Los geht's

StorageGRID software

NetApp
January 21, 2026

Inhalt

Erste Schritte mit einem StorageGRID System . . . 1
Weitere Informationen zu StorageGRID . . . 1
Was ist StorageGRID? . . . 1
Hybrid Clouds mit StorageGRID . . . 3
StorageGRID Architektur und Netzwerktopologie . . . 4
Grid Nodes und Services . . . 7
Managen von Daten mit StorageGRID . . . 20
Entdecken Sie StorageGRID . . . 31
Netzwerkrichtlinien . . . 39
Netzwerkrichtlinien für StorageGRID . . . 39
StorageGRID-Netzwerktypen . . . 40
Beispiele für Netzwerktopologie . . . 44
Netzwerkanforderungen für StorageGRID . . . 50
Netzwerkspezifische Anforderungen für StorageGRID . . . 52
Implementierungs-spezifische Netzwerküberlegungen . . . 54
Netzwerkinstallation und Bereitstellung für StorageGRID . . . 57
Richtlinien nach der Installation für StorageGRID . . . 58
Referenz für Netzwerk-Ports . . . 59
Schnellstart für StorageGRID . . . 67

Erste Schritte mit einem StorageGRID System

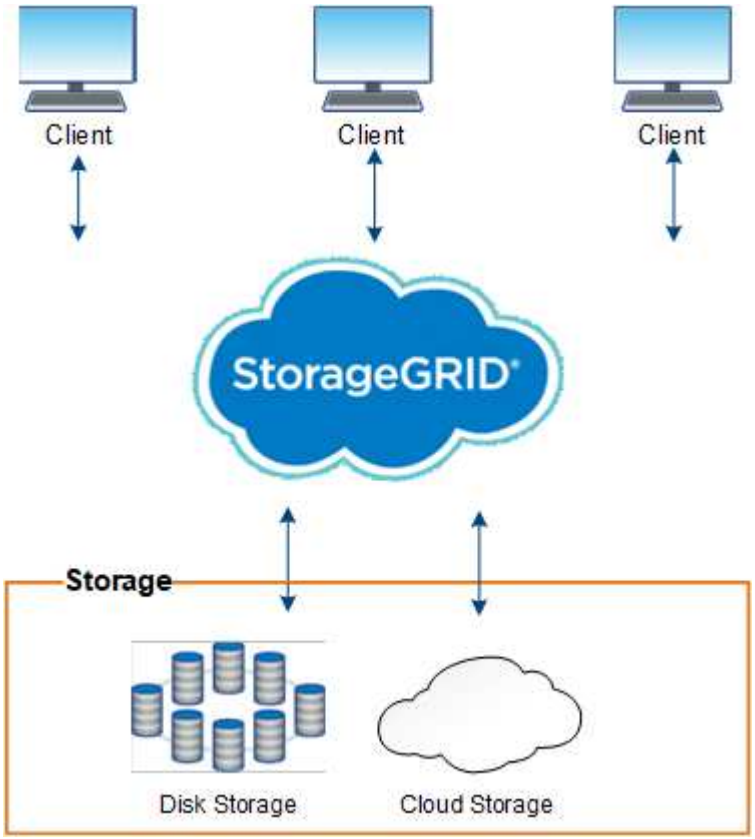
Weitere Informationen zu StorageGRID

Was ist StorageGRID?

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

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

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



Unterstützung für Archive Nodes wurde entfernt. Das Verschieben von Objekten aus einem Archive Node in ein externes Archiv-Storage-System über die S3 API wurde durch ersetzt"ILM Cloud Storage-Pools", die mehr Funktionalität bieten.

Vorteile von StorageGRID

Das StorageGRID System bietet unter anderem folgende Vorteile:

- Extrem skalierbar und leicht zu verwendende Daten-Repositorys mit geografisch verteilten Standorten für unstrukturierte Daten
- Das Standard-Objektspeicherprotokoll Simple Storage Service (S3) von Amazon Web Services.
- Hybrid Cloud-fähig: Richtlinienbasiertes Information Lifecycle Management (ILM) speichert Objekte in Public Clouds, einschließlich Amazon Web Services (AWS) und Microsoft Azure. StorageGRID Plattform-Services ermöglichen die Content-Replizierung, Ereignisbenachrichtigung und Metadatensuche von Objekten, die in Public Clouds gespeichert sind.
- Flexible Datensicherung für Langlebigkeit und Verfügbarkeit Die Daten lassen sich durch Replizierung und ein mehrstufiges Erasure Coding zur Fehlerkorrektur sichern. Überprüfung von Daten im Ruhezustand und auf der Übertragungsstrecke sorgt für Integrität für langfristige Aufbewahrung.
- Dynamisches Lifecycle Management für Daten zum Management der Storage-Kosten Sie können ILM-Regeln erstellen, die den Daten-Lebenszyklus auf Objektebene managen und Datenlokalität, Datenaufbewahrungszeit, Performance, Kosten anpassen. und Aufbewahrungszeit.
- Hochverfügbarkeit des Daten-Storage und einiger Managementfunktionen, mit integriertem Lastausgleich zur Optimierung der Datenlast über StorageGRID-Ressourcen hinweg.
- Unterstützung mehrerer Storage-Mandantenkonten, um die auf dem System gespeicherten Objekte durch unterschiedliche Einheiten zu trennen
- Zahlreiche Tools für das Monitoring des Systemzustands des StorageGRID Systems, einschließlich eines umfassenden Alarmsystems, einer grafischen Konsole und detaillierten Status für alle Knoten und Standorte
- Support für Software- oder hardwarebasierte Implementierung Sie können StorageGRID auf einer der folgenden Methoden implementieren:
  - Virtual Machines in VMware ausgeführt.
  - Container-Engines auf Linux Hosts
  - Von StorageGRID entwickelte Geräte.
    - Storage Appliances bieten Objekt-Storage.
    - Services Appliances stellen Services für die Grid-Administration und den Lastausgleich bereit.
- Erfüllen der relevanten Speicheranforderungen dieser Vorschriften:
  - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), die Börsenmitglieder, Broker oder Händler regelt.
  - Financial Industry Regulatory Authority (FINRA) Rule 4511(c), die die Format- und Medienanforderungen der SEC Rule 17a-4(f) vorgibt.
  - Commodity Futures Trading Commission (CFTC) in der Verordnung 17 CFR § 1.31(c)-(d), die den Handel mit Commodity Futures regelt.
- Unterbrechungsfreie Upgrades und Wartungsvorgänge Zugriff auf Inhalte bleibt während Upgrades, Erweiterungen, Stilllegen und Wartungsarbeiten erhalten.
- Verbundenes Identitätsmanagement. Integration in Active Directory, OpenLDAP oder Oracle Directory Service zur Benutzerauthentifizierung. Unterstützt Single Sign-On (SSO) unter Verwendung des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen StorageGRID und Active Directory Federation Services (AD FS).

Hybrid Clouds mit StorageGRID

Verwenden Sie StorageGRID in einer Hybrid-Cloud-Konfiguration, indem Sie richtlinienbasiertes Datenmanagement implementieren, um Objekte in Cloud-Storage-Pools zu speichern. Dabei werden StorageGRID Plattformservices genutzt und Daten per Tiering von ONTAP zu StorageGRID mit NetApp FabricPool verschoben.

Cloud-Storage-Pools

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

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

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

S3-Plattform-Services

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

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

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

ONTAP Daten-Tiering mit FabricPool

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

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

Verwandte Informationen

- "Was ist ein Cloud-Storage-Pool?"

- "Management von Plattform-Services"
- "Konfigurieren Sie StorageGRID für FabricPool"

StorageGRID Architektur und Netzwerktopologie

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

Erfahren Sie mehr über die"Rasterknotentypen" .

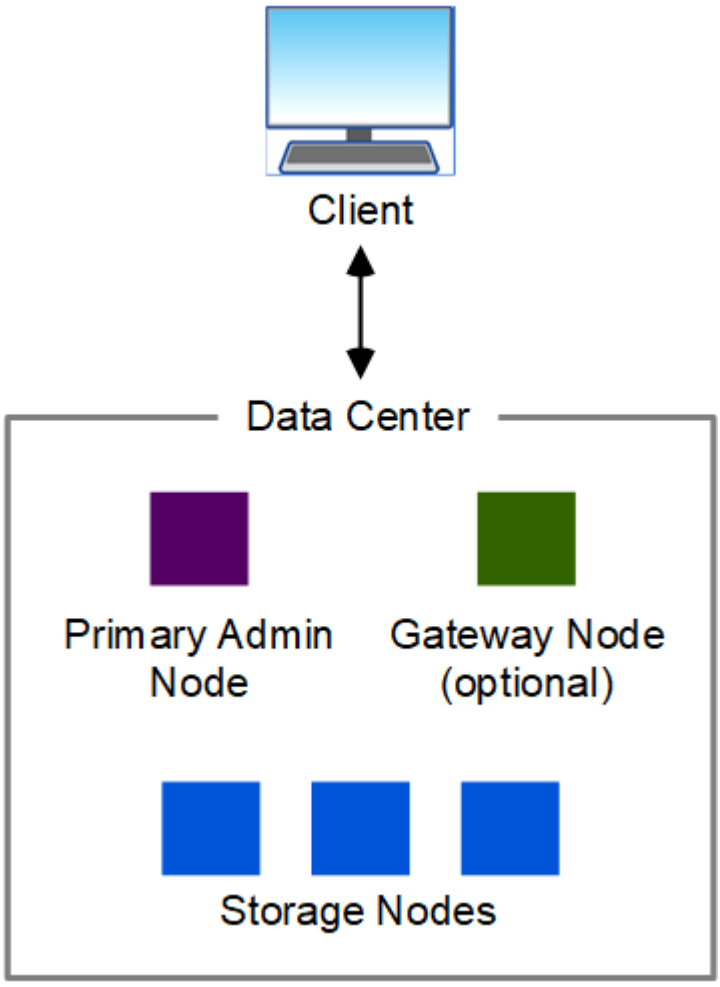
Weitere Informationen zur StorageGRID -Netzwerktopologie, den Anforderungen und der Grid-Kommunikation finden Sie im"Netzwerkrichtlinien" .

Implementierungstopologien

Das StorageGRID -System kann an einem einzelnen oder an mehreren Rechenzentrumsstandorten bereitgestellt werden. Die maximale Anzahl von Sites pro Bereitstellung beträgt 16.

Ein Standort

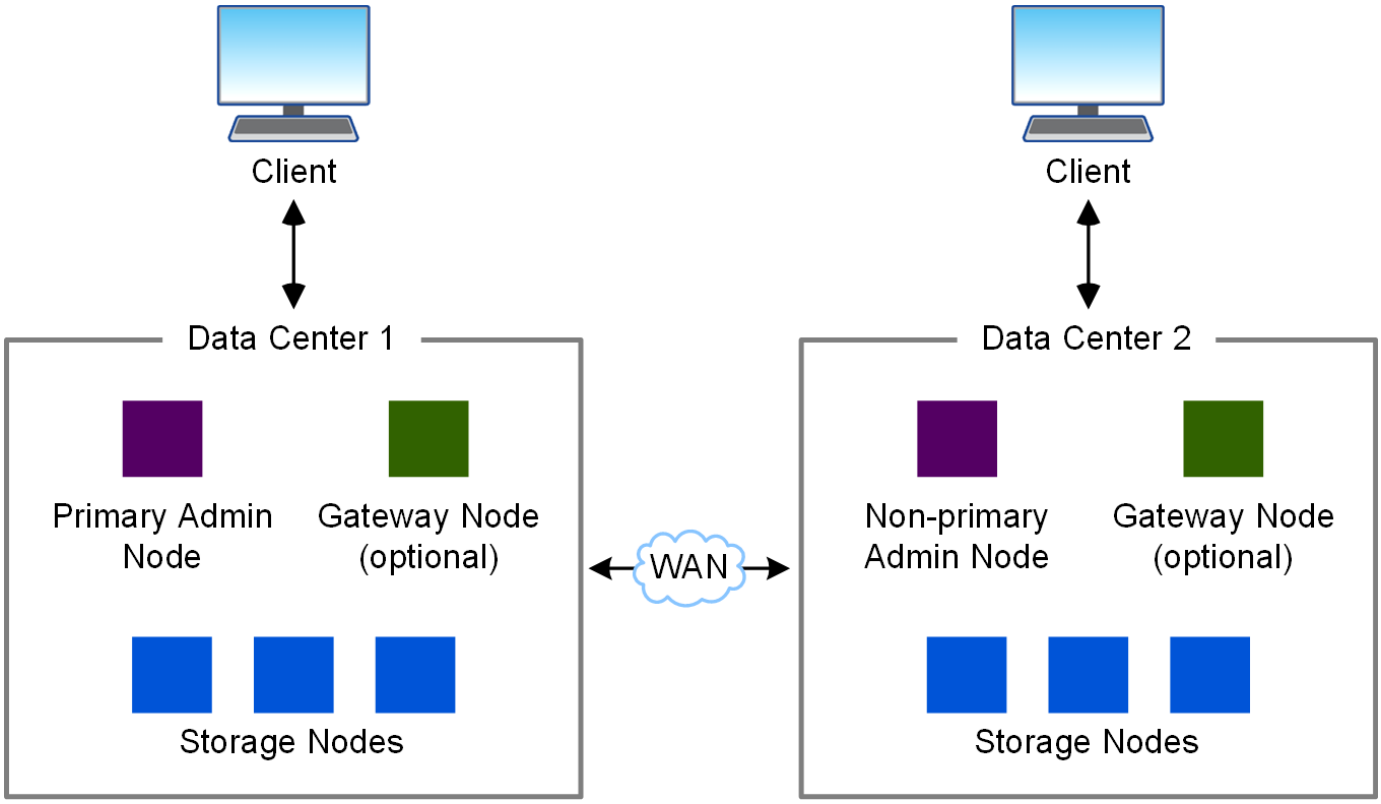
Bei einer Implementierung über einen einzigen Standort werden die Infrastruktur und der Betrieb des StorageGRID Systems zentralisiert.



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.

Die Standorte befinden sich häufig an geografisch unterschiedlichen Standorten in unterschiedlichen Störungsbereichen, beispielsweise an einer Erdbebenverwerfungslinie oder in einem Überschwemmungsgebiet. Datenfreigabe und Notfallwiederherstellung werden durch die automatisierte Verteilung der Daten an andere Standorte erreicht.



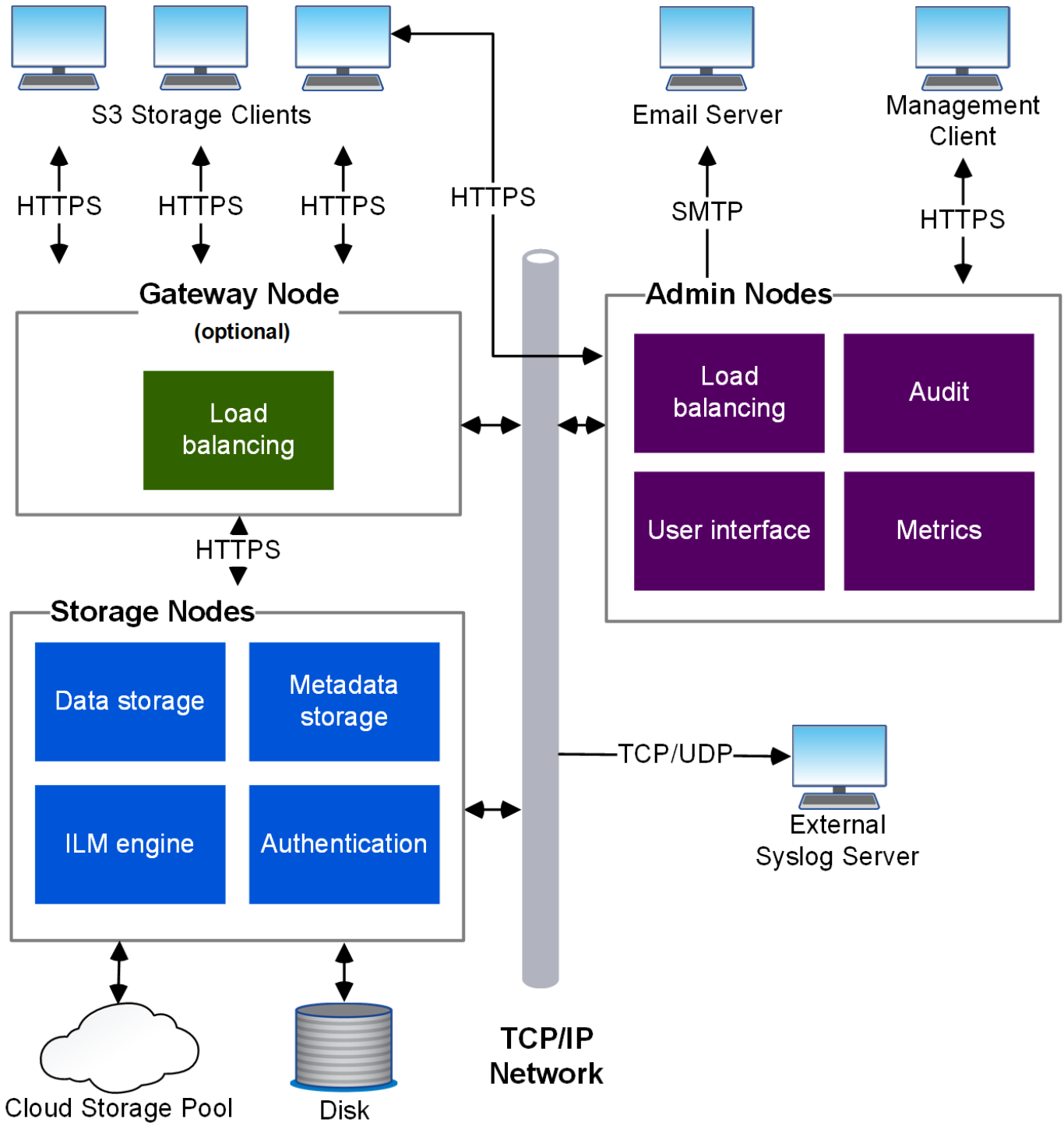
Innerhalb eines einzigen Rechenzentrums können auch mehrere logische Standorte vorhanden sein, um die Verwendung verteilter Replikation und Erasure Coding für eine höhere Verfügbarkeit und Ausfallsicherheit zu ermöglichen.

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 Clients speichern Objekte in StorageGRID und rufen sie ab. Andere Clients werden verwendet, um E-Mail-Benachrichtigungen zu senden, auf die StorageGRID-Managementoberfläche zuzugreifen und optional auf die Audit-Freigabe zuzugreifen.

S3-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-Clients über HTTPS eine direkte Verbindung zu Storage-Nodes herstellen.

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

Grid Nodes und Services

StorageGRID Grid-Knoten 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.

Typen von Grid-Nodes

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

Admin-Nodes

Bereitstellen von Managementservices wie Systemkonfiguration, Monitoring und Protokollierung 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 zum Lastausgleich für S3-Client-Traffic verwendet werden.

Siehe "Was ist ein Admin-Node?"

Storage-Nodes

Management und Speicherung von Objektdaten und Metadaten Jeder Standort im StorageGRID-System muss über mindestens drei Storage-Nodes verfügen.

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

Siehe "Was ist ein Storage-Node?"

Gateway-Nodes (optional)

Stellen Sie eine Schnittstelle für den Lastausgleich bereit, 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.

Siehe "Was ist ein Gateway Node?"

Hardware- und Software-Nodes

StorageGRID Knoten können als StorageGRID Appliance-Knoten oder als softwarebasierte Knoten bereitgestellt werden. Die maximale Anzahl an Knoten (einschließlich aller Knotentypen) pro System beträgt 220.

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.

Im Folgenden erfahren Sie mehr über die verfügbaren Appliances:

- "StorageGRID Appliance-Dokumentation"
- "NetApp Hardware Universe"

Softwarebasierte Nodes

Softwarebasierte Grid-Knoten können als virtuelle VMware-Maschinen oder innerhalb von Container-Engines auf einem Linux-Host bereitgestellt werden. Sehen "Installieren Sie StorageGRID auf softwarebasierten Knoten" .

Verwenden Sie die "NetApp Interoperabilitäts-Matrix-Tool (IMT)", um die unterstützten Versionen zu bestimmen.

StorageGRID Services

Nachfolgend finden Sie eine vollständige Liste der StorageGRID Services.

Service	Beschreibung	Standort
Kontendienst-Forwarder	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.	Load Balancer-Service auf Admin-Nodes und Gateway-Nodes
ADC (Administrative Domain Controller)	Verwaltet Topologiedaten, bietet Authentifizierungsservices und reagiert auf Anfragen aus den LDR- und CMN-Diensten.	Mindestens drei Storage Nodes, die den ADC-Dienst an jedem Standort enthalten
AMS (Audit Management System)	Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textdatei.	Admin-Nodes
Apache Tomcat	Webserver für Java-basierte Anwendungen.	Admin-Nodes
Avahi-Daemon	Verarbeitet mDNS, das zur Namensauflösung und Diensterkennung innerhalb des lokalen Netzwerks verwendet wird.	Alle Nodes
Cache-Dienst	Läuft auf Load Balancer-Knoten (Gateway) und verwaltet einen lokalen Cache mit Objektinhalten.	Gateway-Nodes
Cassandra	Verwaltet die verteilte Datenbank für Objektmetadaten.	Speicherknoten (außer Nur-Daten)
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch.	Storage-Nodes

Service	Beschreibung	Standort
Chunk-Service	Verwaltet Erasure-codierte Daten und Paritätsfragmente.	Storage-Nodes
CMN (Knoten für die Konfigurationsverwaltung)	Management systemweiter Konfigurationen und Grid-Aufgaben Jedes Grid hat einen CMN-Dienst.	Primärer Admin-Node
DDS (Distributed Data Store)	Schnittstellen zur Cassandra-Datenbank zum Management von Objektmetadaten	Storage-Nodes
DMV (Data Mover)	Verschiebt Daten in Cloud-Endpunkte	Storage-Nodes
Dynamische IP (dynap)	Überwacht das Raster auf dynamische IP-Änderungen und aktualisiert lokale Konfigurationen.	Alle Nodes
Grafana	Wird für die Darstellung von Kennzahlen im Grid Manager verwendet.	Admin-Nodes
Hochverfügbarkeit	Verwaltet virtuelle Hochverfügbarkeits-IPs auf Knoten, die auf der Seite „Hochverfügbarkeitsgruppen“ konfiguriert sind. Dieser Service wird auch als „Keepalived Service“ bezeichnet.	Admin- und Gateway-Nodes
Identität (idnt)	Verwaltet lokale Benutzer und Gruppen, Authentifizierung und föderiert Benutzeridentitäten aus LDAP und Active Directory.	Storage-Nodes, die den ADC-Dienst verwenden
Lambda-Schiedsrichter	Verwalten von S3 Select SelectObjectContent Requests.	Alle Nodes
Load Balancer (nginx-gw)	Bietet Lastausgleich für S3-Datenverkehr von Clients zu Storage-Nodes. Der Lastverteilungsservice kann über die Konfigurationsseite Load Balancer Endpoints konfiguriert werden. Dieser Service wird auch als nginx-gw-Service bezeichnet.	Admin- und Gateway-Nodes
LDR (Local Distribution Router)	Verwaltet die Speicherung und Übertragung von Inhalten innerhalb des Grids.	Storage-Nodes

Service	Beschreibung	Standort
MISCd Information Service Control Daemon	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.	Alle Nodes
Nginx	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.	Alle Nodes
nginx-gw Lastenausgleich	Bietet Lastausgleich für S3-Datenverkehr von Clients zu Storage-Nodes. Der Lastverteilungsservice kann über die Konfigurationsseite Load Balancer Endpoints konfiguriert werden. Dieser Service wird auch als nginx-gw-Service bezeichnet.	Admin- und Gateway-Nodes
NMS (Network Management System)	Gibt die Überwachungs-, Berichterstellungs- und Konfigurationsoptionen an, die über den Grid Manager angezeigt werden.	Admin-Nodes
Knotenexporteur (Prometheus-Datensammlung)	Veröffentlicht Statistiken auf Systemebene für die Prometheus-Zeitreihenmetriksammlung.	Alle Nodes
ntp	Network Time Protocol (NTP)-Dienst.	Alle Nodes
Persistenz	Verwaltet Dateien auf dem Root-Laufwerk, die über einen Neustart bestehen müssen.	Alle Nodes
Prometheus	Erfasst Zeitreihungskennzahlen von Services auf allen Knoten.	Admin-Nodes
RSM (Replicated State Machine)	Stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden.	Storage-Nodes, die den ADC-Dienst verwenden
SSM (Server Status Monitor)	Überwacht Hardwarebedingungen und Berichte an den NMS-Service.	Auf jedem Grid-Node ist eine Instanz vorhanden
Server-Manager	Verwaltet StorageGRID -Dienste.	Alle Nodes

Service	Beschreibung	Standort
SNMP-Agent	Reagiert auf SNMP-Anfragen.	Admin-Nodes
SNMP-Portverwaltungsdienst	Verwaltet die dynamische Verwaltung von SNMP-Ports.	Alle Nodes
SSH (Secure Shell)	Verwaltet sicheren Zugriff und Remote-Systemverwaltung.	Alle Nodes
SSM (Systemstatusmonitor)	Überwacht Hardwarebedingungen und Berichte an den NMS-Service.	Alle Nodes
Statistik	Zeichnet zusätzliche Metriken im Zusammenhang mit S3-Buckets auf.	Storage-Nodes
Trace Agent (Jaeger-Agent)	Empfängt und verarbeitet vom Trace-Collector (Jaeger-Collector) übermittelte Tracing-Informationen.	Alle Nodes
Spurensammler (Jaeger-Sammler)	Führt eine Trace-Erfassung durch, um Informationen für den technischen Support zu sammeln. Der Trace Collector-Dienst verwendet die Open-Source-Jaeger-Software.	Admin-Nodes

Was ist ein StorageGRID Admin Node?

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Admin-Nodes können auch zum Lastausgleich für S3-Client-Traffic verwendet werden. Jedes Grid muss einen primären Admin-Node haben und kann eine beliebige Anzahl nicht primärer Admin-Nodes für Redundanz aufweisen.

Unterschiede zwischen primären und nicht primären Admin-Nodes

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

In der Tabelle sind die Funktionen der primären und nicht-primären Admin-Nodes zusammengefasst.

Sorgen	Primärer Admin-Node	Nicht primärer Admin-Node
Umfasst den AMS Service	Ja.	Ja.
Umfasst den CMN Service	Ja.	Nein

Sorgen	Primärer Admin-Node	Nicht primärer Admin-Node
Umfasst den NMS Service	Ja.	Ja.
Umfasst den Prometheus Service	Ja.	Ja.
Umfasst den SSM Service	Ja.	Ja.
Umfasst die Lastausgleich und Hochverfügbarkeit Services	Ja.	Ja.
Unterstützung Management Application Program Interface(Management-API)	Ja.	Ja.
Kann für alle netzwerkbezogenen Wartungsaufgaben verwendet werden, z. B. für die Änderung der IP-Adresse und die Aktualisierung von NTP-Servern	Ja.	Nein
Kann Wiederherstellungspaket herunterladen	Ja.	Ja.
EC-Neuverteilung nach der Storage-Node-Erweiterung möglich	Ja.	Nein
Kann für die Wiederherstellung des Volumens verwendet werden	Ja.	Ja.
Kann Protokolldateien und Systemdaten von einem oder mehreren Nodes erfassen	Ja.	Ja.
Kann Speicher, Gateway und nicht primäre Admin-Knoten wiederherstellen	Ja.	Ja.
Kann den primären Admin-Knoten wiederherstellen	Ja.	Nein
Sendet Warnmeldungen, AutoSupport-Pakete und SNMP-Traps und informiert	Ja. Fungiert als Bevorzugter Absender.	Ja. Fungiert als Standby-Sender.

Administratorknoten des bevorzugten Absenders

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Pakete und SNMP-Traps und -Benachrichtigungen.

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

In diesen Fällen können mehrere Benachrichtigungen gesendet werden:

- Wenn Admin-Knoten voneinander „islanded“ werden, versuchen sowohl der bevorzugte Sender als auch der Standby-Sender, Benachrichtigungen zu senden, und es können mehrere Kopien von Benachrichtigungen empfangen werden.
- Wenn ein Standby-Absender Probleme mit dem bevorzugten Absender erkennt und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Absender möglicherweise seine Fähigkeit zum Senden von Benachrichtigungen wiedererlangen. In diesem Fall werden möglicherweise doppelte Benachrichtigungen gesendet. Der Standby-Absender stellt das Senden von Benachrichtigungen ein, wenn er beim bevorzugten Absender keine Fehler mehr erkennt.

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

Primäre Dienste für Admin-Nodes

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

Service	Tastenfunktion
Audit Management System (AMS)	Verfolgt Systemaktivitäten und -Ereignisse.
Configuration Management Node (CMN)	Verwaltet die systemweite Konfiguration.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. **Hinweis:** dieser Service befindet sich auch auf Gateway Nodes.
Load Balancer	Bietet Lastausgleich für S3-Datenverkehr von Clients zu Storage-Nodes. **Hinweis:** dieser Service befindet sich auch auf Gateway Nodes.
Management-Applikations-Programmierschnittstelle (Management-API)	Verarbeitet Anforderungen aus der Grid-Management-API und der Mandantenmanagement-API.
Network Management System (NMS)	Bietet Funktionen für den Grid Manager.
Prometheus	Sammelt und speichert Zeitreihenmetriken von den Services auf allen Knoten.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Was ist ein StorageGRID Storage Node?

Storage-Nodes managen und speichern Objektdaten und Metadaten. Storage-Nodes umfassen die Services und Prozesse, die zum Speichern, Verschieben, Überprüfen und Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind.

Jeder Standort im StorageGRID-System muss über mindestens drei Storage-Nodes verfügen.

Typen von Storage-Nodes

Während der Installation können Sie den Typ des Storage-Node auswählen, den Sie installieren möchten. Diese Typen sind für softwarebasierte Storage Nodes und Appliance-basierte Storage Nodes verfügbar, die die Funktion unterstützen:

- Storage-Node für Daten und Metadaten kombiniert
- Storage-Node nur für Metadaten
- Rein datenrein Storage-Node

Sie können den Typ des Storage-Node in folgenden Situationen auswählen:

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

Storage Node für Daten und Metadaten (kombiniert)

Standardmäßig werden auf allen neuen Storage-Nodes sowohl Objektdaten als auch Metadaten gespeichert. Dieser Typ von Storage Node wird als *Combined* Storage Node bezeichnet.

Storage-Node nur für Metadaten

Die ausschließliche Verwendung eines Storage-Knotens für Metadaten kann sinnvoll sein, wenn Ihr Grid eine sehr große Anzahl kleiner Objekte speichert. Die Installation von dedizierten Metadaten bietet ein besseres Gleichgewicht zwischen dem für eine große Anzahl an kleinen Objekten erforderlichen Speicherplatz und dem für diese Objekte erforderlichen Speicherplatz. Darüber hinaus können Storage-Nodes, die auf hochperformanten Appliances gehostet werden, auf nur Metadaten ausgerichtet sind, die Performance steigern.

Storage-Nodes, die nur Metadaten enthalten, erfüllen spezifische Hardwareanforderungen:

- Bei Verwendung von StorageGRID Appliances können nur Nodes mit Metadaten auf SGF6112-Appliances mit zwölf 1.9-TB- oder zwölf 3.8-TB-Laufwerken konfiguriert werden.
- Bei der Verwendung von softwarebasierten Nodes müssen die auf Metadaten auslaufenden Node-Ressourcen mit den vorhandenen Storage-Nodes übereinstimmen. Beispiel:
  - Wenn der bestehende StorageGRID Standort SG6000 oder SG6100 Appliances verwendet, müssen die rein softwarebasierten Nodes mit Metadaten die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM
    - 8-Core-CPU
    - 8 TB SSD oder äquivalenter Storage für die Cassandra-Datenbank (rangedb/0)
  - Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten

ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0)).

- Beim Hinzufügen einer neuen StorageGRID -Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandener Sites entsprechen. Die Ressourcen an einem neuen Standort sollten mit den Speicherknoten an vorhandenen Standorten übereinstimmen.

> Obwohl reine Metadaten-Storage-Nodes S3-Client-Anforderungen enthalten LDR-Serviceund verarbeiten können, erhöht sich die StorageGRID-Performance möglicherweise nicht.

Rein datenrein Storage-Node

Ein Storage-Node ausschließlich für Daten ist sinnvoll, wenn Ihre Storage-Nodes unterschiedliche Performance-Merkmale aufweisen. Um beispielsweise die Performance potenziell zu steigern, können Sie reine Daten-Storage-Nodes mit einer hohen Kapazität und gleichzeitig hochperformante Storage-Nodes mit Metadaten verwenden.

Darüber hinaus können Sie mehr Metadatenkapazität erhalten, indem Sie Knoten mit wenig RAM aus Cassandra entfernen, wodurch sich das Metadatenkapazitätslimit pro Knoten erhöht. Weitere Informationen finden Sie unter "Management von Objekt-Metadaten-Storage" .

Sie können einen Storage Node konvertieren, der nicht dieADC-Dienst zu einem reinen Datenspeicherknoten. Weitere Informationen finden Sie unter "Konvertieren eines Speicherknotens in einen Nur-Datenknoten" .

Erforderliche Speicherknoten pro Grid und pro Site

Beachten Sie bei der Auswahl der in Ihrer Topologie zu verwendenden Speicherknoten, dass das Raster bzw. jeder Standort im Raster Folgendes enthalten muss:

- Pro Site (in einem Single- oder Multi-Site-Raster): DreiADC Speicherknoten (kann eine beliebige Kombination aus kombinierten und reinen Metadaten-Speicherknoten sein)
- Single-Site-Grid: Mindestens zwei Objektspeicherknoten (kann eine beliebige Kombination aus kombinierten und Nur-Daten-Knoten sein)
- Multi-Site-Raster: Mindestens ein Objektspeicherknoten pro Site (kann entweder kombiniert oder nur für Daten sein)

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. Dieser Dienst wird nicht von reinen Datenspeicherknoten gehostet.

Service	Tastenfunktion
Administrativer Domänencontroller (ADC)	Aufrechterhaltung der Topologie und Grid-Konfiguration Dieser Dienst wird nicht von reinen Datenspeicherknoten gehostet. **Details** Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen miteinander. Der ADC-Dienst wird auf mindestens drei Storage Nodes an einem Standort gehostet. Der ADC-Dienst verwaltet Topologiedaten, einschließlich Standort und Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden muss, kontaktiert er einen ADC-Service, um den besten Grid-Knoten für die Bearbeitung seiner Anforderung zu finden. Darüber hinaus behält der ADC-Service eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung bei, sodass jeder Grid-Node aktuelle Konfigurationsinformationen abrufen kann. Zur Erleichterung von verteilten und isanded-Operationen synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Services und Topologie mit den anderen ADC-Diensten im StorageGRID-System. Im Allgemeinen unterhalten alle Rasterknoten eine Verbindung zu mindestens einem ADC-Dienst. So wird sichergestellt, dass die Grid-Nodes immer auf die neuesten Informationen zugreifen. Wenn sich Grid-Nodes verbinden, werden die Zertifikate anderer Grid-Nodes zwischengespeichert, sodass die Systeme mit bekannten Grid-Nodes weiterarbeiten können, selbst wenn ein ADC-Dienst nicht verfügbar ist. Neue Grid-Knoten können nur Verbindungen über einen ADC-Dienst herstellen. Durch die Verbindung jedes Grid-Knotens kann der ADC-Service Topologiedaten erfassen. Die Informationen zu diesem Grid-Node umfassen die CPU-Last, den verfügbaren Festplattenspeicher (wenn der Storage vorhanden ist), unterstützte Services und die Standort-ID des Grid-Node. Andere Dienste fragen den ADC-Service nach Topologiedaten durch Topologieabfragen. Der ADC-Dienst reagiert auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID-System empfangen wurden.
Cassandra	Speichert und sichert Objekt-Metadaten. Dieser Dienst wird nicht von reinen Datenspeicherknoten gehostet.
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch. Dieser Dienst wird nicht von reinen Datenspeicherknoten gehostet.
Chunk	Verwaltet Erasure-codierte Daten und Paritätsfragmente.

Service	Tastenfunktion
Data Mover (dmv)	Verschiebt Daten in Cloud-Storage-Pools
Verteilter Datenspeicher (DDS)	Überwacht Objekt-Metadaten-Storage **Details** Jeder Storage Node umfasst den Distributed Data Store (DDS)-Service. Dieser Service ist mit der Cassandra-Datenbank verbunden, um Hintergrundaufgaben für die im StorageGRID-System gespeicherten Objektmetadaten auszuführen. Der DDS-Service verfolgt die Gesamtanzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtanzahl der über die unterstützten Schnittstellen (S3) des Systems aufgenommenen Objekte.
Identität (idnt)	Föderiert Benutzeridentitäten von LDAP und Active Directory Dieser Dienst wird nicht von reinen Datenspeicherknoten gehostet.

Service	Tastenfunktion
Local Distribution Router (LDR)	Verarbeitet Protokollanfragen von Objekt-Storage und managt Objektdaten auf der Festplatte.

Service	Tastenfunktion
Replicated State Machine (RSM)	Stellt sicher, dass Serviceanfragen der S3-Plattform an ihre jeweiligen Endpunkte gesendet werden. Dieser Dienst wird nicht von reinen Datenspeicherknoten gehostet.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Was ist ein StorageGRID Gateway Node?

Gateway-Nodes bieten eine dedizierte Schnittstelle für den Lastausgleich, über die S3-Client-Applikationen eine Verbindung mit StorageGRID herstellen können. Load Balancing maximiert die Geschwindigkeit und die Verbindungskapazität, indem der Workload auf mehrere Storage Nodes verteilt wird. Gateway Nodes sind optional.

Der StorageGRID Load Balancer wird auf allen Admin-Nodes und allen Gateway Nodes angeboten. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her. Der Load Balancer Service leitet Clients nahtlos an einen optimalen Storage Node weiter, sodass der Ausfall von Nodes oder sogar eines ganzen Standorts transparent ist.

Sie konfigurieren einen oder mehrere Load Balancer-Endpunkte, um den Port und das Netzwerkprotokoll (HTTPS oder HTTP) zu definieren, mit dem eingehende und ausgehende Client-Anfragen auf die Load Balancer-Dienste auf Gateway- und Admin-Nodes zugreifen. Der Load Balancer-Endpunkt definiert außerdem den Client-Typ (S3), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten. Siehe "Überlegungen zum Lastausgleich".

Bei Bedarf können Sie die Netzwerkschnittstellen mehrerer Gateway Nodes und Admin-Nodes in einer HA-Gruppe (High Availability, Hochverfügbarkeit) gruppieren. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload der Client-Applikation managen. Siehe "Managen Sie Hochverfügbarkeitsgruppen (High Availability Groups, HA-Gruppen)".

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
Cache-Dienst	Verwaltet einen lokalen Cache mit Objektinhalten.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. **Hinweis:** dieser Service befindet sich auch auf Admin Nodes.
Lastausgleich	Ermöglicht Layer-7-Lastausgleich für S3-Datenverkehr von Clients zu Storage-Nodes. Dies ist der empfohlene Lastausgleichmechanismus. **Hinweis:** dieser Service befindet sich auch auf Admin Nodes.

Der LDR-Service übernimmt folgende Aufgaben:

- Abfragen
- Information Lifecycle Management-Aktivitäten (ILM)
- Löschen von Objekten
- Objektspeicher
- Objektdatenübertragung von einem anderen LDR-Service (Storage Node)
- Datenspeicherverwaltung
- S3 Protokollschnittstelle

Der LDR-Service ordnet jedes S3-Objekt seiner eindeutigen UUID zu.

Objektspeicher

Der zugrunde liegende Datenspeicher eines LDR-Service wird in eine feste Anzahl an Objektspeichern (auch Storage-Volumes genannt) unterteilt. Jeder Objektspeicher ist ein separater Bereitstellungspunkt.

Das Objekt speichert in einem Storage-Node werden durch eine Hexadezimalzahl zwischen 0000 und 002F identifiziert, die als Volume-ID bezeichnet wird. Der Speicherplatz ist im ersten Objektspeicher (Volume 0) für Objekt-Metadaten in einer Cassandra-Datenbank reserviert. Für Objektdaten werden alle verbleibenden Speicherplatz auf diesem Volume verwendet. Alle anderen Objektspeichern werden ausschließlich für Objektdaten verwendet, zu denen replizierte Kopien und nach dem Erasure-Coding-Verfahren Fragmente gehören.

Weitere Informationen finden Sie unter "Management von Objekt-Metadaten-Storage".

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

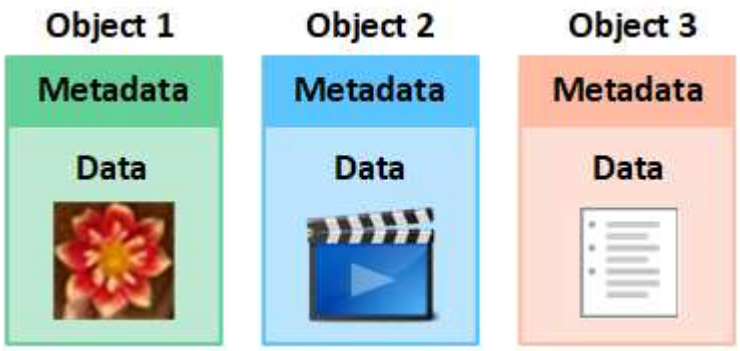
Managen von Daten mit StorageGRID

Was ist ein StorageGRID Objekt

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

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

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



Was sind Objektdaten?

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

Was sind Objekt-Metadaten?

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

Objektmetadaten enthalten Informationen wie die folgenden:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des Namens des S3-Buckets, des Namens oder der ID des Mandantenkontos, der logischen Größe des Objekts, des Datums und der Uhrzeit, zu der das Objekt zum ersten Mal erstellt wurde sowie des Datums und der Uhrzeit, zu der das Objekt zuletzt geändert wurde.
- 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 darüber, wie und wo StorageGRID Objektmetadaten speichert, finden Sie unter "Management von Objekt-Metadaten-Storage".

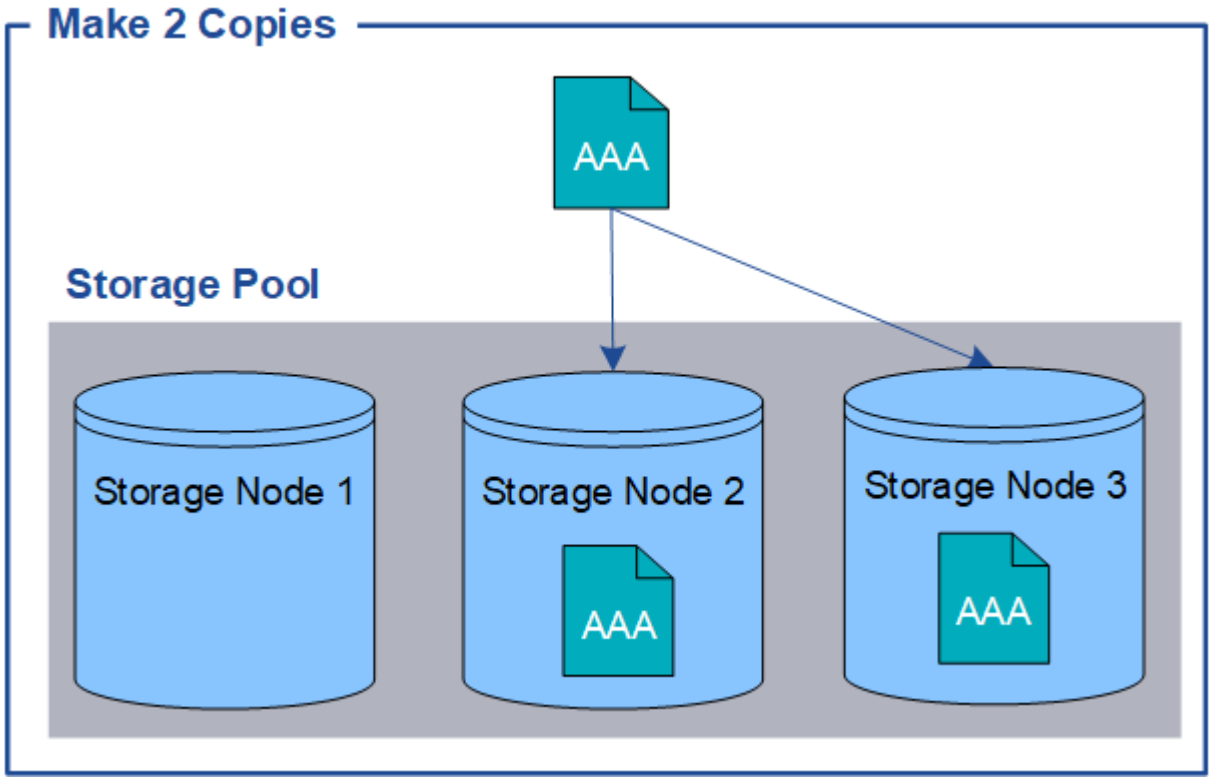
Wie werden Objektdaten gesichert?

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

Replizierung

Wenn StorageGRID Objekte einer ILM-Regel (Information Lifecycle Management) zuordnet, die zum Erstellen replizierter Kopien konfiguriert ist, erstellt das System exakte Kopien von Objektdaten und speichert diese auf Storage-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.

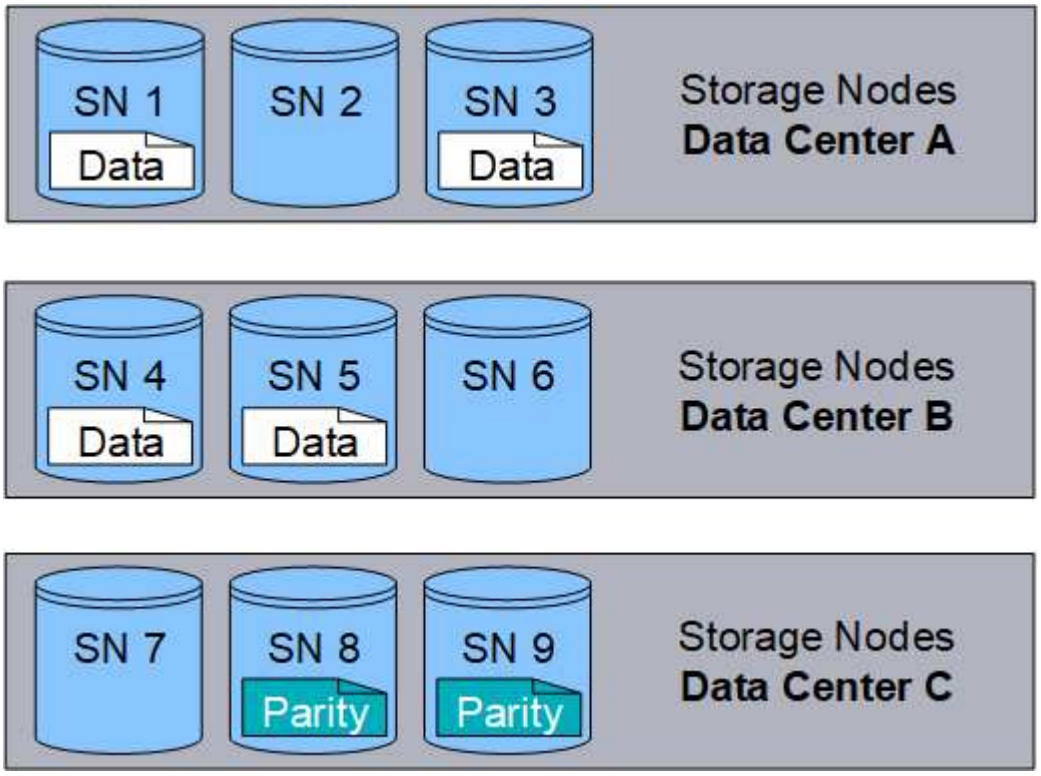


Erasure Coding

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. Das verwendete Erasure Coding-Schema wird durch ILM-Regeln und Erasure Coding-Profile bestimmt.

Das folgende Beispiel zeigt den Einsatz von Erasure Coding für Objektdaten. In diesem Beispiel verwendet die

ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente ist in drei Datacentern auf einem anderen Storage Node gespeichert, um bei Node-Ausfällen oder Standortausfällen ihre Daten zu sichern.



Verwandte Informationen

- "Objektmanagement mit ILM"
- "Verwenden Sie das Information Lifecycle Management"

Objektlebenszyklus in StorageGRID

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-Client-Anwendung, die ein Objekt über HTTP im StorageGRID-System speichert. In dieser Phase beginnt das StorageGRID-System mit der Verwaltung des Objekts.
- **Copy-Management**: Management replizierter und mit Erasure-Coded-Kopien in StorageGRID, wie in den ILM-Regeln der aktiven ILM-Richtlinien beschrieben. Während der Phase des Copy-Managements schützt StorageGRID Objektdaten vor Verlust, indem die angegebene Anzahl und der Typ der Objektkopien auf Storage Nodes oder in einem Cloud-Storage-Pool erstellt und aufrechterhalten wird.
- **Retrieve**: Der Prozess einer Client-Anwendung, die auf ein vom StorageGRID-System gespeichertes Objekt zugreift. Der Client liest das Objekt, das aus einem Storage Node oder Cloud Storage Pool abgerufen wird.
- **Löschen**: Der Vorgang, bei dem alle Objektkopien aus dem Raster entfernt werden. Objekte können entweder gelöscht werden, wenn eine Client-Applikation eine Löschanfrage an das StorageGRID System sendet, oder infolge eines automatischen Prozesses, der StorageGRID nach Ablauf der Nutzungsdauer

des Objekts durchführt.

Verwandte Informationen

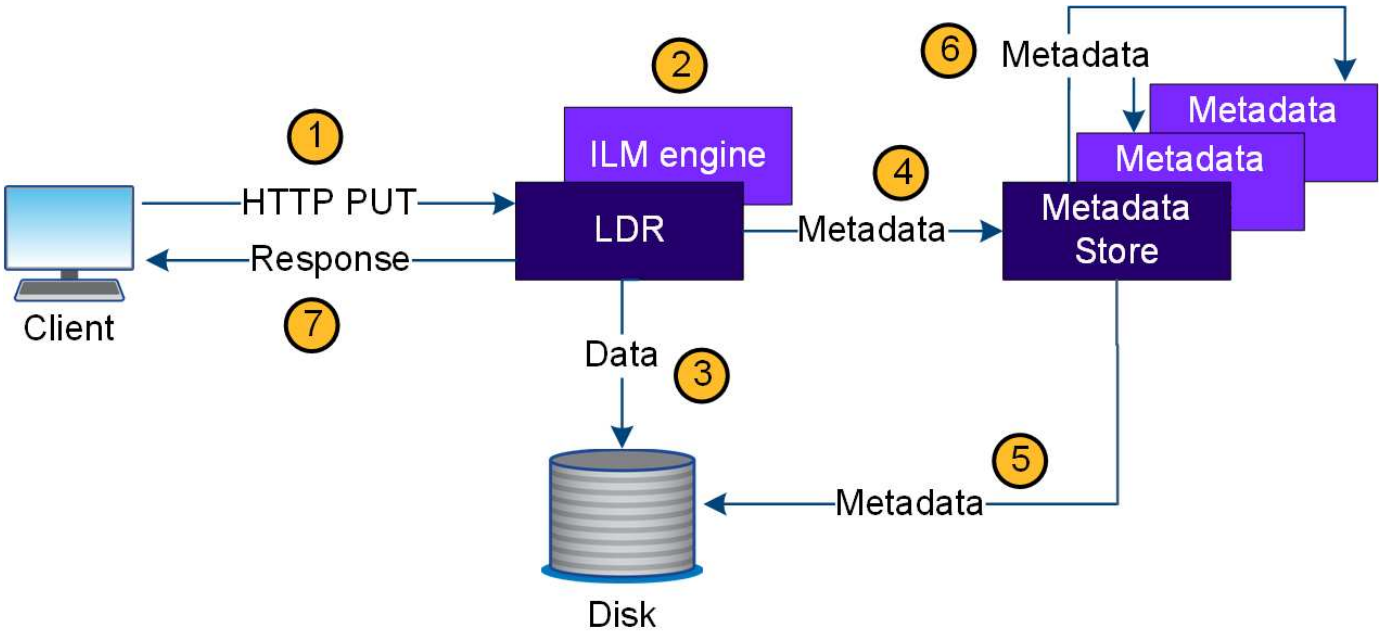
- "Objektmanagement mit ILM"
- "Verwenden Sie das Information Lifecycle Management"

Wie StorageGRID die Objektaufnahme handhabt

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

Datenfluss

Wenn ein Client ein Objekt in das StorageGRID-System einspeist, verarbeitet der LDR-Service auf Storage-Nodes die Anforderung und speichert die Metadaten und Daten auf der Festplatte.



1. Die Client-Applikation erstellt das Objekt und sendet es über eine HTTP PUT-Anforderung an das StorageGRID System.
2. Das Objekt wird anhand der ILM-Richtlinie des Systems bewertet.
3. Der LDR-Service speichert die Objektdaten als replizierte Kopie oder als Kopie, die zur Fehlerkorrektur codiert wurde. (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.

Wie StorageGRID Objektkopien verwaltet

Objektdaten werden über die aktiven ILM-Richtlinien und zugehörigen ILM-Regeln gemanagt. Mithilfe von ILM-Regeln werden replizierte oder unter Erasure-Coding-Kopien erstellt, um Objektdaten vor Verlust zu schützen.

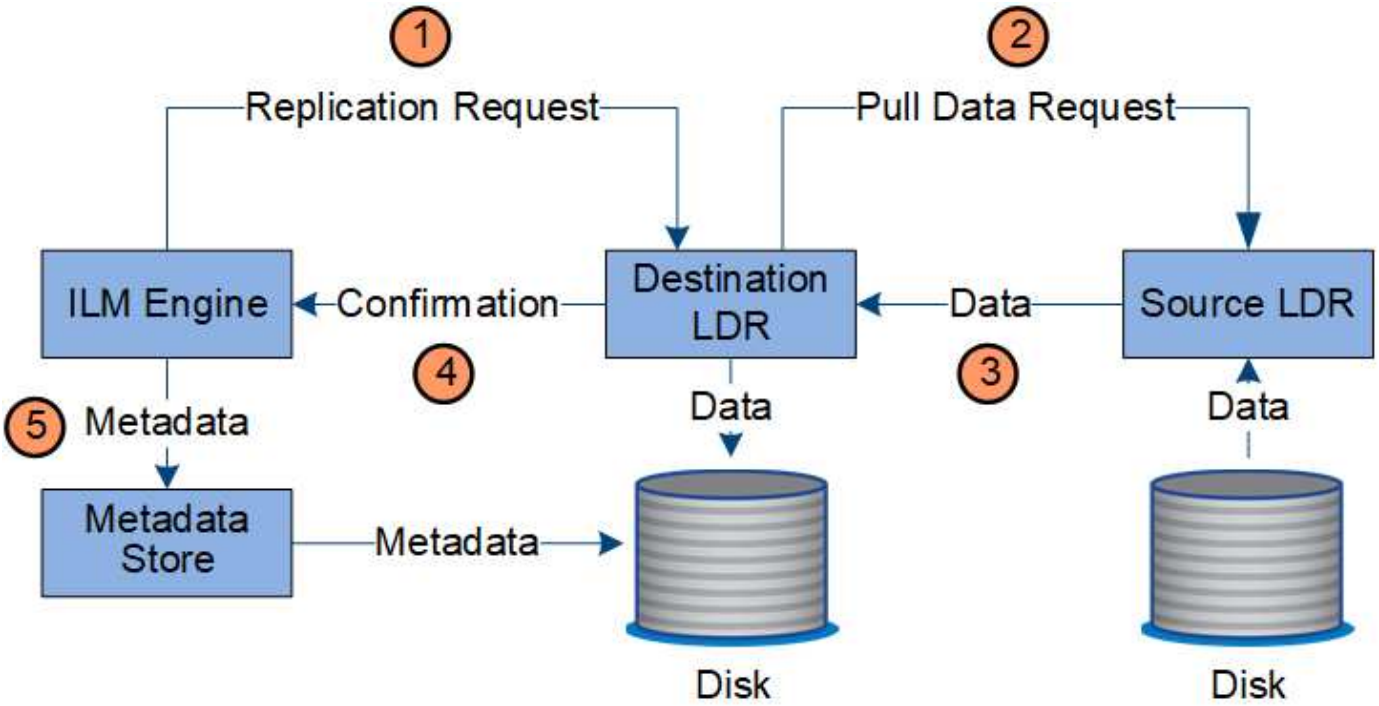
Unterschiedliche Typen und Standorte von Objektkopien können zu unterschiedlichen Zeiten der Lebensdauer des Objekts erforderlich sein. ILM-Regeln werden regelmäßig überprüft, um sicherzustellen, dass Objekte nach Bedarf platziert werden.

Objektdaten werden vom LDR-Service gemanagt.

Content-Schutz: Replikation

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

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



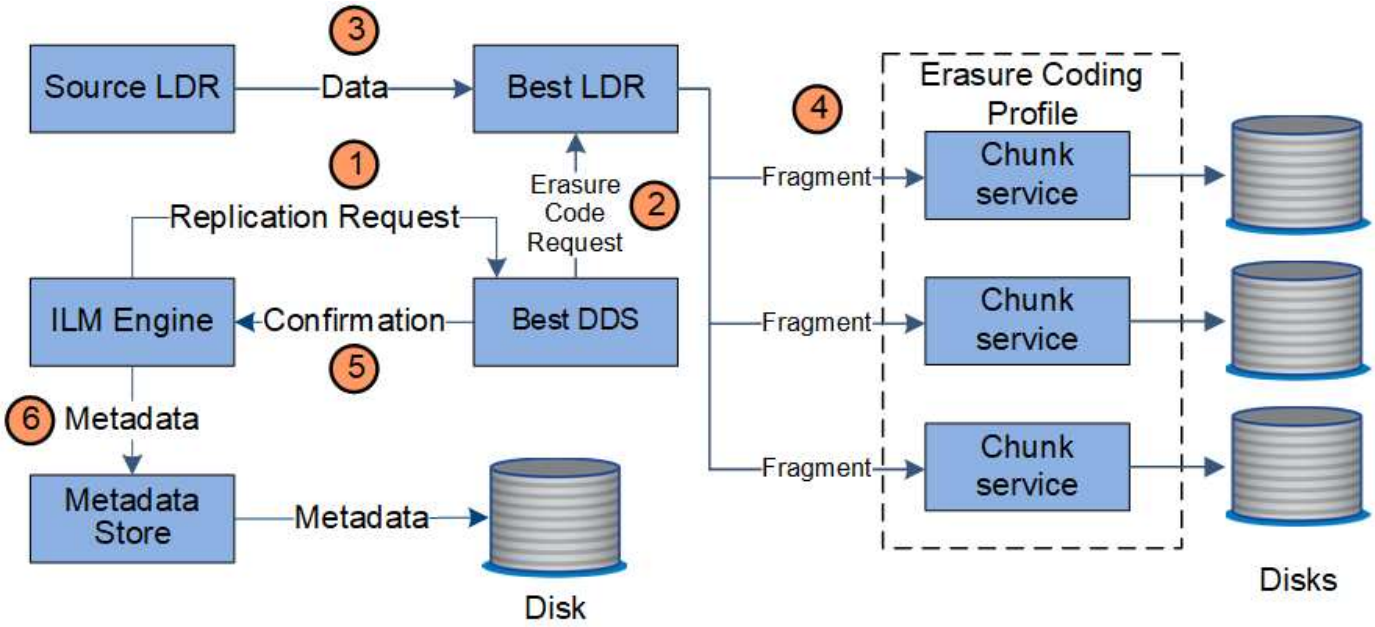
1. Die ILM-Engine fragt den ADC-Service ab, um den besten Ziel-LDR-Service innerhalb des durch die ILM-Regel festgelegten Storage-Pools zu ermitteln. Er sendet dann diesen LDR-Service einen Befehl, um die Replikation zu initiieren.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellspeicherort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

3. Der Quell-LDR-Service sendet eine Kopie an den Ziel-LDR-Service.
4. Der Ziel-LDR-Service benachrichtigt die ILM Engine, dass die Objektdaten gespeichert wurden.
5. Die ILM-Engine aktualisiert den Metadatenspeicher mit Objektspeichermetadaten.

Content Protection: Erasure Coding

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

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

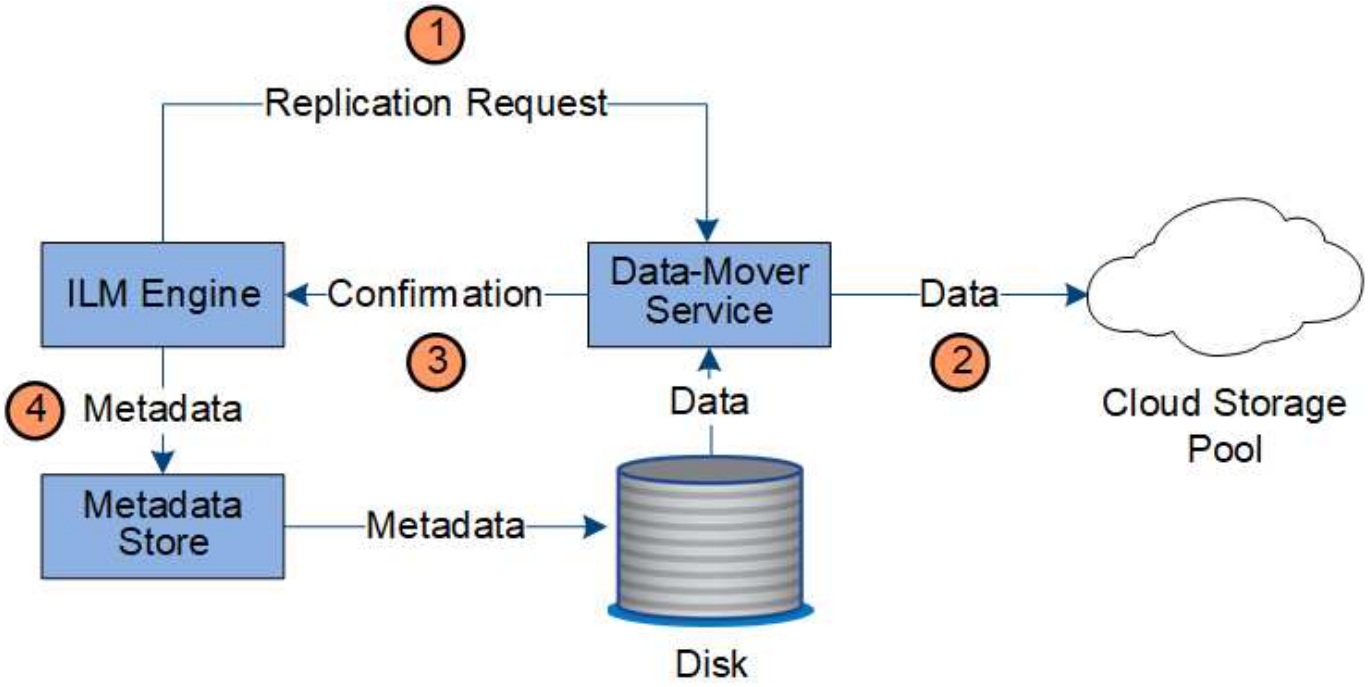


1. Die ILM-Engine fragt den ADC-Service ab, um zu bestimmen, welcher DDS-Service den Erasure Coding-Vorgang am besten ausführen kann. Wenn festgestellt, sendet die ILM-Engine eine „Initiierung“-Anforderung an diesen Service.
2. Der DDS-Dienst weist ein LDR an, den Code der Objektdaten zu löschen.
3. Der Quell-LDR-Service sendet eine Kopie an den für das Erasure Coding ausgewählten LDR-Service.
4. Nach der Erstellung der entsprechenden Anzahl von Parität und Datenfragmenten verteilt der LDR-Service diese Fragmente auf die Storage Nodes (Chunk-Services), aus denen 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 wird, werden Objektdaten in den externen S3-Bucket oder Azure Blob-Storage-Container dupliziert, der für den Cloud Storage-Pool angegeben wurde.

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



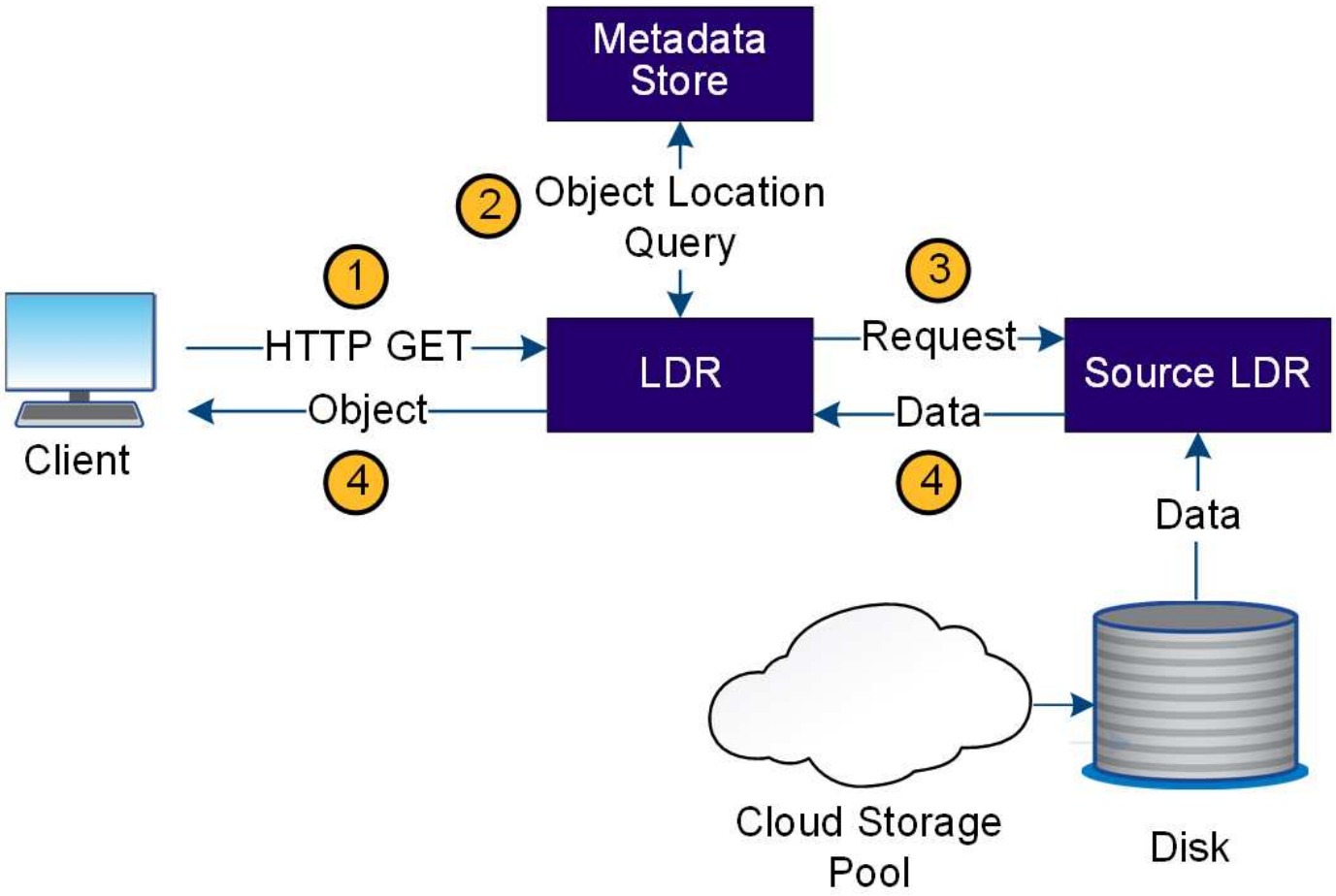
1. Die ILM-Engine wählt einen Data Mover-Service zur Replizierung in den Cloud-Storage-Pool aus.
2. Der Data Mover-Service sendet die Objektdaten an den Cloud-Speicherpool.
3. Der Data Mover-Service benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM-Engine aktualisiert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

Wie StorageGRID den Objektabruf handhabt

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, falls erforderlich, einem Cloud-Storage-Pool nachzuverfolgen.

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 Storage-Node nicht verfügbar ist, wird die Abrufanforderung an einen Cloud-Speicherpool weitergeleitet.

> Wenn sich die einzige Objektkopie auf AWS Glacier Storage oder in der Azure Archiv-Tier befindet, muss die Client-Applikation eine Anfrage für S3 RestoreObject ausgeben, um eine abrufbare Kopie im 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.

Wie StorageGRID das Löschen von Objekten handhabt

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

Löschhierarchie

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

- **S3 Object Lock**: Wenn die globale S3 Object Lock-Einstellung für das Grid aktiviert ist, können S3-Clients Buckets mit aktivierter S3-Objektsperre erstellen und dann über die S3-REST-API Aufbewahrungseinstellungen für jede Objektversion festlegen, die diesem Bucket hinzugefügt wurde.
  - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.

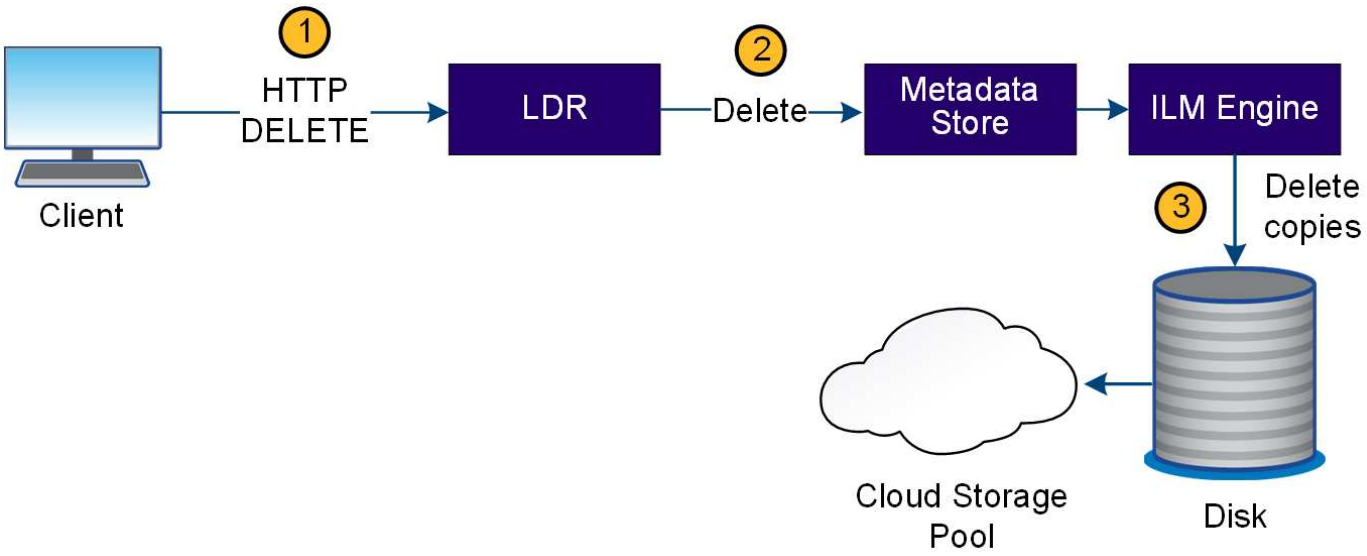
- Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
- Objekte in Buckets mit aktivierter S3 Objektsperre werden von ILM „ewig“ aufbewahrt. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder den Ablauf des Bucket-Lebenszyklus gelöscht werden.
- Wenn S3-Clients ein Standarddatum für die Aufbewahrung bis auf den Bucket anwenden, müssen sie für jedes Objekt kein „bis zur Aufbewahrung“ angeben.

- **Client delete Request**: Ein S3-Client kann eine delete-Objekt-Anfrage ausgeben. Wenn ein Client ein Objekt löscht, werden alle Kopien des Objekts aus dem StorageGRID System entfernt.
- **Objekte in Bucket löschen**: Tenant Manager-Benutzer können diese Option verwenden, um alle Kopien der Objekte und Objektversionen in ausgewählten Buckets dauerhaft aus dem StorageGRID-System zu entfernen.
- **S3-Bucket-Lebenszyklus**: S3-Clients können eine Lebenszykluskonfiguration zu ihren Buckets hinzufügen, die eine Ablaufaktion angibt. Wenn ein Bucket-Lebenszyklus vorhanden ist, löscht StorageGRID automatisch alle Kopien eines Objekts, wenn das in der Aktion „Ablaufdatum“ angegebene Datum oder die Anzahl der Tage erfüllt werden, es sei denn, der Client löscht das Objekt zuerst.
- **ILM-Platzierungsanweisungen**: Vorausgesetzt, dass für den Bucket keine S3-Objektsperre aktiviert ist und es keinen Bucket-Lebenszyklus gibt, löscht StorageGRID automatisch ein Objekt, wenn der letzte Zeitraum der ILM-Regel endet und es keine weiteren Platzierungen für das Objekt gibt.

> ⓘ Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Lifecycle-Ablaufaktionen die ILM-Richtlinie für Objekte, die mit dem Lifecycle-Filter übereinstimmen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflegen des Objekts verfallen sind.

Weitere Informationen finden Sie unter "So werden Objekte gelöscht" .

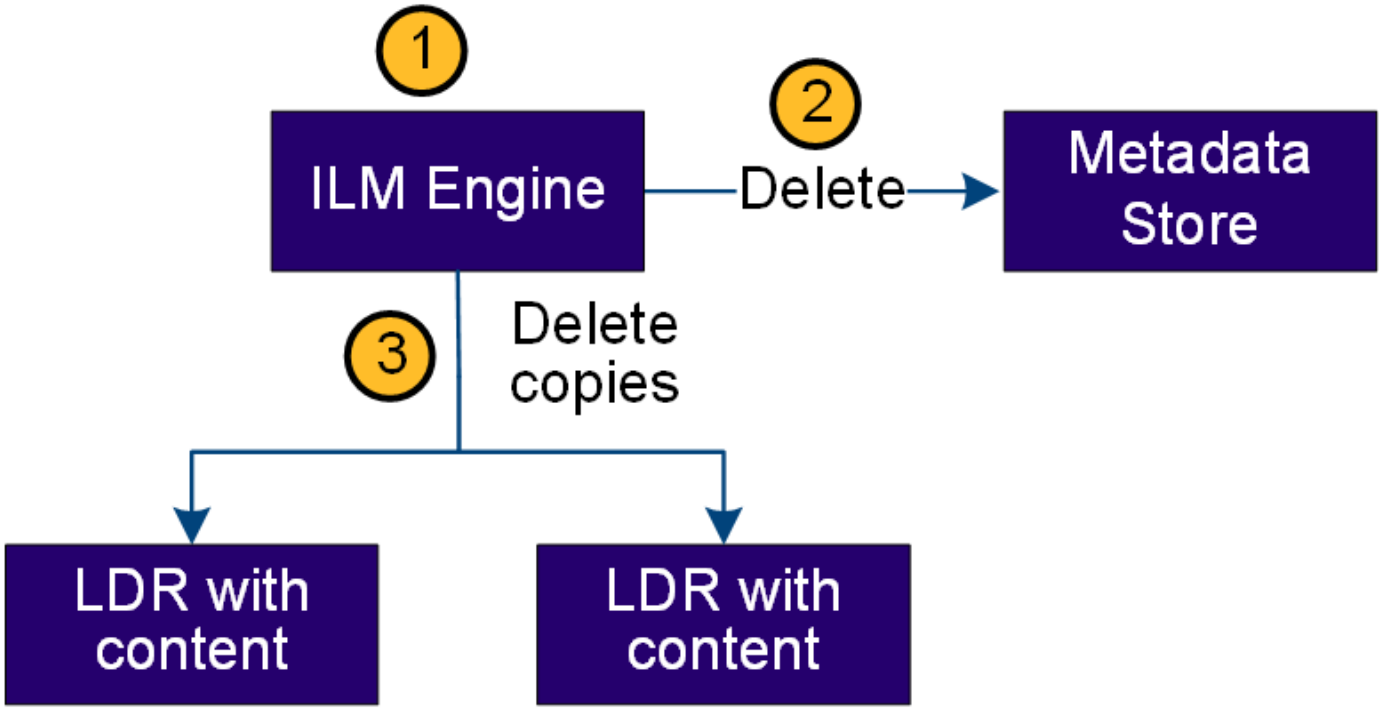
Datenfluss für Clientlöschungen



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.

Informationslebenszyklusmanagement in StorageGRID

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

ILM-Regeln definieren:

- Welche Objekte sollen gespeichert werden? Eine Regel kann für alle Objekte gelten, oder Sie können Filter angeben, um zu ermitteln, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder bestimmten Metadatenwerten verknüpft sind.
- Speichertyp und -Standort. Objekte können auf Storage-Nodes oder in Cloud-Speicherpools gespeichert werden.
- Der Typ der Objektkopien, die erstellt wurden. Kopien können repliziert oder zur Fehlerkorrektur codiert werden.

- Für replizierte Kopien die Anzahl der Kopien, die erstellt werden.
- Für Kopien, die nach Erasure Coding codiert wurden, wird das Verfahren zur Fehlerkorrektur 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.

Beispiel für eine ILM-Regel

Eine ILM-Regel könnte beispielsweise Folgendes angeben:

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

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

Bewertung von Objekten durch eine ILM-Richtlinie

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

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

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

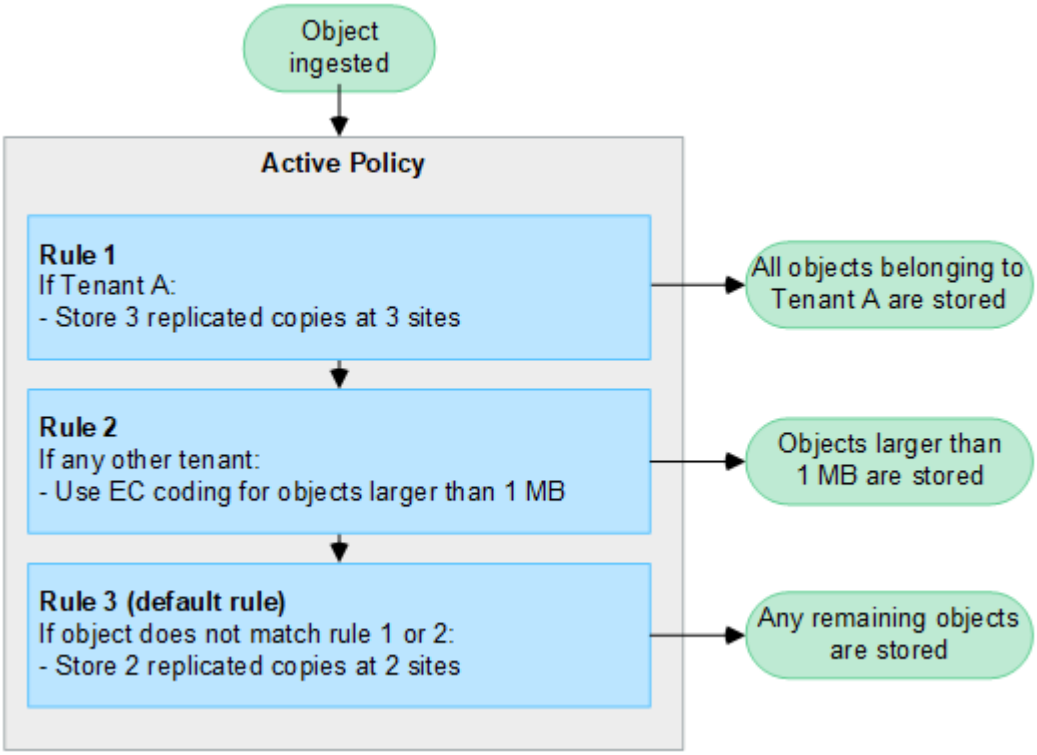
Beispiel für eine ILM-Richtlinie

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

- **Regel 1: Replizierte Kopien für Mandant A**

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

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



Verwandte Informationen

- "Objektmanagement mit ILM"

Entdecken Sie StorageGRID

Erkunden Sie den StorageGRID Grid Manager

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

Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispielbildern auf dieser Seite überein.

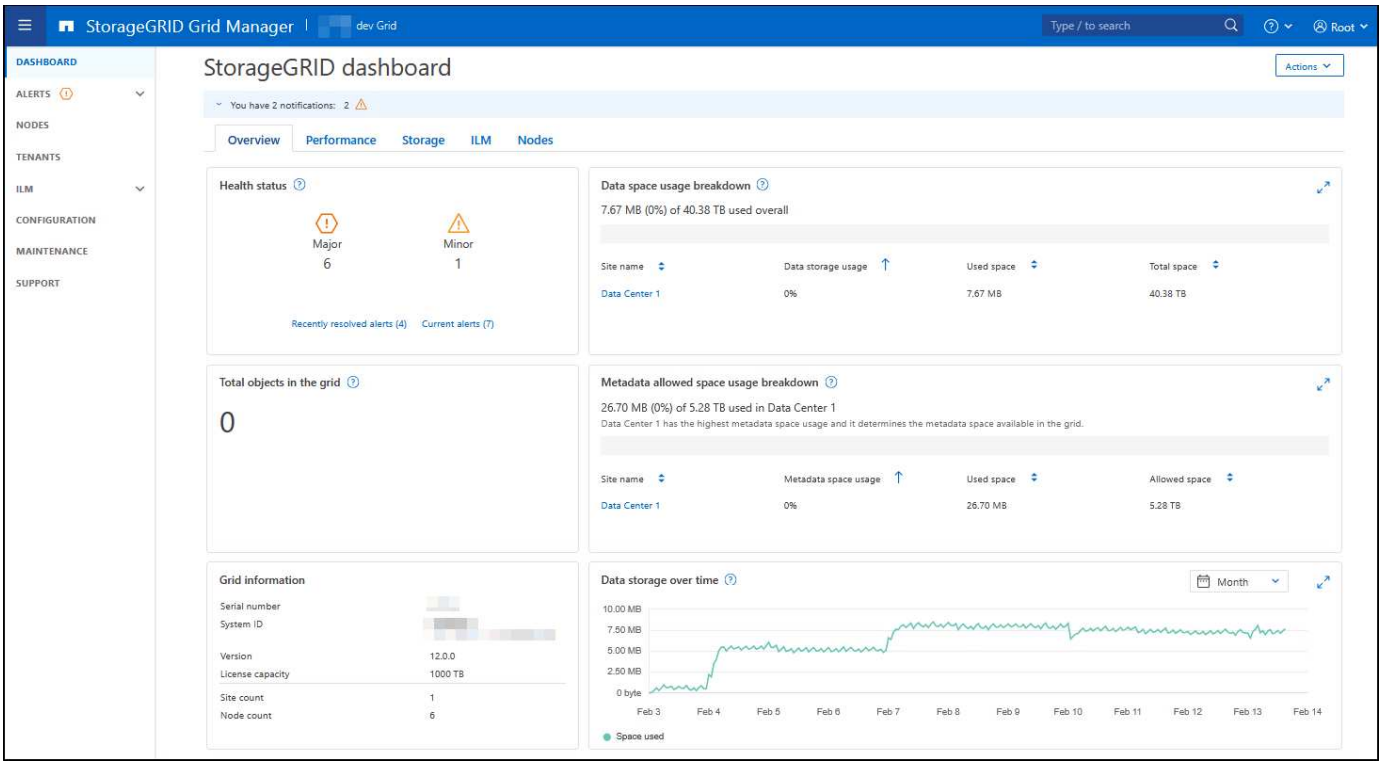
Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Jedes StorageGRID System umfasst einen primären Admin-Node und eine beliebige Anzahl nicht primärer Admin-Nodes. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten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

Sie können den Grid-Manager über einen aufrufen"Unterstützter Webbrowser".

Grid Manager Dashboard

Wenn Sie sich zum ersten Mal beim Grid Manager anmelden, haben Sie im Dashboard Zugriff auf "Überwachen Sie Systemaktivitäten"einen Blick.

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



Um eine Erklärung der auf jeder Karte angezeigten Informationen zu erhalten, wählen Sie das Hilfesymbol (?) für diese Karte aus.

Suchfeld

Mit dem Feld **Suche** in der Kopfzeile können Sie schnell zu einer bestimmten Seite in Grid Manager navigieren. Sie können beispielsweise **km** eingeben, um auf die Seite Key Management Server (KMS) zuzugreifen.

Sie können **Suche** verwenden, um Einträge in der Seitenleiste des Grid Managers sowie in den Menüs Konfiguration, Wartung und Support zu finden. Sie können auch nach Namen nach Elementen wie Grid-Nodes und Mandantenkonten suchen.

Hilfe-Menü

Über das Hilfemenü  können Sie auf Folgendes zugreifen:

- Der"FabricPool" Und"S3-Einrichtung" Zauberer
- Die StorageGRID -Dokumentationsseite für die aktuelle Version
- "API-Dokumentation"
- Informationen darüber, welche Version von StorageGRID derzeit installiert ist

Menü „Meldungen“

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

Über das Menü „Alarme“ können Sie folgende Aktionen ausführen"Managen von Warnmeldungen":

- Überprüfen Sie aktuelle Warnmeldungen
- Überprüfen Sie behobene Warnmeldungen
- Konfigurieren Sie Stille, um Benachrichtigungen zu unterdrücken
- Definieren Sie Alarmregeln für Bedingungen, die Warnmeldungen auslösen
- Konfigurieren Sie den E-Mail-Server für Warnmeldungen

Knoten Seite

Der"Knoten Seite" zeigt Informationen zum gesamten Raster, zu jedem Standort im Raster und zu jedem Knoten an einem Standort an. Um Informationen zu einer bestimmten Site oder einem bestimmten Knoten anzuzeigen, wählen Sie die Site oder den Knoten aus.

Mandanten werden gestartet

"Mandanten werden gestartet"Mit können Sie "Erstellen und überwachen Sie die Konten von Storage-Mandanten"für Ihr StorageGRID-System. Sie müssen mindestens ein Mandantenkonto erstellen, um anzugeben, wer Objekte speichern und abrufen kann und welche Funktionen ihnen zur Verfügung stehen.

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

ILM-Menü

Das ermöglicht Ihnen "Konfigurieren Sie die Regeln und Richtlinien für Information Lifecycle Management (ILM)"das "ILM-Menü"Regieren von Datenaufbewahrungszeit und -Verfügbarkeit. Sie können auch eine Objekt-ID eingeben, um die Metadaten für das Objekt anzuzeigen.

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Storage-Pools

- Lagergüten
- Regionen
- Suche nach Objektmetadaten

Konfigurationsmenü

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

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

- "Management von Hochverfügbarkeitsgruppen"
- "Verwalten von Load Balancer-Endpunkten"
- "Konfigurieren Sie die Domänennamen des S3-Endpunkts"
- "Verwalten von Richtlinien zur Verkehrsklassifizierung"
- "Konfigurieren Sie die VLAN-Schnittstellen"
- "Aktivieren Sie StorageGRID CORS für eine Verwaltungsschnittstelle"

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

- "Verwalten von Sicherheitszertifikaten"
- "Interne Firewall-Kontrollen verwalten"
- "Konfigurieren von Verschlüsselungsmanagement-Servern"
- Konfigurieren Sie Sicherheitseinstellungen, einschließlich der"TLS- und SSH-Richtlinie" ,"Optionen für die Netzwerk- und Objektsicherheit" ,"Sicherheitseinstellungen der Schnittstelle" , Und"SSH-Zugriffsoptionen"
- Konfigurieren Sie Einstellungen für eine"Storage-Proxy" oder ein"Admin-Proxy"

Systemaufgaben

Zu den Systemaufgaben gehören:

- Verwenden"Grid-Verbund" zum Klonen von Mandantenkontoinformationen und Replizieren von Objektdaten zwischen zwei StorageGRID Systemen
- Aktivieren Sie optional die"Gespeicherte Objekte komprimieren" Option
- Konfigurieren Sie optional die"Standardeinstellung für die Bucket-Konsistenz"
- "S3-Objektsperre verwalten"
- Verstehen Sie Speichereinstellungen wie"Wasserzeichen für Storage-Volumes"
- "Profile für das Erasure Coding managen"

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- "Konfigurieren der Protokollverwaltung"
- "Verwenden Sie SNMP-Überwachung"

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugriffssteuerung gehören:

- "Managen von Admin-Gruppen"
- "Verwalten von Administratorbenutzern"
- Ändern Sie die"Provisionierungs-Passphrase" oder"Passwörter für die Node-Konsole"
- "Verwenden Sie den Identitätsverbund"
- "SSO konfigurieren"

Menü Wartung

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

Aufgaben

Zu den Wartungsarbeiten gehören:

- "Stilllegungsvorgänge" Um nicht verwendete Grid-Nodes und -Standorte zu entfernen
- "Erweiterungsoperationen" Um neue Grid-Nodes und -Standorte hinzuzufügen
- "Verfahren zur Recovery von Grid-Nodes" Zum Ersetzen eines fehlerhaften Node und Wiederherstellen von Daten
- "Verfahren umbenennen" Ändern der Anzeigenamen des Rasters, der Standorte und Knoten
- "Vorgänge zur Überprüfung der Objektexistenz" Um das Vorhandensein von Objektdaten (wenn auch nicht die Richtigkeit) zu überprüfen
- Führen Sie einen"Neustart wird durchgeführt" um mehrere Grid-Knoten neu zu starten
- "Volume-Wiederherstellungsvorgänge"

System

Sie können folgende Systemwartungsaufgaben ausführen:

- "Zeigen Sie StorageGRID Lizenzinformationen an"oder"Lizenzinformationen aktualisieren"
- Generieren und Herunterladen der"Wiederherstellungspaket"
- StorageGRID Software-Updates, einschließlich Software-Upgrades und Hotfixes, sowie Updates für die SANtricity OS Software auf ausgewählten Appliances
  - "Upgrade-Verfahren"
  - "Hotfix-Verfahren"
  - "Aktualisieren Sie das SANtricity Betriebssystem auf SG6000 Storage Controllern mithilfe des Grid Manager"
  - "Aktualisieren Sie das SANtricity Betriebssystem auf SG5700 Storage Controllern mithilfe des Grid Manager"

Netzwerk

Sie können folgende Aufgaben zur Netzwerkwartung ausführen:

- "Konfigurieren Sie DNS-Server"
- "Aktualisieren von Grid-Netzwerk-Subnetzen"
- "Managen von NTP-Servern"

Menü „Support“

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

Tools

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

- "Konfigurieren Sie AutoSupport"
- "Führen Sie eine Diagnose aus" Auf den aktuellen Zustand des Rasters
- "Erfassen von Protokolldateien und Systemdaten"
- "Prüfen von Support-Kennzahlen"

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

Sonstiges

Im anderen Bereich des Menüs „Support“ haben Sie folgende Möglichkeiten:

- Konfigurieren"E/A-Priorisierung"
- Konfigurieren"AutoSupport -E-Mail-Setup (Legacy)"
- Managen "Verbindungskosten"
- Anzeigen von Knotendienst-IDs
- Managen "Storage-Wasserzeichen"

Erkunden Sie den StorageGRID Tenant Manager

Das "Mandanten-Manager" ist die browserbasierte grafische Schnittstelle, auf die Mandantenbenutzer zugreifen, um ihre Storage-Konten zu konfigurieren, zu managen und zu überwachen.

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

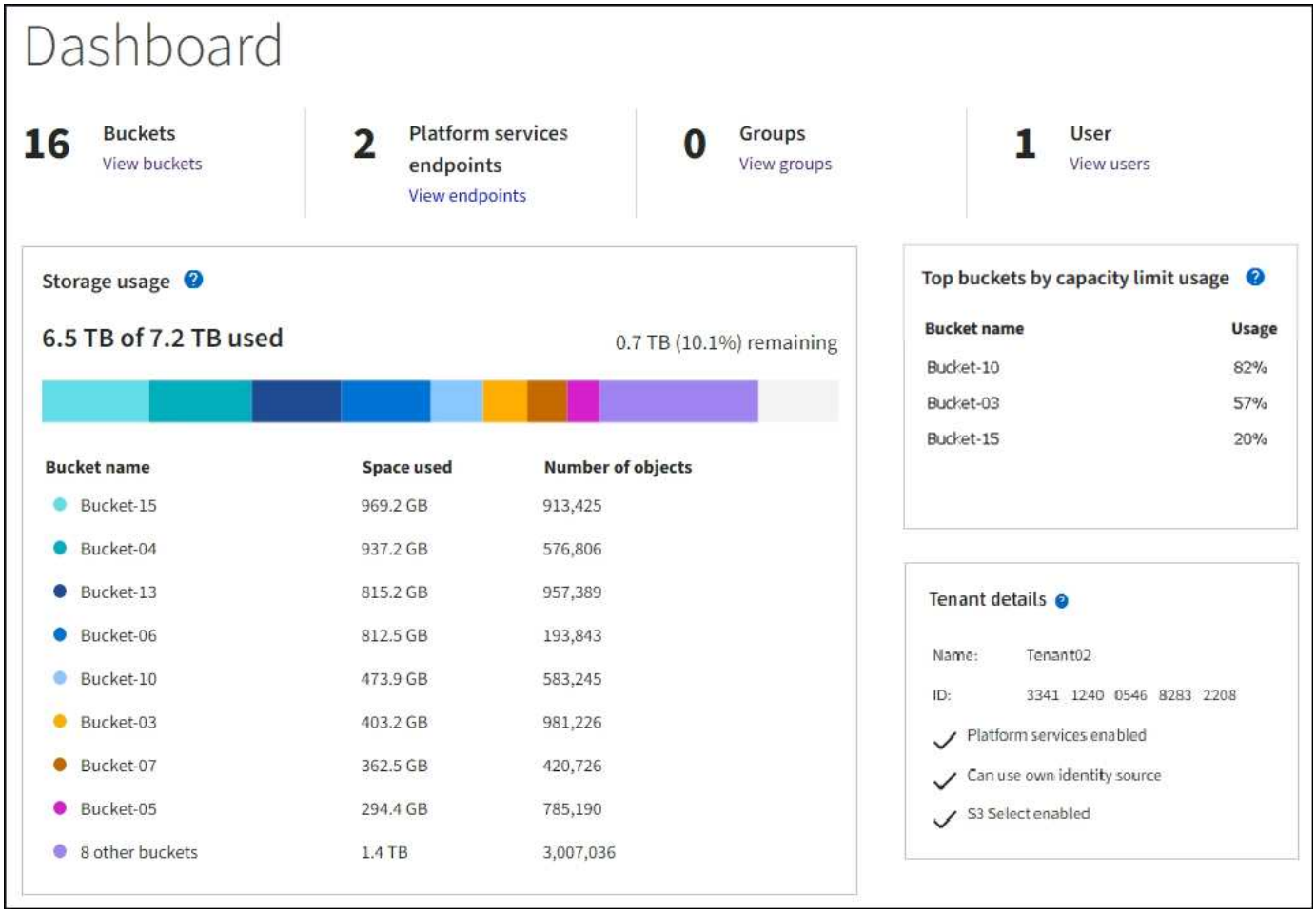
Wenn sich Mandantenbenutzer beim Mandanten-Manager anmelden, stellen sie eine Verbindung zu einem Admin-Node her.

Mandanten-Manager Dashboard

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

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

Der über dem Balkendiagramm angezeigte Wert ist 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.



Speichermenü (S3)

Über dieses Menü können S3-Benutzer:

- Zugriffsschlüssel verwalten
- Buckets erstellen, verwalten und löschen
- Verwalten von Plattform-Services-Endpunkten
- Alle Grid-Föderation-Verbindungen anzeigen, die sie verwenden dürfen

Meine Zugriffsschlüssel

S3-Mandantenbenutzer können die Zugriffschlüssel wie folgt managen:

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

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

Buckets

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

- Buckets erstellen
- Aktivieren der S3-Objektsperre für einen neuen Bucket (vorausgesetzt, dass die S3-Objektsperre für das StorageGRID-System aktiviert ist)
- Aktualisieren Sie die Konsistenzwerte
- Aktivieren und deaktivieren Sie die Zeitaktualisierungen für den letzten Zugriff
- Aktivieren oder Anhalten der Objektversionierung
- Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung
- Konfiguration der Cross-Origin Resource Sharing (CORS)
- Löschen aller Objekte in einem Bucket
- Leere Buckets löschen
- Mit "S3-Konsole"können Sie Bucket-Objekte managen

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

Plattform-Services-Endpunkte

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

Netzverbundverbindungen

Wenn ein Grid-Administrator die Verwendung einer Grid-Verbundverbindung für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit Root-Zugriffsberechtigungen den Verbindungsnamen anzeigen und die Seite mit Bucket-Details für jeden Bucket aufrufen, für den die Grid-übergreifende Replizierung aktiviert ist, Und zeigen Sie den letzten Fehler an, der beim Replizieren von Bucket-Daten in das andere Grid in der Verbindung auftritt. Siehe "Anzeigen von Verbindungen mit Grid Federation".

Öffnen Sie das Menü Management

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

Netzwerkrichtlinien

Netzwerkrichtlinien für StorageGRID

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

Informationen zu diesen Anweisungen

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

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

- Speichern und Abrufen von Objektdaten
- Benachrichtigungen erhalten
- Zugriff auf die StorageGRID Management-Schnittstelle (Grid Manager und MandantenManager)
- Zugriff auf die Revisionsfreigabe (optional)
- Die Bereitstellung von Services wie:
  - Network Time Protocol (NTP)
  - Domain Name System (DNS)
  - Verschlüsselungsmanagement-Server (KMS)

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

Bevor Sie beginnen

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

Bevor Sie das Netzwerk konfigurieren, machen Sie sich mit der StorageGRID-Architektur vertraut, wie in beschrieben"Weitere Informationen zu StorageGRID".

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

Installieren Sie Appliance-Knoten

- "Appliance-Hardware installieren"

Installation softwarebasierter Nodes

- "Installieren Sie StorageGRID auf softwarebasierten Knoten"

StorageGRID Software konfigurieren und verwalten

- "StorageGRID verwalten"
- "Versionshinweise"

StorageGRID-Netzwerktypen

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

Verkehrstypen

Verkehrstyp	Beschreibung	Netzwerktyp
Grid-Traffic	Der interne StorageGRID-Datenverkehr zwischen allen Nodes im Grid. Alle Grid-Nodes müssen über dieses Netzwerk mit allen anderen Grid-Nodes kommunizieren können.	Grid-Netzwerk (erforderlich)
Admin-Datenverkehr	Der für die Systemadministration und -Wartung verwendete Datenverkehr.	Admin-Netzwerk (optional), VLAN-Netzwerk (optional)
Client-Traffic	Der Datenverkehr, der zwischen externen Client-Applikationen und dem Grid übertragen wird, einschließlich aller Objekt-Storage-Anforderungen von S3-Clients.	Client-Netzwerk (optional), VLAN-Netzwerk (optional)

Sie haben folgende Möglichkeiten zur Konfiguration des Netzwerks:

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

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

administrativen und Client-Datenverkehr verwenden.

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

Netzwerkschnittstellen

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

Netzwerk	Schnittstellenname
Grid-Netzwerk (erforderlich)	eth0
Admin-Netzwerk (optional)	eth1
Client-Netzwerk (optional)	eth2

Weitere Informationen zum Zuordnen virtueller oder physischer Ports zu Knotennetzwerkschnittstellen finden Sie unter"Installieren Sie StorageGRID auf softwarebasierten Knoten" .

Appliance-Nodes

- "Storage Appliance SG6160"
- "Storage Appliance SGF6112"
- "Storage Appliance SG6000"
- "Storage Appliance SG5800"
- "Storage Appliance SG5700"
- "Service Appliances für SG110 und SG1100"
- "SG100- und SG1000-Services-Appliances"

Netzwerkinformationen für jeden Node

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

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

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

Hochverfügbarkeitsgruppen

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

Grid-Netzwerk

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

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

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

Wenn Sie das Grid-Netzwerk konfigurieren, müssen Sie sicherstellen, dass das Netzwerk von nicht vertrauenswürdigen Clients, wie denen im offenen Internet, geschützt ist.

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

- Das Grid-Netzwerk-Gateway muss konfiguriert werden, wenn es mehrere Grid-Subnetze gibt.
- Das Grid-Netzwerk-Gateway ist der Node-Standard-Gateway, bis die Grid-Konfiguration abgeschlossen ist.
- Statische Routen werden automatisch für alle Nodes zu allen Subnetzen generiert, die in der globalen Grid-Netzwerk-Subnetliste konfiguriert sind.
- Wenn ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway vom Grid-Netzwerk-Gateway zum Client-Netzwerk-Gateway, wenn die Grid-Konfiguration abgeschlossen ist.

Admin-Netzwerk

Das Admin-Netzwerk ist optional. Bei der Konfiguration kann diese für die Systemadministration und für den Wartungs-Traffic verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Knoten routingfähig sein.

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

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

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

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

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

- Das Admin-Netzwerk-Gateway ist erforderlich, wenn Verbindungen außerhalb des Subnetz Admin-

Netzwerks hergestellt werden oder wenn mehrere Admin-Netzwerk-Subnetze konfiguriert sind.

- Für jedes in der Admin-Netzwerk-Subnetz-Liste des Node konfigurierte Subnetz werden statische Routen erstellt.

Client-Netzwerk

Das Client-Netzwerk ist optional. Bei entsprechender Konfiguration wird er für den Zugriff auf Grid-Services für Client-Applikationen wie S3 verwendet. Wenn Sie StorageGRID Daten für eine externe Ressource zugänglich machen möchten (z. B. einen Cloud-Speicherpool oder den StorageGRID CloudMirror Replikationsservice), kann die externe Ressource auch das Client-Netzwerk nutzen. Grid-Knoten können mit jedem Subnetz kommunizieren, das über das Client-Netzwerk-Gateway erreichbar ist.

Sie können auswählen, auf welchen Grid-Knoten das Client-Netzwerk aktiviert sein soll. Alle Knoten müssen sich nicht im gleichen Client-Netzwerk befinden, und Knoten kommunizieren nie über das Client-Netzwerk miteinander. Das Client-Netzwerk ist erst nach Abschluss der Grid-Installation betriebsbereit.

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

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Datenverkehr nicht über das Grid-Netzwerk geleitet werden. Der 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 und den S3-Client-Zugriff auf das Grid bieten.
- Storage-Nodes, da diese Nodes Zugriff auf das S3-Protokoll, auf Cloud-Storage-Pools und den CloudMirror Replizierungsservice bieten.
- Admin-Nodes, um sicherzustellen, dass Mandantenbenutzer eine Verbindung zum Tenant Manager herstellen können, ohne das Admin-Netzwerk verwenden zu müssen.

Beachten Sie Folgendes für das Client-Netzwerk-Gateway:

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

Optionale VLAN-Netzwerke

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

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

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

konfiguriert.

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

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

Anweisungen und Richtlinien finden Sie unter"Konfigurieren Sie die VLAN-Schnittstellen".

VLAN-Schnittstellen werden nur in HA-Gruppen verwendet und auf dem aktiven Node werden VIP-Adressen zugewiesen. Anweisungen und Richtlinien finden Sie unter"Management von Hochverfügbarkeitsgruppen".

Beispiele für Netzwerktopologie

Grid-Netzwerktopologie für StorageGRID

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.

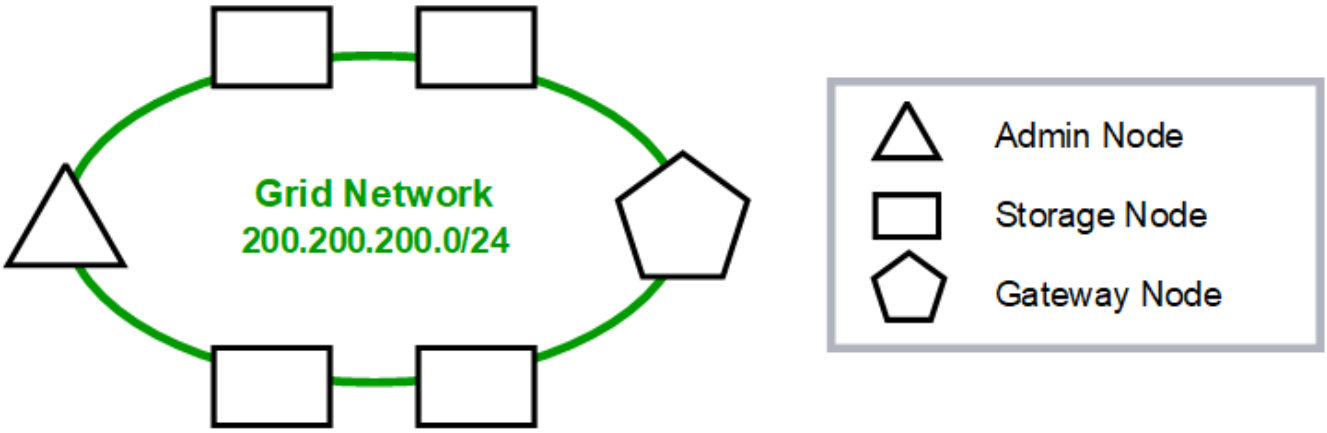
Während der Konfiguration müssen Sie alle Grid-Netzwerk-Subnetze der Grid-Netzwerk-Subnetz-Liste (GNSL) hinzufügen. Diese Liste enthält alle Subnetze für alle Standorte und kann auch externe Subnetze enthalten, die den Zugriff auf kritische Services wie NTP, DNS oder LDAP bieten.

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 wird für jeden Datenverkehr dasselbe Netzwerk verwendet, einschließlich Datenverkehr in Verbindung mit S3-Client-Anforderungen sowie Administrations- und Wartungsfunktionen.

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

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
	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 für StorageGRID

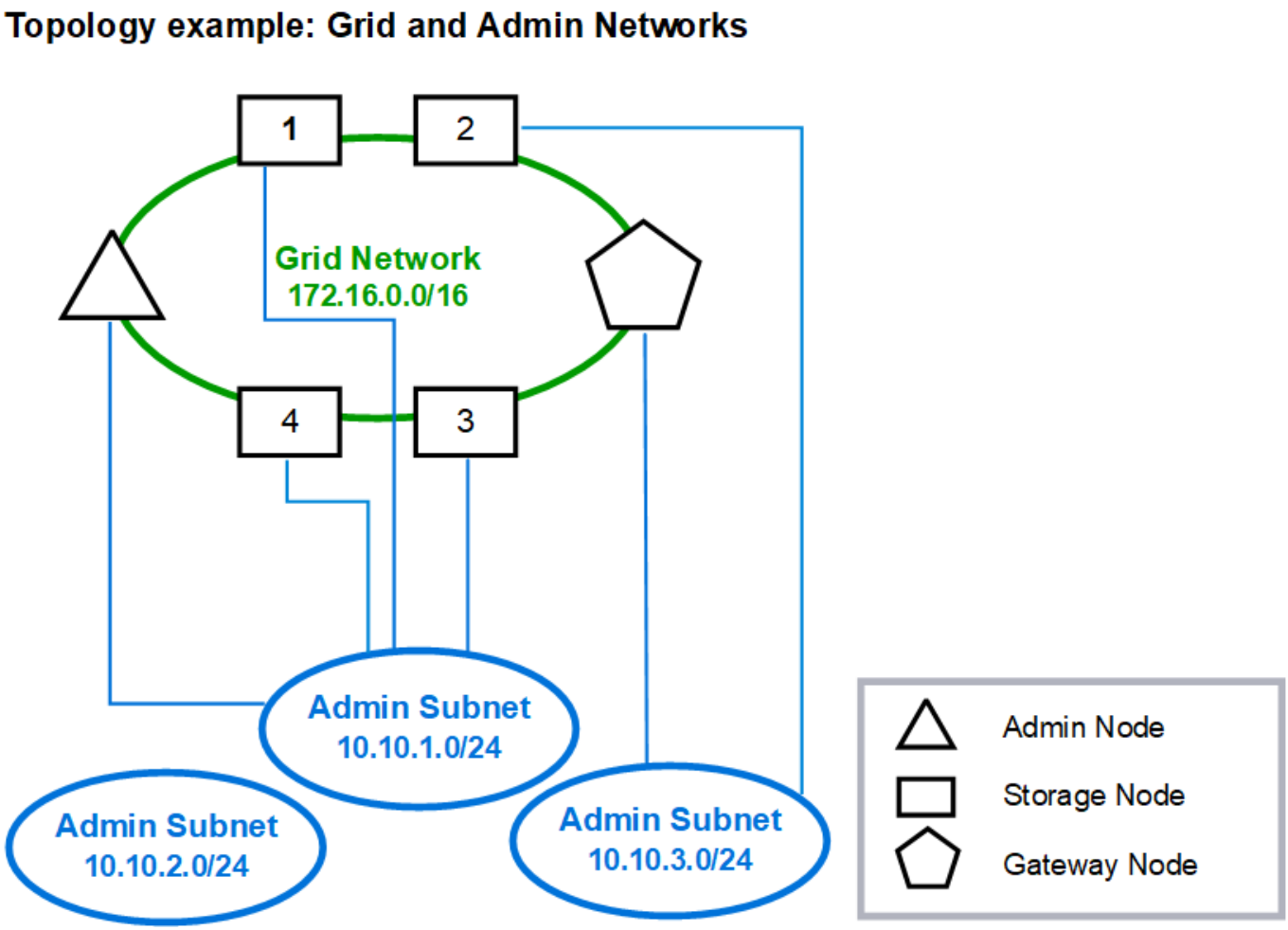
Die Verwendung eines Admin-Netzwerks ist optional. Eine Möglichkeit, wie Sie ein Admin-Netzwerk und ein Grid-Netzwerk verwenden können, besteht darin, ein routingbares Grid-Netzwerk und ein verbundes Admin-Netzwerk für jeden Knoten zu konfigurieren.

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-Netzwerk für Datenverkehr im Zusammenhang mit S3-Clientanforderungen und Objektmanagement verwendet, 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 für StorageGRID

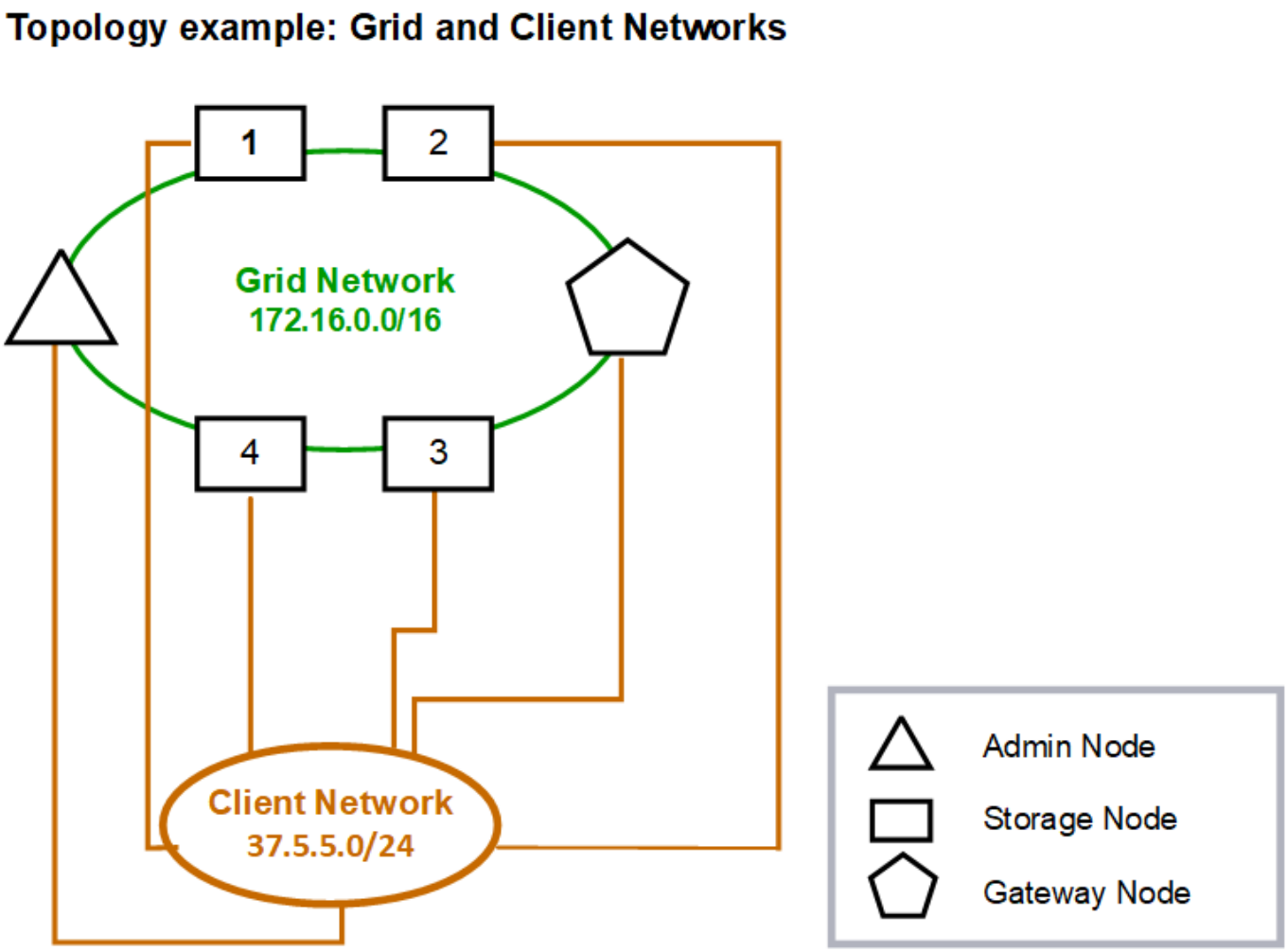
Ein Client-Netzwerk ist optional. Durch die Verwendung eines Client-Netzwerks kann der Client-Netzwerk-Traffic (beispielsweise S3) vom internen Grid-Traffic getrennt werden, sodass Grid-Netzwerke sicherer sind. Wenn das Admin-Netzwerk nicht konfiguriert ist, kann der administrative Datenverkehr entweder 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-Clientanforderungen und für Administrationsfunktionen

verwendet, während das Grid-Netzwerk für interne Objektverwaltungsvorgänge reserviert ist.



Provisioned

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

System Generated

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

Verwandte Informationen

"Ändern der Node-Netzwerkkonfiguration"

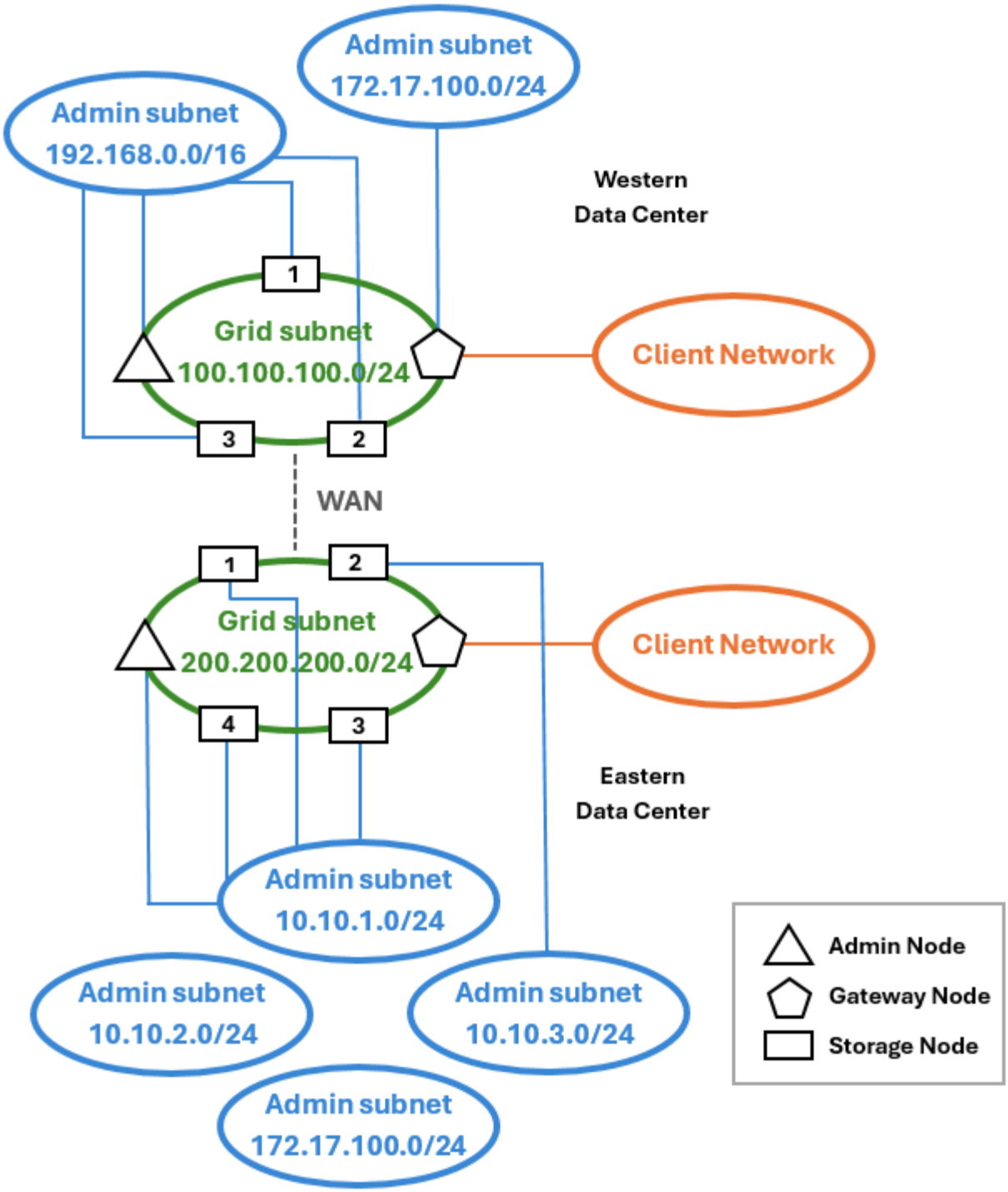
Netzwerktopologie für alle drei StorageGRID Netzwerke

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 im Zusammenhang mit S3-Clientanforderungen verwendet.

Topologiebeispiel: Grid, Admin und Client-Netzwerke



Netzwerkanforderungen für StorageGRID

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 vom Admin-Knoten zu einem oder einem vom `support.netapp.com` Kunden konfigurierten Proxy.
- **Externer Schlüsselverwaltungsserver**: Ausgehende TCP-Verbindung von jedem Appliance-Knoten mit aktivierter Node-Verschlüsselung.
- Eingehende TCP-Verbindungen von S3-Clients.
- Ausgehende Anforderungen von StorageGRID Plattform-Services wie CloudMirror Replizierung oder von Cloud-Storage-Pools.

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

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

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

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

Wide Area Networks (WANs) für mehrere Standorte

Bei der Konfiguration eines StorageGRID-Systems mit mehreren Standorten muss die WAN-Verbindung zwischen den Standorten eine Mindestbandbreite von 25 Mbit/s in jeder Richtung aufweisen, bevor der Client-Datenverkehr berücksichtigt wird. Datenreplizierung oder Erasure Coding zwischen Standorten, Erweiterung von Nodes oder Standorten, Recovery von Nodes und anderen Vorgängen oder Konfigurationen erfordern zusätzliche Bandbreite.

Die tatsächlichen Anforderungen an die WAN-Mindestbandbreite hängen von der Client-Aktivität und dem ILM-

Schutzschema ab. Wenden Sie sich an Ihren NetApp Professional Services Berater, um die Mindestanforderungen an die WAN-Bandbreite einschätzen zu können.

Verbindungen für Admin-Nodes und Gateway-Nodes

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

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

Verwendung von NAT (Network Address Translation)

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

Netzwerkspezifische Anforderungen für StorageGRID

Befolgen Sie die Anforderungen für jeden StorageGRID Netzwerktyp.

Netzwerk-Gateways und -Router

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

Subnetze

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

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

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

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

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

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

- Das Grid-Netzwerk-Subnetz für jeden Node muss in der GNSL enthalten sein.
- Das Subnetz Admin Network darf sich nicht mit dem Subnetz Grid Network, dem Subnetz Client Network oder einem Subnetz im GNSL überlappen.
- Die Subnetze im AESL dürfen sich nicht mit Subnetzen im GNSL überlappen.
- Das Client-Netzwerk-Subnetz darf sich nicht mit dem Subnetz des Grid-Netzwerks, dem Subnetz des Admin-Netzwerks, einem beliebigen Subnetz im GNSL oder einem beliebigen Subnetz im AESL überlappen.

Grid-Netzwerk

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

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

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

Admin-Netzwerk

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

Typische Verwendungszwecke des Admin-Netzwerks sind Managementverbindungen, AutoSupport, KMS und Verbindungen zu kritischen Servern wie NTP, DNS und LDAP, wenn diese Verbindungen nicht über das Grid-Netzwerk oder das Client-Netzwerk bereitgestellt werden.

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

Sie müssen mindestens ein Subnetz im Admin-Netzwerk definieren, um eingehende Verbindungen aus externen Subnetzen zu aktivieren. Für jedes Subnetz in der AESL werden automatisch statische Routen auf jedem Knoten erzeugt.

Client-Netzwerk

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

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

Verwandte Informationen

"Ändern der Node-Netzwerkkonfiguration"

Implementierungs-spezifische Netzwerküberlegungen

Netzwerkkonfiguration für StorageGRID Linux-Bereitstellungen

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

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

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

Siehe die"Installationsanweisungen" .

Hostnetzwerkkonfiguration für Container-Engine-Implementierungen

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

Physische Hosts

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

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

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

- Öffnen Sie die erforderlichen Ports zum Host.
- Wenn Sie beabsichtigen, VLAN-Schnittstellen in StorageGRID zu verwenden, muss der Host über eine oder mehrere Trunk-Schnittstellen verfügen, die Zugriff auf die gewünschten VLANs bieten. Diese Schnittstellen können als eth0, eth2 oder als zusätzliche Schnittstellen in den Node-Container übergeben werden. Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:
  - **Linux (vor der Installation des Knotens)**:"Erstellen von Node-Konfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**:"Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Knoten"

> „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Bereitstellung. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

Empfehlungen für die minimale Bandbreite

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

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

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

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

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

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

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

Einige empfohlene Methoden zum Konfigurieren physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung Ihrer StorageGRID Bereitstellung finden Sie unter"Konfigurieren Sie das Hostnetzwerk" .

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

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

Networking für Plattform-Services

Wie in und beschrieben"Management von Plattform-Services für Mandanten""Management von Plattform-Services", umfassen Plattformservices externe Dienste, die Suchintegration, Ereignisbenachrichtigung und CloudMirror-Replikation bieten.

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

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

Netzwerk für Cloud-Storage-Pools

Cloud-Storage-Pools erfordern außerdem Zugriff von Storage-Nodes auf die Endpunkte, die durch einen

externen Service wie Amazon S3 Glacier oder Microsoft Azure Blob Storage bereitgestellt werden. Weitere Informationen finden Sie unter "Was ist ein Cloud-Storage-Pool".

Ports für Plattform-Services und Cloud-Storage-Pools

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

- **80**: Für Endpunkt-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. Siehe "Referenz für Netzwerk-Ports".

Wenn Sie einen nicht transparenten Proxy-Server verwenden, müssen Sie auch "Konfigurieren Sie Speicher-Proxy-Einstellungen"zulassen, dass Nachrichten an externe Endpunkte wie z. B. einen Endpunkt im Internet gesendet werden.

VLANs und Plattform-Services und Cloud-Storage-Pools

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

Netzwerkkonfiguration für StorageGRID Appliance-Nodes

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

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

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

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

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

Netzwerkinstallation und Bereitstellung für StorageGRID

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, das Python-Skript oder die Installations-API verwenden `configure-storagegrid.py`, um das Raster zu konfigurieren und die registrierten Knoten 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 Genehmigungsprozesses des Knotens entfernen oder das Tool IP ändern verwenden, nachdem die Installation abgeschlossen ist (siehe "Konfigurieren Sie IP-Adressen").

Richtlinien nach der Installation für StorageGRID

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

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

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

  > Nodes werden neu gebootet, wenn die Grid-Netzwerkkonfiguration durch DHCP geändert wird. Dies kann zu Ausfällen führen, wenn eine DHCP-Änderung sich auf mehrere Nodes gleichzeitig auswirkt.

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

Referenz für Netzwerk-Ports

Interne Grid-Knotenkommunikation für StorageGRID

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

> NetApp empfiehlt, ICMP (Internet Control Message Protocol)-Datenverkehr zwischen den Grid-Knoten zu aktivieren. Wenn ICMP-Datenverkehr zugelassen wird, kann die Failover-Performance verbessert werden, wenn ein Grid-Knoten nicht erreicht werden kann.

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

Richtlinien für Linux-basierte Knoten

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

> Die Unterstützung für die Neuzuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter"Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts" .

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 die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports neu zuordnen, wenn Sie Knoten mithilfe des VMware vSphere Web Client bereitstellen oder indem Sie bei der Automatisierung der Grid-Knotenbereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen zur Port-Neuzuordnung und zu den Konfigurationsparametern für die Bereitstellung finden Sie in den Anweisungen für"Installieren von StorageGRID auf VMware" .

> Die Unterstützung für die Neuzuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter"Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts" .

Richtlinien für Appliance-Nodes

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

> Die Unterstützung für die Neuzuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter"Entfernen Sie Port-Neuzuordnungen auf StorageGRID -Geräten" .

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.
1055	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
1139	TCP	Storage-Nodes	Storage-Nodes	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Nodes	Storage-Nodes mit ADC	Reporting-, Audit- und Konfigurationsdatenverkehr.
1502	TCP	Alle Nodes	Storage-Nodes	Interner S3-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.

Port	TCP oder UDP	Von	Bis	Details
1511	TCP	Alle Nodes	Storage-Nodes	Interner Metadaten-Datenverkehr:
5353	UDP	Alle Nodes	Alle Nodes	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
7001	TCP	Storage-Nodes	Storage-Nodes	Cassandra TLS zwischen Nodes-Cluster-Kommunikation
7443	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Node	Appliance-Nodes	Interner Datenverkehr im Zusammenhang mit dem Wartungsmodus.
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 für die Weiterleitung von AutoSupport-Paketen vom E-Series SANtricity System Manager zum primären Admin-Node verwendet.
10342	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
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.

Port	TCP oder UDP	Von	Bis	Details
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	Alle Nodes	Alle Nodes	Interner Datenverkehr des Chunk-Dienstes für Erasure Coding und Replikation
18082	TCP	Admin/Storage-Nodes	Storage-Nodes	Interner S3-Datenverkehr.
18086	TCP	Alle Nodes	Storage-Nodes	Interner Datenverkehr im Zusammenhang mit dem LDR-Dienst.
18200	TCP	Admin/Storage-Nodes	Storage-Nodes	Weitere Statistiken zu Client-Anforderungen.
19000	TCP	Admin/Storage-Nodes	Storage-Nodes mit ADC	Keystone-Service: Interner Datenverkehr.

Verwandte Informationen

"Externe Kommunikation"

Externe Kommunikation für StorageGRID

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

Eingeschränkter Zugriff auf Ports

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, können Sie einen der folgenden Schritte ausführen:

- Mit "Load Balancer-Endpunkte" können Sie den Zugriff auf benutzerdefinierte Ports zulassen.
- Weisen Sie bei der Implementierung von Nodes Ports neu zu. Sie sollten jedoch die Load Balancer-Endpunkte nicht neu zuordnen. Weitere Informationen zur Port-Neuzuweisung für den StorageGRID-Node finden Sie unter:

Die Unterstützung für die Neuzuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter"Entfernen Sie Port-Neuzuordnungen auf StorageGRID -Geräten" oder"Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts" .

- "Port-Neuzuordnungsschlüssel für StorageGRID auf Red hat Enterprise Linux"
- "Ports für StorageGRID auf VMware neu zuordnen"
- "Optional: Netzwerkports für Appliance neu zuordnen"

Anschlüsse für externe Kommunikation

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

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

Port	TCP oder UDP	Protokoll	Von	Bis	Details
22	TCP	SSH	Service-Laptop	Alle Nodes	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden. **Hinweis**: Dieser Port wird nur benötigt, wenn Sie den SSH-Zugriff für bestimmte Wartungsarbeiten aktivieren müssen.
25	TCP	SMTP	Admin-Nodes	E-Mail-Server	Wird für Warnungen und E-Mail-basierte AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 über die Seite „E-Mail-Server“ außer Kraft setzen.
53	TCP/UDP	DNS	Alle Nodes	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Nodes	DHCP-Service	Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für statisch konfigurierte Grids ausgeführt.
68	UDP	DHCP	DHCP-Service	Alle Nodes	Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für Raster ausgeführt, die statische IP-Adressen verwenden.
80	TCP	HTTP	Browser	Admin-Nodes	Port 80 wird für die Admin-Node-Benutzeroberfläche an Port 443 umgeleitet.

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-Nachrichten verwendet, die an AWS oder andere externe Services gesendet werden, die HTTP verwenden. Mandanten können beim Erstellen eines Endpunkts die Standard-HTTP-Porteinstellung 80 außer Kraft setzen.
80	TCP	HTTP	Storage-Nodes	AWS	Cloud-Storage-Pools-Anfragen werden an AWS-Ziele mit HTTP gesendet. Grid-Administratoren können die HTTP-Porteinstellung von 80 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen.
123	UDP	NTP	Primäre NTP-Knoten	Externe NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Nodes synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.
161	TCP/UDP	SNMP	SNMP-Client	Alle Nodes	Wird für SNMP-Abfrage verwendet. Alle Nodes bieten grundlegende Informationen, Admin-Nodes stellen auch Warnungsdaten bereit. 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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
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.
443	TCP	HTTPS	Browser	Admin-Nodes	Wird von Webbrowsern und Management-API-Clients verwendet, um auf den Grid Manager und den Tenant Manager zuzugreifen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren Sie die Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.
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	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 beim Erstellen eines Endpunkts die Standard-HTTP-Porteinstellung 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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
5353	UDP	MDNS	Alle Nodes	Alle Nodes	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
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.
8443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren Sie die Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.
8443	TCP	HTTPS	Browser	Appliances	Wird von Webbrowsern und Verwaltungs-API-Clients verwendet, um auf das StorageGRID Appliance Installer zuzugreifen. **Hinweis**: Port 443 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
9022	TCP	SSH	Service-Laptop	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.
9092	TCP	Kafka	Storage-Nodes mit ADC	Kafka-Cluster	Wird für Meldungen über Plattformdienste verwendet, die an ein Kafka-Cluster gesendet werden. Mandanten können beim Erstellen eines Endpunkts die Standard-Kafka-Porteinstellung 9092 außer Kraft setzen.
9443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Verwaltungs-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen.
18082	TCP	HTTPS	S3-Clients	Storage-Nodes	S3-Client-Traffic direkt zu Storage-Nodes (HTTPS).
18084	TCP	HTTP	S3-Clients	Storage-Nodes	S3-Client-Traffic direkt zu Storage-Nodes (HTTP).
23000-23999	TCP	HTTPS	Alle Nodes im Quell-Grid für die Grid-übergreifende Replizierung	Admin Nodes und Gateway Nodes im Ziel-Grid für Grid-übergreifende Replizierung	Dieser Port-Bereich ist für Grid Federation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden den gleichen Port.

Schnellstart für StorageGRID

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

Lernen, Planen und Sammeln von Daten

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

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

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

Überprüfen "Weitere Informationen zu StorageGRID" und die "Netzwerkrichtlinien".

Installieren Sie Nodes

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

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

Mehr erfahren:

- "Appliance-Hardware installieren"
- "Installieren Sie StorageGRID auf softwarebasierten Knoten"

Melden Sie sich an und prüfen Sie den Systemzustand

Wenn die Grid-Installation abgeschlossen ist, können Sie sich beim Grid Manager anmelden. Von dort aus können Sie den allgemeinen Zustand Ihres neuen Systems überprüfen, AutoSupport und Warn-E-Mails aktivieren und S3-Endpunktdomänennamen einrichten.

Mehr erfahren:

- "Melden Sie sich beim Grid Manager an"
- "Systemzustand überwachen"
- "Konfigurieren Sie AutoSupport"
- "Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"
- "Konfigurieren Sie die Domänennamen des S3-Endpunkts"

Konfiguration und Management

Die Konfigurationsaufgaben, die Sie für ein neues StorageGRID-System durchführen müssen, hängen davon

ab, wie Sie Ihr Grid verwenden. Sie richten mindestens den Systemzugriff ein, verwenden die FabricPool- und S3-Assistenten und managen verschiedene Storage- und Sicherheitseinstellungen.

Mehr erfahren:

- "Kontrolle über den StorageGRID-Zugriff"
- "Verwenden Sie den S3-Einrichtungsassistenten"
- "Verwenden Sie den FabricPool-Einrichtungsassistenten"
- "Sicherheitsmanagement"
- "Systemhärtung"

Richten Sie ILM ein

Sie steuern die Platzierung und Dauer jedes Objekts in Ihrem StorageGRID System, indem Sie eine ILM-Richtlinie (Information Lifecycle Management) konfigurieren, die aus einer oder mehreren ILM-Regeln besteht. Die ILM-Regeln erklären StorageGRID, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien über einen längeren Zeitraum gemanagt werden.

Mehr erfahren: "Objektmanagement mit ILM"

Verwenden Sie StorageGRID

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

Mehr erfahren:

- "Verwenden Sie ein Mandantenkonto"
- "Verwenden der S3-REST-API"

Überwachung und Fehlerbehebung

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

Mehr erfahren:

- "Monitoring von StorageGRID"
- "Fehler bei StorageGRID beheben"

Erweiterung, Wartung und Recovery

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

Mehr erfahren:

- "Erweitern Sie ein Raster"
- "Grid warten"
- "Knoten wiederherstellen"