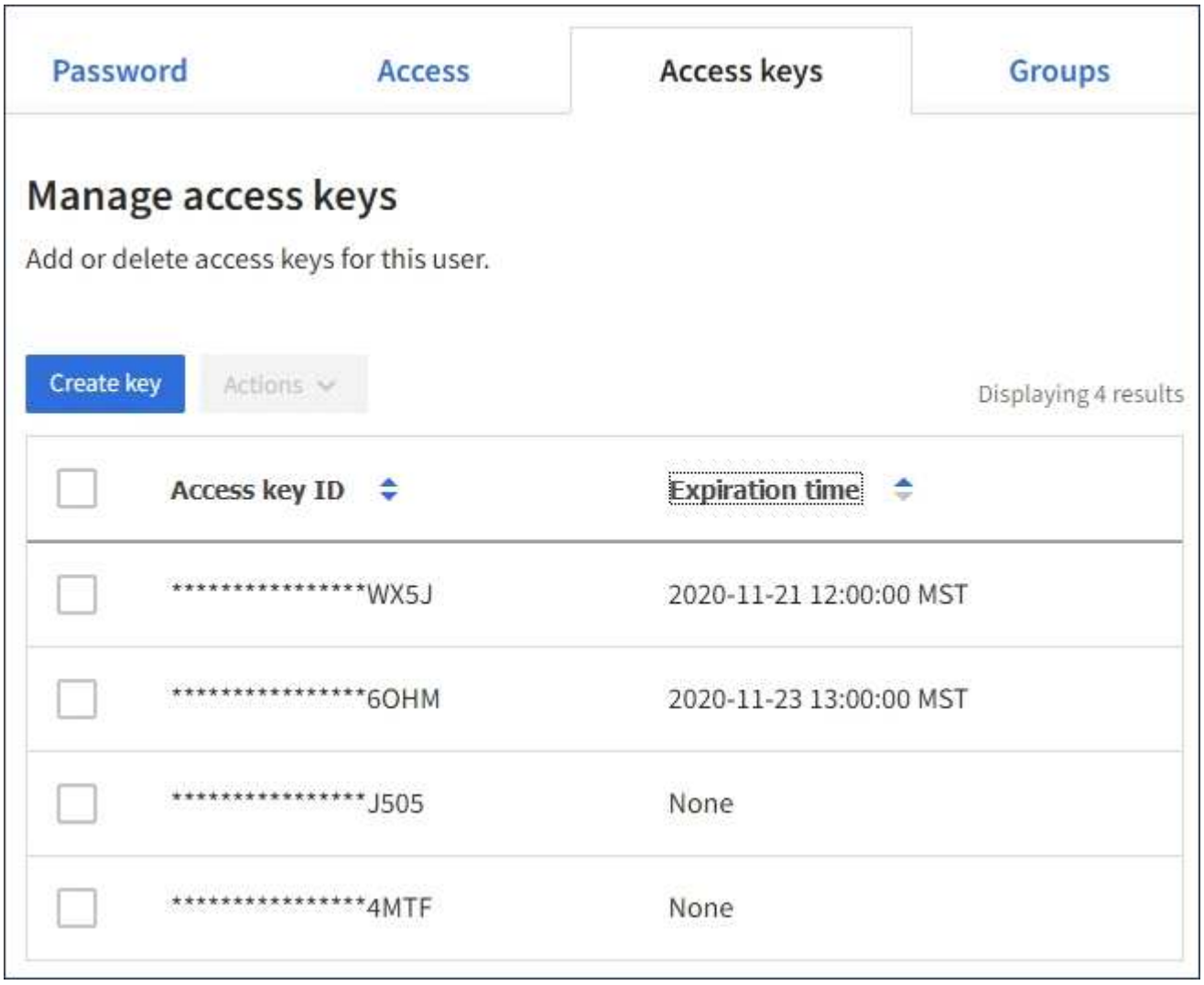
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.

   Die Seite Benutzer wird angezeigt und listet die vorhandenen Benutzer auf.

2. Wählen Sie den Benutzer aus, dessen S3-Zugriffstasten Sie anzeigen möchten.

   Die Seite Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten**.



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 der S3-Zugriffsschlüssel eines anderen Benutzers"

Löschen der S3-Zugriffsschlüssel eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

> 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**.

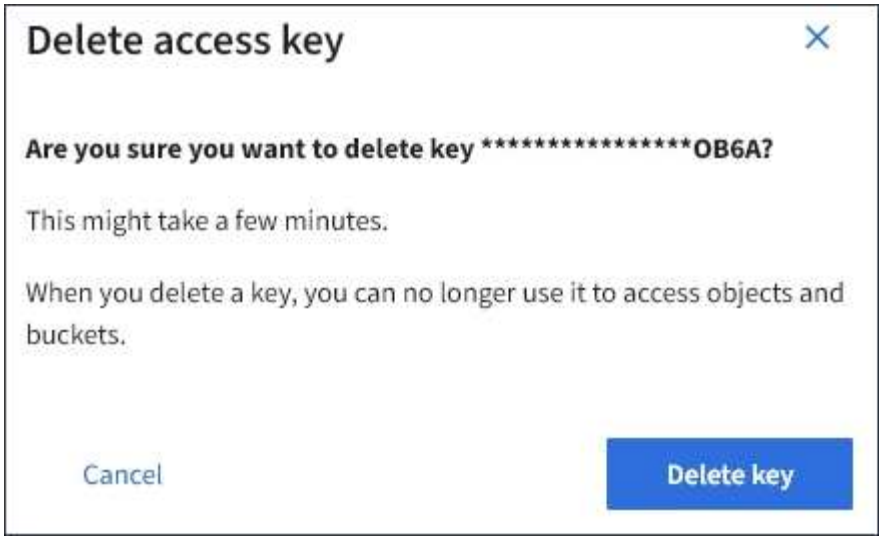
   Die Seite Benutzer wird angezeigt und listet die vorhandenen Benutzer auf.

2. Wählen Sie den Benutzer aus, dessen S3-Zugriffsschlüssel Sie managen möchten.

   Die Seite Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten** aus, und aktivieren Sie dann das Kontrollkästchen für jeden zu löschenden Zugriffsschlüssel.
4. Wählen Sie **Aktionen** > **Ausgewählte Taste löschen**.

   Ein Bestätigungsdialogfeld wird angezeigt.



5. Wählen Sie * Taste löschen*.

   In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Management von S3-Buckets

Wenn Sie einen S3-Mandanten mit entsprechenden Berechtigungen verwenden, können Sie S3-Buckets erstellen, anzeigen und löschen, Einstellungen für Konsistenzstufen aktualisieren, Cross-Origin Resource Sharing (CORS) konfigurieren, Einstellungen für Updates der letzten Zugriffszeit aktivieren bzw. deaktivieren und S3-Plattformservices managen.

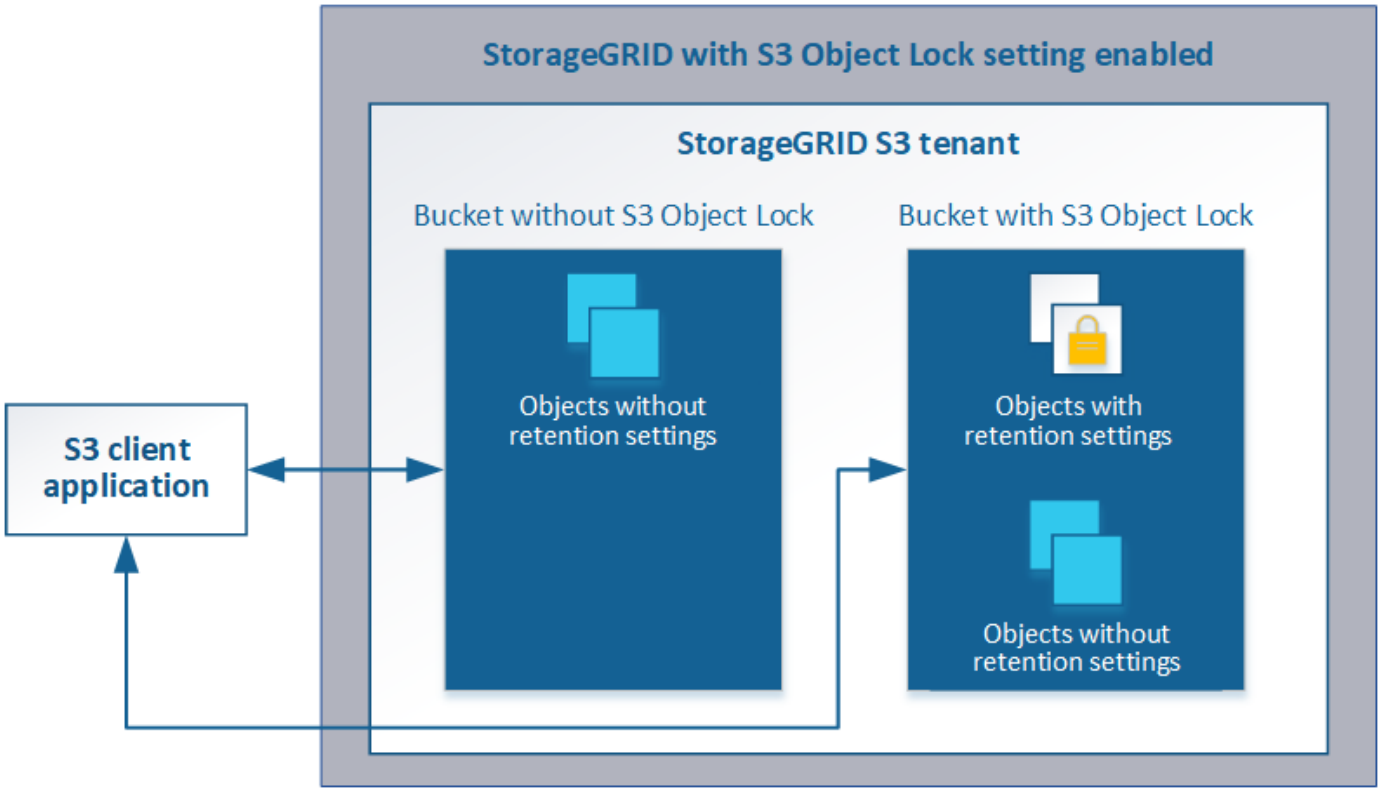
Verwenden der S3-Objektsperre

Sie können die S3-Objektsperrfunktion in StorageGRID verwenden, wenn Ihre Objekte die gesetzlichen Aufbewahrungsvorgaben 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 in einem Bucket S3-Objektsperre aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion in diesem Bucket angeben. Eine Objektversion muss über Aufbewahrungseinstellungen verfügen, die durch S3 Object Lock geschützt werden sollen.



Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

Wenn in einem Bucket S3-Objektsperre aktiviert ist, kann die S3-Client-Applikation beim Erstellen oder Aktualisieren eines Objekts optional eine oder beide der folgenden Aufbewahrungseinstellungen auf Objektebene angeben:

- **Bis-Datum aufbewahren**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Bei Bedarf kann das Aufbewahrungsdatum eines Objekts erhöht werden, dieses Datum kann jedoch nicht verringert werden.
- **Legal Hold**: Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflichten haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

Weitere Informationen zu diesen Einstellungen finden Sie unter „`Using S3 object Lock`“ in "Unterstützte Vorgänge und Einschränkungen durch S3-REST-API".

Management älterer, konformer Buckets

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. Weitere Informationen finden Sie im NetApp Knowledge Base Artikel.

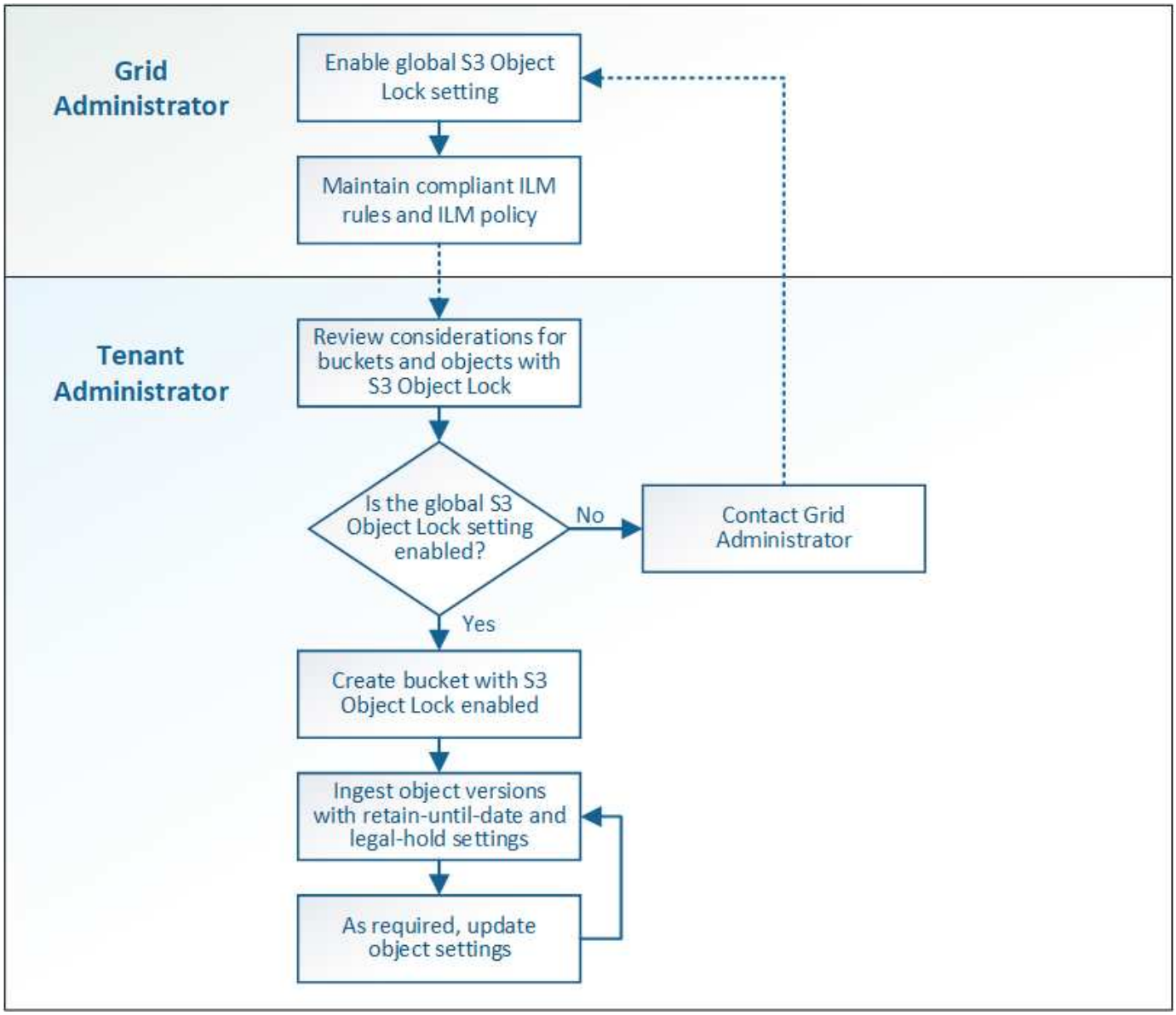
"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

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-Objektsperreneinstellung 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 zum Verwalten von Objekten mit Information Lifecycle Management.

Nachdem die globale S3-Objektsperre aktiviert wurde, können Sie Buckets mit aktivierter S3-Objektsperre erstellen. Anschließend können Sie mithilfe der S3-Client-Applikation optional Aufbewahrungseinstellungen für jede Objektversion angeben.



Verwandte Informationen

"Objektmanagement mit ILM"

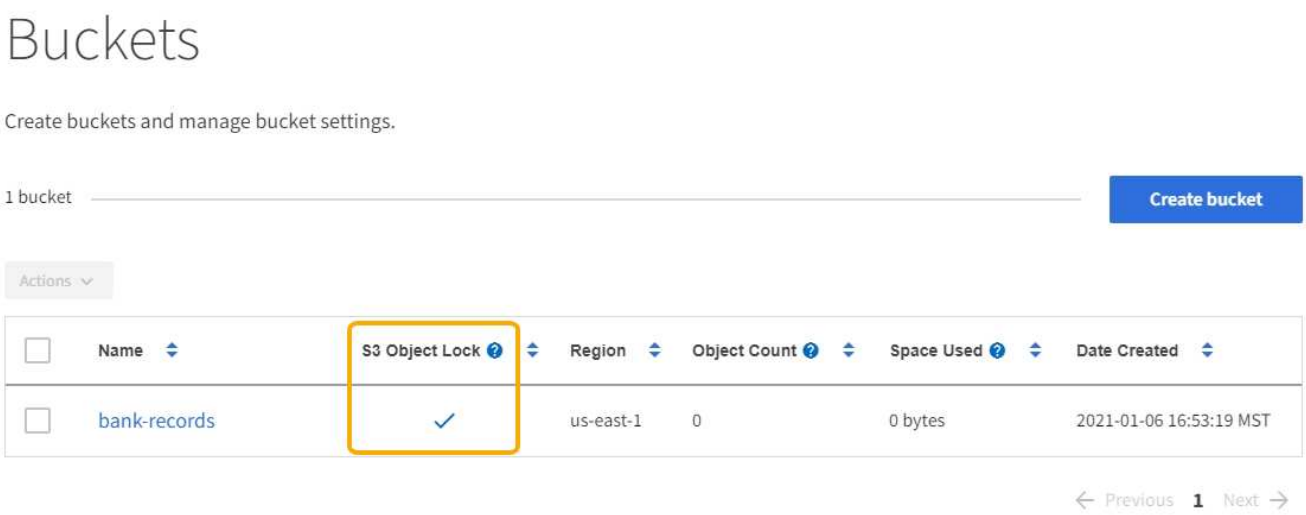
Anforderungen für die S3-Objektsperre

Bevor Sie die S3-Objektsperre für einen Bucket aktivieren, überprüfen Sie die Anforderungen für S3-Objektsperren-Buckets und -Objekte sowie den Lebenszyklus von Objekten in Buckets, wobei S3-Objektsperre aktiviert ist.

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.

  In diesem Beispiel aus dem Tenant Manager wird ein Bucket angezeigt, in dem S3 Object Lock aktiviert ist.



- 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.
- Bucket-Versionierung ist mit S3 Object Lock erforderlich. Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket.
- Nachdem Sie einen Bucket mit aktivierter S3-Objektsperre erstellt haben, können Sie die S3-Objektsperre oder die Versionierung für diesen Bucket nicht deaktivieren.
- Ein StorageGRID-Bucket mit aktivierter S3-Objektsperre hat keinen standardmäßigen Aufbewahrungszeitraum. Stattdessen kann die S3-Client-Applikation optional für jede Objektversion, die zu diesem Bucket hinzugefügt wird, ein Aufbewahrungsdatum und eine Einstellung für die Aufbewahrung gemäß den gesetzlichen Aufbewahrungspflichten festlegen.
- Bucket-Lifecycle-Konfiguration wird für S3-Objekt-Lifecycle-Buckets unterstützt.
- 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

- Die S3-Client-Applikation muss Aufbewahrungseinstellungen für jedes Objekt angeben, das durch die S3-Objektsperre geschützt werden muss.
- Sie können das Aufbewahrungsdatum für eine Objektversion erhöhen, diesen Wert jedoch nie reduzieren.
- Wenn Sie über eine ausstehende rechtliche oder behördliche Untersuchung informiert werden, können Sie relevante Informationen erhalten, indem Sie eine gesetzliche Aufbewahrungspflichten auf eine Objektversion setzen. Wenn eine Objektversion unter einer gesetzlichen Aufbewahrungspflichten liegt,

kann das Objekt nicht aus StorageGRID gelöscht werden, auch wenn es seine Aufbewahrungsfrist bis zum letzten Tag erreicht hat. Sobald die gesetzliche Aufbewahrungspflichten aufgehoben sind, kann die Objektversion gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.

- Für die S3-Objektsperre ist die Verwendung versionierter Buckets erforderlich. 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 Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft drei Phasen:

1. **Objektaufnahme**
   - Beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre kann die S3-Client-Applikation optional Aufbewahrungseinstellungen für das Objekt festlegen (bis dato, gesetzliche Aufbewahrungspflichten oder beides). StorageGRID generiert dann Metadaten für dieses Objekt, einschließlich einer eindeutigen Objekt-ID (UUID) sowie Datum und Uhrzeit der Aufnahme.
   - Nach der Aufnahme einer Objektversion mit Aufbewahrungseinstellungen können seine Daten und benutzerdefinierten S3-Metadaten nicht mehr geändert werden.
   - StorageGRID speichert die Objektmetadaten unabhängig von den Objektdaten. Es behält drei Kopien aller Objektmetadaten an jedem Standort.
2. **Aufbewahrung von Objekten**
   - StorageGRID speichert mehrere Kopien des Objekts. Die genaue Anzahl und Art der Kopien und der Speicherorte werden durch die konformen Regeln in der aktiven ILM-Richtlinie festgelegt.
3. **Löschen von Objekten**
   - Ein Objekt kann gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
   - Ein Objekt, das sich unter einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht gelöscht werden.

Erstellen eines S3-Buckets

Sie können im Mandanten-Manager S3-Buckets für Objektdaten erstellen. Wenn Sie einen Bucket erstellen, müssen Sie Namen und Region des Bucket angeben. Wenn die globale S3-Objektsperre für das StorageGRID-System aktiviert ist, können Sie optional die S3-Objektsperre für den Bucket aktivieren.

Was Sie benötigen

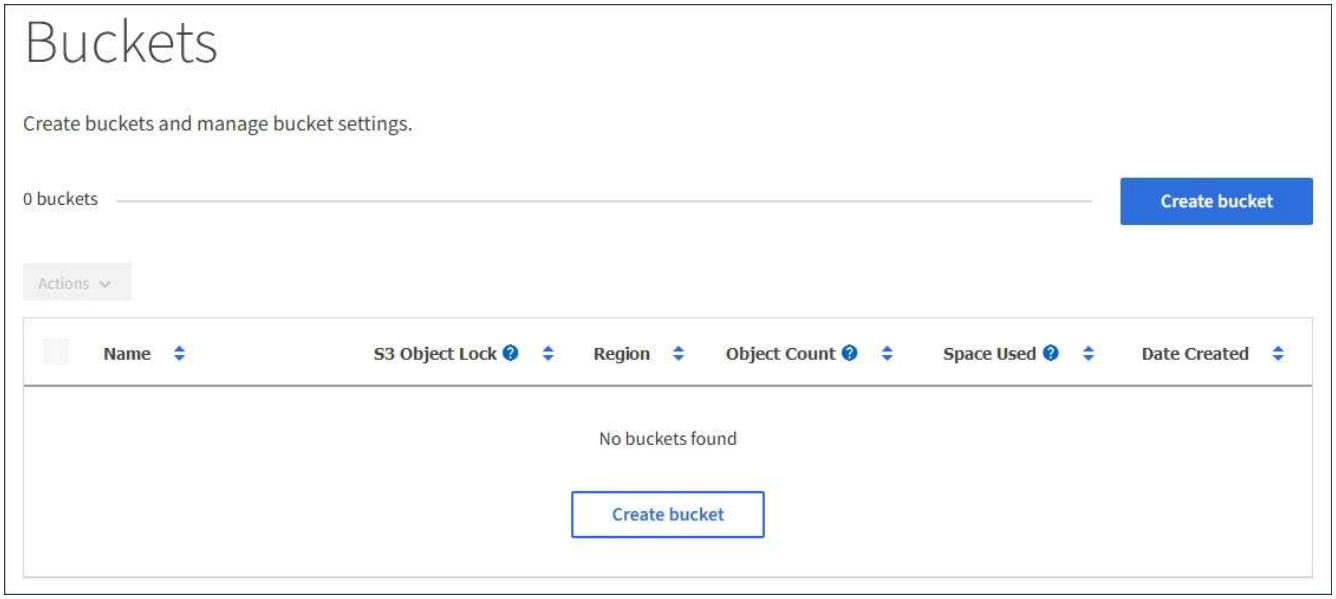
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Wenn Sie einen Bucket mit S3-Objektsperre erstellen möchten, muss die globale S3-Objektsperre für das StorageGRID-System aktiviert worden sein und Sie müssen die Anforderungen für S3-Objektsperren-Buckets und -Objekte überprüft haben.

  "Verwenden der S3-Objektsperre"

Schritte

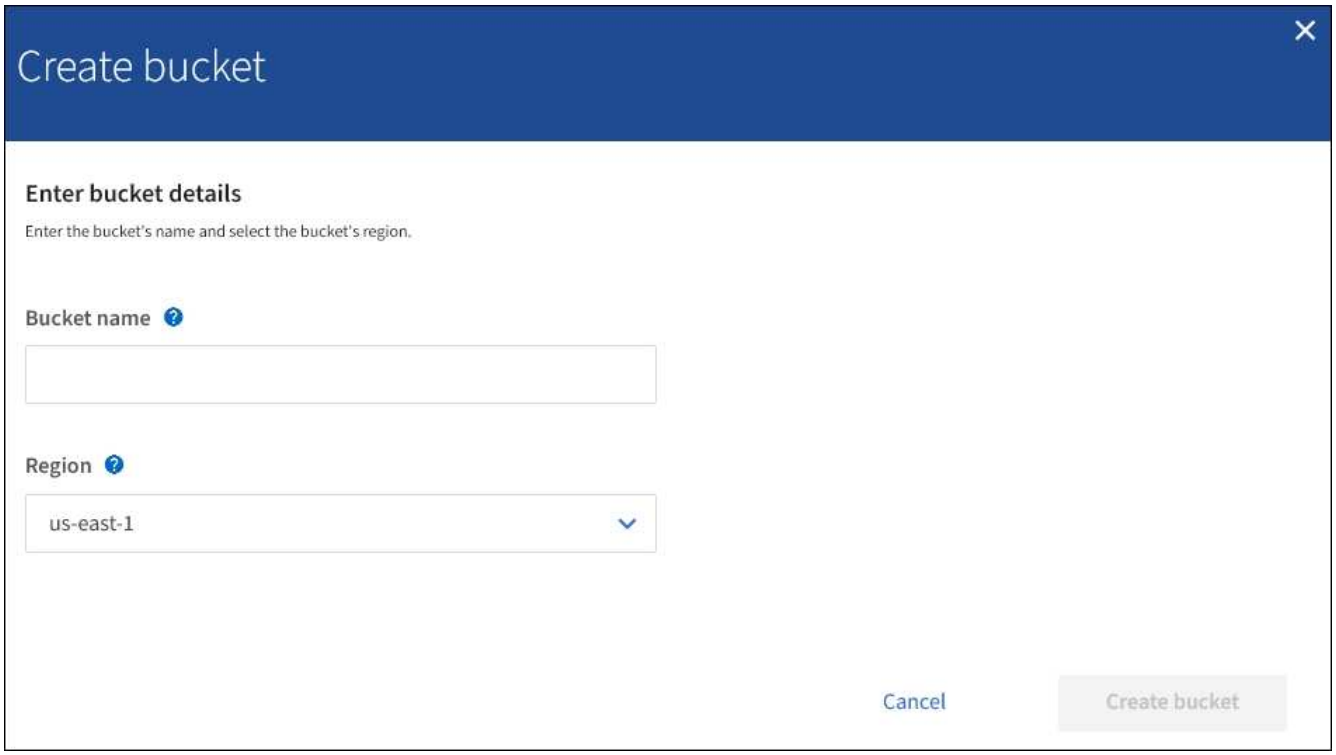
1. Wählen Sie **STORAGE (S3)** > **Buckets** aus.

   Die Seite Buckets wird angezeigt und listet alle Buckets auf, die bereits erstellt wurden.



2. Wählen Sie **Eimer erstellen**.

   Der Bucket-Assistent Erstellen wird angezeigt.



   Wenn die globale S3-Objektsperre aktiviert ist, enthält Create Bucket einen zweiten Schritt zum Managen der S3-Objektsperre für den Bucket.

3. Geben Sie einen eindeutigen Namen für den Bucket ein.

Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

Bucket-Namen müssen folgende Regeln einhalten:

- 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.

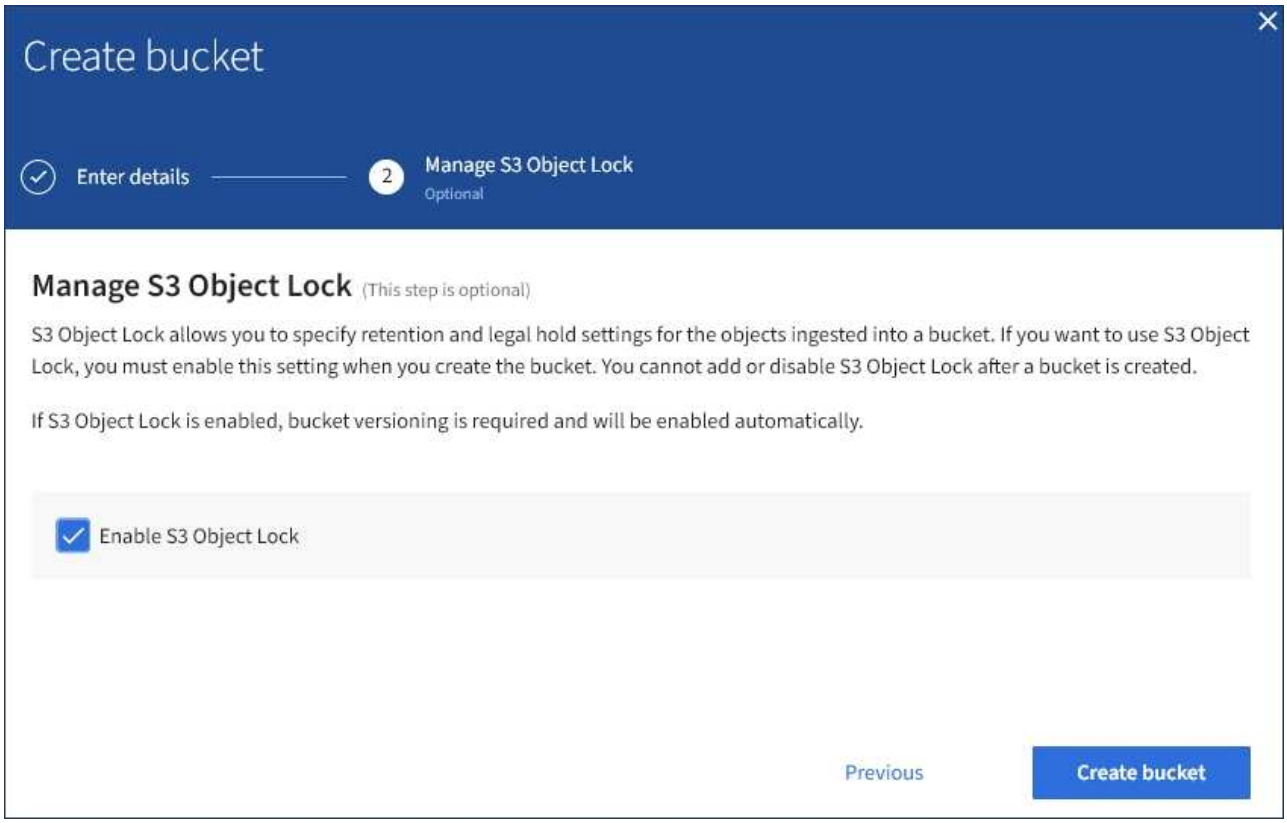
Weitere Informationen finden Sie in der Dokumentation zu Amazon Web Services (AWS).

4. Wählen Sie die Region für diesen Bucket aus.

   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 `us-east-1` Werden.

   Nach dem Erstellen des Buckets können Sie die Region nicht ändern.

5. Wählen Sie **Eimer erstellen** oder **Weiter**.
   - Wenn die globale S3-Objektsperre nicht aktiviert ist, wählen Sie **Bucket erstellen** aus. Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.
   - Wenn die globale S3-Objektsperre aktiviert ist, wählen Sie **Weiter**. Schritt 2, S3-Objektsperre verwalten, wird angezeigt.



6. Aktivieren Sie optional das Kontrollkästchen, um die S3-Objektsperre für diesen Bucket zu aktivieren.

   S3-Objektsperre muss für den Bucket aktiviert sein, bevor eine S3-Client-Applikation für die dem Bucket hinzugefügten Objekte Haltungs- bis datums- und gesetzliche Aufbewahrungs-Einstellungen festlegen kann.

   > Sie können die S3-Objektsperre nach dem Erstellen des Buckets nicht aktivieren oder deaktivieren.

   > Wenn Sie S3 Object Lock für einen Bucket aktivieren, wird die Bucket-Versionierung automatisch aktiviert.

7. Wählen Sie **Eimer erstellen**.

   Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.

Verwandte Informationen

"Objektmanagement mit ILM"

"Das Mandantenmanagement-API von NetApp"

"S3 verwenden"

Anzeigen von S3-Bucket-Details

Sie können eine Liste der Buckets und Bucket-Einstellungen in Ihrem Mandantenkonto anzeigen.

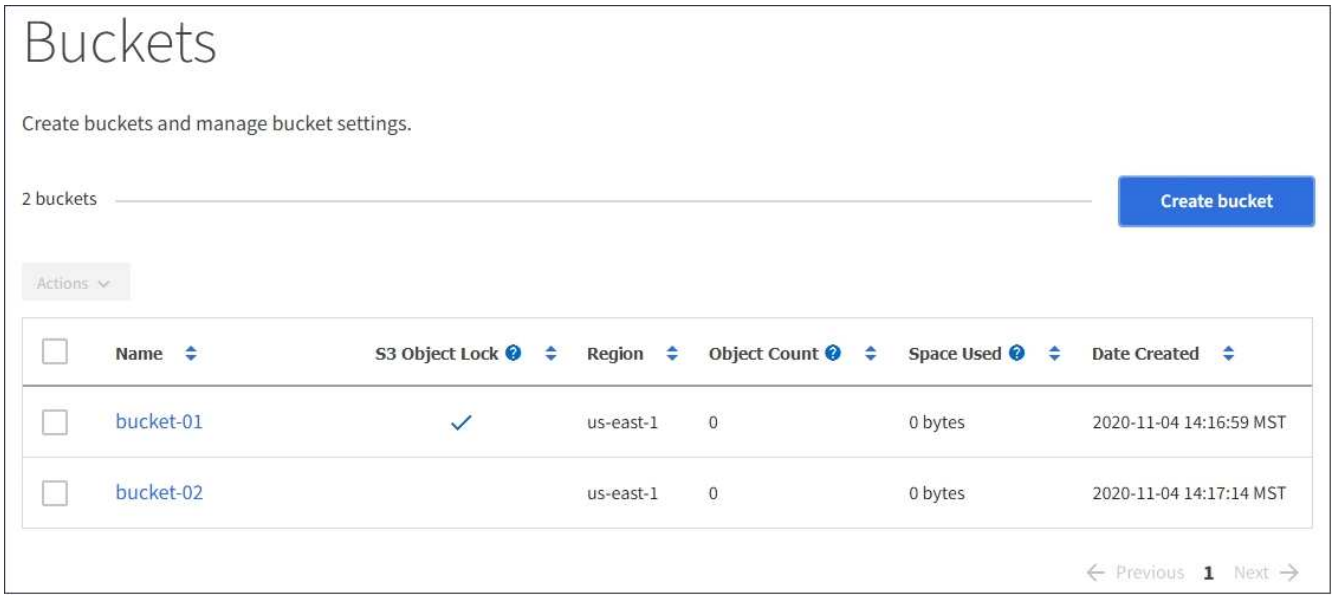
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Buckets** aus.

   Die Seite Buckets wird angezeigt und enthält alle Buckets für das Mandantenkonto.



2. Überprüfen Sie die Informationen 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.

   - Name: Der eindeutige Name des Buckets, der nicht geändert werden kann.
   - S3 Object Lock: Ob S3 Object Lock für diesen Bucket aktiviert ist.

     Diese Spalte wird nicht angezeigt, wenn die globale S3-Objektsperre deaktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.

   - Region: Die Eimer-Region, die nicht geändert werden kann.
   - Objektanzahl: Die Anzahl der Objekte in diesem Bucket.
   - Verwendeter Speicherplatz: Die logische Größe aller Objekte in diesem Bucket. Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.
   - Erstellungsdatum: Das Datum und die Uhrzeit, zu der der Bucket erstellt wurde.

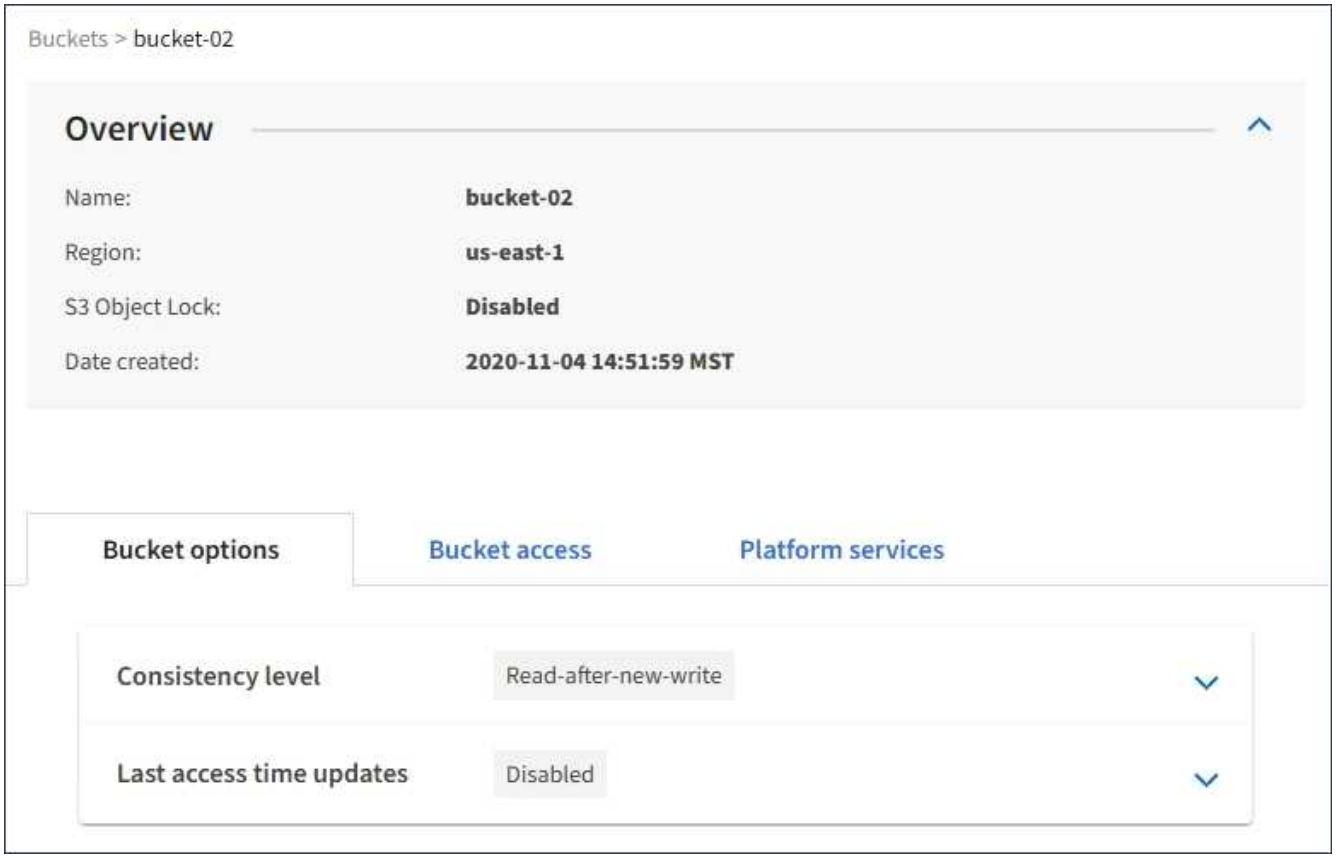
   > Die angezeigten Werte für Objektanzahl und verwendeter Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

3. Um die Einstellungen für einen Bucket anzuzeigen und zu managen, wählen Sie den Bucket-Namen aus.

   Die Seite mit den Bucket-Details wird angezeigt.

Auf dieser Seite können Sie die Einstellungen für Bucket-Optionen, Bucket-Zugriff und Plattform-Services anzeigen und bearbeiten.

Weitere Informationen zur Konfiguration der einzelnen Einstellungen oder des Plattform-Service finden Sie in den Anweisungen.



Verwandte Informationen

"Ändern der Konsistenzstufe"

"Aktivieren oder Deaktivieren von Updates der letzten Zugriffszeit"

"Konfigurieren der Cross-Origin Resource Sharing (CORS)"

"CloudMirror-Replizierung wird konfiguriert"

"Ereignisbenachrichtigungen werden konfiguriert"

"Konfigurieren des Suchintegrationsservice"

Ändern der Konsistenzstufe

Wenn Sie einen S3-Mandanten verwenden, können Sie mithilfe des Mandanten Manager oder der Mandanten-Management-API die Konsistenzkontrolle für Vorgänge ändern, die in den Objekten in S3 Buckets ausgeführt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.

- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Die Konsistenzstufe sorgt für einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten 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.

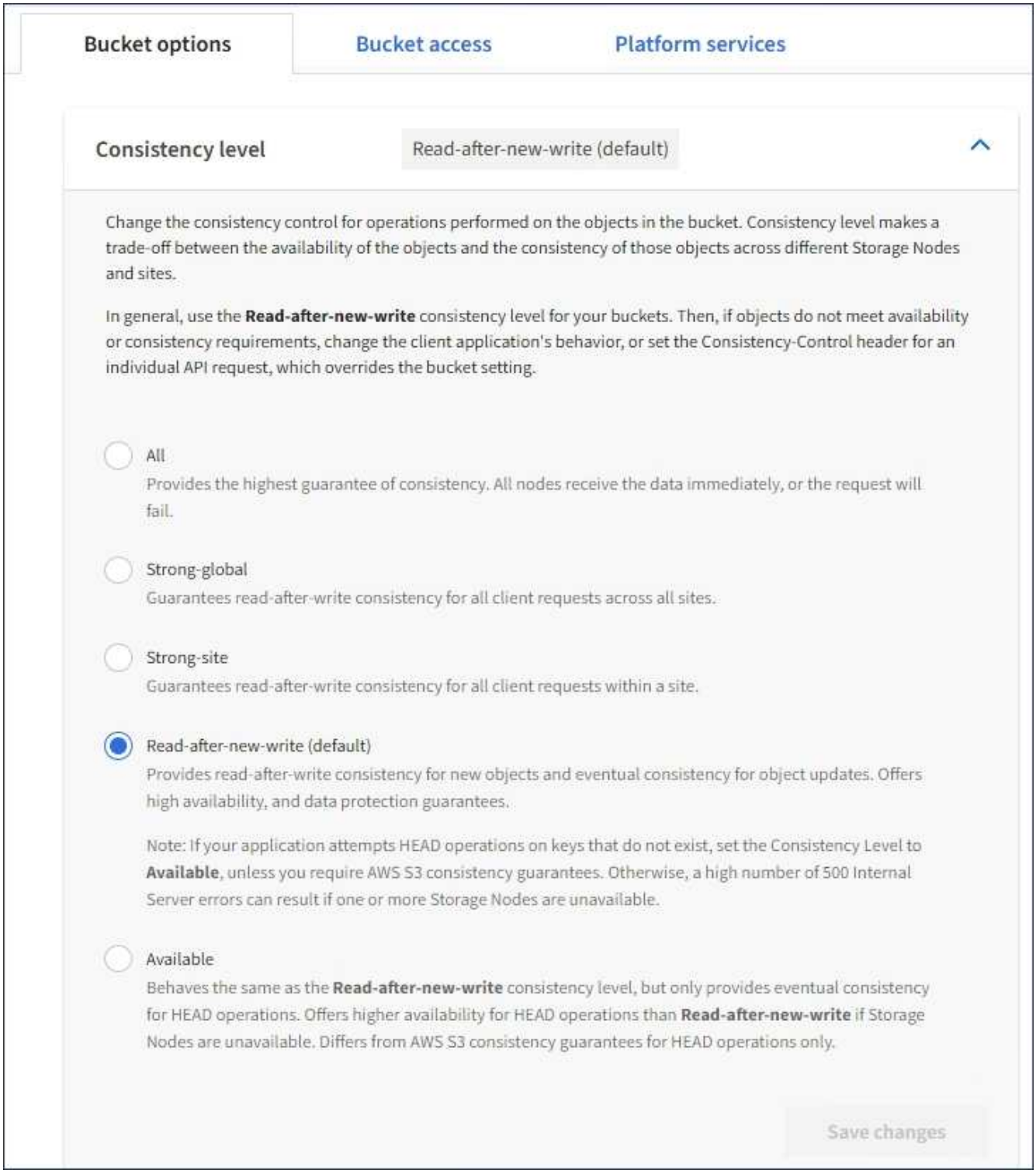
> Wenn Sie die Konsistenzstufe eines Buckets ändern, werden nur die Objekte, die nach der Änderung aufgenommen werden, garantiert, um die überarbeitete Ebene zu erfüllen.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.

   Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie **Bucket-Optionen** > **Konsistenzstufe** aus.



4. Wählen Sie eine Konsistenzstufe für Operationen aus, die an den Objekten in diesem Bucket durchgeführt werden.

Konsistenzstufe	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.

Konsistenzstufe	Beschreibung
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 (Standard)	Ermöglicht Konsistenz von Lese- nach Schreibvorgängen für neue Objekte und die eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung versucht, HEAD-Operationen auf Schlüssel, die nicht vorhanden sind, setzen Sie die Consistency Level auf **available**, es sei denn, Sie benötigen Amazon S3 Consistency Guarantees. Andernfalls kann eine hohe Anzahl von 500 internen Serverfehlern führen, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenz **Read-after-New-write**, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit für DEN HAUPTBETRIEB als **Read-after-New-write**, wenn Speicherknoten nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

5. Wählen Sie **Änderungen speichern**.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

Aktivieren oder Deaktivieren von 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 **Last Access Time** in ihrer Platzierungsanleitung verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Letzter Zugriffszeitpunkt ist eine der Optionen für die **Referenzzeit**-Platzierungsanweisung für eine ILM-Regel. Durch Festlegen der Referenzzeit für eine Regel auf Letzter Zugriffszeit können Grid-Administratoren

festlegen, dass Objekte an bestimmten Speicherorten platziert werden, basierend auf dem Zeitpunkt, an dem diese Objekte zuletzt abgerufen wurden (gelesen oder angezeigt).

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 Speicherknoten verbleiben.
- Objekte, die im letzten Monat nicht abgerufen wurden, sollten an einen externen Standort verschoben werden.

> Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Standardmäßig werden Updates zur letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID-System eine ILM-Regel enthält, die die Option **Last Access Time** verwendet und diese Option auf Objekte in diesem Bucket angewendet werden soll, müssen Sie Aktualisierungen für die letzte Zugriffszeit für die in dieser Regel festgelegten S3-Buckets 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.

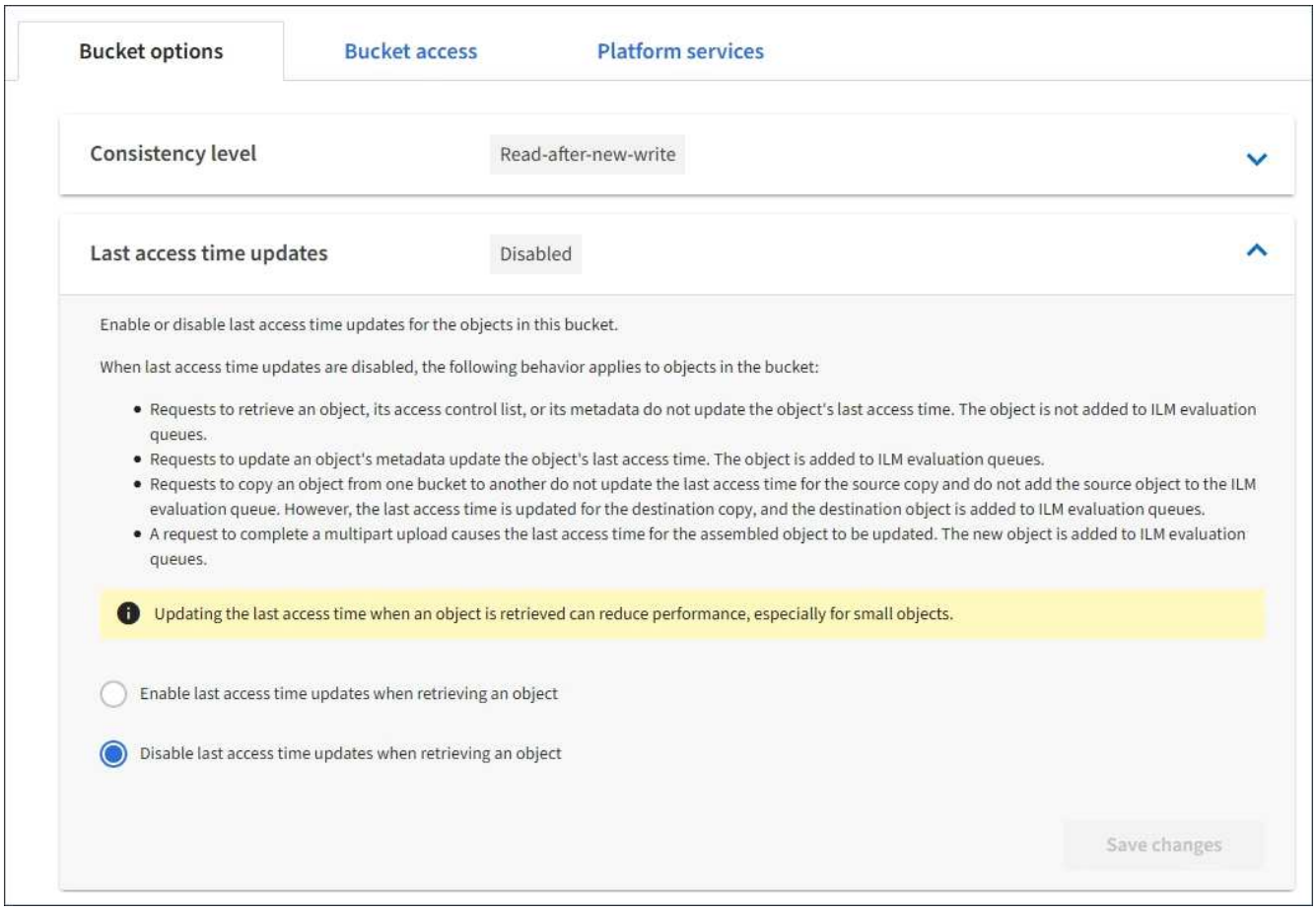
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
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 **STORAGE (S3)** > **Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.

   Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie **Bucket-Optionen** > **Letzte Aktualisierung der Zugriffszeit** aus.
4. Wählen Sie das entsprechende Optionsfeld aus, um Aktualisierungen der letzten Zugriffszeit zu aktivieren oder zu deaktivieren.



5. Wählen Sie **Änderungen speichern**.

Verwandte Informationen

"Mandantenmanagement-Berechtigungen"

"Objektmanagement mit ILM"

Konfigurieren der Cross-Origin Resource Sharing (CORS)

Die Cross-Origin Resource Sharing (CORS) kann für einen S3-Bucket konfiguriert werden, wenn für Web-Applikationen in anderen Domänen auf diesen Bucket und Objekte in diesem Bucket zugegriffen werden soll.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Cross-Origin Resource Sharing (CORS) 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`.

Schritte

1. Verwenden Sie einen Texteditor, um die XML-Datei zu erstellen, die für die Aktivierung von CORS erforderlich ist.

   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.

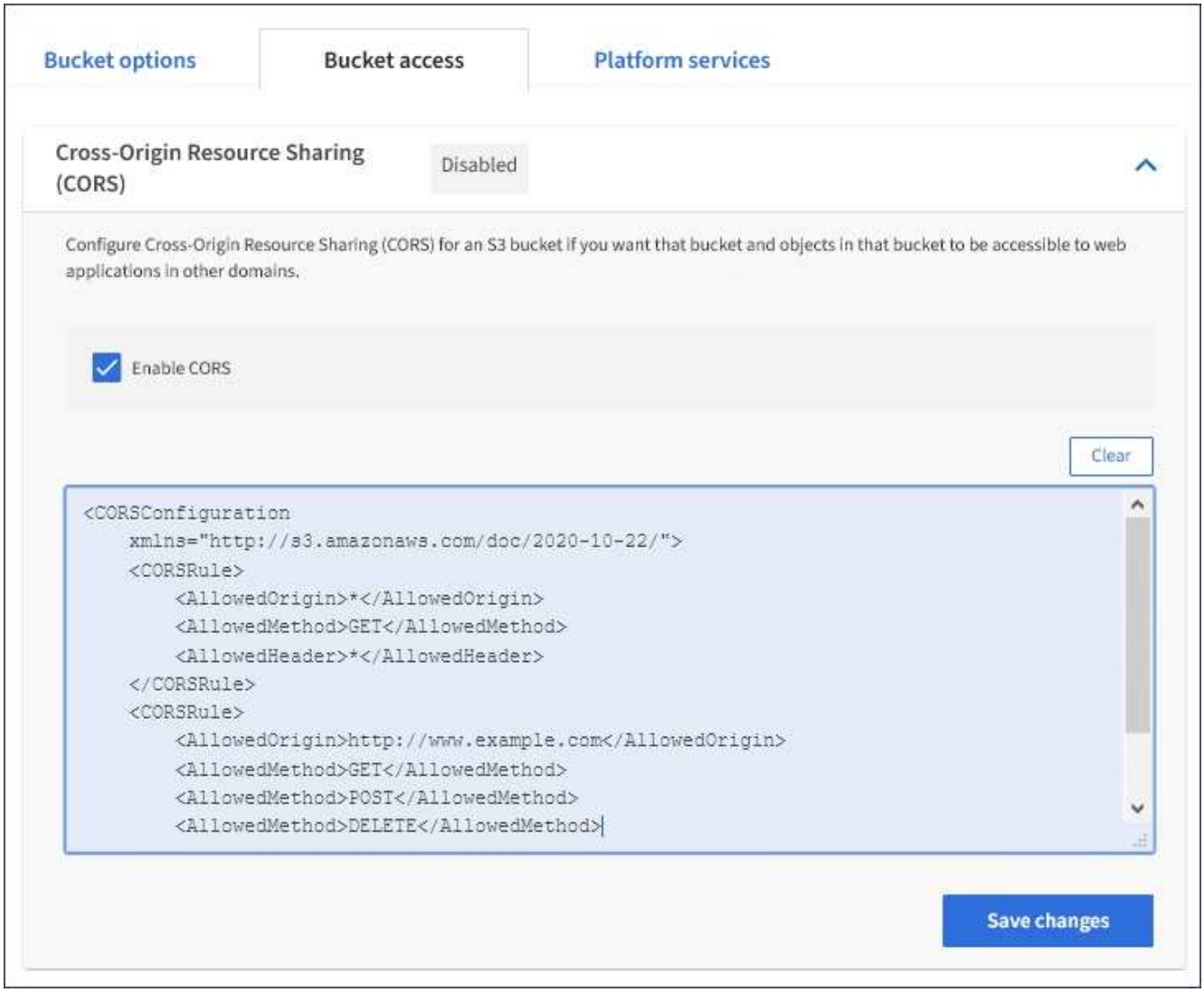
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</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 im Tenant Manager **STORAGE (S3)** > **Buckets** aus.
3. Wählen Sie den Bucket-Namen aus der Liste aus.

   Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Bucket-Zugriff** > **Cross-Origin Resource Sharing (CORS)** aus.
5. Aktivieren Sie das Kontrollkästchen * CORS aktivieren*.
6. Fügen Sie die CORS-Konfigurations-XML in das Textfeld ein und wählen Sie **Änderungen speichern**.



7. Um die CORS-Einstellung für den Bucket zu ändern, aktualisieren Sie die CORS-Konfigurations-XML im Textfeld oder wählen Sie **Löschen**, um neu zu starten. Wählen Sie dann **Änderungen speichern**.
8. Um CORS für den Bucket zu deaktivieren, deaktivieren Sie das Kontrollkästchen **CORS** aktivieren* und wählen dann **Änderungen speichern** aus.

Löschen eines S3-Buckets

Sie können den Mandanten-Manager verwenden, um einen leeren S3-Bucket zu löschen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Diese Anweisungen beschreiben das Löschen eines S3-Buckets mithilfe von Tenant Manager. Sie können auch S3-Buckets mithilfe der Mandantenmanagement-API oder der S3-REST-API löschen.

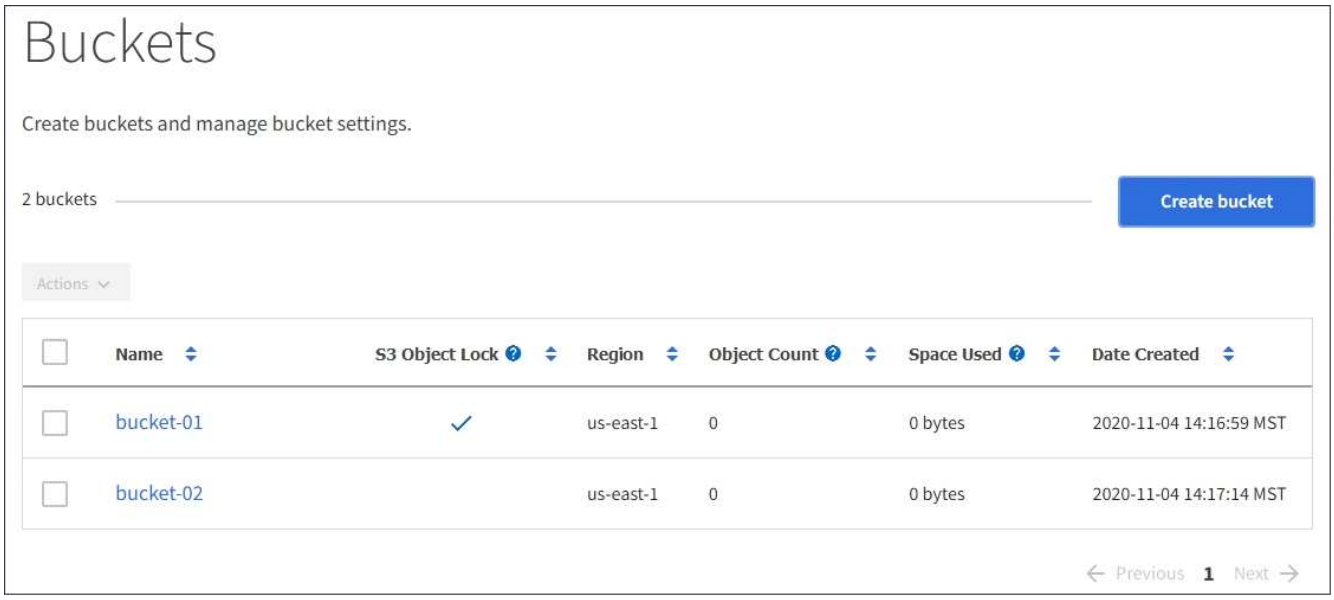
Ein S3-Bucket kann nicht gelöscht werden, wenn er Objekte oder nicht aktuelle Objektversionen enthält.

Informationen zum Löschen von S3-versionierten Objekten finden Sie in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Buckets** aus.

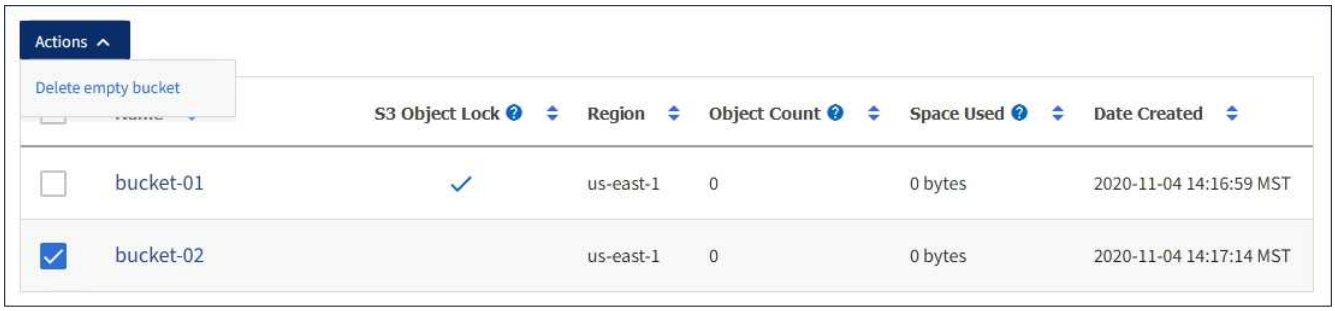
   Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.



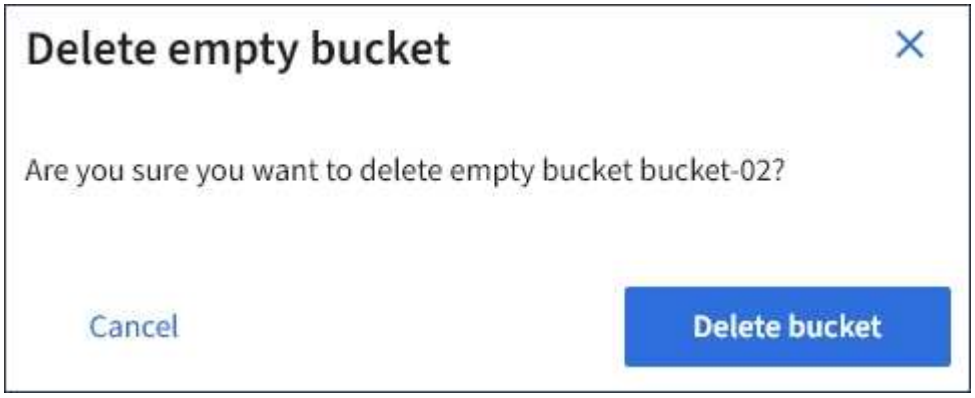
2. Aktivieren Sie das Kontrollkästchen für den leeren Bucket, den Sie löschen möchten.

   Das Menü Aktionen ist aktiviert.

3. Wählen Sie im Menü Aktionen die Option **leerer Eimer löschen** aus.



   Eine Bestätigungsmeldung wird angezeigt.



4. Wenn Sie sicher sind, dass Sie den Bucket löschen möchten, wählen Sie **Bucket löschen**.

   StorageGRID bestätigt, dass der Bucket leer ist und löscht dann den Bucket. Dieser Vorgang kann einige Minuten dauern.

   Wenn der Bucket nicht leer ist, wird eine Fehlermeldung angezeigt. Sie müssen alle Objekte löschen, bevor Sie den Bucket löschen können.

Verwandte Informationen

"Objektmanagement mit ILM"

Verwalten von S3-Plattformservices

Wenn die Nutzung von Plattform-Services für Ihr S3-Mandantenkonto zulässig ist, können Sie Plattform-Services verwenden, um externe Services zu nutzen und die Replizierung und Benachrichtigungen von CloudMirror und die Integration von S3-Buckets zu konfigurieren.

- "Um welche Plattform-Services geht es"
- "Überlegungen bei der Verwendung von Plattform-Services"
- "Konfigurieren von Endpunkten für Plattformservices"
- "CloudMirror-Replizierung wird konfiguriert"
- "Ereignisbenachrichtigungen werden konfiguriert"
- "Verwenden des Suchintegrationsdienstes"

Um welche Plattform-Services geht es

StorageGRID Plattform-Services unterstützen Sie bei der Implementierung einer Hybrid-Cloud-Strategie.

Falls die Verwendung von Plattform-Services für Ihr Mandantenkonto zulässig ist, können Sie die folgenden Services für jeden S3-Bucket konfigurieren:

- **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 wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen**: Per Bucket-Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen über bestimmte Aktionen, die an Objekten ausgeführt werden, an einen bestimmten externen Amazon

Simple Notification Service™ (SNS) zu senden.

Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.

> Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationsdienst**: Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

  Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.

  > Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperrmetadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

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 Plattformdiensten 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 mit dem Tenant Manager oder der Mandantenmanagement-API konfigurieren. 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 Endpunkt erstellt haben, können Sie einen Plattformservice für einen Bucket aktivieren, indem Sie dem Bucket die 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 Plattformdienst, den Sie konfigurieren möchten, separate XML-Konfigurationen hinzufügen. Beispiel:

1. 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.
2. Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert sind, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
3. 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	• GET Bucket-Replizierung • PUT Bucket-Replizierung
Benachrichtigungen	• Bucket-Benachrichtigung ABRUFEN • PUT Bucket-Benachrichtigung
Integration von Suchen	• Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration Diese Vorgänge sind individuell für StorageGRID.

Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung, wie StorageGRID diese APIs implementiert.

Verwandte Informationen

"S3 verwenden"

"Allgemeines zum CloudMirror Replikationsservice"

"Allgemeines zu Benachrichtigungen für Buckets"

"Beschreibung des Suchintegrationsservice"

"Überlegungen bei der Verwendung von Plattform-Services"

Allgemeines zum 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.

Wenn Sie die CloudMirror-Replizierung für einen vorhandenen Bucket aktivieren, werden nur die neuen, zu

diesem Bucket hinzugefügten Objekte repliziert. Alle bestehenden Objekte im 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 mithilfe von CloudMirror-Replizierung Objekte in ein AWS S3-Ziel kopieren, beachten Sie, dass Amazon S3 die Größe benutzerdefinierter Metadaten in jeder PUT-Anforderungs-Kopfzeile 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 auf mehrere Buckets 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 einen bidirektionalen CloudMirror zwischen zwei Grids.

Die Einzigartigkeit und Bestellung von Veranstaltungen 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.

Verwandte Informationen

"CloudMirror-Replizierung wird konfiguriert"

Allgemeines zu 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.

Sie können Ereignisbenachrichtigungen konfigurieren, indem Sie eine XML-Benachrichtigungskonfiguration mit einem Quell-Bucket verknüpfen. 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 Einzigartigkeit 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

Die StorageGRID-Ereignisbenachrichtigung folgt der Amazon S3-API und unterliegt folgenden Einschränkungen:

- Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden **nicht** unterstützt.
  - `s3:ReducedRedundancyLostObject`
  - `s3:ObjectRestore:Completed`
- Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der Tabelle dargestellt:

Schlüsselname	Wert von StorageGRID
EventSource	`sgws:s3`
AwsRegion	Nicht enthalten
X-amz-id-2	Nicht enthalten
arn	`urn:sgws:s3:::bucket_name`

Verwandte Informationen

"Ereignisbenachrichtigungen werden konfiguriert"

Beschreibung des Suchintegrationsservice

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-Integrationsservice 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 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. Benachrichtigungen werden jedoch nicht für Objekte gesendet, die sich bereits im Bucket befanden. 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-Integrationsservice 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. Ermitteln Sie mit dem *Interoperability Matrix Tool* die unterstützten Versionen von Elasticsearch.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Konfigurations-XML für die Integration der Suche"

"Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"

"Vom Suchintegrations-Service generierter JSON"

"Konfigurieren des Suchintegrationsservice"

Überlegungen bei der Verwendung von Plattform-Services

Vor der Implementierung von Plattform-Services sollten Sie die Empfehlungen und Überlegungen zu deren Verwendung überprüfen.

Überlegungen bei der Verwendung von Plattform-Services

Überlegungen	Details
Ziel-Endpoint-Monitoring	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.
Drosselung des Zielendpunkts	StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten. Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich. CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.
Bestellgarantien	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. 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.

Überlegungen	Details
ILM-gesteuerte Objektlöschungen	CloudMirror und Ereignisbenachrichtigungen werden nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID ILM-Regeln gelöscht wird, um das Löschverhalten der AWS CRR- und SNS-Services anzupassen. Beispiel: Es werden keine Anfragen für CloudMirror- oder Ereignisbenachrichtigungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht. Suchintegrationsanfragen werden dagegen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	StorageGRID unterstützt das nicht `x-amz-replication-status` Kopfzeile.
Objektgröße	Die maximale Größe für Objekte, die vom CloudMirror-Replikationsservice in einen Ziel-Bucket repliziert werden können, beträgt 5 TB. Dies ist die gleiche wie die von StorageGRID unterstützte maximale Objektgröße.
Bucket-Versionierung und VersionIDs	Wenn die Versionierung im S3-Quell-Bucket von StorageGRID aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren. 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. **Hinweis**: Version-IDs für den Quell-Bucket in StorageGRID stehen nicht im Zusammenhang mit den Version-IDs für den Ziel-Bucket.

Tagging für Objektversionen	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 Versionskennungen für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass ein Tag-Update auf eine bestimmte Version-ID repliziert wird. Im Gegensatz dazu repliziert der CloudMirror-Service PUT-Objekt-Tagging-Anforderungen 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.
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` Der 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 Replikationsvorgang mit einem AccessDenied-Fehler fehl.

Verwandte Informationen

"S3 verwenden"

Konfigurieren von Endpunkten für Plattformservices

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 Berechtigung zum Verwalten von Endpunkten oder Root-Zugriff in einem Grid sein, dessen Netzwerk konfiguriert wurde, damit Storage-Nodes auf externe Endpoint-Ressourcen 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 von einem StorageGRID-Bucket auf einen S3-Bucket replizieren möchten, erstellen Sie einen Endpunkt für Plattformservices, der die Informationen und Anmeldeinformationen enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket von AWS 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 einer anderen Umgebung 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"

Festlegen des URN für einen Endpunkt der Plattformdienste

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 Plattformdienst 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 AWS 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
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, die auf AWS gehostet werden

Für AWS Einheiten ist Complete 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.

Erstellen eines Endpunkts für Plattformservices

Sie müssen mindestens einen Endpunkt des richtigen Typs erstellen, bevor Sie einen Plattformdienst aktivieren können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Endpunkte verwalten verfügt.
- Die Ressource, auf die der Endpunkt der Plattformservices verweist, muss erstellt worden sein:
  - CloudMirror Replizierung: S3 Bucket
  - Ereignisbenachrichtigung: SNS-Thema
  - Suchbenachrichtigung: Elasticsearch-Index, wenn das Ziel-Cluster nicht konfiguriert ist, Indizes automatisch zu erstellen.
- Sie müssen über die Informationen zur Zielressource verfügen:
  - 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)

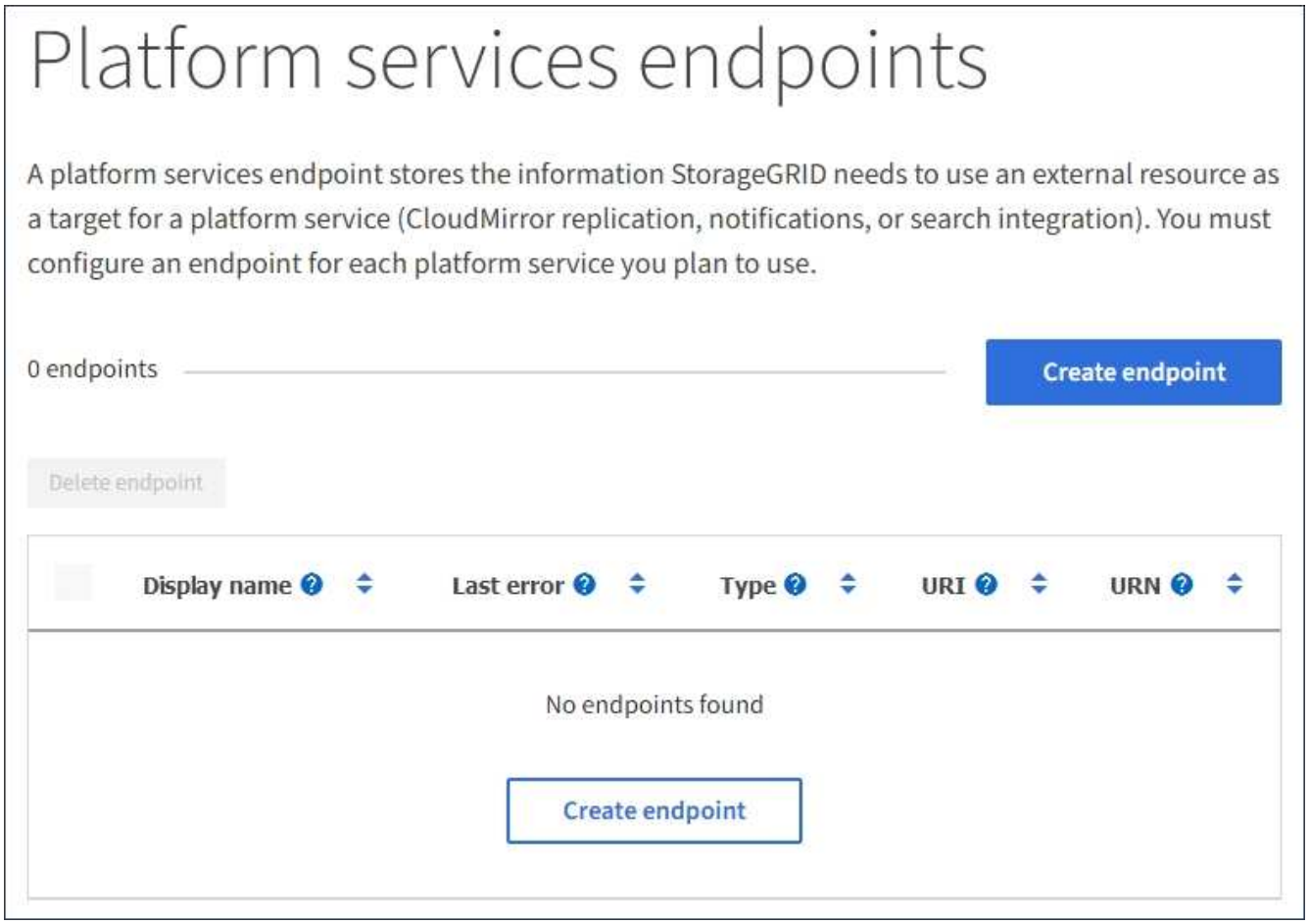
    "Festlegen des URN für einen Endpunkt der Plattformdienste"

  - Authentifizierungsdaten (falls erforderlich):
    - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
    - Basic HTTP: Benutzername und Passwort
  - Sicherheitszertifikat (bei Verwendung eines benutzerdefinierten CA-Zertifikats)

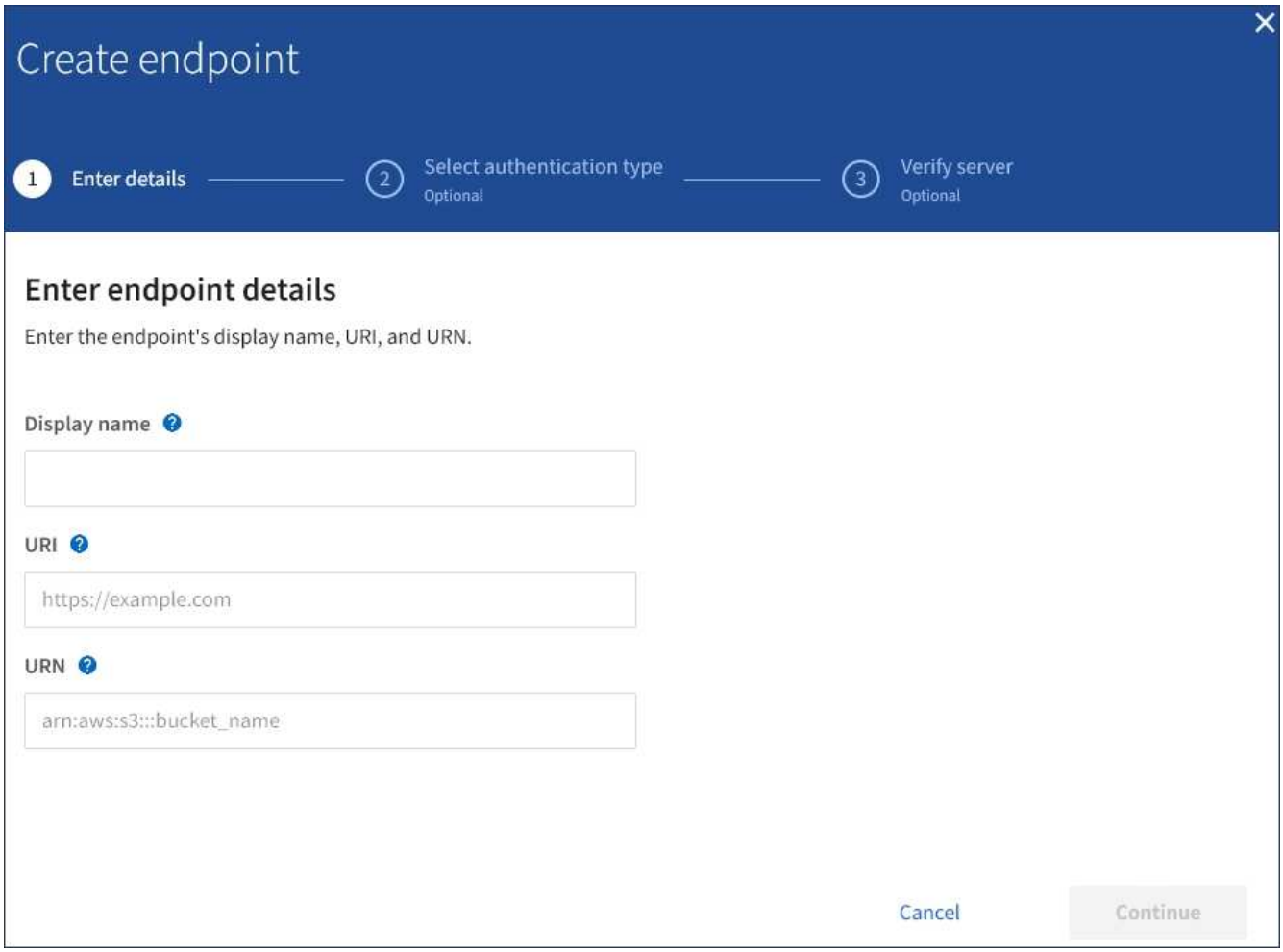
Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattform-Services-Endpunkte** aus.

   Die Seite „Endpunkte der Plattformdienste“ wird angezeigt.



2. Wählen Sie **Endpunkt erstellen**.



3. Geben Sie einen Anzeigenamen ein, um den Endpunkt und seinen Zweck kurz zu beschreiben.

   Der vom Endpunkt unterstützte Plattformdienst wird neben dem Endpunkt-Namen angezeigt, wenn er auf der Seite Endpoints aufgeführt wird. Sie müssen diese Informationen also nicht in den Namen einfügen.

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 verwendet, und Port 80 wird 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 möglich, sollten Sie sich mit einer HA-Gruppe von Lastausgleichs Nodes verbinden, um einen Single Point of Failure zu vermeiden.

Auf ähnliche Weise kann der URI für einen Bucket sein, der auf AWS gehostet wird,:

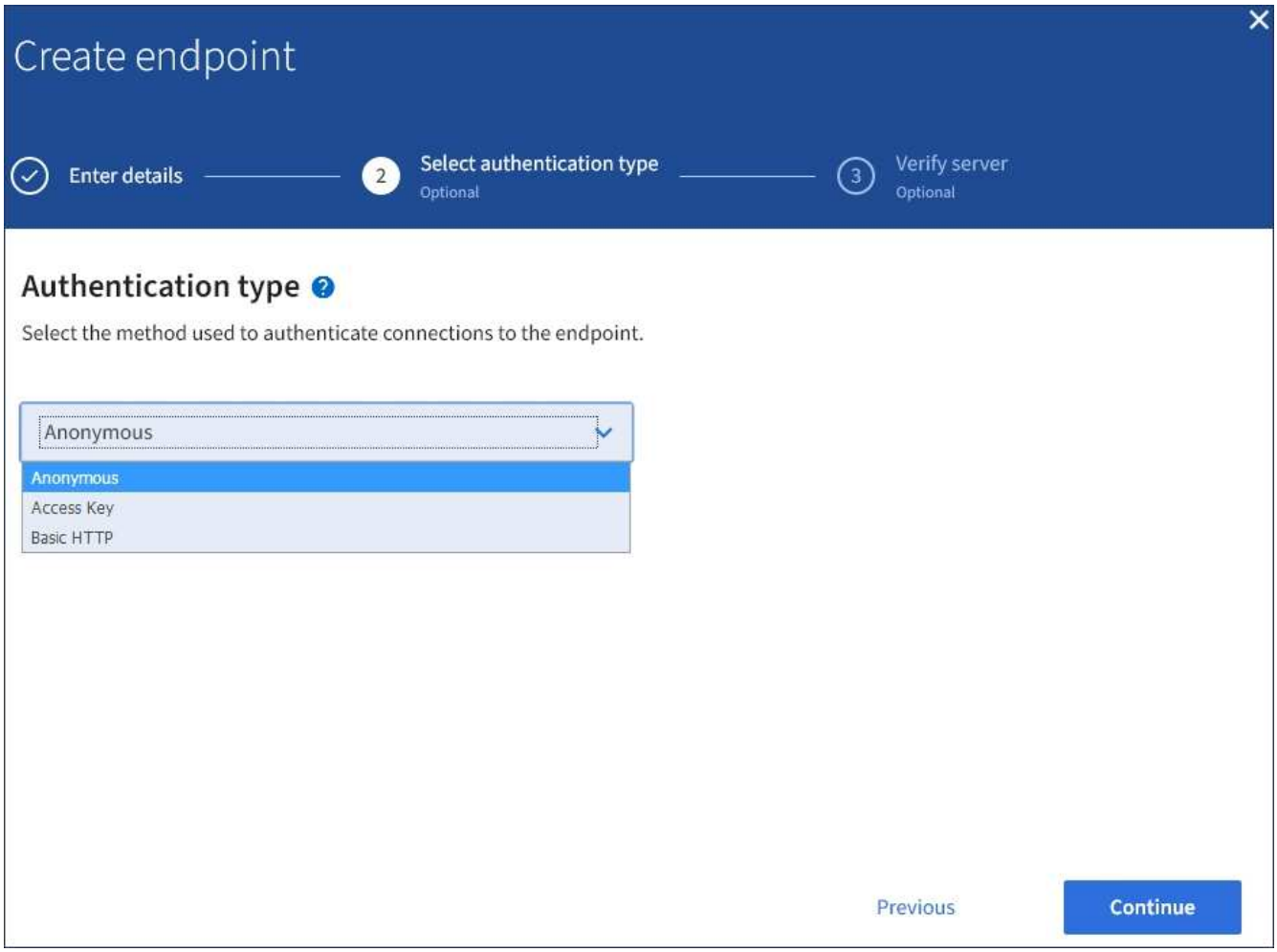
```
https://s3-aws-region.amazonaws.com
```

Wenn der Endpunkt für den CloudMirror-Replikationsservice verwendet wird, geben 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 den URN eines Endpunktes nicht ändern, nachdem der Endpunkt erstellt wurde.

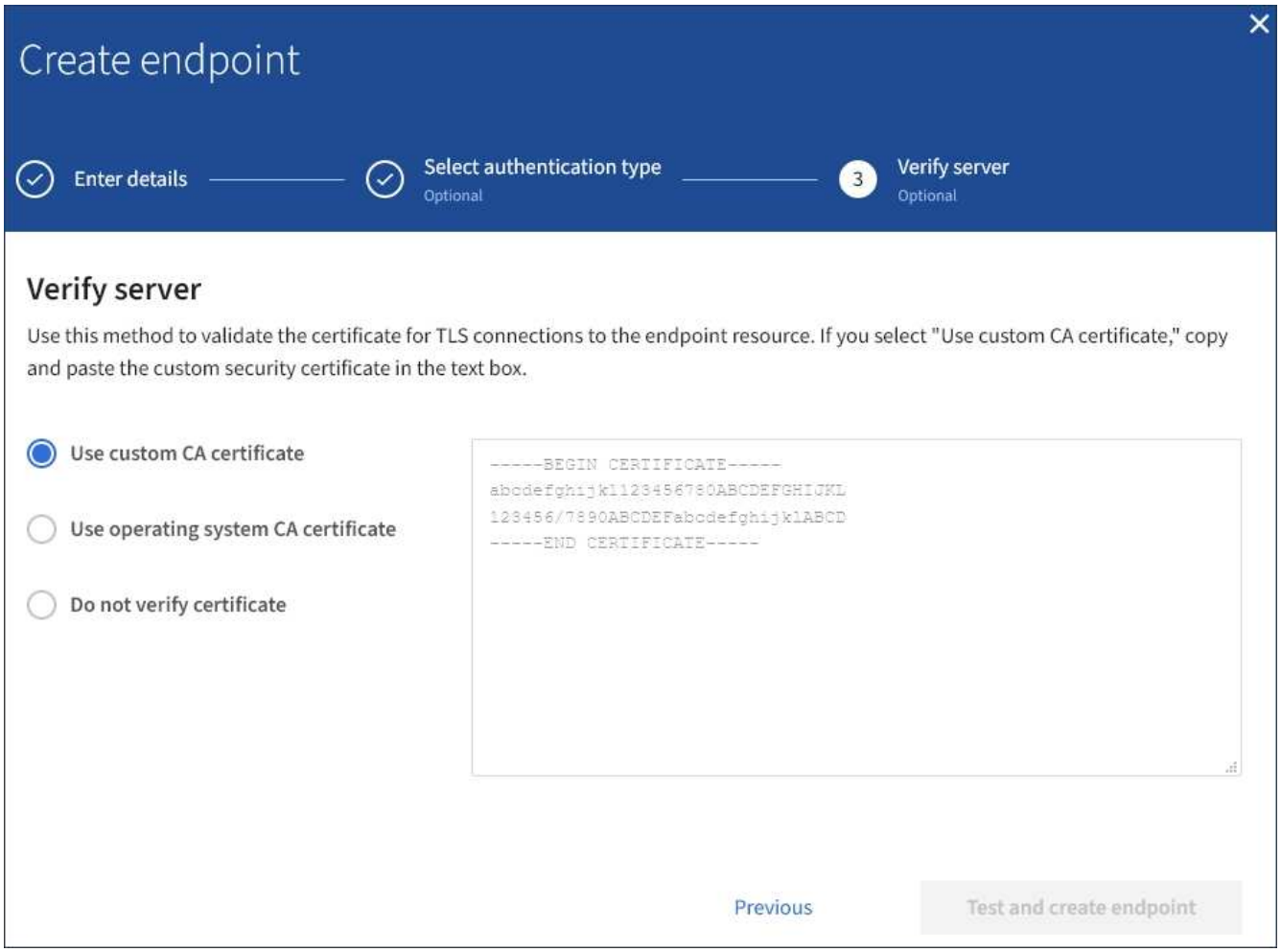
6. Wählen Sie **Weiter**.
7. Wählen Sie einen Wert für **Authentifizierungstyp** aus, und geben Sie dann die erforderlichen Anmeldedaten ein.



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	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Basis-HTTP	Verwendet einen Benutzernamen und ein Passwort, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

8. Wählen Sie **Weiter**.
9. Wählen Sie eine Optionsschaltfläche für **Server überprüfen** aus, um auszuwählen, wie die TLS-Verbindung zum Endpunkt verifiziert wird.



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-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 Endpoint-Erstellung 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

"Festlegen des URN für einen Endpunkt der Plattformdienste"

"CloudMirror-Replizierung wird konfiguriert"

"Ereignisbenachrichtigungen werden konfiguriert"

"Konfigurieren des Suchintegrationsservice"

Testen der Verbindung für einen 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Endpunkte verwalten verfügt.

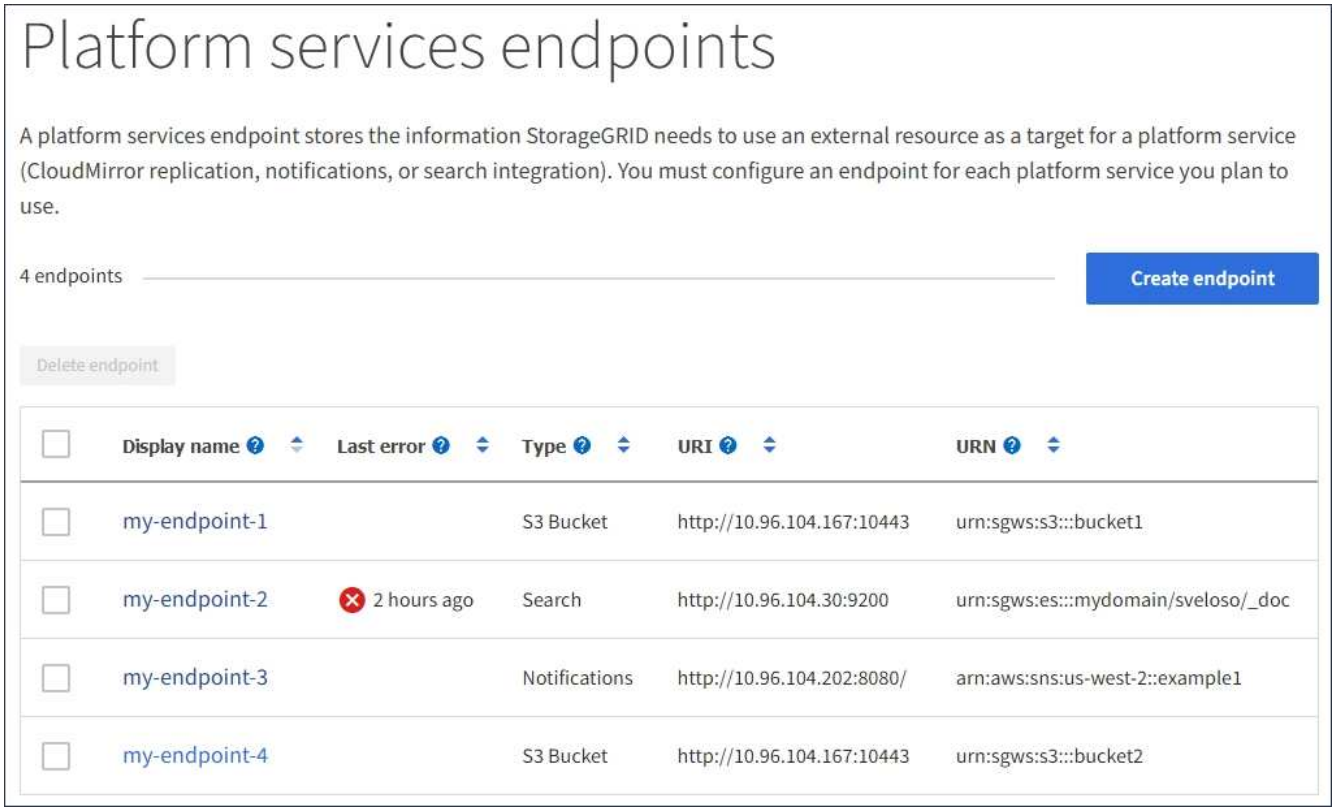
Über diese Aufgabe

StorageGRID überprüft nicht, ob die Anmeldeinformationen die richtigen Berechtigungen haben.

Schritte

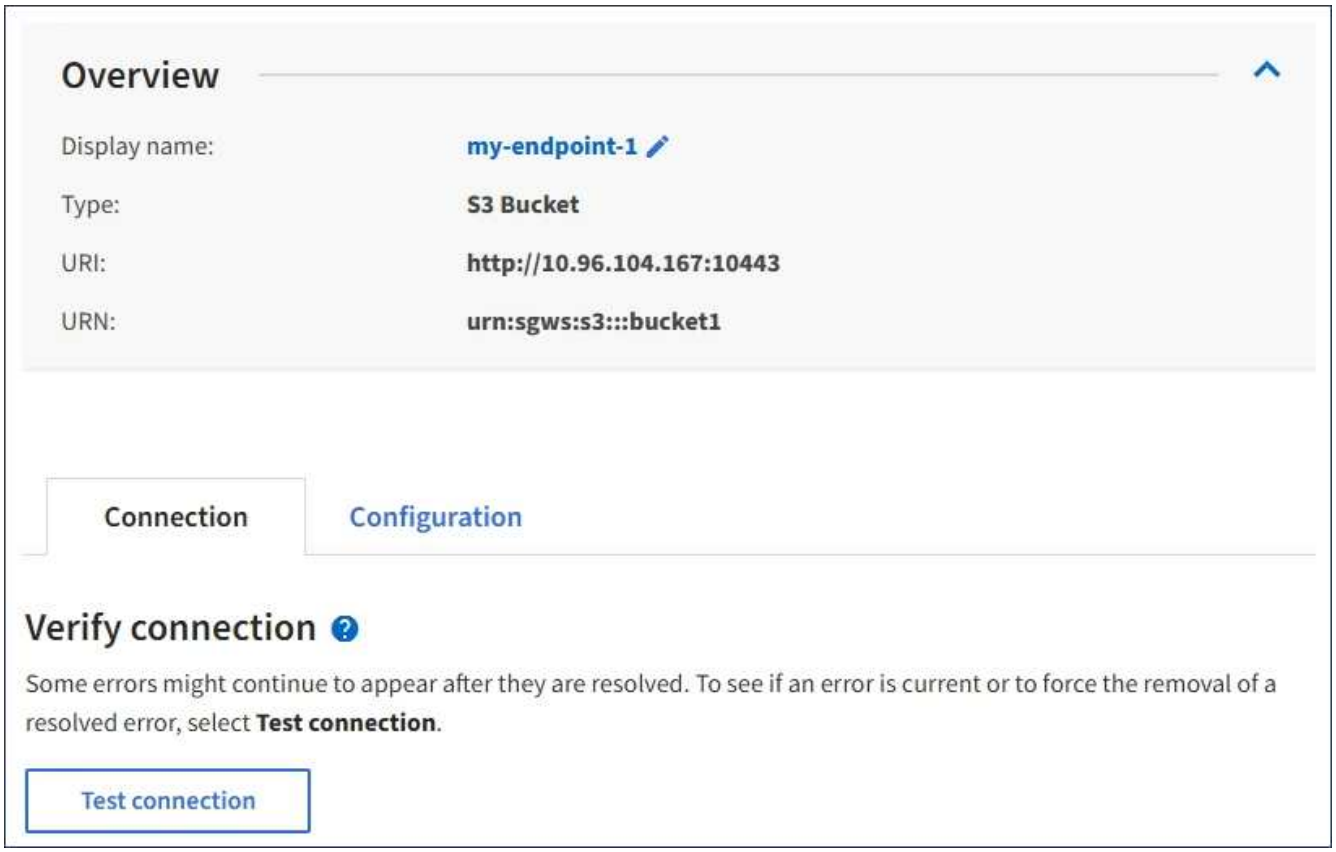
1. Wählen Sie **STORAGE (S3)** > **Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.



2. Wählen Sie den Endpunkt aus, dessen Verbindung Sie testen möchten.

   Die Seite mit den Details des Endpunkts wird angezeigt.



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**.

Bearbeiten eines Endpunkts für Plattformservices

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 den URN für einen Endpunkt für Plattformdienste nicht ändern.

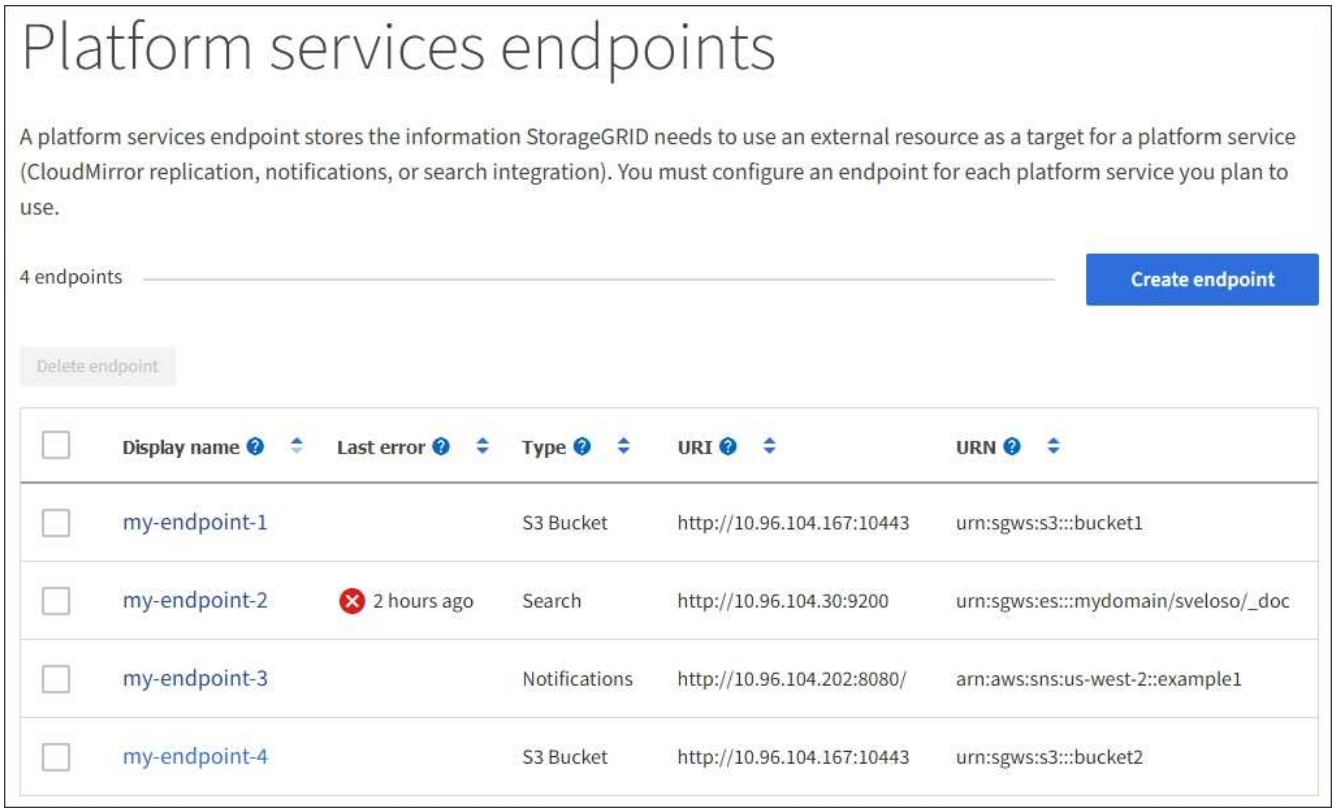
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Endpunkte verwalten verfügt.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattform-Services-Endpunkte** aus.

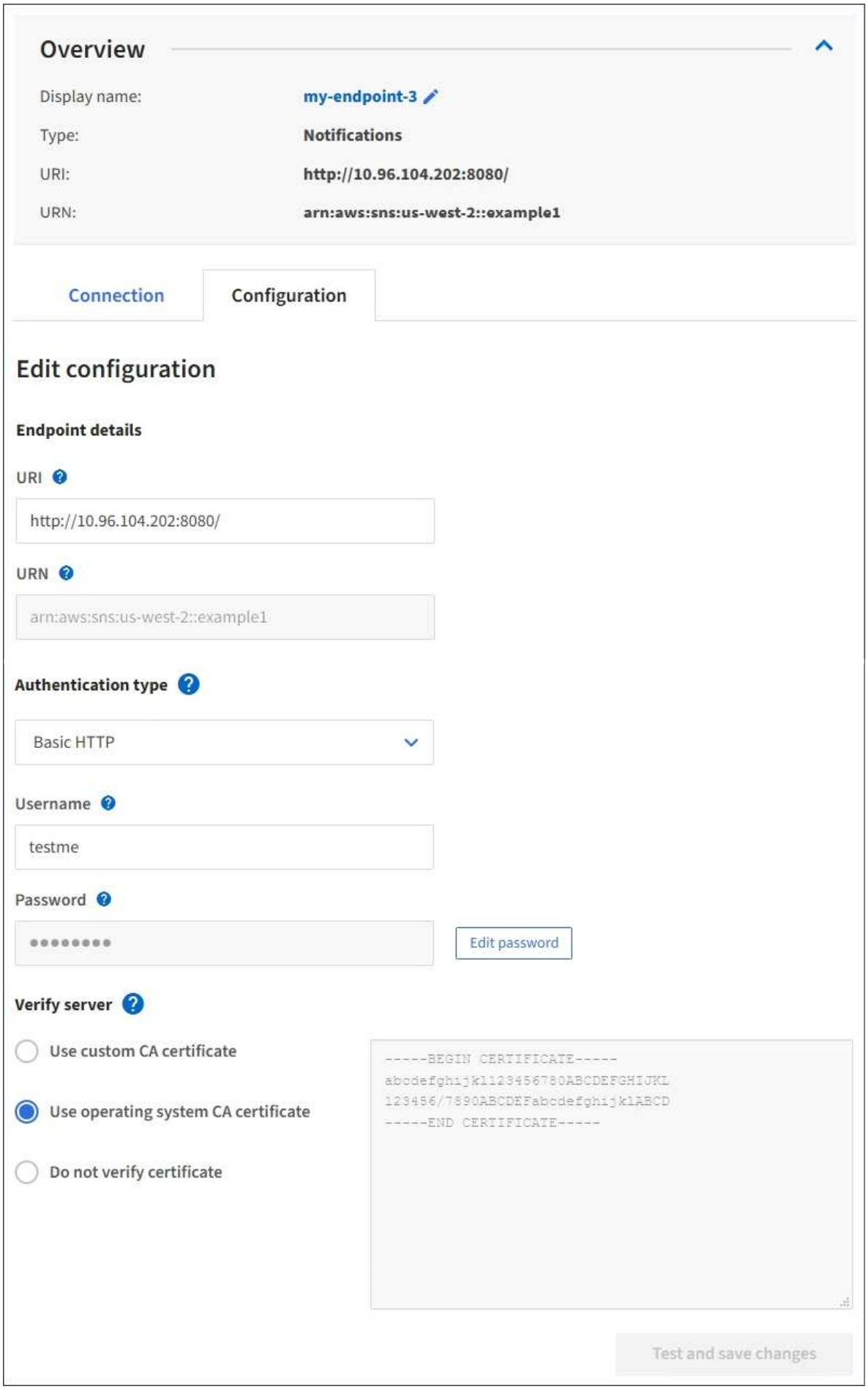
   Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.



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-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.

   Sie können den URN eines Endpunktes 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.
      - 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 abbrechen müssen, wählen Sie **Passwort zurücksetzen Bearbeiten**.
      - 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 abbrechen müssen, wählen Sie **S3-Taste Edit** rückgängig machen.
   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**.

Verwandte Informationen

"Erstellen eines Endpunkts für Plattformservices"

Löschen eines Endpunkts für Plattformservices

Sie können einen Endpunkt löschen, wenn Sie den zugeordneten Plattformdienst nicht mehr verwenden möchten.

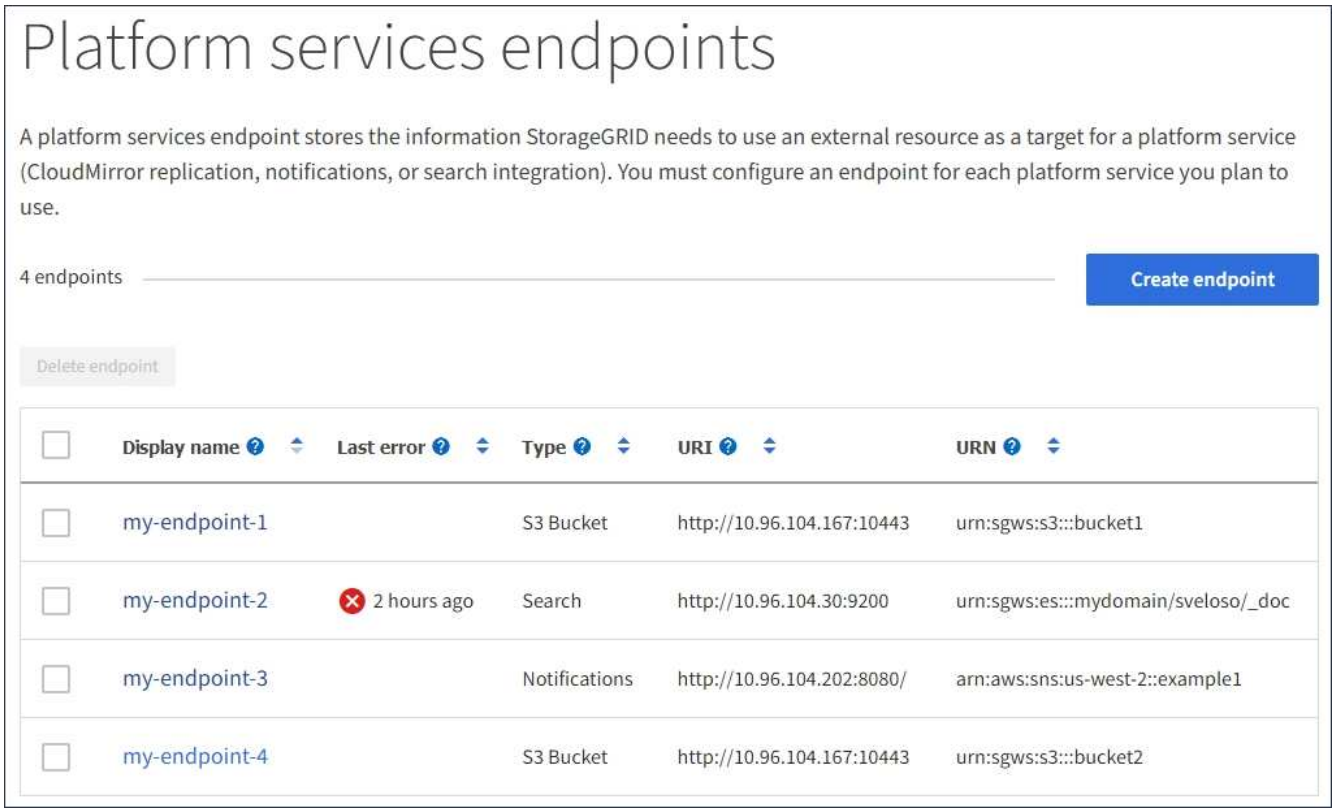
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die die Berechtigung **Endpunkte verwalten** besitzt.

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.

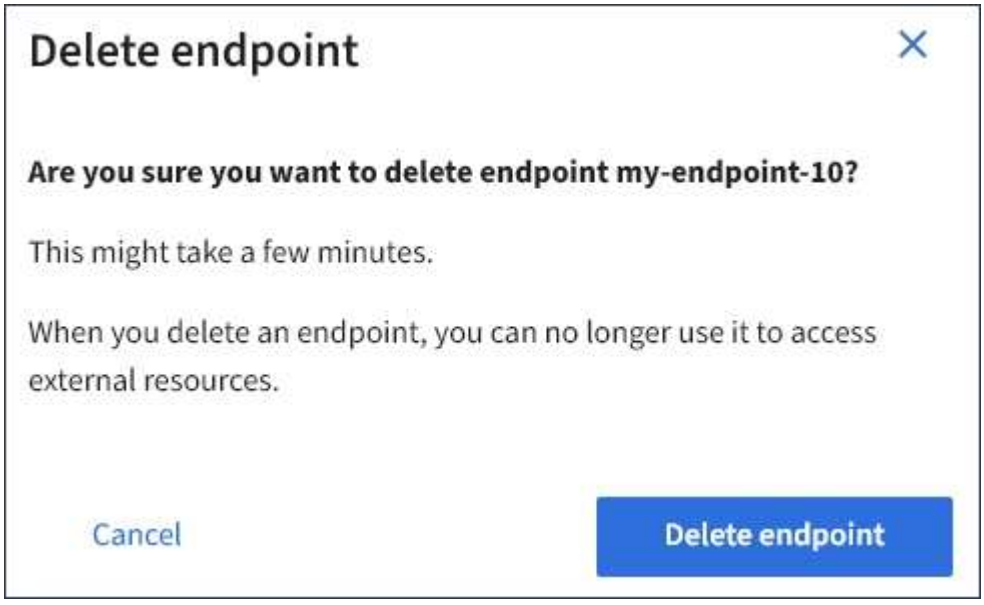


2. Aktivieren Sie das Kontrollkästchen für jeden zu löschenden Endpunkt.

> 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.



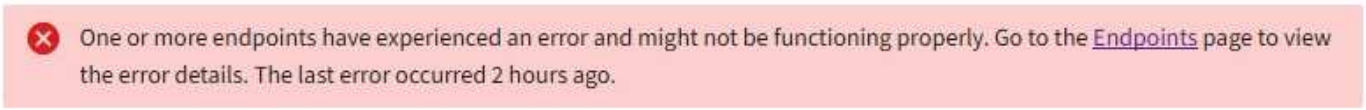
4. Wählen Sie **Endpunkt löschen**.

Fehlerbehebung bei Endpoint-Fehlern bei Plattform-Services

Wenn ein Fehler auftritt, wenn StorageGRID versucht, mit einem Endpunkt für Plattformdienste zu kommunizieren, wird auf dem Dashboard eine Meldung 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, ob ein Fehler aufgetreten ist

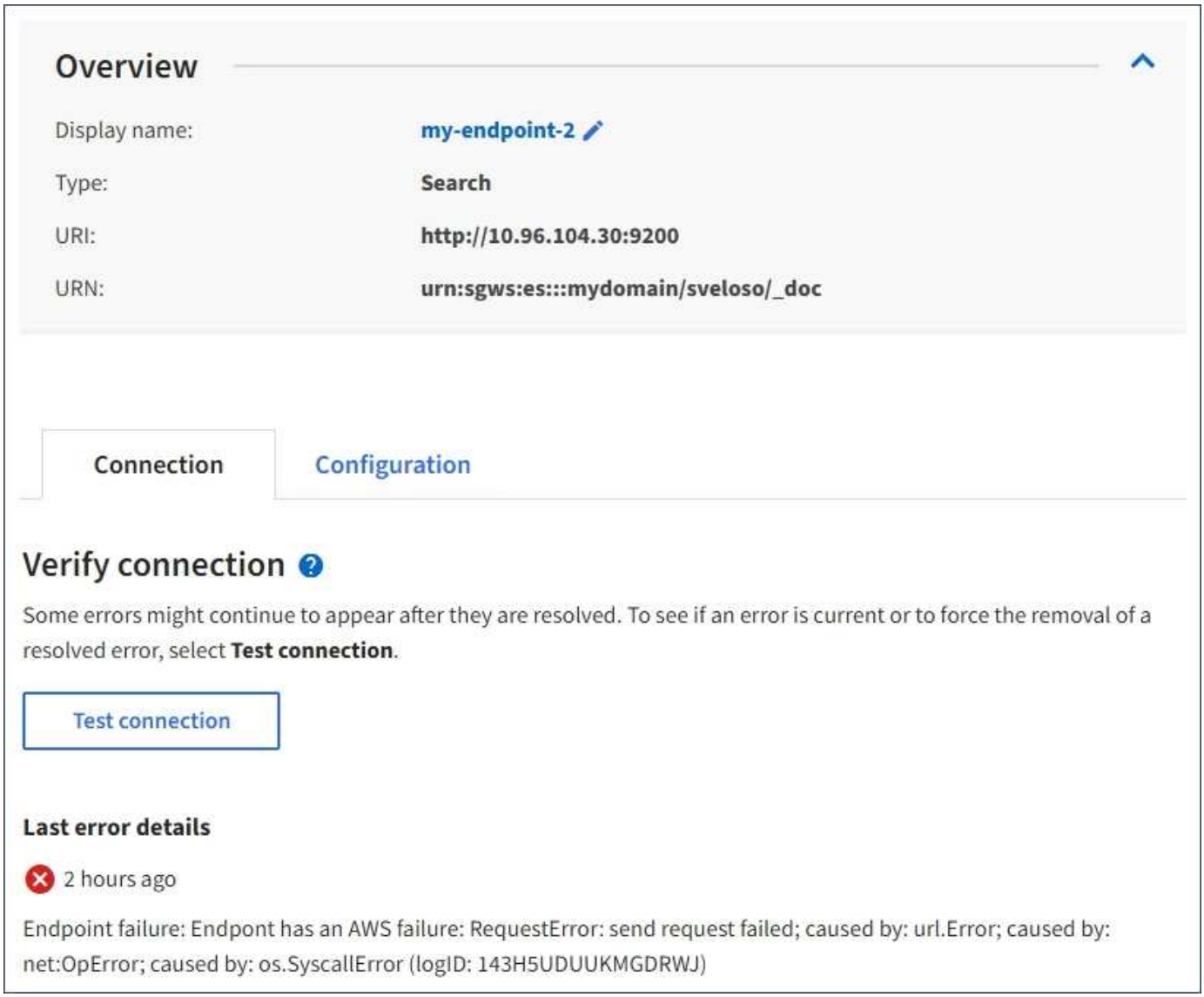
Wenn in den letzten 7 Tagen Endpoint-Fehler bei Plattformservices aufgetreten sind, zeigt das Tenant Manager Dashboard eine Warnmeldung an. Auf der Seite Plattform-Services-Endpunkte finden Sie weitere Details zum Fehler.



Der gleiche Fehler, der auf dem Dashboard angezeigt wird, wird ebenfalls oben auf der Seite „Plattform-Services-Endpunkte“ 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.



Überprüfen, ob ein Fehler noch 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.

Beseitigung von Endpunktfehlern

Sie können die Meldung **Letzter Fehler** auf der Seite Details zum Endpunkt verwenden, um zu ermitteln, was

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: Durch die Auswahl von **Änderungen testen und speichern** wird StorageGRID den aktualisierten Endpunkt validieren und bestätigen, 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 Endpunktkonfiguration 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.

Zusätzliche Plattform-Services Fehlerbehebung

Weitere Informationen zur Fehlerbehebung bei Plattform-Services finden Sie in den Anweisungen für die Administration von StorageGRID.

"StorageGRID verwalten"

Verwandte Informationen

"Erstellen eines Endpunkts für Plattformservices"

"Testen der Verbindung für einen Endpunkt der Plattformservices"

"Bearbeiten eines Endpunkts für Plattformservices"

CloudMirror-Replizierung wird konfiguriert

Der CloudMirror Replikationsservice ist einer der drei StorageGRID Plattform-Services. Mithilfe der CloudMirror Replizierung können Sie Objekte automatisch in einen externen S3-Bucket replizieren.

Was Sie benötigen

- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen bereits einen Bucket erstellt haben, um als Replikationsquelle zu fungieren.

- Der Endpunkt, den Sie als Ziel für die CloudMirror-Replikation verwenden möchten, muss bereits vorhanden sein, und Sie müssen über seinen URN verfügen.
- Sie müssen zu einer Benutzergruppe gehören, die über die Berechtigung Alle Buckets verwalten oder Stammzugriff verfügt, sodass Sie die Einstellungen für alle S3-Buckets in Ihrem Mandantenkonto verwalten können. 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. 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 in der Amazon-Dokumentation zur regionsübergreifenden Replizierung (CRR). Informationen dazu, wie StorageGRID die S3-Bucket-Replizierungskonfigurations-API implementiert, finden Sie in den Anweisungen zur Implementierung von S3-Client-Applikationen.

Wenn Sie die CloudMirror-Replizierung auf einem Bucket aktivieren, der Objekte enthält, werden neue, dem Bucket hinzugefügte Objekte repliziert, die vorhandenen Objekte jedoch nicht im Bucket. 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 Zielsystemanbieter.

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:

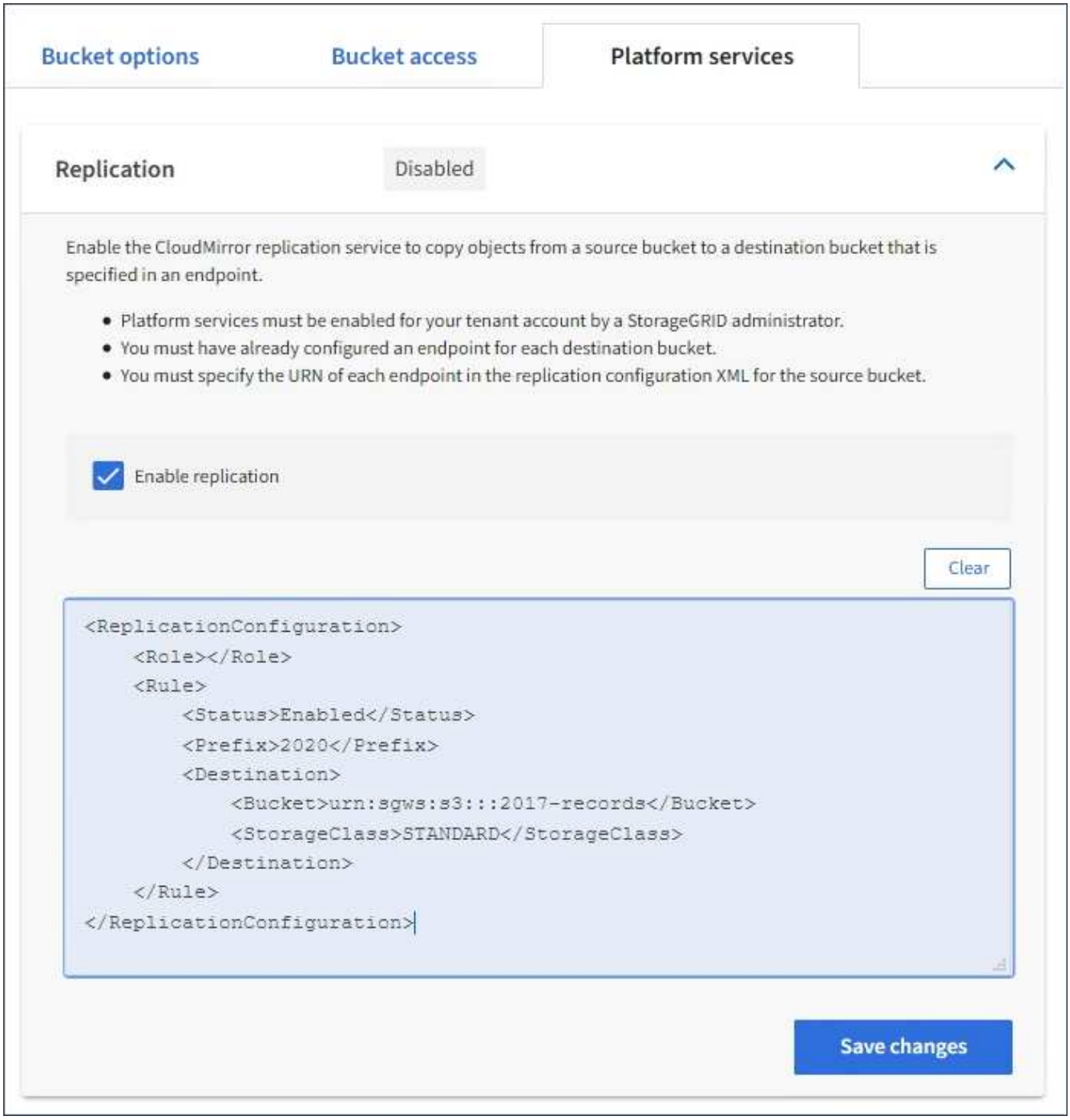
   - Beachten Sie, dass StorageGRID nur V1 der Replizierungskonfiguration unterstützt. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstützt `Filter` Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.
   - 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 Speicherklasse angeben, wird das 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 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** > **Replikation**.
5. Aktivieren Sie das Kontrollkästchen * Replikation aktivieren*.
6. Fügen Sie die XML-Replikationskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.



Plattformservices 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

"Allgemeines zum CloudMirror Replikationsservice"

"S3 verwenden"

"Erstellen eines Endpunkts für Plattformservices"

Ereignisbenachrichtigungen werden konfiguriert

Der Benachrichtigungsservice ist einer der drei StorageGRID-Plattformdienste. Sie können Benachrichtigungen aktivieren, damit ein Bucket Informationen zu bestimmten Ereignissen an einen Zieldienst sendet, der den AWS Simple Notification Service™ (SNS) unterstützt.

Was Sie benötigen

- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen bereits einen Bucket erstellt haben, um als Quelle für Benachrichtigungen zu fungieren.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, muss bereits vorhanden sein, und Sie müssen über seinen URN verfügen.
- Sie müssen zu einer Benutzergruppe gehören, die über die Berechtigung Alle Buckets verwalten oder Stammzugriff verfügt, sodass Sie die Einstellungen für alle S3-Buckets in Ihrem Mandantenkonto verwalten können. 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 dazu, wie StorageGRID die S3-Bucket-Benachrichtigungs-API implementiert, finden Sie in den Anweisungen zur Implementierung 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

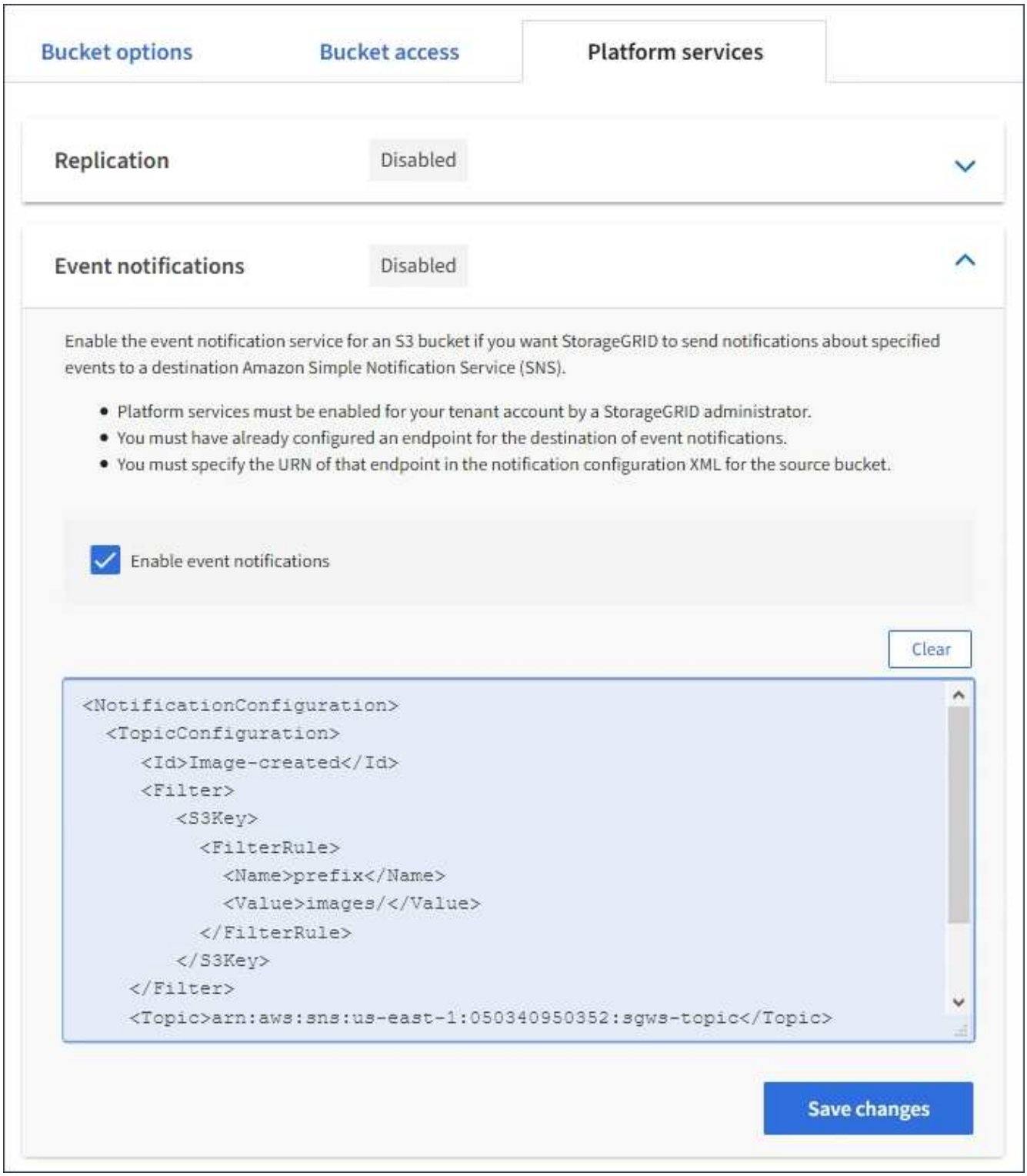
1. Benachrichtigungen für Ihren Quell-Bucket aktivieren:
    - Verwenden Sie einen Texteditor, um die XML-Benachrichtigungskonfiguration zu erstellen, die für die Aktivierung von Ereignisbenachrichtigungen erforderlich ist, wie in der S3-Benachrichtigungs-API angegeben.
    - Verwenden Sie bei der XML-Konfiguration 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**.



Plattformservices 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":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

Wenn die Benachrichtigung im Zielthema empfangen wird, haben Sie Ihren Quell-Bucket für StorageGRID-Benachrichtigungen erfolgreich konfiguriert.

Verwandte Informationen

"Allgemeines zu Benachrichtigungen für Buckets"

"S3 verwenden"

"Erstellen eines Endpunkts für Plattformservices"

Verwenden des Suchintegrationsdienstes

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.

Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung zu den folgenden benutzerdefinierten StorageGRID S3-REST-API-Vorgängen:

- Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen LÖSCHEN
- Konfigurationsanforderung FÜR Bucket-Metadaten-Benachrichtigungen ABRUFEN
- PUT Anforderung der Bucket-Metadaten-Benachrichtigung

Verwandte Informationen

"Konfigurations-XML für die Integration der Suche"

"Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"

"Vom Suchintegrations-Service generierter JSON"

"Konfigurieren des Suchintegrationsservice"

"S3 verwenden"

Konfigurations-XML für die Integration der Suche

Der Such-Integrationsservice wird anhand einer Reihe von Regeln konfiguriert, die in enthalten sind `<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 senden `/images` An ein Ziel und die Metadaten für Objekte mit dem Präfix `/videos` Nach anderen. Konfigurationen mit sich überschneidenden Präfixen sind ungültig und werden beim Einreichen abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix enthält `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 Regelelement.	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	Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt. In das Element Regel aufgenommen.	Ja.
Präfix	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.
Urne	URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein: • `es` Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular `domain-name/myindex/mytype`. Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl. Urne ist im Element Ziel enthalten.	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-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

"S3 verwenden"

"Vom Suchintegrations-Service generierter JSON"

"Konfigurieren des Suchintegrationsservice"

Der Suchintegrations-Service sendet Objektmetadaten an einen Zielindex bei jedem Erstellen, Löschen oder Aktualisieren der zugehörigen Metadaten oder Tags.

Was Sie benötigen

- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen bereits einen S3-Bucket erstellt haben, dessen Inhalt Sie indexieren möchten.
- Der Endpunkt, den Sie als Ziel für den Suchintegrationsdienst verwenden möchten, muss bereits vorhanden sein, und Sie müssen seinen URN haben.
- Sie müssen zu einer Benutzergruppe gehören, die über die Berechtigung Alle Buckets verwalten oder Stammzugriff verfügt, sodass Sie die Einstellungen für alle S3-Buckets in Ihrem Mandantenkonto verwalten können. 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-Integrationsservice 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 Such-Integrationsservice 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

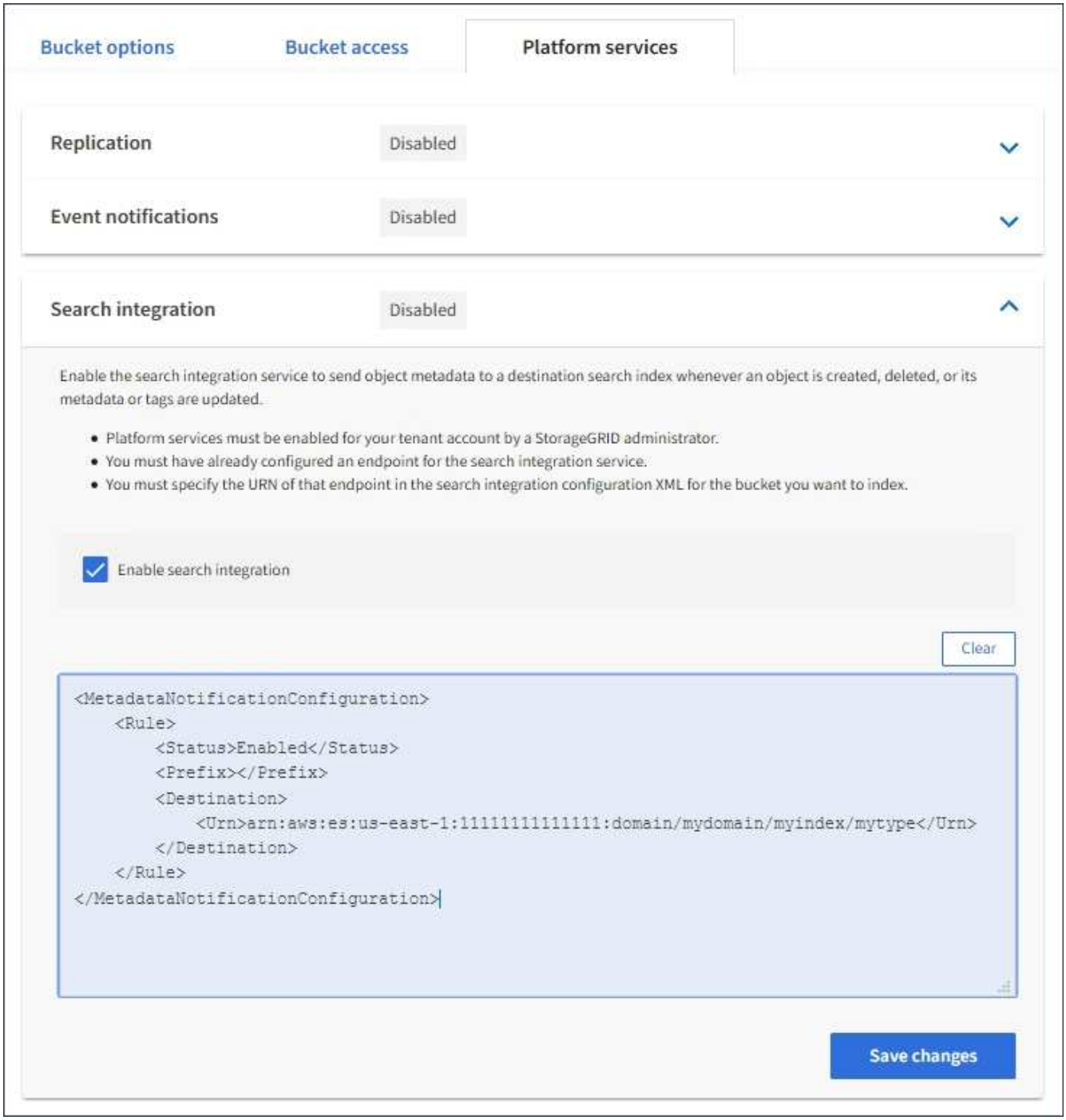
1. Verwenden Sie einen Texteditor, um die XML-XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
   - Informationen zur Integration der Suchfunktion finden Sie in den XML-Konfigurationsdaten.
   - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt zur Integration der Suche als Ziel.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111: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 **Suchintegration aktivieren**.
6. Fügen Sie die Konfiguration der Metadatenbenachrichtigung in das Textfeld ein, und wählen Sie **Änderungen speichern**.



Plattformservices 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:

a. 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** aus, und deaktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
- 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

"Beschreibung des Suchintegrationsservice"

"Konfigurations-XML für die Integration der Suche"

"S3 verwenden"

"Erstellen eines Endpunkts für Plattformservices"

Vom Suchintegrations-Service generierter JSON

Wenn Sie den Such-Integrationsservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielendpunkt 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 bearbeiten.

S3 verwenden

Lesen Sie, wie Client-Applikationen die S3-API für die Schnittstelle mit dem StorageGRID-System nutzen.

- "Unterstützung für die S3-REST-API"
- "Mandantenkonten und -Verbindungen werden konfiguriert"
- "So implementiert StorageGRID die S3-REST-API"
- "Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"
- "StorageGRID S3 REST-API-Operationen"
- "Bucket- und Gruppenzugriffsrichtlinien"
- "Sicherheit wird für DIE REST API konfiguriert"
- "Monitoring und Auditing von Vorgängen"
- "Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen"

Unterstützung für die S3-REST-API

StorageGRID unterstützt die S3-API (Simple Storage Service), die als Satz Rest-Web-Services (Representational State Transfer) implementiert wird. Dank der Unterstützung der S3-REST-API können serviceorientierte Applikationen, die für S3-Webservices entwickelt wurden, mit On-Premises-Objekt-Storage über das StorageGRID System verbunden werden. Hierfür sind nur minimale Änderungen an der aktuellen Nutzung von S3-REST-API-Aufrufen einer Client-Applikation erforderlich.

- "Änderungen an der Unterstützung für die S3-REST-API"
- "Unterstützte Versionen"
- "Unterstützung von StorageGRID Plattform-Services"

Änderungen an der Unterstützung für die S3-REST-API

Bei Änderungen an der Unterstützung des StorageGRID-Systems für die S3-REST-API sollten Sie auf sich aufmerksam machen.

Freigabe	Kommentare
11.5	• 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 `Content-MD5` Die Anforderungsüberschrift wird jetzt korrekt unterstützt.
11.4	• Unterstützung für DELETE Bucket-Tagging, GET Bucket-Tagging und PUT Bucket-Tagging. Kostenzuordnungs-Tags 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 `s3:ObjectRestore:Post` 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. • Zusätzliche Unterstützung für TLS 1.3 und aktualisierte Liste der unterstützten TLS-Chiffre-Suites. • Der CLB-Service ist veraltet.
11.3	• 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 `x-amz-expiration` 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. • Aktualisierte Liste der unterstützten TLS-Cipher-Suites. TLS 1.1-Chiffren werden nicht mehr unterstützt.

Freigabe	Kommentare
11.2	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. **Hinweis:** die Verwendung von ARN/URN in anderen Konfigurationen JSON/XML, einschließlich derjenigen, die in benutzerdefinierten StorageGRID-Funktionen verwendet werden, hat sich nicht geändert.
11.1	Zusätzliche Unterstützung für Cross-Origin Resource Sharing (CORS), HTTP für S3-Client-Verbindungen 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 PutOverwriteObject.
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 *Simple Storage Service API Reference* lautet 2006-03-01.

Unterstützte Versionen

StorageGRID unterstützt die folgenden spezifischen Versionen von S3 und HTTP.

Element	Version
S3-Spezifikation	*Simple Storage Service API Reference* 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"

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-Replizierung
Benachrichtigungen	Sendet Benachrichtigungen zu Ereignissen in einem StorageGRID-Quell-Bucket an einen konfigurierten SNS-Endpunkt (Simple Notification Service).	PUT Bucket-Benachrichtigung
Integration von Suchen	Sendet Objektmetadaten für Objekte, die in einem StorageGRID Bucket gespeichert sind, an einen konfigurierten Elasticsearch-Index.	PUT Bucket-Metadaten-Benachrichtigung **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. 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.

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 bei einem S3-Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror-Replizierung aktiviert sind, empfiehlt NetApp, dass auf dem Zielendpunkt 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.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"StorageGRID verwalten"

"Operationen auf Buckets"

"PUT Anforderung der Bucket-Metadaten-Benachrichtigung"

Mandantenkonten und -Verbindungen werden konfiguriert

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 S3-Mandantenkonten

Bevor S3-API-Clients Objekte auf StorageGRID speichern und abrufen können, ist ein S3-Mandantenkonto erforderlich. Jedes Mandantenkonto hat seine eigene Konto-ID, Gruppen und Benutzer sowie Container und Objekte.

S3-Mandantenkonten werden von einem StorageGRID Grid-Administrator erstellt, der den Grid Manager oder die Grid Management API verwendet. Beim Erstellen eines S3-Mandantenkontos gibt der Grid-Administrator die folgenden Informationen an:

- Anzeigename für den Mandanten (die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden).
- Gibt an, ob das Mandantenkonto Plattform-Services nutzen darf. Wenn die Nutzung von Plattformdiensten zulässig ist, muss das Grid so konfiguriert werden, dass es seine Verwendung unterstützt.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte verfügbar sind. Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.

- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.
- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Nachdem ein S3-Mandantenkonto erstellt wurde, können Mandantenbenutzer auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Richten Sie einen Identitätsverbund ein (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet), und erstellen Sie lokale Gruppen und Benutzer
- Managen von S3-Zugriffsschlüsseln
- Erstellung und Management von S3-Buckets, einschließlich Buckets, für die S3-Objektsperre aktiviert ist
- Verwenden von Plattform-Services (falls aktiviert)
- Monitoring der Storage-Auslastung

> Benutzer von S3-Mandanten können mit Mandanten-Manager S3-Buckets erstellen und managen. Dafür sind jedoch S3-Zugriffsschlüssel sowie die S3-REST-API erforderlich, um Objekte aufzunehmen und zu managen.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

Wie Client-Verbindungen konfiguriert werden können

Ein Grid-Administrator trifft Konfigurationsmöglichkeiten, die Einfluss darauf haben, wie S3-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 mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten

> Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- 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).

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.

Weitere Informationen zu den einzelnen Optionen finden Sie in den Anweisungen zur Administration von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

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. Wenden Sie sich an Ihren StorageGRID-Administrator, um weitere Informationen zu erhalten, oder lesen Sie die Anweisungen zur Administration von StorageGRID, um eine Beschreibung der Informationen im Grid-Manager zu erhalten.

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
HA-Gruppe	CLB **Hinweis:** der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
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
Gateway-Node	CLB **Hinweis:** der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node **Hinweis:** standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: • HTTPS: 18082 • HTTP: 18084

Beispiel

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen S3-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 192.0.2.5 lautet und die Portnummer eines S3 Load Balancer Endpunkts 10443 ist, kann ein S3-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.5:10443`

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.

Verwandte Informationen

"StorageGRID verwalten"

Entscheidung über 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 Client-Verbindungen zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Knoten zu verwenden, müssen Sie dessen Verwendung aktivieren.

Wenn Client-Anwendungen eine Verbindung zu Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, müssen sie für alle Verbindungen verschlüsseltes HTTPS verwenden. Optional können Sie weniger sichere HTTP-Verbindungen aktivieren, indem Sie im Grid Manager die Option **HTTP-Verbindung** aktivieren auswählen. Eine Client-Anwendung kann beispielsweise HTTP verwenden, wenn die Verbindung zu einem Speicherknoten in einer nicht produktiven Umgebung getestet wird.

Achten Sie bei der Aktivierung von HTTP für ein Produktionsraster darauf, dass die Anforderungen unverschlüsselt gesendet werden.

Der CLB-Service ist veraltet.

Wenn die Option **HTTP-Verbindung aktivieren** ausgewählt ist, müssen Clients für HTTP unterschiedliche Ports verwenden als für HTTPS. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

"Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen"

Endpoint-Domain-Namen für S3-Anforderungen

Bevor Sie S3-Domänennamen für Client-Anforderungen verwenden können, muss ein StorageGRID-Administrator das System so konfigurieren, dass Verbindungen angenommen werden, die S3-Domänennamen im S3-Pfadstil und virtuelle S3-Hosted-Style-Anforderungen 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 lautet `s3.company.com`, Der Grid-Administrator muss sicherstellen, dass das Zertifikat, das für HTTPS-Verbindungen verwendet wird, das umfasst `s3.company.com` endpunkt und Wildcard-alternativer Name (SAN) des Endpunkts: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server, um DNS-Datensätze mit den Endpunktdomänennamen, einschließlich aller erforderlichen Platzhalterdatensätze, einzuschließen.

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, und jeder Endpunkt kann so konfiguriert werden, dass verschiedene Endpunkt-Domain-Namen erkannt werden.

Wenn der Client Storage-Knoten oder den CLB-Dienst auf Gateway-Knoten verbindet, ist das Zertifikat, das der Grid-Administrator konfiguriert, das einzelne benutzerdefinierte Serverzertifikat, das für das Grid verwendet wird.

Der CLB-Service ist veraltet.

Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Nach Abschluss dieser Schritte können Sie virtuelle Anfragen im Hosted-Style verwenden (z. B. `bucket.s3.company.com`).

Verwandte Informationen

"StorageGRID verwalten"

"Sicherheit wird für DIE REST API konfiguriert"

Testen Ihrer 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.

Was Sie benötigen

- Sie müssen die AWS CLI von heruntergeladen und installiert haben "aws.amazon.com/cli".
- Sie müssen ein S3-Mandantenkonto im StorageGRID System erstellt haben.

Schritte

1. Konfigurieren Sie die Einstellungen für Amazon Web Services so, dass Sie das im StorageGRID System erstellte Konto verwenden:
   a. Konfigurationsmodus aufrufen: `aws configure`
   b. Geben Sie die AWS Zugriffsschlüssel-ID für das erstellte Konto ein.
   c. Geben Sie den AWS-Schlüssel für den geheimen Zugriff für das 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:

   ```
   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
```

So implementiert StorageGRID die S3-REST-API

Eine Client-Applikation kann S3-REST-API-Aufrufe zur Verbindung mit StorageGRID nutzen, um Buckets zu erstellen, zu löschen und zu ändern sowie Objekte zu speichern und abzurufen.

- "In Konflikt stehende Clientanforderungen"
- "Konsistenzkontrollen"
- "Managen von Objekten durch StorageGRID ILM-Regeln"
- "Objektversionierung"
- "Empfehlungen für die Implementierung der S3-REST-API"

In Konflikt stehende Clientanforderungen

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.

Konsistenzkontrollen

Konsistenzkontrollen ermöglichen je nach Anforderung eine Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage-Nodes und -Standorte.

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:

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 Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „`available`“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

Verwenden der Consistency Controls „`read-after-New-write`“ und „`available`“

Wenn ein KOPF- oder GET-Vorgang die Konsistenzkontrolle „`read-after-New-write`“ verwendet oder EIN GET-Vorgang die Konsistenzkontrolle „`available`“ verwendet, führt StorageGRID die Suche in mehreren Schritten durch:

- Es sieht zunächst das Objekt mit einer niedrigen Konsistenz.
- Falls dieses Lookup fehlschlägt, wird das Lookup auf der nächsten Konsistenzebene wiederholt, bis es die höchste Konsistenzstufe „`all`,“ erreicht, sodass alle Kopien der Objektmetadaten verfügbar sein müssen.

Wenn ein KOPF- oder GET-Vorgang die Konsistenzkontrolle „`read-after-New-write`“ verwendet, aber das Objekt nicht vorhanden ist, erreicht die Objekt-Lookup immer die Konsistenzstufe „`all`“. Da auf dieser Konsistenzstufe alle Kopien der Objektmetadaten verfügbar sein müssen, können Sie eine hohe Anzahl von 500 Fehlern des internen Servers erhalten, wenn ein oder mehrere Storage-Nodes nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien wie Amazon S3 benötigen, können Sie diese Fehler bei DEN HEAD-Operationen vermeiden, indem Sie die Consistency Control auf „`available`“ setzen. Wenn ein HAUPTBETRIEB die Konsistenzkontrolle „`Available`“ verwendet, bietet StorageGRID eventuell nur Konsistenz. Ein fehlgeschlagener Vorgang wird erst wieder versucht, wenn es die Konsistenzstufe „`all`“ erreicht. Daher müssen nicht alle Kopien der Objektmetadaten verfügbar sein.

Angeben der Consistency Control für einen API-Vorgang

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: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

> Sie müssen für DEN PUT-Objekt- und DEN GET-Objektbetrieb dasselbe Konsistenzsteuerelement verwenden.

Angeben der Konsistenzkontrolle für einen 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 sollte für Buckets die standardmäßige Konsistenzkontrolle verwendet werden, „`read-after-New-write.`“ Wenn Anforderungen nicht korrekt funktionieren, ändern Sie das Verhalten des Anwendungs-Clients, 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.

Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung 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:

- **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.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Kunden zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

> 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 Objektdaten an den Remote-Standort repliziert wurden, doch 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-Konsistenzanforderung"

"PUT Bucket-Konsistenzanforderung"

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 „Last Access Time“ verwendet, müssen Sie für die in dieser Regel angegebenen S3-Buckets Updates für die letzte Zugriffszeit aktivieren. Sie können Updates der letzten Zugriffszeit mithilfe der Anforderung PUT Bucket Last Access Time, des Checkbox **S3** > **Buckets** > **Letzter Zugriffszeitpunkt konfigurieren** im Tenant Manager oder mithilfe der Tenant Management API aktivieren. Beachten Sie bei der Aktivierung von Updates der letzten Zugriffszeit, dass die Performance von StorageGRID möglicherweise reduziert wird, insbesondere bei Systemen mit kleinen Objekten.

- Speicherortbeschränkung
- Objektgröße
- Benutzermetadaten
- Objekt-Tag

Weitere Informationen zum ILM finden Sie in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Objektmanagement mit ILM"

"PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs"

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 mit Versionierung aktivierten Buckets können Sie mithilfe der Versionierung ILM-Regeln erstellen, die nicht aktuelle Zeit als Referenzzeit verwenden. Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht aktuell. Mithilfe eines nicht aktuellen Zeitfilters 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.

Anweisungen zum Managen von Objekten mit Information Lifecycle Management finden Sie in den Anweisungen, wie z. B. eine ILM-Richtlinie für versionierte Objekte mit S3 enthält.

Verwandte Informationen

"Objektmanagement mit ILM"

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 in einem Pfad existiert, in dem Sie nicht erwarten, dass das Objekt tatsächlich vorhanden ist, 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

Bei Buckets, die in StorageGRID 11.4 oder höher erstellt wurden, ist es nicht mehr erforderlich, Objektschlüsselnamen auf die Performance-Best-Practices zu beschränken. Sie können jetzt beispielsweise Zufallswerte für die ersten vier Zeichen von Objektschlüsselnamen verwenden.

Befolgen Sie bei Buckets, die in Versionen vor StorageGRID 11.4 erstellt wurden, weiterhin die folgenden Empfehlungen für Objektschlüsselnamen:

- Als die ersten vier Zeichen von Objektschlüsseln sollten Sie keine Zufallswerte verwenden. Dies steht im Gegensatz zu der früheren AWS Empfehlung für wichtige Präfixe. 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 Schlüsselpräfixen zu verwenden, sollten Sie die Objektschlüssel mit einem Verzeichnisnamen vorschreiben. Verwenden Sie dieses Format:

```
mybucket/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mybucket/f8e3-image3132.jpg
```

Empfehlungen für „`Range reads`“

Wenn die Option **komprimiere gespeicherte Objekte** ausgewählt ist (**Konfiguration** > **Grid-Optionen**), sollten S3-Client-Anwendungen verhindern, DASS GET-Objekt-Operationen ausgeführt werden, die einen Bereich von Bytes angeben. 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.

Verwandte Informationen

"Konsistenzkontrollen"

"PUT Bucket-Konsistenzanforderung"

"StorageGRID verwalten"

Unterstützte Vorgänge und Einschränkungen durch S3-REST-API

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.

- "Authentifizierung von Anforderungen"
- "Betrieb auf dem Service"
- "Operationen auf Buckets"
- "Benutzerdefinierte Vorgänge für Buckets"
- "Operationen für Objekte"
- "Vorgänge für mehrteilige Uploads"
- "Fehlerantworten"

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 Zeitzonenversatz 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 gemeinsame Anfrageheader, die von der *Simple Storage Service API Reference* definiert wurden, mit einer Ausnahme.

Kopfzeile der Anfrage	Implementierung
Autorisierung	Vollständige Unterstützung für AWS Signature Version 2 Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen: • Der SHA256-Wert wird für den Körper der Anforderung nicht berechnet. Der vom Benutzer eingereichte Wert wird ohne Validierung angenommen, als ob der Wert `UNSIGNED-PAYLOAD` War für die vorgesehen `x-amz-content-sha256` Kopfzeile.
X-amz-Sicherheits-Token	Nicht implementiert. Kehrt Zurück `XNotImplemented`.

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

Verwandte Informationen

"Amazon Web Services (AWS) Dokumentation: Amazon Simple Storage Service API Reference"

Authentifizierung von Anforderungen

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 der HTTP-Autorisierungsüberschrift

Das HTTP `Authorization` Kopfzeile wird von allen S3-API-Operationen verwendet außer anonymen Anfragen, sofern dies durch die Bucket-Richtlinie zulässig ist. Der `Authorization` Der Header enthält alle erforderlichen Signierungsdaten, um eine Anforderung zu authentifizieren.

Abfrageparameter werden verwendet

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 vorsignierten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zugreifen zu können, wodurch Sie einen eingeschränkten Zugriff auf eine Ressource durch Dritte ermöglichen können.

Betrieb auf dem Service

Das StorageGRID System unterstützt die folgenden Vorgänge beim Service.

Betrieb	Implementierung
GET Service	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.
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 `OPTIONS /` 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

"Storage-Nutzungsanforderung ABRUFEN"

Operationen auf Buckets

Das StorageGRID System unterstützt für jedes S3-Mandantenkonto maximal 1,000 Buckets.

Einschränkungen für Bucket-Namen folgen den regionalen Beschränkungen für AWS US Standard. Sie sollten sie jedoch noch weiter auf DNS-Namenskonventionen beschränken, um Anfragen im Stil von virtuellen S3-Hosted-Style zu unterstützen.

"Amazon Web Services (AWS) Dokumentation: Bucket-Einschränkungen und -Einschränkungen"

"Endpoint-Domain-Namen für S3-Anforderung"

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	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.
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 dem Bucket hinzugefügte Objekte werden jedoch nicht verschlüsselt.
Bucket-Lebenszyklus LÖSCHEN	Bei diesem Vorgang wird die Lebenszyklukonfiguration aus dem Bucket gelöscht.
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 `tagging` unterressource, um alle Tags aus einem Bucket zu entfernen

Betrieb	Implementierung
Get Bucket (Listenobjekte), Version 1 und Version 2	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 `REDUCED_REDUNDANCY` Option für Storage-Klasse: • `STANDARD`, Die angibt, dass das Objekt in einem Speicherpool gespeichert wird, der aus Storage-Nodes besteht. • `GLACIER`, Dies bedeutet, dass das Objekt in den vom Cloud-Speicherpool angegebenen externen Bucket verschoben wurde. Wenn der Bucket eine große Anzahl von gelöschten Schlüsseln enthält, die dasselbe Präfix haben, kann die Antwort einige enthalten `CommonPrefixes` Die keine Schlüssel enthalten.
Bucket-acl ABRUFEN	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.
Bucket-Cors ABRUFEN	Dieser Vorgang gibt den zurück `cors` Konfiguration für den Bucket.
Get Bucket-Verschlüsselung	Dieser Vorgang gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
BUCKET-Lebenszyklus ABRUFEN	Dieser Vorgang gibt die Lifecycle-Konfiguration für den Bucket zurück.
Bucket-Speicherort ABRUFEN	Dieser Vorgang gibt die Region zurück, die mit dem festgelegt wurde `LocationConstraint` Element in DER PUT Bucket Anforderung. Wenn der Eimer-Bereich ist `us-east-1`, Eine leere Zeichenfolge wird für die Region zurückgegeben.
Bucket-Benachrichtigung ABRUFEN	Dieser Vorgang gibt die Benachrichtigungskonfiguration an den Bucket zurück.
Get Bucket-Objektversionen	Mit LESEZUGRIFF auf einen Bucket erfolgt dieser Vorgang mit dem `versions` unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.

Betrieb	Implementierung
Get Bucket-Richtlinie	Dieser Vorgang gibt die Richtlinie zurück, die dem Bucket zugeordnet ist.
GET Bucket-Replizierung	Dieser Vorgang gibt die am Bucket angeschlossene Replizierungskonfiguration zurück.
Get Bucket-Tagging	Dieser Vorgang verwendet das `tagging` unterressource, um alle Tags für einen Bucket zurückzugeben
Get Bucket-Versionierung	Diese Implementierung verwendet das `versioning` subressource zur Rückgabe des Versionierungsstatus eines Buckets. Der zurückgegebene Versionierungsstatus gibt an, ob der Bucket die Version „`Unversioniert`“ oder die Version „`Enabled`“ oder „`Suspended`“ `lautet.`
Konfiguration der Objektsperre ABRUFEN	Dieser Vorgang legt fest, ob die S3-Objektsperre für einen Bucket aktiviert ist. "Verwenden der S3-Objektsperre"
EIMER	Dieser Vorgang bestimmt, ob ein Bucket vorhanden ist und Sie über die Berechtigung zum Zugriff auf ihn verfügen.

Betrieb	Implementierung
Put Bucket	Durch diesen Vorgang wird ein neuer Bucket erstellt. Mit dem Erstellen des Buckets werden Sie zum Bucket-Eigentümer. • Bucket-Namen müssen die folgenden Regeln einhalten: ◦ 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 erstellt `us-east-1` Region; jedoch können Sie die verwenden `LocationConstraint` Anforderungselement im Anforderungskörper, um eine andere Region anzugeben. Bei Verwendung des `LocationConstraint` 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 Namen der zu verwendenden Region nicht kennen. **Hinweis**: Ein Fehler tritt auf, wenn Ihre PUT Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde. • Sie können die einschließen `x-amz-bucket-object-lock-enabled` Kopfzeile zum Erstellen eines Buckets anfordern, wobei S3-Objektsperre aktiviert ist. Sie müssen die S3-Objektsperre aktivieren, wenn Sie den Bucket erstellen. Sie können S3 Object Lock 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.

Betrieb	Implementierung
Bucket-Cors EINGEBEN	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 `images` Zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für das `images` Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden `http://www.example.com`.
Bucket-Verschlüsselung	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. 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 `x-amz-server-side-encryption-*` Kopfzeile der Anfrage).

Betrieb	Implementierung
PUT Bucket-Lebenszyklus	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: • Ablauf (Tage, Datum) • NoncurrentVersionExpiration (NoncurrentDays) • Filter (Präfix, Tag) • Status • ID StorageGRID bietet folgende Maßnahmen nicht: • AbortInsetteMultipartUpload • ExpiredObjectDeleteMarker • Übergang Informationen dazu, wie die Aktion zum Ablauf in einem Bucket-Lebenszyklus mit den Anweisungen zur ILM-Platzierung interagiert, finden Sie unter „`wie ILM während der gesamten Lebensdauer eines Objekts funktioniert`“ in den Anweisungen für das Management von Objekten mit Information Lifecycle Management. **Hinweis**: Die Konfiguration des Bucket-Lebenszyklus kann für Buckets verwendet werden, für die S3-Objektsperre aktiviert ist. Die Bucket-Lebenszykluskonfiguration wird jedoch für ältere kompatible Buckets nicht unterstützt.

Betrieb	Implementierung

PUT Bucket-Benachrichtigung	Mit diesem Vorgang werden Benachrichtigungen für den Bucket mithilfe der im Anfraentext enthaltenen XML-Benachrichtigungskonfiguration konfiguriert. Sie sollten folgende Implementierungsdetails kennen:
	
	• StorageGRID unterstützt SNS-Themen (Simple Notification Service) als Ziele. Simple Queue Service (SQS)- oder Amazon Lambda-Endpunkte werden nicht unterstützt.
	• Das Ziel für Benachrichtigungen muss als URN eines StorageGRID-Endpunkts angegeben werden. Endpunkte können mit dem Mandanten-Manager oder der Mandanten-Management-API erstellt werden.
	
	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`.
	
	• Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden **nicht** unterstützt.
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der folgenden Liste gezeigt:
	
	• **EventSource**
	
	`sgws:s3`
	
	• **AwsRegion**
	
	Nicht enthalten
	
	• * X-amz-id-2*
	
	Nicht enthalten
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

Betrieb	Implementierung
Bucket-Richtlinie	Dieser Vorgang legt die Richtlinie fest, die an den Bucket gebunden ist.

Betrieb	Implementierung
PUT Bucket-Replizierung	Dieser Vorgang konfiguriert die StorageGRID CloudMirror-Replikation für den Bucket mithilfe der im Anforderungsgremium bereitgestellten Replikationskonfigurations-XML. Für die CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten: • StorageGRID unterstützt nur V1 der Replizierungskonfiguration. 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. • 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. Der Endpunkt muss vorhanden sein, damit die Replizierungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, schlägt die Anforderung als a fehl `400 Bad Request`. In der Fehlermeldung steht: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Sie müssen kein angeben `Role` 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 `STANDARD` 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: ◦ Wenn Sie das Objekt oder Bucket vor der Replizierung löschen, wird das Objekt/Bucket nicht repliziert, und Sie werden nicht benachrichtigt. Wenn Sie das Objekt oder Bucket nach der

Betrieb	Implementierung
PUT Bucket-Tagging	Dieser Vorgang verwendet das `tagging` unterressource, um einen Satz von Tags für einen Bucket hinzuzufügen oder zu aktualisieren Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen: • 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	Diese Implementierung verwendet das `versioning` unterressource, um den Versionierungsstatus eines vorhandenen Buckets festzulegen. Sie können den Versionierungsstatus mit einem der folgenden Werte festlegen: • 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 `null`.

Verwandte Informationen

"Amazon Web Services (AWS) Dokumentation: Regionsübergreifende Replizierung"

"Konsistenzkontrollen"

"Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN"

"Bucket- und Gruppenzugriffsrichtlinien"

"Verwenden der S3-Objektsperre"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

Erstellen einer S3-Lebenszykluskonfiguration

Sie können eine S3-Lebenszyklukonfiguration 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. Alle Details zum Erstellen von S3-Lebenszykluskonfigurationen finden Sie im Abschnitt zum Lifecycle Management von Objekten im *Amazon Simple Storage Service Developer Guide*. Beachten Sie, dass StorageGRID nur Aktionen nach Ablauf unterstützt. Es werden keine Aktionen zur Transition unterstützt.

"Amazon Simple Storage Service Developer Guide: Lifecycle Management von Objekten"

Was für eine Lebenszykluskonfiguration 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 Lebensdauer eines Objekts`“ in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

> 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

Erstellen der Lebenszykluskonfiguration

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"
        }
    ]
}
```

Anwenden einer Lebenszykluskonfiguration auf einen Bucket

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`:Eimer

```
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.

Überprüfung, ob der Bucket-Lebenszyklus für ein 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`“ in den Anweisungen zur Durchführung der StorageGRID-Administration.

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": {}
}
```

Verwandte Informationen

"Operationen auf Buckets"

"Objektmanagement mit ILM"

Benutzerdefinierte Vorgänge für Buckets

Das StorageGRID System unterstützt benutzerdefinierte Bucket-Vorgänge, die der S3-REST-API hinzugefügt wurden und sich speziell auf das System bezieht.

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-Konsistenzanforderung"

Betrieb	Beschreibung	Finden Sie weitere Informationen
PUT Bucket-Konsistenz	Legt die Konsistenzstufe für einen bestimmten Bucket fest.	"PUT Bucket-Konsistenzanforderung"
ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Gibt an, ob Updates der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert wurden.	"Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN"
PUT Bucket-Zeit für den letzten Zugriff	Hiermit können Sie Updates der letzten Zugriffszeit für einen bestimmten Bucket aktivieren oder deaktivieren.	"PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs"
Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Löscht die XML-Konfiguration für die Metadatenbenachrichtigung, die mit einem bestimmten Bucket verknüpft ist.	"Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen LÖSCHEN"
Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Gibt die XML-XML-Benachrichtigungskonfiguration für Metadaten zurück, die einem bestimmten Bucket zugeordnet ist.	"Konfigurationsanforderung FÜR Bucket-Metadaten-Benachrichtigungen ABRUFEN"
PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket	"PUT Anforderung der Bucket-Metadaten-Benachrichtigung"
Bucket-Änderungen für Compliance	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mit aktivierter Compliance mehr erstellen.	"Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen"
Bucket-Compliance	Veraltet, aber unterstützt: Gibt die Compliance-Einstellungen zurück, die derzeit für einen vorhandenen Legacy-konformen Bucket wirksam sind.	"Veraltet: GET Bucket-Compliance-Anforderung"
BUCKET-Compliance	Veraltet, aber unterstützt: Ermöglicht es Ihnen, die Compliance-Einstellungen für einen vorhandenen, älteren konformen Bucket zu ändern.	"Veraltet: PUT Bucket-Compliance-Anforderung"

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.

- "Verwenden der S3-Objektsperre"
- "Mit Servver-seitiger Verschlüsselung"
- "GET Objekt"
- "HEAD Objekt"
- "WIEDERHERSTELLUNG VON POSTOBJEKTEN"
- "PUT Objekt"
- "PUT Objekt - Kopieren"

Die folgenden Bedingungen gelten für alle Objektvorgänge:

- StorageGRID Consistency Controls werden von allen Operationen für Objekte unterstützt, mit Ausnahme der folgenden:
  - GET Objekt-ACL
  - `OPTIONS /`
  - LEGALE Aufbewahrung des Objekts EINGEBEN
  - AUFBEWAHRUNG von Objekten
- Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die „`latest-WINS` “ -Bewertung basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf dem, 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.
- Auf Datenobjekte, die über Swift in das StorageGRID-System aufgenommen werden, kann nicht über S3 zugegriffen werden.

In der folgenden Tabelle wird beschrieben, wie StorageGRID S3-REST-API-Objektvorgänge implementiert.

Betrieb	Implementierung
Objekt LÖSCHEN	Multi-Faktor Authentication (MFA) und Response Header `x-amz-mfa` Werden nicht unterstützt. 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. Falls nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Standort vorübergehend nicht verfügbar ist), warteschlangen StorageGRID die Kopien zum Entfernen und zeigen dann den Erfolg des Clients an. **Versionierung** Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und den verwenden `versionId` unterressource. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn der `versionId` Entspricht einer Löschen-Markierung, dem Antwortkopf `x-amz-delete-marker` Wird auf festgelegt `true`. • Wird ein Objekt ohne gelöscht `versionId` unterressource auf einem Bucket mit Versionsfunktion führt zur Generierung einer Löschmarkierung. Der `versionId` Für die Löschen-Markierung wird mit dem zurückgegeben `x-amz-version-id` Kopfzeile der Antwort und das `x-amz-delete-marker` Der Antwortkopf wird auf festgelegt `true`. • Wird ein Objekt ohne gelöscht `versionId` unterressource in einem Version suspended Bucket führt es zu einer dauerhaften Löschung einer bereits vorhandenen 'null' Version oder eines 'null' Löschmarker und der Generierung eines neuen 'null' Löschmarker. Der `x-amz-delete-marker` Der Antwortkopf wird auf festgelegt `true`. **Hinweis**: In bestimmten Fällen können für ein Objekt mehrere Löschen-Marker vorhanden sein.
LÖSCHEN Sie mehrere Objekte	Multi-Faktor Authentication (MFA) und Response Header `x-amz-mfa` Werden nicht unterstützt. In derselben Anforderungsmeldung können mehrere Objekte gelöscht werden.

Betrieb	Implementierung
Objekt-Tagging LÖSCHEN	Verwendet das `tagging` unterressource, um alle Tags aus einem Objekt zu entfernen. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. **Versionierung** Wenn der `versionId` 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 `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.
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	"Verwenden der S3-Objektsperre"
Aufbewahrung von Objekten	"Verwenden der S3-Objektsperre"
GET Objekt-Tagging	Verwendet das `tagging` unterressource, um alle Tags für ein Objekt zurückzugeben. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert **Versionierung** Wenn der `versionId` 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 `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.
HEAD Objekt	"HEAD Objekt"
WIEDERHERSTELLUNG VON POSTOBJEKTEN	"WIEDERHERSTELLUNG VON POSTOBJEKTEN"

Betrieb	Implementierung
PUT Objekt	"PUT Objekt"
PUT Objekt - Kopieren	"PUT Objekt - Kopieren"
LEGALE Aufbewahrung des Objekts EINGEBEN	"Verwenden der S3-Objektsperre"
AUFBEWAHRUNG von Objekten	"Verwenden der S3-Objektsperre"

Betrieb	Implementierung
PUT Objekt-Tagging	Verwendet das `tagging` unterressource, um einem vorhandenen Objekt einen Satz von Tags hinzuzufügen. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert **Tag-Updates und Aufnahmeverhalten** 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. Das bedeutet, dass, wenn die ILM-Regel die strikte Option für das Ingest-Verhalten verwendet, keine Maßnahmen ergriffen werden, wenn die erforderlichen Objektplatzierungen nicht durchgeführt werden können (z. B. weil ein neu benötigter Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist. • Konflikte lösen* Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die „`latest-WINS` “ -Bewertung basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf dem, wenn S3-Clients einen Vorgang starten. **Versionierung** Wenn der `versionId` 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 `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

Verwandte Informationen

"Konsistenzkontrollen"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

Wenn die globale S3-Objektsperre für Ihr StorageGRID System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperre erstellen und dann für jede zu diesem Bucket addieren Objektversion noch bis dato und Legal-Hold-Einstellungen festlegen.

Mit S3 Object Lock können Sie Einstellungen auf Objektebene angeben, um das Löschen oder Überschreiben von Objekten für einen bestimmten Zeitraum oder für einen bestimmten Zeitraum zu verhindern.

Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

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. Sie können eine der folgenden Methoden verwenden:

- Erstellen Sie den Bucket mit Tenant Manager.

  "Verwenden Sie ein Mandantenkonto"

- Erstellen Sie den Bucket mithilfe einer PUT-Bucket-Anforderung zusammen mit dem `x-amz-bucket-object-lock_enabled` Kopfzeile der Anfrage.

  "Operationen auf Buckets"

Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem der Bucket erstellt wurde. Für die S3-Objektsperre ist eine Bucket-Versionierung erforderlich. Diese wird bei der Erstellung des Buckets automatisch aktiviert.

Ein Bucket mit aktivierter S3-Objektsperre kann eine Kombination von Objekten mit und ohne S3-ObjektLock-Einstellungen enthalten. StorageGRID unterstützt nicht die Standard-Aufbewahrung der Objekte in S3 Objektsperren-Buckets, daher wird der Vorgang PUT Object Lock Configuration nicht unterstützt.

Ermitteln, ob die S3-Objektsperre für einen Bucket aktiviert ist

Um festzustellen, ob die S3-Objektsperre aktiviert ist, verwenden Sie die Konfigurationsanforderung FÜR DIE OBJEKTSPERRE ABRUFEN.

"Operationen auf Buckets"

Erstellen eines Objekts mit S3 Object Lock Einstellungen

Zum Festlegen von S3-Objektsperreinstellungen beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre geben Sie ein PUT-Objekt aus, PUT Object - Copy oder initiieren Sie die Anforderung zum Hochladen mehrerer Teile. Verwenden Sie die folgenden Anfrageheader.

> Sie müssen die S3-Objektsperre aktivieren, wenn Sie einen Bucket erstellen. Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde.

- `x-amz-object-lock-mode`, Die COMPLIANCE sein muss (Groß-/Kleinschreibung muss beachtet werden).

  > 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.
- Eine Anfrage zur späteren LÖSCHUNG von Objekten oder ZUM LÖSCHEN von Objektversionen schlägt fehl, wenn sie sich vor dem Datum der Aufbewahrung bis zum Datum befindet oder wenn eine gesetzliche Aufbewahrungspflichten vorliegen.

Einstellungen für die S3-Objektsperre werden aktualisiert

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 Moduswert muss COMPLIANCE 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.

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

"PUT Objekt"

"PUT Objekt - Kopieren"

"Initiieren Von Mehrteiligen Uploads"

"Objektversionierung"

"Amazon Simple Storage Service Benutzerhandbuch: S3 Object Lock verwenden"

Mit serverseitiger 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 von 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

SSE-C verwenden

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-kodiert 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 CloudMirror-Replikation für den Bucket konfiguriert ist, können Sie SSE-C-Objekte nicht aufnehmen. Der Aufnahmevorgang schlägt fehl.

Verwandte Informationen

"GET Objekt"

"HEAD Objekt"

"PUT Objekt"

"PUT Objekt - Kopieren"

"Initiieren Von Mehrteiligen Uploads"

"Hochladen Von Teilen"

"Hochladen Von Teilen - Kopieren"

"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.

Teilenummer-Anforderungsparameter wird nicht unterstützt

Der `partNumber` Der Anforderungsparameter wird für GET-Objektanforderungen nicht unterstützt. Sie können keine Anforderung ZUM ABRUFEN eines bestimmten Teils eines mehrteiligen Objekts ausführen. Ein nicht implementierter Fehler 501 wird mit folgender Meldung zurückgegeben:

```
GET Object by partNumber is not implemented
```

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 zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. ABFRAGEN für ein Objekt mit entgangenen UTF-8 Zeichen in benutzerdefinierten Metadaten WERDEN nicht zurückgegeben `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 A `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`.

Verhalten DES GET Object für Cloud-Storage-Pool-Objekte

Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wurde (siehe Anweisungen zum Managen von Objekten mit Information Lifecycle Management), hängt das Verhalten einer GET-Objektanforderung vom Status des Objekts ab. Weitere Informationen finden Sie unter „`HEAD Object`“.

> 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 eine Wiederherstellungsanforderung FÜR DAS OBJEKT NACH DEM Wiederherstellen, um das Objekt in einen aufrufbaren Zustand wiederherzustellen.
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`.

Verwandte Informationen

"Mit serverseitiger Verschlüsselung"

"Objektmanagement mit ILM"

"WIEDERHERSTELLUNG VON POSTOBJEKTEN"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

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 Übergangsstatus des Objekts bestimmen.

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 zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. HEAD-Anfragen für ein Objekt mit entgangenen 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`

Antwortkopfzeilen für Cloud-Storage-Pool-Objekte

Wenn das Objekt in einem Cloud-Storage-Pool gespeichert ist (siehe Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management), werden die folgenden Antwortheader 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`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Bis das Objekt in einen nicht aufrufbaren Zustand überführt wird, wird der Wert für `expiry-date` Wird in der Zukunft auf eine ferne Zeit gesetzt. Die genaue Zeit der Transition wird nicht durch das StorageGRID System gesteuert.

Das Objekt ist in den nicht aufrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Grid vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Der Wert für `expiry-date` Wird in der Zukunft auf eine ferne Zeit gesetzt.
	
	Hinweis: Wenn die Kopie im Raster nicht verfügbar ist (z. B. ein Speicherknoten ist nicht verfügbar), müssen Sie eine ANFRAGE ZUR WIEDERHERSTELLUNG DES POSTOBJEKTS stellen, um die Kopie aus dem Cloud-Speicherpool wiederherzustellen, bevor Sie das Objekt erfolgreich abrufen können.

Das Objekt wurde in einen nicht abrufbaren Zustand versetzt, und es ist keine Kopie im Grid vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Status des Objekts	Reaktion auf HEAD Objekt

Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Der `expiry-date` Gibt an, wann das Objekt im Cloud Storage Pool wieder in einen Zustand zurückversetzt werden soll, der nicht abrufbar ist.

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 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.

Versionierung

Wenn A `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`.

Verwandte Informationen

"Mit serverseitiger Verschlüsselung"

"Objektmanagement mit ILM"

"WIEDERHERSTELLUNG VON POSTOBJEKTEN"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

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 nicht angeben `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 wiederrufbaren Zustand überführt wurde, können Sie dessen nicht ändern `expiry-date`.
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 `Tier` Element anfordern, um zu bestimmen, wie lange der Wiederherstellungsauftrag dauern wird (`Expedited`, `Standard`, Oder `Bulk`). Wenn Sie nicht angeben `Tier`, Das `Standard` Tier wird verwendet. **Achtung**: Wenn ein Objekt auf das S3 Glacier Deep Archive migriert wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, kann es nicht über den wiederhergestellt werden `Expedited` Ebene: Der folgende Fehler wird zurückgegeben `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class.`

Status des Objekts	Verhalten DER WIEDERHERSTELLUNG NACH Objekten
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 `expiry-date` Indem Sie die Anforderung zur Wiederherstellung DES POSTOBJEKTS mit einem neuen Wert für neu ausgeben `Days`. Das Wiederherstellungsdatum wird zum Zeitpunkt der Anfrage aktualisiert.

Verwandte Informationen

"Objektmanagement mit ILM"

"HEAD Objekt"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

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 „`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.

Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

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-<em>name</em>: <em>value</em>
```

Wenn Sie die Option **benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie sie 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 ausgewogenen oder strengen Optionen für das Aufnahmeverhalten verwenden. Beim Erstellen der ILM-Regel wird ein Fehler zurückgegeben.

- `x-amz-tagging`
- S3-Objektsperrungs-Anfrageheader
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"Verwenden der S3-Objektsperre"

- 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`

"Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"

Nicht unterstützte Anforderungsheader

Die folgenden Anfragezeilen 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 aufgenommene 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). Nach der Bewertung des ILM bestimmt StorageGRID, ob diese anfänglichen vorläufigen Kopien den Anweisungen zur Platzierung in der Regel entsprechen. Andernfalls müssen möglicherweise neue Objektkopien an verschiedenen Standorten erstellt werden, wobei die anfänglichen vorläufigen Kopien unter Umständen gelöscht werden müssen.
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt und StorageGRID nicht sofort alle Kopien erstellen kann, die in der Regel angegeben sind, erstellt StorageGRID zwei Zwischenkopien auf unterschiedlichen Storage-Nodes.

    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).
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten 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.

Achtung: Nur eine Kopie für einen beliebigen Zeitraum zu haben bedeutet, dass Daten dauerhaft verloren gehen. 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.

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.

Hinweis: Wenn Sie ein Objekt in einen Eimer mit aktivierter S3-Objektsperre aufnehmen, wird der 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.

Achtung: die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie 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.`“

Hinweis: Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket-Ebene 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.

Verwandte Informationen

"Objektmanagement mit ILM"

"Operationen auf Buckets"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

"Mit serverseitiger Verschlüsselung"

"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 „`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.

Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

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-Objektsperrungs-Anfrageheader:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"Verwenden der S3-Objektsperre"

- 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`

"Anforderungsheader für serverseitige Verschlüsselung"

Nicht unterstützte Anforderungsheader

Die folgenden Anfragezeilen 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-Aufnahmevorgang 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-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitaler 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 bedeutet, dass, wenn die ILM-Regel die strikte Option für das Ingest-Verhalten verwendet, keine Maßnahmen ergriffen werden, wenn die erforderlichen Objektplatzierungen nicht durchgeführt werden können (z. B. weil ein neu benötigter 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 gestellen 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` Angeben `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key` Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten, 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.

Achtung: die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie 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.`“

- 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`

Hinweis: Das `server-side-encryption` Der 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"

"Mit serverseitiger Verschlüsselung"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

"PUT Objekt"

Vorgänge für mehrteilige Uploads

In diesem Abschnitt wird beschrieben, wie StorageGRID Vorgänge für mehrteilige Uploads unterstützt.

- "Mehrteilige Uploads auflisten"
- "Initiieren Von Mehrteiligen Uploads"
- "Hochladen Von Teilen"
- "Hochladen Von Teilen - Kopieren"
- "Abschließen Von Mehrteiligen Uploads"

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 einzigartiges Objekt betrachtet wird, verringert der StorageGRID-Metadaten-Overhead durch große Teilgrößen.
  - Verwenden Sie für Objekte, die kleiner als 5 gib sind, stattdessen einen Upload ohne mehrere Teile.
- ILM wird für jeden Teil eines mehrteiligen Objekts bei Aufnahme und für das Objekt als Ganzes, wenn der Multipart-Upload abgeschlossen ist, bewertet, wenn die ILM-Regel das strenge oder ausgeglichene Aufnahmeverhalten verwendet. Sie sollten sich bewusst sein, wie dies die Objekt- und Teileplatzierung beeinflusst:
  - Wenn sich ILM-Änderungen während des Hochladen 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 Standorten gespeichert werden können, die die ILM-Anforderungen für das Objekt als Ganzes 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

Betrieb	Implementierung
Teile Auflisten	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert

Verwandte Informationen

"Konsistenzkontrollen"

"Mit serverseitiger 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`
- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

Der `delimiter` Der Parameter der Anforderung wird nicht unterstützt.

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

Mit dem Vorgang „Mehrteilerupload initiieren“ wird ein mehrtei. Upload für ein Objekt initiiert und eine Upload-ID zurückgegeben.

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 aufgenommene 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). Nach der Bewertung des ILM bestimmt StorageGRID, ob diese anfänglichen vorläufigen Kopien den Anweisungen zur Platzierung in der Regel entsprechen. Andernfalls müssen möglicherweise neue Objektkopien an verschiedenen Standorten erstellt werden, wobei die anfänglichen vorläufigen Kopien unter Umständen gelöscht werden müssen.

  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt und StorageGRID nicht sofort alle Kopien erstellen kann, die in der Regel angegeben sind, erstellt StorageGRID zwei Zwischenkopien auf unterschiedlichen Storage-Nodes.

    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).
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten 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.

Achtung: Nur eine Kopie für einen beliebigen Zeitraum zu haben bedeutet, dass Daten dauerhaft verloren gehen. 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.

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.

Hinweis: Wenn Sie ein Objekt in einen Eimer mit aktivierter S3-Objektsperre aufnehmen, wird der 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 **benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie sie 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-Objektsperrungs-Anfrageheader:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"Verwenden der S3-Objektsperre"

- 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`

"Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"

> Informationen zum Umgang von UTF-8-Zeichen mit StorageGRID finden Sie in der Dokumentation ZU PUT Object.

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein mehrteitiges 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 Anforderungen zum Hochladen von Teilen 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.

Achtung: die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie 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.`“

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"

"Mit serverseitiger Verschlüsselung"

"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

"Mit serverseitiger 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.

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 „`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.

Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

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-Aufnahmevorgang 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-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitaler 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.

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 diese 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 **Knoten** > ***Speicherknoten*** > **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
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

Name	HTTP-Status
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
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
XComplianceKonflict	Vorgang aufgrund von Compliance-Einstellungen abgelehnt.	403 Verbotene
XComplianceReducedRAID-RedundanzVerbotenen	Reduzierte Redundanz ist in einem älteren, konformen Bucket nicht zulässig	400 Fehlerhafte Anfrage
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
XNotImplemsted	Die von Ihnen gestellte Anfrage beinhaltet Funktionen, die nicht implementiert sind.	501 Nicht Implementiert

StorageGRID S3 REST-API-Operationen

Auf der S3-REST-API wurden Vorgänge hinzugefügt, die speziell für das StorageGRID-System gelten.

Get Bucket-Konsistenzanforderung

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 müssen über die berechtigung s3:GetBucketConsistency verfügen oder als Account root vorliegen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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.
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 Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „`available`“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

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-Konsistenzanforderung

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.

Sie müssen über die berechtigung s3:PutBucketConsistency verfügen oder als Account root vorliegen, 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.

Konsistenzkontrolle	Beschreibung
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „`available`“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

Hinweis: im Allgemeinen sollten Sie den Wert der Consistency consistency consistency control “read-after-New-write” verwenden. Wenn Anforderungen nicht korrekt funktionieren, ändern Sie das Verhalten des Anwendungs-Clients, 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Verwandte Informationen

"Konsistenzkontrollen"

Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN

In der Anforderung „letzte Bucket-Zugriffszeit“ KÖNNEN Sie festlegen, ob Updates der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind.

Sie müssen über die berechtigung s3:GetBucketLastAccessTime verfügen oder als Kontostamm vorliegen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 Anforderung der Uhrzeit des letzten Bucket-Zugriffs

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 müssen über die s3:PutBucketLastAccessTime-Berechtigung für einen Bucket verfügen oder als Account-Root dienen, 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 zum letzten Zugriffszeitpunkt mithilfe der Anforderung PUT Bucket Last Access Time, des Checkbox **S3** > **Buckets** > **Letzte Zugriffseinstellung ändern** im Tenant Manager oder der Tenant Management API aktivieren oder deaktivieren.

Wenn Updates der letzten Zugriffszeit für einen Bucket deaktiviert wurden, wird das folgende Verhalten auf die Vorgänge auf dem Bucket angewendet:

- Anforderungen FÜR GET Object, GET Object ACL, GET Object Tagging und HEAD Object aktualisieren die letzte Zugriffszeit nicht. 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 der letzten Zugriffszeit für den Quell-Bucket deaktiviert sind, AKTUALISIERT 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Dieses Beispiel deaktiviert die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen 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 müssen über die berechtigung s3:DeleteBucketMetadataNotification für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Dieses Beispiel zeigt die Deaktivierung des Suchintegrationsservice für einen Bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Konfigurationsanforderung FÜR 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 müssen über die berechtigung s3:GetBucketMetadataNotification verfügen oder als Kontowurzel dienen, 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelelement.	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.
Präfix	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.

Name	Beschreibung	Erforderlich
Urne	URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein: • `es` Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular `domain-name/myindex/mytype`. Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl. Urne ist im Element Ziel enthalten.	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 gesendet `current` Und geben Sie den Namen ein `2017` Das wird in einer AWS-Domäne mit dem Namen gehostet `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

PUT Anforderung der Bucket-Metadaten-Benachrichtigung

Die Konfigurationsanforderung FÜR PUT Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, den Such-Integrationsservice für einzelne Buckets zu aktivieren. Die XML-XML-Konfiguration für die Metadatenbenachrichtigung, die Sie im Anforderungsindex angeben, gibt die Objekte an, deren Metadaten an den Zielsuchindex gesendet werden.

Sie müssen über die berechtigung s3:PutBucketMetadataNotification für einen Bucket verfügen oder als Account-Root dienen, 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 senden `/images` An ein Ziel und Objekte mit dem Präfix `/videos` Nach anderen.

Konfigurationen mit sich überschneidenden Präfixen sind ungültig und werden beim Einreichen abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix enthielt `test` 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 Regelelement.	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	Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt. In das Element Regel aufgenommen.	Ja.
Präfix	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.

Name	Beschreibung	Erforderlich
Urne	URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein: • `es` Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular `domain-name/myindex/mytype`. Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl. Urne ist im Element Ziel enthalten.	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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Vom Suchintegrations-Service generierter JSON

Wenn Sie den Such-Integrationsservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielendpunkt 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 `us-east-1`
System-Metadaten	Größe	Objektgröße (in Byte) wie für einen HTTP-Client sichtbar
System-Metadaten	md5	Objekt-Hash
Benutzer-Metadaten	Metadaten *`key:value`*	Alle Benutzer-Metadaten des Objekts als Schlüssel-Wert-Paare
Tags	tags *`key:value`*	Alle für das Objekt definierten Objekt-Tags als Schlüsselwert-Paare

Hinweis: für Tags und Benutzer-Metadaten übergibt StorageGRID Daten und Nummern als Strings oder als S3-Ereignisbenachrichtigungen an Elasticsearch. 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 bearbeiten.

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 keine „stabile globale“ Konsistenz erreicht werden kann, versucht StorageGRID, die Nutzungsinformationen in einer starken Konsistenz des Standorts abzurufen.

Sie müssen über die s3:ListAllMyBuchets-Berechtigung verfügen oder als Kontostamm vorliegen, um diese Operation abzuschließen.

Anforderungsbeispiel

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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. Markierungen löschen 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, wird die globale S3-Objektsperre beim Upgrade auf StorageGRID 11.5 automatisch 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.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

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.

"Verwenden der S3-Objektsperre"

"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.
```

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

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.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

Um diesen Vorgang abzuschließen, müssen Sie über die berechtigung s3:GetBucketCompliance verfügen

oder als Stammverzeichnis für das Konto verfügen.

Anforderungsbeispiel

In dieser Beispielanforderung können Sie die Compliance-Einstellungen für den Bucket mit dem Namen festlegen `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 Aufbewahrungspflichten auf diesem Bucket vorhanden. Jedes Objekt wird nach einem Jahr automatisch gelöscht.

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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.

Name	Beschreibung
LegalAlte	• Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn die gesetzliche Aufbewahrungsphase 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	• 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`.

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

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.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

Sie müssen über die s3:PutBucketCompliance-Berechtigung verfügen oder als Kontoroot vorliegen, 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: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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. **Achtung:** Wenn Sie einen neuen Wert für RetentionPeriodMinutes angeben, müssen Sie einen Wert angeben, der der aktuellen Aufbewahrungsdauer des Buckets entspricht oder größer ist. Nach der Festlegung des Aufbewahrungszeitraums des Buckets können Sie diesen Wert nicht verringern; Sie können ihn nur erhöhen.
LegalAlte	• Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn die gesetzliche Aufbewahrungsphase 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.

Name	Beschreibung
Automatisches Löschen	• 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 **stark-global** nicht erreichen kann, da ein Datacenter-Standort 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"

"Verwenden Sie ein Mandantenkonto"

"Objektmanagement mit ILM"

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.

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.

Element	Beschreibung
Zustand	Das Bedingungselement 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 Ressource können Sie die Platzhalterzeichen (*) und (?) verwenden. Während das Sternchen (*) mit 0 oder mehr Zeichen übereinstimmt, ist das Fragezeichen (?) Entspricht einem beliebigen Zeichen.

Im Principal-Element werden Platzhalterzeichen nicht unterstützt, außer wenn anonymer Zugriff festgelegt wird, der allen die Berechtigung erteilt. 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.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

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 des 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 Identitätressource 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.

Festlegen von Ressourcen in einer Richtlinie

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.

Verwandte Informationen

"Festlegen von Variablen in einer Richtlinie"

Prinzipale in einer Richtlinie 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. Richtlinienerklärungen in einer Gruppenpolitik benötigen das Hauptelement nicht, da die Gruppe als Hauptbestandteil 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 beitritt 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.

Festlegen von Berechtigungen in einer Richtlinie

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.

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
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	
s3:GetReplicationConfiguration	GET Bucket-Replizierung	
s3:ListAllMyBuchs	• GET Service • GET Storage-Auslastung	Ja, für GET Storage Usage

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:ListBucket	• Bucket ABRUFEN (Objekte auflisten) • EIMER • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:ListBucketMultipartUploads	• 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	• Bucket Cors† LÖSCHEN • Bucket-Cors EINGEBEN	
s3:PutVerschlüsselungKonfiguration	• 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	Geben Sie Bucket mit dem EIN `x-amz-bucket-object-lock-enabled: true` Kopfzeile anfordern (erfordert auch die Berechtigung s3:CreateBucket)	
s3:PutBucketPolicy	Bucket-Richtlinie	
s3:PutBucketTagging	• Bucket-Tagging† löschen • PUT Bucket-Tagging	
s3:PutBucketVersionierung	PUT Bucket-Versionierung	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutLifecycleKonfiguration	• Bucket-Lebenszyklus LÖSCHEN† • PUT Bucket-Lebenszyklus	
s3:PuteReplikationKonfiguration	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:AbortMehrteilaUpload	• Abbrechen Von Mehrteiligen Uploads • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:DeleteObject	• 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)	
s3:GetObject	• GET Objekt • HEAD Objekt • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:GetObjectAcl	GET Objekt-ACL	
s3:GetObjectLegalOld	HOLD-Aufbewahrung für Objekte	
s3:GetObjectRetention	Aufbewahrung von Objekten	
s3:GetObjectTagging	Get Objekt-Tagging	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
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	• PUT Objekt • PUT Objekt - Kopieren • WIEDERHERSTELLUNG VON POSTOBJEKTEN • Initiieren Von Mehrteiligen Uploads • Abschließen Von Mehrteiligen Uploads • Hochladen Von Teilen • Hochladen Von Teilen - Kopieren	
s3:PuttObjectLegalOld	LEGALE Aufbewahrung des Objekts EINGEBEN	
s3:PutObjectRetention	AUFBEWAHRUNG von Objekten	
s3:PuttObjectTagging	PUT Objekt-Tagging	
s3:PuttObjectVersionTagging	PUT Objekt-Tagging (eine bestimmte Version des Objekts)	
s3:PutOverwrite Object	• PUT Objekt • PUT Objekt - Kopieren • PUT Objekt-Tagging • Objekt-Tagging LÖSCHEN • Abschließen Von Mehrteiligen Uploads	Ja.
s3:RestoreObject	WIEDERHERSTELLUNG VON POSTOBJEKTEN	

Verwenden der Berechtigung PutOverwriteObject

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 des Objekts, benutzerdefinierte Metadaten oder S3 Objekt-Tagging 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 eine Überschreibung zulässt und die Berechtigung PutOverwriteObject auf Deny gesetzt ist, kann der Client die Daten eines Objekts, benutzerdefinierte Metadaten oder Objekt-Tagging nicht überschreiben. Wenn zusätzlich das Kontrollkästchen **Client Modification** verhindern* aktiviert ist (**Configuration** > **Grid Options**), überschreibt diese Einstellung die Einstellung der PutOverwriteObject-Berechtigung.

Verwandte Informationen

"Beispiele für S3-Gruppenrichtlinien"

Festlegen von Bedingungen in einer Richtlinie

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 Bedingungselement kann mehrere Bedingungen enthalten, und jede Bedingung kann mehrere Schlüsselwert-Paare enthalten. Der Bedingungsblock verwendet das folgende Format:

```
Condition: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

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).
StringEqusIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird ignoriert).
StringNotEqualesIgnoreCase	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.
Ziffern	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf exakter Übereinstimmung basiert.

Bedingungsoperatoren	Beschreibung
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 negatiertem Abgleich.
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.

Unterstützte Bedingungsschlüssel

Kategorie	Die entsprechenden Bedingungsschlüssel	Beschreibung
IP-Operatoren	aws:SourceIp	Vergleicht mit der IP-Adresse, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden **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. **Hinweis**: Wenn ein Drittanbieter-, nicht-transparenter Load Balancer verwendet wird, wird dies mit der IP-Adresse dieses Load Balancer verglichen. Alle `X-Forwarded-For` Kopfzeile wird ignoriert, da seine Gültigkeit nicht ermittelt werden kann.
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.

Festlegen von Variablen in einer Richtlinie

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
`${aws:SourceIp}`	Verwendet den SourceIp-Schlüssel als bereitgestellte Variable.
`${aws:username}`	Verwendet den Benutzernamen-Schlüssel als bereitgestellte Variable.
`${s3:prefix}`	Verwendet den Service-spezifischen Präfixschlüssel als bereitgestellte Variable.
`${s3:max-keys}`	Verwendet die Service-spezifische max-keys als die angegebene Variable.
`${*}`	Sonderzeichen. Verwendet das Zeichen als Literal * -Zeichen.
`${?}`	Sonderzeichen. Verwendet den Charakter als Literal ? Zeichen.
`${$}`	Sonderzeichen. Verwendet das Zeichen als Literal USD Zeichen.

Erstellen von Richtlinien, die eine besondere 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-Benutzers des Kontos. Die StorageGRID S3-REST-API-Implementierung ist bei der Richtlinienvalidierung weniger restriktiv als Amazon, aber auch bei der Richtlinienbewertung 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 Richtlinienzugelassen 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 Richtlinienzugelassen 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:

- Wählen Sie im Grid Manager die Option **Konfiguration** > **Grid-Optionen** 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 all 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

"Objektmanagement mit ILM"

"Erstellen von Richtlinien, die eine besondere Handhabung erfordern"

"Managen von Objekten durch StorageGRID ILM-Regeln"

"Beispiele für S3-Gruppenrichtlinien"

Beispiele für S3-Richtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID-Zugriffsrichtlinien für Buckets und Gruppen zu erstellen.

Beispiele für S3-Bucket-Richtlinien

Bucket-Richtlinien geben die Zugriffsberechtigungen für den Bucket an, mit dem die Richtlinie verknüpft ist. Bucket-Richtlinien werden mithilfe der S3-PutBucketPolicy-API konfiguriert.

Eine Bucket-Richtlinie kann mithilfe der AWS CLI wie folgt konfiguriert werden:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

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/*"
    }
  ]
}
```

Verwandte Informationen

"Operationen auf Buckets"

Beispiele für S3-Gruppenrichtlinien

Gruppenrichtlinien legen die Zugriffsberechtigungen für die Gruppe fest, der die Richtlinie zugeordnet ist. Es gibt keine `Principal` Element in der Richtlinie, da sie implizit ist. Gruppenrichtlinien werden mit dem Tenant Manager oder der API konfiguriert.

Beispiel: Festlegen der Gruppenrichtlinie mit Tenant Manager

Wenn Sie den Tenant Manager zum Hinzufügen oder Bearbeiten einer Gruppe verwenden, können Sie auswählen, wie Sie die Gruppenrichtlinie erstellen möchten, die definiert, welche S3-Zugriffsberechtigungen Mitglieder dieser Gruppe haben. Gehen Sie wie folgt vor:

- **Kein S3-Zugriff**: Standardoption. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat 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. Sie können diesen String nicht bearbeiten.
- **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. Sie können diesen String nicht bearbeiten.
- **Benutzerdefiniert**: Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

  In diesem Beispiel dürfen Mitglieder der Gruppe nur ihren spezifischen Ordner (Schlüsselpräfix) im angegebenen Bucket auflisten und darauf zugreifen.

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}/*"
    }
  ]
}
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Verwenden der Berechtigung PutOverwriteObject"

"WORM-Schutz (Write Once, Read Many)"

Sicherheit wird für DIE REST API konfiguriert

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 Speicherknoten und den CLB-Service auf Gateway-Knoten.

  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.

  Der CLB-Service ist veraltet.

- 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 eine Verbindung zum Lastverteilungsservice auf Gateway-Knoten oder Admin-Nodes, direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes herstellen.

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 Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems (die von der Systemzertifikatbehörde signiert sind) für Speicherknoten generiert wurden. 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 StorageGRID zum Konfigurieren von Load Balancer-Endpunkten finden Sie in den Anweisungen zum Hinzufügen eines einzelnen benutzerdefinierten Serverzertifikats für TLS-Verbindungen direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes.

Zusammenfassung

Die folgende Tabelle zeigt, wie Sicherheitsprobleme in den S3 und Swift REST-APIs implementiert werden:

Sicherheitsproblem	Implementierung für REST-API
Verbindungssicherheit	TLS

Sicherheitsproblem	Implementierung für REST-API
Serverauthentifizierung	X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde
Client-Authentifizierung	• S3: S3-Konto (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel) • Swift: Swift-Konto (Benutzername und Passwort)
Client-Autorisierung	• 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.

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.

Unterstützte Chiffren-Suiten

TLS-Version	IANA Name der Chiffre Suite
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHACHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

Veraltete Chiffre-Suiten

Die folgenden Chiffren Suiten sind veraltet. Die Unterstützung für diese Chiffren wird in einer zukünftigen Version entfernt.

IANA-Name
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Verwandte Informationen

"Wie Client-Verbindungen konfiguriert werden können"

Monitoring und Auditing 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.

- "Monitoring der Objekteinspeisung und -Abrufraten"
- "Aufrufen und Prüfen von Prüfprotokollen"

Monitoring der Objekteinspeisung und -Abrufraten

Die Überwachung von Objekteraufnahmeraten 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 über einen unterstützten Browser beim Grid Manager an.
2. Suchen Sie im Dashboard den Abschnitt Protokollvorgänge.

   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**.

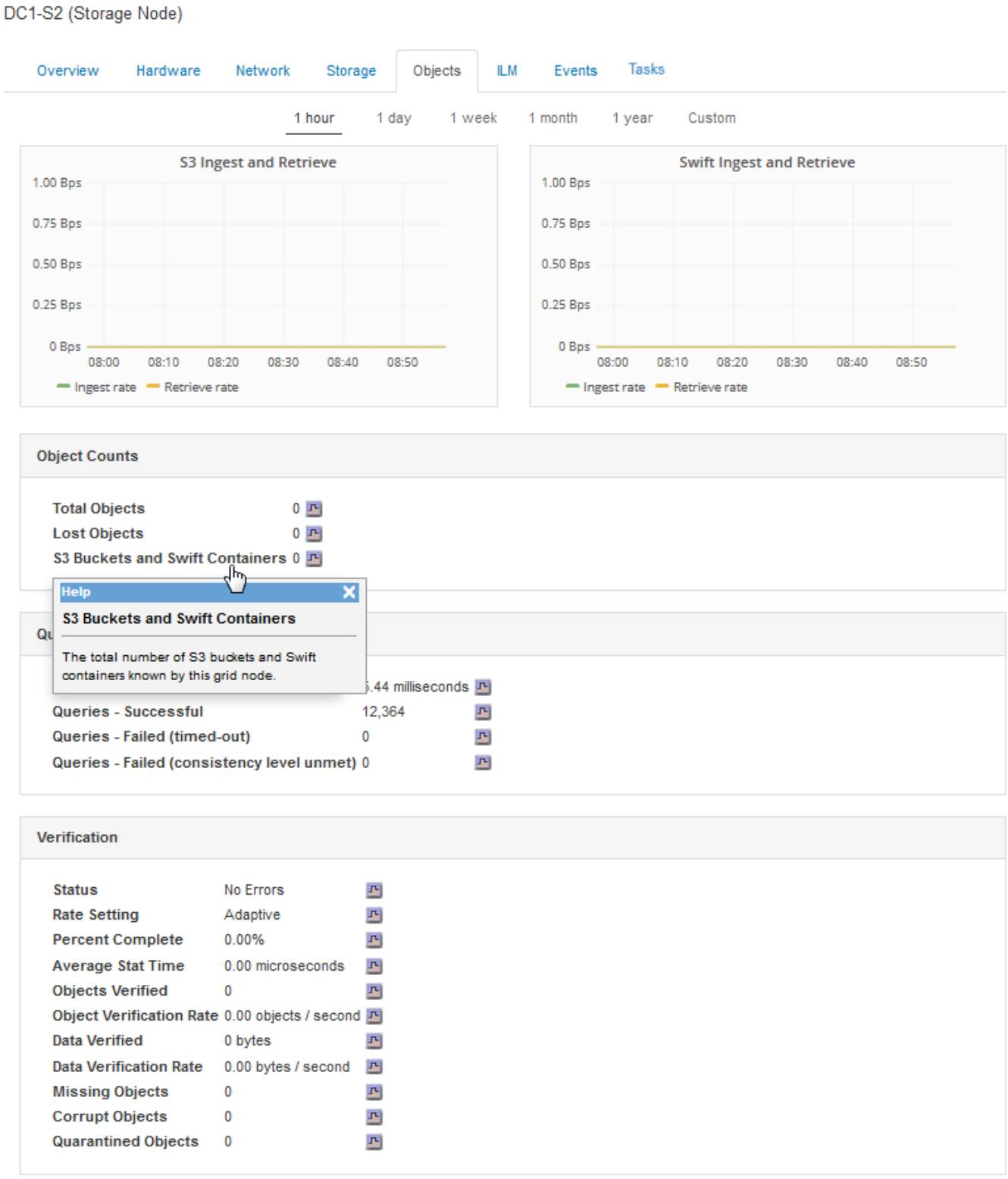
   Die Diagramme zeigen Trends für den gesamten Client-Datenverkehr an Load Balancer-Endpunkte im Raster. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

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.

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 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.



7. Wenn Sie noch mehr Details wünschen:

a. Wählen Sie **Support** > **Tools** > **Grid Topology** 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.

Was Sie benötigen

- 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 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:

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 strenge oder ausgeglichene Aufnahmeverhalten verwendet)
- Hochladen von Teilen – Kopieren (Wenn die ILM-Regel das strenge oder ausgeglichene 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

Verwandte Informationen

- "Vorteile, wenn inaktive HTTP-Verbindungen offen gehalten werden"
- "Vorteile von aktiven HTTP-Verbindungen"
- "Vorteile gleichzeitiger HTTP-Verbindungen"
- "Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge"

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 oder zum CLB-Dienst (veraltet) auf Gateway-Knoten sollten Sie die Dauer einer aktiven HTTP-Verbindung auf maximal 10 Minuten beschränken, auch 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.

Für Client-Verbindungen zu Storage-Nodes oder zum CLB-Service bietet die Beschränkung aktiver HTTP-Verbindungen folgende Vorteile:

- Ermöglicht einen optimalen Lastausgleich über das StorageGRID System hinweg.

  Bei der Nutzung des CLB-Dienstes sollten Sie lange-durchlebte TCP/IP-Verbindungen verhindern, um den Lastenausgleich über das StorageGRID-System zu optimieren. Sie sollten Client-Anwendungen so konfigurieren, dass die Dauer jeder HTTP-Verbindung verfolgt und die HTTP-Verbindung nach einer festgelegten Zeit geschlossen wird, damit die HTTP-Verbindung wiederhergestellt und ausgeglichen werden kann.

  Der CLB-Dienst gleicht die Last über das StorageGRID-System aus, wenn eine Client-Anwendung eine HTTP-Verbindung herstellt. 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.

  Der CLB-Service ist veraltet.

- 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.

Verwenden Sie Swift

Lesen Sie, wie Client-Applikationen die OpenStack Swift API zur Schnittstelle mit dem StorageGRID System nutzen.

- "Unterstützung für OpenStack Swift API in StorageGRID"
- "Mandantenkonten und -Verbindungen werden konfiguriert"
- "Von Swift UNTERSTÜTZTE REST-API-Operationen"
- "StorageGRID Swift REST-API-Operationen"
- "Sicherheit wird für DIE REST API konfiguriert"
- "Monitoring und Auditing von Vorgängen"

Unterstützung für OpenStack Swift API in StorageGRID

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
11.5	Schwache Konsistenzkontrolle entfernt. Stattdessen wird die verfügbare Konsistenzstufe verwendet.
11.4	Unterstützung für TLS 1.3 und aktualisierte Liste der unterstützten TLS-Chiffre-Suites hinzugefügt. CLB ist veraltet. 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. Aktualisierte Liste der unterstützten TLS-Cipher-Suites. 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.

Freigabe	Kommentare
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 die 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. Die ILM-Regeln und -Richtlinie bestimmen, wie StorageGRID Kopien von Objektdaten erstellt und verteilt und wie diese Kopien mit der Zeit 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 StorageGRID-Administrator, wenn Sie wissen müssen, welche Auswirkungen die ILM-Regeln und Richtlinien des Grid auf die Objekte in Ihrem Swift-Mandantenkonto haben.

In Konflikt stehende Clientanforderungen

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 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. 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.

StorageGRID ermöglicht Ihnen außerdem die Kontrolle der Konsistenz einzelner Container. Sie können die Consistency Control ändern, um je nach Anforderung zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte in verschiedenen Storage Nodes und Standorten einen Kompromiss zwischen der Verfügbarkeit der Objekte herzustellen.

Verwandte Informationen

"Objektmanagement mit ILM"

"ABRUFEN der Container-Konsistenzanforderung"

"PUT Container-Konsistenzanforderung"

Empfehlungen für die Implementierung der 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 in einem Pfad existiert, in dem Sie nicht erwarten, dass das Objekt tatsächlich vorhanden ist, 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 Konsistenzkontrolle „`verfügbar`“ für jeden Container mithilfe der PUT Container-Konsistenzanforderung festlegen.

Empfehlungen für Objektnamen

Als die ersten vier Zeichen von Objektnamen sollten keine Zufallswerte verwendet werden. Stattdessen sollten Sie nicht-zufällige, nicht-eindeutige Präfixe verwenden, wie z. B. Bild.

Wenn Sie in Objektnamen-Präfixen zufällige und eindeutige Zeichen verwenden müssen, 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 die Option **komprimiere gespeicherte Objekte** ausgewählt ist (**Konfiguration** > **Systemeinstellungen** > **Grid-Optionen**), sollten Swift-Client-Anwendungen vermeiden, GET-Objektoperationen durchzuführen, die einen Bereich von Bytes angeben. 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.

Verwandte Informationen

"ABRUFEN der Container-Konsistenzanforderung"

"PUT Container-Konsistenzanforderung"

"StorageGRID verwalten"

Mandantenkonten und -Verbindungen werden konfiguriert

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.

Beim Erstellen eines Swift-Mandantenkontos gibt der Grid-Administrator folgende Informationen an:

- Anzeigename für den Mandanten (die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden)
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte 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) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.
- Wenn SSO aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.

Nach der Erstellung eines Swift-Mandantenkontos können Benutzer mit Root Access-Berechtigung auf den Mandanten-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 den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht 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.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"Unterstützte Swift-API-Endpunkte"

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 mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten

> Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- 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).

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.

Weitere Informationen zu den einzelnen Optionen finden Sie in den Anweisungen zur Administration von StorageGRID.

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. Wenden Sie sich an Ihren StorageGRID-Administrator, um weitere Informationen zu erhalten, oder lesen Sie die Anweisungen zur Administration von StorageGRID, um eine Beschreibung der Informationen im Grid-Manager zu erhalten.

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
HA-Gruppe	CLB **Hinweis:** der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	Swift-Standardports: • HTTPS: 8083 • HTTP: 8085
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
Gateway-Node	CLB **Hinweis:** der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node **Hinweis:** standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	Swift-Standardports: • HTTPS: 8083 • HTTP: 8085
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.

Entscheidung über 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 Client-Verbindungen zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Knoten zu verwenden, müssen Sie dessen Verwendung aktivieren.

Wenn Client-Anwendungen eine Verbindung zu Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, müssen sie für alle Verbindungen verschlüsseltes HTTPS verwenden. Optional können Sie weniger sichere HTTP-Verbindungen aktivieren, indem Sie im Grid Manager die Option **HTTP-Verbindung** aktivieren auswählen. Eine Client-Anwendung kann beispielsweise HTTP verwenden, wenn die Verbindung zu einem Speicherknoten in einer nicht produktiven Umgebung getestet wird.

> Achten Sie bei der Aktivierung von HTTP für ein Produktionsraster darauf, dass die Anforderungen unverschlüsselt gesendet werden.

> Der CLB-Service ist veraltet.

Wenn die Option **HTTP-Verbindung aktivieren** ausgewählt ist, müssen Clients für HTTP unterschiedliche Ports verwenden als für HTTPS. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Testen der 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.

Was Sie benötigen

- Sie müssen Python-swiftclient, den Swift-Befehlszeilen-Client, heruntergeladen und installiert haben.
- 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"

"Sicherheit wird für DIE REST API konfiguriert"

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 Antwortheader 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 Domänennamen 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

"Wie Client-Verbindungen konfiguriert werden können"

"Erstellen und Konfigurieren von Swift Mandantenkonten"

"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

"In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"

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

"In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"

Objekt-Operationen

Die folgenden Swift-API-Vorgänge werden an Objekten durchgeführt.

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. Falls nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Standort vorübergehend nicht verfügbar ist), warteschlangen StorageGRID die Kopien zum Entfernen und zeigen dann den Erfolg des Clients an.

Weitere Informationen zum Löschen von Objekten finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

GET Objekt

Dieser Vorgang ruft den Objektinhalt 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 TB.

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 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 Punkte `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 in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (Objektbezogene Metadaten)

  Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie den Wert in einem benutzerdefinierten Header mit dem Namen 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).
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten 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`

Verwandte Informationen

"Objektmanagement mit ILM"

"In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"

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 auth URL 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
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

Die Konsistenzstufe sorgt für einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten 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-consistency`	Gibt den Anforderungstyp an, wobei `true` = GET Containerkonsistenz, und `false` = 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
`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.

HTTP-Kopfzeile für Antwort	Beschreibung
`x-ntap-sg-consistency`	Die auf den Container angewendete Konsistenzkontrollebene. Folgende Werte werden unterstützt: • **Alle**: 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**: Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung **Hinweis**: Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht existieren, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, verwenden Sie die Ebene „`Available`“. • **Verfügbar** (eventuelle Konsistenz für KOPFOPERATIONEN): Verhält sich wie das “read-after-New-write” Konsistenzniveau, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind.

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
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

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-consistency`	Die Konsistenzkontrollebene gilt für Container-Operationen. Folgende Werte werden unterstützt: • **Alle**: 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**: Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung **Hinweis**: Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht existieren, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, verwenden Sie die Ebene „`Available`“. • **Verfügbar** (eventuelle Konsistenz für KOPFOPERATIONEN): Verhält sich wie das “read-after-New-write” Konsistenzniveau, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind.
`Host`	Der Hostname, auf den die Anforderung gerichtet ist.

Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung 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:

- **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.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Kunden zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

> 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.

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
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Sicherheit wird für DIE REST API konfiguriert

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 Speicherknoten und den CLB-Service auf Gateway-Knoten.

  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.

  Der CLB-Service ist veraltet.

- 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 eine Verbindung zum Lastverteilungsservice auf Gateway-Knoten oder Admin-Nodes, direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes herstellen.

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 Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems (die von der Systemzertifikatbehörde signiert sind) für Speicherknoten generiert wurden. 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 StorageGRID zum Konfigurieren von Load Balancer-Endpunkten finden Sie in den Anweisungen zum Hinzufügen eines einzelnen benutzerdefinierten Serverzertifikats für TLS-Verbindungen direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-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	• S3: S3-Konto (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel) • Swift: Swift-Konto (Benutzername und Passwort)
Client-Autorisierung	• 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.

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.

Unterstützte Chiffren-Suiten

TLS-Version	IANA Name der Chiffre Suite
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Veraltete Chiffre-Suiten

Die folgenden Chiffren Suiten sind veraltet. Die Unterstützung für diese Chiffren wird in einer zukünftigen Version entfernt.

IANA-Name
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Verwandte Informationen

"Wie Client-Verbindungen konfiguriert werden können"

Monitoring und Auditing 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.

Monitoring der Objekteinspeisung und -Abrufraten

Die Überwachung von Objekteraufnahmeraten 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 über einen unterstützten Browser beim Grid Manager an.
2. Suchen Sie im Dashboard den Abschnitt Protokollvorgänge.

   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**.

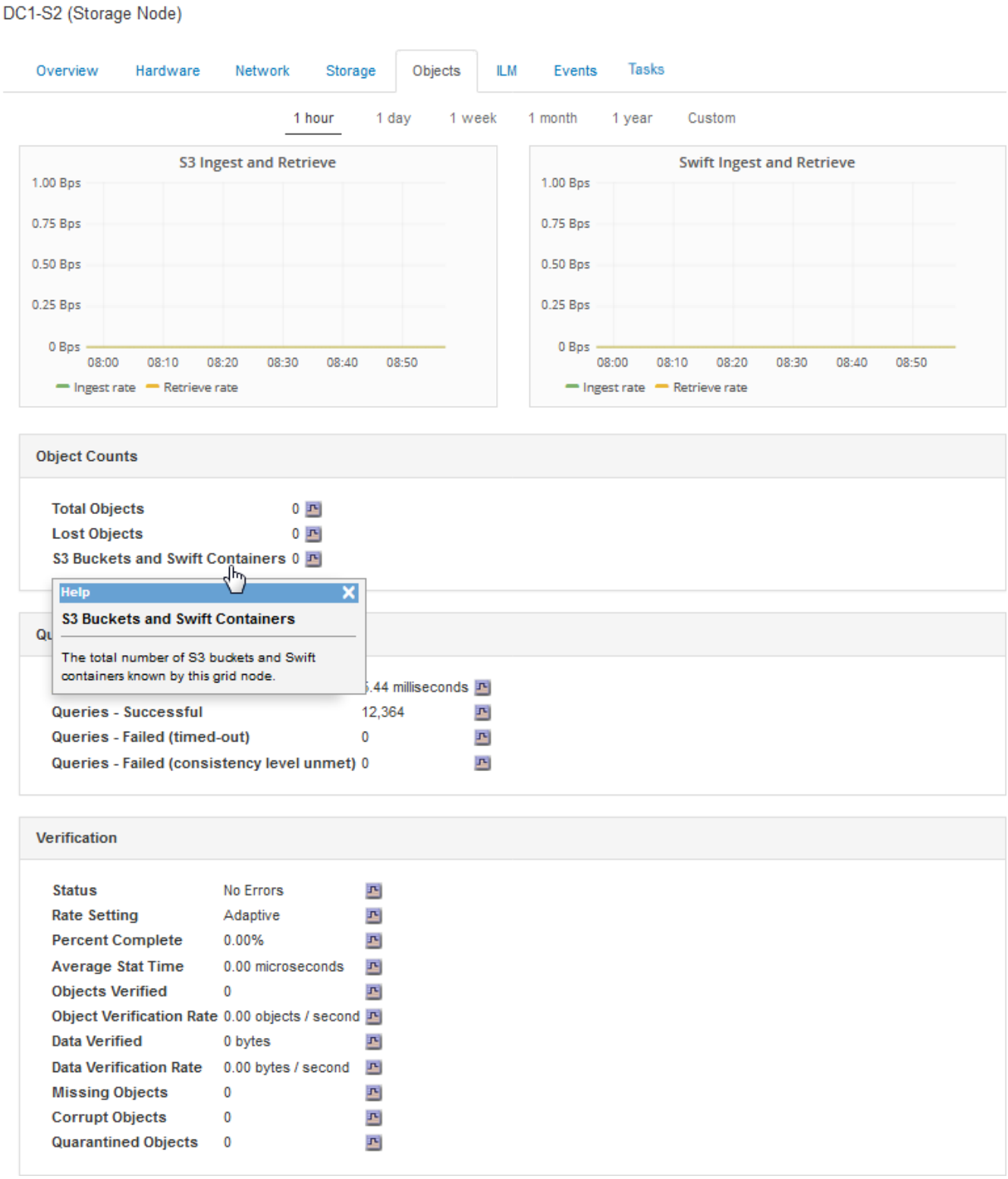
   Die Diagramme zeigen Trends für den gesamten Client-Datenverkehr an Load Balancer-Endpunkte im Raster. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

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.

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 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.



7. Wenn Sie noch mehr Details wünschen:
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** 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.

Was Sie benötigen

- 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 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 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:
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.

Verwandte Informationen

"Prüfung von Audit-Protokollen"

In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt

Alle erfolgreichen Vorgänge zum LÖSCHEN, ABRUFEN, NACHFÜHREN, POSTEN und PUT werden im StorageGRID Audit-Protokoll verfolgt. Fehler werden weder protokolliert, noch sind Info-, Auth- oder OPTIONSANFORDERUNGEN.

Weitere Informationen zu den für die folgenden Swift-Vorgänge erfassten Informationen finden Sie unter *Audit-Meldungen*.

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

Verwandte Informationen

"Prüfung von Audit-Protokollen"

"Konto-Operationen"

"Container-Operationen"

"Objekt-Operationen"

Monitoring und Fehlerbehebung

Überwachen Sie ein StorageGRID System

Erfahren Sie, wie Sie ein StorageGRID System überwachen und eventuelle Probleme bewerten. Listet alle Systemmeldungen auf.

- "Verwenden des Grid Managers zur Überwachung"
- "Informationen, die Sie regelmäßig überwachen sollten"
- "Verwalten von Meldungen und Alarmen"
- "Verwendung von SNMP-Überwachung"
- "Erfassung weiterer StorageGRID-Daten"
- "Fehlerbehebung für ein StorageGRID System"
- "Alerts Referenz"
- "Alarmreferenz (Altsystem)"
- "Referenz für Protokolldateien"

Verwenden des Grid Managers zur Überwachung

Der Grid Manager ist das wichtigste Tool für das Monitoring Ihres StorageGRID Systems. In diesem Abschnitt wird das Grid Manager Dashboard vorgestellt sowie ausführliche Informationen zu den Seiten Nodes bereitgestellt.

- "Anforderungen an einen Webbrowser"
- "Anzeigen des Dashboards"
- "Anzeigen der Seite Knoten"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

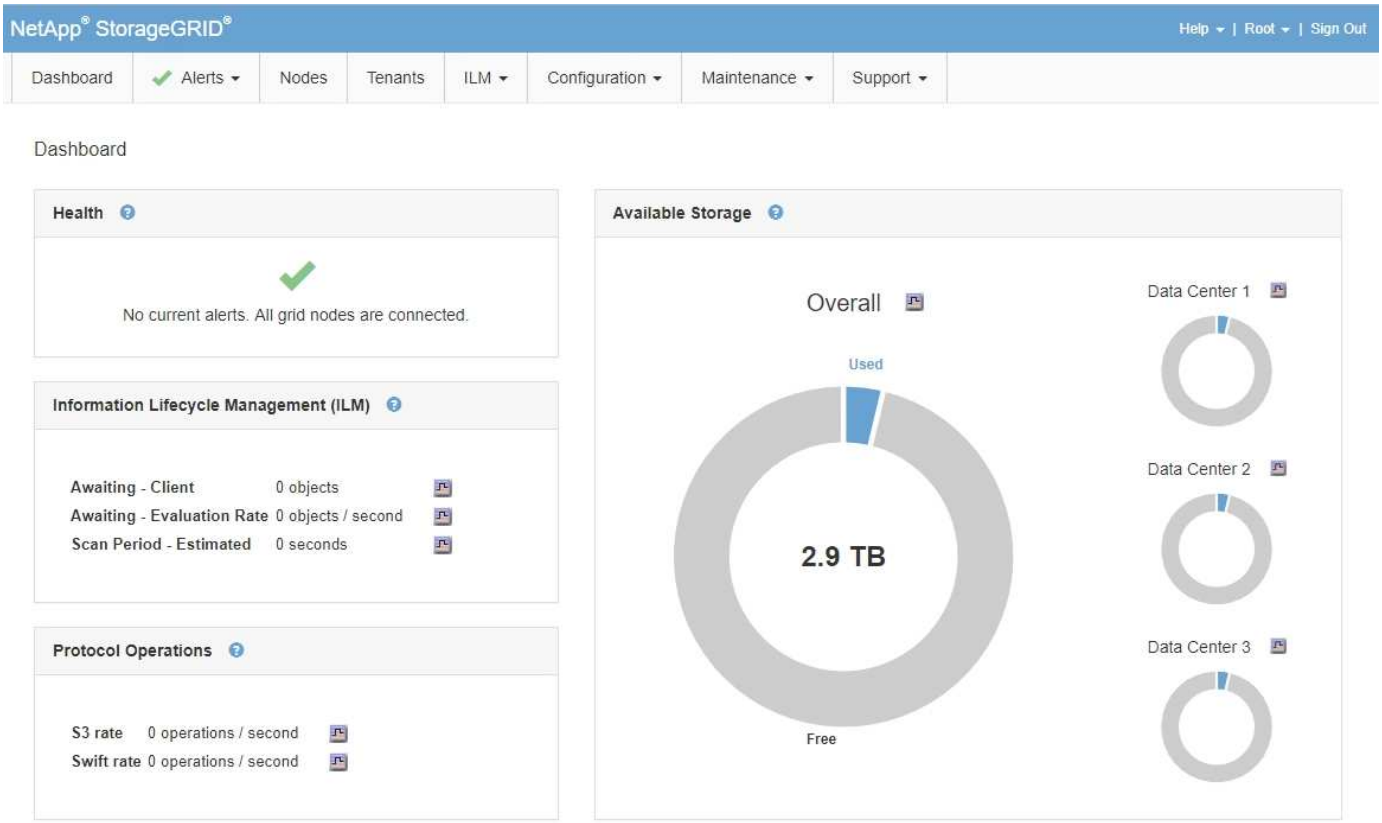
Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024

Browserbreite	Pixel
Optimal	1280

Anzeigen des Dashboards

Wenn Sie sich zum ersten Mal beim Grid Manager anmelden, können Sie über das Dashboard Systemaktivitäten auf einen Blick überwachen. Das Dashboard enthält Informationen zum Systemzustand, über Auslastungsmetriken sowie über Betriebstrends und -Diagramme.



Systemzustand

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Fasst den Systemzustand zusammen. Ein grünes Häkchen bedeutet, dass keine aktuellen Warnmeldungen vorhanden sind und alle Grid-Nodes verbunden sind. Jedes andere Symbol bedeutet, dass mindestens eine aktuelle Warnung oder ein nicht getrennter Knoten vorhanden ist.	Möglicherweise werden mindestens ein der folgenden Links angezeigt: • **Grid Details**: Wird angezeigt, wenn Knoten getrennt sind (Verbindungsstatus unbekannt oder Administrativ ausgefallen). Klicken Sie auf den Link oder klicken Sie auf das blaue oder graue Symbol, um zu ermitteln, welche Nodes betroffen sind. • **Aktuelle Meldungen**: Wird angezeigt, wenn derzeit Alarme aktiv sind. Klicken Sie auf den Link oder klicken Sie auf **kritisch**, **Major** oder **Minor**, um die Details auf der Seite **Alarme** > **Aktuell** anzuzeigen. • **Kürzlich behobene Alarme**: Wird angezeigt, wenn alle in der letzten Woche ausgelösten Benachrichtigungen jetzt behoben sind. Klicken Sie auf den Link, um die Details auf der Seite **Alerts** > **aufgelöst** anzuzeigen. • **Legacy-Alarme**: Wird angezeigt, wenn derzeit Alarme (Legacy-System) aktiv sind. Klicken Sie auf den Link, um die Details auf der Seite **Support** > **Alarme (alt)** > **Aktuelle Alarme** anzuzeigen. • **Lizenz**: Wird angezeigt, wenn ein Problem mit der Softwarelizenz für dieses StorageGRID-System vorliegt. Klicken Sie auf den Link, um die Details auf der Seite **Wartung** > **System** > **Lizenz** anzuzeigen.	• "Monitoring der Verbindungsstatus der Nodes" • "Anzeigen aktueller Meldungen" • "Anzeigen gelöster Warnmeldungen" • "Anzeigen von Legacy-Alarmen" • "StorageGRID verwalten"

Bereich „Verfügbare Lagerung“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die verfügbare und genutzte Speicherkapazität im gesamten Grid an, nicht einschließlich Archivmedien. Das Gesamtdiagramm stellt die Gesamtgesamtwerte für das gesamte Grid dar. Ist dies ein Grid mit mehreren Standorten, werden für jeden Datacenter-Standort zusätzliche Diagramme angezeigt. Anhand dieser Informationen können Sie den verwendeten Speicher mit dem verfügbaren Speicher vergleichen. Wenn Sie ein Grid mit mehreren Standorten verwenden, können Sie feststellen, welcher Standort mehr Storage verbraucht.	• Um die Kapazität anzuzeigen, platzieren Sie den Cursor über die verfügbaren und genutzten Kapazitätsbereiche des Diagramms. • Um Kapazitätstrends über einen Datumsbereich anzuzeigen, klicken Sie auf das Diagrammsymbol Für das Gesamtraster oder einen Standort im Datacenter. • Um Details anzuzeigen, wählen Sie **Knoten**. Anschließend können Sie die Registerkarte „Storage“ für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen.	• "Anzeigen der Registerkarte „Speicher“" • "Monitoring der Storage-Kapazität"

Bereich „Information Lifecycle Management“ (ILM)

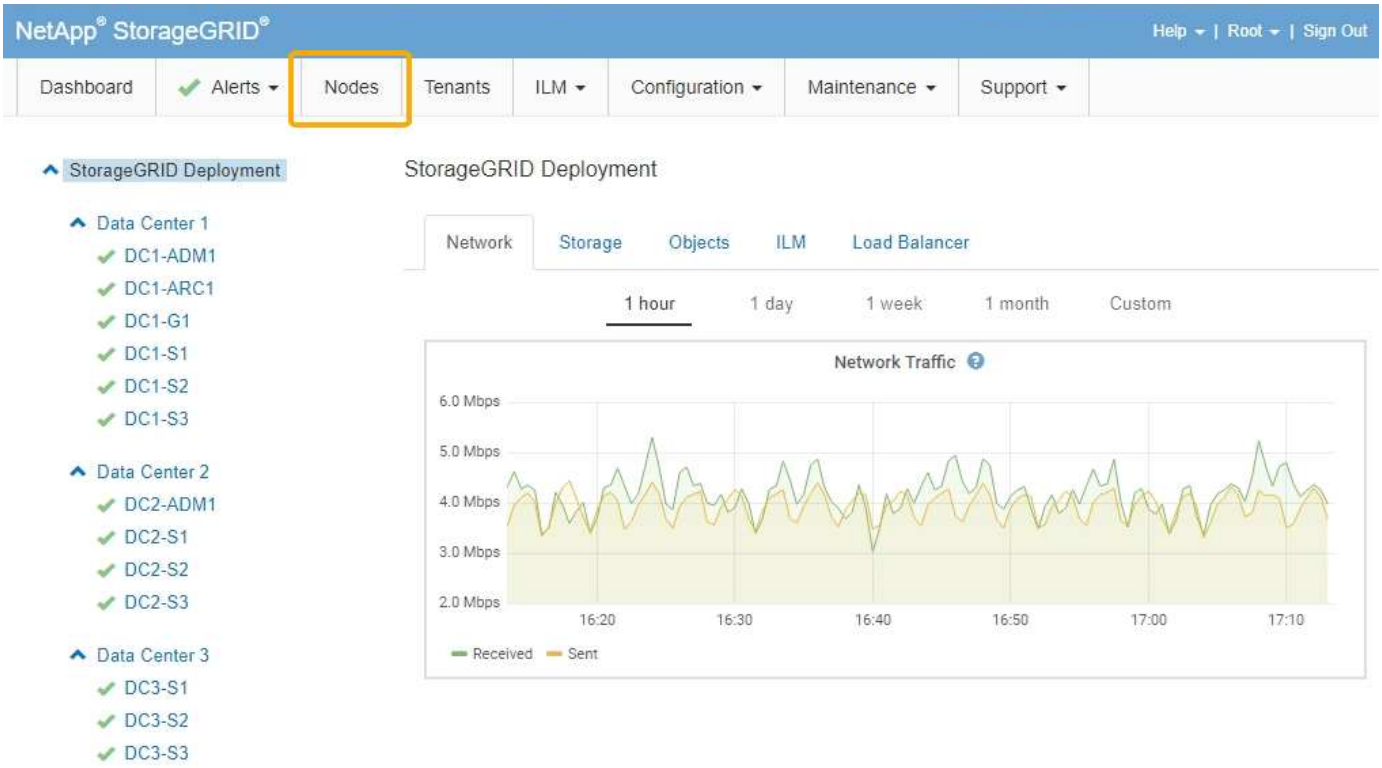
Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die aktuellen ILM-Vorgänge und ILM-Warteschlangen für das System an. Sie können diese Informationen für das Monitoring der Arbeitsbelastung Ihres Systems verwenden. • **Ausstehend - Client**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aus Client-Operationen warten (zum Beispiel Aufnahme). • **Ausstehend - Evaluation Rate**: Die aktuelle Rate, mit der Objekte ausgewertet werden, entspricht der ILM-Richtlinie im Grid. • **Scan Period - Estimated**: Die geschätzte Zeit, um einen vollständigen ILM-Scan aller Objekte abzuschließen. **Hinweis:** Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde.	• Um Details anzuzeigen, wählen Sie **Knoten**. Anschließend können Sie die ILM-Registerkarte für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen. • Um die vorhandenen ILM-Regeln anzuzeigen, wählen Sie **ILM** > **Regeln**. • Um die vorhandenen ILM-Richtlinien anzuzeigen, wählen Sie **ILM** > **Richtlinien**.	• "Anzeigen der Registerkarte ILM" • "StorageGRID verwalten".

Bereich „Protokollbetrieb“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die Anzahl der protokollspezifischen Vorgänge (S3 und Swift) an, die vom System durchgeführt werden. Sie können diese Informationen nutzen, um die Workloads und die Effizienz Ihres Systems zu überwachen. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.	• Um Details anzuzeigen, wählen Sie **Knoten**. Anschließend können Sie die Registerkarte Objekte für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen. • Um Trends über einen Datumsbereich anzuzeigen, klicken Sie auf das Diagrammsymbol Rechts neben der S3- oder Swift-Protokollrate.	• "Anzeigen der Registerkarte Objekte" • "S3 verwenden" • "Verwenden Sie Swift"

Anzeigen der Seite Knoten

Wenn Sie detailliertere Informationen über Ihr StorageGRID-System als das Dashboard erhalten, können Sie auf der Seite Nodes Metriken für das gesamte Grid, jeden Standort im Raster und jeden Node an einem Standort anzeigen.



In der Baumansicht links sehen Sie alle Standorte und alle Knoten in Ihrem StorageGRID-System. Das Symbol für jeden Knoten gibt an, ob der Knoten verbunden ist oder ob aktive Warnmeldungen vorliegen.

Symbole für Verbindungsstatus

Wenn ein Knoten von der Tabelle getrennt wird, zeigt die Strukturansicht ein blaues oder graues Verbindungssymbol an, nicht das Symbol für die zugrunde liegenden Warnungen.

- **Nicht verbunden - Unbekannt**: Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom 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.

- **Nicht verbunden - Administrativ 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.

Warnungssymbole

Wenn ein Knoten mit dem Raster verbunden ist, wird in der Strukturansicht eines der folgenden Symbole angezeigt, je nachdem, ob aktuelle Warnmeldungen für den Knoten vorhanden sind.

- * 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 sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
- **Normal**: Es sind keine Alarme aktiv, und der Knoten ist mit dem Raster verbunden.

Anzeigen von Details zu einem System, Standort oder Node

Um die verfügbaren Informationen anzuzeigen, klicken Sie auf die entsprechenden Links auf der linken Seite, wie folgt:

- Wählen Sie den Grid-Namen aus, um eine Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen. (Der Screenshot zeigt ein System mit dem Namen „StorageGRID Deployment“.)
- 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.

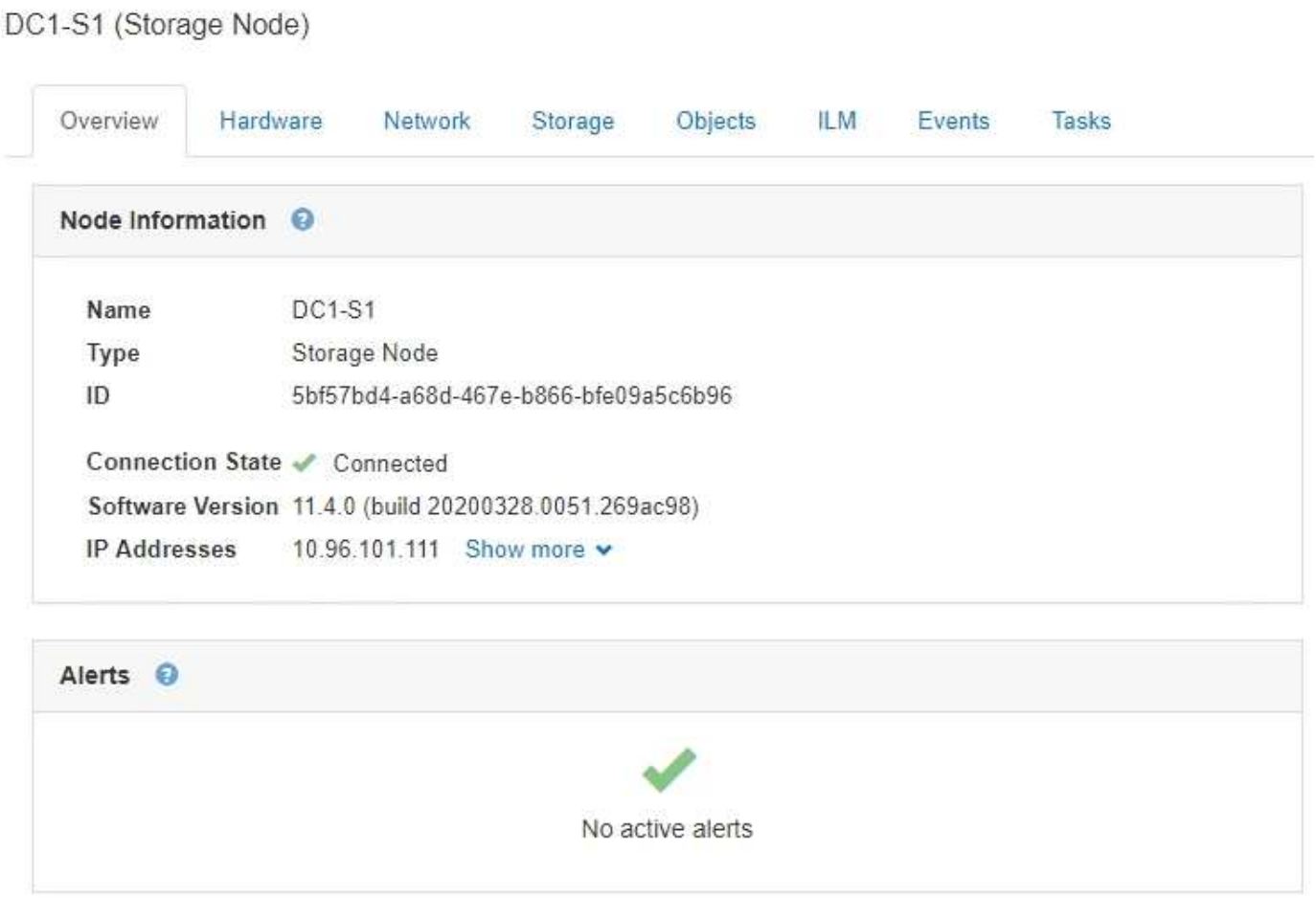
Anzeigen der Registerkarte Übersicht

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 auf der Registerkarte Übersicht werden grundlegende Informationen zum Grid-Knoten angezeigt.



Die Übersichtsinformationen für einen Knoten umfassen Folgendes:

- **Name**: Der Hostname, der dem Knoten zugewiesen und im Grid Manager angezeigt wird.
- **Typ**: Der Node-Typ - Admin-Node, Storage Node, Gateway-Node oder Archiv-Node.
- **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.
  - **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.

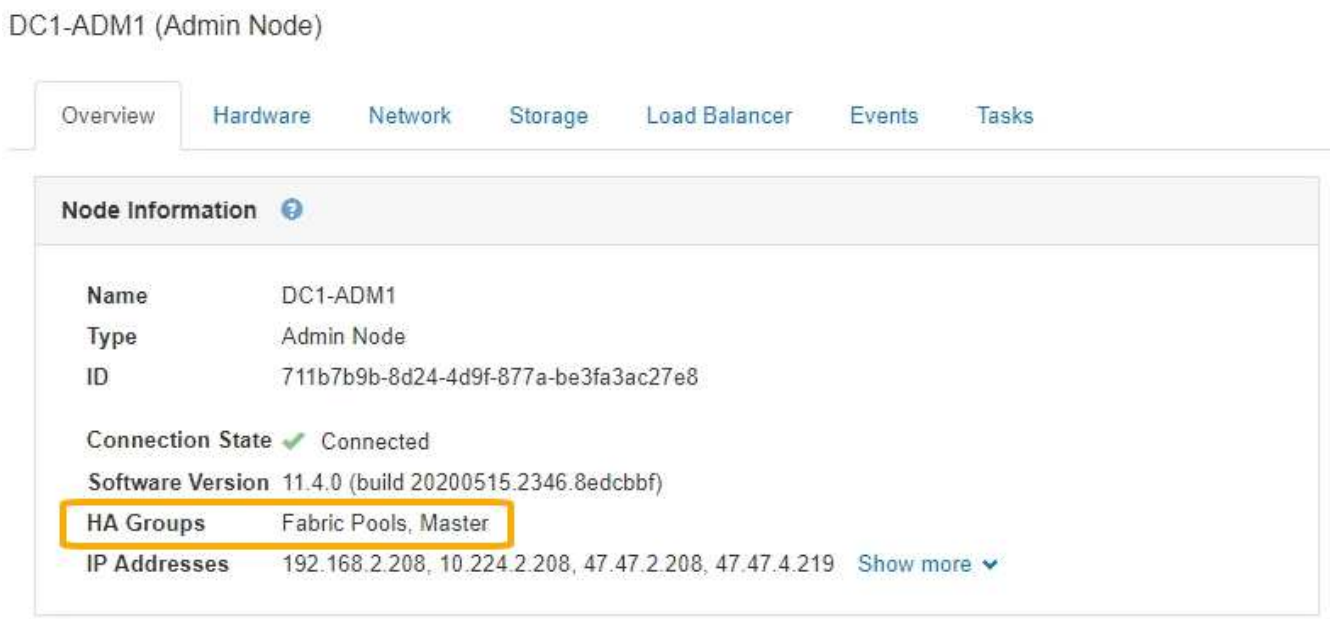
    Ein Node wird möglicherweise während des verwalteten Herunterfahrens als „Unbekannt“ angezeigt. In diesen Fällen können Sie den Status Unbekannt ignorieren.

  - **Nicht verbunden - Administrativ 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.

- **Software-Version**: Die Version von StorageGRID, die auf dem Knoten installiert ist.
- **HA-Gruppen**: Nur für Admin-Node und Gateway-Knoten. Wird angezeigt, ob eine Netzwerkschnittstelle auf dem Knoten in einer Hochverfügbarkeitsgruppe enthalten ist und ob diese Schnittstelle der Master oder der Backup ist.



- **IP-Adressen**: Die IP-Adressen des Knotens. Klicken Sie auf **Mehr anzeigen**, um die IPv4- und IPv6-Adressen und Schnittstellenzuordnungen des Knotens anzuzeigen:
  - Eth0: Grid Network
  - Eth1: Admin Network
  - Eth2: Client-Netzwerk

Meldungen

Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle Warnmeldungen aufgeführt, die derzeit diesen Knoten betreffen, die nicht stummgeschaltet wurden. Klicken Sie auf den Namen der Warnmeldung, um weitere Details und empfohlene Aktionen anzuzeigen.

Verwandte Informationen

"Monitoring der Verbindungsstatus der Nodes"

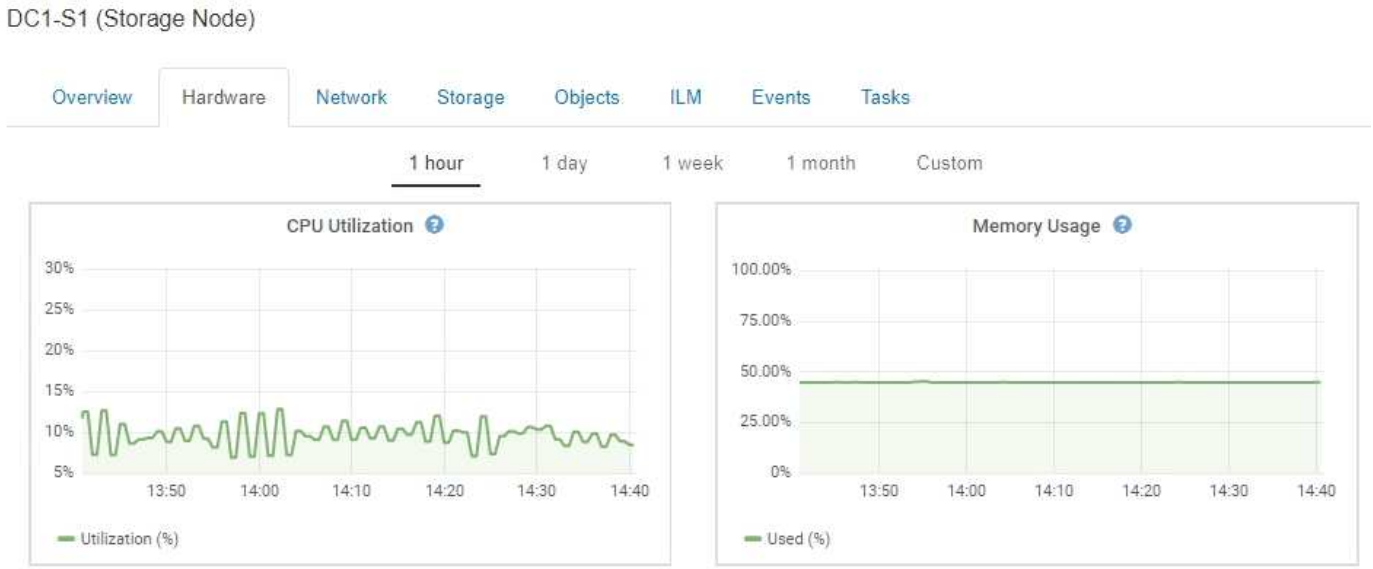
"Anzeigen aktueller Meldungen"

"Anzeigen einer bestimmten Meldung"

Anzeigen der Registerkarte Hardware

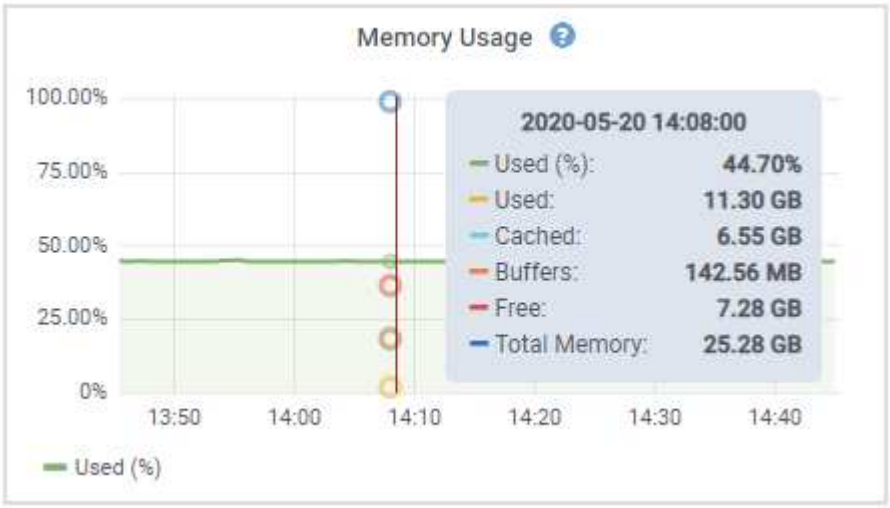
Auf der Registerkarte Hardware werden für jeden Node CPU-Auslastung und Arbeitsspeicherauslastung sowie zusätzliche Hardware-Informationen über Appliances angezeigt.

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.

Wenn Sie Details zur CPU-Auslastung und Arbeitsspeicherauslastung anzeigen möchten, bewegen Sie den Mauszeiger über jedes Diagramm.



Wenn der Knoten ein Appliance-Node ist, enthält diese Registerkarte auch einen Abschnitt mit weiteren Informationen zur Appliance-Hardware.

Verwandte Informationen

"Anzeigen von Informationen zu Appliance-Speicherknoten"

"Anzeigen von Informationen zu Appliance Admin Nodes und Gateway Nodes"

Registerkarte Netzwerk anzeigen

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.

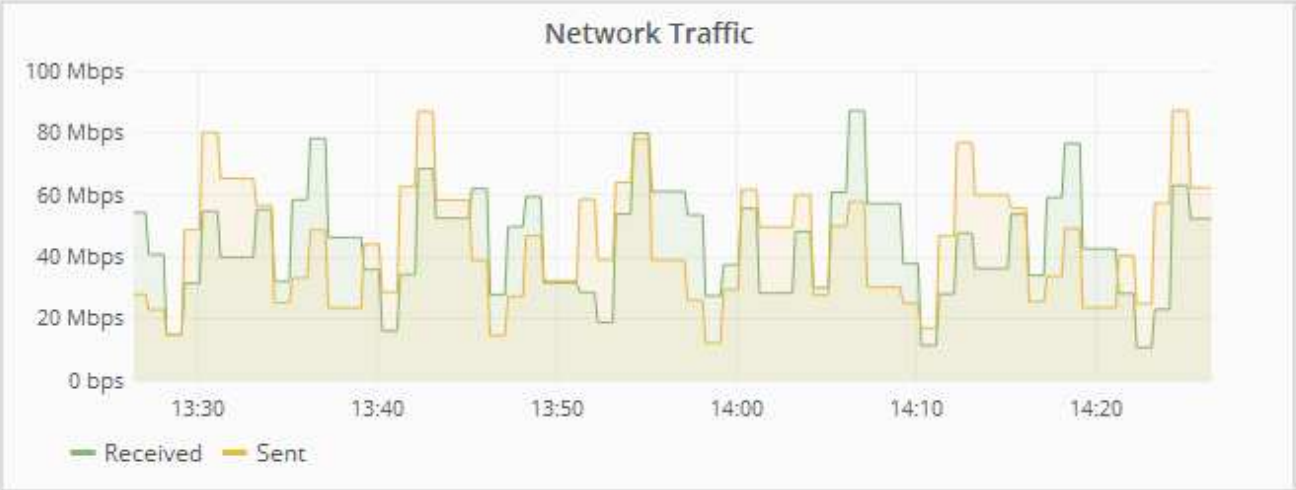
Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, mit dem Sie Datum und Zeitbereiche festlegen können.

Für Knoten bietet die Tabelle Netzwerkschnittstellen Informationen zu den physischen Netzwerkports jedes Node. Die Tabelle Netzwerkkommunikation enthält Details zu den Empfangs- und Übertragungsvorgängen jedes Knotens sowie zu den vom Treiber gemeldeten Fehlerzählern.

DC1-S1-226 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events

1 hour | 1 day | 1 week | 1 month | 1 year | Custom



Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	00:50:56:A8:2A:75	10 Gigabit	Full	Off	Up

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	738.858 GB	904,587,345	0	14,340	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	677.555 GB	465,715,998	0	0	0	0

Verwandte Informationen

"Monitoring von Netzwerkverbindungen und Performance"

Anzeigen der Registerkarte „Speicher“

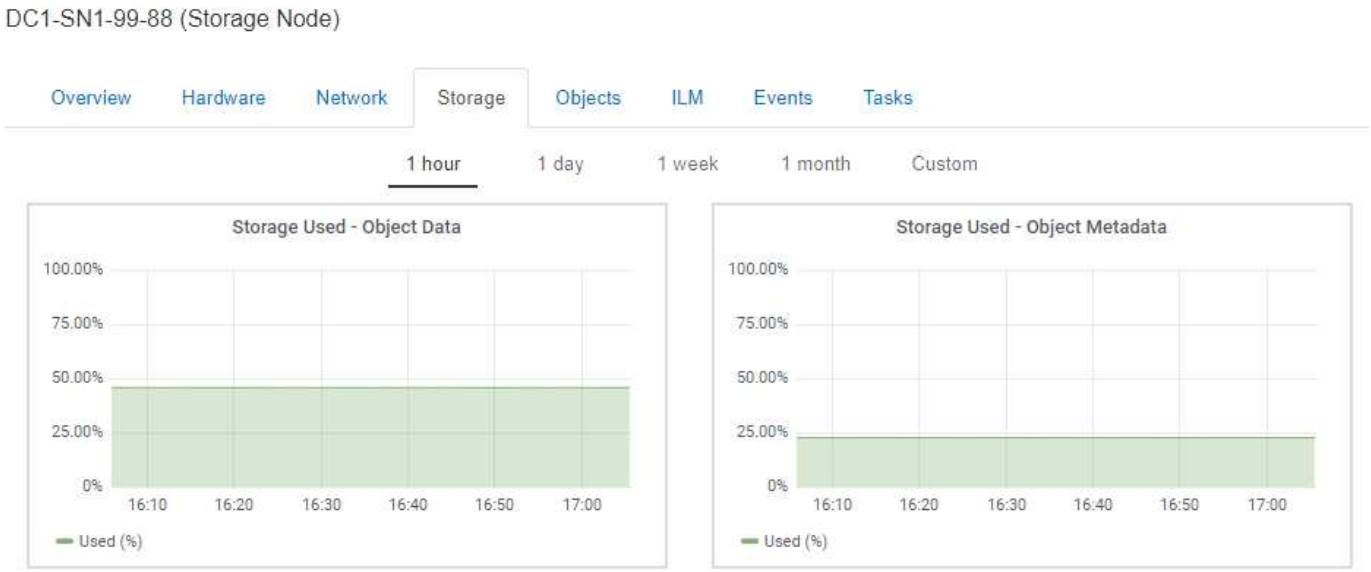
Die Registerkarte „Storage“ fasst Storage-Verfügbarkeit und andere Storage-Metriken zusammen.

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.

Die Gesamtwerte für einen Standort oder das Grid enthalten keine Nodes, die mindestens fünf Minuten lang keine Kennzahlen enthalten, z. B. Offline-Nodes.



Festplattengeräte, Volumes und Objektspeichertabellen

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	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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

"Überwachung der Storage-Kapazität für das gesamte Grid"

"Monitoring der Storage-Kapazität für jeden Storage-Node"

"Monitoring der Objekt-Metadaten-Kapazität für jeden Storage Node"

Anzeigen der Registerkarte Ereignisse

Auf der Registerkarte Ereignisse wird die Anzahl der Systemfehler oder Fehlerereignisse für einen Node angezeigt, einschließlich der Fehler, z. B. Netzwerkfehler.

Die Registerkarte Ereignisse wird für alle Nodes angezeigt.

Wenn Probleme mit einem bestimmten Knoten auftreten, erfahren Sie auf der Registerkarte Ereignisse mehr über das Problem. Der technische Support kann auch die Informationen auf der Registerkarte Ereignisse verwenden, um Ihnen bei der Fehlerbehebung zu helfen.

Sie können diese Aufgaben über die Registerkarte Ereignisse ausführen:

- Verwenden Sie die Informationen aus dem Feld **Letztes Ereignis** oben in der Tabelle, um festzustellen, welches Ereignis zuletzt aufgetreten ist.
- Klicken Sie auf das Diagrammsymbol Für ein bestimmtes Ereignis, um zu sehen, wann dieses Ereignis im Laufe der Zeit aufgetreten ist.

- Zurücksetzen der Ereignisanzahl auf Null nach Behebung von Problemen.

Verwandte Informationen

"Monitoring von Ereignissen"

"Anzeigen von Diagrammen und Diagrammen"

"Ereignisanzahl wird zurückgesetzt"

Verwenden der Registerkarte Task zum Neustart eines Grid-Knotens

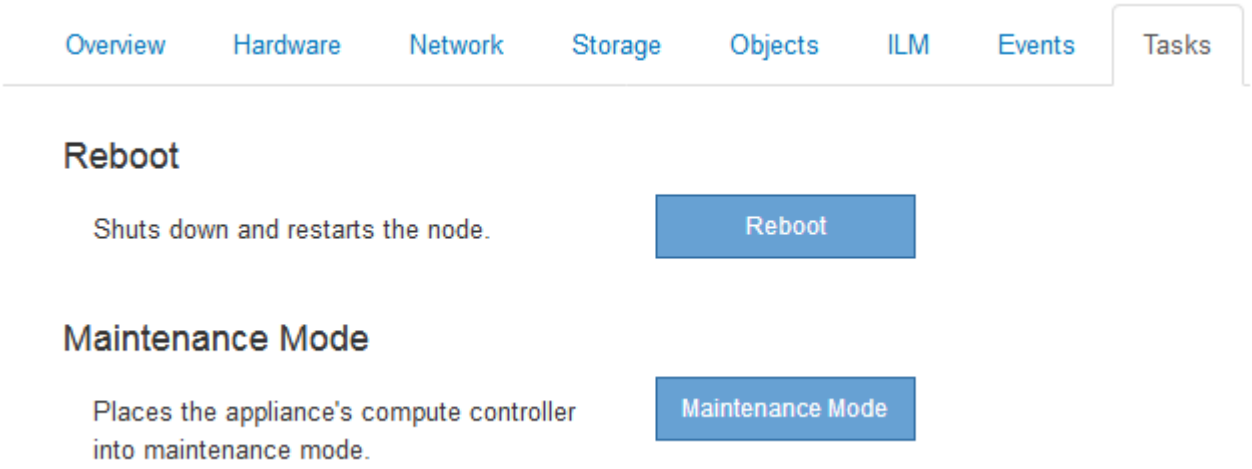
Auf der Registerkarte Task können Sie den ausgewählten Knoten neu starten. Die Registerkarte Task wird für alle Knoten angezeigt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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

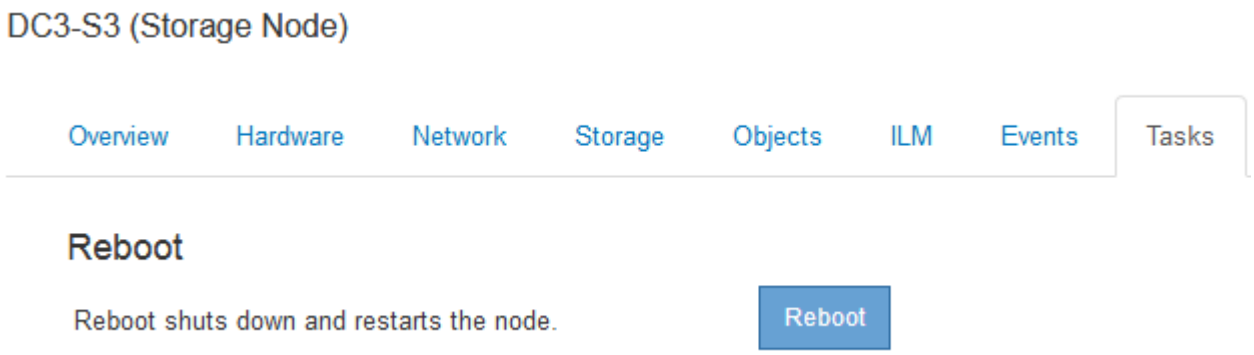
Sie den Node neu booten.

- 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 in der Installations- und Wartungsanleitung für das Gerät.

> Wenn Sie eine Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

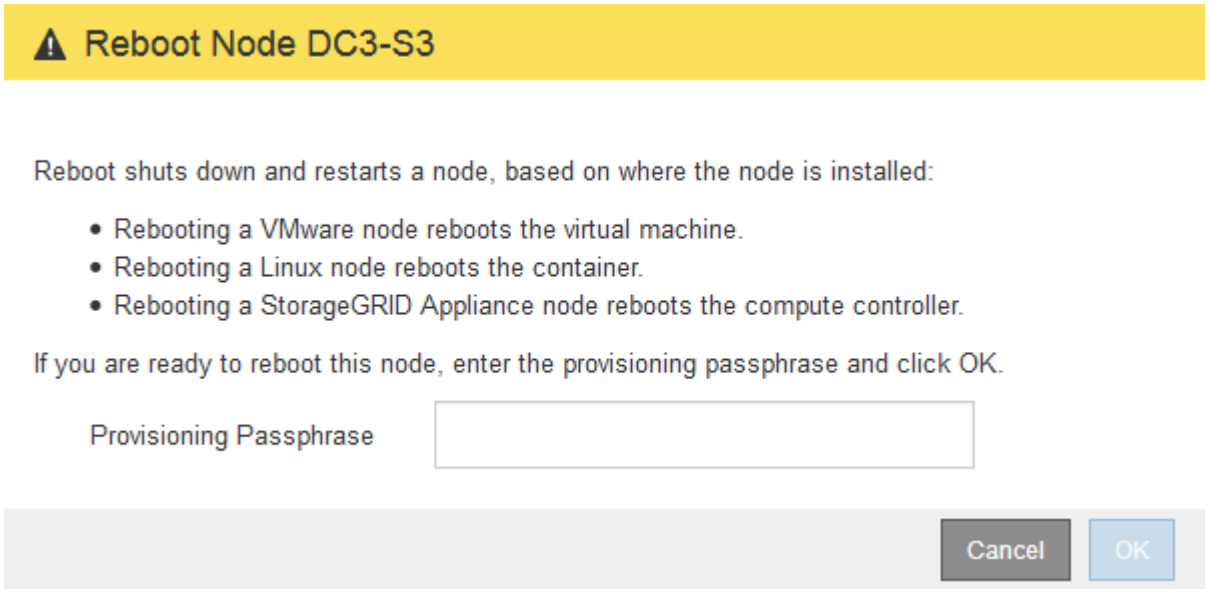
Schritte

1. Wählen Sie **Knoten**.
2. Wählen Sie den Grid-Node aus, den Sie neu booten möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.



4. Klicken Sie Auf **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 klicken Sie auf **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 Knoten angezeigt. Wenn alle Dienste wieder gestartet wurden, ändert sich das Symbol wieder in seine ursprüngliche Farbe.

Verwandte Informationen

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

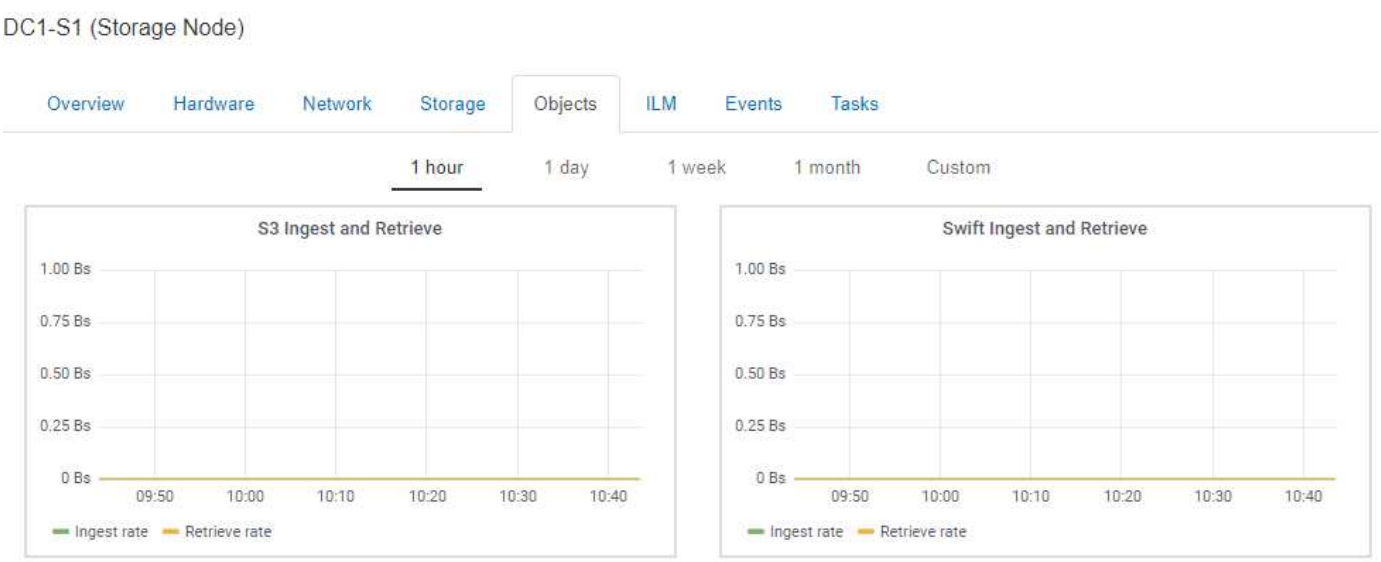
"SG5600 Storage Appliances"

"SG100 SG1000 Services-Appliances"

Anzeigen der Registerkarte Objekte

Die Registerkarte „Objekte“ bietet Informationen zur Aufnahme- und Abrufrate von S3 und Swift.

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.



Object Counts

Total Objects	0
Lost Objects	0
S3 Buckets and Swift Containers	0

Queries

Average Latency	5.74 milliseconds
Queries - Successful	12,403
Queries - Failed (timed-out)	0
Queries - Failed (consistency level unmet)	0

Verification

Status	No Errors
Rate Setting	Adaptive
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

Verwandte Informationen

"S3 verwenden"

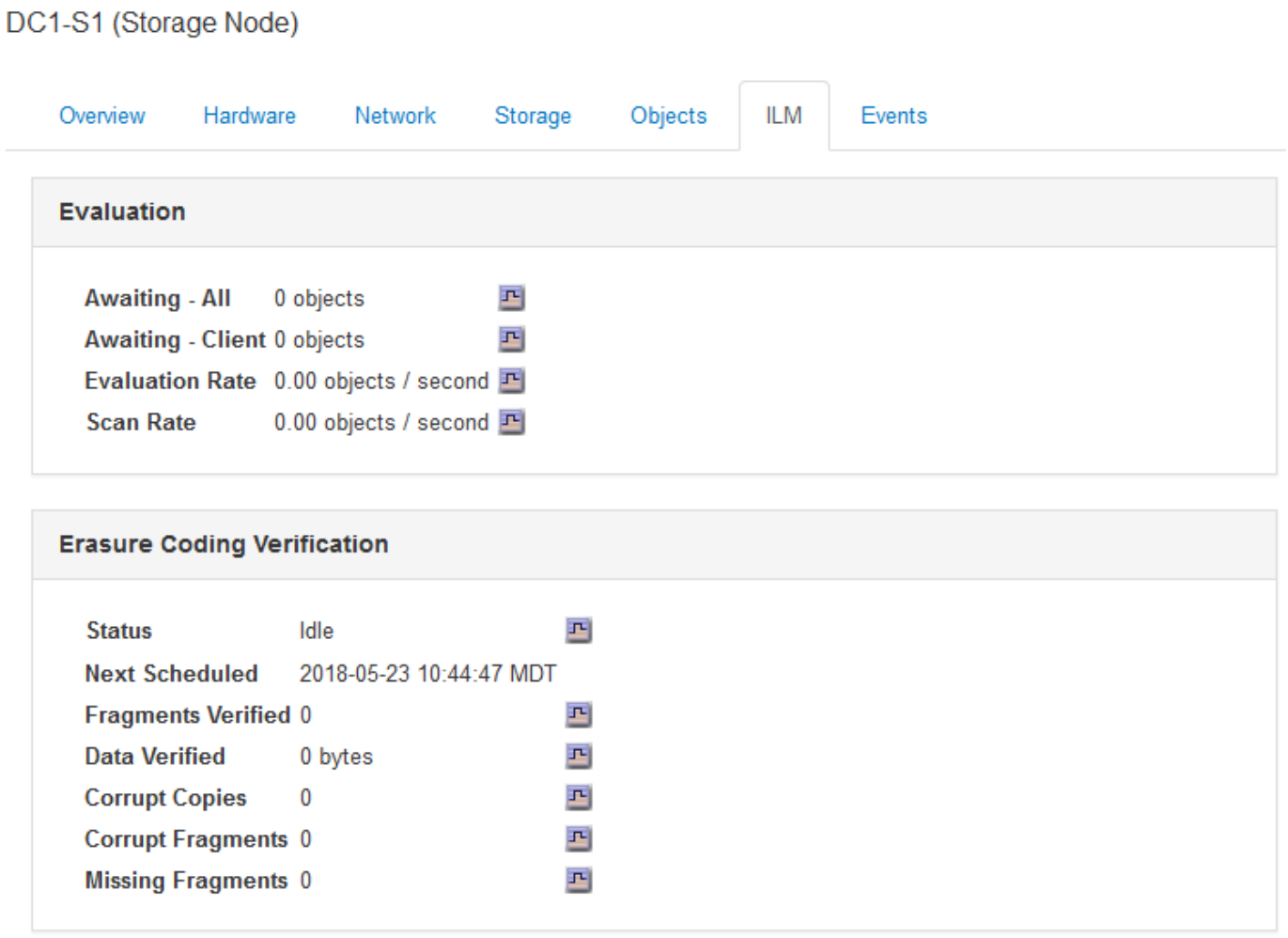
"Verwenden Sie Swift"

Anzeigen der Registerkarte ILM

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.



Verwandte Informationen

"Überwachung des Information Lifecycle Management"

"StorageGRID verwalten"

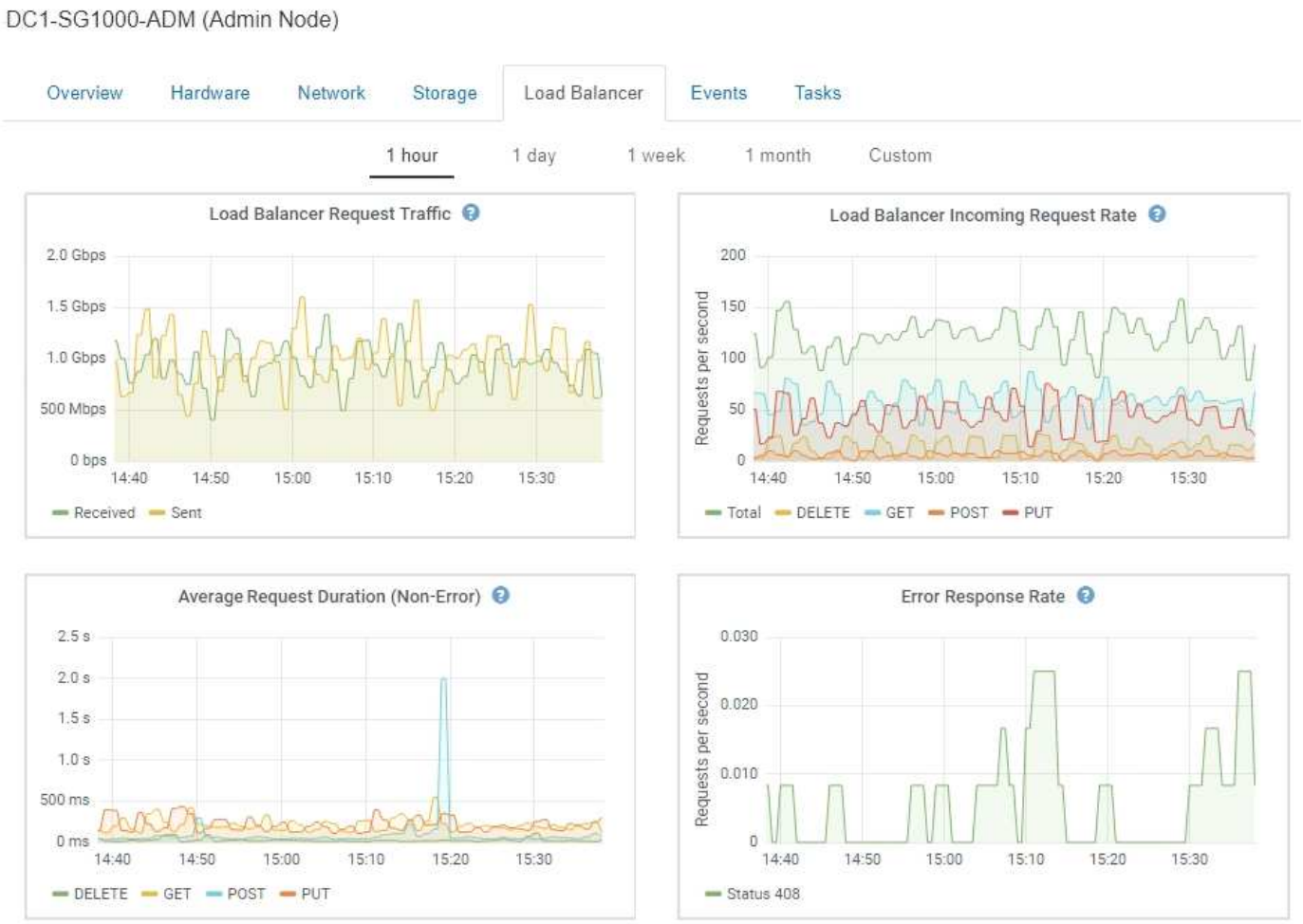
Anzeigen der Registerkarte Load Balancer

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.



Traffic Für Lastausgleichsanfragen

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 Für Den Lastausgleich Des Balancer

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 Anfragendauer (Ohne Fehler)

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.

Fehlerreaktionsrate

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"

Registerkarte Plattformdienste anzeigen

Die Registerkarte Platform Services enthält Informationen zu allen S3-Plattform-Servicevorgängen an einem Standort.

Die Registerkarte Platform Services 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-Plattformservices, einschließlich Details zur Fehlerbehebung, finden Sie in den Anweisungen für die Administration von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Anzeigen von Informationen zu Appliance-Speicherknoten

Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplattengeräte- und Netzwerkressourcen für jeden Appliance Storage Node aufgeführt. Außerdem können Sie den Arbeitsspeicher, die Storage-Hardware, die

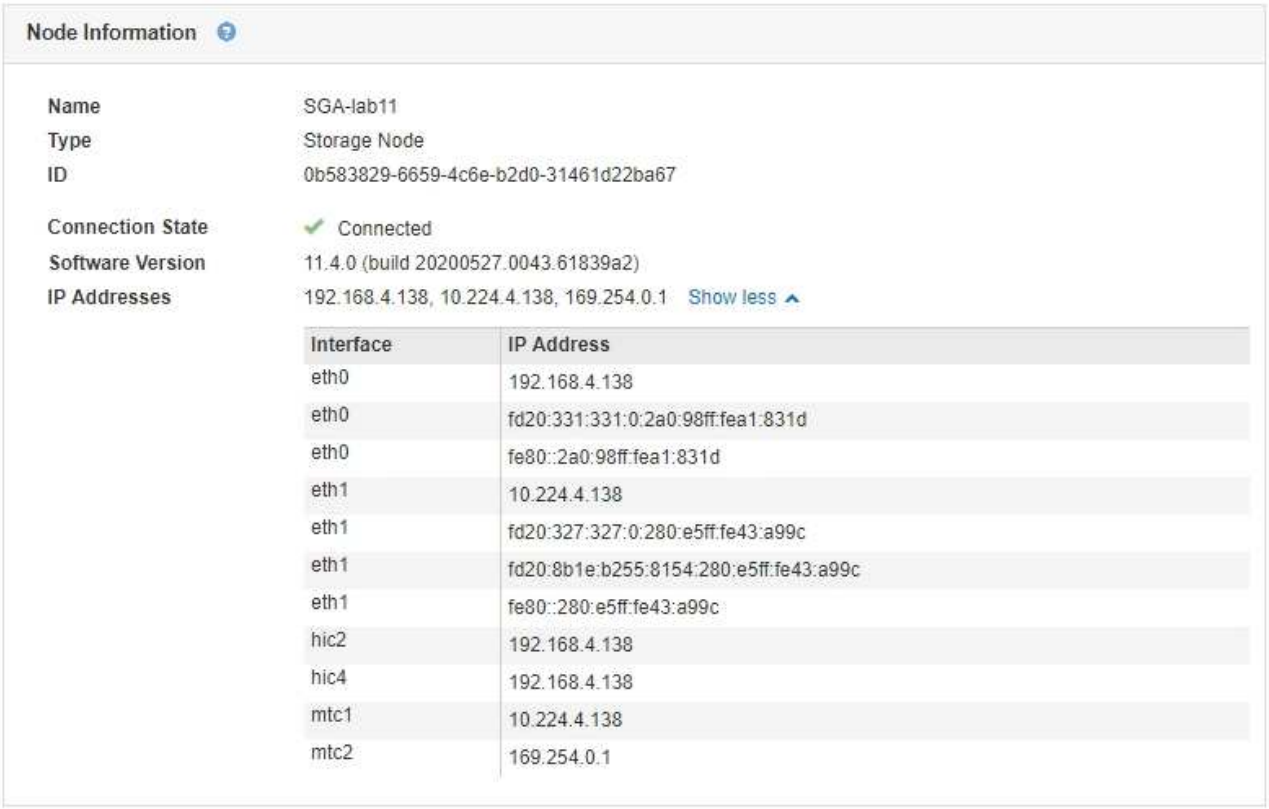
Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen und empfangen und übertragen Daten.

Schritte

1. Wählen Sie auf der Seite Knoten einen Appliance-Speicherknoten aus.
2. Wählen Sie **Übersicht**.

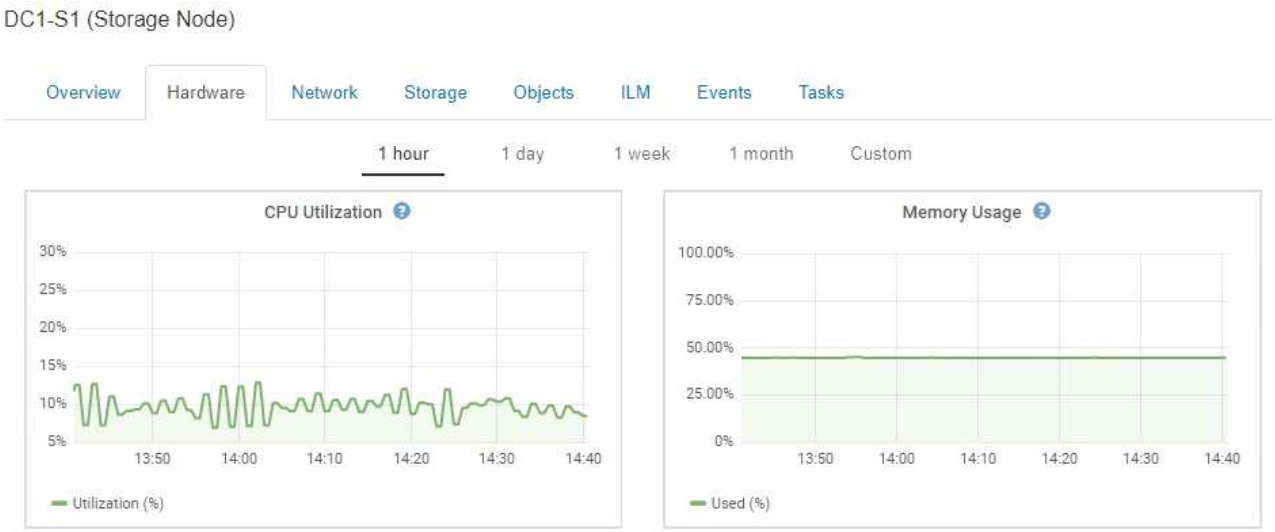
   In der Tabelle Node Information auf der Registerkarte Übersicht werden die ID und der Name des Node, der Node-Typ, die installierte Softwareversion und die dem Node zugeordneten IP-Adressen angezeigt. Die Spalte Interface enthält den Namen der Schnittstelle wie folgt:

   - **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, die mit dem StorageGRID Admin Network (eth1) verbunden oder kalibriert und verbunden werden können.



3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.

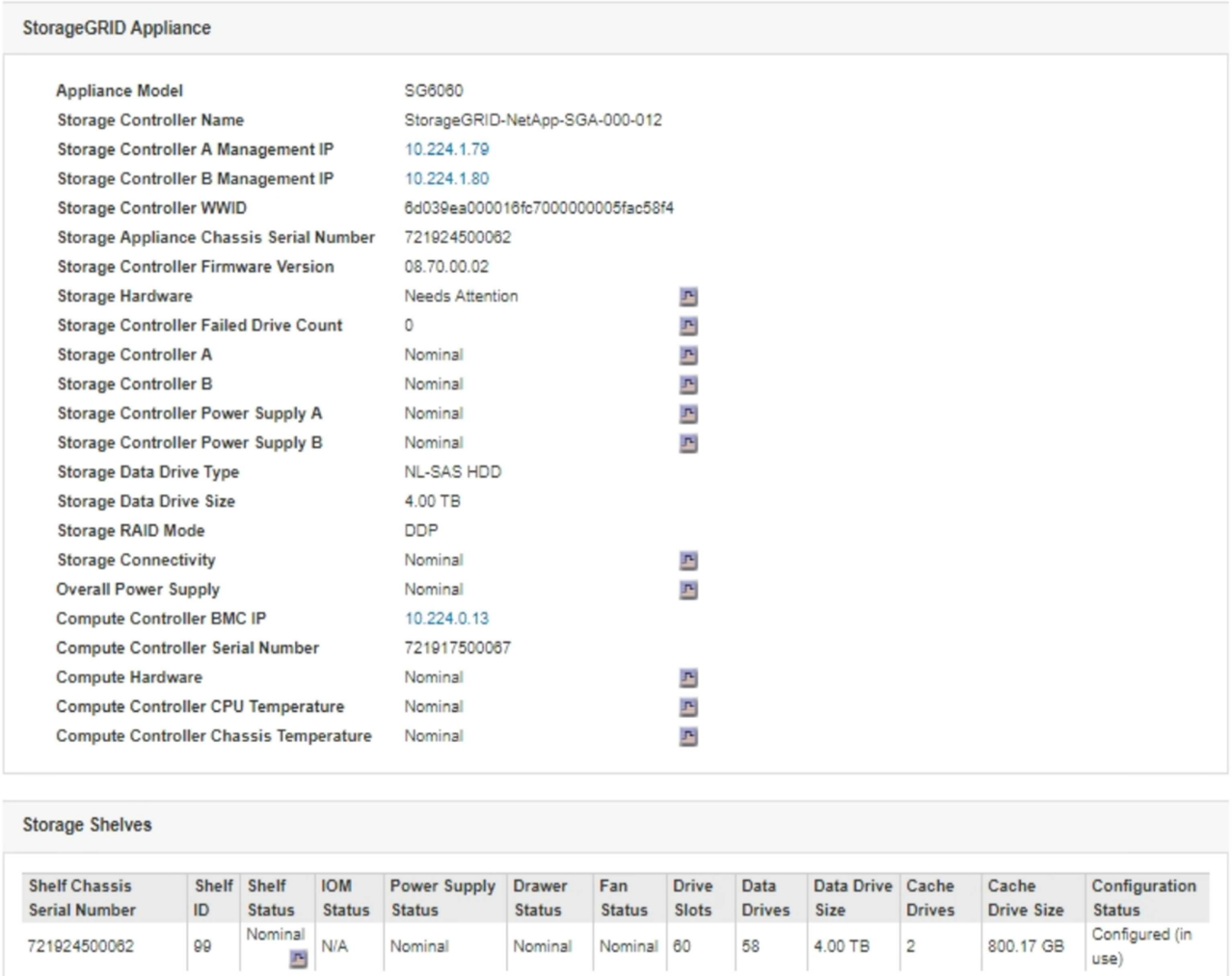
   a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren 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 Compute Hardware, 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.



Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer dieser StorageGRID Appliance, dargestellt in der SANtricity Software.
Storage Controller-Name	Der Name dieser in der SANtricity Software angezeigten StorageGRID Appliance.
Storage Controller A Management-IP	IP-Adresse für Management Port 1 auf Storage Controller A Sie verwenden diese IP für den Zugriff auf die SANtricity Software zur Fehlerbehebung bei Speicherproblemen.
Storage Controller B Management-IP	IP-Adresse für Management Port 1 auf Storage Controller B Sie verwenden diese IP für den Zugriff auf die SANtricity Software zur Fehlerbehebung bei Speicherproblemen. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B

Feld in der Appliance-Tabelle	Beschreibung
WWID des Storage Controller	Die weltweite Kennung des Storage-Controllers in der SANtricity Software.
Seriennummer Des Storage Appliance Chassis	Die Seriennummer des Gehäuses des Geräts.
Firmware-Version Des Speicher-Controllers	Die Version der Firmware auf dem Storage Controller für dieses Gerät.
Storage-Hardware	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. Wenn der Status „`Anforderungen einer Warnung erfüllt,`“ zunächst den Storage Controller mithilfe der SANtricity Software prüfen. Stellen Sie dann sicher, dass keine weiteren Alarme vorhanden sind, die für den Rechencontroller gelten.
Anzahl Ausgefallener Speicher-Controller-Laufwerke	Anzahl an Laufwerken, die nicht optimal sind.
Storage Controller A	Der Status von Speicher-Controller A.
Storage Controller B	Der Status von Storage Controller B. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B
Netzteil A für Speichercontroller	Der Status von Netzteil A für den Storage Controller.
Speicher-Controller-Netzteil B	Der Status von Netzteil B für den Speicher-Controller.
Typ Des Storage-Datenlaufwerks	Die Art der Laufwerke in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe Der Speicherdatenlaufwerke	Gesamtkapazität einschließlich aller Datenlaufwerke in der Appliance.
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.
Storage-Konnektivität	Der Status der Storage-Konnektivität.

Feld in der Appliance-Tabelle	Beschreibung
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 Appliance-Modelle 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 keine separate Computing-Hardware und Speicherhardware besitzen.
CPU-Temperatur für Compute Controller	Der Temperaturstatus der CPU des Compute-Controllers.
Temperatur Im Computing-Controller-Chassis	Der Temperaturstatus des Compute-Controllers.

+

Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Seriennummer Des Shelf-Chassis	Die Seriennummer für das Storage Shelf-Chassis.
Shelf-ID	Die numerische Kennung für das Storage-Shelf. • 99: Storage Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf **Hinweis:** Erweiterungseinschübe gelten nur für das SG6060.
Shelf-Status	Der Gesamtstatus des Storage Shelf.
IOM-Status	Der Status der ein-/Ausgangsmodule (IOMs) in beliebigen Erweiterungs-Shelfs. K. A., wenn es sich nicht um ein Erweiterungs-Shelf handelt

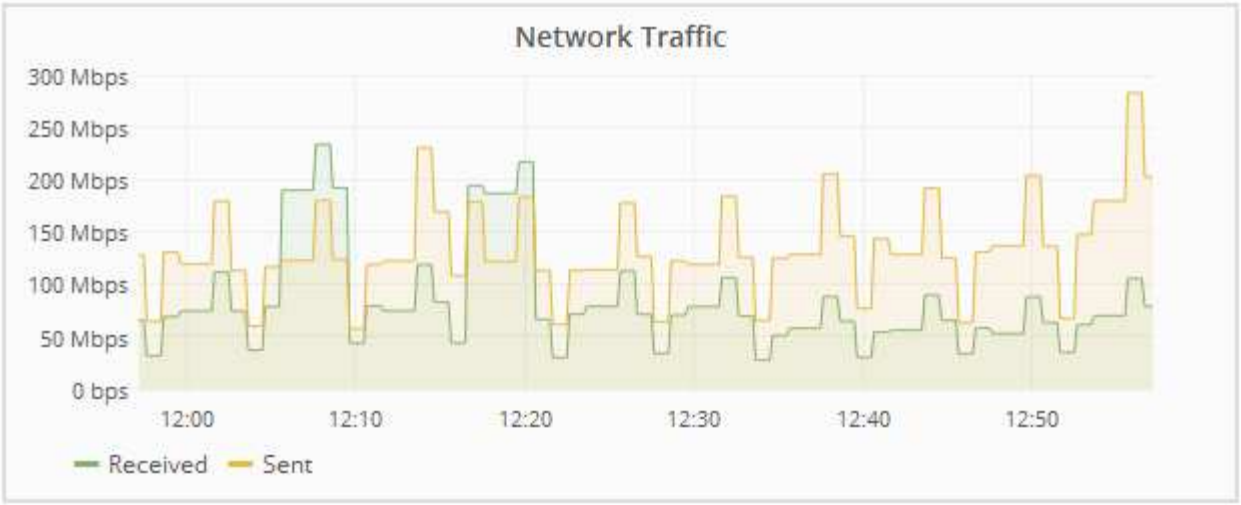
Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Netzteilstatus	Der Gesamtstatus der Netzteile für das Storage Shelf.
Status Der Schublade	Der Zustand der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Lüfter im Storage Shelf.
Laufwerksteckplätze	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.

4. 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.

5. Wählen Sie **Netzwerk**, um Informationen für jedes Netzwerk anzuzeigen.

   Das Diagramm „Netzwerkverkehr“ bietet eine Zusammenfassung des gesamten Netzwerkverkehr.



a. Lesen Sie den Abschnitt Netzwerkschnittstellen.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	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

Verbindungsmodus	Bond-Modus	Einzelne HIC-Verbindungsgeschwindigkeit (Schluck1, 2, Schluck3, Schluck4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0,eth2)
Fest	LACP	25	50
Fest	Aktiv/Backup	25	25
Aggregat	LACP	10	40
Fest	LACP	10	20
Fest	Aktiv/Backup	10	10

Weitere Informationen zur Konfiguration der 10/25-GbE-Ports finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

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

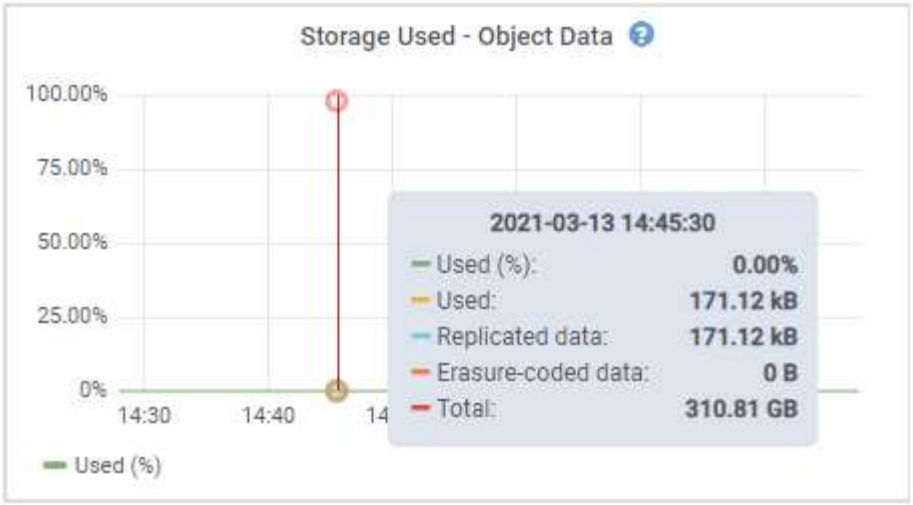
Receive

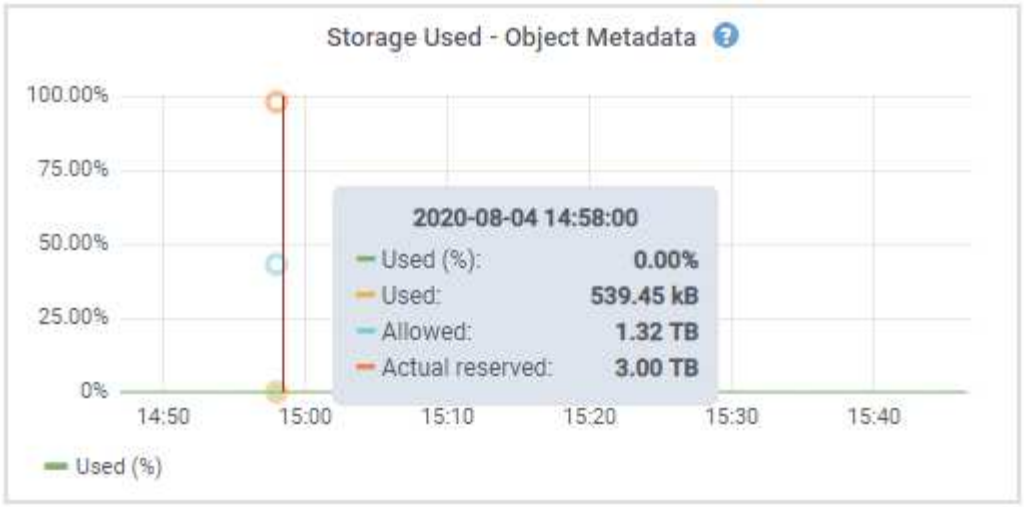
Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

6. 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.

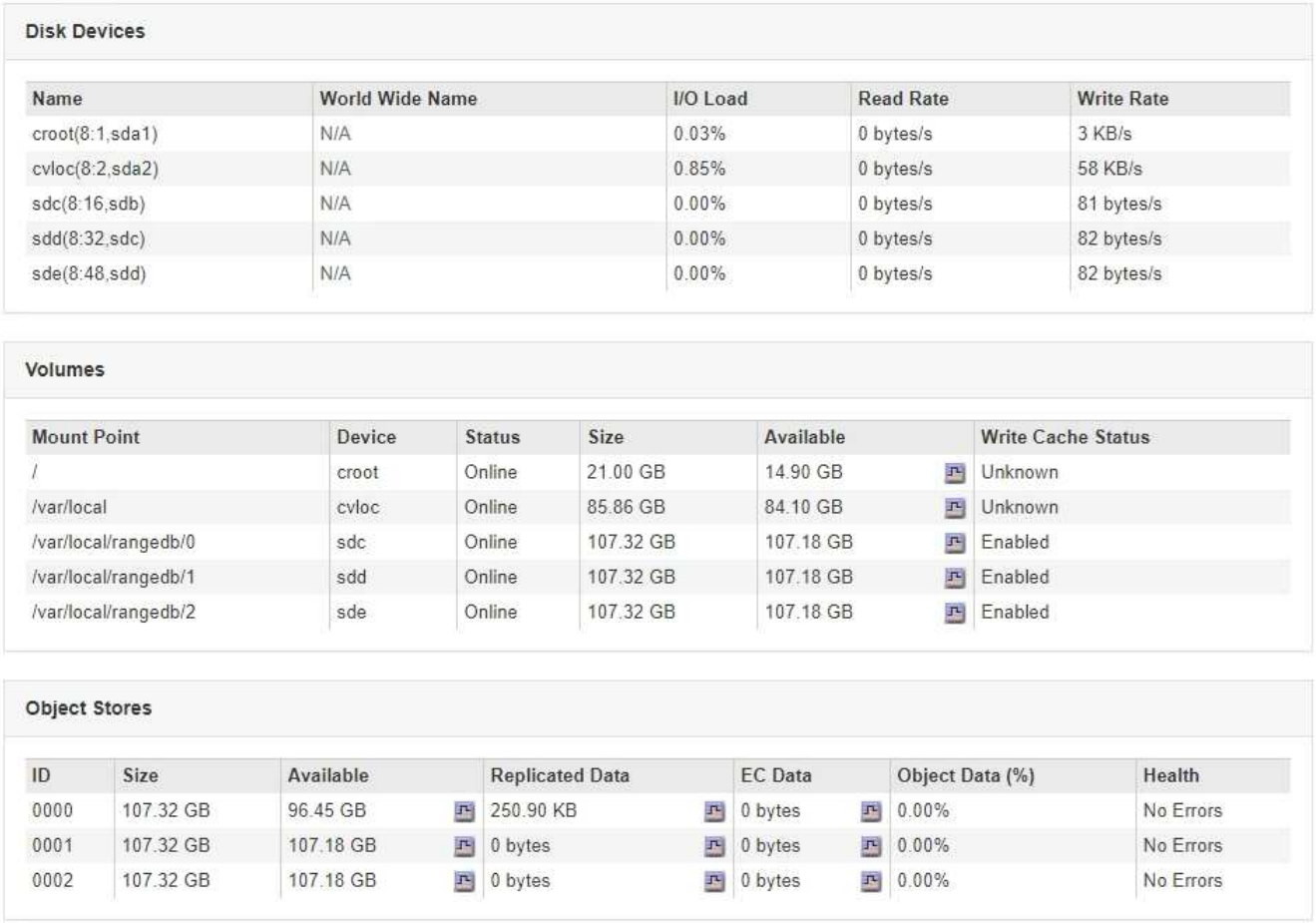




a. Blättern Sie nach unten, um die verfügbaren Speichermengen für jedes Volume und jeden Objektspeicher anzuzeigen.

   Der weltweite Name jeder Festplatte entspricht der World-Wide Identifier (WWID) des Volumes, die angezeigt wird, wenn Sie die standardmäßigen Volume-Eigenschaften in der SANtricity Software anzeigen (die Management-Software, die mit dem Storage Controller der Appliance verbunden ist).

   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	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Anzeigen der Registerkarte SANtricity System Manager

Über die Registerkarte „SANtricity System Manager“ können Sie auf SANtricity System Manager zugreifen, ohne den Managementport der Storage Appliance konfigurieren oder verbinden 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 für Storage-Appliance-Nodes angezeigt.

Mit SANtricity System Manager sind folgende Vorgänge möglich:

- Sie erhalten Performance-Daten wie Performance auf Storage-Array-Ebene, I/O-Latenz, CPU-Auslastung des Storage-Controllers und Durchsatz
- Überprüfen Sie den Status der Hardwarekomponenten
- Sie bieten Support-Funktionen, einschließlich Anzeige von Diagnosedaten und Konfiguration der E-Series AutoSupport

So konfigurieren Sie mit SANtricity System Manager einen Proxy für E-Series AutoSupport: Lesen Sie die Anweisungen in Administration StorageGRID.

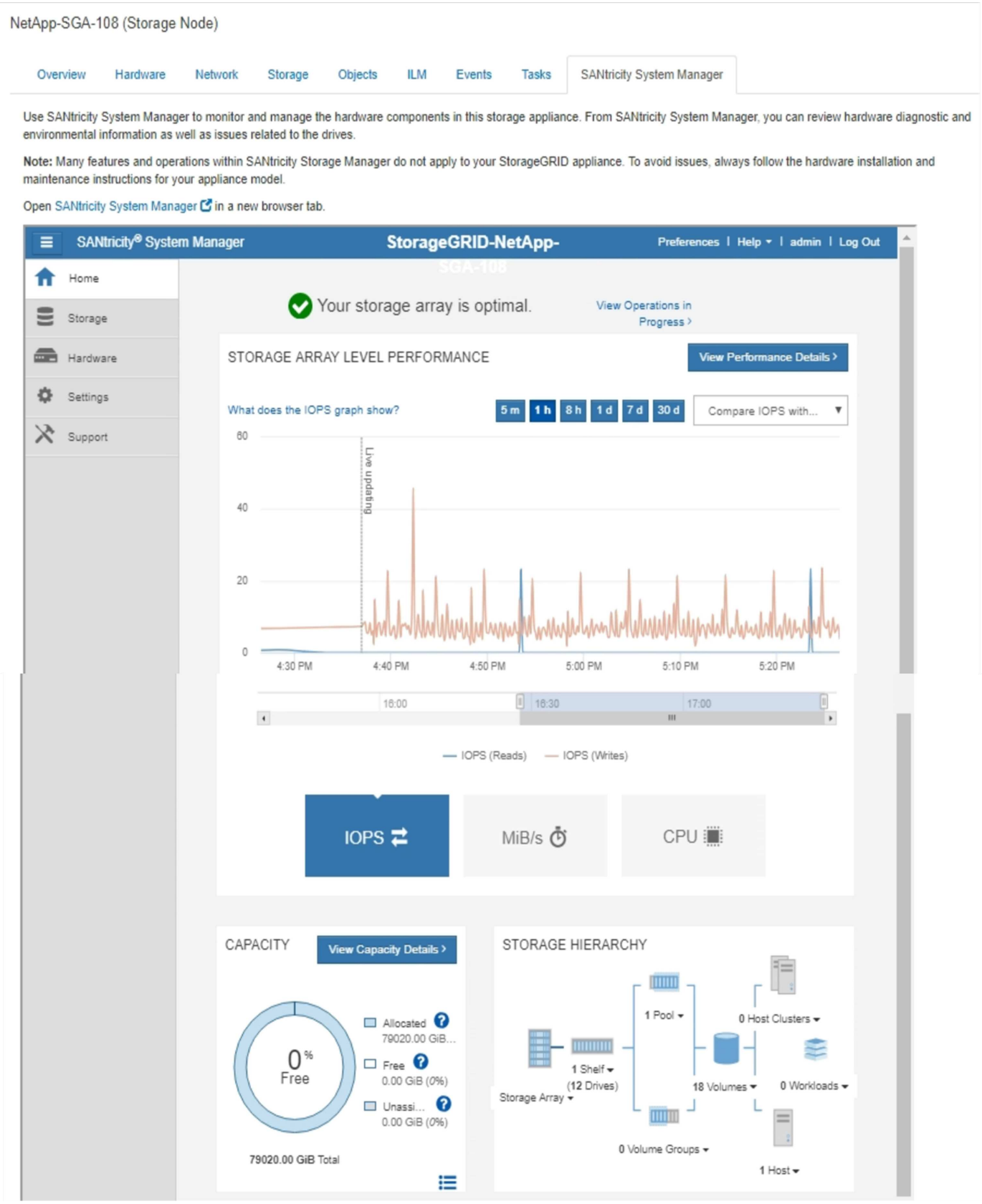
"StorageGRID verwalten"

Um über den Grid Manager auf SANtricity System Manager zuzugreifen, müssen Sie über die Administratorberechtigung für die Speicheranwendung oder über die Berechtigung für den Root-Zugriff 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, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Installations- und Wartungsanweisungen für Ihr Gerät.

Die Registerkarte zeigt die Startseite von SANtricity System Manager an



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 des Storage Array anzeigen möchten, halten Sie

den Mauszeiger über jedes Diagramm.

Weitere Informationen zum Anzeigen der Informationen, auf die über die Registerkarte SANtricity System Manager zugegriffen werden kann, finden Sie in den Informationen in "NetApp E-Series Systems Documentation Center"

Anzeigen von Informationen zu Appliance Admin Nodes und Gateway Nodes

Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplatten- und Netzwerkressourcen für jede Service-Appliance, die für einen Admin-Node oder einen 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**.

   In der Tabelle Node Information auf der Registerkarte Übersicht werden die ID und der Name des Node, der Node-Typ, die installierte Softwareversion und die dem Node zugeordneten IP-Adressen angezeigt. Die Spalte Interface enthält den Namen der Schnittstelle wie folgt:

   - **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, die mit dem StorageGRID Admin Network (eth1) verbunden oder kalibriert und verbunden werden können.

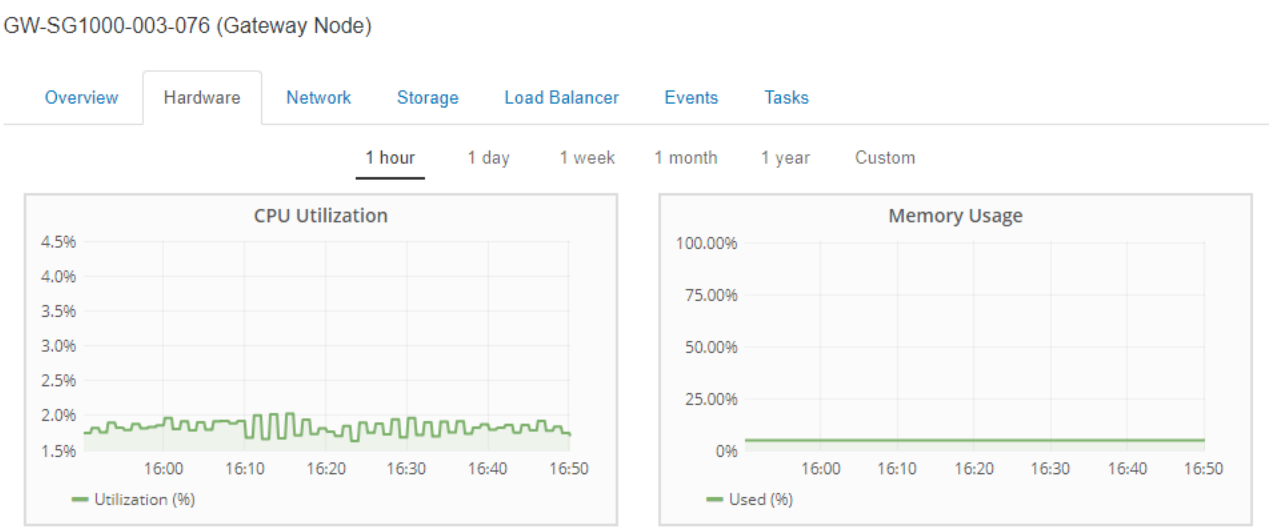
Node Information

ID	46702fe0-2bca-4097-8f61-f3fe6b22ed75
Name	GW-SG1000-003-076
Type	Gateway Node
Software Version	11.3.0 (build 20190708.2304.71ba19a)
IP Addresses	169.254.0.1, 172.16.3.76, 10.224.3.76, 47.47.3.76 Show less

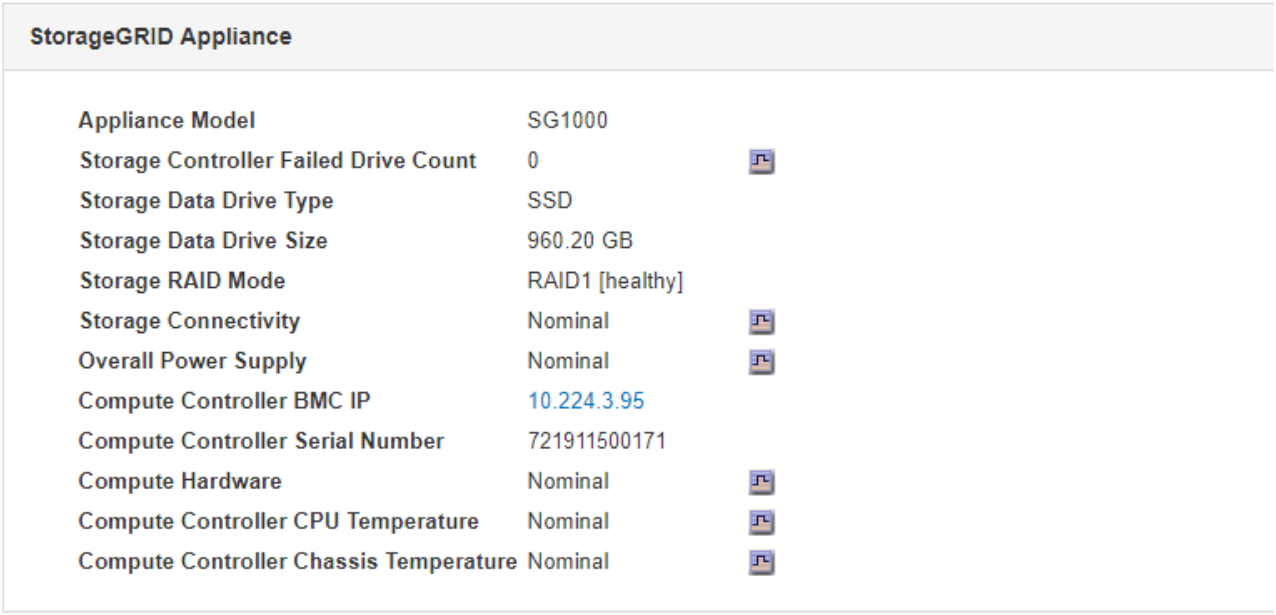
Interface	IP Address
adllb	fe80::c020:17ff:fe59:1cf3
adlli	169.254.0.1
adlli	fd20:327:327:0:408f:84ff:fe80:a9
adlli	fd20:8b1e:b255:8154:408f:84ff:fe80:a9
adlli	fe80::408f:84ff:fe80:a9
eth0	172.16.3.76
eth0	fd20:328:328:0:9a03:9bff:fe98:a272
eth0	fe80::9a03:9bff:fe98:a272
eth1	10.224.3.76
eth1	fd20:327:327:0:b6a9:fcff:fe08:4e49
eth1	fd20:8b1e:b255:8154:b6a9:fcff:fe08:4e49
eth1	fe80::b6a9:fcff:fe08:4e49
eth2	47.47.3.76
eth2	fd20:332:332:0:9a03:9bff:fe98:a272
eth2	fe80::9a03:9bff:fe98:a272
hic1	47.47.3.76
hic2	47.47.3.76
hic3	47.47.3.76
hic4	47.47.3.76
mtc1	10.224.3.76
mtc2	10.224.3.76

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.



Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance.
Anzahl Ausgefallener Speicher-Controller-Laufwerke	Anzahl an Laufwerken, die nicht optimal sind.
Typ Des Storage-Datenlaufwerks	Die Art der Laufwerke in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe Der Speicherdatenlaufwerke	Gesamtkapazität einschließlich aller Datenlaufwerke in der Appliance.

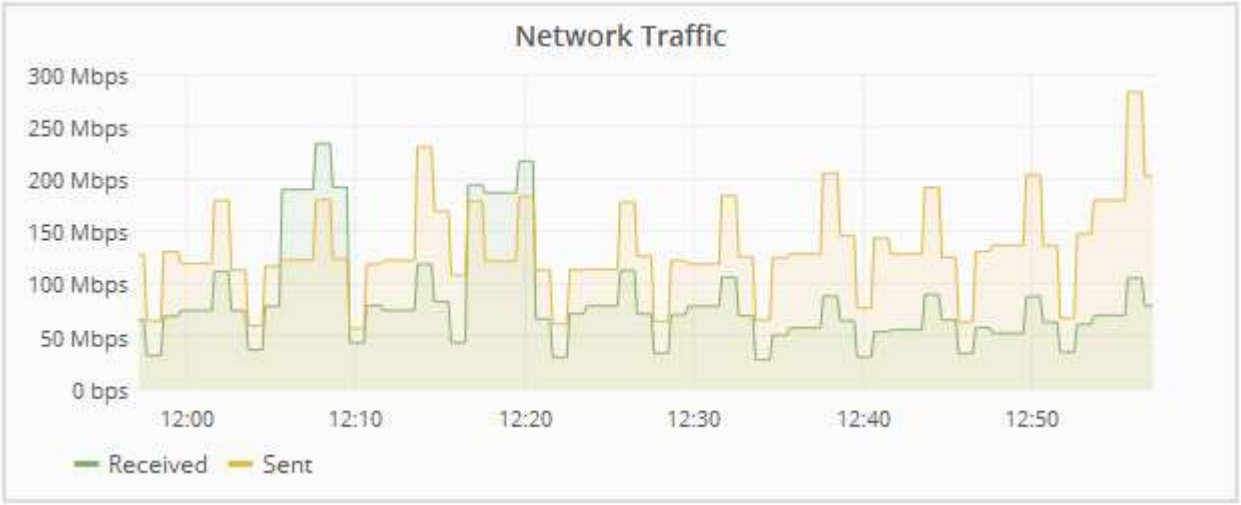
Feld in der Appliance-Tabelle	Beschreibung
Storage RAID-Modus	Der RAID-Modus für die Appliance.
Gesamtnetzteil	Der Status aller Netzteile im Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird nicht für Appliance-Modelle angezeigt, die keinen BMC enthalten.
Seriennummer Des Computing-Controllers	Die Seriennummer des Compute-Controllers.
Computing-Hardware	Der Status der Compute-Controller-Hardware
CPU-Temperatur für Compute Controller	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 Netzwerkverkehr.



a. Lesen Sie den Abschnitt Netzwerkschnittstellen.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
adllb	C2:20:17:59:1C:F3	10 Gigabit	Full	Off	Up
adlli	42:8F:84:80:00:A9	10 Gigabit	Full	Off	Up
eth0	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
eth1	B4:A9:FC:08:4E:49	10 Gigabit	Full	Off	Up
eth2	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
hic1	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic2	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic3	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic4	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
mtc1	B4:A9:FC:08:4E:49	Gigabit	Full	On	Up
mtc2	B4:A9:FC:08:4E:49	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

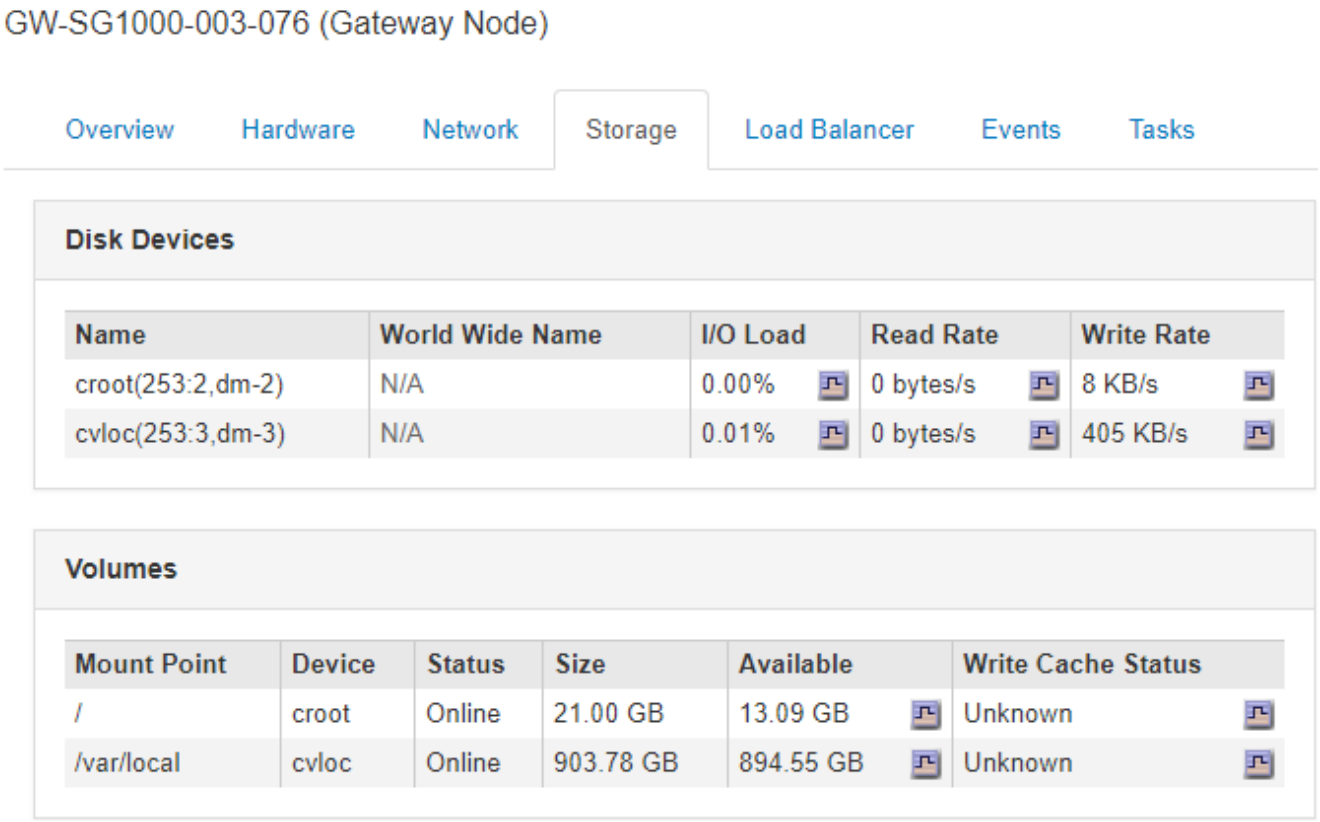
Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

5. Wählen Sie **Storage** aus, um Informationen zu den Festplattengeräten und Volumes auf der Services Appliance anzuzeigen.



Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Informationen, die Sie regelmäßig überwachen sollten

StorageGRID ist ein fehlertolerantes, verteiltes Storage-System, das den Betrieb selbst bei Fehlern oder Nichtverfügbarkeit von Nodes oder Standorten unterstützt. Sie müssen den Systemzustand, die Workloads und die Nutzungsstatistiken proaktiv überwachen, damit Sie Maßnahmen ergreifen können, um potenzielle Probleme zu beheben, bevor sie die Effizienz oder Verfügbarkeit des Grid beeinträchtigen.

Ein überlastetes System generiert große Datenmengen. Dieser Abschnitt enthält eine Anleitung zu den wichtigsten Informationen, die fortlaufend überwacht werden sollen. Dieser Abschnitt enthält die folgenden Unterabschnitte:

- "Monitoring des Systemzustands"
- "Monitoring der Storage-Kapazität"
- "Überwachung des Information Lifecycle Management"
- "Monitoring der Performance-, Netzwerk- und Systemressourcen"
- "Monitoring der Mandantenaktivitäten"
- "Monitoring der Archivierungskapazität"
- "Monitoring von Lastverteilungsvorgängen"
- "Anwenden von Hotfixes oder Aktualisieren der Software, falls erforderlich"

Was überwacht werden soll	Frequenz
Die Systemintegritätsdaten, die im Grid Manager DashboardHinweis angezeigt werden, wenn sich etwas vom vorherigen Tag geändert hat.	Täglich
Rate, mit welcher Objekt- und Metadatenkapazität des Storage-Node genutzt wird	Wöchentlich
Information Lifecycle Management-Operationen	Wöchentlich
Performance-, Netzwerk- und Systemressourcen: • Abfragelatenz • Konnektivität und Networking • Ressourcen auf Node-Ebene	Wöchentlich
Mandantenaktivität	Wöchentlich
Kapazität des externen Archiv-Storage-Systems	Wöchentlich
Lastverteilung	Nach der Erstkonfiguration und nach Konfigurationsänderungen
Verfügbarkeit von Software-Hotfixes und Software-Upgrades	Monatlich

Monitoring des Systemzustands

Sie sollten täglich den allgemeinen Zustand Ihres StorageGRID Systems überwachen.

Das StorageGRID System ist fehlertolerant und funktioniert weiterhin, wenn Teile des Grids nicht verfügbar sind. Das erste Anzeichen eines potenziellen Problems mit Ihrem StorageGRID System ist wahrscheinlich eine Warnmeldung oder ein Alarm (Legacy-System) und nicht unbedingt ein Problem beim Systembetrieb. Wenn Sie die Systemintegrität beachten, können Sie kleinere Probleme erkennen, bevor sie den Betrieb oder die Netzeffizienz beeinträchtigen.

Das Teilfenster „Systemzustand“ im Grid Manager Dashboard bietet eine Zusammenfassung von Problemen, die Ihr System möglicherweise beeinträchtigen. Sie sollten alle auf dem Dashboard angezeigten Probleme untersuchen.

> Damit Sie über Warnungen benachrichtigt werden können, sobald sie ausgelöst werden, können Sie E-Mail-Benachrichtigungen für Warnungen einrichten oder SNMP-Traps konfigurieren.

1. Melden Sie sich beim Grid Manager an, um das Dashboard anzuzeigen.
2. Überprüfen Sie die Informationen im Bedienfeld „Systemzustand“.

Wenn Probleme bestehen, werden Links angezeigt, mit denen Sie weitere Details anzeigen können:

Verlinken	Zeigt An
Grid-Details	Wird angezeigt, wenn Knoten getrennt sind (Verbindungsstatus unbekannt oder Administrativ ausgefallen). Klicken Sie auf den Link oder klicken Sie auf das blaue oder graue Symbol, um zu ermitteln, welche Nodes betroffen sind.
Aktuelle Meldungen	Wird angezeigt, wenn derzeit Meldungen aktiv sind. Klicken Sie auf den Link oder klicken Sie auf **kritisch**, **Major** oder **Minor**, um die Details auf der Seite **Alarme** > **Aktuell** anzuzeigen.
Kürzlich behobene Warnmeldungen	Wird angezeigt, wenn in der letzten Woche ausgelöste Benachrichtigungen jetzt behoben sind. Klicken Sie auf den Link, um die Details auf der Seite **Alerts** > **aufgelöst** anzuzeigen.
Ältere Alarme	Wird angezeigt, wenn derzeit Alarme (Legacy-System) aktiv sind. Klicken Sie auf den Link, um die Details auf der Seite **Support** > **Alarme (alt)** > **Aktuelle Alarme** anzuzeigen. **Hinweis:** während das alte Alarmsystem weiterhin unterstützt wird, bietet das Alarmsystem erhebliche Vorteile und ist einfacher zu bedienen.
Lizenz	Wird angezeigt, wenn es ein Problem mit der Softwarelizenz für dieses StorageGRID-System gibt. Klicken Sie auf den Link, um die Details auf der Seite **Wartung** > **System** > **Lizenz** anzuzeigen.

Verwandte Informationen

"StorageGRID verwalten"

"Einrichten von E-Mail-Benachrichtigungen für Meldungen"

"Verwendung von SNMP-Überwachung"

Monitoring der Verbindungsstatus der Nodes

Wenn ein oder mehrere Nodes vom Grid getrennt werden, können kritische StorageGRID-Vorgänge beeinträchtigt werden. Sie müssen den Status der Node-Verbindung überwachen und Probleme unverzüglich beheben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Nodes können einen von drei Verbindungszuständen haben:

- **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom 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.

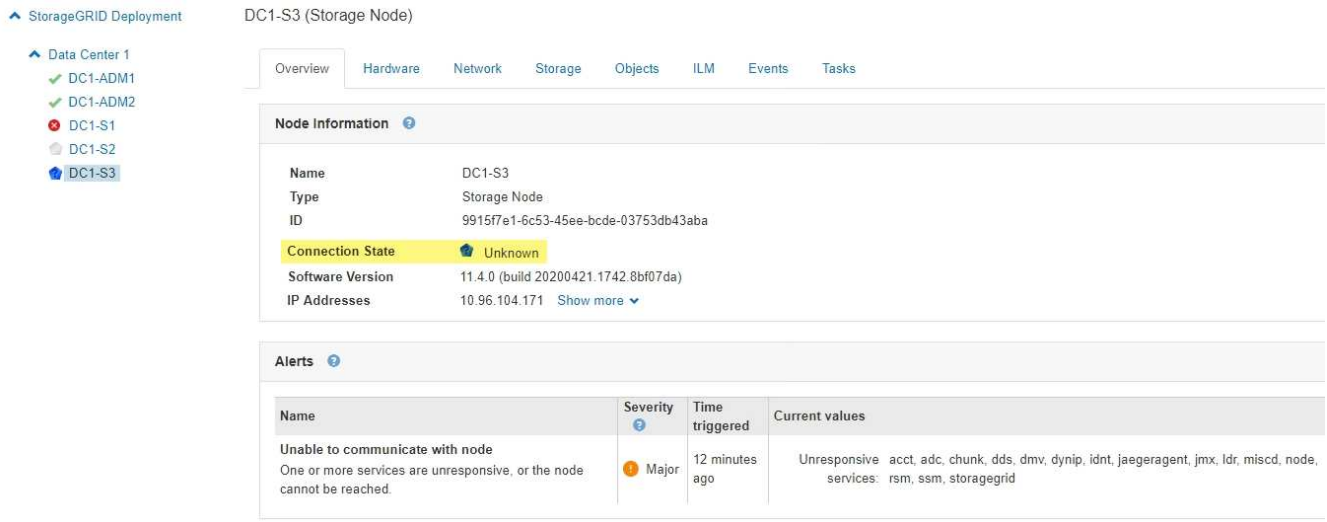
- **Nicht verbunden - Administrativ unten** : Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise auch aktiv.
- * Verbunden* : Der Knoten ist mit dem Raster verbunden.

Schritte

1. Wenn im Bedienfeld „Systemzustand“ des Dashboards ein blaues oder graues Symbol angezeigt wird, klicken Sie auf das Symbol oder klicken Sie auf **Rasterdetails**. (Die blauen oder grauen Symbole und der Link **Grid Details** werden nur angezeigt, wenn mindestens ein Knoten vom Raster getrennt ist.)

   Die Übersichtsseite des ersten blauen Knotens in der Knotenstruktur wird angezeigt. Wenn keine blauen Knoten vorhanden sind, wird die Übersichtsseite für den ersten grauen Knoten in der Struktur angezeigt.

   Im Beispiel hat der Speicherknoten DC1-S3 ein blaues Symbol. Der **Verbindungsstatus** im Fenster Knoteninformationen lautet **Unbekannt**, und die Warnung **mit Knoten** kann nicht kommunizieren* ist aktiv. Die Meldung gibt an, dass ein oder mehrere Services nicht mehr reagiert oder der Node nicht erreicht werden kann.



2. Wenn ein Knoten über ein blaues Symbol verfügt, führen Sie die folgenden Schritte aus:
   a. Wählen Sie jede Warnung in der Tabelle aus, und befolgen Sie die empfohlenen Aktionen.

      Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten.

   b. Wenn der Node nicht wieder in den Online-Modus versetzt werden kann, wenden Sie sich an den technischen Support.
3. Wenn ein Knoten über ein graues Symbol verfügt, führen Sie die folgenden Schritte aus:

   Graue Nodes werden während der Wartungsvorgänge erwartet und sind möglicherweise mit einem oder mehreren Warnmeldungen verbunden. Basierend auf dem zugrunde liegenden Problem werden diese „`administrativ unterliegenden`“ Nodes oft ohne Eingreifen wieder online geschaltet.

   a. Überprüfen Sie den Abschnitt „Meldungen“ und bestimmen Sie, ob Warnmeldungen diesen Node beeinträchtigen.
   b. Wenn eine oder mehrere Warnmeldungen aktiv sind, wählen Sie jede Warnung in der Tabelle aus, und befolgen Sie die empfohlenen Aktionen.
   c. Wenn der Node nicht wieder in den Online-Modus versetzt werden kann, wenden Sie sich an den technischen Support.

Verwandte Informationen

"Alerts Referenz"

"Verwalten Sie erholen"

Anzeigen aktueller Meldungen

Wenn eine Meldung ausgelöst wird, wird auf dem Dashboard ein Meldungssymbol angezeigt. Auf der Seite Knoten wird auch ein Warnungssymbol für den Knoten angezeigt. Es kann auch eine E-Mail-Benachrichtigung gesendet werden, es sei denn, die Warnung wurde stummgeschaltet.

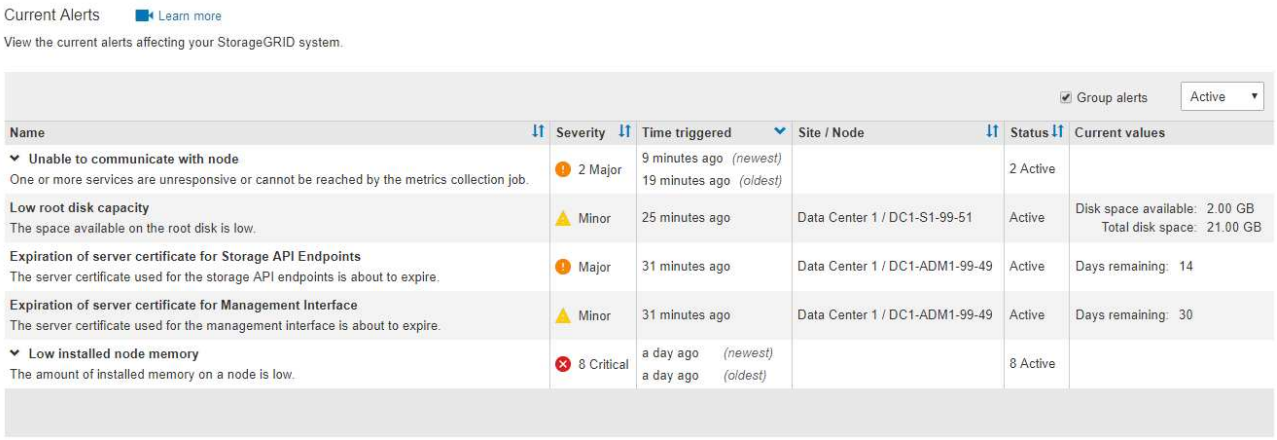
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wenn eine oder mehrere Warnmeldungen aktiv sind, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Fenster Systemzustand des Dashboards auf das Warnsymbol oder klicken Sie auf **Aktuelle Meldungen**. (Ein Warnsymbol und der Link **Current Alerts** werden nur angezeigt, wenn mindestens eine Warnung aktuell aktiv ist.)
   - Wählen Sie **Alarme** > **Aktuell**.

   Die Seite Aktuelle Meldungen wird angezeigt. Er listet alle Warnmeldungen auf, die derzeit Ihr StorageGRID System beeinträchtigen.



   Standardmäßig werden Alarme wie folgt angezeigt:

   - Die zuletzt ausgelösten Warnmeldungen werden zuerst angezeigt.
   - Mehrere Warnmeldungen desselben Typs werden als Gruppe angezeigt.
   - Meldungen, 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 Meldungen“ wird alle zwei Minuten aktualisiert.

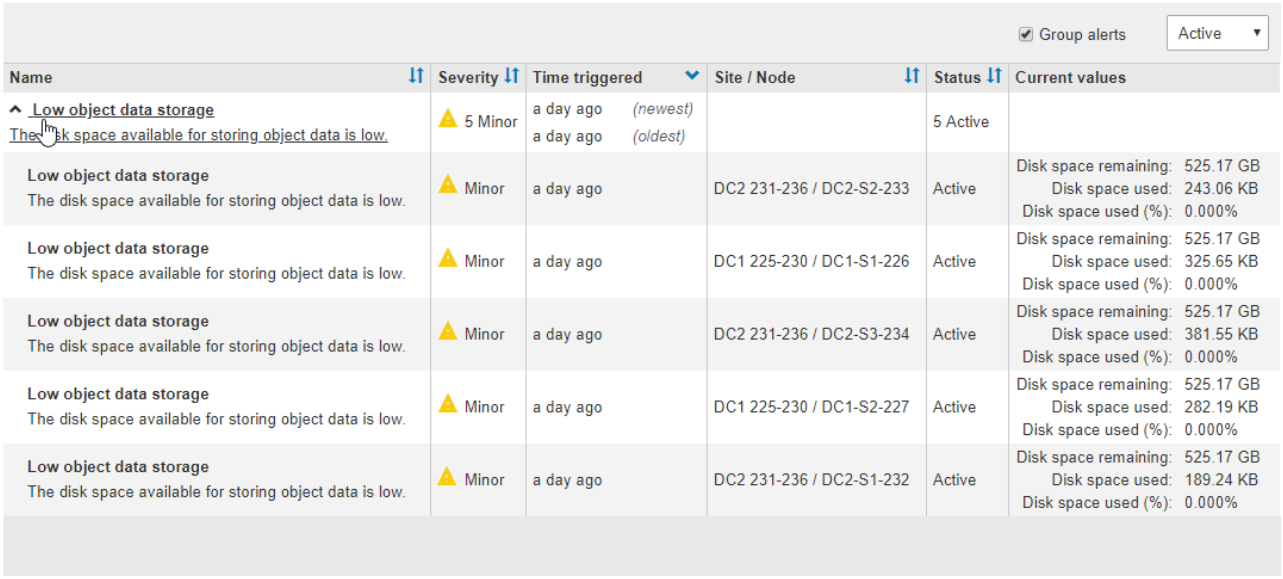
2. Überprüfen Sie die Informationen in der Tabelle.

Spaltenüberschrift	Beschreibung
Name	Der Name der Warnmeldung und deren Beschreibung.

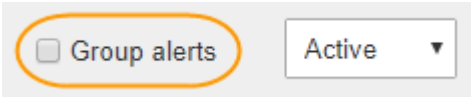
Spaltenüberschrift	Beschreibung
Schweregrad	Der Schweregrad der Meldung. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens 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 sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
Auslösezeit	Wie lange vor der Warnmeldung ausgelöst wurde. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile Zeiten für die letzte Instanz der Warnmeldung (*neueste*) und die älteste Instanz der Warnmeldung (*älteste*) an.
Standort/Knoten	Der Name des Standorts und des Nodes, an dem die Meldung ausgeführt wird. Wenn mehrere Warnmeldungen gruppiert sind, werden die Standort- und Node-Namen in der Titelzeile nicht angezeigt.

Spaltenüberschrift	Beschreibung
Status	Gibt an, ob die Warnung aktiv ist oder stummgeschaltet wurde. 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.
Aktuelle Werte	Der aktuelle Wert der Metrik, der die Meldung ausgelöst 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 Warnungen gruppiert sind, werden die aktuellen Werte in der Titelzeile nicht angezeigt.

3. So erweitern und reduzieren Sie Alarmgruppen:
   - Um die einzelnen Alarme in einer Gruppe anzuzeigen, klicken Sie auf das nach-unten-Symbol ⌄ In der Überschrift, oder klicken Sie auf den Namen der Gruppe.
   - Um die einzelnen Alarme in einer Gruppe auszublenden, klicken Sie auf das nach-oben-Symbol ⌃ In der Überschrift, oder klicken Sie auf den Namen der Gruppe.



4. Um einzelne Warnungen anstelle von Meldegruppen anzuzeigen, deaktivieren Sie das Kontrollkästchen **Gruppenwarnungen** oben in der Tabelle.



5. Zum Sortieren von Warnungen oder Warnungsgruppen klicken Sie auf die nach-oben/unten-Pfeile ⇅ 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** nicht ausgewählt ist, wird die gesamte Liste der Warnungen sortiert. Beispielsweise können Sie alle Warnungen nach **Node/Site** sortieren, um alle Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.
6. Um die Warnungen nach Status zu filtern, verwenden Sie das Dropdown-Menü oben in der Tabelle.

   - Wählen Sie * Alle Alarme*, um alle aktuellen Warnungen anzuzeigen (sowohl aktive als auch stummgeschaltet).
   - Wählen Sie **aktiv** aus, um nur die aktuellen Alarme anzuzeigen, die aktiv sind.
   - Wählen Sie **stummgeschaltet** aus, um nur die aktuellen Meldungen anzuzeigen, die zum Schweigen gebracht wurden.
7. Um Details zu einer bestimmten Warnmeldung anzuzeigen, wählen Sie die Warnmeldung aus der Tabelle aus.

   Ein Dialogfeld für die Meldung wird angezeigt. Siehe Anweisungen zum Anzeigen einer bestimmten Warnmeldung.

Verwandte Informationen

"Anzeigen einer bestimmten Meldung"

"Stummschalten von Warnmeldungen"

Anzeigen gelöster Warnmeldungen

Sie können den Verlauf der behobenen Warnungen suchen und anzeigen.

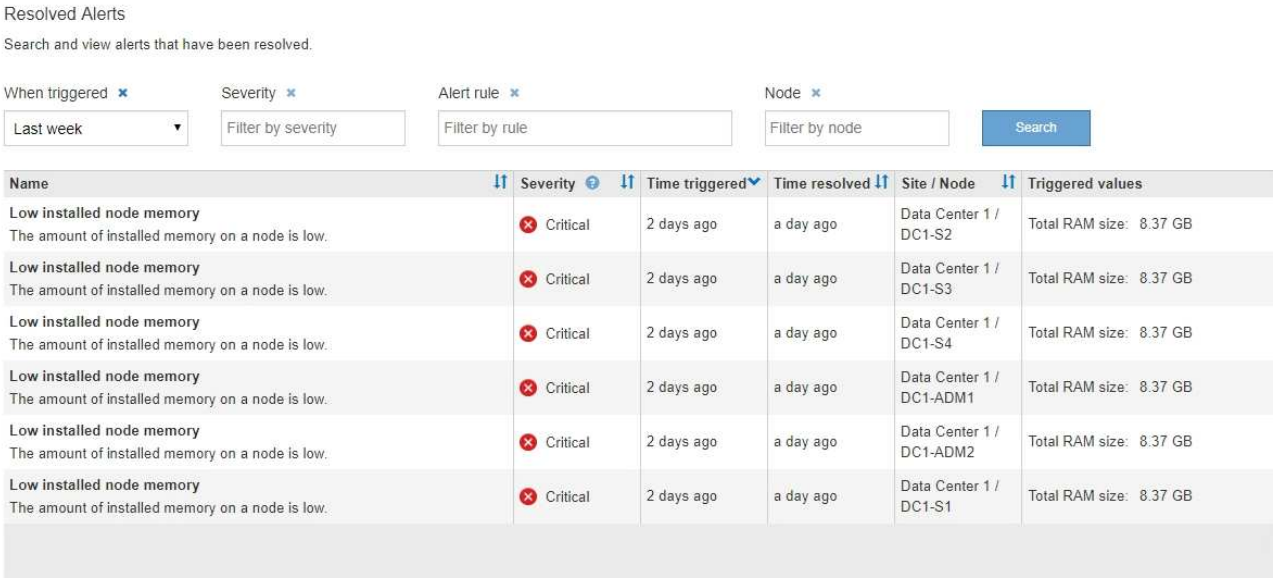
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Führen Sie einen der folgenden Schritte aus, um aufgelöste Warnmeldungen anzuzeigen:
   - Klicken Sie im Bedienfeld „Systemzustand“ auf **Zuletzt behobene Alarme**.

     Der Link **Kürzlich behobene Alarme** wird nur angezeigt, wenn in der letzten Woche eine oder mehrere Warnungen ausgelöst wurden und nun behoben wurden.
   - Wählen Sie **Alarme** > **Aufgelöst**. Die Seite „behobene Warnmeldungen“ wird angezeigt. Standardmäßig werden behobene Benachrichtigungen, die in der letzten Woche ausgelöst wurden, angezeigt, wobei zuerst die zuletzt ausgelösten Meldungen angezeigt werden. Die Warnmeldungen auf dieser Seite wurden zuvor auf der Seite „Aktuelle Meldungen“ oder in einer E-Mail-Benachrichtigung angezeigt.



2. Überprüfen Sie die Informationen in der Tabelle.

Spaltenüberschrift	Beschreibung
Name	Der Name der Warnmeldung und deren Beschreibung.
Schweregrad	Der Schweregrad der Meldung. • * 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 sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.

Spaltenüberschrift	Beschreibung
Auslösezeit	Wie lange vor der Warnmeldung ausgelöst wurde.
Zeit für eine Lösung	Wie lange zuvor wurde die Warnung behoben.
Standort/Knoten	Der Name des Standorts und des Node, auf dem die Meldung aufgetreten ist.
Ausgelöste Werte	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.

3. Um die gesamte Liste der aufgelösten Warnmeldungen zu sortieren, klicken Sie auf die Pfeile nach oben/unten ⇅ In jeder Spaltenüberschrift.

   Sie können beispielsweise aufgelöste Warnmeldungen nach **Site/Node** sortieren, um die Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.

4. Optional können Sie die Liste der aufgelösten Warnmeldungen mithilfe der Dropdown-Menüs oben in der Tabelle filtern.
   a. Wählen Sie im Dropdown-Menü **When Triggered** einen Zeitraum aus, um aufgelöste Warnmeldungen anzuzeigen, basierend darauf, wie lange sie ausgelöst wurden.

      Sie können nach Benachrichtigungen suchen, die innerhalb der folgenden Zeiträume ausgelöst wurden:

      - Letzte Stunde
      - Letzter Tag
      - Letzte Woche (Standardansicht)
      - Letzten Monat
      - Zu jedem Zeitpunkt
      - Benutzerdefiniert (ermöglicht das Festlegen des Anfangsdatums und des Enddatum für den Zeitraum)

   b. Wählen Sie im Dropdown-Menü **Severity** einen oder mehrere Schweregrade aus, um nach gelösten Warnmeldungen eines bestimmten Schweregrads zu filtern.
   c. 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.
   d. Wählen Sie im Dropdown-Menü **Node** einen oder mehrere Knoten aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einem bestimmten Knoten verbunden sind.
   e. Klicken Sie Auf **Suchen**.

5. Um Details zu einer bestimmten aufgelösten Warnmeldung anzuzeigen, wählen Sie die Warnmeldung aus der Tabelle aus.

   Ein Dialogfeld für die Meldung wird angezeigt. Siehe Anweisungen zum Anzeigen einer bestimmten Warnmeldung.

Verwandte Informationen

"Anzeigen einer bestimmten Meldung"

Anzeigen einer bestimmten Meldung

Sie können detaillierte Informationen zu einer Meldung anzeigen, die derzeit Ihr StorageGRID System beeinträchtigt, oder eine Meldung, die behoben wurde. Zu den Details gehören empfohlene Korrekturmaßnahmen, der Zeitpunkt, zu dem die Meldung ausgelöst wurde, und der aktuelle Wert der Metriken in Bezug auf diese Meldung. Optional können Sie eine aktuelle Warnung stummschalten oder die Alarmregel aktualisieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

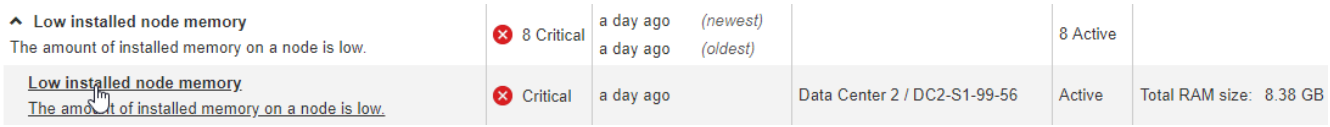
1. Führen Sie einen der folgenden Schritte aus, je nachdem, ob Sie eine aktuelle oder behobene Warnmeldung anzeigen möchten:

Spaltenüberschrift	Beschreibung
Aktueller Alarm	• Klicken Sie im Fenster Systemzustand des Dashboards auf den Link **Aktuelle Meldungen**. Dieser Link wird nur angezeigt, wenn mindestens eine Warnung aktuell aktiv ist. Dieser Link ist ausgeblendet, wenn keine aktuellen Warnmeldungen vorhanden sind oder alle aktuellen Warnmeldungen stummgeschaltet wurden. • Wählen Sie **Alarme** > **Aktuell**. • Wählen Sie auf der Seite **Nodes** die Registerkarte **Übersicht** für einen Knoten mit einem Warnsymbol. Klicken Sie dann im Abschnitt Meldungen auf den Namen der Warnmeldung.

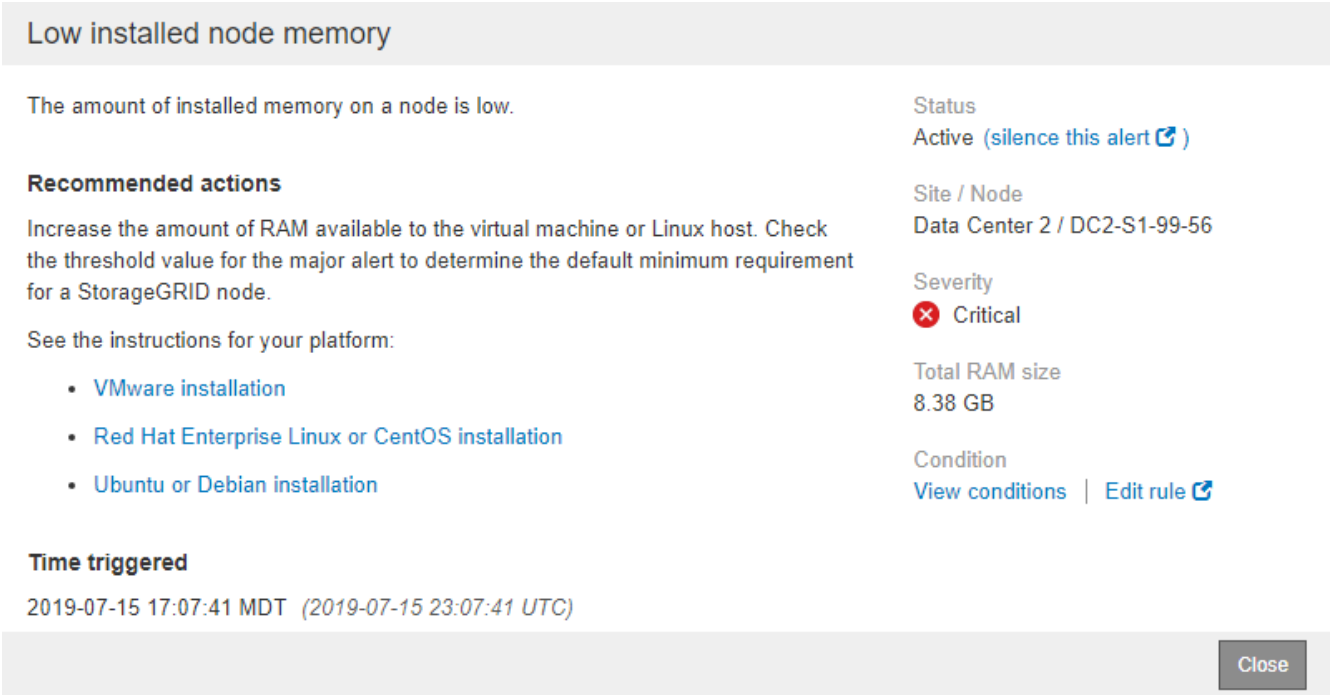
Spaltenüberschrift	Beschreibung
Alarm wurde behoben	• Klicken Sie im Fenster Systemzustand des Dashboards auf den Link **Zuletzt behobene Alarme**. (Dieser Link wird nur angezeigt, wenn in der vergangenen Woche eine oder mehrere Warnmeldungen ausgelöst wurden und jetzt behoben werden. Dieser Link ist ausgeblendet, wenn in der letzten Woche keine Warnmeldungen ausgelöst und behoben wurden.) • Wählen Sie **Alarme** > **Aufgelöst**.

2. Erweitern Sie je nach Bedarf eine Gruppe von Warnungen, und wählen Sie dann die Warnmeldung aus, die Sie anzeigen möchten.

Wählen Sie die Meldung und nicht die Überschrift einer Gruppe von Warnungen aus.



Ein Dialogfeld wird angezeigt und enthält Details für die ausgewählte Warnmeldung.



3. Prüfen Sie die Warnmeldungsdetails.

Informationsdaten	Beschreibung
Titel	Der Name der Warnmeldung.

Informationsdaten	Beschreibung
Erster Absatz	Die Beschreibung der Warnmeldung.
Empfohlene Maßnahmen	Die empfohlenen Aktionen für diese Warnmeldung.
Auslösezeit	Datum und Uhrzeit der Auslösung der Warnmeldung zu Ihrer lokalen Zeit und zu UTC.
Zeit für eine Lösung	Nur bei gelösten Warnmeldungen wurde das Datum und die Uhrzeit der Behebung der Warnmeldung in Ihrer lokalen Zeit und in UTC angegeben.
Status	Der Status der Warnmeldung: Aktiv, stummgeschaltet oder gelöst.
Standort/Knoten	Der Name des von der Meldung betroffenen Standorts und Nodes.
Schweregrad	Der Schweregrad der Meldung. • * 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 sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.

Informationsdaten	Beschreibung
Datenwerte	Der aktuelle Wert der Metrik für diese Meldung. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Warnung für **Low-Metadaten-Speicher** enthalten beispielsweise den Prozentsatz des belegten Speicherplatzes, den gesamten Speicherplatz und die Menge des verwendeten Festplattenspeichers.

4. Klicken Sie optional auf **stummschalten Sie diese Warnung**, um die Alarmregel, die diese Warnung ausgelöst hat, stillzuschalten.

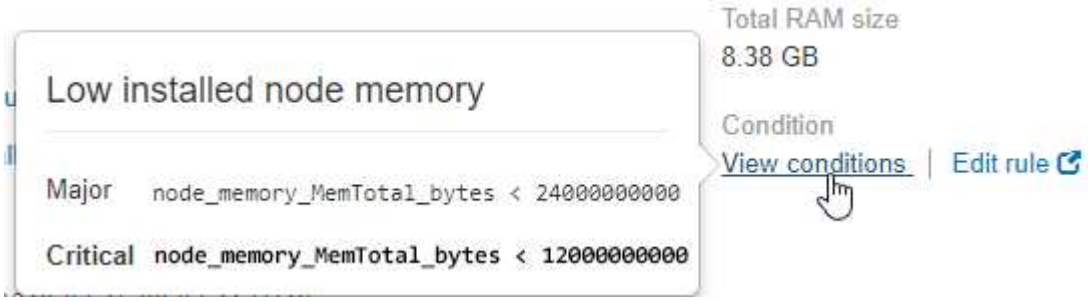
   Sie müssen über die Berechtigung Warnungen verwalten oder Root-Zugriff verfügen, um eine Alarmregel stillzuschalten.

   > 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.

5. So zeigen Sie die aktuellen Bedingungen für die Meldungsregel an:

   a. Klicken Sie in den Alarmdetails auf **Bedingungen anzeigen**.

      Es wird ein Popup-Fenster mit dem Prometheus-Ausdruck für jeden definierten Schweregrad angezeigt.



   a. Um das Popup-Fenster zu schließen, klicken Sie außerhalb des Popup-Dialogfenster auf eine beliebige Stelle.

6. Klicken Sie optional auf **Regel bearbeiten**, um die Warnregel zu bearbeiten, die die Warnung ausgelöst hat:

   Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen, um eine Alarmregel zu 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.

7. Klicken Sie zum Schließen der Warnungsdetails auf **Schließen**.

Verwandte Informationen

"Stummschalten von Warnmeldungen"

"Bearbeiten einer Meldungsregel"

Anzeigen von Legacy-Alarmen

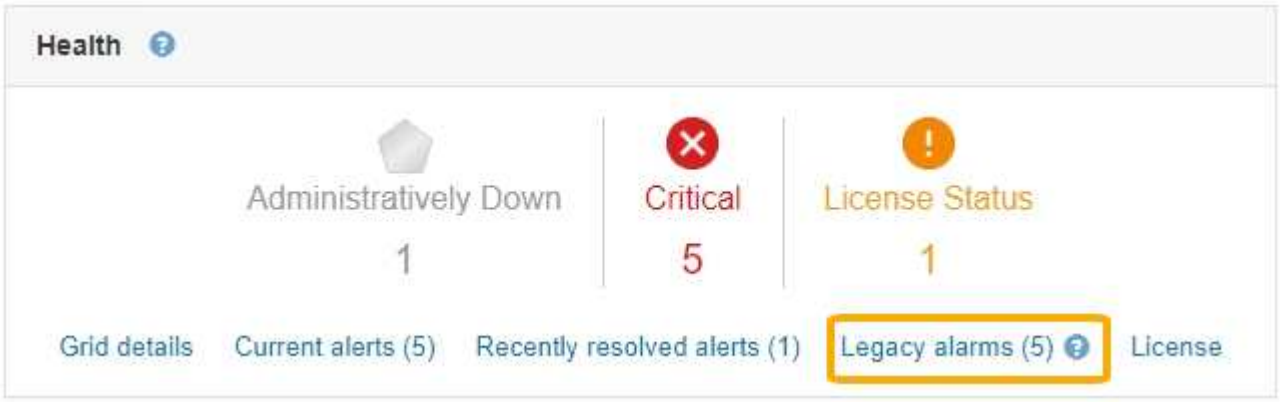
Alarme (Altsystem) werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Sie können die derzeit aktiven Alarme über das Dashboard oder die Seite Aktuelle Alarme anzeigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn einer oder mehrere der älteren Alarme derzeit aktiv sind, enthält das Bedienfeld „Systemzustand“ auf dem Dashboard einen Link „Legacy-Alarme*“. Die Zahl in Klammern gibt an, wie viele Alarme derzeit aktiv sind.



Die Zählung der **Legacy-Alarme** auf dem Dashboard wird immer dann erhöht, wenn ein älterer Alarm ausgelöst wird. Diese Zählung wird sogar erhöht, wenn Sie Alarm-E-Mail-Benachrichtigungen deaktiviert haben. Sie können diese Zahl in der Regel ignorieren (da Warnmeldungen eine bessere Übersicht über das System bieten) oder die derzeit aktiven Alarme anzeigen.

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

Schritte

1. Führen Sie einen der folgenden Schritte aus, um die vorhandenen Alarme anzuzeigen:
   - Klicken Sie im Bedienfeld „Systemzustand“ auf **Legacy-Alarme**. Dieser Link wird nur angezeigt, wenn derzeit mindestens ein Alarm aktiv ist.
   - Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**. Die Seite Aktuelle Alarme wird angezeigt.

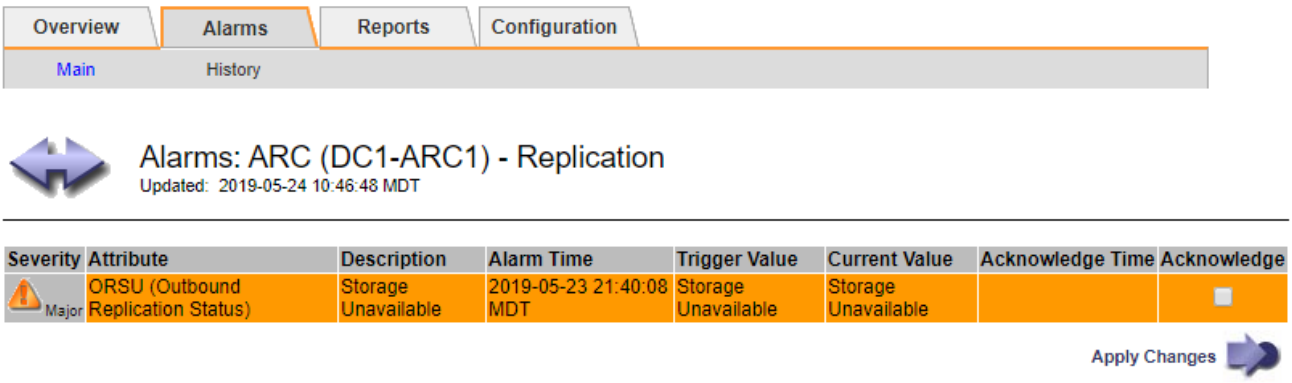
Das Alarmsymbol zeigt den Schweregrad jedes Alarms wie folgt an:

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.

Symbol	Farbe	Alarmschweregrad	Bedeutung
	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.

1. Um mehr über das Attribut zu erfahren, das den Alarm ausgelöst hat, klicken Sie mit der rechten Maustaste auf den Attributnamen in der Tabelle.
2. 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**).



3. 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)"

"Bestätigen aktueller Alarme (Altsystem)"

"Deaktivieren von Alarmen (Altsystem)"

Monitoring der Storage-Kapazität

Sie müssen den insgesamt nutzbaren Speicherplatz auf Storage-Nodes überwachen, um sicherzustellen, dass dem StorageGRID System nicht der Speicherplatz für Objekte oder Objekt-Metadaten zur Verfügung steht.

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.

Sie können Storage-Kapazitätsinformationen für das gesamte Grid, für jeden Standort und für jeden Storage-Node in Ihrem StorageGRID-System anzeigen.

Verwandte Informationen

"Anzeigen der Registerkarte „Speicher“"

Überwachung der Storage-Kapazität für das gesamte Grid

Die Storage-Gesamtkapazität für das Grid muss überwacht werden, um zu gewährleisten, dass ausreichend freier Speicherplatz für Objekt- und Objekt-Metadaten 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.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

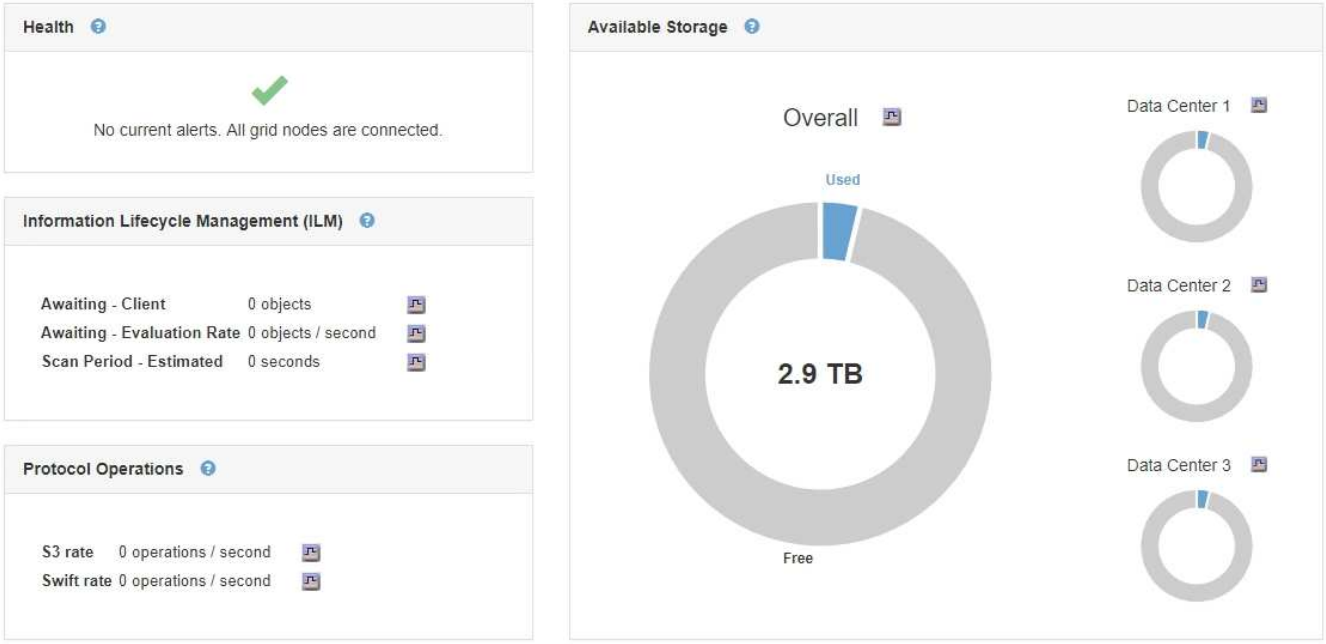
Über diese Aufgabe

Über das Dashboard im Grid Manager können Sie schnell ermitteln, wie viel Storage für das gesamte Grid und für jedes Datacenter zur Verfügung steht. Die Seite Knoten enthält detailliertere Werte für Objektdaten und Objektmetadaten.

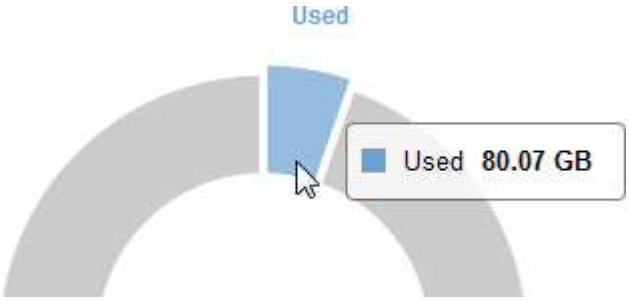
Schritte

1. Beurteilen Sie, wie viel Storage für das gesamte Grid und das jeweilige Datacenter verfügbar ist.
   a. Wählen Sie **Dashboard**.
   b. Notieren Sie sich im Fenster Verfügbare Speicherkapazität die Zusammenfassung der freien und genutzten Speicherkapazität.

      Die Zusammenfassung enthält keine Archivierungsmedien.



a. Platzieren Sie den Cursor über die freien bzw. genutzten Kapazitätsbereiche des Diagramms, um genau zu sehen, wie viel Speicherplatz frei oder verwendet wird.



b. Sehen Sie sich das Diagramm für die einzelnen Datacenter an, um Grids für mehrere Standorte zu verwenden.

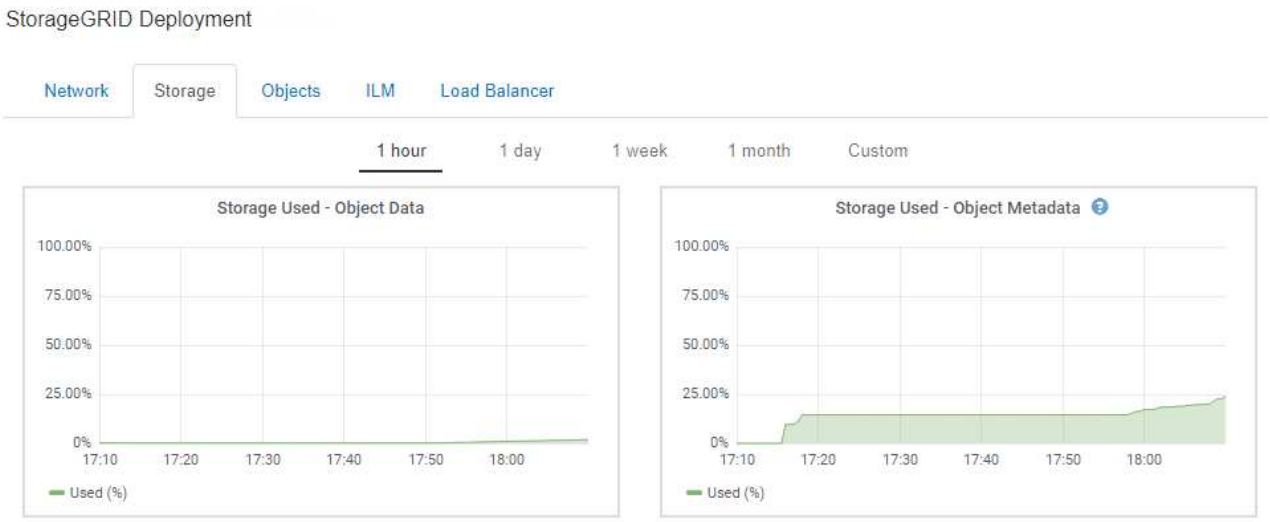
c. Klicken Sie auf das Diagrammsymbol Für das Gesamtdiagramm oder für ein einzelnes Datacenter, um ein Diagramm anzuzeigen, in dem die Kapazitätsauslastung im Laufe der Zeit dargestellt wird.

   Eine Grafik zeigt den prozentualen Anteil an der genutzten Storage-Kapazität (%) gegenüber Die Uhrzeit wird angezeigt.

2. Ermitteln Sie, wie viel Storage genutzt wurde und wie viel Storage für Objekt- und Objekt-Metadaten verfügbar ist.

   a. Wählen Sie **Knoten**.

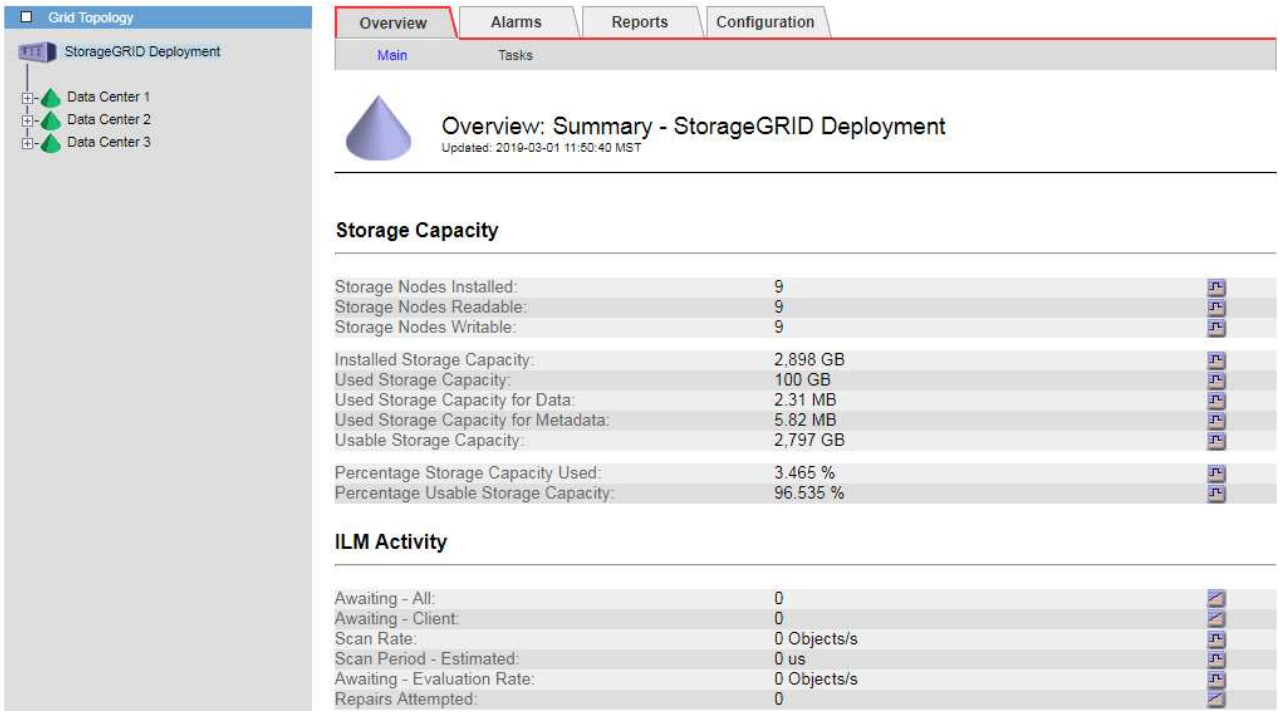
   b. Wählen Sie ***Grid*** > **Storage** aus.



c. Bewegen Sie den Mauszeiger über den Speicher verwendet - Objektdaten und den verwendeten Speicher - Objektmetadaten-Diagramme, um zu ermitteln, wie viel Objekt-Storage und Objekt-Metadaten im gesamten Grid zur Verfügung stehen und wieviel Storage über die Zeit verwendet wurde.

> ⓘ Die Gesamtwerte für einen Standort oder das Grid enthalten keine Nodes, die mindestens fünf Minuten lang keine Kennzahlen enthalten, z. B. Offline-Nodes.

3. Sehen Sie sich gemäß dem technischen Support weitere Details zur Speicherkapazität Ihres Grids an.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***Grid*** > **Übersicht** > **Main**.



4. 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 in den Anweisungen zur Erweiterung von StorageGRID.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

Monitoring der Storage-Kapazität für jeden Storage-Node

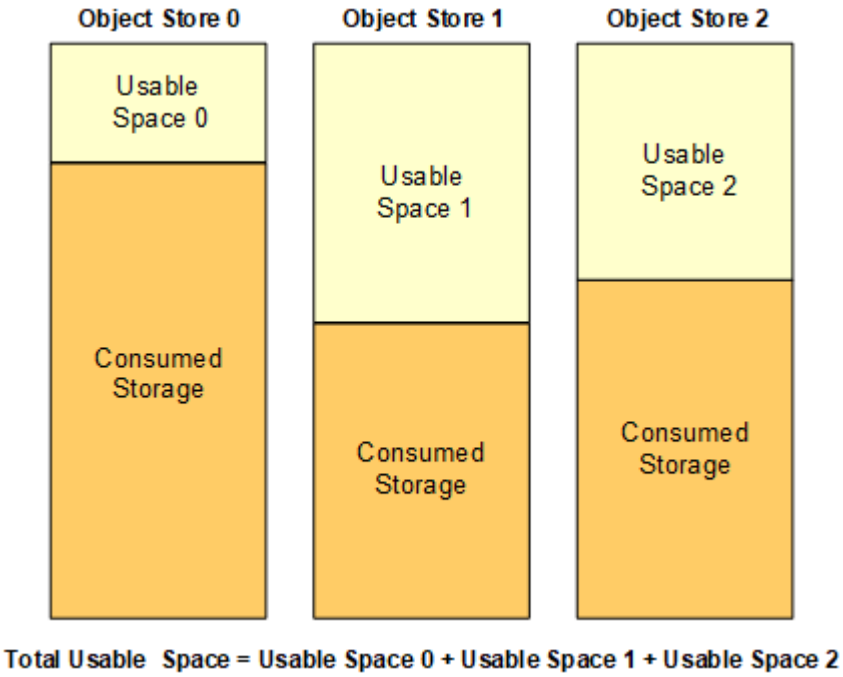
Sie müssen den gesamten nutzbaren Speicherplatz für jeden Storage-Node überwachen, um sicherzustellen, dass der Node über genügend Speicherplatz für neue Objektdaten verfügt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

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.



Schritte

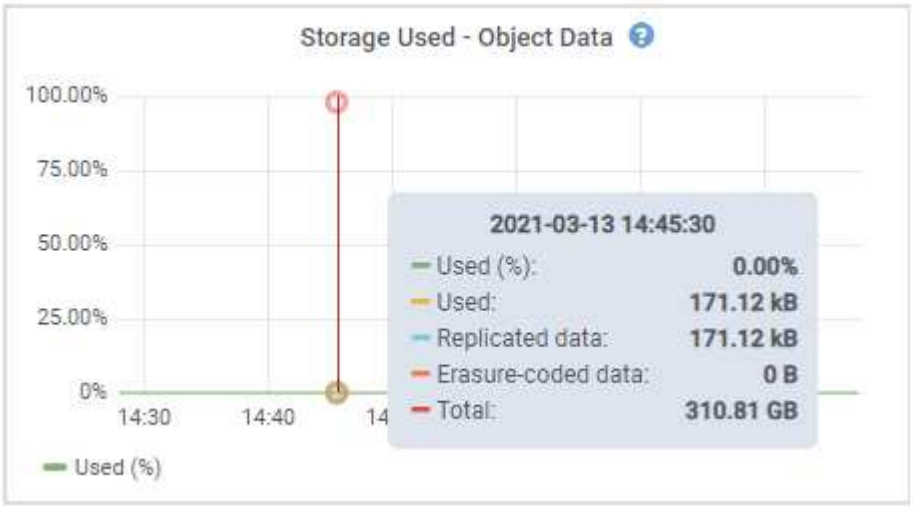
1. Wählen Sie **Nodes** > ***Storage Node*** > **Storage** Aus.

   Die Diagramme und Tabellen für den Node werden angezeigt.

2. Bewegen Sie den Mauszeiger über das Diagramm „verwendete Daten – 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.
   - **Erasure-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	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Überwachen Sie die Werte im Zeitbereich, um die Rate abzuschätzen, mit der der nutzbare Speicherplatz belegt wird.
5. 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 in den Anweisungen zur Erweiterung von StorageGRID.

   Der Alarm * Low Object Data Storage* und der Legacy Storage Status (SSTS) werden ausgelöst, wenn nicht genügend Speicherplatz zum Speichern von Objektdaten auf einem Storage Node vorhanden ist.

Verwandte Informationen

"StorageGRID verwalten"

"Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“"

"Erweitern Sie Ihr Raster"

Monitoring der Objekt-Metadaten-Kapazität für jeden Storage Node

Sie müssen die Metadatennutzung für jeden Storage-Node überwachen, um sicherzustellen, dass ausreichend Speicherplatz für wichtige Datenbankvorgänge verfügbar bleibt. Sie müssen an jedem Standort neue Storage-Nodes hinzufügen, bevor die Objektmetadaten 100 % des zulässigen Metadaten-Speicherplatzes übersteigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

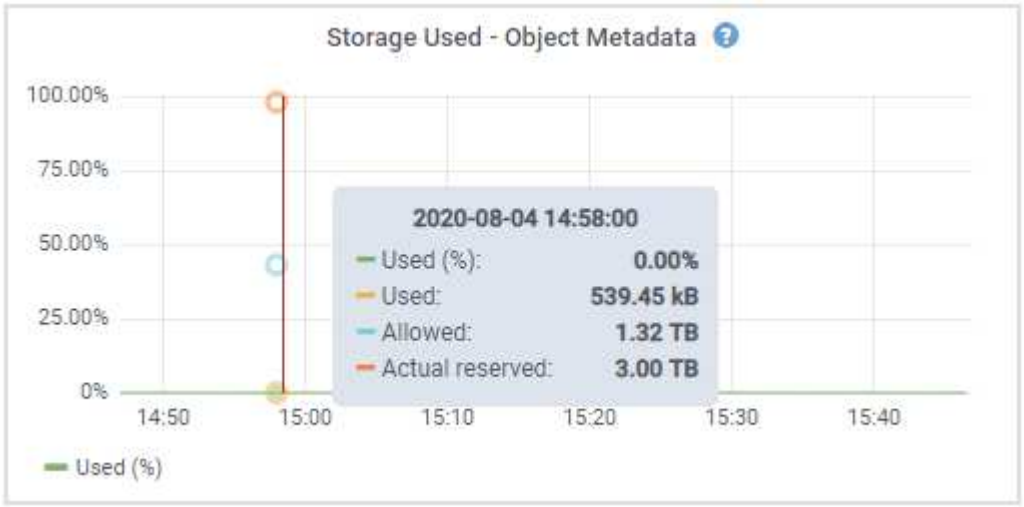
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage 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 Metadatennutzung 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 „verwendete Objekte – Metadaten“, um die Werte für eine bestimmte Zeit anzuzeigen.



Wert	Beschreibung	Prometheus metrisch
Nutzung (%)	Der Prozentsatz des zulässigen Metadaten-Speicherplatzes, der auf diesem Storage-Node verwendet wurde.	`storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes`
Verwendet	Die Bytes des zulässigen Metadaten-Speicherplatzes, der auf diesem Speicherknoten verwendet wurde.	`storagegrid_storage_utilization_metadata_bytes`
Zulässig	Der zulässige Speicherplatz für Objektmetadaten auf diesem Storage-Node. Erfahren Sie, wie dieser Wert für die einzelnen Speicherknoten bestimmt ist, und lesen Sie die Anweisungen zur Verwaltung von StorageGRID.	`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 die einzelnen Storage-Nodes berechnet wird, finden Sie in den Anweisungen für die Administration von StorageGRID.	`storagegrid_storage_utilization_metadata_reserved_bytes`

Die Gesamtwerte für einen Standort oder das Grid enthalten keine Nodes, die Kennzahlen für mindestens fünf Minuten nicht 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. Anweisungen zum erweitern eines StorageGRID-Systems finden Sie in den Anweisungen.

Verwandte Informationen

"Fehlerbehebung für Storage-Warnmeldungen bei niedrigen Metadaten"

"StorageGRID verwalten"

"Erweitern Sie Ihr Raster"

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.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

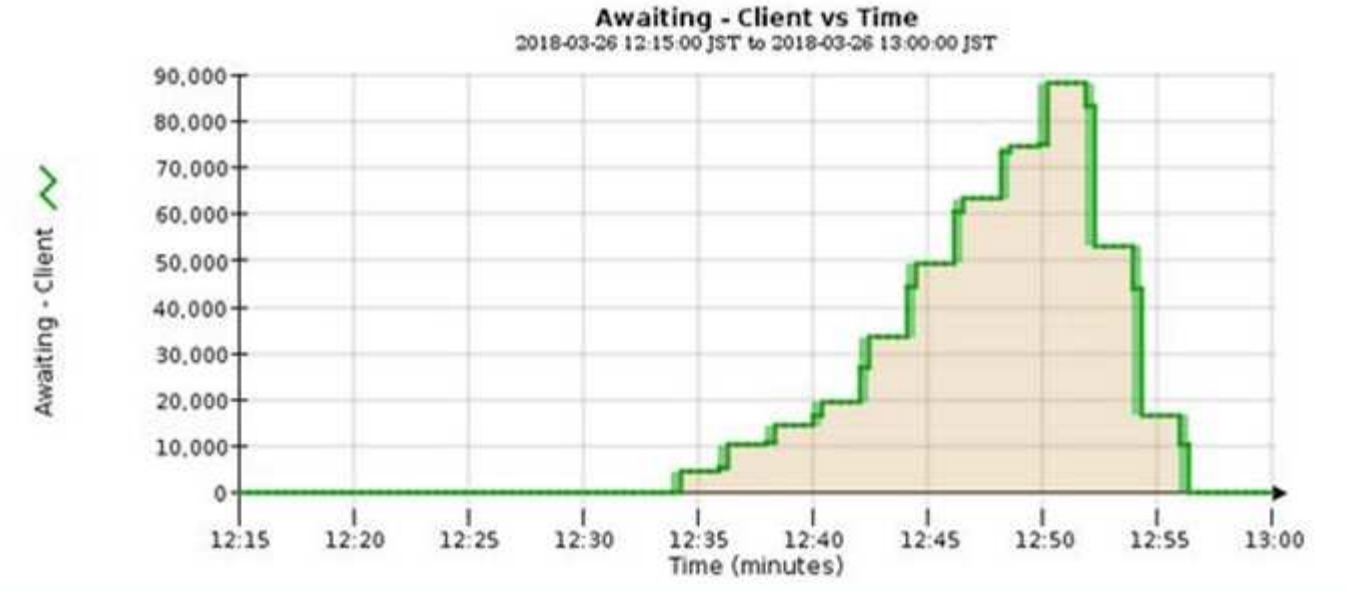
Das StorageGRID System managt Objekte mithilfe der aktiven ILM-Richtlinie. Die ILM-Richtlinie und die zugehörigen ILM-Regeln bestimmen die Anzahl der Kopien, die Art der erstellten Kopien, das Erstellen von Kopien und die Dauer der Aufbewahrung jeder Kopie.

Bei der Objektaufnahme und anderen objektbezogenen Aktivitäten kann die Rate überschritten werden, mit der StorageGRID ILM bewerten kann. Das System muss dann Objekte in eine Warteschlange stellen, deren ILM-Platzierung nicht nahezu in Echtzeit erfüllt werden kann. 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 über das Dashboard im Bereich Information Lifecycle Management (ILM) den Eintrag **wartet auf - 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 aufrechtzuerhalten 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.

Sie können ILM-Warteschlangen mithilfe der Seite **Nodes** genauer untersuchen.

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.

Monitoring der Performance-, Netzwerk- und Systemressourcen

Sie sollten die Performance-, Netzwerk- und Systemressourcen überwachen, um zu ermitteln, ob StorageGRID die aktuelle Last bewältigen kann und ob die Client-Performance im Laufe der Zeit nicht abnimmt.

Monitoring der Abfragelatenz

Client-Aktionen wie Speichern, Abrufen oder Löschen von Objekten erstellen Abfragen für die verteilte Datenbank der Objektmetadaten des Grid. Sie sollten Trends bei der Abfragelatenz überwachen, um sicherzustellen, dass die Grid-Ressourcen für die aktuelle Auslastung ausreichend sind.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

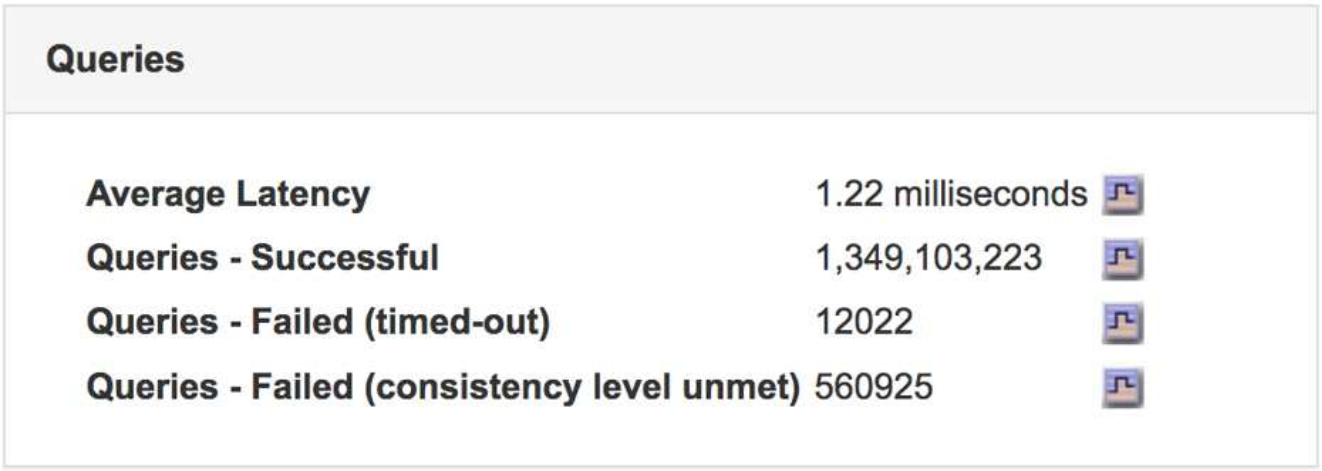
Temporäre Steigerungen der Abfragelatenz sind normal und können durch eine plötzliche Zunahme der Aufnahmeraten verursacht werden. Ausgefallene Abfragen sind ebenfalls normal und können aus vorübergehenden Netzwerkproblemen oder Knoten resultieren, die vorübergehend nicht verfügbar sind. Wenn jedoch die durchschnittliche Zeit für eine Abfrage steigt, sinkt die Gesamtleistung des Grids.

Wenn Sie feststellen, dass die Abfragelatenz im Laufe der Zeit zunimmt, sollten Sie in Erwägung ziehen, weitere Storage-Nodes in einem Erweiterungsverfahren hinzuzufügen, um zukünftige Workloads zu erfüllen.

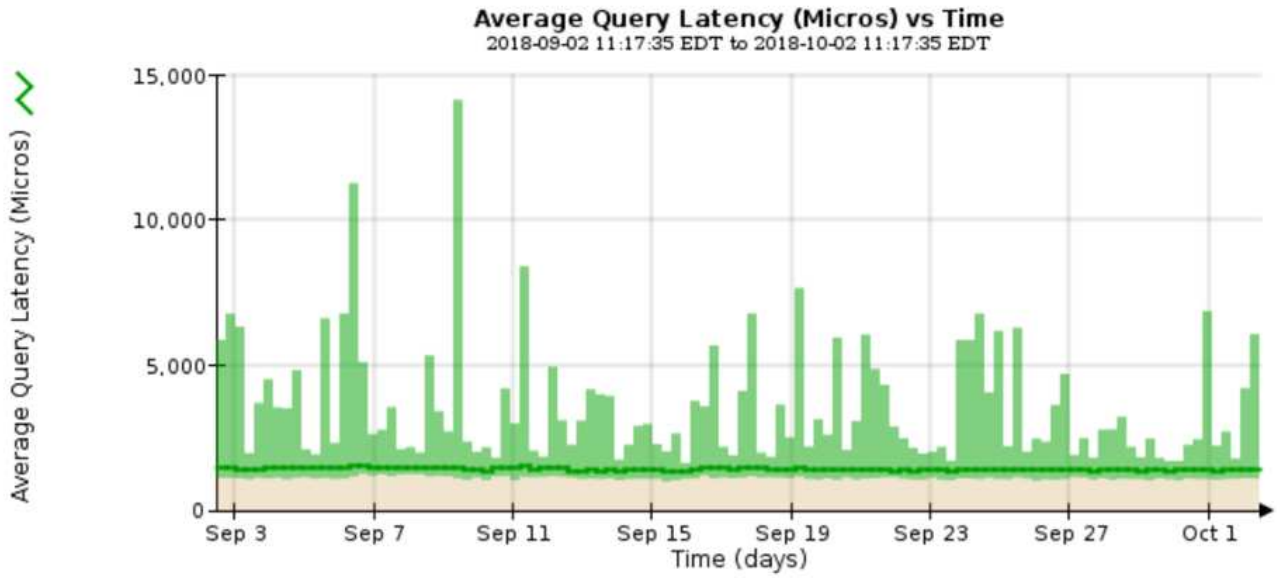
Die Warnung **hohe Latenz für Metadatenabfragen** wird ausgelöst, wenn die durchschnittliche Zeit für Abfragen zu lang ist.

Schritte

1. Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte** Aus.
2. Blättern Sie nach unten zur Tabelle Abfragen, und zeigen Sie den Wert für die durchschnittliche Latenz an.



3. Klicken Sie auf das Diagrammsymbol Um den Wert im Zeitverlauf zu erstellen.



Das Beispieldiagramm zeigt Spitzen in der Abfragelatenz während des normalen Grid-Betriebs.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

Monitoring von Netzwerkverbindungen und Performance

Die Grid-Nodes müssen miteinander kommunizieren können, damit das Grid betrieben werden kann. Die Integrität des Netzwerks zwischen Knoten und Standorten und die Netzwerkbandbreite zwischen Standorten sind für einen effizienten Betrieb entscheidend.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Netzwerkkonnektivität 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 führen (wenn die strikte Aufnahme-Option für ILM-Regeln ausgewählt ist) oder zu unzureichenden Aufnahme-Performance und ILM-Backlogs.

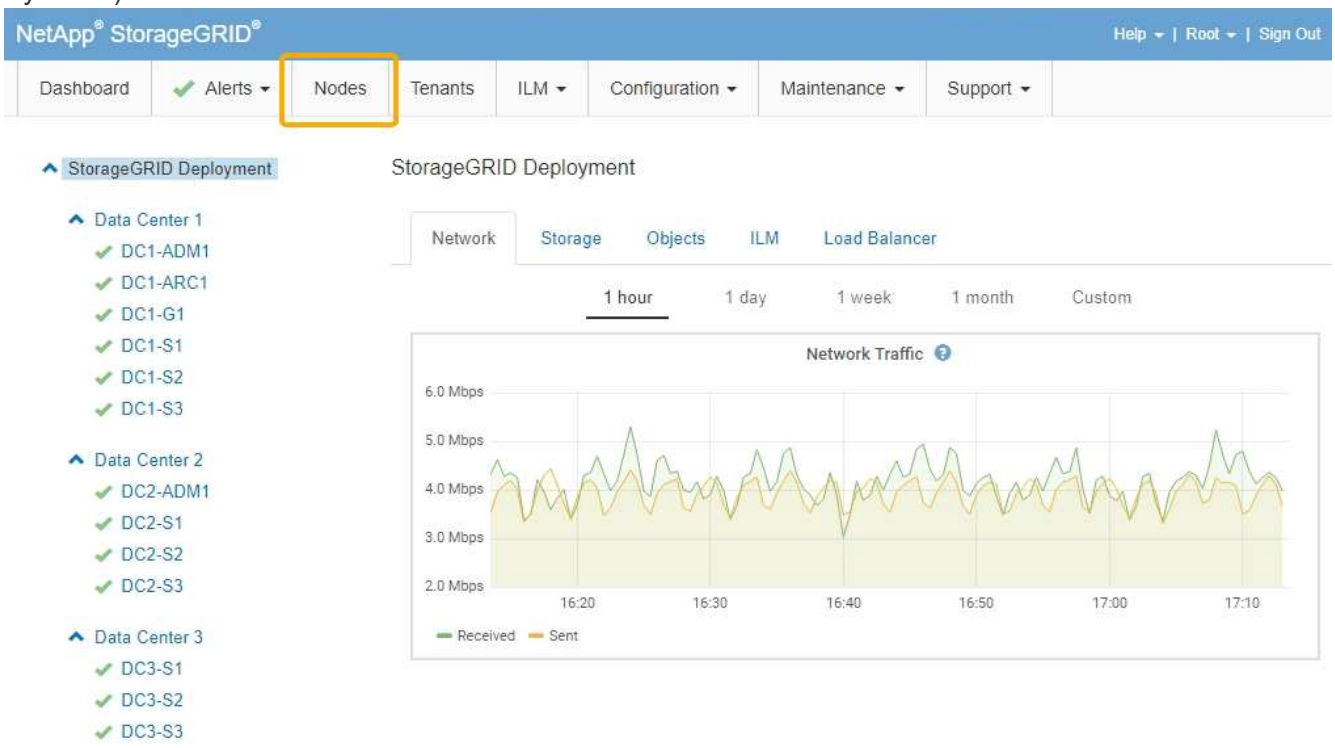
Mit dem Grid Manager können Sie die Konnektivität und die Netzwerk-Performance überwachen, damit Sie Probleme umgehend beheben können.

Darüber hinaus sollten Richtlinien für die Klassifizierung des Netzwerkverkehrs erstellt werden, um den Datenverkehr im Zusammenhang mit bestimmten Mandanten, Buckets, Subnetzen oder Load Balancer-Endpunkten zu überwachen und einzuschränken. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Schritte

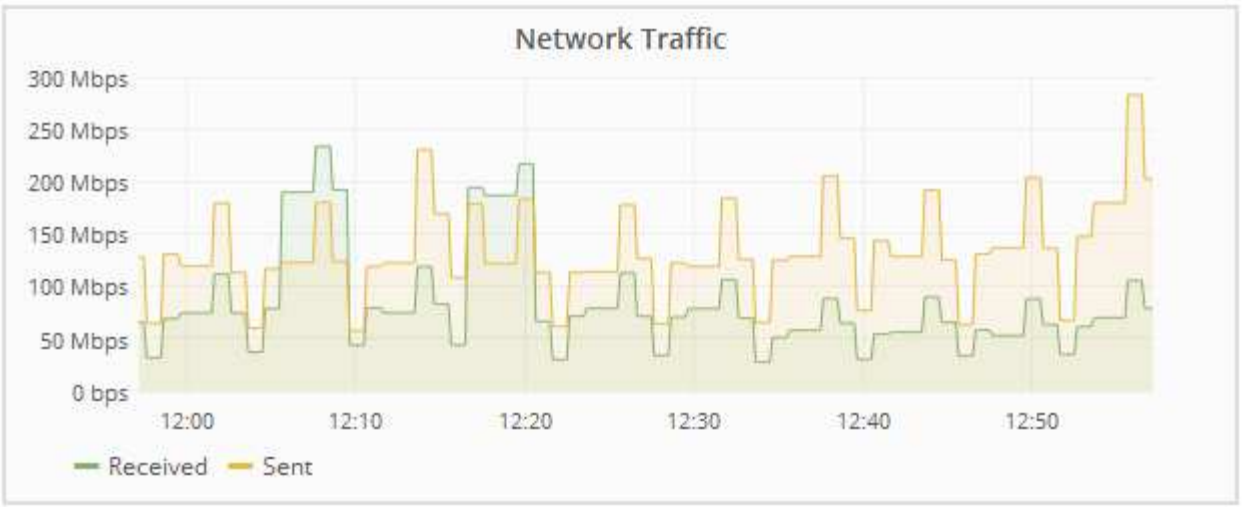
1. Wählen Sie **Knoten**.

   Die Seite Knoten wird angezeigt. Die Knotensymbole zeigen auf einen Blick an, welche Knoten verbunden sind (grünes Häkchen-Symbol) und welche Knoten getrennt sind (blaue oder graue Symbole).



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.



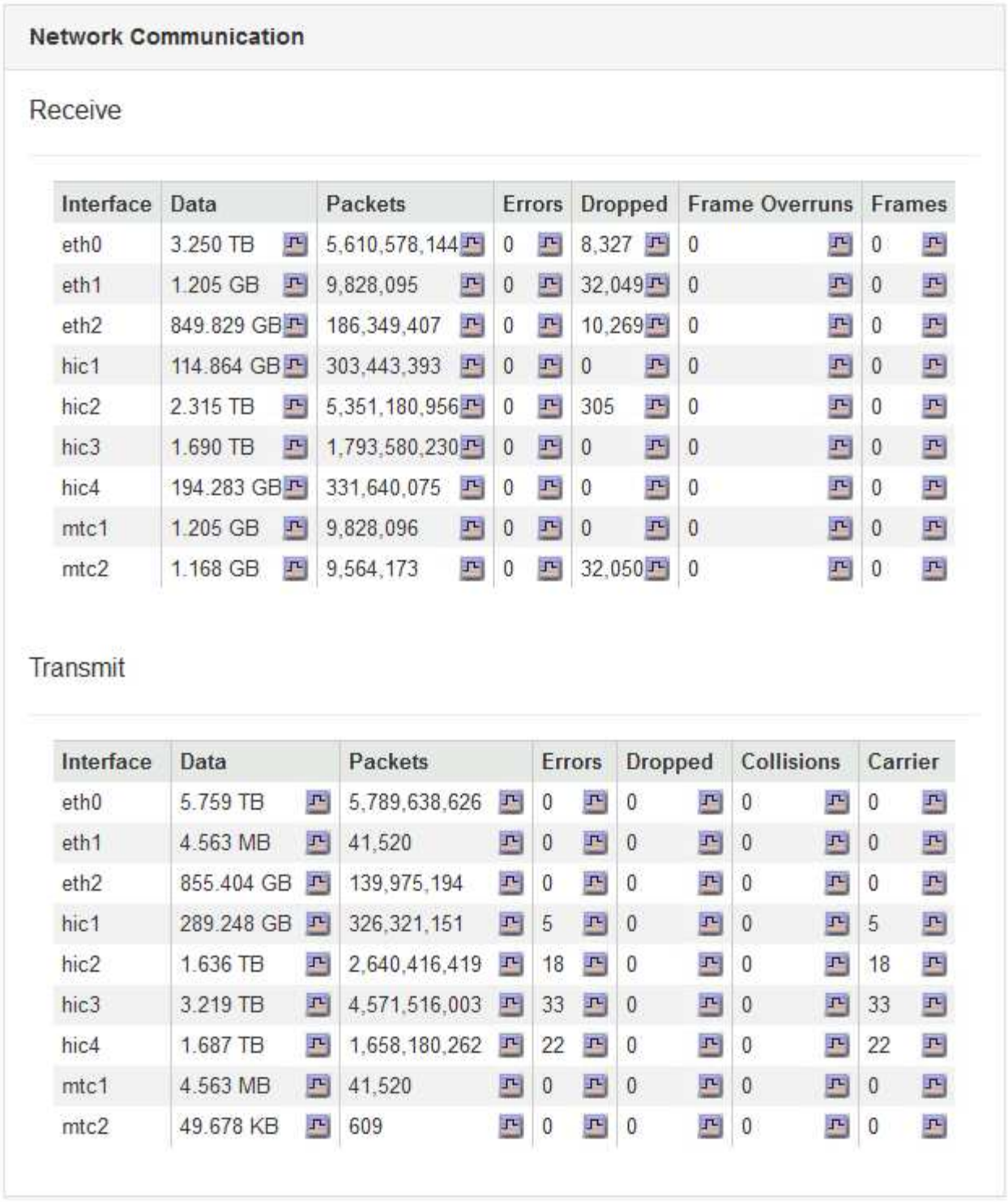
a. Wenn Sie einen Rasterknoten ausgewählt haben, scrollen Sie nach unten, um den Abschnitt **Netzwerkschnittstellen** auf der Seite anzuzeigen.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	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	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

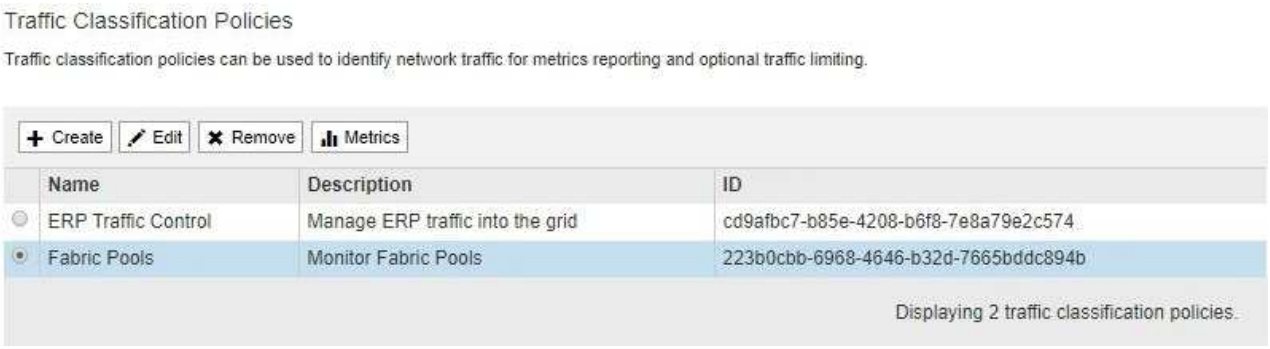
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

3. Verwenden Sie die Metriken für Ihre Traffic-Klassifizierungsrichtlinien zur Überwachung des Netzwerkverkehrs.

   a. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

      Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



b. 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**.

c. 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. Passen Sie von Zeit zu Zeit jede Richtlinie für die Verkehrsklassifizierung nach Bedarf an.

Informationen zum Erstellen, Bearbeiten oder Löschen von Richtlinien für die Verkehrsklassifizierung finden Sie in den Anweisungen für die Verwaltung von StorageGRID.

Verwandte Informationen

"Registerkarte Netzwerk anzeigen"

"Monitoring der Verbindungsstatus der Nodes"

"StorageGRID verwalten"

Monitoring der Ressourcen auf Node-Ebene

Sie sollten einzelne Grid-Nodes überwachen, um die Ressourcenauslastung zu überprüfen.

Was Sie benötigen

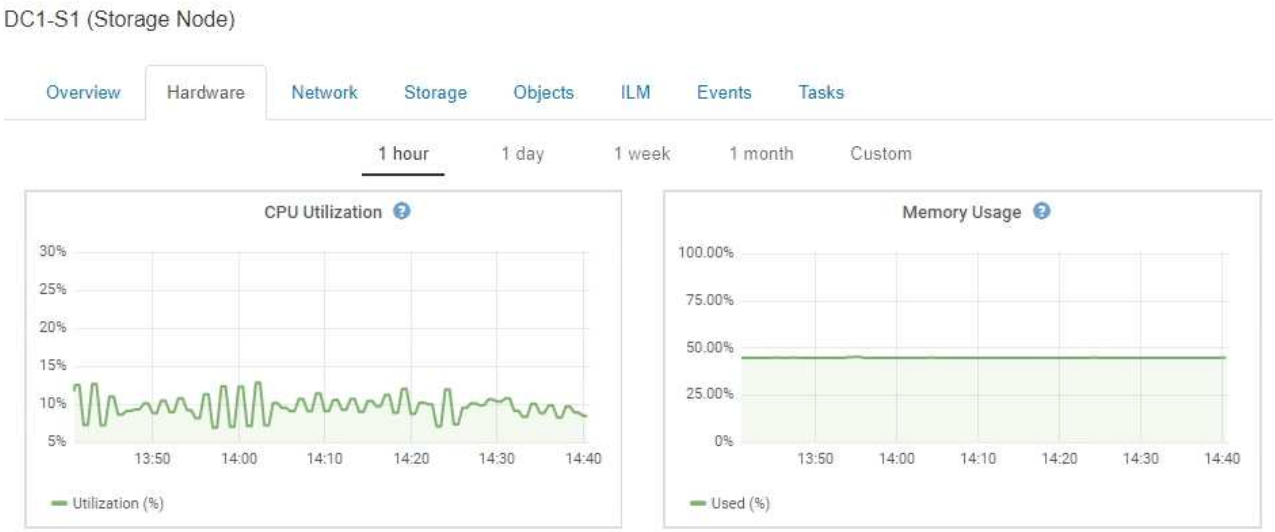
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Sind Nodes konsistent überlastet, sind möglicherweise mehr Nodes erforderlich, um einen effizienten Betrieb zu gewährleisten.

Schritte

1. So zeigen Sie Informationen zur Hardwareauslastung eines Grid-Node an:
   a. Wählen Sie auf der Seite **Nodes** den Knoten aus.
   b. Wählen Sie die Registerkarte **Hardware** aus, um Grafiken der CPU-Auslastung und der Speicherauslastung anzuzeigen.



c. 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.

d. 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

"Anzeigen von Informationen zu Appliance-Speicherknoten"

"Anzeigen von Informationen zu Appliance Admin Nodes und Gateway Nodes"

Monitoring der Mandantenaktivitäten

Alle Client-Aktivitäten sind mit einem Mandantenkonto verknüpft. Mit dem Grid Manager lässt sich die Storage-Nutzung oder der Netzwerk-Traffic eines Mandanten überwachen. Alternativ können mit dem Audit-Protokoll oder Grafana Dashboards ausführlichere Informationen zur Verwendung von StorageGRID durch Mandanten erstellt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über Root Access oder Administrator-Berechtigung verfügen.

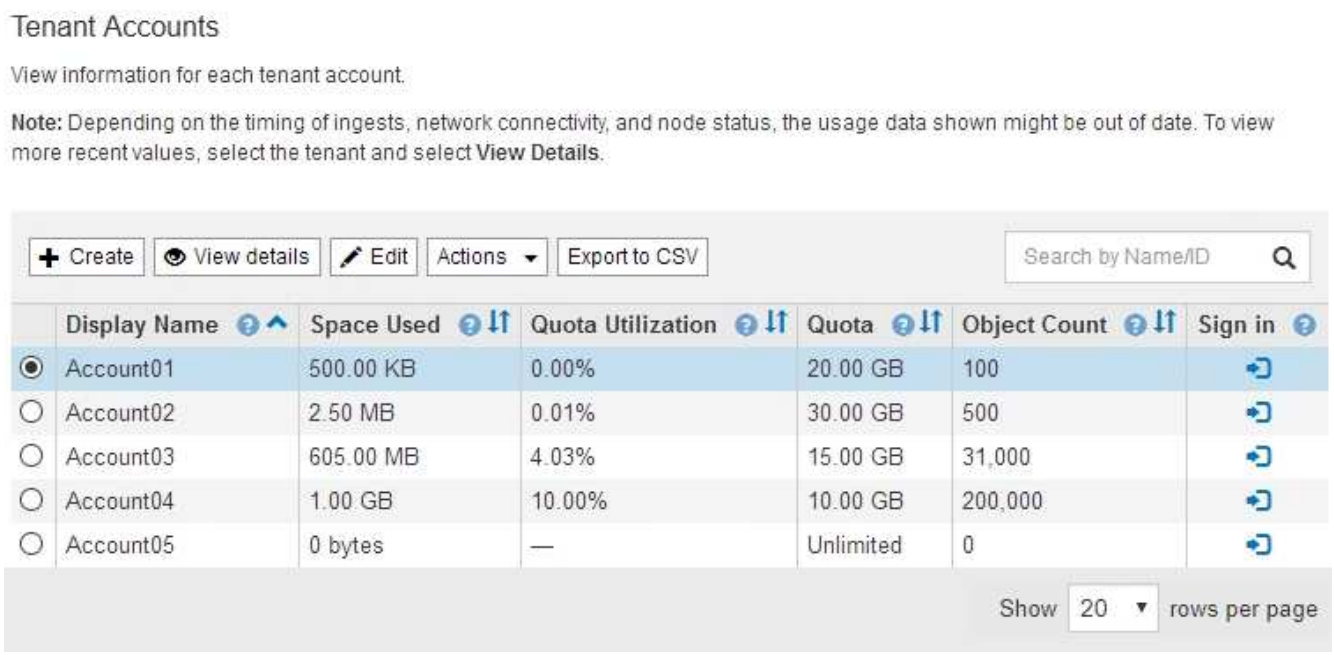
Über diese Aufgabe

Die Werte für den genutzten Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

Schritte

1. Wählen Sie **Mieter** aus, um den von allen Mietern genutzten Speicherplatz zu überprüfen.

   Für jeden Mandanten werden der genutzte Speicherplatz, die Kontingentnutzung, die Kontingente und die Objektanzahl aufgelistet. Wenn kein Kontingent für einen Mandanten festgelegt ist, enthält das Feld Quotenauslastung einen Strich (-) und das Quota-Feld gibt „`Unlimited`“ an.



Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

Sie können sich bei einem Mandantenkonto anmelden, indem Sie den Link in der Spalte **Anmelden** der Tabelle auswählen.

2. Wählen Sie optional **in CSV exportieren** aus, um eine .csv-Datei anzuzeigen und zu exportieren, die die Nutzungswerte für alle Mandanten enthält.

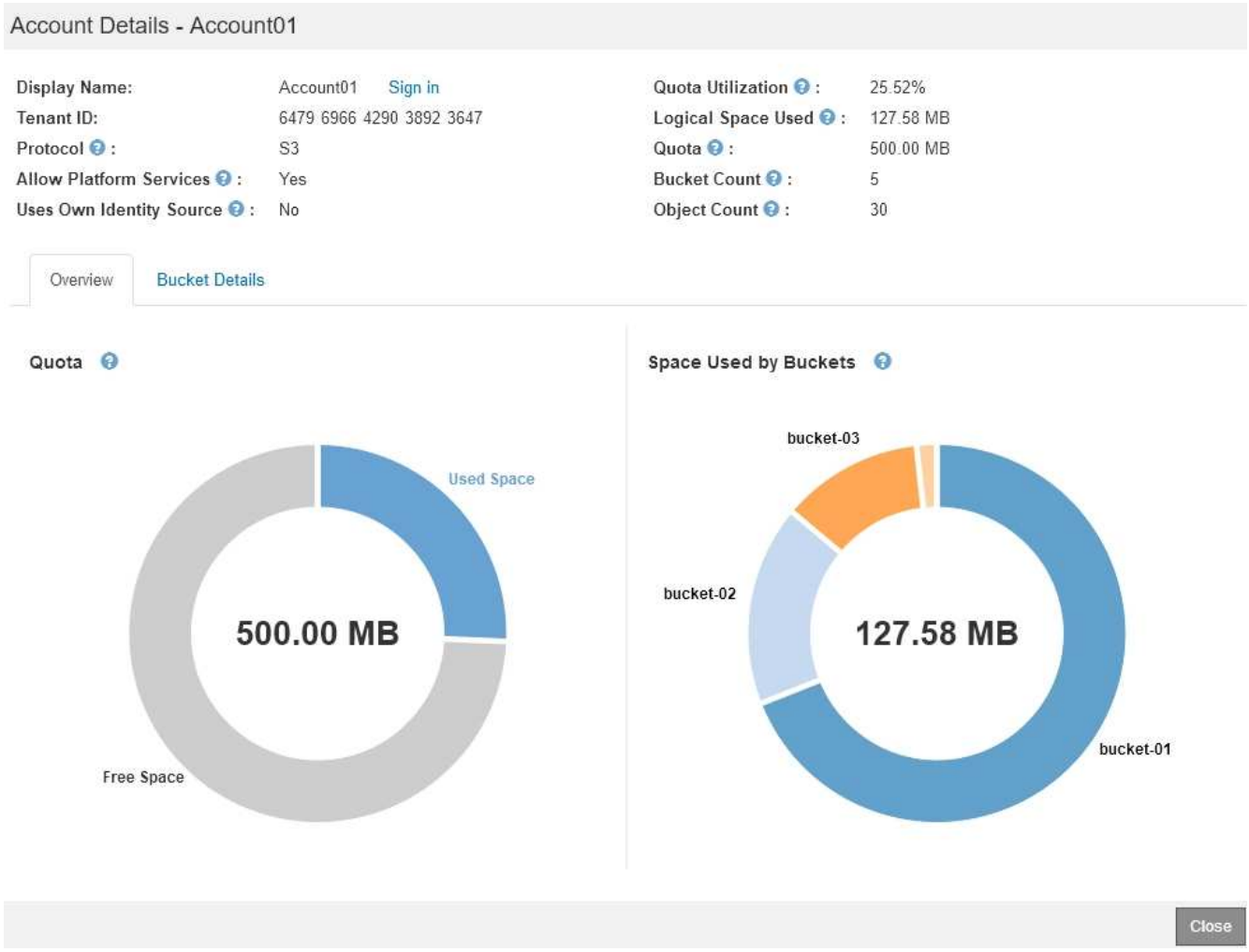
   Sie werden aufgefordert, das zu öffnen oder zu speichern `.csv` Datei:

   Der Inhalt einer .csv-Datei sieht wie das folgende Beispiel aus:

   Sie können die .csv-Datei in einer Tabellenkalkulationsanwendung öffnen oder sie automatisiert verwenden.

3. Um Details für einen bestimmten Mieter einschließlich der Nutzungsdiagramme anzuzeigen, wählen Sie auf der Seite Mandantenkonten das Mandantenkonto aus und wählen dann **Details anzeigen**.

   Die Seite Kontodetails wird angezeigt und enthält zusammenfassende Informationen, ein Diagramm, das die Anzahl der verwendeten und verbleibenden Kontingente darstellt, sowie ein Diagramm, das die Menge der Objektdaten in Buckets (S3) oder Containern (Swift) darstellt.



- **Quote**

  Wenn für diesen Mieter eine Quote festgelegt wurde, zeigt das Diagramm **quota** an, wie viel von dieser Quote dieser Mieter verwendet hat und wie viel noch verfügbar ist. Wenn kein Kontingent festgelegt wurde, hat der Mieter eine unbegrenzte Quote und eine Informationsmeldung wird angezeigt. 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 Segment „verwendeter Speicherplatz“ platzieren, um die Anzahl der gespeicherten Objekte und die insgesamt verwendeten Bytes anzuzeigen. Sie können den Cursor über das Segment Freier Speicherplatz platzieren, um zu sehen, wie viele Bytes Speicherplatz verfügbar sind.

  > 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.

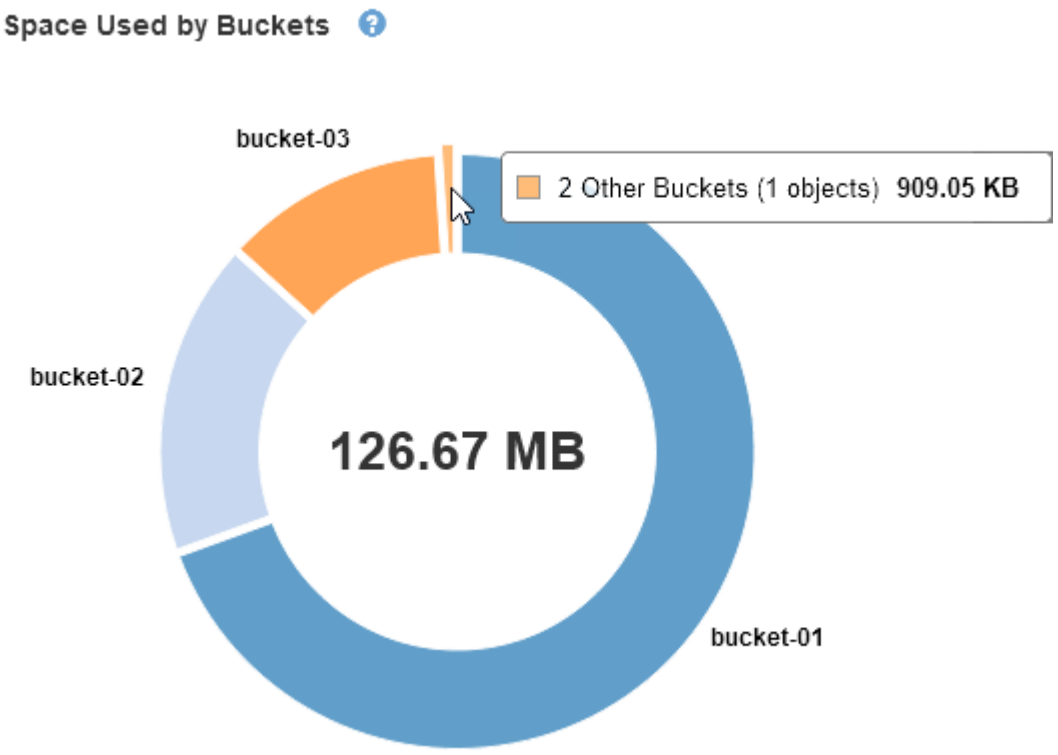
Die Kontingentnutzung eines Mandanten gibt die Gesamtanzahl der Objektdaten an, die der Mandant auf StorageGRID (logische Größe) hochgeladen hat. Die Kontingentnutzung stellt nicht den Speicherplatz dar, der zur Speicherung von Kopien dieser Objekte und ihrer Metadaten verwendet wird (physische Größe).

Sie können die Warnung * Tenant Quotenverbrauch hoch* aktivieren, um festzustellen, ob Mieter ihre Quoten verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Weitere Informationen finden Sie in der Referenz zu Warnmeldungen.

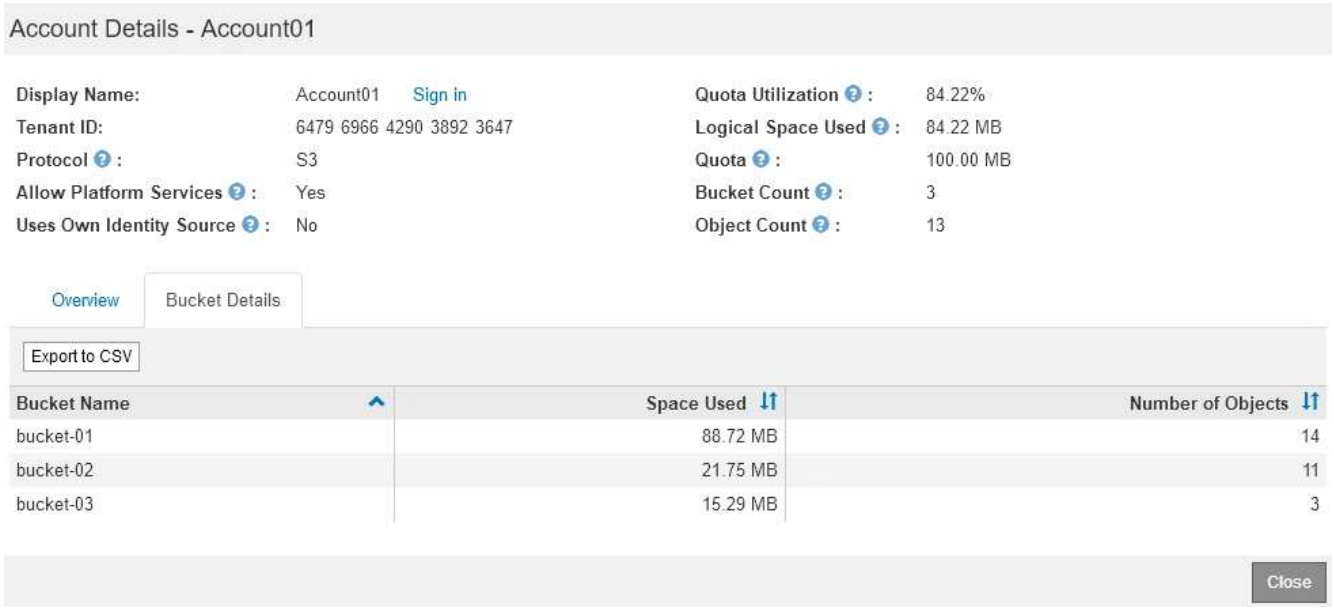
- **Verwendeter Platz**

  Das Diagramm **Space used by Buckets** (S3) or **Space used by Containers** (Swift) zeigt die größten Eimer für den Mieter. Der verwendete Speicherplatz ist die Gesamtgröße der Objektdaten im Bucket. Dieser Wert stellt nicht den Storage-Platzbedarf für ILM-Kopien und Objekt-Metadaten dar.

  Wenn der Mandant mehr als neun Buckets oder Container enthält, werden sie in einem Segment zusammengefasst, das als „Sonstige“ bezeichnet wird. Einige Diagrammsegmente sind möglicherweise zu klein, um ein Etikett aufzunehmen. Sie können den Cursor auf ein beliebiges Segment setzen, um die Beschriftung zu sehen und weitere Informationen zu erhalten, darunter die Anzahl der gespeicherten Objekte und die Gesamtzahl der Bytes für jeden Bucket oder Container.



4. Wählen Sie **Bucket Details** (S3) oder **Container Details** (Swift) aus, um eine Liste der verwendeten Abstände und die Anzahl der Objekte für die einzelnen Buckets oder Container des Mandanten anzuzeigen.



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.

   Sie werden aufgefordert, die .csv-Datei zu öffnen oder zu speichern.

   Der Inhalt der .csv-Datei eines einzelnen S3-Mandanten sieht wie folgt aus:

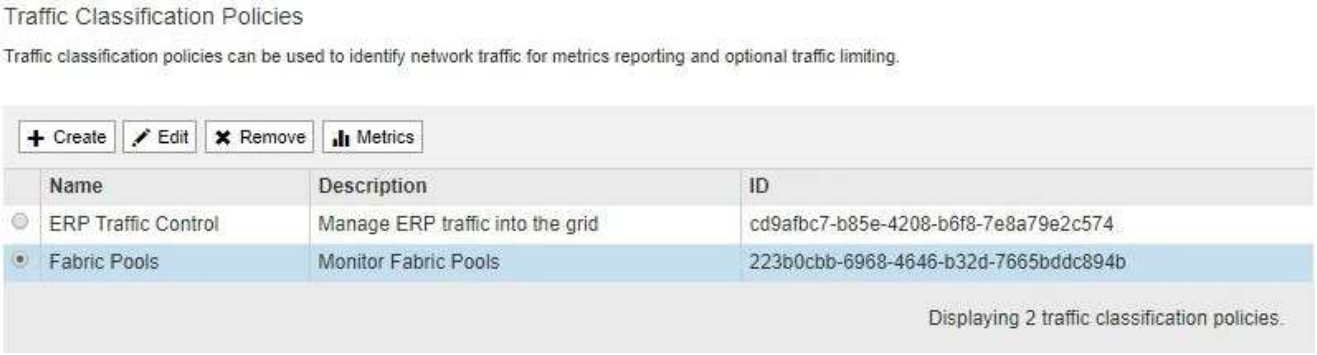
Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   Sie können die .csv-Datei in einer Tabellenkalkulationsanwendung öffnen oder sie automatisiert verwenden.

6. Wenn Richtlinien zur Traffic-Klassifizierung für einen Mandanten vorhanden sind, überprüfen Sie den Netzwerkverkehr für diesen Mandanten.

   a. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

      Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



   a. Anhand der Liste der Richtlinien können Sie diejenigen ermitteln, die für einen bestimmten Mandanten

gelten.

b. Um Metriken anzuzeigen, die mit einer Richtlinie verknüpft sind, wählen Sie das Optionsfeld links neben der Richtlinie aus, und klicken Sie dann auf **Metriken**.

c. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

   Informationen zum Erstellen, Bearbeiten oder Löschen von Richtlinien für die Verkehrsklassifizierung finden Sie in den Anweisungen für die Verwaltung von StorageGRID.

7. Optional können Sie das Audit-Protokoll verwenden, um eine granularere Überwachung der Aktivitäten eines Mandanten zu ermöglichen.

   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. Weitere Informationen finden Sie in den Anweisungen zum Verständnis von Überwachungsmeldungen.

8. Optional können Sie mit den Prometheus Kennzahlen die Mandantenaktivität erfassen:

   - Wählen Sie im Grid Manager die Option **Support** > **Tools** > **Metriken** aus. 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 **Hilfe** > **API-Dokumentation**. Sie können die Kennzahlen im Abschnitt „Kennzahlen“ der Grid Management API verwenden, um benutzerdefinierte Alarmregeln und Dashboards für Mandantenaktivitäten zu erstellen.

Verwandte Informationen

"Alerts Referenz"

"Prüfung von Audit-Protokollen"

"StorageGRID verwalten"

"Überprüfen von Support-Metriken"

Monitoring der 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.

Was Sie benötigen

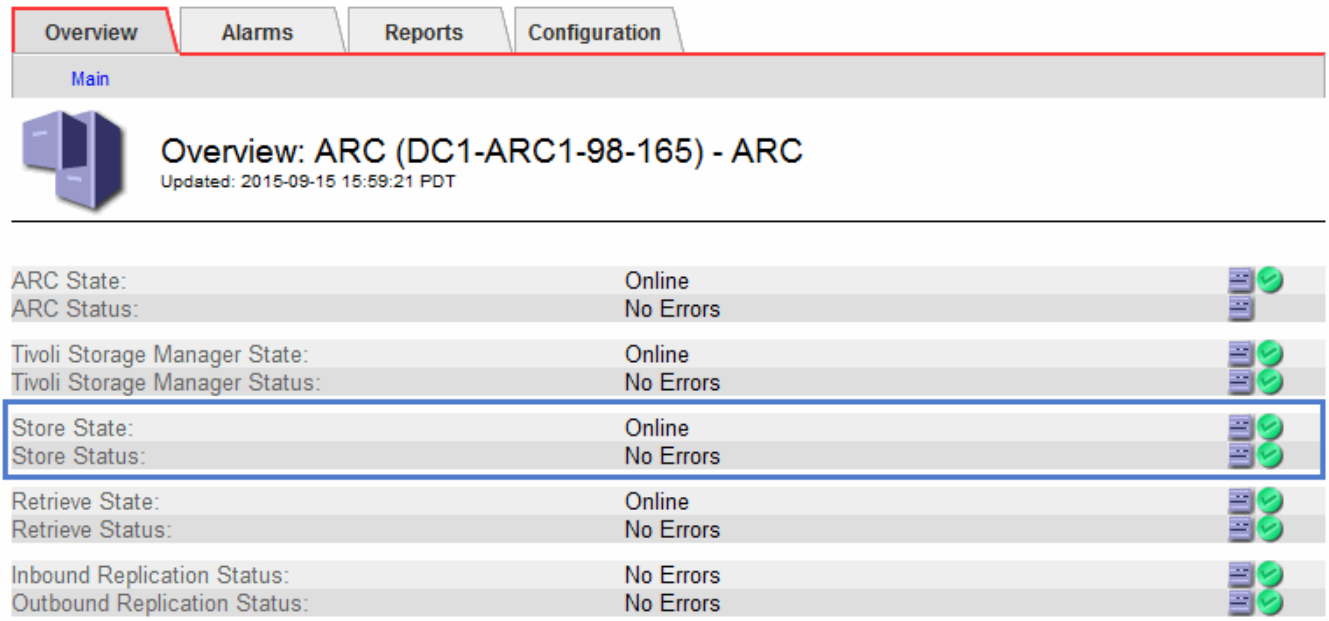
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 Topology** 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.



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.

Verwandte Informationen

"StorageGRID verwalten"

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Sie können den Load Balancer-Service auf Admin-Nodes oder Gateway-Nodes, einen externen Load Balancer eines Drittanbieters oder den CLB-Service auf Gateway-Knoten verwenden, um Client-Anforderungen über mehrere Storage-Nodes zu verteilen.

Der CLB-Service ist veraltet.

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.

Lesen Sie den Abschnitt zum Konfigurieren von Client-Verbindungen in den Anweisungen zur Administration von StorageGRID.

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. Überprüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle des Master hat.

      Nodes mit der Rolle „Master“ und Nodes, die sich nicht in einer HA-Gruppe befinden, sollten Anfragen aktiv an die Clients verteilen.

   d. Wählen Sie für jeden Knoten, der Clientanforderungen aktiv verteilen soll, die Registerkarte **Load Balancer** aus.
   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 anhand von Traffic-Klassifizierungsrichtlinien eine detailliertere Aufschlüsselung des vom Load Balancer Service servierten Datenverkehrs anzeigen.
2. Wenn S3- oder Swift-Clients eine Verbindung über den CLB-Service (veraltet) herstellen, führen Sie die folgenden Prüfungen durch:
   a. Wählen Sie **Knoten**.
   b. Wählen Sie einen Gateway-Node aus.
   c. Überprüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle des Master hat.

      Nodes mit der Rolle „Master“ und Nodes, die sich nicht in einer HA-Gruppe befinden, sollten Anfragen

aktiv an die Clients verteilen.

d. Wählen Sie für jeden Gateway Node, der Clientanforderungen aktiv verteilen soll, **Support** > **Tools** > **Grid Topology** aus.

e. Wählen Sie ***Gateway Node*** > **CLB** > **HTTP** > **Übersicht** > **Main** aus.

f. Überprüfen Sie die Anzahl der **eingehenden Sitzungen - eingerichtet**, um zu überprüfen, ob der Gateway-Node aktiv Anforderungen bearbeitet hat.

3. 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.

Verwandte Informationen

"StorageGRID verwalten"

"Anzeigen der Registerkarte Load Balancer"

Anwenden von Hotfixes oder Aktualisieren der Software, falls erforderlich

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

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

"NetApp Downloads: StorageGRID"

2. 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*

3. Überprüfen Sie die Änderungen, die im Update enthalten sind:

a. Wählen Sie die Version aus dem Pulldown-Menü aus und klicken Sie auf **Go**.

b. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.

c. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.

Die Download-Seite für die ausgewählte Version wird angezeigt.

4. Erfahren Sie mehr über die Änderungen in der Softwareversion oder Hotfix.

- Informationen zu einer neuen Softwareversion finden Sie im Thema „`Was ist neu`“ in den Anweisungen zum Aktualisieren von StorageGRID.
- Für einen Hotfix laden Sie die README-Datei herunter, um eine Zusammenfassung der Änderungen im Hotfix zu erhalten.

5. Wenn Sie entscheiden, dass ein Softwareupdate erforderlich ist, suchen Sie die Anweisungen, bevor Sie fortfahren.
   - Folgen Sie bei einer neuen Softwareversion sorgfältig den Anweisungen für das Upgrade von StorageGRID.
   - Suchen Sie bei einem Hotfix in der Recovery- und Wartungsanleitung nach dem Hotfix-Verfahren

Verwandte Informationen

"Software-Upgrade"

"Verwalten Sie erholen"

Verwalten von Meldungen und Alarmen

Das StorageGRID Alert System wurde entwickelt, um Sie über betriebliche Probleme zu informieren, die Ihre Aufmerksamkeit erfordern. Bei Bedarf können Sie auch das alte Alarmsystem zur Überwachung Ihres Systems verwenden. Dieser Abschnitt enthält die folgenden Unterabschnitte:

- "Vergleichen von Meldungen und Alarmen"
- "Verwalten von Meldungen"
- "Verwalten von Alarmen (Altsystem)"

StorageGRID beinhaltet zwei Systeme, mit denen Sie über Probleme informiert werden.

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 Dashboard im Grid Manager wird ein Symbol für den Schweregrad „Meldungen“ angezeigt, und die Anzahl der aktuellen Meldungen wird erhöht.
- Die Warnmeldung wird 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

Das Alarmsystem wird unterstützt, gilt jedoch als ein altes System. 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.

Wenn ein Alarm ausgelöst wird, treten folgende Aktionen auf:

- Die Anzahl der älteren Alarme auf dem Dashboard wird erhöht.
- 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 Alarme gesendet.)

Vergleichen von Meldungen und Alarmen

Es gibt eine Reihe von 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?	• Klicken Sie im Dashboard auf den Link **Aktuelle Alarme**. • Klicken Sie auf der Seite **Nodes** > **Übersicht** auf den Hinweis. • Wählen Sie **Alarme** > **Aktuell**. "Anzeigen aktueller Meldungen"	• Klicken Sie im Dashboard auf den Link **Legacy-Alarme**. • Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**. "Anzeigen von Legacy-Alarmen"
Was bewirkt, dass eine Meldung oder eine Warnung ausgelöst wird?	Alarme werden ausgelöst, wenn ein Prometheus-Ausdruck in einer Alarmregel für die spezifische Triggerbedingung und -Dauer als wahr bewertet wird. "Anzeigen von Meldungsregeln"	Alarme werden ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht. "Alarmauslöselogik (Älteres System)"

	Meldungen	Alarme (Altsystem)
Wie kann ich das zugrunde liegende Problem lösen, wenn eine Meldung oder ein Alarm ausgelöst wird?	Die empfohlenen Aktionen für eine Warnmeldung sind in E-Mail-Benachrichtigungen enthalten und stehen auf den Alerts-Seiten im Grid Manager zur Verfügung. Falls erforderlich, werden weitere Informationen in der StorageGRID-Dokumentation bereitgestellt. "Alerts Referenz"	Sie können sich über einen Alarm informieren, indem Sie auf den Attributnamen klicken. Alternativ können Sie in der StorageGRID-Dokumentation nach einem Alarmcode suchen. "Alarmreferenz (Altsystem)"
Wo kann eine Liste der Warnungen oder Alarme gelöst werden?	• Klicken Sie auf dem Dashboard auf den Link * Kürzlich aufgelöste Warnmeldungen*. • Wählen Sie **Alarme** > **Aufgelöst**. "Anzeigen gelöster Warnmeldungen"	Wählen Sie **Support** > **Alarme (alt)** > **Historische Alarme**. "Überprüfung historischer Alarme und Alarmfrequenz (Altsystem)"
Wo kann ich die Einstellungen verwalten?	Wählen Sie **Alarme**. Verwenden Sie anschließend die Optionen im Menü Meldungen. "Verwalten von Meldungen"	Wählen Sie **Support**. Verwenden Sie dann die Optionen im Abschnitt **Alarme (alt)** des Menüs. "Verwalten von Alarmen (Altsystem)"
Welche Benutzergruppenberechtigungen brauche ich?	• Jeder, der sich beim Grid Manager anmelden kann, kann aktuelle und behobene Warnmeldungen anzeigen. • Sie müssen über die Berechtigung zum Verwalten von Warnungen verfügen, um Stille, Warnmeldungen und Alarmregeln zu verwalten. "StorageGRID verwalten"	• Jeder, der sich beim Grid Manager anmelden kann, kann ältere Alarme anzeigen. • Sie müssen über die Berechtigung Alarme quittieren verfügen, um Alarme zu quittieren. • Zur Verwaltung globaler Alarme und E-Mail-Benachrichtigungen müssen Sie sowohl über die Seitenkonfiguration der Grid-Topologie als auch über andere Grid-Konfigurationen verfügen. "StorageGRID verwalten"

	Meldungen	Alarme (Altsystem)
Wie managt ich E-Mail-Benachrichtigungen?	Wählen Sie **Alarme** > **E-Mail-Einrichtung**. **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. "Verwalten von Warnmeldungen"	Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. "Konfigurieren von Benachrichtigungen für Alarme (Legacy-System)"
Wie verwalte ich SNMP Benachrichtigungen?	Wählen Sie **Konfiguration** > **Überwachung** > **SNMP-Agent**. "Verwendung von SNMP-Überwachung"	Wählen Sie **Konfiguration** > **Überwachung** > **SNMP-Agent**. "Verwendung von SNMP-Überwachung" **Hinweis**: SNMP-Benachrichtigungen werden nicht für jeden Alarm oder Alarm Schweregrad gesendet. "Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"
Wie kontrolliere ich, wer Benachrichtigungen erhält?	1. Wählen Sie **Alarme** > **E-Mail-Einrichtung**. 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. "Einrichten von E-Mail-Benachrichtigungen für Meldungen"	1. Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. 2. Mailingliste wird erstellt. 3. Wählen Sie **Benachrichtigungen**. 4. Wählen Sie die Mailingliste aus. "Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)" "Konfigurieren von E-Mail-Benachrichtigungen für Alarme (Altsystem)"
Welche Admin Nodes senden Benachrichtigungen?	Ein einziger Admin-Node (der „`bevorzugte Absender`“). "StorageGRID verwalten"	Ein einziger Admin-Node (der „`bevorzugte Absender`“). "StorageGRID verwalten"

	Meldungen	Alarme (Altsystem)
Wie kann ich einige Benachrichtigungen unterdrücken?	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. **Hinweis**: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. "Stummschalten von Warnmeldungen"	1. Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. 2. Wählen Sie **Benachrichtigungen**. 3. Wählen Sie eine Mailingliste aus, und wählen Sie **unterdrücken**. "Unterdrückung von Alarmmeldungen für eine Mailingliste (Legacy-System)"
Wie kann ich alle Benachrichtigungen unterdrücken?	Wählen Sie **Alarme** > **Stille** und dann **Alle Regeln**. **Hinweis**: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. "Stummschalten von Warnmeldungen"	1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**. 2. Aktivieren Sie das Kontrollkästchen **Benachrichtigung Alle unterdrücken**. **Hinweis**: Das Unterdrückung von E-Mail-Benachrichtigungen systemweit unterdrückt auch ereignisgesteuerte AutoSupport-E-Mails. "Systemweite Unterdrückung von E-Mail-Benachrichtigungen"

	Meldungen	Alarme (Altsystem)
Wie kann ich die Bedingungen und Trigger anpassen?	1. Wählen Sie **Alarme** > **Warnregeln**. 2. Wählen Sie eine Standardregel zum Bearbeiten aus, oder wählen Sie **benutzerdefinierte Regel erstellen**. "Bearbeiten einer Meldungsregel" "Erstellen benutzerdefinierter Warnungsregeln"	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. "Erstellen von globalen benutzerdefinierten Alarmen (Legacy-System)"
Wie deaktiviere ich eine einzelne Warnung oder einen einzelnen Alarm?	1. Wählen Sie **Alarme** > **Warnregeln**. 2. Wählen Sie die Regel aus, und klicken Sie auf **Regel bearbeiten**. 3. Deaktivieren Sie das Kontrollkästchen **aktiviert**. "Deaktivieren einer Meldungsregel"	1. Wählen Sie **Support** > **Alarme (alt)** > **Globale Alarme**. 2. Wählen Sie die Regel aus, und klicken Sie auf das Symbol Bearbeiten. 3. Deaktivieren Sie das Kontrollkästchen **aktiviert**. "Deaktivieren eines Standardalarms (älteres System)" "Deaktivieren von globalen benutzerdefinierten Alarmen (Legacy-System)"

Verwalten von Meldungen

Mithilfe von Meldungen können Sie verschiedene Ereignisse und Bedingungen innerhalb des StorageGRID Systems überwachen. Sie können Benachrichtigungen verwalten, indem Sie benutzerdefinierte Warnmeldungen erstellen, Standardwarnungen bearbeiten oder deaktivieren, E-Mail-Benachrichtigungen für Warnungen einrichten und Benachrichtigungen deaktivieren.

Verwandte Informationen

"Anzeigen aktueller Meldungen"

"Anzeigen gelöster Warnmeldungen"

"Anzeigen einer bestimmten Meldung"

"Alerts Referenz"

Um welche Warnmeldungen geht es

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

- Das Warnsystem konzentriert sich auf umsetzbare Probleme im System. Anders als bei einigen Alarmen im Legacy-System werden bei Ereignissen, die eine sofortige Aufmerksamkeit erfordern, Warnmeldungen ausgelöst und nicht bei Ereignissen, die sicher ignoriert werden können.
- Die Seite „Aktuelle Meldungen“ bietet eine benutzerfreundliche Oberfläche zum Anzeigen aktueller Probleme. Sie können die Liste nach einzelnen Warnungen und Alarmgruppen sortieren. Beispielsweise können Sie alle Meldungen nach Node/Standort sortieren, um zu sehen, welche Meldungen sich auf einen bestimmten Node auswirken. Oder Sie möchten die Meldungen in einer Gruppe nach der Zeit sortieren, die ausgelöst wird, um die letzte Instanz einer bestimmten Warnmeldung zu finden.
- Die Seite „gelöste Warnmeldungen“ enthält ähnliche Informationen wie auf der Seite „Aktuelle Meldungen“. Sie können jedoch einen Verlauf der behobenen Warnmeldungen suchen und anzeigen, einschließlich des Auslöseverlaufs und der Behebung des Alarms.
- Mehrere Warnmeldungen desselben Typs werden in einer E-Mail gruppiert, um die Anzahl der Benachrichtigungen zu reduzieren. Darüber hinaus werden auf der Seite „Meldungen“ mehrere Warnmeldungen desselben Typs als Gruppe angezeigt. Sie können Warnungsgruppen erweitern oder ausblenden, um die einzelnen Warnmeldungen ein- oder auszublenden. Wenn z. B. mehrere Knoten die Meldung **nicht in der Lage, mit Knoten** zu kommunizieren ungefähr zur gleichen Zeit melden, wird nur eine E-Mail gesendet und die Warnung wird als Gruppe auf der Seite Warnungen angezeigt.
- Warnmeldungen verwenden intuitive Namen und Beschreibungen, um das Problem schnell zu verstehen. Meldungsbenachrichtigungen umfassen Details zum betroffenen Node und Standort, den Schweregrad der Warnmeldung, den Zeitpunkt, zu dem die Meldungsregel ausgelöst wurde, und den aktuellen Wert der Metriken in Bezug auf die Meldung.
- Warnmeldungen per E-Mail und die auf den Seiten „Aktuelle Warnmeldungen und gelöste Warnmeldungen“ angezeigten Warnmeldungen enthalten empfohlene Aktionen zur Behebung von Warnmeldungen. Dazu gehören häufig direkte Links zum StorageGRID Dokumentationszentrum, damit detailliertere Fehlerbehebungsmaßnahmen leichter gefunden und zugänglich sind.
- Wenn Sie die Benachrichtigungen für eine Warnung vorübergehend auf einem oder mehreren Schweregraden unterdrücken müssen, können Sie ganz einfach eine bestimmte Alarmregel für eine bestimmte Dauer und für das gesamte Grid, eine einzelne Site oder einen einzelnen Node stummschalten. Sie können auch während einer geplanten Wartung, z. B. einer Software-Aktualisierung, alle Alarmregeln stummschalten.
- Sie können die standardmäßigen Alarmregeln nach Bedarf bearbeiten. Sie können eine Meldungsregel vollständig deaktivieren oder deren Triggerbedingungen und -Dauer ändern.
- Sie können benutzerdefinierte Alarmregeln erstellen, um auf die für Ihre Situation relevanten spezifischen Bedingungen abzielen und eigene Empfehlungen auszuarbeiten. Um die Bedingungen für eine benutzerdefinierte Warnung zu definieren, erstellen Sie Ausdrücke mithilfe der Prometheus-Metriken, die im Abschnitt Kennzahlen der Grid Management API verfügbar sind.

Verwalten von Meldungsregeln

Alarmregeln definieren die Bedingungen, die bestimmte Warnmeldungen auslösen. StorageGRID enthält eine Reihe von Standardwarnregeln, die Sie unverändert verwenden oder ändern können, oder Sie können individuelle Alarmregeln erstellen.

Anzeigen von Meldungsregeln

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.

Was Sie benötigen

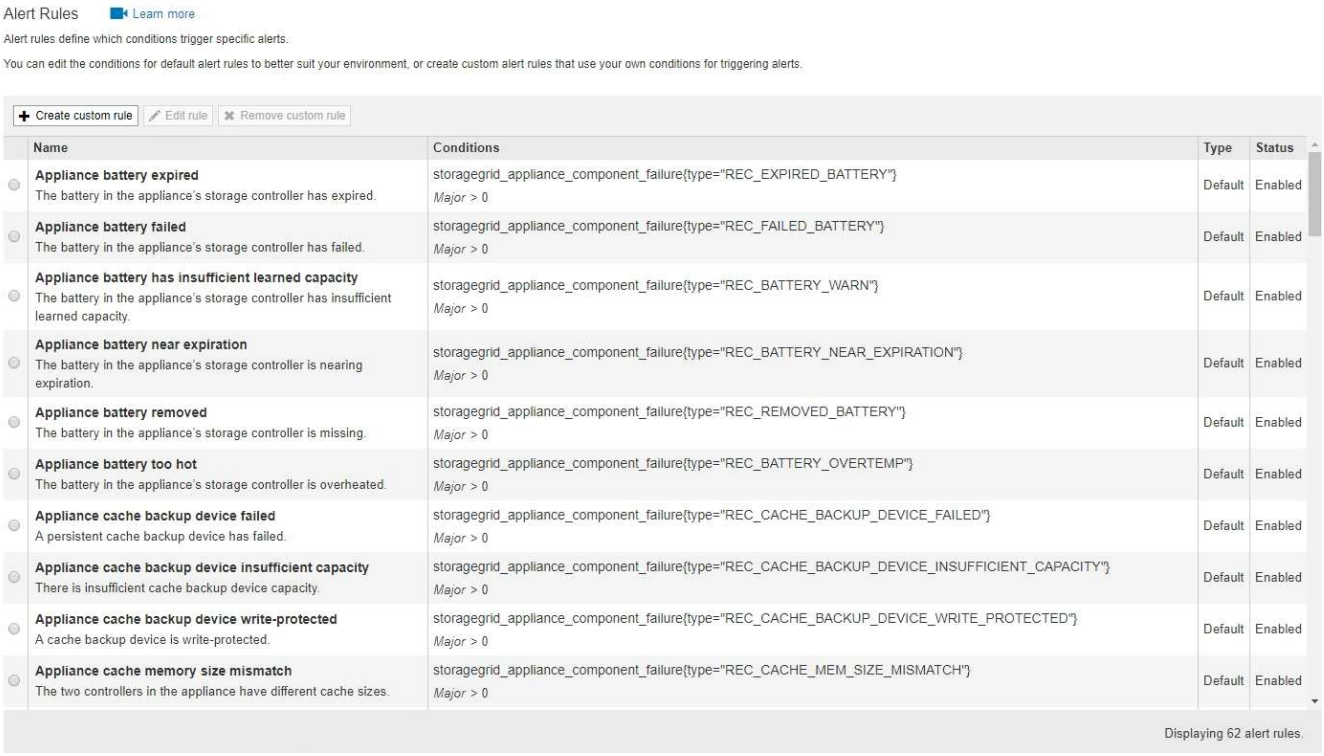
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.



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	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. • * 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 sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
Typ	Der Typ der Warnregel: • **Standard**: Eine mit dem System bereitgestellte Warnregel. Sie können eine Standardwarnregel deaktivieren oder die Bedingungen und Dauer für eine Standardwarnregel bearbeiten. Sie können keine Standardwarnregel entfernen. • **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.

Spaltenüberschrift	Beschreibung
Status	Gibt an, ob diese Warnungsregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnregeln werden nicht ausgewertet, sodass keine Warnmeldungen ausgelöst werden.

Verwandte Informationen

"Alerts Referenz"

Erstellen benutzerdefinierter Warnungsregeln

Sie können benutzerdefinierte Alarmregeln erstellen, um eigene Bedingungen für das Auslösen von Warnmeldungen zu definieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

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.
- Wenn Sie einen Ausdruck mit der Grid Management API testen, beachten Sie, dass eine „`successful`“-Antwort einfach nur ein leerer Antwortkörper sein kann (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 Meldung funktioniert, es sei denn, Sie haben überprüft, dass die Meldung erwartungsgemäß ausgelöst wird.

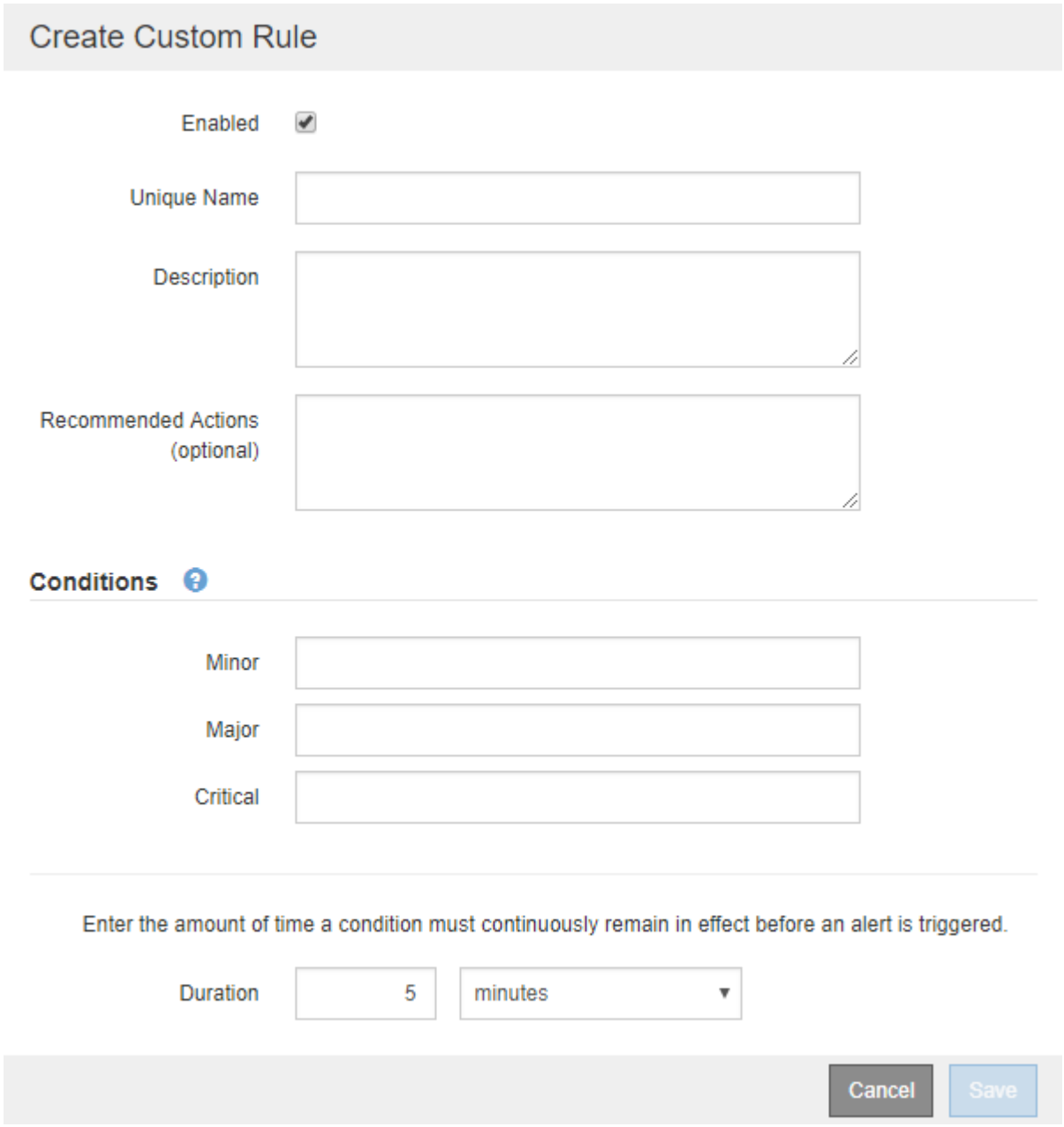
Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie **eigene Regel erstellen**.

Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.



3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **aktiviert**, um festzustellen, ob diese Alarmregel derzeit aktiviert ist.

   Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

4. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der 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 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.

   Klicken Sie auf das Hilfesymbol, um verfügbare Metriken anzuzeigen und Prometheus-Ausdrücke zu testen Und folgen Sie dem Link zum Abschnitt Metriken der Grid Management API.

   Informationen über die Verwendung der Grid-Management-API finden Sie in den Anweisungen für die Administration von StorageGRID. Einzelheiten zur Syntax der Prometheus-Abfragen finden Sie in der Dokumentation für Prometheus.

   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
   ```

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. Klicken Sie Auf **Speichern**.

   Das Dialogfeld wird geschlossen, und die neue benutzerdefinierte Alarmregel wird in der Tabelle Alarmregeln angezeigt.

Verwandte Informationen

"StorageGRID verwalten"

"Häufig verwendete Prometheus-Kennzahlen"

"Prometheus: Grundlagen der Abfrage"

Bearbeiten einer Meldungsregel

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

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.

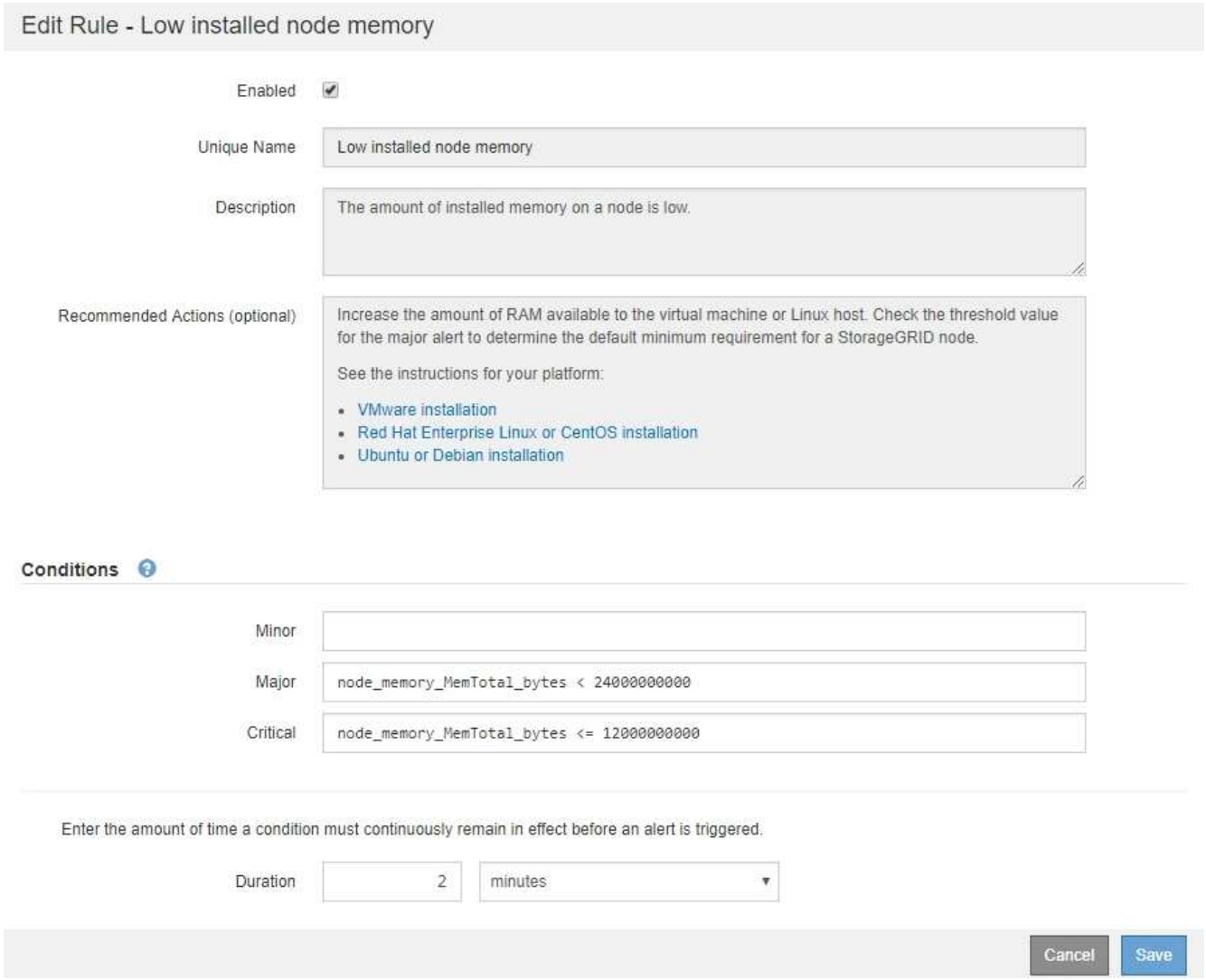
Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   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. In diesem Beispiel wird eine Standardwarnregel angezeigt: Die Felder eindeutiger Name, Beschreibung und empfohlene Aktionen sind deaktiviert und können nicht bearbeitet werden.



4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **aktiviert**, um festzustellen, ob diese Alarmregel derzeit aktiviert ist.

   Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen 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.

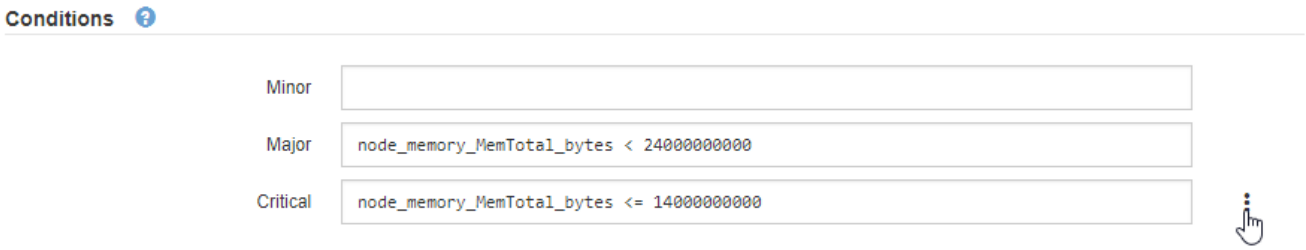
5. Aktualisieren Sie für benutzerdefinierte Warnungsregeln die folgenden Informationen, falls erforderlich.

   Diese Informationen können nicht für Standardwarnregeln bearbeitet werden.

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 Formatierungscodes). 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, klicken Sie rechts neben der geänderten Bedingung auf die drei Punkte.



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 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.

Klicken Sie auf das Hilfesymbol, um verfügbare Metriken anzuzeigen und Prometheus-Ausdrücke zu testen Und folgen Sie dem Link zum Abschnitt Metriken der Grid Management API.

Informationen über die Verwendung der Grid-Management-API finden Sie in den Anweisungen für die Administration von StorageGRID. Einzelheiten zur Syntax der Prometheus-Abfragen finden Sie in der Dokumentation für Prometheus.

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. Klicken Sie Auf **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.

Verwandte Informationen

"StorageGRID verwalten"

"Häufig verwendete Prometheus-Kennzahlen"

"Prometheus: Grundlagen der Abfrage"

Deaktivieren einer Meldungsregel

Sie können den aktivierten/deaktivierten Status für eine Standard- oder eine benutzerdefinierte Warnungsregel ändern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Über diese Aufgabe

Wenn eine Meldungsregel deaktiviert ist, werden seine Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen 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 **Alarme** > **Warnregeln**.

   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 **aktiviert**, um festzustellen, ob diese Alarmregel derzeit aktiviert ist.

   Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen 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. Klicken Sie Auf **Speichern**.

   Deaktiviert wird in der Spalte **Status** angezeigt.

Entfernen einer benutzerdefinierten Warnungsregel

Sie können eine benutzerdefinierte Alarmregel entfernen, wenn Sie sie nicht mehr verwenden möchten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie das Optionsfeld für die benutzerdefinierte Alarmregel, die Sie entfernen möchten.

   Sie können keine Standardwarnregel entfernen.

3. Klicken Sie auf **Benutzerdefinierte Regel entfernen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf **OK**, um die Warnregel zu entfernen.

   Alle aktiven Instanzen der Warnmeldung werden innerhalb von 10 Minuten behoben.

Verwalten von Warnmeldungen

Wenn eine Warnmeldung ausgelöst wird, kann StorageGRID E-Mail-Benachrichtigungen und SNMP-Benachrichtigungen (Simple Network Management Protocol) senden.

Einrichten von SNMP-Benachrichtigungen für Alarme

Wenn StorageGRID SNMP-Benachrichtigungen senden soll, wenn Warnmeldungen auftreten, müssen Sie den StorageGRID SNMP-Agent aktivieren und ein oder mehrere Trap-Ziele konfigurieren.

Über diese Aufgabe

Sie können im Grid Manager die Option **Konfiguration** > **Überwachung** > **SNMP-Agent** 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 im Abschnitt zur Verwendung der SNMP-Überwachung.

Nachdem Sie den StorageGRID SNMP-Agent konfiguriert haben, können zwei Arten von ereignisgesteuerten Benachrichtigungen gesendet werden:

- Traps sind Benachrichtigungen, die vom SNMP-Agent gesendet werden, die keine Bestätigung durch das Managementsystem benötigen. 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. Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde. Standardmäßig ist der primäre Admin-Node ausgewählt. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

> Trap- und Informieren-Benachrichtigungen werden auch dann gesendet, wenn bestimmte Alarme (Legacy-System) mit einem bestimmten Schweregrad oder höher ausgelöst werden. SNMP-Benachrichtigungen werden jedoch nicht für jeden Alarm oder jeden Schweregrad gesendet.

Verwandte Informationen

"Verwendung von SNMP-Überwachung"

"Stummschalten von Warnmeldungen"

"StorageGRID verwalten"

"Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"

Einrichten von E-Mail-Benachrichtigungen für Meldungen

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Was Sie benötigen

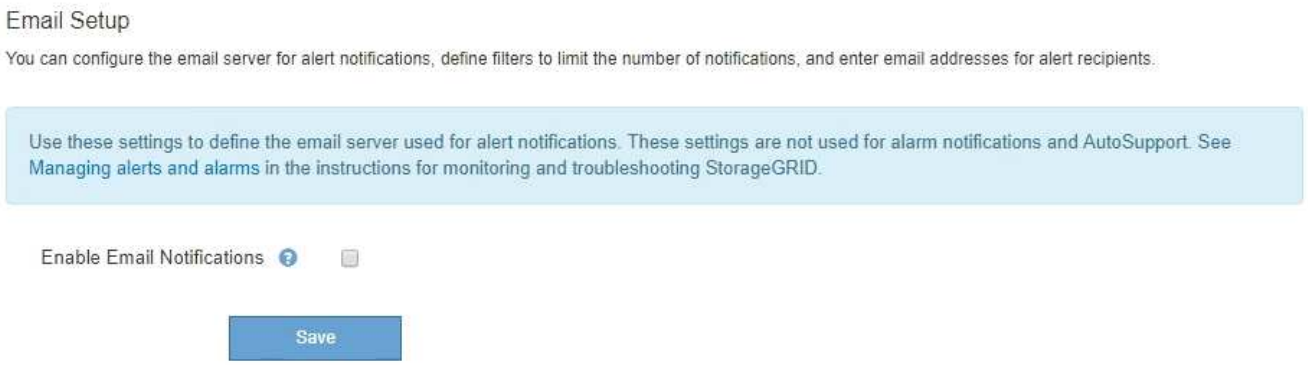
Da es sich bei den Alarmen um unabhängige Systeme handelt, wird das E-Mail-Setup, das für Alarmbenachrichtigungen verwendet wird, nicht für Alarmbenachrichtigungen und AutoSupport-Meldungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden.

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten enthält, können Sie auswählen, welcher Admin-Knoten der bevorzugte Absender von Warnmeldungen sein soll. Der gleiche „`bevorzugte Absender`“ wird auch für Benachrichtigungen zu Alarmen und AutoSupport-Nachrichten verwendet. Standardmäßig ist der primäre Admin-Node ausgewählt. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Schritte

1. Wählen Sie **Alarme** > **E-Mail-Einrichtung**.

   Die Seite E-Mail-Einrichtung wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, um anzugeben, dass Benachrichtigungen-E-Mails gesendet werden sollen, wenn Alarme 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. Außerdem müssen Sie TLS benötigen und ein CA-Zertifikat vorlegen.

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.

Feld	Eingabe
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.

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.

      Klicken Sie auf das Plus-Symbol ➕ Um Empfänger hinzuzufügen.

5. Aktivieren Sie im Abschnitt Transport Layer Security (TLS) das Kontrollkästchen **TLS erforderlich**, wenn für die Kommunikation mit dem SMTP-Server Transportschichtsicherheit (TLS) erforderlich ist.

   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 klicken Sie auf **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 zur Authentifizierung bereitzustellen.

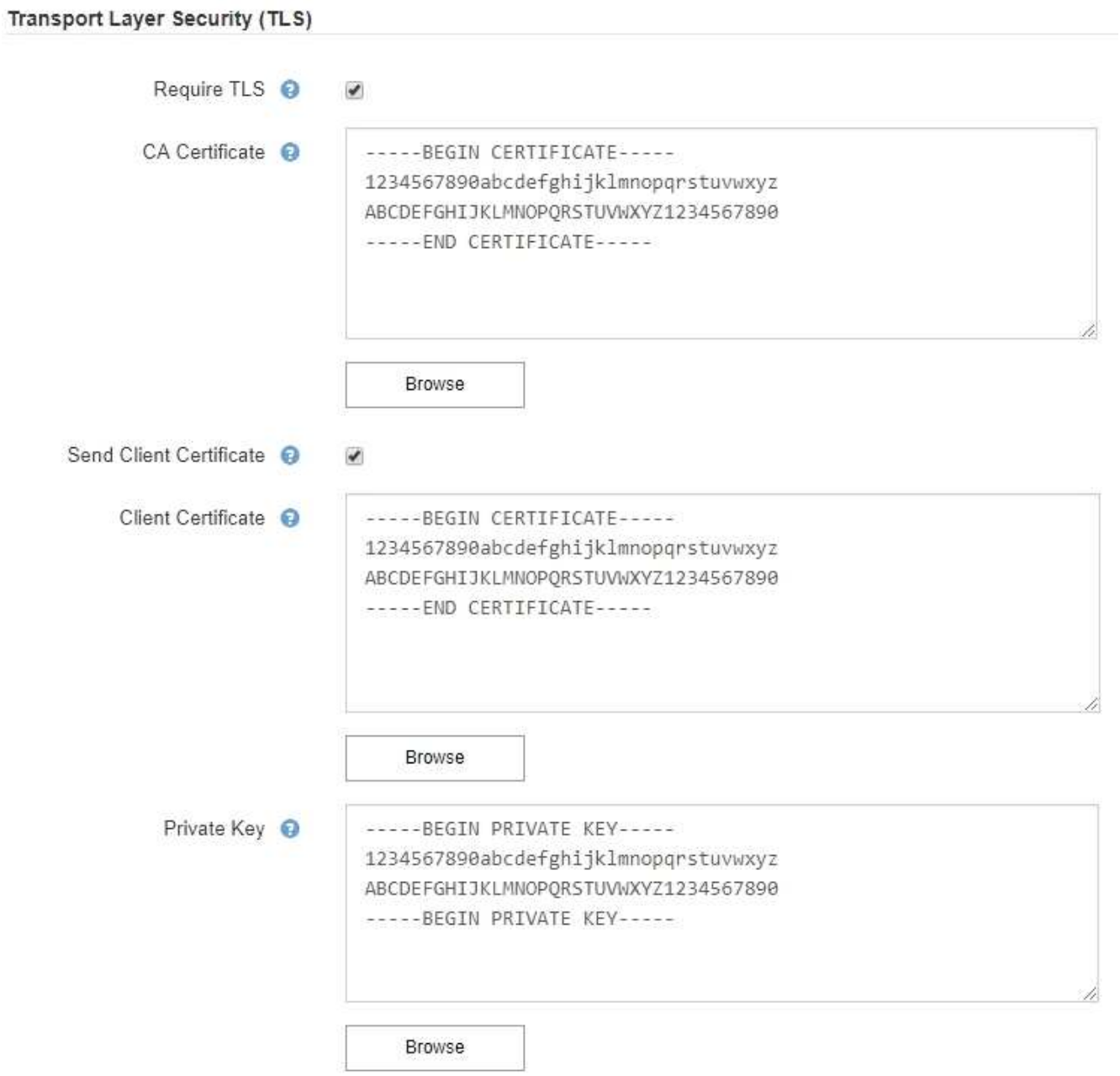
c. Geben Sie im Feld **Client Certificate** das PEM-codierte Clientzertifikat an, das an den SMTP-Server gesendet werden kann.

   Sie können den Inhalt in dieses Feld kopieren und einfügen, oder klicken Sie auf **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 klicken Sie auf **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.



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. Es werden keine Benachrichtigungen für kleinere Warnmeldungen gesendet.

Schweregrad	Beschreibung
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur gesendet, wenn die kritische Bedingung für eine Alarmregel erfüllt ist. Es werden keine Benachrichtigungen für kleinere oder größere Warnmeldungen gesendet.

7. Wenn Sie bereit sind, Ihre E-Mail-Einstellungen zu testen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie Auf **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 Alarmbenachrichtigungen und AutoSupport-Meldungen, bei denen alle Admin-Knoten die Test-E-Mail senden.

8. Klicken Sie Auf **Speichern**.

   Beim Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Klicken Sie auf **Speichern**.

   Die E-Mail-Einstellungen werden gespeichert.

Verwandte Informationen

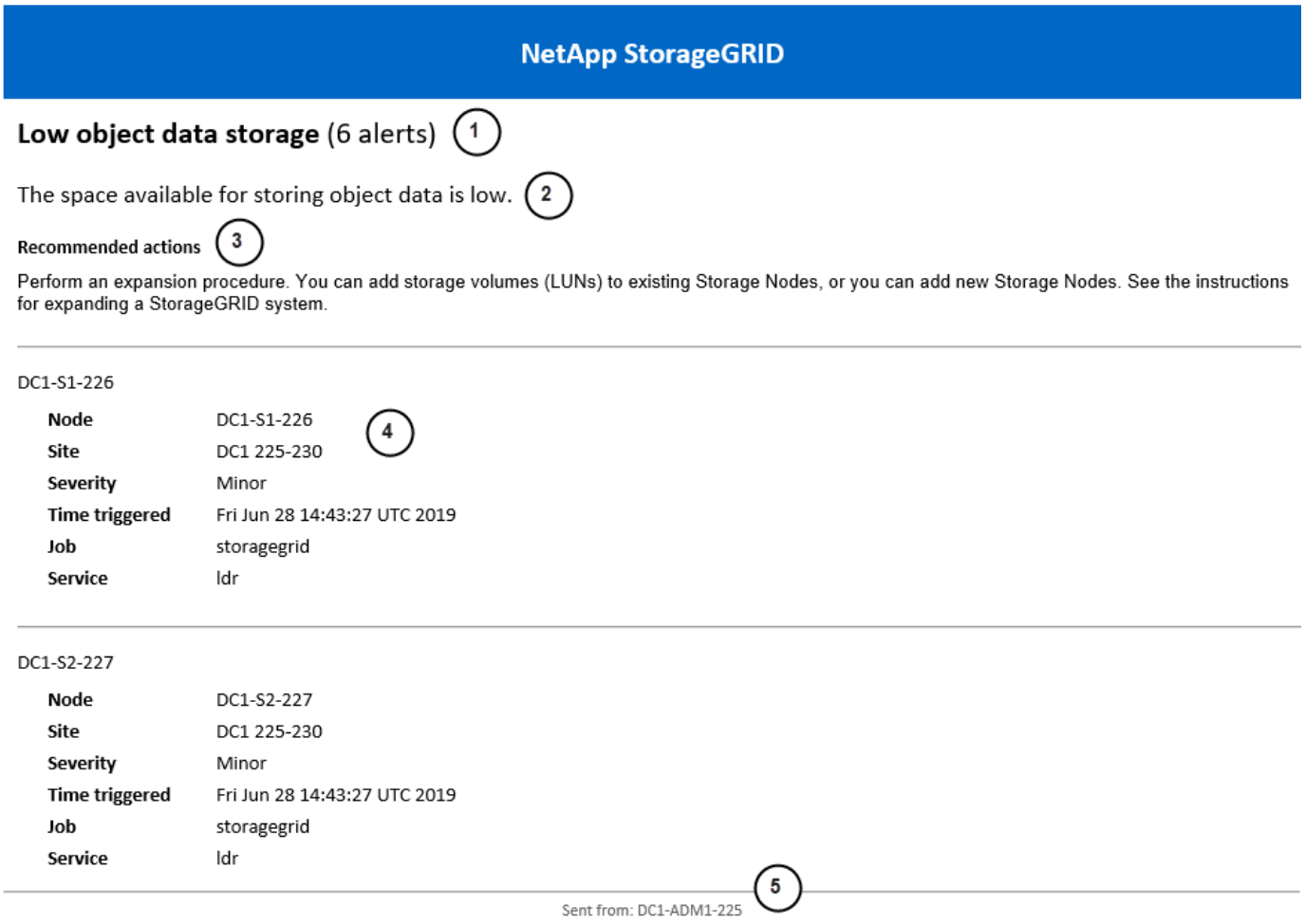
"Fehlerbehebung bei Warnmeldungen per E-Mail"

"Verwalten Sie erholen"

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.

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



	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.

Verwandte Informationen

"Stummschalten von Warnmeldungen"

Wie StorageGRID Alarme in E-Mail-Benachrichtigungen gruppiert

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
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.	• 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.
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.	• Die Warnmeldung A wird ausgelöst und die kleineren, größeren und kritischen Alarmschwellenwerte werden erreicht. Eine Benachrichtigung wird für die kritische Warnmeldung gesendet.
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.	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.
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.	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.

Verhalten	Beispiel
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.	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.
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnmeldung gelöst oder die Alarmregel stummgeschaltet wurde.	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.

Fehlerbehebung bei Warnmeldungen per E-Mail

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Schritte

1. Überprüfen Sie Ihre Einstellungen.
   a. Wählen Sie **Alarme** > **E-Mail-Einrichtung**.
   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.

Verwandte Informationen

"Protokolldateien und Systemdaten werden erfasst"

Stummschalten von Warnmeldungen

Optional können Sie Stille konfigurieren, um Benachrichtigungen vorübergehend zu unterdrücken.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

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.

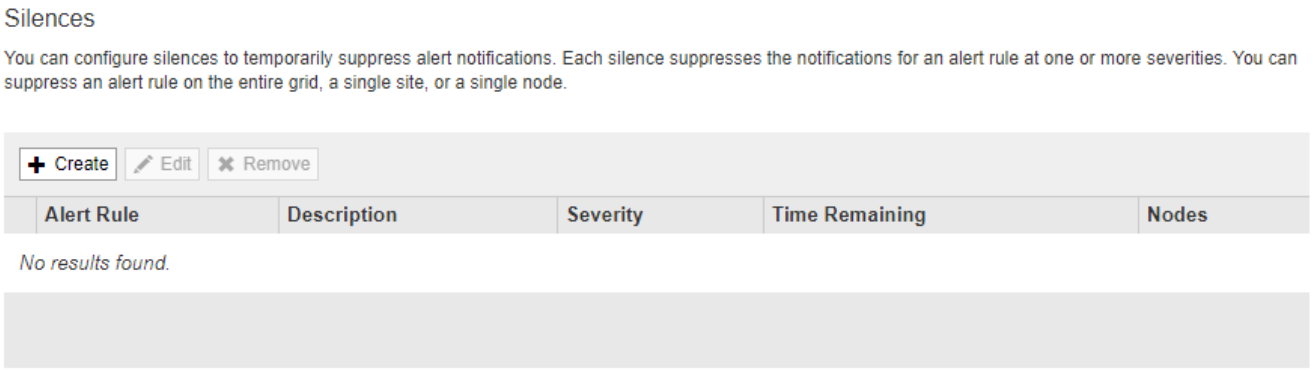
> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn Sie eine Warnmeldung stummschalten, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

> Da es sich bei Alarmmeldungen und Warnmeldungen um unabhängige Systeme handelt, können Sie diese Funktion nicht verwenden, um Alarmbenachrichtigungen zu unterdrücken.

Schritte

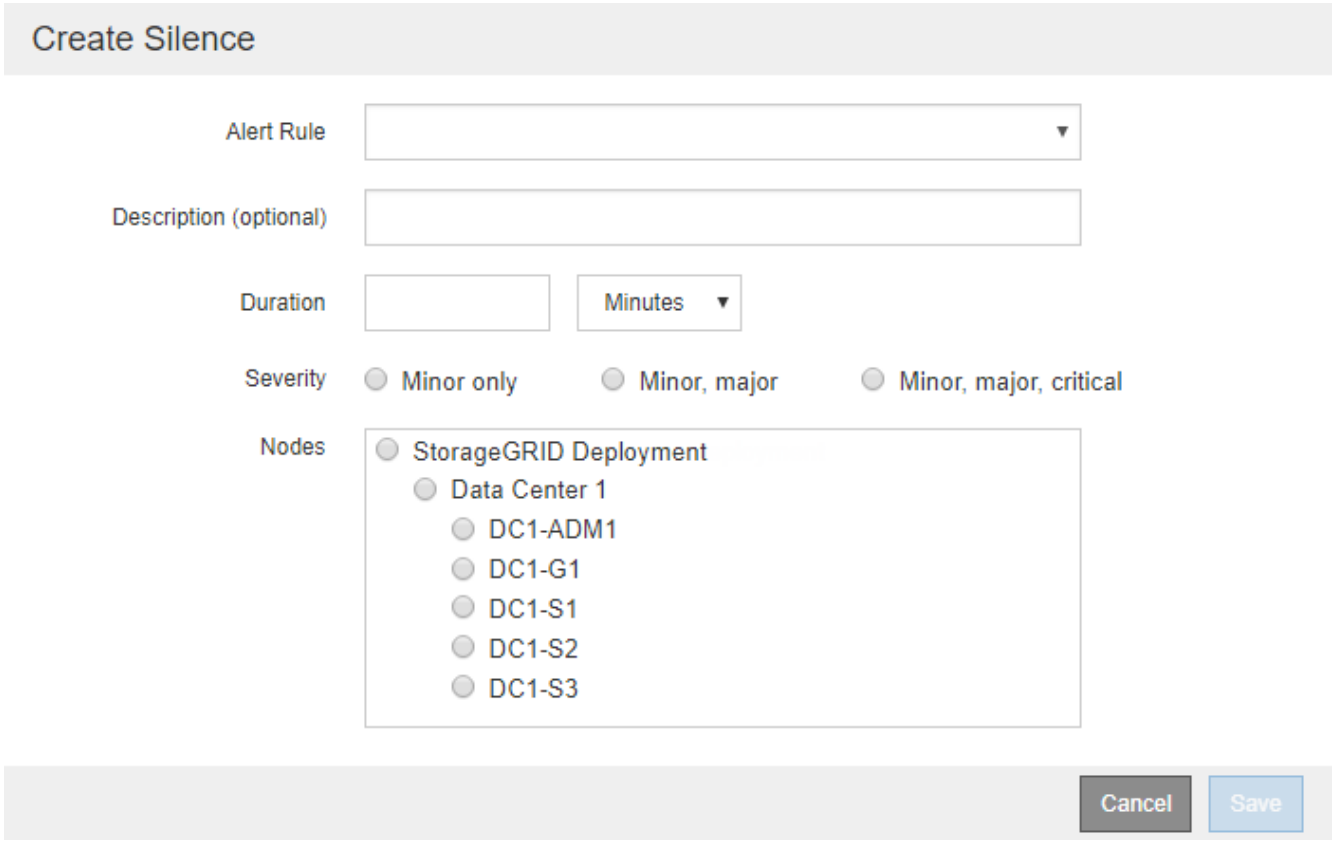
1. Wählen Sie **Alarme** > **Stille**.

   Die Seite „Stille“ wird angezeigt.



2. Wählen Sie **Erstellen**.

   Das Dialogfeld Stille erstellen wird angezeigt.



3. Wählen Sie die folgenden Informationen aus, oder geben Sie sie ein:

Feld	Beschreibung
Meldungsregel	Der Name der Alarmregel, die Sie stumm schalten möchten. Sie können eine beliebige Standard- oder benutzerdefinierte Warnungsregel auswählen, auch wenn die Alarmregel deaktiviert ist. **Hinweis:** Wählen Sie **Alle Regeln** aus, wenn Sie alle Alarmregeln mit den in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.
Beschreibung	Optional eine Beschreibung der Stille. Beschreiben Sie zum Beispiel den Zweck dieser Stille.
Dauer	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. **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.

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	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. **Hinweis:** für jede Stille können Sie nicht mehr als einen oder mehrere Knoten auswählen. Sie müssen zusätzliche Stille erstellen, wenn Sie dieselbe Warnungsregel auf mehr als einem Node oder mehreren Standorten gleichzeitig unterdrücken möchten.

4. Klicken Sie Auf **Speichern**.
5. Wenn Sie eine Stille ändern oder beenden möchten, bevor sie abläuft, können Sie sie bearbeiten oder entfernen.

Option	Beschreibung
Stille bearbeiten	a. Wählen Sie **Alarme** > **Stille**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie bearbeiten möchten. c. Klicken Sie Auf **Bearbeiten**. d. Ändern Sie die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten. e. Klicken Sie Auf **Speichern**.
Entfernen Sie eine Stille	a. Wählen Sie **Alarme** > **Stille**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie entfernen möchten. c. Klicken Sie Auf **Entfernen**. d. Klicken Sie auf **OK**, um zu bestätigen, dass Sie diese Stille entfernen möchten. **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.

Verwandte Informationen

"Konfigurieren des SNMP-Agenten"

Verwalten von Alarmen (Altsystem)

Das StorageGRID-Alarmsystem ist das ältere System, mit dem Störstellen identifiziert werden können, die manchmal während des normalen Betriebs auftreten.

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

Verwandte Informationen

"Alarmreferenz (Altsystem)"

"Anzeigen von Legacy-Alarmen"

"StorageGRID verwalten"

Alarmklassen (altes System)

Ein älterer Alarm kann zu einer von zwei sich gegenseitig ausschließenden Alarmklassen gehören.

Standardalarme

Jedes StorageGRID System verfügt über Standardalarme und kann nicht geändert werden. Sie können jedoch Standardalarme deaktivieren oder überschreiben, indem Sie globale benutzerdefinierte Alarme definieren.

Globale benutzerdefinierte Alarme

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.

Verwandte Informationen

"Anzeigen von Standardalarmen (Legacy-System)"

"Deaktivieren eines Standardalarms (älteres System)"

"Erstellen von globalen benutzerdefinierten Alarmen (Legacy-System)"

"Deaktivieren von globalen benutzerdefinierten Alarmen (Legacy-System)"

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.

Symbol	Farbe	Alarmschweregrad	Bedeutung
	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 Alarmschwerwert und der entsprechende Schwellwert 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 Alarme und Standardalarme 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.

Alarme desselben Schweregrades

Wenn zwei globale benutzerdefinierte Alarme für dasselbe Attribut den gleichen Schweregrad haben, werden die Alarme 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 Alarms

Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
☑	SSM	UMEM (Available Memory)	Minor	under10	<=	1000		

Wird die Reihenfolge umgekehrt, wenn UMEM auf 100MB fällt, wird der erste Alarm (<=100000000) ausgelöst, nicht jedoch der darunter stehende Alarm (= 50000000).

Global Alarms

Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	under10	<=	1000		
☑	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 Topology**. Wählen Sie dann ***Storage-Node*** > **SSM** > **Ressourcen**.)

Sie können den VMFI-Alarm so deaktivieren, dass der VMFI-Alarm auf kritischer Ebene nicht ausgelöst wird (beide derzeit kritischen Alarme erscheinen in der Tabelle als grün); Es ist jedoch nicht möglich, einen einzelnen Alarm in einer Tabellenzeile zu deaktivieren, so dass ein VMFI-Alarm als kritischer Füllstandalarm 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

Bestätigen aktueller Alarme (Altsystem)

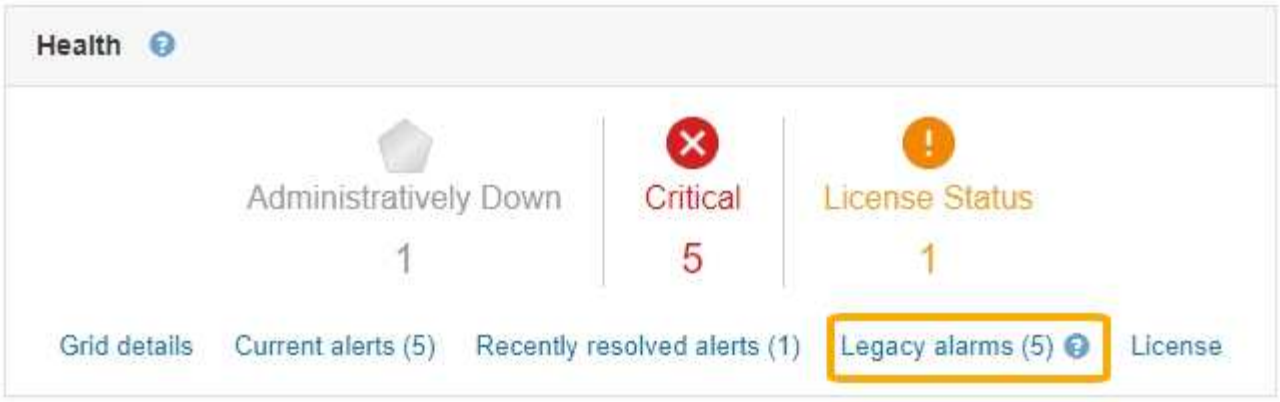
Ältere Alarme werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Wenn Sie die Anzahl der alten Alarme auf dem Dashboard verringern oder löschen möchten, können Sie die Alarme bestätigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Alarme quittieren verfügen.

Über diese Aufgabe

Wenn derzeit ein Alarm aus dem alten System aktiv ist, enthält das Bedienfeld „Systemzustand“ auf dem Dashboard einen Link „Legacy-Alarme*“. Die Zahl in Klammern gibt an, wie viele ältere Alarme derzeit aktiv sind.



Da das veraltete Alarmsystem weiterhin unterstützt wird, wird die Anzahl der auf dem Dashboard angezeigten älteren Alarme erhöht, sobald ein neuer Alarm auftritt. Diese Anzahl wird erhöht, auch wenn E-Mail-Benachrichtigungen nicht mehr für Alarme gesendet werden. Sie können diese Zahl in der Regel einfach ignorieren (da Warnmeldungen eine bessere Übersicht über 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 in die Anzahl der älteren Alarme einbezogen, es sei denn, der Alarm wird auf der nächsten Stufe ausgelöst oder er wird behoben und tritt erneut auf.

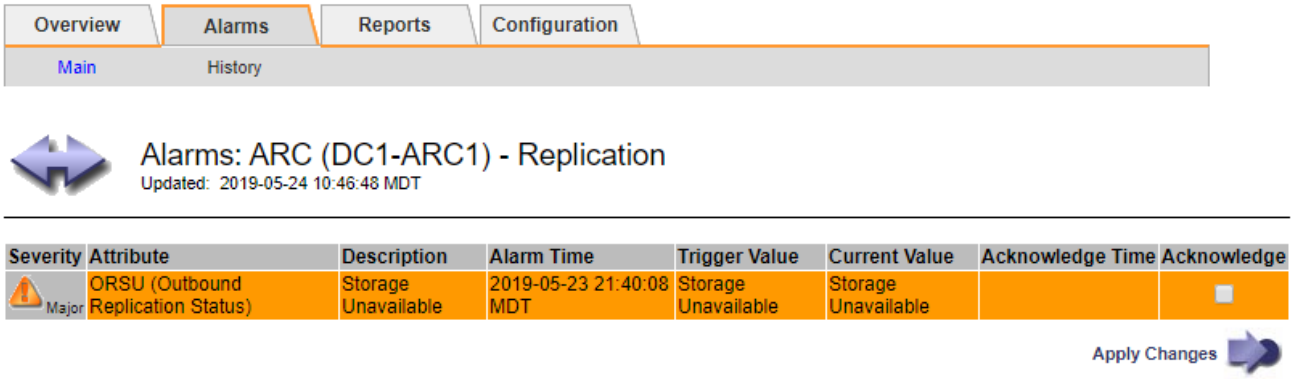
Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Um den Alarm anzuzeigen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Bedienfeld „Systemzustand“ auf **Legacy-Alarme**. Dieser Link wird nur angezeigt, wenn derzeit mindestens ein Alarm aktiv ist.
   - Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**. Die Seite Aktuelle Alarme wird angezeigt.

2. Klicken Sie in der Tabelle auf den Dienstnamen.

   Die Registerkarte Alarme für den ausgewählten Dienst wird angezeigt (**Support** > **Tools** > **Grid Topology** > ***Grid Node*** > ***Service*** > **Alarme**).



3. Aktivieren Sie das Kontrollkästchen * Quittieren* für den Alarm, und klicken Sie auf **Änderungen anwenden**.

   Der Alarm wird nicht mehr auf dem Dashboard oder der Seite Aktuelle Alarme angezeigt.

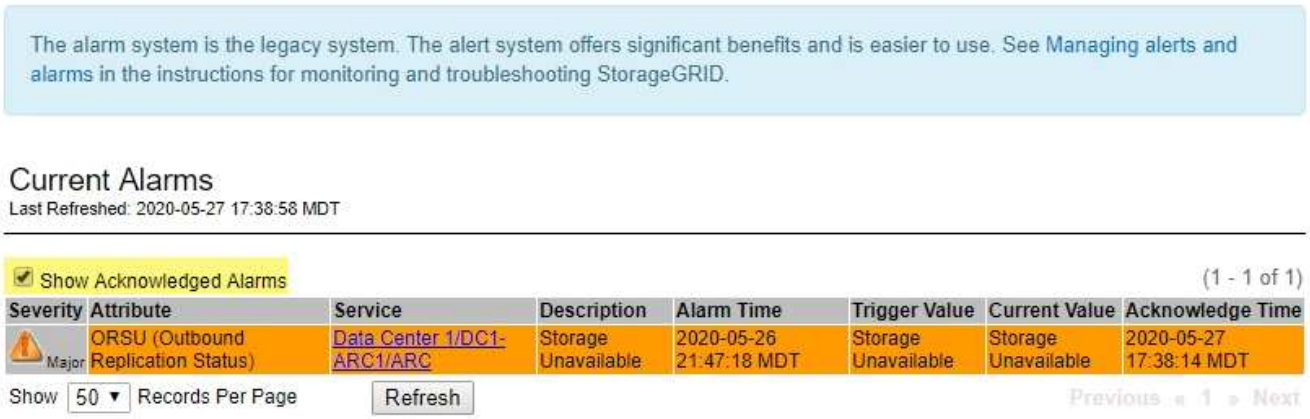
   Wenn Sie einen Alarm bestätigen, wird die Quittierung nicht auf andere Admin-Knoten kopiert. Wenn Sie das Dashboard aus einem anderen Administratorknoten anzeigen, wird möglicherweise weiterhin der aktive Alarm angezeigt.

4. Zeigen Sie bei Bedarf bestätigte Alarme an.

   a. Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**.

   b. Wählen Sie **Bestätigte Alarme Anzeigen**.

      Alle quittierten Alarme werden angezeigt.



Verwandte Informationen

"Alarmreferenz (Altsystem)"

Anzeigen von Standardalarmen (Legacy-System)

Sie können die Liste aller älteren Standardalarme anzeigen.

Was Sie benötigen

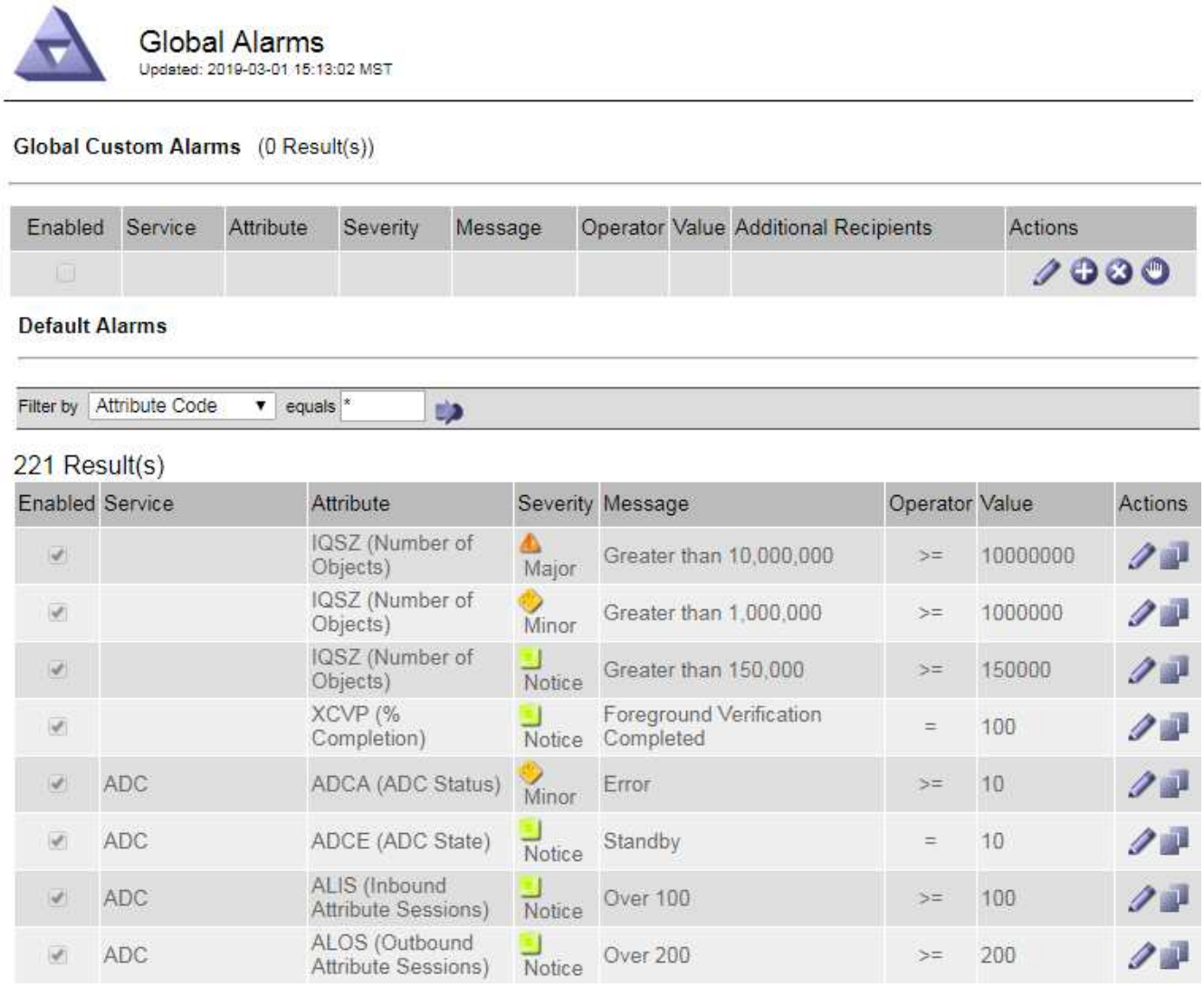
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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.



Überprüfung historischer Alarme und Alarmfrequenz (Altsystem)

Bei der Fehlerbehebung eines Problems können Sie überprüfen, wie oft in der Vergangenheit ein älterer Alarm ausgelöst wurde.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- 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 Topology** 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**.

Verwandte Informationen

"Alarmreferenz (Altsystem)"

Erstellen von globalen benutzerdefinierten Alarmen (Legacy-System)

Sie haben möglicherweise globale benutzerdefinierte Alarme für das alte System verwendet, um bestimmte Überwachungsanforderungen zu erfüllen. Globale benutzerdefinierte Alarme haben möglicherweise Alarmstufen, die Standardalarme überschreiben, oder sie überwachen möglicherweise Attribute, die keinen Standardalarm haben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

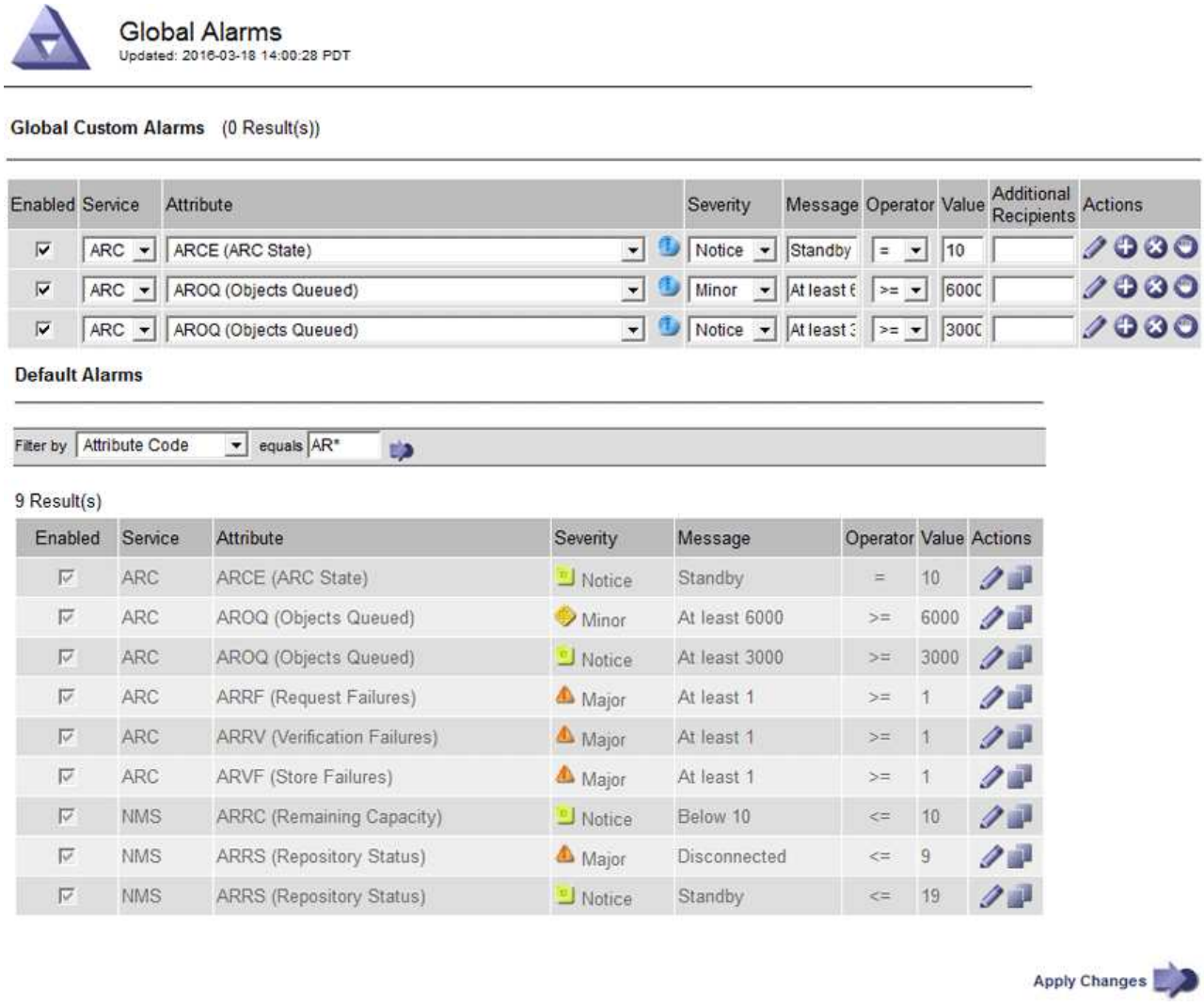
> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

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 sehr 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**.



   - 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.
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: • = gleich • > größer als • < kleiner als • >= größer als oder gleich • <= kleiner als oder gleich • ≠ ist nicht gleich
Wert	Der Schwellwert 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 kommagetrennte 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 benötigen SMTP-Server-Einrichtung, um arbeiten zu können. Bestätigen Sie vor dem Hinzufügen von Mailinglisten, dass SMTP konfiguriert ist. Benachrichtigungen für benutzerdefinierte Alarme können Benachrichtigungen von globalen benutzerdefinierten oder Standardalarmen überschreiben.

Überschrift	Beschreibung
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**.

Verwandte Informationen

"Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"

Deaktivieren von Alarmen (Altsystem)

Die Alarme im alten Alarmsystem sind standardmäßig aktiviert, aber Sie können 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 (älteres System)

Sie können einen der älteren Standardalarme für das gesamte System deaktivieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- 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 die älteren Alarme erst, wenn 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.

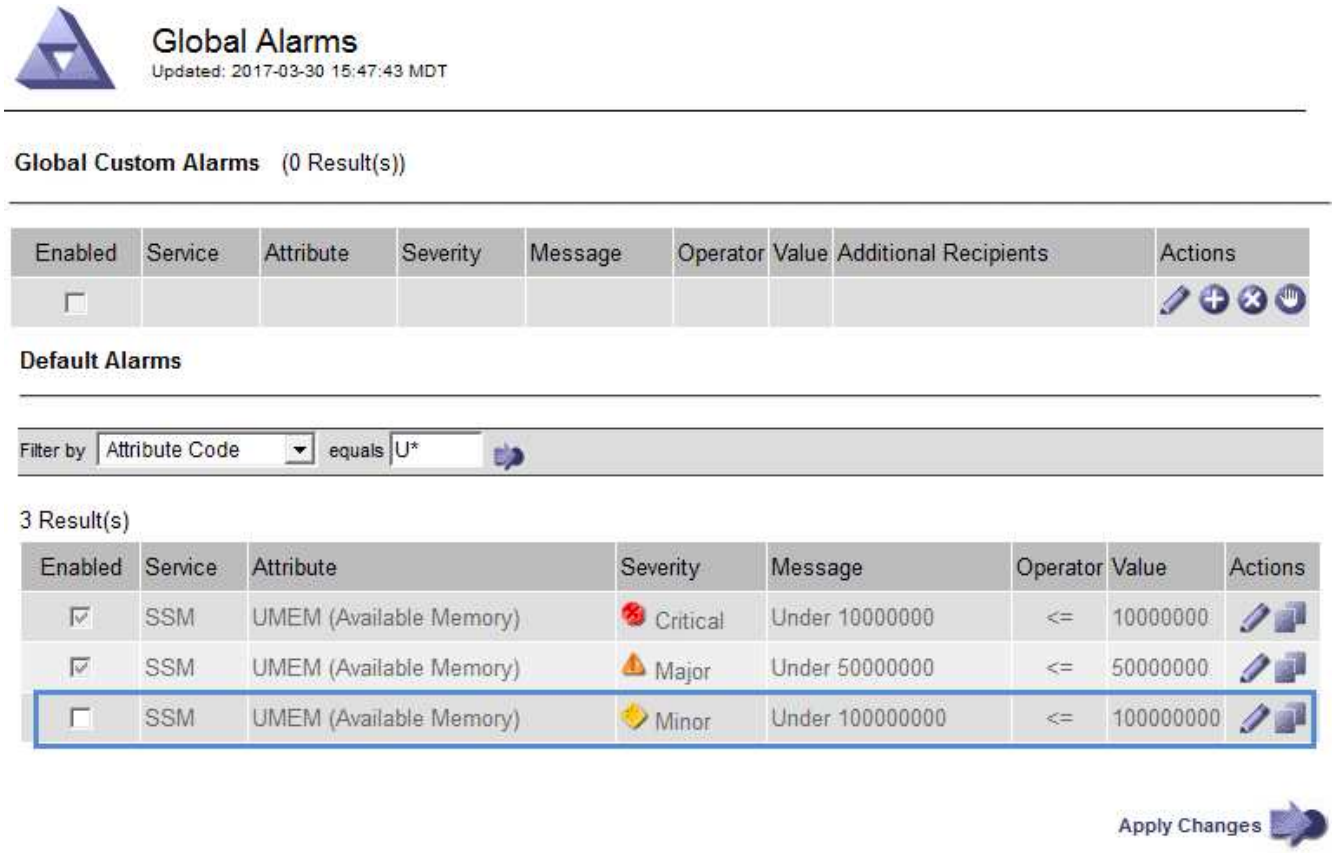
b. Geben Sie einen Suchstring ein.

   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.



   Das Kontrollkästchen **aktiviert** für den ausgewählten Alarm wird aktiviert.

4. Deaktivieren Sie das Kontrollkästchen **aktiviert**.
5. Klicken Sie Auf **Änderungen Übernehmen**.

   Der Standardalarm ist deaktiviert.

Deaktivieren von globalen benutzerdefinierten Alarmen (Legacy-System)

Sie können einen veralteten globalen benutzerdefinierten Alarm für das gesamte System deaktivieren.

Was Sie benötigen

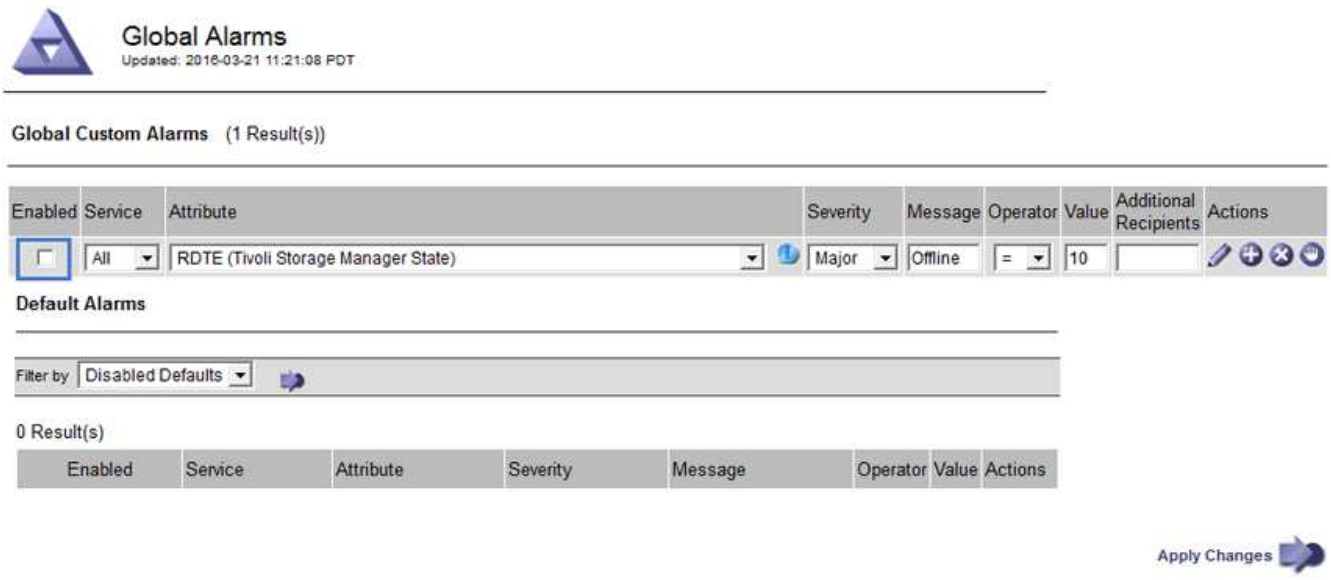
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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**.



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.

Was Sie benötigen

- 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.

Verwandte Informationen

"Deaktivieren von Alarmen (Altsystem)"

Konfigurieren von Benachrichtigungen für Alarme (Legacy-System)

Das StorageGRID System kann automatisch E-Mail- und SNMP-Benachrichtigungen senden, wenn ein Alarm ausgelöst wird oder sich ein Servicestatus 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.

Verwandte Informationen

"Verwendung von SNMP-Überwachung"

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.

Verwandte Informationen

"Konfigurieren von E-Mail-Benachrichtigungen für Alarme (Altsystem)"

Konfigurieren von E-Mail-Servereinstellungen für Alarme (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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- 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 Benachrichtigungen verwendet.

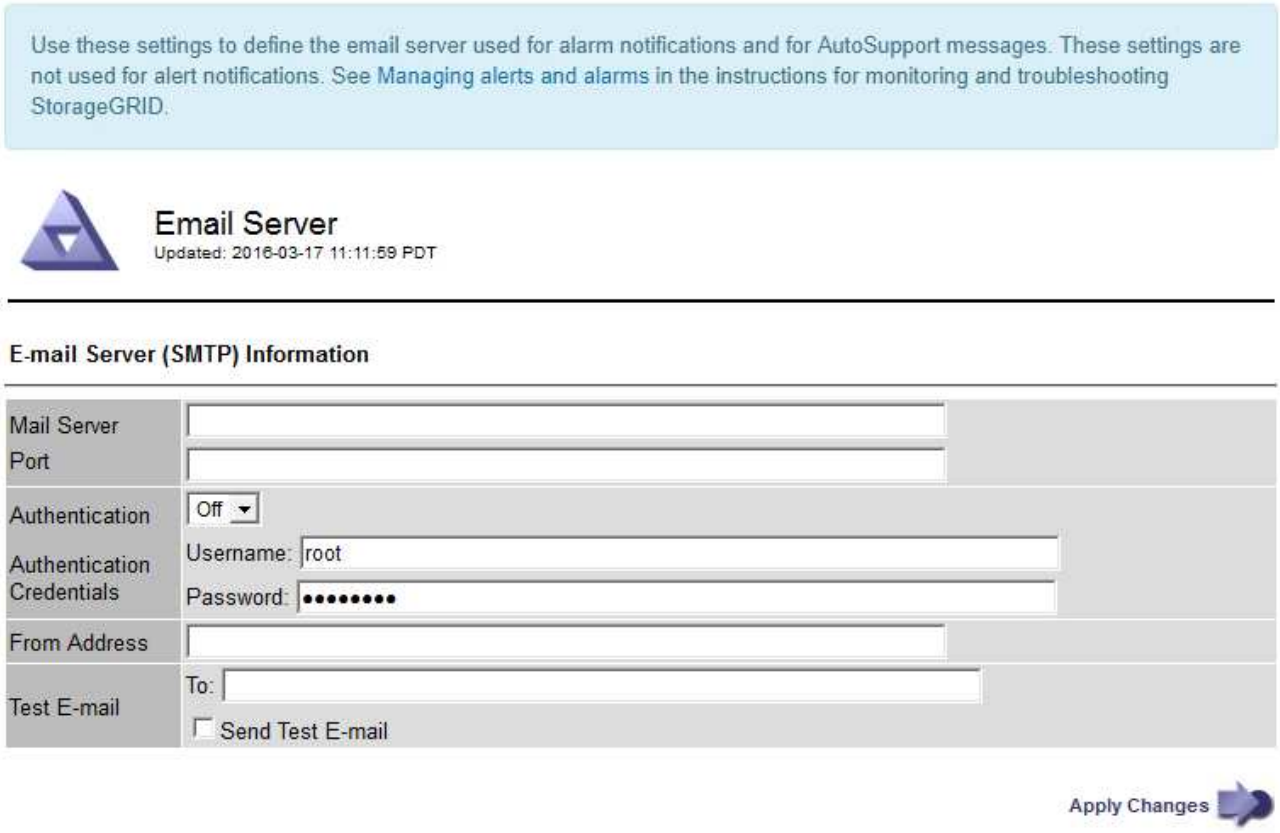
> Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, haben Sie möglicherweise bereits einen SMTP-Mail-Server konfiguriert. Derselbe SMTP-Server wird für Benachrichtigungen über Alarm-E-Mails verwendet, sodass Sie diesen Vorgang überspringen können. Lesen Sie die Anweisungen zum Verwalten 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.



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.
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 E-Mail-Server 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.

Verwandte Informationen

"StorageGRID verwalten"

Erstellen von E-Mail-Vorlagen für Alarme (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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

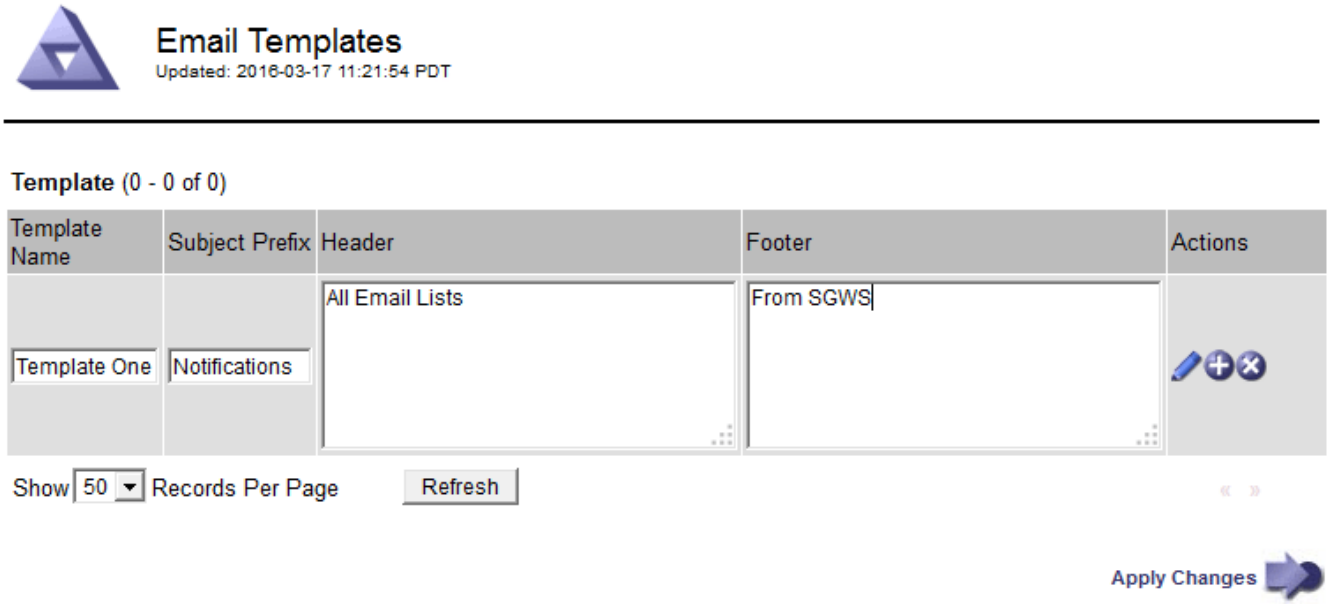
Über diese Aufgabe

Mit diesen Einstellungen können Sie die E-Mail-Vorlagen festlegen, die für ältere Benachrichtigungen verwendet werden. Diese Einstellungen werden nicht für Benachrichtigungen verwendet.

Für unterschiedliche Mailinglisten sind möglicherweise andere Kontaktinformationen erforderlich. Vorlagen enthalten nicht den Textkörper der E-Mail-Nachricht.

Schritte

1. Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Vorlagen**.
3. Klicken Sie Auf **Bearbeiten*** **(Oder *Einfügen** Falls dies nicht die erste Vorlage ist).



4. 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.

5. 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.

Was Sie benötigen

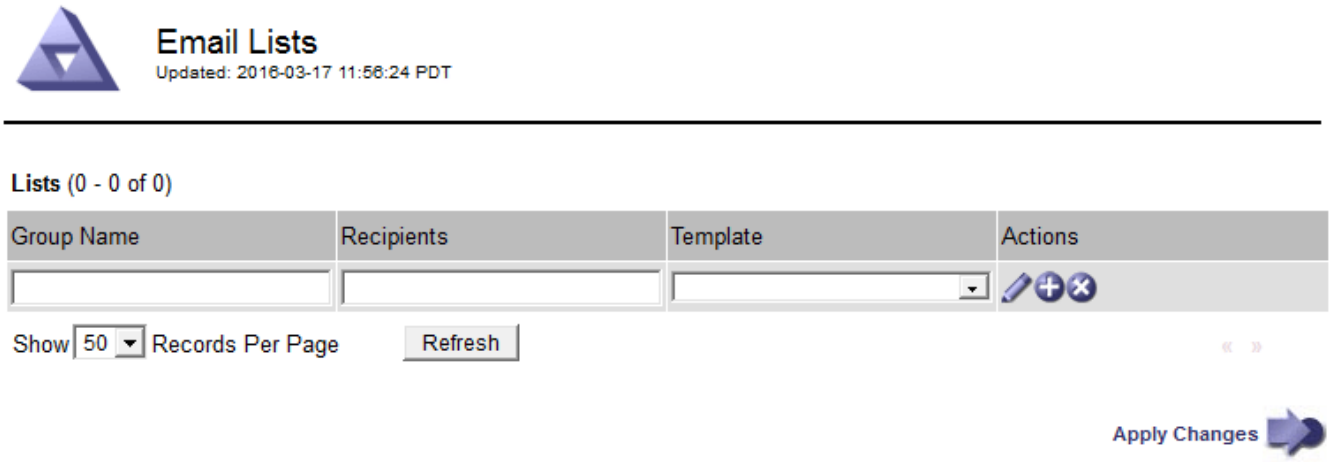
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie eine E-Mail-Vorlage für die Mailingliste (benutzerdefinierte Kopfzeile, Fußzeile und Betreffzeile) angeben möchten, müssen Sie die Vorlage bereits 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 Benachrichtigungen 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).



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

Element	Beschreibung
Gruppenname	Eindeutiger Name zur Identifizierung der Mailingliste. Mailinglistennamen 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.

Element	Beschreibung
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.
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.

Verwandte Informationen

"Erstellen von E-Mail-Vorlagen für Alarme (altes System)"

Konfigurieren von E-Mail-Benachrichtigungen für Alarme (Altsystem)

Um E-Mail-Benachrichtigungen für das alte 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- 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 Alarme konfigurieren. Diese Einstellungen werden nicht für Benachrichtigungen 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 Alarme unabhängig vom Schweregrad erhalten. Eine andere Gruppe benötigt möglicherweise nur Benachrichtigungen für Alarme 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** > **Alarme (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 Alarme mit dem ausgewählten Schweregrad „Alarm“ oder „Service“ ausgelöst oder geändert werden.

Verwandte Informationen

"Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)"

"Arten von Alarmanmeldungen (Legacy-System)"

Unterdrückung von Alarmmeldungen für eine Mailingliste (Legacy-System)

Sie können Alarmbenachrichtigungen 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- 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 Benachrichtigungen per E-Mail.

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 Unterdrückung 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 Alarmbenachrichtigungen werden für die ausgewählten Mailinglisten unterdrückt.

Systemweite Unterdrückung von E-Mail-Benachrichtigungen

Sie können die Fähigkeit des StorageGRID Systems blockieren, E-Mail-Benachrichtigungen für ältere Alarme und AutoSupport-Meldungen mit Ereignisauslösung zu senden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

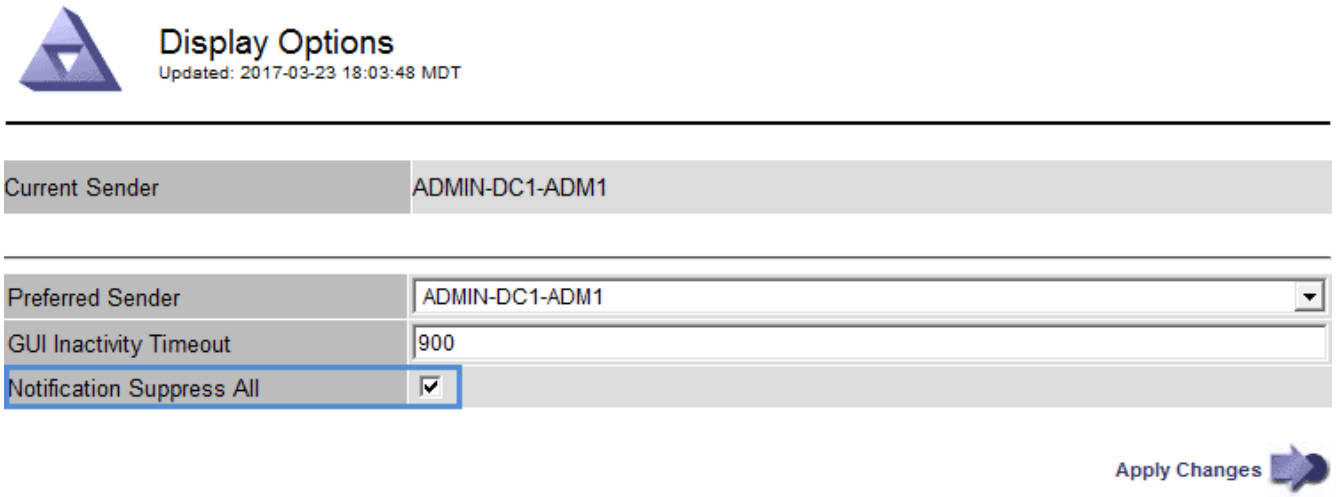
Über diese Aufgabe

Verwenden Sie diese Option, um E-Mail-Benachrichtigungen für ältere Alarme und AutoSupport-Meldungen, bei denen Ereignisse ausgelöst werden, zu unterdrücken.

Diese Option unterdrückt Benachrichtigungen per E-Mail nicht. Zudem werden wöchentliche oder benutzergesteuerte AutoSupport-Meldungen nicht unterdrückt.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie im Menü Anzeigeoptionen die Option **Optionen**.
3. Wählen Sie **Benachrichtigung Alle Unterdrücken**.



4. Klicken Sie Auf **Änderungen Übernehmen**.

   Auf der Seite Benachrichtigungen (**Konfiguration** > **Benachrichtigungen**) wird die folgende Meldung angezeigt:

Verwandte Informationen

"StorageGRID verwalten"

Verwendung von SNMP-Überwachung

Wenn Sie StorageGRID mit dem Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den SNMP-Agent konfigurieren, der in StorageGRID enthalten ist.

- "Konfigurieren des SNMP-Agenten"
- "SNMP-Agent wird aktualisiert"

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine Management

Information Base (MIB) bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Alarme 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.

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-Agent gesendet werden, die keine Bestätigung durch das Verwaltungssystem 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. Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde.
- Bestimmte Alarme (Altsystem) werden mit einem bestimmten Schweregrad oder höher ausgelöst.

> ⓘ SNMP-Benachrichtigungen werden nicht für jeden Alarm oder jeden Schweregrad 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

	SNMPv1	SNMPv2c	SNMPv3
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.

Zugriff auf die MIB

Sie können auf die MIB-Definitionsdatei an der folgenden Stelle auf einem beliebigen StorageGRID-Knoten zugreifen:

/Usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt

Verwandte Informationen

"Alerts Referenz"

"Alarmreferenz (Altsystem)"

"Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"

"Stummschalten von Warnmeldungen"

Konfigurieren des SNMP-Agenten

Sie können den StorageGRID SNMP-Agent konfigurieren, wenn Sie ein Drittanbieter-SNMP-Verwaltungssystem für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwenden möchten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP-Protokolls. Sie können den Agent für eine oder mehrere Versionen konfigurieren.

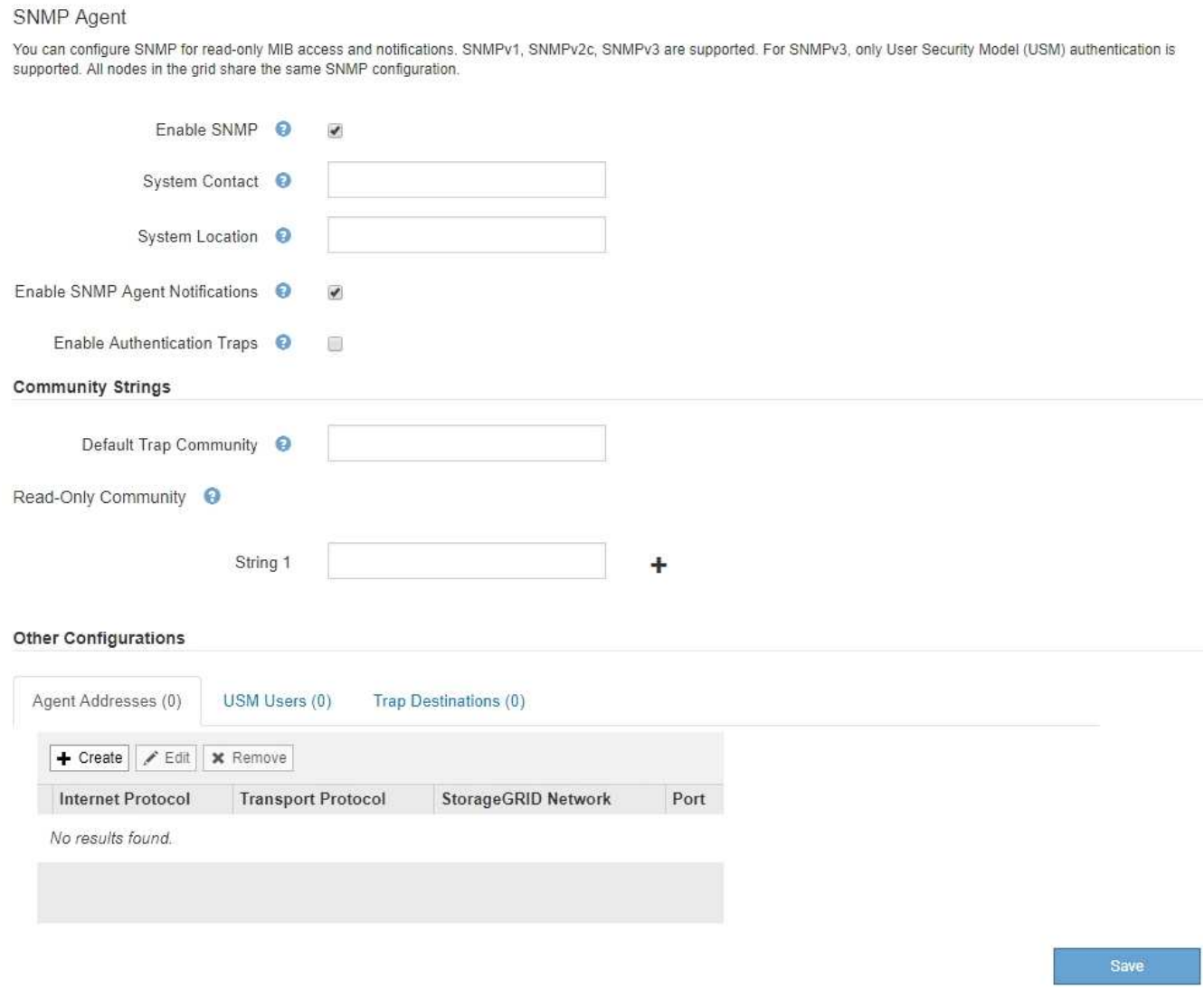
Schritte

1. Wählen Sie **Konfiguration** > **Überwachung** > **SNMP-Agent**.

   Die Seite SNMP-Agent wird angezeigt.

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.



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 ausliefern 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 ausliefern Wert gilt für alle Nodes im StorageGRID System. **Systemposition** kann maximal 255 Zeichen enthalten.

5. Aktivieren Sie das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, wenn der StorageGRID-SNMP-Agent Trap senden und Benachrichtigungen informieren soll.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, unterstützt der SNMP-Agent den schreibgeschützten MIB-Zugriff, aber es sendet keine SNMP-Benachrichtigungen.

6. Aktivieren Sie das Kontrollkästchen **Authentifizierungsfallen aktivieren**, wenn der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap senden soll, wenn er eine nicht ordnungsgemäß authentifizierte Protokollnachricht empfängt.
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.

      Standard Trap Community kann 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. Klicken Sie auf das Pluszeichen ➕ 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 kann maximal 32 Zeichen enthalten und darf keine Leerzeichen enthalten. Es sind bis zu fünf Zeichenfolgen zulässig.

      ⓘ Verwenden Sie nicht „`public`“ als Community-String, um die Sicherheit Ihres StorageGRID-Systems zu gewährleisten. Wenn Sie keine Community-Zeichenfolge eingeben, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID-Systems als Community-String.

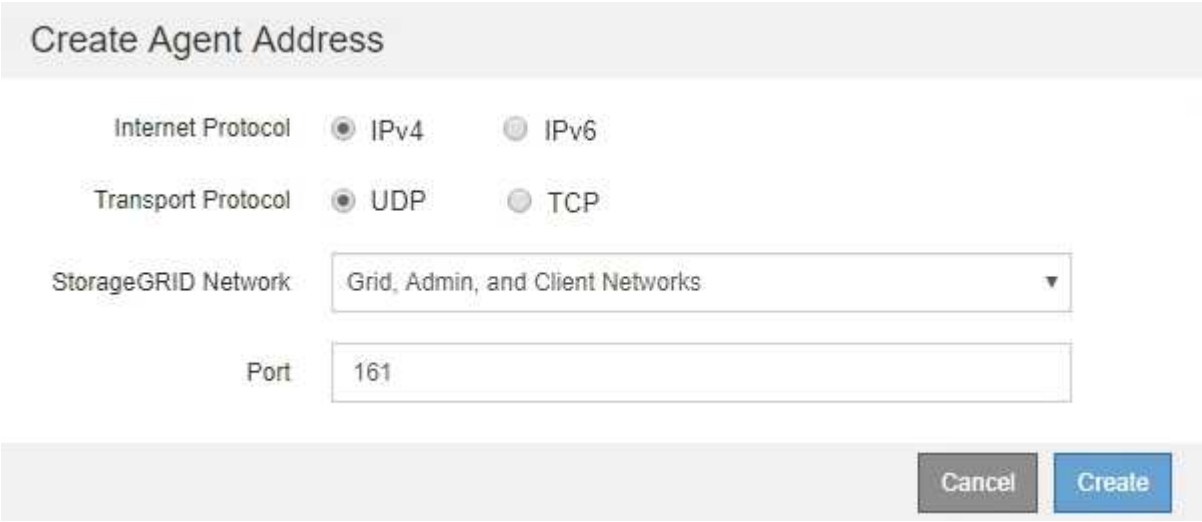
8. Wählen Sie optional im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

   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 Listenadresse UDP-Port 161 in allen StorageGRID-Netzwerken.

   a. Klicken Sie Auf **Erstellen**.

Das Dialogfeld Agentenadresse erstellen wird angezeigt.



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. Klicken Sie Auf **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

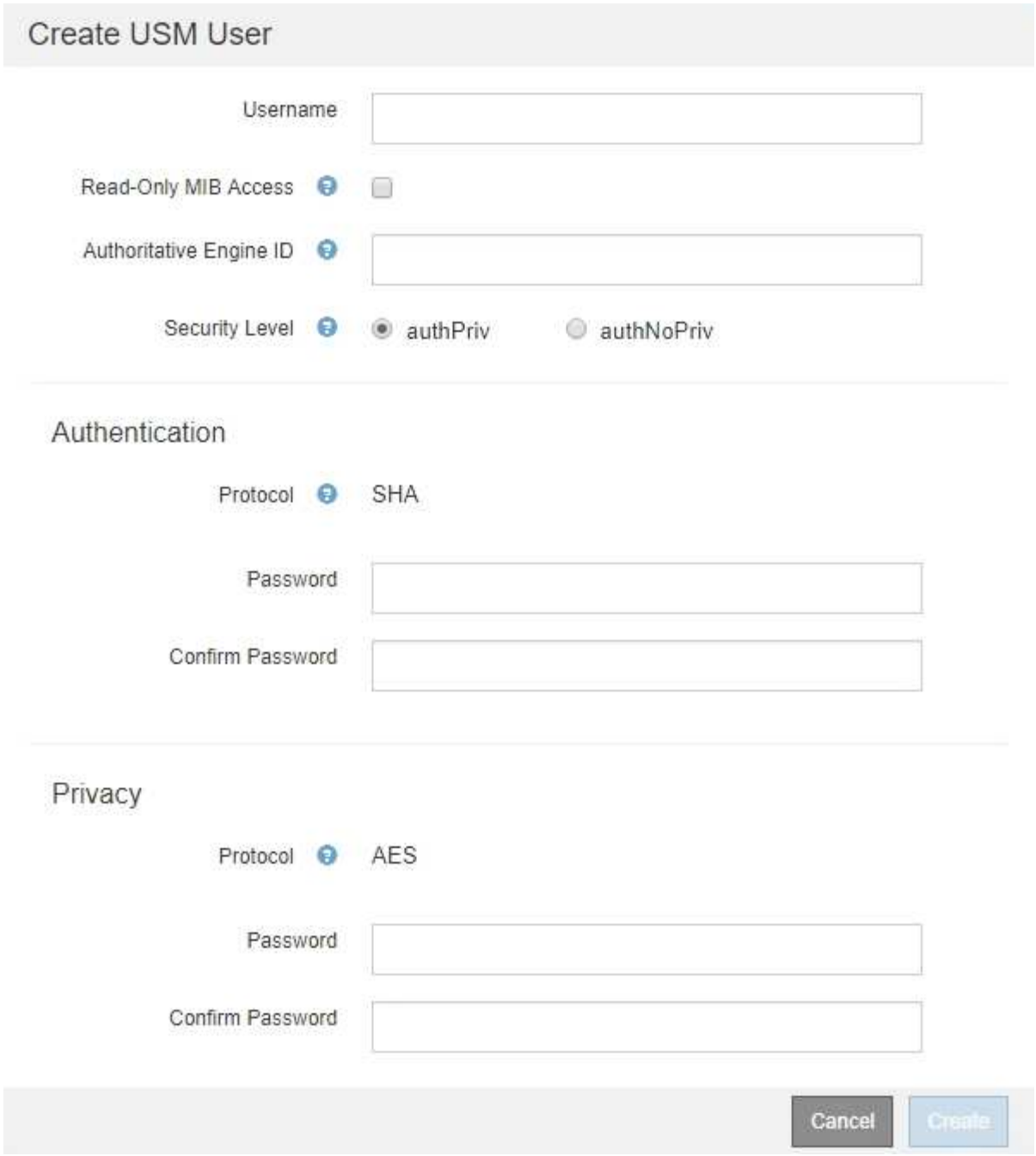
9. Wenn Sie SNMPv3 verwenden, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

   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. Klicken Sie Auf **Erstellen**.

      Das Dialogfeld USM-Benutzer erstellen wird angezeigt.



b. Geben Sie einen eindeutigen **Benutzername** für diesen USM-Benutzer ein.

   Benutzernamen haben maximal 32 Zeichen und können keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht geändert werden.

c. Aktivieren Sie das Kontrollkästchen **schreibgeschütztes MIB Access**, wenn dieser Benutzer nur Lesezugriff 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. 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.

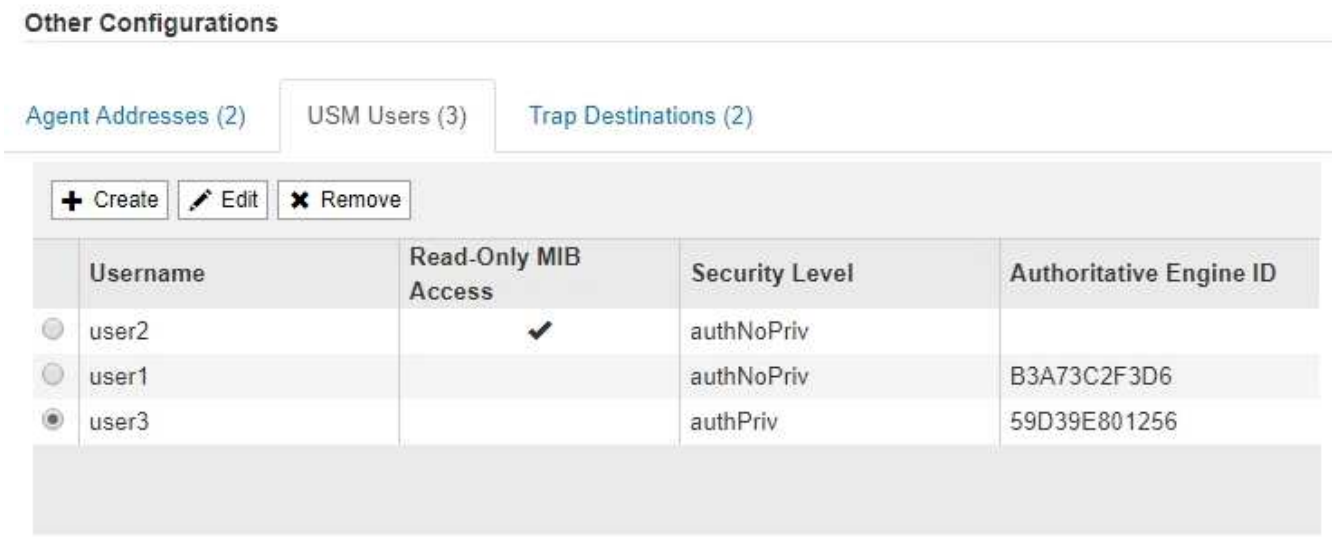
> Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).

g. Wenn Sie **authPriv** ausgewählt haben, geben Sie das Passwort ein und bestätigen Sie es.

> Das einzige unterstützte Datenschutzprotokoll ist AES.

h. Klicken Sie Auf **Erstellen**.

Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

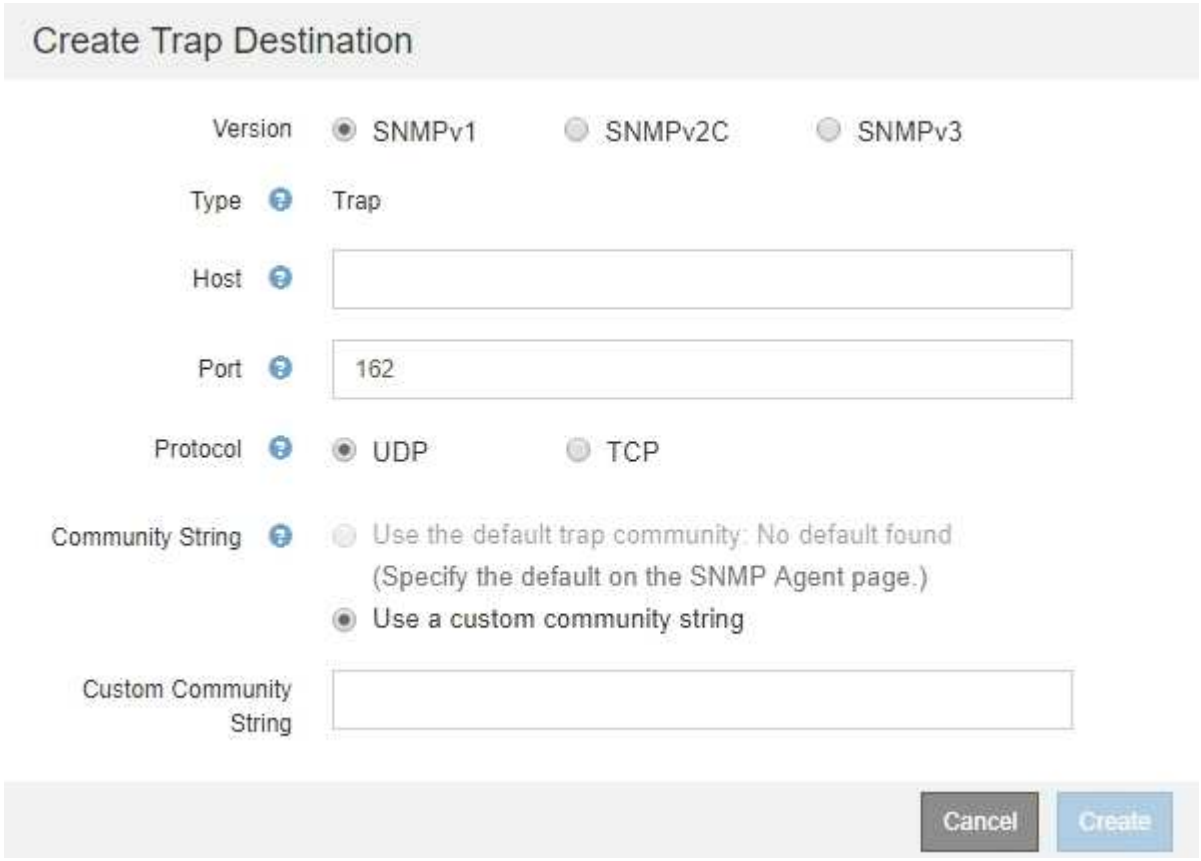


10. Wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Trap-Ziele aus.

Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agent aktivieren und auf **Speichern** klicken, beginnt StorageGRID mit dem Senden von 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. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld Trap-Ziel erstellen wird angezeigt.



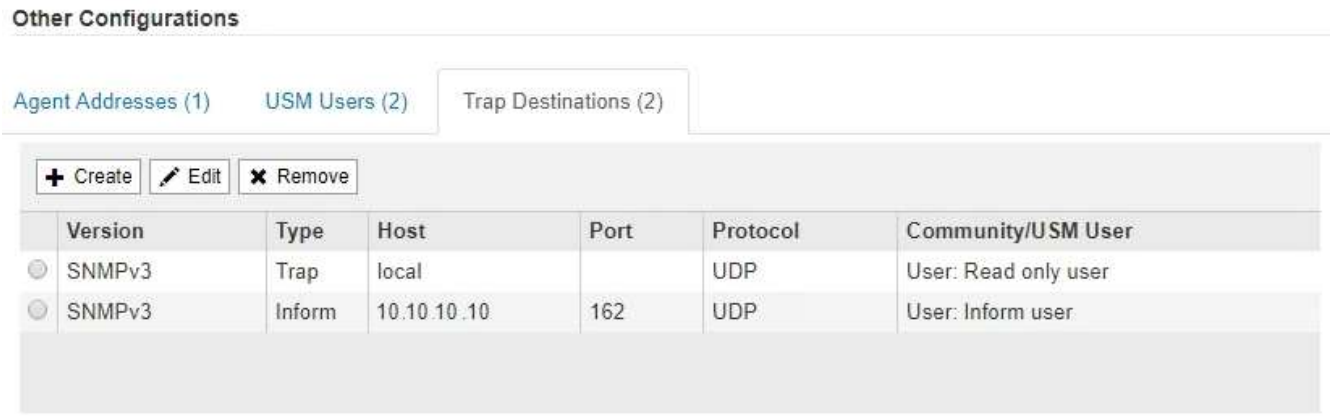
b. Wählen Sie im Feld **Version** die SNMP-Version für diese Benachrichtigung aus.
c. Füllen Sie das Formular aus, basierend auf der ausgewählten Version

Version	Geben Sie diese Informationen an
SNMPv1	**Hinweis:** für SNMPv1 kann der SNMP-Agent nur Traps senden. Informationen werden nicht unterstützt. 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. Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.
SNMPv2c	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. Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.

Version	Geben Sie diese Informationen an
SNMPv3	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. ◦ 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.

d. Klicken Sie Auf **Erstellen**.

Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.



11. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, klicken Sie auf **Speichern**

Die neue SNMP-Agent-Konfiguration wird aktiv.

Verwandte Informationen

"Stummschalten von Warnmeldungen"

SNMP-Agent wird aktualisiert

Sie können SNMP-Benachrichtigungen deaktivieren, Community-Strings aktualisieren

oder Agent-Adressen, USM-Benutzer und Trap-Ziele hinzufügen oder entfernen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Immer wenn Sie die SNMP-Agent-Konfiguration aktualisieren, müssen Sie auf der Seite SNMP-Agent auf **Speichern** klicken, um alle Änderungen zu speichern, 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 klicken Sie auf **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-Agent-Benachrichtigungen aktivieren**, wenn der StorageGRID-SNMP-Agent nicht mehr Trap senden und Benachrichtigungen informieren soll.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, unterstützt der SNMP-Agent den schreibgeschützten MIB-Zugriff, aber es sendet keine SNMP-Benachrichtigungen.

5. Deaktivieren Sie optional das Kontrollkästchen **Authentifizierungsfallen aktivieren**, wenn Sie nicht mehr möchten, dass der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap sendet, wenn er eine nicht ordnungsgemäß 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.

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.

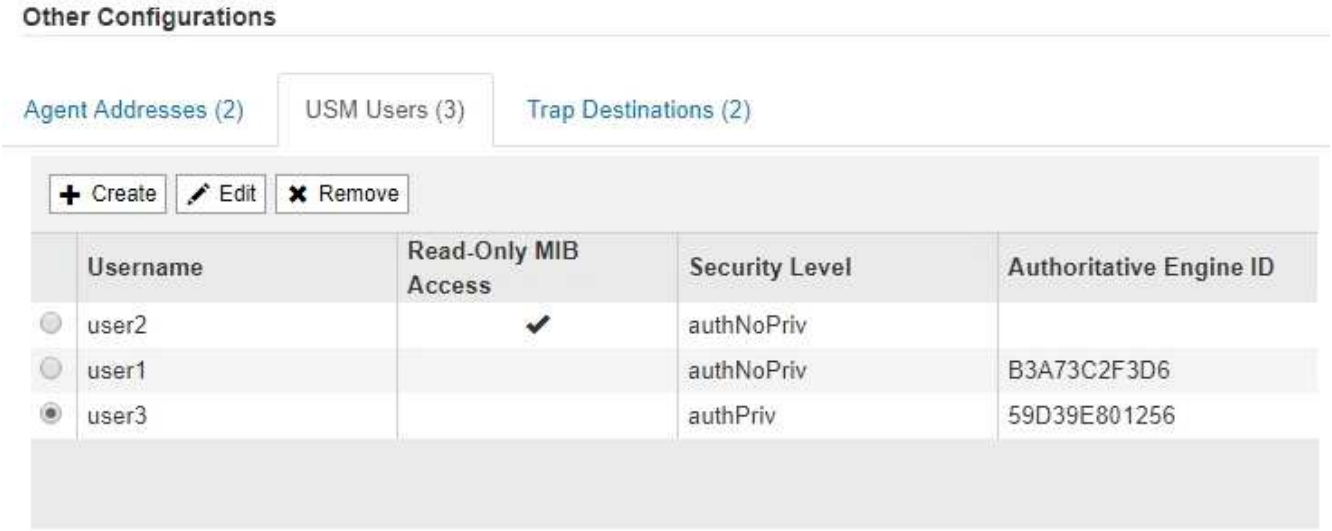
a. Um eine Agentenadresse hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.

b. Um eine Agentenadresse zu bearbeiten, aktivieren Sie das Optionsfeld für die Adresse und klicken auf **Bearbeiten**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.

c. Um eine Agentenadresse zu entfernen, wählen Sie das Optionsfeld für die Adresse aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie diese Adresse entfernen möchten.

d. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

8. Wenn Sie USM-Benutzer aktualisieren möchten, 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.

a. Um einen USM-Benutzer hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für USM-

Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

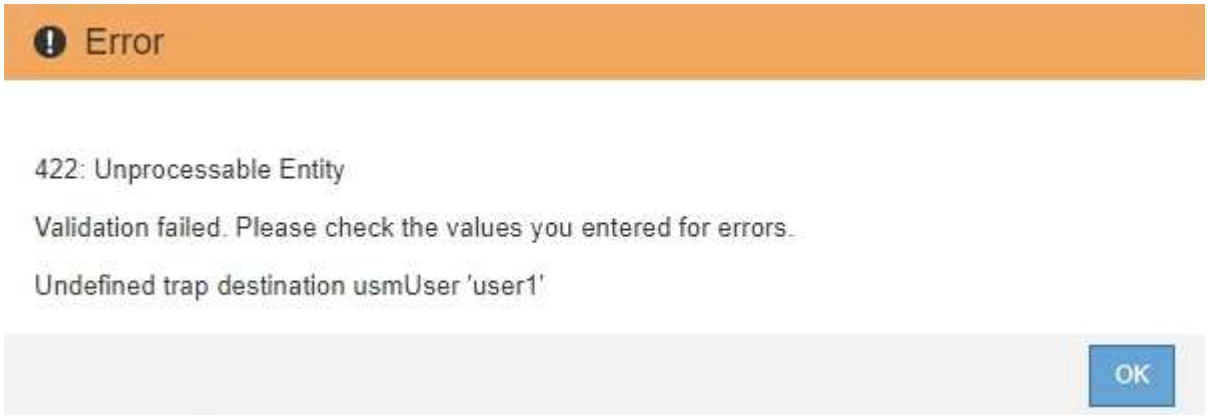
b. Um einen USM-Benutzer zu bearbeiten, wählen Sie das Optionsfeld für den Benutzer aus, und klicken Sie auf **Bearbeiten**. Lesen Sie dann den Schritt für USM-Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

   Der Benutzername für einen bestehenden USM-Benutzer 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.

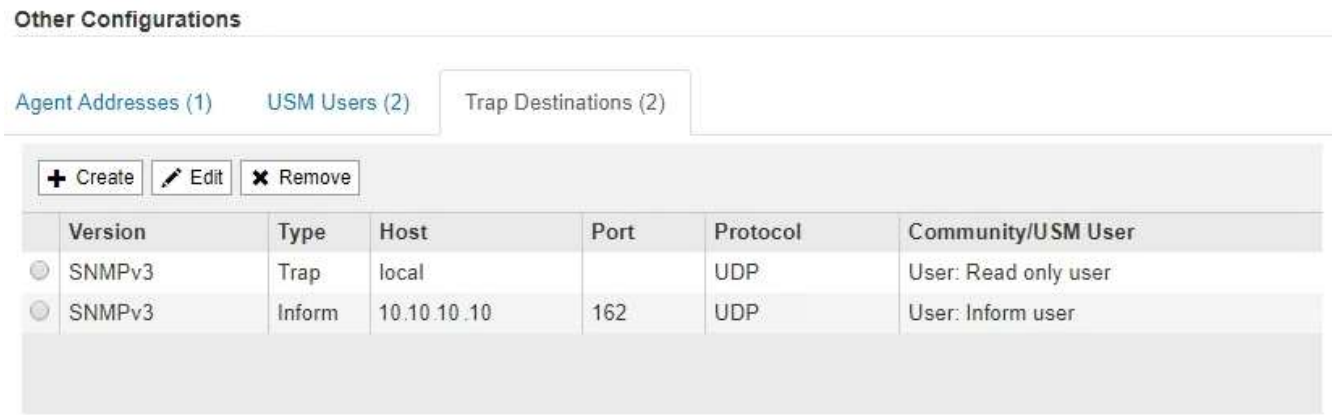
c. Um einen USM-Benutzer zu entfernen, wählen Sie das Optionsfeld für den Benutzer aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie diesen Benutzer entfernen möchten.

   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.



a. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

1. Wenn Sie Trap-Ziele aktualisieren möchten, wählen Sie im Abschnitt Weitere 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-Agent aktivieren und auf **Speichern** klicken, beginnt StorageGRID mit dem Senden von 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, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
b. Um ein Trap-Ziel zu bearbeiten, wählen Sie das Optionsfeld für den Benutzer aus und klicken auf **Bearbeiten**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
c. Um ein Trap-Ziel zu entfernen, wählen Sie das Optionsfeld für das Ziel aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie dieses Ziel entfernen möchten.
d. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

2. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, klicken Sie auf **Speichern**.

Verwandte Informationen

"Konfigurieren des SNMP-Agenten"

Erfassung weiterer StorageGRID-Daten

Es gibt verschiedene zusätzliche Möglichkeiten, Daten zu erfassen und zu analysieren, die bei der Untersuchung des Zustands Ihres StorageGRID Systems oder bei der Arbeit mit dem technischen Support zur Behebung von Problemen hilfreich sein können.

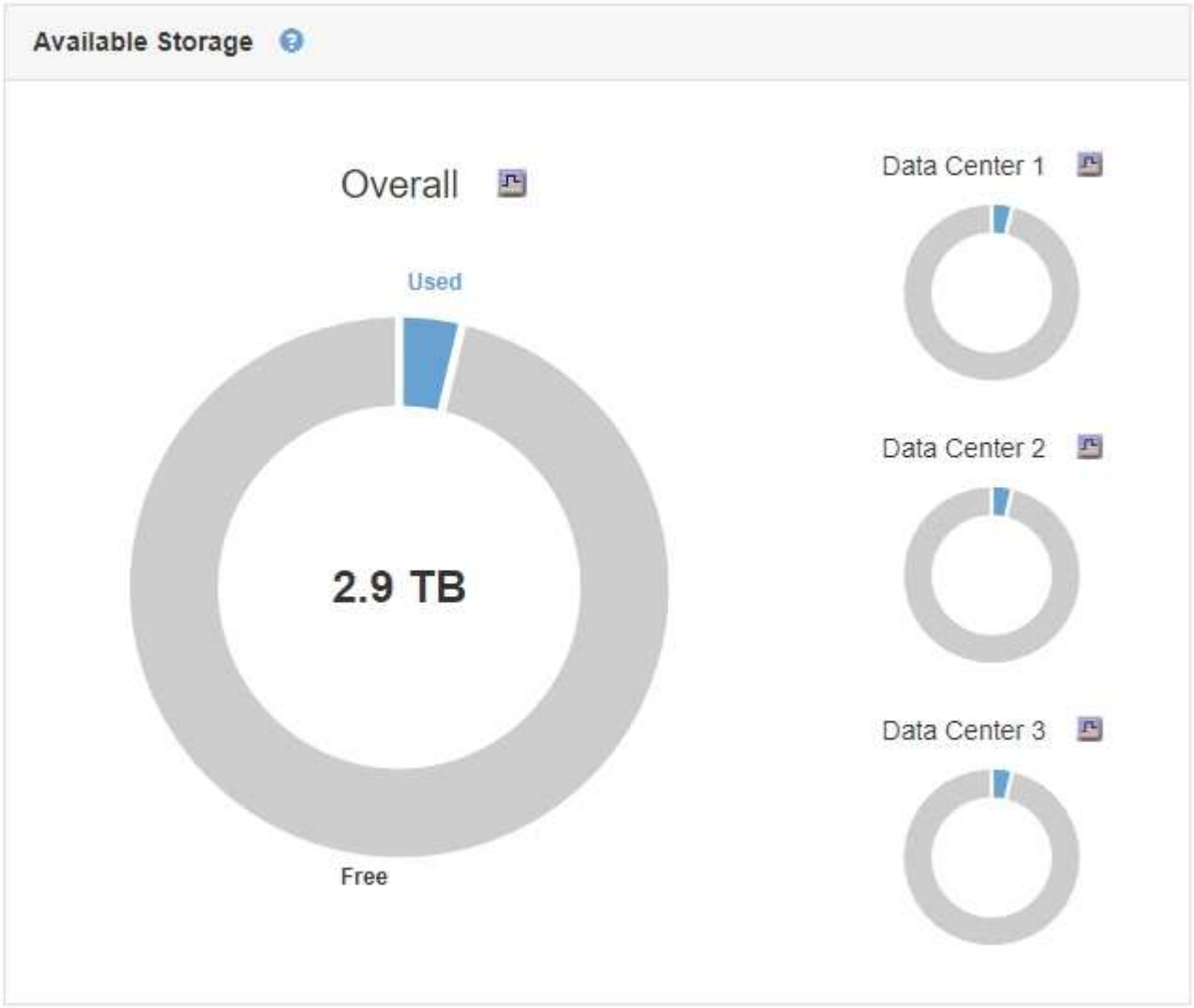
- "Verwenden von Diagrammen und Berichten"
- "Monitoring PUT und GET Performance"
- "Monitoring von Objektverifizierungsvorgängen"
- "Monitoring von Ereignissen"
- "Überprüfen von Audit-Meldungen"
- "Protokolldateien und Systemdaten werden erfasst"
- "Manuelles Auslösen einer AutoSupport-Meldung"
- "Anzeigen der Struktur der Grid Topology"
- "Überprüfen von Support-Metriken"
- "Diagnose wird ausgeführt"
- "Erstellen benutzerdefinierter Überwachungsanwendungen"

Verwenden von Diagrammen und Berichten

Mithilfe von Diagrammen und Berichten lässt sich der Zustand des StorageGRID Systems überwachen und Probleme beheben. Die im Grid Manager verfügbaren Diagrammtypen und Berichte umfassen Tortendiagramme (nur auf dem Dashboard), Diagramme und Textberichte.

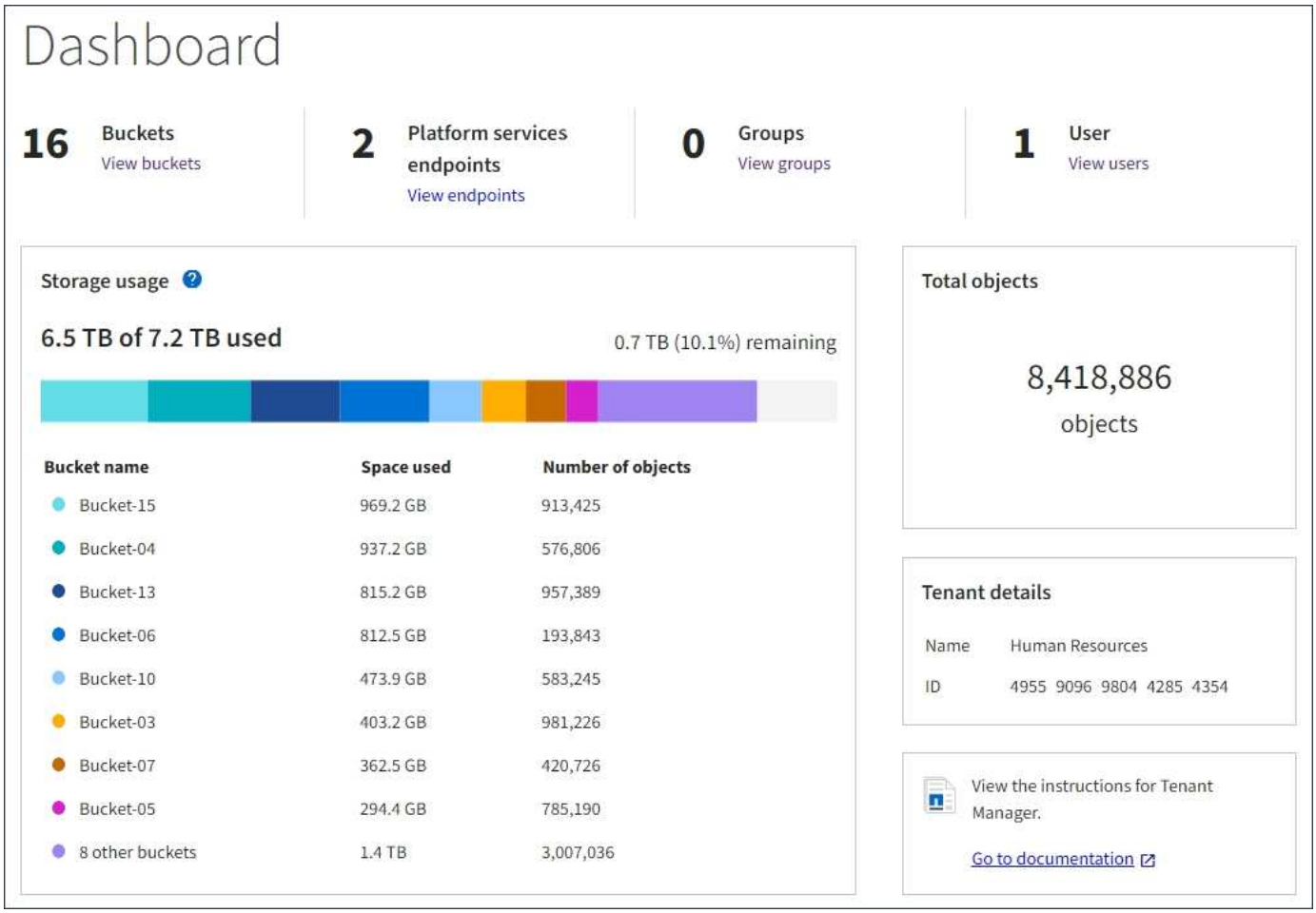
Diagramme und Diagramme fassen die Werte bestimmter StorageGRID-Metriken und -Attribute zusammen.

Das Grid Manager Dashboard enthält PIE-Diagramme (Donut), um den verfügbaren Speicher für das Grid und jeden Standort zusammenzufassen.



Im Bereich Speichernutzung auf dem Tenant Manager Dashboard werden folgende Informationen angezeigt:

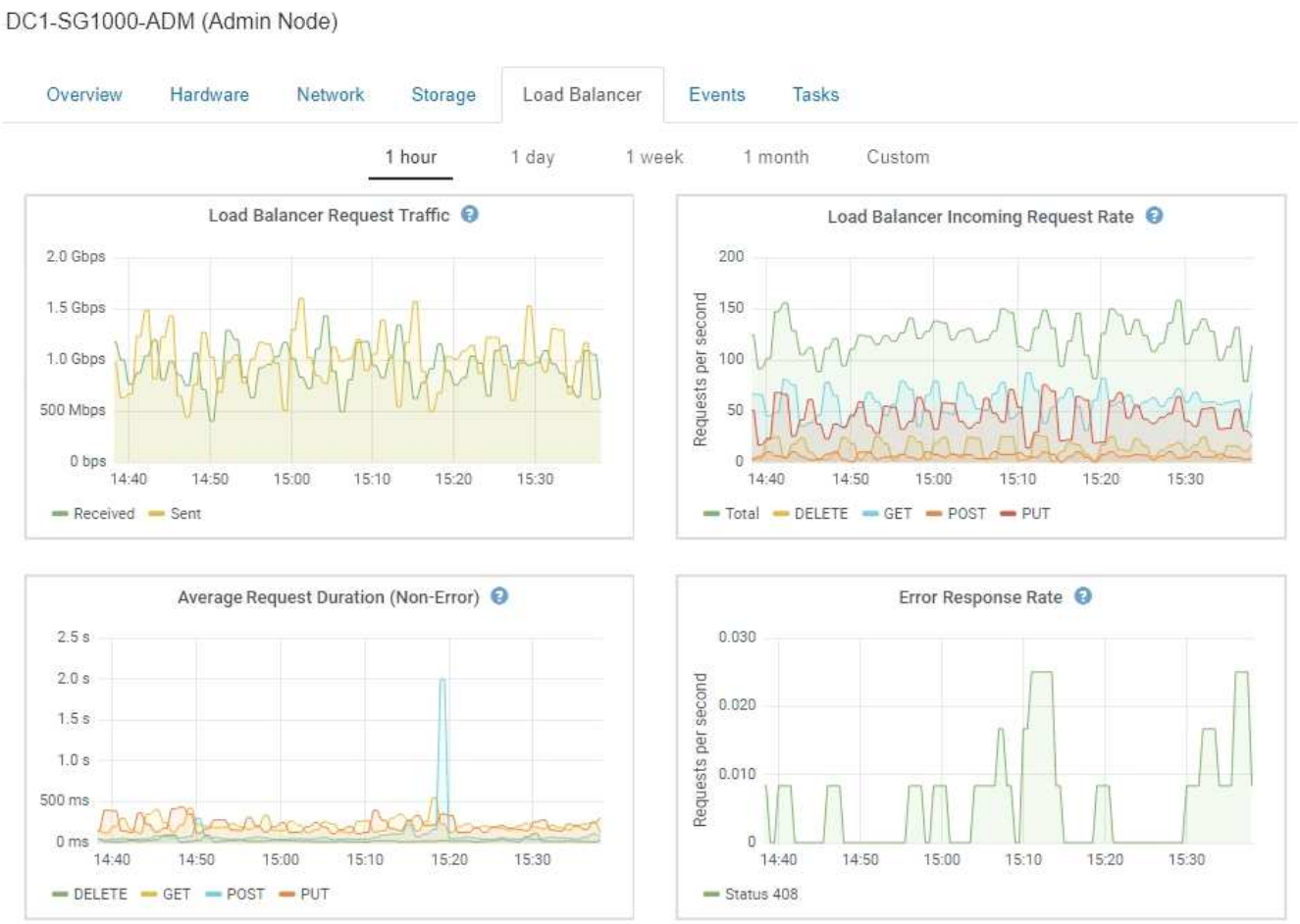
- Eine Liste der größten Buckets (S3) oder Container (Swift) für die Mandanten
- Ein Balkendiagramm, das die relative Größe der größten Buckets oder Container darstellt
- Der insgesamt verwendete Speicherplatz und, wenn ein Kontingent festgelegt ist, die Menge und der Prozentsatz des verbleibenden Speicherplatzes



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 Topology**.

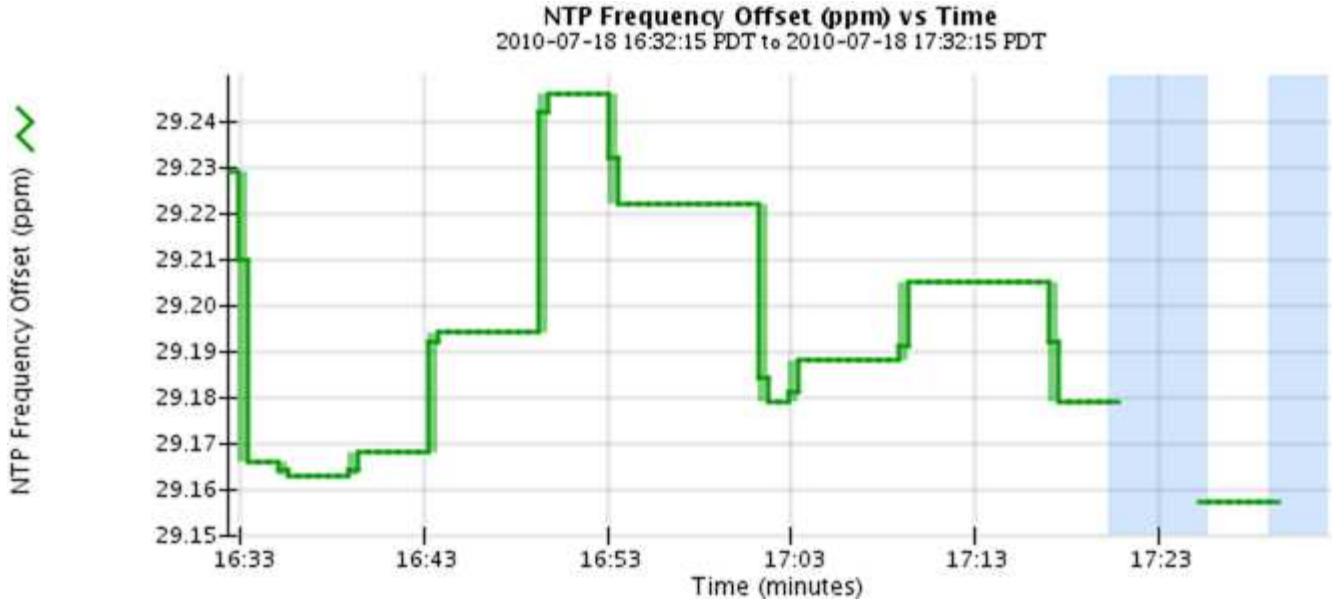
Es gibt vier Arten von Diagrammen:

- **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** > **Load Balancer** für einen Admin-Node enthält beispielsweise vier Grafana-Diagramme.

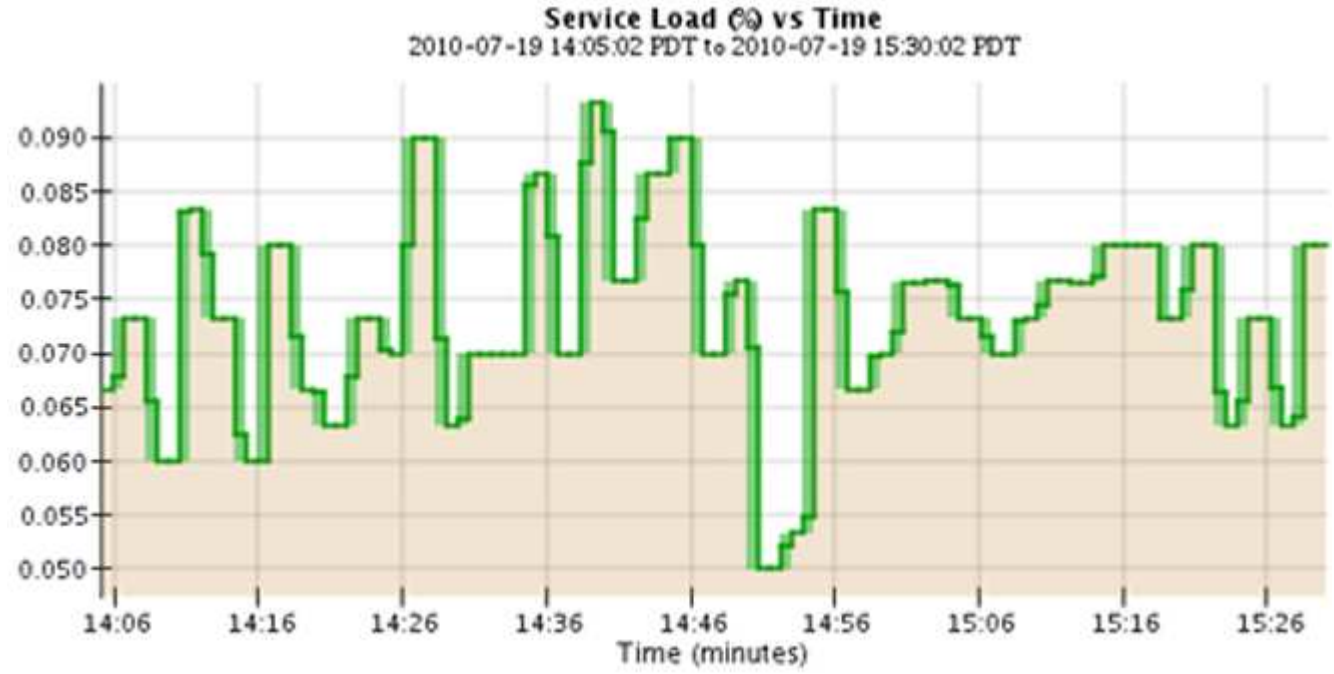


Grafana-Diagramme sind auch auf den vorkonfigurierten Dashboards enthalten, die auf der Seite **Support** > **Tools** > **Metrics** verfügbar sind.

- **Liniendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **Support** > **Tools** > **Grid Topology** (Klicken Sie auf das Chart-Symbol 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.

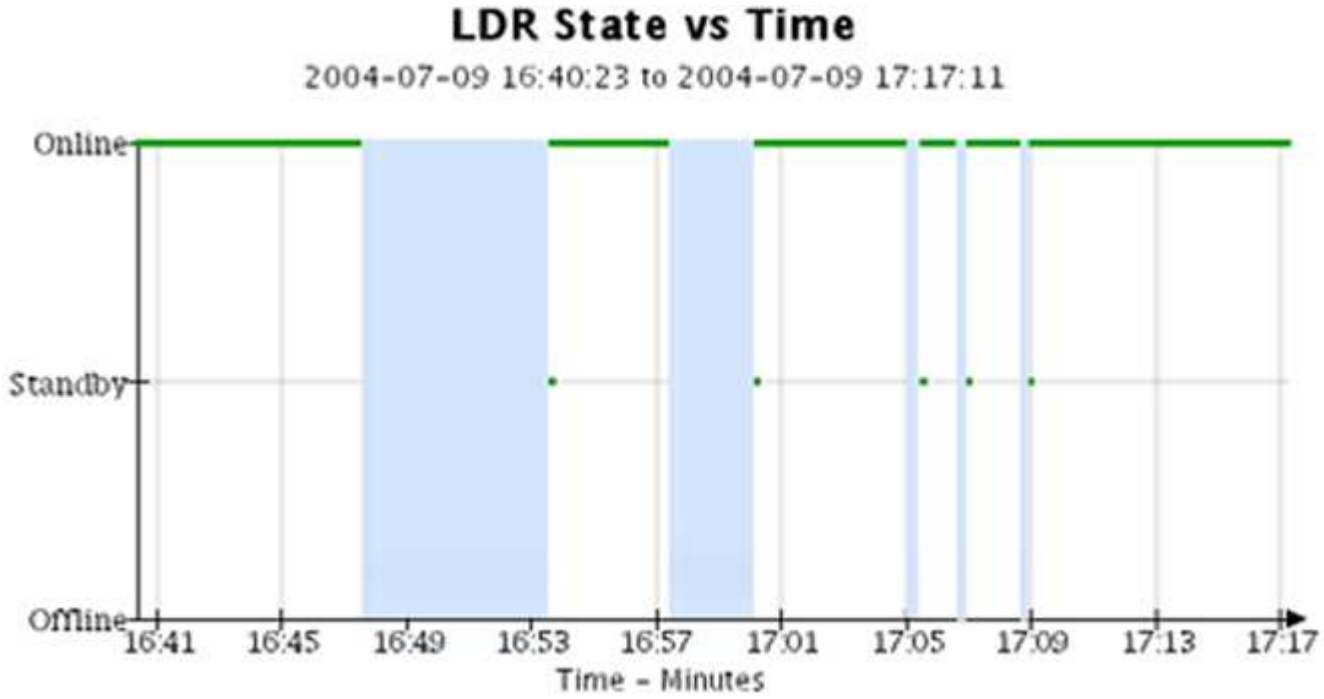


- **Flächendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **Support** > **Tools** > **Grid Topology** (Klicken Sie auf das Diagrammsymbol Nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen zu zeichnen, z. B. Objektanzahl oder Dienstlastwerte. Die Flächendiagramme 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:

- **Zustandsdiagramm**: Verfügbar auf der Seite **Support** > **Tools** > **Grid Topology** (Klicken Sie auf 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

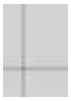
"Anzeigen der Seite Knoten"

"Anzeigen der Struktur der Grid Topology"

"Überprüfen von Support-Metriken"

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 unbekannten 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 unbekannten Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldet, administrativ nach unten lag.

Anzeigen von Diagrammen und Diagrammen

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.

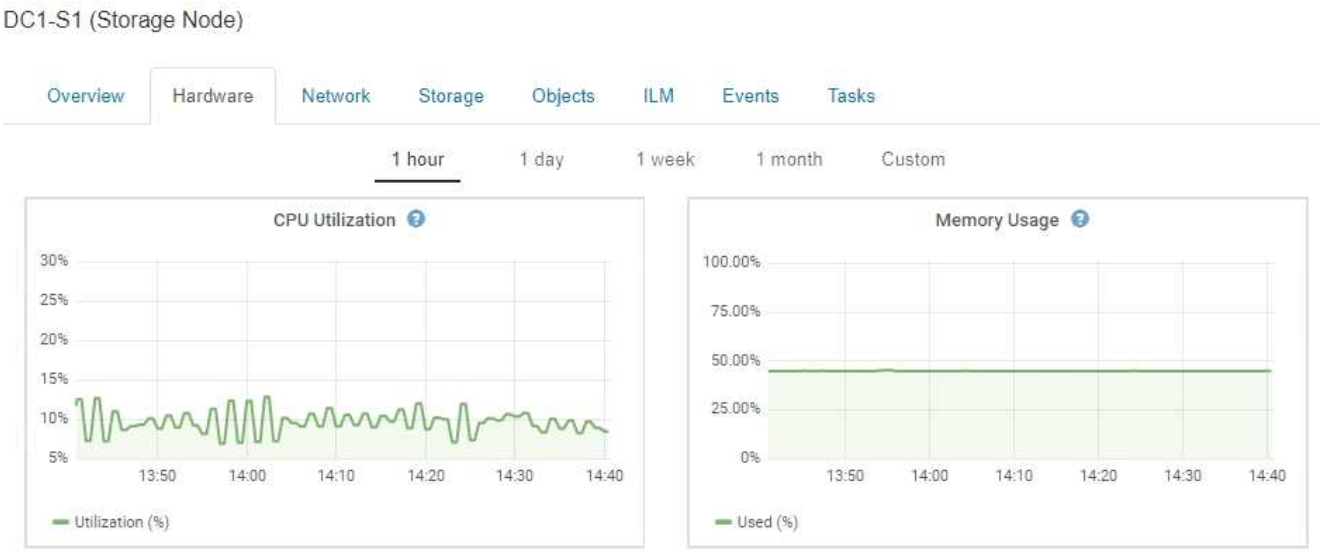
Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

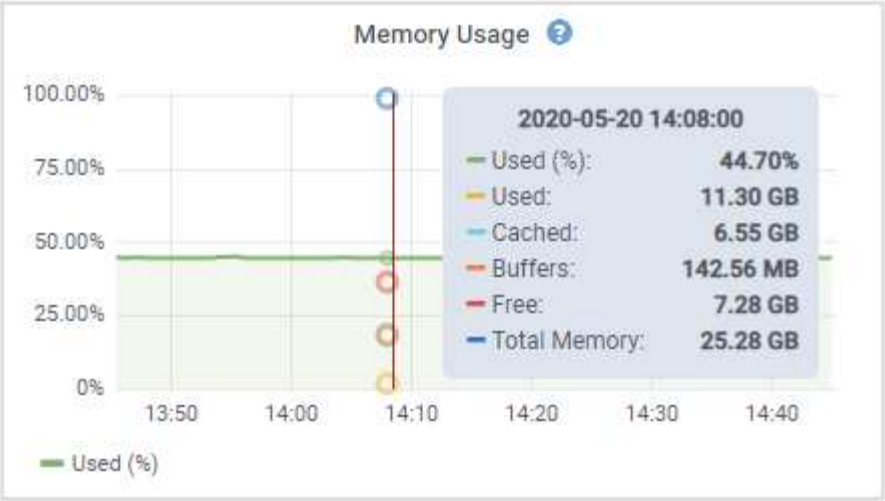
Schritte

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.



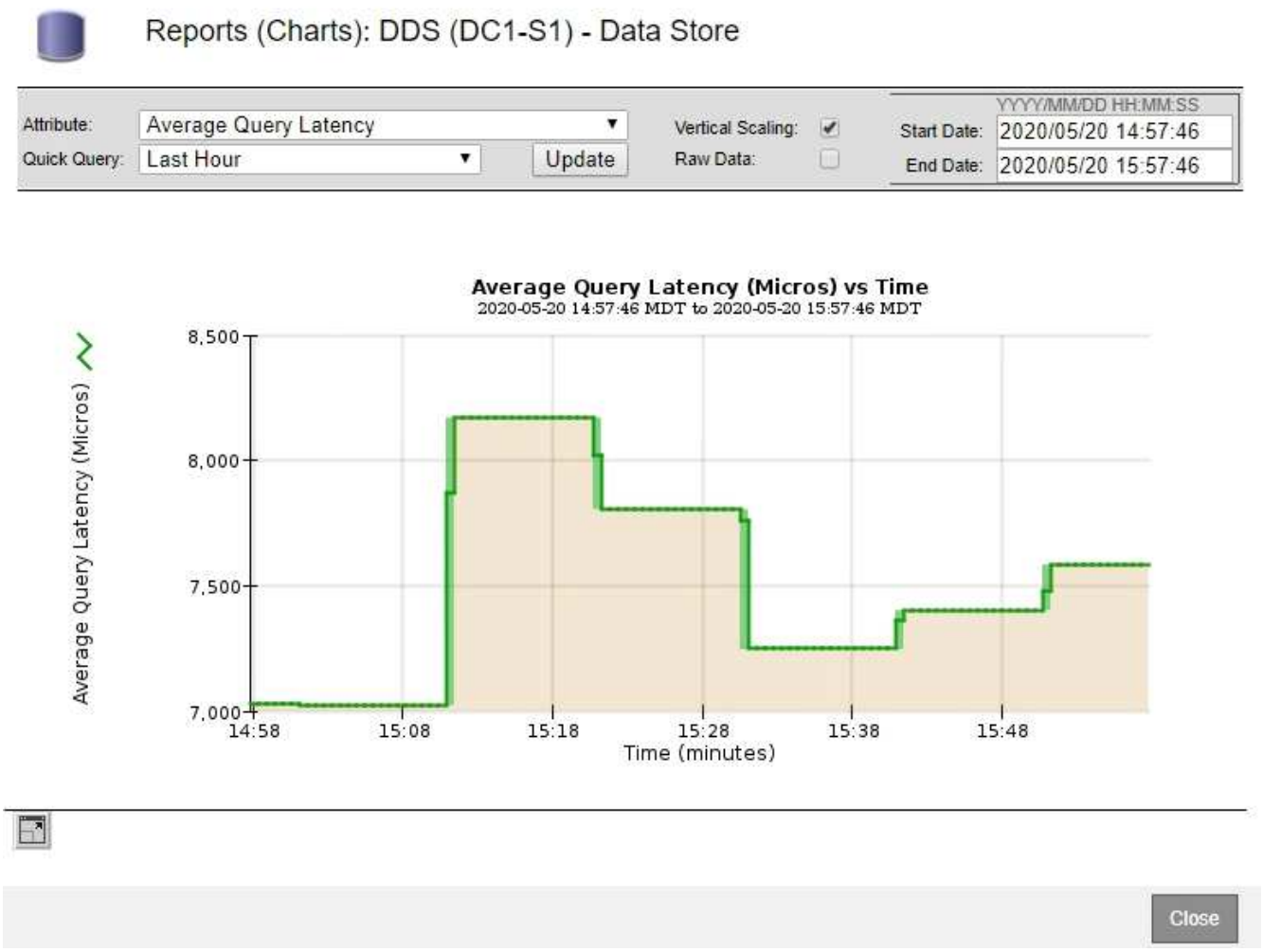
3. Bewegen Sie den Cursor optional über das Diagramm, um detailliertere Werte für einen bestimmten Zeitpunkt anzuzeigen.



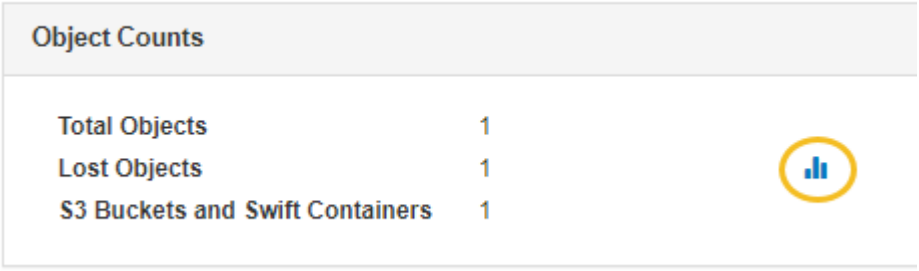
4. Bei Bedarf können Sie oft ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Klicken Sie in der Tabelle auf der Seite Knoten auf das Diagrammsymbol Oder Rechts neben dem Attributnamen.

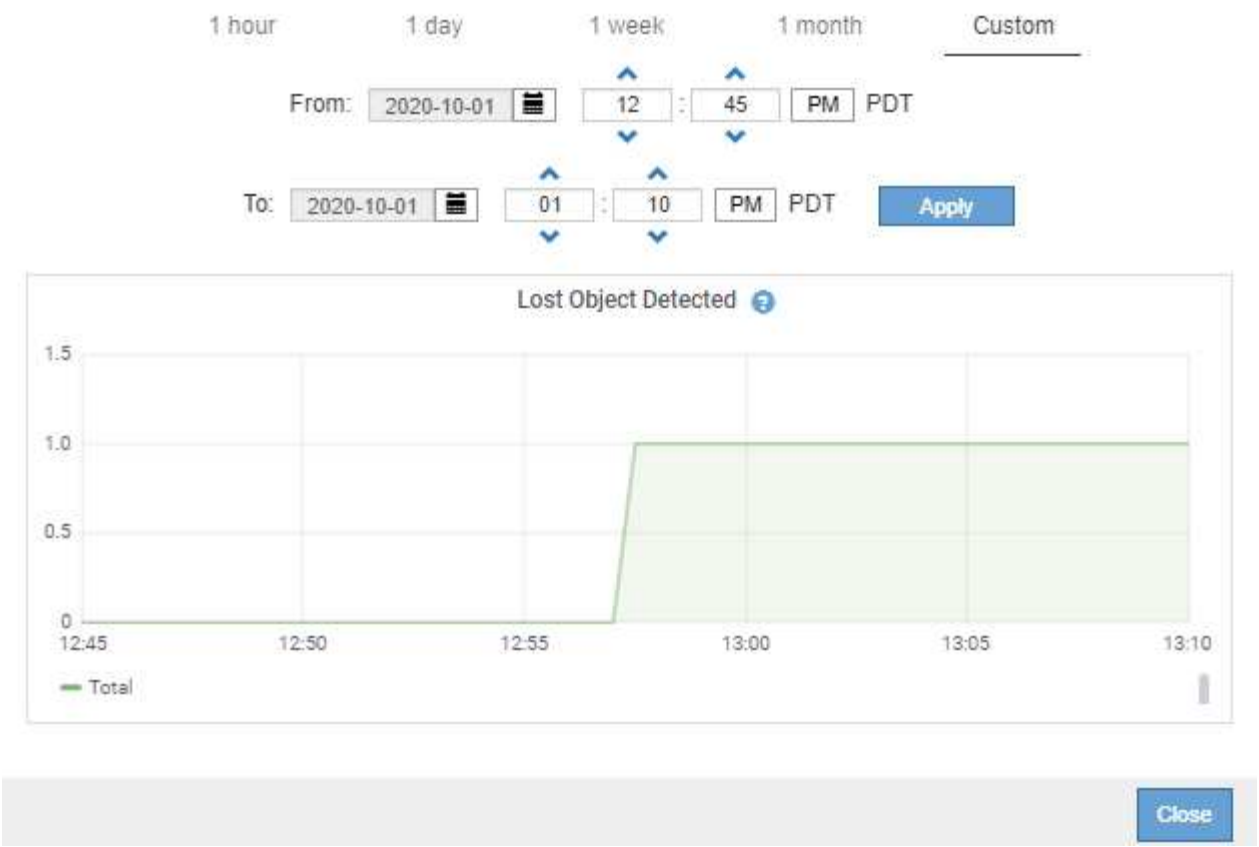
   Diagramme sind nicht für alle Metriken und Attribute verfügbar.

   Beispiel 1: Auf der Registerkarte Objekte für einen Speicherknoten können Sie auf das Diagrammsymbol klicken Um die durchschnittliche Latenz einer Metadatenabfrage im Laufe der Zeit anzuzeigen.



Beispiel 2: Auf der Registerkarte Objekte für einen Speicherknoten können Sie auf das Diagrammsymbol klicken Zeigt die Grafana-Grafik der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte an.





5. Um Diagramme für Attribute anzuzeigen, die nicht auf der Knotenseite angezeigt werden, wählen Sie **Support** > **Tools** > **Grid Topology**.
6. Wählen Sie ***Grid Node*** > ***Component oder Service*** > **Übersicht** > **Main** aus.
7. Klicken Sie auf das Diagrammsymbol Neben dem Attribut.

   Das Display wechselt automatisch zur Seite **Berichte** > **Diagramme**. Das Diagramm zeigt die Daten des Attributs über den letzten Tag an.

Diagramme werden erstellt

Diagramme zeigen eine grafische Darstellung der Attributdatenwerte an. Die Berichte können an Datacenter-Standorten, Grid-Node, Komponenten oder Service erstellt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** 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 die Y-Achse auf Null zu starten, deaktivieren Sie das Kontrollkästchen **Vertikale Skalierung**.

5. Um Werte mit voller Präzision anzuzeigen, aktivieren Sie das Kontrollkästchen **Raw Data** oder um Werte auf maximal drei Dezimalstellen zu runden (z. B. bei Attributen, die als Prozentsätze angegeben werden), deaktivieren Sie das Kontrollkästchen **Raw Data**.
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.

   Das Diagramm erscheint nach wenigen Augenblicken. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen.
7. 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.
8. Klicken Sie Auf **Aktualisieren**.

   Ein Diagramm wird nach wenigen Augenblicken 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.
9. Wenn Sie das Diagramm drucken möchten, klicken Sie mit der rechten Maustaste, und wählen Sie **Drucken**, und ändern Sie die erforderlichen Druckereinstellungen und klicken Sie auf **Drucken**.

Arten von Textberichten

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

Textberichte werden erstellt

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- 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 unbekannten Zustand war.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** 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 (z. B. für als Prozentwert gemeldete Attribute) zu runden, 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.

9. Wenn Sie den Bericht drucken möchten, klicken Sie mit der rechten Maustaste, und wählen Sie **Drucken**, und ändern Sie die erforderlichen Druckereinstellungen und klicken Sie auf **Drucken**.

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 Topology** 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: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
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.

Monitoring PUT und GET Performance

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 im Prüfprotokoll geben 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 erkennen können, die möglicherweise untersucht werden müssen.

- Sie können S3tester von github:https://github.com/s3tester herunterladen

Verwandte Informationen

"Prüfung von Audit-Protokollen"

Monitoring von Objektverifizierungsvorgängen

Das StorageGRID System kann die Integrität von Objektdaten auf Storage-Nodes überprüfen und sowohl beschädigte als auch fehlende Objekte prüfen.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Es gibt zwei Überprüfungsprozesse, die zusammenarbeiten, um die Datenintegrität zu gewährleisten:

- **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 **nicht identifiziertes korruptes Objekt erkannt** wird ausgelöst, wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann.

- **Vordergrundverifizierung** kann von einem Nutzer ausgelöst werden, um die Existenz (obwohl nicht die Richtigkeit) von Objektdaten schneller zu überprüfen.

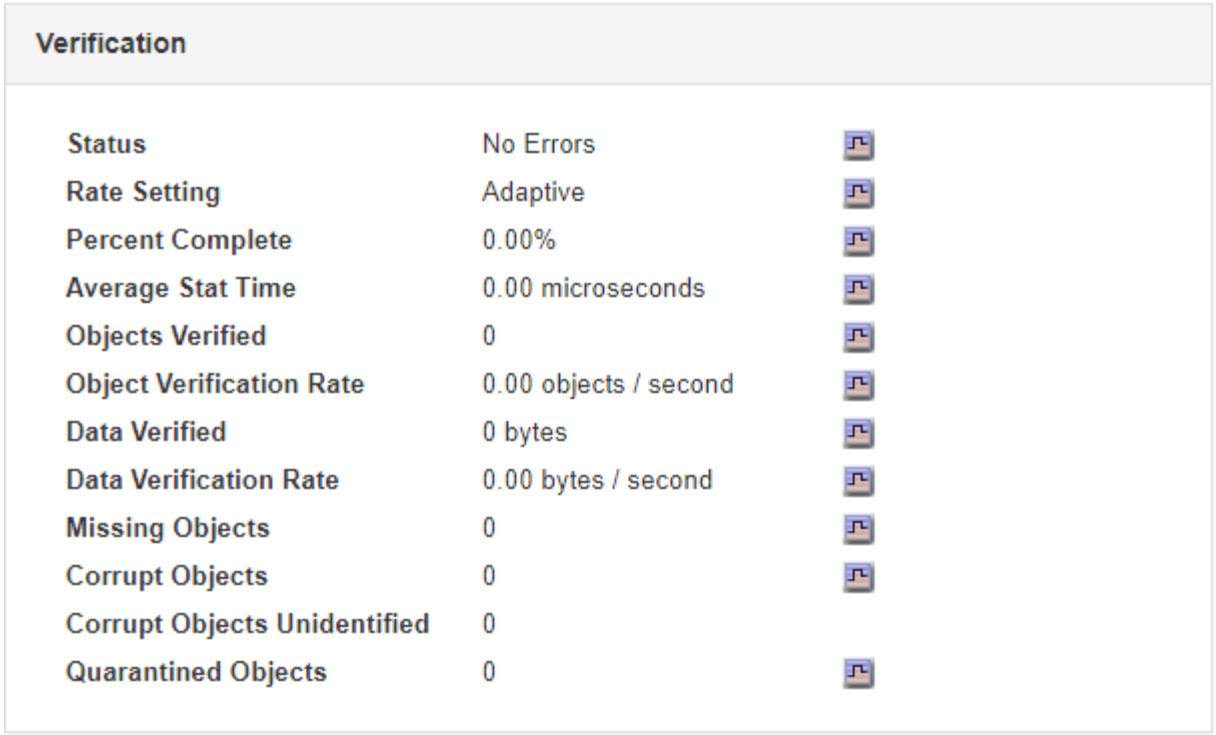
  Bei der Vordergrundüberprüfung können Sie die Existenz replizierter und Erasure-codierter Objektdaten auf einem bestimmten Storage-Node überprüfen und überprüfen, ob alle Objekte vorhanden sein sollen. Sie können die Vordergrundüberprüfung auf allen oder einigen Objektspeichern eines Storage Node ausführen, um festzustellen, ob es bei einem Speichergerät Integritätsprobleme gibt. Eine große Anzahl von fehlenden Objekten kann darauf hindeuten, dass es ein Problem mit der Speicherung gibt.

Um Ergebnisse aus Hintergrund- und Vordergrundverifizierungen, wie z. B. beschädigte oder fehlende Objekte, zu prüfen, können Sie auf der Seite Knoten einen Speicherknoten sehen. Sie sollten alle Instanzen von beschädigten oder fehlenden Objektdaten sofort untersuchen, um die Ursache zu ermitteln.

Schritte

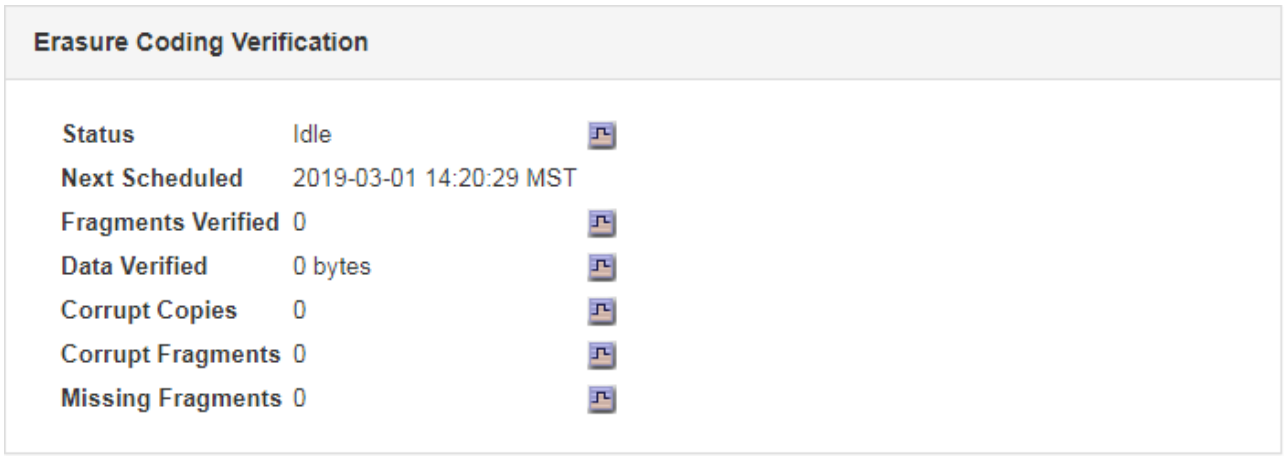
1. Wählen Sie **Knoten**.
2. Wählen Sie ***Speicherknoten*** > **Objekte** Aus.
3. So prüfen Sie die Überprüfungsergebnisse:

   - Um die Verifizierung replizierter Objektdaten zu prüfen, sehen Sie sich die Attribute im Abschnitt Überprüfung an.



Klicken Sie in der Tabelle auf den Namen eines Attributs, um den Hilfetext anzuzeigen.

- Um die Überprüfung von Fragment mit Löschungscode zu überprüfen, wählen Sie ***Storage Node*** > **ILM** aus, und sehen Sie sich die Attribute in der Tabelle „Erasure Coding Verification“ an.



Klicken Sie in der Tabelle auf den Namen eines Attributs, um den Hilfetext anzuzeigen.

Verwandte Informationen

"Überprüfen der Objektintegrität"

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.

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 Alarme aufgetreten sind. Wenn ein Ereignis aufgrund eines bekannten Problems aufgetreten ist, können die Ereigniszähler sicher zurückgesetzt werden.

Überprüfen von Ereignissen auf der Seite Knoten

Auf der Seite Nodes werden die Systemereignisse für jeden Grid-Node aufgeführt.

1. Wählen Sie **Knoten**.
2. Wählen Sie ***Grid Node*** > **Events** aus.
3. Stellen Sie oben auf der Seite fest, ob ein Ereignis für **Letztes Ereignis** angezeigt wird, das das letzte Ereignis beschreibt, das vom Grid-Knoten erkannt wurde.

   Das Ereignis wird wortgetreu vom Grid-Node übermittelt und enthält alle Protokollmeldungen mit dem Schweregrad „FEHLER“ oder „KRITISCH“.
4. Überprüfen Sie in der Tabelle, ob die Anzahl für ein Ereignis oder einen Fehler nicht Null ist.
5. Klicken Sie nach dem Beheben von Problemen auf **Ereignisanzahl zurücksetzen**, um die Zählung auf Null zurückzusetzen.

Überprüfen von Ereignissen auf der Seite Grid Topology

Auf der Seite Grid Topology werden außerdem die Systemereignisse für jeden Grid-Node aufgeführt.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Events** > **Übersicht** > **Main**.

Verwandte Informationen

"Ereignisanzahl wird zurückgesetzt"

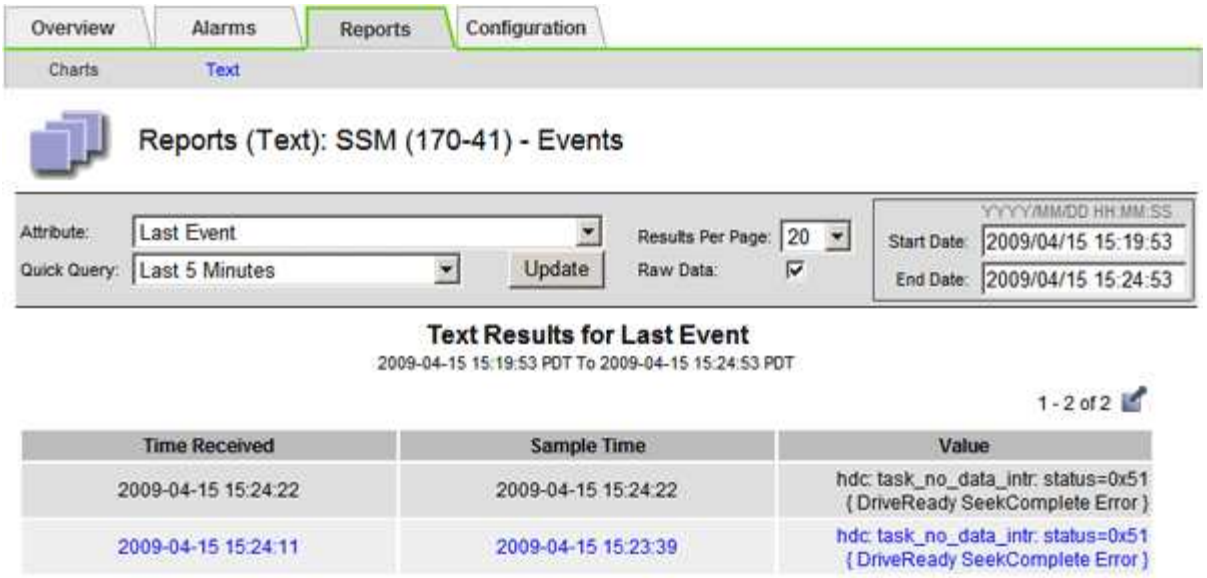
"Referenz für Protokolldateien"

Vorherige Ereignisse überprüfen

Sie können eine Liste vorheriger Ereignismeldungen generieren, um Probleme zu isolieren, die in der Vergangenheit aufgetreten sind.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Events** > **Berichte** aus.
3. Wählen Sie **Text**.

   Das Attribut **Letztes Ereignis** wird in der Ansicht Diagramme nicht angezeigt.
4. Ändern Sie **Attribut** in **Letztes Ereignis**.
5. Wählen Sie optional einen Zeitraum für **Quick Query** aus.
6. Klicken Sie Auf **Aktualisieren**.



Verwandte Informationen

"Verwenden von Diagrammen und Berichten"

Ereignisanzahl wird zurückgesetzt

Nach dem Beheben von Systemereignissen können Sie die Ereignisanzahl auf Null zurücksetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung für die Konfiguration der Seite für die Grid-Topologie verfügen.

Schritte

1. Wählen Sie **Nodes** > ***Grid Node*** > **Events** Aus.
2. Stellen Sie sicher, dass jedes Ereignis mit einer Zählung von mehr als 0 gelöst wurde.
3. Klicken Sie auf **Ereignisanzahl zurücksetzen**.

Events

Last Event No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Heap Out Of Memory Errors	0
Cassandra unhandled exceptions	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	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
Node Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0
Stat Service Events	0
Storage Hardware Events	0
System Time Events	0

Reset event counts

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

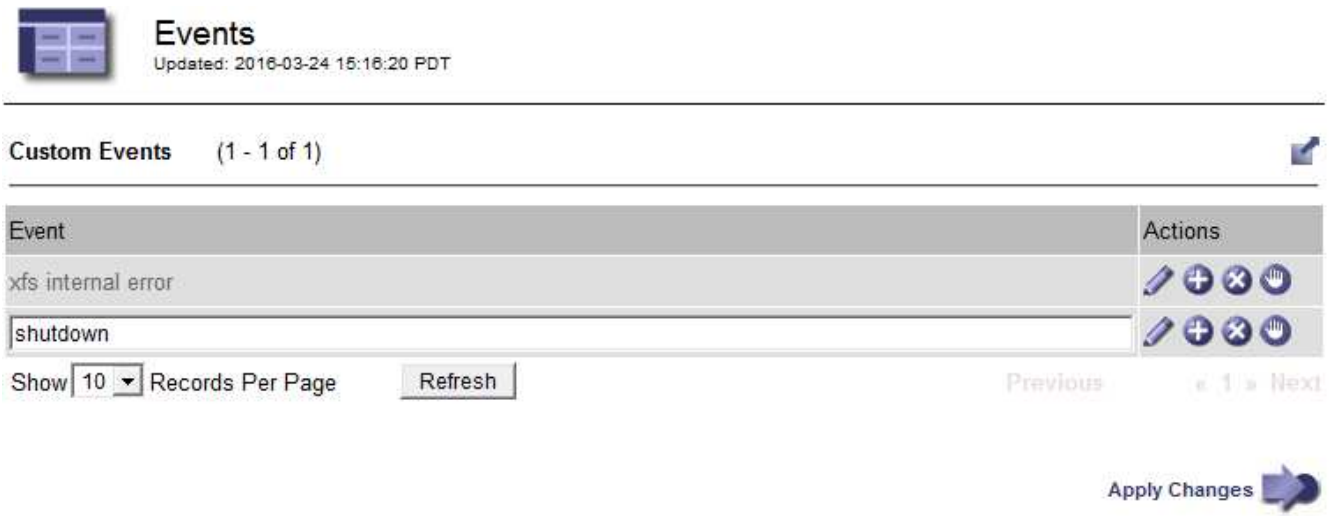
Ziehen Sie in Betracht, benutzerdefinierte Ereignisse zu erstellen, um wiederkehrende Probleme zu überwachen. Die folgenden Überlegungen gelten für benutzerdefinierte Ereignisse.

- Nach der Erstellung eines benutzerdefinierten Ereignisses wird jeder Vorgang überwacht. Auf der Seite **Nodes** > ***GRID Node*** > **Events** können Sie einen kumulativen Zählwert für alle benutzerdefinierten Ereignisse anzeigen.
- So erstellen Sie ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern im `/var/log/messages` Oder `/var/log/syslog` 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/log/messages` Oder `/var/log/syslog` Die Dateien werden abgeglichen, sofern sie nicht die oben genannten Anforderungen erfüllen.

Schritte

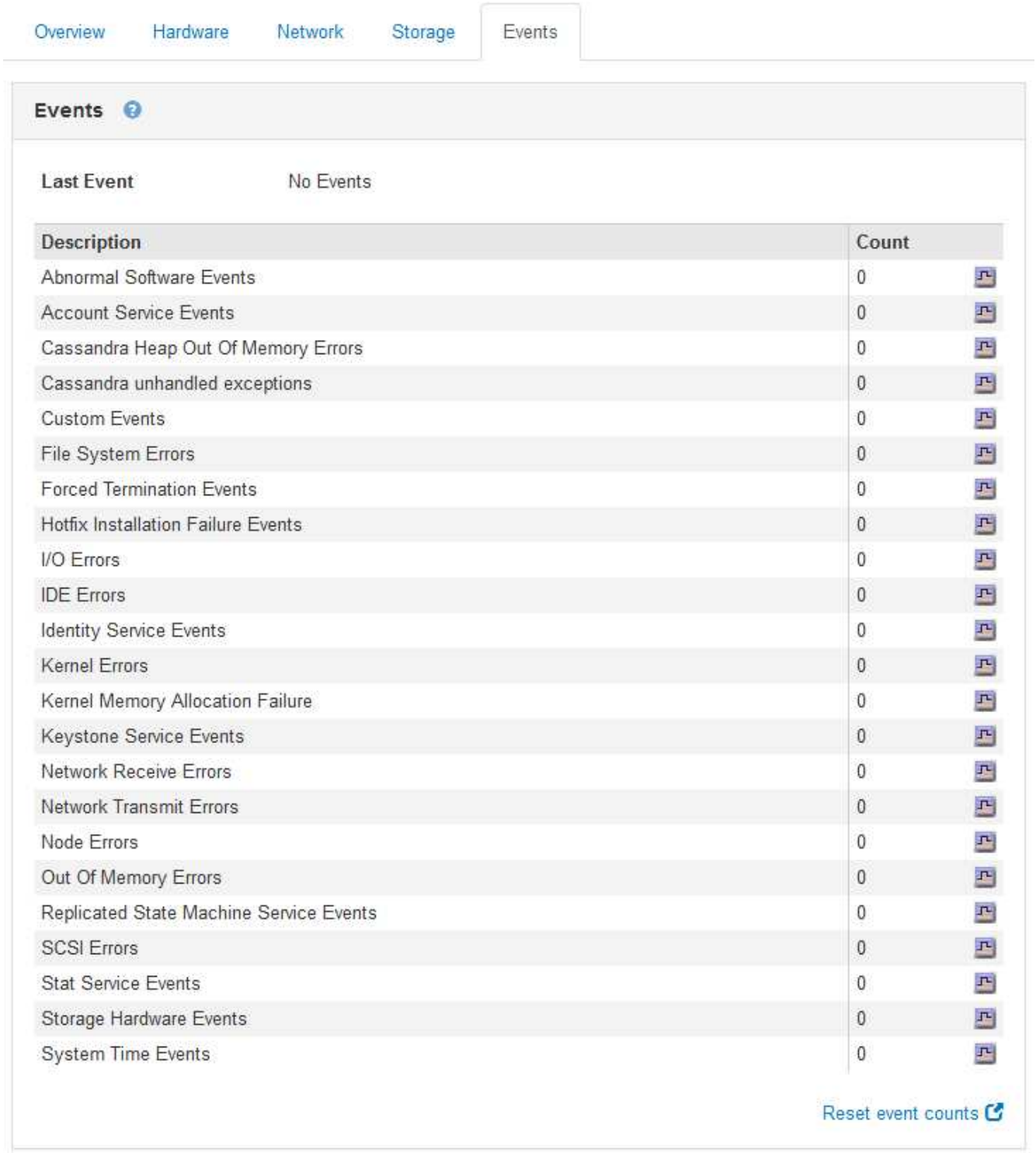
1. Wählen Sie **Konfiguration** > **Überwachung** > **Ereignisse**.
2. Klicken Sie Auf **Bearbeiten** (Oder **Einfügen** Wenn dies nicht das erste Ereignis ist).
3. Geben Sie eine benutzerdefinierte Ereigniszeichenfolge ein, z. B. Herunterfahren



4. Klicken Sie Auf **Änderungen Übernehmen**.
5. Wählen Sie **Knoten**. Wählen Sie dann ***GRID Node*** > **Events** aus.
6. 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.



Zurücksetzen der Anzahl benutzerdefinierter Ereignisse auf Null

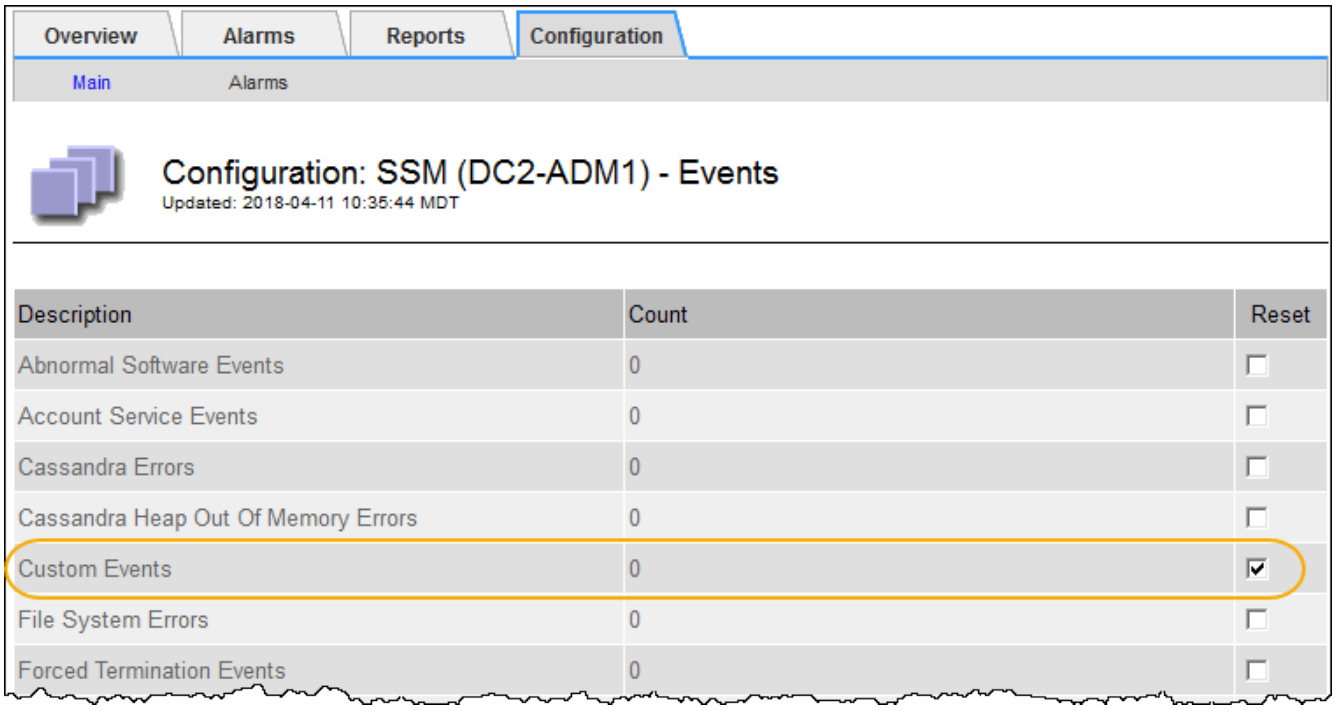
Wenn Sie den Zähler nur für benutzerdefinierte Ereignisse zurücksetzen möchten, müssen Sie die Seite Grid Topology im Menü Support verwenden.

Über diese Aufgabe

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.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Grid Node*** > **SSM** > **Events** > **Konfiguration** > **Main** aus.
3. Aktivieren Sie das Kontrollkästchen **Zurücksetzen** für benutzerdefinierte Ereignisse.



4. Klicken Sie Auf **Änderungen Übernehmen**.

Überprüfen von Audit-Meldungen

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.

Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf die Audit-Share sowohl für NFS als auch für CIFS (veraltet) konfigurieren. Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Details zur Audit-Protokolldatei, zum Format von Audit-Meldungen, zu den Typen von Audit-Meldungen und zu den verfügbaren Tools zur Analyse von Audit-Meldungen finden Sie in den Anweisungen für Audit-Meldungen. Weitere Informationen zum Konfigurieren des Zugriffs auf Audit-Clients finden Sie in den Anweisungen für die Administration von StorageGRID.

Verwandte Informationen

"Prüfung von Audit-Protokollen"

"StorageGRID verwalten"

Protokolldateien und Systemdaten werden erfasst

Mit dem Grid Manager können Sie Protokolldateien und Systemdaten (einschließlich Konfigurationsdaten) für Ihr StorageGRID System abrufen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

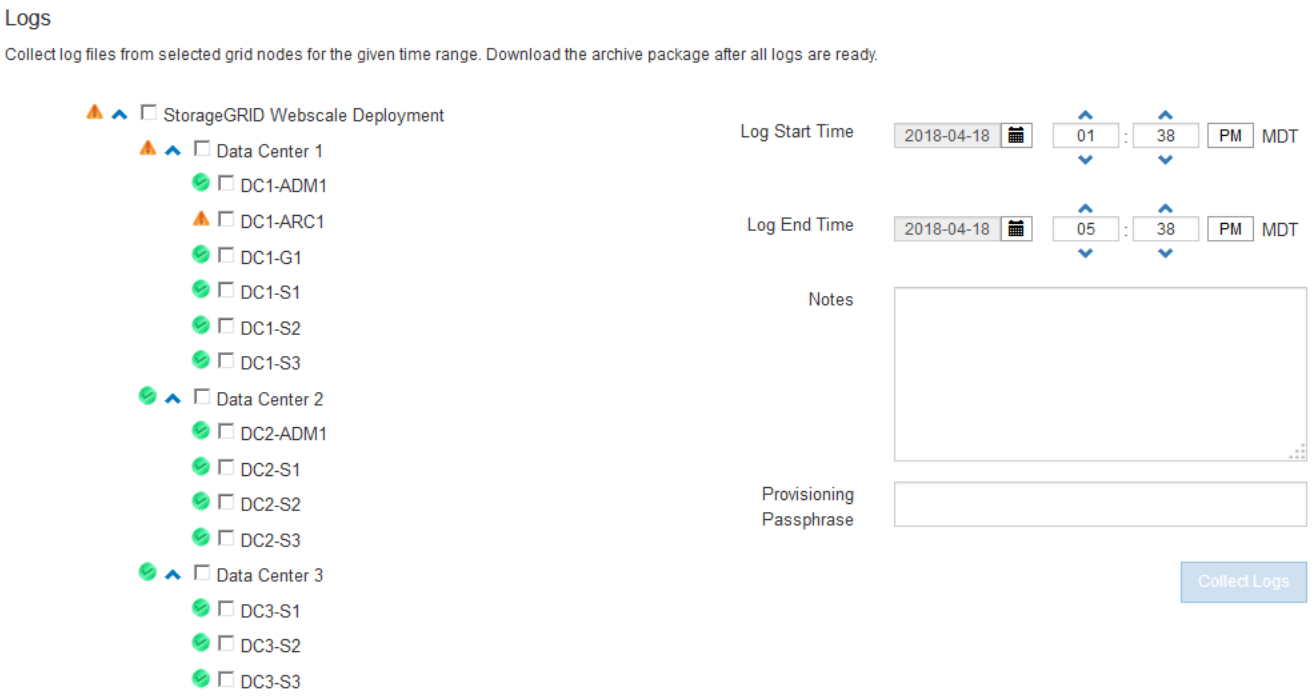
Über diesen Taak

Mit dem Grid Manager können Sie Protokolldateien, Systemdaten und Konfigurationsdaten für den von Ihnen ausgewählten Zeitraum von einem beliebigen Grid-Node aus erfassen. Die Daten werden in einer .tar.gz-Datei gesammelt und archiviert, die Sie dann auf Ihren lokalen Computer herunterladen können.

Da Anwendungsprotokolle sehr groß sein können, muss das Zielverzeichnis, in dem Sie die archivierten Protokolldateien herunterladen, mindestens 1 GB freien Speicherplatz haben.

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.

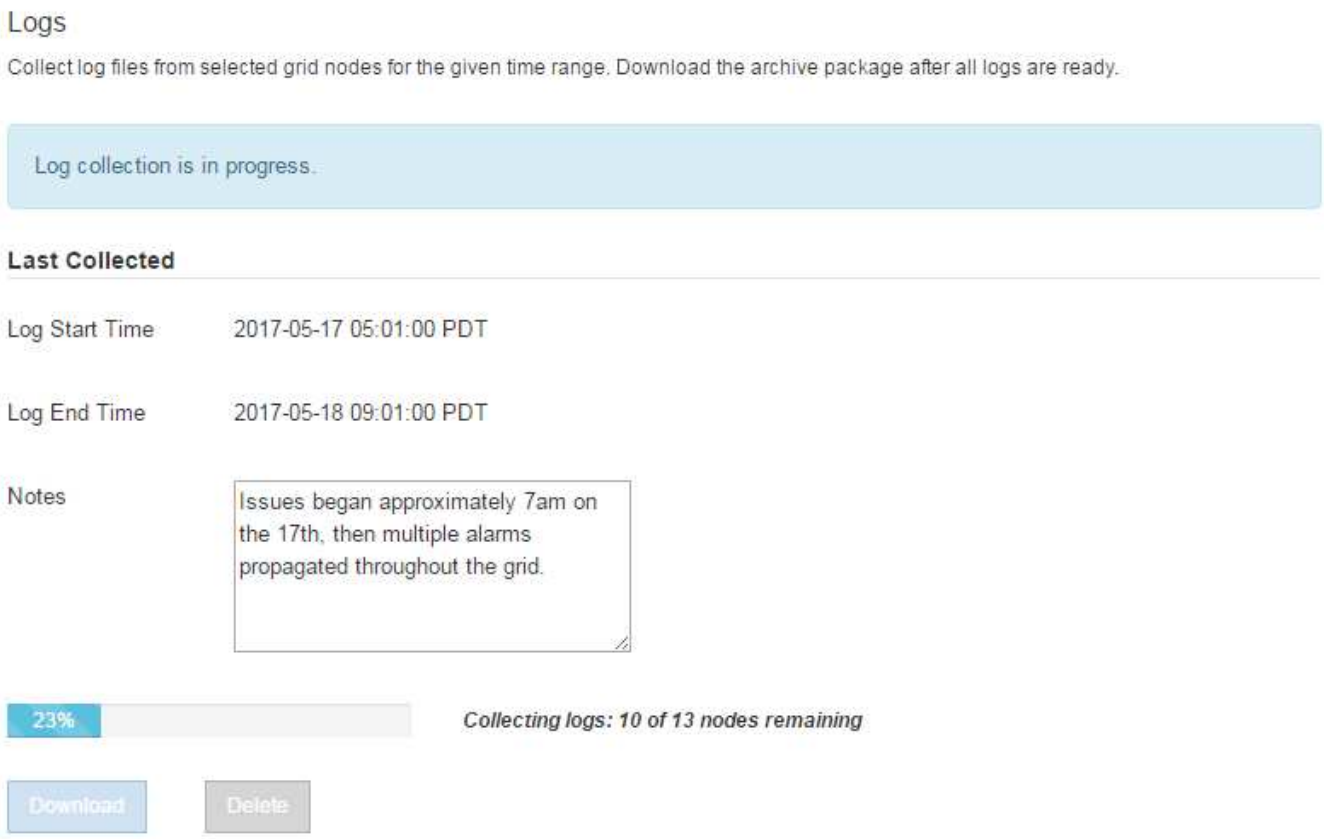
   Wenn Sie einen sehr langen Zeitraum auswählen oder Protokolle von allen Knoten in einem großen Raster sammeln, könnte das Protokollarchiv zu groß werden, um auf einem Knoten gespeichert zu werden, oder zu groß, um zum Download an den primären Admin-Knoten gesammelt zu werden. In diesem Fall müssen Sie die Protokollerfassung mit einem kleineren Datensatz neu starten.

4. Geben Sie optional Hinweise 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.

5. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
6. Klicken Sie Auf **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.

7. Klicken Sie auf **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 auf **Löschen** klicken, 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.

Verwandte Informationen

"Referenz für Protokolldateien"

Manuelles Auslösen einer AutoSupport-Meldung

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Wählen Sie **vom Benutzer ausgelöste AutoSupport senden** aus.

   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.

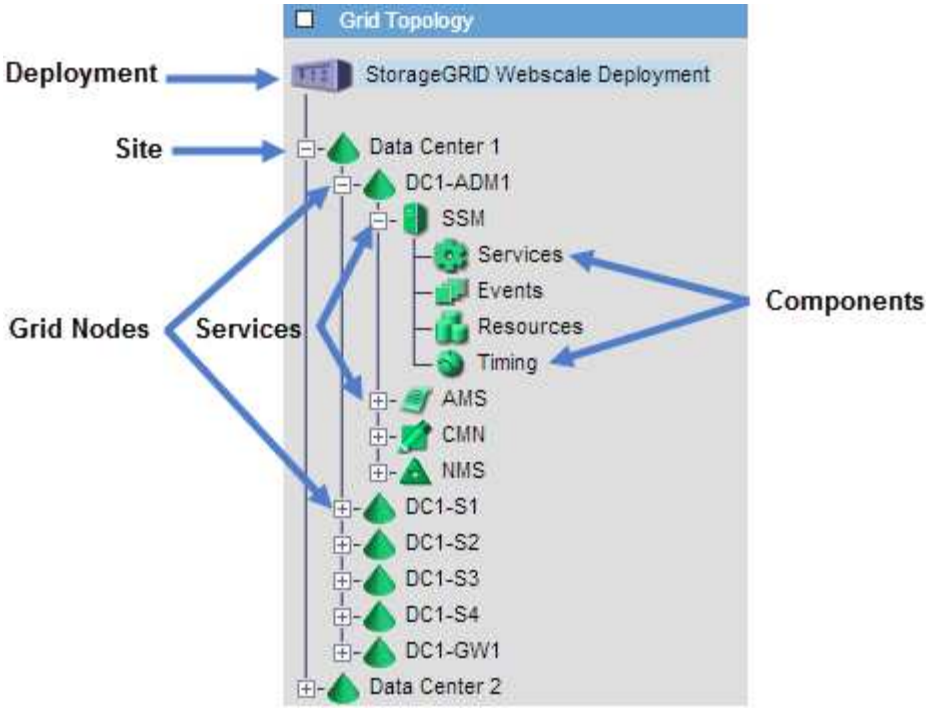
Verwandte Informationen

"Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"

Anzeigen der Struktur der Grid Topology

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 **Support** > **Tools** > **Grid Topology**.



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.

Überprüfen von Support-Metriken

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte Metriken und Diagramme für Ihr StorageGRID System prüfen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

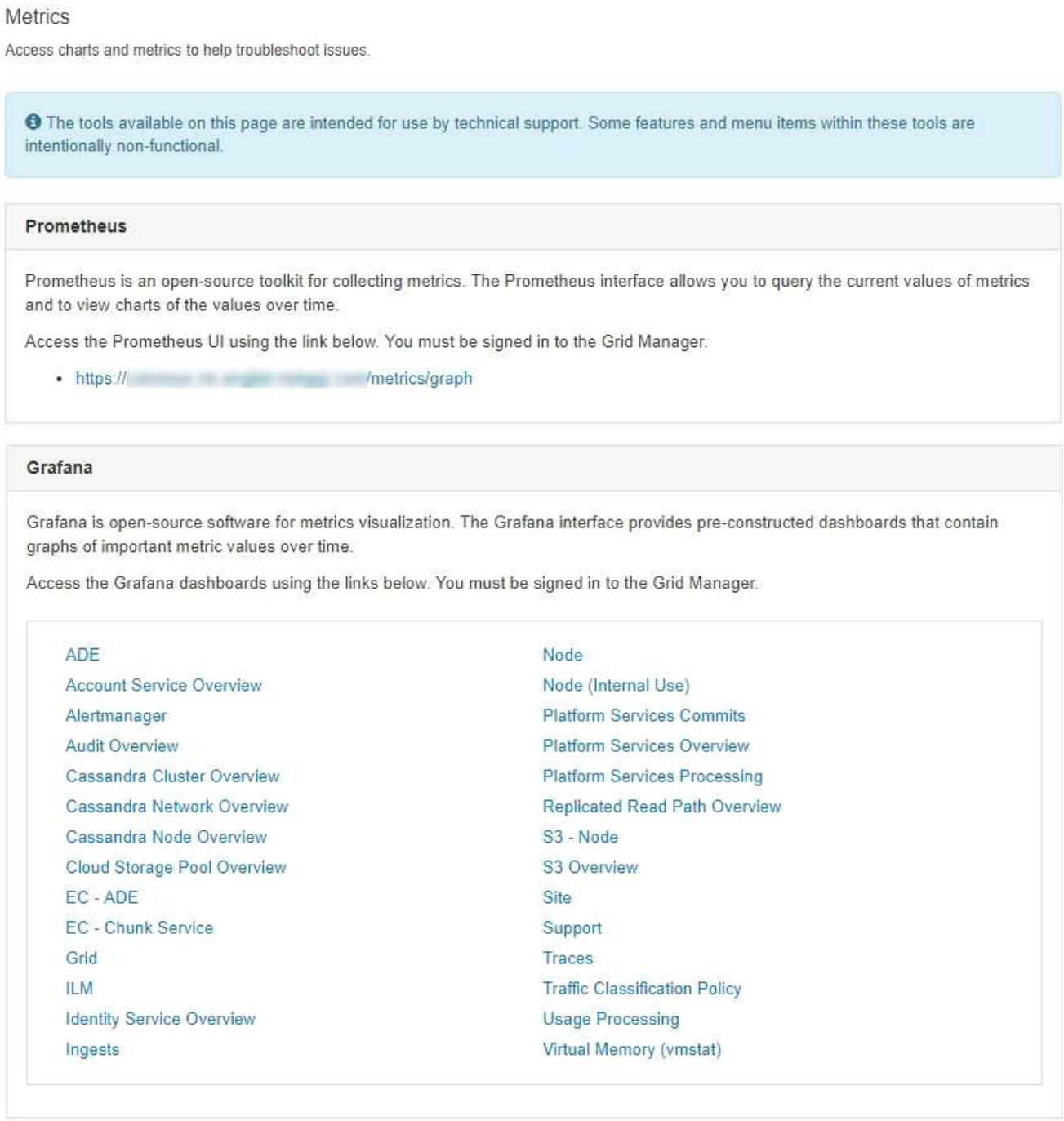
Auf der Seite Metriken können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist Open-Source-Software zum Sammeln von Kennzahlen. Grafana ist Open-Source-Software zur Visualisierung von Kennzahlen.

> ⓘ 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.

Schritte

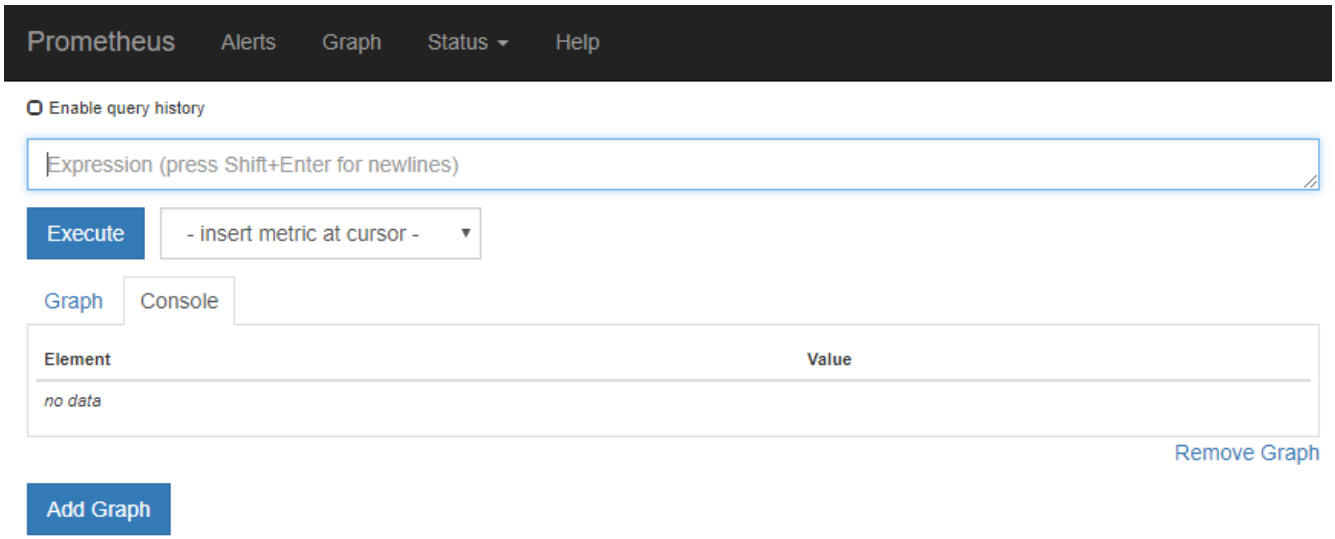
1. Wählen Sie nach Anweisung des technischen Supports **Support** > **Tools** > **Metriken**.

   Die Seite Metriken wird angezeigt.



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.



Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

3. 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.

Verwandte Informationen

"Häufig verwendete Prometheus-Kennzahlen"

Diagnose wird ausgeführt

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support eine Diagnose auf Ihrem StorageGRID-System durchführen und die Ergebnisse überprüfen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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:

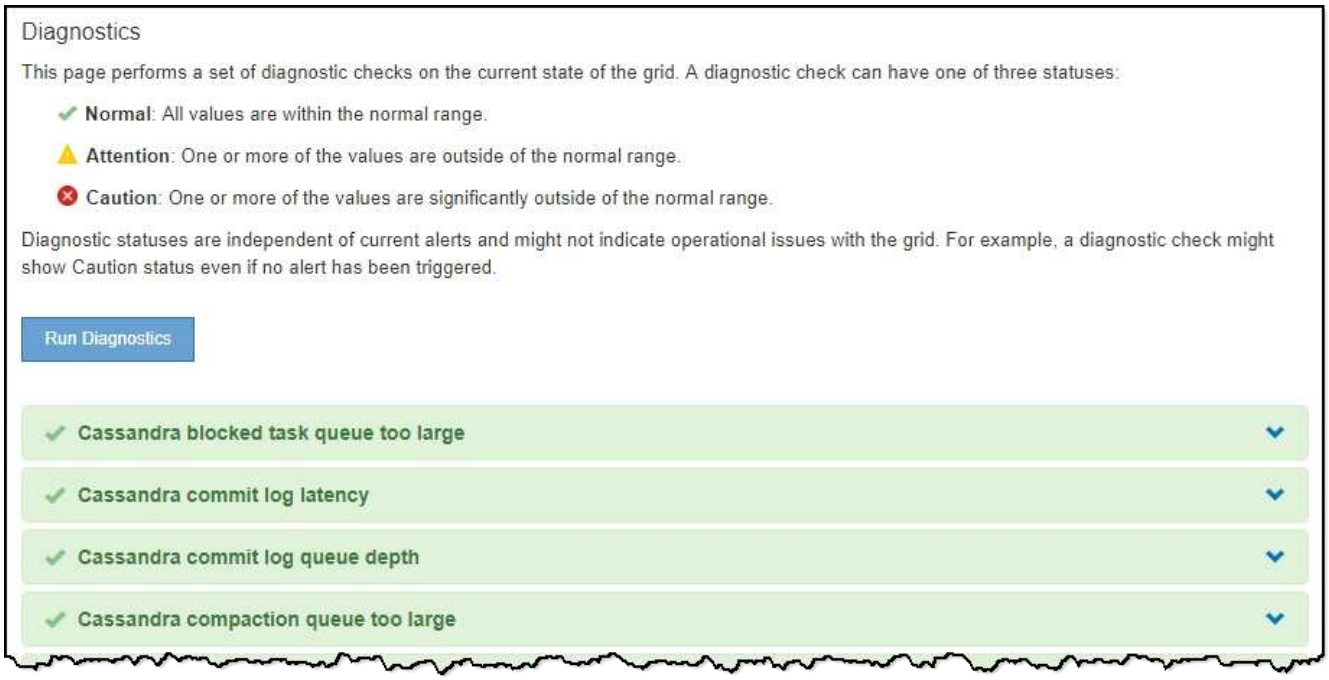
- **Normal**: Alle Werte liegen im Normalbereich.
- **Achtung**: Ein oder mehrere Werte liegen außerhalb des normalen Bereichs.
- **Achtung**: Ein oder mehrere der Werte liegen deutlich außerhalb des normalen Bereichs.

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 Diagnosetest an. Im Beispiel haben alle Diagnosen einen normalen Status.



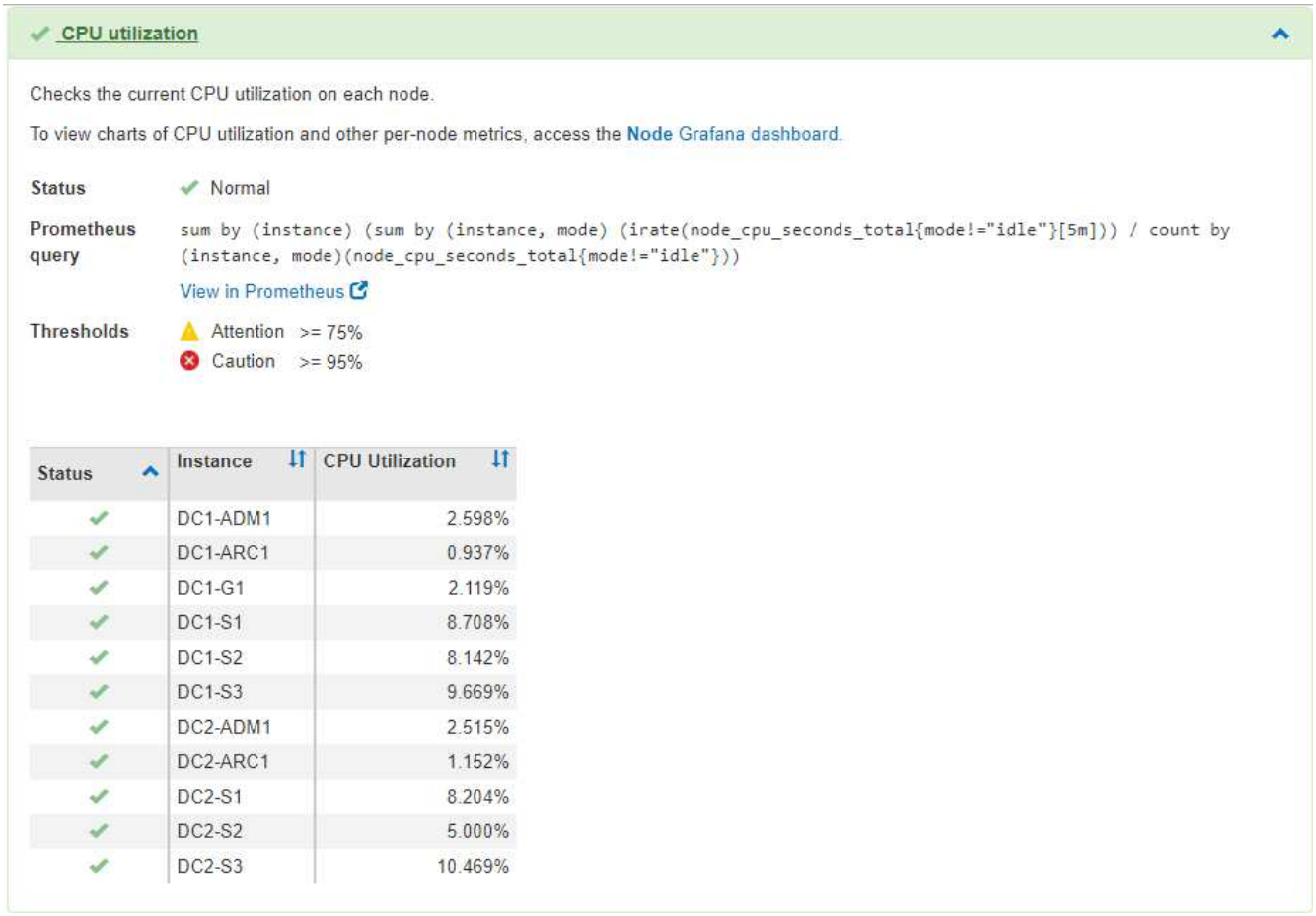
2. Wenn Sie mehr über eine bestimmte Diagnose erfahren möchten, klicken Sie auf eine beliebige Stelle in der Zeile.

   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. (Schwellwerte 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.



3. **Optional**: Um Grafana-Diagramme zu dieser Diagnose anzuzeigen, klicken Sie auf den Link **Grafana Dashboard**.

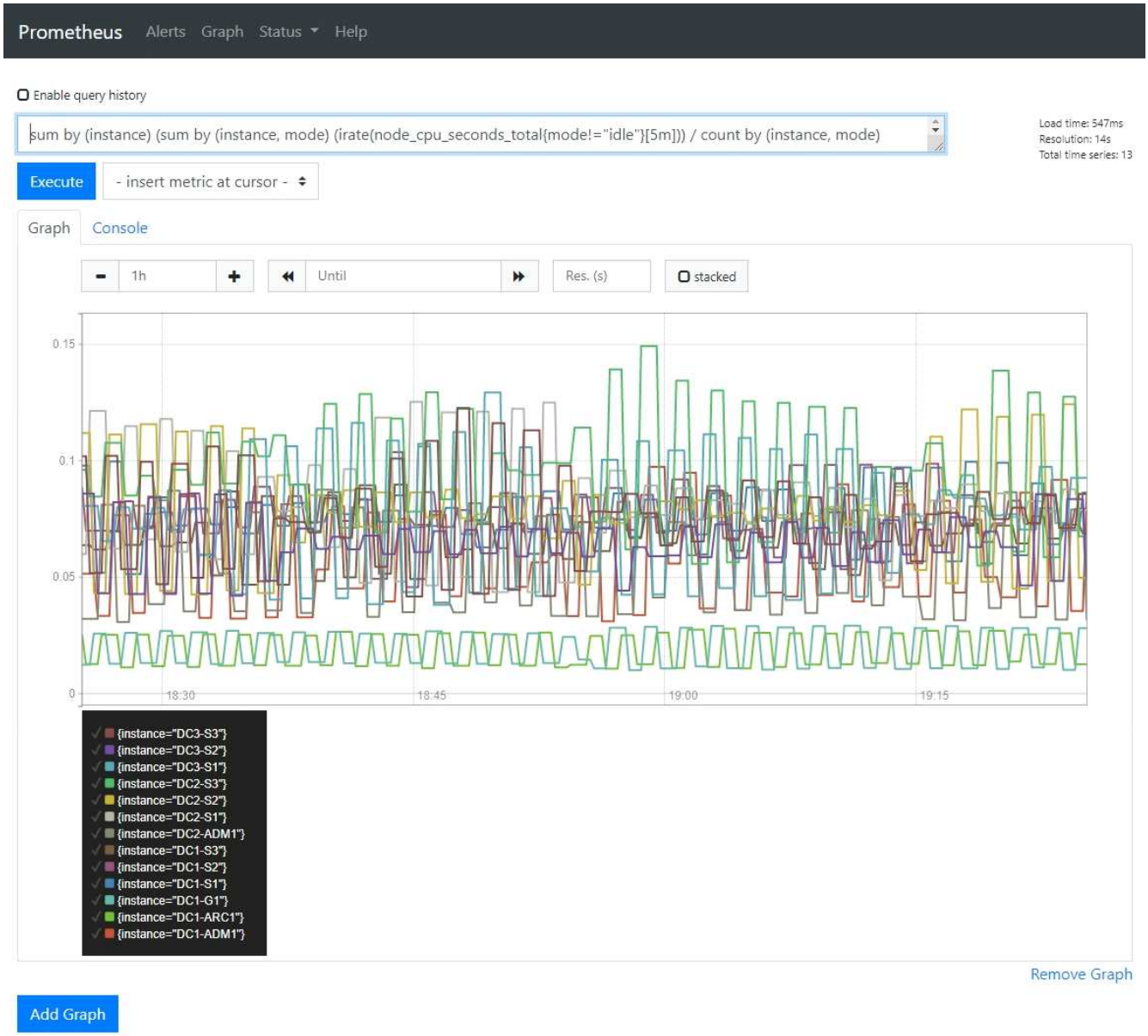
   Dieser Link wird nicht für alle Diagnosen angezeigt.

   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.



Verwandte Informationen

"Überprüfen von Support-Metriken"

"Häufig verwendete Prometheus-Kennzahlen"

Erstellen benutzerdefinierter Überwachungsanwendungen

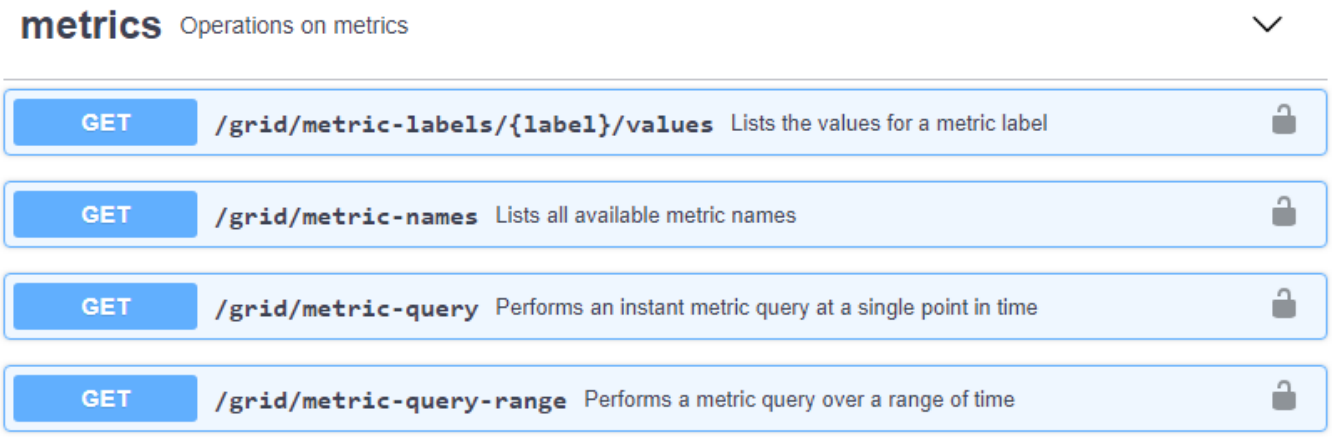
Mithilfe der StorageGRID-Kennzahlen der Grid-Management-API können Sie benutzerdefinierte Monitoring-Applikationen und Dashboards erstellen.

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 mithilfe der Grid Management API die StorageGRID-Kennzahlen abfragen.

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. Lesen Sie die Anweisungen zum

Verwalten von StorageGRID.

Um die Vorgänge der Kennzahlen-API einschließlich der vollständigen Liste der verfügbaren Metriken anzuzeigen, gehen Sie zum Grid Manager und wählen Sie **Hilfe** > **API-Dokumentation** > **Metriken**.



Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung liegen über dem Umfang dieses Leitfadens hinaus.

Verwandte Informationen

"StorageGRID verwalten"

Alerts Referenz

In der folgenden Tabelle sind alle standardmäßigen StorageGRID-Warnmeldungen aufgeführt. Bei Bedarf können Sie benutzerdefinierte Alarmregeln erstellen, die Ihrem Systemmanagement entsprechen.

Hier finden Sie Informationen zu den häufig verwendeten Prometheus-Kennzahlen, um sich über die Metriken zu informieren, die in einigen dieser Warnmeldungen verwendet werden.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts abgelaufen	Der Akku im Speicher-Controller des Geräts ist abgelaufen. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts fehlgeschlagen	Der Akku im Speicher-Controller des Geräts ist ausgefallen. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Akku des Geräts weist nicht genügend Kapazität auf	Der Akku im Speicher-Controller des Geräts weist nicht genügend Kapazität auf. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Akku des Geräts befindet sich nahe dem Ablauf	Der Akku im Speicher-Controller des Geräts läuft langsam ab. 1. Setzen Sie die Batterie bald wieder ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts entfernt	Der Akku im Speicher-Controller des Geräts fehlt. 1. Setzen Sie eine Batterie ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Akku des Geräts ist zu heiß	Die Batterie im Speicher-Controller des Geräts ist überhitzt. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Mögliche Gründe für die Temperaturerhöhung wie Lüfter- oder HLK-Ausfall untersuchen. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Fehler bei der BMC-Kommunikation des Geräts	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren. 1. Vergewissern Sie sich, dass der BMC ordnungsgemäß funktioniert. Wählen Sie **Nodes**, und wählen Sie dann die Registerkarte **Hardware** für den Geräteknoten aus. Suchen Sie das BMC IP-Feld für den Compute Controller, und navigieren Sie zu dieser IP-Adresse. 2. Versuchen Sie, BMC-Kommunikation wiederherzustellen, indem Sie den Knoten in den Wartungsmodus versetzen und dann das Gerät aus- und wieder einschalten. Siehe Installations- und Wartungsanleitung für Ihr Gerät. ◦ "SG6000 Storage-Appliances" ◦ "SG100 SG1000 Services-Appliances" 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Fehler beim Sichern des Appliance-Cache	Ein persistentes Cache-Sicherungsgerät ist fehlgeschlagen. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.
Gerät-Cache-Backup-Gerät unzureichende Kapazität	Die Kapazität des Cache-Sicherungsgeräts ist nicht ausreichend. Wenden Sie sich an den technischen Support.
Appliance Cache Backup-Gerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt. Wenden Sie sich an den technischen Support.
Die Größe des Appliance-Cache-Speichers stimmt nicht überein	Die beiden Controller in der Appliance haben unterschiedliche Cache-Größen. Wenden Sie sich an den technischen Support.
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. 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
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. 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"
Aufmerksamkeit für Compute-Controller ist erforderlich	Im Compute-Controller einer StorageGRID-Appliance wurde ein Hardwarefehler erkannt. 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Ein Problem besteht in der Stromversorgung Des Computercontrollers A des Geräts	Stromversorgung A im Compute-Controller weist ein Problem auf.Diese Warnmeldung weist möglicherweise darauf hin, dass das Netzteil ausgefallen ist oder dass es ein Problem bei der Stromversorgung hat. 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"
Das Netzteil B des Compute-Controllers ist ein Problem	Netzteil B im Compute-Controller weist ein Problem auf.Diese Warnmeldung weist möglicherweise darauf hin, dass das Netzteil ausgefallen ist oder dass es ein Problem bei der Stromversorgung hat. 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Der Service zur Überwachung der Computing-Hardware des Appliances ist ausgesetzt	Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt. 1. Überprüfen Sie den Status des eos-Systemstatusdienstes in der Basis-os. 2. Wenn sich der Dienst im Status „angehalten“ oder „Fehler“ befindet, starten Sie den Dienst neu. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Fibre-Channel-Fehler des Geräts erkannt	Es liegt ein Problem mit der Fibre Channel-Verbindung zwischen den Storage-Controllern und den Computing-Controllern in der Appliance vor. 1. Prüfen Sie die Hardwarekomponenten auf Fehler (**Nodes** > ***Appliance Node*** > **Hardware**). Wenn der Status einer der Komponenten nicht „`Nominal`“ lautet, führen Sie folgende Schritte aus: a. Stellen Sie sicher, dass die Fibre Channel-Kabel zwischen den Controllern vollständig verbunden sind. b. Stellen Sie sicher, dass die Fibre-Channel-Kabel frei von übermäßigen Kurven sind. c. Vergewissern Sie sich, dass die SFP+-Module richtig eingesetzt sind. **Hinweis:** Wenn dieses Problem weiterhin besteht, kann das StorageGRID-System die problematische Verbindung automatisch offline schalten. 1. Bei Bedarf die Komponenten austauschen. Siehe Installations- und Wartungsanleitung für Ihr Gerät.
Fehler des Fibre-Channel-HBA-Ports des Geräts	Ein Fibre Channel-HBA-Port ist ausgefallen oder ist ausgefallen.Kontaktieren Sie den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Appliance Flash Cache Laufwerke sind nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal. 1. Ersetzen Sie die SSD-Cache-Laufwerke. Siehe Installations- und Wartungsanleitung für das Gerät. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Geräteverbindung/Batteriebehälter entfernt	Der Verbindungs-/Batteriebehälter fehlt. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Geräte-LACP-Port fehlt	Ein Port auf einer StorageGRID-Appliance beteiligt sich nicht an der LACP-Verbindung. 1. Überprüfen Sie die Konfiguration für den Switch. Stellen Sie sicher, dass die Schnittstelle in der richtigen Link-Aggregationsgruppe konfiguriert ist. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Das gesamte Netzteil des Geräts ist heruntergestuft	Die Leistung eines StorageGRID-Geräts ist von der empfohlenen Betriebsspannung abweichen. 1. Überprüfen Sie den Status von Netzteil A und B, um festzustellen, welches Netzteil ungewöhnlich funktioniert, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"
Ausfall des Appliance Storage Controller A	Der Speicher-Controller A in einer StorageGRID-Appliance ist ausgefallen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Fehler beim Speicher-Controller B des Geräts	Bei Speicher-Controller B in einer StorageGRID-Appliance ist ein Fehler aufgetreten. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Laufwerksausfall des Appliance-Storage-Controllers	Mindestens ein Laufwerk in einer StorageGRID-Appliance ist ausgefallen oder nicht optimal. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Hardwareproblem des Appliance Storage Controllers	SANtricity meldet, dass für eine Komponente einer StorageGRID Appliance ein Hinweis erforderlich ist. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Ausfall der Stromversorgung des Speicher-Controllers	Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abweichen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Fehler bei Netzteil B des Speicher-Controllers	Stromversorgung B bei einem StorageGRID-Gerät hat von der empfohlenen Betriebsspannung abweichen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Monitordienst der Appliance-Storage-Hardware ist ausgesetzt	Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt. 1. Überprüfen Sie den Status des eos-Systemstatusdienstes in der Basis-os. 2. Wenn sich der Dienst im Status „angehalten“ oder „Fehler“ befindet, starten Sie den Dienst neu. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Appliance Storage-Shelfs ist beeinträchtigt	Der Status einer der Komponenten im Storage Shelf für eine Storage Appliance ist beeinträchtigt. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Gerätetemperatur überschritten	Die nominale oder maximale Temperatur für den Lagercontroller des Geräts wurde überschritten. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Mögliche Gründe für die Temperaturerhöhung wie Lüfter- oder HLK-Ausfall untersuchen. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Temperatursensor des Geräts entfernt	Ein Temperatursensor wurde entfernt. Wenden Sie sich an den technischen Support.
Cassandra Auto-Kompaktor-Fehler	Der Cassandra-Autocompfaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank für Überschreibungen und das Löschen schwerer Workloads. Diese Bedingung bleibt bestehen, aber bei bestimmten Workloads kommt es zu einem unerwartet hohen Metadatenverbrauch. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Auto-Kompaktor-Kennzahlen veraltet	Die Kennzahlen, die den Cassandra Auto-Kompaktor beschreiben, sind veraltet. Der Cassandra Auto-Kompaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank bei Überschreibungen und Löten schwerer Workloads. Während diese Warnung weiterhin angezeigt wird, kommt es bei bestimmten Workloads zu einem unerwartet hohen Metadatenverbrauch. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.
Cassandra Kommunikationsfehler	Die Knoten, auf denen der Cassandra-Service ausgeführt wird, haben Probleme bei der Kommunikation miteinander.Diese Warnung zeigt an, dass etwas die Kommunikation zwischen Knoten beeinträchtigt. Möglicherweise gibt es ein Netzwerkproblem, oder der Cassandra-Service ist auf einem oder mehreren Storage-Nodes nicht verfügbar. 1. Bestimmen Sie, ob ein anderer Alarm einen oder mehrere Speicherknoten betrifft. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Prüfen Sie, ob ein Netzwerkproblem einen oder mehrere Speicherknoten betreffen könnte. 3. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 4. Wählen Sie für jeden Speicherknoten in Ihrem System **SSM** > **Services** aus. Stellen Sie sicher, dass der Status des Cassandra-Service“` läuft.`“ 5. Wenn Cassandra nicht ausgeführt wird, befolgen Sie die Schritte zum Starten oder Neustarten eines Dienstes in den Recovery- und Wartungsanweisungen. 6. Wenn jetzt alle Instanzen des Cassandra-Service ausgeführt werden und die Warnmeldung nicht behoben wurde, wenden Sie sich an den technischen Support. "Verwalten Sie erholen"

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra-Kompensation überlastet	Der Cassandra-Verdichtungsvorgang ist überlastet.Wenn der Verdichtungsvorgang überlastet ist, kann die Lese-Performance beeinträchtigt und der RAM-Speicher möglicherweise aufgebraucht werden. Auch der Cassandra-Service reagiert möglicherweise nicht oder stürzt ab. 1. Starten Sie den Cassandra-Service neu, indem Sie die Schritte zum Neustart eines Service in den Recovery- und Wartungsanweisungen befolgen. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. "Verwalten Sie erholen"
Veraltete Reparaturkennzahlen für Cassandra	Die Kennzahlen, die Cassandra-Reparaturaufträge beschreiben, sind veraltet. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Booten Sie den Node neu. Gehen Sie im Grid Manager zu **Nodes**, wählen Sie den Knoten und wählen Sie die Registerkarte Aufgaben aus. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Cassandra Reparaturfortschritt langsam	Der Fortschritt der Cassandra-Reparaturen ist langsam.bei langsamen Datenbankreparaturen wird die Datenkonsistenz von Cassandra behindert. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Vergewissern Sie sich, dass alle Speicherknoten online sind und keine netzwerkbezogenen Warnmeldungen vorliegen. 2. Überwachen Sie diese Warnung bis zu zwei Tage lang, um zu prüfen, ob das Problem selbst behoben wird. 3. Wenn die Reparatur der Datenbank langsam fortgesetzt wird, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Reparaturservice nicht verfügbar	Der Cassandra-Reparaturservice ist nicht verfügbar.der Cassandra-Reparaturservice ist auf allen Speicherknoten vorhanden und bietet wichtige Reparaturfunktionen für die Cassandra-Datenbank. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 2. Wählen Sie für jeden Speicherknoten in Ihrem System **SSM** > **Services** aus. Stellen Sie sicher, dass der Status des Cassandra Reaper Service „läuft“. 3. Wenn Cassandra Reaper nicht ausgeführt wird, befolgen Sie die Schritte zum Starten oder Neustarten eines Dienstes in den Anweisungen zur Wiederherstellung und Wartung. 4. Wenn jetzt alle Instanzen des Cassandra Reaper Service ausgeführt werden und die Warnmeldung nicht behoben ist, wenden Sie sich an den technischen Support. "Verwalten Sie erholen"
Verbindungsfehler beim Cloud-Storage-Pool	Bei der Zustandsprüfung für Cloud-Storage-Pools wurde ein oder mehrere neue Fehler erkannt. 1. Wechseln Sie auf der Seite „Speicherpools“ zum Abschnitt „Cloud-Speicherpools“. 2. Sehen Sie sich die Spalte Letzter Fehler an, um zu ermitteln, welcher Cloud Storage Pool einen Fehler hat. 3. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management. "Objektmanagement mit ILM"

Alarmname	Beschreibung und empfohlene Aktionen
DHCP-Leasing abgelaufen	Das DHCP-Leasing auf einer Netzwerkschnittstelle ist abgelaufen.Falls das DHCP-Leasing abgelaufen ist, befolgen Sie die empfohlenen Aktionen: 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. "Verwalten Sie erholen"
DHCP-Leasing läuft bald ab	Der DHCP-Lease auf einer Netzwerkschnittstelle läuft bald ab.um zu verhindern, dass der DHCP-Leasing abläuft, befolgen Sie die empfohlenen Maßnahmen: 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. "Verwalten Sie erholen"

Alarmname	Beschreibung und empfohlene Aktionen
DHCP-Server nicht verfügbar	Der DHCP-Server ist nicht verfügbar.der StorageGRID-Node kann den DHCP-Server nicht kontaktieren. Das DHCP-Leasing für die IP-Adresse des Node kann nicht validiert werden. 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. "Verwalten Sie erholen"

Alarmname	Beschreibung und empfohlene Aktionen
Die Festplatten-I/O ist sehr langsam	Sehr langsamer Festplatten-I/O könnte sich auf die StorageGRID-Performance auswirken. 1. Wenn das Problem mit einem Storage Appliance-Node zusammenhängt, überprüfen Sie mithilfe von SANtricity System Manager auf fehlerhafte Laufwerke, Laufwerke mit prognostizierte Fehler oder laufende Festplattenreparaturen. Überprüfen Sie auch den Status der Fibre Channel- oder SAS-Links zwischen den Computing-Ressourcen und den Storage Controllern der Appliance, um zu überprüfen, ob Links ausgefallen sind oder übermäßige Fehlerraten angezeigt werden. 2. Überprüfen Sie das Storage-System, das die Volumes dieses Nodes hostet, um die Ursache des langsamen I/O zu ermitteln und zu korrigieren 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. Betroffene Nodes können Services deaktivieren und sich neu starten, um keine Auswirkungen auf die allgemeine Grid-Performance zu haben. Wenn der zugrunde liegende Zustand beseitigt ist und diese Nodes eine normale I/O-Performance erkennen, wird der gesamte Service automatisch wiederhergestellt.

Alarmname	Beschreibung und empfohlene Aktionen
E-Mail-Benachrichtigung fehlgeschlagen	Die E-Mail-Benachrichtigung für einen Alarm konnte nicht gesendet werden.dieser Alarm wird ausgelöst, wenn eine Benachrichtigung per E-Mail fehlschlägt oder eine Test-E-Mail (gesendet von der Seite **Alerts** > **Email Setup**) nicht zugestellt werden kann. 1. Melden Sie sich über den Admin-Node in der Spalte **Standort/Node** der Warnmeldung bei Grid Manager an. 2. Rufen Sie die Seite **Alerts** > **E-Mail-Setup** auf, überprüfen Sie die Einstellungen und ändern Sie diese, falls erforderlich. 3. Klicken Sie auf **Test-E-Mail senden** und prüfen Sie den Posteingang eines Testempfängers für die E-Mail. Eine neue Instanz dieser Warnmeldung kann ausgelöst werden, wenn die Test-E-Mail nicht gesendet werden kann. 4. Wenn die Test-E-Mail nicht gesendet werden konnte, bestätigen Sie, dass Ihr E-Mail-Server online ist. 5. Wenn der Server funktioniert, wählen Sie **Support** > **Tools** > **Protokolle** aus, und sammeln Sie das Protokoll für den Admin-Knoten. Geben Sie einen Zeitraum an, der 15 Minuten vor und nach der Zeit der Warnmeldung liegt. 6. Extrahieren Sie das heruntergeladene Archiv und überprüfen Sie den Inhalt von `prometheus.log (_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log)`. 7. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.
Ablauf der auf der Seite Client Certificates konfigurierten Zertifikate	Ein oder mehrere Zertifikate, die auf der Seite Clientzertifikate konfiguriert sind, laufen bald ab. 1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Client-Zertifikate**. 2. Wählen Sie ein Zertifikat aus, das bald abläuft. 3. Wählen Sie **Bearbeiten** aus, um ein neues Zertifikat hochzuladen oder zu erstellen. 4. Wiederholen Sie diese Schritte für jedes Zertifikat, das bald abläuft. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
Ablauf des Endpunktzertifikats des Load Balancer	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen kurz vor dem Ablauf. 1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**. 2. Wählen Sie einen Endpunkt mit einem Zertifikat aus, das bald abläuft. 3. Wählen Sie **Endpunkt bearbeiten** aus, um ein neues Zertifikat hochzuladen oder zu erstellen. 4. Wiederholen Sie diese Schritte für jeden Endpunkt mit einem abgelaufenen Zertifikat oder einem Endpunkt, der bald ausläuft. Weitere Informationen zum Verwalten von Endpunkten für den Load Balancer finden Sie in den Anweisungen zum Verwalten von StorageGRID. "StorageGRID verwalten"
Ablauf des Serverzertifikats für die Managementoberfläche	Das für die Managementoberfläche verwendete Serverzertifikat läuft bald ab. 1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**. 2. Laden Sie im Abschnitt Management Interface Server Certificate ein neues Zertifikat hoch. "StorageGRID verwalten"
Ablauf des Serverzertifikats für Storage-API-Endpunkte	Das Serverzertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, läuft bald ab. 1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**. 2. Laden Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte ein neues Zertifikat hoch. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
MTU-Diskrepanz bei dem Grid-Netzwerk	Die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) unterscheidet sich deutlich von den Knoten im Grid.die Unterschiede in den MTU-Einstellungen könnten darauf hindeuten, 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. "Fehlerbehebung bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU"
Hohe Java-Heap-Nutzung	Ein hoher Prozentsatz von Java Heap-Speicherplatz wird verwendet.Wenn der Java-Heap voll wird, können Metadaten-Dienste nicht mehr verfügbar sein und Clientanforderungen können fehlschlagen. 1. Überprüfen Sie die ILM-Aktivitäten auf dem Dashboard. Diese Warnmeldung kann sich selbst beheben, wenn der ILM-Workload abnimmt. 2. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Hohe Latenz bei Metadatenanfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.ein Anstieg der Abfragelatenz kann durch eine Hardwareänderung, wie den Austausch einer Festplatte oder eine Workload-Änderung, wie eine plötzliche Zunahme der Ingests, verursacht werden. 1. Ermitteln, ob sich Hardware- oder Workload-Änderungen während der Erhöhung der Abfragelatenz ergeben. 2. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Synchronisierungsfehler bei der Identitätsföderation	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren. 1. Vergewissern Sie sich, dass der konfigurierte LDAP-Server online und verfügbar ist. 2. Überprüfen Sie die Einstellungen auf der Seite Identity Federation. Vergewissern Sie sich, dass alle Werte aktuell sind. Siehe „`Konfigurieren einer föderierten Identitätsquelle`“ in den Anweisungen zur Verwaltung von StorageGRID. 3. Klicken Sie auf **Verbindung testen**, um die Einstellungen für den LDAP-Server zu validieren. 4. Wenden Sie sich an den technischen Support, wenn das Problem nicht gelöst werden kann. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
ILM-Platzierung nicht erreichbar	Eine Platzierungsanweisung in einer ILM-Regel kann für bestimmte Objekte nicht erreicht werden.Diese Warnung zeigt an, dass ein von einer Platzierungsanweisung erforderlicher Node nicht verfügbar ist oder dass eine ILM-Regel falsch konfiguriert ist. Eine Regel kann beispielsweise mehr replizierte Kopien angeben, als Storage Nodes vorhanden sind. 1. Stellen Sie sicher, dass alle Nodes online sind. 2. Wenn alle Nodes online sind, lesen Sie die Anweisungen zur Platzierung in allen ILM-Regeln, die die aktive ILM-Richtlinie verwenden. Vergewissern Sie sich, dass für alle Objekte gültige Anweisungen vorliegen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management. 3. Aktualisieren Sie bei Bedarf die Regeleinstellungen und aktivieren Sie eine neue Richtlinie. ⓘ Es kann bis zu 1 Tag dauern, bis die Warnung gelöscht wird. 4. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. ⓘ Diese Warnmeldung wird möglicherweise während eines Upgrades angezeigt und kann einen Tag nach Abschluss des Upgrades bestehen. Wenn diese Warnung durch ein Upgrade ausgelöst wird, wird sie von selbst gelöscht. "Objektmanagement mit ILM"

Alarmname	Beschreibung und empfohlene Aktionen
Der ILM-Scan ist zu lang	Die Zeit zum Scannen, Bewerten von Objekten und Anwenden von ILM ist zu lang.Wenn die geschätzte Zeit für die Durchführung eines kompletten ILM-Scans aller Objekte zu lang ist (siehe **Scan Period - Estimated** auf dem Dashboard), wird die aktive ILM-Richtlinie möglicherweise nicht auf neu aufgenommene Objekte angewendet. Änderungen der ILM-Richtlinie werden möglicherweise nicht auf vorhandene Objekte angewendet. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Vergewissern Sie sich, dass alle Speicherknoten online sind. 3. Verringern Sie vorübergehend den Client-Traffic. Wählen Sie beispielsweise im Grid Manager die Option **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung** aus, und erstellen Sie eine Richtlinie, die die Bandbreite oder die Anzahl der Anforderungen begrenzt. 4. Wenn Festplatten-I/O oder -CPU überlastet sind, versuchen Sie, die Last zu reduzieren oder die Ressource zu erhöhen. 5. Aktualisieren Sie ggf. ILM-Regeln für die Verwendung der synchronen Platzierung (Standard für Regeln, die nach StorageGRID 11.3 erstellt wurden). 6. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
ILM-Scan-Rate niedrig	Die ILM-Scan-Rate ist auf weniger als 100 Objekte/Sekunde eingestellt.Diese Warnmeldung gibt an, dass jemand die ILM-Scan-Rate für Ihr System auf weniger als 100 Objekte/Sekunde geändert hat (Standard: 400 Objekte/Sekunde). Die aktive ILM-Richtlinie wird möglicherweise nicht auf neu aufgenommene Objekte angewendet. Nachfolgende Änderungen der ILM-Richtlinie werden nicht auf vorhandene Objekte angewendet. 1. Ermitteln, ob im Rahmen einer laufenden Support-Untersuchung eine temporäre Änderung der ILM-Scanrate vorgenommen wurde. 2. Wenden Sie sich an den technischen Support. Ändern Sie nie die ILM-Scanrate, ohne den technischen Support zu kontaktieren.
ABLAUF DES KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des KMS-Zertifikats (Key Management Server) verwendet wird, läuft bald ab. 1. Aktualisieren Sie mithilfe der KMS-Software das CA-Zertifikat für den Schlüsselverwaltungsserver. 2. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 3. Wählen Sie den KMS aus, der über eine Warnung für den Zertifikatsstatus verfügt. 4. Wählen Sie **Bearbeiten**. 5. Wählen Sie **Weiter** aus, um zu Schritt 2 zu wechseln (Serverzertifikat hochladen). 6. Wählen Sie **Durchsuchen**, um das neue Zertifikat hochzuladen. 7. Wählen Sie **Speichern**. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
ABLAUF DES KMS-Clientzertifikats	Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft bald ab. 1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 2. Wählen Sie den KMS aus, der über eine Warnung für den Zertifikatsstatus verfügt. 3. Wählen Sie **Bearbeiten**. 4. Wählen Sie **Weiter** aus, um zu Schritt 3 zu wechseln (Client-Zertifikate hochladen). 5. Wählen Sie **Durchsuchen**, um das neue Zertifikat hochzuladen. 6. Wählen Sie **Durchsuchen**, um den neuen privaten Schlüssel hochzuladen. 7. Wählen Sie **Speichern**. "StorageGRID verwalten"
KMS-Konfiguration konnte nicht geladen werden	Es ist die Konfiguration für den Verschlüsselungsmanagement-Server vorhanden, konnte aber nicht geladen werden. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
KMS-Verbindungsfehler	Ein Appliance-Node konnte keine Verbindung zum Schlüsselmanagementserver für seinen Standort herstellen. 1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 2. Vergewissern Sie sich, dass die Port- und Hostnamen-Einträge korrekt sind. 3. Vergewissern Sie sich, dass das Serverzertifikat, das Clientzertifikat und der private Schlüssel des Clientzertifikats korrekt und nicht abgelaufen sind. 4. Stellen Sie sicher, dass Firewall-Einstellungen es dem Appliance-Knoten ermöglichen, mit dem angegebenen KMS zu kommunizieren. 5. Beheben Sie alle Netzwerk- oder DNS-Probleme. 6. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt. 1. Vergewissern Sie sich, dass der dem Standort zugewiesene KMS den korrekten Namen für den Verschlüsselungsschlüssel und alle vorherigen Versionen verwendet. 2. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen	Alle Appliance-Volumes wurden entschlüsselt, aber ein oder mehrere Volumes konnten nicht auf den neuesten Schlüssel rotieren.Kontaktieren Sie den technischen Support.
KM ist nicht konfiguriert	Für diesen Standort ist kein Schlüsselverwaltungsserver vorhanden. 1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 2. Fügen Sie für diese Site einen KMS hinzu oder fügen Sie einen Standard-KMS hinzu. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
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. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Stellen Sie sicher, dass auf dem Verschlüsselungsmanagement-Server (KMS) der konfigurierte Verschlüsselungsschlüssel und alle vorherigen Schlüsselversionen vorhanden sind. 3. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
Ablauf DES KMS-Serverzertifikats	Das vom KMS (Key Management Server) verwendete Serverzertifikat läuft in Kürze ab. 1. Aktualisieren Sie mithilfe der KMS-Software das Serverzertifikat für den Schlüsselverwaltungsserver. 2. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
Große Audit-Warteschlange	Die Datenträgerwarteschlange für Überwachungsmeldungen ist voll. 1. Prüfen Sie die Last auf dem System. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen und Sie können die Warnung ignorieren. 2. Wenn die Meldung weiterhin angezeigt wird 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. 3. Verringern Sie die Betriebsrate des Clients oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie das Audit-Level für Client-Schreibvorgänge ändern und der Client auf Fehler oder aus liest (**Konfiguration** > **Überwachung** > **Audit**). "Prüfung von Audit-Protokollen"
Geringe Kapazität der Auditprotokoll-Festplatte	Der für Audit-Protokolle verfügbare Platz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedriger verfügbarer Node-Speicher	Die RAM-Menge, die auf einem Knoten verfügbar ist, ist gering.der niedrige verfügbare RAM kann auf eine Änderung der Arbeitslast oder eine Speicherlecks bei einem oder mehreren Knoten hinweisen. 1. Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. 2. Wenn der verfügbare Speicher unter den Hauptwarnschwellenwert fällt, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Wenig freier Speicherplatz für den Speicherpool	Der Speicherplatz, der zur Speicherung von Objektdaten in einem Speicherpool verfügbar ist, ist gering. 1. Wählen Sie **ILM** > **Storage Pools** aus. 2. Wählen Sie den Speicherpool aus, der in der Warnmeldung aufgeführt ist, und wählen Sie **Details anzeigen**. 3. Ermitteln, wo zusätzliche Storage-Kapazität erforderlich ist Sie können entweder jedem Standort im Speicherpool Storage-Nodes hinzufügen oder einem oder mehreren vorhandenen Storage-Nodes Storage-Volumes (LUNs) hinzufügen. 4. Führen Sie ein Erweiterungsverfahren durch, um die Speicherkapazität zu erhöhen. "Erweitern Sie Ihr Raster"
Wenig installierter Node-Speicher	Der installierte Speicher auf einem Knoten ist gering.Erhöhen Sie die RAM-Menge, die für die virtuelle Maschine oder den Linux-Host verfügbar ist. Überprüfen Sie den Schwellenwert für die Hauptwarnung, um die standardmäßige Mindestanforderung für einen StorageGRID-Node zu bestimmen. Die Installationsanweisungen für Ihre Plattform finden Sie unter: • "Installieren Sie Red hat Enterprise Linux oder CentOS" • "Installieren Sie Ubuntu oder Debian" • "VMware installieren"

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger Metadaten-Storage	Der für die Speicherung von Objektmetadaten verfügbare Platz ist niedrig.**kritischer Alarm** 1. Die Aufnahme von Objekten beenden. 2. Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. **Großalarm** Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. • Kleine Warnung* 1. Überwachen Sie die Rate, mit der Objekt-Metadatenspeicherplatz verwendet wird. Wählen Sie **Nodes** > ***Storage Node*** > **Storage** aus, und zeigen Sie das Diagramm verwendete Speicherdaten - Objektmetadaten an. 2. Fügen Sie Speicherknoten in einem Erweiterungsverfahren So bald wie möglich hinzu. Sobald neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht. "Fehlerbehebung für Storage-Warnmeldungen bei niedrigen Metadaten" "Erweitern Sie Ihr Raster"
Niedrige Kenngrößen für die Festplattenkapazität	Der für die Kennzahlendatenbank verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger Objekt-Storage	Der zur Speicherung von Objektdaten verfügbare Speicherplatz ist gering.Durchführung einer Erweiterung. Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen. "Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“" "Erweitern Sie Ihr Raster"
Niedrige Root-Festplattenkapazität	Der für die Root-Festplatte verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedrige Datenkapazität des Systems	Der verfügbare Speicherplatz für StorageGRID-Systemdaten im /var/local-Dateisystem ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Fehler bei der Node-Netzwerkverbindung	Beim Übertragen der Daten zwischen nodes.Network Verbindungsfehlern sind Fehler aufgetreten, die sich ohne manuelles Eingreifen beheben lassen. Wenden Sie sich an den technischen Support, wenn die Fehler nicht behoben sind. "Fehlerbehebung bei dem NRER-Alarm (Network Receive Error)"

Alarmname	Beschreibung und empfohlene Aktionen
Node-Netzwerkannahme-Frame-Fehler	Bei einem hohen Prozentsatz der von einem Node empfangenen Netzwerkframes sind Fehler aufgetreten.Diese Warnmeldung weist möglicherweise auf ein Hardwareproblem hin, z. B. ein schlechtes Kabel oder ein ausgefallener Transceiver an beiden Enden der Ethernet-Verbindung. 1. Wenn Sie eine Appliance verwenden, versuchen Sie, jeden SFP+ oder SFP28 Transceiver und jedes Kabel nacheinander auszutauschen, um zu prüfen, ob die Warnmeldung gelöscht wird. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Node ist nicht mit dem NTP-Server synchronisiert	Die Zeit des Node ist nicht mit dem NTP-Server (Network Time Protocol) synchronisiert. 1. Vergewissern Sie sich, dass Sie mindestens vier externe NTP-Server angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern. 2. Überprüfen Sie, ob alle NTP-Server normal funktionieren. 3. Überprüfen Sie die Verbindungen zu den NTP-Servern. Stellen Sie sicher, dass sie nicht durch eine Firewall blockiert sind.
Der Node ist nicht mit dem NTP-Server gesperrt	Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt. 1. Vergewissern Sie sich, dass Sie mindestens vier externe NTP-Server angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern. 2. Überprüfen Sie, ob alle NTP-Server normal funktionieren. 3. Überprüfen Sie die Verbindungen zu den NTP-Servern. Stellen Sie sicher, dass sie nicht durch eine Firewall blockiert sind.
Netzwerk außerhalb des Appliance-Node ist ausgefallen	Mindestens ein Netzwerkgerät ist ausgefallen oder nicht verbunden. Diese Warnung zeigt an, dass eine Netzwerkschnittstelle (eth) für einen Knoten, der auf einer virtuellen Maschine oder einem Linux-Host installiert ist, nicht zugänglich ist. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Objekte verloren	Ein oder mehrere Objekte sind aus dem Raster verloren gegangen.Diese Warnung kann darauf hindeuten, dass die Daten dauerhaft verloren gegangen sind und nicht wieder abgerufen werden können. 1. Untersuchen Sie diesen Alarm sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. Sie können auch ein verlorenes Objekt wiederherstellen, wenn Sie eine prompte Aktion ausführen. "Fehlerbehebung verloren gegangene und fehlende Objektdaten" 2. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück: a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. b. Wählen Sie ***site*** > ***Grid Node*** > **LDR** > **Data Store** > **Konfiguration** > **Main** für den Speicherknoten, der die Warnung erhöht hat. c. Wählen Sie **Anzahl der verlorenen Objekte zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
Plattform-Services nicht verfügbar	Zu wenige Speicherknoten mit dem RSM-Dienst laufen oder sind an einem Standort verfügbar.Stellen Sie sicher, dass die meisten Speicherknoten, die den RSM-Dienst am betroffenen Standort haben, ausgeführt werden und in einem nicht fehlerfreien Zustand sind. Siehe „`Fehlerbehebung bei Plattformdiensten`“ in den Anweisungen für die Administration von StorageGRID. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
Services-Appliance-Verbindung am Admin-Netzwerkanschluss 1 getrennt	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie das Kabel und die physische Verbindung zum Admin-Netzwerkanschluss 1. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG100 SG1000 Services-Appliances" ◦ "Deaktivieren einer Meldungsregel"
Services-Appliance-Link im Admin-Netzwerk (oder Client-Netzwerk) herunter	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG100 SG1000 Services-Appliances" ◦ "Deaktivieren einer Meldungsregel"

Alarmname	Beschreibung und empfohlene Aktionen
Services-Appliance-Verbindung an Netzwerkport 1, 2, 3 oder 4 getrennt	Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG100 SG1000 Services-Appliances" ◦ "Deaktivieren einer Meldungsregel"
Die Speicherkonnektivität der Services-Appliance ist herabgesetzt	Einer der beiden SSDs in einer Services-Appliance ist ausgefallen oder die Synchronisierung mit der anderen Appliance-Funktion ist nicht beeinträchtigt. Sie sollten das Problem jedoch sofort beheben. Wenn beide Laufwerke ausfallen, funktioniert die Appliance nicht mehr. 1. Wählen Sie im Grid Manager die Option **Nodes** > ***Services Appliance*, und wählen Sie dann die Registerkarte Hardware** aus. 2. Überprüfen Sie die Meldung im Feld * Storage RAID Mode*. 3. Wenn die Meldung den Status eines Neusynchronisierung anzeigt, warten Sie, bis der Vorgang abgeschlossen ist, und bestätigen Sie dann, dass die Warnmeldung behoben wurde. Eine Neusynchronisierung bedeutet, dass SSD kürzlich ersetzt oder aus einem anderen Grund erneut synchronisiert wird. 4. Wenn die Meldung angibt, dass eine der SSDs ausgefallen ist, ersetzen Sie das ausgefallene Laufwerk so bald wie möglich. Anweisungen zum Austauschen eines Laufwerks in einer Services Appliance finden Sie im Installations- und Wartungshandbuch für SG100- und SG1000-Geräte. "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Verknüpfung der Speicher-Appliance auf Admin-Netzwerk-Port 1 ausgefallen	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie das Kabel und die physische Verbindung zum Admin-Netzwerkanschluss 1. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "Deaktivieren einer Meldungsregel"
Link der Storage Appliance ist im Admin-Netzwerk (oder Client-Netzwerk) inaktiv.	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "Deaktivieren einer Meldungsregel"

Alarmname	Beschreibung und empfohlene Aktionen
Verbindung der Storage Appliance über Netzwerkport 1, 2, 3 oder 4 getrennt	Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "Deaktivieren einer Meldungsregel"
Die Storage-Konnektivität der Storage-Appliance ist herabgesetzt	Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller. 1. Gehen Sie zum Gerät, um die Port-Kontrollleuchten zu überprüfen. 2. Wenn die LEDs eines Ports nicht leuchten, überprüfen Sie, ob das Kabel ordnungsgemäß angeschlossen ist. Ersetzen Sie bei Bedarf das Kabel. 3. Warten Sie bis zu fünf Minuten. Wenn ein zweites Kabel ausgetauscht werden muss, ziehen Sie den Stecker mindestens 5 Minuten lang nicht ab. Andernfalls kann das Root-Volume schreibgeschützt sein und die Hardware neu starten. 4. Wählen Sie im Grid Manager die Option **Nodes** aus. Wählen Sie dann die Registerkarte Hardware des Node aus, auf dem das Problem aufgetreten ist. Vergewissern Sie sich, dass die Alarmbedingung behoben ist.

Alarmname	Beschreibung und empfohlene Aktionen
Speichergerät nicht zugänglich	Auf ein Speichergerät kann nicht zugegriffen werden.Diese Warnung zeigt an, dass ein Volume nicht gemountet oder auf ein Problem mit einem zugrunde liegenden Speichergerät zugegriffen werden kann. 1. Überprüfen Sie den Status aller für den Knoten verwendeten Speichergeräte: ◦ Wenn der Knoten auf einer virtuellen Maschine oder einem Linux-Host installiert ist, befolgen Sie die Anweisungen für Ihr Betriebssystem, um die Hardware-Diagnose auszuführen oder eine Dateisystemprüfung durchzuführen. ▪ "Installieren Sie Red hat Enterprise Linux oder CentOS" ▪ "Installieren Sie Ubuntu oder Debian" ▪ "VMware installieren" ◦ Wenn der Node auf einer SG100-, SG1000- oder SG6000-Appliance installiert ist, verwenden Sie den BMC. ◦ Wenn der Node auf einer SG5600 oder SG5700 Appliance installiert ist, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Hohe Kontingentnutzung für Mandanten	Ein hoher Prozentsatz des Kontingentspeichers wird verwendet. Wenn ein Mieter seine Quote überschreitet, werden Neuanlässe abgelehnt. Diese Warnungsregel ist standardmäßig deaktiviert, da sie eine Vielzahl von Benachrichtigungen erzeugen kann. 1. Wählen Sie im Grid Manager die Option **Miters** aus. 2. Sortieren Sie die Tabelle nach **Quotenausnutzung**. 3. Wählen Sie einen Mandanten aus, dessen Quotenauslastung fast 100 % beträgt. 4. Führen Sie einen oder beide der folgenden Schritte aus: ◦ Wählen Sie **Bearbeiten**, um das Speicherkontingent für den Mieter zu erhöhen. ◦ Benachrichtigen Sie den Mandanten, dass seine Kontingentauslastung hoch ist.

Alarmname	Beschreibung und empfohlene Aktionen
Kommunikation mit Knoten nicht möglich	Ein oder mehrere Dienste reagieren nicht, oder der Node kann nicht erreicht werden.Diese Warnmeldung gibt an, dass ein Node aus einem unbekannten Grund getrennt ist. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren. Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. Wenn das Problem weiterhin besteht: 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Vergewissern Sie sich, dass alle Dienste auf diesem Knoten ausgeführt werden. Wenn ein Dienst angehalten wird, versuchen Sie, ihn zu starten. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. 3. Stellen Sie sicher, dass der Host für den Node eingeschaltet ist. Falls nicht, starten Sie den Host. Wenn mehr als ein Host ausgeschaltet ist, lesen Sie die Recovery- und Wartungsanweisungen. 4. Bestimmen Sie, ob zwischen diesem Knoten und dem Admin-Node ein Problem mit der Netzwerkverbindung besteht. 5. Wenn Sie die Meldung nicht beheben können, wenden Sie sich an den technischen Support. "Verwalten Sie erholen"
Unerwarteter Node-Neustart	Ein Node wurde in den letzten 24 Stunden unerwartet neu gebootet. 1. Überwachen Sie diesen Alarm. Der Alarm wird nach 24 Stunden gelöscht. Wenn der Node jedoch unerwartet neu gebootet wird, wird die Warnmeldung erneut ausgelöst. 2. Wenn Sie die Meldung nicht beheben können, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Nicht identifizierte beschädigte Objekte erkannt	Im replizierten Objekt-Storage wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte. 1. Ermitteln Sie, ob Probleme mit dem zugrunde liegenden Speicher auf einem Speicherknoten auftreten. Führen Sie beispielsweise die Hardwarediagnose aus oder führen Sie eine Dateisystemprüfung durch. 2. Führen Sie nach der Behebung von Storage-Problemen die Vordergrundüberprüfung aus, um festzustellen, ob Objekte fehlen und wenn möglich ersetzt werden. 3. Überwachen Sie diesen Alarm. Die Warnmeldung wird nach 24 Stunden gelöscht, wird jedoch erneut ausgelöst, wenn das Problem noch nicht behoben wurde. 4. Wenn Sie die Meldung nicht beheben können, wenden Sie sich an den technischen Support. "Vordergrundüberprüfung wird ausgeführt"

Verwandte Informationen

"Häufig verwendete Prometheus-Kennzahlen"

Häufig verwendete Prometheus-Kennzahlen

Der Prometheus-Service auf Admin-Knoten sammelt Zeitreihungskennzahlen aus den Diensten auf allen Knoten. Während Prometheus mehr als tausend Kennzahlen erfasst, sind zur Überwachung der wichtigsten StorageGRID Vorgänge eine relativ kleine Zahl erforderlich.

In der folgenden Tabelle sind die am häufigsten verwendeten Prometheus-Kennzahlen aufgeführt und eine Zuordnung jeder Metrik zu dem entsprechenden Attribut (im Alarmsystem verwendet).

Sie können diese Liste nutzen, um die Bedingungen in den Standardwarnregeln besser zu verstehen oder die Bedingungen für benutzerdefinierte Alarmregeln zu erstellen. Für eine vollständige Liste der Metriken wählen Sie **Hilfe** > **API-Dokumentation**.

Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

Die Prometheus Kennzahlen werden 31 Tage lang aufbewahrt.

Prometheus metrisch	Beschreibung
Alertmanager_notifications_failed_total	Die Gesamtzahl der fehlgeschlagenen Warnmeldungen.
Node_Filesystem_verfügbare_Byte	Die Menge an Dateisystemspeicherplatz, die nicht-Root-Benutzern in Bytes zur Verfügung steht.
Node_Memory_MemAvailable_Bytes	Feld Speicherinformationen MemAvailable_Bytes.
Node_Network_Carrier	Transportwert von /sys/class/net/<iface>.
Node_Network_receive_errs_total	Statistik für Netzwerkgeräte receive_errs.
Node_Network_transmit_errs_total	Statistik für Netzwerkgeräte 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 Storage-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 verloren gegangene und fehlende Objektdaten"

Prometheus metrisch	Beschreibung
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.

Prometheus metrisch	Beschreibung
storagegrid_Network_received_Byte	Die Gesamtmenge der seit der Installation empfangenen Daten.
storagegrid_Network_transmited_Byte	Die Gesamtmenge der seit der Installation gesendeten Daten.
storagegrid_ntp_Chooed_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_Servercertifikat_Management_Interface_cert_expiry_days	Die Anzahl der Tage vor Ablauf des Managementschnittstelle-Zertifikats.
storagegrid_Serverzertifikat_Storage_API_endpunkte s_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_Load	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.

Prometheus metrisch	Beschreibung
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_transmited_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_Utifficiendatiy_Metadata_Bytes	Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten auf dem Storage-Node

Prometheus metrisch	Beschreibung
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_Utifficiendatiy_Metadata_Bytes	Die Menge der Objekt-Metadaten auf dem Storage-Volume 0 in Bytes.
storagegrid_Storage_Utisation_Metadata_reservierte_Bytes	Der gesamte Speicherplatz auf Volume 0 jedes Storage-Node, der tatsächlich für Objekt-Metadaten reserviert ist. Für jeden angegebenen Storage-Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Node und der Einstellung des systemweiten reservierten Speicherplatzes ab.
storagegrid_Storage_Utifficienfficienals_total_space_Bytes	Der gesamte Speicherplatz, der allen Objektspeichern zugewiesen ist.
storagegrid_Storage_Utiable_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).

Prometheus metrisch	Beschreibung
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.

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	Stellen Sie die Verbindung zu einem Dienst (einem ADC-Dienst) wieder her, der einen Attributrelais-Dienst so schnell wie möglich ausführt. Wenn keine angeschlossenen Attributrelais vorhanden sind, kann der Grid-Node 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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ACMS	Verfügbare Metadaten	BARC, BLDR, BCMN	Ein Alarm wird ausgelöst, wenn ein LDR- oder ARC-Dienst die Verbindung zu einem DDS-Dienst verliert. In diesem Fall können Transaktionen nicht verarbeitet werden. Wenn die Nichtverfügbarkeit von DDS-Diensten nur ein kurzes vorübergehendes Problem ist, können Transaktionen verzögert werden. Überprüfen und Wiederherstellen der Verbindungen zu einem DDS-Dienst, um diesen Alarm zu löschen und den Service auf die volle Funktionalität zurückzugeben.

Codieren	Name	Service	Empfohlene Maßnahmen
AKTE	Status Des Cloud Tiering Service	LICHTBOGEN	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Cloud Tiering - Simple Storage Service (S3). 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. Wenn ein Hauptalarm aufgrund eines Authentifizierungsfehlers ausgelöst wird, überprüfen Sie ggf. die mit dem Ziel-Bucket verknüpften Anmeldeinformationen und aktualisieren Sie Werte. Wenn aus irgendeinem anderen Grund ein Großalarm ausgelöst wird, wenden Sie sich an den technischen Support.
ADCA	ADC-Status	ADU	Wenn ein Alarm ausgelöst wird, wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***GRID Node*** > **ADC** > **Übersicht** > **Main** und **ADC** > **Alarme** > **Main**, um die Ursache des Alarms zu bestimmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ADCE	ADC-Status	ADU	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. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
AITE	Status Abrufen	BARC	Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). 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. Wenn der Wert des Status „Archivabrueve“ Offline lautet, versuchen Sie, den Status auf Online zu aktualisieren. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abruf** > **Konfiguration** > **Main**, wählen Sie **Archiv Status abrufen** > **Online** und klicken Sie auf **Änderungen anwenden**. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AITU	Status Abrufen	BARC	Wenn der Wert für „Status abrufen“ als Zielfehler gilt, prüfen Sie das ausgewählte externe Archivspeichersystem auf Fehler. 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. Wenn der Wert des Status „Archiv abrufen“ Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.
ALIS	Eingehende Attributsitzungen	ADU	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

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.

Codieren	Name	Service	Empfohlene Maßnahmen
AMQS	Audit-Nachrichten In Queued	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Meldungen nicht sofort an ein Audit-Relais oder ein Repository weitergeleitet werden können, werden die Meldungen in einer Disk-Warteschlange 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: • 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-

Codieren	Name	Service	Empfohlene Maßnahmen
AOTE	Store State	BARC	Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). 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. 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.
AOTU	Speicherstatus	BARC	Wenn der Wert des Speicherstatus „Sitzung verloren“ lautet, prüfen Sie, ob das externe Archivspeichersystem verbunden und online ist. Wenn der Wert von Zielfehler ist, überprüfen Sie das externe Archivspeichersystem auf Fehler. Wenn der Wert des Speicherstatus Unbekannter Fehler lautet, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
APMS	Storage Multipath-Konnektivität	SSM	Wenn der Alarm für den Multipath-Status als „`Dabgestuft`“ angezeigt wird (wählen Sie **Unterstützung** > **Tools** > **Grid-Topologie**, und wählen Sie dann ***site*** > ***Grid-Knoten*** > **SSM** > **Ereignisse**), gehen Sie folgendermaßen vor: 1. Schließen Sie das Kabel an, das keine Kontrollleuchten anzeigt, oder ersetzen Sie es. 2. Warten Sie eine bis fünf Minuten. Ziehen Sie das andere Kabel erst fünf Minuten nach dem Anschließen des ersten Kabels ab. Das zu frühe Auflösen kann dazu führen, dass das Root-Volume schreibgeschützt ist, was erfordert, dass die Hardware neu gestartet wird. 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	BOGENZUSTAND	LICHTBOGEN	Der ARC-Dienst verfügt über einen Standby-Status, bis alle ARC-Komponenten (Replikation, Speicher, Abrufen, Ziel) gestartet wurden. Dann geht es zu Online. Wenn der Wert des ARC-Status nicht von Standby auf Online übergeht, überprüfen Sie den Status der ARC-Komponenten. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
AROQ	Objekte In Queued	LICHTBOGEN	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. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
ARRF	Anfragefehler	LICHTBOGEN	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. 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. 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. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abruf** > **Konfiguration** >
1896			

Codieren	Name	Service	Empfohlene Maßnahmen
ARRV	Verifizierungsfehler	LICHTBOGEN	Wenden Sie sich an den technischen Support, um das Problem zu diagnostizieren und zu beheben. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abrufen** > **Konfiguration** > **Main**, wählen Sie **Fehleranzahl der Überprüfung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
ARVF	Speicherfehler	LICHTBOGEN	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. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** 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**.

Codieren	Name	Service	Empfohlene Maßnahmen
ASXP	Revisionsfreigaben	AMS	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUMA	AMS-Status	AMS	Wenn der Wert für AMS Status DB-Verbindungsfehler ist, starten Sie den Grid-Node neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUME	AMS-Status	AMS	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. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
AUXS	Exportstatus Prüfen	AMS	Wenn ein Alarm ausgelöst wird, beheben Sie das zugrunde liegende Problem und starten Sie dann den AMS-Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
HINZUFÜGEN	Anzahl Ausgefallener Speicher-Controller-Laufwerke	SSM	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.
BASF	Verfügbare Objektkennungen	CMN	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. Wenden Sie sich an den technischen Support, um weitere Kennungen zuzuweisen.

Codieren	Name	Service	Empfohlene Maßnahmen
BASS	Identifier Block Zuordnungsstatus	CMN	Standardmäßig wird ein Alarm ausgelöst, wenn Objektkennungen nicht zugewiesen werden können, da ADC Quorum nicht erreicht werden kann. Die Zuweisung von Identifier-Blöcken im CMN-Dienst erfordert ein Quorum (50 % + 1) der ADC-Dienste, dass sie online und verbunden sind. Wenn Quorum nicht verfügbar ist, kann der CMN-Dienst keine neuen Identifikationsblöcke zuweisen, bis das ADC-Quorum wieder hergestellt wird. 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. 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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
BRDT	Temperatur Im Computing-Controller-Chassis	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur des Compute-Controllers in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Prüfen Sie die Hardware-Komponenten und Umweltprobleme auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
BTSE	Uhrstatus	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CAHP	Java Heap-Nutzung In Prozent	DDS	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-Metadatenspeicher überschreitet. Überprüfen Sie die ILM-Aktivität im Dashboard, oder wählen Sie **Support** > **Tools** > **Grid Topology** und dann ***site*** > ***Grid Node*** > **DDS** > **Ressourcen** > **Übersicht** > **Main**. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CAIH	Anzahl Der Verfügbaren Aufnahmeziele	CLB	Dieser Alarm ist veraltet.
CAQH	Anzahl Der Verfügbaren Ziele	CLB	Dieser Alarm wird gelöscht, wenn die zugrunde liegenden Probleme der verfügbaren LDR-Dienste behoben werden. Stellen Sie sicher, dass die HTTP-Komponente der LDR-Dienste online ist und ordnungsgemäß ausgeführt wird. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CASA	Data Store-Status	DDS	Wenn der Cassandra-Metadatenspeicher nicht mehr verfügbar ist, wird ein Alarm ausgelöst. Den Status von Cassandra überprüfen: 1. Melden Sie sich beim Storage-Node als admin und an `su` Um das Root-Kennwort zu verwenden, das in der Datei Passwords.txt angegeben ist. 2. Geben Sie Ein: `service cassandra status` 3. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: `service cassandra restart` Dieser Alarm kann auch zeigen, dass der Metadatenspeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert. "Fehlerbehebung im Alarm Services: Status - Cassandra (SVST)" Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
FALL	Datenspeicherstatus	DDS	Dieser Alarm wird während der Installation oder Erweiterung ausgelöst, um anzuzeigen, dass ein neuer Datenspeicher in das Raster eingespeist wird.
CES	Eingehende Sitzungen – Eingerichtet	CLB	Dieser Alarm wird ausgelöst, wenn auf dem Gateway Node 20,000 oder mehr HTTP-Sitzungen aktiv (offen) sind. Wenn ein Client zu viele Verbindungen hat, können Verbindungsfehler auftreten. Sie sollten den Workload reduzieren.
CCNA	Computing-Hardware	SSM	Dieser Alarm wird ausgelöst, wenn der Status der Hardware des Computing-Controllers in einer StorageGRID-Appliance zu beachten ist.

Codieren	Name	Service	Empfohlene Maßnahmen
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	DDS	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. Wenn dieser Alarm den Schwellenwert von 90 % erreicht, wird im Dashboard im Grid Manager eine Warnung angezeigt. Sie müssen eine Erweiterung durchführen, um neue Speicherknoten so schnell wie möglich hinzuzufügen. Anweisungen zum erweitern eines StorageGRID-Grids finden Sie in der Anleitung. 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. **Hinweis**: Wenden Sie sich an den technischen Support, wenn Sie keine Speicherknoten hinzufügen können. Sobald neue
1906			

Codieren	Name	Service	Empfohlene Maßnahmen
CLBA	CLB-Status	CLB	Wenn ein Alarm ausgelöst wird, wählen Sie **Support** > **Tools** > **Grid Topologie** und wählen Sie dann ***site*** > ***Grid Node*** > **CLB** > **Übersicht** > **Main** und **CLB** > **Alarme** > **Main**, um die Ursache des Alarms zu ermitteln und das Problem zu beheben. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CLBE	Der Status des CLB	CLB	Wenn der Wert des CLB-Status Standby lautet, setzen Sie die Überwachung der Situation fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Status Offline lautet und keine bekannten Probleme mit der Serverhardware (z. B. nicht angeschlossen) oder eine geplante Ausfallzeit auftreten, starten Sie den Service neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CMNA	CMN-Status	CMN	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. 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). Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CPRC	Verbleibende Kapazität	NMS	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. Wenn ein Alarm ausgelöst wird, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CPSA	Compute Controller Netzteil A	SSM	Wenn ein Problem mit der Stromversorgung A im Rechencontroller eines StorageGRID-Geräts auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.
CPSB	Compute Controller Netzteil B	SSM	Bei einem StorageGRID-Gerät wird ein Alarm ausgelöst, wenn ein Problem mit der Stromversorgung B im Compute-Controller auftritt. Ersetzen Sie die Komponente bei Bedarf.
KFUT	CPU-Temperatur für Compute Controller	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur der CPU im Compute-Controller in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Wenn es sich bei dem Speicherknoten um eine StorageGRID-Appliance handelt, gibt das StorageGRID-System an, dass eine Warnung für den Controller erforderlich ist. Prüfen Sie die Probleme mit den Hardwarekomponenten und der Umgebung auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.

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.

Codieren	Name	Service	Empfohlene Maßnahmen
ECCD	Beschädigte Fragmente Erkannt	LDR	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 höher ist, kann es zu einem Problem mit dem zugrunde liegenden Speicher des Storage-Nodes kommen. 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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ACST	Verifizierungsstatus	LDR	Dieser Alarm zeigt den aktuellen Status des Hintergrundverifizierungsverfahrens für das Löschen codierter Objektdaten auf diesem Speicherknoten an. Bei der Hintergrundüberprüfung wird ein Großalarm ausgelöst.
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	HSTE und HSTU beziehen sich auf das HTTP-Protokoll für den gesamten LDR-Datenverkehr, einschließlich S3, Swift und anderen internen StorageGRID-Datenverkehr. Ein Alarm zeigt an, dass eine der folgenden Situationen aufgetreten ist: • Das HTTP-Protokoll wurde manuell in den Offline-Modus versetzt. • Das Attribut Auto-Start HTTP wurde deaktiviert. • Der LDR-Service wird heruntergefahren. Das Attribut Auto-Start HTTP ist standardmäßig aktiviert. Wenn diese Einstellung geändert wird, kann HTTP nach einem Neustart offline bleiben. Warten Sie gegebenenfalls, bis der LDR-Service neu gestartet wurde. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Storage Node*** > **LDR** > **Konfiguration** aus. Wenn das HTTP-Protokoll offline ist, versetzen Sie es in den Online-Modus. Vergewissern Sie sich, dass das Attribut Auto-Start HTTP aktiviert ist. Wenden Sie sich an den technischen Support, wenn das HTTP-Protokoll offline bleibt.

Codieren	Name	Service	Empfohlene Maßnahmen
HTAS	Automatisches Starten von HTTP	LDR	Gibt an, ob HTTP-Dienste beim Start automatisch gestartet werden sollen. Dies ist eine vom Benutzer angegebene Konfigurationsoption.
IRSU	Status Der Eingehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass die eingehende Replikation deaktiviert wurde. Konfigurationseinstellungen bestätigen: Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** > **Main** aus.

Codieren	Name	Service	Empfohlene Maßnahmen
LATA	Durchschnittliche Latenz	NMS	Überprüfen Sie auf Verbindungsprobleme. 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. Auf mehrere Alarme prüfen. Eine Erhöhung der durchschnittlichen Latenzzeit kann durch eine übermäßige Anzahl von ausgelösten Alarmen angezeigt werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
LDRE	LDR-Status	LDR	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. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
VERLOREN	Verlorene Objekte	DDS, LDR	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. 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. Untersuchen SIE VERLORENE (VERLORENE Objekte) Alarme sofort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. "Fehlerbehebung verloren gegangene und fehlende Objektdaten"

Codieren	Name	Service	Empfohlene Maßnahmen
MCEP	Ablauf Des Managementschnittstelle-Zertifikats	CMN	Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf die Managementoberfläche verwendet wird, kurz vor Ablauf steht. 1. Gehen Sie zu **Konfiguration** > **Serverzertifikate**. 2. Laden Sie im Abschnitt Management Interface Server Certificate ein neues Zertifikat hoch. "StorageGRID verwalten"
MINQ	E-Mail-Benachrichtigungen in Warteschlange	NMS	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. "Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"

Codieren	Name	Service	Empfohlene Maßnahmen
MIN	E-Mail-Benachrichtigungsstatus	BNMS	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. "Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"
MISS	Status der NMS-Schnittstellen-Engine	BNMS	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.
NANG	Einstellung Für Automatische Netzwerkaushandlung	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.

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: • Fehler bei der Vorwärtskorrektur (FEC) stimmen nicht überein • Switch-Port und MTU-NIC stimmen nicht überein • Hohe Link-Fehlerraten • NIC-Klingelpuffer überlaufen "Fehlerbehebung bei dem NRER-Alarm (Network Receive Error)"

Codieren	Name	Service	Empfohlene Maßnahmen
NRLY	Verfügbare Audit-Relais	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Relais nicht an ADC-Dienste angeschlossen sind, können Audit-Ereignisse nicht 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.
NSCE	Bundesland des NMS	NMS	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. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
NSPD	Schnell	SSM	Dies kann durch Probleme mit der Netzwerkverbindung oder der Treiberkompatibilität verursacht werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NTBR	Freie Tablespace	NMS	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. Durch das Anpassen des Alarmschwellenwerts können Sie proaktiv verwalten, wenn zusätzlicher Storage zugewiesen werden muss. Wenn der verfügbare Speicherplatz einen niedrigen Schwellenwert erreicht (siehe Alarmschwelle), wenden Sie sich an den technischen Support, um die Datenbankzuweisung zu ändern.

Codieren	Name	Service	Empfohlene Maßnahmen
NTER	Übertragungsfehler	SSM	Diese Fehler können beseitigt werden, ohne manuell zurückgesetzt zu werden. Wenn sie nicht klar sind, überprüfen Sie die Netzwerk-Hardware. Überprüfen Sie, ob die Adapterhardware und der Treiber korrekt installiert und konfiguriert sind, um mit Ihren Netzwerk-Routern und Switches zu arbeiten. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **SSM** > **Ressourcen** > **Konfiguration** > **Main**, wählen Sie **Zurücksetzen Fehleranzahl für Übertragung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
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.

Codieren	Name	Service	Empfohlene Maßnahmen
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.

Codieren	Name	Service	Empfohlene Maßnahmen
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.
OQRT	Objekte Isoliert	LDR	Nachdem die Objekte automatisch vom StorageGRID-System wiederhergestellt wurden, können die isolierten Objekte aus dem Quarantäneverzeichnis entfernt werden. 1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 2. Wählen Sie **Standort** > **Storage Node** > **LDR** > **Verifizierung** > **Konfiguration** > **Main**. 3. Wählen Sie **Gesperrte Objekte Löschen**. 4. Klicken Sie Auf **Änderungen Übernehmen**. Die isolierten Objekte werden entfernt und die Zählung wird auf Null zurückgesetzt.

Codieren	Name	Service	Empfohlene Maßnahmen
ORSU	Status Der Ausgehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass die 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 Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** aus. Wenn der LDR-Dienst nicht zur Replikation verfügbar ist, wird ein Alarm ausgelöst. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** aus.
OSLF	Shelf-Status	SSM	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.

Codieren	Name	Service	Empfohlene Maßnahmen
PMEM	Speicherauslastung Des Service (In Prozent)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Kann einen Wert von mehr als Y% RAM haben, wobei Y den Prozentsatz des Speichers repräsentiert, der vom Server verwendet wird. Zahlen unter 80 % sind normal. Über 90 % wird als Problem betrachtet. Wenn die Speicherauslastung für einen einzelnen Dienst hoch ist, überwachen Sie die Situation und untersuchen Sie sie. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
PSAS	Stromversorgung A-Status	SSM	Wenn die Stromversorgung A in einem StorageGRID-Gerät von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Ersetzen Sie bei Bedarf das Netzteil A.
PSBS	Netzteil B Status	SSM	Wenn die Stromversorgung B eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Falls erforderlich, ersetzen Sie das Netzteil B.

Codieren	Name	Service	Empfohlene Maßnahmen
RDTE	Status Von Tivoli Storage Manager	BARC	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Status von Tivoli Storage Manager Offline lautet, überprüfen Sie den Status von Tivoli Storage Manager, und beheben Sie alle Probleme. Versetzen Sie die Komponente wieder in den Online-Modus. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Ziel** > **Konfiguration** > **Main**, wählen Sie **Tivoli Storage Manager State** > **Online** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
RDTU	Status Von Tivoli Storage Manager	BARC	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). 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. 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. Wenn der Wert für Tivoli Storage Manager Status Authentifizierungsfehler oder Authentifizierungsfehler ist, kann eine erneute Verbindung hergestellt werden. Das StorageGRID-System kann eine Verbindung zum TSM Middleware-Server herstellen, die Verbindung kann jedoch nicht authentifiziert werden. Überprüfen Sie, ob der TSM Middleware-Server mit dem richtigen Benutzer, Kennwort und Berechtigungen konfiguriert ist, und starten Sie den Service neu.
1928			Wenn der Wert des Tivoli Storage Manager Status

Codieren	Name	Service	Empfohlene Maßnahmen
RIRF	Eingehende Replikationen — Fehlgeschlagen	BLDR, BARC	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. Um die Zählung zurückzusetzen, wählen Sie **Support** > **Tools** > **Grid Topologie** und dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** > **Main**. Wählen Sie **Anzahl der fehlgeschlagene Inbound-Replikation zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
RIRQ	Eingehende Replikationen — In Warteschlange	BLDR, BARC	Alarme 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.
RORQ	Ausgehende Replikationen — In Warteschlange	BLDR, BARC	Die Warteschlange für ausgehende Replizierung enthält Objektdaten, die kopiert werden, um ILM-Regeln und von Clients angeforderte Objekte zu erfüllen. 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.
SAVP	Nutzbarer Speicherplatz (Prozent)	LDR	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.

Codieren	Name	Service	Empfohlene Maßnahmen
SCAS	Status	CMN	Wenn der Wert des Status für die aktive Grid-Aufgabe Fehler ist, suchen Sie die Grid-Task-Meldung. Wählen Sie **Support** > **Tools** > **Grid Topology** 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`“). Nachdem Sie das Problem untersucht und behoben haben, starten Sie die Grid-Aufgabe neu. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **CMN** > **Grid Tasks** > **Konfiguration** > **Main** aus, und wählen Sie **Aktionen** > **Ausführen**. Wenn der Wert des Status für einen abgebrochenen Grid-Task Fehler ist, versuchen Sie, den Grid-Task zu abbrechen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SCEP	Ablaufdatum des Storage API-Service-Endpoints-Zertifikats	CMN	Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, kurz vor Ablauf steht. 1. Gehen Sie zu **Konfiguration** > **Serverzertifikate**. 2. Laden Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte ein neues Zertifikat hoch. "StorageGRID verwalten"
SCHR	Status	CMN	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SCSA	Storage Controller A	SSM	Wenn in einer StorageGRID-Appliance ein Problem mit Storage Controller A auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
SCSB	Storage Controller B	SSM	Wenn ein Problem mit dem Storage Controller B in einer StorageGRID-Appliance auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B
SHLH.	Systemzustand	LDR	Wenn der Wert „Systemzustand“ für einen Objektspeicher „Fehler“ lautet, prüfen und korrigieren Sie Folgendes: • Probleme mit dem zu montiertem Volume • Fehler im Filesystem

Codieren	Name	Service	Empfohlene Maßnahmen
SLSA	CPU-Auslastung durchschnittlich	SSM	Je höher der Wert des Busiers des Systems. 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 Topology**. Wählen Sie dann ***site*** > ***GRID Node*** > **SSM** > **Ressourcen** > **Berichte** > **Diagramme** aus. Wenn die Belastung des Systems nicht hoch ist und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SMST	Überwachungsstatus Protokollieren	SSM	Wenn der Wert des Protokollüberwachungsstatus für einen anhaltenden Zeitraum nicht verbunden ist, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SMTT	Ereignisse Insgesamt	SSM	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 Alarme für Ereignisse insgesamt ausgelöst werden. 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. Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
SNST	Status	CMN	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SOSS	Status Des Storage-Betriebssystems	SSM	Ein Alarm wird ausgelöst, wenn die SANtricity-Software angibt, dass bei einer Komponente in einer StorageGRID-Appliance ein „`muss beachtet werden`“-Problem vorliegt. Wählen Sie **Knoten**. Wählen Sie dann **Appliance Storage Node** > **Hardware**. Blättern Sie nach unten, um den Status der einzelnen Komponenten anzuzeigen. Prüfen Sie in der SANtricity-Software die Komponenten anderer Appliances, um das Problem zu isolieren.

Codieren	Name	Service	Empfohlene Maßnahmen
SSMA	SSM-Status	SSM	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SSME	SSM-Status	SSM	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. 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.

Codieren	Name	Service	Empfohlene Maßnahmen
SSTS	Storage-Status	BLDR	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. 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. 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 in der Ausgabe des Health: Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** > **Übersicht** > **Main** aus. Die Gesundheit des Volumes ist unter Objektspeichern aufgeführt. Wenn der Wert des Speicherstatus Fehler ist, wenden Sie sich an den technischen Support. "Fehlerbehebung beim SSTS-Alarm (Storage Status)"
1938			

Codieren	Name	Service	Empfohlene Maßnahmen
SVST	Status	SSM	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. Wählen Sie **Support** > **Tools** > **Grid Topology** 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: • Der Dienst wurde manuell beendet (`/etc/init.d/<service\> stop`). • 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. Wenn ein Dienst als nicht ausgeführt aufgeführt ist, starten Sie den Dienst neu (`/etc/init.d/<service\> restart`).
			Dieser Alarm kann auch

Codieren	Name	Service	Empfohlene Maßnahmen
TMEM.	Installierter Speicher	SSM	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.
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	Verfügbarer 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.

Codieren	Name	Service	Empfohlene Maßnahmen
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. Ein Wert von Unbekannt oder Offline kann darauf hindeuten, dass das Volume aufgrund eines Problems mit dem zugrunde liegenden Speichergerät nicht gemountet 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	Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** > **Übersicht** > **Main** aus. Überprüfen Sie das Betriebssystem auf Anzeichen von Block- oder Dateisystemfehlern. 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.
XAMS	Nicht Erreichbare Audit-Repositorys	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Überprüfen Sie die Netzwerkverbindung mit dem Server, der den Admin-Node hostet. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)

In der folgenden Tabelle sind die älteren Alarme aufgeführt, die SNMP-Benachrichtigungen generieren. Im Gegensatz zu Warnmeldungen generieren nicht alle Alarme SNMP-Benachrichtigungen. Nur die aufgeführten Alarme erzeugen SNMP-Benachrichtigungen und nur bei dem angegebenen Schweregrad oder höher.

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

Codieren	Name	Schweregrad
ACMS	Verfügbare Metadaten	Kritisch
AITE	Status Abrufen	Gering
AITU	Status Abrufen	Major
AMQS	Audit-Nachrichten In Queued	Hinweis
AOTE	Store State	Gering
AOTU	Speicherstatus	Major
AROQ	Objekte In Queued	Gering
ARRF	Anfragefehler	Major
ARRV	Verifizierungsfehler	Major
ARVF	Speicherfehler	Major
ASXP	Revisionsfreigaben	Gering
AUMA	AMS-Status	Gering
AUXS	Exportstatus Prüfen	Gering
BTOF	Offset	Hinweis
CAHP	Java Heap-Nutzung In Prozent	Major
CAQH	Anzahl Der Verfügbaren Ziele	Hinweis
CASA	Data Store-Status	Major
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	Major
CLBE	Der Status des CLB	Kritisch
DNST	DNS-Status	Kritisch
ACST	Verifizierungsstatus	Major

Codieren	Name	Schweregrad
HSTE	HTTP-Status	Major
HTAS	Automatisches Starten von HTTP	Hinweis
VERLOREN	Verlorene Objekte	Major
MINQ	E-Mail-Benachrichtigungen in Warteschlange	Hinweis
MIN	E-Mail-Benachrichtigungsstatus	Gering
NANG	Einstellung Für Automatische Netzwerkaushandlung	Hinweis
NDUP	Einstellungen Für Den Netzwerkduplex	Gering
NLNK	Network Link Detect	Gering
RER	Fehler Beim Empfang	Hinweis
NSPD	Schnell	Hinweis
NTER	Übertragungsfehler	Hinweis
NTFQ	NTP-Frequenzverschiebung	Gering
NTLK	NTP Lock	Gering
NTOF	NTP-Zeitverschiebung	Gering
NTSJ	Gewählte Zeitquelle Jitter	Gering
NTSU	NTP-Status	Major
OPST	Gesamtstromstatus	Major
ORSU	Status Der Ausgehenden Replikation	Hinweis
PSAS	Stromversorgung A-Status	Major
PSBS	Netzteil B Status	Major

Codieren	Name	Schweregrad
RDTE	Status Von Tivoli Storage Manager	Hinweis
RDTU	Status Von Tivoli Storage Manager	Major
SAVP	Nutzbarer Speicherplatz (Prozent)	Hinweis
SHLH.	Systemzustand	Hinweis
SLSA	CPU-Auslastung durchschnittlich	Hinweis
SMTT	Ereignisse Insgesamt	Hinweis
SNST	Status	
SOSS	Status Des Storage-Betriebssystems	Hinweis
SSTS	Storage-Status	Hinweis
SVST	Status	Hinweis
TMEM.	Installierter Speicher	Gering
UMEM	Verfügbarer Speicher	Gering
VMST	Status	Gering
VPRI	Überprüfungspriorität	Hinweis
VSTU	Status Der Objektüberprüfung	Hinweis

Referenz für Protokolldateien

In den folgenden Abschnitten werden die Protokolle zum Erfassen von Ereignissen, Diagnosemeldungen und Fehlerbedingungen aufgeführt. Möglicherweise werden Sie gebeten, Protokolldateien zu sammeln und an den technischen Support zu leiten, um bei der Fehlerbehebung zu helfen.

- "StorageGRID-Softwareprotokolle"
- "Protokoll für Implementierung und Wartung"
- "Protokolle für Drittanbietersoftware"
- "Etwa bycast.log"

Die Tabellen in diesem Abschnitt 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 außerhalb des Geltungsbereichs dieses Handbuchs.

Um auf diese Protokolle zuzugreifen, können Sie Log-Dateien und Systemdaten (**Support** > **Tools** > **Logs**) sammeln. Wenn der primäre Admin-Node nicht verfügbar ist oder keinen bestimmten Node erreichen kann, können Sie wie folgt auf die Protokolle für jeden Grid-Node 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:

Verwandte Informationen

"Protokolldateien und Systemdaten werden erfasst"

StorageGRID-Softwareprotokolle

Sie können StorageGRID-Protokolle verwenden, um Probleme zu beheben.

Allgemeine StorageGRID-Protokolle

Dateiname	Hinweise	Gefunden am
`/var/local/log/bycast.log`	Die Datei `bycast.log` Ist die primäre StorageGRID-Fehlerbehebungsdatei. Die Datei `bycast-err.log` Enthält eine Untergruppe von `bycast.log` (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes
`/var/local/log/bycast-err.log`	Die Datei `bycast.log` Ist die primäre StorageGRID-Fehlerbehebungsdatei. Die Datei `bycast-err.log` Enthält eine Untergruppe von `bycast.log` (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes

Dateiname	Hinweise	Gefunden am
`/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 `` `/var/local/core/kexec_cmd `` Ist normalerweise auf Appliance-Knoten vorhanden und weist keinen Fehler auf.	Alle 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

Protokolle für StorageGRID-Services

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

Dateiname	Hinweise	Gefunden am
`/var/local/log/cassandra/system.log`	Informationen für den Metadatenspeicher (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
`/var/local/log/clb.errlog`	Fehlerinformationen für den CLB-Dienst. **Hinweis:** der CLB-Service ist veraltet.	Gateway-Nodes
`/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

Dateiname	Hinweise	Gefunden am
`/var/local/log/dynip*`	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`		Speicherknoten, 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`		Speicherknoten, auf denen der ADC-Service ausgeführt wird
`/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 Umgebungskonfigurationen auf dem Node bereitstellt, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Nodes

Dateiname	Hinweise	Gefunden am
`/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 Protokolle für die eingeschränkten Admin-Ports an Admin-Nodes und für den Load Balancer Service, der den Lastenausgleich von 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

Dateiname	Hinweise	Gefunden am
`/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-sysl.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
`/var/local/log/update-utcn.log`	Enthält Protokolle, die sich auf diesem Knoten im Netzwerk des nicht vertrauenswürdigen Clients beziehen.	Alle Nodes

NMS-Protokolle

Dateiname	Hinweise	Gefunden am
`/var/local/log/nms.log`	• 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`	Enthält Fehlermeldungen bezüglich der MySQL-Datenbank-Upgrades. 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.	Admin-Nodes
`/var/local/log/nms.requestlog`	Enthält Informationen über ausgehende Verbindungen von der Management-API zu internen StorageGRID-Diensten.	Admin-Nodes

Verwandte Informationen

"Etwa bycast.log"

"S3 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 Erweiterungereignisse.	Storage-Nodes
`/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

Apache2-Protokolle	`/var/local/log/apache2/access.log`
	`/var/local/log/apache2/error.log`
	
	`/var/local/log/apache2/other_vhosts_access.log`
		Protokolldateien für apache2.	Admin-Nodes

Archivierung	`/var/local/log/dsierror.log`	Fehlerinformationen für TSM Client APIs.	Archiv-Nodes

Kategorie	Dateiname	Hinweise	Gefunden am
MySQL	/Var/local/log/mysql.err`  `/var/local/log/mysql.err` `/var/local/log/mysql-slow.log`	Protokolldateien von MySQL erstellt. Die Datei mysql.err erfasst Datenbankfehler und Ereignisse wie Start-ups und Herunterfahren. Die Datei 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 Topology** Aus. Wählen Sie dann **Topologie** > ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes

NTP	`/var/local/log/ntp.log`
	
	`/var/lib/ntp/var/log/ntpstats/`
		Der `/var/local/log/ntp.log` Enthält die Protokolldatei für NTP-Fehlermeldungen.
		
		Der `/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

Kategorie	Dateiname	Hinweise	Gefunden am
Samba	`/var/local/log/samba/`	Das Samba-Protokollverzeichnis enthält eine Protokolldatei für jeden Samba-Prozess (smb, nmb und winbind) und jeden Client-Hostnamen/jede IP.	Admin-Node für den Export der Revisionsfreigabe über CIFS konfiguriert

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“.

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.

Verwandte Informationen

"Protokolldateien und Systemdaten werden erfasst"

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.

Dies ist ein Beispiel für eine ADE-Nachricht:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE-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
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 Topology** 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
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

Fehlernummer	Fehlercode	Bedeutung
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
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

Fehlernummer	Fehlercode	Bedeutung
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	ENAMETOOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperren verfügbar
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

Fehlernummer	Fehlercode	Bedeutung
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
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

Fehlernummer	Fehlercode	Bedeutung
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	Der Zugriff auf eine erforderliche gemeinsam genutzte Bibliothek ist nicht möglich
080	ELIBBAD	Zugriff auf eine beschädigte, gemeinsam genutzte Bibliothek
081	ELIBSCN	
082	ELIBMAX	Es wird versucht, zu viele gemeinsam genutzte Bibliotheken zu verbinden
083	ELIBEXEC	Kann eine gemeinsam genutzte Bibliothek nicht direkt ausführen
084	EILSEQ	Ungültige Byte-Sequenz
085	ERESTART	Unterbrochener Systemanruf sollte neu gestartet werden

Fehlernummer	Fehlercode	Bedeutung
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
101	ENETUNREACH	Netzwerk nicht erreichbar
102	ENETRESET	Die Verbindung wurde aufgrund von Reset unterbrochen
103	ECONNABORTED	Software verursacht Verbindungsabbruch
104	ECONNNRESET	Verbindungsrücksetzung durch Peer

Fehlernummer	Fehlercode	Bedeutung
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: Keine Spleißung möglich
110	ETIMEDOUT	Zeitüberschreitung bei Verbindung
111	ECONNNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHEOSTUNREACH	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
122	EDQUOT	Kontingent überschritten

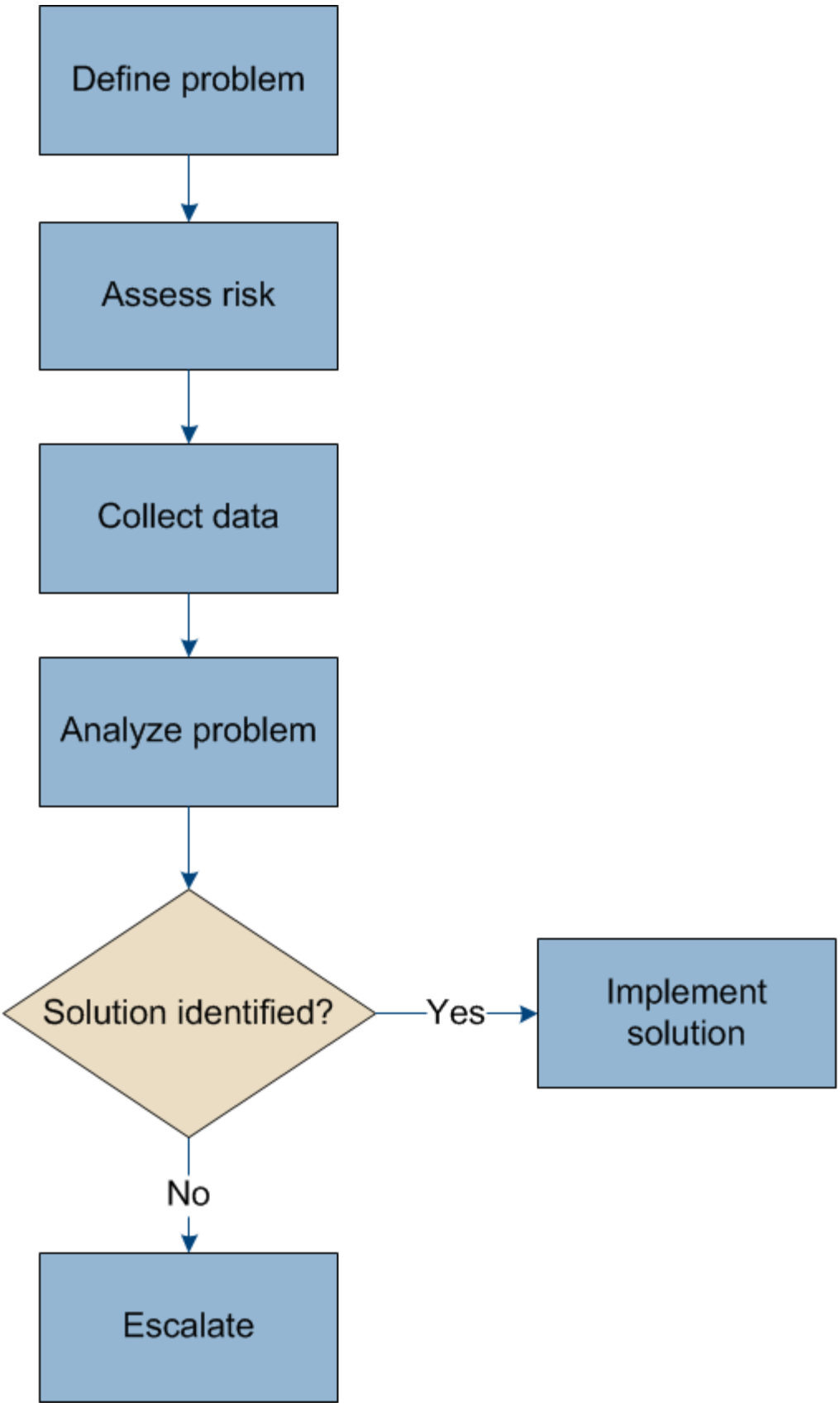
Fehlernummer	Fehlercode	Bedeutung
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ECANCELED	Vorgang Abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEYEXPIRED	Schlüssel abgelaufen
128	EKEYREVOKED	Schlüssel wurde widerrufen
129	EKEYREJECTED	Schlüssel wurde vom Dienst abgelehnt
130	EOWNERDEAD	Für robuste Mutexe: Besitzer starb
131	ENOTRECOVERABLE	Bei robusten Mutation: Status nicht wiederherstellbar

Fehler in einem StorageGRID System beheben

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 der Administration eines StorageGRID-Systems ein Problem auftritt, können Sie das Problem mithilfe des in dieser Abbildung beschriebenen Prozesses identifizieren und analysieren. In vielen Fällen können Sie Probleme selbstständig lösen. In diesem Fall müssen Sie jedoch einige Probleme an den technischen Support eskalieren.



Definition des Problems

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 melden, 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.

Bewertung von Risiken und 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 können nicht.
Sind Daten gefährdet?	Nein
Ist die Fähigkeit, Geschäfte zu führen, stark beeinträchtigt?	Ja, da Client-Applikationen keine Objekte auf dem StorageGRID System speichern und Daten nicht konsistent abgerufen werden können.

Erfassen von Daten

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 diese Daten sammeln	Anweisungen
Zeitplan der neuesten Änderungen erstellen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Erstellen einer Chronik der neuesten Änderungen
Prüfen von Warnungen und Alarmen	Mithilfe von Warnfunktionen und Alarmen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme geben. Überprüfen Sie die Liste der aktuellen Warnungen und Alarme, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat. Prüfen Sie die in der Vergangenheit ausgelösten Warnmeldungen und Alarme, um zusätzliche Einblicke zu erhalten.	• "Anzeigen aktueller Meldungen" • "Anzeigen von Legacy-Alarmen" • "Anzeigen gelöster Warnmeldungen" • "Überprüfung historischer Alarme und Alarmfrequenz (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.	• "Anzeigen der Registerkarte Ereignisse" • "Monitoring von Ereignissen"
Trends anhand von Diagramm- und Textberichten identifizieren	Trends liefern wertvolle Hinweise darauf, wann Probleme zuerst auftraten, und können Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	• "Verwenden von Diagrammen und Berichten"
Basispläne erstellen	Sammeln von Informationen über die normalen Stufen verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Grundlinien können wertvolle Hinweise liefern.	• Basisvorgänge werden erstellt
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.	• "Monitoring PUT und GET Performance"

Art der zu erfassenden Daten	Warum diese Daten 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.	• "Überprüfen von Audit-Meldungen"
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.	"Monitoring von Objektverifizierungsvorgängen".
Datenerfassung für technischen Support	Vom technischen Support werden Sie möglicherweise aufgefordert, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um Probleme zu beheben.	• "Protokolldateien und Systemdaten werden erfasst" • "Manuelles Auslösen einer AutoSupport-Meldung" • "Überprüfen von Support-Metriken"

Erstellen einer Chronik 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: • 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: • 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?

Basisvorgänge werden erstellt

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	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm Speicher verwendet - Objektdaten einen Zeitraum, in dem die Linie ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Storage täglich belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenkverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm „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 jeden Tag belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Geschwindigkeit von S3/Swift Operationen	Vorgänge/Sekunde	Wechseln Sie im Grid Manager zum Fenster Dashboard. Sehen Sie sich im Abschnitt Protokollvorgänge die Werte für die S3-Rate und die Swift-Rate an. Um Einspeis- und Abrufraten und Zählungen für einen bestimmten Standort oder Knoten anzuzeigen, wählen Sie **Knoten** > ***Standort oder Storage Node*** > **Objekte**. Halten Sie den Mauszeiger über das Diagramm Aufnahme und Abruf für S3 oder Swift.
S3/Swift-Vorgänge sind fehlgeschlagen	Betrieb	Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Zeigen Sie auf der Registerkarte Übersicht im Abschnitt API-Vorgänge den Wert für S3-Operationen an – Fehlgeschlagen oder Swift-Vorgänge – Fehlgeschlagen.

Eigenschaft	Wert	Wie zu erhalten
ILM-Auswertungsrate	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 Mauszeiger über das Diagramm, um einen Basiswert für **Evaluierungsrate** 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 Basiswert für **Scanrate** für Ihr System zu schätzen.
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 Mauszeiger über das Diagramm, um einen Basiswert für **Objekte in der Warteschlange (aus Client-Operationen)** für Ihr System zu schätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte** Aus. Zeigen Sie in der Tabelle Abfragen den Wert für durchschnittliche Latenz an.

Datenanalyse

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 selbst 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 Problembehebung nutzen.

✔	Element	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann hat das Problem begonnen? Passiert es konsequent oder intermittierend? Welche Zeiten hat es gelegentlich gegeben? "Definition des Problems"
	Folgenabschätzung	Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation? • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	Wählen Sie **Wartung** > **System** > **Lizenz**. Die StorageGRID System-ID wird im Rahmen der aktuellen Lizenz angezeigt.
	Softwareversion	Klicken Sie auf **Hilfe** > **Info**, um die StorageGRID-Version anzuzeigen.
	Anpassbarkeit	Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf: • Verwendet das Grid Storage-Komprimierung, Storage-Verschlüsselung oder Compliance? • Erstellt ILM replizierte oder Erasure Coding Objekte? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das strenge, ausgewogene oder duale Ingest-Verhalten?
	Log-Dateien und Systemdaten	Erfassen von Protokolldateien und Systemdaten für Ihr System Wählen Sie **Support** > **Extras** > **Protokolle**. Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln. 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.) "Protokolldateien und Systemdaten werden erfasst"
	Basisinformationen	Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch "Basisvorgänge werden erstellt"

✔	Element	Hinweise
	Zeitachse der letzten Änderungen	Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind. "Erstellen einer Chronik 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.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei Objekt- und Storage-Problemen

Sie können verschiedene Aufgaben ausführen, um die Ursachen von Objekt- und Storage-Problemen zu ermitteln.

Bestätigen der Speicherorte von Objektdaten

Je nach Problem sollten Sie überprüfen, wo Objektdaten gespeichert werden. Beispielsweise möchten Sie überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und Objektdaten dort gespeichert werden, wo sie geplant sind.

Was Sie benötigen

- 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**: Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
  - **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. Wählen Sie **ILM** > **Objekt Metadaten Lookup** aus.
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. Klicken Sie Auf **Look Up**.

   Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

   - Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
   - Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
   - Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
   - Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
   - Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
   - Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
   - Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
   - Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

     Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Verwandte Informationen

"Objektmanagement mit ILM"

"S3 verwenden"

"Verwenden Sie Swift"

Fehler beim Objektspeicher (Storage Volume)

Der zugrunde liegende Storage auf einem Storage-Node ist in Objektspeicher unterteilt. Diese Objektspeicher sind physische Partitionen, die als Bereitstellungspunkte für den Storage des StorageGRID Systems fungieren. 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
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s

Volumes

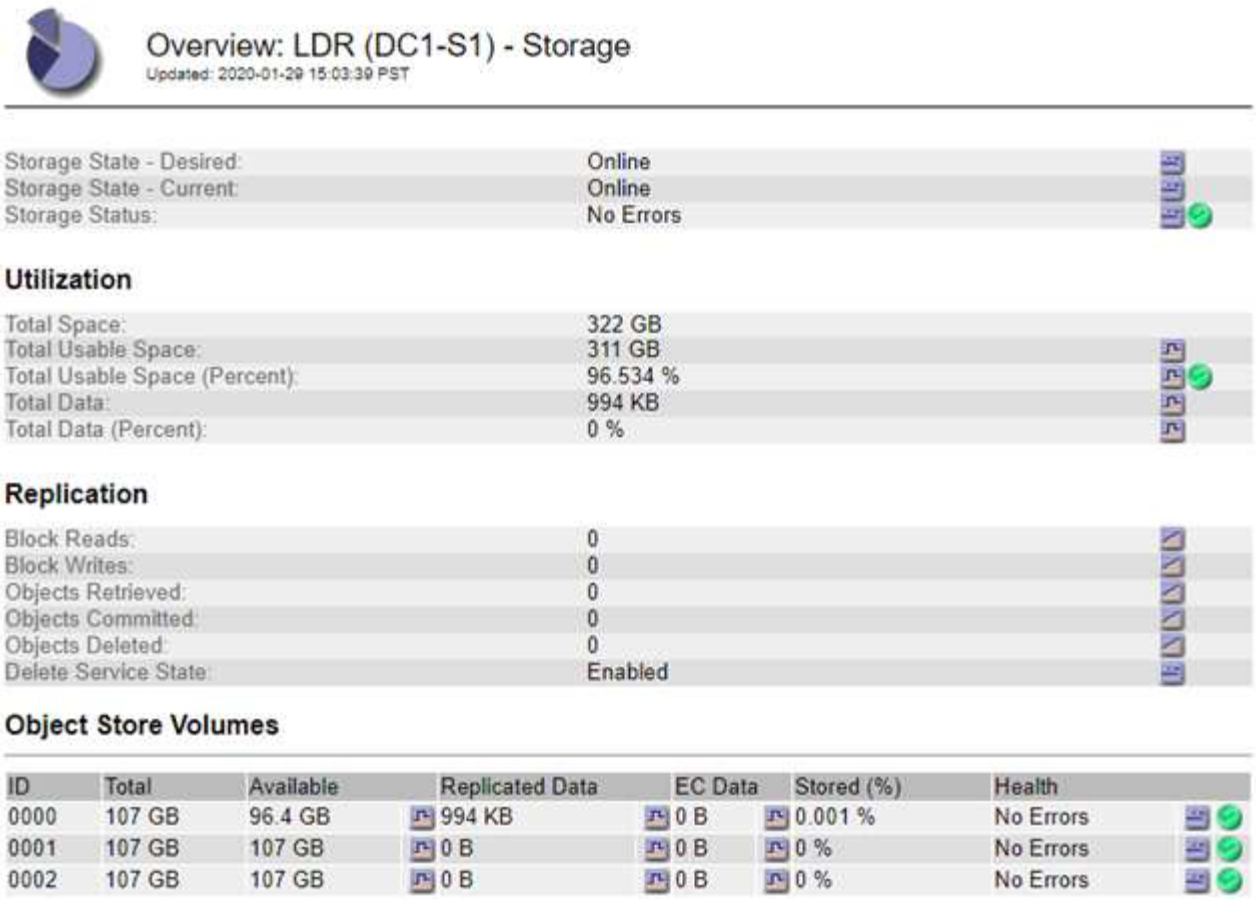
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB	Enabled

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 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

Führen Sie die folgenden Schritte aus, um weitere Details zu jedem Storage-Node anzuzeigen:

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Übersicht** > **Haupt**.



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. Wenn nötig, können Sie auf die Registerkarte **Konfiguration** gehen und den Speicherknoten in einen Read -only Zustand setzen, so dass das StorageGRID System ihn für den Datenabruf verwenden kann, während Sie sich auf eine vollständige Wiederherstellung des Servers vorbereiten.

Verwandte Informationen

"Verwalten Sie erholen"

Überprüfen der Objektintegrität

Das StorageGRID System überprüft die Integrität der Objektdaten auf Storage-Nodes und überprüft sowohl beschädigte als auch fehlende Objekte.

Es gibt zwei Verifizierungsverfahren: Hintergrund- und Vordergrundüberprüfung. Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung wird automatisch ausgeführt und überprüft kontinuierlich die Korrektheit von Objektdaten. Die Vordergrundüberprüfung kann von einem Benutzer ausgelöst werden, um die Existenz (obwohl nicht die Korrektheit) 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 isolierte 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 wiederhergestellt werden kann, wird das Attribut „Corrupt Copies detected (ECOR)“ um eins erhöht und es 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. 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 korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann (weil die Beschädigung verhindert, dass das Objekt identifiziert wird), wird die Warnung **Unerkannter beschädigter Gegenstand erkannt** ausgelöst.

Wenn die Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, da es keine andere Kopie finden kann, werden die Meldung **Objekte verloren** und der ältere Alarm VERLOREN GEGANGENE (verlorene Objekte) ausgelöst.

Ändern der Hintergrundverifizierungsrate

Sie können die Rate ändern, mit der die Hintergrundüberprüfung replizierte Objektdaten auf einem Storage-Node überprüft, wenn Sie Bedenken hinsichtlich der Datenintegrität haben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Sie können die Verifizierungsrate für die Hintergrundüberprüfung eines Speicherknoten ändern:

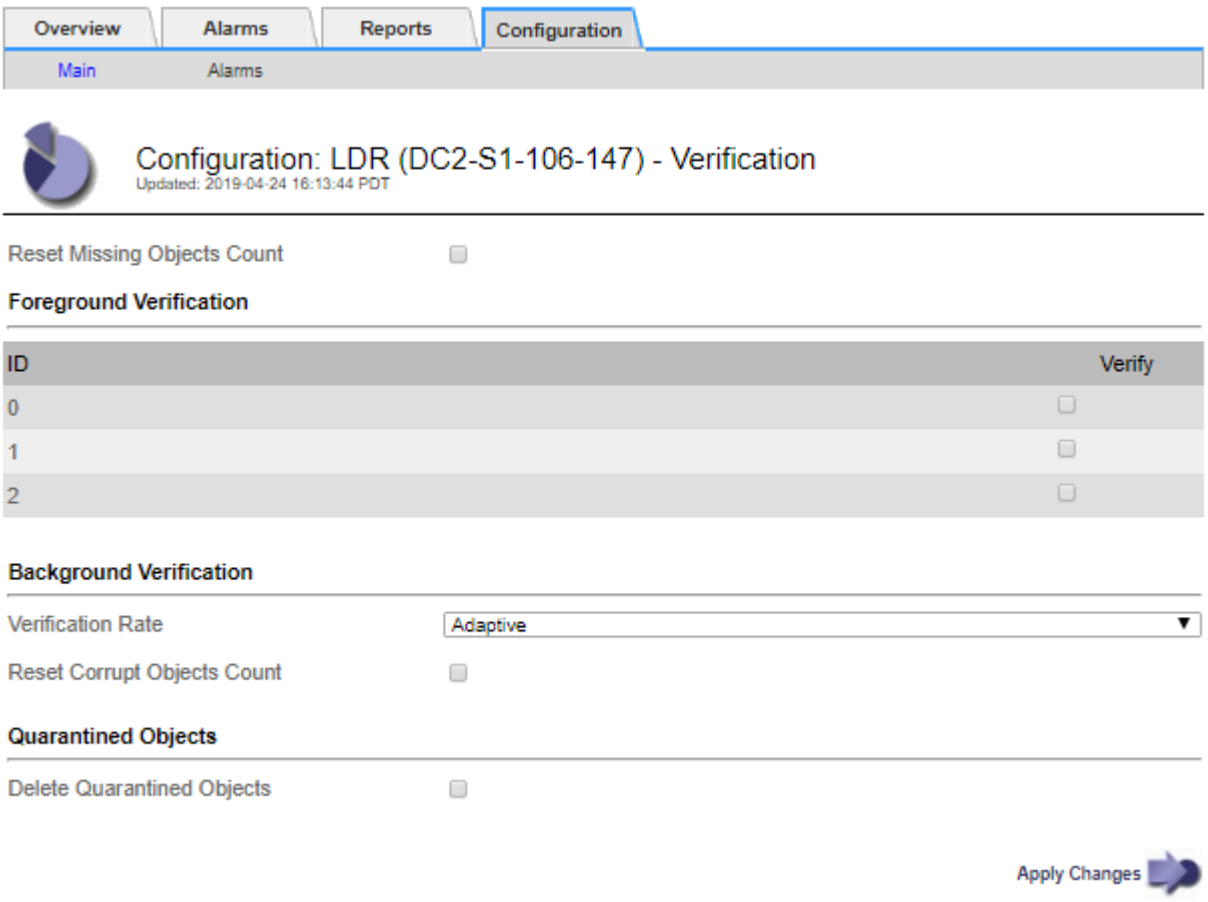
- Adaptiv: Standardeinstellung. Die Aufgabe wurde entwickelt, um maximal 4 MB/s oder 10 Objekte/s zu überprüfen (je nachdem, welcher Wert zuerst überschritten wird).
- Hoch: Die Storage-Verifizierung verläuft schnell und kann zu einer Geschwindigkeit führen, die normale

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 Topology** 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.



Wenn Sie die Verifizierungsrate auf hoch setzen, wird der alte Alarm VPRI (Verification Rate) auf der Melderebene ausgelöst.

1. Klicken Sie Auf **Änderungen Übernehmen**.
2. Überwachen der Ergebnisse der Hintergrundüberprüfung replizierter Objekte
   a. Gehen 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 die Objektkennung nicht extrahiert werden kann (weil sie beschädigt wurde), wird die Metrik **korrupte Objekte nicht identifiziert** erhöht und die Warnung **nicht identifiziertes korruptes Objekt erkannt** ausgelöst.

c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Ursache der Beschädigung zu ermitteln.

3. 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 Topology** 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).

4. Nachdem das StorageGRID System beschädigte Objekte automatisch wiederhergestellt hat, setzen Sie die Anzahl beschädigter Objekte zurück.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***Storage Node* > LDR > Verifizierung > Konfiguration** aus.
   c. Wählen Sie **Anzahl Der Beschädigten Objekte Zurücksetzen**.
   d. Klicken Sie Auf **Änderungen Übernehmen**.
5. 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.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Storage Node*** > **LDR** > **Verifizierung** > **Konfiguration**.
3. Wählen Sie **Gesperrte Objekte Löschen**.
4. Klicken Sie Auf **Änderungen Übernehmen**.

Was ist die Vordergrundüberprüfung

Vordergrundüberprüfung ist ein vom Benutzer initiierter Prozess, der überprüft, ob alle erwarteten Objektdaten auf einem Storage-Node vorhanden sind. Vordergrundüberprüfung wird verwendet, um die Integrität eines Speichergeräts zu überprüfen.

Die Vordergrundüberprüfung ist eine schnellere Alternative zur Hintergrundüberprüfung, die die Existenz von

Objektdaten auf einem Storage-Node, jedoch nicht die Integrität überprüft. Wenn bei der Überprüfung im Vordergrund festgestellt wird, dass viele Elemente fehlen, kann es zu Problemen mit dem gesamten oder einem Teil eines Speichergeräts, das mit dem Speicherknoten verknüpft ist, kommen.

Bei der Vordergrundüberprüfung werden sowohl replizierte Objektdaten als auch mit Erasure-Coding-Objektdaten überprüft:

- **Replizierte Objekte**: Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, die Kopie von an anderer Stelle im System gespeicherten Kopien zu ersetzen. Der Storage Node führt eine vorhandene Kopie durch eine ILM-Bewertung aus. Damit wird ermittelt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da die fehlende Kopie nicht mehr am erwarteten Standort vorhanden ist. Eine neue Kopie wird erstellt und platziert, um die aktive ILM-Richtlinie des Systems zu erfüllen. Diese neue Kopie kann nicht an demselben Speicherort abgelegt werden, an dem die fehlende Kopie gespeichert wurde.
- **Erasure-codierte Objekte**: Wenn ein Fragment eines Löschungskodierten Objekts gefunden wird, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Fragmente neu zu erstellen. Wenn das fehlende Fragment nicht wieder aufgebaut werden kann (weil zu viele Fragmente verloren sind), wird das Attribut Corrupt Copies detected (ECOR) um eins erhöht. ILM versucht anschließend, eine andere Kopie des Objekts zu finden, mit der das Unternehmen eine neue Kopie mit Verfahren zur Fehlerkorrektur erstellen kann.

  Wenn bei der Vordergrundüberprüfung ein Problem mit dem Erasure Coding für ein Storage-Volume erkannt wird, wird bei der Vordergrundverifizierung eine Fehlermeldung angehalten, die das betroffene Volume identifiziert. Sie müssen ein Recovery-Verfahren für alle betroffenen Storage Volumes durchführen.

Wenn im Raster keine weiteren Kopien eines fehlenden replizierten Objekts oder eines beschädigten Erasure-codierten Objekts gefunden werden, werden die Meldung **Objekte verloren** und der Legacy-Alarm FÜR VERLORENE (verlorene Objekte) ausgelöst.

Vordergrundüberprüfung wird ausgeführt

Mit der Vordergrundüberprüfung können Sie die Existenz von Daten auf einem Speicherknoten überprüfen. Fehlende Objektdaten können darauf hindeuten, dass beim zugrunde liegenden Speichergerät ein Problem vorliegt.

Was Sie benötigen

- Sie haben sichergestellt, dass die folgenden Grid-Aufgaben nicht ausgeführt werden:
  - Grid Expansion: Add Server (GEXP), wenn ein Storage Node hinzugefügt wird
  - Storage Node Deaktivierungsfunktion (LDCM) auf demselben Storage-Node Wenn diese Grid-Aufgaben ausgeführt werden, warten Sie, bis sie abgeschlossen sind oder lassen Sie die Sperre frei.
- Sie haben sichergestellt, dass die Speicherung online ist. (Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***Storage Node*** > **LDR** > **Storage** > **Übersicht** > **Haupt** aus. Vergewissern Sie sich, dass **Speicherstatus - Aktuell** online ist.)
- Sie haben sichergestellt, dass die folgenden Wiederherstellungsverfahren nicht auf demselben Speicherknoten ausgeführt werden:
  - Recovery eines ausgefallenen Storage-Volumes
  - Die Recovery eines Storage-Knotens mit einer fehlgeschlagenen Systemlaufwerk-Vordergrundüberprüfung bietet keine nützlichen Informationen, während Recovery-Verfahren ausgeführt werden.

Über diese Aufgabe

Vordergrundüberprüfung werden sowohl fehlende replizierte Objektdaten als auch fehlende, mit Erasure Coding versehenen Objektdaten überprüft:

- Wenn bei der Überprüfung im Vordergrund große Mengen fehlender Objektdaten festgestellt werden, liegt es wahrscheinlich vor, dass der Storage-Node analysiert und behoben werden muss.
- Wenn bei der Überprüfung im Vordergrund ein schwerwiegender Storage-Fehler bei der Datenlöschung festgestellt wird, werden Sie darüber informiert. Sie müssen die Wiederherstellung des Speichervolumes durchführen, um den Fehler zu beheben.

Sie können die Vordergrundüberprüfung so konfigurieren, dass alle Objektspeicher eines Storage Node oder nur bestimmte Objektspeichern überprüft werden.

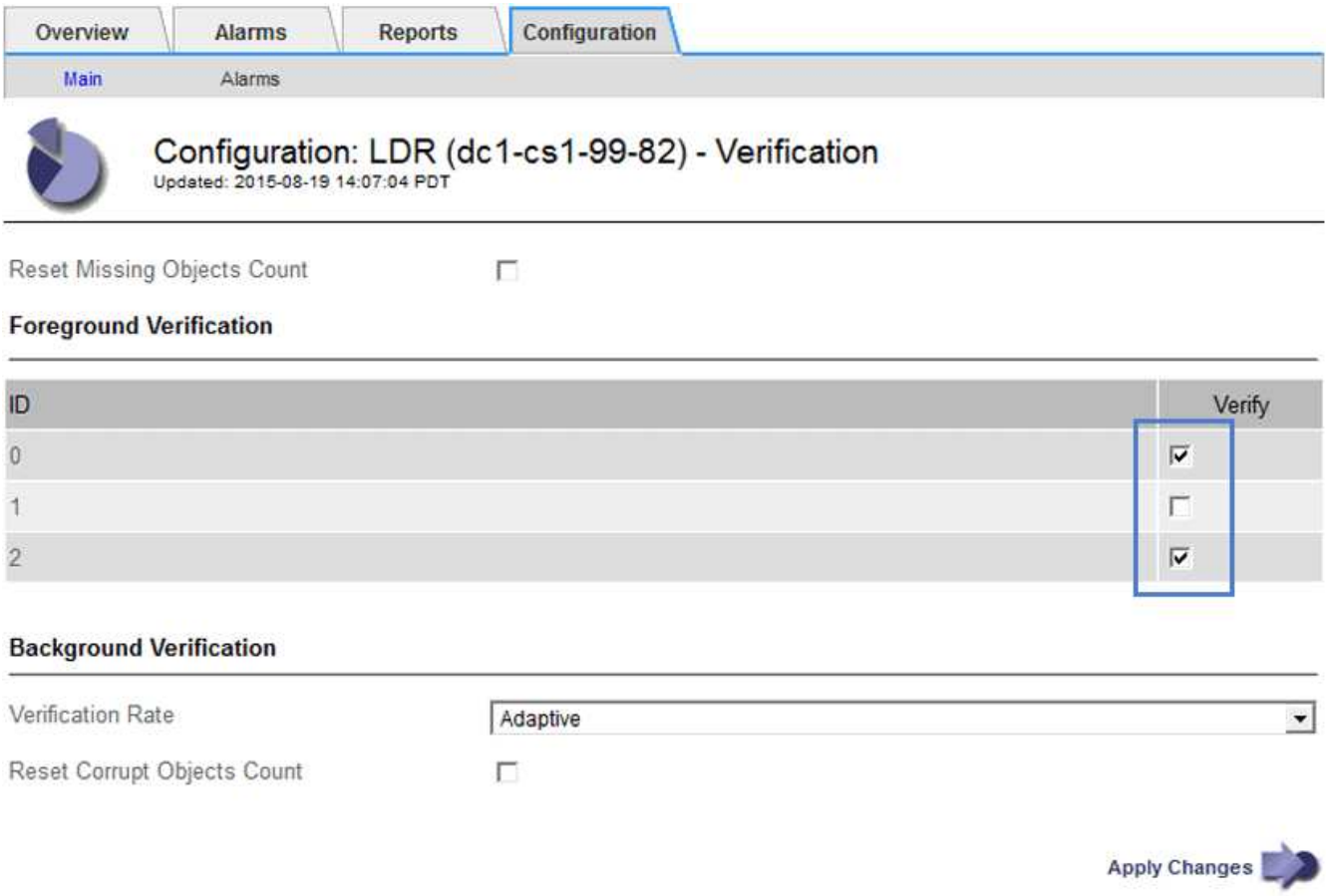
Wenn die Vordergrundüberprüfung fehlende Objektdaten findet, versucht das StorageGRID-System, sie zu ersetzen. Wenn keine Ersatzkopie erstellt werden kann, kann der Alarm „VERLORENE Objekte“ ausgelöst werden.

Die Vordergrundüberprüfung generiert eine LDR-Vordergrundverifizierung, die je nach Anzahl der auf einem Storage-Node gespeicherten Objekte Tage- oder wochenlang dauern kann. Es ist möglich, mehrere Storage-Nodes gleichzeitig auszuwählen. Diese Grid-Aufgaben werden jedoch nicht gleichzeitig ausgeführt. Stattdessen werden sie in eine Warteschlange gestellt und bis zum Abschluss nacheinander ausgeführt. Wenn die Vordergrundüberprüfung auf einem Storage-Node ausgeführt wird, können Sie auf diesem Storage-Node keine andere Überprüfungsaufgabe im Vordergrund starten, obwohl die Option zum Überprüfen zusätzlicher Volumes für den Storage-Node möglicherweise verfügbar ist.

Wenn ein anderer Storage-Node als der, auf dem die Vordergrundüberprüfung ausgeführt wird, offline geschaltet wird, wird die Grid-Aufgabe weiter ausgeführt, bis das Attribut **% complete** 99.99 Prozent erreicht. Das Attribut **% complete** wird dann auf 50 Prozent zurückgestellt und wartet, bis der Speicherknoten wieder in den Online-Status zurückkehrt. Wenn der Status des Speicherknotens wieder online geschaltet wird, wird die Grid-Aufgabe für die Überprüfung des LDR-Vordergrunds fortgesetzt, bis sie abgeschlossen ist.

Schritte

1. Wählen Sie ***Storage Node*** > **LDR** > **Verifizierung** aus.
2. Wählen Sie **Konfiguration** > **Main**.
3. Aktivieren Sie unter **Vordergrundüberprüfung** das Kontrollkästchen für jede Speicher-Volume-ID, die Sie überprüfen möchten.



4. Klicken Sie Auf **Änderungen Übernehmen**.

   Warten Sie, bis die Seite automatisch aktualisiert und neu geladen wird, bevor Sie die Seite verlassen. Sobald die Aktualisierung abgeschlossen ist, stehen Objektspeicher zur Auswahl auf diesem Speicherknoten nicht mehr zur Verfügung.

   Eine LDR-Vordergrundüberprüfungsraster-Aufgabe wird erstellt und ausgeführt, bis sie abgeschlossen, unterbrochen oder abgebrochen wird.

5. Fehlende Objekte oder fehlende Fragmente überwachen:

   a. Wählen Sie ***Storage Node*** > **LDR** > **Verifizierung** aus.

   b. Notieren Sie auf der Registerkarte Übersicht unter **Ergebnisse der Überprüfung** den Wert von **fehlenden Objekten erkannt**.

      Hinweis: Der gleiche Wert wird auf der Seite Knoten als **Lost Objects** angegeben. Gehen Sie zu **Nodes** > ***Storage Node*** und wählen Sie die Registerkarte **Objects** aus.

      Wenn die Anzahl der **fehlenden Objekte erkannt** groß ist (wenn Hunderte von fehlenden Objekten vorhanden sind), liegt wahrscheinlich ein Problem mit dem Speicher des Speicherknoten vor. Wenden Sie sich an den technischen Support.

   c. Wählen Sie ***Storage Node*** > **LDR** > **Erasure Coding** aus.

   d. Notieren Sie auf der Registerkarte Übersicht unter **Ergebnisse der Überprüfung** den Wert von **fehlenden Fragmenten erkannt**.

      Wenn die Anzahl **fehlendes Fragment** groß ist (wenn hunderte von fehlenden Fragmenten vorhanden

sind), liegt wahrscheinlich ein Problem mit dem Speicher des Speicherknoten vor. Wenden Sie sich an den technischen Support.

Wenn die Vordergrundüberprüfung keine beträchtliche Anzahl an fehlenden replizierten Objektkopien oder eine beträchtliche Anzahl an fehlenden Fragmenten erkennt, funktioniert der Speicher normal.

6. Überwachen Sie den Abschluss der Vordergrundüberprüfungsraster-Aufgabe:
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann **site** > ***Admin Node*** > **CMN** > **Grid Task** > **Übersicht** > **Main**.
   b. Stellen Sie sicher, dass das Raster für die Vordergrundverifizierung fehlerfrei fortschreitet.

      Hinweis: Bei Unterbrechung des Vordergrundverifizierungsgitters wird ein Alarm auf Notice-Ebene am Grid Task Status (SCAS) ausgelöst.

   c. Wenn die Rasteraufgabe mit einem angehalten wird `critical storage error`, Das betroffene Volumen wiederherstellen und dann die Vordergrundüberprüfung auf den verbleibenden Volumes ausführen, um auf zusätzliche Fehler zu überprüfen.

      Achtung: Wenn die Aufgabe Vordergrundverifizierung mit der Meldung unterbricht `Encountered a critical storage error in volume volID`, Sie müssen das Verfahren für die Wiederherstellung eines fehlerhaften Speichervolume. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **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.

Verwandte Informationen

"Verwalten Sie erholen"

Fehlerbehebung verloren gegangene und fehlende Objektdaten

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 werden die Warnung **Objekte verloren** und der Alarm für verlorene Objekte (verlorene Objekte) ausgelöst, wie folgt:

- Wenn bei replizierten Kopien eine andere Kopie nicht abgerufen werden kann, gilt das Objekt als verloren, und die Warnung und der Alarm werden ausgelöst.

- Wenn beim Löschen codierter Kopien eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, wird das Attribut „Corrupt Copies Detected (ECOR)“ um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Wenn keine weitere Kopie gefunden wird, werden die Warnung und der Alarm 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.

Wenn Objekt-Daten ohne Kopien verloren gehen, gibt es keine Recovery-Lösung. Sie müssen jedoch den Zähler „Lost Object“ zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren.

Verwandte Informationen

"Untersuchung verlorener Objekte"

"Zurücksetzen verlorener und fehlender Objektanzahl"

Untersuchung verlorener Objekte

Wenn der Alarm * Objects lost* und der Alarm Legacy LOST Objects (Lost Objects) ausgelöst werden, müssen Sie sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Die Warnung **Objekte verloren** und der VERLORENE Alarm zeigen an, dass StorageGRID der Ansicht ist, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

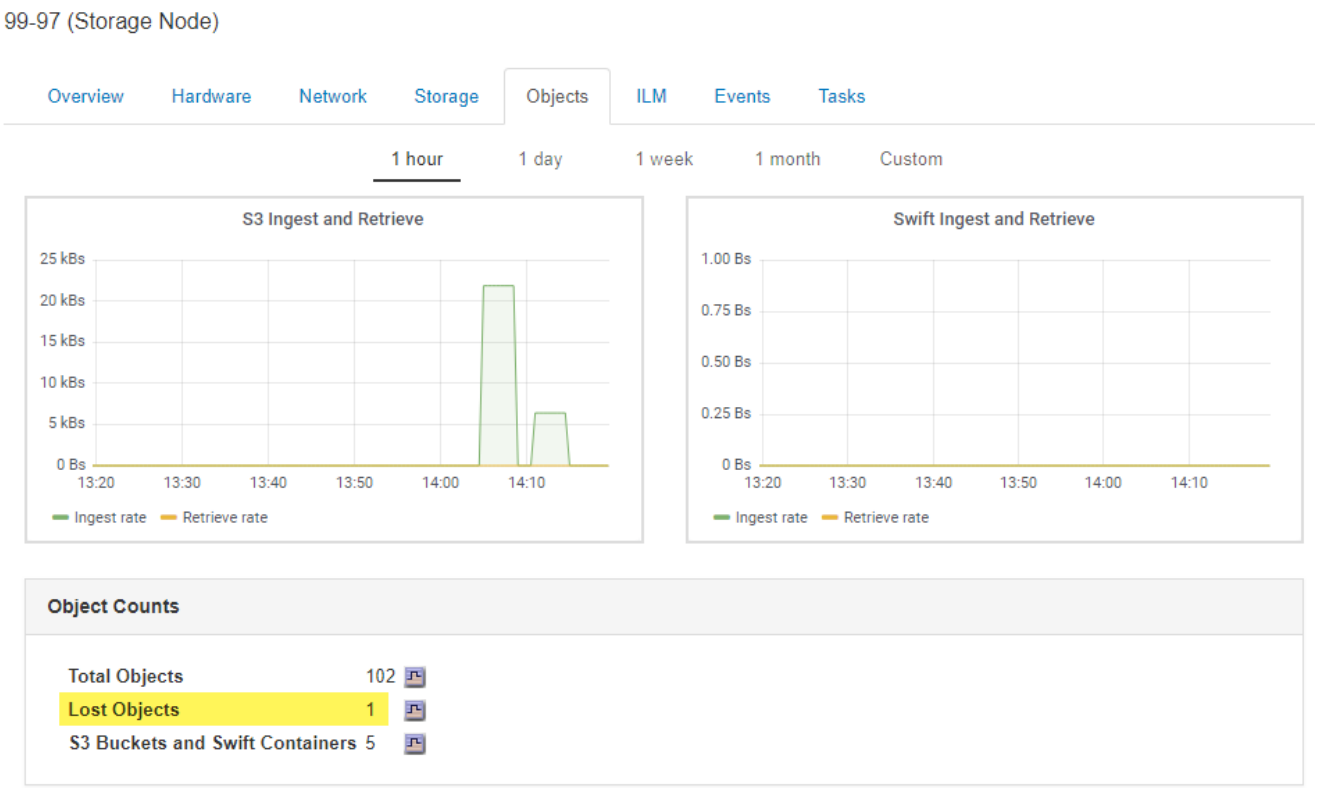
Untersuchen Sie verlorene Objektalarme oder -Warnmeldungen sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. In einigen Fällen können Sie ein verlorenes Objekt wiederherstellen, wenn Sie eine sofortige Aktion ausführen.

Die Anzahl der verlorenen Objekte kann im Grid Manager angezeigt werden.

Schritte

1. Wählen Sie **Knoten**.
2. Wählen Sie ***Speicherknoten*** > **Objekte** Aus.
3. Überprüfen Sie die Anzahl der in der Tabelle Objektanzahl angezeigten verlorenen Objekte.

   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. Greifen Sie von einem Admin-Node aus auf das Audit-Protokoll zu, um die eindeutige Kennung (UUID) des Objekts zu bestimmen, das die Meldung **Objekte verloren** und DEN VERLORENEN Alarm 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 OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. 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“:“)	Wenn das Objekt nicht gefunden wird, wird die Meldung „FEHLER“:“ zurückgegeben. Wenn das Objekt nicht gefunden wird, kann der Alarm sicher ignoriert werden. Das Fehlen eines Objekts bedeutet, dass das Objekt absichtlich gelöscht wurde.
Standorte 0	Wenn im Ausgang Positionen aufgeführt sind, kann der Alarm Lost Objects falsch positiv sein. 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. (Das Verfahren zum Auffinden potenziell verlorener Objekte erläutert, wie Sie die Node-ID verwenden, um den richtigen Storage-Node zu finden.) "Suche nach und Wiederherstellung möglicherweise verlorenen Objekten" Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um den Alarm und die Warnung zu löschen.
Standorte = 0	Wenn in der Ausgabe keine Positionen aufgeführt sind, fehlt das Objekt möglicherweise. Sie können versuchen, das Objekt selbst zu finden und wiederherzustellen, oder Sie können sich an den technischen Support wenden. "Suche nach und Wiederherstellung möglicherweise verlorenen Objekten" Vom technischen Support bitten Sie möglicherweise, zu bestimmen, ob ein Verfahren zur Storage-Recovery durchgeführt wird. Das heißt, wurde auf jedem Storage Node ein Befehl „*Repair-Data*“ ausgegeben, und läuft die Recovery noch? Weitere Informationen zum Wiederherstellen von Objektdaten auf einem Storage-Volume finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.

Verwandte Informationen

"Verwalten Sie erholen"

"Prüfung von Audit-Protokollen"

Suche nach und Wiederherstellung möglicherweise verlorenen Objekten

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 „potentiell verloren“ identifiziert haben.

Was Sie benötigen

- Sie müssen über die UUID eines verlorenen Objekts verfügen, wie in „`Untersuchung verlorener Objekte`“ angegeben.
- Sie müssen die haben `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 die mit dem potenziell verlorenen Objekt verknüpften Audit-Nachrichten zu extrahieren und sie an eine Ausgabedatei zu senden. 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.

f. Suchen Sie den Speicherknoten für diese LDR-Knoten-ID.

Es gibt zwei Möglichkeiten, die Node-ID zum Suchen des Storage Node zu verwenden:

- Wählen Sie im Grid Manager die Option **Support** > **Tools** > **Grid Topology** aus. Wählen Sie dann ***Data Center*** > ***Storage Node*** > **LDR** aus. Die LDR-Knoten-ID befindet sich in der Node-Informationstabelle. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie den gefunden haben, der dieses LDR hostet.
- Laden Sie das Wiederherstellungspaket für das Grid herunter und entpacken Sie es. Das PAKET enthält ein Verzeichnis *\docs*. Wenn Sie die Datei index.html öffnen, zeigt die Serverübersicht alle Knoten-IDs für alle Grid-Knoten an.

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'
```

Hinweis: Fügen Sie den Objektdateipfad immer in einzelne Anführungszeichen, um Sonderzeichen zu entkommen.

- Wenn der Objektpfad nicht gefunden wurde, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wurde, fahren Sie mit Schritt fort Stellen Sie das Objekt in StorageGRID wieder her. Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.

1. 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.

      Hinweis: Wenn der Speicherknoten, in dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf einen beliebigen Speicherknoten kopieren, der online ist. 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 das angezeigt `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'
        ```

      Mit Schritt fortfahren Überprüfen Sie, ob neue Standorte erstellt wurden

1. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, vergewissern Sie sich, dass neue

Speicherorte erstellt wurden.

a. Geben Sie Ein: `cd /proc/OBRP`

b. 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`

2. 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.

b. Setzen Sie die Anzahl der verlorenen Objekte im Grid Manager zurück.

Verwandte Informationen

"Untersuchung verlorener Objekte"

"Bestätigen der Speicherorte von Objektdaten"

"Zurücksetzen verlorener und fehlender Objektanzahl"

"Prüfung von Audit-Protokollen"

Zurücksetzen verlorener und fehlender Objektanzahl

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

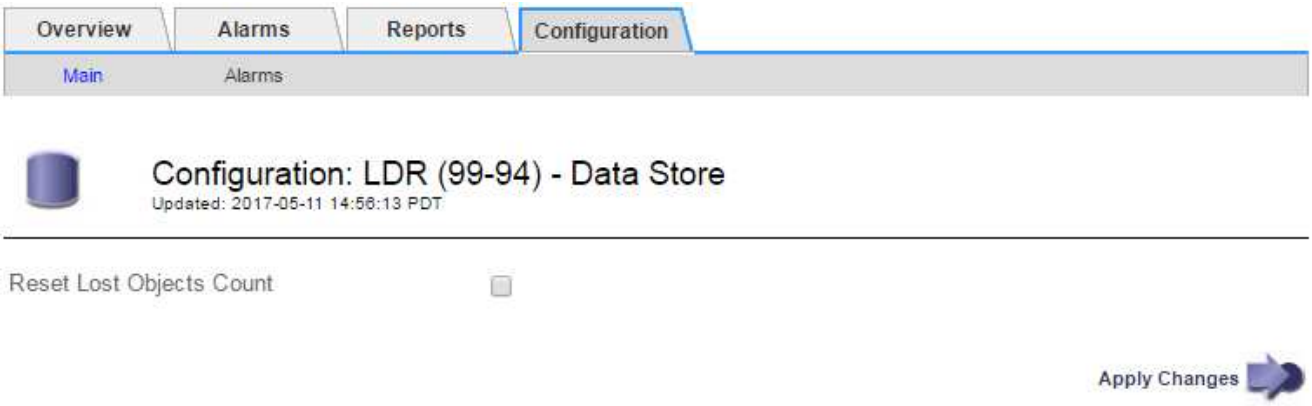
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **Support** > **Tools** > **Grid Topology** > ***site*** **>** ***Storage Node*** > **LDR** > **Data Store** > **Übersicht** > **Main**
- **Support** > **Tools** > **Grid Topology** > ***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 Topology** 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**.

   e. Wählen Sie **Anzahl der fehlenden Objekte zurücksetzen** und **Anzahl der beschädigten Objekte zurücksetzen**.

   f. Wenn Sie sicher sind, dass keine isolierten Objekte erforderlich sind, können Sie **Quarantäne-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.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“

Der Alarm * Low Object Data Storage* überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Storage Node verfügbar ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Der **Low Object Datenspeicher** wird ausgelöst, wenn die Gesamtzahl der replizierten und Erasure codierten Objektdaten auf einem Storage Node eine der Bedingungen erfüllt, 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 **Alarme** > **Aktuell**.

   Die Seite „Meldungen“ wird angezeigt.

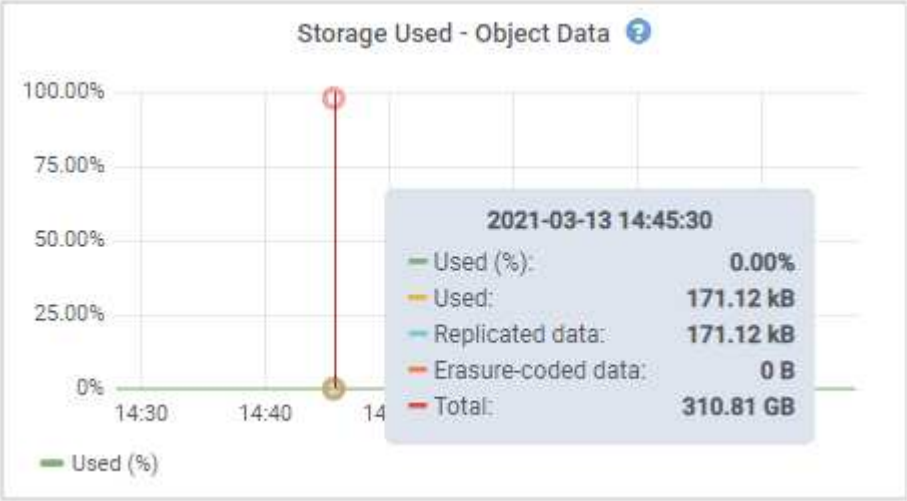
2. Erweitern Sie bei Bedarf aus der Warnmeldungstabelle die Warnungsgruppe **Low Object Data Storage** und wählen Sie die Warnung aus, die angezeigt werden soll.

   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 Mauszeiger über das Diagramm „verwendete Daten – 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.
- **Erasure-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, ein Erweiterungsverfahren für zusätzliche Speicherkapazität durchführen.

   Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen.

   Informationen zum Verwalten eines vollständigen Speicherknoten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"Fehlerbehebung beim SSTS-Alarm (Storage Status)"

"Erweitern Sie Ihr Raster"

"StorageGRID verwalten"

Fehlerbehebung beim SSTS-Alarm (Storage Status)

Der SSTS-Alarm (Storage Status) wird ausgelöst, wenn ein Speicherknoten über nicht

genügend freien Speicherplatz für den Objektspeicher verfügt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- 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 Speicheroptionen Übersicht**) 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

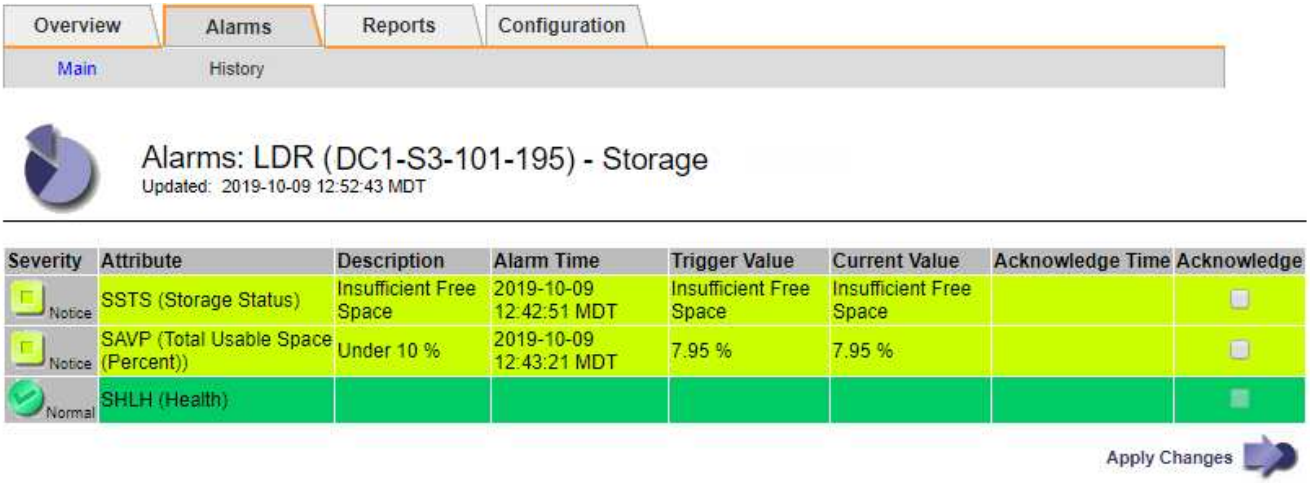
Angenommen, das Speichervolumen-Soft-Read-Only-Wasserzeichen ist auf 10 GB gesetzt, das ist der Standardwert. Der SSTS-Alarm wird ausgelöst, wenn auf jedem Speicher-Volume im Storage-Node weniger als 10 GB nutzbarer Speicherplatz verbleibt. Wenn eines der Volumes über 10 GB oder mehr verfügbaren Speicherplatz 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)** > **Aktuelle Alarme**.
2. Wählen Sie in der Spalte Service das Rechenzentrum, den Node und den Service aus, die dem SSTS-Alarm zugeordnet sind.

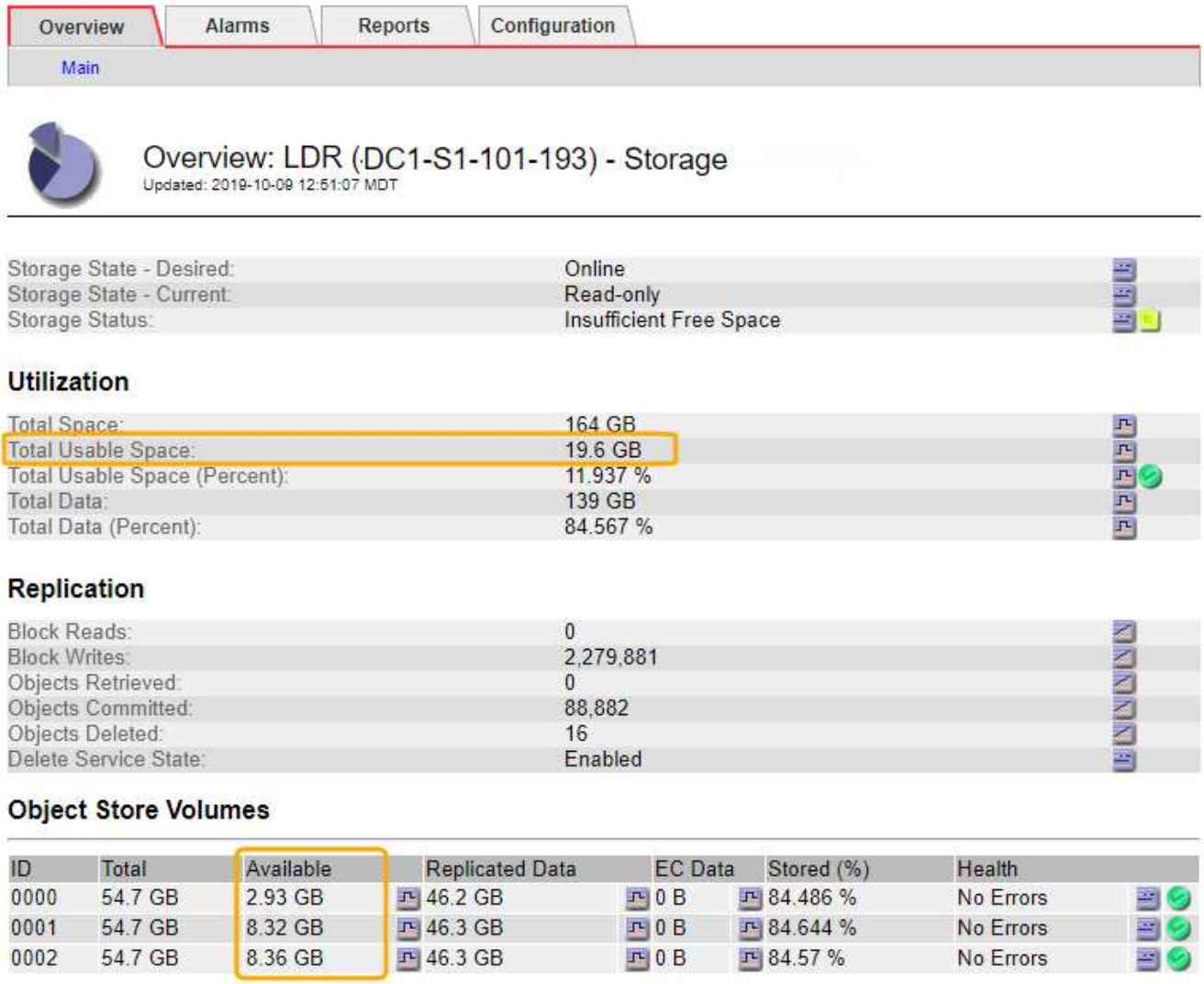
   Die Seite Grid Topology wird angezeigt. Auf der Registerkarte „Alarme“ werden die aktiven Alarme für den ausgewählten Knoten und Dienst angezeigt.



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.

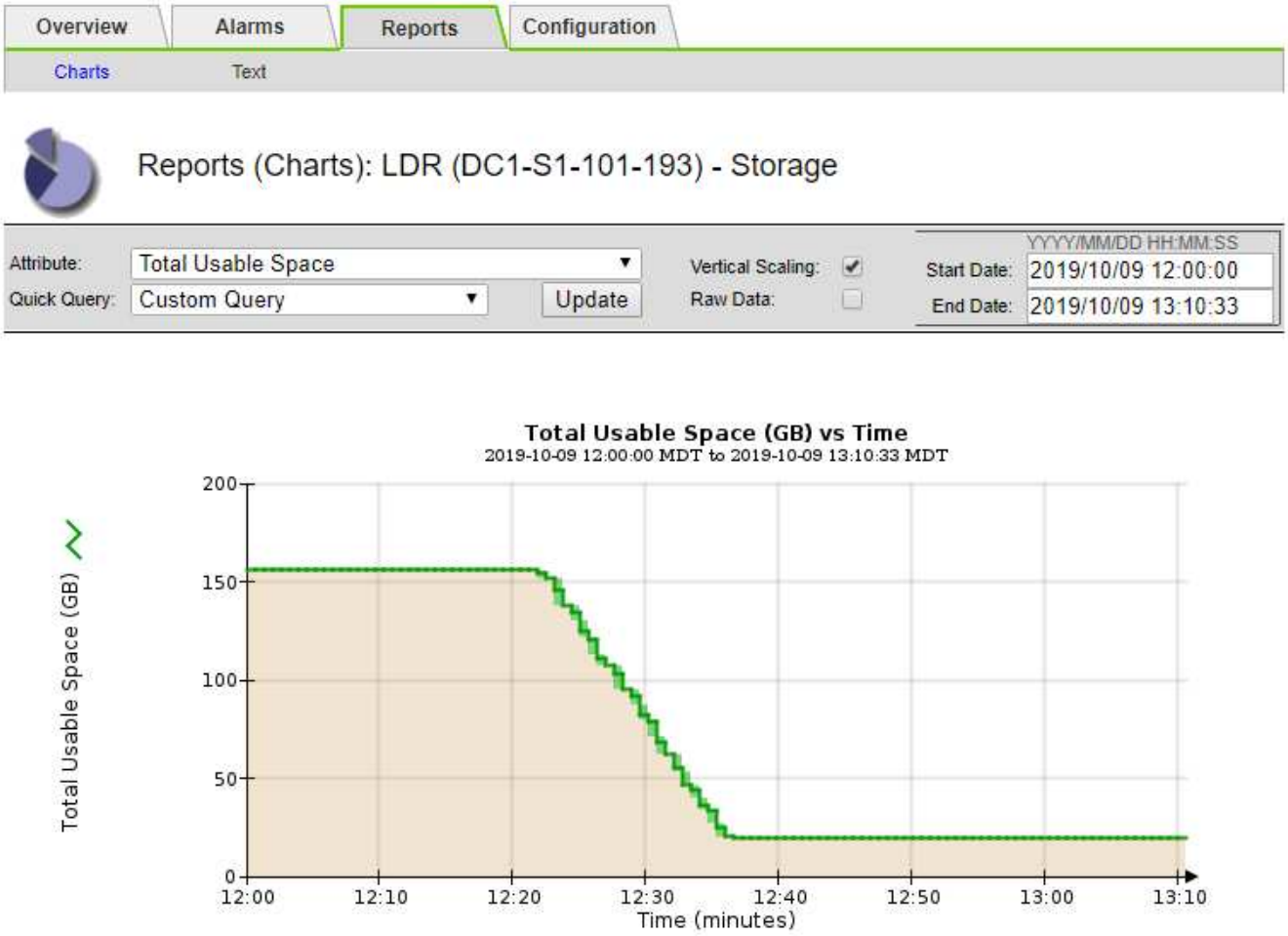
3. Um festzustellen, wie viel nutzbarer Speicherplatz tatsächlich verfügbar ist, wählen Sie **LDR Storage Übersicht**, und suchen Sie das Attribut Total Usable Space (STAS).



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.

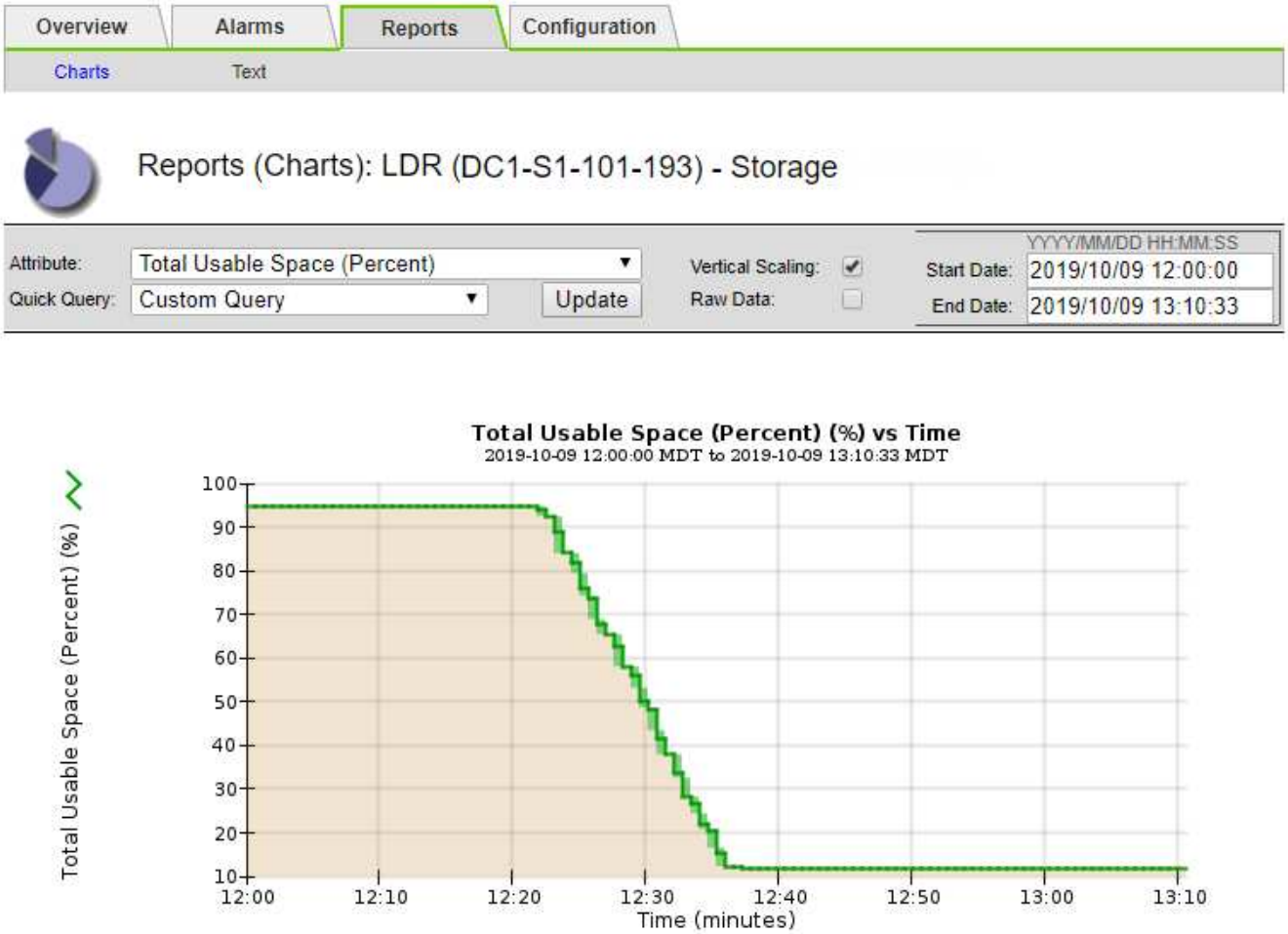
4. Um zu verstehen, wie Speicher im Laufe der Zeit genutzt wurde, wählen Sie die Registerkarte **Berichte** und zeichnen den gesamten nutzbaren Speicherplatz in den letzten Stunden.

   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.



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.



6. Bei Bedarf Erweiterung des StorageGRID Systems Storage-Kapazität hinzufügen.

   Anweisungen zum Verwalten eines vollständigen Speicherknoten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

"StorageGRID verwalten"

Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm)

Der SMTT-Alarm (Total Events) wird im Grid Manager ausgelöst, wenn eine Plattformdienstnachricht an ein Ziel gesendet wird, das die Daten nicht annehmen kann.

Über diese Aufgabe

So kann beispielsweise ein S3-Multipart-Upload erfolgreich sein, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsmeldung nicht an den konfigurierten Endpunkt gesendet 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.

Weitere Informationen zur Fehlerbehebung bei Plattform-Services finden Sie in den Anweisungen für die

Administration von StorageGRID. Möglicherweise müssen Sie über den Tenant Manager auf den Mandanten zugreifen, um einen Plattformdienstfehler zu beheben.

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. Klicken Sie auf **Ereignisanzahl 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.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"Referenz für Protokolldateien"

"Ereignisanzahl wird zurückgesetzt"

Behebung von Metadatenproblemen

Sie können verschiedene Aufgaben ausführen, um die Ursache von Metadatenproblemen zu ermitteln.

Fehlerbehebung für Storage-Warnmeldungen bei niedrigen Metadaten

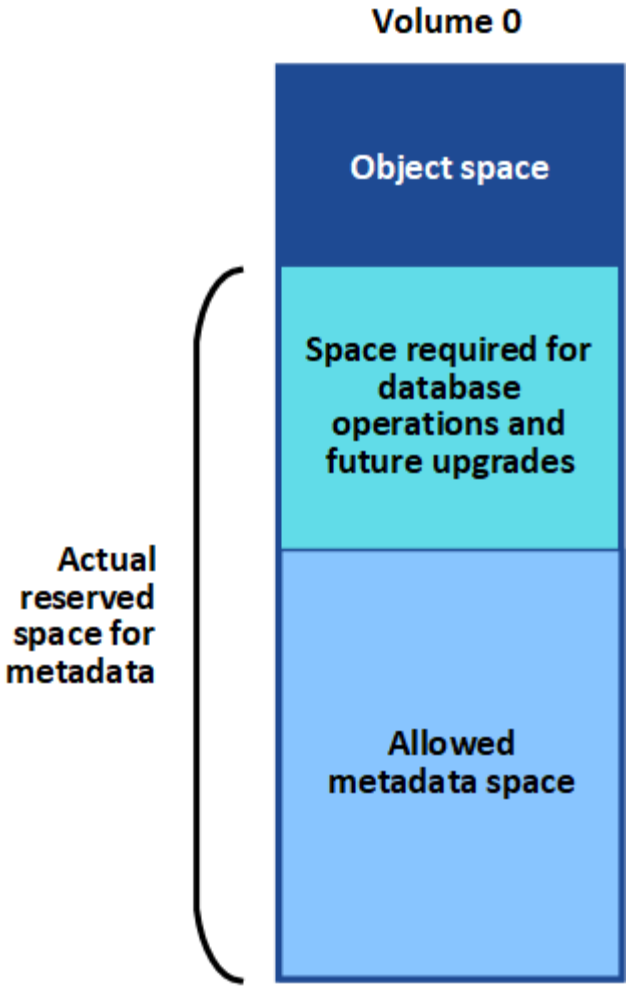
Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

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 Objekt-Metadaten mehr als 100 % des für Metadaten zulässigen Speicherplatzes belegen, können Datenbankvorgänge nicht effizient ausgeführt werden und es treten Fehler auf.

StorageGRID verwendet die folgende Prometheus Kennzahl, um den vollen Umfang des zulässigen Metadaten-Speicherplatzes zu messen:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

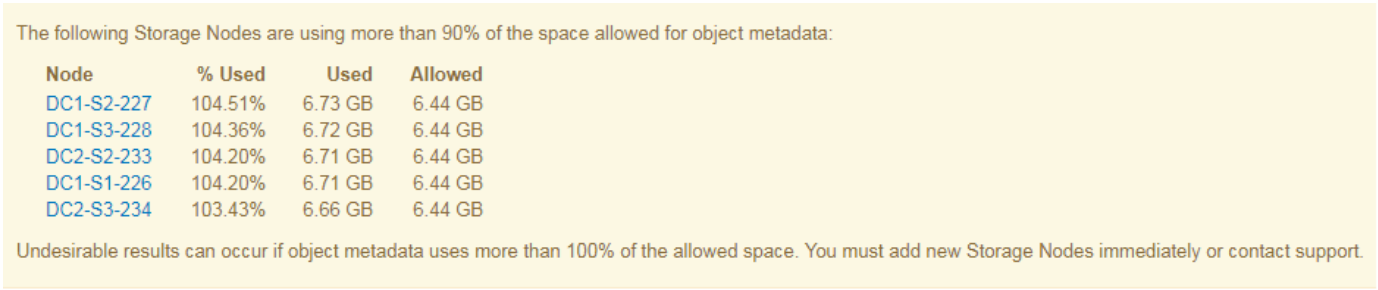
Wenn dieser Prometheus-Ausdruck bestimmte Schwellenwerte erreicht, wird die Warnung **Low Metadaten Storage** ausgelöst.

- **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 Metadaten-Speicherplatzes beanspruchen, wird im Dashboard eine Warnung 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.



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 **Alarme** > **Aktuell**.
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 einem Standort Metadatenkapazität hinzufügen möchten, sollten Sie auch alle anderen Standorte um dieselbe Anzahl von Storage-Nodes erweitern.

   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.

Verwandte Informationen

"Monitoring der Objekt-Metadaten-Kapazität für jeden Storage Node"

"Erweitern Sie Ihr Raster"

Fehlerbehebung im Alarm Services: Status - Cassandra (SVST)

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- 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.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen.

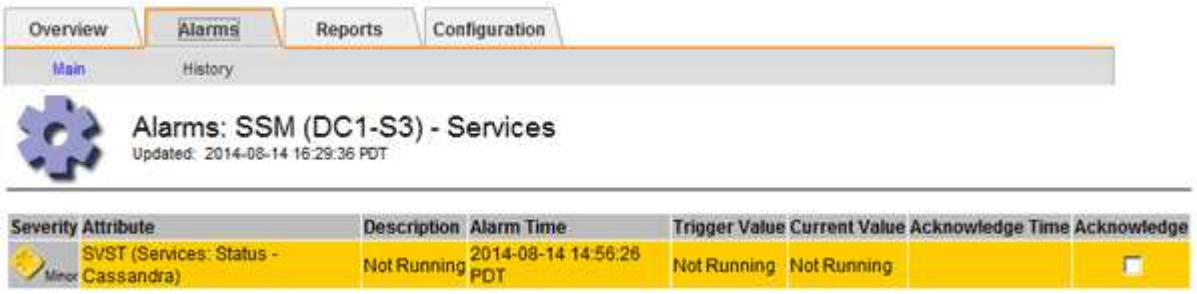
"Diagnose wird ausgeführt"

> Wenn mindestens zwei der Cassandra-Datenbankdienste länger als 15 Tage ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

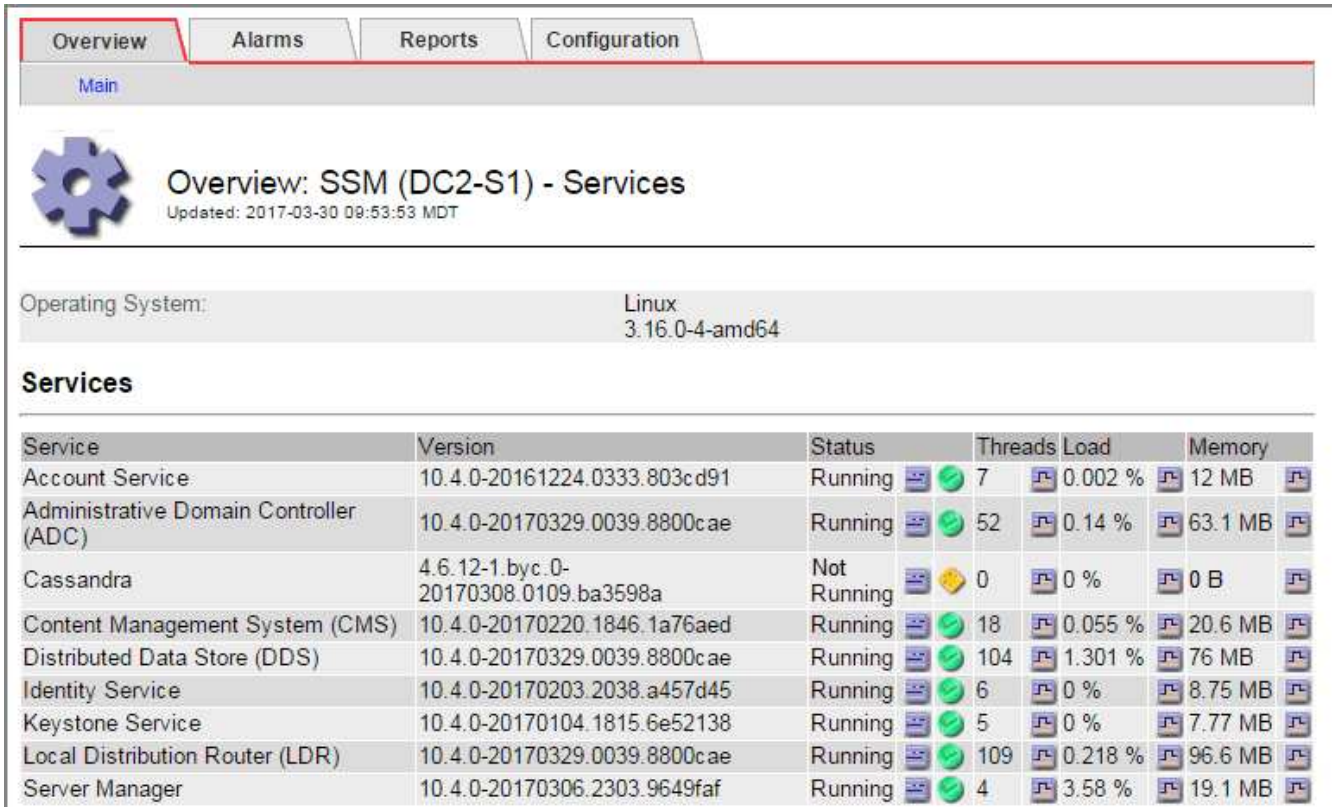
Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** **>** ***Storage Node*** > **SSM** > **Services** > **Alarme** > **Main**, um Alarme anzuzeigen.

   Dieses Beispiel zeigt, dass der SVST-Alarm ausgelöst wurde.



   Auf der SSM Services-Hauptseite wird auch angezeigt, dass Cassandra nicht ausgeführt wird.



1. Versuchen Sie, Cassandra vom Storage-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`
2. 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.

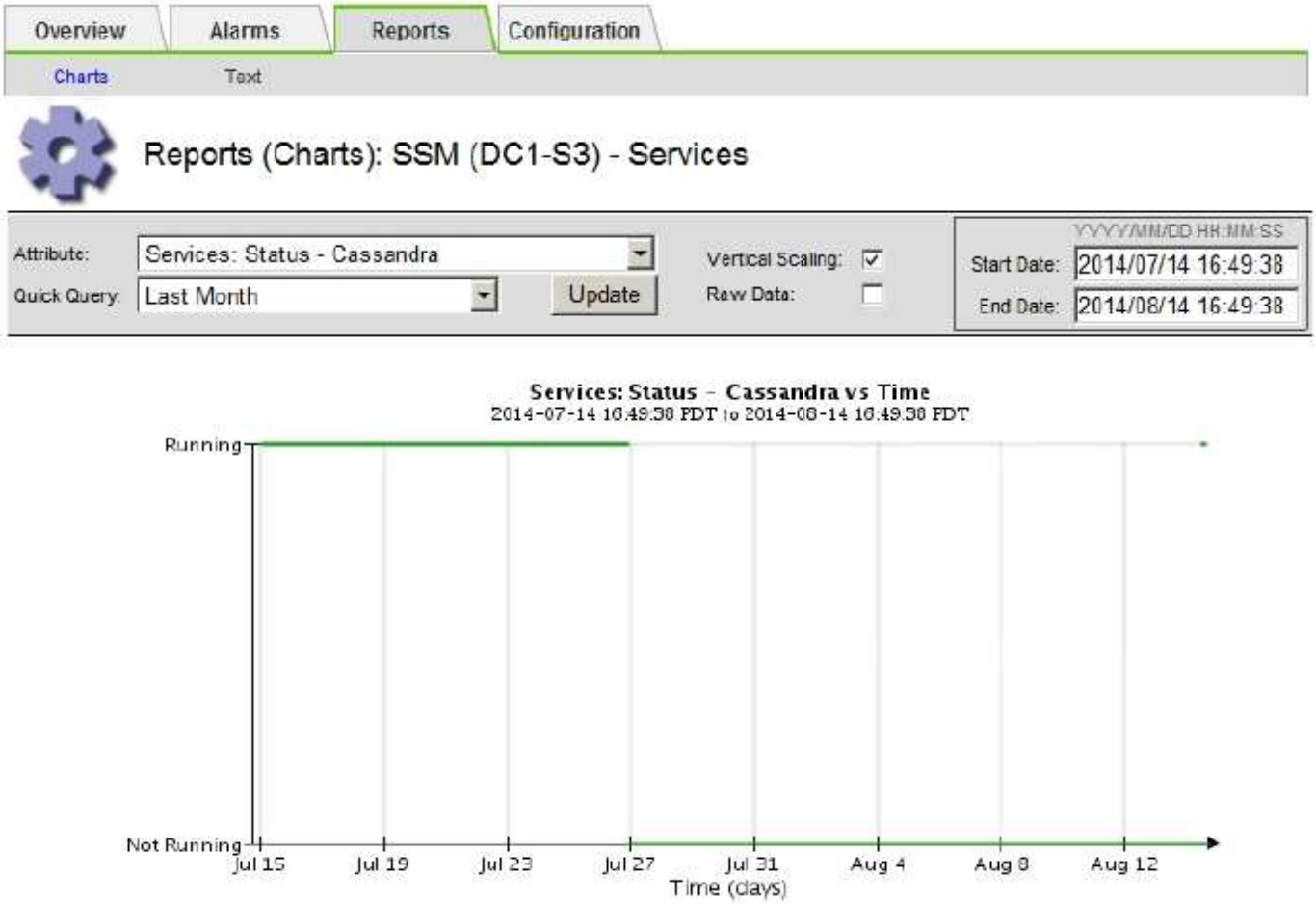
3. Cassandra Diagramm:
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Storage Node*** > **SSM** > **Services** > **Berichte** > **Diagramme** aus.
   b. Wählen Sie **Attribut** > **Service: Status - Cassandra**.
   c. Geben Sie für **Startdatum** ein 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.



1. So prüfen Sie die Datei servermanager.log auf dem 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. 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 „`Wiederherstellen von einem einzelnen Speicherknoten nach unten mehr als 15 Tage`“ in den Anweisungen zur Wiederherstellung und Wartung.

c. Wenden Sie sich an den technischen Support, wenn die Alarme nach dem Wiederaufbau von Cassandra nicht gelöscht werden.

Verwandte Informationen

"Verwalten Sie erholen"

Fehlerbehebung bei Cassandra-Speicherfehlern (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 **Knoten** > ***Grid Node*** > **Ereignisse**.
2. Stellen Sie sicher, dass die Anzahl der Cassandra Heap-Fehler bei einem Speicherfehler mindestens 1 beträgt.

   Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen.

   "Diagnose wird ausgeführt"

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. Wenn das Problem behoben ist, klicken Sie auf **Ereignisanzahl zurücksetzen**.

Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen.

Verwandte Informationen

"Ereignisanzahl wird zurückgesetzt"

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.

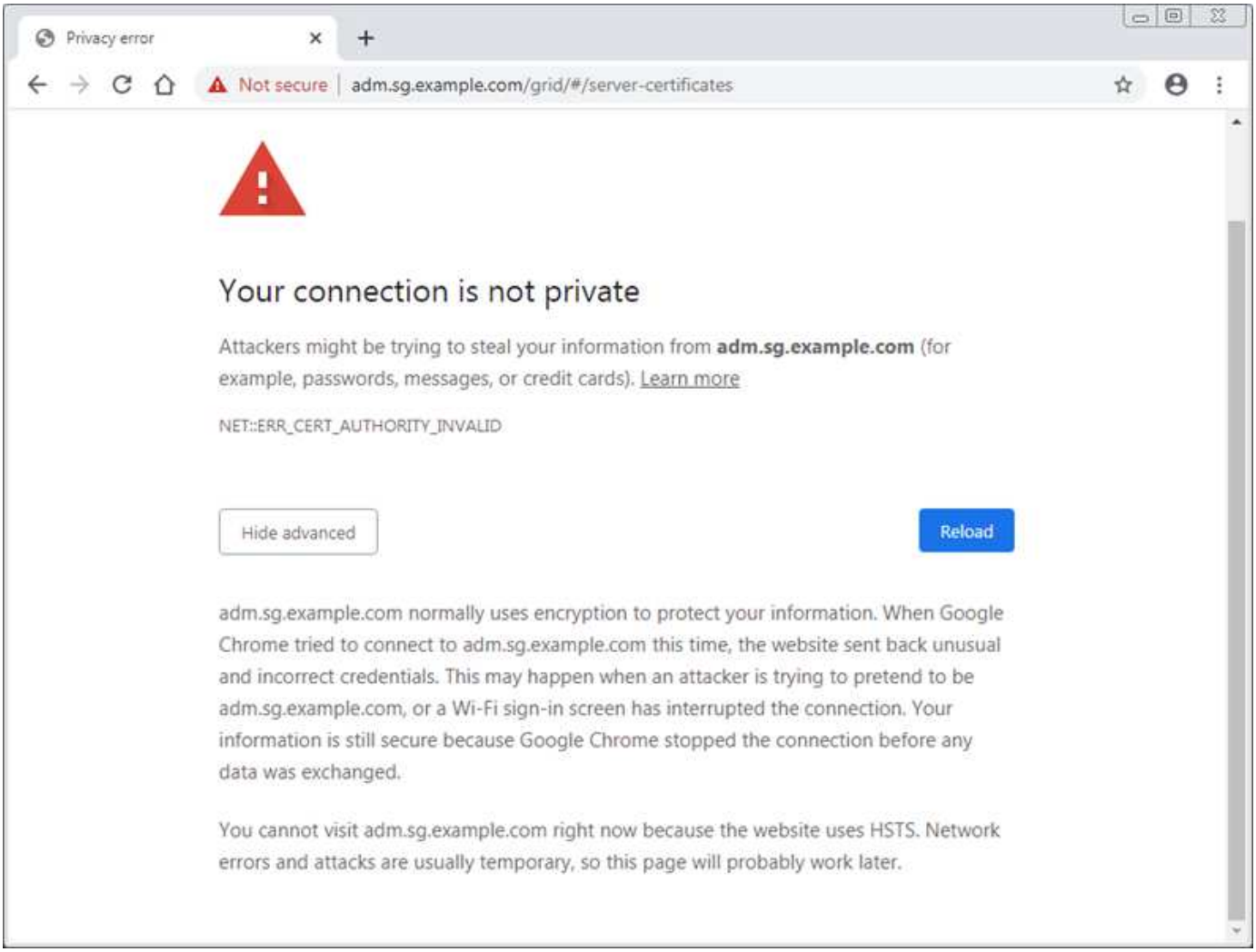
Über diese Aufgabe

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 Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für den benutzerdefinierten Verwaltungsserver läuft ab.
- Sie werden von einem Server-Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Das folgende Beispiel zeigt einen Zertifikatfehler, wenn das Zertifikat des benutzerdefinierten Verwaltungsservers abgelaufen ist:



Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn das Serverzertifikat abläuft.

Wenn Sie Clientzertifikate für die externe Prometheus-Integration verwenden, können Zertifikatfehler durch das StorageGRID Management Interface Server Zertifikat oder durch Client-Zertifikate verursacht werden. Die Warnung **Ablauf von Zertifikaten, die auf der Seite Clientzertifikate** konfiguriert sind, wird ausgelöst, wenn ein Clientzertifikat abläuft.

Schritte

1. Wenn Sie eine Benachrichtigung über ein abgelaufenes Zertifikat erhalten haben, rufen Sie die Zertifikatsdetails auf:
   - Wählen Sie für ein Serverzertifikat **Konfiguration Netzwerkeinstellungen Serverzertifikate** aus.
   - Wählen Sie für ein Clientzertifikat **Konfiguration Zugangskontrolle Clientzertifikate** aus.
2. Überprüfen Sie die Gültigkeitsdauer des Zertifikats.

   Einige Webbrowser und S3- oder Swift-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.

3. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein oder generieren Sie ein neues Zertifikat.
   - Informationen zum Serverzertifikat finden Sie in den Schritten zum Konfigurieren eines

benutzerdefinierten Serverzertifikats für den Grid Manager und den Mandantenmanager in den Anweisungen für die Administration von StorageGRID.

- Informationen zum Konfigurieren eines Client-Zertifikats finden Sie in den Schritten zum Konfigurieren eines Client-Zertifikats in den Anleitungen zum Verwalten von StorageGRID.

4. 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 **Konfiguration Netzwerkeinstellungen Server-Zertifikate** aus, um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
     iii. Lesen Sie in den Anweisungen zum Verwalten von StorageGRID die Schritte zum Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Mandanten-Manager.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei Problemen mit Admin-Knoten 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.

Fehlerbehebung bei Anmeldefehlern

Wenn beim Anmelden bei einem StorageGRID-Admin-Node ein Fehler auftritt, weist Ihr System möglicherweise ein Problem mit der Konfiguration des Identitätsverbunds auf, ein Netzwerk- oder Hardwareproblem, ein Problem mit den Admin-Node-Services oder ein Problem mit der Cassandra-Datenbank auf verbundenen Speicherknoten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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-Node haben oder sich dennoch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Ermitteln, ob die Hardware des Node offline ist
4. Wenn SSO (Single Sign On) für Ihr StorageGRID-System aktiviert ist, lesen Sie in den Anweisungen zur Administration von StorageGRID die Schritte zur Konfiguration der Single Sign-On.

   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 mit einem 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 Alarme.
     ii. Wählen Sie **Konfiguration** > **Identitätsföderation**.
     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 sich der lokale Benutzer nicht anmelden kann und Sie sich 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 Apache-Webserver ausgeführt wird: `# service apache2 status`

1. Verwenden Sie Lumberjack, um Protokolle zu sammeln: `# /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.

1. Überprüfen Sie die folgenden Protokolle:
   - `/var/local/log/bycast.log`
   - `/var/local/log/bycast-err.log`
   - `/var/local/log/nms.log`

- `**/*commands.txt`

2. 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.

3. 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 `#`.

4. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

   Stellen Sie sicher, dass die Services idnt, acct, nginx und cassandra ausgeführt werden.

5. Wiederholen Sie die Schritte Verwenden Sie Lumberjack, um Protokolle zu sammeln Und Protokolle prüfen So prüfen Sie die Protokolle auf den Speicherknoten.
6. 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.

Verwandte Informationen

"StorageGRID verwalten"

"Referenz für Protokolldateien"

Fehlerbehebung bei Problemen mit der Benutzeroberfläche

Nach dem Upgrade auf eine neue Version der StorageGRID-Software sind möglicherweise Probleme mit dem Grid Manager oder dem Tenant Manager zu sehen.

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 einen unterstützten Browser verwenden.

  Die Browser-Unterstützung wurde für StorageGRID 11.5 geändert. Vergewissern Sie sich, dass Sie eine unterstützte Version verwenden.

- 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.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"StorageGRID verwalten"

Überprüfen des Status eines nicht verfügbaren Admin-Knotens

Wenn das StorageGRID-System mehrere Administratorknoten enthält, können Sie den Status eines nicht verfügbaren Admin-Knotens mit einem anderen Admin-Knoten überprüfen.

Was Sie benötigen

Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Melden Sie sich bei einem verfügbaren Admin-Node mit einem unterstützten Browser beim Grid Manager an.
2. Wählen Sie **Support** > **Tools** > **Grid Topology** 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.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung 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.

Fehlerbehebung „`422: Unprocessable Entity`“-Fehler

Der Fehler 422: Unbearbeitbare Einheit kann unter verschiedenen Umständen 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

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Diese Meldung kann auftreten, wenn Sie bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option **TLS nicht verwenden** für Transport Layer Security (TLS) auswählen.
	
	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.

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte 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.
	
	Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eine der von StorageGRID unterstützten Chiffren für ausgehende TLS-Verbindungen verwenden, wie in den Anleitungen zur StorageGRID-Verwaltung dargestellt.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU

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 nach Bedarf, um sicherzustellen, dass sie für die Grid Network Interface (eth0) auf allen Knoten identisch sind.
   - Informationen zu Appliance-Knoten finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.
   - Verwenden Sie für Linux- und VMware-basierte Knoten den folgenden Befehl: `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`
     - Beispiel*: `change-mtu.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-mtu.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
`mtu`	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
`network`	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: • Raster • Admin • Client

+

Optionale Argumente	Beschreibung
`-h, – help`	HilMeldung anzeigen und beenden.
`-n node, --node node`	Der Node. Die Standardeinstellung ist der lokale Knoten.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Fehlerbehebung bei dem NRER-Alarm (Network Receive Error)

NRER-Alarme (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.
    - Wenn der Fehler durch eine nicht übereinstimmende FEC verursacht wird, führen Sie die folgenden Schritte aus:

      Hinweis: Diese Schritte gelten nur für NRER-Fehler, die durch FEC-Diskrepanz auf StorageGRID-Geräten verursacht werden.

        i. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID-Gerät angeschlossen ist.

        ii. Überprüfen Sie die physikalische Integrität der Kabel vom Gerät zum Switch.

        iii. Wenn Sie die FEC-Einstellungen ändern möchten, um den NRER-Alarm zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Konfiguration verknüpfen“ des Installationsprogramms von StorageGRID-Geräten für den **Auto**-Modus konfiguriert ist (siehe Installations- und Wartungsanweisungen für Ihr Gerät). Ändern Sie dann die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

        (Sie können 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.)

Hinweis: StorageGRID-Geräte unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie kein FEC.

- 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 NRR-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 identisch sein.

  > Informationen zum Ändern der MTU-Einstellung finden Sie im Installations- und Wartungshandbuch für Ihre Appliance.

- Wenn der Fehler durch hohe Verbindungsfehlerraten verursacht wird, führen Sie die folgenden Schritte aus:
  i. Aktivieren Sie FEC, falls nicht bereits aktiviert.
  ii. Stellen Sie sicher, dass Ihre Netzwerkkabel von guter Qualität sind und nicht beschädigt oder nicht ordnungsgemäß angeschlossen sind.
  iii. Falls 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.

- Wenn es sich bei dem Fehler um einen NIC-Ringpuffer handelt, wenden Sie sich an den technischen Support.

  Der Ruffuffer kann bei Überlastung des StorageGRID-Systems überlaufen werden und kann Netzwerkereignisse nicht zeitnah verarbeiten.

2. Nachdem Sie das zugrunde liegende Problem gelöst haben, setzen Sie den Fehlerzähler zurück.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** 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

"Fehlerbehebung bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU"

"Alarmreferenz (Altsystem)"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"SG100 SG1000 Services-Appliances"

Fehlerbehebung bei Fehlern 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 Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer 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.

Verwandte Informationen

"Verwalten Sie erholen"

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-Adressenklonens 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 im Installationshandbuch für Ihre Plattform.

> 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 promiskuious-Modus auf dem Hypervisor nicht aktiviert wurde.

Weitere Informationen zum Aktivieren des MAC-Klonens finden Sie in den Anweisungen im Installationshandbuch für Ihre Plattform.

Promiskuous Modus

Wenn Sie kein Klonen der MAC-Adresse verwenden möchten und lieber alle Schnittstellen Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen empfangen und übertragen möchten, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene der virtuellen Switch- und Portgruppen auf **Accept** für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen eingestellt 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.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie 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 Docker-Befehle, 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. Beenden Sie unter Linux den Docker Container und alle steuernden storagegrid Node-Prozesse:`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).

   ```
   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
   ```

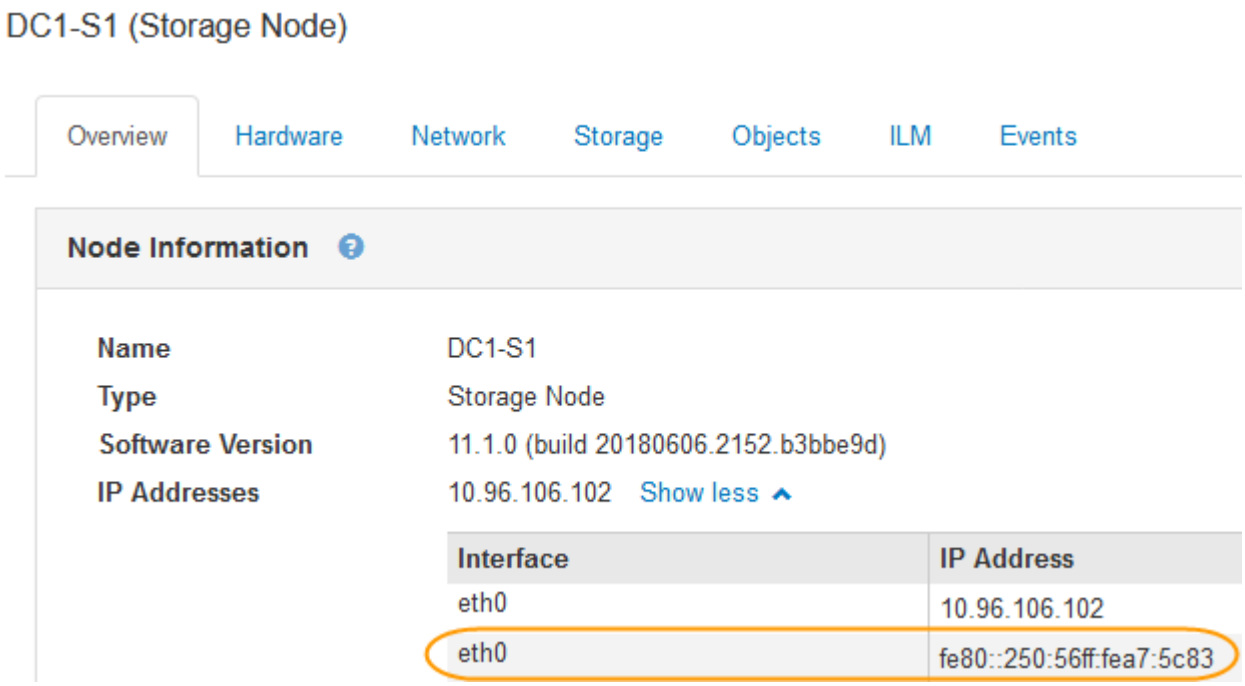
Linux: Fehlerbehebung von IPv6-Unterstützung

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 **Knoten** aus, und wählen Sie den Knoten aus. Klicken Sie dann auf der Registerkarte Übersicht neben **IP-Adressen** auf **Mehr anzeigen**.



- Wählen Sie **Support** > **Tools** > **Grid Topology** 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
```

Prüfung von Audit-Protokollen

Machen Sie sich mit den StorageGRID Systemaudits-Protokollen vertraut und sehen Sie eine Liste aller Audit-Meldungen an.

- "Übersicht über Überwachungsnachrichten"
- "Audit-Log-Datei und Nachrichtenformate"
- "Überwachungsmeldungen und der Lebenszyklus von Objekten"
- "Audit-Meldungen"

Übersicht über Überwachungsnachrichten

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.

Es wird davon ausgegangen, dass Sie die Art der geprüften Aktivitäten innerhalb des StorageGRID-Systems genau kennen. Um die Text-Log-Datei verwenden zu können, müssen Sie auf die konfigurierte Revisionsfreigabe im Admin-Knoten zugreifen können.

Verwandte Informationen

"StorageGRID verwalten"

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:

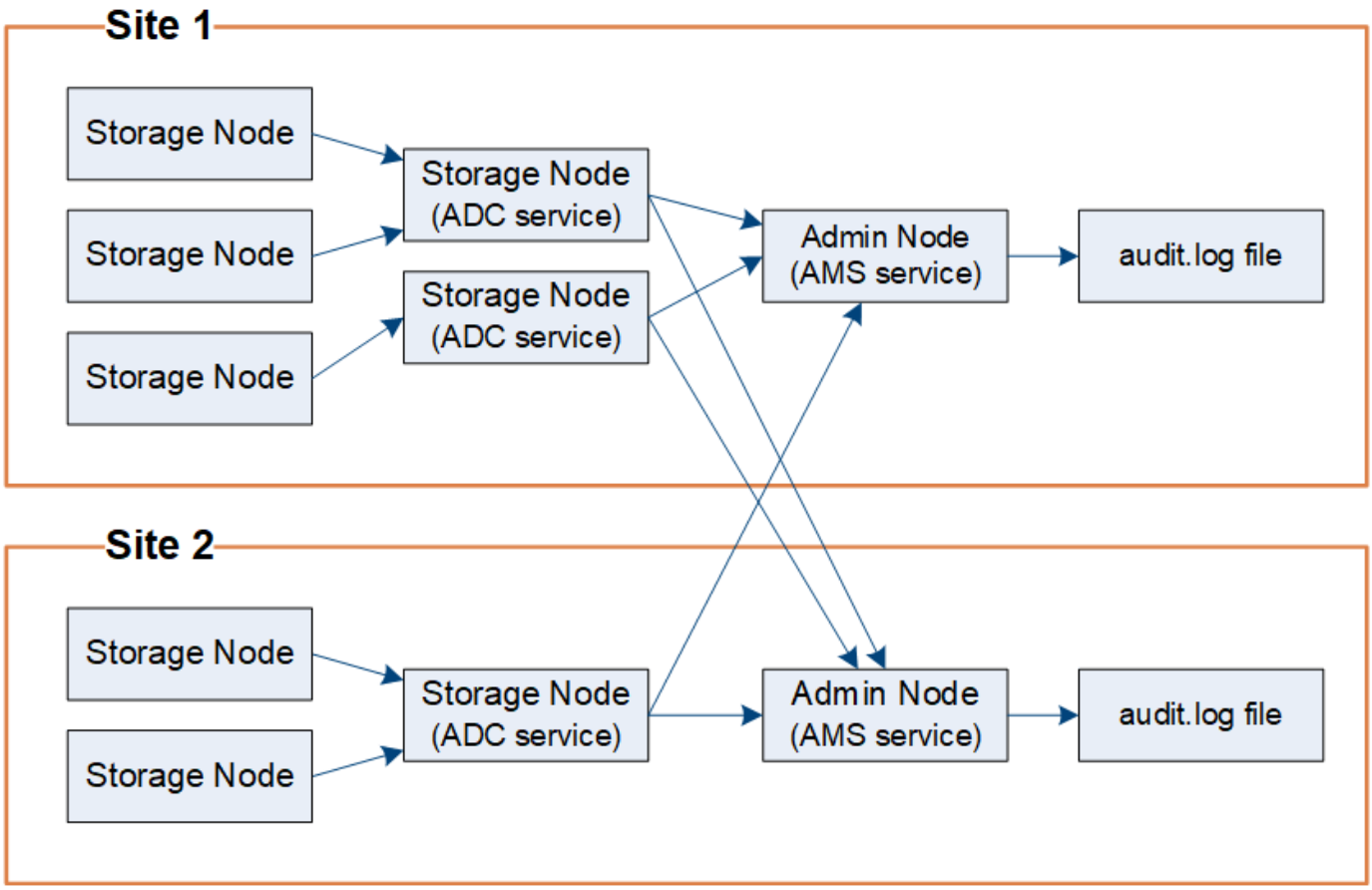
Audit-Nachrichtenfluss

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 Speicherknoten 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.

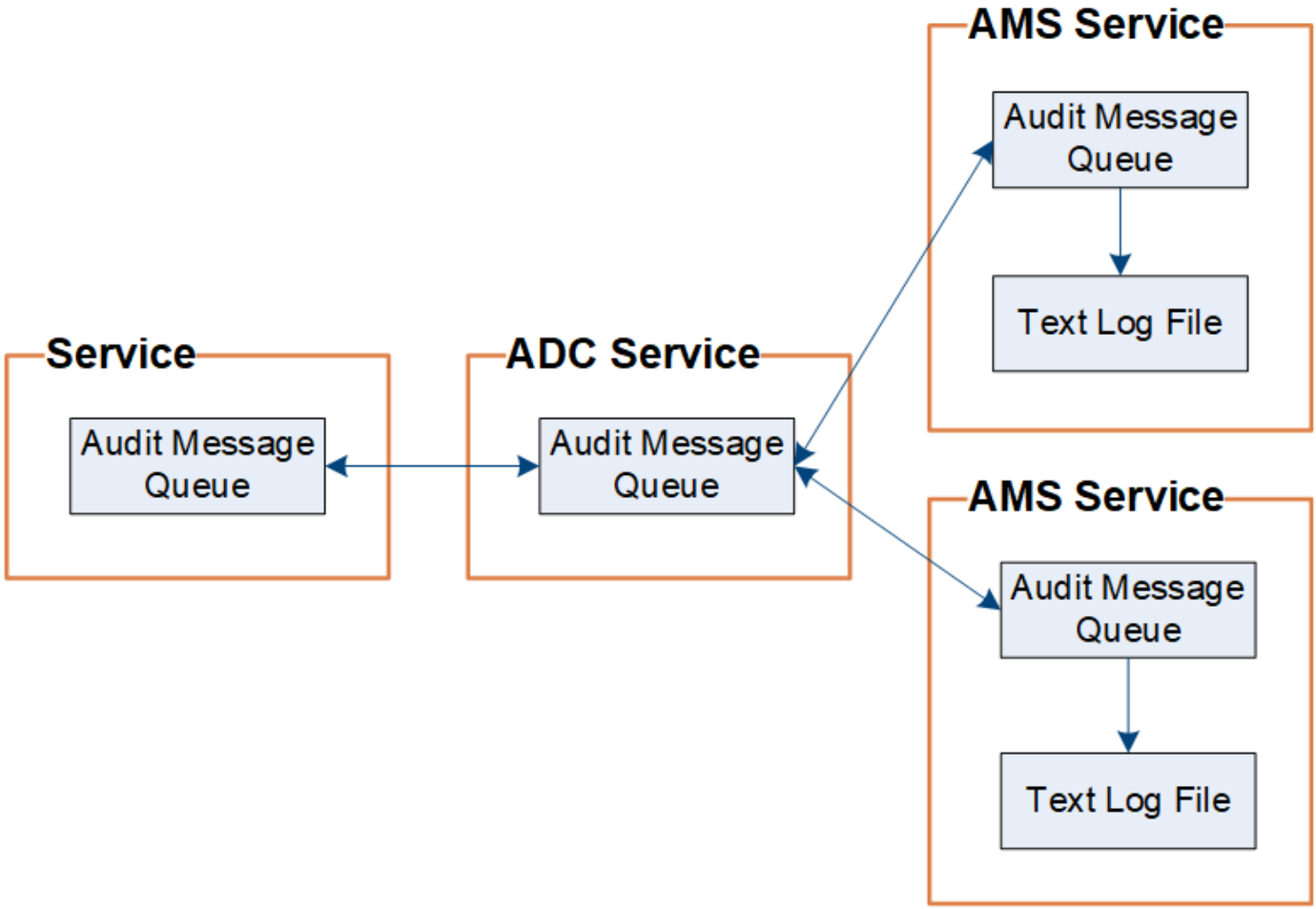
Jeder Admin-Knoten speichert Audit-Meldungen in Text-Log-Dateien; die aktive Protokolldatei wird benannt `audit.log`.



Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschprozess, 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 sind nicht betroffen. 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. S3- und Swift-Client-Anfragen zu anderen Nodes sind nicht betroffen. Der Alarm NRLY (Available Audit Relays) wird ausgelöst, wenn Audit-Relais nicht erreichbar sind.

  > Wenn keine Speicherknoten mit dem ADC-Dienst verfügbar sind, werden die Überwachungsmeldungen von den Speicherknoten lokal gespeichert.

- 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 „“"Ändern der Level von Überwachungsnachrichten".“

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.

Ändern der Level von Überwachungsnachrichten

Sie können die Audiorelevel anpassen, um die Anzahl der im Audit-Protokoll für jede Kategorie von Überwachungsmeldungen aufgezeichneten Audit-Meldungen zu erhöhen oder zu verringern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die im Auditprotokoll aufgezeichneten Überwachungsmeldungen werden basierend auf den Einstellungen auf der Seite **Konfiguration** > **Überwachung** > **Audit** gefiltert.

Sie können für jede der folgenden Meldungskategorien eine andere Überwachungsstufe festlegen:

- **System**: Standardmäßig ist dieser Level auf Normal gesetzt.
- **Speicherung**: Standardmäßig ist diese Ebene auf Fehler gesetzt.

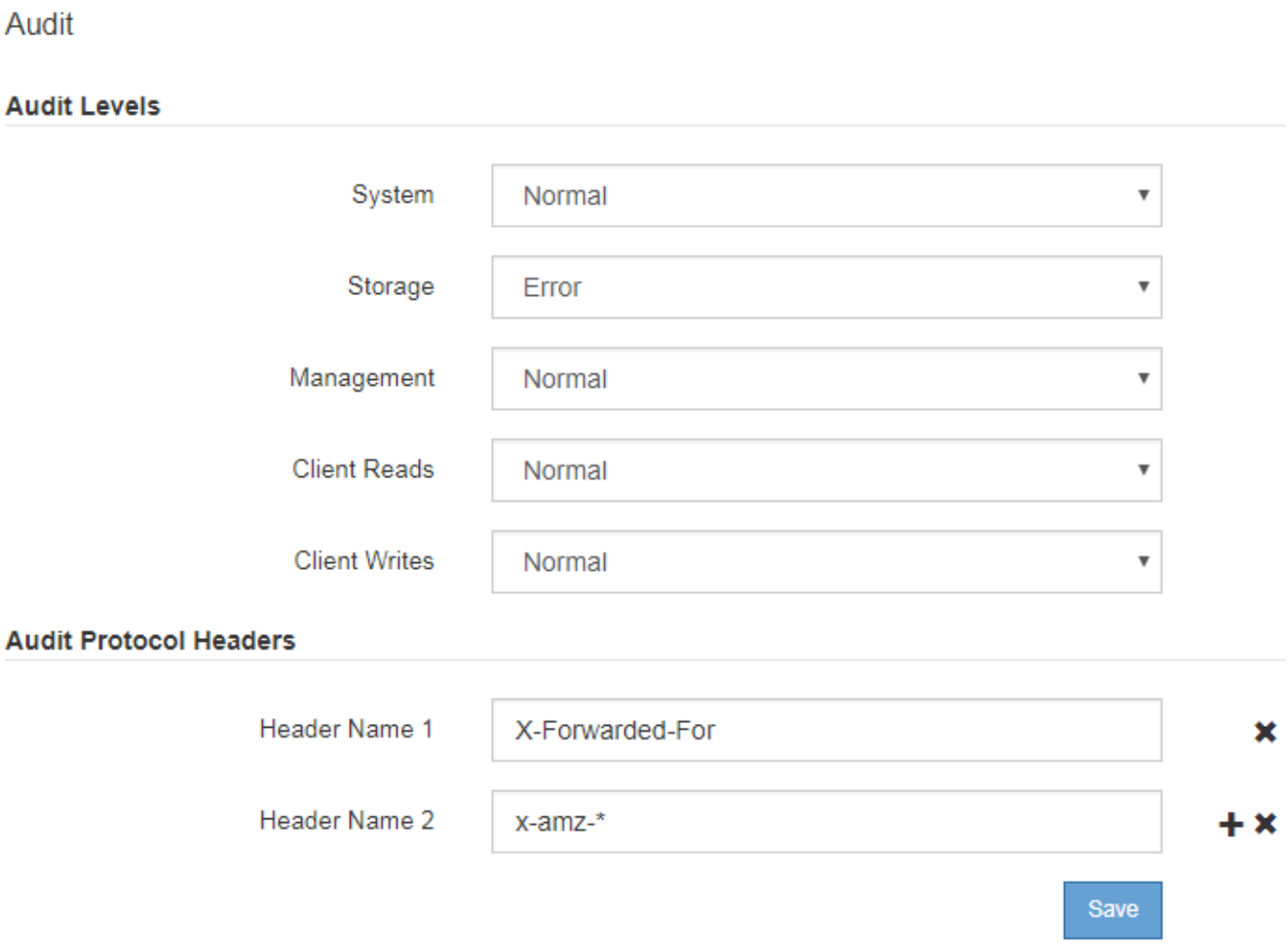
- **Verwaltung**: Standardmäßig ist diese Ebene auf Normal gesetzt.
- **Client liest**: Standardmäßig ist diese Ebene auf Normal gesetzt.
- **Client schreibt**: Standardmäßig ist diese Ebene auf Normal gesetzt.

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 **Konfiguration** > **Überwachung** > **Audit**.



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.
Fehler	Nur Fehlermeldungen sind protokollierte - Audit-Meldungen, für die der Ergebniscode nicht „erfolgreich“ (SUCS) war.

Audit-Level	Beschreibung
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.

3. Geben Sie unter **Audit Protocol Headern** den Namen der HTTP-Request-Header ein, die in den Audit-Meldungen Client Read und Client Write enthalten sein sollen. Verwenden Sie ein Sternchen (*) als Platzhalter, oder verwenden Sie die Escape-Sequenz (*) als wortwörtliche Sternchen. Klicken Sie auf das Pluszeichen, um eine Liste der Kopfzeilennamen-Felder zu erstellen.

   Header für Prüfprotokolle sind nur auf S3 und Swift Anfragen anwendbar.

   Wenn solche 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.

4. Klicken Sie Auf **Speichern**.

Verwandte Informationen

"Systemaudits Meldungen"

"Audit-Meldungen zu Objekt-Storage"

"Management-Audit-Nachricht"

"Client liest Audit-Meldungen"

"StorageGRID verwalten"

Zugriff auf die Audit-Log-Datei

Die Revisionsfreigabe enthält die aktive `audit.log` Datei und alle komprimierten Audit-Log-Dateien. Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf Audit-Shares sowohl für NFS als auch für CIFS (veraltet) konfigurieren. Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Was Sie benötigen

- 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:
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.

Verwandte Informationen

"StorageGRID verwalten"

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`.

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
```

Audit-Log-Datei und Nachrichtenformate

Mit Audit-Protokollen können Informationen zu Ihrem System erfasst und Probleme behoben werden. Sie sollten das Format der Audit-Log-Datei und das allgemeine Format für Audit-Meldungen verstehen.

Format der Auditprotokolldatei

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][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

In ihrem Standardformat sind die Audit-Meldungen in den Audit-Log-Dateien nicht einfach zu lesen oder zu interpretieren. Sie können das verwenden `audit-explain` Tool zum Abrufen vereinfachter Zusammenfassungen der Audit-Meldungen im Audit-Protokoll. Sie können das verwenden `audit-sum` Tool zum Zusammenfassen, wie viele Schreibvorgänge, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

Verwandte Informationen

"Verwenden des Tools zur Erläuterung von Audits"

"Verwenden des Tools Audit-Sum"

Verwenden des Tools zur Erläuterung von Audits

Sie können das verwenden `audit-explain` Tool zum Übersetzen der Audit-Meldungen im Audit-Protokoll in ein einfach zu lesendes Format.

Was Sie benötigen

- 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-Nachrichten 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` Das Tool kann einfache oder komprimierte Prüfprotokolle verarbeiten. Beispiel:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

Der `audit-explain` Das Tool kann auch 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/*
```

Schließlich das `audit-explain` Das Tool kann Eingaben aus einer Leitung annehmen, sodass Sie die Eingabe mit dem filtern und vorverarbeiten können `grep` Befehl oder andere Mittel. Beispiel:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Da Audit-Protokolle sehr groß und langsam zu analysieren sein können, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen 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:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
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 Zeilenlänge zu verringern und die Lesbarkeit zu erleichtern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel anzeigen möchten, verwenden Sie den Zeitstempel (`-t`) Option.

Verwandte Informationen

"SPUT: S3 PUT"

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.

Was Sie benötigen

- 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"

Codieren	Beschreibung	Siehe
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"
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` Das Tool kann einfache oder komprimierte Prüfprotokolle verarbeiten. Beispiel:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

Der `audit-sum` Das Tool kann auch 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/*
```

Schließlich das `audit-sum` Das Tool kann auch Eingaben aus einer Leitung annehmen, sodass Sie die Eingabe mit dem 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:
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           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

In diesem Beispiel sind SGET (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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
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:
   a. 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           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Diese Ergebnisse zeigen, dass 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           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Diese Ergebnisse 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 zur Überprüfung aller 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)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets 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)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Um zu bestimmen, welche Buckets die größte SPUT-Objektgröße haben, verwenden Sie beide `-gb` Und das `-s` Optionen:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Verwandte Informationen

"Verwenden des Tools zur Erläuterung von Audits"

Überwachungsmeldungsformat

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-explain` Und `audit-sum` 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(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

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 `" "`.

Verwandte Informationen

"Verwenden des Tools zur Erläuterung von Audits"

"Verwenden des Tools Audit-Sum"

"Audit-Meldungen"

"Gemeinsame Elemente in Audit-Meldungen"

"Datentypen"

"Beispiele für Überwachungsnachrichten"

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	Vierklarlige Konstante; ein 32-Bit unsigned integer Wert, der als vier ASCII-Zeichen wie "ABCD" dargestellt wird.
IPAD	Wird für IP-Adressen verwendet.

Typ	Beschreibung
CSTR	Ein Array mit variabler Länge von UTF-8 Zeichen. Zeichen können mit den folgenden Konventionen entgangen werden: • 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 Systemereignis spezifisch sind.

Nach der Öffnung `[AUDT:` Container, der die Meldung selbst identifiziert, die nächsten Attribute liefern Informationen über das Ereignis oder die Aktion, die durch die Überwachungsmeldung beschrieben werden. Diese Attribute sind im folgenden Beispiel hervorgehoben:

```
2018-12-05T08:24:45.921845 [AUDT:[RSLT(FC32):SUCS]
[TIME(UI64):11454] [SAIP(IPAD):"10.224.0.100"]
[S3AI(CSTR):"60025621595611246499"]
[SACC(CSTR):"account"]
[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="]
[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]
[SBAI(CSTR):"60025621595611246499"] [SBAC(CSTR):"account"] [S3BK(CSTR):"bucket"]
[S3KY(CSTR):"object"] [CBID(UI64):0xCC128B9B9E428347]
[UUID(CSTR):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"] [CSIZ(UI64):30720]
[AVER(UI32):10]
[ATIM(UI64):1543998285921845] [ATYP(FC32):SHEA] [ANID(UI32):12281045]
[AMID(FC32):S3RQ]
[ATID(UI64):15552417629170647261]]
```

Der `ATYP` Element (unterstrichen im Beispiel) identifiziert, welches Ereignis die Nachricht erzeugt hat. Diese Beispielmeldung enthält den SHEA-Nachrichtencode ([ATYP(FC32):SHEA]), der angibt, dass er von einer erfolgreichen S3-KOPFANFORDERUNG generiert wurde.

Verwandte Informationen

"Gemeinsame Elemente in Audit-Meldungen"

"Audit-Meldungen"

Gemeinsame Elemente in Audit-Meldungen

Alle Meldungen enthalten die allgemeinen Elemente.

Codieren	Typ	Beschreibung
INMITTEN	FC32	Modul-ID: Eine vier-Zeichen-ID der Modul-ID, die die Nachricht generiert hat. Dies gibt das Codesegment an, in dem die Überwachungsmeldung generiert wurde.
ANID	UI32	Node-ID: Die Grid-Node-ID, die dem Service zugewiesen wurde, der die Meldung generiert hat. Jedem Service wird bei Konfiguration und Installation des StorageGRID-Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.
ASES	UI64	Kennung der Auditsitzung: In vorherigen Releases gab dieses Element die Zeit an, zu der das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit der Betriebssystemepoche gemessen (00:00:00 UTC am 1. Januar 1970). **Hinweis:** Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ASQN	UI64	Sequenzanzahl: In vorherigen Releases wurde dieser Zähler für jede erzeugte Überwachungsmeldung auf dem Grid-Node (ANID) erhöht und beim Neustart des Dienstes auf Null zurückgesetzt. **Hinweis:** Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ATID	UI64	Trace-ID: Eine Kennung, die von den Nachrichten, die von einem einzelnen Ereignis ausgelöst wurden, gemeinsam genutzt wird.
ATIM	UI64	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. Möglicherweise ist ein Aufrundung oder Verkürzung des protokollierten Zeitstempels erforderlich. Die lesbare Zeit des Menschen, die zu Beginn der Überwachungsmeldung-angezeigt wird `audit.log` Die Datei ist das ATIM-Attribut im ISO 8601-Format. Das Datum und die Uhrzeit werden als dargestellt *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, Wo der `T` Ist ein Literalzeichenzeichen, das den Beginn des Zeitsegments des Datums angibt. *`UUUUUU`* Nur Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine 4-Zeichen-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.

Codieren	Typ	Beschreibung
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):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Die 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):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Der Wert des ATYP-Attributs ist SPUT. SPUT stellt eine S3-PUT-Transaktion dar, die die Aufnahme eines Objekts in einen Bucket protokolliert.

Die folgende 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):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Um 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 menschliche-lesbare Version des ATIM-Attributs der Prüfmeldung selbst:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM zeichnet die Zeit in Mikrosekunden, seit Beginn der UNIX-Epoche. Im Beispiel der Wert `1405631878959669` Übersetzt bis Donnerstag, 17. Juli 2014 21:17:59 UTC.

Verwandte Informationen

"SPUT: S3 PUT"

"Gemeinsame Elemente in Audit-Meldungen"

Überwachungsmeldungen und der Lebenszyklus von Objekten

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 (S3-Bucket) und/oder S3KY (S3-Schlüssel)
Swift-Vorgänge verknüpfen	WCON (Swift-Container) und/oder WOBJ (Swift-Objekt)

Protokoll	Codieren
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.

Konfiguration der Richtlinien für das Informationslebenszyklus-Management

Bei der ILM-Standardrichtlinie (Baseline 2 Copy) werden Objektdaten einmal für insgesamt zwei Kopien kopiert. Wenn die ILM-Richtlinie mehr als zwei Kopien erfordert, gibt es für jede zusätzliche Kopie einen zusätzlichen Satz von CBRE-, CBSE- und SCMT-Meldungen. Weitere Informationen zu ILM-Richtlinien finden Sie unter Informationen zum Managen von Objekten mit Information Lifecycle Management.

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 Speicherknoten, es sei denn, ES gibt keine SREM (Object Store Remove)-Nachricht und für jede Löschanforderung gibt es eine AREM-Nachricht (Archive Object Remove).

Verwandte Informationen

"Objektmanagement mit ILM"

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"

Codieren	Name	Beschreibung	Verfolgen	Siehe
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 für das Lager, erstellen Sie 2 Kopien.

> 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):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"]<strong
class="S3KY(CSTR):"testobject-0-
3"">[CBID(UI64):0x8EF52DF8025E63A8]</strong>[CSIZ(UI64):30720][AVER(UI32):
10]<strong
class="ATIM(UI64):150032627859669">[ATYP(FC32):SPUT]</strong>[ANID(UI32):1
2086324][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:
<strong>[CBID(UI64):0x50C4F7AC2BC8EDF7]</strong> [RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]<strong class="LOCS(CSTR): *"CLDI 12828634
2148730112">[RSLT(FC32):SUCS][AVER(UI32):10] [ATYP(FC32):ORLM]</strong>
[ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):131
00453][AMID(FC32):BCMS]]
```

Bei Objekten mit Erasure Coding enthält das Feld LOCS die Profile-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][ATYP(FC32):ORLM][ANID(UI32):12355278][AMI
D(FC32):ILMX][ATID(UI64):41685590464737255 60]]
```

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 Löschtransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die zum Verfolgen der Löschtransaktion 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 Löschtransaktion generierten Audit-Meldungen aufgeführt. Es werden nur diejenigen aufgelistet, die mit der S3-Löschtransaktion (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_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"] <strong>[S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
7"][CBID(UI64):0x339F21C5A6964D89]</strong>
[CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669]
<strong>[ATYP(FC32):SDEL]</strong>[ANID(UI32):12086324][AMID(FC32):S3RQ][A
TID(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) abruft, 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(UI
64):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 Beispielmeldung sendet der Client eine GET Object-Anforderung für ein in einem Bucket gespeichertes Objekt, das ihnen nicht gehören. 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"]
<strong>[S3AI(CSTR):"17915054115450519830"][SACC(CSTR):"s3-account-
b"]</strong>[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="]<st
rong
class="SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"">[SBAI(CS
TR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]</strong>[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

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**).

```
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]]
```

Verwandte Informationen

"Ändern der Level von Überwachungsnachrichten"

Audit-Meldungen

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 Auflistung können Sie Informationen zu bestimmten Nachrichten suchen.

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][<stro
ng>ATYP\(FC32\):SYSU</strong>][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(
UI64):9445736326500603516]]
```

Verwandte Informationen

"Audit-Meldungen"

"Ändern der Level von Überwachungsnachrichten"

Kategorien von Überwachungsnachrichten

Sie sollten mit den verschiedenen Kategorien vertraut sein, in denen Audit-Meldungen gruppiert werden. Diese Gruppen sind auf der Grundlage der Aktivitätsklasse organisiert, für die die Nachricht steht.

Systemaudits Meldungen

Sie sollten mit Audit-Meldungen vertraut sein, die zur Systemaudit-Kategorie gehören. Dies sind Ereignisse in Bezug auf das Auditing von Systemen selbst, den Status von Grid-Nodes, systemweite Task-Aktivitäten (Grid-Aufgaben) und Service-Backup-Vorgänge, sodass Sie potenzielle Probleme beheben können.

Codieren	Titel und Beschreibung der Nachricht	Siehe
ECOC	Beschädigte Datenfragment mit Erasure-Code: Zeigt an, dass ein korruptes Datenfragment mit Löschungscode erkannt wurde.	"ECOC: Korrupte, mit Erasure codierte Datenfragment"

Codieren	Titel und Beschreibung der Nachricht	Siehe
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"
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 überschreibtes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Objektbereinigung überschrieben"
LLST	Standort verloren: Diese Überwachungsmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"

Codieren	Titel und Beschreibung der Nachricht	Siehe
OLST	Objekt verloren: Ein angeforderter Gegenstand kann nicht innerhalb des StorageGRID Systems gefunden werden.	"OLST: System hat Lost Object erkannt"
ORLM	Objektregeln erfüllt: Objektdaten werden gemäß den ILM-Regeln gespeichert.	"ORLM: Objektregeln erfüllt"
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"
VLST	Vom Benutzer Initiiertes Volume Verloren: Das `/proc/CMSI/Volume_Lost` Befehl wurde ausgeführt.	"VLST: Vom Benutzer initiiertes Volumen verloren"

Verwandte Informationen

"LKCU: Objektbereinigung überschrieben"

Sie sollten mit Audit-Meldungen vertraut sein, die zur Objektspeicheraudits-Kategorie gehören. Dies sind Ereignisse, die mit der Speicherung und dem Management von Objekten innerhalb des StorageGRID Systems zusammenhängen. 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"
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"

Codieren	Beschreibung	Siehe
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"
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"
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"SCMT: Objekt Store Commit"
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
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-Clients Swift Clients	"OVWR: Objektüberschreibung"

Codieren	Beschreibung	Verwendet von	Siehe
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"

Codieren	Beschreibung	Verwendet von	Siehe
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"

Audit-Meldungen

Wenn Systemereignisse auftreten, generiert das StorageGRID System Audit-Meldungen und zeichnet sie im Revisionsprotokoll auf.

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	Die Kennung des Volumes, auf dem die Daten archiviert wurden.Wenn kein Archivverzeichnis für den Inhalt gefunden wird, wird eine Volume-ID von 0 zurückgegeben.

Codieren	Feld	Beschreibung
RSLT	Abrufergebnis	Der Abschlussstatus des Archivabrufs: • 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: • 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.

Codieren	Feld	Beschreibung
VREN	Überprüfung Aktiviert	Zeigt an, ob eine Überprüfung für Inhaltsblöcke durchgeführt wird. Aktuell definierte Werte sind: • 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: • 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.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
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: • 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.

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	Verbindungskennung	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.
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	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	Verbindungskennung	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	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 endete aufgrund des Empfangs von beschädigten oder ungültigen Daten (kann auf Manipulation hinweisen)

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	Verbindungskennung	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.
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.

Codieren	Feld	Beschreibung
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.

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	Verbindungskennung	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.
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.

Codieren	Feld	Beschreibung
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 endete aufgrund des Empfangs von beschädigten oder ungültigen Daten (kann auf Manipulation hinweisen)

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.

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	Verbindungskennung	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.

Codieren	Feld	Beschreibung
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-Profils 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 Remoteineinheit 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: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.
GNTP	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: • 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.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: • SUCS: Die Grid-Aufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne einen Rollback-Fehler abgebrochen. • ROLF: Die Grid-Aufgabe wurde abgebrochen 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: • 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.

Codieren	Feld	Beschreibung
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.
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: • 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: • 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: • 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.
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 Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
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.
REGEL	Regelbezeichnung	• 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.

Codieren	Feld	Beschreibung
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. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

LKCU: Objektbereinigung überschrieben

Diese Meldung wird generiert, wenn StorageGRID ein überschreibtes 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	*Nur zur internen Verwendung.*
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.
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 erzeugt, wenn ein Speicherort für eine Objektkopie (repliziert oder Erasure Coding) nicht gefunden werden kann.

Codieren	Feld	Beschreibung
CBIL	CBID	Die betroffene CBID.
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
UUID	Universally Unique ID	Die Kennung des betroffenen Objekts im StorageGRID-System.
ECPR	Verfahren Zur Einhaltung Von Datenkonsistenz	Für Erasure-Coding-Objektdaten. Die ID des verwendeten Erasure Coding-Profils.
LTYP	Positionstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für Erasure-codierte Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten
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 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
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

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	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: • 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** **Hinweis:** sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MRMD	Anforderungsmethode	Die HTTP-Anforderungsmethode: • POST • PUT • Löschen • PATCH

Codieren	Feld	Beschreibung
MRSC	Antwortcode	Der Antwortcode.
MRSP	Antwortkörper	Der Inhalt der Antwort (der Antwortkörper) wird standardmäßig protokolliert. **Hinweis:** sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MSIP	Quell-IP-Adresse	Die Client (Quell-) IP-Adresse.
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 erzeugt, 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, der letzte bekannte direkte oder Nearline-Speicherort 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.

Codieren	Feld	Beschreibung
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
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.

Codieren	Feld	Beschreibung
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.
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 verfügbar, wenn das Objekt segmentiert ist.

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.

Die ORLM-Überwachungsmeldung kann für ein einzelnes Objekt mehrmals ausgegeben werden. Sie wird beispielsweise ausgegeben, wenn eines der folgenden Ereignisse stattfindet:

- 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

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.
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.
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 Anfrage gestellt, um das angegebene Objekt oder den angegebenen Bucket 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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.

Codieren	Feld	Beschreibung
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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (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-Mandantenkontoname (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.

Codieren	Feld	Beschreibung
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 gelöscht wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SGET S3 ABRUFEN

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anfrage gestellt, um ein Objekt abzurufen oder die Objekte in einem Bucket 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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
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

Codieren	Feld	Beschreibung
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (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-Mandantenkontoname (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.

Codieren	Feld	Beschreibung
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. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des überprüften Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).

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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
SACC	S3-Mandantenkontoname (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-Mandantenkontoname (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.

Codieren	Feld	Beschreibung
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. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SPOS: S3-BEITRAG

Wenn ein S3-Client eine Anfrage zur WIEDERHERSTELLUNG NACH dem Objekt ausgibt, wird eine Anfrage gestellt, um ein Objekt aus AWS Glacier Storage in einem Cloud Storage Pool wiederherzustellen. 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.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
RSLT	Ergebniscode	Ergebnis der Anforderung ZUR Wiederherstellung DES POSTOBJEKTS. 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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend

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.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (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: `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.

Codieren	Feld	Beschreibung
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Buckets 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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern diese in der PUT Bucket-Anforderung vorhanden sind (gekürzt 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	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
LKEN	Objektsperre Aktiviert	Der Wert der Anfrageüberschrift `x-amz-bucket-object-lock-enabled`, Wenn vorhanden in DER PUT Bucket Anforderung.
LKLH	Gesetzliche Sperren Für Objekte	Der Wert der Anfrageüberschrift `x-amz-object-lock-legal-hold`, Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKMD	Aufbewahrungsmodus Für Objektsperre	Der Wert der Anfrageüberschrift `x-amz-object-lock-mode`, Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKRU	Objektsperre Bis Datum Beibehalten	Der Wert der Anfrageüberschrift `x-amz-object-lock-retain-until-date`, 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.

Codieren	Feld	Beschreibung
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	S3KY	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (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-Mandantenkontoname (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	Die neue Subressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).

Codieren	Feld	Beschreibung
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.
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 Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.
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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert des HTTP-Anfrageheaders Consistency-Control, falls in der Anfrage vorhanden, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
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. Dieses Feld ist nicht in Operationen in Buckets enthalten.
SACC	S3-Mandantenkontoname (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-Mandantenkontoname (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 Versionsnummer der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

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 erneuten Abruf der Daten zu verhindern.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, bei der die Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Fehlertyp Verifikation: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Prüfung des Hashbasierten Nachrichtenauthentifizierungscodes (HMAC) fehlgeschlagen. EHSH: Unerwarteter verschlüsselter Content-Hash. PHSH: Unerwarteter Originalinhalt Hash. SEQC: Falsche Datensequenz auf der Festplatte. PERR: Ungültige Struktur der Festplattendatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.

Hinweis: Diese Nachricht sollte genau überwacht werden. Fehler bei der Inhaltsprüfung können auf Manipulationen an Inhalten oder 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.

Hinweis: die SVRU: Objektspeicher überprüfen Unbekannte Überwachungsmeldung 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 den Versuch hinweisen können, Inhalte zu manipulieren oder Hardware-Ausfälle anzufangen.

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 späteren Neustart gesendet, da die Warteschlange für die Überwachungsmeldung 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. Das RSLT eines SYSD kann nicht auf ein „nicht ordnungsgemäßes“ 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 „nicht ordnungsgemäßes“ 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 (befahl) 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.

VLST: Vom Benutzer initiiertes Volumen verloren

Diese Meldung wird ausgegeben, wenn der `/proc/CMSI/Volume_Lost` Befehl wird ausgeführt.

Codieren	Feld	Beschreibung
VOLL	Volume Identifier Lower	Das untere Ende des betroffenen Volumenbereichs oder eines einzelnen Volumens.

Codieren	Feld	Beschreibung
VOLU	Volume Identifier Ober	Das obere Ende des betroffenen Volumenbereichs. Gleich VOLL wenn ein einzelnes Volume ist.
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
LTYP	Positionstyp	„CLDI“ (Online) oder „CLNL“ (Nearline). Wenn nicht angegeben, ist die Standardeinstellung „CLDI“.
RSLT	Ergebnis	Immer „KEINE“. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

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. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
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.
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. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.

Codieren	Feld	Beschreibung
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. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
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.

Codieren	Feld	Beschreibung
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. Dieses Feld wird nicht von Operationen für Accounts berücksichtigt.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
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. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
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. Dieses Feld wird nicht von Operationen für Accounts berücksichtigt.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.

Codieren	Feld	Beschreibung
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. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `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).
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

Codieren	Feld	Beschreibung
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. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

Wartung

Erweitern Sie Ihr Raster

Erfahren Sie, wie Sie ein StorageGRID System ohne Unterbrechung des Systembetriebs erweitern können.

- "StorageGRID-Erweiterung geplant"
- "Vorbereitung auf eine Erweiterung"
- "Überblick über das Expansionsverfahren"
- "Hinzufügen von Storage-Volumes zu Storage-Nodes"
- "Einem vorhandenen Standort Grid-Nodes hinzufügen oder einen neuen Standort hinzufügen"
- "Konfiguration des erweiterten StorageGRID-Systems"
- "Kontakt mit dem technischen Support"

StorageGRID-Erweiterung geplant

StorageGRID lässt sich erweitern, um die Storage-Kapazität zu erhöhen, Metadaten hinzuzufügen, Redundanz oder neue Funktionen hinzuzufügen oder einen neuen Standort hinzuzufügen. Die Anzahl, der Typ und der Standort der Nodes, die Sie hinzufügen müssen, hängt vom Grund der Erweiterung ab.

- "Erweiterung der Storage-Kapazität"
- "Hinzufügen von Metadaten-Kapazität"
- "Grid-Nodes werden hinzugefügt, um Funktionen zu Ihrem System hinzuzufügen"
- "Hinzufügen eines neuen Standorts"

Erweiterung der Storage-Kapazität

Wenn vorhandene Storage-Nodes voll werden, müssen Sie die Storage-Kapazität Ihres StorageGRID Systems erhöhen.

Um die Storage-Kapazität zu erhöhen, müssen Kunden zunächst verstehen, wo die Daten aktuell gespeichert sind, und dann alle erforderlichen Kapazitäten erweitern. Wenn Sie beispielsweise derzeit Kopien von Objektdaten an mehreren Standorten speichern, muss die Storage-Kapazität jedes Standorts erhöht werden.

- "Richtlinien zum Hinzufügen von Objektkapazität"
- "Hinzufügen von Speicherkapazität für replizierte Objekte"
- "Hinzufügen von Storage-Kapazität für Objekte mit Erasure-Coding-Verfahren"
- "Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind"

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 festzustellen, wo und wann Storage-Volumes hinzugefügt werden müssen, um die Storage-Kapazität für replizierte oder Erasure-codierte Objekte zu erhöhen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.
- Die Metadatenkapazität des Systems kann nicht durch Hinzufügen von Storage-Volumes erhöht werden, da Objektmetadaten 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.
- Sie können keine Speicher-Volumes zu einer anderen Speicher-Appliance hinzufügen.
- Sie können die Größe eines vorhandenen Speichervolumens nicht erhöhen.
- Sie können Storage-Volumes nicht gleichzeitig einem Storage-Node hinzufügen, wenn Sie ein System-Upgrade, Recovery-Vorgang 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:

- Informationen zum Hinzufügen von Erweiterungs-Shelfs zu einer SG6060-Speicher-Appliance finden Sie in den Anweisungen zur Installation und Wartung der SG6000-Appliance.

  "SG6000 Storage-Appliances"

- Befolgen Sie die Anweisungen zum Hinzufügen von Storage-Volumes zu Storage-Nodes, 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 festzustellen, wo und wann Storage-Nodes hinzugefügt werden müssen, um den Storage für replizierte oder Erasure-codierte Objekte zu erhöhen.
- 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 Erweiterungsvorgang beginnen, müssen Sie bestätigen, dass alle Datenreparaturvorgänge, die im Rahmen einer Wiederherstellung durchgeführt werden, abgeschlossen sind. Siehe die Schritte zum Überprüfen von Datenreparaturjobs in den Anweisungen für Wiederherstellung und Wartung.
- 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 den ADC-Service auf Speicherknoten

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, dass an jedem Standort und zu jeder Zeit ein Quorum von ADC-Services verfügbar ist.

  Erfahren Sie mehr über das ADC-Quorum in den Anweisungen zur Wiederherstellung und Wartung.

- 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 sichergestellt, dass ein neuer ADC-Service verfügbar ist, bevor der alte Service entfernt wird.
- Der ADC-Dienst kann nicht einem Node hinzugefügt werden, nachdem er bereitgestellt wurde.

Verwandte Informationen

"Objektmanagement mit ILM"

"SG6000 Storage-Appliances"

"Hinzufügen von Storage-Volumes zu Storage-Nodes"

"Verwalten Sie erholen"

"Durchführung der Erweiterung"

Hinzufügen von Speicherkapazität für replizierte Objekte

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 Sie ein Grid mit zwei Standorten und eine ILM-Regel haben, die an jedem Standort eine Objektkopie erstellt, müssen Sie jedem Standort Storage hinzufügen, um die allgemeine Objektkapazität des Grids zu erhöhen.

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. Mit dem Grid Manager können Sie die Storage-Kapazität überwachen und Diagramm verwenden, wie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID beschrieben.

Denken Sie bei der Planung des Zeitpunkts einer Erweiterung daran, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern könnte.

Verwandte Informationen

"Objektmanagement mit ILM"

"Monitor Fehlerbehebung"

Hinzufügen von Storage-Kapazität für Objekte mit Erasure-Coding-Verfahren

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 einen Site-Loss-Schutz bietet, müssen Sie jedem Standort Storage hinzufügen.

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.

Um die Faktoren, die zu dieser Empfehlung führen, besser zu verstehen oder einen genaueren Plan für Ihren Standort zu entwickeln, überprüfen Sie den nächsten Abschnitt. Wenden Sie sich an Ihren NetApp Ansprechpartner, um eine für Ihre Situation optimierte Empfehlung zu erhalten.

Berechnung der Anzahl der zu addierenden Erweiterungs-Speicherknoten für Objekte mit Löschungscode

Um die Erweiterung einer Implementierung zur Speicherung von Objekten, die mit Erasure-Coding-Verfahren codiert wurden, zu optimieren, müssen Sie viele Faktoren berücksichtigen:

- Verwendung eines Schemas zur Einhaltung von Datenkonsistenz (Erasure Coding)
- Merkmale des für das Verfahren zur Einhaltung von Datenkonsistenz verwendeten Storage Pools, einschließlich der Anzahl der Nodes an jedem Standort und der Menge an freiem Speicherplatz auf jedem Node
- Gibt an, ob das Grid zuvor erweitert wurde (da sich der freie Speicherplatz pro Storage-Node möglicherweise nicht in etwa auf allen Nodes identisch befindet)
- Die genaue Natur der ILM-Richtlinie, beispielsweise darüber, ob ILM-Regeln replizierte und Erasure-Coding-Objekte erstellen

Die folgenden Beispiele zeigen, welche Auswirkungen das Erasure Coding-Schema hat, die Anzahl der Nodes im Storage-Pool und die Menge an freiem Speicherplatz auf jedem Node.

Ähnliche Überlegungen wirken sich auf die Berechnungen für eine ILM-Richtlinie aus, die sowohl replizierte Daten als auch Daten mit Erasure-Coding-Verfahren speichert und die Berechnungen für ein zuvor erweitertes Grid enthält.

> ⓘ Die Beispiele in diesem Abschnitt stellen die Best Practices für das Hinzufügen von Speicherkapazität zu einem StorageGRID System dar. Wenn Sie die empfohlene Anzahl an Nodes nicht hinzufügen können, müssen Sie möglicherweise das EC-Ausgleichverfahren durchführen, um zusätzliche, mit Erasure Coding versehenen Objekte zu speichern.
>
> "Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind"

Beispiel 1: Erweiterung eines Grid mit einem Standort, das 2+1 Erasure Coding verwendet

Dieses Beispiel zeigt, wie ein einfaches Raster erweitert wird, das nur drei Storage-Nodes enthält.

> ⓘ Dieses Beispiel verwendet nur drei Storage-Nodes zur Vereinfachung. Es wird jedoch nicht empfohlen, nur drei Speicherknoten zu verwenden: Ein tatsächliches Produktionsnetz sollte mindestens *k*+*m* + 1 Speicherknoten verwenden, um Redundanz zu erhalten, was vier Speicherknoten (2+1+1) entspricht.

Gehen Sie folgendermaßen vor:

- Alle Daten werden mithilfe des 2+1-Schemas zur Einhaltung von Datenkonsistenz gespeichert. Mit dem Erasure Coding-Schema 2+1 wird jedes Objekt als drei Fragmente gespeichert und jedes Fragment auf einem anderen Storage Node gespeichert.
- Es gibt einen Standort mit drei Storage-Nodes. Jeder Storage-Node hat eine Gesamtkapazität von 100 TB.

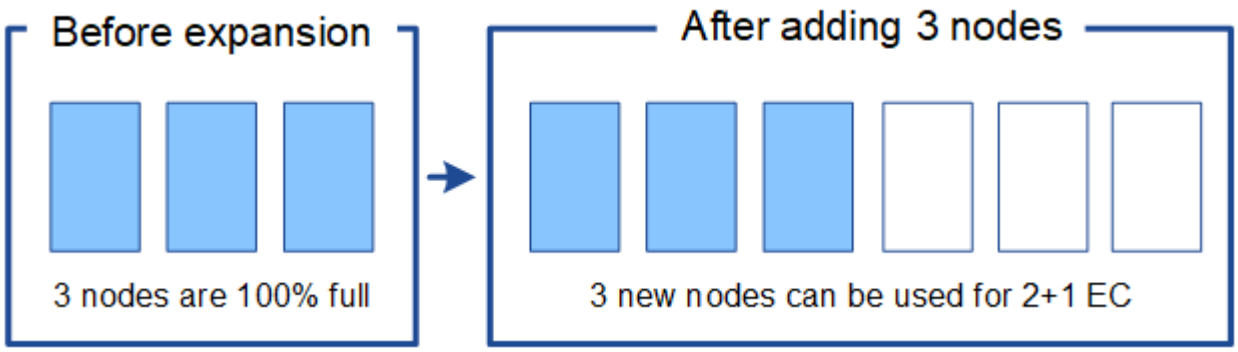
- Sie möchten erweitern, indem Sie neue 100-TB-Storage-Nodes hinzufügen.
- Ziel ist es, mithilfe von Erasure Coding Daten auf die alten und neuen Nodes einen Ausgleich zu finden.

Je nachdem, wie voll die Speicherknoten sind, wenn Sie die Erweiterung durchführen, stehen verschiedene Optionen zur Verfügung.

- **Fügen Sie drei 100 TB Storage Nodes hinzu, wenn die vorhandenen Knoten zu 100% voll sind**

  In diesem Beispiel sind die vorhandenen Nodes zu 100 % ausgelastet. Da keine freie Kapazität vorhanden ist, müssen Sie sofort drei Nodes hinzufügen, um mit dem Erasure Coding von 2+1 fortzufahren.

  Nach Abschluss der Erweiterung werden bei Erasure-Coding von Objekten alle Fragmente auf die neuen Nodes platziert.

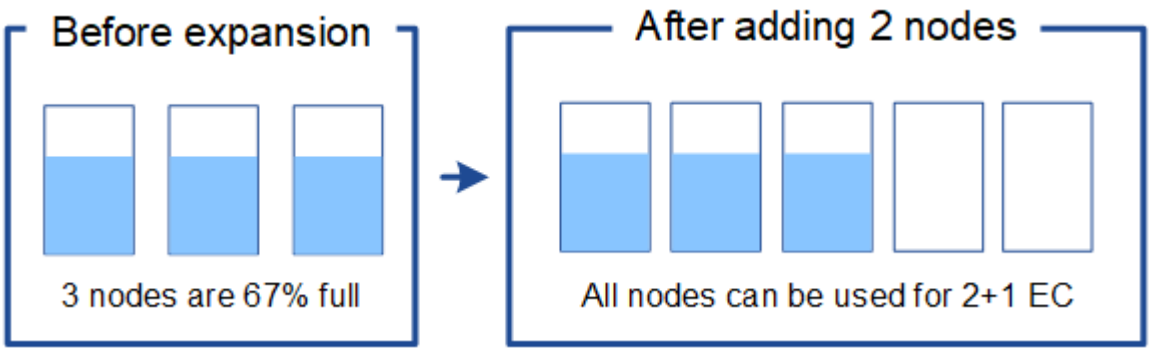


> Durch diese Erweiterung werden Nodes *k+m* hinzugefügt. Das Hinzufügen von vier Nodes wird aus Redundanzgründen empfohlen. Wenn Sie Storage-Nodes mit *k+m*-Erweiterung hinzufügen, wenn vorhandene Nodes zu 100 % voll sind, müssen alle neuen Objekte auf den Erweiterungs-Nodes gespeichert werden. Wenn einer der neuen Nodes nicht verfügbar ist, kann StorageGRID die ILM-Anforderungen selbst vorübergehend nicht erfüllen.

- **Fügen Sie zwei 100 TB Storage-Nodes hinzu, wenn die vorhandenen Storage-Nodes zu 67 % voll sind**

  In diesem Beispiel sind die vorhandenen Nodes zu 67 % ausgelastet. Da auf den vorhandenen Nodes 100 TB an freier Kapazität verfügbar sind (33 TB pro Node), müssen Sie nur noch zwei Nodes hinzufügen, wenn Sie die Erweiterung jetzt durchführen.

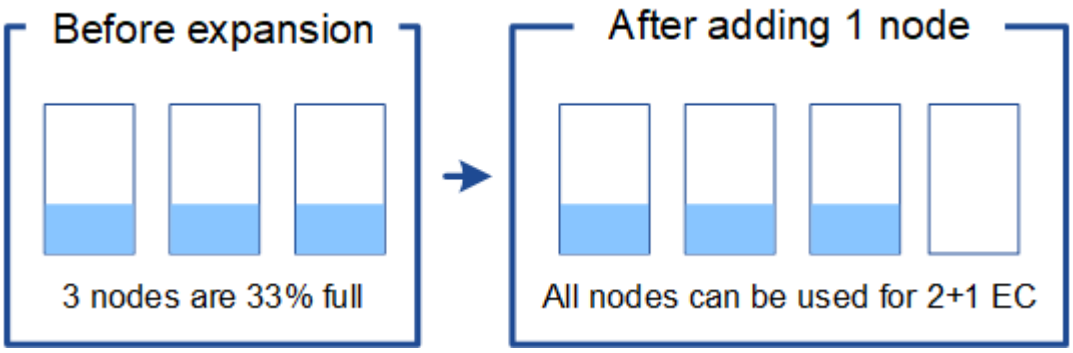
  Wenn Sie 200 TB zusätzliche Kapazität hinzufügen, können Sie das 2+1 Erasure Coding fortsetzen und die Daten, die mit Erasure Coding versehen sind, auf allen Nodes einen Ausgleich finden.



- **Fügen Sie einen 100 TB Storage Node hinzu, wenn die vorhandenen Speicherknoten zu 33% voll sind**

  In diesem Beispiel sind die vorhandenen Nodes zu 33 % ausgelastet. Da auf den vorhandenen Nodes 200 TB an freier Kapazität verfügbar sind (67 TB pro Node), müssen Sie nur noch einen Node hinzufügen, wenn Sie die Erweiterung jetzt durchführen.

  Wenn Sie 100 TB zusätzliche Kapazität hinzufügen, können Sie das 2+1 Erasure Coding fortsetzen und die Daten, die mit Erasure Coding versehen sind, auf allen Nodes einen Ausgleich finden.



Beispiel 2: Erweiterung eines Grids für drei Standorte, das Erasure Coding für 6+3 verwendet

Dieses Beispiel zeigt, wie ein Erweiterungsplan für ein Grid mit mehreren Standorten entwickelt wird, das über ein Erasure Coding-Schema mit einer größeren Anzahl von Fragmenten verfügt. Trotz der Unterschiede zwischen diesen Beispielen ist der empfohlene Erweiterungsplan sehr ähnlich.

Gehen Sie folgendermaßen vor:

- Alle Daten werden mithilfe des Erasure Coding-Schemas von 6+3 gespeichert. Mit dem Erasure Coding-Schema 6+3 wird jedes Objekt als 9 Fragmente gespeichert und jedes Fragment wird auf einem anderen Storage Node gespeichert.
- Sie verfügen über drei Standorte und jeder Standort hat vier Storage-Nodes (insgesamt 12 Nodes). Jeder Node hat eine Gesamtkapazität von 100 TB.
- Sie möchten erweitern, indem Sie neue 100-TB-Storage-Nodes hinzufügen.
- Ziel ist es, mithilfe von Erasure Coding Daten auf die alten und neuen Nodes einen Ausgleich zu finden.

Je nachdem, wie voll die Speicherknoten sind, wenn Sie die Erweiterung durchführen, stehen verschiedene Optionen zur Verfügung.

- **Fügen Sie neun 100 TB Storage-Nodes (drei pro Standort) hinzu, wenn vorhandene Knoten zu 100 % voll sind**

  In diesem Beispiel sind die 12 vorhandenen Nodes zu 100 % ausgelastet. Da keine freie Kapazität zur Verfügung steht, müssen Sie sofort neun Nodes (900 TB zusätzliche Kapazität) hinzufügen, um mit dem Erasure Coding für 6+3 fortzufahren.

  Nach Abschluss der Erweiterung werden bei Erasure-Coding von Objekten alle Fragmente auf die neuen Nodes platziert.

Durch diese Erweiterung werden Nodes *k+m* hinzugefügt. Das Hinzufügen von 12 Nodes (vier pro Standort) wird aus Redundanzgründen empfohlen. Wenn Sie Storage-Nodes mit *k+m*-Erweiterung hinzufügen, wenn vorhandene Nodes zu 100 % voll sind, müssen alle neuen Objekte auf den Erweiterungs-Nodes gespeichert werden. Wenn einer der neuen Nodes nicht verfügbar ist, kann StorageGRID die ILM-Anforderungen selbst vorübergehend nicht erfüllen.

- **Hinzufügen von sechs 100 TB Storage-Nodes (zwei pro Standort), wenn vorhandene Knoten zu 75 % voll sind**

  In diesem Beispiel sind die 12 vorhandenen Nodes zu 75 % ausgelastet. Da 300 TB freie Kapazität (25 TB pro Node) zur Verfügung stehen, müssen Sie nur sechs Nodes hinzufügen, wenn Sie die Erweiterung jetzt durchführen. Sie würden jedem der drei Standorte zwei Nodes hinzufügen.

  Wenn Sie 600 TB Storage-Kapazität hinzufügen, können Sie das Erasure Coding von 6 und 3 fortsetzen und einen Ausgleich für Daten mit Erasure Coding auf allen Nodes erzielen.

- **Fügen Sie drei 100 TB Storage-Nodes (einer pro Standort) hinzu, wenn vorhandene Knoten zu 50 % voll sind**

  In diesem Beispiel sind die 12 vorhandenen Nodes zu 50 % ausgelastet. Da 600 TB freie Kapazität (50 TB pro Node) zur Verfügung stehen, müssen Sie nur drei Nodes hinzufügen, wenn Sie die Erweiterung jetzt durchführen. Sie würden jedem der drei Standorte einen Node hinzufügen.

  Wenn Sie 300 TB Storage-Kapazität hinzufügen, können Sie das Erasure Coding von 6 und 3 fortsetzen und einen Ausgleich für Daten mit Erasure Coding auf allen Nodes erzielen.

Verwandte Informationen

"Objektmanagement mit ILM"

"Monitor Fehlerbehebung"

"Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind"

Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind

Wenn Sie eine Erweiterung zum Hinzufügen von Storage-Nodes durchführen und Ihre ILM-Richtlinie eine oder mehrere ILM-Regeln zum Löschen von Code-Daten enthält, müssen Sie nach Abschluss der Erweiterung möglicherweise das EC-Ausgleichverfahren durchführen.

Wenn Sie beispielsweise nicht die empfohlene Anzahl von Speicherknoten in einer Erweiterung hinzufügen können, müssen Sie möglicherweise das EC-Ausgleichverfahren ausführen, damit zusätzliche Objekte mit Löschungscode gespeichert werden können.

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. Bei Ausführung des EC-Ausgleichs verteilt StorageGRID Fragmente, die mit Erasure Coding codiert wurden, auf die vorhandenen und neu erweiterten Storage-Nodes an einem Standort.

Wenn das EC-Ausgleichverfahren ausgeführt wird:

- Es werden nur Objektdaten verschoben, die mit Erasure-Coding-Verfahren codiert wurden. Es werden keine replizierten Objektdaten verschoben.
- Die Daten werden an einem Standort neu verteilt. Es werden keine Daten zwischen Standorten verschoben.
- Die Daten werden auf alle Storage-Nodes an einem Standort verteilt. Daten werden nicht innerhalb von Storage Volumes neu verteilt.

Wenn das EC-Ausgleichverfahren abgeschlossen ist:

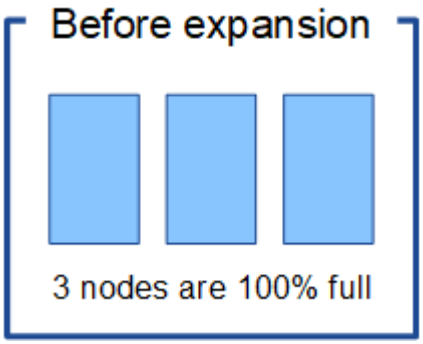
- Die Daten, die mithilfe von Erasure-Coding-Verfahren codiert wurden, werden von Storage-Nodes mit weniger verfügbarem Speicherplatz zu Storage-Nodes mit mehr verfügbarem Speicherplatz verschoben.
- Verwendete (%) Werte können sich zwischen Storage Nodes unterscheiden, da der EC-Ausgleichvorgang keine replizierten Objektkopien verschiebt.
- Die Datensicherung von Objekten, die mit Erasure Coding versehen sind, wird unverändert beibehalten.

Wenn das EC-Ausgleichverfahren ausgeführt wird, ist die Performance von ILM-Vorgängen sowie S3- und Swift-Client-Operationen wahrscheinlich beeinträchtigt. Aus diesem Grund sollten Sie dieses Verfahren nur in begrenzten Fällen durchführen.

Wann sollte ein EC-Ausgleich nicht durchgeführt werden

Als Beispiel für den Fall, dass Sie keinen EC-Ausgleich durchführen müssen, sollten Sie Folgendes berücksichtigen:

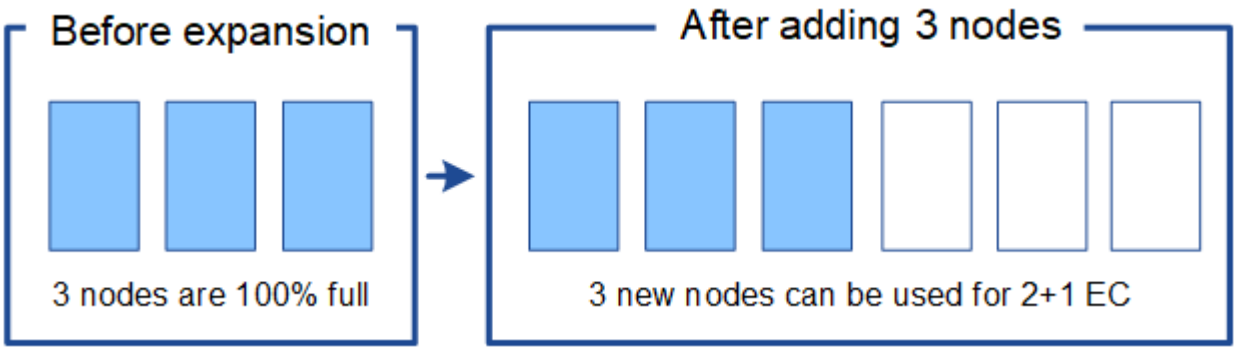
- StorageGRID wird an einem Standort ausgeführt, der drei Storage-Nodes enthält.
- Die ILM-Richtlinie verwendet eine 2+1-Regel zur Einhaltung von Datenkonsistenz für alle Objekte, die größer als 0.2 MB sind, und eine Replizierungsregel mit 2 Kopien für kleinere Objekte.
- Alle Speicherknoten sind voll geworden, und die Warnung **Low Object Storage** wurde auf dem Hauptschweregrade ausgelöst. Die empfohlene Aktion ist, eine Erweiterungsmaßnahme zum Hinzufügen von Speicherknoten durchzuführen.



Um den Standort in diesem Beispiel zu erweitern, wird empfohlen, drei oder mehr neue Speicherknoten hinzuzufügen. StorageGRID benötigt drei Storage-Nodes für das Erasure Coding von 2+1, damit die zwei Datenfragmente und das ein Paritätsfragment auf verschiedenen Nodes platziert werden können.

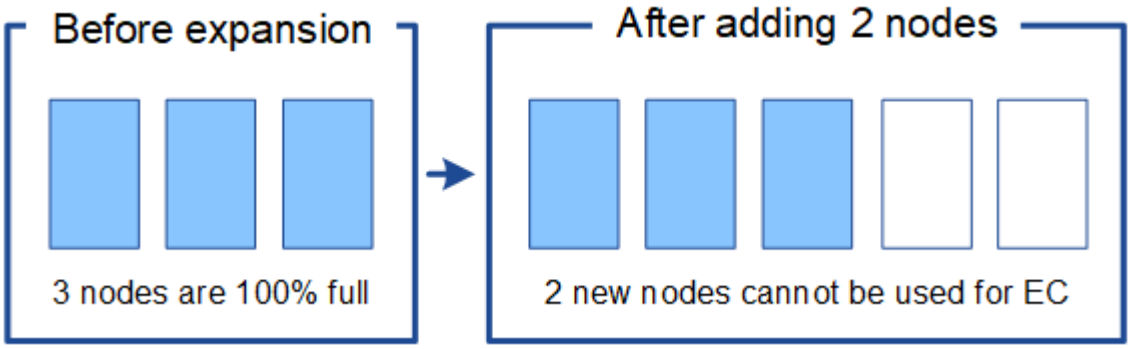
Nachdem Sie die drei Storage-Nodes hinzugefügt haben, bleiben die ursprünglichen Storage-Nodes voll, die Objekte können jedoch weiterhin in das Erasure Coding-Schema 2+1 auf den neuen Nodes aufgenommen werden. Das Ausführen des EC-Ausgleichs-Verfahrens wird in diesem Fall nicht empfohlen: Durch das

Ausführen des Verfahrens wird die Performance vorübergehend verringert, was sich auf den Client-Betrieb auswirken könnte.

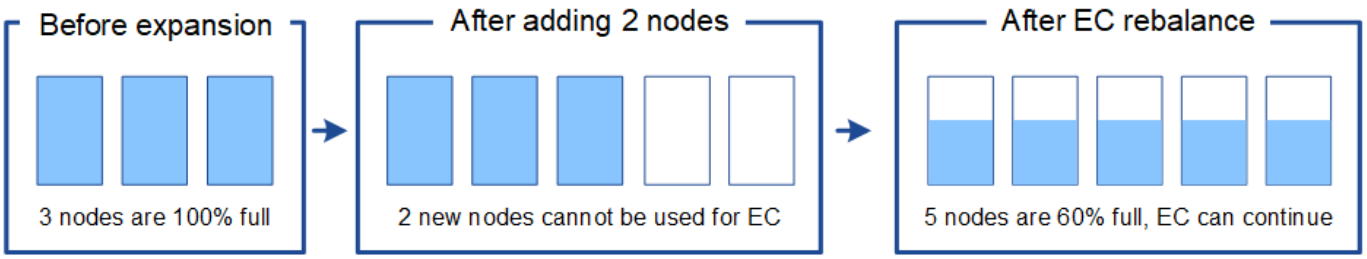


Wann muss ein EC-Ausgleich durchgeführt werden

Als Beispiel für den Fall, dass Sie den EC-Ausgleichvorgang durchführen sollten, betrachten Sie das gleiche Beispiel, gehen Sie aber davon aus, dass Sie nur zwei Storage-Nodes hinzufügen können. Da für das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) 2+1 mindestens drei Storage-Nodes erforderlich sind, können die neuen Nodes nicht für Daten mit Erasure Coding verwendet werden.



Um dieses Problem zu lösen und die neuen Speicherknoten zu nutzen, können Sie das EC-Ausgleichverfahren ausführen. Im Rahmen dieses Verfahrens StorageGRID werden Daten und Paritätsfragmente, die mit Datenkonsistenz (Erasure Coding) versehen werden, auf alle Storage-Nodes am Standort neu verteilt. 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.



Überlegungen zur Neuausrichtung der EG

Im Allgemeinen sollten Sie nur in begrenzten Fällen das EC-Ausgleichverfahren durchführen. Insbesondere sollten Sie eine Neuausrichtung der EG nur durchführen, wenn alle folgenden Aussagen wahr sind:

- 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 die empfohlene Anzahl neuer Speicherknoten für das verwendete Erasure-Coding-Schema nicht hinzufügen.

  "Hinzufügen von Storage-Kapazität für Objekte mit Erasure-Coding-Verfahren"

- Während das EC-Ausgleichverfahren läuft, tolerieren Ihre S3- und Swift-Clients eine niedrigere Performance bei Schreib- und Leseoperationen.

Wie das EC-Ausgleichungsverfahren mit anderen Wartungsaufgaben interagiert

Sie können bestimmte Wartungsverfahren nicht gleichzeitig durchführen, während Sie das EC-Ausgleichverfahren ausführen.

Verfahren	Während des EC-Ausgleichs erlaubt?
Weitere EC-Ausgleichverfahren	Nein Sie können nur ein EC-Ausgleichverfahren gleichzeitig ausführen.
Verfahren zur Deaktivierung EC-Datenreparaturauftrag	Nein • Während des EC-Ausgleichs werden Sie daran gehindert, eine Stilllegung oder eine EC-Datenreparatur zu starten. • Sie können den EC-Ausgleichvorgang nicht starten, während ein Ausmustern von Storage Nodes oder eine EC-Datenreparatur ausgeführt wird.
Expansionsverfahren	Nein Wenn Sie neue Storage-Nodes zu einer Erweiterung hinzufügen müssen, sollten Sie warten, bis Sie alle neuen Nodes hinzugefügt haben. Wenn während des Hinzufügens eines neuen Storage-Nodes ein Verfahren zur Ausgleich der EC ausgeführt wird, werden die Daten nicht zu diesen Nodes verschoben.
Upgrade-Verfahren	Nein Wenn Sie ein Upgrade der StorageGRID-Software durchführen müssen, sollten Sie das Upgrade-Verfahren vor oder nach dem Ausführen des EC-Ausgleichs durchführen. Bei Bedarf können Sie den EC-Ausgleichvorgang beenden, um ein Software-Upgrade durchzuführen.

Verfahren	Während des EC-Ausgleichs erlaubt?
Klonvorgang für Appliance-Node	Nein Wenn Sie einen Appliance-Storage-Node klonen müssen, sollten Sie warten, bis der EC-Ausgleichvorgang ausgeführt wurde, nachdem Sie den neuen Node hinzugefügt haben. Wenn während des Hinzufügens eines neuen Storage-Nodes ein Verfahren zur Ausgleich der EC ausgeführt wird, werden die Daten nicht zu diesen Nodes verschoben.
Hotfix-Verfahren	Ja. Sie können einen StorageGRID-Hotfix anwenden, während der EC-Ausgleichvorgang ausgeführt wird.
Andere Wartungsarbeiten	Nein Sie müssen das EC-Ausgleichverfahren beenden, bevor Sie andere Wartungsverfahren durchführen.

Wie das EC-Ausgleichverfahren mit ILM interagiert

Während des EC-Ausgleichs ausgeführt wird, vermeiden Sie ILM-Änderungen, die den Standort vorhandener Objekte, die mit Erasure-Coding-Verfahren codiert wurden, ändern könnten. Beginnen Sie beispielsweise nicht mit der Verwendung einer ILM-Regel, die ein anderes Erasure Coding-Profil hat. Wenn Sie solche ILM-Änderungen vornehmen müssen, sollten Sie den EC-Ausgleichvorgang abbrechen.

Verwandte Informationen

"Balancieren Sie Daten aus, die im Erasure-Coding-Verfahren codiert wurden, nach dem Hinzufügen von Storage"

Hinzufügen von Metadaten-Kapazität

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 Metadatenspeicherplatz bestimmte Schwellenwerte erreicht. Weitere Informationen finden Sie in den Anweisungen zum StorageGRID Monitoring und zur Fehlerbehebung.

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.

Richtlinien zur Erhöhung der Metadaten-Kapazität

Bevor Sie Storage-Nodes hinzufügen, um die Metadatenkapazität zu steigern, lesen Sie die folgenden Richtlinien und Einschränkungen:

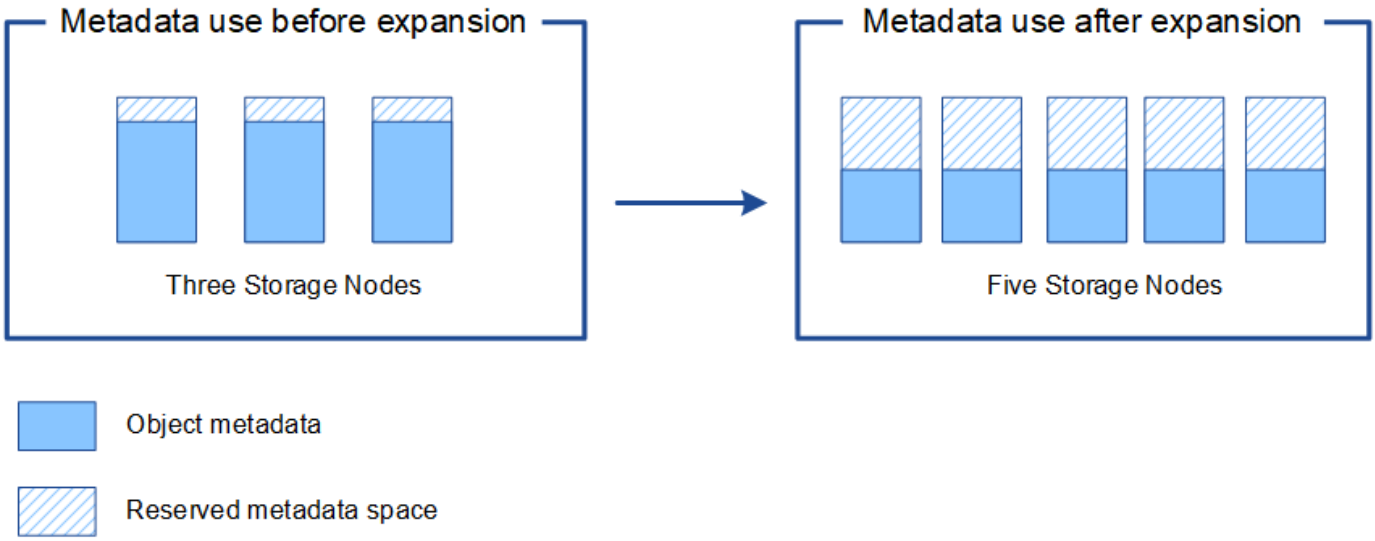
- Wenn eine ausreichende Objekt-Storage-Kapazität verfügbar ist, erhöht sich aufgrund der Verfügbarkeit von mehr Speicherplatz für Objekt-Metadaten die Anzahl der Objekte, die Sie in Ihrem StorageGRID System speichern können.
- Die Metadatenkapazität eines Grids lässt sich erhöhen, indem jedem Standort 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. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.
- Vorhandene Storage-Nodes können nicht erhöht werden, da Metadaten nur auf Volume 0 gespeichert werden.
- Sie können die Metadatenkapazität nicht erhöhen, indem Sie einen neuen Standort hinzufügen.
- 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.

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.



Verwandte Informationen

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

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.

Sie können beispielsweise zusätzliche Gateway-Nodes hinzufügen, um die Erstellung von Hochverfügbarkeitsgruppen von Gateway-Nodes zu unterstützen, oder Sie können einen Admin-Node an einem Remote-Standort hinzufügen, um die Überwachung über einen lokalen Knoten 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
- Archiv-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.

  "Erweiterung der Storage-Kapazität"

- Wenn Sie Archiv-Nodes hinzufügen, beachten Sie, dass jeder Archiv-Node nur Tape über die TSM Middleware (Tivoli Storage Manager) unterstützt.

- Wenn die Option **New Node Client Network Standard** auf der Seite nicht vertrauenswürdige Clientnetzwerke auf **nicht vertrauenswürdig** gesetzt ist, müssen Client-Anwendungen, die sich mit Erweiterungs-Nodes über das Client-Netzwerk verbinden, über einen Load Balancer-Endpunkt-Port (**Konfiguration** > **Netzwerkeinstellungen** > **nicht vertrauenswürdiges Client-Netzwerk**) eine Verbindung herstellen. Informationen zum Verwalten von StorageGRID finden Sie in den Anweisungen zum Ändern der Einstellung für den neuen Node und zum Konfigurieren von Load Balancer-Endpunkten.

Verwandte Informationen

"StorageGRID verwalten"

Hinzufügen eines neuen Standorts

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.
- Grid-Nodes können einem vorhandenen Standort nicht als Teil derselben Erweiterung hinzugefügt werden.
- 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.

  Informationen zum Monitoring der Kapazität von Objektmetadaten finden Sie in den Anweisungen für das Monitoring und die Fehlerbehebung von StorageGRID.

- 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 nicht auf dem neuen Standort gespeichert werden, bis 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 in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Verwandte Informationen

"Objektmanagement mit ILM"

Vorbereitung auf eine Erweiterung

Als Vorbereitung auf die StorageGRID-Erweiterung müssen Sie die erforderlichen Materialien erhalten und neue Hardware und Netzwerke installieren und konfigurieren.

Sammeln der erforderlichen Materialien

Bevor Sie eine Erweiterung durchführen, müssen Sie die in der folgenden Tabelle aufgeführten Materialien erfassen.

Element	Hinweise
StorageGRID Installationsarchiv	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. Weitere Informationen finden Sie in den Anweisungen zum Herunterladen und Extrahieren der StorageGRID-Installationsdateien. **Hinweis:** Sie müssen keine Dateien herunterladen, wenn Sie vorhandenen Speicherknoten neue Speichervolumen hinzufügen oder eine neue StorageGRID Appliance installieren.
Service-Laptop	Das Service-Laptop muss die folgenden Anforderungen erfüllen: • Netzwerkport • SSH-Client (z. B. PuTTY) • Unterstützter Browser
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:
StorageGRID-Dokumentation	• *Verwalten von StorageGRID* • *StorageGRID Versionshinweise* • Installationsanweisungen für Ihre Plattform
Aktuelle Dokumentation für Ihre Plattform	Informationen zu unterstützten Versionen finden Sie in der Interoperabilitäts-Matrix.

Verwandte Informationen

"StorageGRID verwalten"

"Versionshinweise"

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"NetApp Interoperabilitäts-Matrix-Tool"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Herunterladen und Extrahieren der StorageGRID-Installationsdateien

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. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "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**.
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
VMware	StorageGRID-Webscale-*version*-VMware-*uniqueID*.zip StorageGRID-Webscale-*Version* -VMware-*uniqueID*.tgz
Red hat Enterprise Linux oder CentOS	StorageGRID-Webscale-*version*-RPM-*uniqueID*.zip StorageGRID-Webscale-*Version*-RPM-*uniqueID*.tgz
Ubuntu oder Debian und Appliance	StorageGRID-Webscale-*version*-DEB-*uniqueID*.zip StorageGRID-Webscale-*Version*-DEB-*uniqueID*.tgz
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 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.
/vsphere/NetApp-SG-*Version*-SHA.vmdk	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.

Pfad und Dateiname	Beschreibung
	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 Speicherknoten.
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 `deploy-vsphere-ovftool.sh` Skript:
	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.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:

9. 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 `configure-storagegrid.py` Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` 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.

10. 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.

Pfad und Dateiname	Beschreibung
	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`.
	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.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` 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.

11. 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.

Pfad und Dateiname	Beschreibung
	Prüfsumme des DEB-Installationspakets, das vom Installationsprogramm der StorageGRID-Appliance verwendet wird, um zu überprüfen, ob das Paket nach dem Hochladen intakt ist.

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

Bevor Sie mit der Erweiterung Ihres StorageGRID-Systems beginnen, müssen Sie sicherstellen, dass die erforderliche Hardware installiert und konfiguriert wurde, um die neuen Grid-Nodes oder den neuen Standort zu unterstützen.

Informationen zu unterstützten Versionen finden Sie in der Interoperabilitäts-Matrix.

Sie müssen auch die Netzwerkverbindung zwischen Servern am Standort überprüfen und bestätigen, dass der primäre Admin-Node mit allen Erweiterungsservern kommunizieren kann, die das StorageGRID-System hosten sollen.

Wenn Sie eine Erweiterungsaktivität durchführen, die das Hinzufügen eines neuen Subnetzes beinhaltet, müssen Sie das neue Grid-Subnetz hinzufügen, bevor Sie den Erweiterungsvorgang starten.

Verwenden Sie keine NAT (Network Address Translation) 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.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"Subnetze für das Grid-Netzwerk aktualisieren"

Überblick über das Expansionsverfahren

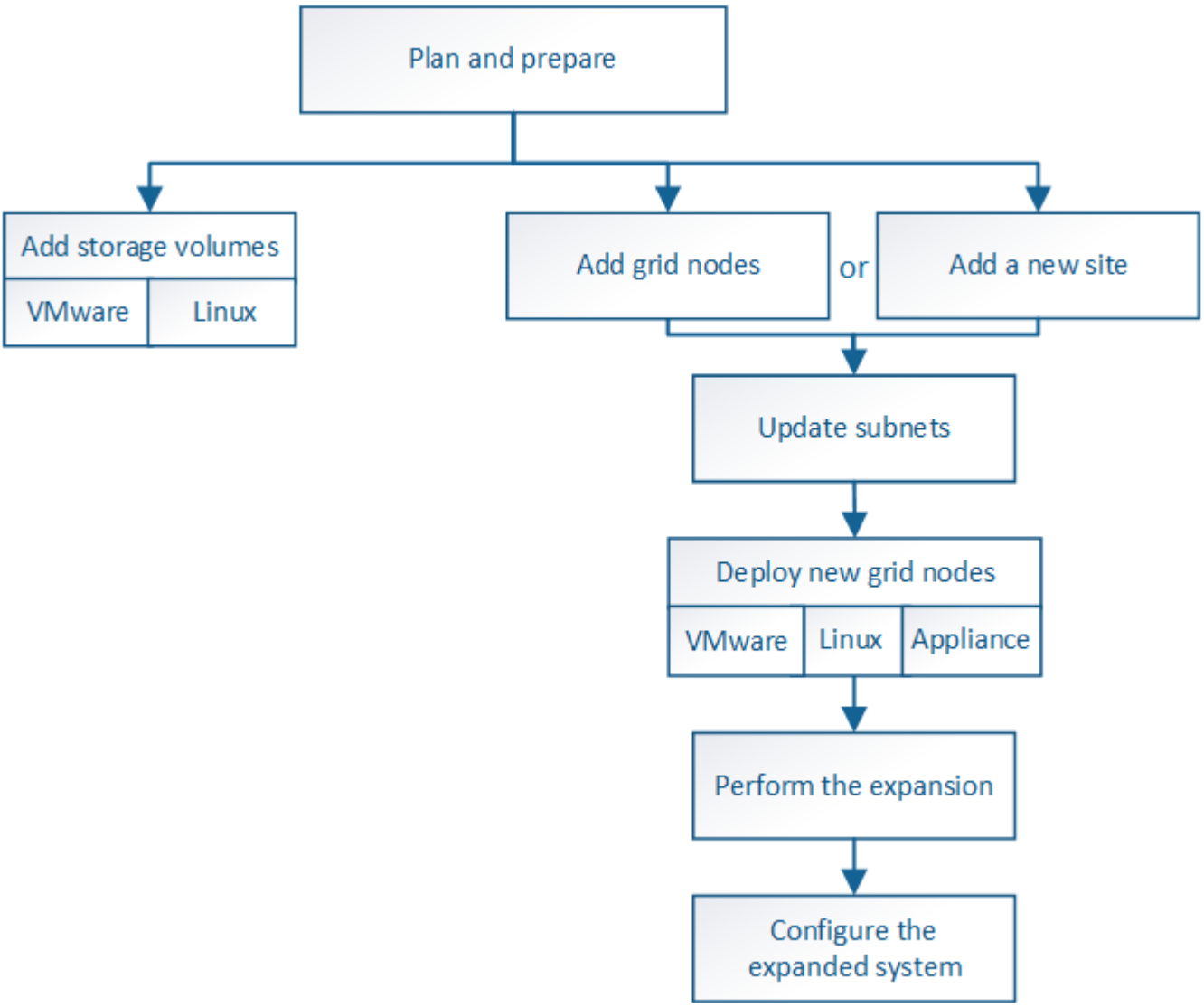
Die grundlegenden Schritte zur Durchführung einer StorageGRID-Erweiterung variieren für die verschiedenen Erweiterungstypen: Hinzufügen von Storage-Volumes zu einem Storage-Node, Hinzufügen neuer Nodes zu einem vorhandenen Standort oder Hinzufügen eines neuen Standorts. In allen Fällen können Sie eine Erweiterung durchführen, ohne den Betrieb des aktuellen Systems zu unterbrechen.

Der Node-Typ, den Sie zum Raster hinzufügen, oder der Grund, warum Sie Nodes hinzufügen, hat keine Auswirkungen auf das grundlegende Erweiterungsverfahren. Wie in der nachstehenden Workflow-Grafik

dargestellt, variieren die Schritte beim Hinzufügen von Nodes in geringem Umfang, je nachdem, ob Sie StorageGRID Appliances oder Hosts mit VMware oder Linux hinzufügen.

Festplattendateien und Skripte von NetApp für neue Installationen oder Erweiterungen von StorageGRID auf OpenStack werden nicht mehr unterstützt. Weitere Informationen zum erweitern einer bestehenden Implementierung auf OpenStack finden Sie in den Schritten für Ihre Linux-Distribution.

„Linux“ bezieht sich auf eine Red hat® Enterprise Linux®-, Ubuntu®-, CentOS- oder Debian®-Bereitstellung. Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.



Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

"StorageGRID-Erweiterung geplant"

"Vorbereitung auf eine Erweiterung"

"Hinzufügen von Storage-Volumes zu Storage-Nodes"

"Einem vorhandenen Standort Grid-Nodes hinzufügen oder einen neuen Standort hinzufügen"

Hinzufügen von Storage-Volumes zu Storage-Nodes

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.

Was Sie benötigen

Lesen Sie vor dem Hinzufügen von Speicher-Volumes die Richtlinien zum Hinzufügen von Speicherkapazität, um sicherzustellen, dass Sie wissen, wo Volumes hinzugefügt werden müssen, um die Anforderungen Ihrer ILM-Richtlinie zu erfüllen.

"Erweiterung der Storage-Kapazität"

> Diese Anweisungen gelten nur für softwarebasierte Speicherknoten. In der Installations- und Wartungsanleitung für die SG6060 Appliance erfahren Sie, wie Sie Storage-Volumes zum SG6060 durch die Installation von Erweiterungs-Shelfs hinzufügen. Andere Appliance-Speicherknoten können nicht erweitert werden.
>
> "SG6000 Storage-Appliances"

Über diese Aufgabe

Der zugrunde liegende Storage eines Storage-Node ist in eine Reihe von 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. Das heißt, der Objektspeicher mit einer ID von 0000 entspricht dem `/var/local/rangedb/0` Bereitstellungspunkt.

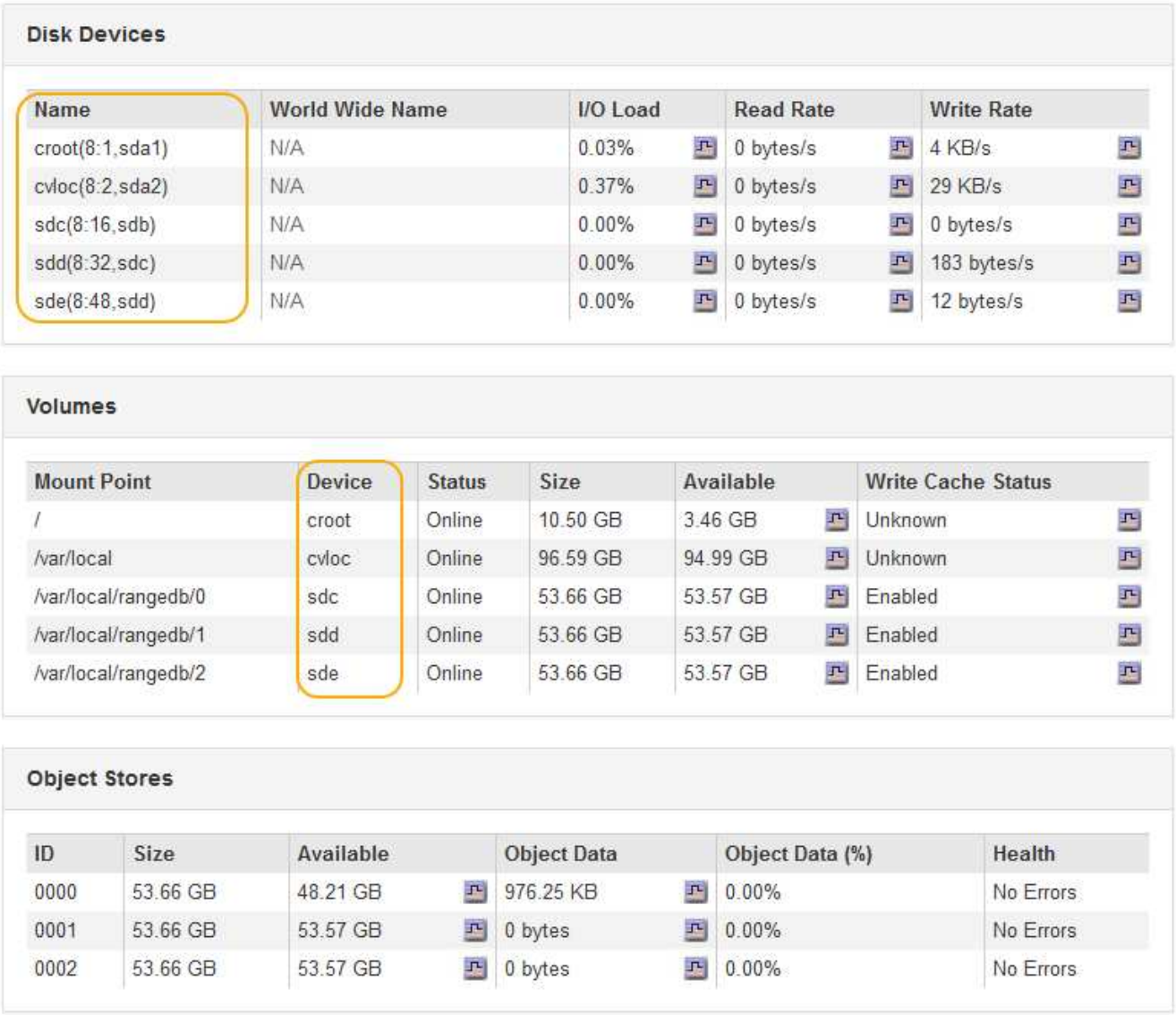
Bevor Sie neue Speicher-Volumes hinzufügen, zeigen Sie mit Grid Manager die aktuellen Objektspeicher für jeden Storage-Node sowie die entsprechenden Mount-Punkte an. Diese Informationen können Sie beim Hinzufügen von Speicher-Volumes verwenden.

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 jedes Laufwerks der weltweiten Kennung (WWID) des Volumes, die angezeigt wird, wenn Sie die standardmäßigen Volume-Eigenschaften in der SANtricity Software anzeigen (die mit dem Storage Controller des Geräts verbundene Managementsoftware).

   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	0.03%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.37%	0 bytes/s	29 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	0 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	183 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	12 bytes/s

Volumes

Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	10.50 GB	3.46 GB	Unknown
/var/local	cvloc	Online	96.59 GB	94.99 GB	Unknown
/var/local/rangedb/0	sdc	Online	53.66 GB	53.57 GB	Enabled
/var/local/rangedb/1	sdd	Online	53.66 GB	53.57 GB	Enabled
/var/local/rangedb/2	sde	Online	53.66 GB	53.57 GB	Enabled

Object Stores

ID	Size	Available	Object Data	Object Data (%)	Health
0000	53.66 GB	48.21 GB	976.25 KB	0.00%	No Errors
0001	53.66 GB	53.57 GB	0 bytes	0.00%	No Errors
0002	53.66 GB	53.57 GB	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 Speicher-Volumes zu einem Speicherknoten"
   - "Linux: Hinzufügen von Direct-Attached- oder SAN-Volumes zu einem Storage-Node"

VMware: Hinzufügen von Speicher-Volumes zu einem Speicherknoten

Wenn ein Storage-Node weniger als 16 Storage-Volumes enthält, können Sie seine Kapazität mithilfe von VMware vSphere erhöhen, um Volumes hinzuzufügen.

Was Sie benötigen

- Sie benötigen Zugriff auf die Anweisungen für die Installation von StorageGRID für VMware-Bereitstellungen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Versuchen Sie nicht, Speicher-Volumes zu einem Speicherknoten hinzuzufügen, während ein Software-Upgrade, 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 sind häufiger verwendet und einfacher zu managen. RDMs können zudem eine bessere Performance für Workloads mit größeren Objektgrößen bieten (z. B. 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 zum Neustart der virtuellen Maschine nicht **Power Off** oder **Reset**.

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.

   a. Geben Sie **y** ein, um die Formatierung zu akzeptieren.

   b. 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. Die Speicher-Volumes sind formatiert.

   c. Geben Sie auf Nachfrage **y** ein, um Storage-Services zu beenden.

   Die Storage-Services werden angehalten, und das `setup_rangedbs.sh` Skript wird automatisch

ausgeführt. Nachdem die Volumes als Rangedbs bereit sind, starten die Dienste erneut.

5. Überprüfen Sie, ob die Dienste richtig starten:

   a. Anzeigen einer Liste des Status aller Dienste auf dem Server:

      ```
      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 über einen unterstützten Browser beim Grid Manager an.
   b. Wählen Sie **Support** > **Tools** > **Grid Topology** 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**.
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 jetzt die erweiterte Kapazität der Speicherknoten zum Speichern von Objektdaten verwenden.

Verwandte Informationen

"VMware installieren"

Linux: Hinzufügen von Direct-Attached- oder SAN-Volumes zu einem 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.

Was Sie benötigen

- Sie müssen Zugriff auf die Anweisungen für die Installation von StorageGRID für Ihre Linux-Plattform haben.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Versuchen Sie nicht, Speicher-Volumes zu einem Speicherknoten hinzuzufügen, während ein Software-Upgrade, 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 Festplattenlaufwerke an, und aktualisieren Sie die RAID-Controller-Konfiguration nach Bedarf, oder weisen Sie die neuen SAN-LUNs auf den gemeinsam genutzten Speicher-Arrays zu, damit der Linux-Host auf sie zugreifen kann.
   - 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 als Root unterstützt, 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
<strong>BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-
4</strong>
<strong>BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-
5</strong>
<strong>BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-
6</strong>
<strong>BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-
7</strong>
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 Blockgerätzuordnungen 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. Anzeigen einer Liste des Status aller Dienste auf dem Server:
       `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.

    a. Geben Sie **y** ein, um die Speicher-Volumes zu formatieren.
    b. 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. Die Speicher-Volumes sind formatiert.

c. Geben Sie auf Nachfrage **y** ein, um Storage-Services zu beenden.

Die Storage-Services werden angehalten, und das `setup_rangedbs.sh` Skript wird automatisch ausgeführt. Nachdem die Volumes als Rangedbs bereit sind, starten die Dienste erneut.

14. Überprüfen Sie, ob die Dienste richtig starten:

a. Anzeigen einer Liste des Status aller Dienste auf dem Server:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

a. Warten Sie, bis alle Dienste ausgeführt oder verifiziert sind.

b. Statusbildschirm verlassen:

```
Ctrl+C
```

15. Vergewissern Sie sich, dass der Speicherknoten online ist:

a. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.

b. Wählen Sie **Support** > **Tools** > **Grid Topology** 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**.

16. 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.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Einem vorhandenen Standort Grid-Nodes hinzufügen oder einen neuen Standort hinzufügen

Gehen Sie folgendermaßen vor, um vorhandenen Standorten Grid-Nodes hinzuzufügen oder einen neuen Standort hinzuzufügen, aber Sie können nicht beide Erweiterungstypen gleichzeitig ausführen.

Was Sie benötigen

- Sie müssen über Root- oder Wartungsberechtigungen verfügen. Weitere Informationen finden Sie unter

Informationen über die Kontrolle des Systemzugriffs mit Administratorkonten und -Gruppen.

- Alle bestehenden Nodes im Grid müssen über alle Standorte hinweg betriebsbereit sein.
- Alle vorherigen Erweiterungs-, Upgrade-, Ausmusterungs- oder Recovery-Verfahren müssen abgeschlossen sein.

> 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 das Grid-Netzwerk aktualisieren"
2. "Neue Grid-Nodes implementieren"
3. "Durchführung der Erweiterung"

Subnetze für das Grid-Netzwerk 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.

Was Sie benötigen

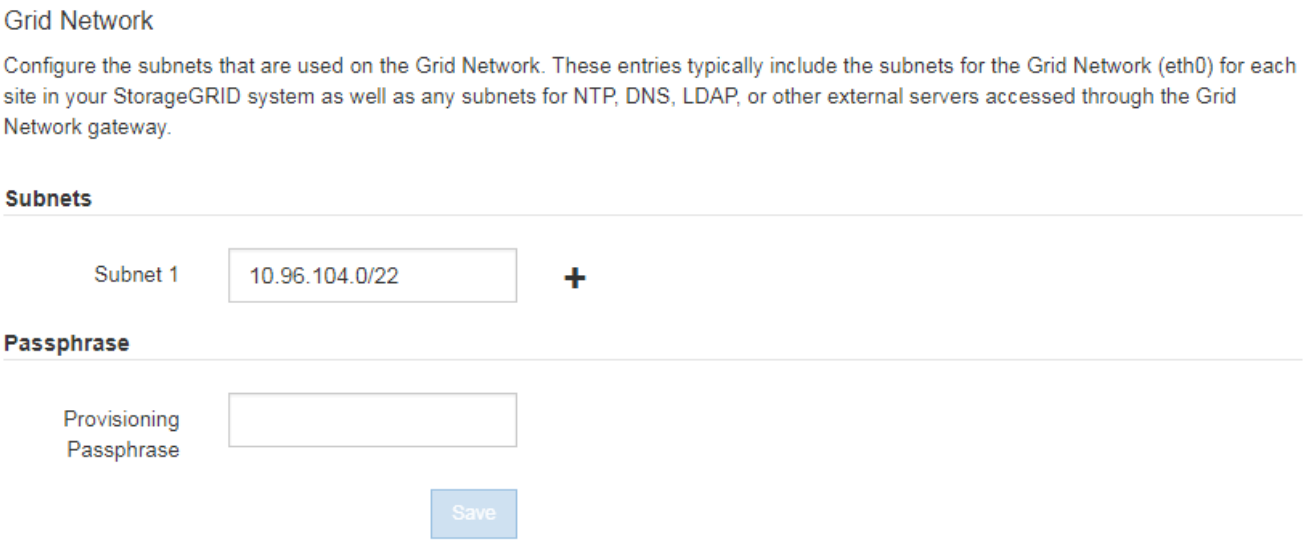
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen die Netzwerkadressen in CIDR-Notation der Subnetze haben, die Sie konfigurieren möchten.

Über diese Aufgabe

Wenn Sie eine Erweiterungsaktivität durchführen, die das Hinzufügen eines neuen Subnetzes beinhaltet, müssen Sie das neue Grid-Subnetz hinzufügen, bevor Sie den Erweiterungsvorgang starten.

Schritte

1. Wählen Sie **Wartung Netzwerk Grid-Netzwerk**.



2. Klicken Sie in der Liste Subnetze auf das Pluszeichen, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

   Geben Sie beispielsweise 10.96.104.0/22 ein.

3. Geben Sie die Provisionierungs-Passphrase ein, und klicken Sie auf **Speichern**.

   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 hinzuzufügenden Nodes nicht mit den vorhandenen Node-Typen übereinstimmen. VMware Nodes, Linux Container-basierte Nodes oder Appliance-Nodes lassen sich hinzufügen.

VMware: Implementieren der Grid-Nodes

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 Grid-Node als Virtual Machine und verbinden Sie ihn mit einem oder mehreren StorageGRID-Netzwerken.

   Bei der Implementierung des Node können Sie optional Node-Ports neu zuordnen oder CPU- oder Speichereinstellungen erhöhen.

   "StorageGRID-Knoten als virtuelle Maschine implementieren"

2. Nachdem Sie alle neuen VMware-Knoten bereitgestellt haben, fahren Sie mit diesen Anweisungen zum Erweiterungsvorgang zurück.

"Durchführung der Erweiterung"

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.

Was Sie benötigen

- Sie haben Anweisungen zum Installieren von StorageGRID für Ihre Linux-Version und haben die Hardware- und Speicheranforderungen geprüft.
- 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 Speicherknoten 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 AFF 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.

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 die Erweiterung durchführen.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"Durchführung der Erweiterung"

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.

Was Sie benötigen

- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Sie haben mit dem Installationsprogramm der StorageGRID Appliance alle Schritte „`Configuring the Hardware`“ in der Installations- und Wartungsanleitung für die Appliance abgeschlossen.

  Das Konfigurieren der Appliance-Hardware umfasst die erforderlichen Schritte zum Konfigurieren von StorageGRID-Verbindungen (Netzwerkverbindungen und IP-Adressen) sowie die optionalen Schritte zum Aktivieren der Node-Verschlüsselung, zum Ändern des RAID-Modus und zum erneuten Zuordnen von Netzwerkports.

- 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 Installationsversion der StorageGRID Appliance auf der Ersatzanwendung stimmt mit der Softwareversion des StorageGRID-Systems überein. (Wenn die Versionen nicht übereinstimmen, müssen Sie die StorageGRID Appliance Installer-Firmware aktualisieren.)

  Anweisungen hierzu finden Sie in der Installations- und Wartungsanleitung des Geräts.

  - "SG100 SG1000 Services-Appliances"
  - "SG5600 Storage Appliances"
  - "SG5700 Storage-Appliances"
  - "SG6000 Storage-Appliances"
- Sie verfügen über einen Service-Laptop mit einem unterstützten 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 automatisieren `configure-sga.py` Installationsskript 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	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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 klicken Sie auf **Speichern**.

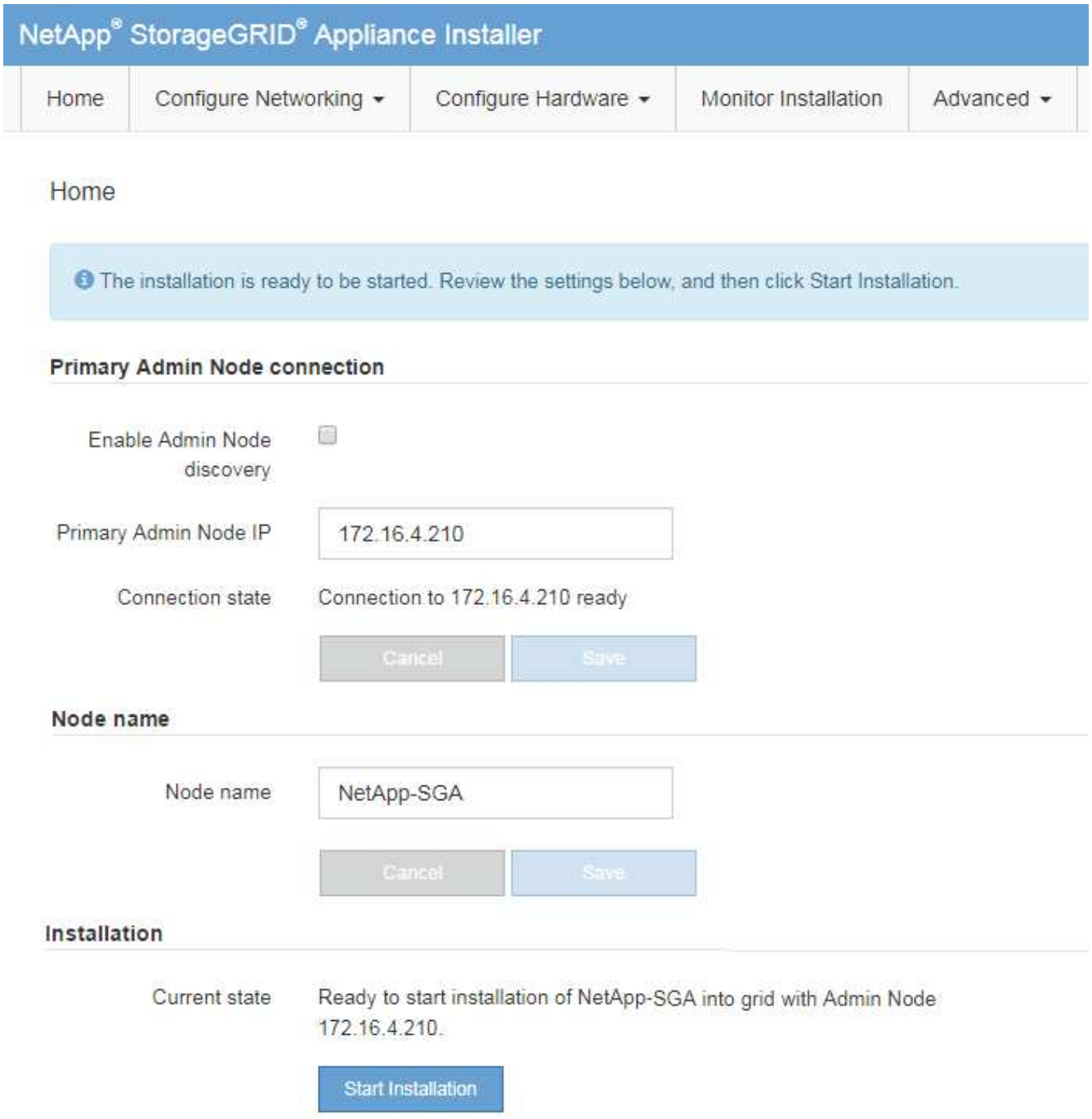
   Der Node-Name wird diesem Appliance-Node im StorageGRID-System zugewiesen. Sie wird im Grid Manager auf der Seite Nodes (Registerkarte Übersicht) angezeigt. Bei Bedarf können Sie den Namen ändern, wenn Sie den Knoten genehmigen.

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 Installations- und Wartungsanleitung für Ihr Gerät.

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.

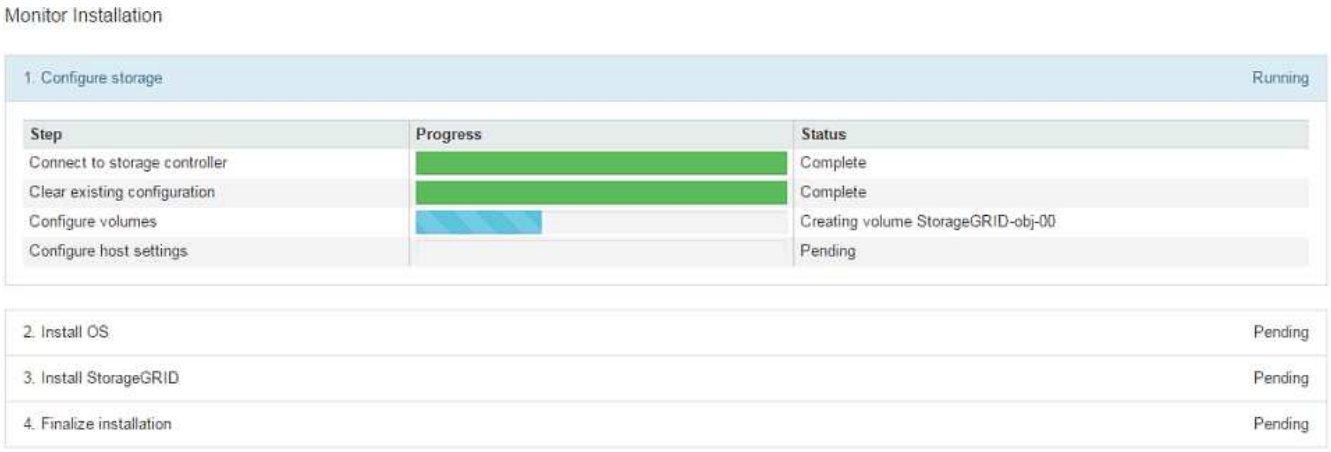
7. Wenn Ihre Erweiterung mehrere Appliance-Nodes umfasst, wiederholen Sie die vorherigen Schritte für

jede Appliance.

> Wenn Sie mehrere Appliance Storage Nodes gleichzeitig bereitstellen müssen, können Sie den Installationsprozess mithilfe des Installationsskripts für die configure-sga.py Appliance automatisieren.

8. Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**.

   Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.



   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 „`Skipped.`“ angezeigt.

9. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

   1. Gerät konfigurieren

   In dieser Phase tritt eines der folgenden Prozesse auf:

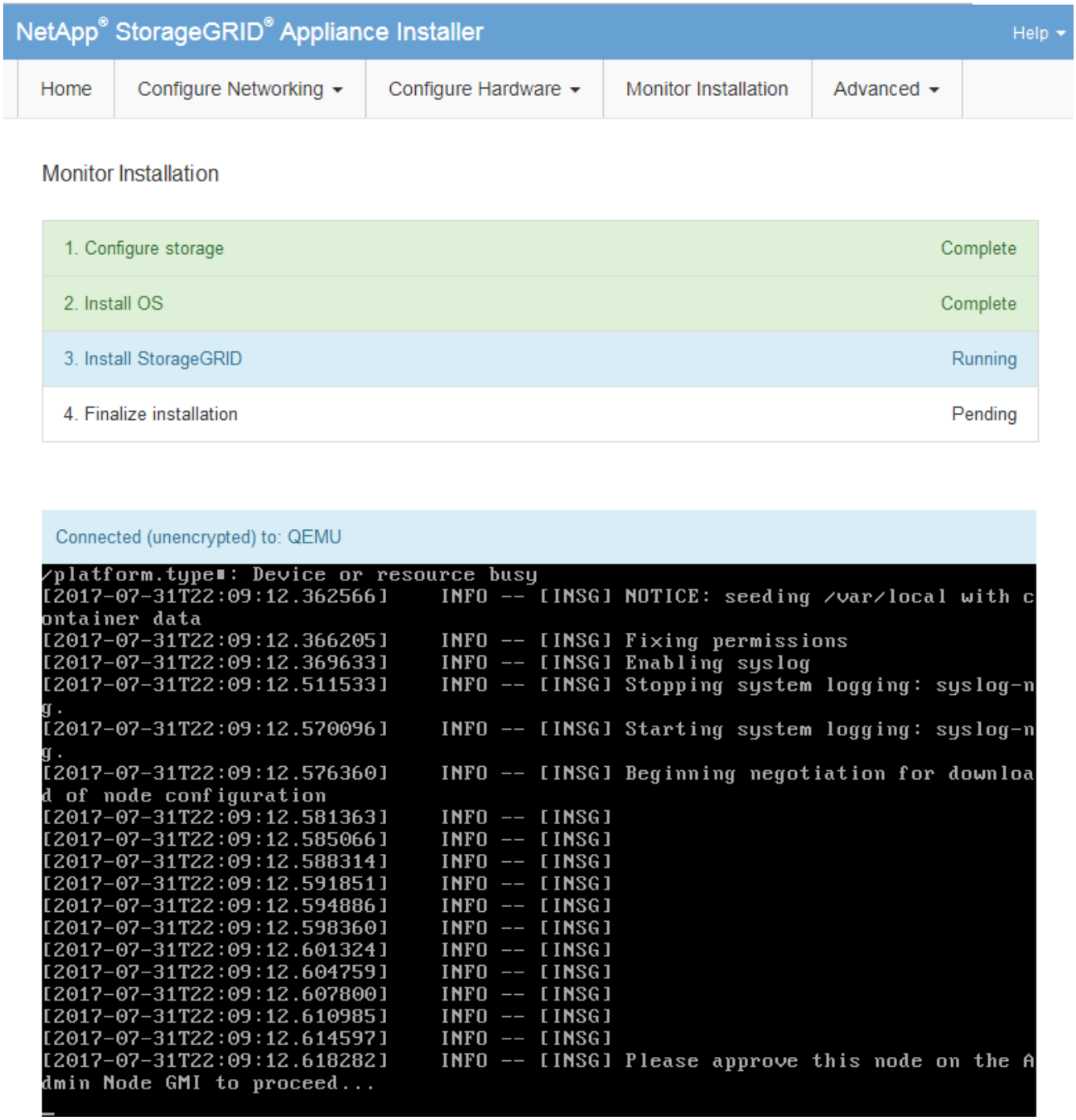
   - Bei einer Storage Appliance stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.
   - Bei einer Services-Appliance löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken im Compute-Controller und konfiguriert die Hosteinstellungen.

   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.



Verwandte Informationen

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"SG6000 Storage-Appliances"

"SG100 SG1000 Services-Appliances"

Durchführung der Erweiterung

Wenn die Erweiterung durchgeführt wird, werden die neuen Grid-Nodes zu Ihrer bestehenden StorageGRID Implementierung hinzugefügt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen alle Grid-Nodes, die in dieser Erweiterung hinzugefügt werden, implementiert haben.
- Beim Hinzufügen von Speicherknoten müssen Sie bestätigt haben, dass alle Datenreparaturvorgänge, die im Rahmen einer Wiederherstellung durchgeführt werden, abgeschlossen sind. Siehe die Schritte zum Überprüfen von Datenreparaturjobs in den Anweisungen für Wiederherstellung und Wartung.
- Wenn Sie einen neuen Standort hinzufügen, müssen Sie ILM-Regeln prüfen und aktualisieren, bevor Sie die Erweiterung starten, um sicherzustellen, dass Objektkopien erst nach Abschluss der Erweiterung auf dem neuen Standort gespeichert werden. Wenn eine Regel beispielsweise den Standard-Speicherpool (Alle Speicherknoten) verwendet, müssen Sie einen neuen Speicherpool erstellen, der nur die vorhandenen Speicherknoten enthält, und die ILM-Regel 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 finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Über diese Aufgabe

Während der Erweiterung umfasst die folgenden Phasen:

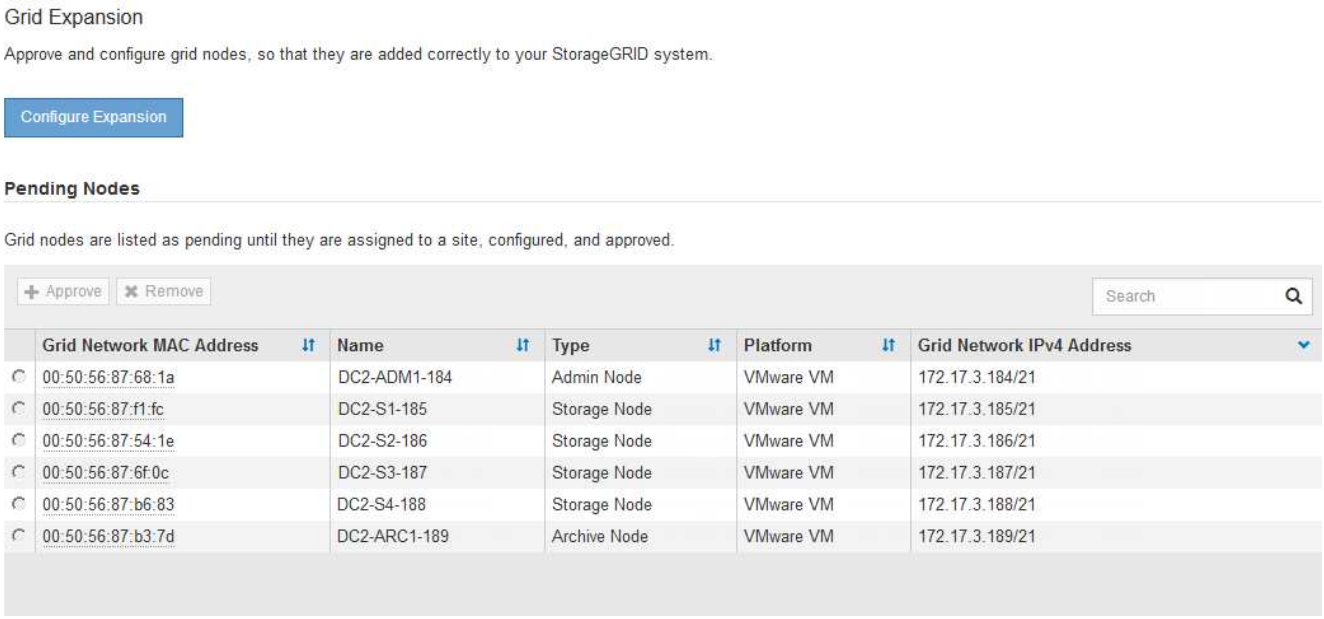
1. Sie konfigurieren die Erweiterung, indem Sie angeben, ob Sie neue Grid-Nodes oder einen neuen Standort hinzufügen und die Grid-Nodes genehmigen, die Sie hinzufügen möchten.
2. Sie starten die Erweiterung.
3. Während der Erweiterungsprozess ausgeführt wird, laden Sie eine neue Wiederherstellungspaket-Datei herunter.
4. Sie überwachen den Status der Grid-Konfigurationsaufgaben, die automatisch ausgeführt werden. Die Aufgabengruppe hängt davon ab, welche Typen von Grid-Nodes hinzugefügt werden und ob ein neuer Standort hinzugefügt wird.

> ⓘ Bei einigen Aufgaben kann die Ausführung auf einem großen Grid sehr viel Zeit in Anspruch nehmen. Das Streaming von Cassandra auf einen neuen Storage-Node kann beispielsweise nur wenige Minuten dauern, wenn die Cassandra-Datenbank relativ leer ist. Wenn die Cassandra-Datenbank jedoch eine große Menge an Objekt-Metadaten enthält, kann diese Phase mehrere Stunden oder länger dauern. Sie können sich den Prozentsatz „`sTreamed`“ ansehen, der während der Phase „`STarting Cassandra and Streaming Data`“ angezeigt wird, um festzustellen, wie vollständig der Cassandra-Streaming-Vorgang ist.

Schritte

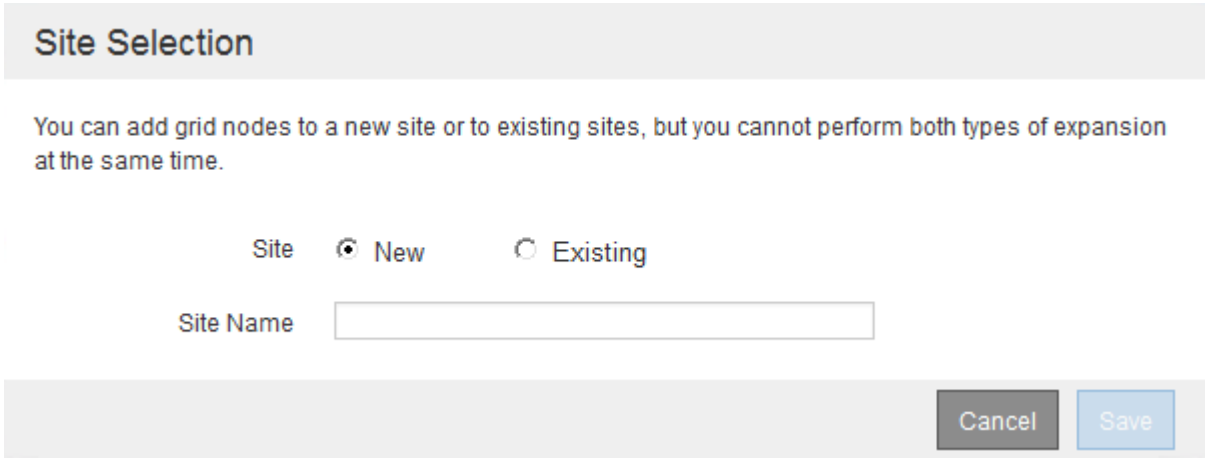
1. Wählen Sie **Wartung** > **Wartungsaufgaben** > **Erweiterung**.

   Die Seite Rastererweiterung wird angezeigt. Im Abschnitt Ausstehende Knoten werden alle Knoten aufgeführt, die hinzugefügt werden können.



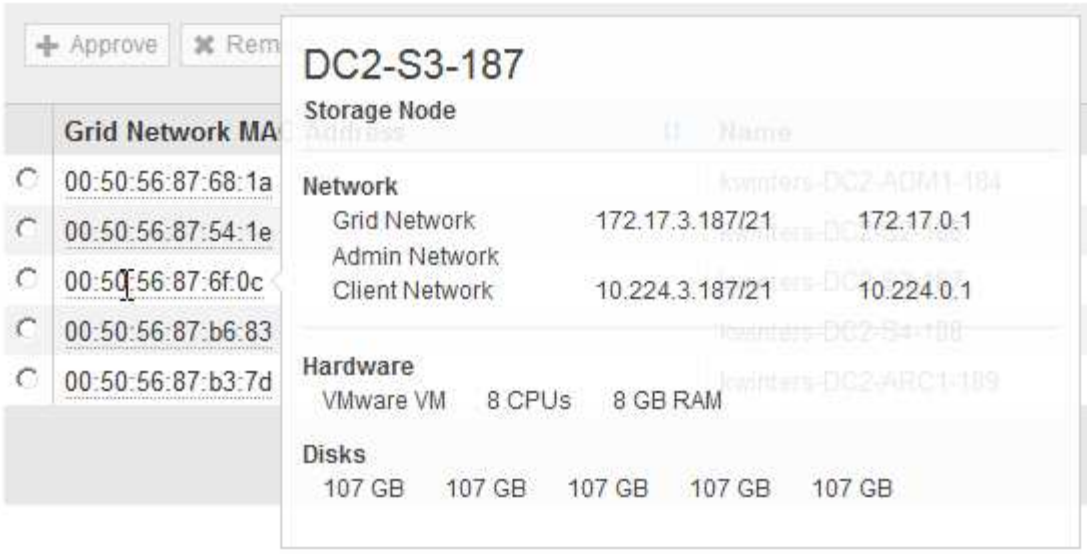
2. Klicken Sie Auf **Erweiterung Konfigurieren**.

   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 einem vorhandenen Standort Rasterknoten hinzufügen, wählen Sie **vorhandene**.
4. Klicken Sie Auf **Speichern**.
5. Überprüfen Sie die Liste **Ausstehende Knoten** und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

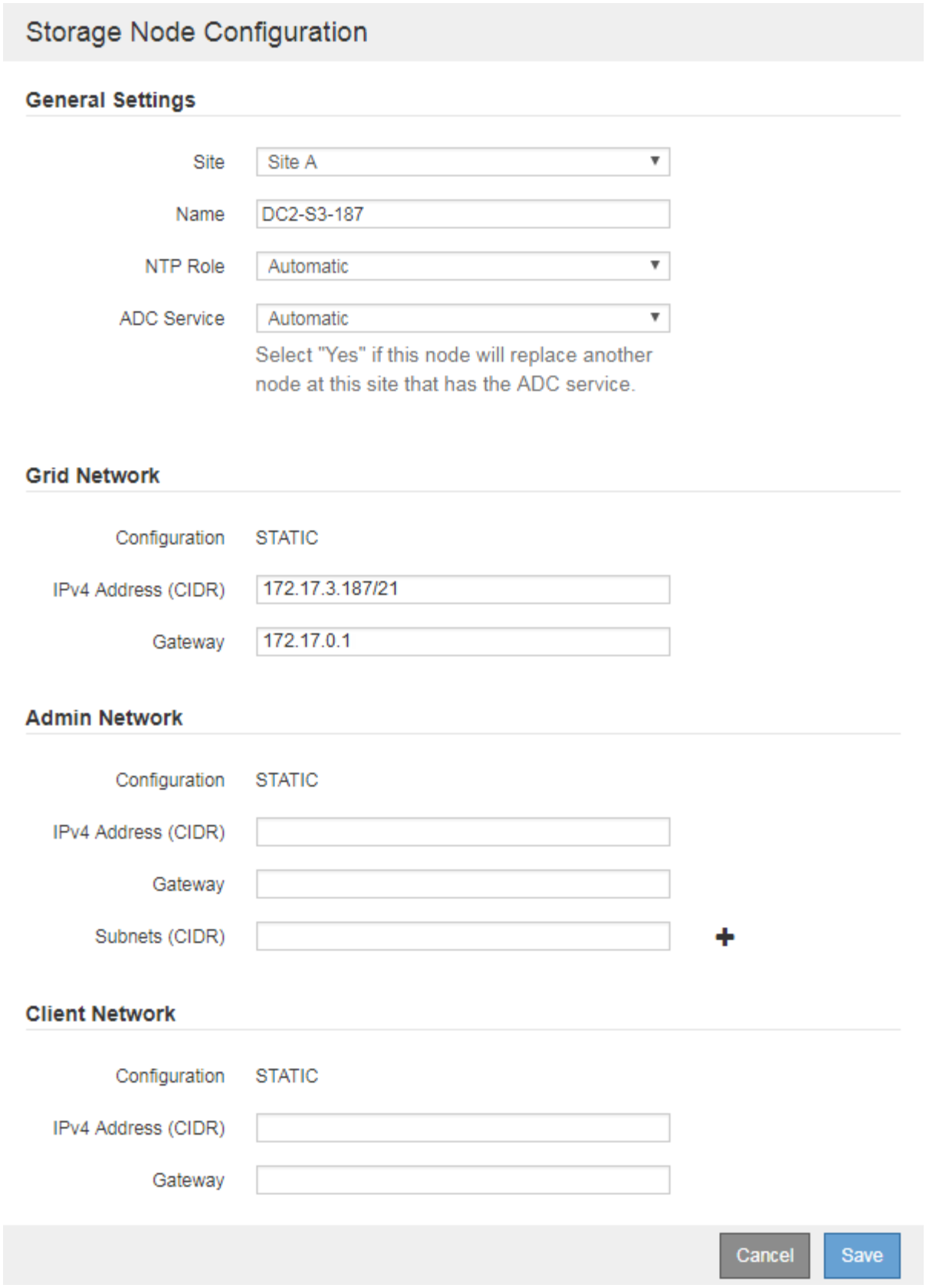
   Bei Bedarf können Sie den Cursor über die **Grid Network MAC Address** eines Knotens bewegen, um Details zu diesem Knoten anzuzeigen.



Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

6. Genehmigen Sie in der Liste der ausstehenden Knoten die Grid-Knoten für diese Erweiterung.
   a. Aktivieren Sie das Optionsfeld neben dem ersten ausstehenden Rasterknoten, den Sie genehmigen möchten.
   b. Klicken Sie Auf **Genehmigen**.

      Das Konfigurationsformular für den Grid-Node wird angezeigt.



c. Ändern Sie bei Bedarf die allgemeinen Einstellungen:

   - **Standort**: Der Name des Standorts, dem der Grid-Node zugeordnet ist. 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 Hostname, der dem Knoten zugewiesen wird, und der Name, der im Grid Manager angezeigt wird.
- **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.

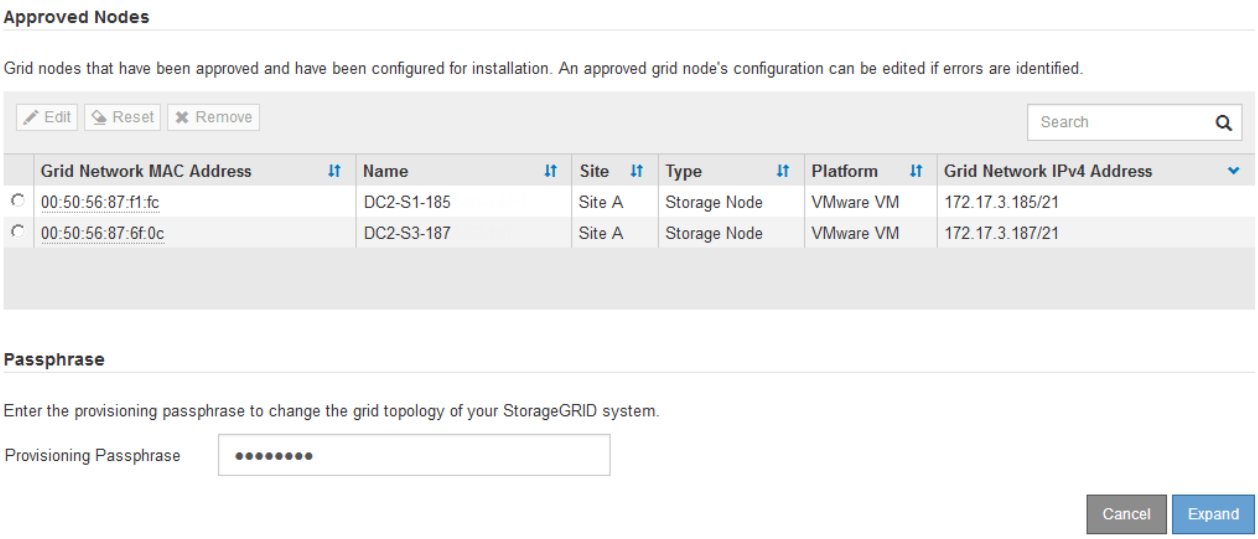
  Weisen Sie die primäre NTP-Rolle mindestens zwei Nodes an jedem Standort zu. Dadurch erhalten Sie redundanten Zugriff auf externe Zeitquellen.

- **ADC Service** (nur Speicherknoten): Ob dieser Speicherknoten den Dienst Administrative Domain Controller (ADC) ausführen wird. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, nachdem er bereitgestellt wurde.
  - Wenn Sie diesen Knoten hinzufügen, um einen Speicherknoten zu ersetzen, wählen Sie **Ja** aus, wenn der Knoten, den Sie ersetzen, den ADC-Dienst enthält. Da ein Storage-Node nicht stillgelegt werden kann, wenn zu wenige ADC-Dienste verbleiben, wird sichergestellt, dass ein neuer ADC-Service verfügbar ist, bevor der alte Service entfernt wird.
  - Wählen Sie andernfalls **automatisch** aus, damit das System feststellen kann, ob dieser Knoten den ADC-Dienst erfordert. Erfahren Sie mehr über das ADC-Quorum in den Anweisungen zur Wiederherstellung und Wartung.

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
   - **Gateway**: Das Standard-Gateway des Grid-Knotens. Beispiel: 172.16.10.1
   - **Subnetze (CIDR)**: Ein oder mehrere Unternetzwerke für das Admin-Netzwerk.

e. Klicken Sie Auf **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 klicken Sie auf **Bearbeiten**.
- Um einen genehmigten Rasterknoten zurück in die Liste ausstehender Knoten zu verschieben, wählen Sie dessen Optionsfeld aus und klicken Sie auf **Zurücksetzen**.
- Um einen genehmigten Grid-Node dauerhaft zu entfernen, schalten Sie den Node aus. Wählen Sie dann das entsprechende Optionsfeld aus, und klicken Sie auf **Entfernen**.

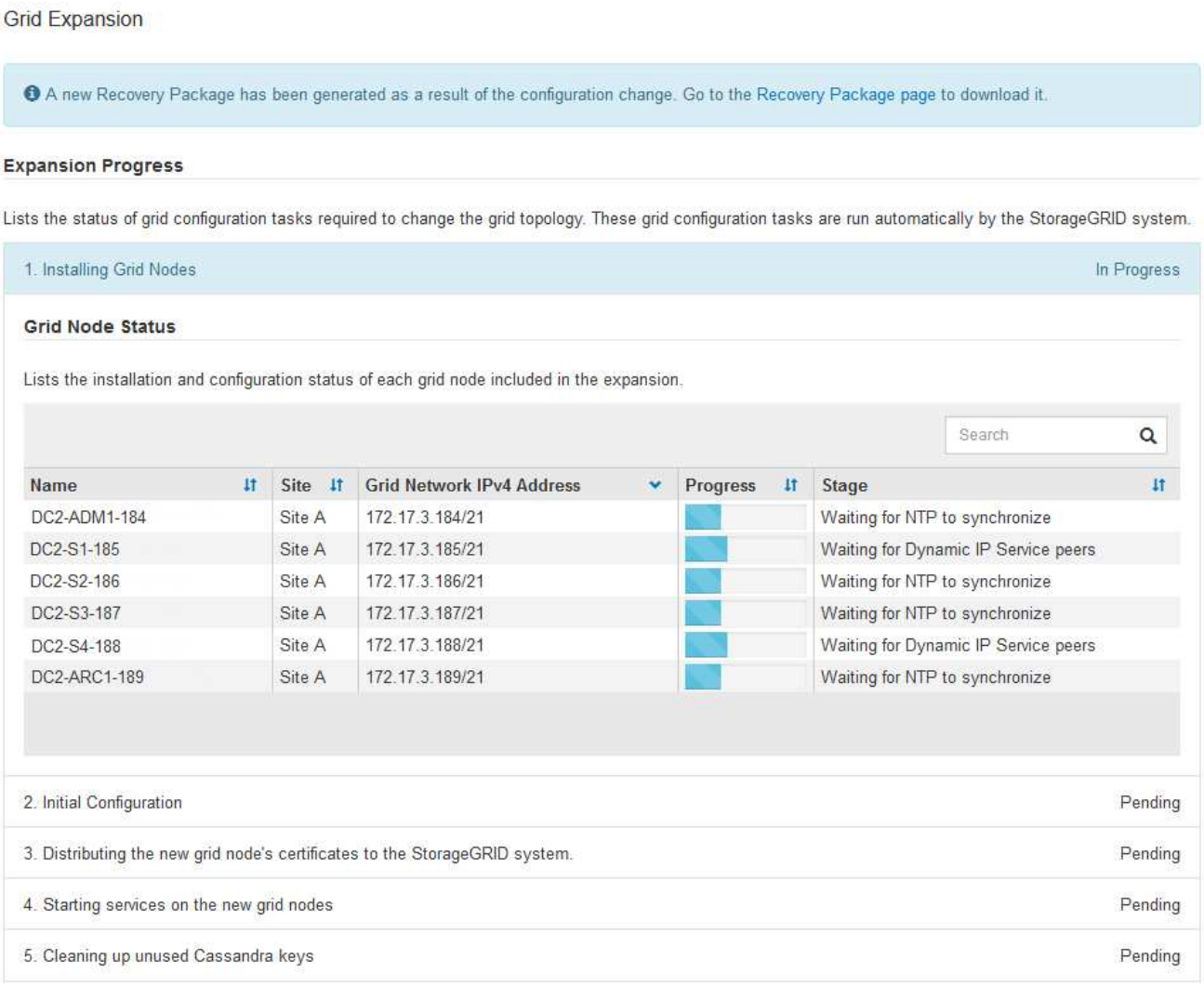
f. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.

> 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 klicken Sie auf **erweitern**.

   Nach einigen Minuten wird diese Seite aktualisiert, um den Status des Erweiterungsverfahrens anzuzeigen. Wenn Aufgaben ausgeführt werden, die sich auf einzelne Grid-Nodes auswirken, enthält der Abschnitt Status des Grid-Knotens den aktuellen Status für jeden Grid-Node.

   > Während dieses Prozesses zeigt das Installationsprogramm für StorageGRID-Geräte, dass die Installation von Phase 3 auf Stufe 4 verschoben wird, und schließt die Installation ab. Wenn Phase 4 abgeschlossen ist, wird der Controller neu gestartet.



Eine Standorterweiterung umfasst eine zusätzliche Aufgabe zur Konfiguration von Cassandra für den neuen Standort.

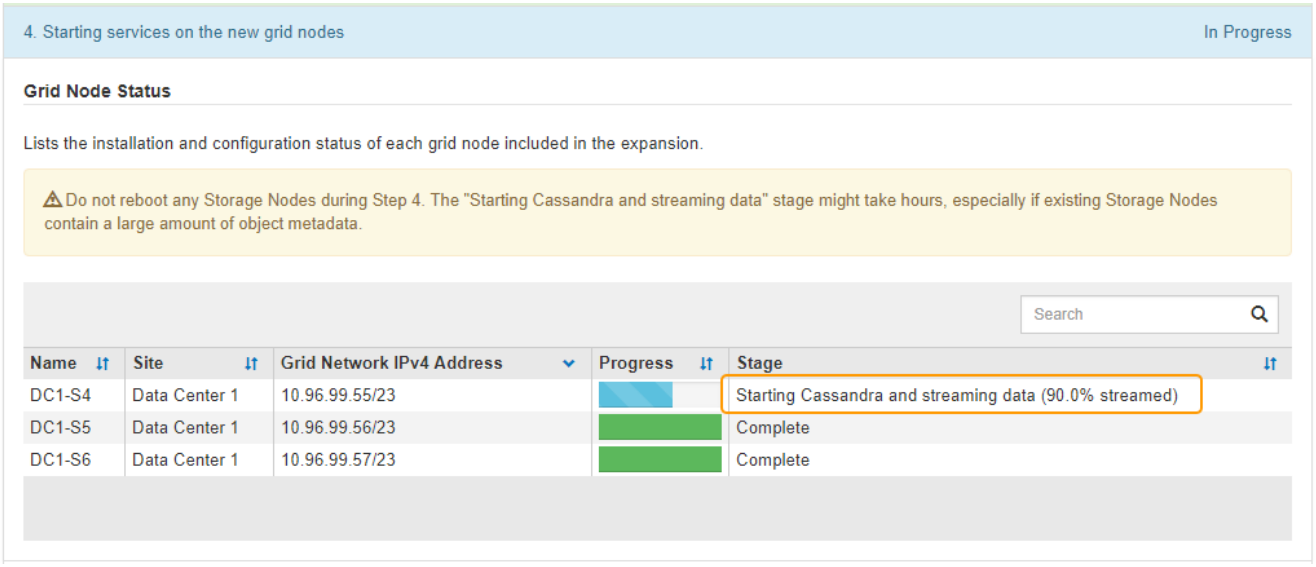
8. Sobald der Link **Download Recovery Package** angezeigt wird, laden Sie die Recovery Package Datei herunter.

   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. Klicken Sie auf den Download-Link.
   b. Geben Sie die Provisionierungs-Passphrase ein, und klicken Sie auf **Download starten**.
   c. Wenn der Download abgeschlossen ist, öffnen Sie das `.zip` Datei und bestätigen Sie, dass es ein enthält `gpt-backup` Verzeichnis und A `_SAID.zip` Datei: Dann extrahieren Sie den `_SAID.zip` Wechseln Sie zur Datei `/GID*_REV*` Telefonbuch und bestätigen Sie, dass Sie das öffnen können `passwords.txt` Datei:
   d. Kopieren Sie die heruntergeladene Recovery Package-Datei (.zip) in 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.

9. Wenn Sie einen oder mehrere Storage-Nodes hinzufügen, überwachen Sie den Fortschritt der Phase „`STarting Cassandra and Streaming Data`“, indem Sie den in der Statusmeldung angezeigten Prozentsatz überprüfen.



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.

Starten Sie keine Storage Nodes während Schritt 4 neu (Starting Services on the New Grid Nodes). Die Phase „`STarting Cassandra und Streaming Data`“ kann für jeden neuen Storage Node Stunden dauern, insbesondere wenn vorhandene Storage-Nodes eine große Anzahl von Objekt-Metadaten enthalten.

10. 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, müssen Sie zusätzliche Integrations- und Konfigurationsschritte durchführen.

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwalten Sie erholen"

"Konfiguration des erweiterten StorageGRID-Systems"

Konfiguration des erweiterten StorageGRID-Systems

Nach Abschluss einer Erweiterung müssen Sie weitere Integrations- und Konfigurationsschritte durchführen.

Über diese Aufgabe

Sie müssen die unten aufgeführten Konfigurationsaufgaben für die Grid-Nodes ausführen, die Sie in Ihrer Erweiterung hinzufügen. Einige Aufgaben können optional sein, je nachdem, welche Optionen bei der Installation und Verwaltung des Systems ausgewählt wurden, und wie Sie die während der Erweiterung hinzugefügten Grid-Nodes konfigurieren möchten.

Schritte

1. Wenn Sie einen Speicherknoten hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus.

Konfigurationsaufgaben für Storage-Nodes	Zur Information
Überprüfen Sie die in Ihren ILM-Regeln verwendeten Speicherpools, um sicherzustellen, dass der neue Speicher verwendet wird. • Wenn Sie einen Standort hinzufügen, erstellen Sie einen Speicherpool für den Standort und aktualisieren Sie ILM-Regeln, um den neuen Speicherpool zu verwenden. • Wenn Sie einem vorhandenen Standort einen Speicherknoten hinzugefügt haben, bestätigen Sie, dass der neue Node die richtige Speicherklasse verwendet. **Hinweis:** standardmäßig wird ein neuer Speicherknoten der Speicherklasse Alle Speicherknoten zugewiesen und zu Speicherpools hinzugefügt, die diese Klasse für den Standort verwenden. Wenn ein neuer Knoten eine benutzerdefinierte Speicherklasse verwenden soll, müssen Sie ihn der benutzerdefinierten Klasse manuell zuweisen (**ILM** > **Storage-Klasse**).	"Objektmanagement mit ILM"
Vergewissern Sie sich, dass der Speicherknoten Objekte erfasst.	"Überprüfen, ob der Speicherknoten aktiv ist"
Ausgleich von Daten mit Verfahren zur Einhaltung von Datenkonsistenz (nur wenn die empfohlene Anzahl von Storage-Nodes nicht hinzugefügt werden konnte)	"Balancieren Sie Daten aus, die im Erasure-Coding-Verfahren codiert wurden, nach dem Hinzufügen von Storage"

2. Wenn Sie einen Gateway-Node hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus.

Konfigurationsaufgaben für Gateway Node	Zur Information
Wenn Hochverfügbarkeitsgruppen für Client-Verbindungen verwendet werden, fügen Sie die Gateway-Nodes einer HA-Gruppe hinzu. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen** aus, um die Liste der vorhandenen HA-Gruppen zu überprüfen und die neuen Nodes hinzuzufügen.	"StorageGRID verwalten"

3. Wenn Sie einen Admin-Node hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus.

Konfigurationsaufgaben für Admin-Node	Zur Information
Wenn Single Sign-On für Ihr StorageGRID-System aktiviert ist, müssen Sie für den neuen Admin-Knoten ein Vertrauensverhältnis der Vertrauensbasis in Active Directory Federation Services (AD FS) erstellen. Sie können sich erst beim Knoten anmelden, wenn Sie dieses Vertrauen der Vertrauensbasis erstellen.	"Konfigurieren der Single Sign-On-Konfiguration"
Wenn Sie den Load Balancer-Service auf Admin-Nodes verwenden möchten, müssen Sie die Admin-Nodes möglicherweise den Gruppen für hohe Verfügbarkeit hinzufügen. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Hochverfügbarkeitsgruppen** aus, um die Liste der vorhandenen HA-Gruppen zu überprüfen und die neuen Nodes hinzuzufügen.	"StorageGRID verwalten"
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.	"Die Admin-Knoten-Datenbank wird kopiert"
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.	"Kopieren von Prometheus-Kennzahlen"
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.	"Prüfprotokolle werden kopiert"
Konfigurieren Sie optional den Zugriff auf das System für Audit-Zwecke über eine NFS- oder CIFS-Dateifreigabe. **Hinweis:** der Audit-Export über CIFS/Samba ist veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.	"StorageGRID verwalten"
Ändern Sie optional den bevorzugten Absender für Benachrichtigungen. Sie können den Erweiterungs-Admin-Knoten zum bevorzugten Absender machen. Andernfalls sendet ein vorhandener als bevorzugter Absender konfigurierter Admin-Node weiterhin Benachrichtigungen, einschließlich AutoSupport-Nachrichten, SNMP-Benachrichtigungen, Alarm-E-Mails und Alarm-E-Mails (Legacy-System).	"StorageGRID verwalten"

4. Wenn Sie einen Archivknoten hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus.

Konfigurationsaufgaben für Archivierungs-Knoten	Zur Information
Konfigurieren Sie die Verbindung des Archiv-Knotens mit dem angestrebten externen Archiv-Storage-System. Wenn Sie die Erweiterung abgeschlossen haben, befinden sich Archiv-Knoten in einem Alarmzustand, bis Sie die Verbindungsinformationen über die Komponente **ARC** > **Ziel** konfigurieren.	"StorageGRID verwalten"
Aktualisieren Sie die ILM-Richtlinie, um Objektdaten über den neuen Archivierungs-Node zu archivieren.	"Objektmanagement mit ILM"
Konfigurieren Sie benutzerdefinierte Alarme für die Attribute, die zur Überwachung der Geschwindigkeit und Effizienz des Datenabrufs von Objektdaten von Archiv-Nodes verwendet werden.	"StorageGRID verwalten"

5. Um zu überprüfen, ob Erweiterungsknoten mit einem nicht vertrauenswürdigen Client-Netzwerk hinzugefügt wurden oder um zu ändern, ob das Client-Netzwerk eines Knotens nicht vertrauenswürdig oder vertrauenswürdig ist, gehen Sie zu **Konfiguration** > **Netzwerkeinstellungen** > **nicht vertrauenswürdiges Client-Netzwerk**.

   Wenn das Client-Netzwerk auf dem Erweiterungsknoten nicht vertrauenswürdig ist, müssen Verbindungen zum Knoten im Client-Netzwerk über einen Load Balancer-Endpunkt hergestellt werden. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

6. Konfigurieren Sie das Domain Name System (DNS).

   Wenn Sie für jeden Grid-Node DNS-Einstellungen separat angegeben haben, müssen Sie für die neuen Nodes benutzerdefinierte DNS-Einstellungen pro Node hinzufügen. Weitere Informationen zum Ändern der DNS-Konfiguration für einen einzelnen Grid-Node finden Sie in den Anweisungen zur Recovery und Wartung.

   Eine Best Practice besteht in der netzweiten DNS-Server-Liste, die einige DNS-Server enthält, auf die von jedem Standort aus lokal zugegriffen werden kann. Wenn Sie gerade einen neuen Standort hinzugefügt haben, fügen Sie der Grid-weiten DNS-Konfiguration neue DNS-Server für den Standort hinzu.

   > Geben Sie zwei bis sechs IPv4-Adressen für DNS-Server an. Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen. Weitere Informationen finden Sie in den Informationen zum Ändern der DNS-Konfiguration in den Wiederherstellungsanleitungen und Wartungsanweisungen.

7. Wenn Sie einen neuen Standort hinzugefügt haben, vergewissern Sie sich, dass auf die NTP-Server (Network Time Protocol) von diesem Standort aus zugegriffen werden kann.

   > 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.

Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Verwandte Informationen

"Objektmanagement mit ILM"

"Überprüfen, ob der Speicherknoten aktiv ist"

"Die Admin-Knoten-Datenbank wird kopiert"

"Kopieren von Prometheus-Kennzahlen"

"Prüfprotokolle werden kopiert"

"Software-Upgrade"

"Verwalten Sie erholen"

Überprüfen, ob 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 über einen unterstützten Browser beim Grid Manager an.
2. Wählen Sie **Nodes** > ***Erweiterungs-Speicherknoten*** > **Storage** Aus.
3. Bewegen Sie den Cursor über das Diagramm **verwendete Speicherung - Objektdaten**, um den Wert für **verwendet** anzuzeigen. Dies ist die Menge des insgesamt nutzbaren Speicherplatzes, 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.

Die Admin-Knoten-Datenbank wird kopiert

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.

Was Sie benötigen

- Sie müssen die erforderlichen Erweiterungsschritte abgeschlossen haben, um einen Admin-Node hinzuzufügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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 von 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.

Was Sie benötigen

- Der neue Admin-Node muss installiert und ausgeführt werden.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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 werden kopiert

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. Sie können Prüfprotokolle von einem zuvor installierten Admin-Knoten auf den neuen ErweiterungAdmin-Knoten kopieren, so dass er mit dem Rest des StorageGRID-Systems synchronisiert ist.

Was Sie benötigen

- Sie müssen die erforderlichen Erweiterungsschritte abgeschlossen haben, um einen Admin-Node hinzuzufügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Um die historischen Audit-Meldungen von anderen Admin-Knoten auf dem Erweiterungs-Admin-Knoten verfügbar zu machen, müssen Sie die Audit-Log-Dateien manuell vom primären Admin-Node oder einem anderen vorhandenen Admin-Node auf den Erweiterungs-Admin-Node kopieren.

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
```

Balancieren Sie Daten aus, die im Erasure-Coding-Verfahren codiert wurden, nach dem Hinzufügen von Storage

In einigen Fällen müssen Sie möglicherweise nach dem Hinzufügen neuer Storage-Nodes einen Ausgleich für Daten schaffen, die mit Erasure Coding versehen sind.

Was Sie benötigen

- Sie müssen die Erweiterungsschritte abgeschlossen haben, um die neuen Speicherknoten hinzuzufügen.
- Sie müssen die Überlegungen für eine Ausbalancierung, wenn Daten zur Fehlerkorrektur codiert wurden, überprüft haben.

  "Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind"

> Führen Sie diesen Vorgang nur aus, wenn die Warnung **Low Object Storage** für einen oder mehrere Speicherknoten an einem Standort ausgelöst wurde und Sie die empfohlene Anzahl neuer Speicherknoten nicht hinzufügen konnten.

- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Wenn das EC-Ausgleichverfahren ausgeführt wird, ist die Performance von ILM-Vorgängen sowie S3- und Swift-Client-Operationen wahrscheinlich beeinträchtigt. Aus diesem Grund sollten Sie dieses Verfahren nur in begrenzten Fällen durchführen.

> Das EG-Ausgleichverfahren 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-Ausgleichverfahren fehl. Speicherreservierungen werden freigegeben, wenn der EC-Ausgleichvorgang abgeschlossen ist, unabhängig davon, ob der Vorgang fehlgeschlagen oder erfolgreich war.

> S3- und Swift-API-Operationen zum Hochladen von Objekten (oder Objektteilen) können während des EC-Ausgleichs fehlschlagen, wenn sie mehr als 24 Stunden benötigen. Langfristige PUT-Vorgänge funktionieren nicht, wenn die anwendbare ILM-Regel eine strenge oder ausgewogene 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. Halten Sie den Mauszeiger über das Diagramm „verwendete Daten – Objektdaten“, um die aktuelle Menge der replizierten Daten und mit Erasure Coding versehenen Daten auf dem Storage-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. Geben Sie den folgenden Befehl ein:

   ```
   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-Ausgleichvorgang 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.
   - Wenn der Status lautet `Failure`, Führen Sie die Fehlerschritte.
   - Wenn der Status lautet `Success`, Führen Sie die Erfolg.
7. Wenn das EC-Ausgleichverfahren 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-Ausgleichverfahren beenden müssen (z. B. um ein StorageGRID-Software-Upgrade durchzuführen), geben Sie Folgendes ein:

   ```
   rebalance-data abort --job-id job-id
   ```

Wenn Sie ein EC-Ausgleichverfahren beenden, verbleiben alle bereits verschobenen Datenfragmente am neuen Standort. Daten werden nicht zurück an den ursprünglichen Speicherort verschoben.

9. Wenn der Status des EC-Ausgleichs lautet `Failure`, Folgen Sie folgenden Schritten:
   a. Vergewissern Sie sich, dass alle Speicherknoten am Standort mit dem Raster verbunden sind.
   b. Überprüfen Sie, ob Warnmeldungen vorliegen, die sich auf diese Speicherknoten auswirken könnten, und beheben Sie sie.

      Informationen zu bestimmten Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung.

   c. Starten Sie das EC-Ausgleichverfahren neu:
      `rebalance-data start --job-id job-id`
   d. Wenn der Status des EC-Ausgleichs noch immer ist `Failure`, Wenden Sie sich an den technischen Support.
10. Wenn der Status des EC-Ausgleichs-Verfahrens 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.

    Replizierte Objektdaten werden nicht durch das EC-Ausgleichverfahren verschoben.

11. Wenn Sie Erasure Coding an mehreren Standorten verwenden, führen Sie dieses Verfahren für alle anderen betroffenen Standorte aus.

Verwandte Informationen

"Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind"

"Monitor Fehlerbehebung"

Kontakt mit dem 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-Betriebssystems, während Port 22 der SSH-Port des Docker Containers ist, auf dem 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	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf` (Für jeden ausgefallenen Node) • `/var/log/storagegrid/nodes/<node-name>.log` (Für jeden ausgefallenen Node; ist möglicherweise nicht vorhanden)

Halten Sie Recoverys ein

Erfahren Sie, wie Sie einen Hotfix anwenden, einen ausgefallenen Grid-Node wiederherstellen, Grid-Nodes und -Standorte ausmustern und Objekte im Falle eines Systemausfalls wiederherstellen.

- "Einführung in StorageGRID Recovery und Wartung"
- "StorageGRID Hotfix Verfahren"
- "Verfahren zur Recovery von Grid-Nodes"
- "Durchführen der Standortwiederherstellung durch den technischen Support"
- "Verfahren zur Deaktivierung"
- "Netzwerkwartungsverfahren"
- "Verfahren auf Host-Ebene und Middleware"
- "Verfahren für den Grid-Node"
- "Klonen von Appliance-Nodes"

Einführung in StorageGRID Recovery und Wartung

Die Recovery- und Wartungsverfahren für StorageGRID umfassen die Anwendung eines Software-Hotfix, die Wiederherstellung von Grid-Nodes, die Wiederherstellung eines ausgefallenen Standorts, die Stilllegung von Grid-Nodes oder einem gesamten Standort, die Durchführung von Netzwerkwartung, die Durchführung von Wartungsvorgängen auf

Host- und Middleware-Ebene sowie die Durchführung von Grid Node-Verfahren.

Alle Recovery- und Wartungsaktivitäten erfordern ein umfassendes Verständnis des StorageGRID Systems. Sie sollten die Topologie Ihres StorageGRID Systems überprüfen, um sicherzustellen, dass Sie die Grid-Konfiguration kennen.

Sie müssen alle Anweisungen genau befolgen und alle Warnungen beachten.

Nicht beschriebene Wartungsmaßnahmen werden nicht unterstützt oder erfordern ein Serviceprojekt.

Hardwareverfahren finden Sie in der Installations- und Wartungsanleitung für Ihre StorageGRID Appliance.

> „Linux“ bezieht sich auf eine Red hat® Enterprise Linux®-, Ubuntu®-, CentOS- oder Debian®-Bereitstellung. Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Verwandte Informationen

"Gittergrundierung"

"Netzwerkrichtlinien"

"StorageGRID verwalten"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"NetApp Interoperabilitäts-Matrix-Tool"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024

Browserbreite	Pixel
Optimal	1280

Herunterladen des Wiederherstellungspakets

Die Wiederherstellungspakedatei ermöglicht Ihnen die Wiederherstellung des StorageGRID-Systems bei einem Fehler.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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:
   a. Öffnen Sie das `.zip` Datei:
   b. Bestätigen Sie, dass es ein gpt-Backup-Verzeichnis und eine interne enthält `.zip` Datei:
   c. Entnehmen Sie die Innenseite `.zip` Datei:
   d. Bestätigen Sie, dass Sie den öffnen können `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.

Verwandte Informationen

"StorageGRID verwalten"

StorageGRID Hotfix Verfahren

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"
- "Auswirkungen auf Ihr System beim Anwenden eines Hotfix"
- "Beschaffung der erforderlichen Materialien für einen Hotfix"
- "Hotfix-Datei wird heruntergeladen"
- "Überprüfen Sie den Zustand des Systems, bevor Sie einen Hotfix anwenden"
- "Anwenden des Hotfix"

Überlegungen für die Anwendung eines Hotfix

Wenn Sie einen Hotfix anwenden, wird eine kumulative Reihe von Softwareupdates auf die Knoten in Ihrem StorageGRID-System angewendet.

Ein StorageGRID-Hotfix kann nicht angewendet werden, wenn ein anderer Wartungsvorgang ausgeführt wird. Sie können beispielsweise keinen Hotfix anwenden, während ein Decommission-, Expansions- oder Wiederherstellungsverfahren 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.

> Je nach Bedarf zur Anpassung der Grid-Version können Sie beim Bereitstellen des Node eine Nebenversion verwenden; es ist nicht erforderlich, das Hauptversion zuerst zu implementieren.

4. Anschließend wenden Sie Hotfix 11.*A.B.y* auf den primären Admin-Node an.

Verwandte Informationen

"Konfigurieren des primären Ersatzadministratorknotens"

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. Informationen zum Konfigurieren von Hochverfügbarkeitsgruppen finden Sie in den Anweisungen zur Administration von StorageGRID.

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. das Angeben von Grid Network Subnets oder das Genehmigen ausstehender Grid-Nodes), bis der Hotfix auf alle Nodes angewendet wurde.

- Aktualisieren Sie die ILM-Konfiguration erst, wenn der Hotfix auf alle Knoten angewendet wurde.

Beschaffung der erforderlichen Materialien für einen Hotfix

Bevor Sie einen Hotfix anwenden, müssen Sie alle erforderlichen Materialien erhalten.

Element	Hinweise
StorageGRID-Hotfix-Datei	Sie müssen die StorageGRID-Hotfix-Datei herunterladen.
• Netzwerkport • Unterstützter Webbrowser • SSH-Client (z. B. PuTTY)	Siehe „`Webbrowser-Anforderungen`“.
Wiederherstellungspaket (`.zip`) Datei	Vor dem Anwenden eines Hotfix, laden Sie die neueste Wiederherstellungspaket-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.
Passwords.txt-Datei	Optional und nur verwendet, wenn Sie einen Hotfix manuell mit dem SSH-Client anwenden. Der `Passwords.txt` Die Datei ist im GENANNTEN Paket enthalten, das Teil des Wiederherstellungspakets ist `.zip` 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 `Passwords.txt` Datei:
Zugehörige Dokumentation	`readme.txt` Datei für den Hotfix. Diese Datei ist auf der Download-Seite des Hotfix enthalten. Schauen Sie sich die an `readme` Vor dem Anwenden des Hotfix sorgfältig ablesen.

Verwandte Informationen

"Hotfix-Datei wird heruntergeladen"

"Herunterladen des Wiederherstellungspakets"

Hotfix-Datei wird heruntergeladen

Sie müssen die Hotfix-Datei herunterladen, bevor Sie den Hotfix anwenden können.

Schritte

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "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 gerade den primären Admin-Knoten wiederhergestellt haben und einen Hotfix anwenden müssen, 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**.

Verwandte Informationen

"Konfigurieren des primären Ersatzadministratorknotens"

Überprüfen Sie den Zustand des Systems, bevor Sie einen Hotfix anwenden

Sie müssen überprüfen, ob das System bereit ist, um den Hotfix aufzunehmen.

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
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.

   Informationen zu bestimmten Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

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 ein Decommission-, Expansions- oder Wiederherstellungsverfahren 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.

Verwandte Informationen

"Monitor Fehlerbehebung"

"Anhalten und Fortsetzen des Stilllegen-Prozesses für Storage Nodes"

Anwenden des Hotfix

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.

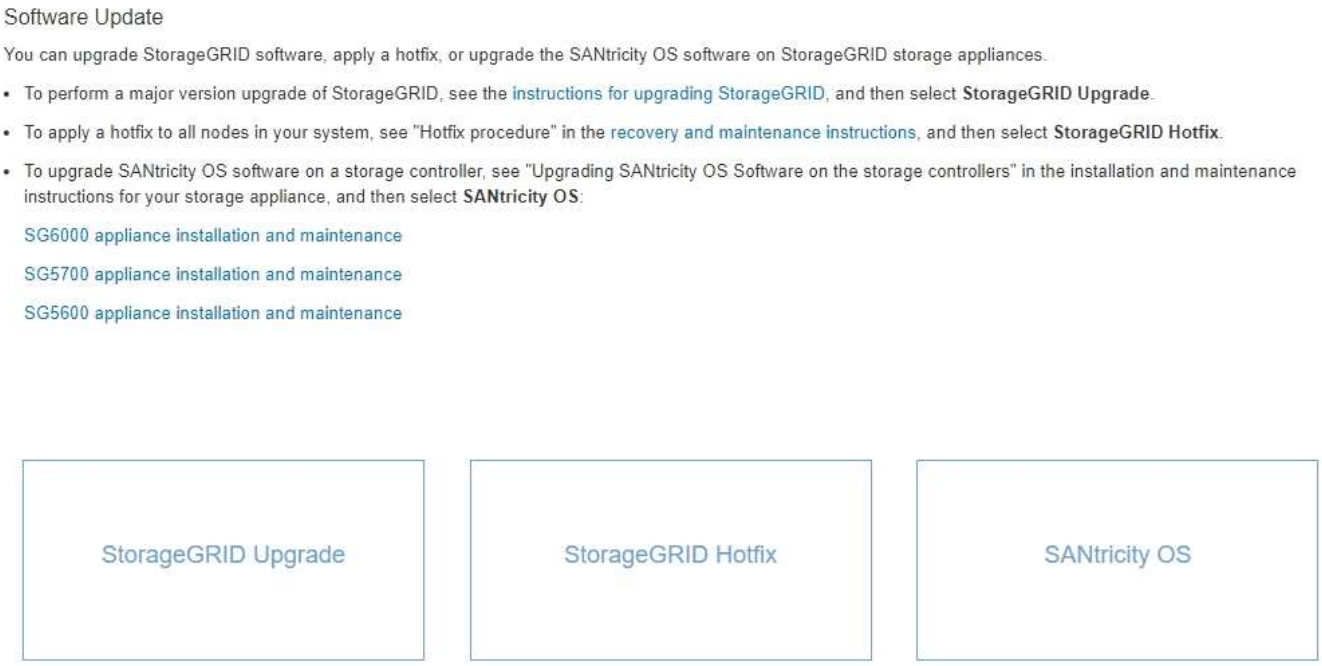
Was Sie benötigen

- Sie haben alle Überlegungen geprüft und alle Schritte in “Hotfix Planung und Vorbereitung.” abgeschlossen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen über Root Access oder die Wartungsberechtigung verfügen.
- 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 erst nach Abschluss des Hotfix-Vorgangs ein StorageGRID Software-Upgrade oder ein SANtricity OS-Upgrade durchführen.

Schritte

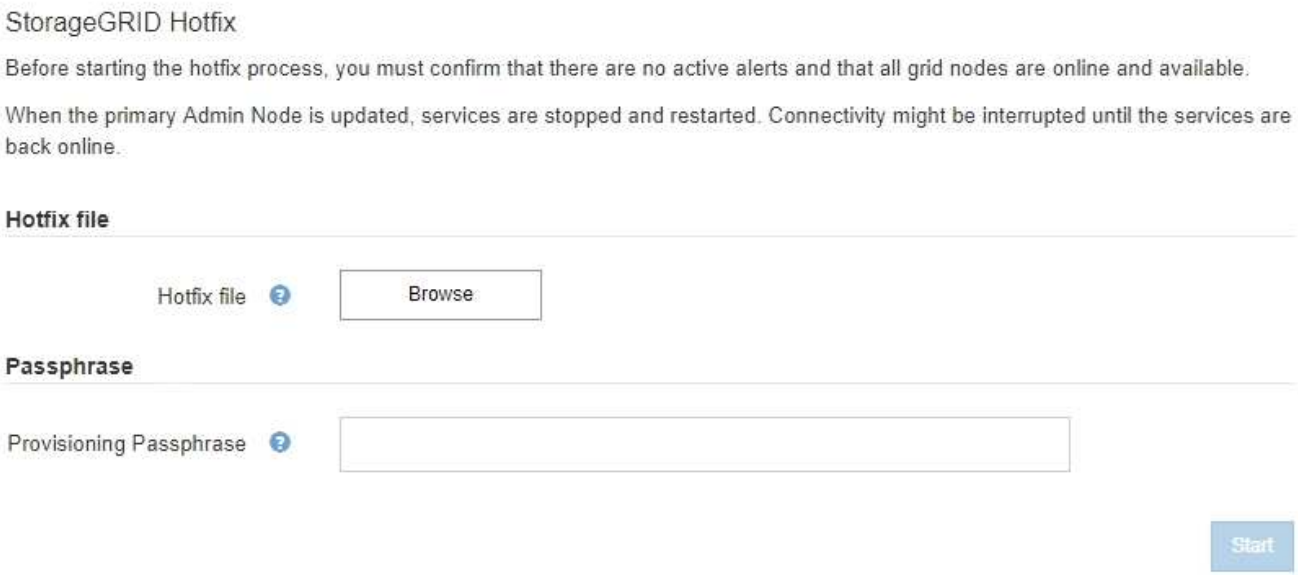
1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. Wählen Sie **Wartung System Software-Update**.

   Die Seite Software-Aktualisierung wird angezeigt.



3. Wählen Sie **StorageGRID Hotfix**.

   Die Seite StorageGRID Hotfix wird angezeigt.



4. Wählen Sie die Hotfix-Datei aus, die Sie von der NetApp Support-Webseite heruntergeladen haben.

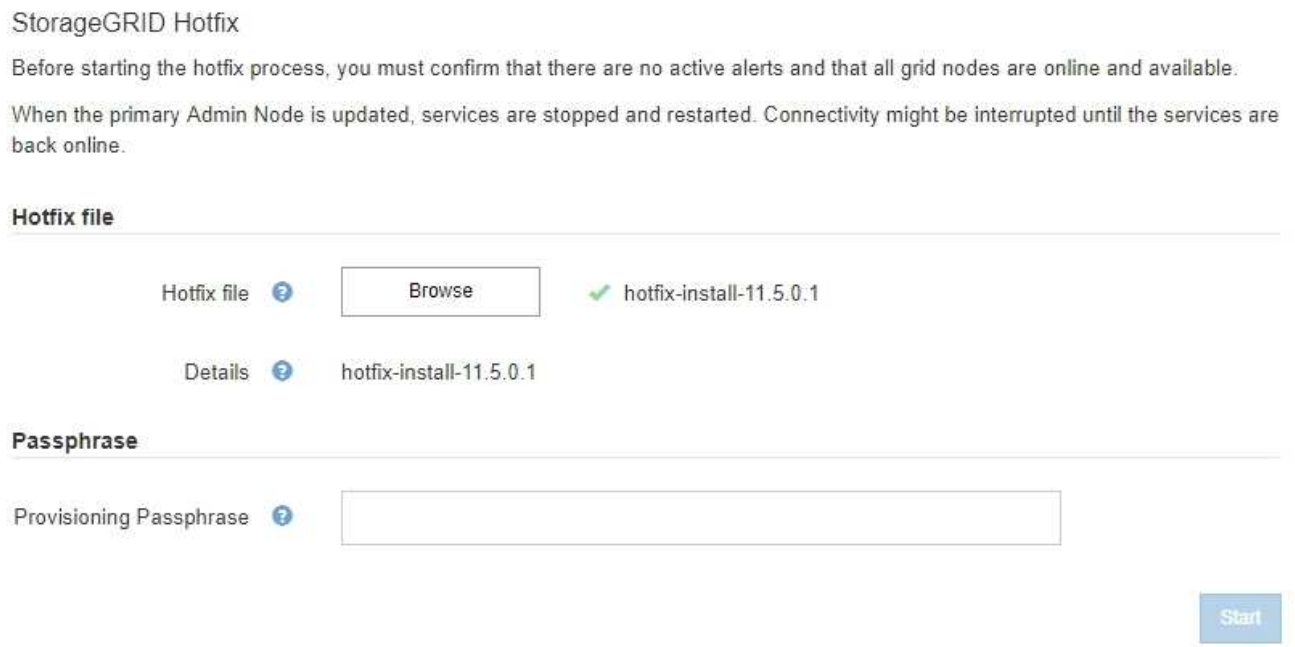
   a. Wählen Sie **Durchsuchen**.
   b. Suchen und wählen Sie die Datei aus.

      `hotfix-install-version`

   c. Wählen Sie **Offen**.

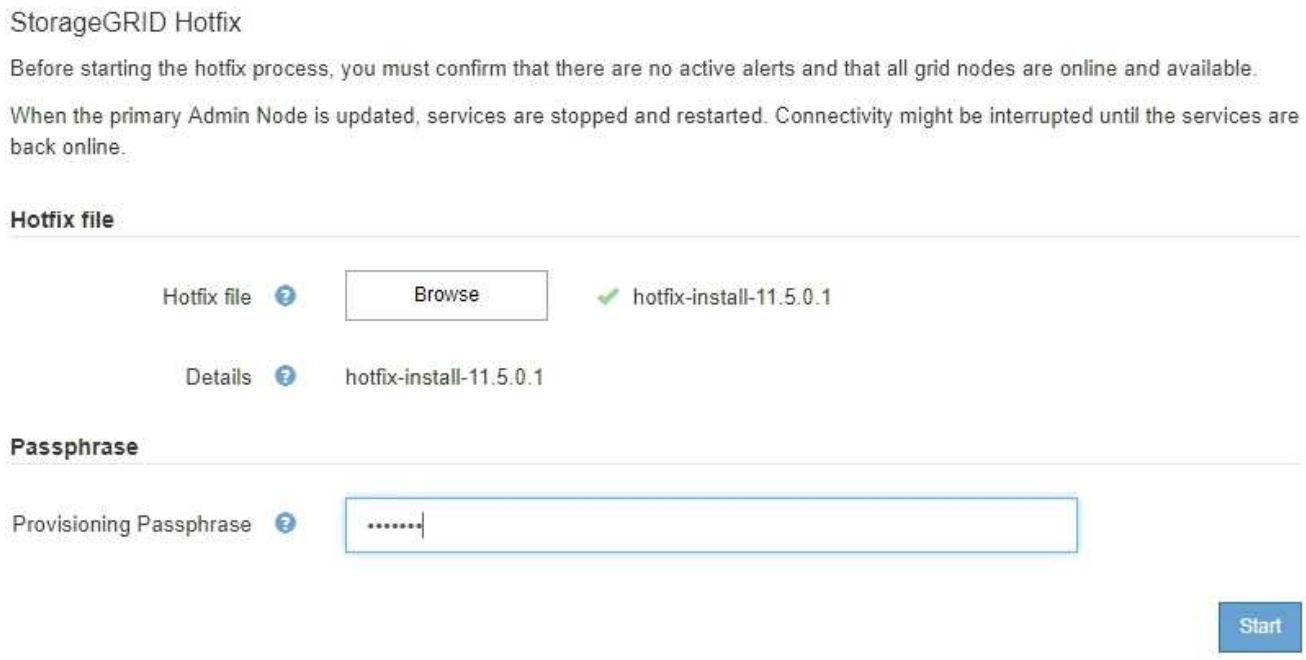
      Die Datei wurde hochgeladen. Nach Abschluss des Uploads wird der Dateiname im Feld Details angezeigt.

Ändern Sie den Dateinamen nicht, da er Teil des Verifizierungsvorgangs 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:

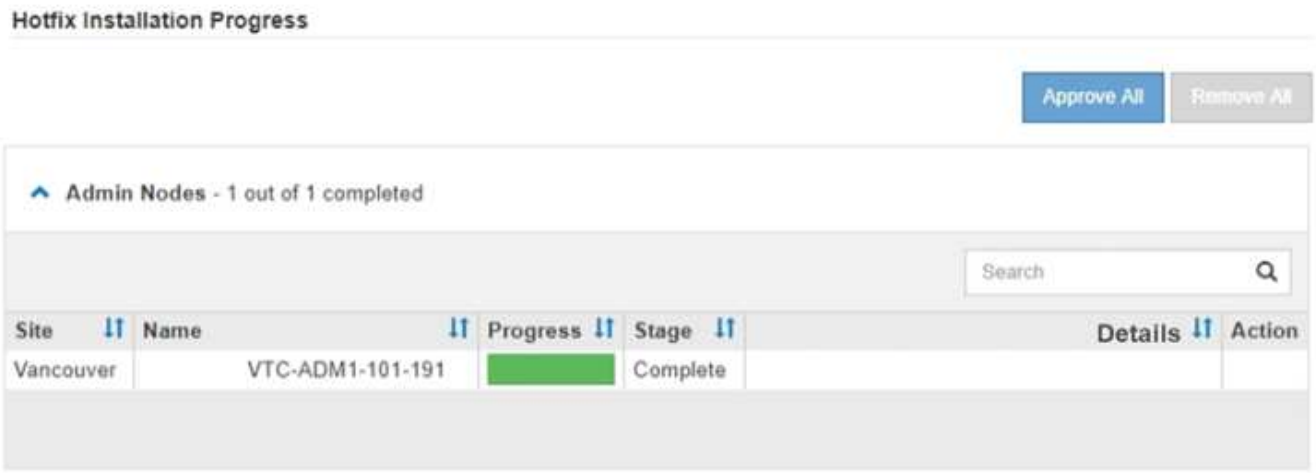
a. Die Hotfix-Validierungen werden ausgeführt.

> 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 in der Tabelle aufgeführten Nodes sind nach Typ gruppiert:

- Admin-Nodes
- Gateway-Nodes
- Storage-Nodes
- Archiv-Nodes

> Der Fortschrittsbalken erreicht den Abschluss, und dann wird der primäre Admin-Node zuerst mit der Phase „`Complete`“ angezeigt.



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 nicht für einen Knoten, es sei denn, Sie sind sicher, dass der Knoten bereit ist, aktualisiert zu werden.Wenn das Hotfix auf einen Grid-Knoten angewendet wird, werden einige Dienste auf diesem Knoten möglicherweise 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.

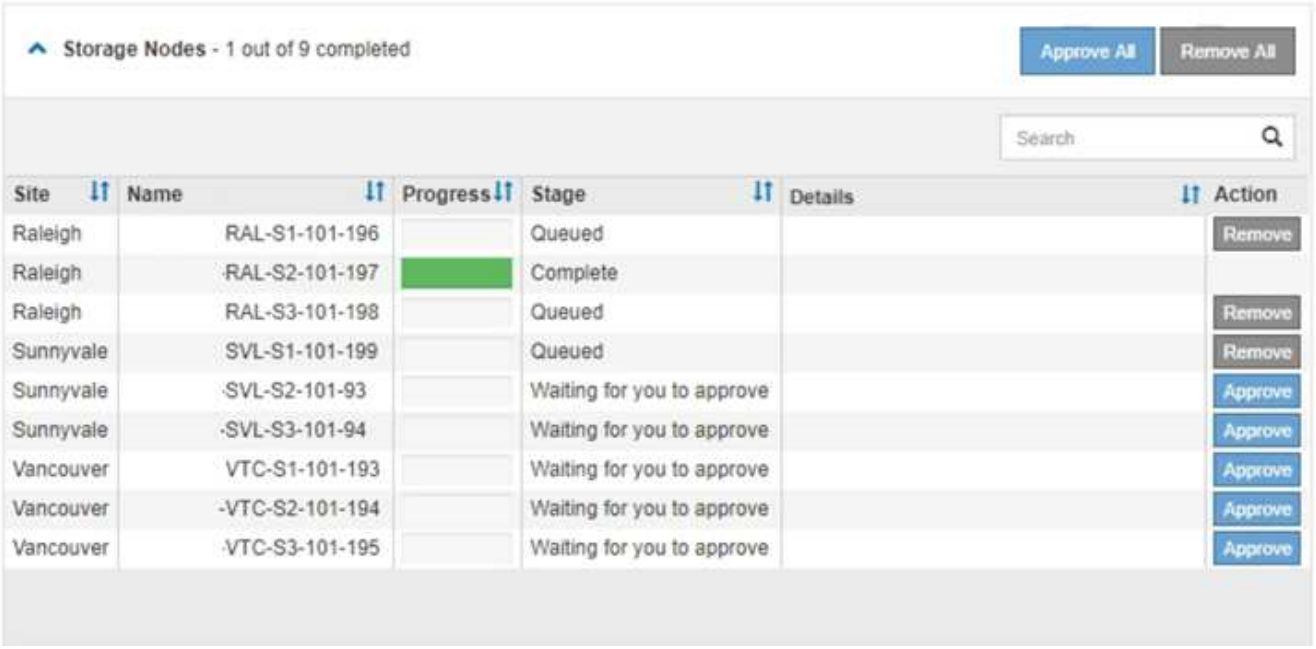
Die Schaltfläche **Alle genehmigen** oben auf der Seite genehmigt alle Knoten, die auf der Seite aufgeführt sind, während die Schaltfläche **Alle genehmigen** oben in einer Tabellengruppierung nur alle Knoten in dieser Gruppe genehmigt. Wenn die Reihenfolge, in der Knoten aktualisiert werden, wichtig 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.

10. Wenn Sie einen Knoten oder alle Knoten aus der Hotfix-Warteschlange entfernen müssen, wählen Sie **Entfernen** oder **Alle entfernen**.

    Wie im Beispiel gezeigt, wird die Phase über „`Queued`“ hinaus ausgeblendet und Sie können den Knoten nicht mehr aus dem Hotfix-Prozess entfernen.



11. Warten Sie, bis der Hotfix auf jeden genehmigten Grid-Knoten angewendet wird.

    Wenn der Hotfix erfolgreich auf allen Knoten installiert wurde, wird die Fortschrittstabelle für die Hotfix-Installation geschlossen. Ein grünes Banner zeigt das Datum und die Uhrzeit an, zu der der Hotfix abgeschlossen wurde.

12. 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.

Verwandte Informationen

"Hotfix Planung und Vorbereitung"

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

Verfahren zur Recovery von Grid-Nodes

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 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 wiederherzustellenden Datenmenge maximiert und Ihre Geschäftsziele erreicht.

Verwandte Informationen

"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 Festplattenschnappschüsse, um Grid-Knoten 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 Version für das Installationsprogramm der StorageGRID Appliance auf der Ersatz-Appliance entspricht der Softwareversion Ihres StorageGRID Systems, wie in der Hardwareinstallation und -Wartung zum Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance beschrieben.
  - "SG100 SG1000 Services-Appliances"
  - "SG5600 Storage Appliances"
  - "SG5700 Storage-Appliances"
  - "SG6000 Storage-Appliances"
- 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 mithilfe 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.

Sammeln der erforderlichen Materialien für die Recovery von Grid Nodes

Bevor Sie Wartungsmaßnahmen durchführen, müssen Sie sicherstellen, dass die zur Wiederherstellung eines ausgefallenen Grid-Node erforderlichen Materialien vorhanden sind.

Element	Hinweise
StorageGRID Installationsarchiv	Wenn Sie einen Grid-Knoten wiederherstellen müssen, benötigen Sie das StorageGRID Installationsarchiv für Ihre Plattform. **Hinweis:** Sie müssen keine Dateien herunterladen, wenn Sie fehlgeschlagene Speichervolumen auf einem Speicherknoten wiederherstellen.
Wiederherstellungspaket `.zip` Datei	Erhalten Sie eine Kopie des aktuellsten Wiederherstellungspakets `.zip` Datei: `sgws-recovery-package-id-revision.zip` 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. Wenn der primäre Admin-Node normal funktioniert, können Sie das Wiederherstellungspaket aus dem Grid Manager herunterladen. Wählen Sie **Wartung System Wiederherstellungspaket**. Wenn Sie nicht auf den Grid Manager zugreifen können, können Sie auf einigen Speicherknoten, die den ADC-Dienst enthalten, verschlüsselte Kopien des Wiederherstellungspakets finden. Untersuchen Sie auf jedem Speicherknoten diesen Speicherort für das Wiederherstellungspaket: `/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg` Verwenden Sie das Wiederherstellungspaket mit der höchsten Versionsnummer.
`Passwords.txt` Datei	Enthält die Passwörter, die für den Zugriff auf Grid-Nodes in der Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.
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:
Aktuelle Dokumentation für Ihre Plattform	Die derzeit unterstützten Versionen Ihrer Plattform finden Sie im Interoperabilitäts-Matrix-Tool. "NetApp Interoperabilitäts-Matrix-Tool" Dokumentation finden Sie auf der Website des Plattformanbieters.

Verwandte Informationen

"Herunterladen und Extrahieren der StorageGRID-Installationsdateien"

"Anforderungen an einen Webbrowser"

Bevor Sie StorageGRID Grid-Nodes wiederherstellen können, müssen Sie die Software herunterladen und die Dateien extrahieren.

Sie müssen die Version von StorageGRID verwenden, die derzeit im Raster ausgeführt wird.

Schritte

1. Bestimmen Sie, welche Version der Software derzeit installiert ist. Gehen Sie vom Grid Manager zu **Hilfe über**.
2. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

   "NetApp Downloads: StorageGRID"

3. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.

   StorageGRID-Software-Versionen 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**.
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
VMware	StorageGRID-Webscale-*version*-VMware-*uniqueID*.zip StorageGRID-Webscale-*Version*-VMware-*uniqueID*.tgz
Red hat Enterprise Linux oder CentOS	StorageGRID-Webscale-*version*-RPM-*uniqueID*.zip StorageGRID-Webscale-*Version*-RPM-*uniqueID*.tgz
Ubuntu oder Debian Oder Appliances	StorageGRID-Webscale-*version*-DEB-*uniqueID*.zip StorageGRID-Webscale-*Version*-DEB-*uniqueID*.tgz
OpenStack oder anderen Hypervisor	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 zum Ersetzen eines Linux-Knotens.

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 VMware-System wiederherstellen, 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.
/vsphere/NetApp-SG-*Version*-SHA.vmdk	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.
/vsphere/vsphere-Archive.ovf ./vsphere/vsphere-Archive.mf	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 Speicherknoten.
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 `deploy-vsphere-ovftool.sh` Skript:
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.

Pfad und Dateiname	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:

10. Wenn Sie ein Red hat Enterprise Linux oder CentOS System wiederherstellen, 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 `configure-storagegrid.py` Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.

Pfad und Dateiname	Beschreibung
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` 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.

11. Wenn Sie ein Ubuntu oder Debian-System wiederherstellen, 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 `/debs/storagegrid-webscale-images-version-SHA.deb`
	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.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` Skript:

Pfad und Dateiname	Beschreibung
	Eine leere Konfigurationsdatei für die Verwendung mit dem `configure-storagegrid.py` 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.

12. 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.
	Prüfsumme des DEB-Installationspakets, das vom Installationsprogramm der StorageGRID-Appliance verwendet wird, um zu überprüfen, ob das Paket nach dem Hochladen intakt ist.

Hinweis: für die Installation von Geräten sind diese Dateien nur erforderlich, wenn Sie den Netzwerkverkehr vermeiden müssen. Die Appliance kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Verwandte Informationen

"VMware installieren"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Auswählen eines Wiederherstellungsverfahrens für Knoten

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"

Grid-Node	Wiederherstellungsvorgang
Ein einzelner Storage-Node	Das Speicherknoten-Wiederherstellungsverfahren hängt vom Typ und der Dauer des Ausfalls ab. "Wiederherstellung nach Storage-Node-Ausfällen"
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 von 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 Storage-Node-Ausfällen

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
• Mehr als ein Speicherknoten ist ausgefallen. • Ein zweiter Speicherknoten ist weniger als 15 Tage nach Ausfall oder Wiederherstellung eines Speicherknotens ausgefallen. Dies schließt den Fall ein, dass ein Speicherknoten während der Wiederherstellung eines anderen Speicherknoten noch in Arbeit ist.	Wenden Sie sich an den technischen Support.	Wenn sich alle ausgefallenen Speicherknoten am selben Standort befinden, ist es möglicherweise erforderlich, ein Verfahren zur Standortwiederherstellung durchzuführen. Der technische Support prüft Ihre Situation und erstellt einen Recovery-Plan. "Durchführen der Standortwiederherstellung durch den technischen Support" 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. Der technische Support kann bestimmen, wann die Wiederherstellung eines zweiten Storage Node sicher gestartet werden kann. **Hinweis**: Wenn mehr als ein Speicherknoten, der den ADC-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattformdienstanfragen für diesen Standort.
Ein Speicherknoten ist seit mehr als 15 Tagen offline.	"Wiederherstellen eines Speicherknoten, der länger als 15 Tage ausgefallen ist"	Dieses Verfahren ist erforderlich, um die Integrität der Cassandra-Datenbank sicherzustellen.
Ein Appliance-Speicherknoten ist fehlgeschlagen.	"Wiederherstellen eines Speicherknoten für StorageGRID-Geräte"	Das Wiederherstellungsverfahren für Appliance Storage Nodes ist bei allen Ausfällen gleich.
Ein oder mehrere Storage-Volumes sind ausgefallen, das Systemlaufwerk ist jedoch intakt	"Die Wiederherstellung nach einem Ausfall des Storage-Volumes ist bei intaktem Systemlaufwerk möglich"	Dieses Verfahren wird für softwarebasierte Speicherknoten verwendet.

Problem	Aktion	Hinweise
Das Systemlaufwerk ist ausgefallen.	"Wiederherstellung nach einem Systemausfall"	Das Verfahren zum Austausch der Nodes hängt von der Implementierungsplattform ab und ob auch Storage Volumes ausgefallen sind.

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.

Wiederherstellen eines Speicherknoten, der länger als 15 Tage ausgefallen ist

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.

Was Sie benötigen

- 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 die Option **Wartung Wartungsaufgaben Dekommission**.)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Erweiterung**.)

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 Storage-Node kann erst wieder dem Grid beitreten, wenn Cassandra mithilfe von Informationen anderer Storage-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 den folgenden Wiederherstellungsvorgang 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 den folgenden Wiederherstellungsvorgang nicht durch. Es kann zu Datenverlusten kommen.

Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Wenden Sie sich an den technischen Support.

"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 das Verfahren zum Wiederherstellen nach einem Systemausfall durch. "Wiederherstellung nach einem Systemausfall"

1. 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 Topology** aus.

   c. Wählen Sie *site* **Storage Node SSM Services** aus. Vergewissern Sie sich, dass der Cassandra-Service angezeigt wird `Not Running`.

   d. Wählen Sie **Storage Node SSM Ressourcen**. 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
```

2. Geben Sie diesen Befehl ein, und überwachen Sie die Skriptausgabe: `check-cassandra-rebuild`
   - Wenn Speicherservices ausgeführt werden, werden Sie aufgefordert, diese zu beenden. Geben Sie ein: **Y**
   - 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.

3. Führen Sie nach Abschluss der Neuerstellung die folgenden Prüfungen durch:
   a. Wählen Sie im Grid Manager **Support Tools Grid Topology** aus.
   b. Wählen Sie *site* **wiederhergestellten Speicherknoten 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.

Verwandte Informationen

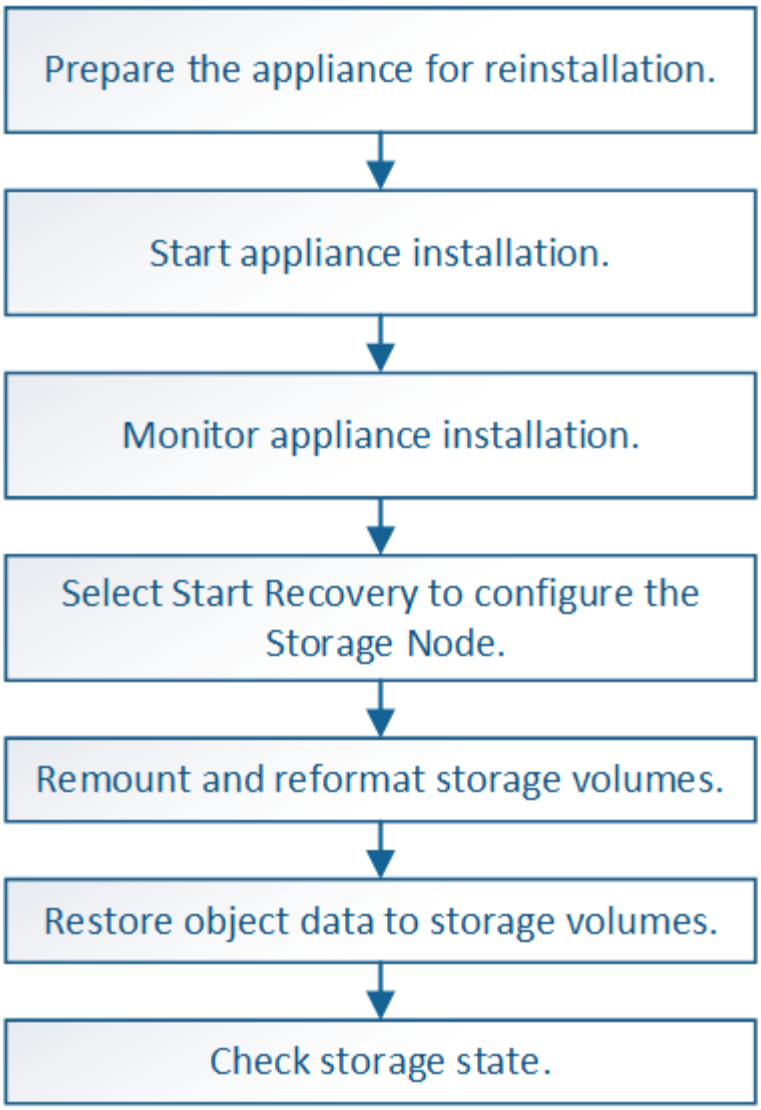
"Wiederherstellung nach einem Systemausfall"

Wiederherstellen eines Speicherknoten für StorageGRID-Geräte

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-Volumes durchführen.

Über diese Aufgabe

Sie müssen die Appliance vorbereiten und Software neu installieren, den Node so konfigurieren, dass er wieder in das Grid eingespeist wird, Speicher neu formatiert und Objektdaten wiederhergestellt werden.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie den folgenden Wiederherstellungsvorgang 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. Wenden Sie sich an den technischen Support.

"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 „Service: Status – Cassandra (SVST)“ (Service: Status – Cassandra) ausgegeben wird, lesen Sie die Überwachungs- und Fehlerbehebungsanweisungen zur Wiederherstellung des Alarms durch Neuaufbau von Cassandra. 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-Wartungsarbeiten, wie z. B. Anweisungen zum Austausch eines Controllers oder zur Neuinstallation von SANtricity OS, finden Sie in der Installations- und Wartungsanleitung für Ihre Storage Appliance.

Verwandte Informationen

"Monitor Fehlerbehebung"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Schritte

- "Vorbereiten eines Appliance-Speicherknotens zur Neuinstallation"
- "Starten der Installation der StorageGRID Appliance"
- "Überwachen der Installation der StorageGRID Appliance"
- "Wählen Sie Wiederherstellung starten, um einen Appliance-Speicherknoten zu konfigurieren"
- "Erneutes Mounten und Neuformatieren von Appliance-Storage-Volumes („`MAnual Steps`“)"
- "Wiederherstellung von Objektdaten auf einem Storage Volume für eine Appliance"
- "Überprüfen des Speicherstatus nach der Wiederherstellung eines Appliance-Speicherknoten"

Vorbereiten eines Appliance-Speicherknotens zur Neuinstallation

Wenn Sie einen Appliance-Speicherknoten wiederherstellen, müssen Sie zuerst die Appliance für die Neuinstallation der StorageGRID-Software vorbereiten.

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.

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 der Installation der StorageGRID Appliance

Um StorageGRID auf einem Appliance-Speicherknoten zu installieren, verwenden Sie das StorageGRID-Appliance-Installationsprogramm, das in der Appliance enthalten ist.

Was Sie benötigen

- 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 erforderlichen Aufgaben gemäß den Installations- und Wartungsanweisungen für Ihre Storage Appliance ausgeführt:
  - "SG5600 Storage Appliances"
  - "SG5700 Storage-Appliances"
  - "SG6000 Storage-Appliances"
- Sie verwenden einen unterstützten 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 Namen des Knotens an oder bestätigen sie.
- 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.

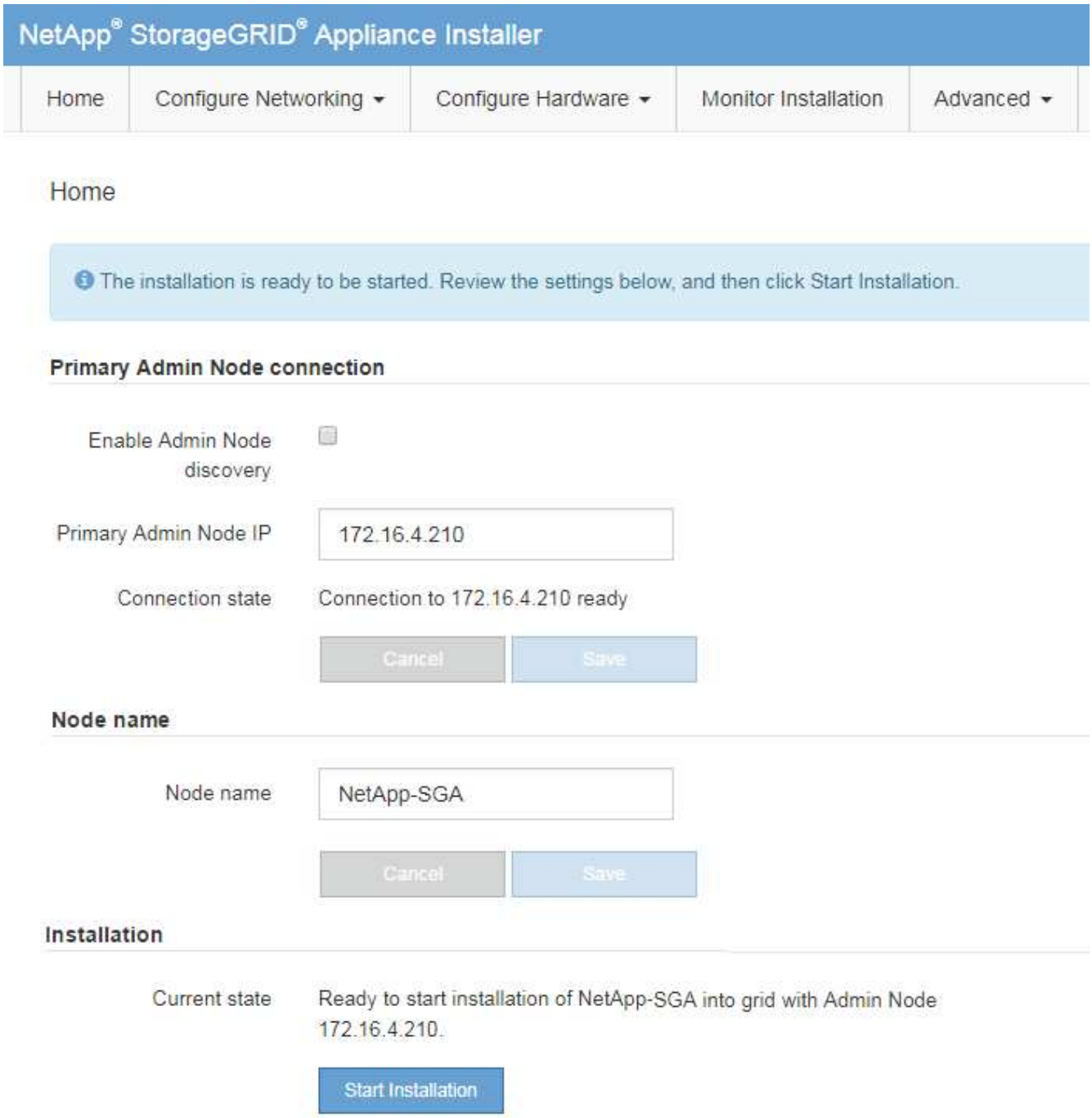
3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Schritte
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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 **Knotenname** den gleichen Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.
5. Bestätigen Sie im Abschnitt Installation, dass der aktuelle Status „`bereit zum Starten der Installation des Knotennamens in das Grid mit Primary 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 Installations- und Wartungsanleitung für Ihr Gerät.

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 in der Menüleiste auf **Monitor-Installation**.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

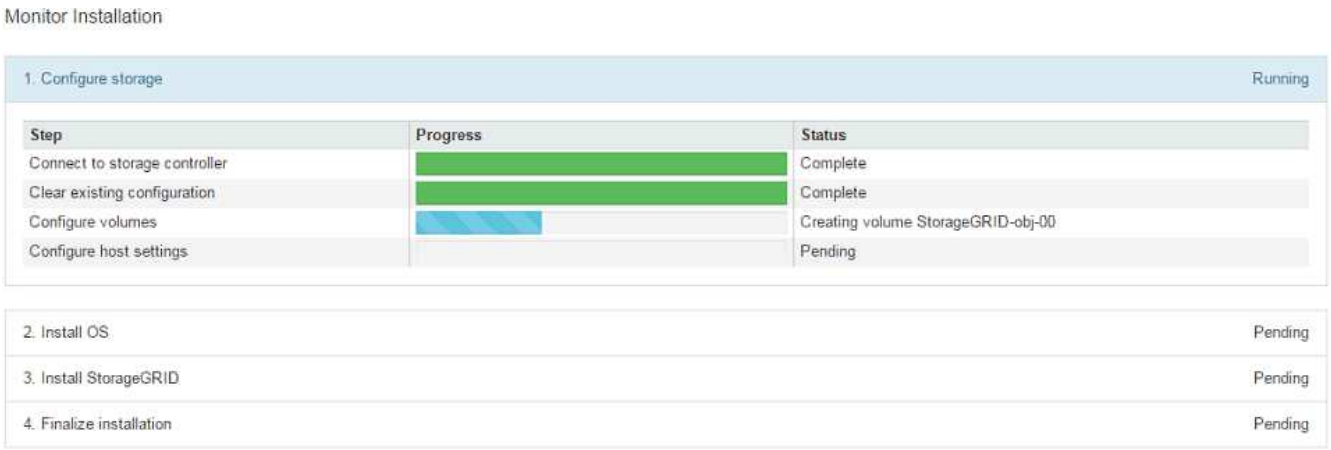
"SG5600 Storage Appliances"

Überwachen der 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.

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

   Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.



   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 „`Skipped.`“ angezeigt.

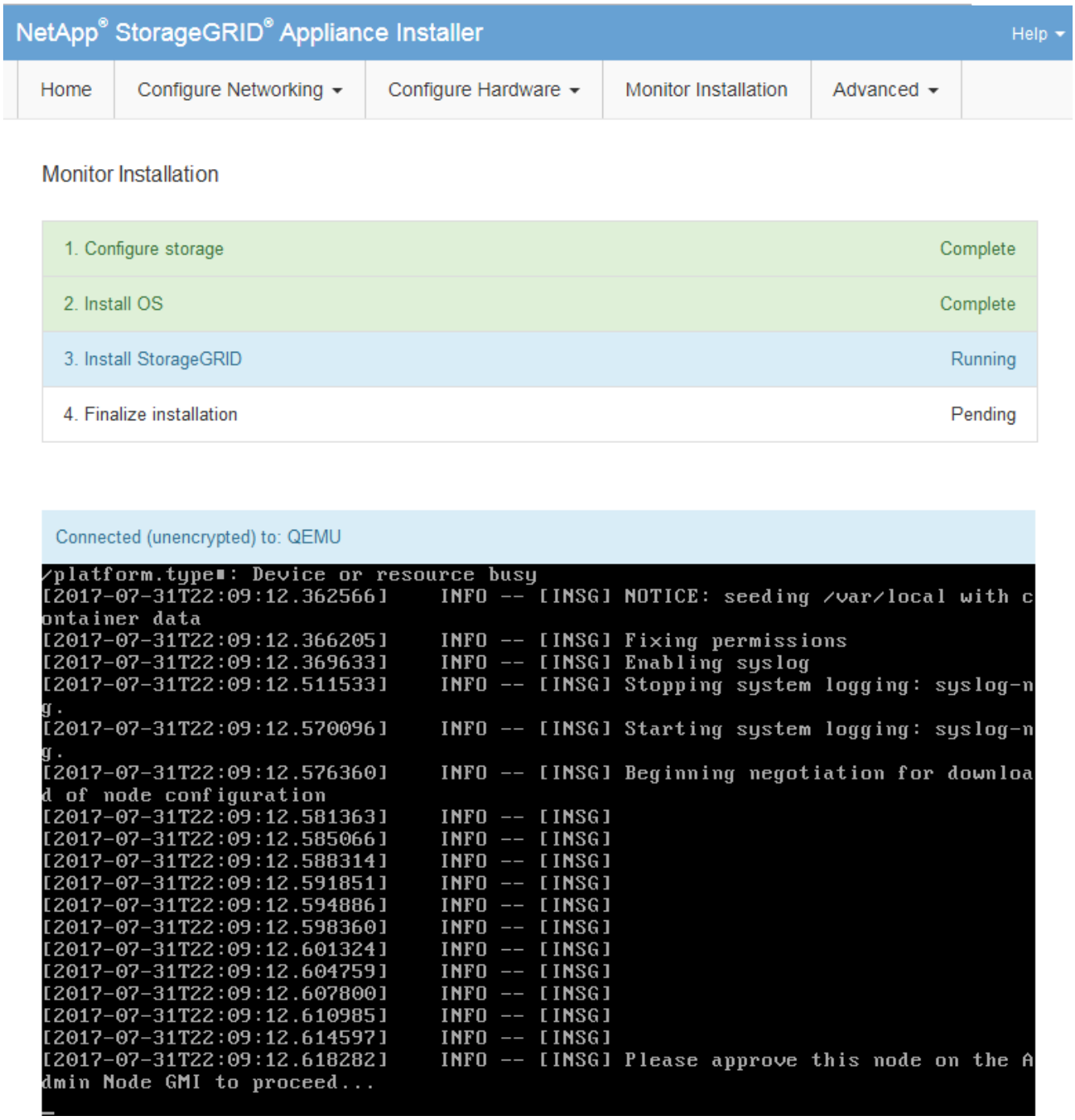
2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.
   - **1. Speicher konfigurieren**

     In dieser Phase stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.

   - **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.



4. Gehen Sie zum Verfahren zum Konfigurieren des Appliance-Speicherknoten.

Wählen Sie Wiederherstellung starten, um einen Appliance-Speicherknoten zu konfigurieren

Sie müssen im Grid Manager die Option Wiederherstellung starten auswählen, um einen Appliance-Speicherknoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

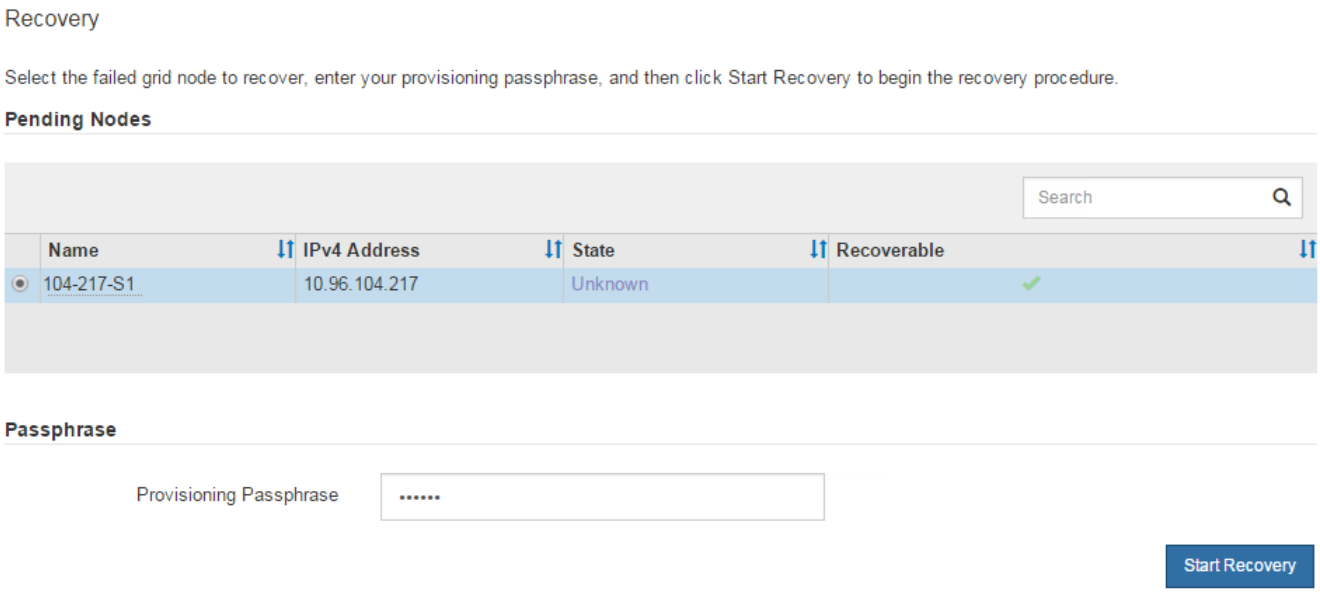
- Sie müssen einen Speicher-Node für die Wiederherstellungsanwendung bereitgestellt haben.
- Sie müssen das Startdatum aller Reparaturaufträge für Daten mit Löschungscode kennen.
- Sie müssen überprüft haben, dass der Speicherknoten innerhalb der letzten 15 Tage nicht neu aufgebaut wurde.

Schritte

1. Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Recovery** aus.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

   Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

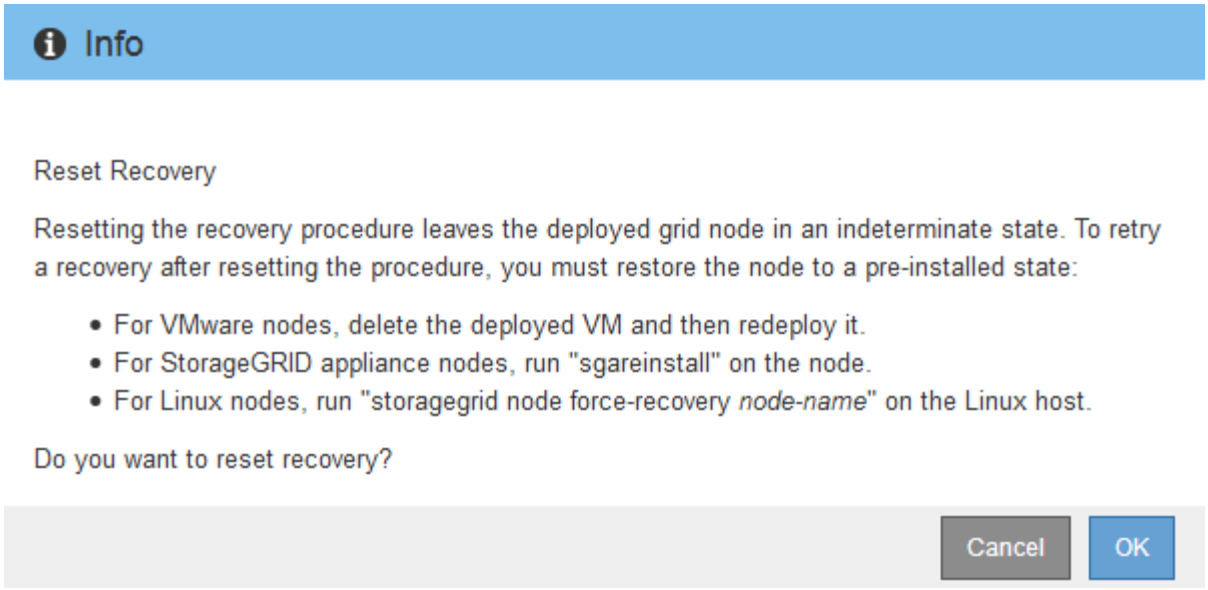
3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten 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. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.



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.

Erneutes Einbinden und Neuformatieren von Speicher-Volumes für Geräte („Manuelle Schritte“)

Führen Sie manuell zwei Skripte aus, um noch intaerte 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.

Was Sie benötigen

- 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 die Option **Wartung Wartungsaufgaben Dekommission**.)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Erweiterung**.)

> 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 Speicherknoten während der Wiederherstellung nicht neu, bevor Sie ausführen `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:
   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.

Do not continue to the next step if you believe that the data
remaining on this volume cannot 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.

Do not continue to the next step if you believe that the data
remaining on this volume cannot 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 kein Speicher-Volume mounten kann, wird 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 `volID` Die Datei stimmt nicht mit der ID für diesen Speicherknoten überein (der `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 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 Speichervolume nicht zu diesem Speicherknoten gehört.

   Im Beispiel enthält die Ausgabe für /dev/sde die folgende Fehlermeldung:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Wenn ein 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 Speicher-Volume nicht angehängt oder nicht ordnungsgemäß formatiert werden kann, und Sie mit dem nächsten Schritt fortfahren, werden das Volume und alle 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 der Meinung sind, dass die in einem ausgefallenen Storage Volume verbliebenen Daten nicht von einer anderen Stelle im Grid wiederhergestellt werden können (falls Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie macht, oder falls 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:

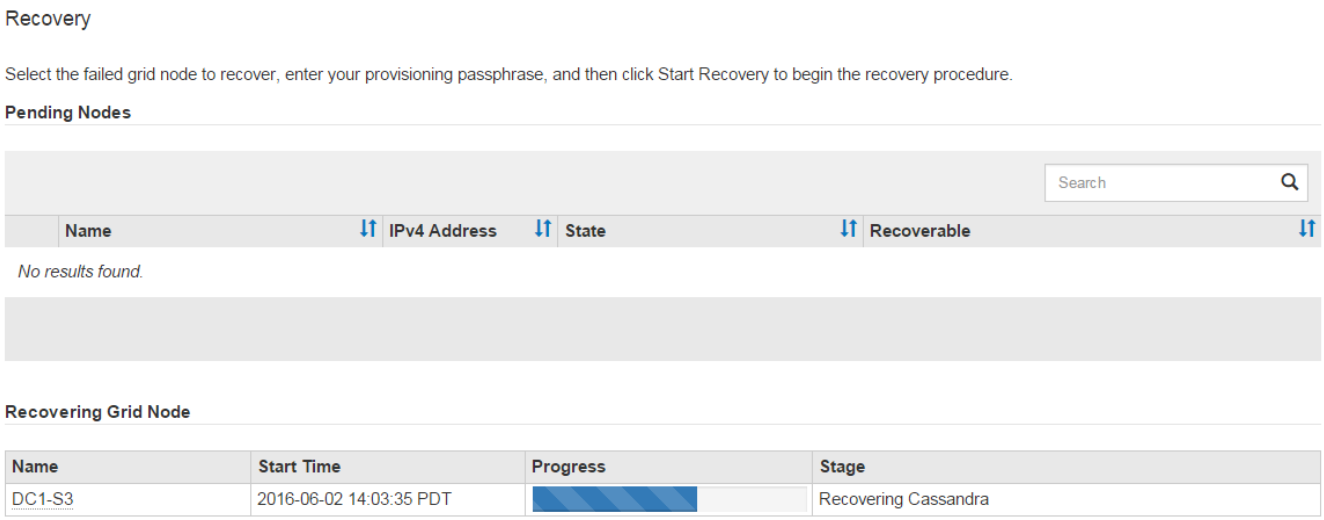
   - Das Skript kann Stunden in Anspruch nehmen.
   - Im Allgemeinen sollten Sie die SSH-Sitzung allein lassen, während das Skript ausgeführt wird.
   - Drücken Sie nicht **Strg+C**, wenn die SSH-Sitzung aktiv ist.
   - Das Skript wird im Hintergrund ausgeführt, wenn eine Netzwerkunterbrechung auftritt 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:



6. Kehren Sie zur Seite „Installation überwachen“ des Installationsprogramms für StorageGRID-Geräte zurück, indem Sie eingeben `http://Controller_IP:8080`, Verwendung der IP-Adresse des Compute-Controllers.

   Auf der Seite „Installation überwachen“ wird der Installationsfortschritt angezeigt, während das Skript ausgeführt wird.

Nach dem `sn-recovery-postinstall.sh` Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speicher-Volumes wiederherstellen, die durch das Skript formatiert wurden, wie im nächsten Verfahren beschrieben.

Verwandte Informationen

"Überprüfen von Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken"

"Wiederherstellung von Objektdaten auf einem Storage Volume für eine Appliance"

Wiederherstellung von Objektdaten auf einem Storage Volume für eine Appliance

Nach der Wiederherstellung von Storage-Volumes für den Appliance-Storage-Node können Sie die Objektdaten wiederherstellen, die bei einem Ausfall des Storage-Node verloren gegangen sind.

Was Sie benötigen

- 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.

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. Aufgrund der Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen dauert die Wiederherstellung von Objektdaten in einen Storage Node aus einem Archiv-Node länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes.

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. Sie verwenden verschiedene Optionen mit dem `repair-data` Skript, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding Daten wiederherstellen:

- **Replizierte Daten**: Für die Wiederherstellung replizierter Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- **Erasure Coded (EC) Data**: Zwei Befehle stehen zur Wiederherstellung von Erasure-codierten Daten zur Verfügung. Dabei wird darauf basierend, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

  Reparaturen an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind. Sie können Reparaturen von Daten, die mit Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```

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.

Weitere Informationen zur Verwendung des `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile 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. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die wiederhergestellten Speicher-Volumes zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`
3. Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. (Wenn nur einige Volumes ausgefallen sind, fahren Sie mit dem nächsten Schritt fort.)

   Sie können nicht ausgeführt werden `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

   - Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

     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
     ```

     Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

   - 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 zum

Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die Erasure Coding-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 an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

- Wenn im Grid Daten repliziert und mit Erasure-Coding-Verfahren codiert sind, führen Sie beide Befehle aus.

4. Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren.

   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.

   - Wenn Ihr Grid replizierte Daten enthält, verwenden Sie das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. 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
```

> Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

- 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. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

  Einzelnes Volume: Dieser Befehl stellt gelöscht codierte Daten auf das Volumen 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 gelöscht codierte Daten auf alle Volumes im Bereich `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 gelöscht codierten Daten auf Volumes wieder `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 an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

- Wenn im Grid Daten repliziert und mit Erasure-Coding-Verfahren codiert sind, führen Sie beide Befehle aus.

5. Monitoring der Reparatur replizierter Daten
   a. Wählen Sie **Nodes Storage Node wird repariert ILM**.

b. Verwenden Sie die Attribute im Abschnitt Bewertung, um festzustellen, ob Reparaturen abgeschlossen sind.

   Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut „wartet – Alle“ 0 Objekte an.

c. Um die Reparatur genauer zu überwachen, wählen Sie **Support Tools Grid Topology**.

d. Wählen Sie **Grid Storage Node wird repariert LDR Data Store**.

e. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.

   > Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

   - **Reparted (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 **Repears 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.

6. Überwachen Sie die Reparatur von Daten, die mit Erasure Coding codiert wurden, und versuchen Sie alle fehlgeschlagenen Anfragen erneut.

   a. Status von Datenreparaturen mit Löschungscode ermitteln:

      - 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time  End Time  State  Est Bytes
Affected/Repaired Retry Repair
================================================================================
================
 949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
 949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0     Yes
 949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0     Yes
 949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0     Yes
```

b. 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 mit der Reparatur-ID erneut versucht `83930030303133434`:

   ```
   repair-data start-ec-node-repair --repair-id 83930030303133434
   ```

   Dieser Befehl versucht eine fehlerhafte Volume-Reparatur mit der Reparatur-ID `83930030303133434`:

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Verwandte Informationen

"Monitor Fehlerbehebung"

Überprüfen des Speicherstatus nach der Wiederherstellung eines 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.

2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten LDR Storage Speicherzustand — gewünscht** und **Speicherzustand — Strom**.

   Der Wert beider Attribute sollte Online sein.

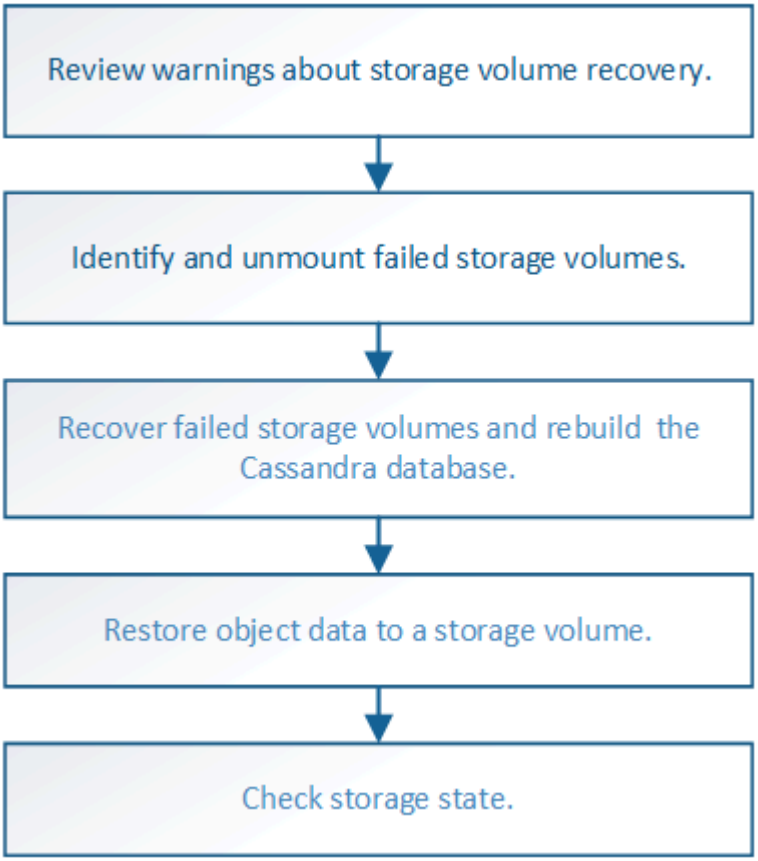
3. Wenn der Speicherstatus — gewünscht auf schreibgeschützt eingestellt ist, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die Registerkarte **Konfiguration**.
   b. Wählen Sie aus der Dropdown-Liste **Storage State — gewünschte** die Option **Online** aus.
   c. Klicken Sie Auf **Änderungen Übernehmen**.
   d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

Die Wiederherstellung nach einem Ausfall des Storage-Volumes ist bei intaktem Systemlaufwerk möglich

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.

Über diese Aufgabe

Dieses Wiederherstellungsverfahren gilt nur für softwarebasierte Speicherknoten. Wenn Speichervolumen auf einem Appliance-Speicherknoten ausgefallen sind, gehen Sie wie folgt vor: „`Wiederherstellen eines StorageGRID-Appliance-Speicherknoten`“.



Verwandte Informationen

"Wiederherstellen eines Speicherknoten für StorageGRID-Geräte"

Schritte

- "Überprüfen von Warnungen zur Wiederherstellung von Speichervolumen"
- "Identifizierung und Aufheben von fehlgeschlagenen Storage-Volumes"
- "Wiederherstellung ausgefallener Storage-Volumes und Wiederherstellung der Cassandra-Datenbank"
- "Wiederherstellung von Objektdaten auf einem Storage-Volume, auf dem das Systemlaufwerk intakt ist"
- "Überprüfung des Storage-Status nach der Wiederherstellung von Storage Volumes"

Überprüfen von Warnungen zur Wiederherstellung von Speichervolumen

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 den folgenden Wiederherstellungsvorgang 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. Wenden Sie sich an den technischen Support.

"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 „Service: Status – Cassandra (SVST)“ (Service: Status – Cassandra) ausgegeben wird, lesen Sie die Überwachungs- und Fehlerbehebungsanweisungen zur Wiederherstellung des Alarms durch Neuaufbau von Cassandra. 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

"Monitor Fehlerbehebung"

"Warnungen und Überlegungen für die Wiederherstellung von Grid Nodes"

Identifizierung und Aufheben von fehlgeschlagenen 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.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

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 die Daten auf dem Volume nicht mehr 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:

Schritte

1. Führen Sie die folgenden Schritte durch, um die fehlgeschlagenen Speicher-Volumes und deren Gerätenamen aufzunehmen:

   a. Wählen Sie **Support** > **Tools** > **Grid Topology** 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. Auswählen **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
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Melden Sie sich beim 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 Speicherdienste zu stoppen und die Bereitstellung eines fehlerhaften Speicher-Volumes 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 die Speicherdienste auf dem Speicherknoten zu stoppen.

   Wenn die Storage-Services bereits angehalten wurden, werden Sie nicht aufgefordert. Der Cassandra-Service wird nur für Volume 0 angehalten.

   ```
   root@Storage-180:~ # sn-unmount-volume 0
   Storage services (ldr, chunk, dds, cassandra) are not down.
   Storage services must be stopped before running this script.
   Stop storage services [y/N]? y
   Shutting down storage services.
   Storage services stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   In wenigen Sekunden werden die Speicherservices angehalten und das Volume wird abgehängt. Die Meldungen werden angezeigt, die jeden Schritt des Prozesses angeben. Die letzte Meldung gibt an, dass das Volume abgehängt wurde.

Wiederherstellung 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.

- Sie müssen die haben `Passwords.txt` Datei:
- Die Systemlaufwerke auf dem Server müssen intakt sein.
- Die Fehlerursache muss ermittelt worden sein und bei Bedarf muss bereits Ersatz-Storage-Hardware angeschafft worden sein.
- Die Gesamtgröße des Ersatzspeichers muss mit dem Original übereinstimmen.
- 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 die Option **Wartung Wartungsaufgaben Dekommission**.)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Erweiterung**.)
- Sie haben die Warnungen zur Wiederherstellung von Speichervolumen geprüft.

  "Überprüfen von Warnungen zur Wiederherstellung von Speichervolumen"

a. 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.

   Stellen Sie nach dem Ersetzen des Speichers sicher, dass Sie ihn erneut scannen oder neu booten, um sicherzustellen, dass er vom Betriebssystem erkannt wird, die Volumes jedoch nicht neu mounten. Der Speicher wird neu eingebunden und hinzugefügt `/etc/fstab` In einem späteren Schritt.

b. Melden Sie sich beim fehlgeschlagenen Speicherknoten 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 `#`.

c. 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.

d. 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 Speicherservices ausgeführt werden, werden Sie aufgefordert, diese zu beenden. Geben Sie ein: **Y**

- 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 Speichervolume wird hinzugefügt `/etc/fstab` Datei:
  - **N** wenn das Laufwerk keine Fehler enthält und Sie es nicht neu formatieren wollen.

> 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
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
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 c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

Verwandte Informationen

"Überprüfen von Warnungen zur Wiederherstellung von Speichervolumen"

Wiederherstellung von Objektdaten auf einem Storage-Volume, auf dem das Systemlaufwerk intakt ist

Nach der Wiederherstellung eines Storage-Volumes auf einem Storage-Node, auf dem das Systemlaufwerk intakt ist, können Sie die Objektdaten wiederherstellen, die bei einem Ausfall des Storage-Volume verloren gegangen sind.

Was Sie benötigen

- 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.

> 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. Aufgrund der Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen dauert die Wiederherstellung von Objektdaten in einen Storage Node aus einem Archiv-Node länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes.

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. Sie verwenden verschiedene Optionen mit dem `repair-data` Skript, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding Daten wiederherstellen:

- **Replizierte Daten**: Für die Wiederherstellung replizierter Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- **Erasure Coded (EC) Data**: Zwei Befehle stehen zur Wiederherstellung von Erasure-codierten Daten zur Verfügung. Dabei wird darauf basierend, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

  Reparaturen an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind. Sie können Reparaturen von Daten, die mit Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```

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.

Weitere Informationen zur Verwendung des `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile 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. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die wiederhergestellten Speicher-Volumes zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`
3. Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. (Wenn nur einige Volumes ausgefallen sind, fahren Sie mit dem nächsten Schritt fort.)

   Sie können nicht ausgeführt werden `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

   - Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

     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
     ```

     Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

   - 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 zum

Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die Erasure Coding-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 an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

- Wenn im Grid Daten repliziert und mit Erasure-Coding-Verfahren codiert sind, führen Sie beide Befehle aus.

4. Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren.

   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.

   - Wenn Ihr Grid replizierte Daten enthält, verwenden Sie das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. 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
```

> Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

- 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. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

  Einzelnes Volume: Dieser Befehl stellt gelöscht codierte Daten auf das Volumen 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 gelöscht codierte Daten auf alle Volumes im Bereich `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 gelöscht codierten Daten auf Volumes wieder `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 an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

- Wenn im Grid Daten repliziert und mit Erasure-Coding-Verfahren codiert sind, führen Sie beide Befehle aus.

5. Monitoring der Reparatur replizierter Daten
   a. Wählen Sie **Nodes Storage Node wird repariert ILM**.

b. Verwenden Sie die Attribute im Abschnitt Bewertung, um festzustellen, ob Reparaturen abgeschlossen sind.

   Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut „wartet – Alle“ 0 Objekte an.

c. Um die Reparatur genauer zu überwachen, wählen Sie **Support Tools Grid Topology**.

d. Wählen Sie **Grid Storage Node wird repariert LDR Data Store**.

e. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.

   > Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

   - **Reparted (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 **Repears 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.

6. Überwachen Sie die Reparatur von Daten, die mit Erasure Coding codiert wurden, und versuchen Sie alle fehlgeschlagenen Anfragen erneut.

   a. Status von Datenreparaturen mit Löschungscode ermitteln:

      - 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

 Repair ID Scope  Start Time  End Time  State  Est Bytes
Affected/Repaired Retry Repair
================================================================================
 949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
 949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0     Yes
 949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0     Yes
 949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0     Yes
```

b. 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 83930030303133434 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 83930030303133434
   ```

   Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 83930030303133434 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Verwandte Informationen

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

Überprüfung des Storage-Status 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten LDR Storage Speicherzustand — gewünscht** und **Speicherzustand — 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 Systemausfall

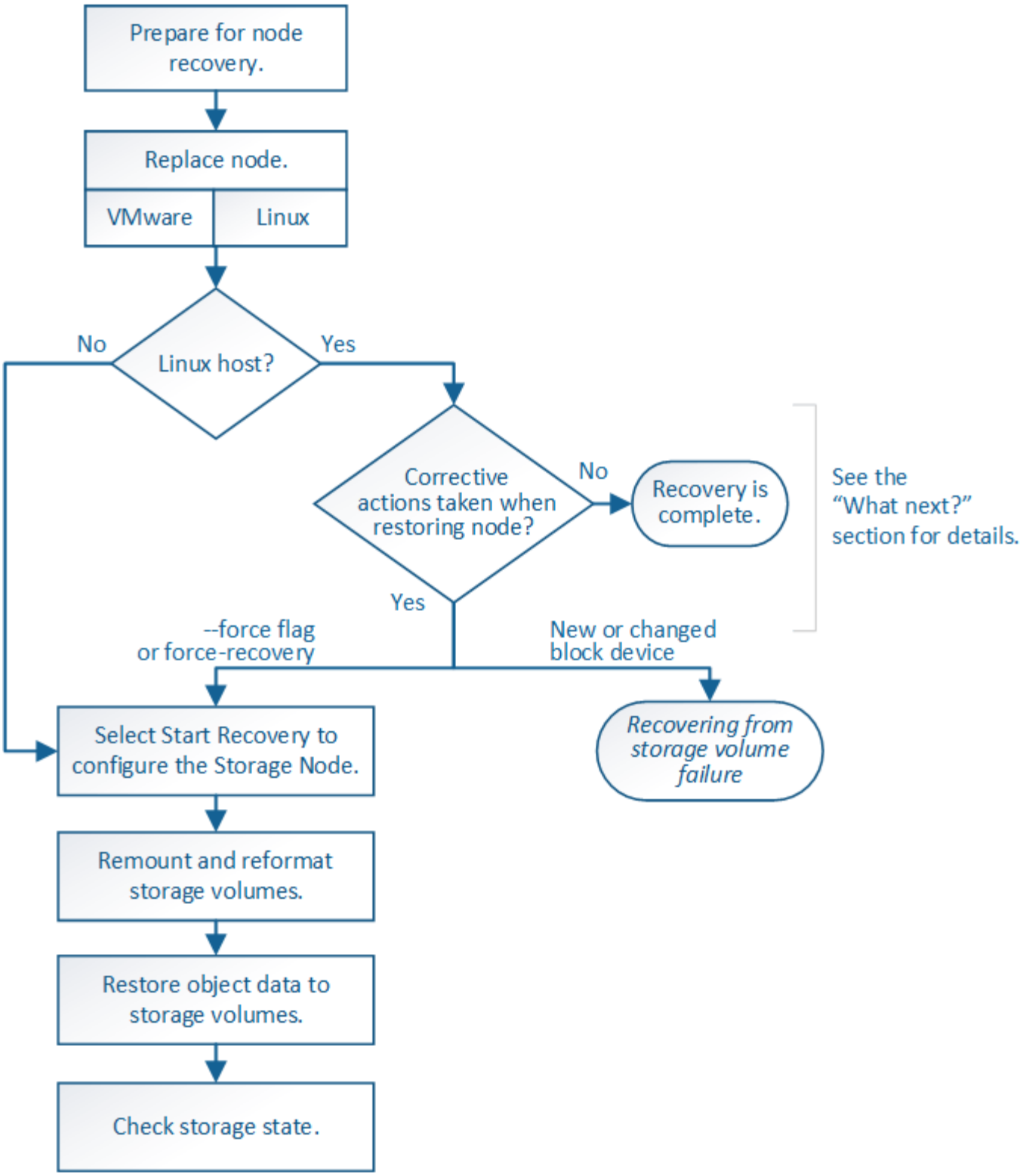
Wenn das Systemlaufwerk auf einem softwarebasierten Speicherknoten ausgefallen ist, steht der Speicherknoten dem StorageGRID-System nicht zur Verfügung. Sie müssen einen bestimmten Satz von Aufgaben zur Wiederherstellung nach einem Systemausfall ausführen.

Über diese Aufgabe

Gehen Sie folgendermaßen vor, um nach einem Systemlaufwerksausfall auf einem softwarebasierten Speicherknoten wiederherzustellen. Dieses Verfahren umfasst die folgenden Schritte, wenn auch Storage-Volumes ausgefallen sind oder nicht neu eingebunden werden können.

> Dieses Verfahren gilt nur für softwarebasierte Speicherknoten. Sie müssen ein anderes Verfahren befolgen, um einen Appliance-Speicherknoten wiederherzustellen.

"Wiederherstellen eines Speicherknoten für StorageGRID-Geräte"



Schritte

- "Überprüfen von Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken"
- "Ersetzen des Speicherknotens"
- "Wählen Sie Wiederherstellung starten, um einen Speicherknoten zu konfigurieren"
- "Erneutes Mounten und Neuformatieren von Storage Volumes („`MAnual Steps`“)"
- "Wiederherstellen von Objektdaten in einem Storage Volume, falls erforderlich"

- "Überprüfen des Speicherstatus nach der Wiederherstellung eines Speicherknoten-Systemlaufwerks"

Überprüfen von Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken

Bevor Sie ein ausgefallenes Systemlaufwerk eines Speicherknoten wiederherstellen, müssen Sie die folgenden Warnungen überprüfen.

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 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 den folgenden Wiederherstellungsvorgang 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. Wenden Sie sich an den technischen Support.

"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 Speichervolumes zu ermöglichen, stellen Sie Volumes auf dem Speicherknoten mit fehlerhaften Speicher-Volumes wieder her, bevor Sie diesen fehlgeschlagenen Speicherknoten wiederherstellen. Beachten Sie die Anweisungen für die Wiederherstellung nach einem Verlust von Storage-Volumes, bei denen das Systemlaufwerk intakt ist.

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 „Service: Status – Cassandra (SVST)“ (Service: Status – Cassandra) ausgegeben wird, lesen Sie die Überwachungs- und Fehlerbehebungsanweisungen zur Wiederherstellung des Alarms durch Neuaufbau von Cassandra. 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

"Monitor Fehlerbehebung"

"Warnungen und Überlegungen für die Wiederherstellung von Grid Nodes"

"Die Wiederherstellung nach einem Ausfall des Storage-Volumes ist bei intaktem Systemlaufwerk möglich"

Ersetzen des Speicherknotens

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 ein anderes Verfahren befolgen, um einen Appliance-Speicherknoten wiederherzustellen.

"Wiederherstellen eines Speicherknoten für StorageGRID-Geräte"

Linux: Wenn Sie sich nicht sicher sind, ob Ihr Systemlaufwerk ausgefallen ist, befolgen Sie die Anweisungen, um den Knoten zu ersetzen, um festzustellen, welche Wiederherstellungsschritte erforderlich sind.

Plattform	Verfahren
VMware	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
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 zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um einen 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.
- Sie müssen das Startdatum aller Reparaturaufträge für Daten mit Löschungscode kennen.
- Sie müssen überprüft haben, dass der Speicherknoten innerhalb der letzten 15 Tage nicht neu aufgebaut 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:

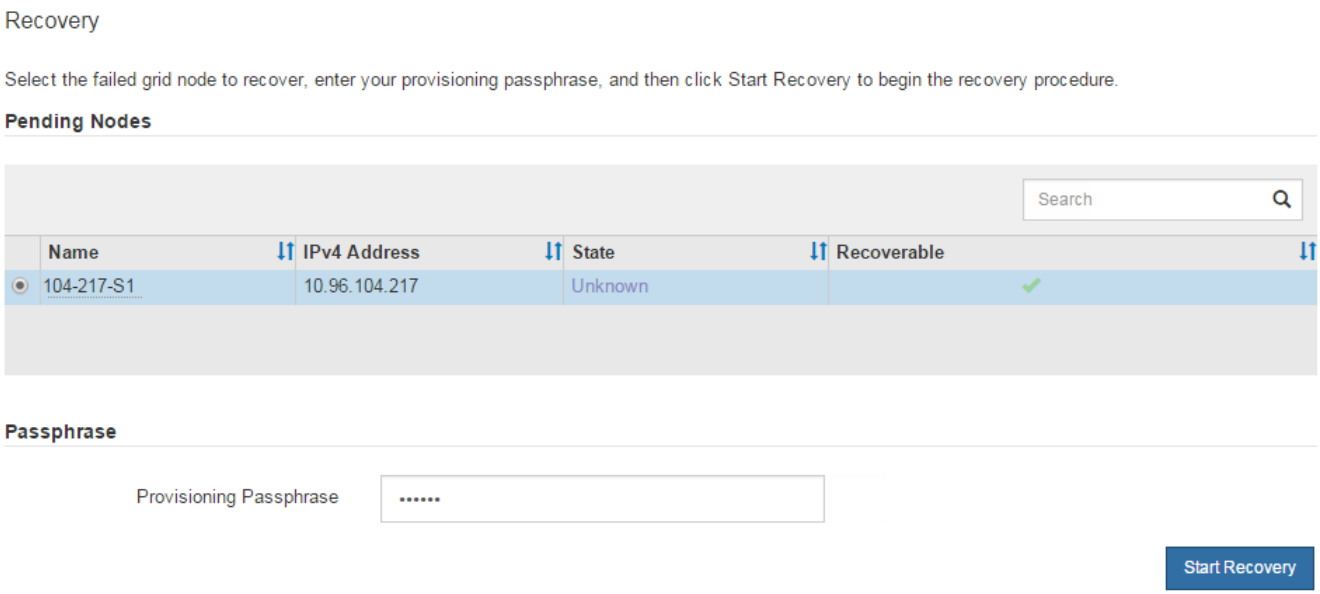
- Man musste das benutzen `--force` Flag, um den Knoten zu importieren, oder Sie haben ausgegeben `storagegrid node force-recovery node-name`
- Sie mussten eine vollständige Neuinstallation des Knotens durchführen oder /var/local wiederherstellen.

Schritte

1. Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Recovery** aus.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

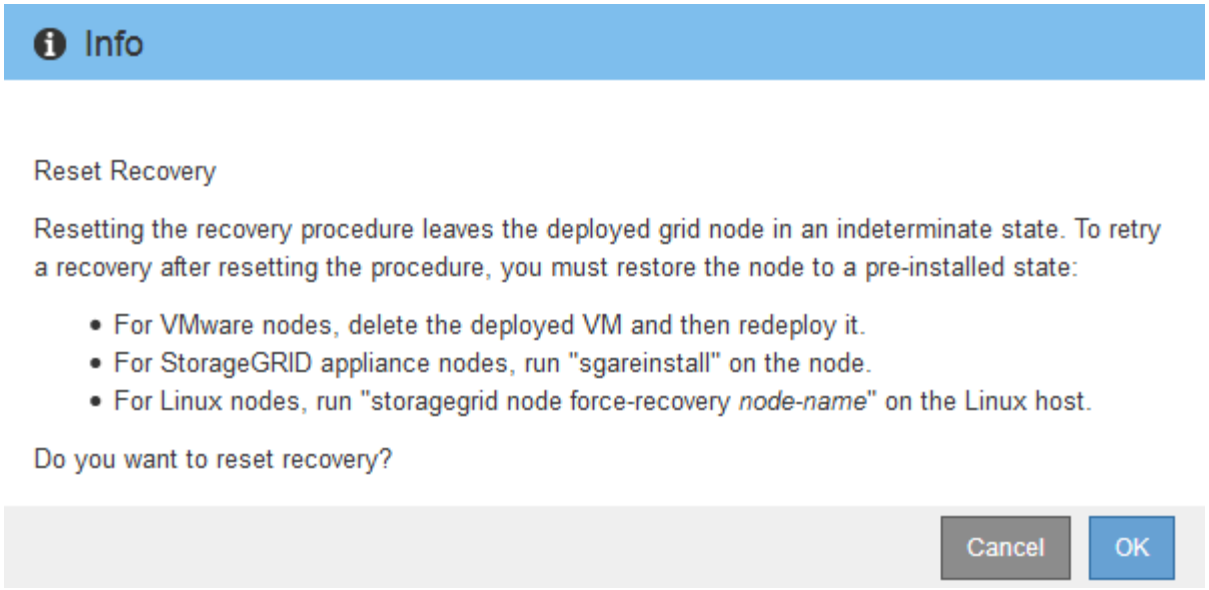
   Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.

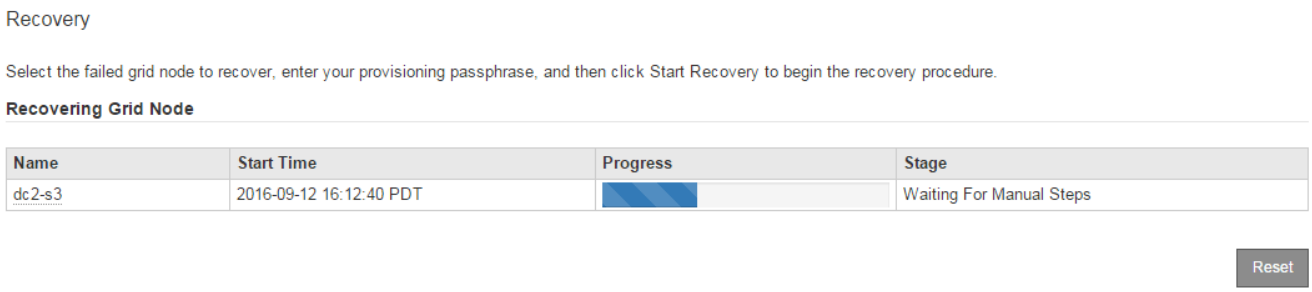
> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.



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 Speicherknoten die Stufe „`Warten auf manuelle Schritte`“ erreicht hat, gehen Sie zur nächsten Aufgabe im Wiederherstellungsverfahren, um Speicher-Volumes neu zu mounten und neu zu formatieren.



Verwandte Informationen

"Vorbereiten eines Geräts für die Neuinstallation (nur Plattformaustausch)"

Erneutes Mounten und Neuformatieren von Speicher-Volumes („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.

Was Sie benötigen

- 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 die Option **Wartung Wartungsaufgaben Dekommission**.)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Erweiterung**.)
- Sie haben die Warnungen für die Wiederherstellung des Speicherknoten-Systemlaufwerks überprüft.

  "Überprüfen von Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken"

> 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 Speicherknoten während der Wiederherstellung nicht neu, bevor Sie ausführen `sn-recovery-postinstall.sh` (Siehe Schritt für Skript nach der Installation) Zum Neuformatieren 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.

  - 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.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot 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.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot 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 kein Speicher-Volume mounten kann, wird 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 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 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 Speicher-Volume nicht angehängt oder nicht ordnungsgemäß formatiert werden kann, und Sie mit dem nächsten Schritt fortfahren, werden das Volume und alle 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 der Meinung sind, dass die in einem ausgefallenen Storage Volume verbliebenen Daten nicht von einer anderen Stelle im Grid wiederhergestellt werden können (falls Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie macht, oder falls 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:

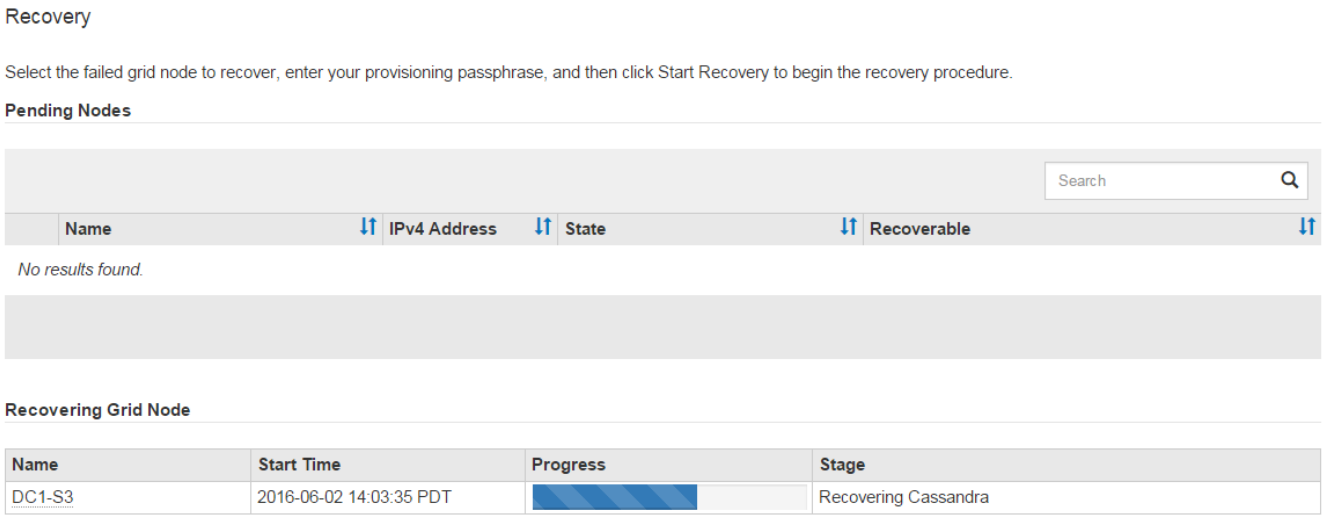
   - Das Skript kann Stunden in Anspruch nehmen.
   - Im Allgemeinen sollten Sie die SSH-Sitzung allein lassen, während das Skript ausgeführt wird.
   - Drücken Sie nicht **Strg+C**, wenn die SSH-Sitzung aktiv ist.
   - Das Skript wird im Hintergrund ausgeführt, wenn eine Netzwerkunterbrechung auftritt 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:



Nach dem `sn-recovery-postinstall.sh` Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speicher-Volumes wiederherstellen, die durch das Skript formatiert wurden, wie in diesem Verfahren beschrieben.

Verwandte Informationen

"Überprüfen von Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken"

"Wiederherstellen von Objektdaten in einem Storage Volume, falls erforderlich"

Wiederherstellen von Objektdaten in einem Storage Volume, falls erforderlich

Wenn der `sn-recovery-postinstall.sh` Skript ist erforderlich, um ein oder mehrere fehlgeschlagene Speicher-Volumes neu zu formatieren, müssen Sie Objektdaten auf dem neu formatierten Speicher-Volume von anderen Speicherknoten und Archiv-Nodes wiederherstellen. Diese Schritte sind erst dann erforderlich, wenn ein oder mehrere Storage Volumes neu formatiert wurden.

Was Sie benötigen

- 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.

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. Aufgrund der Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen dauert die Wiederherstellung von Objektdaten in einen Storage Node aus einem Archiv-Node länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes.

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. Sie verwenden verschiedene Optionen mit dem `repair-data` Skript, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding Daten wiederherstellen:

- **Replizierte Daten**: Für die Wiederherstellung replizierter Daten stehen zwei Befehle zur Verfügung, je nachdem, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- **Erasure Coded (EC) Data**: Zwei Befehle stehen zur Wiederherstellung von Erasure-codierten Daten zur Verfügung. Dabei wird darauf basierend, ob Sie den gesamten Knoten oder nur bestimmte Volumes auf dem Knoten reparieren müssen:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

  Reparaturen an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind. Sie können Reparaturen von Daten, die mit Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```

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.

Weitere Informationen zur Verwendung des `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile 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. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die wiederhergestellten Speicher-Volumes zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`
3. Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. (Wenn nur einige Volumes ausgefallen sind, fahren Sie mit dem nächsten Schritt fort.)

   > Sie können nicht ausgeführt werden `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

   - Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

     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
     ```

     > Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

   - 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 zum Reparieren des gesamten Speicherknoten.

     Mit diesem Befehl werden die Erasure Coding-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 an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

- Wenn im Grid Daten repliziert und mit Erasure-Coding-Verfahren codiert sind, führen Sie beide Befehle aus.

4. Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren.

   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.

   - Wenn Ihr Grid replizierte Daten enthält, verwenden Sie das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. 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
     ```

     > Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

   - 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. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt gelöscht codierte Daten auf das Volumen 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 gelöscht codierte Daten auf alle Volumes im Bereich `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 gelöscht codierten Daten auf Volumes wieder `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 an Erasure-codierten Daten können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

- Wenn im Grid Daten repliziert und mit Erasure-Coding-Verfahren codiert sind, führen Sie beide Befehle aus.

5. Monitoring der Reparatur replizierter Daten
   a. Wählen Sie **Nodes Storage Node wird repariert ILM**.
   b. Verwenden Sie die Attribute im Abschnitt Bewertung, um festzustellen, ob Reparaturen abgeschlossen sind.

      Wenn die Reparaturen abgeschlossen sind, zeigt das Attribut „wartet – Alle“ 0 Objekte an.

   c. Um die Reparatur genauer zu überwachen, wählen Sie **Support Tools Grid Topology**.
   d. Wählen Sie **Grid Storage Node wird repariert LDR Data Store**.
   e. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.

      > Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reparted (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 **Repears 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.

6. Überwachen Sie die Reparatur von Daten, die mit Erasure Coding codiert wurden, und versuchen Sie alle fehlgeschlagenen Anfragen erneut.

   a. Status von Datenreparaturen mit Löschungscode ermitteln:

   - 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est Bytes Affected/Repaired
Retry Repair
================================================================================
=============
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0 Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0 Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0 Yes
```

b. 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 83930030303133434 erneut versucht:

   ```
   repair-data start-ec-node-repair --repair-id 83930030303133434
   ```

   Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 83930030303133434 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Verwandte Informationen

"StorageGRID verwalten"

"Monitor Fehlerbehebung"

Überprüfen des Speicherstatus nach der Wiederherstellung eines 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten LDR Storage Speicherzustand — gewünscht** und **Speicherzustand — Strom**.

   Der Wert beider Attribute sollte Online sein.

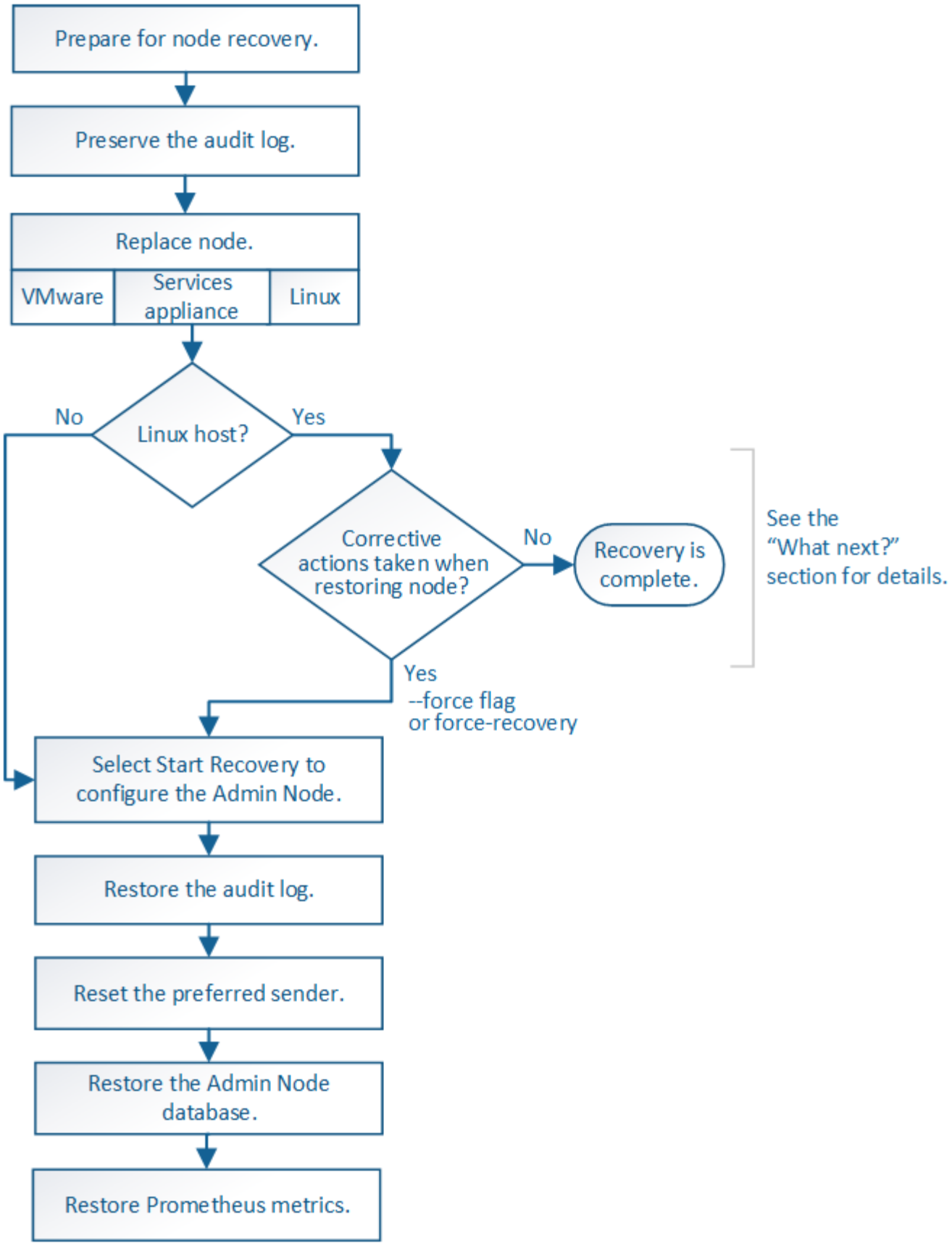
3. Wenn der Speicherstatus — gewünscht auf schreibgeschützt eingestellt ist, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die Registerkarte **Konfiguration**.
   b. Wählen Sie aus der Dropdown-Liste **Storage State — gewünschte** die Option **Online** aus.
   c. Klicken Sie Auf **Änderungen 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 bei Ausfällen von Admin-Nodes

Der Wiederherstellungsprozess für einen Admin-Knoten hängt davon ab, ob es sich um den primären Admin-Knoten oder einen nicht-primären Admin-Knoten handelt.

Über diese Aufgabe

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.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Wahlmöglichkeiten

- "Wiederherstellung nach Ausfällen des primären Admin-Nodes"
- "Wiederherstellung nach Ausfällen eines Admin-Knotens außerhalb des primären Standorts"

Wiederherstellung nach Ausfällen des primären Admin-Nodes

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.

Über diese Aufgabe

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 erst dann aufgenommen werden, wenn Identifikatoren 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.

Schritte

- "Prüfprotokolle werden vom fehlgeschlagenen primären Admin-Node kopiert"
- "Ersetzen des primären Admin-Knotens"
- "Konfigurieren des primären Ersatzadministratorknotens"
- "Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten primären Administrator-Knoten"
- "Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten primären Admin-Knoten"
- "Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines primären Admin-Knotens"
- "Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines primären Admin-Knotens"

Prüfprotokolle werden vom fehlgeschlagenen primären Admin-Node kopiert

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.

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 jetzt auf dem fehlgeschlagenen Admin-Node die Überwachungsprotokolle nicht mehr zugegriffen werden kann, können Sie später, z. B. nach der Hostwiederherstellung, darauf zugreifen.

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, z. B. yyyy-mm-dd.txt.1. Beispielsweise können Sie die Datei audit.log in 2015-10-25.txt.1 umbenennen`cd /var/local/audit/export/`
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`

Ersetzen des primären Admin-Knotens

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	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
SG100- und SG1000-Services-Appliances	"Ersetzen einer 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 zum Ersetzen eines Linux-Knotens.

Konfigurieren des primären Ersatzadministratorknotens

Der Ersatzknoten muss als primärer Admin-Node für Ihr StorageGRID System konfiguriert sein.

Was Sie benötigen

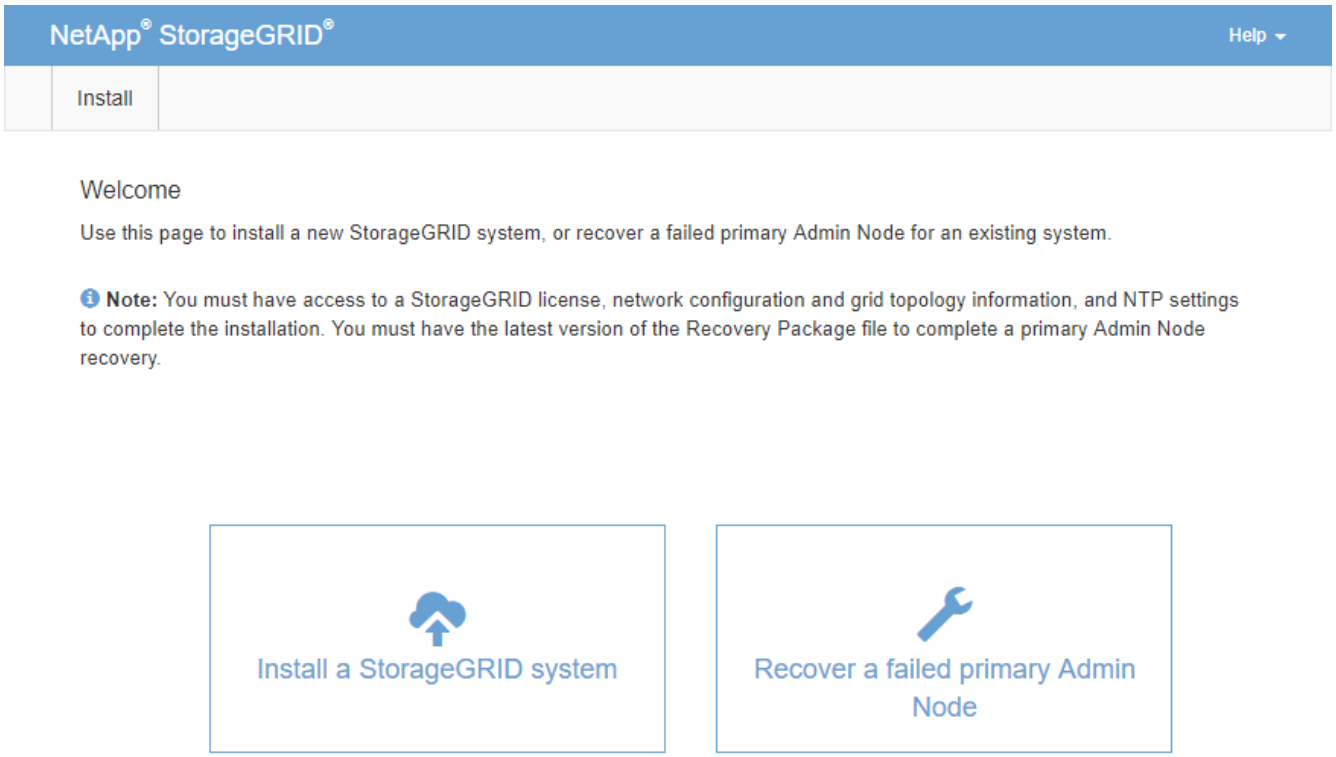
- Für primäre Admin-Knoten, die auf virtuellen Maschinen gehostet werden, muss die virtuelle Maschine bereitgestellt, eingeschaltet und initialisiert werden.
- Für primäre Admin-Nodes, die auf einer Services-Appliance gehostet werden, haben Sie die Appliance ersetzt und die installierte Software installiert. Informationen zum Gerät finden Sie im Installationshandbuch.

  "SG100 SG1000 Services-Appliances"

- Sie müssen über die neueste Sicherung der Wiederherstellungspaket-Datei verfügen (`sgws-recovery-package-`*`id-revision`*`.zip`).
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu `https://primary_admin_node_ip`.



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 Standardzertifikat für Verwaltungsschnittstellen-Server konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Knotens auf die Vertrauensbasis in Active Directory-Föderationsdienste (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.

   > Informationen zum Konfigurieren eines Vertrauensverhältnisses mit einer vertrauenswürdigen Partei finden Sie in den Anweisungen zur Verwaltung von StorageGRID. 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 über einen unterstützten Browser beim Grid Manager an.

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 **Softwareversion** angezeigten Versionen anders sind, müssen Sie einen Hotfix anwenden, um den wiederhergestellten primären Admin-Knoten auf dieselbe Version zu aktualisieren.

Verwandte Informationen

"StorageGRID verwalten"

"StorageGRID Hotfix Verfahren"

Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten primären Administrator-Knoten

Wenn Sie das Revisionsprotokoll vom fehlgeschlagenen primären Admin-Knoten erhalten konnten, können Sie es in den primären Admin-Knoten kopieren, den Sie wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Nachdem der ursprüngliche Admin-Node fehlgeschlagen ist, müssen Sie die Prüfprotokolle an einen anderen Speicherort kopiert haben.

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, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen in das Auditprotokoll, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.

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 in den Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten primären Admin-Knoten

Wenn der primäre Admin-Knoten, den Sie wiederherstellen, derzeit als bevorzugter Absender von Warnmeldungen, Alarmanmeldungen und AutoSupport-Meldungen eingestellt ist, müssen Sie diese Einstellung neu konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie den wiederhergestellten Admin-Knoten aus der Dropdown-Liste **bevorzugter Absender** aus.
3. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

"StorageGRID verwalten"

Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines primären Admin-Knotens

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.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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 einen primären Admin-Knoten hat, 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.

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`

Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines primären Admin-Knotens

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.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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 einen primären Admin-Knoten hat, 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.

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 eines Admin-Knotens außerhalb des primären Standorts

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.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Schritte

- "Prüfprotokolle werden vom fehlgeschlagenen nicht-primären Admin-Node kopiert"
- "Ersetzen eines nicht-primären Admin-Knotens"
- "Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren"
- "Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten nicht-primären Admin-Knoten"
- "Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten nicht-primären Admin-Node"
- "Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines nicht-primären Admin-

Knotens"

- "Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines nicht primären Admin-Nodes"

Prüfprotokolle werden vom fehlgeschlagenen nicht-primären Admin-Node kopiert

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 jetzt auf dem fehlgeschlagenen Admin-Node die Überwachungsprotokolle nicht mehr zugegriffen werden kann, können Sie später, z. B. nach der Hostwiederherstellung, darauf zugreifen.

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, z. B. yyyy-mm-dd.txt.1. Beispielsweise können Sie die Datei audit.log in 2015-10-25.txt.1 umbenennen`cd /var/local/audit/export/`

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`

Ersetzen eines nicht-primären Admin-Knotens

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	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
SG100- und SG1000-Services-Appliances	"Ersetzen einer 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 zum 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

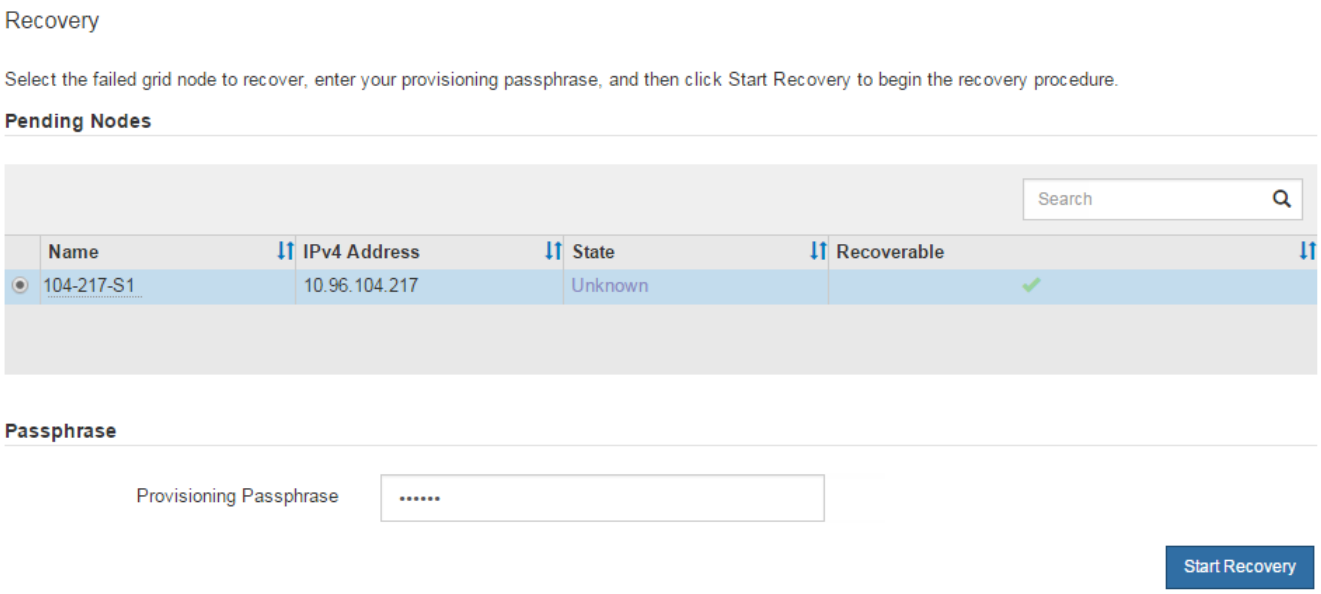
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Recovery** aus.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

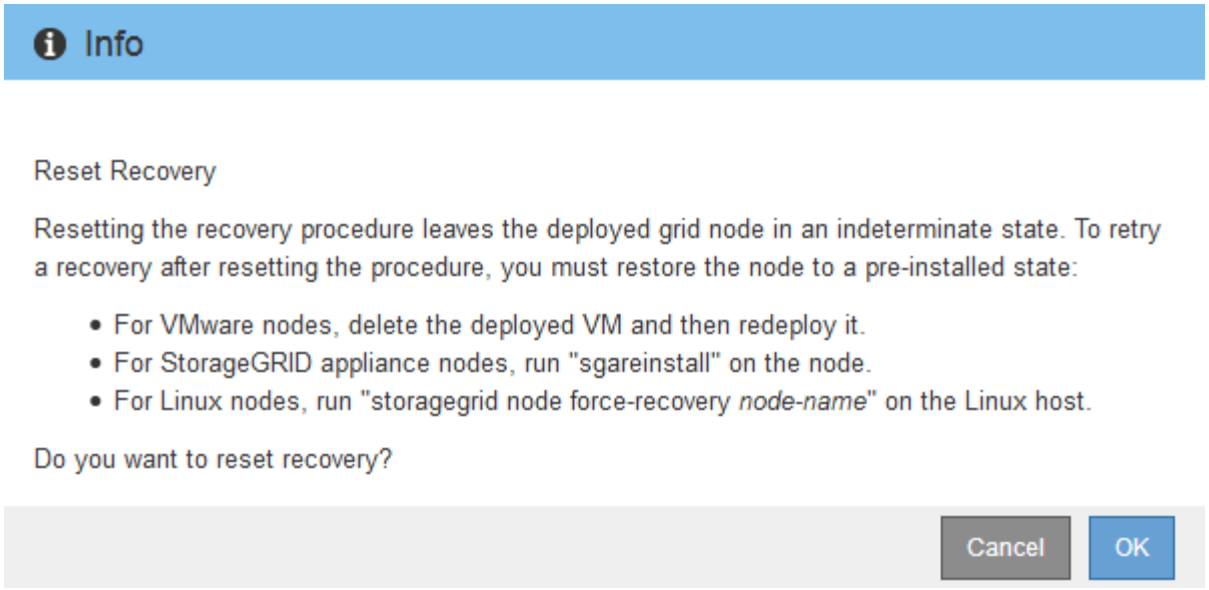
   Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.

> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.



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.

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Standardzertifikat für Verwaltungsschnittstellen-Server konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Knotens auf die Vertrauensbasis in Active Directory-Föderationsdienste (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.

> Informationen zum Konfigurieren eines Vertrauensverhältnisses mit einer vertrauenswürdigen Partei finden Sie in den Anweisungen zur Verwaltung von StorageGRID. 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:

Verwandte Informationen

"StorageGRID verwalten"

"Vorbereiten eines Geräts für die Neuinstallation (nur Plattformaustausch)"

Wiederherstellen des Prüfprotokolls auf dem wiederhergestellten nicht-primären Admin-Knoten

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.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Nachdem der ursprüngliche Admin-Node fehlgeschlagen ist, müssen Sie die Prüfprotokolle an einen anderen Speicherort kopiert haben.

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, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen in das Auditprotokoll, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.

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 in den Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Zurücksetzen des bevorzugten Senders auf dem wiederhergestellten nicht-primären Admin-Node

Wenn der nicht-primäre Admin-Node, den Sie wiederherstellen, derzeit als bevorzugter Absender von Warnmeldungen, Alarmbenachrichtigungen und AutoSupport-Meldungen eingestellt ist, müssen Sie diese Einstellung im StorageGRID-System neu konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie den wiederhergestellten Admin-Knoten aus der Dropdown-Liste **bevorzugter Absender** aus.
3. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

"StorageGRID verwalten"

Wiederherstellen der Admin-Knoten-Datenbank bei der Wiederherstellung eines nicht-primären Admin-Knotens

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.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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.

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 Ein:`ssh-add -D`
6. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Wiederherstellen von Prometheus-Kennzahlen bei der Wiederherstellung eines nicht primären Admin-Nodes

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem nicht primären Admin-Node gewartet wurden, der ausgefallen ist.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

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.

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:

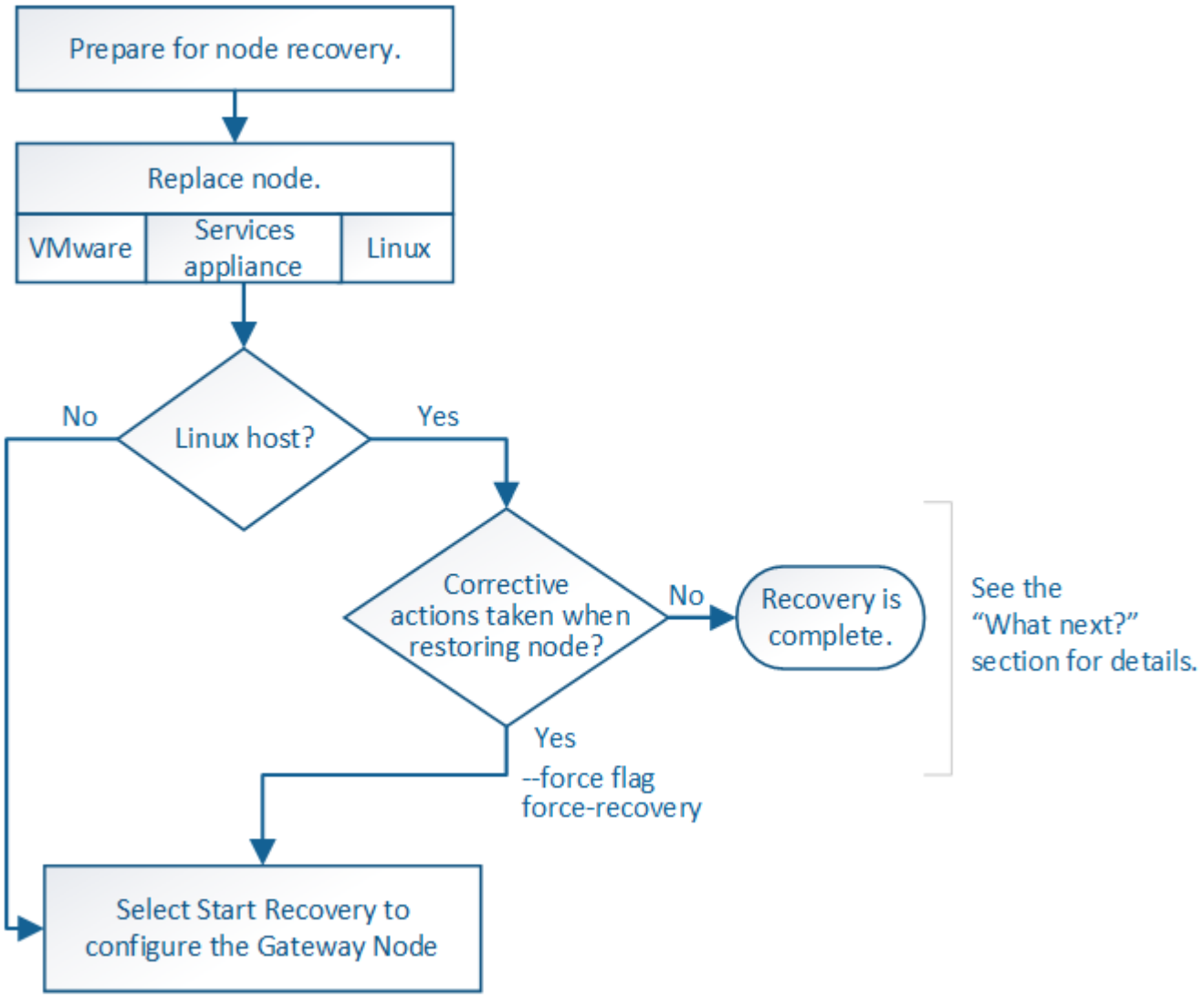
Datenbank geklont, Dienste starten

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

Sie müssen eine Reihe von Aufgaben genau durchführen, um nach einem Gateway Node-Ausfall wiederherstellen zu können.



Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Schritte

- "Ersetzen eines Gateway-Node"
- "Wählen Sie Wiederherstellung starten, um einen Gateway-Node zu konfigurieren"

Ersetzen eines Gateway-Node

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	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
SG100- und SG1000-Services-Appliances	"Ersetzen einer 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 zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um einen 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.

Was Sie benötigen

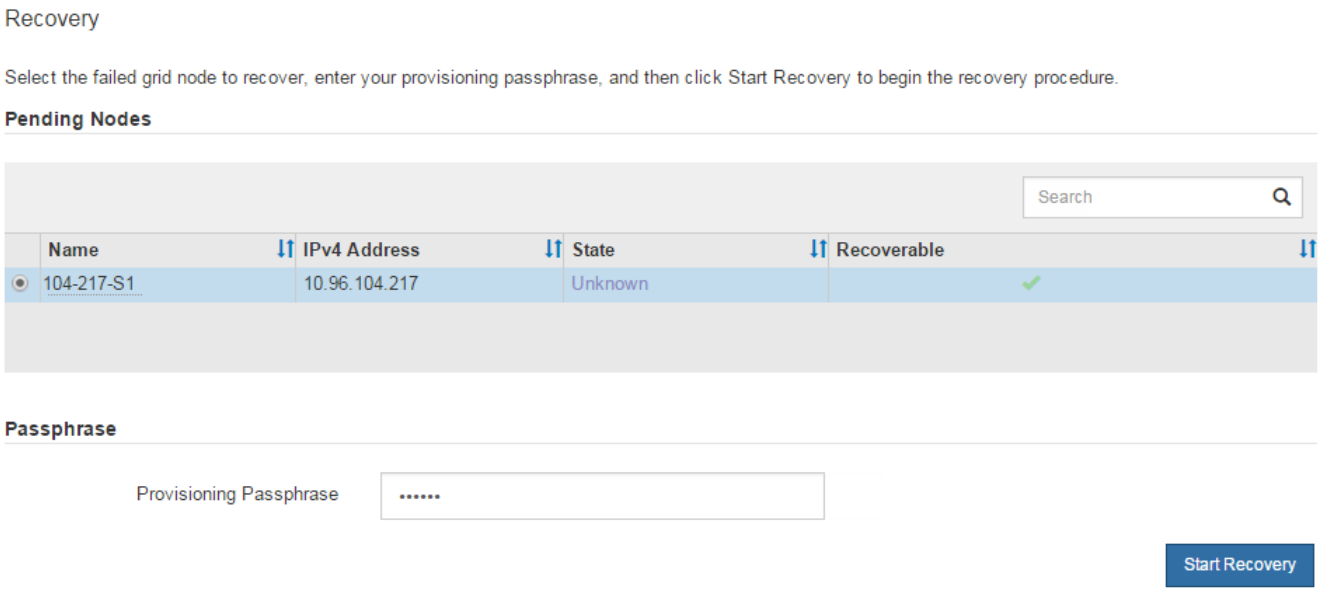
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Recovery** aus.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

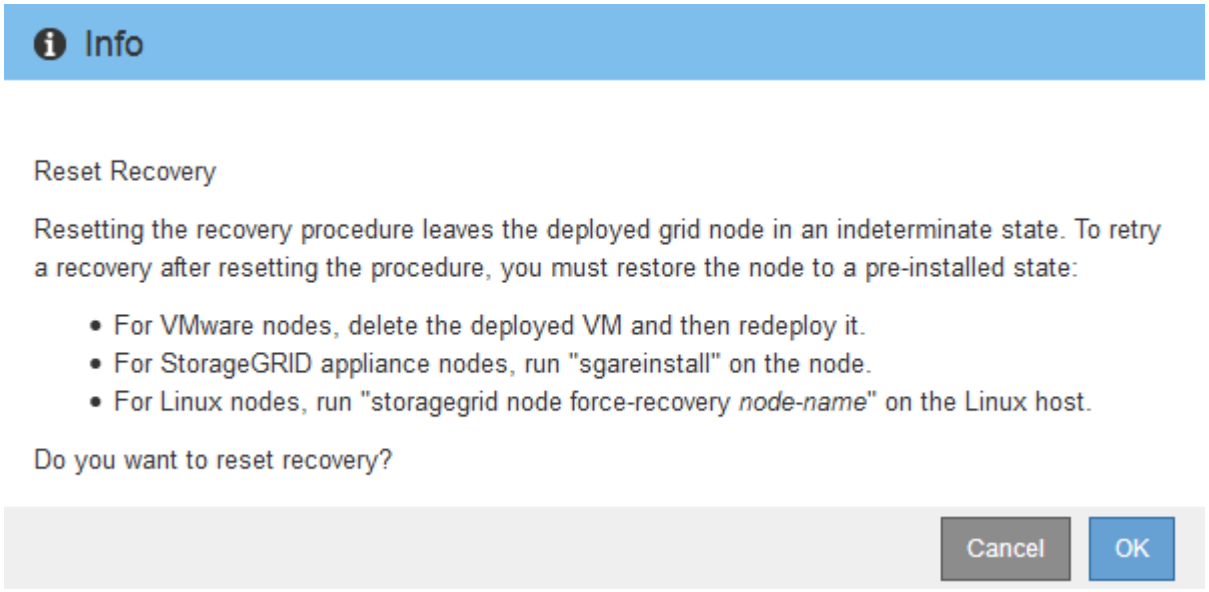
   Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.

> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.



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

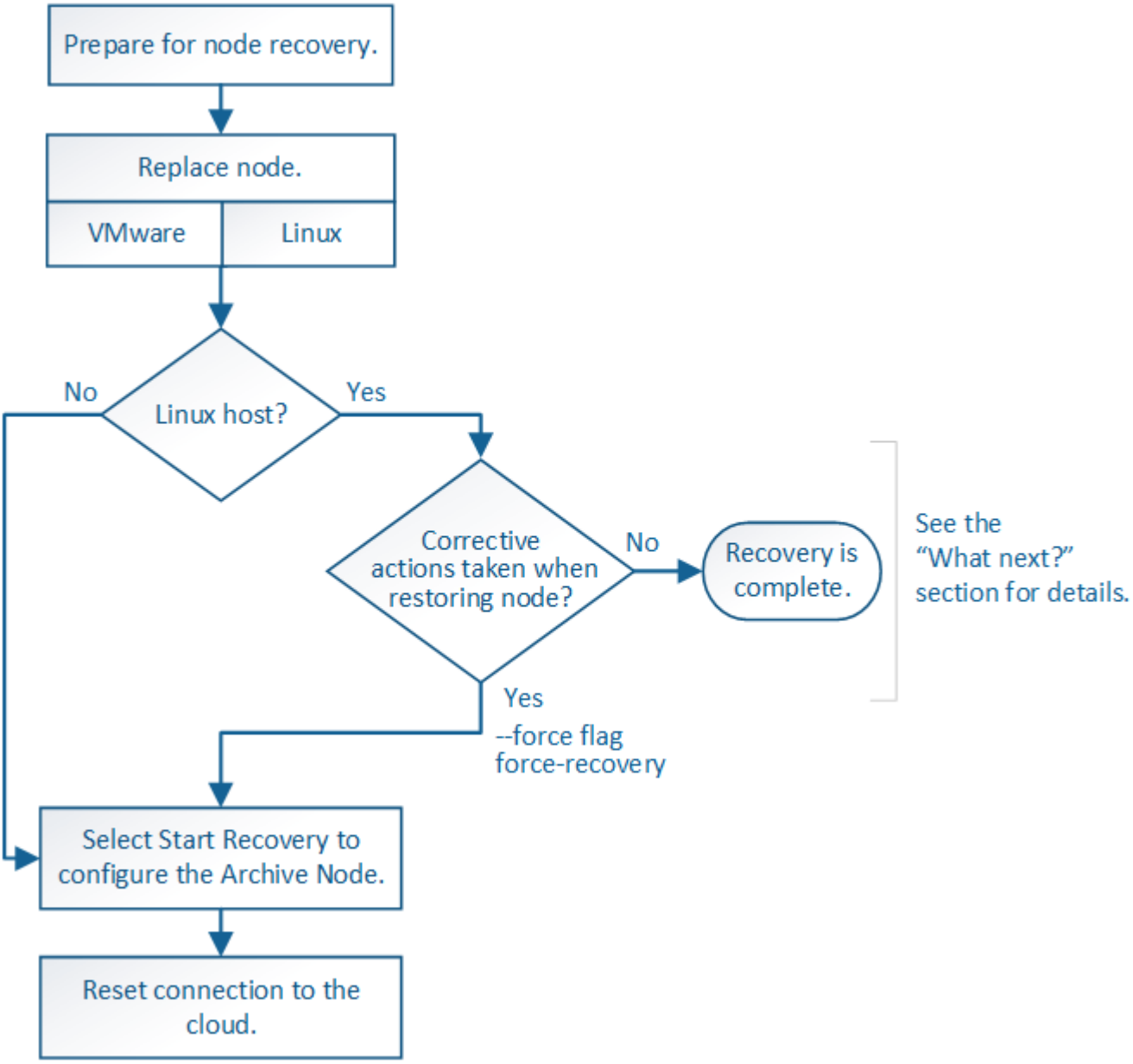
wiederherstellen `sgareinstall` Auf dem Node.

Verwandte Informationen

"Vorbereiten eines Geräts für die Neuinstallation (nur Plattformaustausch)"

Wiederherstellung nach Ausfällen des Archivierungs-Nodes

Sie müssen eine Reihe von Aufgaben genau durchführen, um nach einem Ausfall des Archivierungs-Knotens wiederherstellen zu können.



Über diese Aufgabe

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 Speicherknotens ein Ausfall des Archivknotens 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.

Schritte

- "Ersetzen eines Archivknotens"
- "Wählen Sie „Wiederherstellung starten“, um einen Archiv-Knoten zu konfigurieren"
- "Verbindung des Archivknotens zur Cloud wird zurückgesetzt"

Ersetzen eines Archivknotens

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	"Austausch eines VMware Node"
Linux	"Ersetzen eines Linux-Knotens"
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 zum Ersetzen eines Linux-Knotens.

Wählen Sie „Wiederherstellung starten“, um einen Archiv-Knoten 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.

Was Sie benötigen

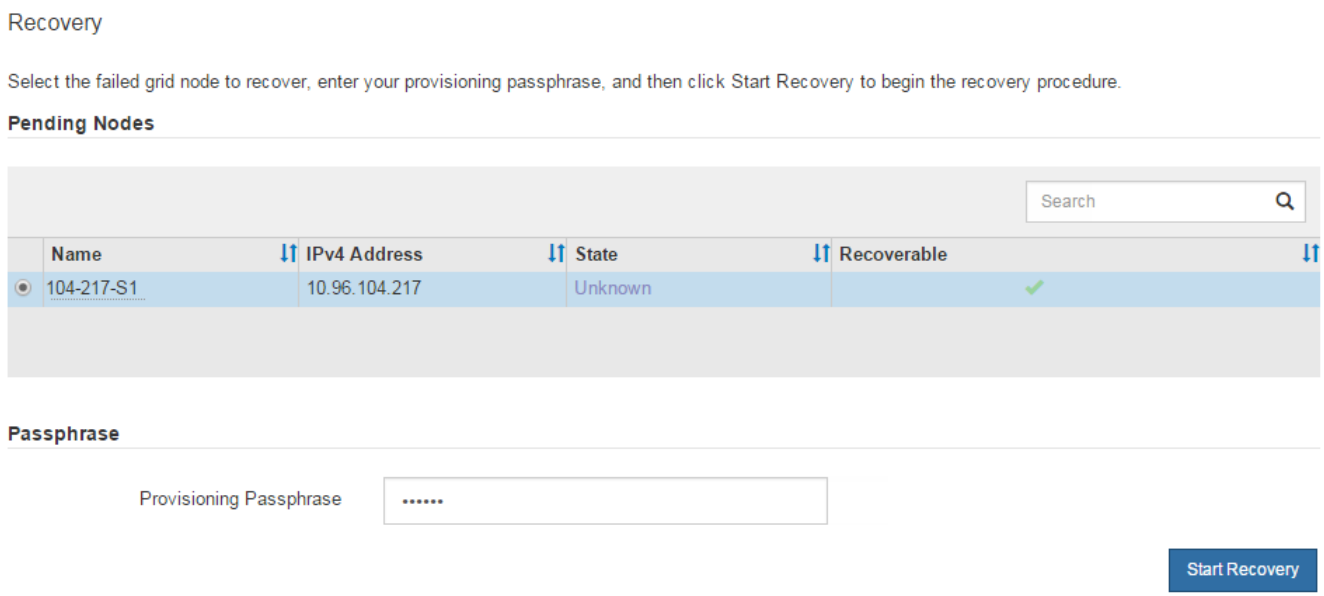
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **Wartung Wartungsaufgaben Recovery** aus.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

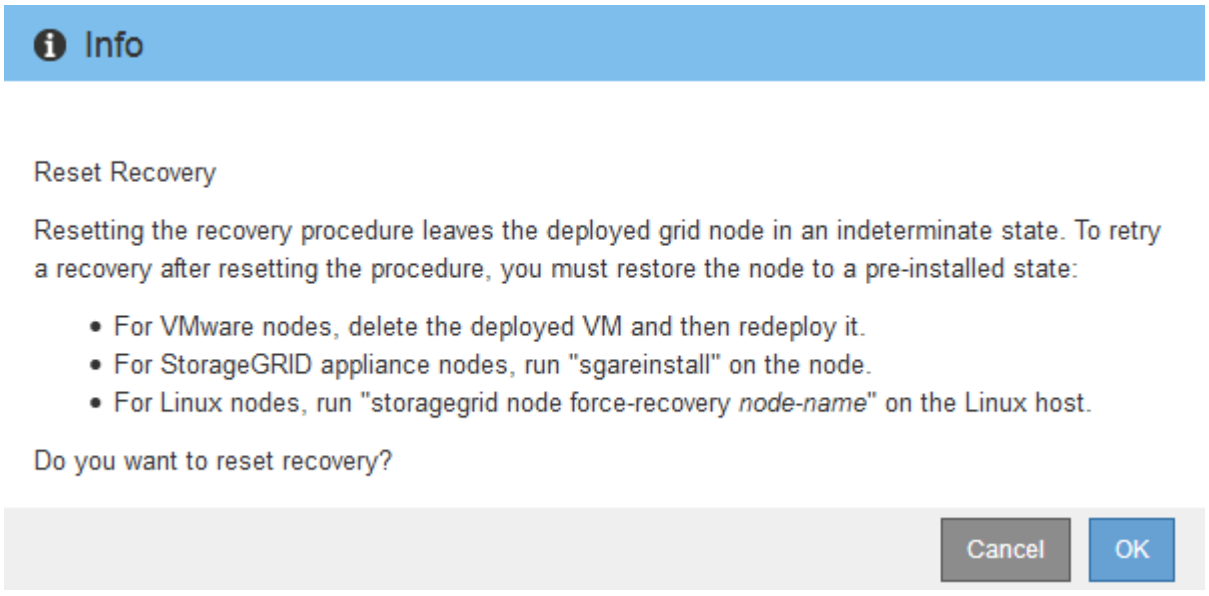
   Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.



5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.

> Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.



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`

Verbindung des Archivknotens zur Cloud wird zurückgesetzt

Nachdem Sie einen Archiv-Node wiederhergestellt haben, der die Cloud über die S3-API anzielt, müssen Sie die Konfigurationseinstellungen ändern, um Verbindungen zurückzusetzen. Ein ORSU-Alarm (Outbound Replication Status) wird ausgelöst, wenn der Archivknoten keine Objektdaten abrufen kann.

Wenn der Archivknoten über die TSM Middleware mit externem Storage verbunden ist, wird der Node automatisch zurückgesetzt und Sie müssen es nicht neu konfigurieren.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** 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: Austausch eines VMware Node

Wenn Sie einen ausgefallenen StorageGRID-Node wiederherstellen, der auf VMware gehostet wurde, müssen Sie den ausgefallenen Node entfernen und einen Recovery-Node implementieren.

Was Sie benötigen

Sie müssen festgestellt haben, 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 **Aktionen Alle vCenter-Aktionen Löschen von 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.

   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.

   Weitere Informationen:

   "VMware installieren" StorageGRID-Knoten als virtuelle Maschine implementieren

8. Führen Sie das Recovery-Verfahren für den Node anhand des Node aus, den Sie wiederherstellen.

Node-Typ	Gehen Sie zu
Primärer Admin-Node	"Konfigurieren des primären Ersatzadministratorknotens"
Nicht primärer Admin-Node	"Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren"
Gateway-Node	"Wählen Sie Wiederherstellung starten, um einen Gateway-Node zu konfigurieren"
Storage-Node	"Wählen Sie Wiederherstellung starten, um einen Speicherknoten zu konfigurieren"
Archiv-Node	"Wählen Sie „Wiederherstellung starten“, um einen Archiv-Knoten zu konfigurieren"

Alle Grid-Node-Typen: Austausch eines Linux-Node

Wenn ein Ausfall erfordert, dass Sie einen oder mehrere neue physische oder virtuelle Hosts bereitstellen oder Linux auf einem vorhandenen Host neu installieren, müssen Sie den Ersatz-Host implementieren und konfigurieren, 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. Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

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 wiederherenden 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.

1. "Bereitstellen neuer Linux-Hosts"
2. "Wiederherstellen von Grid-Nodes auf dem Host"
3. "Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen"

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Bereitstellen neuer 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, befolgen Sie das Verfahren zur Vorbereitung der Hosts in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

Dieses Verfahren umfasst Schritte zur Durchführung folgender Aufgaben:

1. Installieren Sie Linux.
2. Konfigurieren Sie das Hostnetzwerk.
3. Hostspeicher konfigurieren.
4. Installation Von Docker:
5. Installieren Sie den StorageGRID Host Service.

> Beenden Sie den Vorgang „`StorageGRID Host Service` installieren“ in den Installationsanweisungen. Starten Sie nicht die Aufgabe „`DBereitstellung von 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 Shared Storage zur Unterstützung Ihrer StorageGRID Nodes verwenden oder einige oder alle Festplatten oder SSDs von den ausgefallenen auf die Ersatz-Nodes verschoben haben, müssen Sie die gleichen 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 AFF 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.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Wiederherstellen von Grid-Nodes auf dem Host

Um einen fehlgeschlagenen Grid-Node auf einem neuen Linux-Host wiederherzustellen, stellen Sie die Node-Konfigurationsdatei mit den entsprechenden Befehlen wieder her.

Bei einer Neuinstallation 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.

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.

Schritte

- "Wiederherstellen und Validieren von Grid-Nodes"
- "Starten des StorageGRID Host Service"
- "Wiederherstellung von Nodes, die nicht ordnungsgemäß gestartet werden können"

Wiederherstellen und Validieren von 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 fehlende Knoten nicht importiert werden können, müssen Sie ihre 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 wiederherzuenden Node verwendet wurde.

Weitere Informationen zum Standort des finden Sie in den Installationsanweisungen `/var/local` Volume für einen Node:

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` Für das Flag sind zusätzliche Wiederherstellungsschritte erforderlich, bevor sie das Raster erneut verbinden können, wie unter „`zusätzliche Wiederherstellungsschritte ausführen, falls erforderlich`.“ beschrieben.

3. Für Grid-Nodes, die keinen über einen verfügen `/var/local` Volume: Erstellen Sie die Konfigurationsdatei des Node neu, um sie auf dem Host wiederherzustellen.

   Befolgen Sie die Richtlinien unter „`Erstellen von Node-Konfigurationsdateien`“ in den

Installationsanweisungen.

> Wenn Sie die Konfigurationsdatei für einen Node neu erstellen, müssen Sie denselben Namen für den Austausch-Node verwenden, der für den wiederherzuenden 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 Knoten neu erstellen, befolgen Sie alle Richtlinien unter „`Beheben fehlender 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.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"Beheben fehlender Netzwerkschnittstellenfehler"

"Beheben fehlender Blockgerätfehler"

"Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen"

Beheben fehlender Netzwerkschnittstellenfehler

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` Für Node_Node-Name_...`
`ERROR: node-name: GRID_NETWORK_TARGET = host-interface-name` *Node-Name*: Schnittstelle '*Host-Interface-Name*' existiert nicht`

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, stellen Sie sicher, dass Sie die Schritte unter „`Dbereitstellen neuer Linux-Hosts`“ abgeschlossen haben. 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.

Verwandte Informationen

"Bereitstellen neuer Linux-Hosts"

Beheben fehlender 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 existiert nicht`
```

Es bedeutet das `/etc/storagegrid/nodes/node-name.conf` Ordnet das von *Node-Name* verwendete Blockgerät dem angegebenen Pfad-Namen im Linux-Dateisystem zu, aber an diesem Speicherort gibt es keine gültige Sonderdatei für Blockgeräte oder keinen Softlink zu einer Sonderdatei für Blockgeräte.

Stellen Sie sicher, dass Sie die Schritte in „`DBereitstellung neuer Linux-Hosts`“ abgeschlossen haben. Verwenden Sie für alle Blockgeräte dieselben persistenten Gerätenamen, die auf dem ursprünglichen Host verwendet wurden.

Wenn Sie die fehlende Sonderdatei für Blockgeräte nicht wiederherstellen oder neu erstellen können, können Sie ein neues Blockgerät mit der entsprechenden Größe und Speicherkategorie zuweisen und die Knotenkonfigurationsdatei bearbeiten, um den Wert VON BLOCK_DEVICE_PURPOSE zu ändern, um auf die neue Sonderdatei für Blockgeräte zu verweisen.

Bestimmen Sie die geeignete Größe und Speicherkategorie aus den Tabellen im Abschnitt „`STorage Requirements`“ der Installationsanleitung für Ihr Linux-Betriebssystem. Lesen Sie die Empfehlungen unter „`Hostspeicher konfigurieren`“, bevor Sie mit dem Austausch von Blockgeräten fortfahren.

Wenn Sie ein neues Blockspeichergerät für eine der Konfigurationsdateivariablen angeben müssen, die mit beginnen `BLOCK_DEVICE_` Da das ursprüngliche Blockgerät mit dem ausgefallenen Host verloren gegangen ist, 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 Block Storage noch gültige Daten für den wiederherzustellenden Node 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
```

Verwandte Informationen

"Bereitstellen neuer Linux-Hosts"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Starten des 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.

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`

   Führen Sie für jeden Node, der den Status „nicht ausgeführt“ oder „angehalten“ zurückgibt, den folgenden Befehl aus:

   `sudo storagegrid node start node-name`

3. 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 ordnungsgemäß wieder in das Grid kommt und nicht als wiederherstellbar angezeigt wird, kann er beschädigt werden. Sie können den Node in den Recovery-Modus erzwingen.

So erzwingen Sie den Knoten in den Wiederherstellungsmodus:

```
sudo storagegrid node force-recovery node-name
```

Bestätigen Sie vor Ausgabe dieses Befehls, dass die Netzwerkkonfiguration des Node korrekt ist. Möglicherweise ist es aufgrund falscher Netzwerkschnittstellenzuordnungen oder einer falschen Grid-Netzwerk-IP-Adresse oder eines falschen Gateways fehlgeschlagen, das Grid-Netzwerk erneut anzuschließen.

Nach Ausstellung des `storagegrid node force-recovery node-name` Befehl, Sie müssen zusätzliche Recovery-Schritte für *Node-Name* durchführen.

Verwandte Informationen

"Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen"

Was ist weiter: Durchführung zusätzlicher Recovery-Schritte, falls 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

Beim Austausch eines Node sind möglicherweise folgende Korrekturmaßnahmen erforderlich:

- 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	"Konfigurieren des primären Ersatzadministratorknotens"

Art der Wiederherstellung	Nächster Schritt
Nicht primärer Admin-Node	"Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren"
Gateway-Node	"Wählen Sie Wiederherstellung starten, um einen Gateway-Node zu konfigurieren"
Archiv-Node	"Wählen Sie „Wiederherstellung starten“, um einen Archiv-Knoten zu konfigurieren"
Storage-Node (softwarebasiert): • Wenn man das benutzen musste `--force` Flag, um den Knoten zu importieren, oder Sie haben ausgegeben `storagegrid node force-recovery node-name` • Wenn Sie eine vollständige Neuinstallation des Knotens durchführen mussten, oder Sie müssen /var/local wiederherstellen	"Wählen Sie Wiederherstellung starten, um einen Speicherknoten zu konfigurieren"
Storage-Node (softwarebasiert): • Wenn Sie ein neues Blockgerät hinzugefügt haben. • Wenn, 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.	"Die Wiederherstellung nach einem Ausfall des Storage-Volumes ist bei intaktem Systemlaufwerk möglich"

Ersetzen eines fehlerhaften Knotens durch eine Services-Appliance

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.

Was Sie benötigen

- Sie müssen festgestellt haben, dass eine der folgenden Situationen zutrifft:
  - Die virtuelle Maschine, die den Node 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 müssen sicherstellen, dass die Installationsversion von StorageGRID Appliance auf der Services Appliance mit der Softwareversion des StorageGRID Systems übereinstimmt. Diese wird in der Hardwareinstallation und -Wartung für die Überprüfung und das Upgrade der Installationsversion von

StorageGRID Appliance beschrieben.

"SG100 SG1000 Services-Appliances"

Stellen Sie keine SG100- und SG1000-Service-Appliance am selben Standort bereit. 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 ausgefallene Node wurde auf VMware oder Linux gehostet (Plattformänderung)
- Der ausgefallene Node wurde auf einer Service Appliance gehostet (Plattformaustausch).

Schritte

- "Installieren einer Services Appliance (nur Plattformänderung)"
- "Vorbereiten eines Geräts für die Neuinstallation (nur Plattformaustausch)"
- "Starten der Softwareinstallation auf einer Service-Appliance"
- "Monitoring der Installation von Services Appliances"

Installieren einer Services Appliance (nur Plattformänderung)

Wenn Sie einen fehlgeschlagenen Grid-Node wiederherstellen, der auf VMware oder einem Linux-Host gehostet wurde und eine SG100- oder SG1000-Services-Appliance für den Ersatzknoten verwenden, müssen Sie zuerst die neue Appliance-Hardware mit dem gleichen Node-Namen wie der ausgefallene Node installieren.

Sie müssen über die folgenden Informationen zum ausgefallenen Node verfügen:

- **Knotenname**: Sie müssen die Services-Appliance mit dem gleichen Knotennamen wie der ausgefallene Knoten installieren.
- **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.

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.

1. Befolgen Sie die Anweisungen zum Installieren einer neuen SG100- oder SG1000-Services-Appliance.
2. Verwenden Sie bei der Aufforderung zu einem Node-Namen den Node-Namen des ausgefallenen Node.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Vorbereiten eines Geräts für die Neuinstallation (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. Führen Sie diese Schritte nicht aus, wenn der ausgefallene Node ursprünglich auf VMware oder einem Linux-Host gehostet wurde.

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 einer Service-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.

Was Sie benötigen

- Die Appliance muss in einem Rack installiert, mit dem Netzwerk verbunden und eingeschaltet sein.
- Netzwerkverbindungen und IP-Adressen müssen für die Appliance mithilfe des StorageGRID Appliance Installer konfiguriert werden.
- 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 Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, müssen in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert sein.

Anweisungen zum Abschließen dieser Vorraussaufgaben finden Sie in der Installations- und Wartungsanleitung für eine SG100- oder SG1000-Service-Appliance.

- Sie müssen einen unterstützten Webbrowser verwenden.

- Sie müssen eine der IP-Adressen kennen, 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 in der StorageGRID-Bereitstellung verwendeten Version übereinstimmt, benötigen Sie die Installationsdateien nicht.

Über diese Aufgabe

So installieren Sie die StorageGRID-Software auf einer SG100- oder SG1000-Services-Appliance:

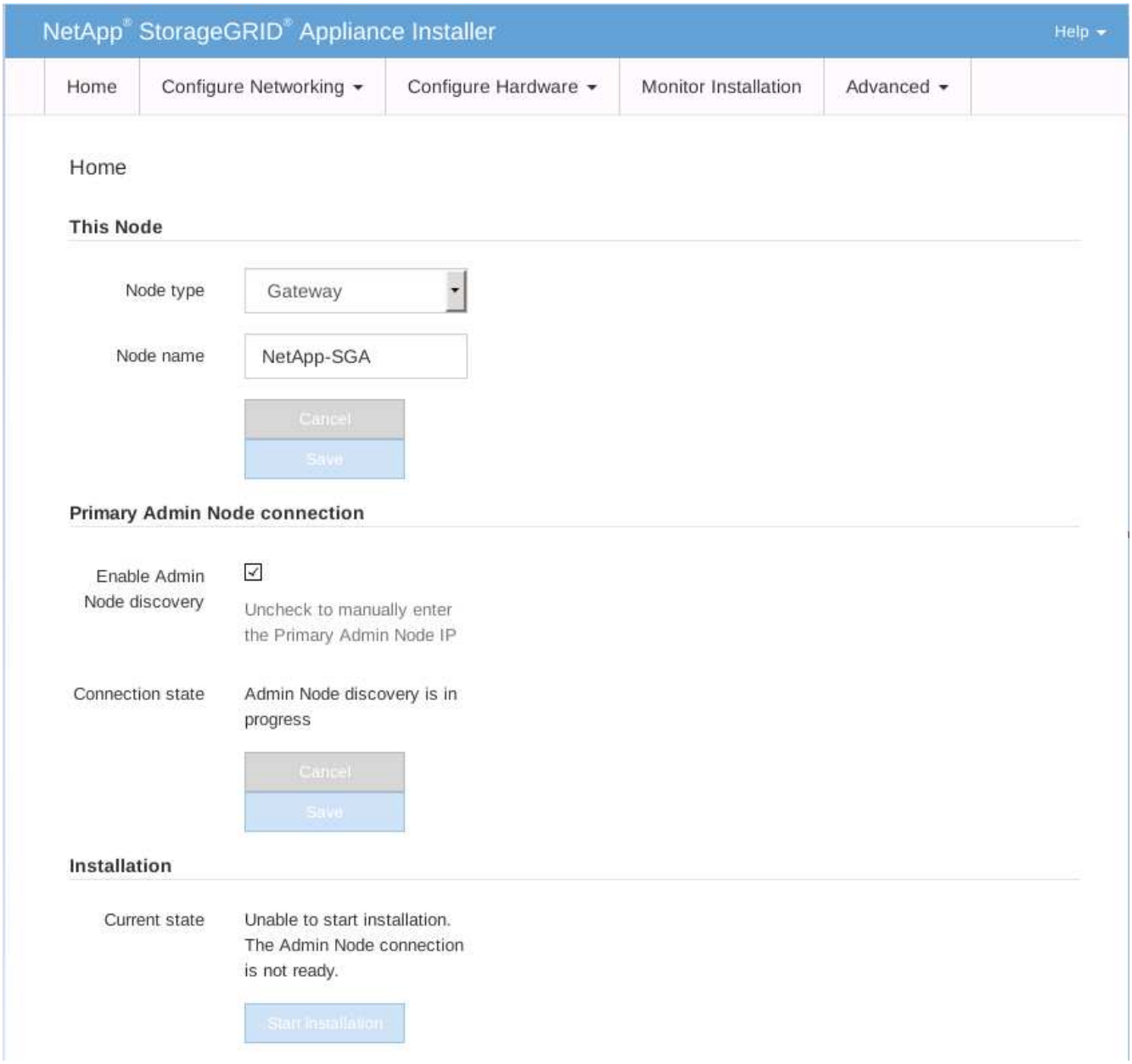
- Für einen primären Admin-Node geben Sie den Namen des Knotens an und laden dann die entsprechenden Softwarepakete hoch (falls erforderlich).
- Für einen nicht-primären Admin-Node oder einen Gateway-Node geben Sie die IP-Adresse des primären Admin-Node und den Namen des Node an oder bestätigen Sie diese.
- 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.



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	a. Deaktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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	a. Aktivieren Sie das Kontrollkästchen **Admin Node Discovery** 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 Installations- und Wartungsanleitung für Ihr Gerät.

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

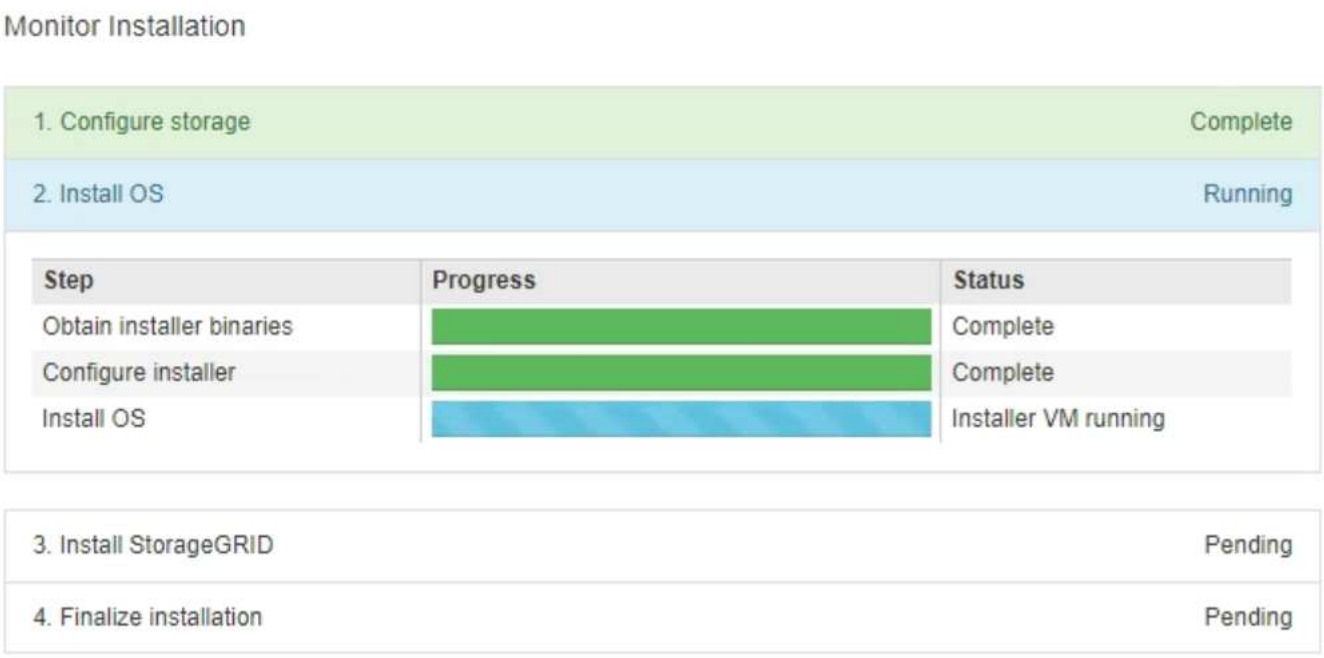
"SG100 SG1000 Services-Appliances"

Monitoring der Installation von Services Appliances

Das Installationsprogramm der StorageGRID Appliance stellt den Status bereit, bis die Installation abgeschlossen ist. Nach Abschluss der Softwareinstallation wird die Appliance neu gestartet.

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

   Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.



   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 „`Skipped.`“ angezeigt.

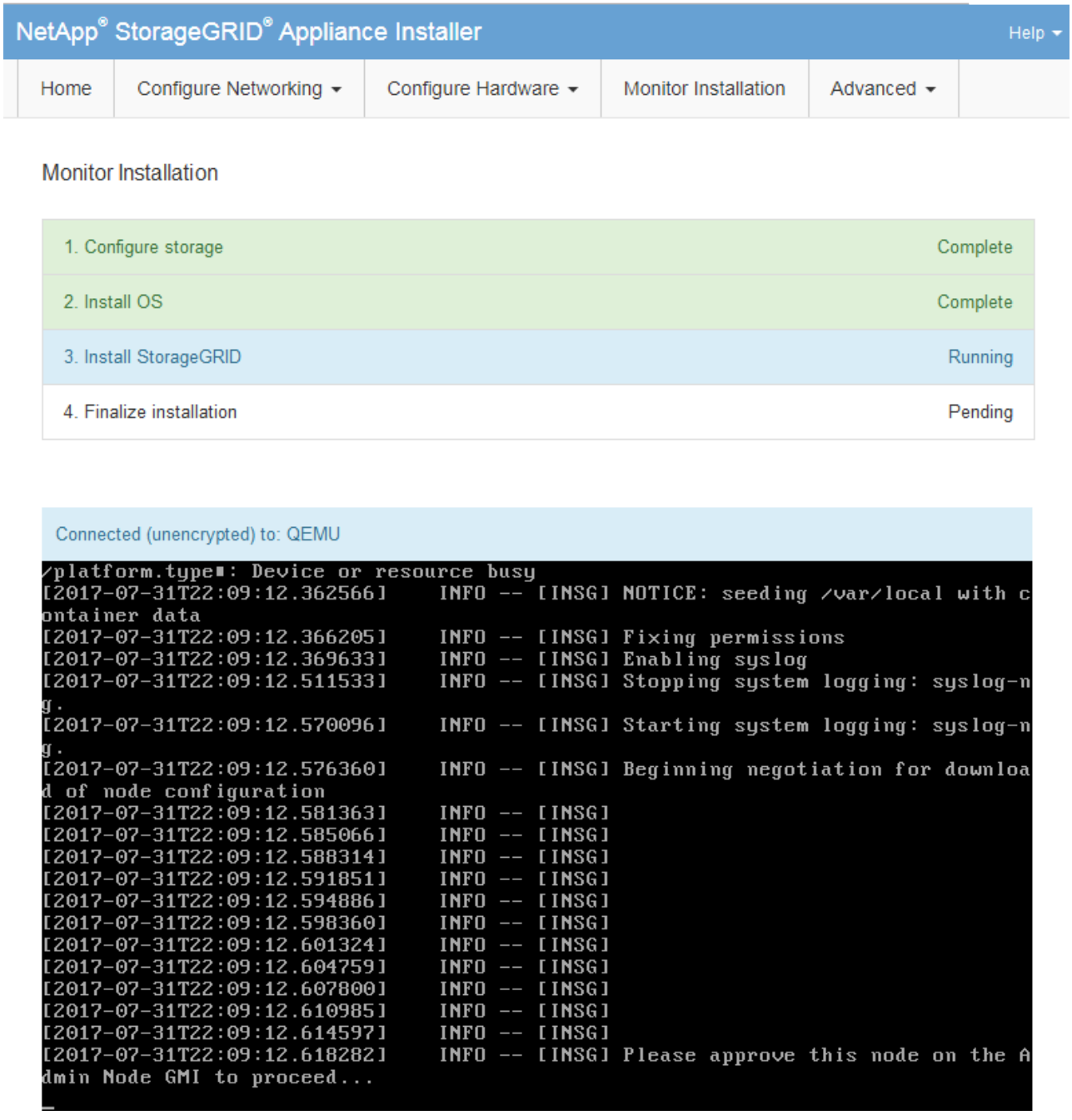
2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.
   - **1. Speicher konfigurieren**

     In dieser Phase löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken und konfiguriert die Hosteinstellungen.

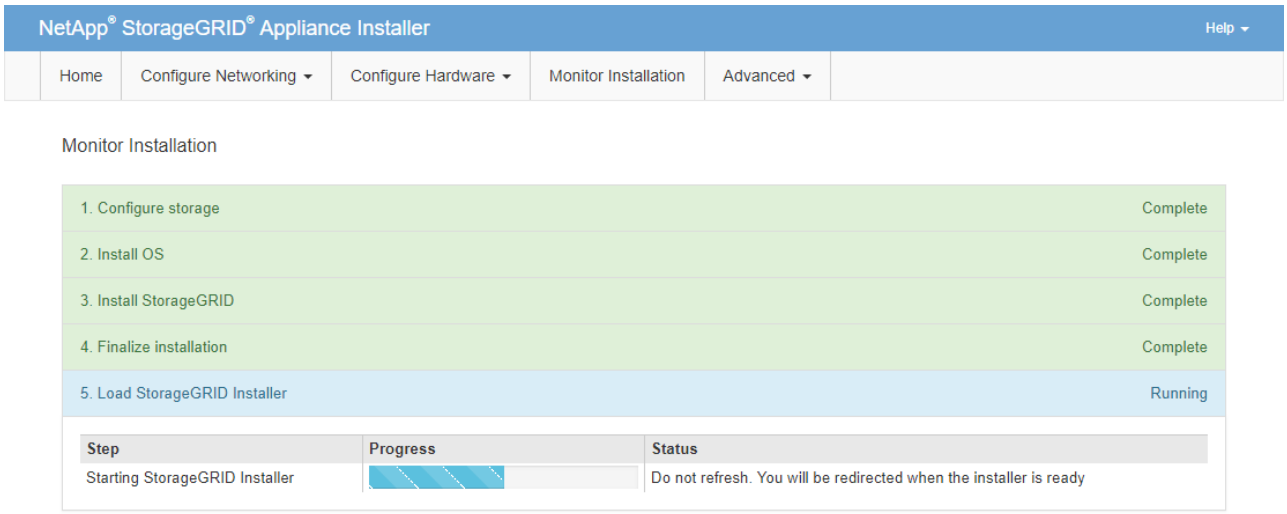
   - **2. Installieren Sie das Betriebssystem**

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.



   - 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.



4. Fahren Sie mit dem nächsten Schritt des Recovery-Prozesses für den Typ des Appliance-Grid-Node fort, den Sie wiederherstellen.

Art der Wiederherstellung	Referenz
Gateway-Node	"Wählen Sie Wiederherstellung starten, um einen Gateway-Node zu konfigurieren"
Nicht primärer Admin-Node	"Wählen Sie Wiederherstellung starten, um einen nicht primären Admin-Node zu konfigurieren"
Primärer Admin-Node	"Konfigurieren des primären Ersatzadministratorknotens"

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 Ausfalls**: Vor Beginn der Standortwiederherstellung ist es wichtig festzustellen, ob alle Knoten am ausgefallenen Standort intakt sind oder ob Speicherknoten wiederherstellbare Objekte

enthalten. 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.

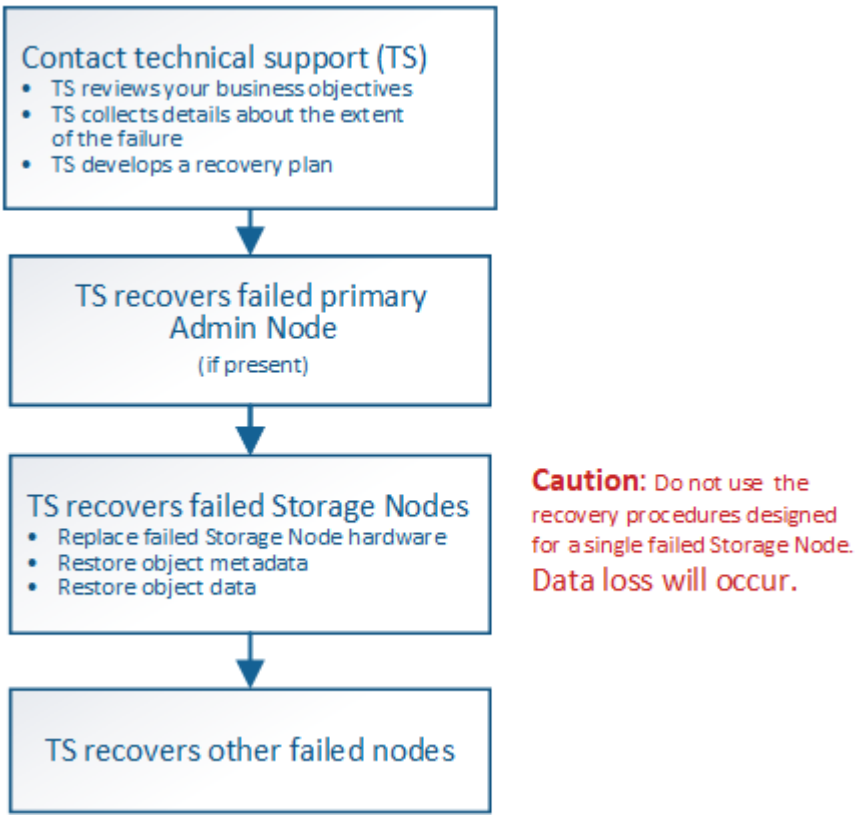
> Wenn ein Standort die einzige Kopie eines Objekts enthält und der Standort verloren geht, geht das Objekt verloren.

- **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.



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

"Außerbetriebnahme von Standorten"

Verfahren zur Deaktivierung

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 einen **Knoten außer Betrieb** aus, 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 eine Deaktivierung einer Site mit * Connected Site durch, um eine Site zu entfernen, auf der alle Nodes mit StorageGRID verbunden sind.
- Führen Sie eine Deaktivierung der Site durch **getrennt**, um eine Site zu entfernen, in der alle Nodes 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.

Verwandte Informationen

"Ausmusterung von Grid-Nodes"

"Außerbetriebnahme von Standorten"

Ausmusterung von Grid-Nodes

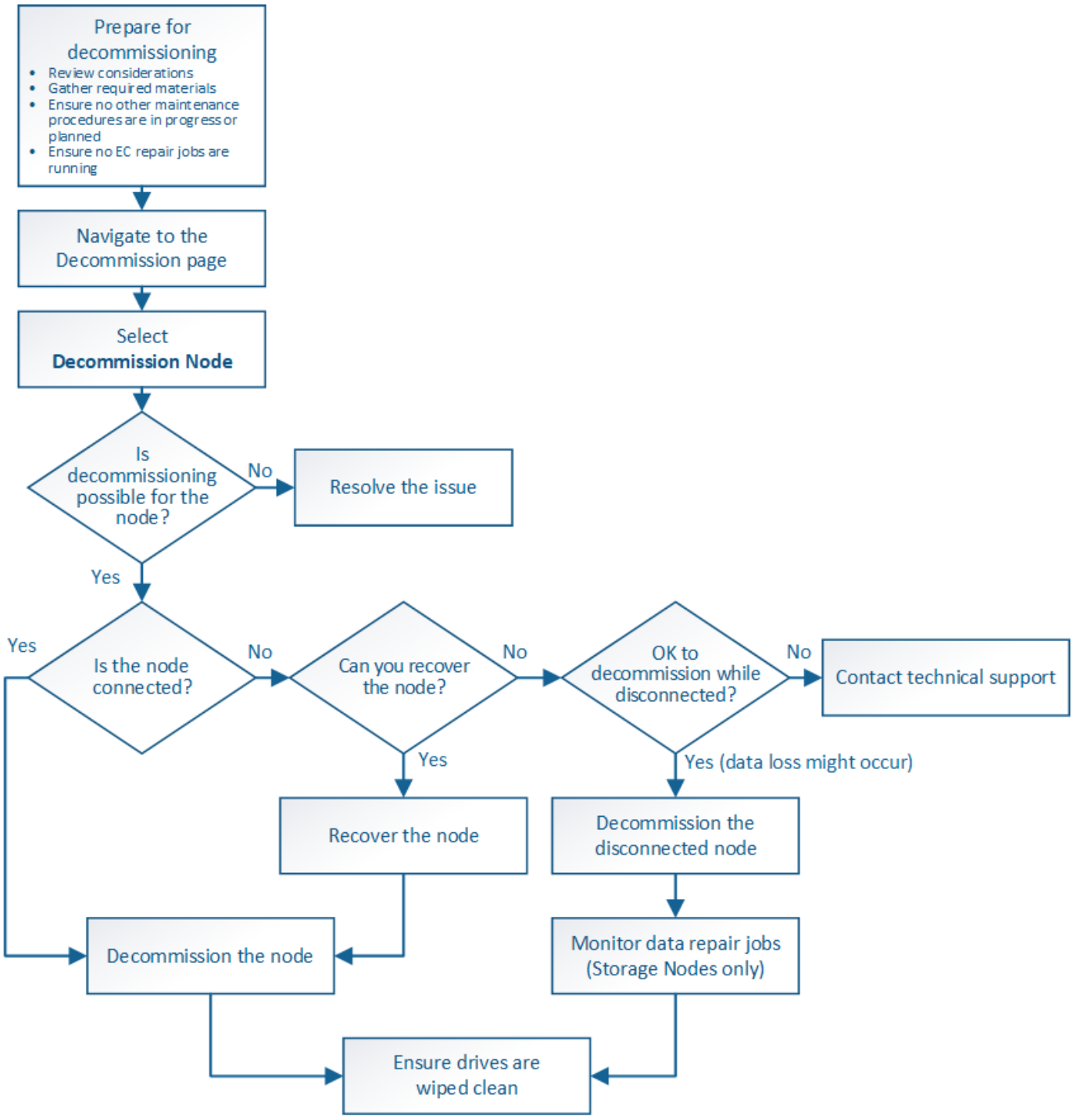
Sie können den Node Decounter-Vorgang verwenden, um einen oder mehrere Storage-Nodes, Gateway-Nodes oder nicht-primäre Admin-Nodes an einem oder mehreren Standorten zu entfernen. Sie können den primären Admin-Node oder einen Archiv-Node nicht stilllegen.

Im Allgemeinen sollten die Grid-Knoten nur deaktiviert werden, wenn sie mit dem StorageGRID-System verbunden sind und alle Knoten im normalen Zustand sind (haben grüne Symbole 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 Grid enthält einen getrennten Node, den Sie nicht wiederherstellen können oder wieder online schalten können.

Das Flussdiagramm zeigt die grundlegenden Schritte zur Deaktivierung von Grid-Nodes.



Schritte

- "Grid-Nodes werden vorbereitet"
- "Sammeln der erforderlichen Materialien"
- "Auf die Seite Decommission Nodes zugreifen"
- "Keine getrennten Grid-Nodes mehr"
- "Deaktivierung verbundener Grid-Nodes"
- "Anhalten und Fortsetzen des Stilllegen-Prozesses für Storage Nodes"
- "Fehlerbehebung bei der Ausmusterung von Nodes"

Grid-Nodes werden vorbereitet

Sie müssen die Überlegungen zum Entfernen von Grid-Nodes prüfen und bestätigen, dass keine Reparaturaufträge für Daten mit Erasure-Coding-Verfahren aktiv sind.

Schritte

- "Überlegungen für die Deaktivierung von Storage-Nodes"
- "Datenreparaturaufträge werden überprüft"

Überlegungen für die Deaktivierung 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 stilllegen, wenn Sie dies tun, bleibt die StorageGRID in einem ungültigen Status. Folgende Regeln werden durchgesetzt:

- Sie können den primären Admin-Node nicht stilllegen.
- Sie können Archiv-Knoten nicht stilllegen.
- Sie können einen Admin-Node oder einen Gateway-Node nicht stilllegen, wenn eine seiner Netzwerkschnittstellen Teil einer HA-Gruppe (High Availability, Hochverfügbarkeit) ist.
- Sie können einen Speicherknoten nicht stilllegen, wenn sich dessen Entfernung auf das ADC-Quorum auswirkt.
- 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 in Ihrem Grid keine getrennten Knoten enthalten sind (Knoten, deren Zustand unbekannt oder administrativ ausgefallen ist). Sie müssen zunächst die getrennten Nodes außer Betrieb nehmen oder wiederherstellen.
- Wenn Ihr Grid mehrere getrennte Nodes enthält, muss die Software gleichzeitig außer Betrieb genommen werden. Dadurch steigt das Risiko unerwarteter Ergebnisse.
- Wenn ein nicht getrennter Knoten nicht entfernt werden kann (z. B. ein Speicherknoten, der für das ADC-Quorum benötigt wird), kann kein anderer nicht getrennter Knoten entfernt werden.
- Wenn Sie eine ältere Appliance durch eine neuere Appliance ersetzen möchten, sollten Sie eventuell das Klonverfahren für den Appliance-Node verwenden, anstatt den alten Node abzubauen und den neuen Node zu einer Erweiterung hinzuzufügen.

  "Klonen von Appliance-Nodes"

> Entfernen Sie die virtuelle Maschine oder andere Ressourcen eines Grid-Node erst, wenn Sie dazu aufgefordert werden, dies in Stilllegen-Verfahren zu tun.

Überlegungen für die Deaktivierung von Admin-Nodes oder Gateway-Nodes

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.
- Sie können den primären Admin-Node nicht stilllegen.
- Sie können einen Admin-Node oder einen Gateway-Node nicht stilllegen, wenn eine seiner Netzwerkschnittstellen Teil einer HA-Gruppe (High Availability, Hochverfügbarkeit) ist. Sie müssen zuerst die Netzwerkschnittstellen aus der HA-Gruppe entfernen. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.
- 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.

Verwandte Informationen

"StorageGRID verwalten"

Überlegungen für die Deaktivierung von Storage-Nodes

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 Aufgabe zur Ausmusterung ausgeführt wird, können auf keinem Grid-Node Reparaturvorgänge

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 Alarme 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

"Wiederherstellen von Objektdaten in einem Storage Volume, falls erforderlich"

"Allgemeines zum ADC-Quorum"

"Überprüfung der ILM-Richtlinie und Storage-Konfiguration"

"Getrennte Storage-Nodes werden deaktiviert"

"Konsolidieren Von Storage-Nodes"

"Ausmusterung mehrerer Storage-Nodes"

Allgemeines zum ADC-Quorum

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.

Ein Speicherknoten kann nicht stillgelegt werden, wenn das Entfernen des Knotens dazu führt, 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 * *`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"

Überprüfung 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 unter „`Consolidating Storage Nodes`,“ beschrieben, sollten Sie neue Storage-Nodes hinzufügen, bevor alte entfernt werden. 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 zufriedenstellend ist, 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

"Konsolidieren Von Storage-Nodes"

"Objektmanagement mit ILM"

"Erweitern Sie Ihr Raster"

Getrennte Storage-Nodes werden deaktiviert

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:

- Ein getrennter Node sollte niemals außer Betrieb genommen werden, es sei denn, Sie können ihn nicht online oder wiederhergestellt werden.

> Führen Sie dieses Verfahren nicht aus, wenn Sie glauben, dass möglicherweise 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 Löschungscode auf aktuell verbundenen Storage-Nodes vorhanden sind.

- Wenn Sie einen getrennten Storage-Node ausmustern, wird der Vorgang der Ausmusterung relativ schnell abgeschlossen. Die Ausführung der Reparatur von Daten kann jedoch Tage oder Wochen dauern und wird nicht durch den Außerbetriebnahme überwacht. Sie müssen diese Jobs manuell überwachen und nach Bedarf neu starten. Siehe Anweisungen zur Datenreparatur-Überwachung.

  "Datenreparaturaufträge werden überprüft"

- 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 mehr als ein getrennter Speicherknoten vorhanden ist, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

Konsolidieren Von Storage-Nodes

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.

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"

Ausmusterung 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.

Datenreparaturaufträge werden überprüft

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 getrennten Speicherknoten stilllegen müssen, führen Sie diese Schritte auch aus, nachdem der Vorgang abgeschlossen wurde, um sicherzustellen, dass der Reparaturauftrag 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 Reparaturaufträge 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.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
================================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. Wenn der Zustand für alle Reparaturen ist `Success`, Sie müssen keine Reparaturaufträge neu starten.
4. Wenn der Status für eine Reparatur ist `Failure`, 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 `Success`.

Sammeln der erforderlichen Materialien

Bevor Sie einen Grid-Node außer Betrieb nehmen, müssen Sie die folgenden Informationen erhalten.

Element	Hinweise
Wiederherstellungspaket `.zip` Datei	Sie müssen das neueste Wiederherstellungspaket herunterladen `.zip` Datei (`sgws-recovery-package-`*`id-revision`*`.zip`). Sie können die Recovery Package-Datei verwenden, um das System wiederherzustellen, wenn ein Fehler auftritt.
`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"

"Herunterladen des Wiederherstellungspakets"

Auf die Seite Decommission Nodes zugreifen

Wenn Sie im Grid Manager auf die Seite Decommission Nodes zugreifen, sehen Sie auf einen Blick, welche Knoten deaktiviert werden können.

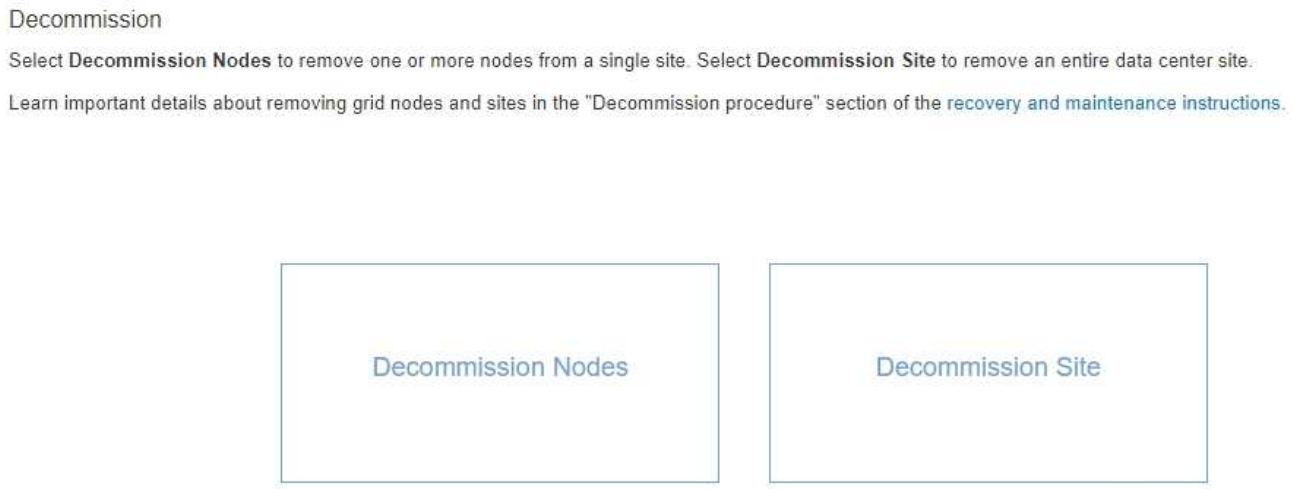
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.

Schritte

1. Wählen Sie **Wartung** > **Wartungsaufgaben** > **Dekommission**.

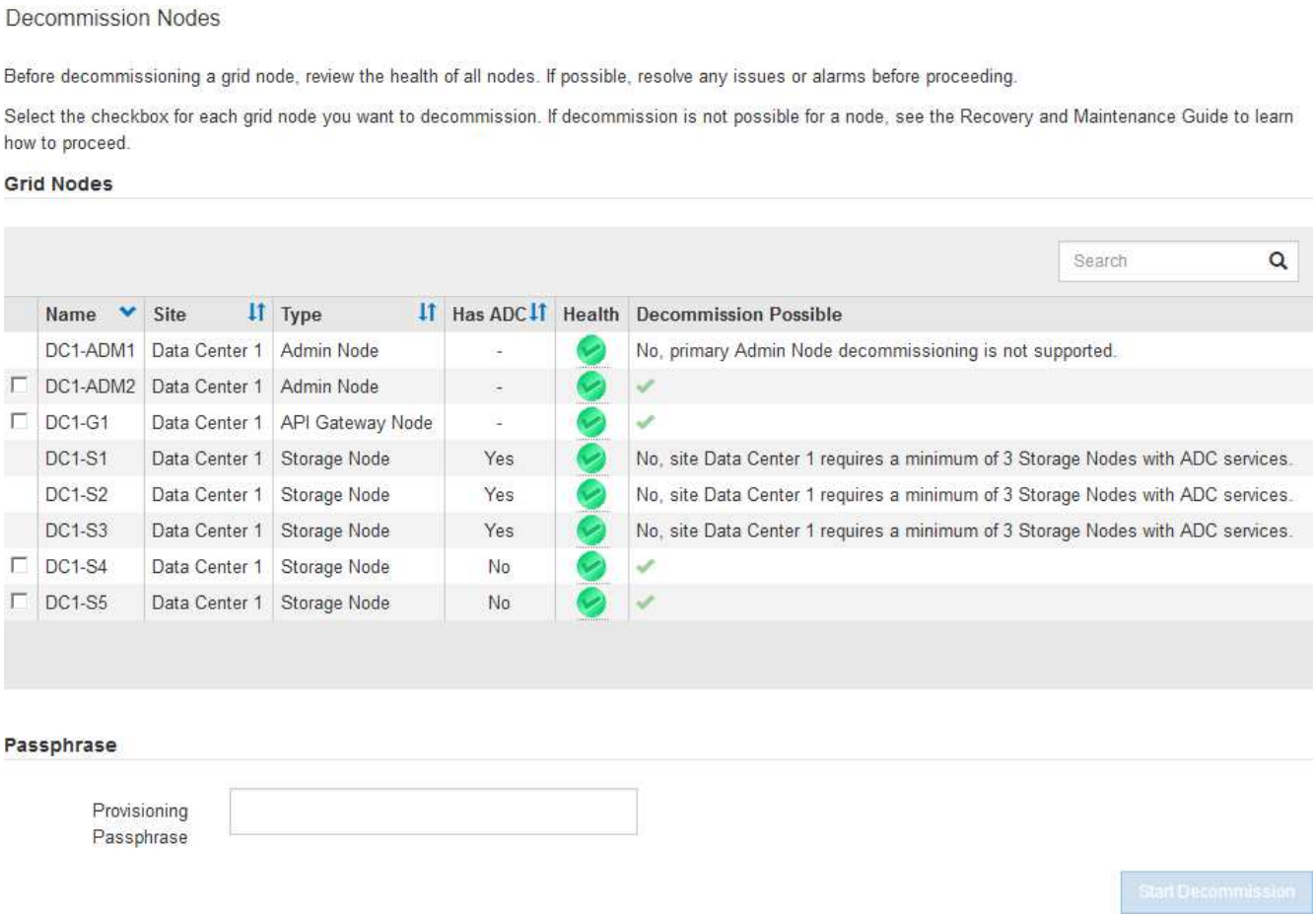
   Die Seite Decommission wird angezeigt.



2. Klicken Sie auf die Schaltfläche **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 alle Grid-Nodes in einem einzelnen Datacenter angezeigt. Die Spalte Decommission Mögliche gibt an, dass Sie den nicht-primären Admin-Node, den Gateway-Node und zwei der fünf Storage-Nodes außer Betrieb nehmen können.



3. Überprüfen Sie die Spalte **Decommission möglich** für jeden Knoten, den Sie stilllegen möchten.

   Wenn ein Grid-Node deaktiviert werden kann, enthält diese Spalte ein grünes Häkchen, und in der Spalte links ist das Kontrollkästchen enthalten. Wenn ein Node nicht außer Betrieb genommen werden kann, wird in dieser Spalte das Problem beschrieben. Wenn ein Node nicht mehr außer einem Grund außer Betrieb genommen werden kann, wird der kritischste 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 Archiv-Node nicht stilllegen.	Keine.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, mindestens ein Grid-Node ist getrennt. **Hinweis:** Diese Meldung wird nur für verbundene Grid-Knoten angezeigt.	Sie können einen verbundenen Grid-Node nicht stilllegen, wenn ein Grid-Node getrennt ist. Die Spalte **Health** enthält eines der folgenden Symbole für getrennte Grid-Knoten: • (Grau): Administrativ nach unten • (Blau): Unbekannt	Wechseln Sie zum Schritt, in dem die Optionen für das Stilllegen aufgeführt sind.
Nein, ein oder mehrere erforderliche Nodes sind derzeit getrennt und müssen wiederhergestellt werden. **Hinweis:** Diese Meldung wird nur für getrennte Gitterknoten angezeigt.	Ein nicht getrennter Grid-Node kann nicht stillgelegt werden, wenn auch ein oder mehrere erforderliche Nodes getrennt sind (z. B. ein Storage-Node, der für das ADC-Quorum erforderlich ist).	a. Überprüfen Sie die möglichen Meldungen zur Dekommission für alle nicht verbundenen Knoten. b. Legen Sie fest, welche Nodes nicht außer Betrieb genommen werden können, da sie erforderlich sind. ◦ 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.
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 oder einen Gateway-Node nicht außer Betrieb nehmen, wenn eine Node-Schnittstelle einer HA-Gruppe (High Availability, Hochverfügbarkeit) angehört.	Bearbeiten Sie die HA-Gruppe, um die Schnittstelle des Node zu entfernen, oder entfernen Sie die gesamte HA-Gruppe. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, Standort *x* erfordert mindestens *n* Storage Nodes mit ADC-Services.	**Nur Speicherknoten.** ein Speicherknoten kann nicht stillgelegt werden, wenn nicht genügend Knoten am Standort verbleiben würden, um 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 über das ADC-Quorum.
Nein, mindestens ein Erasure Coding-Profil benötigt mindestens *n* Storage-Nodes. Wenn das Profil in einer ILM-Regel nicht verwendet wird, können Sie es deaktivieren.	**Nur Speicherknoten.** Sie können einen Speicherknoten nicht stilllegen, es sei denn, es würden genügend Knoten für die vorhandenen Erasure Coding Profile übrig bleiben. Wenn beispielsweise ein Erasure Coding-Profil für das Erasure Coding-Verfahren von 4+2 vorhanden ist, müssen mindestens 6 Storage-Nodes verbleiben.	Führen Sie für jedes betroffene Erasure Coding-Profil einen der folgenden Schritte aus, je nachdem, wie das Profil verwendet wird: • **In der aktiven ILM-Richtlinie verwendet**: Eine Erweiterung durchführen. Fügen Sie genügend neue Storage-Nodes hinzu, um das Erasure Coding-Verfahren fortzusetzen. Weitere Informationen finden Sie in den Anweisungen zum erweitern von StorageGRID. • **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. • **Nicht in einer ILM-Regel verwendet**: Deaktivieren Sie das Erasure Coding-Profil. **Hinweis:** eine Fehlermeldung erscheint, wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren und Objektdaten weiterhin mit dem Profil verknüpft sind. Sie müssen möglicherweise mehrere Wochen warten, bevor Sie den Deaktivierungsprozess erneut versuchen. Erfahren Sie mehr über die Deaktivierung eines Erasure Coding-Profils in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

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	"Keine getrennten Grid-Nodes mehr"
Nur verbundene Grid-Nodes	"Deaktivierung verbundener Grid-Nodes"

Verwandte Informationen

"Datenreparaturaufträge werden überprüft"

"Allgemeines zum ADC-Quorum"

"Objektmanagement mit ILM"

"Erweitern Sie Ihr Raster"

"StorageGRID verwalten"

Keine getrennten Grid-Nodes mehr

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).

Was Sie benötigen

- Sie kennen die Anforderungen und Überlegungen für die Deaktivierung von Grid-Nodes.

  "Überlegungen für die Deaktivierung von Grid-Nodes"

- Sie haben alle erforderlichen Elemente erhalten.
- Sie haben sichergestellt, dass keine Datenreparaturjobs aktiv sind.

  "Datenreparaturaufträge werden überprüft"

- 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 müssen über eine Passphrase für die Bereitstellung verfügen.

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 Nodes enthält, muss die Software gleichzeitig außer Betrieb genommen werden. Dadurch steigt das Risiko unerwarteter Ergebnisse.

  > Gehen Sie sehr vorsichtig vor, wenn Sie mehrere getrennte Grid-Nodes gleichzeitig außer Betrieb nehmen. Dies gilt insbesondere dann, wenn Sie mehrere getrennte Storage-Nodes auswählen.

- Wenn ein nicht getrennter Knoten nicht entfernt werden kann (z. B. ein Speicherknoten, der für das ADC-Quorum benötigt wird), kann kein anderer nicht getrennter Knoten entfernt werden.

Beachten Sie vor dem Stilllegen eines nicht verbundenen **Storage Node** Folgendes

- Sie sollten niemals einen getrennten Storage-Knoten außer Betrieb nehmen, wenn Sie sicher sind, dass er nicht online oder wiederhergestellt werden kann.

  Wenn Sie glauben, dass Objektdaten weiterhin über den Node wiederhergestellt werden können, führen Sie dieses Verfahren nicht aus. 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 mehr als ein getrennter Speicherknoten vorhanden ist, 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 der Reparatur von Daten kann jedoch Tage oder Wochen dauern und wird nicht durch den Außerbetriebnahme überwacht. Sie müssen diese Jobs manuell überwachen und nach Bedarf neu starten. Siehe Anweisungen zur Datenreparatur-Überwachung.

  "Datenreparaturaufträge werden überprüft"

- 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 Löschungscode 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 getrennten Grid-Node nicht wiederherstellen können und ihn während der Trennung außer Betrieb setzen möchten, aktivieren Sie das Kontrollkästchen für diesen Node.

   Wenn Ihr Grid mehrere getrennte Nodes enthält, muss die Software gleichzeitig außer Betrieb genommen werden. Dadurch steigt das Risiko unerwarteter Ergebnisse.

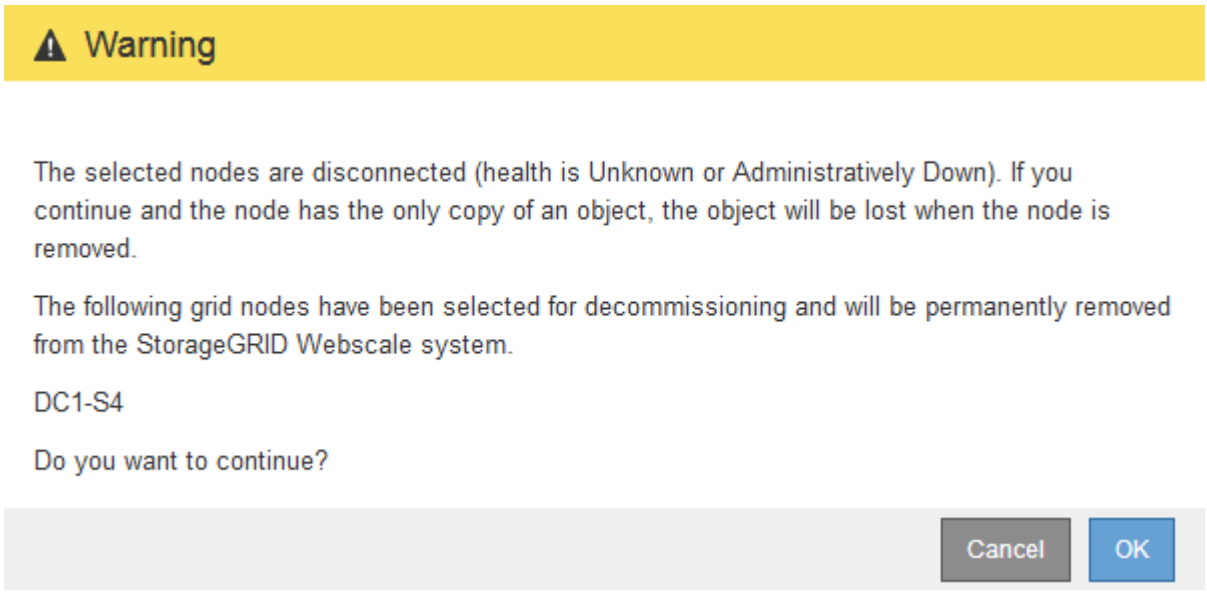
Gehen Sie sehr vorsichtig vor, wenn Sie mehrere getrennte Grid-Nodes gleichzeitig deaktivieren möchten, insbesondere wenn Sie mehrere getrennte Storage-Nodes auswählen. Wenn mehr als ein getrennter Speicherknoten vorhanden ist, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

3. Geben Sie die Provisionierungs-Passphrase ein.

   Die Schaltfläche **Start Decommission** ist aktiviert.

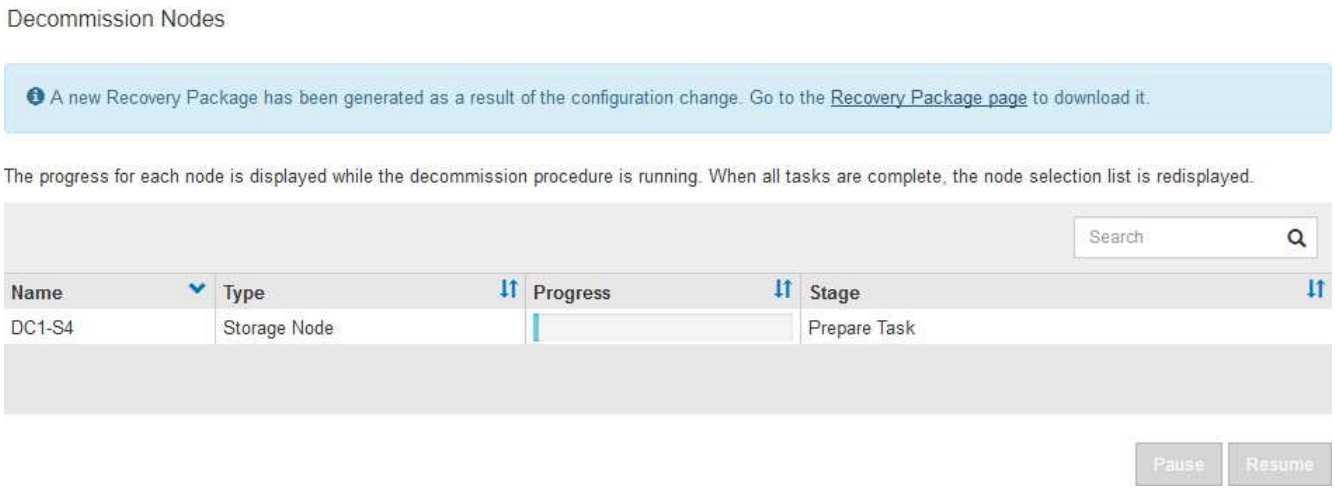
4. Klicken Sie Auf **Start Decommission**.

   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.



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.



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:

Lesen Sie die Anweisungen zum 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 Datenreparaturaufgaben, die während des Stilllegungsvorgangs automatisch gestartet werden.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie **StorageGRID Deployment** oben in der Grid Topology Tree aus.
   c. Suchen Sie auf der Registerkarte „Übersicht“ den Abschnitt „ILM-Aktivität“.
   d. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.

      > Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

      - **Reparted (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

Repears 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.

e. Verwenden Sie die folgenden Befehle, um Reparaturen zu verfolgen oder neu zu starten:

   - Verwenden Sie die `repair-data show-ec-repair-status` Befehl zum Nachverfolgen von Reparaturen an Erasure-codierten Daten.
   - Verwenden Sie die `repair-data start-ec-node-repair` Befehl mit dem `--repair-id` Option zum Neustart einer fehlgeschlagenen Reparatur. Informationen zum Überprüfen von Datenreparaturjobs finden Sie in den Anweisungen.

10. Verfolgen Sie den Status der EC-Datenreparaturen weiter, bis alle Reparaturaufträge erfolgreich abgeschlossen wurden.

    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 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.

  "SG100 SG1000 Services-Appliances"

  "SG5600 Storage Appliances"

  "SG5700 Storage-Appliances"

  "SG6000 Storage-Appliances"

Verwandte Informationen

"Verfahren zur Recovery von Grid-Nodes"

"Herunterladen des Wiederherstellungspakets"

"Datenreparaturaufträge werden überprüft"

Deaktivierung verbundener Grid-Nodes

Sie können Nodes, die mit dem Grid verbunden sind, außer Betrieb nehmen und dauerhaft entfernen.

Was Sie benötigen

- Sie kennen die Anforderungen und Überlegungen für die Deaktivierung von Grid-Nodes.

"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. 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.
- Sie haben die Provisionierungs-Passphrase.
- Die Grid-Nodes sind verbunden.
- Die Spalte **Decommission möglich** für den Knoten oder Knoten, die deaktiviert werden sollen, enthält ein grünes Häkchen.
- 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. Informationen zum Überprüfen von Datenreparaturjobs finden Sie in den Anweisungen.

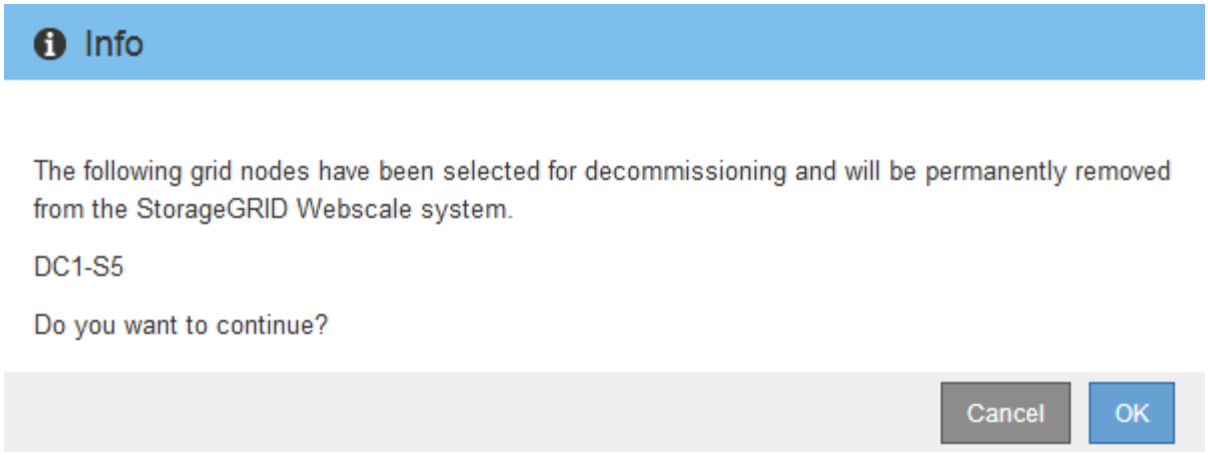
Entfernen Sie die virtuelle Maschine oder andere Ressourcen eines Grid-Node erst, wenn Sie dazu in diesem Verfahren aufgefordert werden.

Schritte

1. Aktivieren Sie auf der Seite Decommission Nodes das Kontrollkästchen für jeden Grid-Knoten, den Sie stilllegen möchten.
2. Geben Sie die Provisionierungs-Passphrase ein.

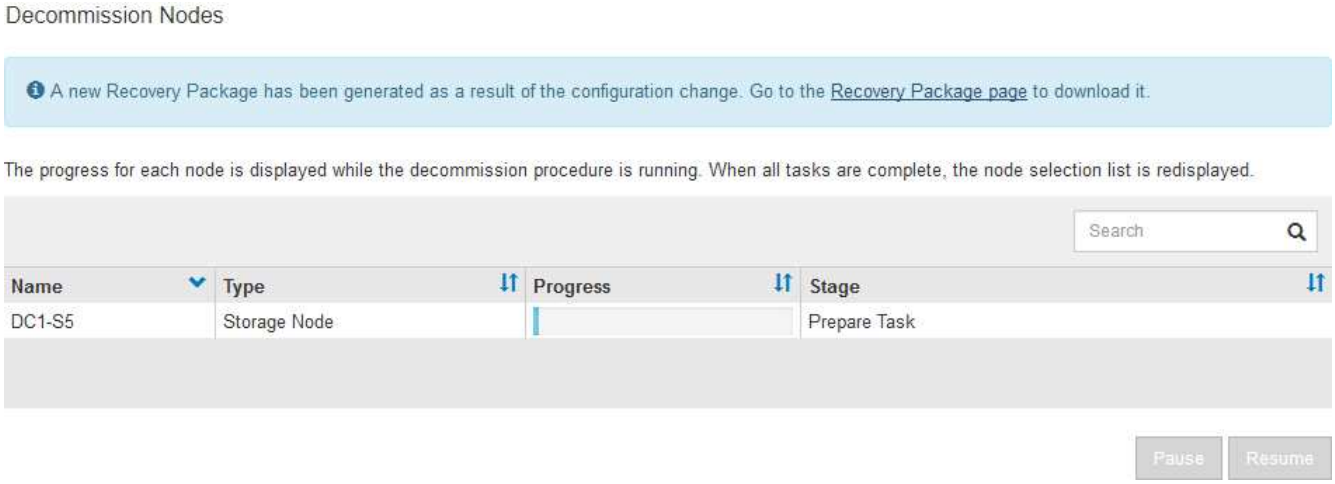
   Die Schaltfläche **Start Decommission** ist aktiviert.
3. Klicken Sie Auf **Start Decommission**.

   Ein Bestätigungsdialogfeld wird angezeigt.



4. Überprüfen Sie die Liste der ausgewählten Knoten, 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.



> Nehmen Sie einen Storage Node nicht in den Offline-Modus, nachdem der Vorgang zur Deaktivierung 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:

   Lesen Sie die Anweisungen zum 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 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 in einem anderen Raster verwenden möchten, müssen Sie die KMS-Konfiguration löschen.

  "SG100 SG1000 Services-Appliances"

  "SG5600 Storage Appliances"

  "SG5700 Storage-Appliances"

  "SG6000 Storage-Appliances"

Verwandte Informationen

"Datenreparaturaufträge werden überprüft"

"Herunterladen des Wiederherstellungspakets"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

Anhalten und Fortsetzen des Stilllegen-Prozesses für Storage Nodes

Sie können den Decommission-Vorgang für einen Storage-Node gegebenenfalls während bestimmter Phasen unterbrechen. Sie müssen die Deaktivierung auf einem Storage-Node unterbrechen, bevor Sie ein zweites Wartungsverfahren starten können. Nachdem das andere Verfahren abgeschlossen ist, können Sie die Stilllegung fortsetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.

Schritte

1. Wählen Sie **Wartung** > **Wartungsaufgaben** > **Dekommission**.

Die Seite Decommission wird angezeigt.

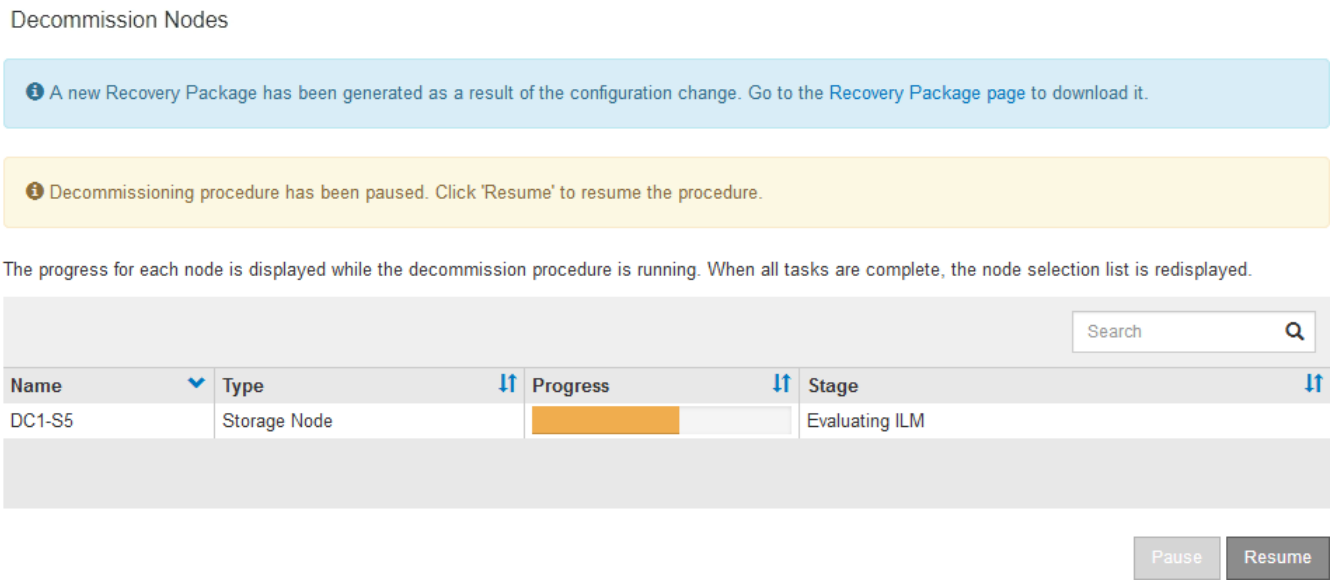
2. Klicken Sie Auf **Decommission Nodes**.

   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 stilllegung

3. Klicken Sie auf **Pause**, um den Vorgang zu unterbrechen.

   Die aktuelle Phase wird angehalten, und die Schaltfläche **Fortsetzen** ist aktiviert.



4. Klicken Sie nach Abschluss des anderen Wartungsverfahrens auf **Fortsetzen**, 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.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

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

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Erweitern Sie in der Struktur Grid Topology jeden Storage Node-Eintrag und überprüfen Sie, ob die DDS- und LDR-Dienste online sind.

   Um die Ausmusterung von Storage-Nodes durchzuführen, müssen die DDS-Services des StorageGRID Systems (gehostet durch Storage-Nodes) online sein. Dies ist eine Anforderung einer ILM-Neubewertung.

3. Um die aktiven Grid-Aufgaben anzuzeigen, wählen Sie **Primary Admin Node CMN Grid Tasks Übersicht**.
4. Überprüfen Sie den Status der Task „Stilllegen“.

    a. Wenn der Status des DeaktivierungsGrid-Tasks ein Problem beim Speichern von Grid Task Bundles anzeigt, wählen Sie **Primary Admin Node CMN Events Übersicht** aus

    b. 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.

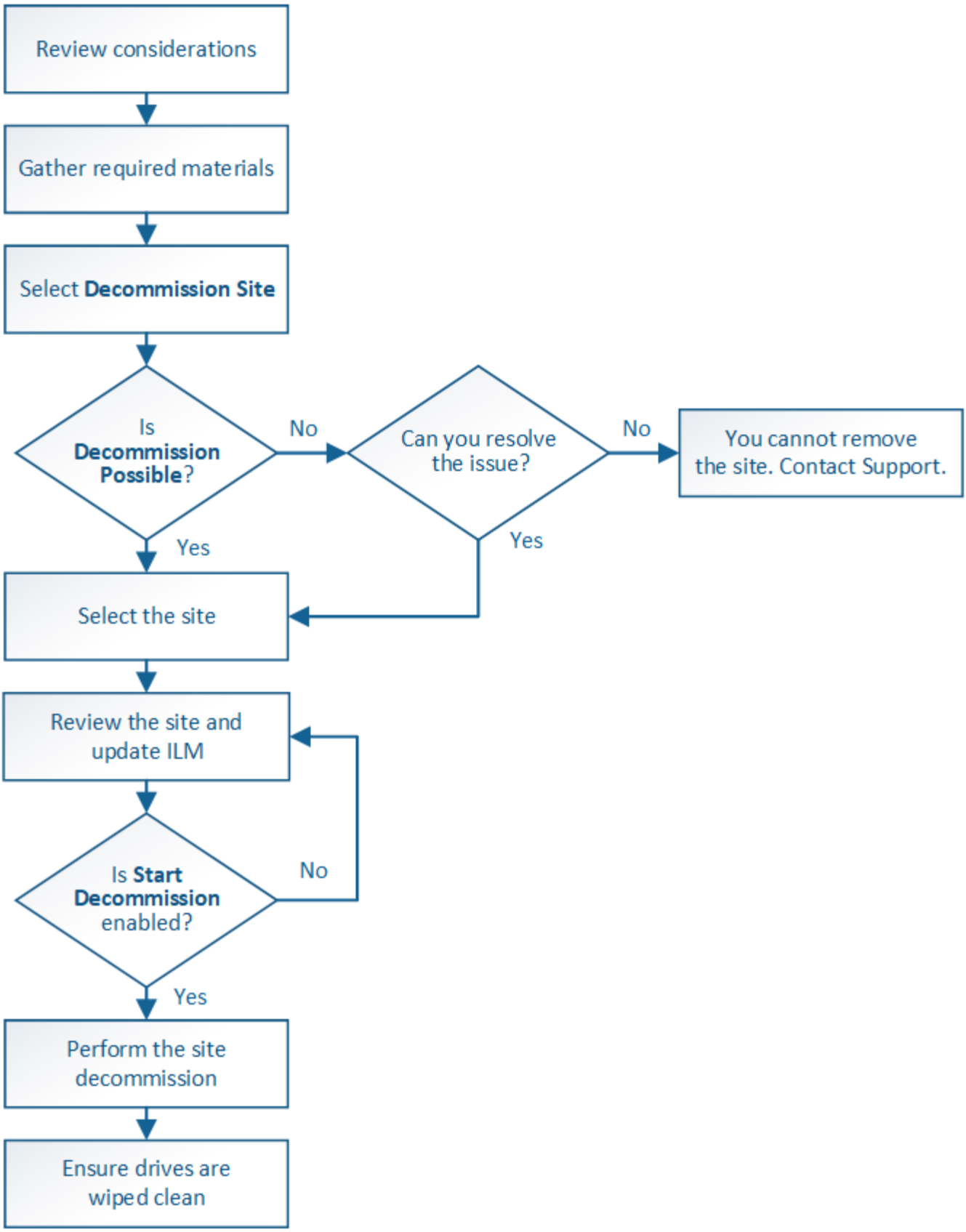
Der CMN-Dienst muss mit mindestens einem ADC-Dienst verbunden sein, und eine Mehrheit (50 Prozent plus einer) der ADC-Dienste des StorageGRID-Systems muss verfügbar sein, damit eine Grid-Aufgabe von einer Phase der Stilllegung in eine andere und zum Abschluss verschoben werden kann.

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.

Außerbetriebnahme von Standorten

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.



Schritte

- "Überlegungen zum Entfernen eines Standorts"
- "Sammeln der erforderlichen Materialien"

- "Schritt 1: Standort Auswählen"
- "Schritt 2: Details Anzeigen"
- "Schritt 3: ILM-Richtlinie überarbeiten"
- "Schritt 4: Entfernen Sie ILM-Referenzen"
- "Schritt 5: Auflösen von Knotenkonflikten (und Start der Stilllegung)"
- "Schritt 6: Überwachung Der Dekommission"

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 Storage-Pools oder Erasure Coding-Profile mehr verwenden, die auf den Standort verwiesen wurden. Wenn StorageGRID einen Standort dekomprimiert, werden diese Storage-Pools automatisch entfernt und diese Erasure Coding-Profile 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 keinen Standort außer Betrieb nehmen, der den primären Admin-Node enthält.
- Sie können keine Site außer Betrieb setzen, die einen Archiv-Node enthält.
- Sie können einen Standort nicht stilllegen, 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 verbundener (enthält Und getrennt (Oder) Knoten.
- Sie können einen Standort nicht stilllegen, wenn ein Node an einem anderen Standort getrennt ist (Oder).
- Sie können den Vorgang zur Deaktivierung des Standorts nicht starten, wenn derzeit ein ec-Node-Reparaturvorgang ausgeführt wird. Im folgenden Thema finden Sie Informationen zur Nachverfolgung von Reparaturen von Daten, die mit der Löschung versehen sind.

  "Datenreparaturaufträge werden überprüft"

- Während die Deaktivierung der Website läuft:
  - Sie können keine ILM-Regeln erstellen, die sich auf die auszugemusterte Site beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf die Site zu verweisen.
  - Sie können keine anderen Wartungsvorgänge wie z. B. Erweiterung oder Upgrade 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.
- Sie können nicht mehrere Standorte gleichzeitig außer Betrieb nehmen.
- 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 die Site, auch wenn diese Regeln nicht in der aktiven oder vorgeschlagenen Richtlinie verwendet werden. Sie müssen alle Regeln, die sich auf die Website beziehen, löschen oder bearbeiten.

Wenn StorageGRID den Standort dekomprimiert, werden automatisch alle nicht verwendeten Erasure Coding-Profile deaktiviert, die auf den Standort verweisen. Außerdem werden alle nicht verwendeten Speicherpools, die sich auf den Standort beziehen, automatisch gelöscht. Der standardmäßige Speicherpool Alle Speicherknoten wird 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 alle Kenntnisse über die Funktionsweise von ILM haben und dass Sie mit der Erstellung von Storage-Pools, Erasure Coding-Profilen, ILM-Regeln sowie der Simulation und Aktivierung einer ILM-Richtlinie vertraut sind. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

"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 ausreichend Kapazität verfügbar ist, müssen Sie möglicherweise einem vorhandenen Standort Storage-Volumes oder Speicherknoten hinzufügen oder einen neuen Standort hinzufügen, bevor Sie diesen Vorgang ausführen. Anweisungen zum erweitern eines StorageGRID-Systems finden Sie in den Anweisungen.

- 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 abschließen, der den Stilllegen-Prozess startet, es sei denn, alle Knoten sind verbunden.

- Wenn der Standort, den Sie entfernen möchten, einen Gateway-Node oder einen Admin-Node enthält, der zum Load Balancing verwendet wird, müssen Sie möglicherweise ein Erweiterungsverfahren durchführen, um einen entsprechenden neuen Node an einem anderen Standort hinzuzufügen. Es muss sichergestellt sein, dass Clients eine Verbindung zum Ersatz-Node herstellen können, bevor der Standort ausmustern 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 abschließen. Dieser startet den Ausmustern-Prozess, 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 Ihr StorageGRID System möglicherweise um Storage Nodes, Storage Volumes oder neue Standorte erweitern, bevor Sie eine angeschlossene Website ausmustern.
- 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.

- Alle Nodes am Standort müssen einen Verbindungsstatus von einer der folgenden aufweisen:
  - * Unbekannt* (): Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen.
  - **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** (verfügen); 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, wenn die Site die einzige Kopie eines Objekts enthielt und nicht abgerufen werden kann.

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. Die Konsistenzstufe gibt einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten 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.

Verwandte Informationen

"Durchführen der Standortwiederherstellung durch den technischen Support"

"Objektmanagement mit ILM"

"Erweitern Sie Ihr Raster"

Sammeln der 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 (`sgws-recovery-package-id-revision.zip`). Sie können die Recovery Package-Datei verwenden, um das System wiederherzustellen, wenn ein Fehler auftritt.
`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"

"Herunterladen des Wiederherstellungspakets"

Schritt 1: Standort Auswählen

Um zu bestimmen, ob eine Site deaktiviert werden kann, öffnen Sie zunächst den Assistenten zur Deaktivierung der Site.

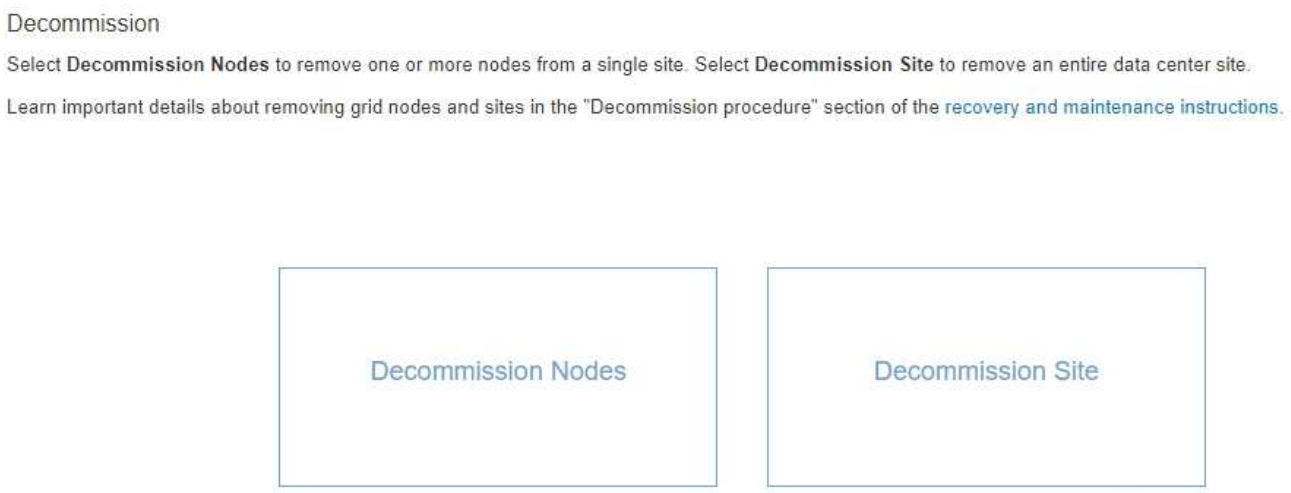
Was Sie benötigen

- Sie müssen alle erforderlichen Materialien erhalten haben.
- Sie müssen die Überlegungen zum Entfernen eines Standorts geprüft haben.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Stammzugriff oder die Wartungs- und ILM-Berechtigungen verfügen.

Schritte

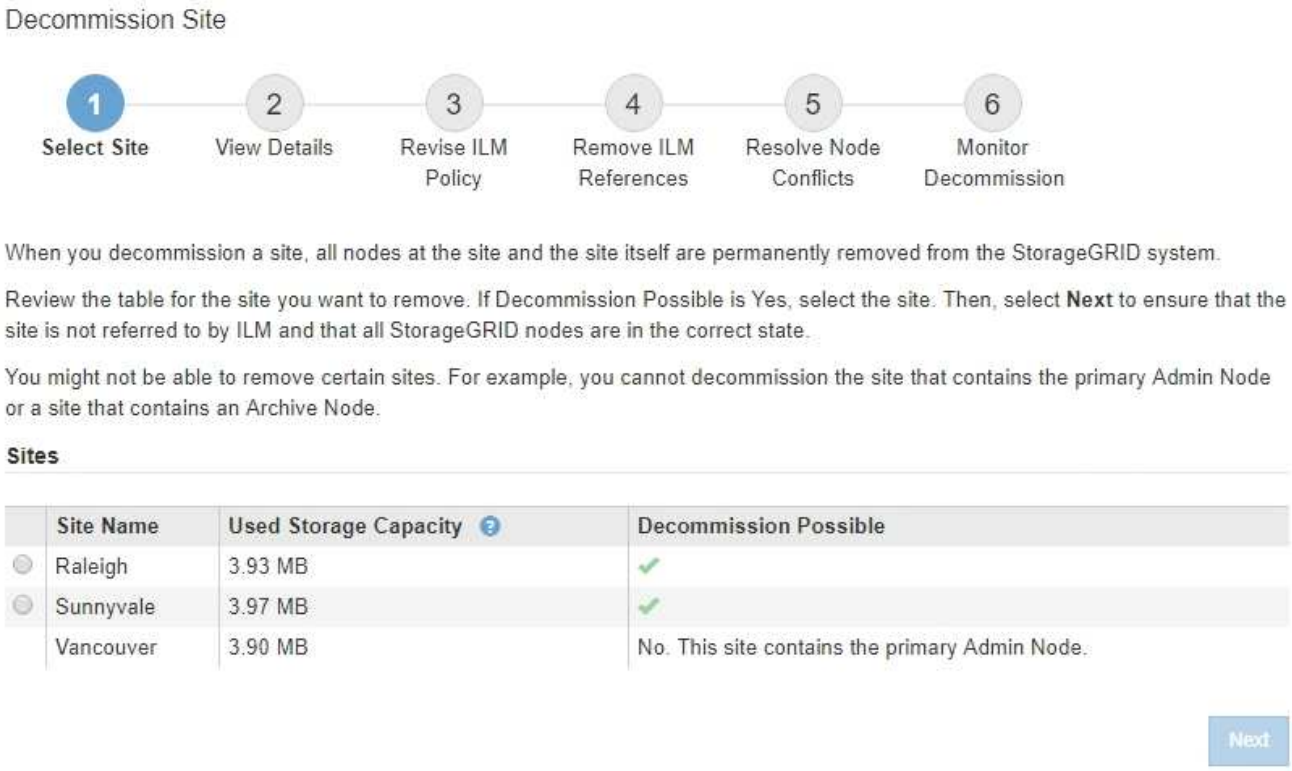
1. Wählen Sie **Wartung** > **Wartungsaufgaben** > **Dekommission**.

Die Seite Decommission wird angezeigt.



2. Klicken Sie auf die Schaltfläche **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.



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.

> Gibt es mehr als einen Grund, warum ein Standort nicht stillgelegt werden kann, wird der kritischste Grund angezeigt.

Möglichen Grund einer Deaktivierung	Beschreibung	Nächster Schritt
Grünes Häkchen (✔)	Sie können diese Website außer Betrieb nehmen.	Gehen Sie zu Im nächsten Schritt.
Nein Dieser Standort enthält den primären Admin-Knoten.	Sie können keine Site außer Betrieb nehmen, die den primären Admin-Node enthält.	Keine. Sie können dieses Verfahren nicht durchführen.
Nein Diese Site enthält mindestens einen Archiv-Knoten.	Sie können keine Site außer Betrieb setzen, die einen Archiv-Node enthält.	Keine. Sie können dieses Verfahren nicht durchführen.
Nein Alle Knoten an diesem Standort werden getrennt. Wenden Sie sich an Ihren NetApp Account-Ansprechpartner.	Sie können eine Deaktivierung einer verbundenen Site nur dann ausführen, wenn jeder Node auf der Site 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 den Standort in Vancouver jedoch nicht stilllegen, da er den primären Admin-Node 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.

Was Sie benötigen

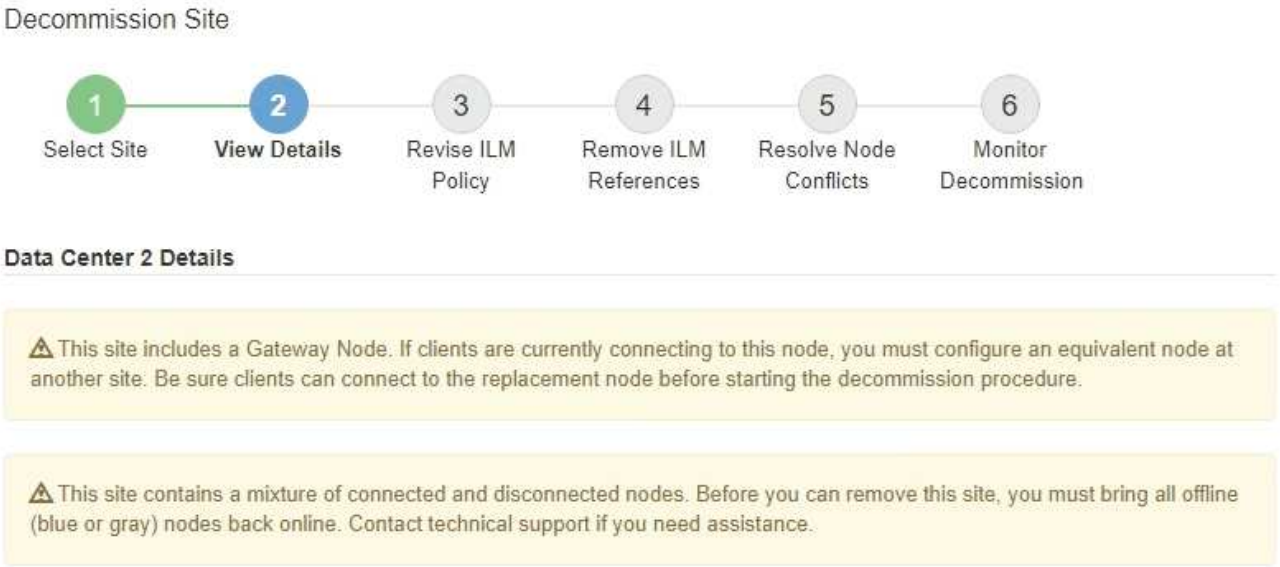
Bevor Sie einen Standort außer Betrieb nehmen, müssen Sie überprüfen, wie viele Objektdaten am Standort vorhanden sind.

- 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 getrennte Site außer Betrieb nehmen, 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.

Schritte

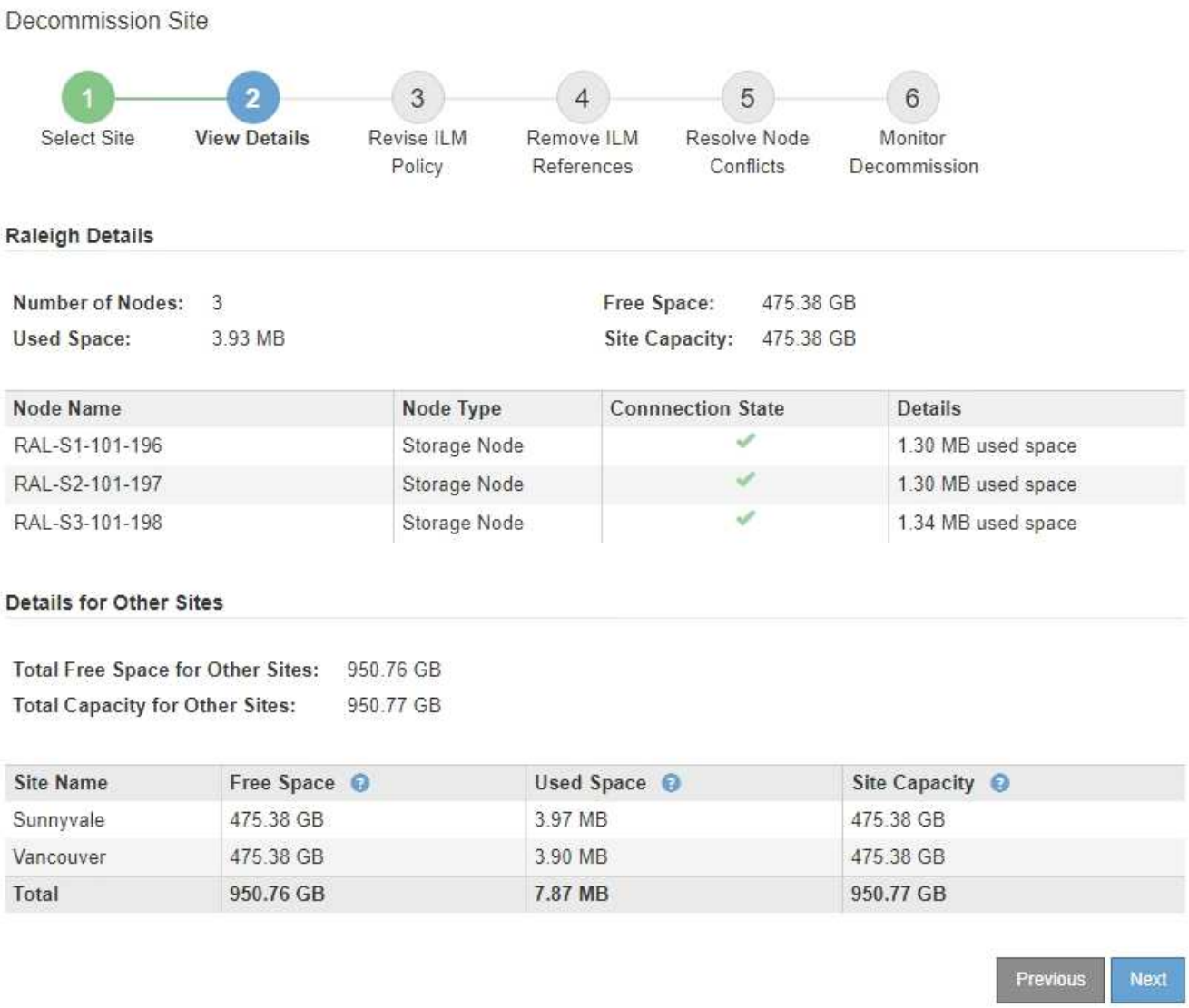
1. Überprüfen Sie ab Schritt 2 (Details anzeigen) alle Warnungen im Zusammenhang mit dem zu entfernenden Standort.



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.



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. Bevor Sie die Ausmusterung beginnen, müssen Sie HA-Gruppen bearbeiten, um alle Nodes am Standort zu entfernen. Oder Sie können die HA-Gruppe entfernen, wenn sie nur Nodes von diesem Standort enthält.

    "StorageGRID verwalten"

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.

Verwandte Informationen

"Objektmanagement mit ILM"

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.

Was Sie benötigen

Sie wissen gut, wie ILM funktioniert und kennen die Erstellung von Storage-Pools, Erasure Coding-Profilen, ILM-Regeln und die Simulation und Aktivierung einer ILM-Richtlinie bereits.

"Objektmanagement mit ILM"

Über diese Aufgabe

StorageGRID kann einen Standort nicht stilllegen, wenn auf diesen Standort durch eine ILM-Regel in der aktiven ILM-Richtlinie verwiesen 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.
- Ein Erasure-Coding-Profil, das sich auf den Standort bezieht, kann nicht verwendet werden.
- Der Standard * Alle Speicherknoten* oder der Standard **Alle Standorte**-Standort kann nicht verwendet werden.
- Kann den Bestand nicht verwenden **Regel 2 Kopien erstellen**.
- 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** aus, um zu Schritt 4 zu wechseln (ILM-Referenzen entfernen)

   "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 auf einer neuen Registerkarte „Browser“ 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-Profile zu erstellen.

   Sie müssen Speicherpools auswählen, die sich nicht auf den Standort beziehen.

   Verwenden Sie nicht den Speicherpool **All Storage Nodes** in den Erasure Coding-Profilen.

4. Wählen Sie **ILM Regeln** aus und klonen Sie jede der Regeln, die in der Tabelle für Schritt 3 aufgeführt sind (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 Erasure Coding-Profile, die auf den Standort verweisen, und ersetzen Sie sie durch neue Speicherpools oder Erasure Coding-Profile.

      Verwenden Sie den **Alle Speicherknoten** nicht in den neuen Regeln.

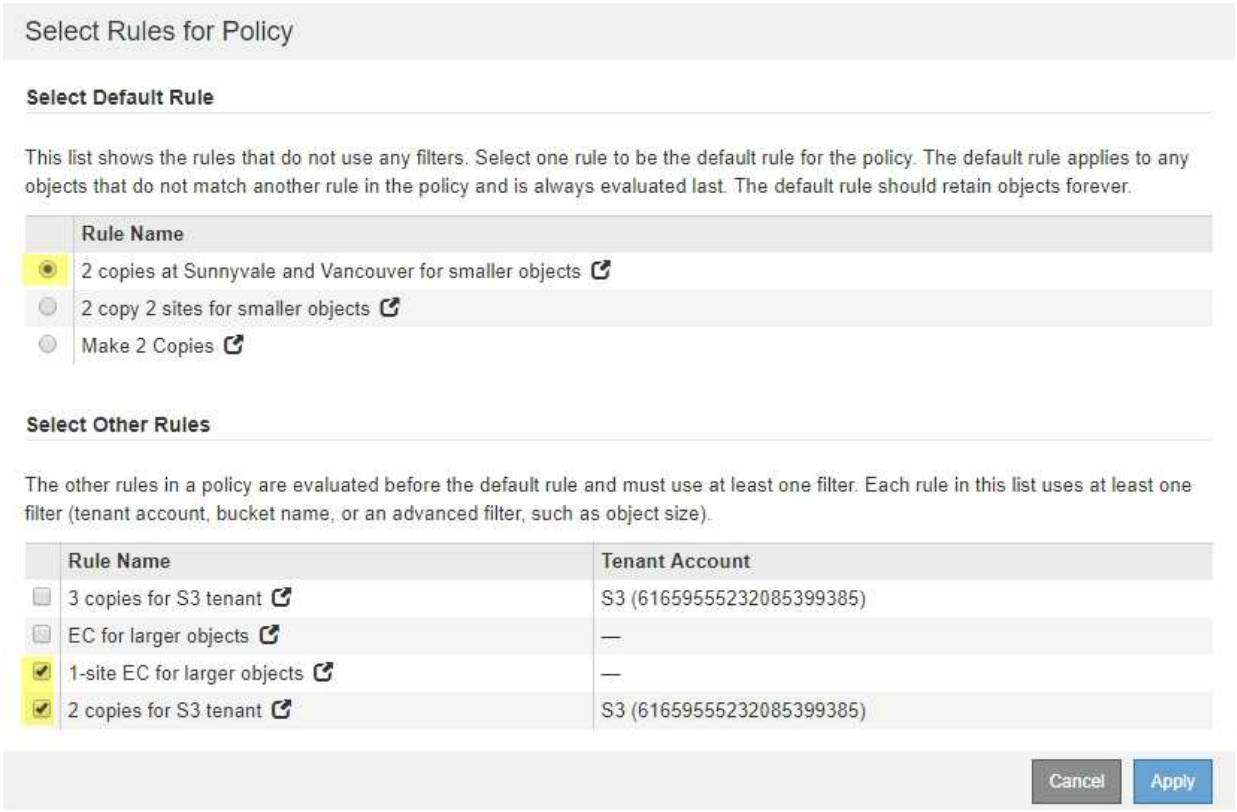
5. Wählen Sie **ILM Richtlinien** und erstellen Sie eine neue Richtlinie, die die neuen Regeln verwendet.

   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.
      - Deaktivieren Sie alle Regeln, die für Schritt 3 (ILM-Richtlinie überarbeiten) auf der Seite „Dekommission Site“ aufgeführt sind.
      - Wählen Sie eine Standardregel aus, die sich nicht auf die Site bezieht.

        Wählen Sie nicht die Regel **2 Kopien** aus, da diese Regel den **Alle Speicherknoten** -Speicherpool verwendet, der nicht erlaubt ist.

      - Wählen Sie die anderen Ersatzregeln aus, die Sie erstellt haben. Diese Regeln sollten sich nicht auf die Website
        beziehen.



d. Wählen Sie **Anwenden**.

e. Ziehen Sie die Zeilen per Drag-and-Drop, 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 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.

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).

8. 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.

Wenn Regeln aufgeführt sind, müssen Sie eine neue ILM-Richtlinie erstellen und aktivieren, bevor Sie fortfahren können.

9. 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.

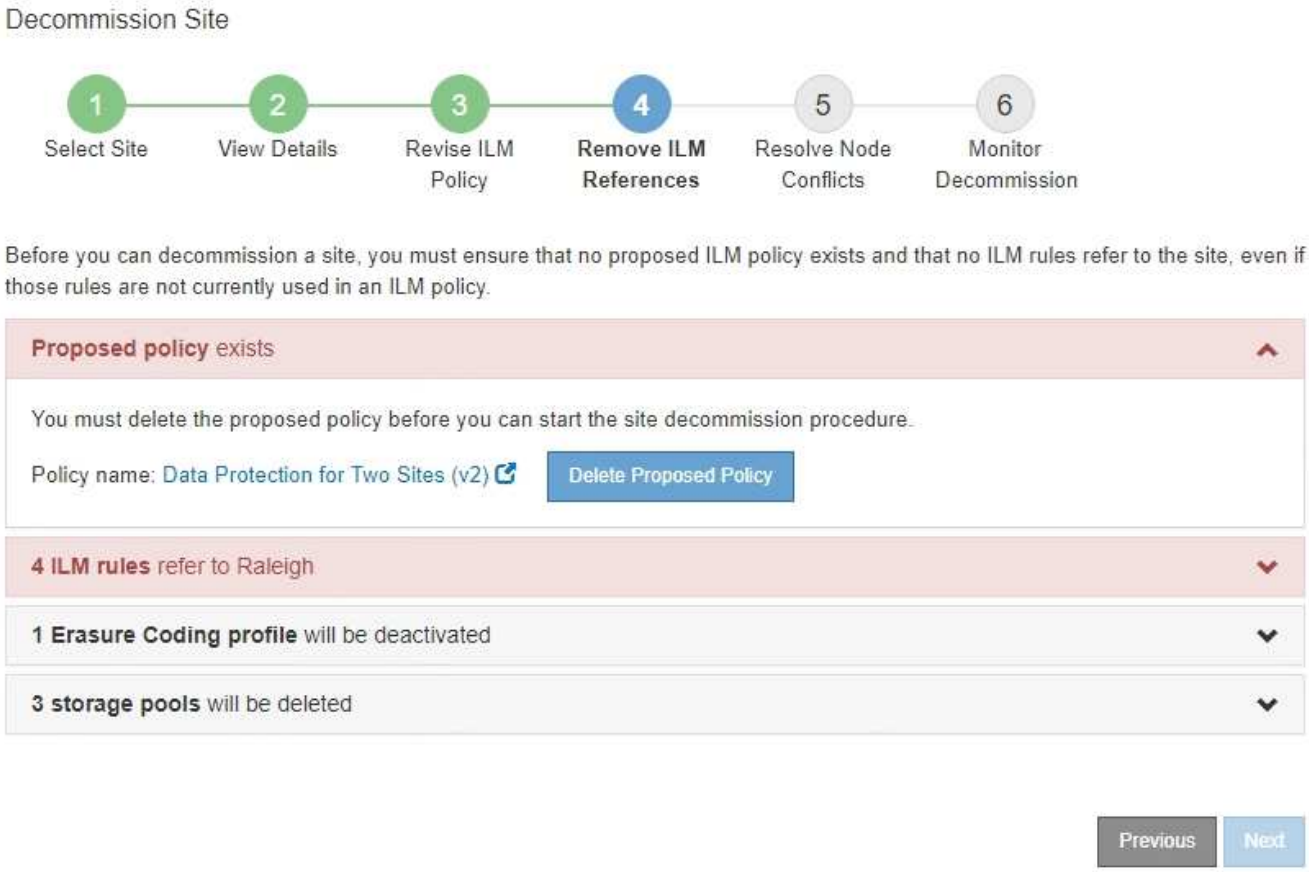
Über diese Aufgabe

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.

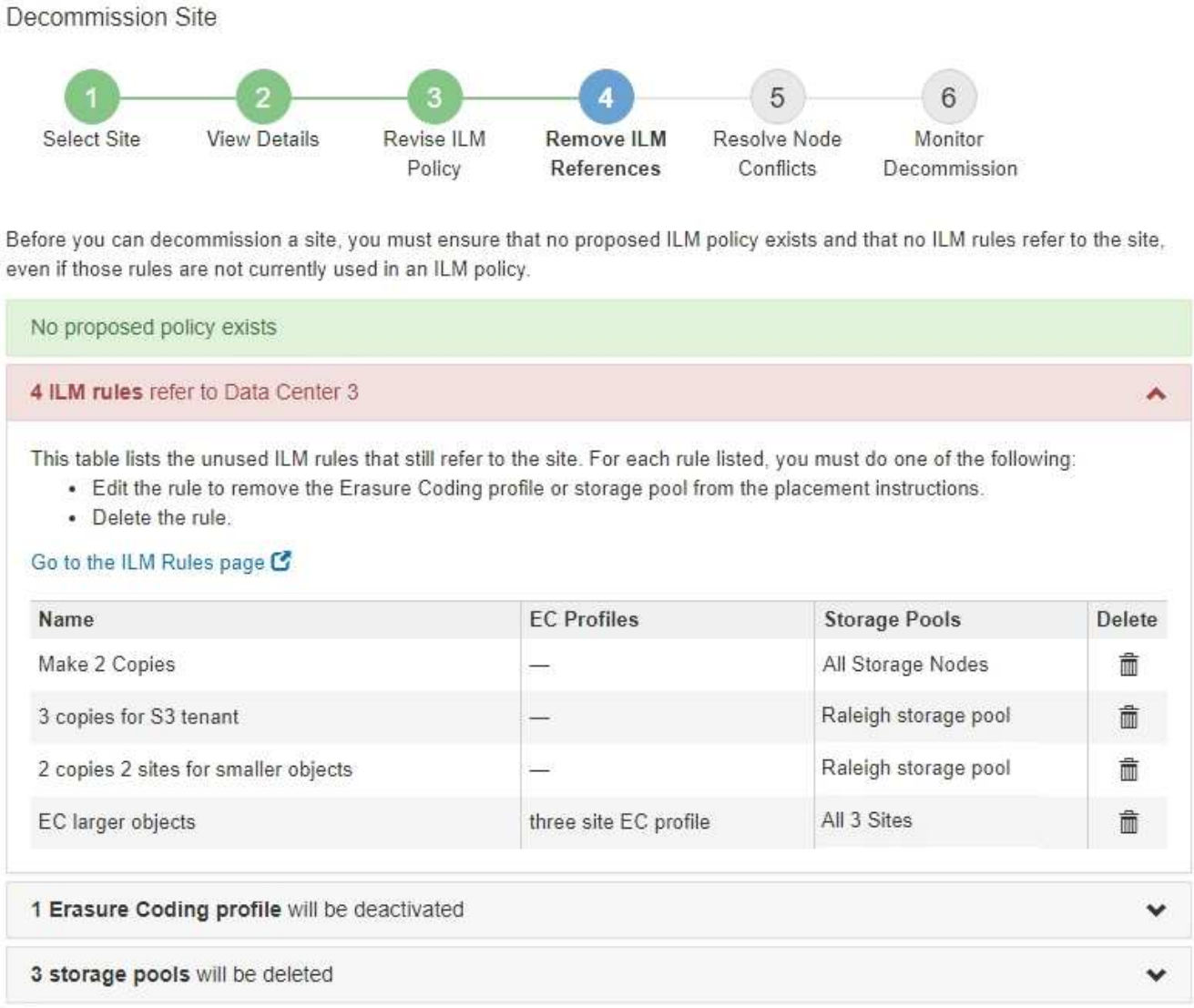
Schritte

1. Wenn eine vorgeschlagene Richtlinie aufgeführt ist, entfernen Sie sie.



a. Wählen Sie **Vorgeschlagene Richtlinie Löschen**.
b. Wählen Sie im Bestätigungsdialogfeld * OK* aus.

2. Stellen Sie fest, ob sich ungenutzte ILM-Regeln auf den Standort beziehen.



ILM-Regeln, die aufgeführt sind, beziehen sich immer noch auf die Site, werden aber in keinen Richtlinien verwendet. Im Beispiel:

- Die Stock **make 2 Kopien** Regel verwendet den Systemstandard **Alle Speicherknoten** Speicherpool, der die Seite Alle Sites 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 ungenutzten **EC-Regeln für größere Objekte** verwenden die Raleigh-Site im Profil **Alle 3 Sites** Erasure Coding.
- Wenn keine ILM-Regeln aufgeführt sind, wählen Sie **Weiter** aus, um zu **Schritt 5 (Node-Konflikte auflösen)** zu wechseln.

  "Schritt 5: Auflösen von Knotenkonflikten (und Start der Stilllegung)"

Wenn StorageGRID den Standort dekomprimiert, werden automatisch alle nicht verwendeten Erasure Coding-Profile deaktiviert, die auf den Standort verweisen. Außerdem werden alle nicht verwendeten Speicherpools, die sich auf den Standort beziehen, automatisch gelöscht. Der standardmäßige Speicherpool Alle Speicherknoten wird entfernt, da er den Standort Alle Standorte verwendet.

- Wenn eine oder mehrere ILM-Regeln aufgeführt sind, fahren Sie mit dem nächsten Schritt fort.

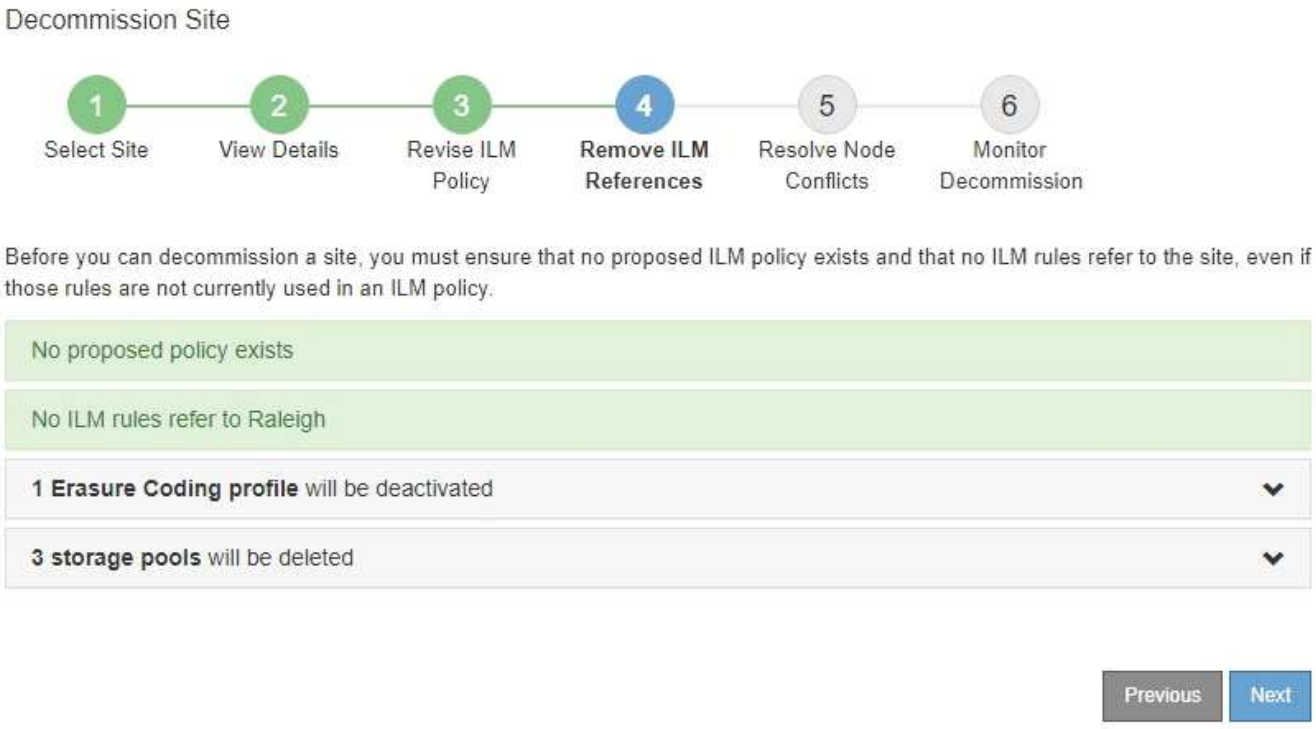
3. Bearbeiten oder Löschen jeder nicht verwendeten Regel:
   - Um eine Regel zu bearbeiten, gehen Sie auf der Seite ILM-Regeln und aktualisieren Sie alle Platzierungen, die ein Erasure Coding-Profil oder einen Speicherpool verwenden, der sich auf den Standort bezieht. Kehren Sie dann zu **Schritt 4 (ILM-Referenzen 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 für Lagerbestand **Erstellen von 2 Kopien** löschen, bevor Sie eine Website 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.



5. Wählen Sie **Weiter**.

Alle verbleibenden Speicherpools und Erasure Coding-Profile, die sich auf den Standort beziehen, werden ungültig, wenn der Standort entfernt wird. Wenn StorageGRID den Standort dekomprimiert, werden automatisch alle nicht verwendeten Erasure Coding-Profile deaktiviert, die auf den Standort verweisen. Außerdem werden alle nicht verwendeten Speicherpools, die sich auf den Standort beziehen, automatisch gelöscht. Der standardmäßige Speicherpool Alle Speicherknoten 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.

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.

- Kein Node an dem gerade entfernenden Standort kann eine Schnittstelle besitzen, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehört.

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.

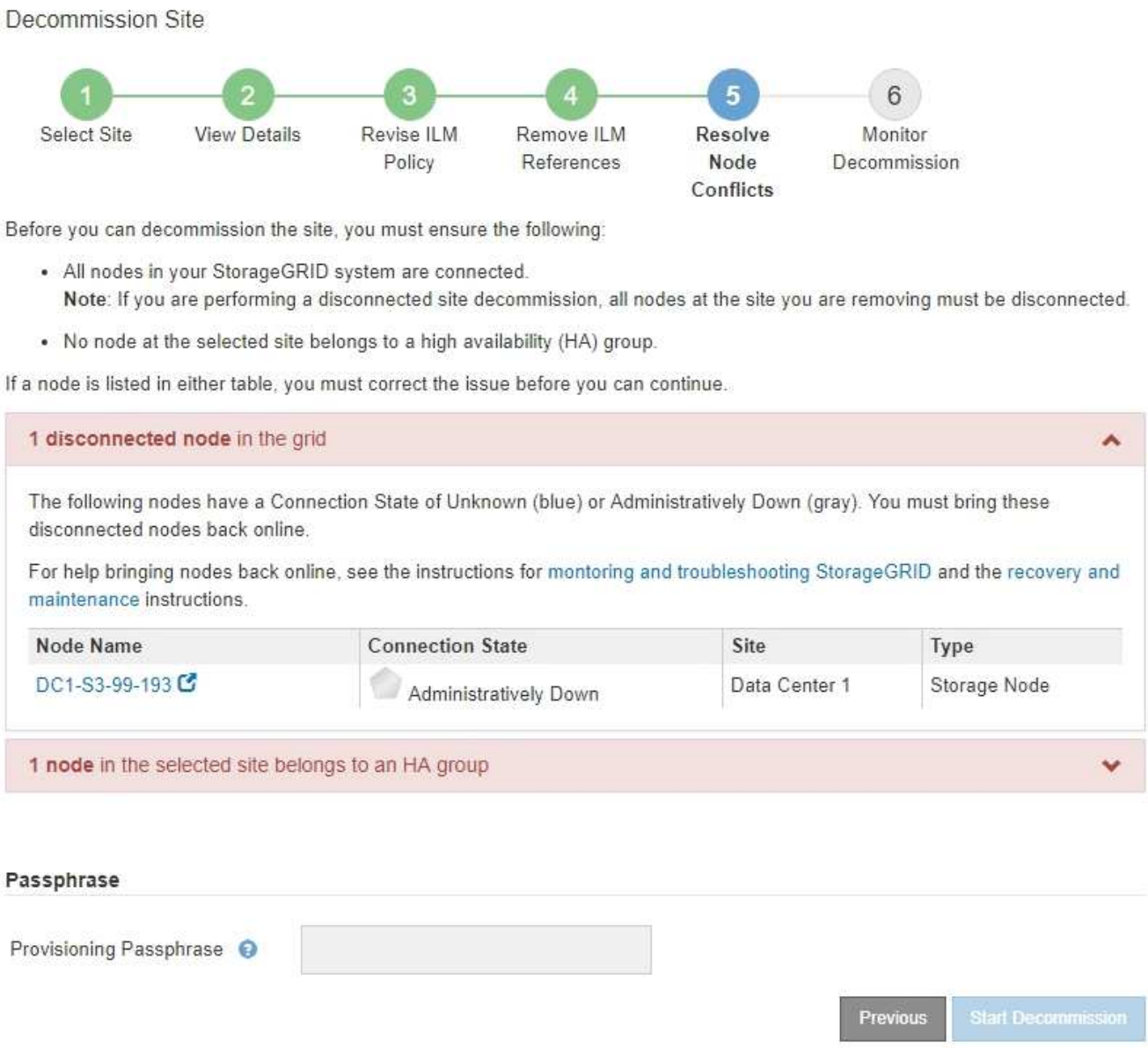
- Während die Deaktivierung der Website läuft:
  - Sie können keine ILM-Regeln erstellen, die sich auf die auszugemusterte Site beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf die Site zu verweisen.
  - Sie können keine anderen Wartungsvorgänge wie z. B. Erweiterung oder Upgrade 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 (aufweisen) Oder Administrativ Down ( ).

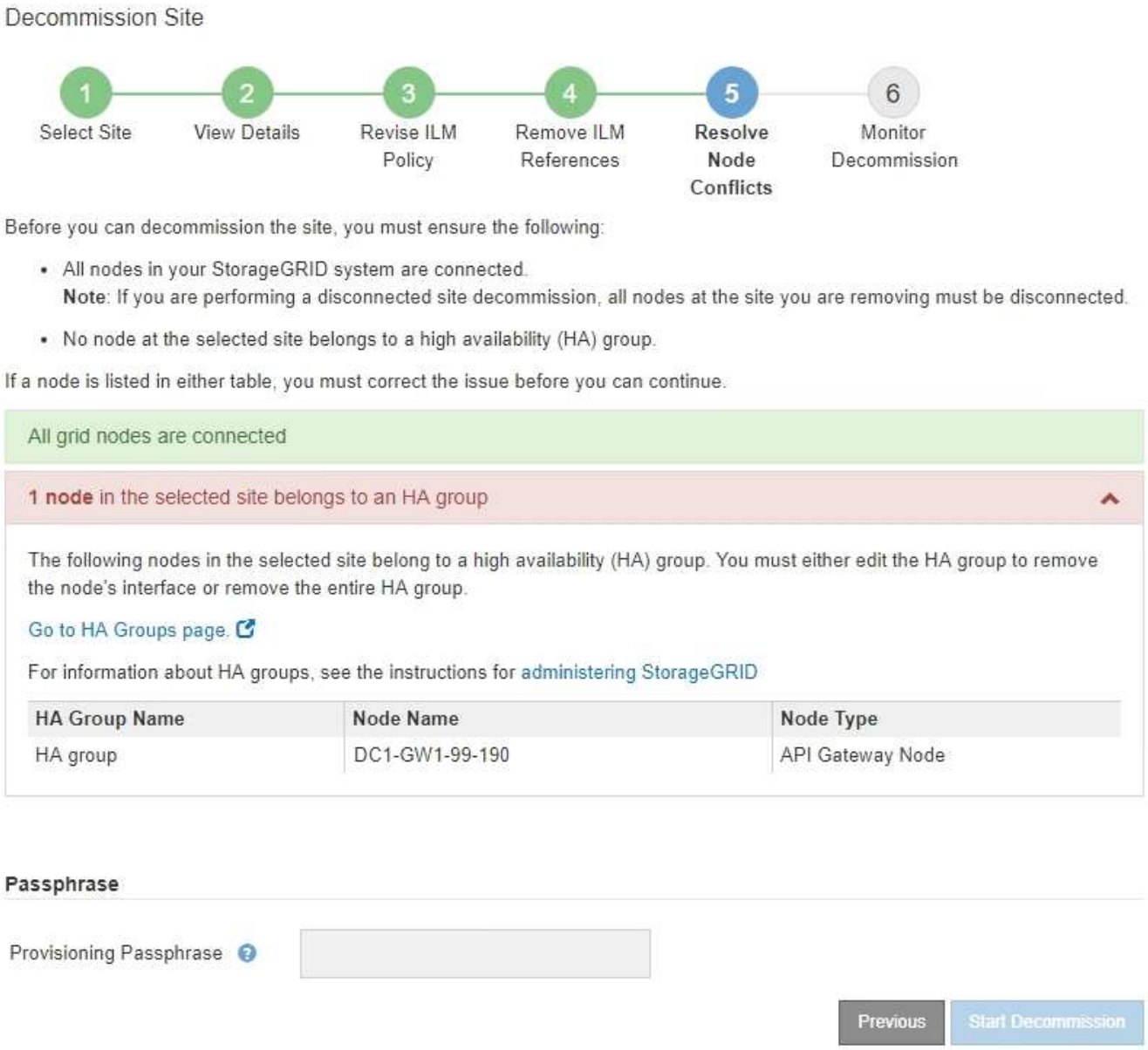


2. Wenn Knoten getrennt werden, bringen Sie sie wieder in den Online-Modus.

   Anweisungen zum Monitoring und zur Fehlerbehebung für StorageGRID und die Verfahren für den Grid-Node finden Sie in den Anweisungen. 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.



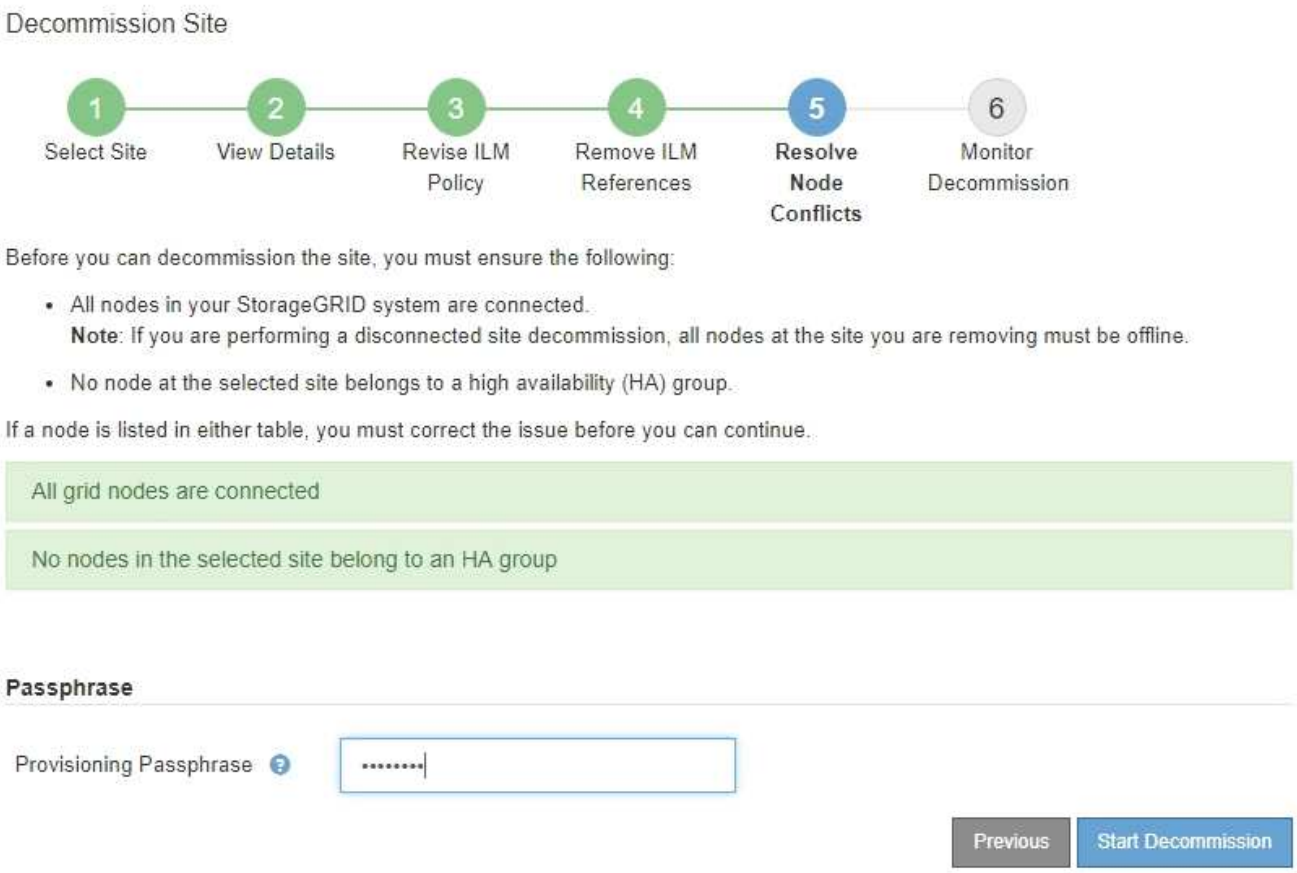
4. Wenn alle Knoten aufgelistet sind, führen Sie einen der folgenden Schritte aus:

   - 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.

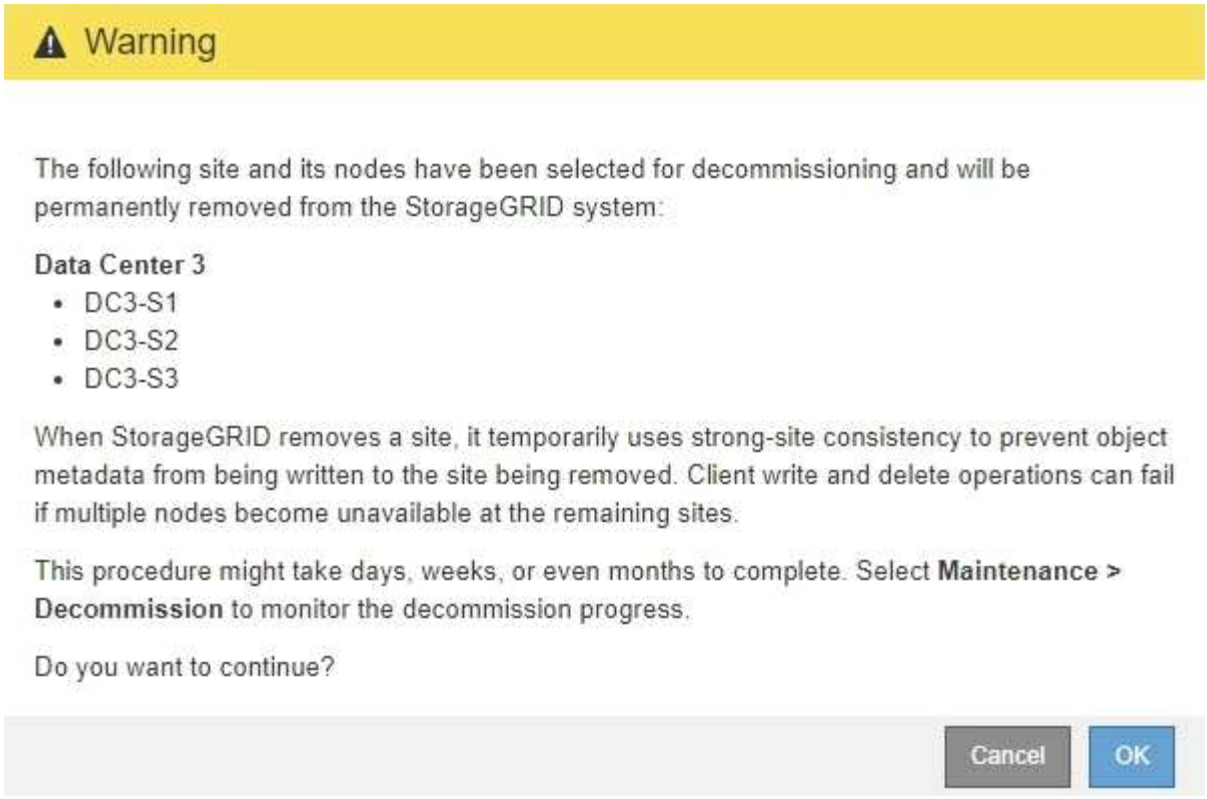
5. Geben Sie die Provisionierungs-Passphrase ein.

   Die Schaltfläche **Start Decommission** wird aktiviert.



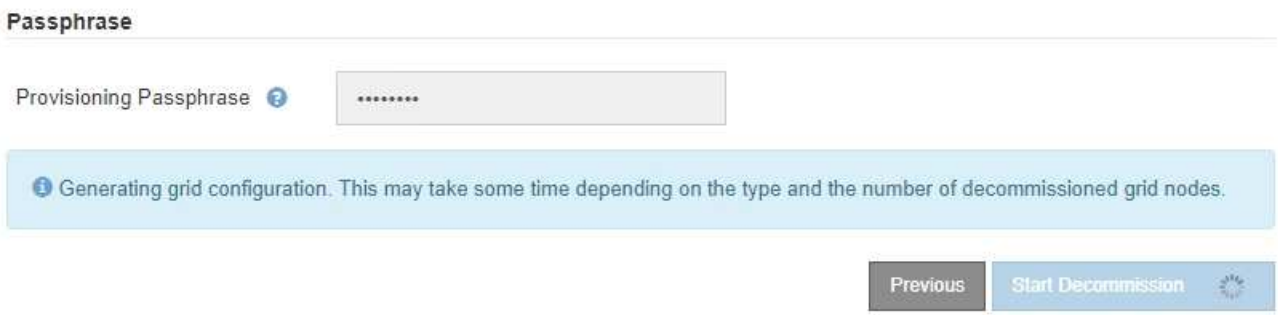
6. Wenn Sie bereit sind, den Vorgang zur Deaktivierung der Website zu starten, wählen Sie **Start Decommission**.

   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.



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.



   Wenn die neue Grid-Konfiguration generiert wurde, wird Schritt 6 (Monitor Decommission) angezeigt.

   Die Schaltfläche * Previous* bleibt deaktiviert, bis die Stilllegung abgeschlossen ist.

Verwandte Informationen

"Monitor Fehlerbehebung"

"Verfahren für den Grid-Node"

"StorageGRID verwalten"

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.

> 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**.

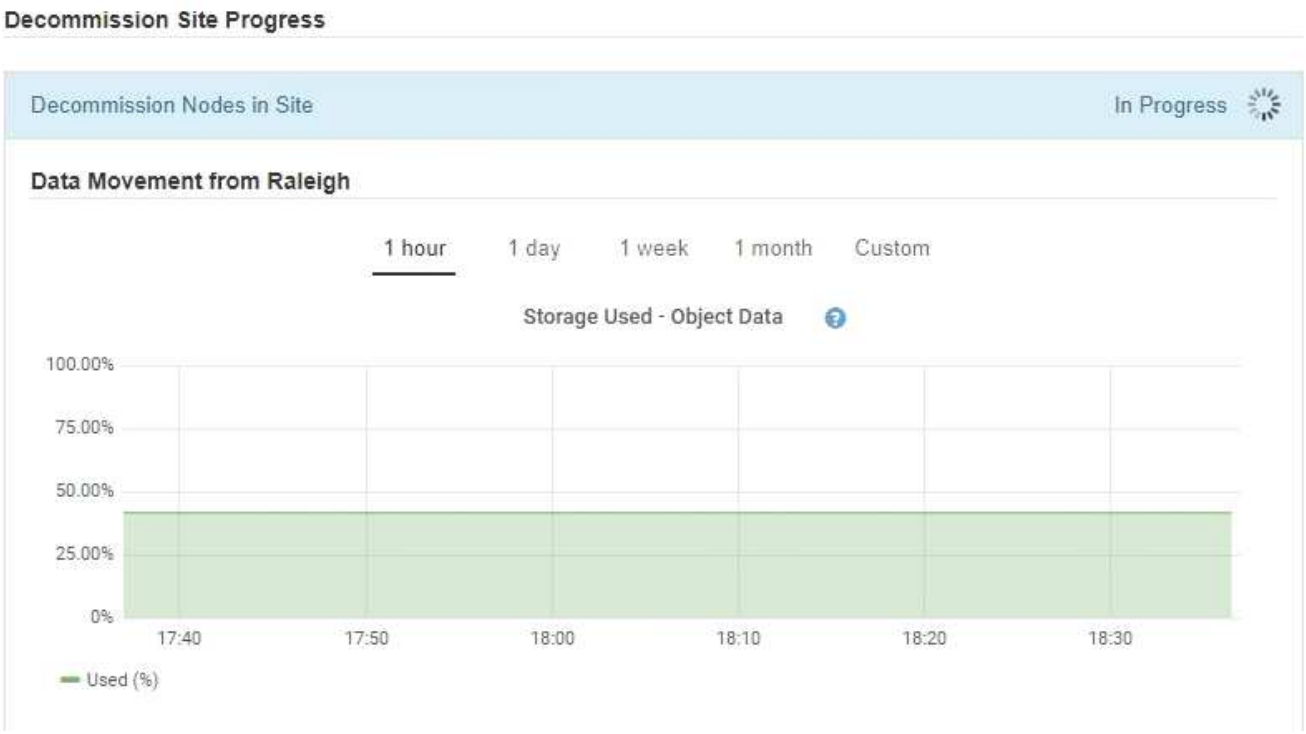
b. Laden Sie die herunter `.zip` Datei:

   Lesen Sie die Anweisungen zum 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.

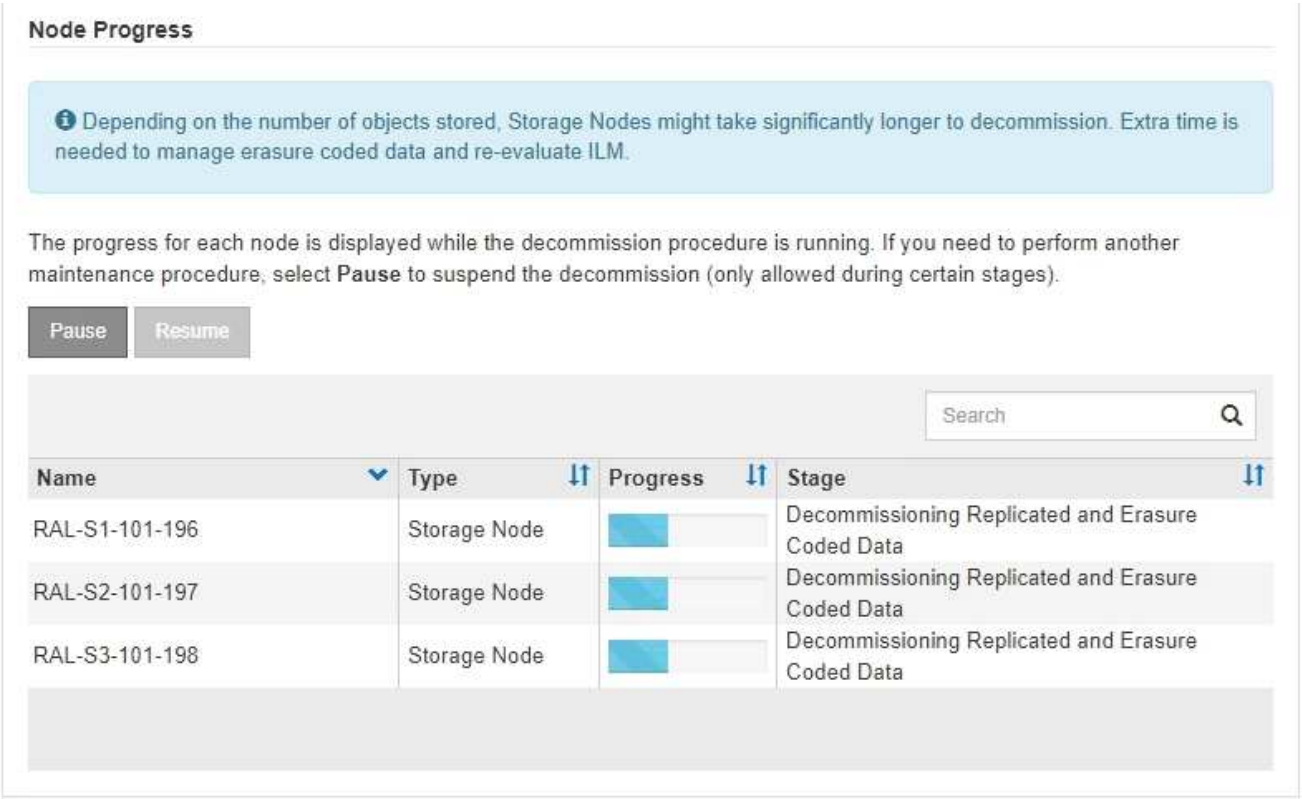
2. Überwachen Sie mithilfe des Diagramms für die Datenverschiebung das Verschieben von Objektdaten von dieser Seite zu anderen Standorten.

   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.



Wenn Sie den Fortschritt der Deaktivierung einer verbundenen Site überwachen, lesen Sie diese Tabelle, um die Phasen zur Ausmusterung eines Storage Node zu verstehen:

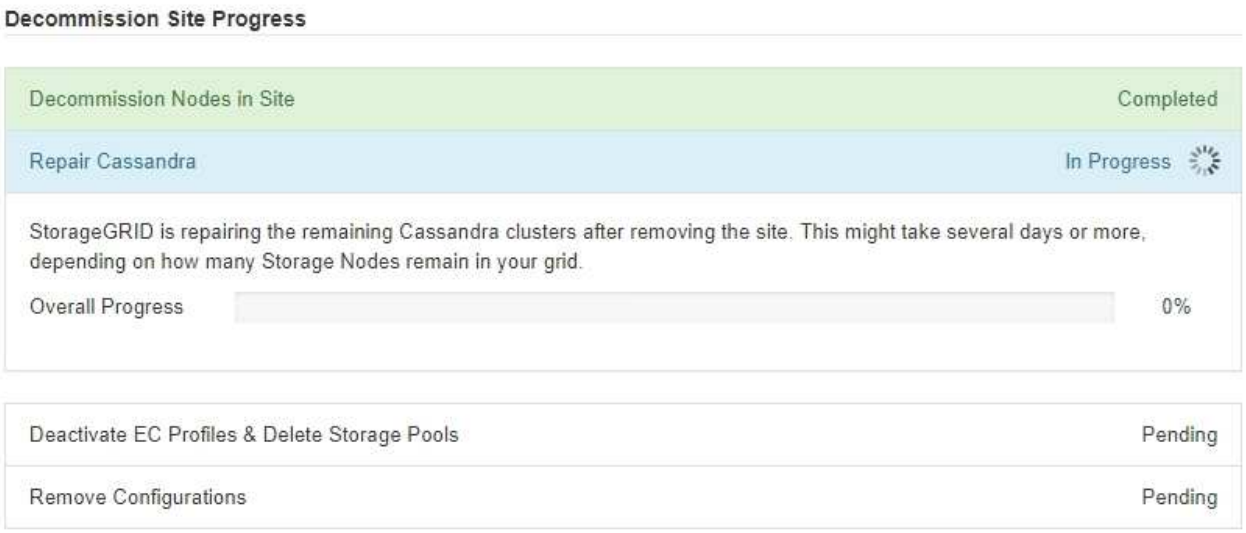
Stufe	Geschätzte Dauer
Ausstehend	Minuten oder weniger
Warten Sie auf Sperren	Minuten
Aufgabe Vorbereiten	Minuten oder weniger
Markieren von LDR deaktiviert	Minuten
Stilllegung replizierter und Erasure Coding von Daten	Stunden, Tage oder Wochen, basierend auf der Datenmenge **Hinweis**: Wenn Sie weitere 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
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.



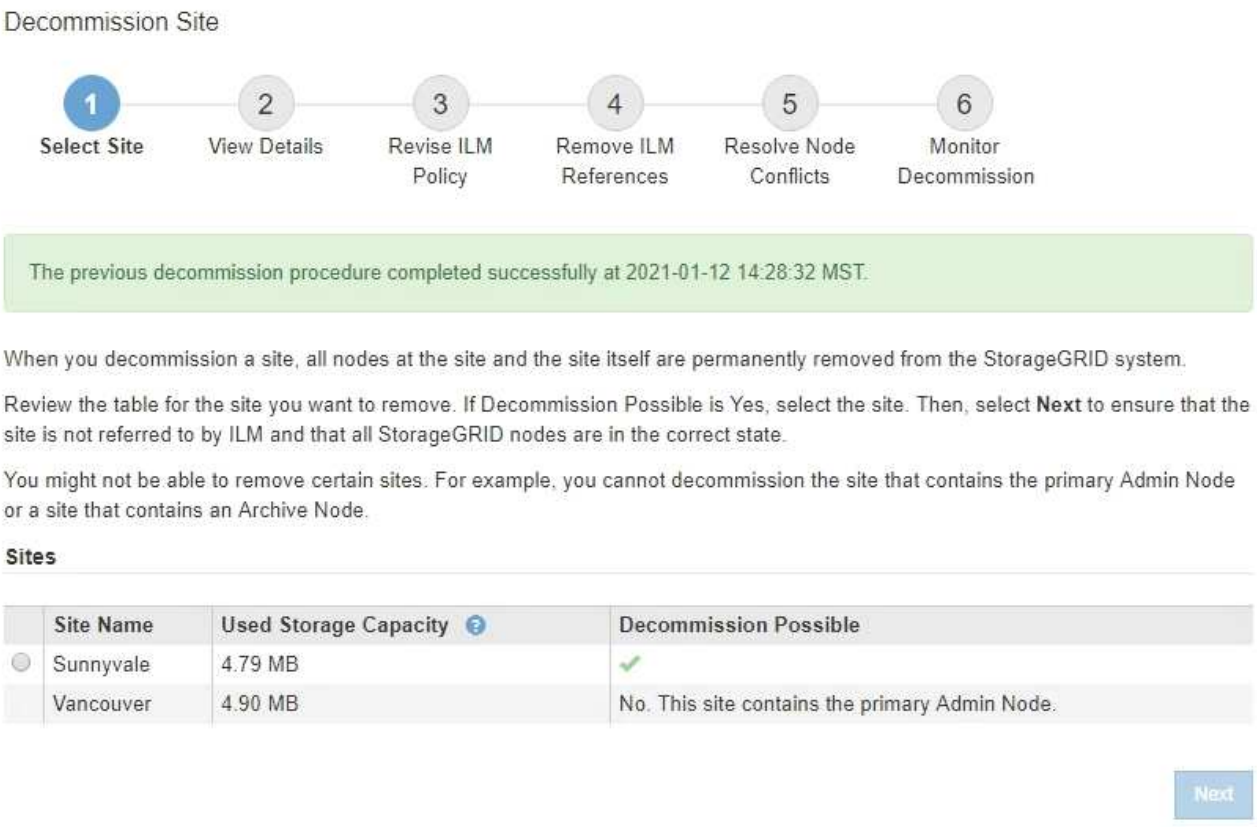
   - Während des Schritts **EC-Profile deaktivieren & Speicherpools löschen** werden folgende ILM-Änderungen vorgenommen:
     - Alle auf den Standort verwiesen Erasure Coding-Profile werden deaktiviert.

- Alle Speicherpools, die auf den Standort verwiesen werden gelöscht.

  Der systemstandardmäßige Speicherpool „Alle Speicherknoten“ 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.

5. Nach Abschluss des Stilllegen-Verfahrens wird auf der Seite Decommission Site eine Meldung angezeigt, die den entfernten Standort nicht mehr anzeigt.



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.

Verwandte Informationen

"Herunterladen des Wiederherstellungspakets"

Netzwerkwartungsverfahren

Sie können die Liste der Subnetze im Grid-Netzwerk konfigurieren oder IP-Adressen, DNS-Server oder NTP-Server für Ihr StorageGRID-System aktualisieren.

Wahlmöglichkeiten

- "Subnetze für das Grid-Netzwerk aktualisieren"
- "IP-Adressen werden konfiguriert"
- "DNS-Server werden konfiguriert"
- "Konfigurieren von NTP-Servern"
- "Wiederherstellen der Netzwerkverbindung für isolierte Knoten"

Subnetze für das Grid-Netzwerk 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.

Was Sie benötigen

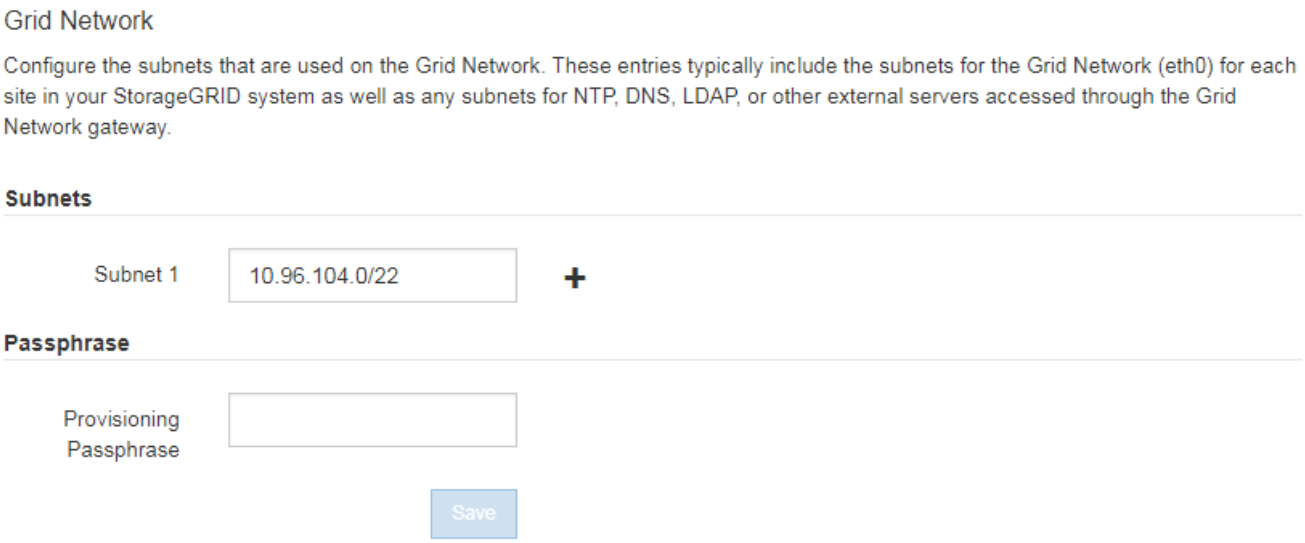
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen die Netzwerkadressen in CIDR-Notation der Subnetze haben, die Sie konfigurieren möchten.

Über diese Aufgabe

Wenn Sie eine Erweiterungsaktivität durchführen, die das Hinzufügen eines neuen Subnetzes beinhaltet, müssen Sie das neue Grid-Subnetz hinzufügen, bevor Sie den Erweiterungsvorgang starten.

Schritte

1. Wählen Sie **Wartung Netzwerk Grid-Netzwerk**.



2. Klicken Sie in der Liste Subnetze auf das Pluszeichen, 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 klicken Sie auf **Speichern**.

   Die angegebenen Subnetze werden automatisch für Ihr StorageGRID System konfiguriert.

IP-Adressen werden konfiguriert

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.

Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Raster ändern möchten, verwenden Sie das spezielle Verfahren für Grid-weite Änderungen.

"Ändern der IP-Adressen für alle Nodes im Grid"

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.

Das IP-Änderungsverfahren kann eine UnterbrechungsMaßnahme sein. Teile des Rasters sind möglicherweise erst verfügbar, wenn die neue Konfiguration angewendet wird.

- 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 wird auf der Registerkarte **SSM Ressourcen** die Grid-, Admin- und Client-Netzwerk-IP-Adresse angezeigt, die anderen Schnittstellen zusätzlich zu eth0, eth1 oder eth2 zugewiesen ist.

DHCP

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

- Die Client-Netzwerk-IP-Adresse kann nicht außerhalb des Subnetzes einer HA-Gruppe geändert werden, die in der Client-Netzwerkschnittstelle konfiguriert ist.
- Sie können die IP-Adresse des Client-Netzwerks nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die von einer HA-Gruppe zugewiesen wurde, die in der Client-Netzwerkschnittstelle konfiguriert ist.
- Die Grid-Netzwerk-IP-Adresse kann nicht außerhalb des Subnetzes einer auf der Grid-Netzwerkschnittstelle konfigurierten HA-Gruppe geändert werden.
- Sie können die IP-Adresse des Grid-Netzwerks nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die von einer HA-Gruppe zugewiesen wurde, die auf der Grid-Netzwerkschnittstelle konfiguriert ist.

Wahlmöglichkeiten

- "Ändern der Netzwerkkonfiguration eines Node"
- "Hinzufügen oder Ändern von Subnetzlisten im Admin-Netzwerk"
- "Hinzufügen oder Ändern von Subnetzlisten im Grid-Netzwerk"
- "Linux: Hinzufügen von Schnittstellen zu einem vorhandenen Node"
- "Ändern der IP-Adressen für alle Nodes im Grid"

Ändern der Netzwerkkonfiguration eines Knotens

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.

Was Sie benötigen

Sie müssen die haben `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.

Appliances: bei StorageGRID-Geräten, wenn das Client- oder Admin-Netzwerk während der Erstinstallation nicht im StorageGRID Appliance Installer konfiguriert wurde, kann das Netzwerk nicht mit dem Change IP-Tool hinzugefügt werden. Zunächst müssen Sie das Gerät in den Wartungsmodus versetzen, die Links konfigurieren, das Gerät in den normalen Betriebsmodus zurückversetzen und die Netzwerkkonfiguration mithilfe des Tools IP ändern ändern. Informationen zum Konfigurieren von Netzwerkverbindungen finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

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.

IP-Adressenschwalben sind 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 Domänennamens, 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. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

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.

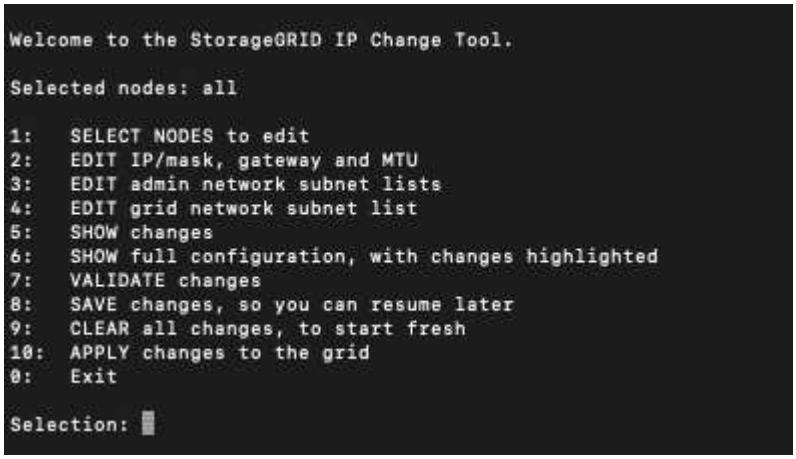
Schritte

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.



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 durchgestrickter 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.

- **Abbrechen**: Nehmen Sie 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 zu einem Admin-Netzwerk oder Client-Netzwerk hinzufügen, stellen Sie sicher, dass Sie die Schnittstelle wie unter „`Hinzufügen von Schnittstellen zu einem vorhandenen Knoten`“ hinzugefügt haben.

    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

"Linux: Hinzufügen von Schnittstellen zu einem vorhandenen Node"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"StorageGRID verwalten"

"IP-Adressen werden konfiguriert"

Hinzufügen oder Ändern von Subnetzlisten im Admin-Netzwerk

Sie können die Subnetze in der Subnetz-Liste Admin-Netzwerk eines oder mehrerer Nodes hinzufügen, löschen oder ändern.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei:

Sie können Subnetze zu allen Nodes in der Subnetz-Liste des Admin-Netzwerks hinzufügen, löschen oder ändern.

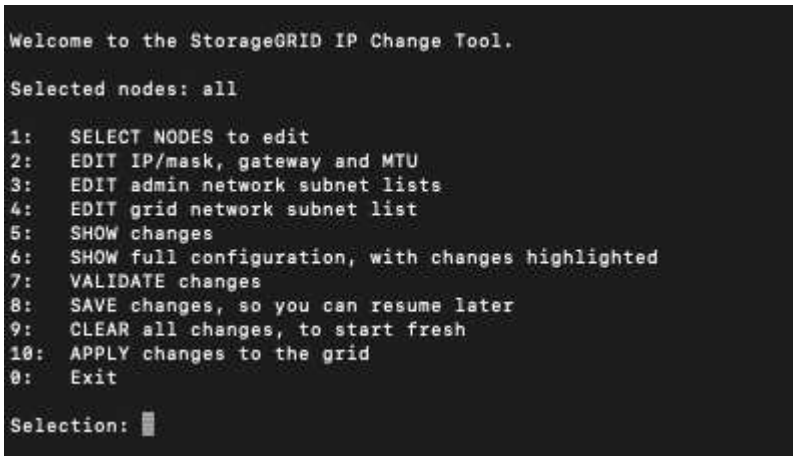
Schritte

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.



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, müssen Sie **Enter** (ohne **q**) drücken, 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 durchgestrickter 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 are not
     persistent. Host routes (/32 subnets) are applied automatically if
     the IP addresses provided for external services such as NTP or DNS
     are not 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 do not 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 Host-Route nicht löschen, wird sie beibehalten, nachdem Sie Änderungen an der Subnetz-Liste vorgenommen haben.

     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 Stufendschicht 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.

Verwandte Informationen

"IP-Adressen werden konfiguriert"

Hinzufügen oder Ändern von Subnetzlisten im Grid-Netzwerk

Mithilfe des Tools IP ändern können Sie Subnetze im Grid Network hinzufügen oder ändern.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Sie können Subnetze in der Netznetznetznetznetznetznetzsubnetliste 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 durchgestrickter 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 Stufendschicht 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, müssen Sie den Knoten nach der Staging so schnell wie möglich neu starten, um Störungen zu minimieren.

- **Abbrechen**: Nehmen Sie 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 den IP-Änderungsvorgang abzubrechen und zum Hauptmenü zurückzukehren, geben Sie **A** ein.
    - Um den fehlgeschlagenen Vorgang erneut zu versuchen, geben Sie **r** ein.
    - Um mit der nächsten Operation fortzufahren, geben Sie **c** ein.

      Der fehlgeschlagene Vorgang kann später 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.
    a. Wählen Sie **Wartung** > **System** > **Wiederherstellungspaket**.
    b. 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.

Verwandte Informationen

"IP-Adressen werden konfiguriert"

Linux: Hinzufügen von Schnittstellen zu einem vorhandenen Node

Wenn Sie eine Schnittstelle zu einem Linux-basierten Node hinzufügen möchten, den Sie anfangs nicht installiert haben, müssen Sie diese Vorgehensweise anwenden.

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 StorageGRID-Installationsanweisungen 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. Informationen zum Ändern der Netzwerkkonfiguration eines Node finden Sie unter.

"Ändern der Netzwerkkonfiguration eines Node"

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Node gehostet wird, der die neue Netzwerkzuweisung benötigt.
2. Bearbeiten Sie die Konfigurationsdatei des Knotens unter `/etc/storagegrid/nodes/node-name.conf`.

   Geben Sie keine anderen Netzwerkparameter an, oder ein Validierungsfehler führt zu einem Ergebnis.

   a. Fügen Sie das neue Netzwerkziel hinzu.

   ```
   CLIENT_NETWORK_TARGET = bond0.3206
   ```

   b. Optional: Fügen Sie eine MAC-Adresse hinzu.

   ```
   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`

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"Ändern der Netzwerkkonfiguration eines Node"

Ändern der 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 eine Grid-Netzwerk-IP-Änderung nicht unter Verwendung des Verfahrens zum Ändern einzelner Knoten vornehmen.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Um sicherzustellen, dass das Raster erfolgreich gestartet wird, müssen Sie alle Änderungen gleichzeitig vornehmen.

Dieses Verfahren gilt nur für das Grid-Netzwerk. Mit diesem Verfahren können Sie keine IP-Adressen in Admin- oder Client-Netzwerken ändern.

Wenn Sie die IP-Adressen und die MTU nur für die Nodes an einem Standort ändern möchten, befolgen Sie die Anweisungen zum Ändern der Netzwerkkonfiguration eines Node.

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 Domänennamen, 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. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

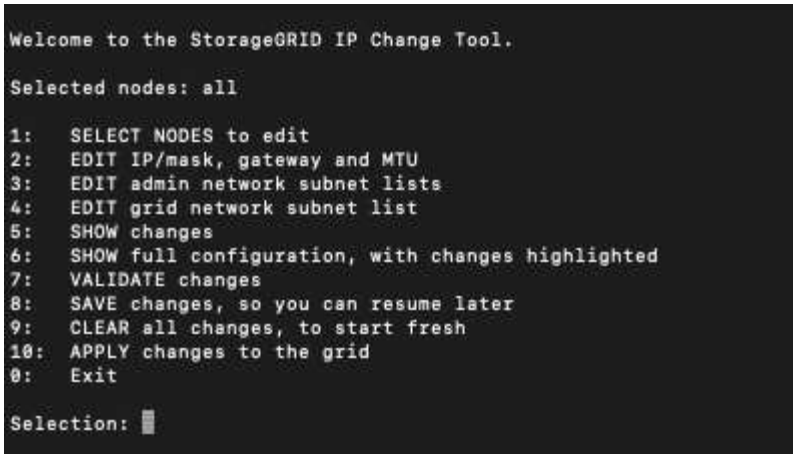
   Fügen Sie bei Bedarf das neue Subnetz für die neuen IP-Adressen hinzu.

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`.



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 durchgestrickter 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** statt **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

"StorageGRID verwalten"

"Ändern der Netzwerkkonfiguration eines Node"

"Hinzufügen oder Ändern von Subnetzlisten im Grid-Netzwerk"

"Herunterfahren eines Grid-Node"

DNS-Server werden konfiguriert

Sie können DNS-Server (Domain Name System) hinzufügen, entfernen und aktualisieren, sodass Sie vollständig qualifizierte Domain Name (FQDN) Hostnamen anstelle von IP-Adressen verwenden können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen die IP-Adressen der DNS-Server konfigurieren.

Über diese Aufgabe

Wenn Sie DNS-Serverinformationen angeben, können Sie vollständig qualifizierte Domänennamen (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail- oder SNMP-Benachrichtigungen und AutoSupport verwenden. Es wird empfohlen, mindestens zwei DNS-Server anzugeben.

> Geben Sie zwei bis sechs IP-Adressen für DNS-Server ein. Im Allgemeinen wählen Sie DNS-Server aus, auf die jeder Standort im Falle einer NetzwerkisLanding lokal zugreifen kann. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen.

"Ändern der DNS-Konfiguration für einen einzelnen Grid-Node"

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. Wählen Sie **Wartung Netzwerk DNS Server**.
2. Fügen Sie im Abschnitt „Server“ nach Bedarf Aktualisierungen hinzu oder entfernen Sie DNS-Servereinträge.

   Als Best Practice empfehlen wir, mindestens zwei DNS-Server pro Standort anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Klicken Sie Auf **Speichern**.

Ändern der DNS-Konfiguration für einen einzelnen Grid-Node

Anstatt das Domain Name System (DNS) global für die gesamte Bereitstellung zu konfigurieren, können Sie ein Skript ausführen, um DNS für jeden Grid-Knoten unterschiedlich zu konfigurieren.

Im Allgemeinen sollten Sie die Option **Wartung Netzwerk DNS Server** 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.

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`

Konfigurieren von NTP-Servern

Sie können NTP-Server (Network Time Protocol) hinzufügen, aktualisieren oder entfernen, um sicherzustellen, dass die Daten zwischen den Grid-Nodes in Ihrem StorageGRID-System korrekt synchronisiert werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen die IPv4-Adressen der NTP-Server konfigurieren.

Über diese Aufgabe

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, denen Sie zuvor primäre NTP-Rollen zugewiesen haben. Aus diesem Grund wird die Angabe von mindestens zwei Nodes mit primären NTP-Rollen empfohlen.

> 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.

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 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"

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.

Schritte

1. Wählen Sie **Wartung Netzwerk NTP Server**.
2. Fügen Sie im Abschnitt „Server“ bei Bedarf Update hinzu oder entfernen Sie NTP-Servereinträge.

   Sie sollten mindestens 4 NTP-Server enthalten, und Sie können bis zu 6 Server angeben.

3. Geben Sie im Textfeld **Provisioning Passphrase** die Provisioning-Passphrase für Ihr StorageGRID-System ein und klicken Sie auf **Speichern**.

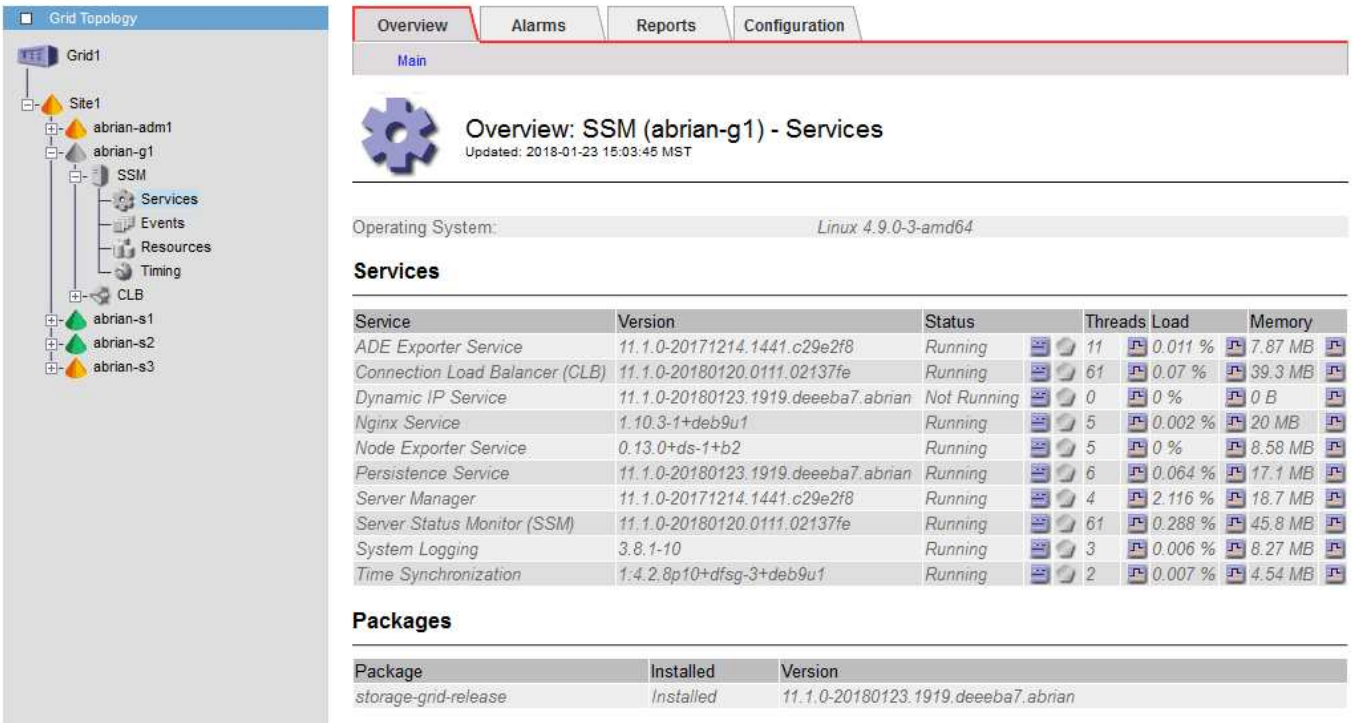
   Der Status des Verfahrens wird oben auf der Seite angezeigt. Die Seite wird deaktiviert, bis die Konfigurationsaktualisierungen abgeschlossen sind.

   Wenn alle NTP-Server den Verbindungstest nicht ausführen, nachdem Sie die neuen NTP-Server gespeichert haben, fahren Sie nicht fort. Wenden Sie sich an den technischen Support.

Wiederherstellen der Netzwerkverbindung für isolierte Knoten

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.

Wenn ein Knoten grau ist, oder wenn ein Knoten blau ist und viele seiner Dienste einen anderen Status als laufen zeigen, sollten Sie im Grid Manager (**Support** > **Tools** > **Grid Topology**) auf Knotenisolierung prüfen.



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 die im Dashboard für den Mandanten-Manager angezeigten Werte für Storage-Auslastung und Kontingente möglicherweise 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 Domain Name System (mDNS) in den Netzwerken deaktiviert ist, muss möglicherweise auf jedem isolierten Knoten das Befehlszeilendienstprogramm 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 may 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 dynamischen 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

Einige Wartungsverfahren sind für Linux oder VMware Implementierungen von StorageGRID oder speziell für andere Komponenten der StorageGRID Lösung entwickelt.

Linux: Migration eines Grid-Node zu einem neuen Host

Sie können StorageGRID Nodes von einem Linux-Host auf einen anderen migrieren, um Host-Wartungsarbeiten (wie BS-Patches und Neustart) durchzuführen, ohne die Funktionalität oder Verfügbarkeit Ihres Grid zu beeinträchtigen.

Sie migrieren einen oder mehrere Knoten von einem Linux-Host (der „`source Host`“) zu einem anderen Linux-Host (der „`target-Host`“). Der Zielhost muss bereits für die Verwendung mit StorageGRID vorbereitet sein.

Sie können diese Prozedur nur verwenden, wenn Sie die StorageGRID-Bereitstellung mit Migrationssupport geplant haben.

Um einen Grid-Node auf einen neuen Host zu migrieren, müssen beide der folgenden Bedingungen erfüllt sein:

- Shared Storage wird für alle Storage Volumes pro Node verwendet
- Netzwerkschnittstellen haben zwischen Hosts einheitliche Namen

Führen Sie in einer Produktionsimplementierung nicht mehr als einen Speicherknoten 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 haben (z. B. zwei Gateway-Nodes), installieren Sie nicht alle Instanzen auf demselben Host.

Weitere Informationen finden Sie unter „`Node Migration Requirements`“ in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

Verwandte Informationen

"Bereitstellen neuer Linux-Hosts"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Linux: Exportieren des Knotens vom Quell-Host

Fahren Sie den Grid-Node herunter, und exportieren Sie ihn vom Linux-Quell-Host.

Führen Sie den folgenden Befehl auf dem Linux-Quell-Host aus.

1. Abrufen des Status aller derzeit auf dem Quell-Host ausgeführten Nodes

```
sudo storagegrid node status all
```

```
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 dessen Ausführungszustand lautet `Running`.

```
sudo storagegrid node stop DC1-S3
```

```
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
```

```
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. Beachten Sie die `import command suggested in the output of the `export` Befehl.

   Im nächsten Schritt führen Sie diesen Befehl auf dem Zielhost aus.

Linux: Importieren des Knotens auf dem Zielhost

Nachdem Sie den Knoten vom Quell-Host exportiert haben, importieren und validieren Sie den Knoten auf dem Ziel-Linux-Host. Die Validierung bestätigt, dass der Knoten

Zugriff auf denselben Block-Speicher und Netzwerkschnittstellengeräte hat, wie er auf dem Quell-Host hatte.

Führen Sie den folgenden Befehl auf dem Ziel-Linux-Host aus.

1. Importieren Sie den Knoten auf dem Zielhost.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

```
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
```

```
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.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Linux: Der migrierte Knoten wird gestartet

Nachdem Sie den migrierten Node validiert haben, starten Sie den Node durch Ausführen eines Befehls auf dem Linux-Zielhost.

Schritte

1. Starten Sie den Knoten auf dem neuen Host.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. Überprüfen Sie im Grid Manager, ob der Status des Knotens grün ist und keine Alarme dagegen ausgelöst werden.

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.

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 Knoten einen Run-State von hat `Running`.

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 Archivierungs-Knotens 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 der 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.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie **Archivknoten ARC Ziel Konfiguration Main**.
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 dsmadmc-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 `dsmadmc` 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 dsmadmc 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 dsmadmc 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 Grid Topology**. Wählen Sie dann **Archiv-Knoten ARC Abrufen 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 so konfiguriert ist, dass eine ILM-Regel verwendet wird, die eine einzelne Objektkopie erstellt und die 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.

Was Sie benötigen

- 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

Dieses Beispiel dient nur zu Ihren Informationen. Dieses Verfahren kann Ihnen nicht dabei helfen, alle Ausfallbedingungen zu identifizieren, die zu nicht verfügbaren Objekten oder Bandvolumes 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 Archiv-Node abgerufen werden kann, zeigt die ARCE-Überwachungsmeldung (Archivobjekt Retrieve End) IM Ergebnisfeld ARUN (nicht verfügbare Archiv-Middleware) oder GERR (allgemeiner Fehler) an. 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][A
   MID(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 **Archiv-Node 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** aus. Wählen Sie dann **Archiv-Node 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 nicht bereits beim Archiv-Node 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 die ILM-Regel für das Objekt angegeben hat, dass nur eine Kopie erstellt wurde und nun 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 Abruf Konfiguration**, und wählen Sie **Fehleranzahl der Anforderung zurücksetzen**.

b. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

"StorageGRID verwalten"

"Prüfung von Audit-Protokollen"

VMware: Konfiguration einer virtuellen Maschine für automatischen Neustart

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

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`

Wahlmöglichkeiten

- "Anzeigen von Status und Version von Server Manager"
- "Anzeigen des aktuellen Status aller Dienste"
- "Starten von Server Manager und allen Diensten"
- "Neustart von Server Manager und allen Diensten"
- "Beenden von Server Manager und allen Diensten"
- "Anzeigen des aktuellen Status eines Dienstes"

- "Anhalten eines Dienstes"
- "Versetzen einer Appliance in den Wartungsmodus"
- "Beendigung eines Dienstes erzwingen"
- "Starten oder Neustarten eines Dienstes"
- "Entfernen von Port-Remaps"
- "Entfernen von Port-Remaps auf Bare-Metal-Hosts"
- "Neubooten eines Grid-Node"
- "Herunterfahren eines Grid-Node"
- "Herunterfahren eines Hosts"
- "Ausschalten und Einschalten aller Knoten im Grid"
- "Verwenden einer DoNotStart-Datei"
- "Fehlerbehebung Für Server Manager"

Anzeigen von Status und Version von Server Manager

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.

Was Sie benötigen

Sie müssen die haben `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
   ```

   Dieser Status ist das Äquivalent zum Status, der in der Kopfzeile der lokalen Konsolenanzeige angezeigt wird.

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 Befehlsshell ab: **`exit`**

Anzeigen des aktuellen Status aller Dienste

Sie können jederzeit den aktuellen Status aller auf einem Grid-Node ausgeführten Services anzeigen.

Was Sie benötigen

Sie müssen die haben `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:

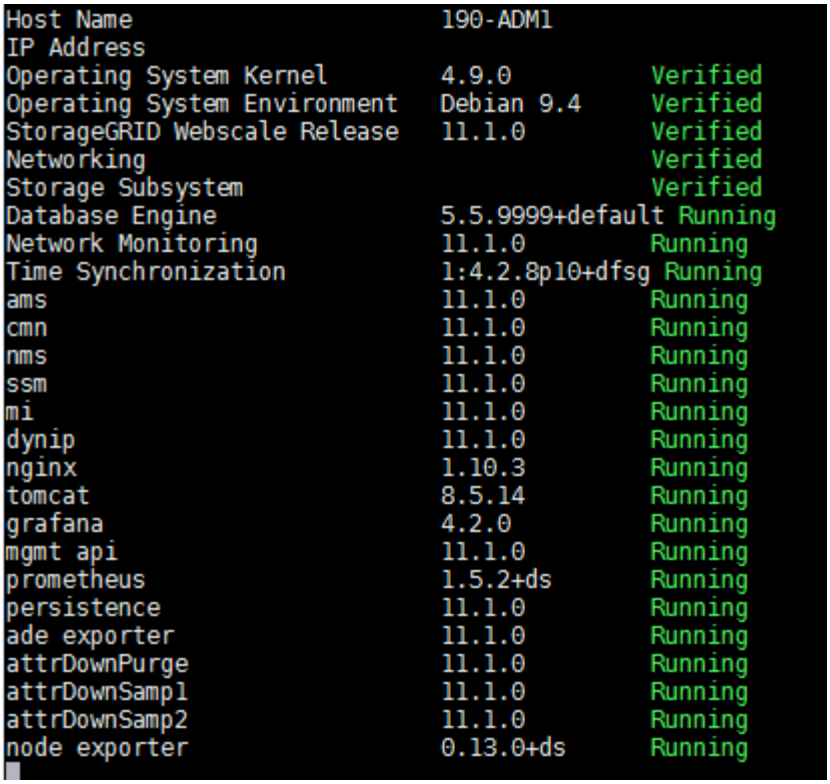
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   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.



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 von Server Manager und allen Diensten

Möglicherweise müssen Sie Server Manager starten, der auch alle Dienste auf dem Grid-Knoten startet.

Was Sie benötigen

Sie müssen die haben `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`

Neustart von Server Manager und allen Diensten

Möglicherweise müssen Sie den Server-Manager und alle Dienste, die auf einem Grid-Knoten ausgeführt werden, neu starten.

Was Sie benötigen

Sie müssen die haben `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 von Server Manager und allen Diensten

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.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Das einzige Szenario, in dem Sie den Server Manager anhalten müssen, während das Betriebssystem ausgeführt wird, ist, wenn Sie Server Manager in andere Dienste integrieren müssen. Wenn der Server Manager für die Wartung der Hardware oder die Neukonfiguration des Servers angehalten werden muss, sollte der gesamte Server angehalten werden.

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`

Anzeigen des aktuellen Status eines Dienstes

Sie können jederzeit den aktuellen Status einer auf einem Grid-Node ausgeführten Services anzeigen.

Was Sie benötigen

Sie müssen die haben `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`**

Anhalten eines Dienstes

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.

Was Sie benötigen

Sie müssen die haben `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

"Beendigung eines Dienstes erzwingen"

Versetzen einer Appliance in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

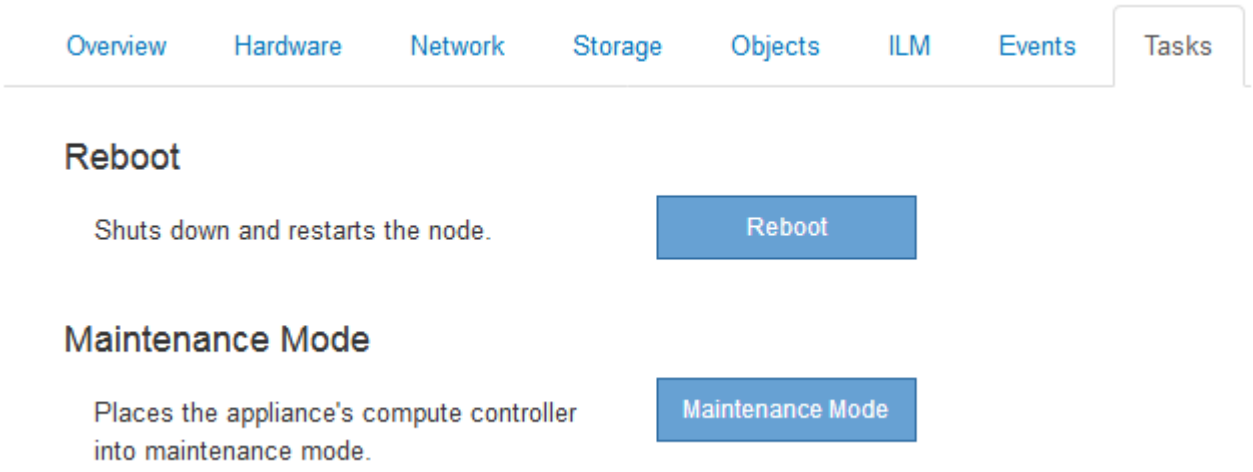
Über diese Aufgabe

Wenn Sie eine StorageGRID Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

> Das Passwort und der Hostschlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem, als das Gerät in Betrieb war.

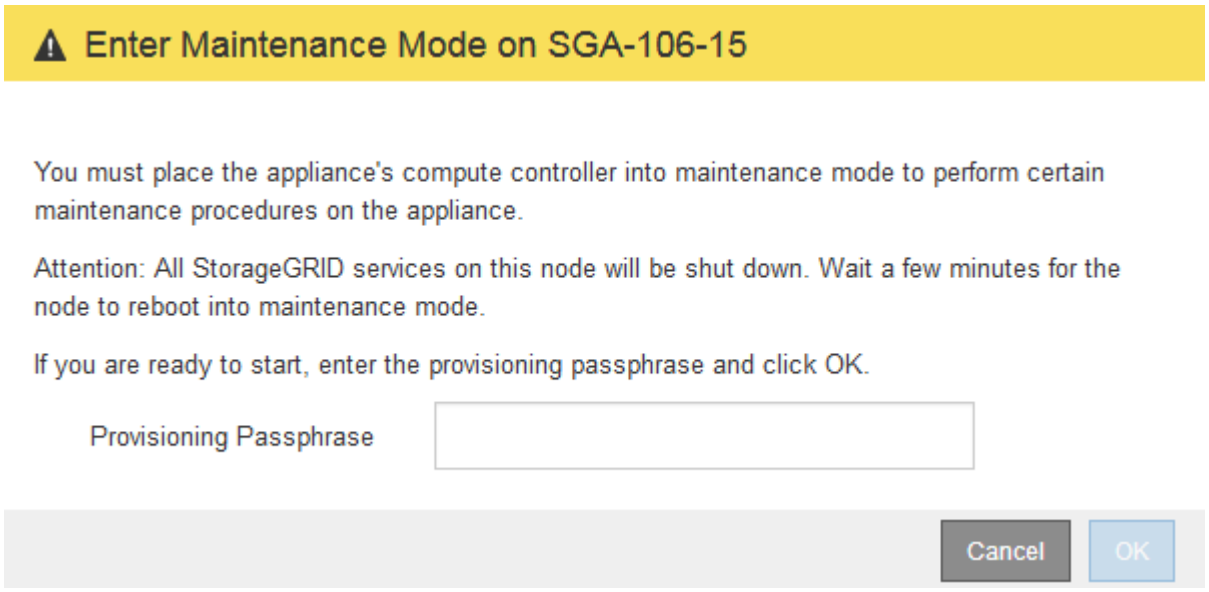
Schritte

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**.

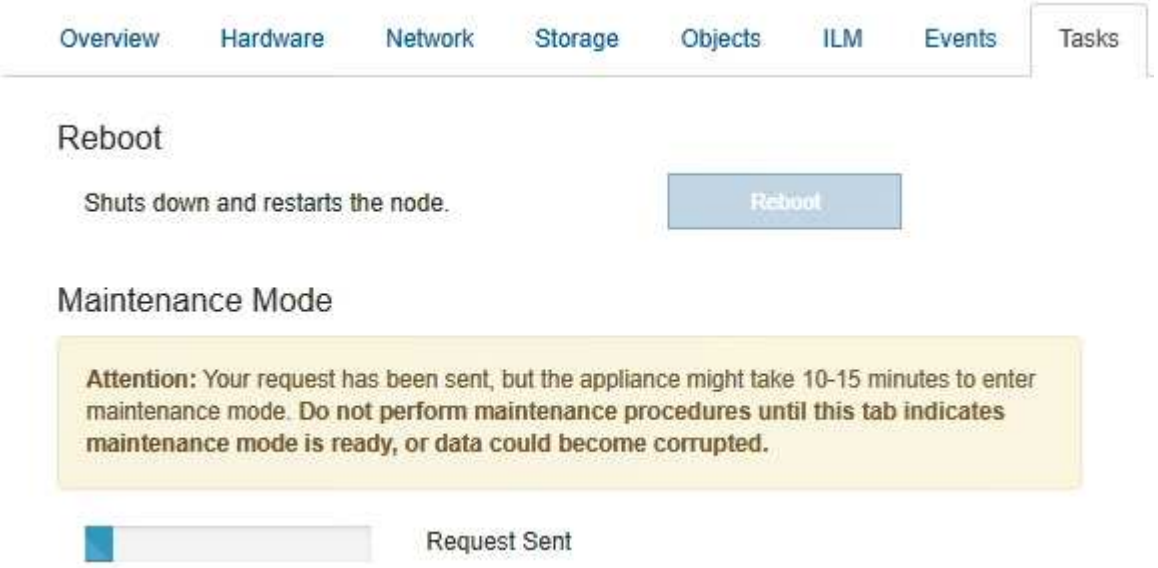
   Ein Bestätigungsdialogfeld wird angezeigt.



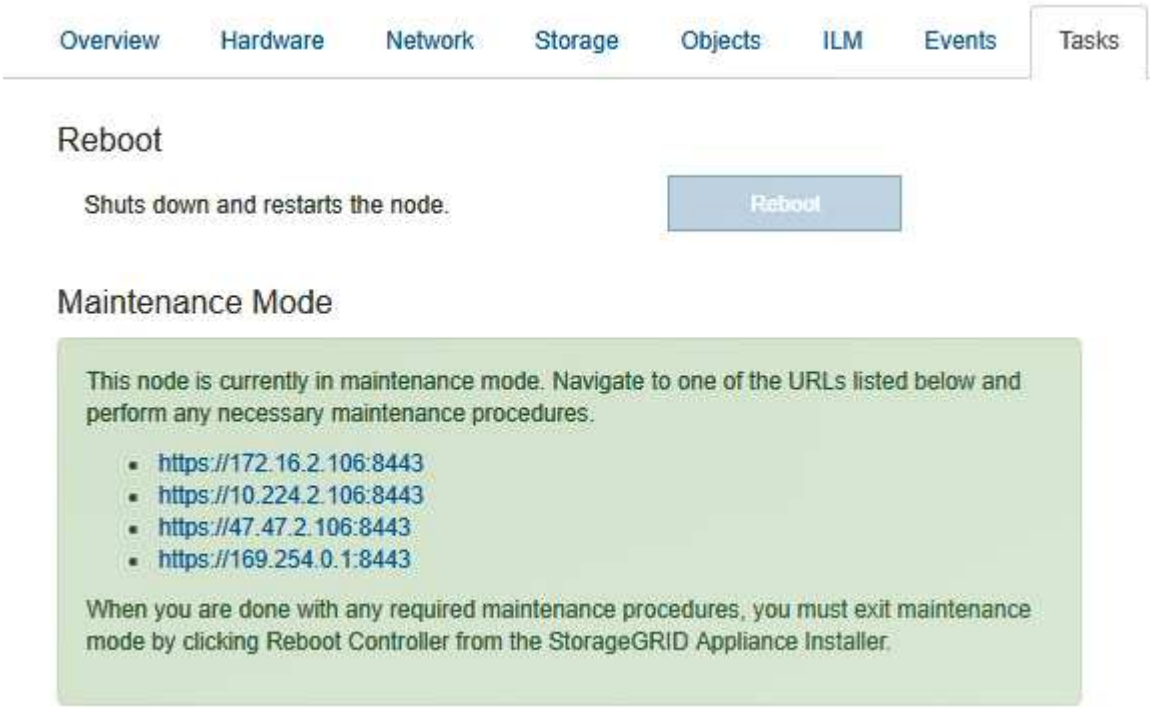
5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

   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.



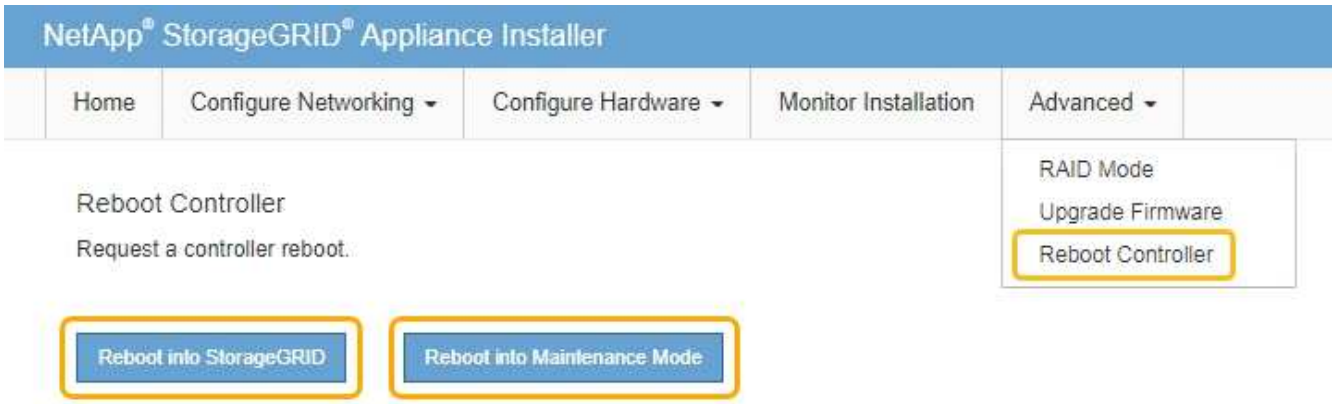
6. Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

   Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.

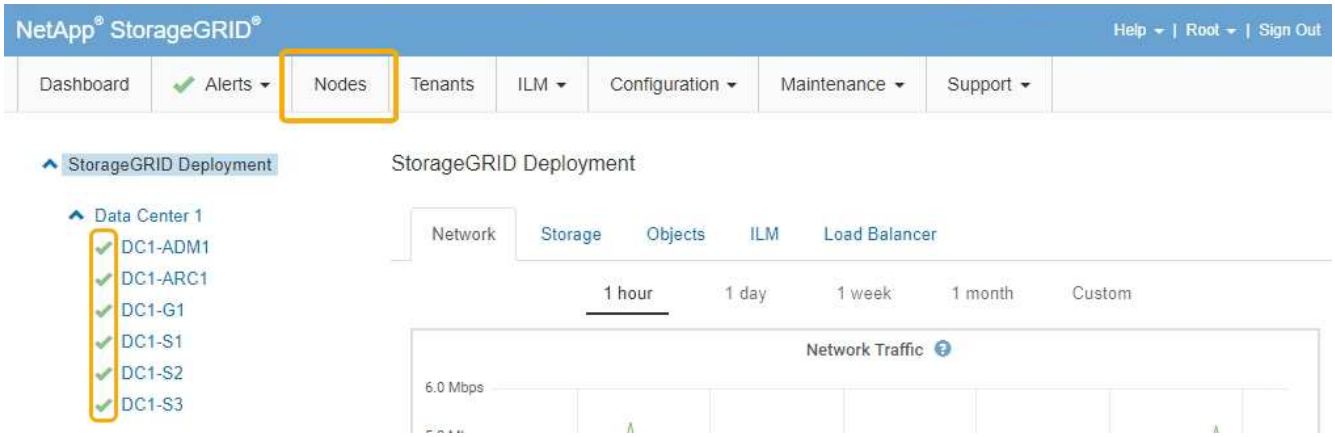
   > Zugriff Auf `https://169.254.0.1:8443` Erfordert eine direkte Verbindung zum lokalen Management-Port.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

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.



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 Registerkarte **Nodes** sollte ein normaler Status angezeigt werden ✔ Für den Appliance-Node gibt an, dass keine Meldungen aktiv sind und der Node mit dem Grid verbunden ist.



Beendigung eines Dienstes erzwingen

Wenn Sie einen Dienst sofort beenden müssen, können Sie den verwenden `force-stop` Befehl.

Was Sie benötigen

Sie müssen die haben `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`

Starten oder Neustarten eines Dienstes

Möglicherweise müssen Sie einen Dienst starten, der angehalten wurde, oder Sie müssen einen Dienst anhalten und neu starten.

Was Sie benötigen

Sie müssen die haben `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 von 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.

> 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.

> Wenn die Port-Remap Client-Zugriff bietet, sollte der Client neu konfiguriert werden, um einen anderen Port zu verwenden, der, wenn möglich, als Load Balancer-Endpunkt konfiguriert ist, um einen Serviceverlust zu vermeiden, andernfalls führt das Entfernen der Port-Zuordnung zu einem 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. Lesen Sie die Anweisungen zum 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-Betriebssystems, während Port 22 der SSH-Port des Docker

Containers ist, auf dem 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 zum Neubooten eines Grid-Node.

4. Wiederholen Sie diese Schritte auf jedem Admin-Node und Gateway-Node mit gegensätzlichen neu zugeordneten Ports.

Verwandte Informationen

"StorageGRID verwalten"

"Neubooten eines Grid-Node"

"Entfernen von Port-Remaps auf Bare-Metal-Hosts"

Entfernen von 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. 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
<strong>PORT_REMAP = client/tcp/8082/443</strong>
<strong>PORT_REMAP_INBOUND = client/tcp/8082/443</strong>
```

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.
   a. 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.

Neubooten eines Grid-Node

Sie können einen Grid-Node aus dem Grid Manager oder aus der Befehlshaber des Node neu booten.

Über diese Aufgabe

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 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.

Verwandte Informationen

"StorageGRID verwalten"

Wahlmöglichkeiten

- "Neubooten eines Grid-Node aus dem Grid Manager"
- "Neubooten eines Grid-Node aus der Eingabeaufforderung"

Neubooten eines Grid-Node aus dem Grid Manager

Beim Neubooten eines Grid-Node aus dem Grid Manager wird der Probleme auftreten `reboot` Befehl auf dem Ziel-Node.

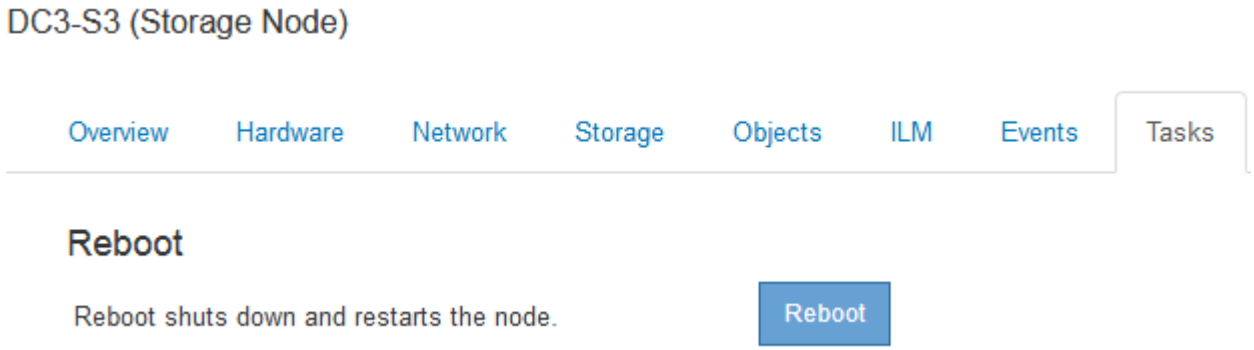
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

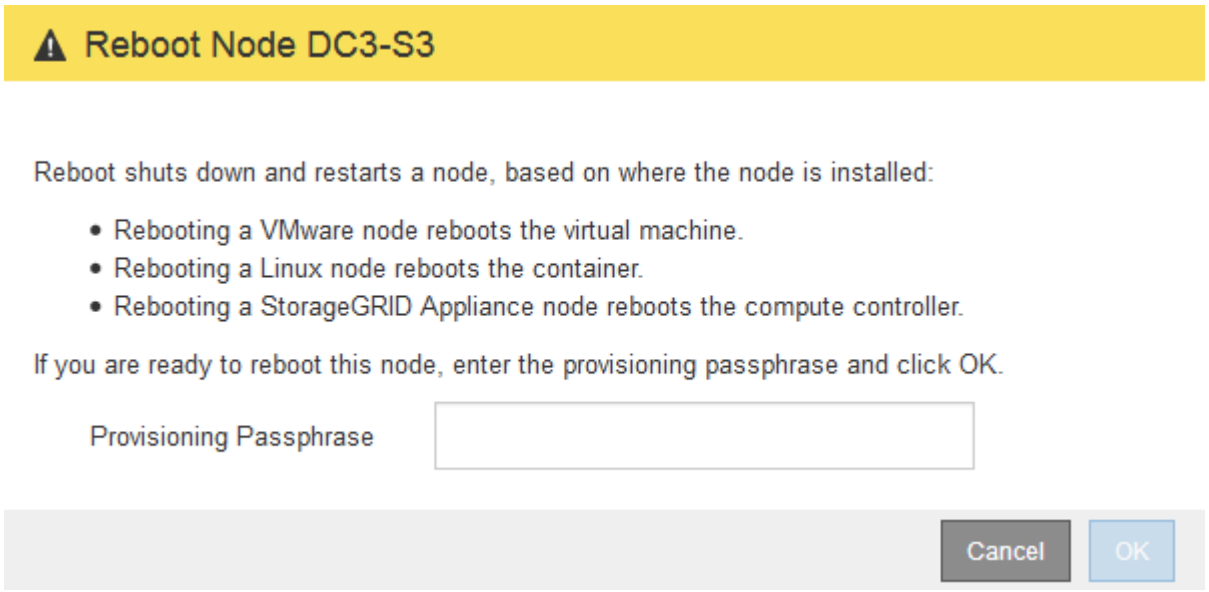
Schritte

1. Wählen Sie **Knoten**.
2. Wählen Sie den Grid-Node aus, den Sie neu booten möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.



4. Klicken Sie Auf **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 klicken Sie auf **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 Knoten angezeigt. Wenn alle Dienste wieder gestartet wurden, ändert sich das Symbol wieder in seine ursprüngliche Farbe.

Neubooten eines Grid-Node aus der Eingabeaufforderung

Wenn Sie den Neustart genauer überwachen müssen oder nicht auf den Grid Manager zugreifen können, können Sie sich beim Grid-Node anmelden und den Befehl Server Manager reboot über die Befehlszeile ausführen.

Was Sie benötigen

- Sie müssen die haben `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`

Herunterfahren eines Grid-Node

Sie können einen Grid-Node über die Befehlshaber des Node herunterfahren.

Was Sie benötigen

- Sie müssen die haben `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.
- Schalten Sie einen Node während eines Wartungsvorgangs nicht herunter, es sei denn, er wird ausdrücklich von der Dokumentation oder vom technischen Support 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 Storage-Nodes herunterfahren 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 Speicherknoten an einem bestimmten Standort herunterfahren möchten, können Sie während des Herunterfahrens möglicherweise nicht auf diese Objekte zugreifen.
  - Um sicherzustellen, dass Sie bei Herunterfahren eines Storage-Nodes auf alle Objekte zugreifen können, beenden Sie die Aufnahme von Objekten an einem Standort für etwa eine Stunde, bevor Sie den Node herunterfahren.

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 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. Melden Sie sich aus der Befehlsshell ab: `exit`

Nach dem Herunterfahren können Sie den Grid-Node ausschalten.

"Herunterfahren eines Hosts"

Verwandte Informationen

"StorageGRID verwalten"

Herunterfahren eines Hosts

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 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.

6. Wenn Sie einen Appliance-Node herunterfahren:
   - Für die SG100- oder SG1000-Services-Appliance
     i. Schalten Sie das Gerät aus.
     ii. Warten Sie, bis die blaue Betriebs-LED erlischt.
   - Für das SG6000-Gerät
     i. 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.

     ii. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.
   - Für die SG5700 Appliance
     i. 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.

     ii. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.
7. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

Ausschalten und Einschalten aller Knoten im Grid

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.

Beenden von Services und Herunterfahren von Grid-Nodes

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, Docker Container und StorageGRID Appliances herunterfahren.

Über diese Aufgabe

Wenn möglich, sollten Sie Dienste auf den Grid-Knoten in dieser Reihenfolge stoppen:

- Stoppen Sie zuerst Dienste auf Gateway Nodes.
- Stoppen Sie die Dienste auf dem primären Admin-Knoten zuletzt.

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 Nodes von einem Linux-Host auf einen anderen migrieren, um die Host-Wartung durchzuführen, ohne die Funktionalität oder Verfügbarkeit Ihres Grid zu beeinträchtigen.

"Linux: Migration eines Grid-Node zu einem neuen Host"

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 ausgeben `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 Appliance-Nodes haben:
   - Für die SG100- oder SG1000-Services-Appliance
     i. Schalten Sie das Gerät aus.
     ii. Warten Sie, bis die blaue Betriebs-LED erlischt.
   - Für das SG6000-Gerät
     i. 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.

     ii. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.
   - Für die SG5700 Appliance
     i. 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.

ii. 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.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

Die Grid-Nodes starten

Folgen Sie dieser Sequenz, um die Grid-Knoten nach einem vollständigen Herunterfahren zu 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 für die Wiederherstellung von Cassandra-Daten zu verwenden. Dies kann zu Datenverlust führen.

Über diese Aufgabe

Wenn möglich, sollten Sie die Netzknoten in dieser Reihenfolge einschalten:

- 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

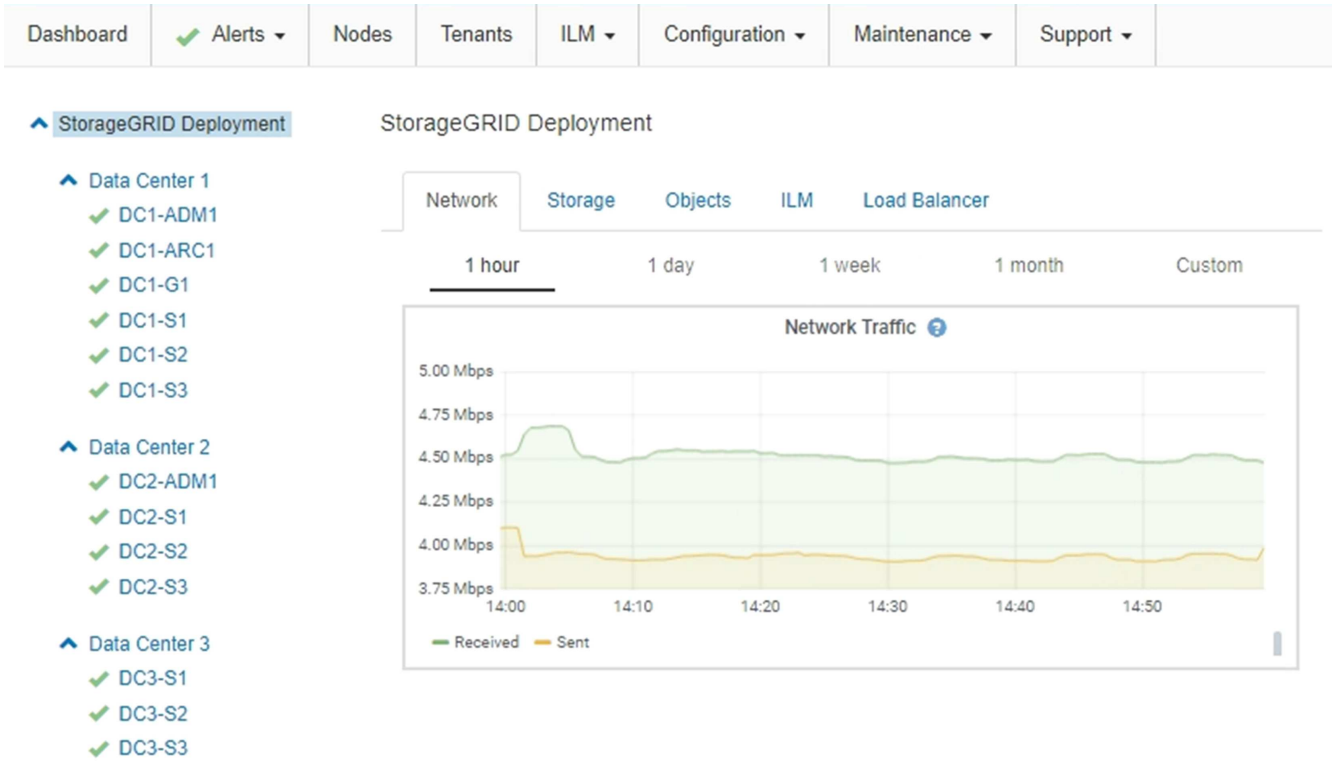
1. Schalten Sie die Hosts für den primären Admin-Node und alle nicht-primären Admin-Nodes ein.

   > 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. Klicken Sie auf **Knoten**, und überwachen Sie den Status der Rasterknoten. Vergewissern Sie sich, dass alle Nodes in den Status „`grün`“ zurückkehren.



Verwenden einer 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 angefangente Dienst beim nächsten Start oder Neustart von Server Manager gestartet. Dienste werden beim Entfernen der DoNotStart-Datei nicht automatisch gestartet.

Der effizienteste Weg, um einen Neustart aller Dienste zu verhindern, ist, dass der NTP-Dienst nicht gestartet wird. Alle Dienste sind vom NTP-Dienst abhängig und können nicht ausgeführt werden, wenn der NTP-Dienst nicht ausgeführt wird.

Hinzufügen einer DoNotStart-Datei für einen Dienst

Sie können verhindern, dass ein einzelner Dienst gestartet wird, indem Sie dem Verzeichnis dieses Dienstes auf einem Grid-Node eine DoNotStart-Datei hinzufügen.

Was Sie benötigen

Sie müssen die haben `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 Befehlsshell ab: `exit`

Entfernen einer DoNotStart-Datei für einen Dienst

Wenn Sie eine DoNotStart-Datei entfernen, die den Start eines Dienstes verhindert, müssen Sie diesen Dienst starten.

Was Sie benötigen

Sie müssen die haben `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 Befehlsshell ab: `exit`

Fehlerbehebung Für Server Manager

Der technische Support leitet Sie möglicherweise zur Fehlerbehebung, um die Quelle der mit Server Manager verbundenen Probleme zu ermitteln.

Zugriff auf die Protokolldatei von 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.

Was Sie benötigen

Sie müssen die haben `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 Anweisungen zum 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`

Verwandte Informationen

"Entfernen einer DoNotStart-Datei für einen Dienst"

Klonen von Appliance-Nodes

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 des vorhandenen Nodes an die neue Appliance übertragen, ein Hardware-Upgrade-Prozess ist einfach durchzuführen und eine Alternative zur Ausmusterung und Erweiterung beim Austausch von Appliances zu bieten.

Funktionsweise des Appliance-Node-Klonens

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 von ihr ersetzte Appliance-Node, müssen Sie für jedes dieser Netzwerke auf der Ersatzanwendung 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 Ersatz-Speicher-Appliance muss die gleiche oder höhere Kapazität aufweisen als der Speicherknoten, den sie ersetzt.
  - Wenn die Ziel-Speicher-Appliance die gleiche Anzahl von Laufwerken wie der Quellknoten hat, müssen die Laufwerke in der ZielAppliance dieselbe Kapazität (in TB) oder größer haben.
  - Wenn die Anzahl der Standardlaufwerke, die in einer Ziel-Storage Appliance installiert sind, kleiner als die Anzahl der Laufwerke im Quell-Node ist, da Solid State Drives (SSDs) installiert sind, wird die gesamte Storage-Kapazität der Standardlaufwerke in der Ziel-Appliance (in TB) Die Gesamtkapazität aller Laufwerke im Quell-Storage-Node muss erreicht oder überschritten werden.

    Wenn beispielsweise eine SG5660 Quell-Storage Node Appliance mit 60 Laufwerken auf eine SG6060 Ziel-Appliance mit 58 Standardlaufwerken geklont wird, sollten vor dem Klonen größere Laufwerke in der SG6060 Ziel-Appliance installiert werden, um die Storage-Kapazität erhalten zu können. (Die zwei Laufwerksschächte mit SSDs in der Ziel-Appliance sind nicht in der gesamten Appliance-Storage-

Kapazität enthalten.)

Wenn jedoch eine SG5660 Quell-Node-Appliance mit 60 Laufwerken mit SANtricity Dynamic Disk Pools DDP-8 konfiguriert ist, kann die Konfiguration einer SG6060 Ziel-Appliance mit 58 Laufwerken und DDP-16 die SG6060 Appliance aufgrund der verbesserten Storage-Effizienz als gültiges Klonziel machen.

Informationen zum aktuellen RAID-Modus des Quell-Appliance-Knotens können Sie auf der Seite **Nodes** im Grid Manager anzeigen. Wählen Sie die Registerkarte * Storage* für das Gerät aus.

Welche Informationen sind nicht geklont?

Die folgenden Appliance-Konfigurationen werden während des Klonens 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 vom gleichen Appliance-Typ sein. Bei Änderungen des Appliance-Typs 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 denselben Appliance-Typ sein. Die Ziel-Appliance muss jedoch dieselbe oder größere Storage-Kapazität aufweisen wie die Quell-Appliance.

  So können Sie beispielsweise eine SG5600 Node-Appliance durch eine SG5700 oder SG6000 Appliance 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-Node 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 klonenden Quell-Node-Appliance und werden nach Abschluss des Klonens nicht benötigt. 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 überprüfen, ob die Node-Verschlüsselung auf dem Quell-Appliance-Node aktiviert ist, wie in der Appliance-Installation beschrieben.

  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.

  - "SG100 SG1000 Services-Appliances"
  - "SG5600 Storage Appliances"
  - "SG5700 Storage-Appliances"
  - "SG6000 Storage-Appliances"
- 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. Informationen zum aktuellen RAID-Modus des Quell-Appliance-Knotens können Sie auf der Seite **Nodes** im Grid Manager 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.

Klonen von 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.

Was Sie benötigen

- 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).
- "Überlegungen und Anforderungen zum Klonen von Appliance-Nodes"

  "SG100 SG1000 Services-Appliances"

  "SG5600 Storage Appliances"

  "SG5700 Storage-Appliances"

  "SG6000 Storage-Appliances"

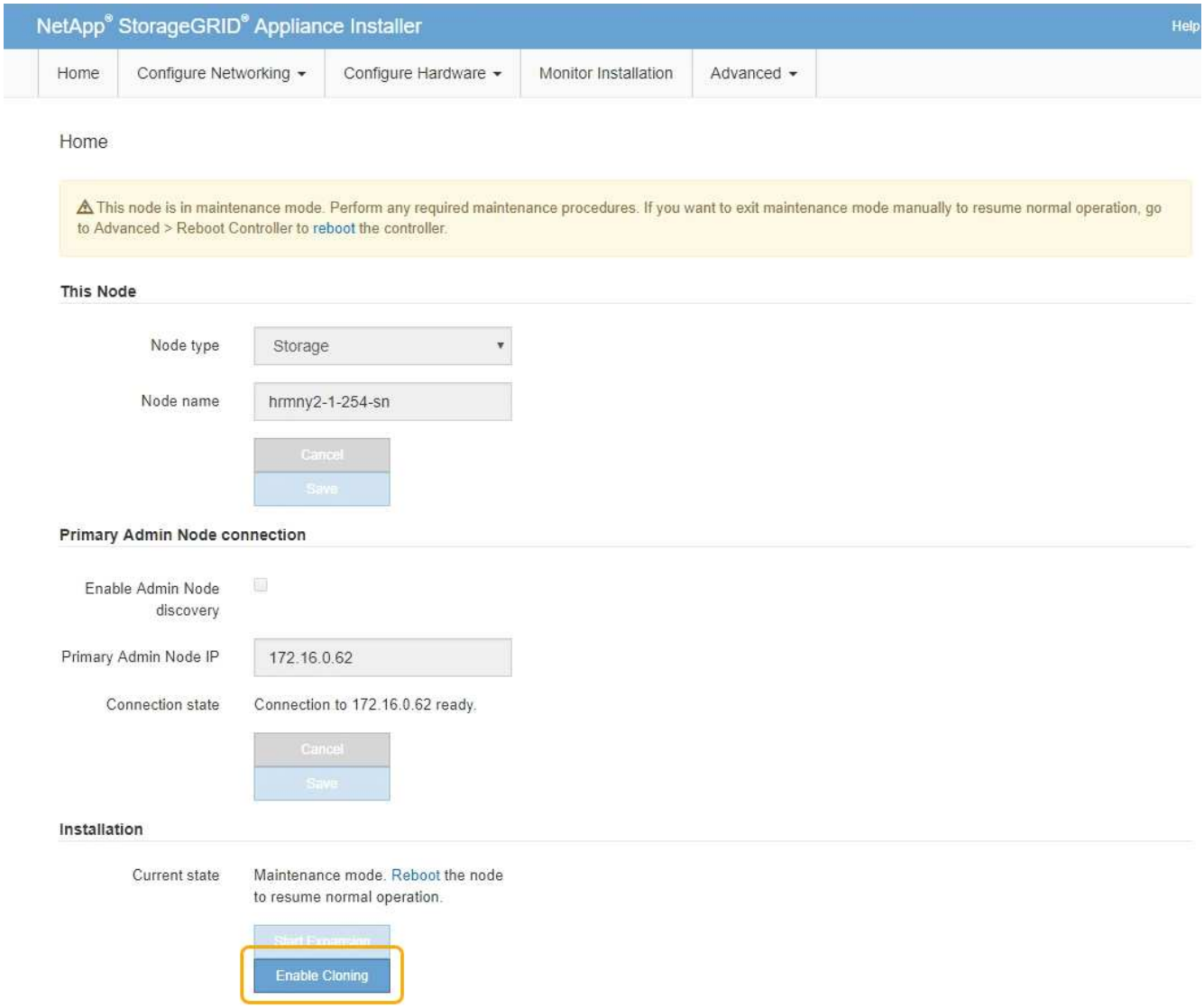
Sie sollten jeweils nur einen Appliance-Node klonen, um die Netzwerk-Performance und Datenverfügbarkeit von StorageGRID zu erhalten.

Schritte

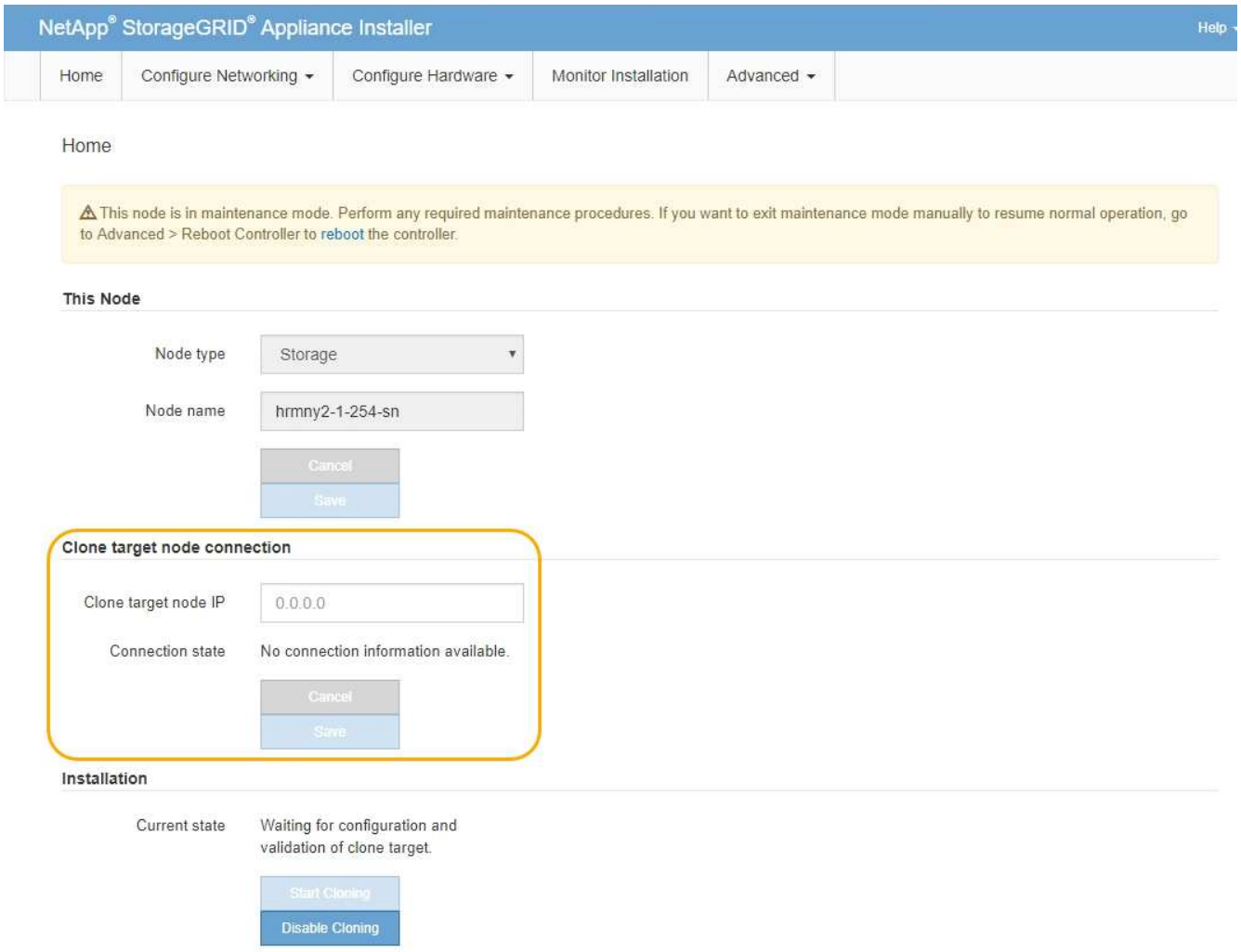
1. Platzieren Sie den Quellknoten, den Sie klonen, in den Wartungsmodus.

   "Versetzen einer Appliance 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.

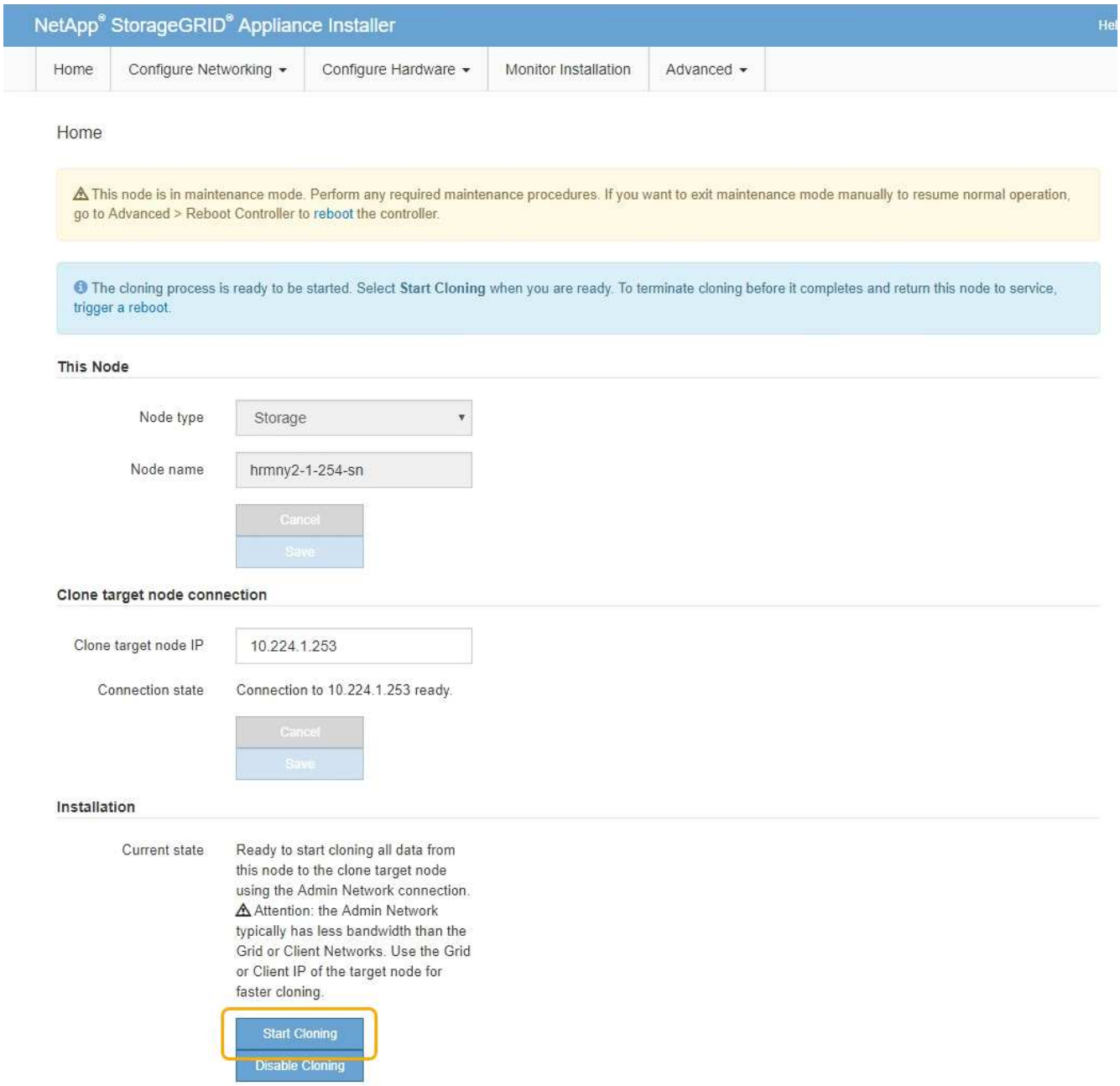


3. Geben Sie für **Zielknoten-IP** die temporäre IP-Adresse ein, die dem Zielknoten zugewiesen ist, das Netzwerk für den Datenverkehr der Klondatenübertragung verwenden soll, und wählen Sie dann **Speichern** aus.

   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.



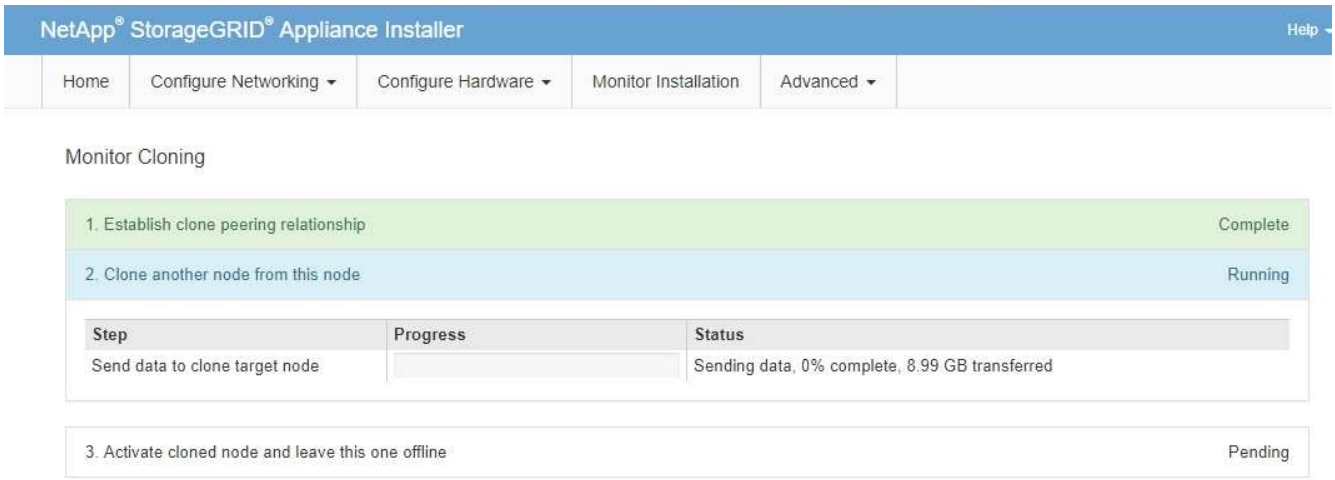
Wenn Probleme bestehen, die das Klonen verhindern, ist **Klonen starten** nicht aktiviert und Probleme, die Sie lösen müssen, werden als **Verbindungsstatus** aufgeführt. Diese Probleme sind auf der Startseite des StorageGRID-Appliance-Installationsprogramms sowohl des Quell-Knotens als auch der Ziel-Appliance 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.

"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.



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 im vorinstallierten Zustand, als ob Sie sie zur Neuinstallation vorbereitet hätten.

  "Vorbereiten eines Geräts für die Neuinstallation (nur Plattformaustausch)"

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. Bitten Sie den StorageGRID-Support bei Bedarf, die Quell-Appliance zu löschen, damit diese Daten zerstört werden können.

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.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"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/"

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/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis zu StorageGRID 11.5"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.