Los geht's

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Los geht’s

Gittergrundierung

Lernen Sie die Grundlagen eines NetApp StorageGRID Systems kennen.

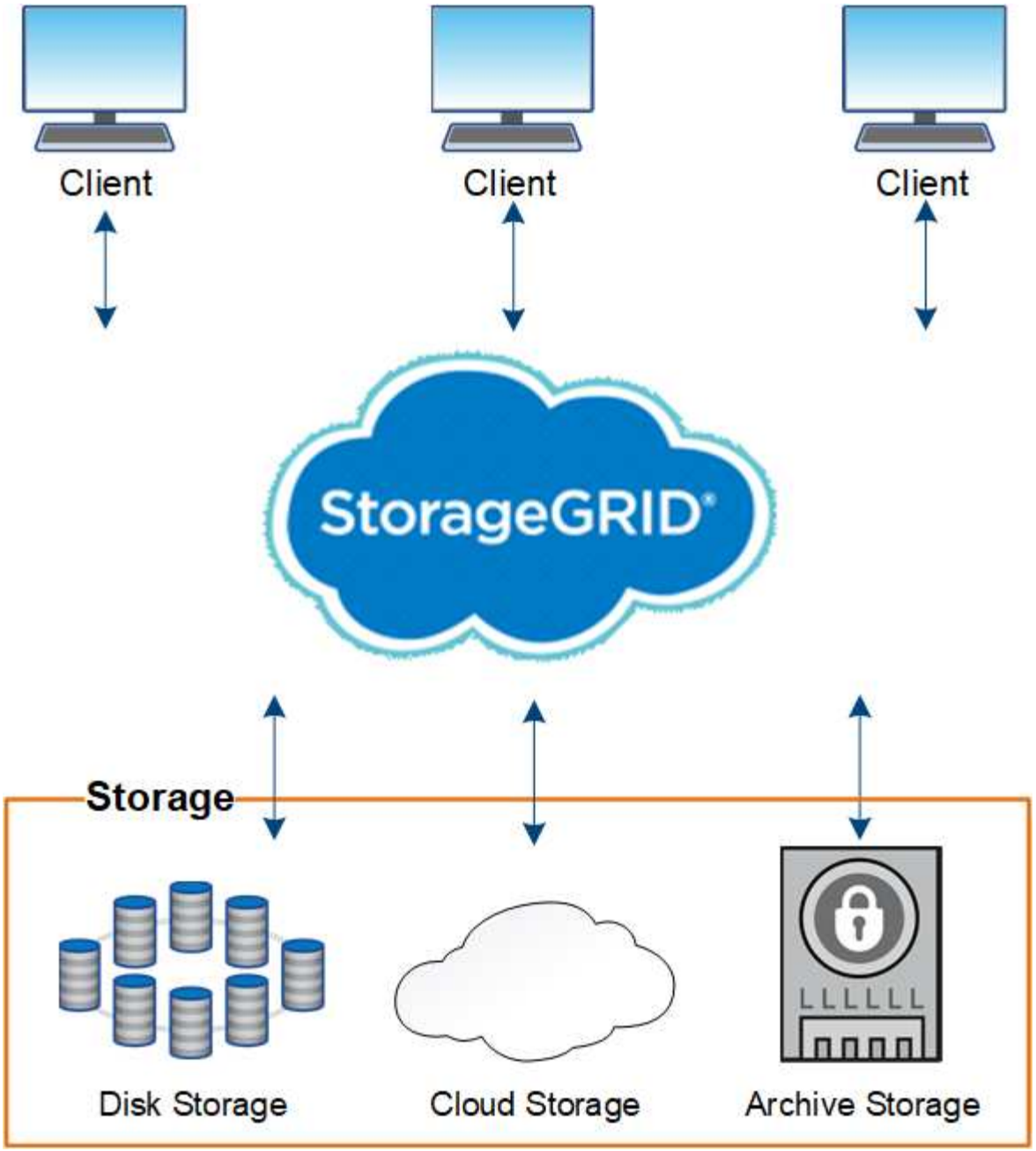
- "Informationen zu StorageGRID"
- "StorageGRID Architektur und Netzwerktopologie"
- "Managen von Daten mit StorageGRID"
- "Wie Grid Manager zu sehen ist"
- "Entdecken Sie den Tenant Manager"
- "Verwenden von StorageGRID"

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

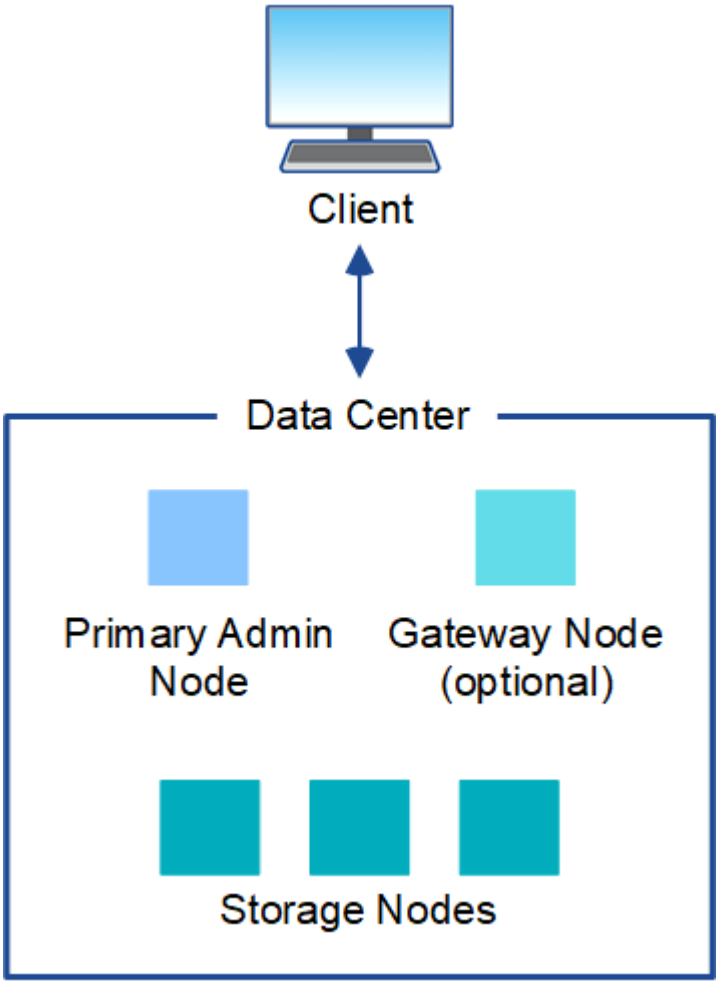
"Netzwerkrichtlinien"

Implementierungstopologien

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

Ein Standort

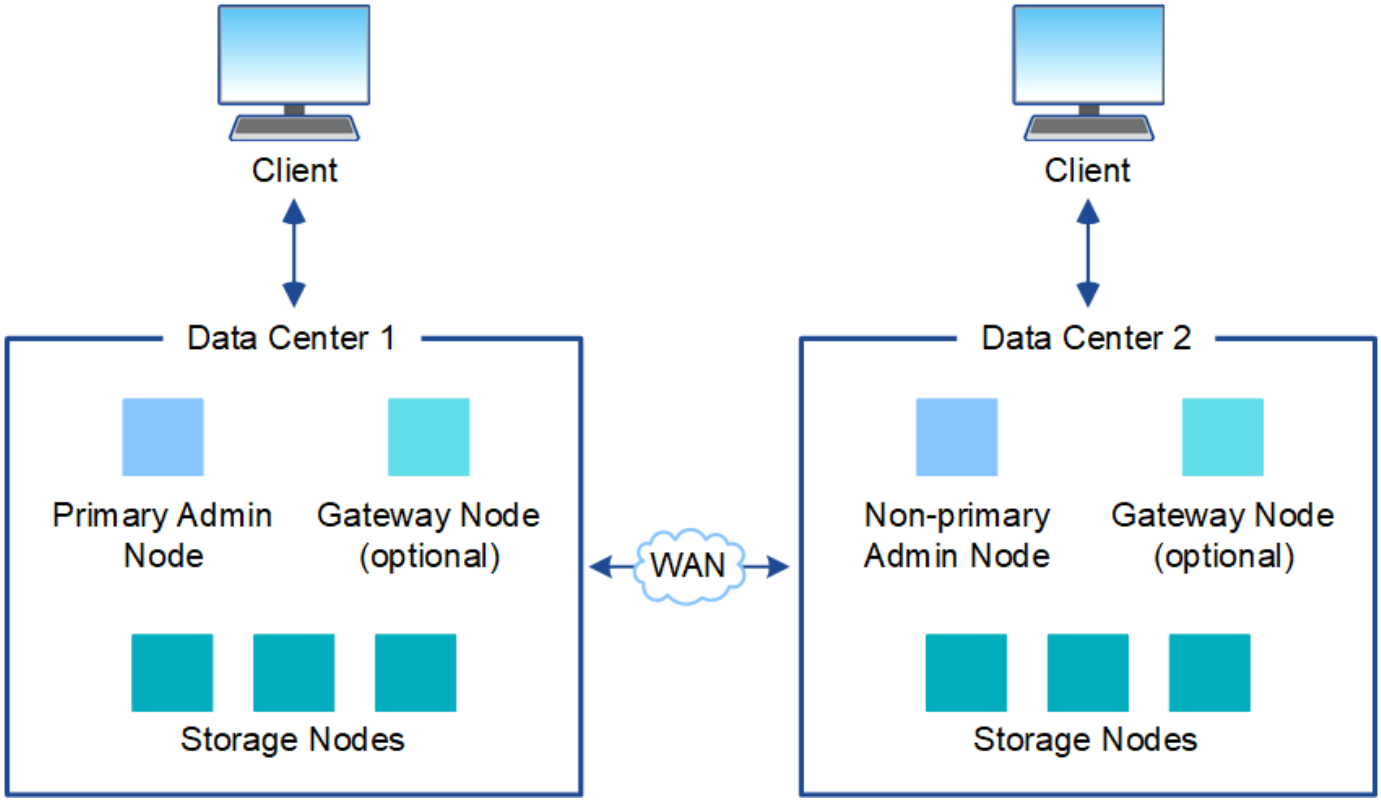
Bei einer Implementierung über einen einzigen Standort werden die Infrastruktur und der Betrieb des StorageGRID Systems zentralisiert.



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.



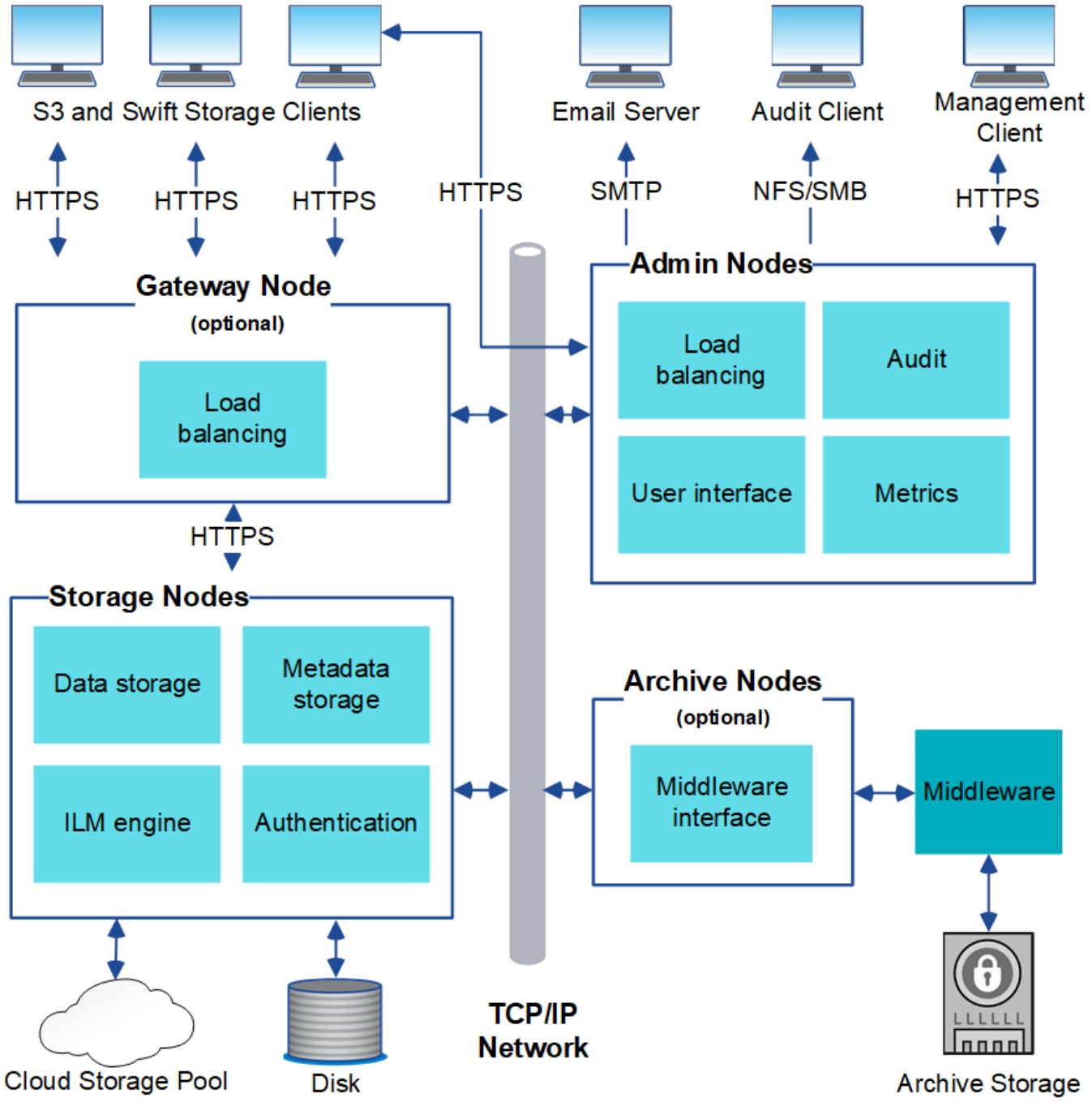
Darüber hinaus können mehrere logische Standorte innerhalb eines einzigen Datacenters eingesetzt werden, um die Verfügbarkeit und Ausfallsicherheit durch verteilte Replizierung und Erasure Coding zu verbessern.

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.

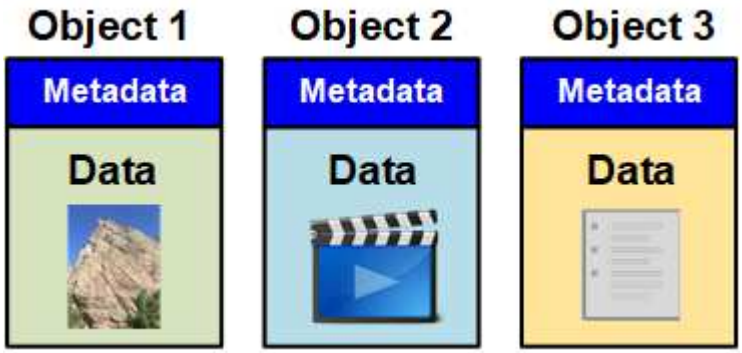
- "Was ist ein Objekt"
- "Schutz von Objektdaten"
- "Das Leben eines Objekts"

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

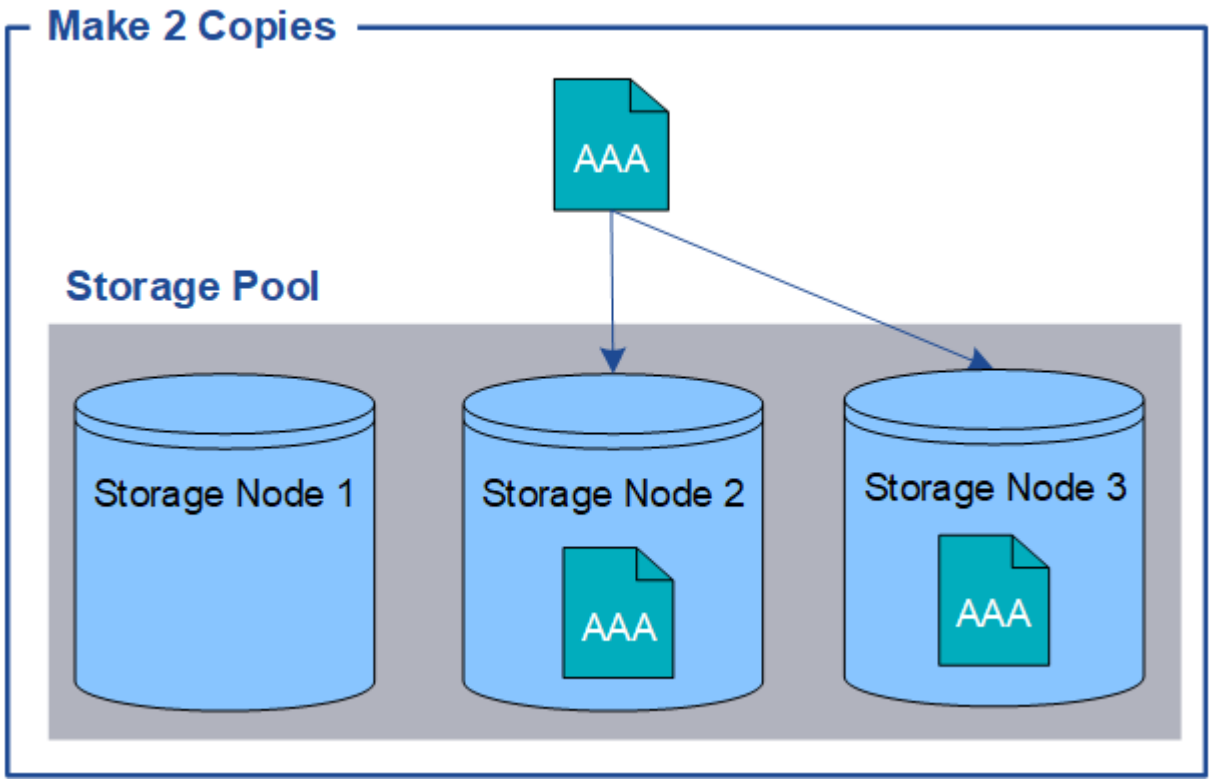
Das StorageGRID System bietet zwei Mechanismen zum Schutz von Objektdaten vor Verlust: Replizierung und Erasure Coding.

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.

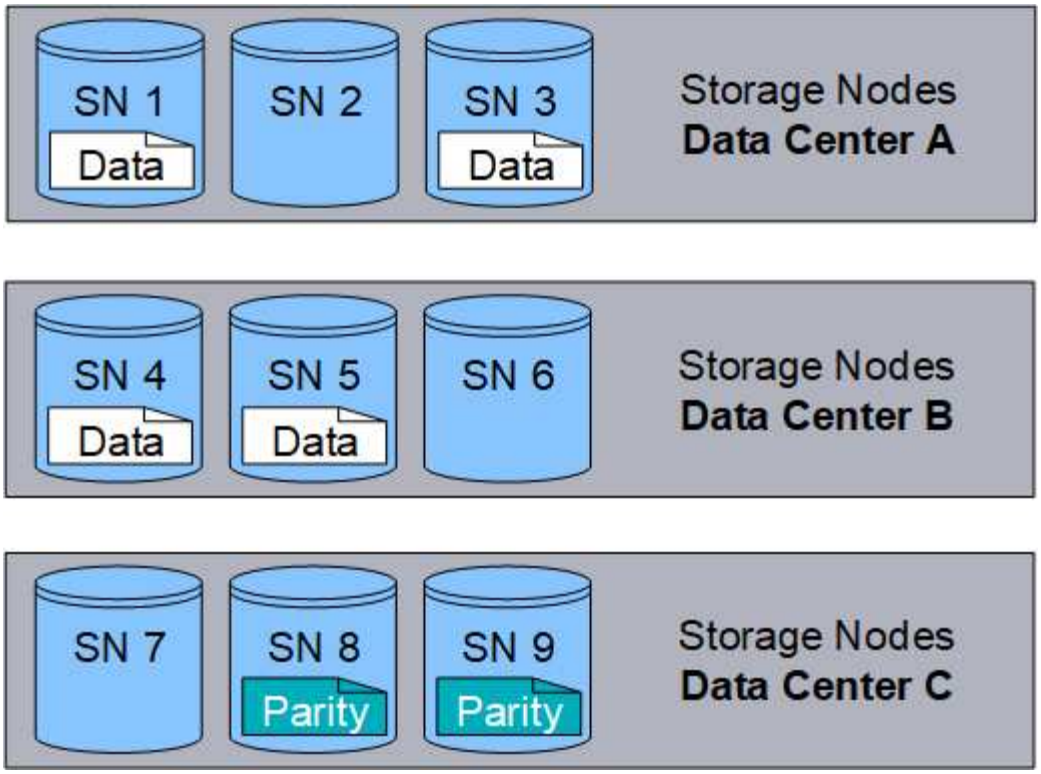
Im folgenden Beispiel gibt die Regel „2 Kopien erstellen“ an, dass zwei replizierte Kopien jedes Objekts in einem Speicherpool platziert werden, der drei Storage-Nodes enthält.



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"

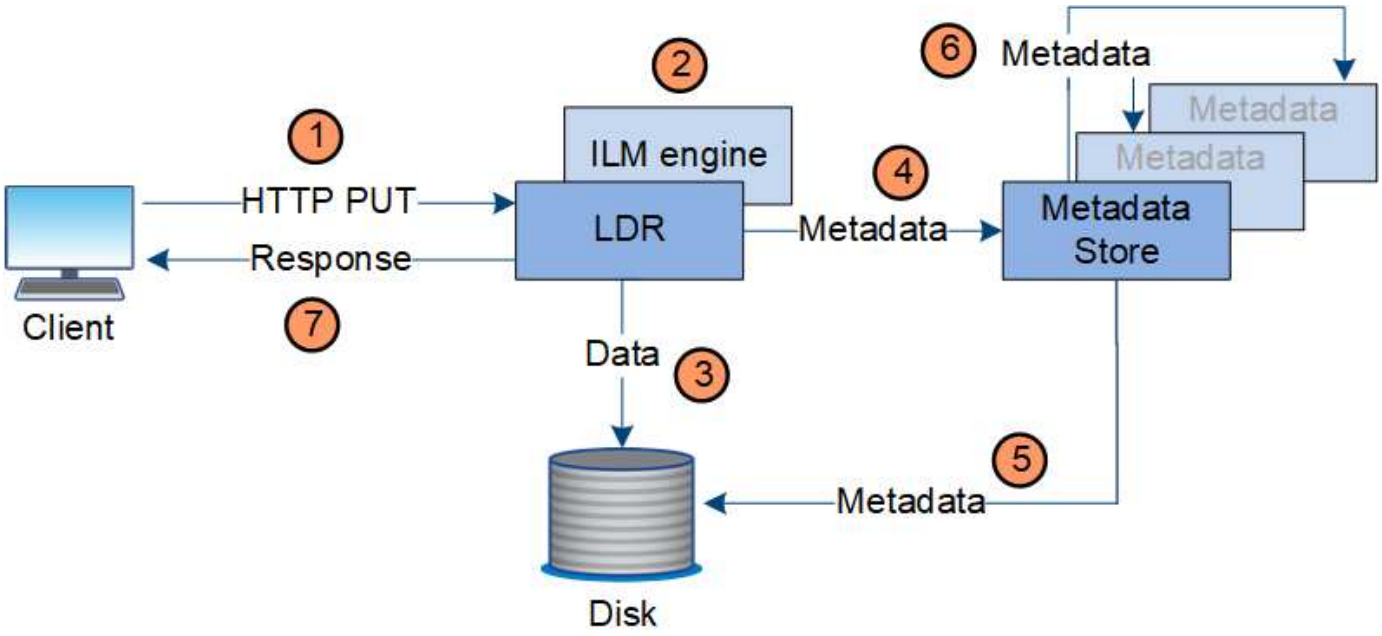
"Mit Information Lifecycle Management"

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.

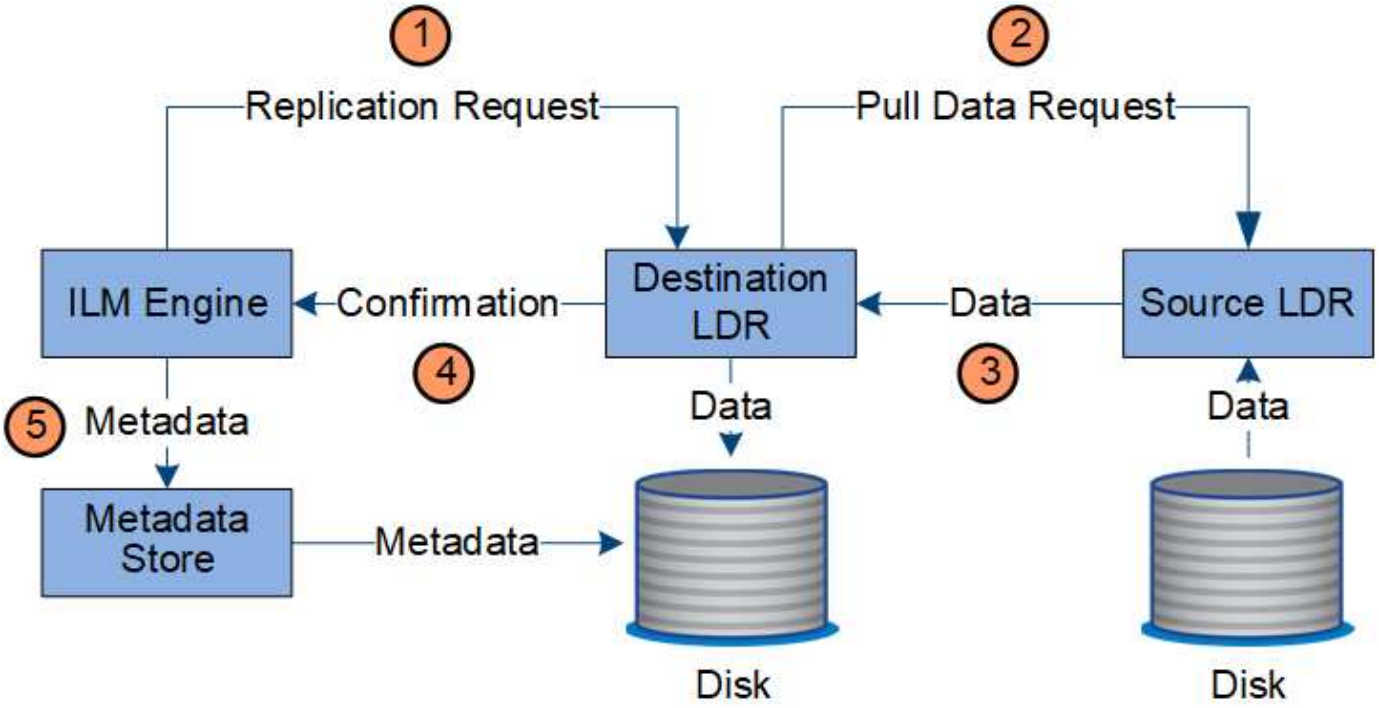
Objektdaten werden vom LDR-Service gemanagt.

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.



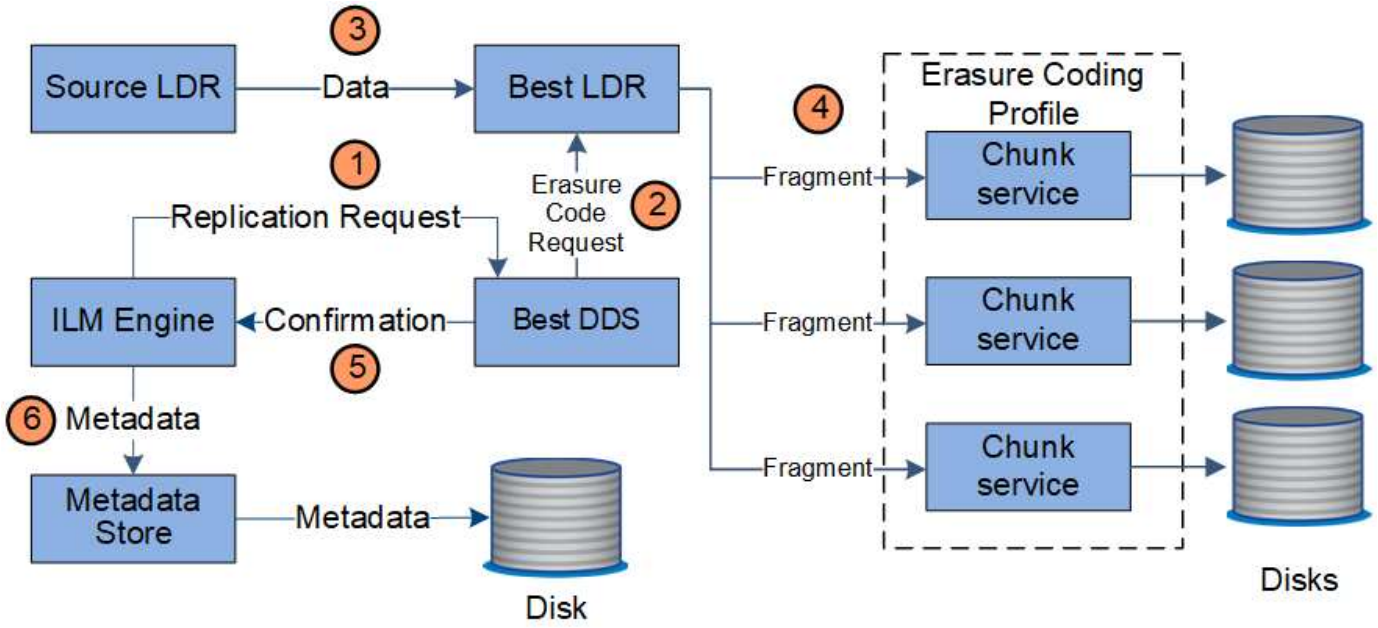
1. Die ILM-Engine fragt den ADC-Service ab, um den besten Ziel-LDR-Service innerhalb des durch die ILM-Regel festgelegten Storage-Pools zu ermitteln. Er sendet dann diesen LDR-Service einen Befehl, um die Replikation zu initiieren.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellspeicherort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



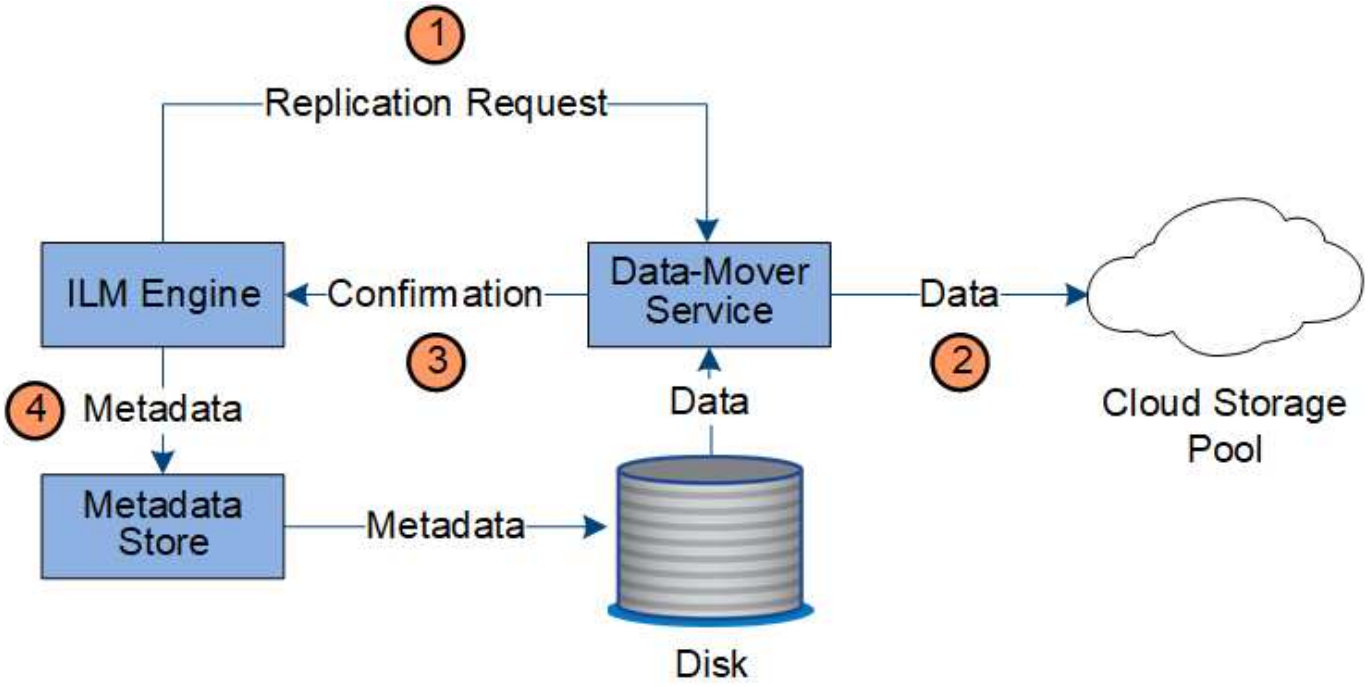
1. Die ILM-Engine fragt den ADC-Service ab, um zu bestimmen, welcher DDS-Service den Erasure Coding-Vorgang am besten ausführen kann. Sobald die ILM-Engine ermittelt wurde, sendet sie eine „Initiierung"-Anforderung an den Service.
2. Der DDS-Dienst weist ein LDR an, den Code der Objektdaten zu löschen.
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.

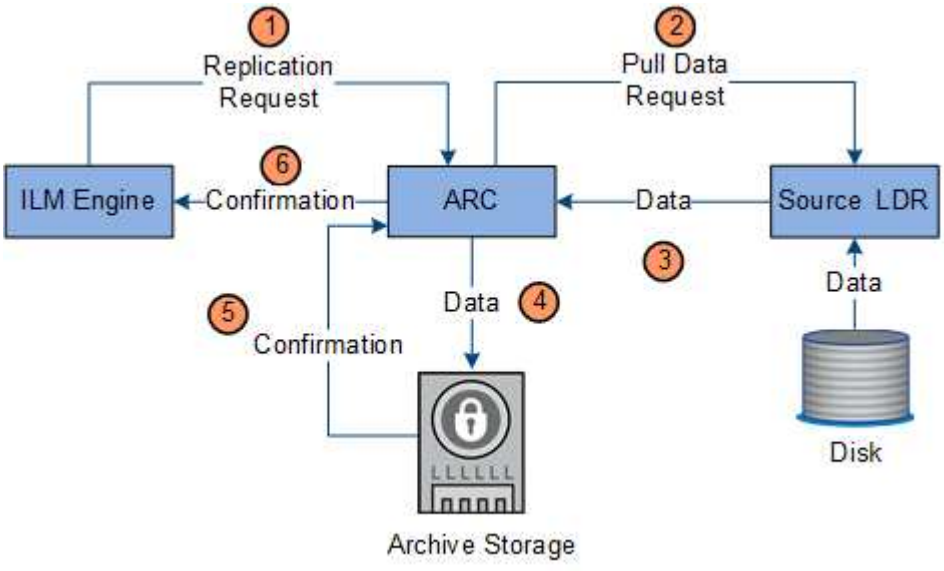


1. Die ILM-Engine wählt einen Data Mover-Service zur Replizierung in den Cloud-Storage-Pool aus.
2. Der Data Mover-Service sendet die Objektdaten an den Cloud-Speicherpool.
3. Der Data Mover-Service benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM-Engine aktualisiert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



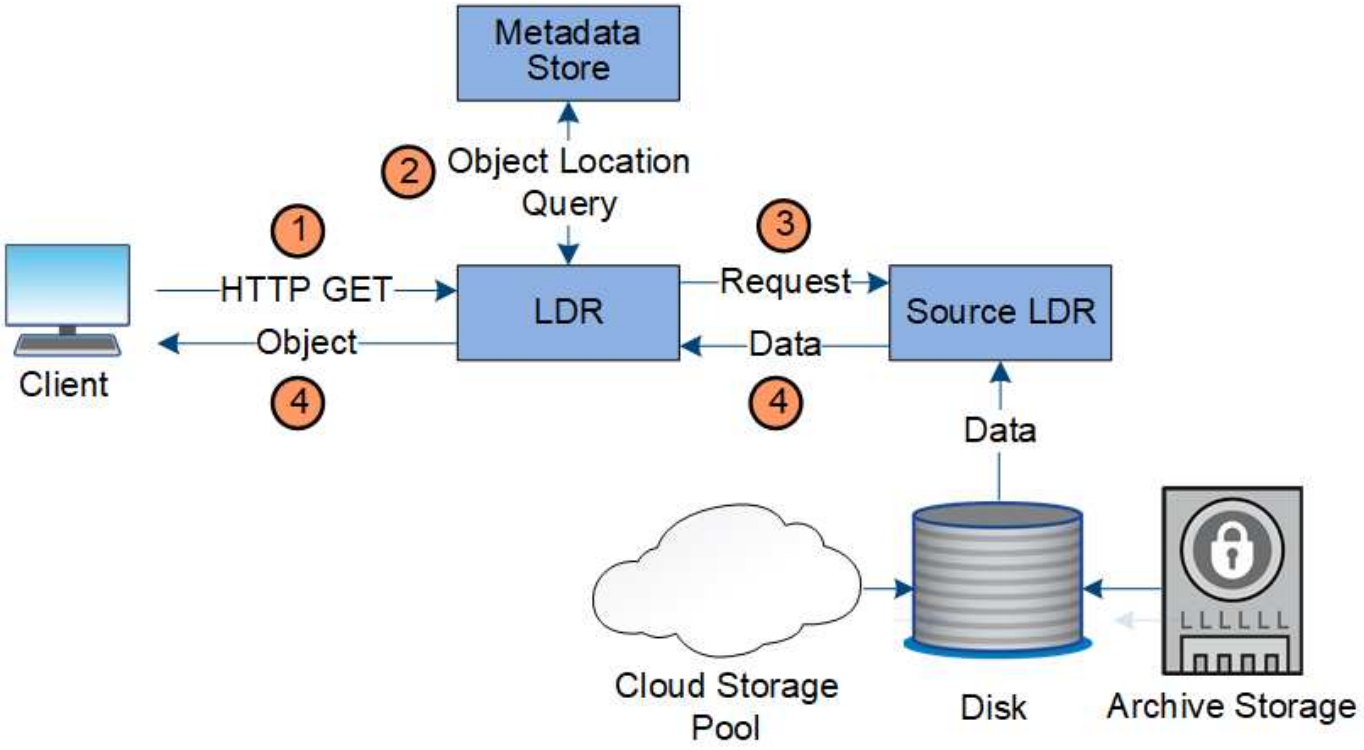
1. Die ILM-Engine sendet eine Anforderung an den ARC-Service, eine Kopie auf Archivmedien zu speichern.
2. Der ARC-Dienst fragt den ADC-Service nach dem besten Quellspeicherort ab und sendet eine Anfrage an den Quell-LDR-Dienst.
3. Der ARC-Dienst ruft Objektdaten aus dem LDR-Dienst ab.
4. Der ARC-Dienst 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.

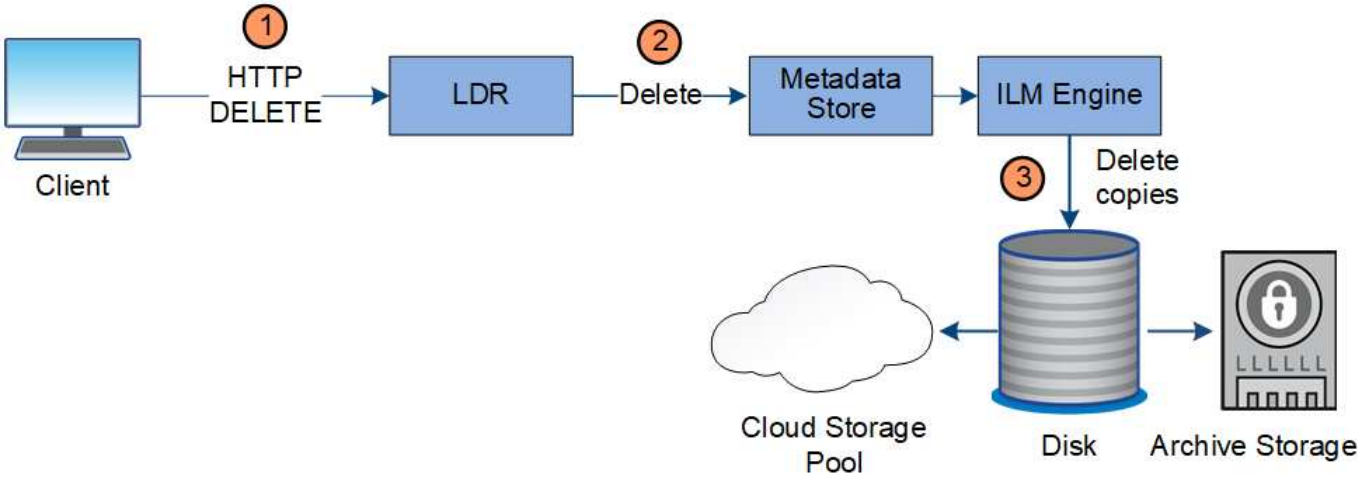
Löschhierarchie

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.

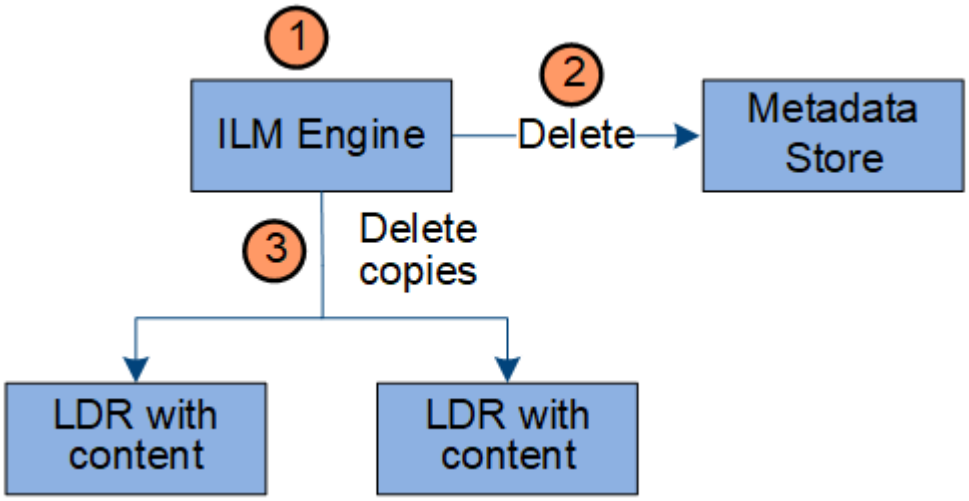
> ⓘ Die Aktion „Ablaufdatum“ in einem S3-Bucket-Lebenszyklus überschreibt immer die ILM-Einstellungen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflegen des Objekts verfallen sind.

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

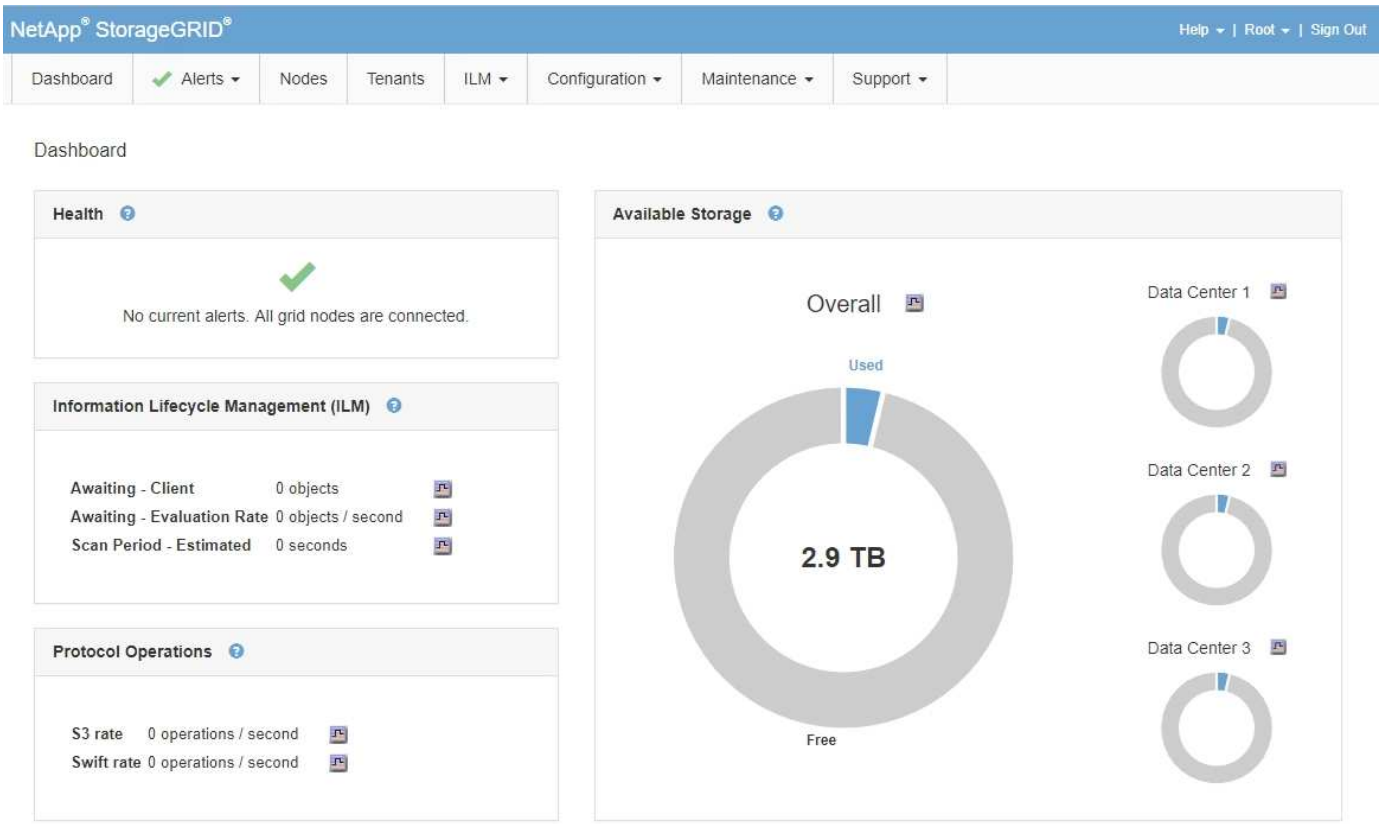
Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

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.



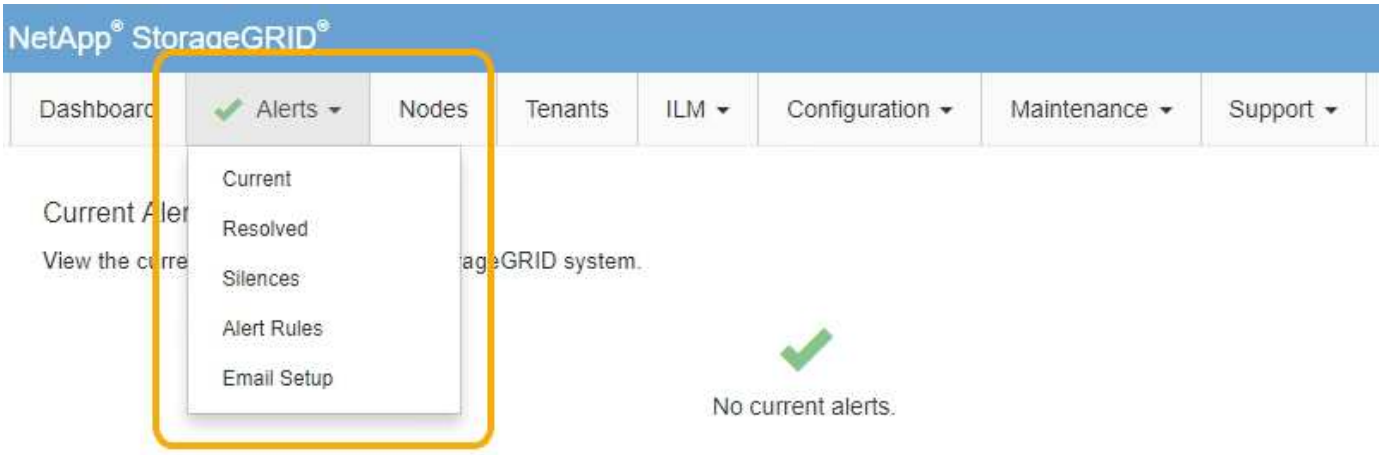
Um die Informationen in den einzelnen Bedienfelds zu erläutern, klicken Sie auf das Hilfesymbol Für dieses Panel.

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

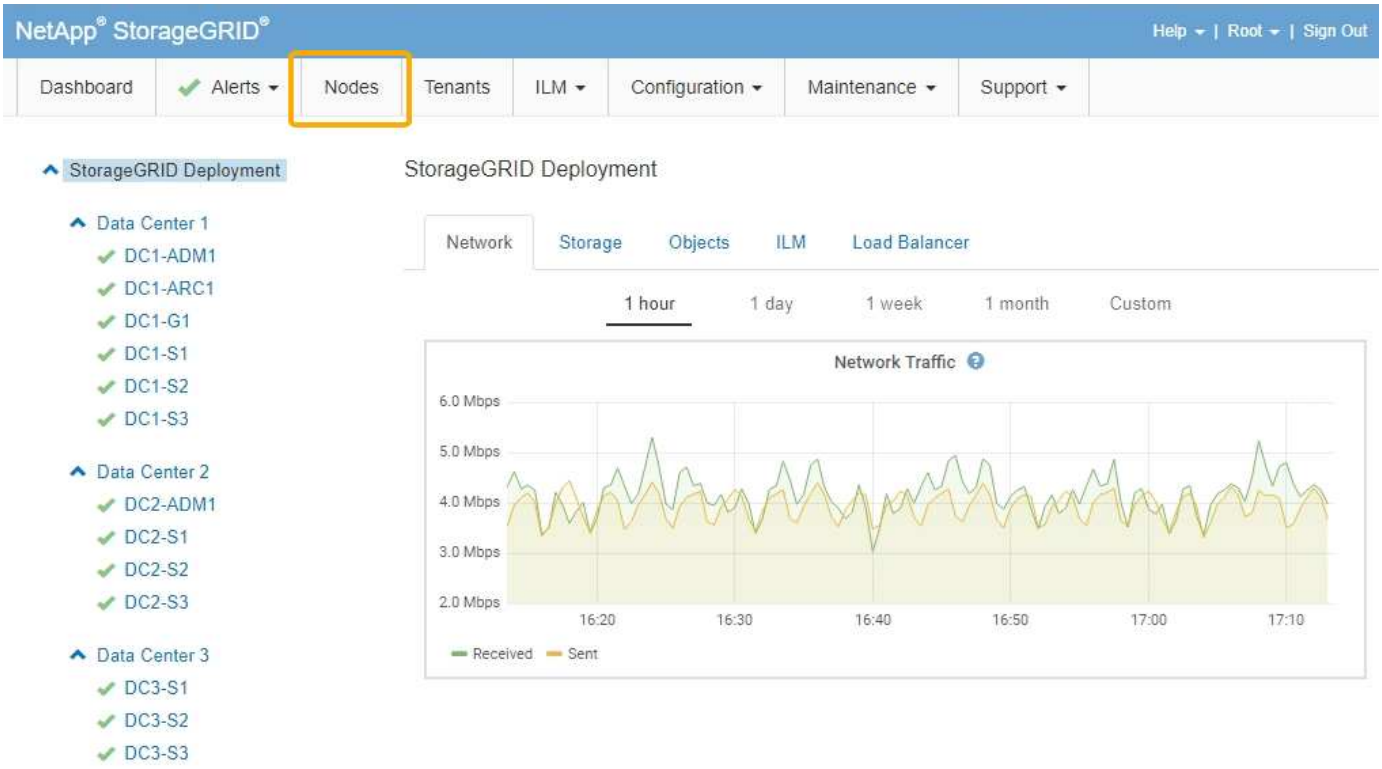
"Monitoring und Management von Warnmeldungen"

"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

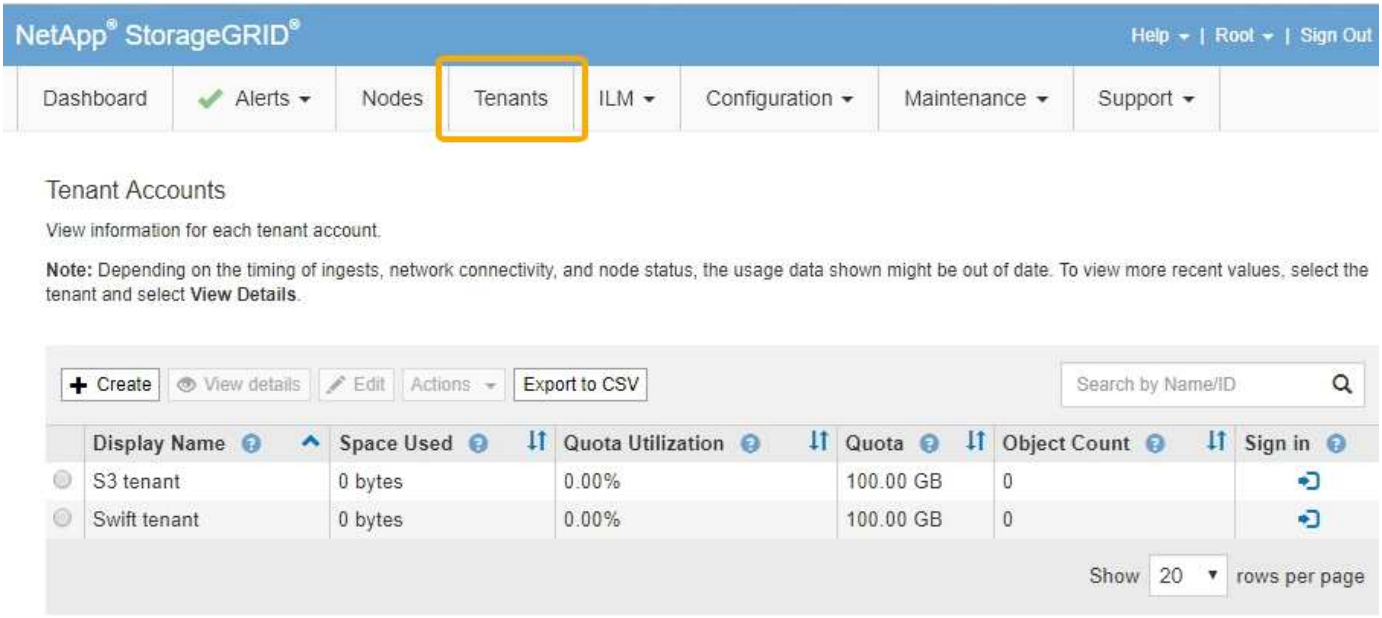
"Anzeigen der Seite Knoten"

"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

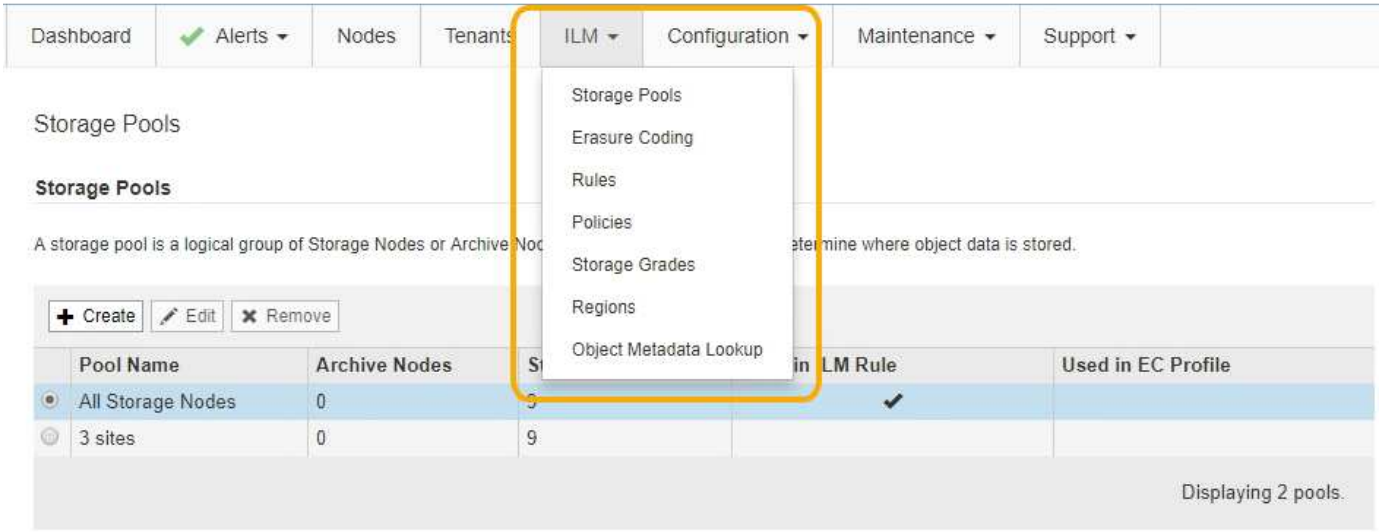
"Management von Mandanten und Client-Verbindungen"

"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"

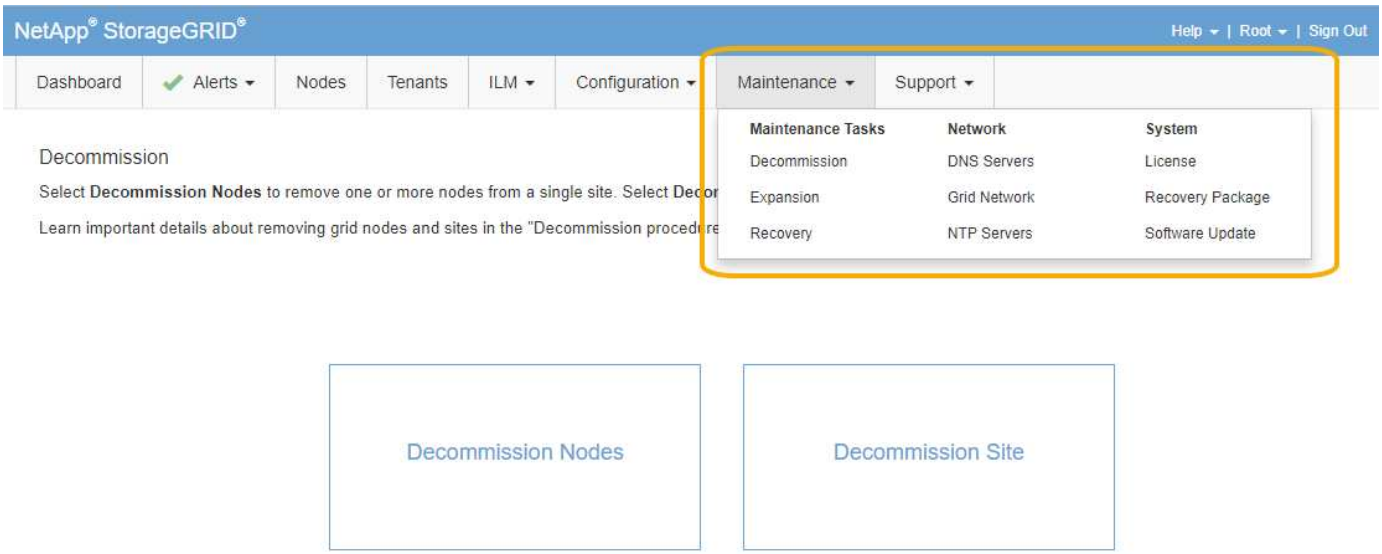
"StorageGRID verwalten"

"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"

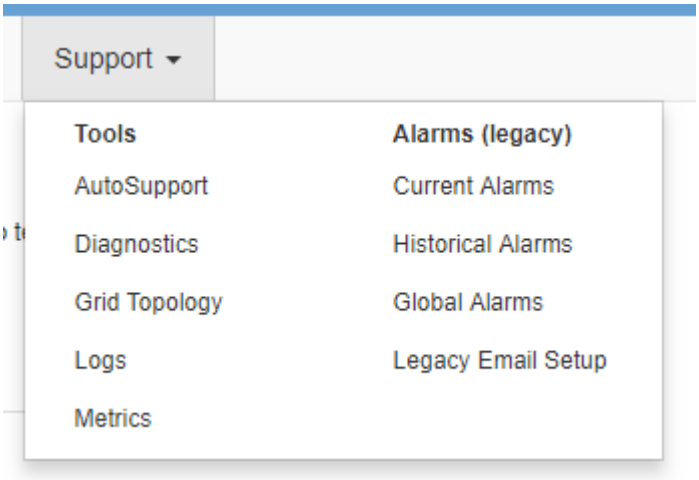
"SG6000 Storage-Appliances"

"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"

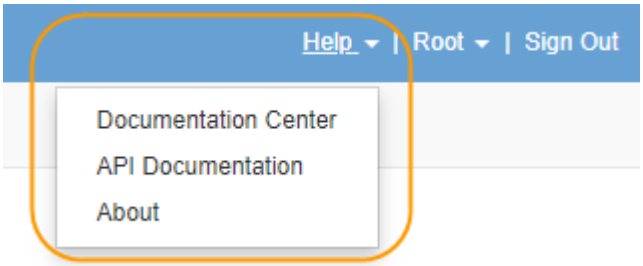
"Verwenden von StorageGRID Support-Optionen"

"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"

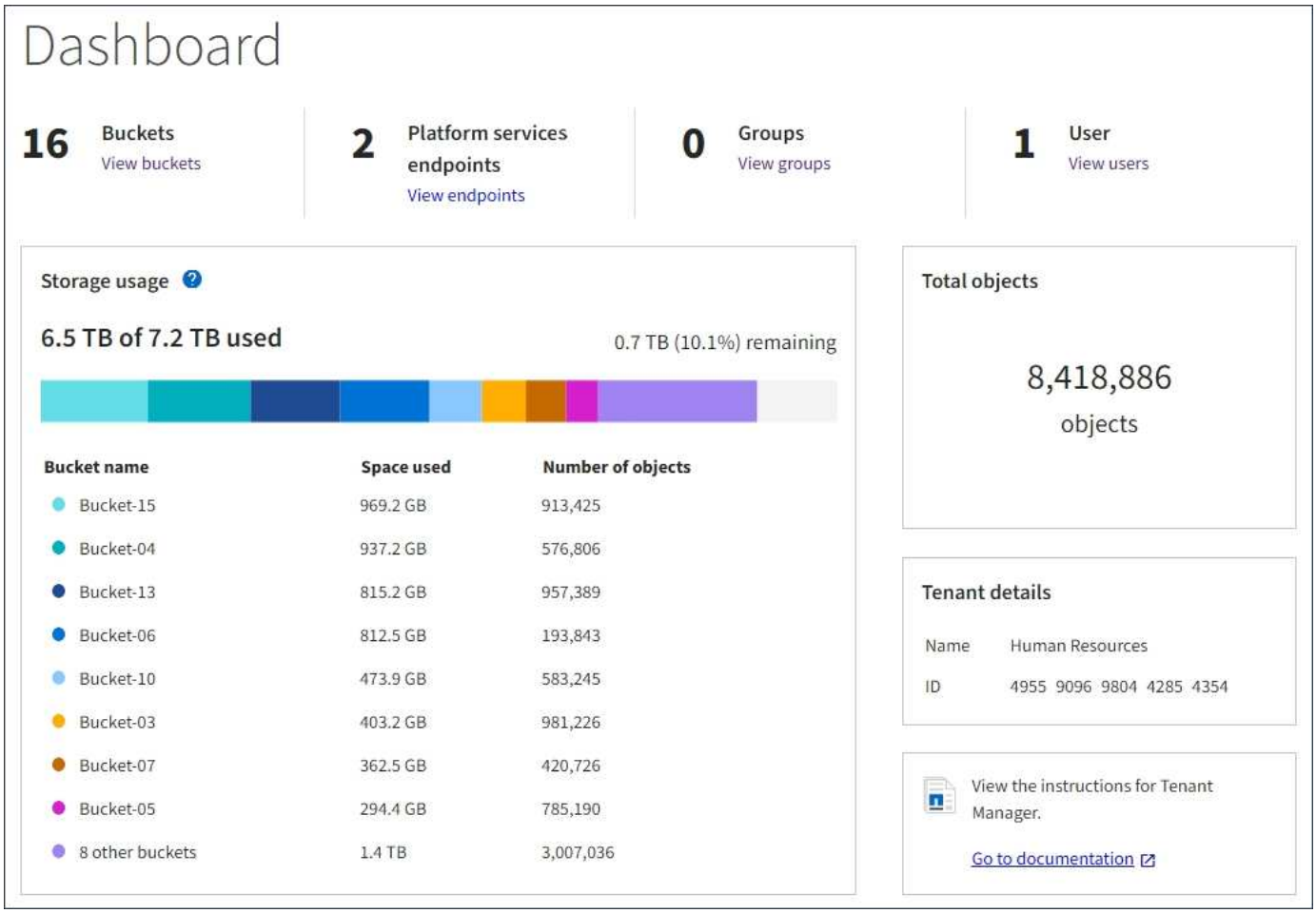
"Verwenden Sie ein Mandantenkonto"

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:

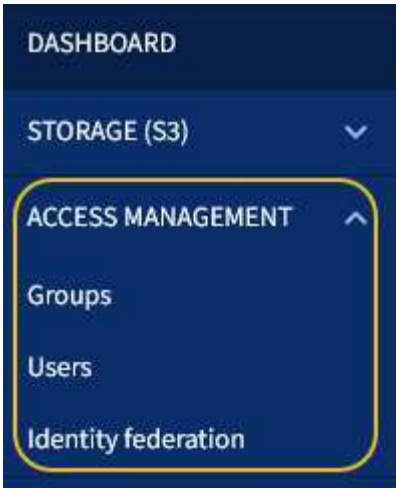
- Konfigurieren Sie S3-Ereignisbenachrichtigungen, die an einen Ziel-Service gesendet werden können, der den AWS Simple Notification Service™ (SNS) unterstützt.
- Konfigurieren Sie die CloudMirror-Replizierung, mit der Mandanten Objekte automatisch in einen externen S3-Bucket replizieren können.
- Die 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.

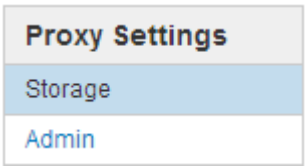
Load Balancer-Endpunkte

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.

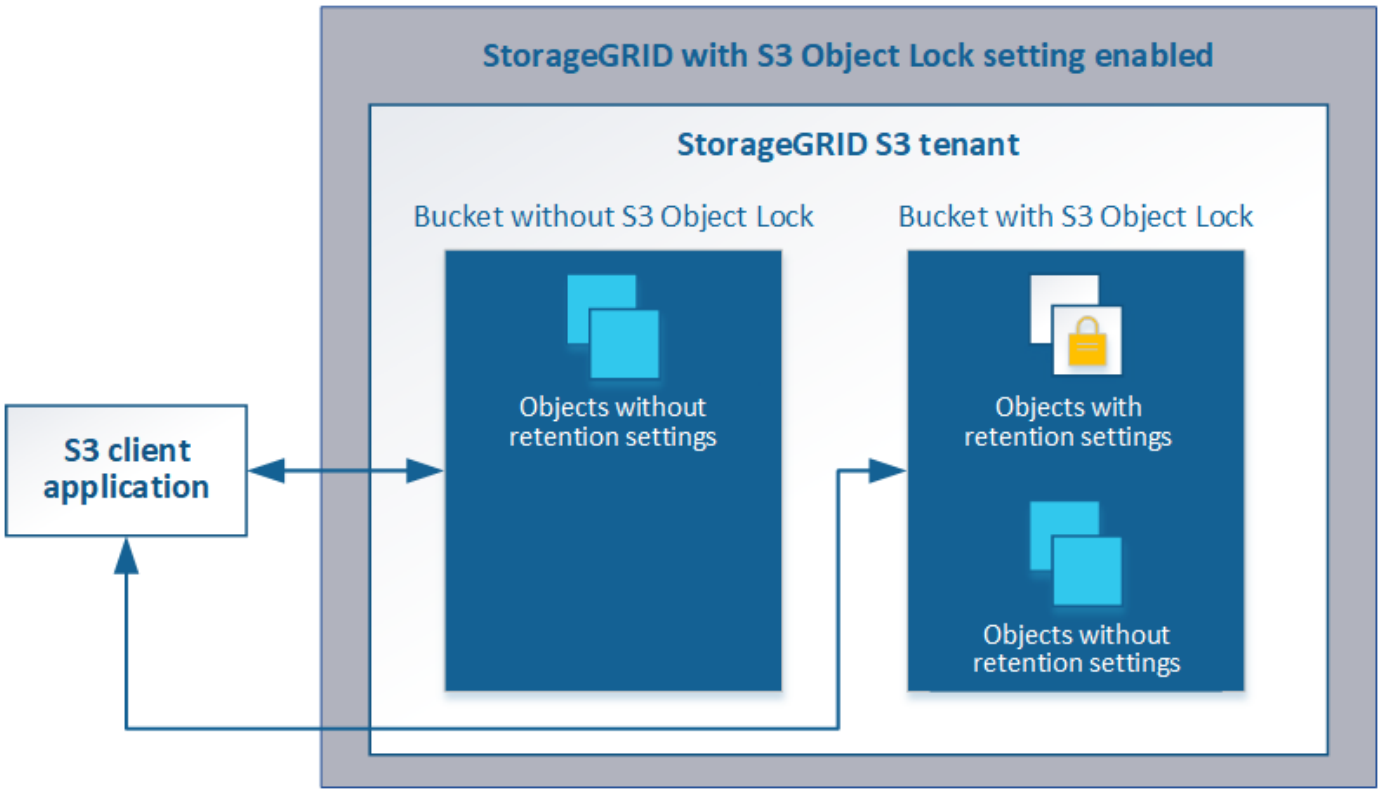
Für Schlüsselmanagement-Server

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:

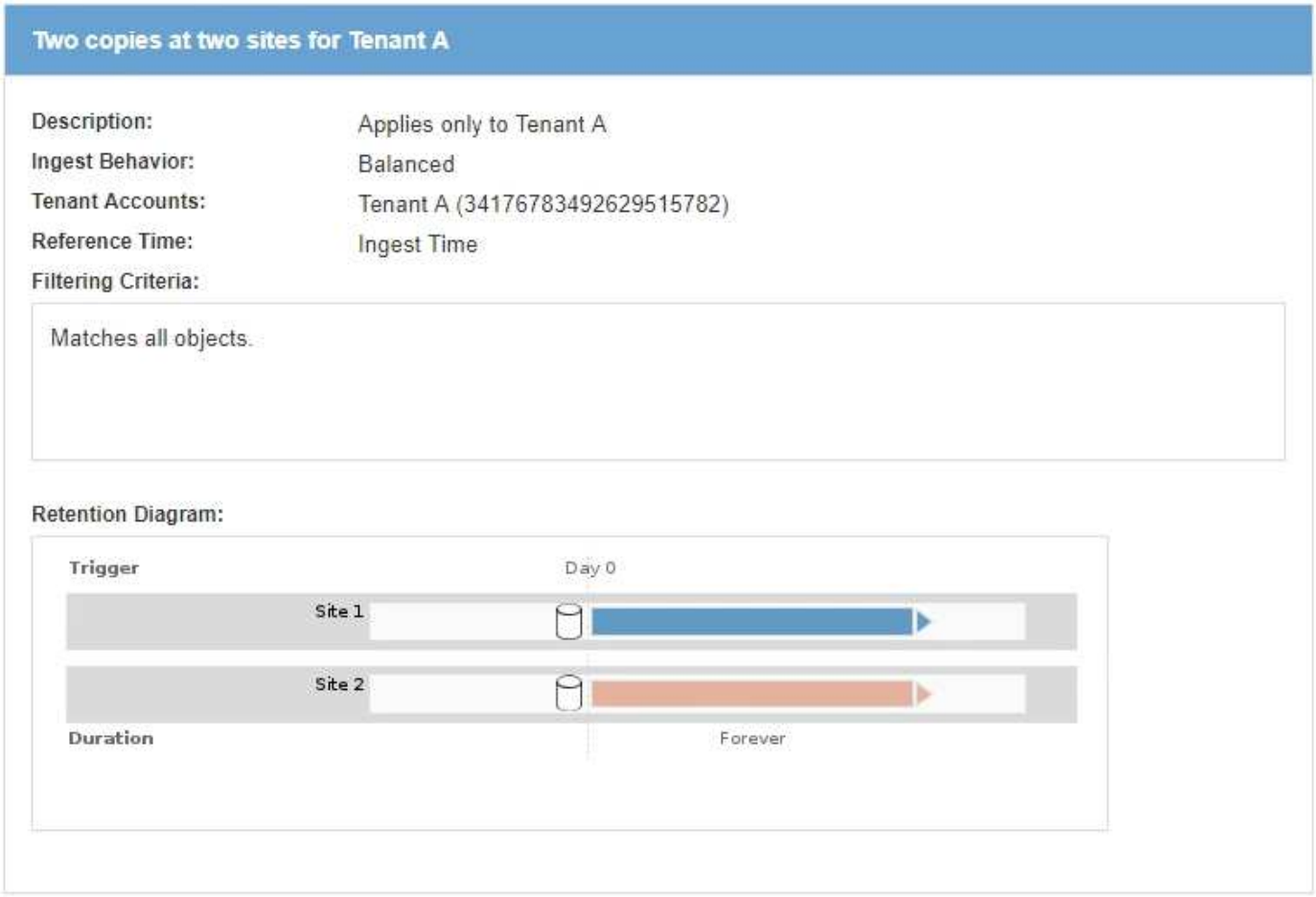
- Welche Objekte sollten gespeichert werden. Eine Regel kann auf alle Objekte angewendet werden, oder Sie können Filter angeben, um zu identifizieren, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder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

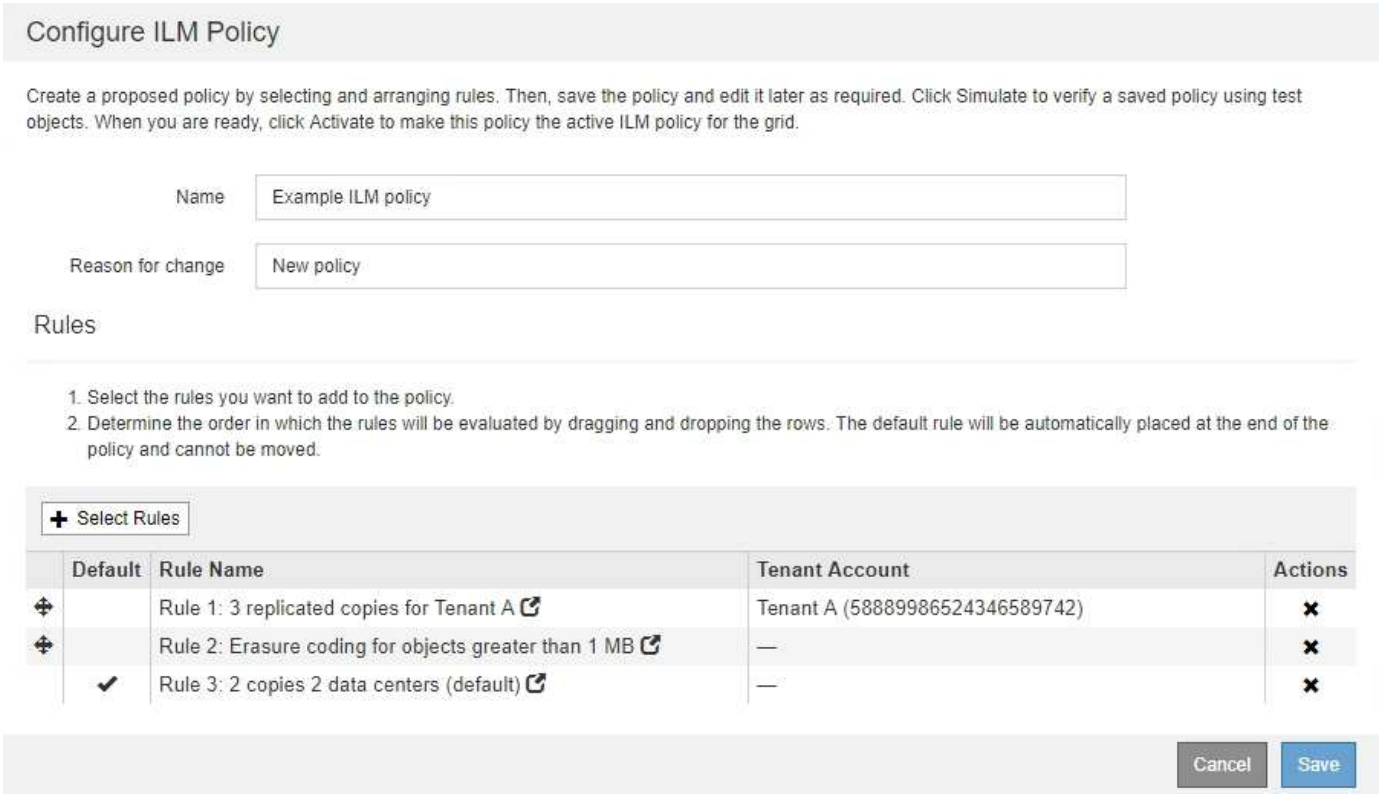
Die aktive ILM-Richtlinie für Ihr StorageGRID System steuert die Platzierung, Dauer und Datensicherung aller Objekte.

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

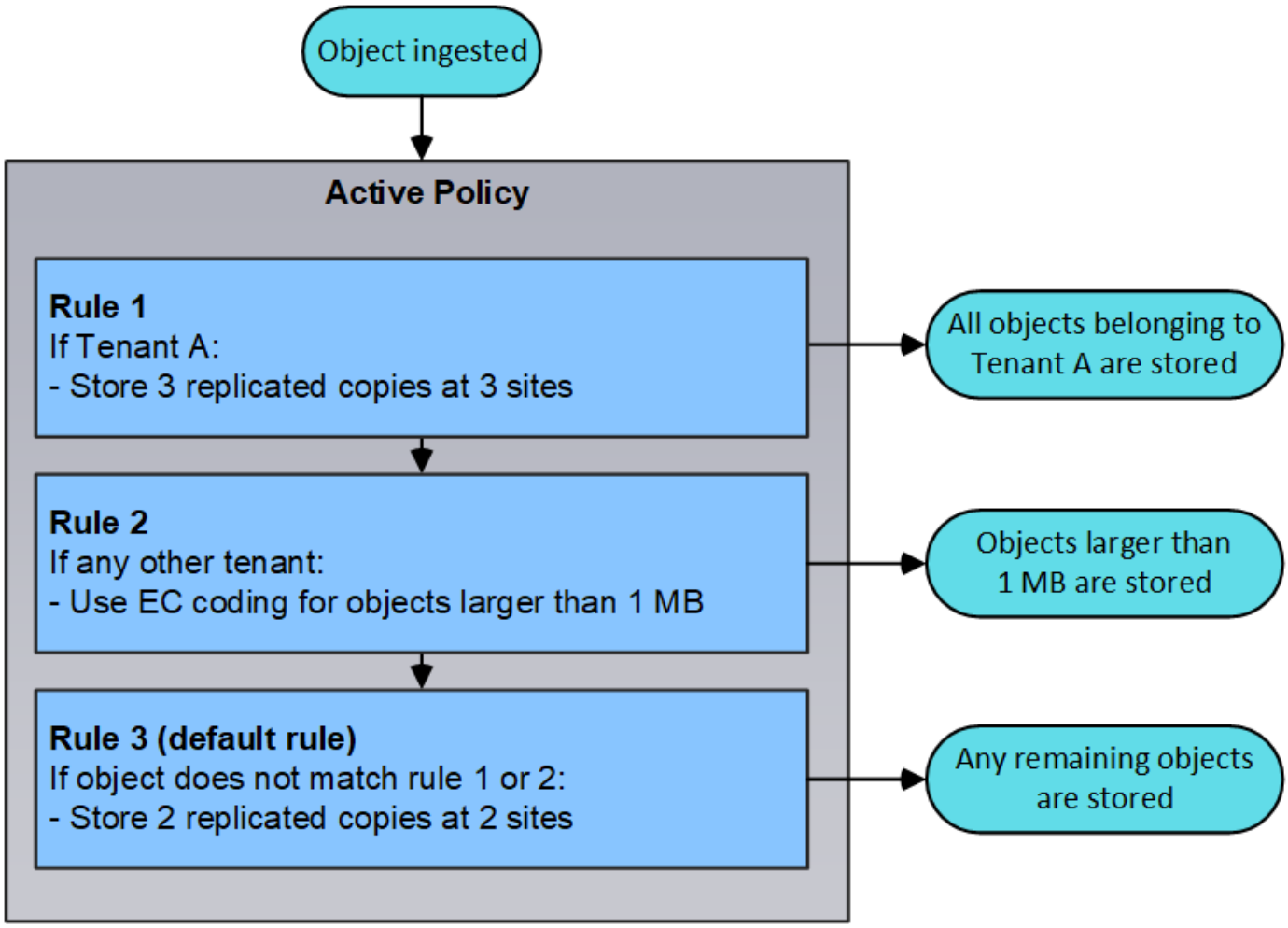
In diesem Beispiel verwendet die ILM-Richtlinie drei ILM-Regeln.



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"

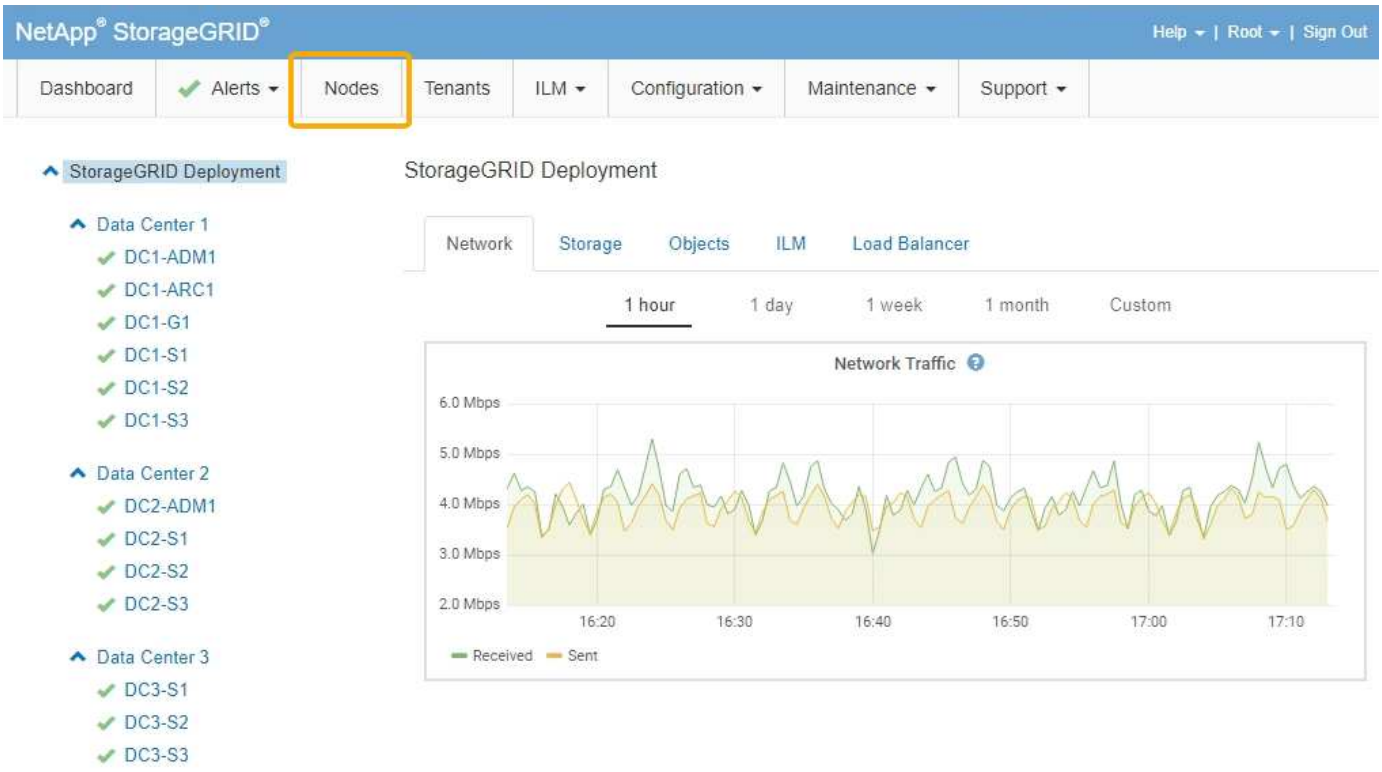
Monitoring der StorageGRID Vorgänge

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

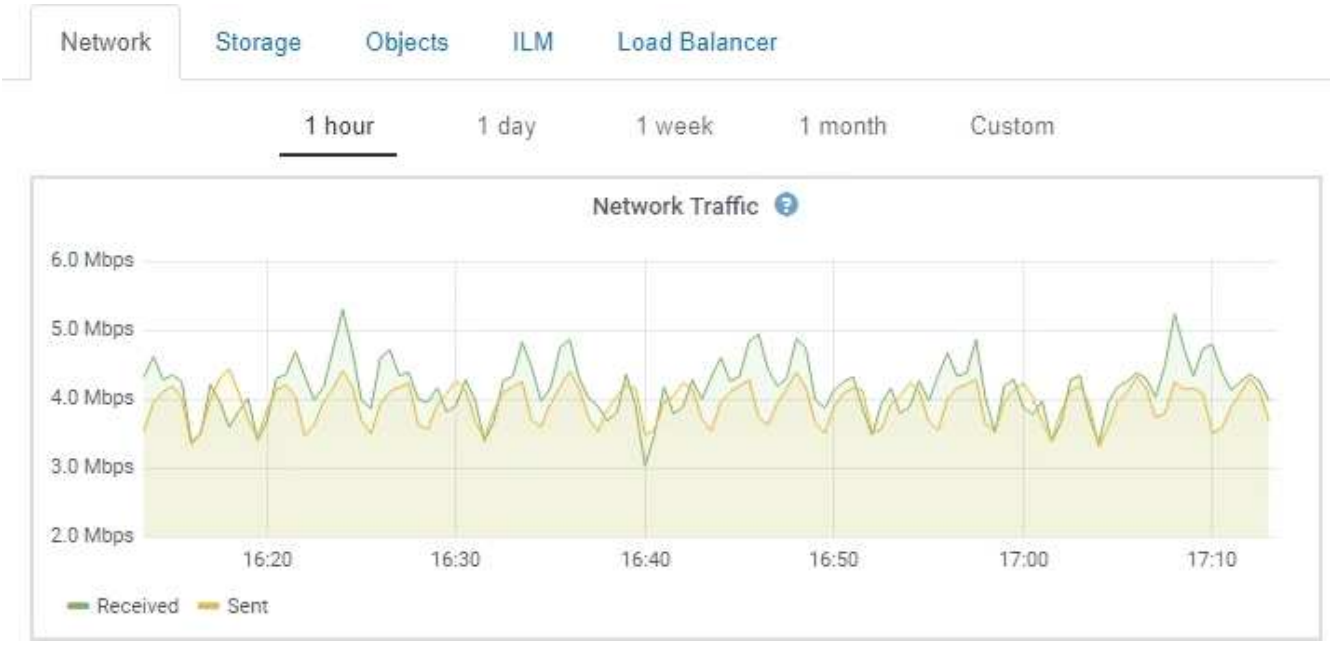
Registerkartenname	Beschreibung	Enthalten für
SANtricity System Manager	Zugriff auf SANtricity System Manager Vom SANtricity System Manager können Sie die Hardware-Diagnose und Umgebungsinformationen für den Storage Controller sowie Probleme im Zusammenhang mit den Laufwerken überprüfen.	Nodes von Storage-Appliances **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"

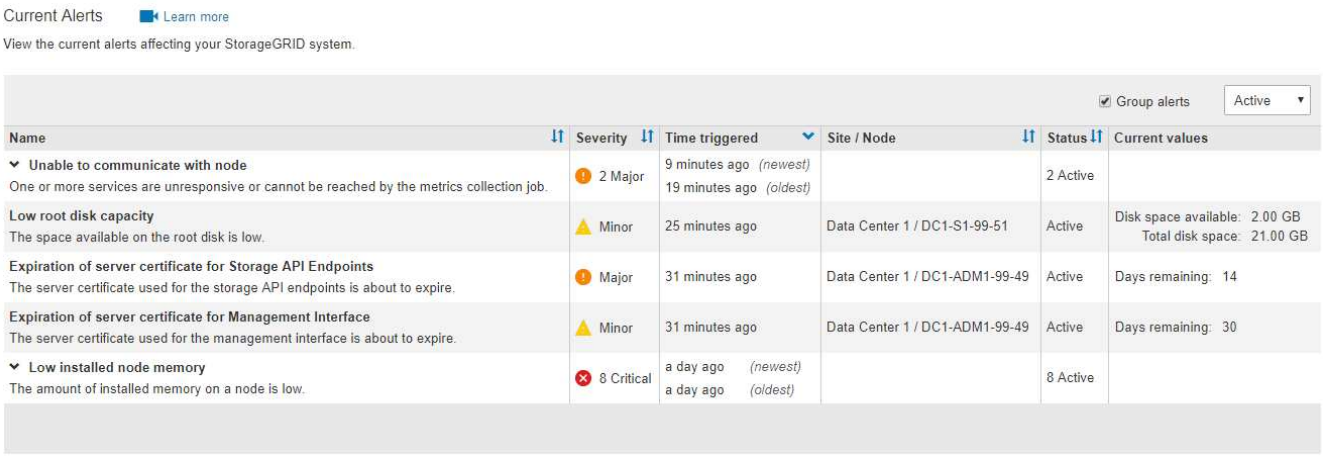
Monitoring und Management von Warnmeldungen

Das Warnsystem bietet eine benutzerfreundliche Oberfläche zum Erkennen, Bewerten

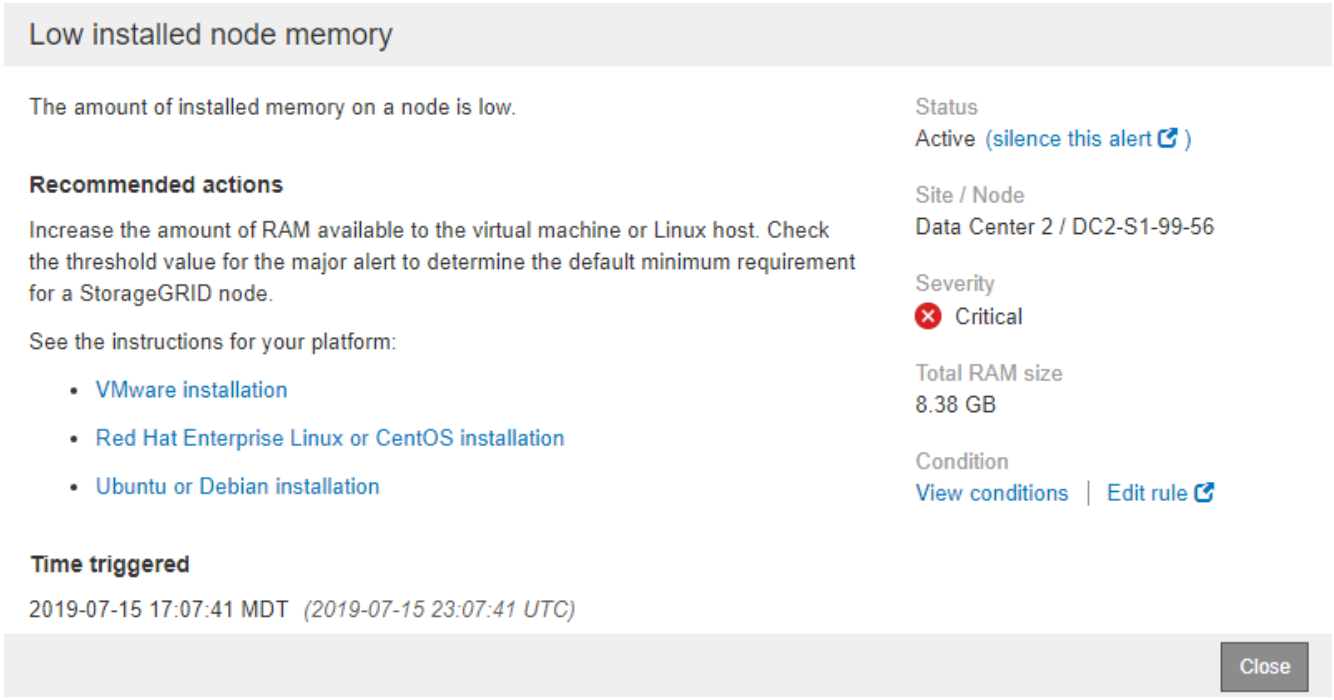
und Beheben von Problemen, die während des StorageGRID-Betriebs auftreten können.

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.

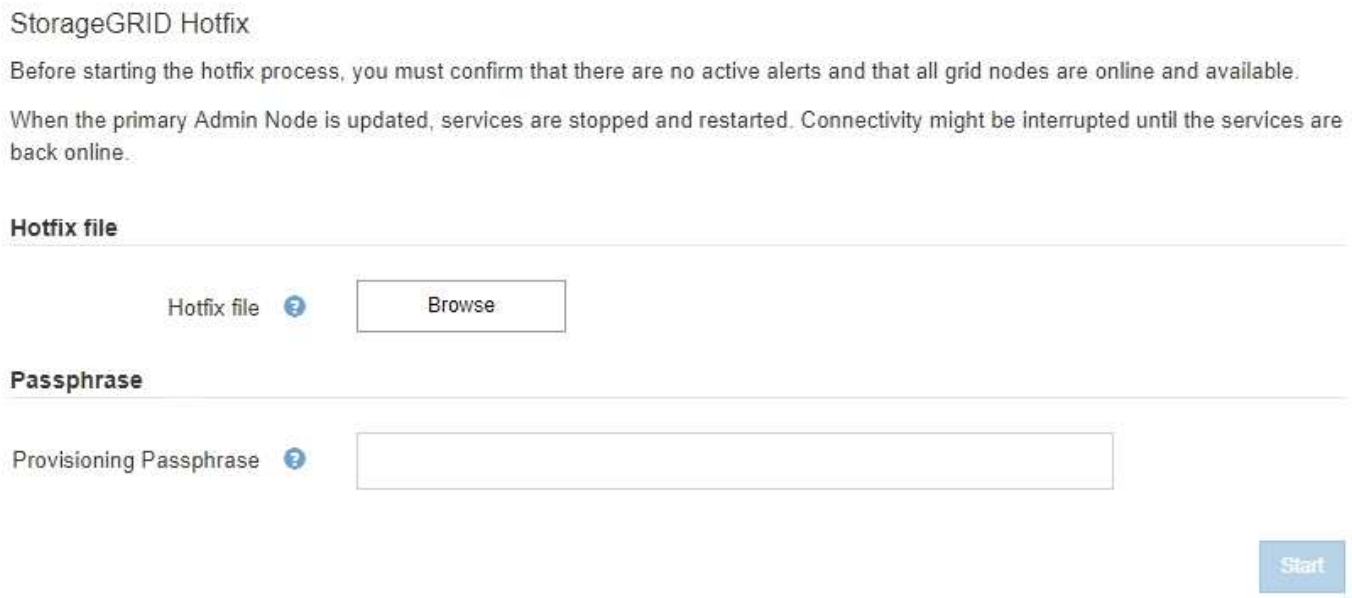
Bei einem StorageGRID Software-Upgrade können Client-Applikationen weiterhin Objektdaten aufnehmen und abrufen.

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.



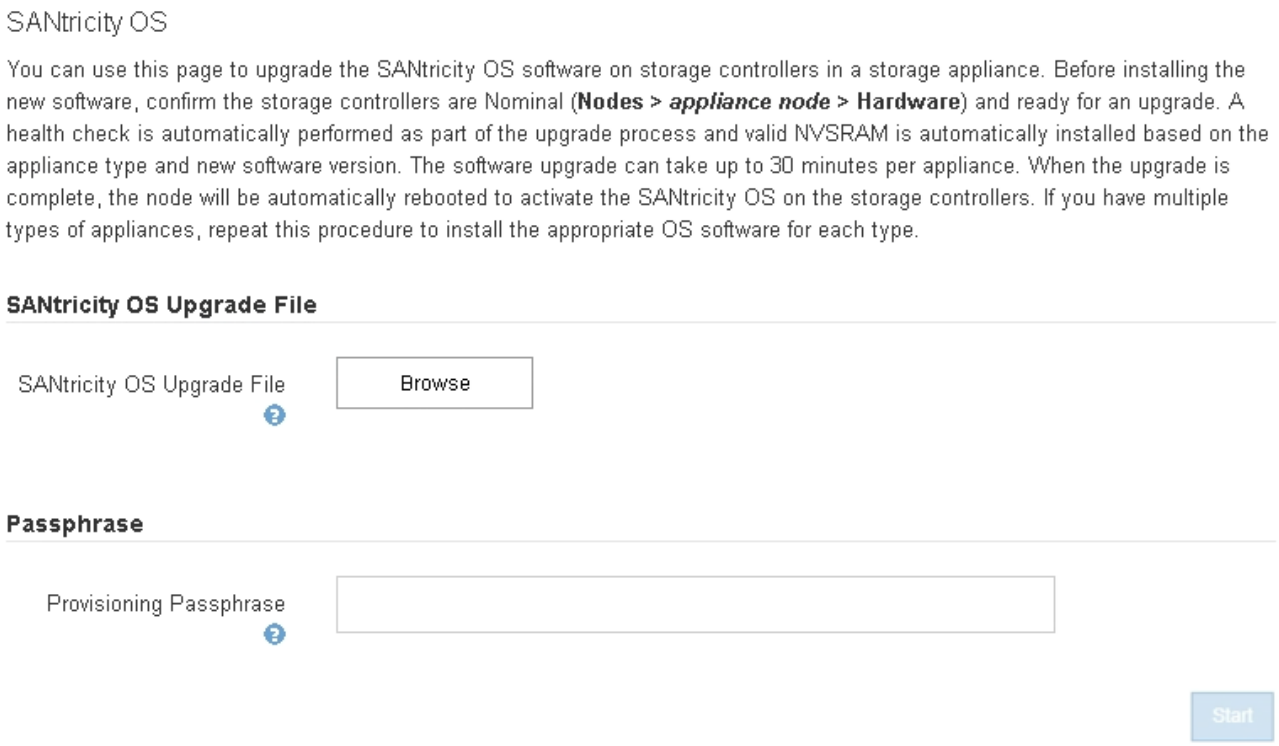
Der Hotfix wird zuerst auf den primären Admin-Knoten angewendet. Anschließend müssen Sie die Anwendung des Hotfix für andere Grid-Knoten genehmigen, bis alle Knoten im StorageGRID-System dieselbe Softwareversion ausführen. Sie können die Genehmigungssequenz anpassen, indem Sie auswählen, ob einzelne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

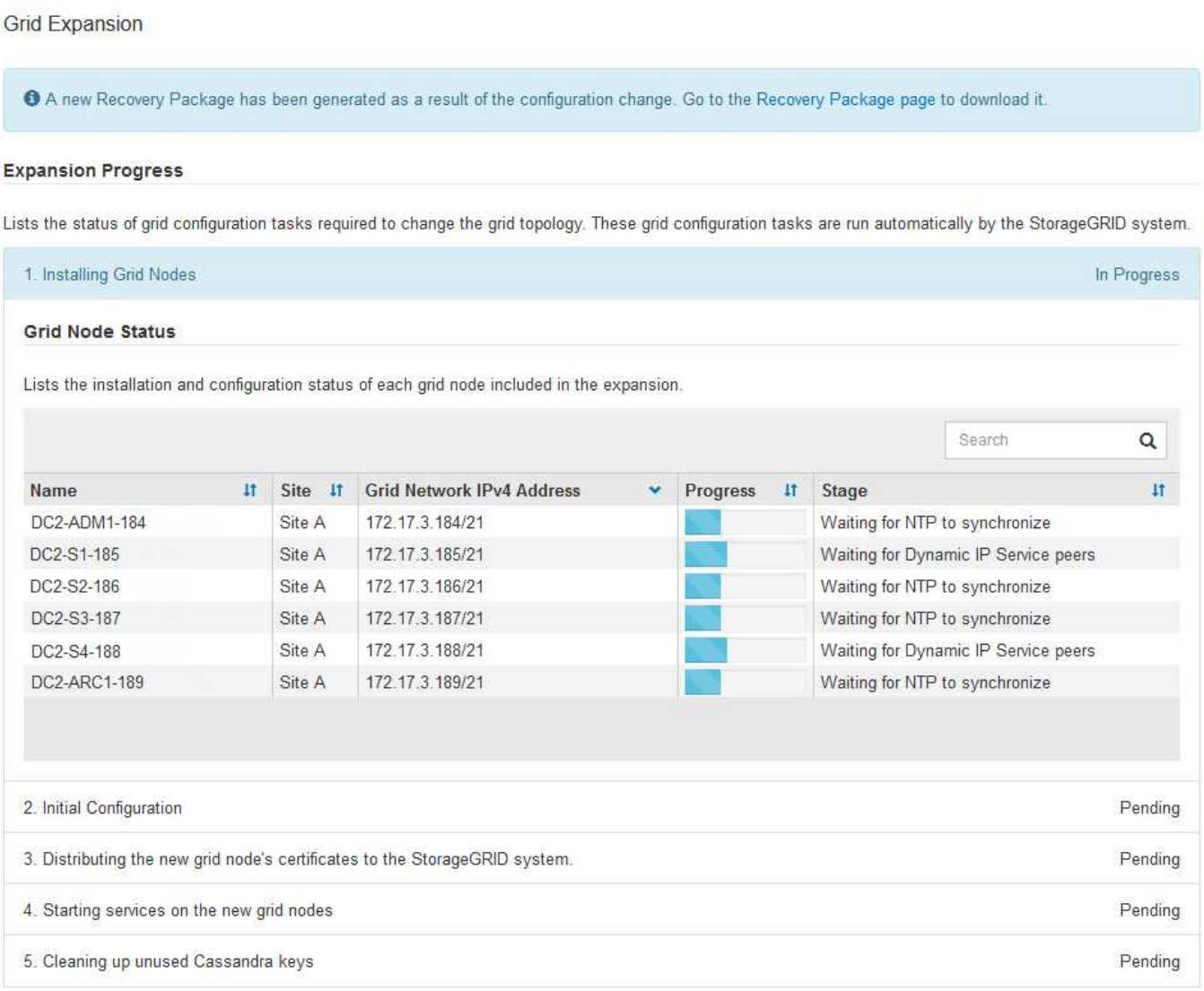


Nach dem Hochladen der Datei können Sie das Upgrade auf einzelnen Storage-Nodes oder allen Nodes genehmigen. Die Möglichkeit, Nodes selektiv zu genehmigen, erleichtert Ihnen die Planung des Upgrades. Nachdem Sie einen Node für das Upgrade genehmigt haben, führt das System eine Zustandsprüfung durch und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

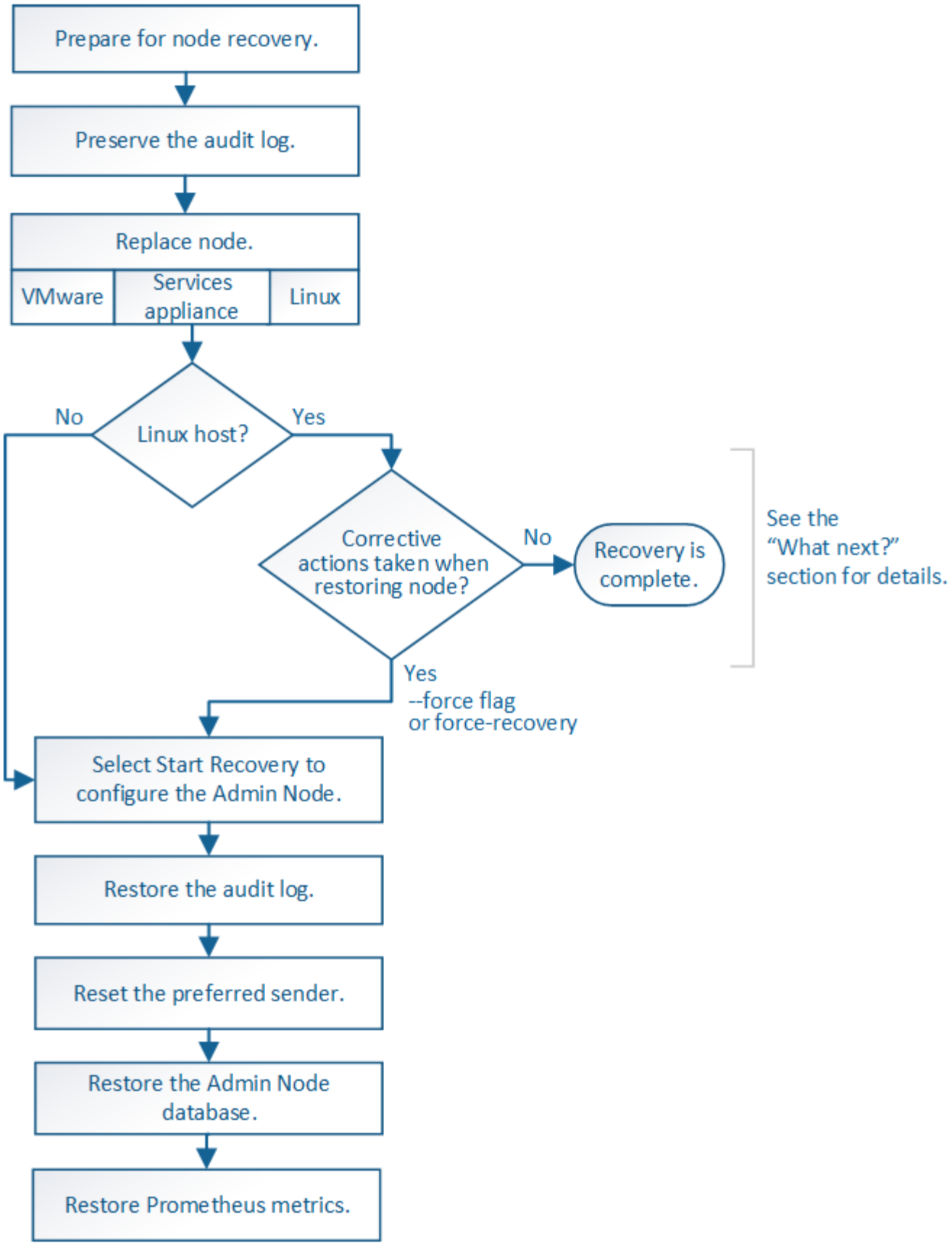


Recovery-Verfahren für die Nodes

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

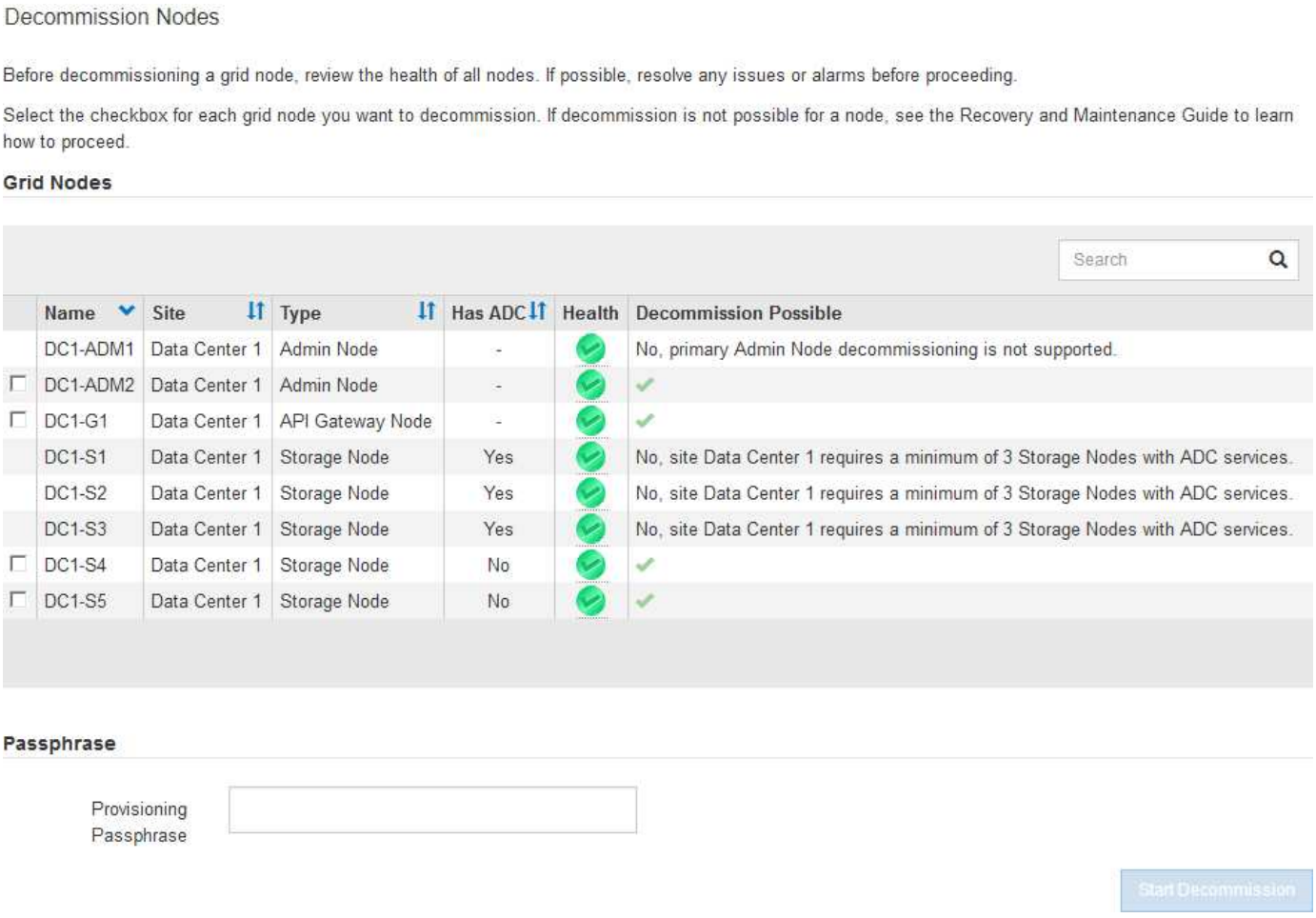
Es besteht die Möglichkeit, die Grid-Nodes oder den gesamten Datacenter-Standort vom StorageGRID-System entfernt zu werden.

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"

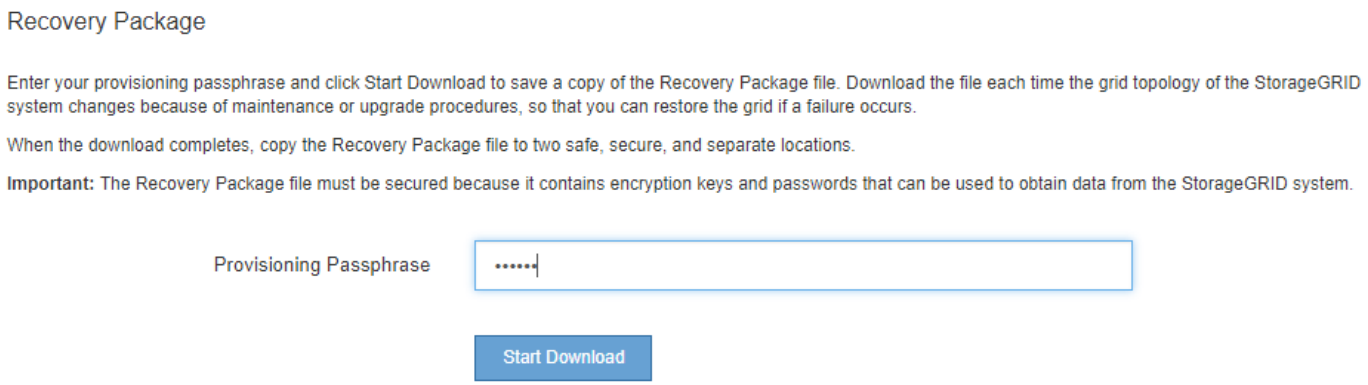
Herunterladen des Wiederherstellungspakets

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

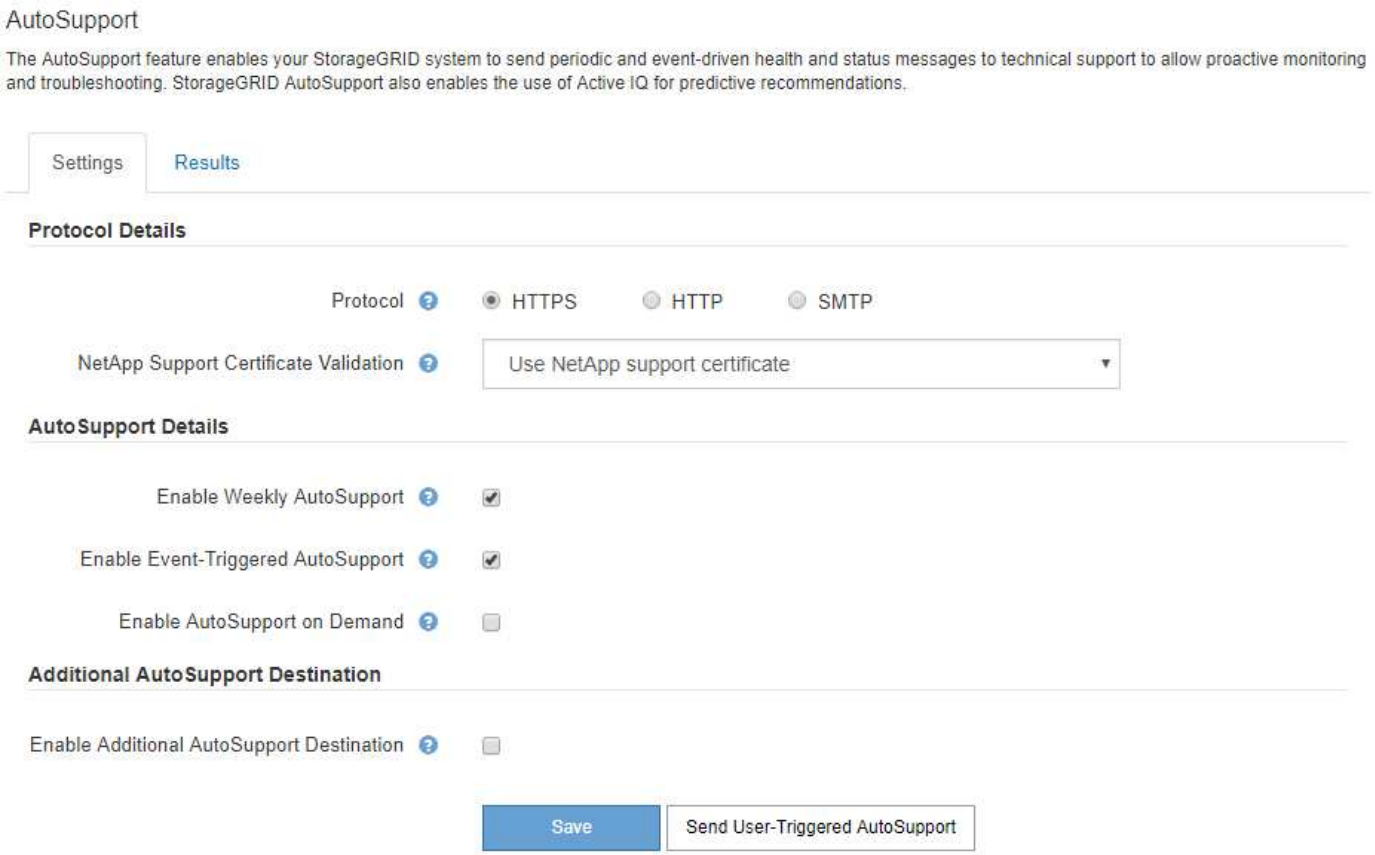
Active IQ ist ein Cloud-basierter digitaler Berater, der prädiktive Analysen und Community-Wissen aus der installierten Basis von NetApp nutzt. Kontinuierliche Risikobewertungen, prädiktive Warnungen, beschreibende Tipps und automatisierte Aktionen helfen Ihnen, Probleme zu vermeiden, bevor sie auftreten.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

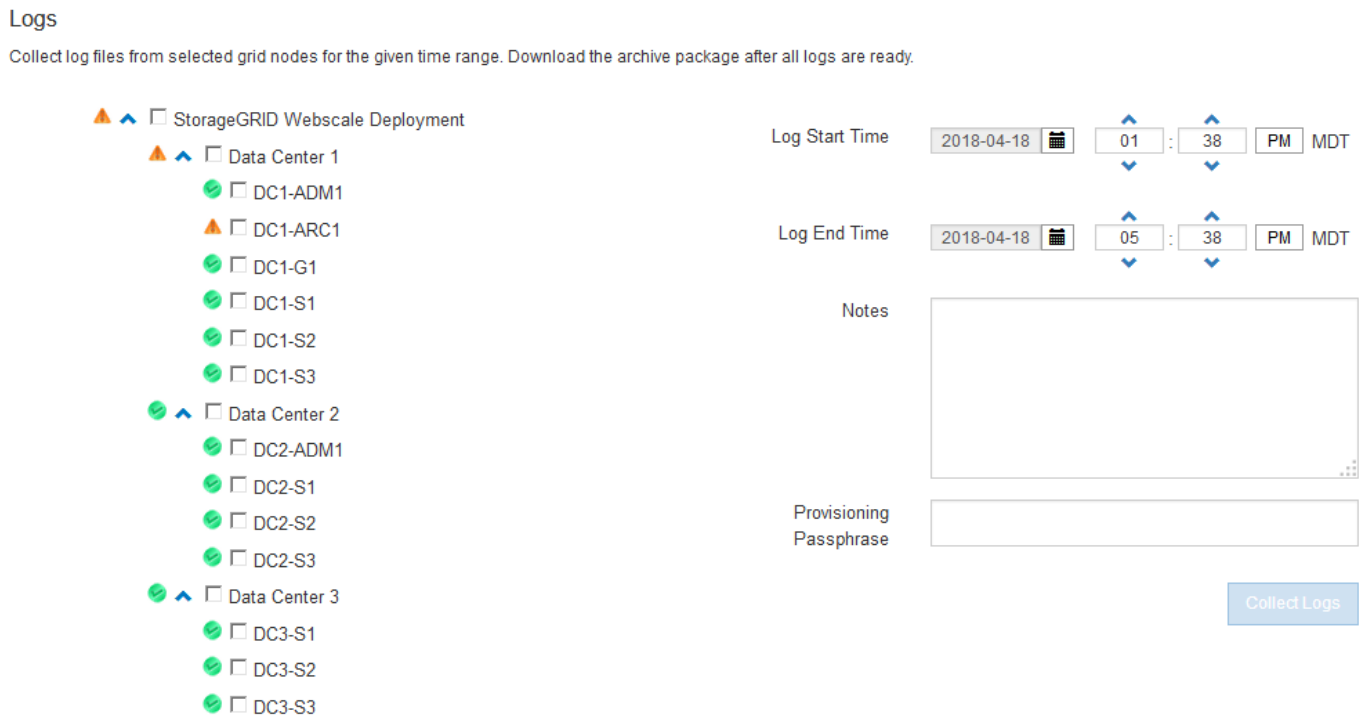
"Netzwerkeinstellungen werden konfiguriert"

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

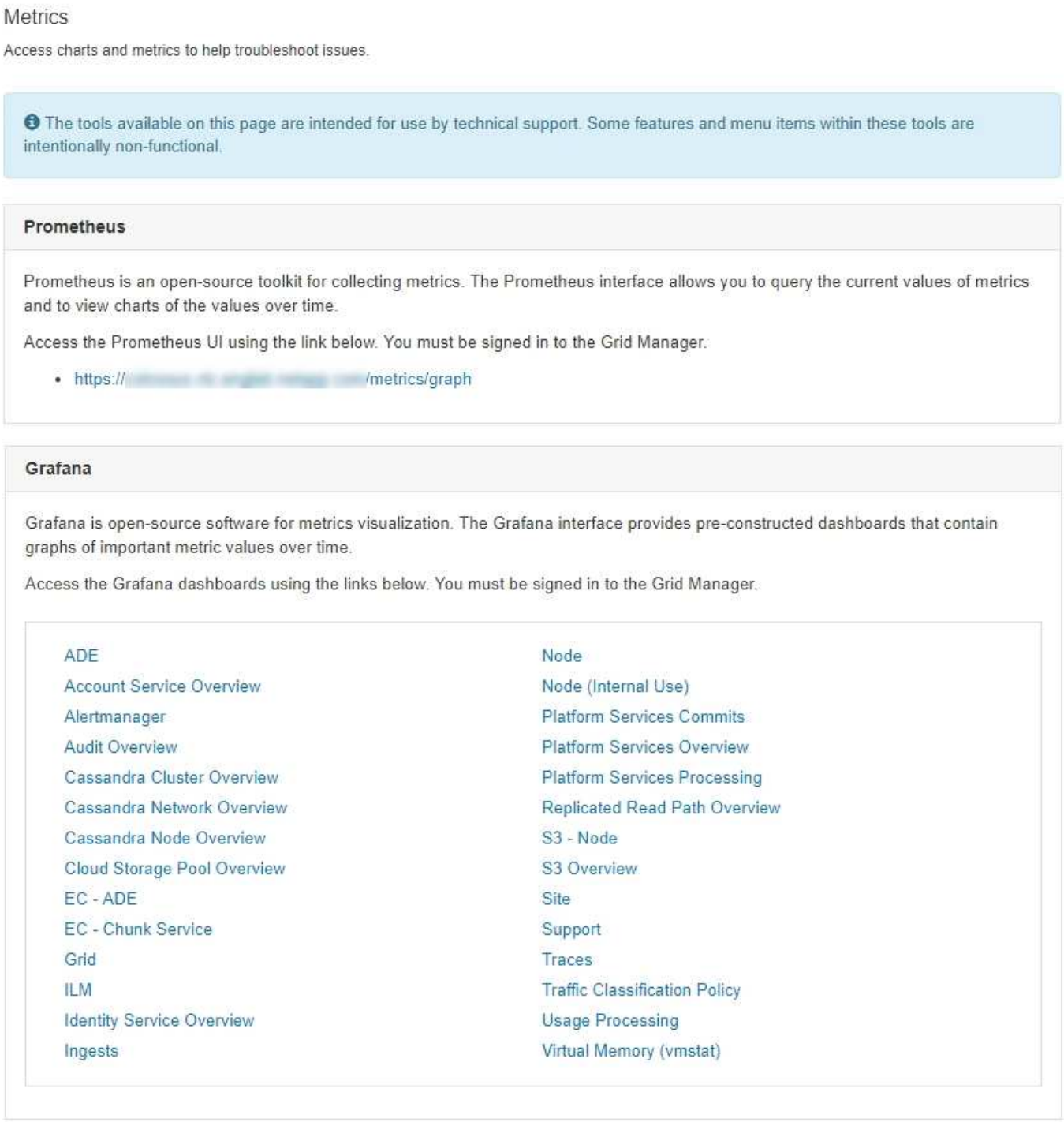
Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte

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

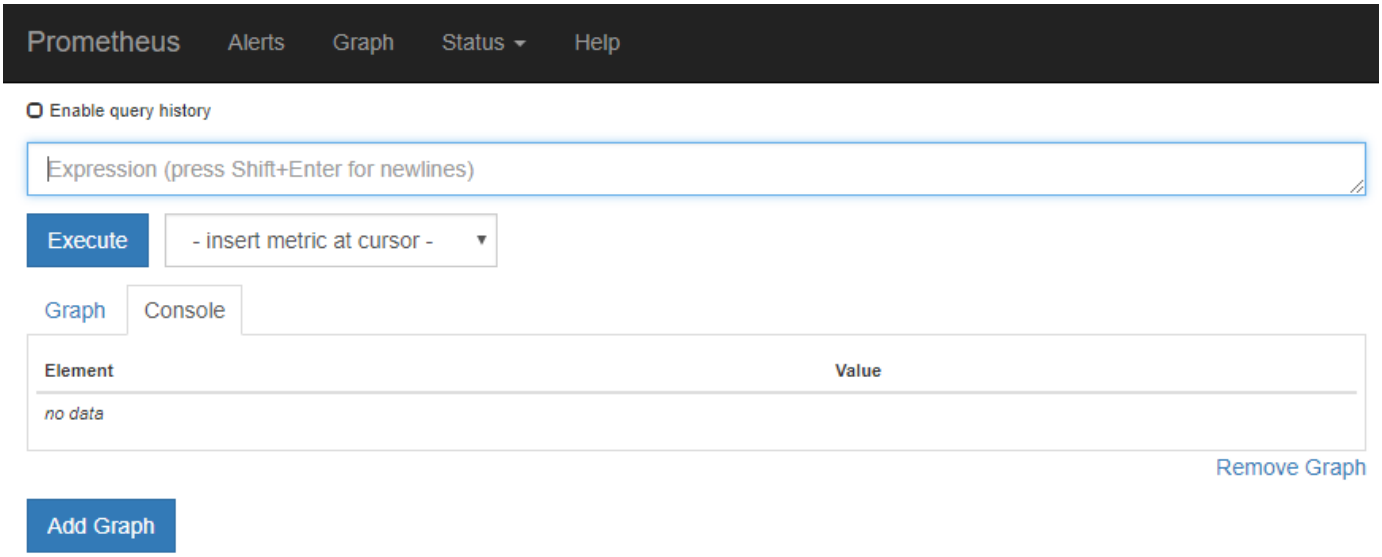
Seite „Kennzahlen“

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.

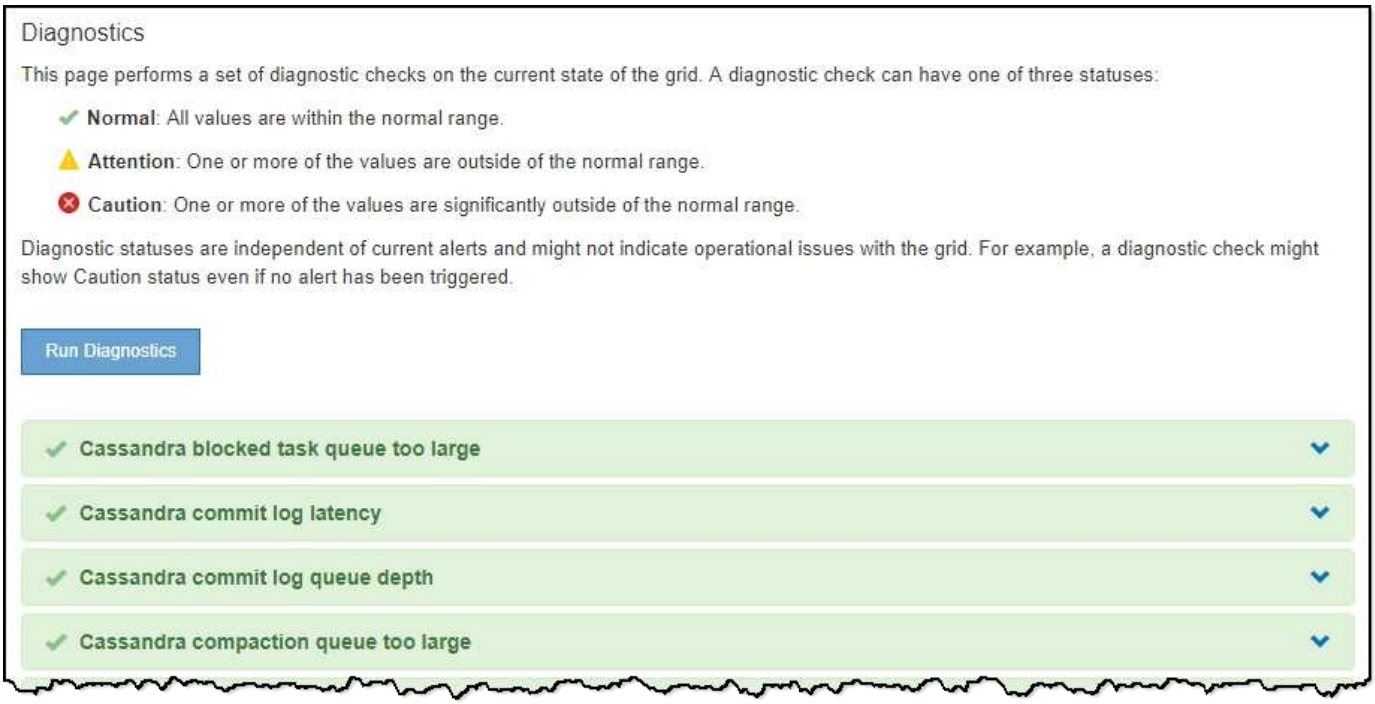


Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

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

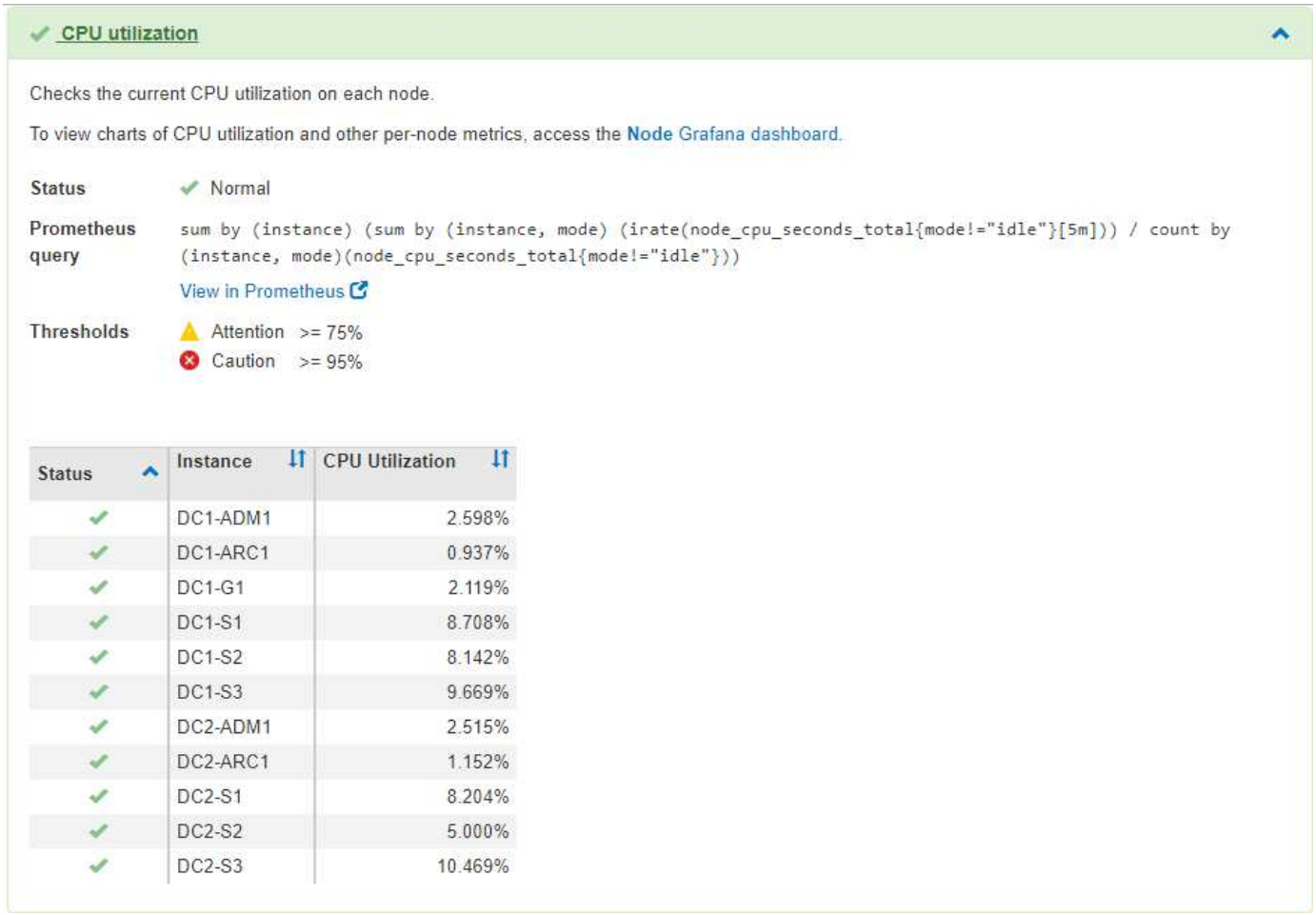
Diagnoseseite

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.

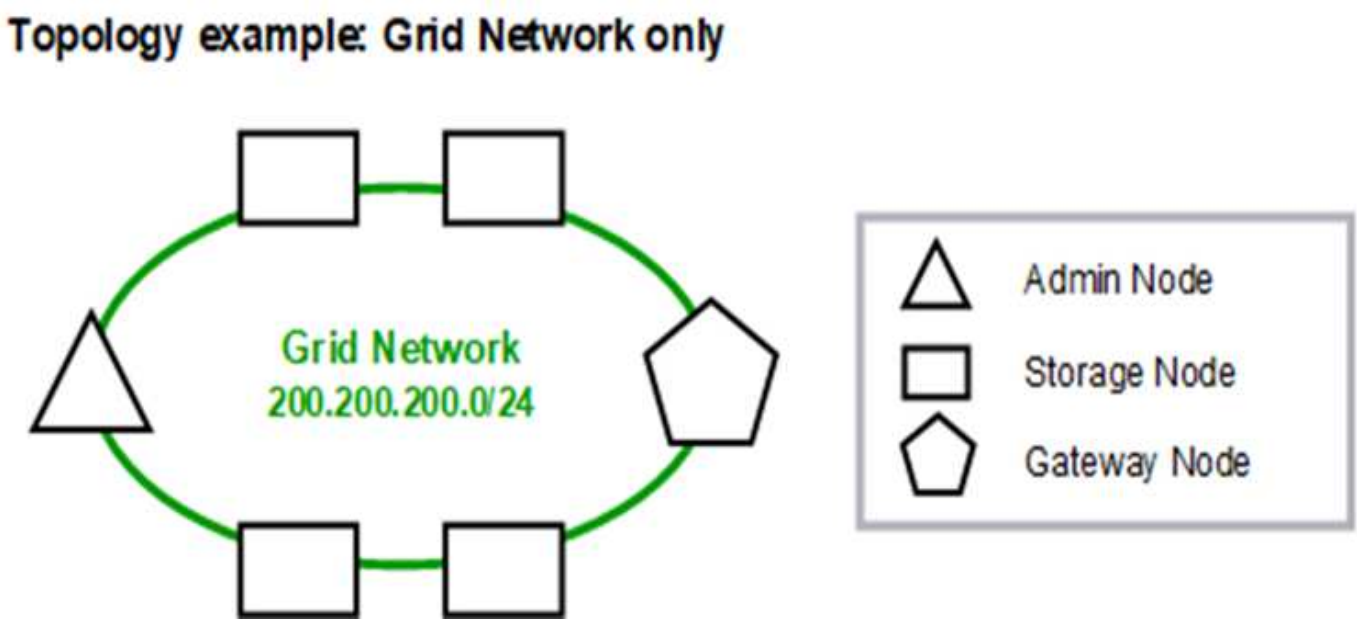
Wenn Sie das Grid-Netzwerk konfigurieren, stellen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Node ein.

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

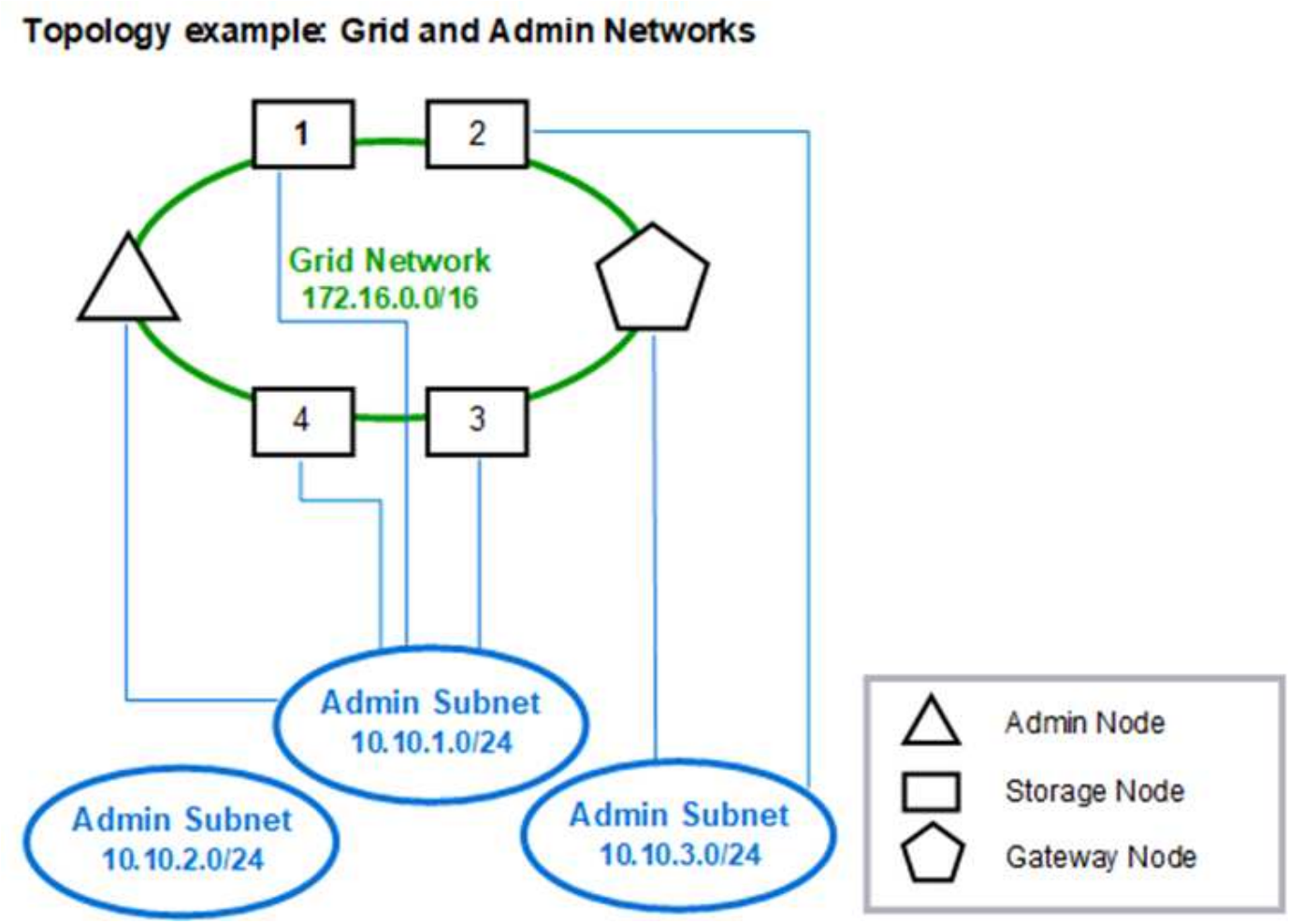
Die Verwendung eines Admin-Netzwerks ist optional. Eine Möglichkeit, wie Sie ein Admin-Netzwerk und ein Grid-Netzwerk verwenden können, besteht darin, ein

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

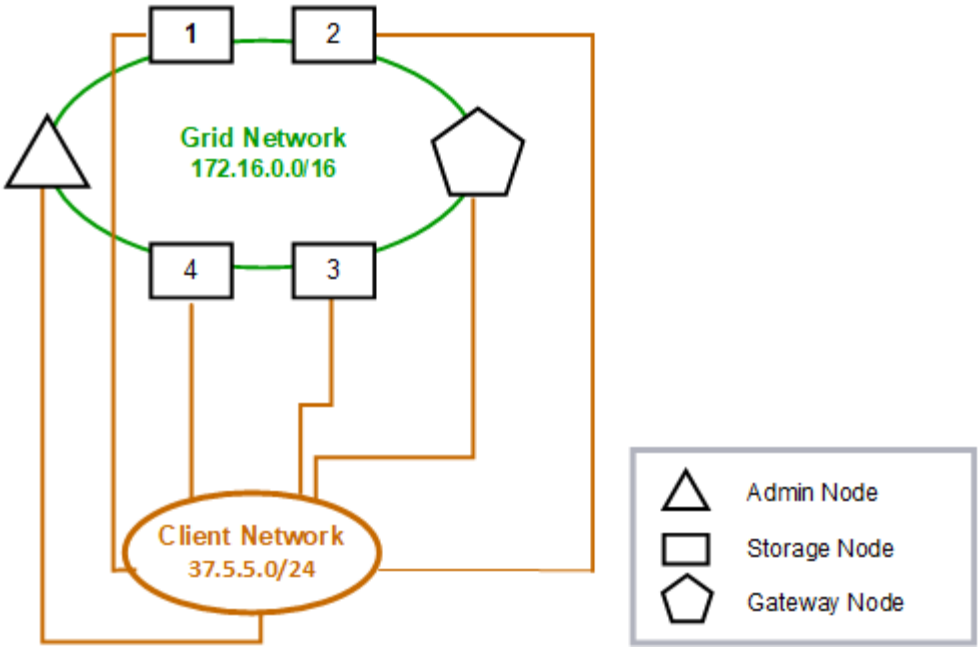
Ein Client-Netzwerk ist optional. Über ein Client-Netzwerk kann der Netzwerk-Traffic des Clients (z. B. S3 und Swift) vom internen Grid-Datenverkehr getrennt werden, wodurch die Sicherheit des Grid-Netzwerks erhöht wird. Wenn das Admin-Netzwerk nicht konfiguriert ist, kann der administrative Datenverkehr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

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

System Generated

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

Topologie für alle drei Netzwerke

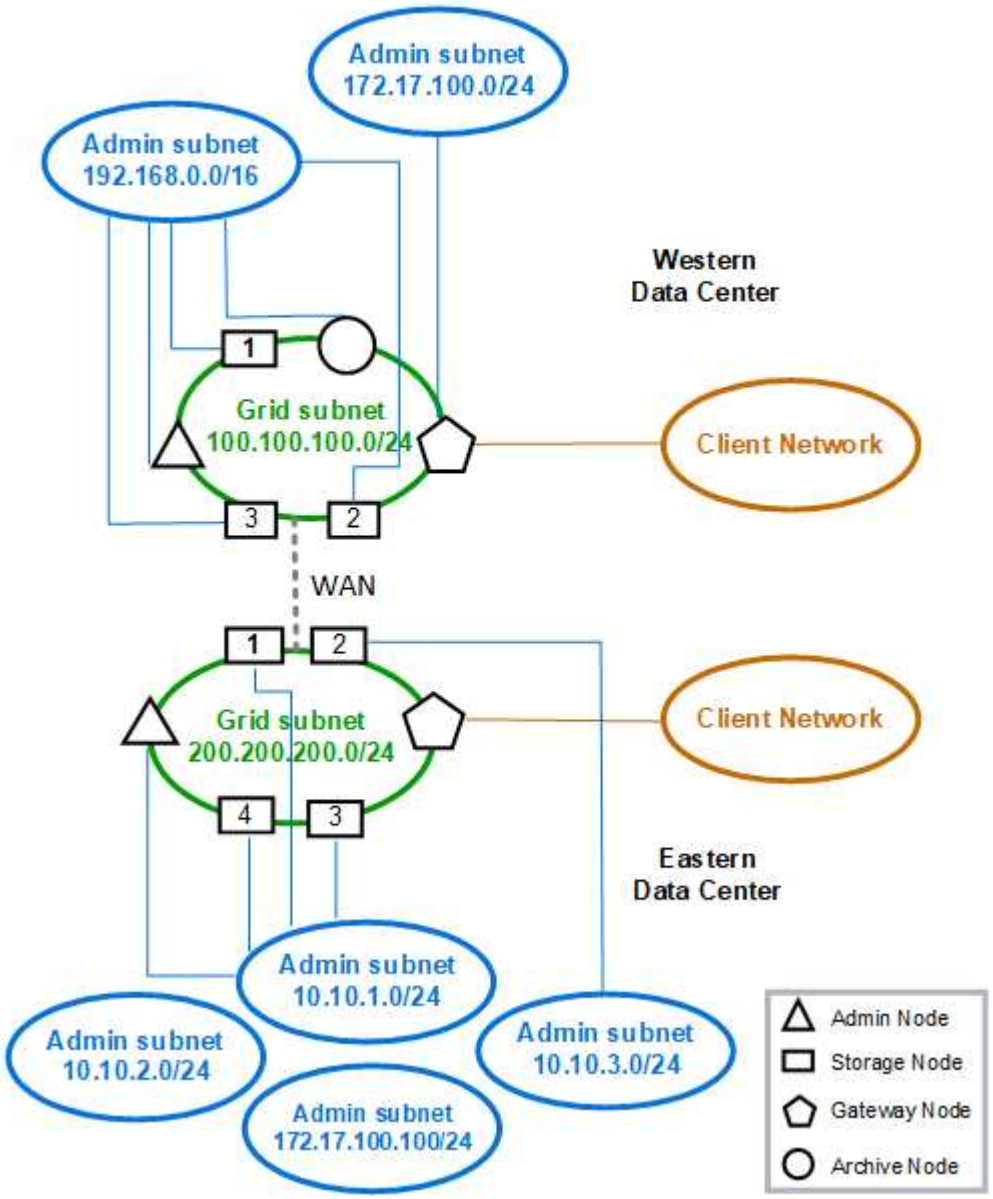
Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, eingeschränkten standortspezifischen Admin-Netzwerken und

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"