Los geht's

StorageGRID software

NetApp
July 23, 2026

Inhalt

Einstieg in ein StorageGRID System

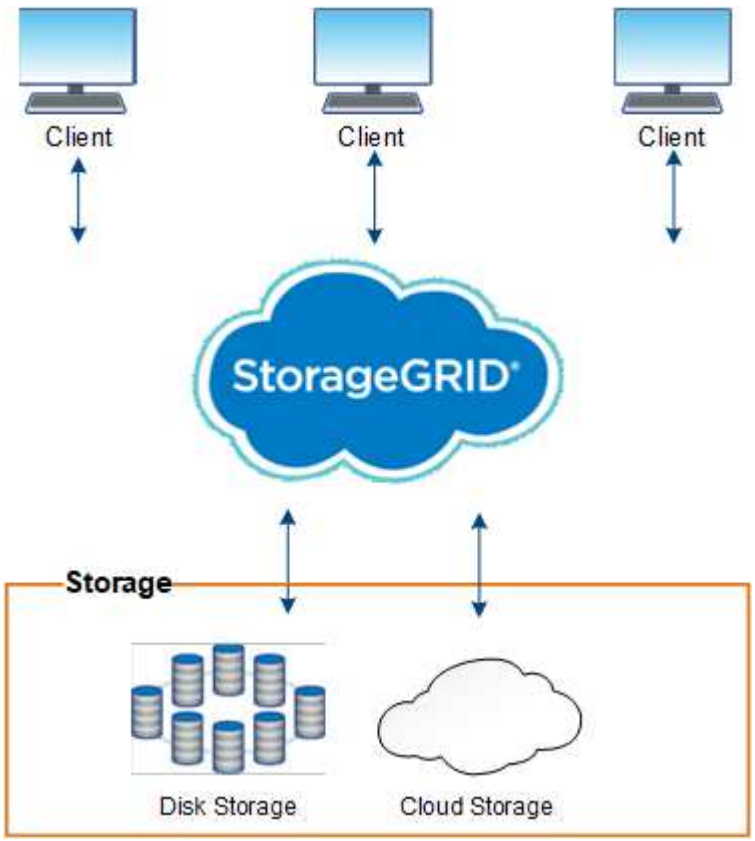
Informationen zu StorageGRID

Was ist StorageGRID?

NetApp® StorageGRID® ist eine softwaredefinierte Objektspeicherlösung, die ein breites Spektrum an Anwendungsfällen in öffentlichen, privaten und hybriden Multicloud-Umgebungen unterstützt. StorageGRID bietet native Unterstützung für die Amazon S3 API und liefert branchenführende Innovationen wie automatisiertes Lifecycle-Management, um unstrukturierte Daten kosteneffizient über lange Zeiträume zu speichern, zu sichern, zu schützen und zu erhalten.

StorageGRID bietet sicheren, dauerhaften Speicher für unstrukturierte Daten in großem Umfang. Integrierte, metadatengesteuerte Lifecycle-Management-Richtlinien optimieren, wo Ihre Daten während ihres gesamten Lebens gespeichert werden. Inhalte werden am richtigen Ort, zur richtigen Zeit und auf der richtigen Storage-Ebene abgelegt, um Kosten zu senken.

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



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

StorageGRID Vorteile

Zu den Vorteilen des StorageGRID Systems gehören die folgenden:

- Ein massiv skalierbares und benutzerfreundliches, geografisch verteiltes Datenrepository für unstrukturierte Daten.
- Das Standard-Objektspeicherprotokoll Amazon Web Services Simple Storage Service (S3).
- Hybrid Cloud enabled. Richtlinienbasiertes Information Lifecycle Management (ILM) speichert Objekte in öffentlichen Clouds, darunter Amazon Web Services (AWS) und Microsoft Azure. StorageGRID Plattformdienste ermöglichen die Replikation von Inhalten, Ereignisbenachrichtigungen und die Metadatensuche von Objekten, die in öffentlichen Clouds gespeichert sind.
- Flexibler Datenschutz gewährleistet Langlebigkeit und Verfügbarkeit. Daten können durch Replikation und mehrstufige Löschungscodierung geschützt werden. Die Überprüfung ruhender und übertragener Daten sichert deren Integrität für die Langzeitarchivierung.
- Dynamisches Datenlebenszyklusmanagement zur Optimierung der Speicherkosten. ILM-Regeln können erstellt werden, die den Datenlebenszyklus auf Objektebene verwalten und Datenlokalität, Haltbarkeit, Leistung, Kosten und Aufbewahrungsdauer individuell anpassen.
- Hohe Verfügbarkeit von Datenspeicherung und einigen Verwaltungsfunktionen, mit integriertem Lastausgleich zur Optimierung der Datenlast über StorageGRID Ressourcen.
- Unterstützung für mehrere Speichermandantenkonten, um die auf Ihrem System gespeicherten Objekte nach verschiedenen Entitäten zu trennen.
- Zahlreiche Tools zur Überwachung des Zustands Ihres StorageGRID Systems, darunter ein umfassendes Alarmsystem, ein grafisches Dashboard und detaillierte Statusinformationen für alle Knoten und Standorte.
- Unterstützung für software- oder hardwarebasierte Bereitstellung. StorageGRID kann auf einer der folgenden Plattformen bereitgestellt werden:
  - Virtuelle Maschinen, die in VMware ausgeführt werden.
  - Container-Engines auf Linux Hosts.
  - StorageGRID Appliances.
    - Speichergeräte bieten Objektspeicherung.
    - Servicegeräte bieten Grid-Administration und Lastausgleichsdienste.
- Entspricht den einschlägigen Storage-Anforderungen dieser Verordnungen:
  - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), welche Börsenmitglieder, Broker oder Händler reguliert.
  - Regel 4511(c) der Financial Industry Regulatory Authority (FINRA), die sich auf die Format- und Medienanforderungen der SEC Rule 17a-4(f) bezieht.
  - Commodity Futures Trading Commission (CFTC) in Verordnung 17 CFR § 1.31(c)-(d), die den Handel mit Rohstoff-Futures regelt.
- Unterbrechungsfreie Upgrade- und Wartungsarbeiten. Der Zugriff auf Inhalte bleibt während Upgrade-, Erweiterungs-, Stilllegungs- und Wartungsverfahren erhalten.
- Föderiertes Identitätsmanagement. Integration mit Active Directory, OpenLDAP oder Oracle Directory Service zur Benutzerauthentifizierung. Unterstützt Single Sign-On (SSO) mithilfe des Security Assertion Markup Language 2.0 (SAML 2.0) Standards zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen StorageGRID und Active Directory Federation Services (AD FS).

Hybrid Clouds mit StorageGRID

StorageGRID kann in einer Hybrid-Cloud-Konfiguration eingesetzt werden, indem richtlinienbasiertes Datenmanagement implementiert wird, um Objekte in Cloud Storage Pools zu speichern, die StorageGRID Plattformdienste genutzt werden und Daten von ONTAP zu StorageGRID mit NetApp FabricPool gestuft werden.

Cloud-Storage-Pools

Cloud Storage Pools ermöglichen das Speichern von Objekten außerhalb des StorageGRID Systems. Beispielsweise kann es sinnvoll sein, selten genutzte Objekte in kostengünstigeren Cloud Storage wie Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archive-Zugriffsebene in Microsoft Azure Blob storage zu verschieben. Oder es kann ein Cloud-Backup der StorageGRID Objekte vorgehalten werden, das zur Wiederherstellung von Daten dient, die durch einen Ausfall eines Storage-Volumes oder Storage Node verloren gegangen sind.

Speicherlösungen von Drittanbietern werden ebenfalls unterstützt, darunter Festplatten- und Tape-Storage.

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

S3 Plattformdienste

S3-Plattformdienste bieten die Möglichkeit, Remote-Services als Endpunkte für Objektreplikation, Ereignisbenachrichtigungen oder Suchintegration zu nutzen. Plattformdienste arbeiten unabhängig von den ILM-Regeln des Grids und sind für einzelne S3 Buckets aktiviert. Die folgenden Dienste werden unterstützt:

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

Beispielsweise kann die CloudMirror-Replikation genutzt werden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und anschließend AWS-Services für Analysen der Daten zu verwenden.

ONTAP Datentiering mit FabricPool

Die Kosten für ONTAP Storage lassen sich senken, indem Daten mit FabricPool zu StorageGRID getiert werden. FabricPool ermöglicht das automatisierte Tiering von Daten auf kostengünstige Objektspeicher-Tiers, sowohl lokal als auch extern.

Im Gegensatz zu manuellen Tiering-Lösungen reduziert FabricPool die Gesamtbetriebskosten, indem das Tiering von Daten automatisiert wird, um die Speicherkosten zu senken. Die Vorteile der Cloud-Ökonomie werden durch Tiering in öffentliche und private Clouds, einschließlich StorageGRID, bereitgestellt.

Verwandte Informationen

- "Was ist ein Cloud Storage Pool?"
- "Plattformdienste verwalten"
- "StorageGRID für FabricPool konfigurieren"

StorageGRID Architektur und Netzwerktopologie

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

Informationen zu "Grid-Node-Typen".

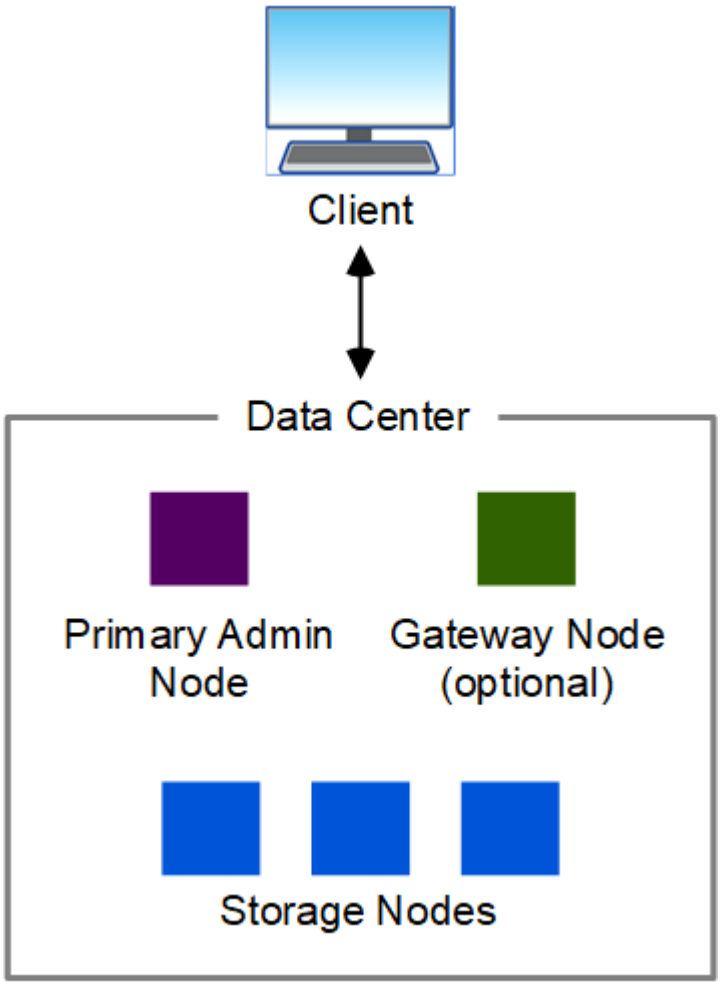
Weitere Informationen zur StorageGRID Netzwerktopologie, zu den Anforderungen und zur Grid-Kommunikation enthält die Dokumentation "Netzwerkrichtlinien".

Bereitstellungstopologien

Das StorageGRID System kann an einem einzelnen Rechenzentrumsstandort oder an mehreren Rechenzentrumsstandorten eingesetzt werden. Die maximale Anzahl von Standorten pro Bereitstellung beträgt 16.

Einzelstandort

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

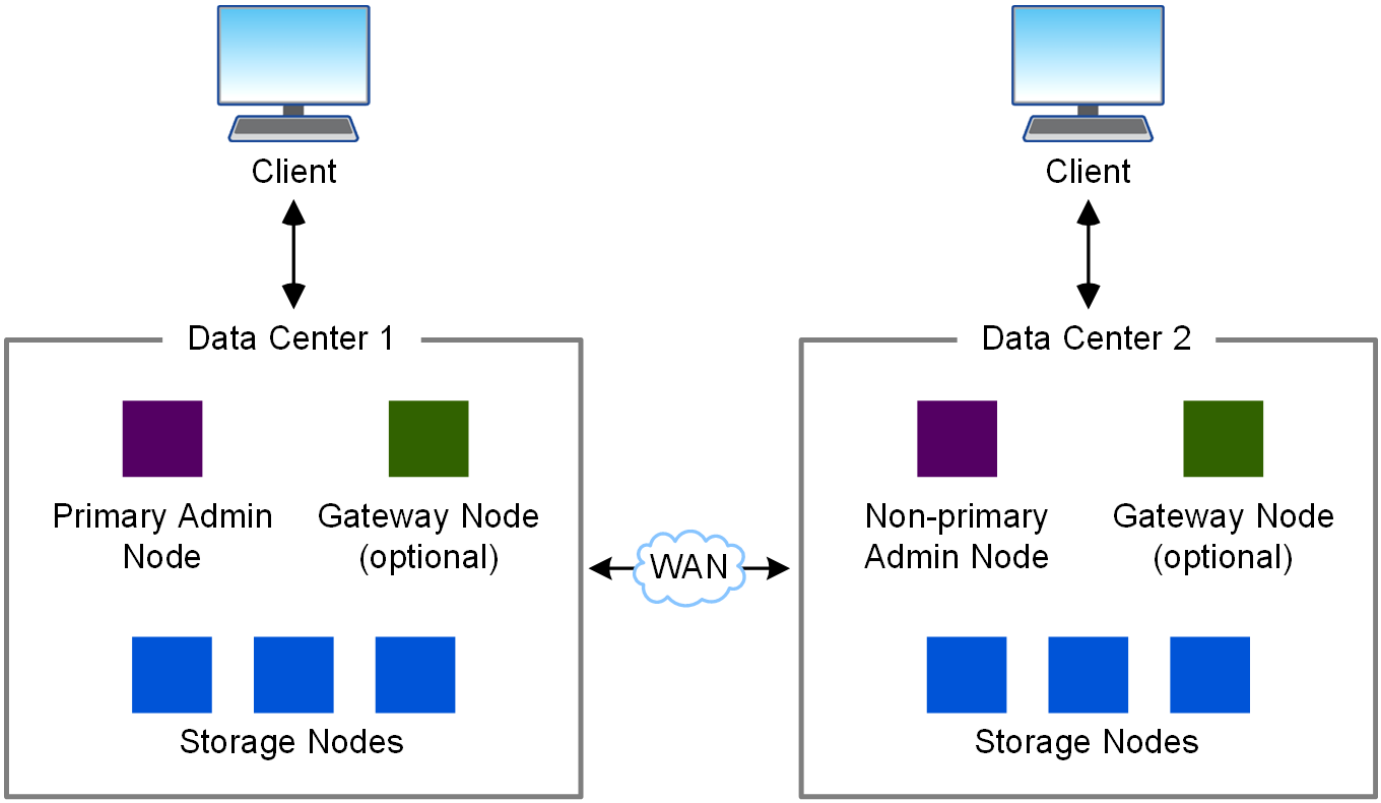


Mehrere Standorte

In einer Bereitstellung mit mehreren Standorten können an jedem Standort unterschiedliche Arten und Anzahlen von StorageGRID Ressourcen installiert werden. Beispielsweise kann in einem Rechenzentrum

mehr Speicher benötigt werden als in einem anderen.

Die Standorte befinden sich oft an geografisch unterschiedlichen Orten in verschiedenen Ausfallbereichen, beispielsweise entlang einer Erdbebenverwerfung oder in einem Überschwemmungsgebiet. Datenaustausch und Disaster Recovery erfolgen durch die automatisierte Verteilung von Daten an andere Standorte.



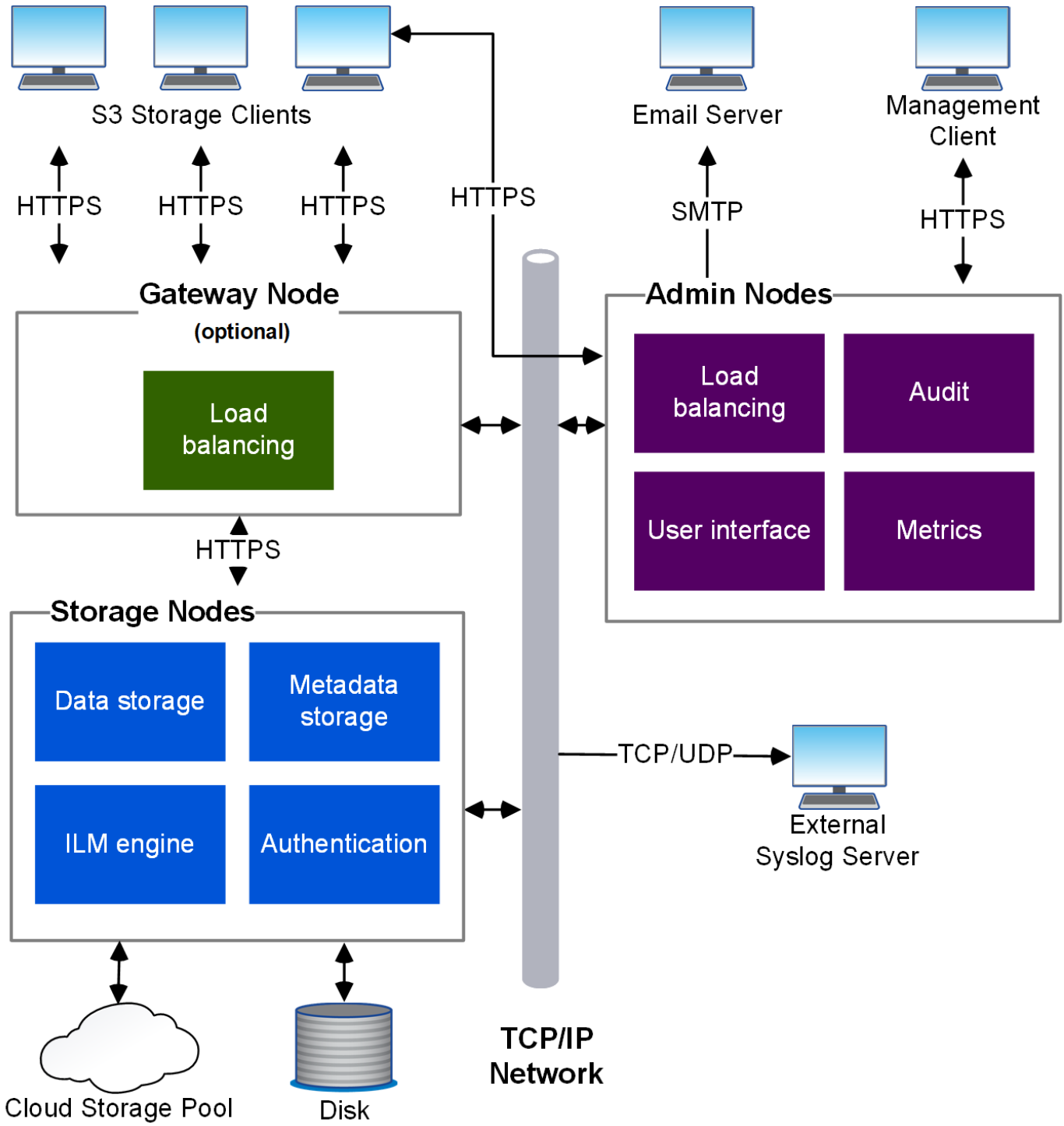
Innerhalb eines einzigen Rechenzentrums können auch mehrere logische Standorte existieren, um die Nutzung von verteilter Replikation und Erasure Coding für erhöhte Verfügbarkeit und Ausfallsicherheit zu ermöglichen.

Redundanz der Grid-Knoten

Bei einer Bereitstellung an einem oder mehreren Standorten kann optional mehr als ein Admin Node oder Gateway Node zur Redundanz einbezogen werden. Beispielsweise ist es möglich, mehr als einen Admin Node an einem einzelnen Standort oder über mehrere Standorte hinweg zu installieren. Allerdings kann jedes StorageGRID System nur einen primären Admin Node haben.

Systemarchitektur

Dieses Diagramm zeigt, wie die Grid-Knoten in einem StorageGRID System angeordnet sind.



S3-Clients speichern und rufen Objekte in StorageGRID ab. Andere Clients dienen dazu, E-Mail-Benachrichtigungen zu versenden, auf die StorageGRID Managementoberfläche zuzugreifen und optional auf die Audit-Freigabe zuzugreifen.

S3-Clients können sich mit einem Gateway Node oder einem Admin Node verbinden, um die Lastausgleichsoberfläche zu Storage Nodes zu nutzen. Alternativ können S3-Clients direkt über HTTPS eine Verbindung zu Storage Nodes herstellen.

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

Grid-Knoten und Dienste

StorageGRID Grid-Knoten und Services

Der grundlegende Baustein eines StorageGRID Systems ist der Grid-Knoten. Knoten enthalten Dienste, also Softwaremodule, die einem Grid-Knoten eine Reihe von Funktionen bereitstellen.

Arten von Grid-Knoten

Das StorageGRID System verwendet drei Arten von Grid-Knoten:

Admin-Nodes

Bereitstellung von Verwaltungsdiensten wie Systemkonfiguration, Überwachung und Protokollierung. Bei der Anmeldung am Grid Manager erfolgt die Verbindung zu einem Admin Node. Jedes Grid muss über einen primären Admin Node verfügen und kann zur Redundanz zusätzliche nicht-primäre Admin Nodes haben. Eine Verbindung kann zu jedem Admin Node hergestellt werden, und jeder Admin Node zeigt eine ähnliche Ansicht des StorageGRID Systems an. Wartungsverfahren sind jedoch mit dem primären Admin Node durchzuführen.

Admin Nodes können auch zum Lastausgleich des S3-Client-Datenverkehrs verwendet werden.

Siehe "Was ist ein Admin Node?"

Speicherknoten

Objektdaten und Metadaten werden verwaltet und gespeichert. Jeder Standort in Ihrem StorageGRID System muss mindestens drei Storage Nodes haben.

Während der Erstinstallation eines neuen Storage Node kann festgelegt werden, dass dieser nur für "Metadaten speichern" verwendet wird.

Siehe "Was ist ein Speicherknoten?"

Gateway-Nodes (optional)

Eine Lastausgleichs-Schnittstelle steht zur Verfügung, über die Clientanwendungen eine Verbindung zu StorageGRID herstellen können. Ein Load Balancer leitet Clients nahtlos zu einem optimalen Storage Node, sodass der Ausfall einzelner Nodes oder sogar eines gesamten Standorts transparent bleibt.

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 Knoten

StorageGRID Hardware-Appliances sind speziell für den Einsatz in einem StorageGRID System konzipiert. Einige Appliances können als Storage Nodes verwendet werden. Andere Appliances können als Admin Nodes oder Gateway Nodes verwendet werden. Es besteht die Möglichkeit, Appliance-Knoten mit softwarebasierten Knoten zu kombinieren oder vollständig entwickelte, ausschließlich aus Appliances bestehende Grids bereitzustellen, die keine Abhängigkeiten von externen Hypervisoren, Storage oder Compute-Hardware aufweisen.

Im Folgenden sind Informationen zu den verfügbaren Geräten aufgeführt:

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

Softwarebasierte Knoten

Softwarebasierte Grid-Knoten können als VMware-VMs oder innerhalb von Container-Engines auf einem Linux-Host bereitgestellt werden. Siehe "StorageGRID auf softwarebasierten Knoten installieren".

Die Funktion "NetApp Interoperabilitätsmatrix Tool (IMT)" dient zur Bestimmung der unterstützten Versionen.

StorageGRID Dienste

Im Folgenden befindet sich eine vollständige Liste der StorageGRID Dienste.

Service	Beschreibung	Standort
Account-Service-Forwarder	Bietet eine Schnittstelle für den Load Balancer Service, um den Account Service auf Remote-Hosts abzufragen, und stellt dem Load Balancer Service Benachrichtigungen über Änderungen der Load Balancer Endpoint-Konfiguration bereit.	Load Balancer Dienst auf Admin-Knoten und Gateway-Knoten
ADC (Administrativer Domänencontroller)	Pflegt Topologieinformationen, bietet Authentifizierungsdienste und beantwortet Anfragen der LDR- und CMN-Dienste.	Mindestens drei Speicherknoten mit dem ADC-Dienst an jedem Standort
AMS (Audit Management System)	Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textprotokolldatei.	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 Knoten
Cache Service	Läuft auf Load Balancer-Knoten (Gateway) und verwaltet einen lokalen Cache für Objektinhalte.	Gateway-Nodes
Cassandra	Verwaltet die verteilte Datenbank für Objektmetadaten.	Speicherknoten (außer Datenknoten)
Cassandra Reaper	Führt automatische Reparaturen an Objektmetadaten durch.	Speicherknoten

Service	Beschreibung	Standort
Chunk Service	Verwaltet löschcodierte Daten und Paritätsfragmente.	Speicherknoten
CMN (Konfigurationsverwaltungsknoten)	Verwaltet systemweite Konfigurationen und Grid-Aufgaben. Jedes Grid verfügt über einen CMN Service.	Primärer Admin-Knoten
DDS (Verteilter Datenspeicher)	Schnittstellen mit der Cassandra Datenbank zur Verwaltung von Objektmetadaten.	Speicherknoten
DMV (Data Mover)	Verschiebt Daten an Cloud-Endpunkte.	Speicherknoten
Dynamische IP (dynip)	Überwacht das Grid auf dynamische IP-Änderungen und aktualisiert lokale Konfigurationen.	Alle Knoten
Grafana	Wird zur Visualisierung von Metriken im Grid Manager verwendet.	Admin-Nodes
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IPs auf Knoten, die auf der Seite „High Availability Groups“ konfiguriert sind. Dieser Service ist auch als keepalived Service bekannt.	Admin- und Gateway-Knoten
Identität (idnt)	Verwaltet lokale Benutzer und Gruppen, Authentifizierung und führt Benutzeridentitäten aus LDAP und Active Directory zusammen.	Speicherknoten, die den ADC Service nutzen
Lambda Arbitrator	Verwaltet S3 Select SelectObjectContent Anfragen.	Alle Knoten
Load Balancer (nginx-gw)	Bietet Lastausgleich des S3-Datenverkehrs von Clients zu Storage Nodes. Der Load Balancer Service kann über die Load Balancer Endpoints Konfigurationsseite konfiguriert werden. Dieser Service ist auch als nginx-gw Service bekannt.	Admin- und Gateway-Knoten
LDR (Local Distribution Router)	Verwaltet die Speicherung und Übertragung von Inhalten innerhalb des Grids.	Speicherknoten

Service	Beschreibung	Standort
MISCd Information Service Control Daemon	Bietet eine Schnittstelle zum Abfragen und Verwalten von Diensten auf anderen Knoten sowie zum Verwalten von Umgebungskonfigurationen auf dem Knoten, wie zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Knoten
nginx	Dient als Authentifizierung und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und Dynamic IP), um über HTTPS-APIs mit Diensten auf anderen Knoten kommunizieren zu können.	Alle Knoten
nginx-gw Load Balancer	Bietet Lastausgleich des S3-Datenverkehrs von Clients zu Storage Nodes. Der Load Balancer Service kann über die Load Balancer Endpoints Konfigurationsseite konfiguriert werden. Dieser Service ist auch als nginx-gw Service bekannt.	Admin- und Gateway-Knoten
NMS (Netzwerkmanagementsystem)	Ermöglicht die Überwachungs-, Berichts- und Konfigurationsoptionen, die über den Grid Manager angezeigt werden.	Admin-Nodes
Node Exporter (Prometheus Datenerfassung)	Veröffentlicht Systemstatistiken für die Prometheus-Zeitreihenmetrikerfassung.	Alle Knoten
ntp	Network Time Protocol (NTP) Dienst.	Alle Knoten
Persistenz	Verwaltet Dateien auf der Stammfestplatte, die auch nach einem Neustart erhalten bleiben müssen.	Alle Knoten
Prometheus	Erfasst Zeitreihenmetriken von Diensten auf allen Knoten.	Admin-Nodes
RSM (Replicated State Machine)	Stellt sicher, dass Plattform-Serviceanfragen an die jeweiligen Endpunkte gesendet werden.	Speicherknoten, die den ADC Service nutzen
SSM (Server Status Monitor)	Überwacht den Zustand der Hardware und meldet diesen an den NMS Service.	Auf jedem Grid-Node ist eine Instanz vorhanden.
Server-Manager	Verwaltet StorageGRID Dienste.	Alle Knoten
SNMP-Agent	Reagiert auf SNMP-Anfragen.	Admin-Nodes

Service	Beschreibung	Standort
SNMP Portverwaltungsdienst	Übernimmt die dynamische Verwaltung von SNMP-Ports.	Alle Knoten
SSH (Secure Shell)	Gewährleistet sicheren Zugriff und die Verwaltung von Remote-Systemen.	Alle Knoten
SSM (Systemstatusmonitor)	Überwacht den Zustand der Hardware und meldet diesen an den NMS Service.	Alle Knoten
Statistik	Erfasst zusätzliche Metriken im Zusammenhang mit S3 Buckets.	Speicherknoten
Trace Agent (jaeger-agent)	Empfängt und verarbeitet vom Trace Collector (jaeger-collector) übermittelte Tracing-Informationen.	Alle Knoten
Trace Collector (jaeger-collector)	Führt die Sammlung von Traces durch, um Informationen für den technischen Support zu erfassen. Der Trace Collector Service verwendet die Open-Source-Software Jaeger.	Admin-Nodes

Was ist ein StorageGRID Admin Node?

Admin Nodes stellen Managementdienste wie Systemkonfiguration, Überwachung und Protokollierung bereit. Admin Nodes können auch zum Lastausgleich des S3-Client-Datenverkehrs verwendet werden. Jedes Grid muss über einen primären Admin Node verfügen und kann zur Redundanz beliebig viele nicht-primäre Admin Nodes enthalten.

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 Node her. Sie können sich mit jedem Admin Node verbinden, und jeder Admin Node zeigt eine ähnliche Ansicht des StorageGRID Systems an. Der primäre Admin Node bietet jedoch mehr Funktionen als die nicht-primären Admin Nodes. Beispielsweise müssen die meisten Wartungsarbeiten vom primären Admin Node aus durchgeführt werden.

Die Tabelle fasst die Fähigkeiten von primären und nicht-primären Admin Nodes zusammen.

Fähigkeiten	Primärer Admin-Knoten	Nicht-primärer Admin-Node
Beinhaltet den AMS Service	Ja	Ja
Beinhaltet den CMN Service	Ja	Nein
Beinhaltet den NMS Service	Ja	Ja

Fähigkeiten	Primärer Admin-Knoten	Nicht-primärer Admin-Node
Beinhaltet den Prometheus Service	Ja	Ja
Beinhaltet den SSM Service	Ja	Ja
Beinhaltet die Lastverteiler und Hochverfügbarkeit Services	Ja	Ja
Unterstützt die Management-Anwendungsprogrammierschnittstelle (mgmt-api)	Ja	Ja
Kann für alle netzwerkbezogenen Wartungsaufgaben verwendet werden, zum Beispiel IP-Adressänderung und Aktualisierung von NTP-Servern	Ja	Nein
Kann Wiederherstellungspaket herunterladen	Ja	Ja
Nach der Erweiterung des Storage Node kann ein EC-Lastausgleich durchgeführt werden.	Ja	Nein
Kann für das Volumenwiederherstellungsverfahren verwendet werden	Ja	Ja
Kann Protokolldateien und Systemdaten von einem oder mehreren Knoten erfassen	Ja	Ja
Kann Storage-, Gateway- und nicht-primäre Admin-Nodes wiederherstellen	Ja	Ja
Kann den primären Admin-Node wiederherstellen	Ja	Nein
Sendet Warnmeldungen, AutoSupport-Pakete und SNMP-Traps und informiert	Ja. Fungiert als bevorzugter Absender.	Ja. Fungiert als Standby-Sender.

Bevorzugter Absender Admin Node

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

Im Normalbetrieb sendet nur der bevorzugte Absender Benachrichtigungen. Alle anderen Admin Nodes überwachen jedoch den bevorzugten Absender. Wenn ein Problem erkannt wird, fungieren die anderen Admin Nodes als Ersatzabsender.

In diesen Fällen werden möglicherweise mehrere Benachrichtigungen gesendet:

- Wenn Admin-Knoten voneinander „isoliert“ werden, versuchen sowohl der bevorzugte Absender als auch die Standby-Absender, Benachrichtigungen zu senden, und es könnten mehrere Kopien von

Benachrichtigungen empfangen werden.

- Wenn ein Ersatzsender Probleme mit dem bevorzugten Sender feststellt und Benachrichtigungen versendet, kann der bevorzugte Sender seine Fähigkeit zum Versenden von Benachrichtigungen wiedererlangen. In diesem Fall können doppelte Benachrichtigungen versendet werden. Der Ersatzsender stellt den Versand von Benachrichtigungen ein, sobald er keine Fehler mehr beim bevorzugten Sender feststellt.

> Wenn Sie AutoSupport-Pakete testen, senden alle Admin-Knoten den Test. Wenn Sie Alarmbenachrichtigungen testen, ist eine Anmeldung an jedem Admin-Knoten erforderlich, um die Konnektivität zu überprüfen.

Primäre Dienste für Admin-Knoten

Die folgende Tabelle zeigt die primären Dienste für Admin Nodes; diese Tabelle listet jedoch nicht alle Knotendienste auf.

Service	Schlüsselfunktion
Audit Management System (AMS)	Erfasst Systemaktivitäten und Ereignisse.
Konfigurationsverwaltungsknoten (CMN)	Verwaltet die systemweite Konfiguration.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. **Hinweis:** Dieser Dienst ist auch auf Gateway Nodes verfügbar.
Load Balancer	Bietet Lastausgleich für S3-Datenverkehr von Clients zu Storage Nodes. **Hinweis:** Dieser Dienst ist auch auf Gateway Nodes verfügbar.
Management Application Program Interface (mgmt-api)	Verarbeitet Anfragen von der Grid Management API und der Tenant Management API.
Netzwerkmanagementsystem (NMS)	Bietet Funktionalität für den Grid Manager.
Prometheus	Sammelt und speichert Zeitreihenmetriken von den Diensten auf allen Knoten.
Server Status Monitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein StorageGRID Storage Node?

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

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

Arten von Speicherknoten

Während der Installation kann der Typ des zu installierenden Storage Node ausgewählt werden. Diese Typen sind für softwarebasierte Storage Nodes und für Appliance-basierte Storage Nodes verfügbar, die diese Funktion unterstützen:

- Kombinierter Daten- und Metadaten Storage Node
- Speicherknoten nur für Metadaten
- reiner Datenspeicherknoten

In folgenden Situationen kann der Storage Node-Typ ausgewählt werden:

- Bei der Erstinstallation eines Storage Node
- Wenn während der StorageGRID Systemerweiterung ein Speicherknoten hinzugefügt wird

Daten- und Metadaten Storage Node (kombiniert)

Standardmäßig speichern alle neuen Storage Nodes sowohl Objektdaten als auch Metadaten. Dieser Typ von Storage Node wird als *kombinierter* Storage Node bezeichnet.

Speicherknoten nur für Metadaten

Die Verwendung eines Storage Node ausschließlich für Metadaten kann sinnvoll sein, wenn Ihr Grid eine sehr große Anzahl kleiner Objekte speichert. Die Installation dedizierter Metadatenkapazität sorgt für ein besseres Gleichgewicht zwischen dem Speicherplatzbedarf für eine sehr große Anzahl kleiner Objekte und dem Speicherplatzbedarf für die Metadaten dieser Objekte. Zusätzlich können reine Metadaten-Storage Nodes, die auf Hochleistungsgeräten gehostet werden, die Performance erhöhen.

Nur-Metadaten-Speicherknoten haben spezifische Hardwareanforderungen:

- Bei Verwendung von StorageGRID Appliances können Metadaten-Only-Knoten nur auf SGF6112 Appliances mit zwölf 1,9-TB- oder zwölf 3,8-TB-Laufwerken konfiguriert werden.
- Bei Verwendung softwarebasierter Knoten müssen die Metadaten-Knotenressourcen mit den vorhandenen Storage Nodes Ressourcen übereinstimmen. Beispielsweise:
  - Wenn der bestehende StorageGRID Standort SG6000 oder SG6100 Appliances verwendet, müssen die softwarebasierten Metadaten-only Nodes die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM
    - 8-Core-CPU
    - 8 TB SSD oder gleichwertiger Speicherplatz für die Cassandra Datenbank (rangedb/0)
  - Wenn die bestehende StorageGRID Site virtuelle Storage Nodes mit 24 GB RAM, 8 Core CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Metadaten-only Nodes ähnliche Ressourcen verwenden (24 GB RAM, 8 Core CPU und 4 TB Metadatenspeicher (rangedb/0)).
- Beim Hinzufügen eines neuen StorageGRID Standorts sollte die Gesamtkapazität der Metadaten des neuen Standorts mindestens der Kapazität bestehender Standorte entsprechen. Die Ressourcen eines neuen Standorts sollten den Storage Nodes bestehender Standorte entsprechen.

Obwohl Speicherknoten, die nur Metadaten enthalten, die LDR-Service enthalten und S3-Clientanfragen verarbeiten können, könnte sich die Leistung von StorageGRID möglicherweise nicht erhöhen.

reiner Datenspeicherknoten

Die Verwendung eines Storage Node ausschließlich für Daten kann sinnvoll sein, wenn Ihre Storage Nodes unterschiedliche Leistungsmerkmale aufweisen. Beispielsweise könnten zur potenziellen Leistungssteigerung Daten-only Storage Nodes mit einer hohen Kapazität und Festplattenlaufwerken zusammen mit Metadaten-only Storage Nodes mit hoher Leistung eingesetzt werden.

Zusätzlich kann mehr Metadatenkapazität erzielt werden, indem Knoten mit geringem Arbeitsspeicher aus Cassandra entfernt werden, was das Metadatenkapazitätslimit pro Knoten erhöht. Siehe "Objekt-Metadaten-Speicher verwalten".

Ein Storage Node, der nicht die ADC-Service enthält, kann in einen reinen Daten-Storage Node umgewandelt werden. Weitere Informationen finden Sie unter "Einen Speicherknoten in einen reinen Datenknoten umwandeln".

Erforderliche Speicherknoten pro Grid und pro Standort

Bei der Auswahl der Storage Nodes für Ihre Topologie ist zu beachten, dass das Grid bzw. jeder Standort im Grid Folgendes enthalten muss:

- Pro Standort (in einem Einzel- oder Mehrstandort-Grid): Drei ADC Storage Nodes (kann jede Kombination aus kombinierten und nur Metadaten-Storage Nodes sein)
- Einzelstandort-Grid: Mindestens zwei Objektspeicherknoten (jede Kombination aus kombinierten und nur Daten enthaltenden Knoten ist möglich)
- Multi-site Grid: Mindestens ein Objekt Storage Node pro Standort (kann entweder kombiniert oder nur Daten enthalten)

Primäre Dienste für Storage Nodes

Die folgende Tabelle zeigt die primären Dienste für Storage Nodes; diese Tabelle listet jedoch nicht alle Knotendienste auf.

Einige Dienste, wie beispielsweise der ADC Service und der RSM Service, existieren typischerweise nur auf drei Storage Nodes an jedem Standort.

Service	Schlüsselfunktion
Konto (acct)	Verwaltet Mieterkonten. Reine Datenspeicherknoten hosten diesen Dienst nicht.

Service	Schlüsselfunktion
Administrativer Domain Controller (ADC)	Die Topologie und die gridweite Konfiguration werden aufrechterhalten. Reine Datenspeicherknoten hosten diesen Dienst nicht. **Details** Der Dienst des administrativen Domänencontrollers (ADC) authentifiziert Grid-Knoten und deren Verbindungen untereinander. Der ADC-Dienst wird an einem Standort auf mindestens drei Storage Nodes gehostet. Der ADC-Dienst verwaltet Topologieinformationen, 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 soll, kontaktiert er einen ADC-Dienst, um den am besten geeigneten Grid-Knoten für die Bearbeitung seiner Anfrage zu finden. Zusätzlich behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann. Um verteilte und isolierte Betriebsabläufe zu ermöglichen, synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Dienste und Topologie mit den anderen ADC-Diensten im StorageGRID System. Im Allgemeinen unterhalten alle Grid-Knoten eine Verbindung zu mindestens einem ADC-Dienst. Dies stellt sicher, dass die Grid-Knoten stets auf die neuesten Informationen zugreifen. Wenn Grid-Knoten eine Verbindung herstellen, speichern sie die Zertifikate anderer Grid-Knoten im Cache, sodass Systeme auch dann mit bekannten Grid-Knoten weiterarbeiten können, wenn kein ADC-Dienst verfügbar ist. Neue Grid-Knoten können Verbindungen nur mithilfe eines ADC-Dienstes herstellen. Die Verbindung jedes Grid-Knotens ermöglicht es dem ADC-Dienst, Topologieinformationen zu erfassen. Diese Grid-Knoten-Informationen umfassen die CPU-Auslastung, den verfügbaren Speicherplatz (sofern Speicher vorhanden ist), die unterstützten Dienste und die Standort-ID des Grid-Knotens. Andere Dienste fordern beim ADC-Dienst Topologieinformationen über Topologieabfragen an. Der ADC-Dienst antwortet auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID System empfangen wurden.
Cassandra	Speichert und schützt Objektmetadaten. Reine Datenspeicherknoten hosten diesen Dienst nicht.
Cassandra Reaper	Führt automatische Reparaturen an Objektmetadaten durch. Reine Datenspeicherknoten hosten diesen Dienst nicht.
Chunk	Verwaltet löschcodierte Daten und Paritätsfragmente.

Service	Schlüsselfunktion
Data Mover (dmv)	Verschiebt Daten in Cloud Storage Pools.
Verteilter Datenspeicher (DDS)	Überwacht die Speicherung von Objektmetadaten. **Details** Jeder Speicherknoten beinhaltet den Distributed Data Store (DDS) Dienst. Dieser Dienst kommuniziert mit der Cassandra Datenbank, um Hintergrundaufgaben für die im StorageGRID System gespeicherten Objektmetadaten auszuführen. Der DDS-Dienst erfasst die Gesamtzahl der in das StorageGRID System aufgenommenen Objekte sowie die Gesamtzahl der über jede der vom System unterstützten Schnittstellen (S3) aufgenommenen Objekte.
Identität (idnt)	Föderiert Benutzeridentitäten aus LDAP und Active Directory. Reine Datenspeicherknoten hosten diesen Dienst nicht.

Service	Schlüsselfunktion
Lokaler Distribution Router (LDR)	Verarbeitet Anfragen nach dem Objektspeicherprotokoll und verwaltet Objektdaten auf der Festplatte.

Service	Schlüsselfunktion
Replikierte Zustandsmaschine (RSM)	Stellt sicher, dass Anfragen an S3-Plattformdienste an die jeweiligen Endpunkte gesendet werden. Reine Datenspeicherknoten hosten diesen Dienst nicht.
Server Status Monitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein StorageGRID Gateway Node?

Gateway Nodes bieten eine dedizierte Load-Balancing-Schnittstelle, die S3-Clientanwendungen für die Verbindung zu StorageGRID verwenden können. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität, indem die Arbeitslast auf mehrere Storage Nodes verteilt wird. Gateway Nodes sind optional.

Der StorageGRID Load Balancer Service ist auf allen Admin Nodes und allen Gateway Nodes verfügbar. Er übernimmt die Transport Layer Security (TLS) Terminierung von Client-Anfragen, prüft diese und stellt neue sichere Verbindungen zu den Storage Nodes her. Der Load Balancer Service leitet Clients nahtlos zu einem optimalen Storage Node weiter, sodass der Ausfall von Nodes oder sogar eines gesamten Standorts transparent bleibt.

Ein oder mehrere Load Balancer-Endpunkte werden konfiguriert, um den Port und das Netzwerkprotokoll (HTTPS oder HTTP) festzulegen, die eingehende und ausgehende Clientanfragen für den Zugriff auf die Load Balancer-Services auf Gateway- und Admin-Knoten verwenden. Der Load Balancer-Endpunkt definiert außerdem den Clienttyp (S3), den Bindungsmodus und optional eine Liste zulässiger oder gesperrter Mandanten. Siehe "Überlegungen zum Lastausgleich".

Bei Bedarf lassen sich die Netzwerkschnittstellen mehrerer Gateway Nodes und Admin Nodes zu einer Hochverfügbarkeitsgruppe (HA-Gruppe) zusammenfassen. Fällt die aktive Schnittstelle in der HA-Gruppe aus, kann eine Backup-Schnittstelle die Client-Anwendungs-Workload verwalten. Siehe "Hochverfügbarkeitsgruppen (HA) verwalten".

Primäre Dienste für Gateway-Knoten

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

Service	Schlüsselfunktion
Cache Service	Verwaltet einen lokalen Cache von Objektinhalten.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. **Hinweis:** Dieser Dienst ist auch auf Admin Nodes verfügbar.

Der LDR Dienst übernimmt die folgenden Aufgaben:

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

Der LDR Service ordnet außerdem jedem S3-Objekt seine eindeutige UUID zu.

Objektspeicher

Der zugrundeliegende Datenspeicher eines LDR Dienstes ist in eine feste Anzahl von Objektspeichern (auch Speichervolumes genannt) unterteilt. Jeder Objektspeicher ist ein separater Mountpunkt.

Die Objektspeicher in einem Storage Node werden durch eine Hexadezimalzahl von 0000 bis 002F identifiziert, die als Volume-ID bezeichnet wird. Im ersten Objektspeicher (Volume 0) ist Platz für Objektmetadaten in einer Cassandra Datenbank reserviert; der verbleibende Speicherplatz auf diesem Volume wird für Objektdaten verwendet. Alle anderen Objektspeicher werden ausschließlich für Objektdaten verwendet, einschließlich replizierter Kopien und löschcodierter Fragmente.

StorageGRID speichert Objektmetadaten in einer Cassandra Datenbank, die mit dem LDR Service interagiert.

Um Redundanz und damit Schutz vor Verlust zu gewährleisten, werden an jedem Standort drei Kopien der Objektmetadaten vorgehalten. Diese Replikation ist nicht konfigurierbar und erfolgt automatisch. Weitere Einzelheiten finden sich unter "Objekt-Metadaten-Speicher verwalten".

Service	Schlüsselfunktion
Lastverteiler	Bietet Layer 7-Lastverteilung für den S3-Datenverkehr von Clients zu Storage Nodes. Dies ist der empfohlene Lastverteilungsmechanismus. **Hinweis:** Dieser Dienst ist auch auf Admin Nodes verfügbar.
Server Status Monitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

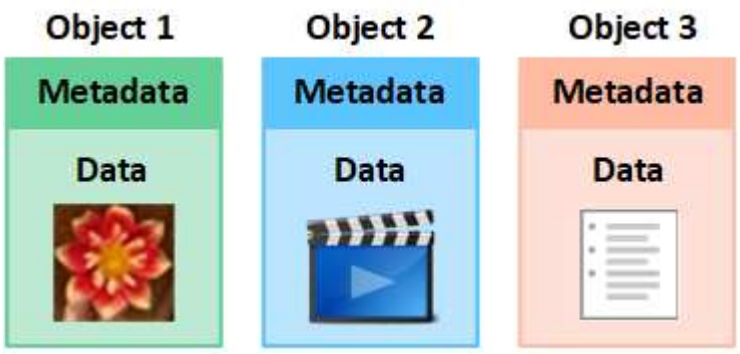
Wie StorageGRID Daten verwaltet

Was ist ein StorageGRID Objekt

Bei objektorientierter Speicherung ist die Speichereinheit ein Objekt, nicht eine Datei oder ein Block. Anders als die baumartige Hierarchie eines Dateisystems oder einer Blockspeicherung organisiert die objektorientierte Speicherung Daten in einem flachen, unstrukturierten Layout.

Objektspeicher entkoppelt den physischen Speicherort der Daten von der Methode, die zum Speichern und Abrufen dieser Daten verwendet wird.

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



Was sind Objektdaten?

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

Was sind Objektmetadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus jedes Objekts im Laufe der Zeit zu verwalten.

Objektmetadaten enthalten unter anderem folgende Informationen:

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

- Der aktuelle Speicherort jeder Objektkopie oder jedes erasure-codierten Fragments.
- Sämtliche Benutzermetadaten, die mit dem Objekt verknüpft sind.

Objektmetadaten sind anpassbar und erweiterbar, wodurch sie für Anwendungen flexibel einsetzbar sind.

Detaillierte Informationen darüber, wie und wo StorageGRID Objektmetadaten speichert, sind unter "Objekt-Metadaten-Speicher verwalten" zu finden.

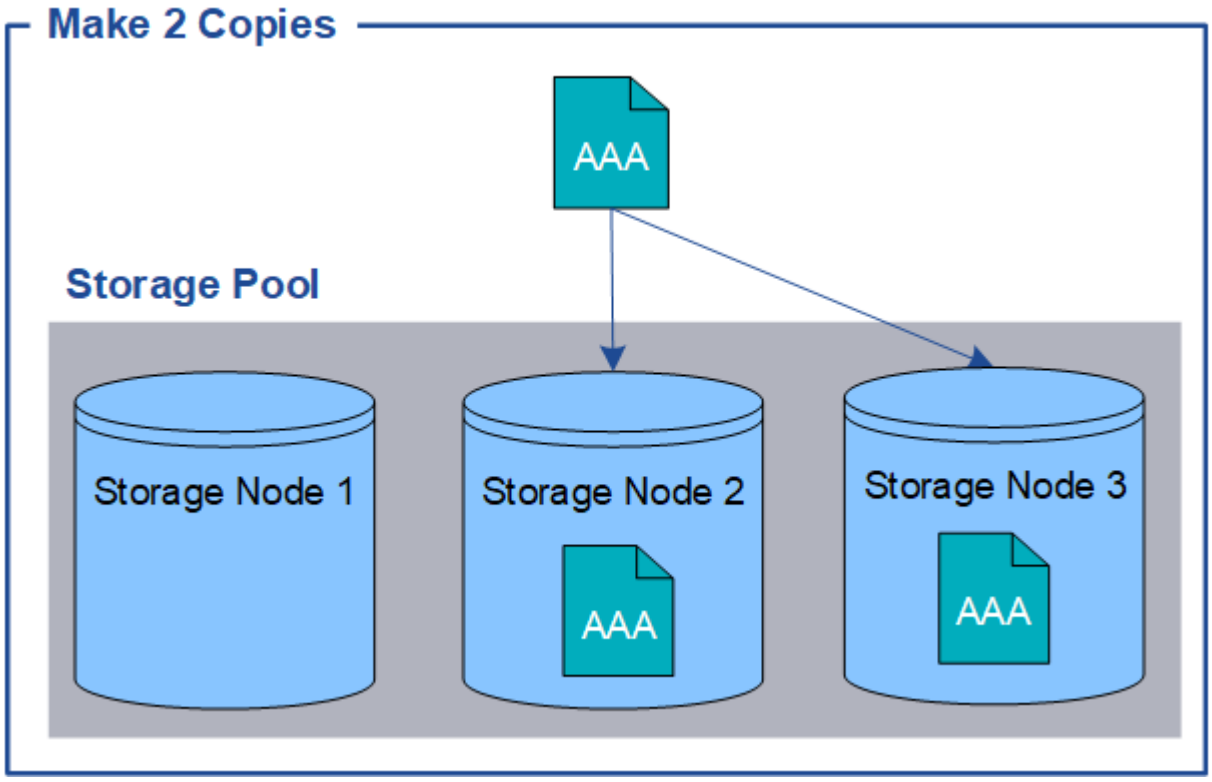
Wie werden Objektdaten geschützt?

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

Replication

Wenn StorageGRID Objekte einer Information Lifecycle Management (ILM)-Regel zuordnet, die für die Erstellung replizierter Kopien konfiguriert ist, erstellt das System exakte Kopien der Objektdaten und speichert sie auf Storage Nodes oder in Cloud Storage Pools. ILM-Regeln bestimmen die Anzahl der erstellten Kopien, deren Speicherort und wie lange sie vom System aufbewahrt werden. Geht eine Kopie verloren, zum Beispiel durch den Ausfall eines Storage Node, bleibt das Objekt verfügbar, sofern eine Kopie davon an anderer Stelle im StorageGRID System existiert.

Im folgenden Beispiel legt die Regel „2 Kopien erstellen“ fest, dass zwei replizierte Kopien jedes Objekts in einem Storage-Pool mit drei Storage-Nodes abgelegt werden.

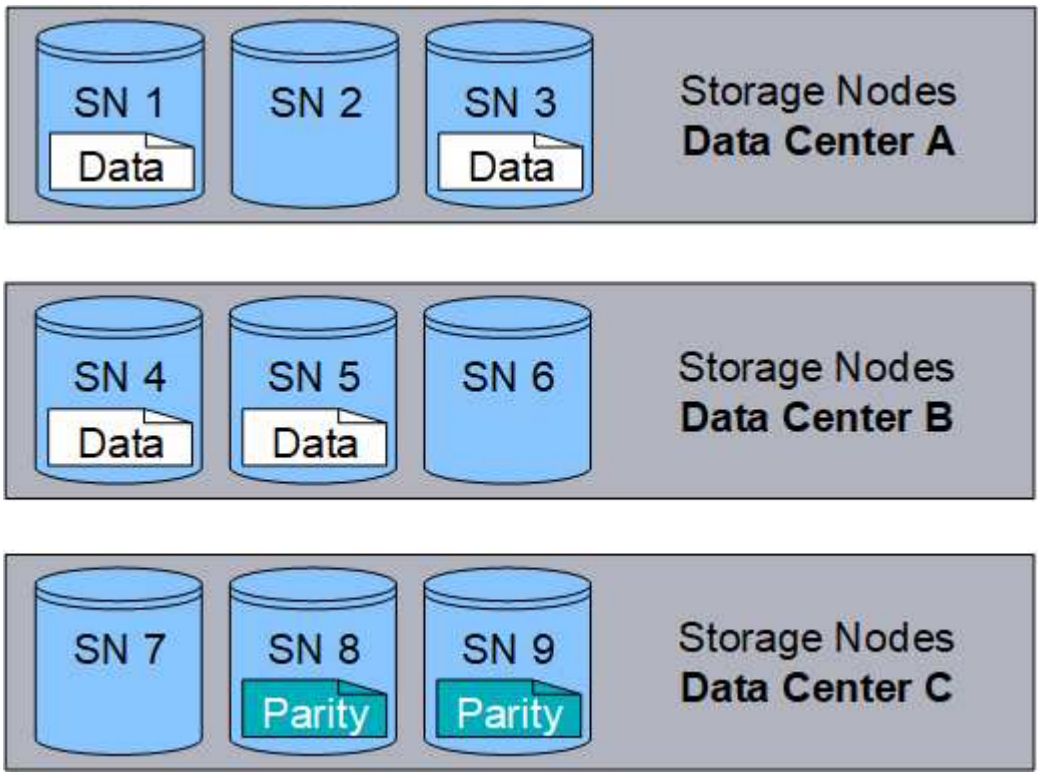


Erasure Coding

Wenn StorageGRID Objekte einer ILM-Regel zuordnet, die für die Erstellung von erasure-codierten Kopien konfiguriert ist, werden die Objektdaten in Datenfragmente zerlegt, zusätzliche Paritätsfragmente berechnet und jedes Fragment auf einem anderen Storage Node gespeichert. Beim Zugriff auf ein Objekt wird es mithilfe

der gespeicherten Fragmente wieder zusammengesetzt. Wenn ein Daten- oder Paritätsfragment beschädigt wird oder verloren geht, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten- und Paritätsfragmente rekonstruieren. ILM-Regeln und Erasure-Coding-Profile bestimmen das verwendete Erasure-Coding-Schema.

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



Verwandte Informationen

- "Objekte mit ILM verwalten"
- "Informationslebenszyklusmanagement verwenden"

Objektlebenszyklus in StorageGRID

Das Leben eines Objekts besteht aus verschiedenen Phasen. Jede Phase repräsentiert die Vorgänge, die mit dem Objekt stattfinden.

Zum Lebenszyklus eines Objekts gehören die Vorgänge des Erfassens, der Kopierverwaltung, des Abrufens und des Löschens.

- **Ingest**: Der Prozess, bei dem eine S3-Clientanwendung ein Objekt über HTTP im StorageGRID-System speichert. In dieser Phase beginnt das StorageGRID-System mit der Verwaltung des Objekts.
- **Kopienverwaltung**: Der Prozess der Verwaltung replizierter und mit Löschcodierung versehener Kopien in StorageGRID, wie in den ILM-Regeln der aktiven ILM-Richtlinien beschrieben. Während der Kopienverwaltungsphase schützt StorageGRID Objektdaten vor Verlust, indem die angegebene Anzahl und Art von Objektkopien auf Storage Nodes oder in einem Cloud Storage Pool erstellt und verwaltet wird.

- **Abrufen**: Der Vorgang, bei dem eine Clientanwendung auf ein vom StorageGRID System gespeichertes Objekt zugreift. Die Clientanwendung liest das Objekt, das von einem Storage Node oder Cloud Storage Pool abgerufen wird.
- **Löschen**: Der Vorgang, bei dem alle Objektkopien aus dem Grid entfernt werden. Objekte können entweder durch eine Löschanforderung der Clientanwendung an das StorageGRID System entfernt werden oder durch einen automatischen Prozess, den StorageGRID ausführt, wenn die Lebensdauer des Objekts abläuft.

Verwandte Informationen

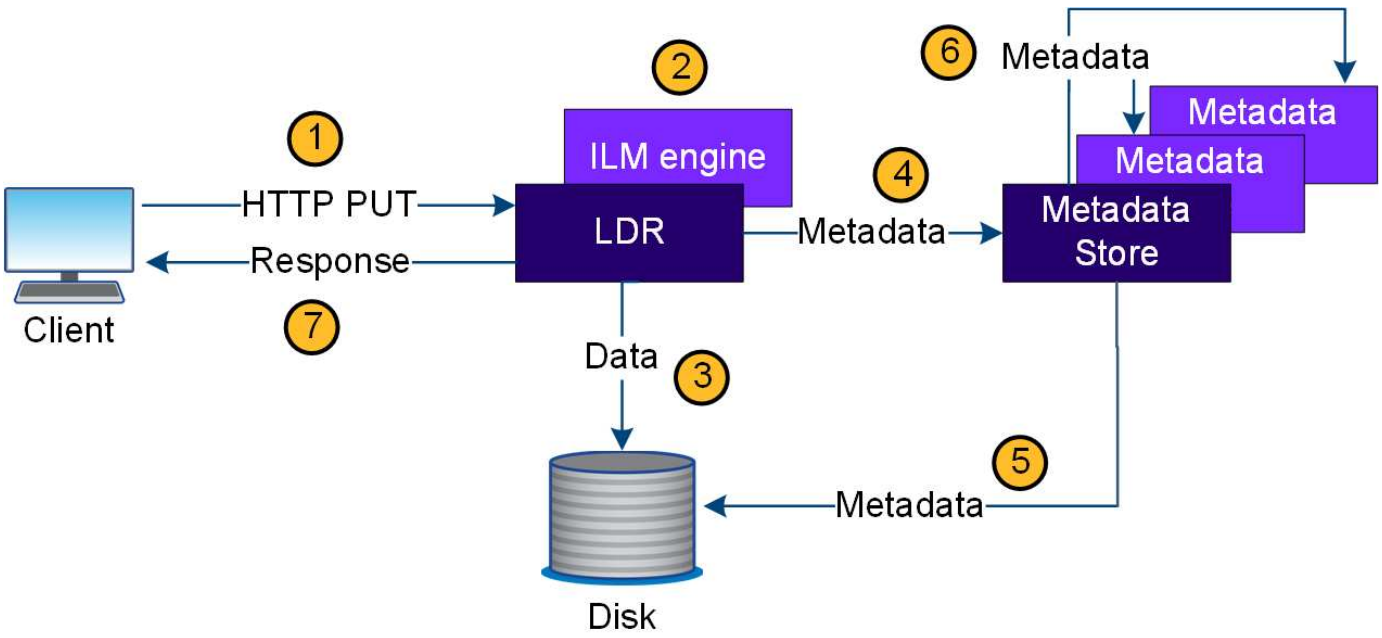
- "Objekte mit ILM verwalten"
- "Informationslebenszyklusmanagement verwenden"

Wie StorageGRID die Objektaufnahme handhabt

Ein Datenimport bzw. Speichervorgang besteht aus einem definierten Datenfluss zwischen dem Client und dem StorageGRID System.

Datenfluss

Wenn ein Client ein Objekt in das StorageGRID System einliest, verarbeitet der LDR-Dienst auf den Storage Nodes die Anfrage und speichert die Metadaten und Daten auf der Festplatte.



1. Die Clientanwendung erstellt das Objekt und sendet es über eine HTTP PUT-Anfrage an das StorageGRID System.

2. Das Objekt wird anhand der ILM-Richtlinie des Systems bewertet.
3. Der LDR-Dienst speichert die Objektdaten als replizierte Kopie oder als löschcodierte Kopie. (Das Diagramm zeigt eine vereinfachte Darstellung der Speicherung einer replizierten Kopie auf der Festplatte.)
4. Der LDR-Dienst sendet die Objektmetadaten an den Metadatenspeicher.
5. Der Metadatenspeicher speichert die Objektmetadaten auf der Festplatte.
6. Der Metadatenspeicher verteilt Kopien der Objektmetadaten an andere Storage Nodes. Diese Kopien werden ebenfalls 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 durch die aktiven ILM-Richtlinien und zugehörigen ILM-Regeln verwaltet. ILM-Regeln erstellen Replikate oder mit Erasure Coding versehene Kopien, um Objektdaten vor Verlust zu schützen.

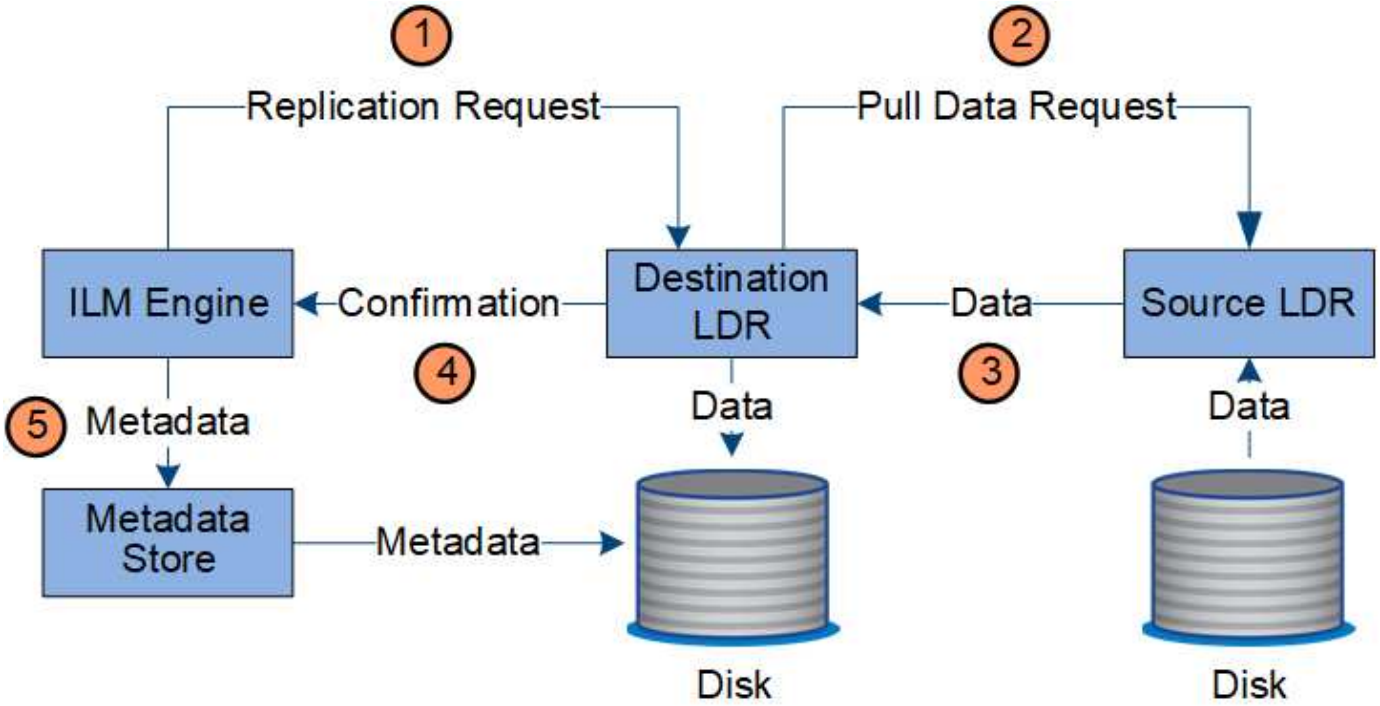
Je nach Lebenszyklus eines Objekts können unterschiedliche Arten oder Speicherorte von Objektkopien erforderlich sein. ILM-Regeln werden regelmäßig ausgewertet, um sicherzustellen, dass Objekte wie benötigt platziert werden.

Die Objektdaten werden vom LDR Service verwaltet.

Inhaltsschutz: Replikation

Wenn die Inhaltsplatzierungsanweisungen einer ILM-Regel replizierte Kopien von Objektdaten erfordern, werden Kopien von den Storage Nodes, aus denen der konfigurierte Speicherpool besteht, erstellt und auf Festplatten gespeichert.

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

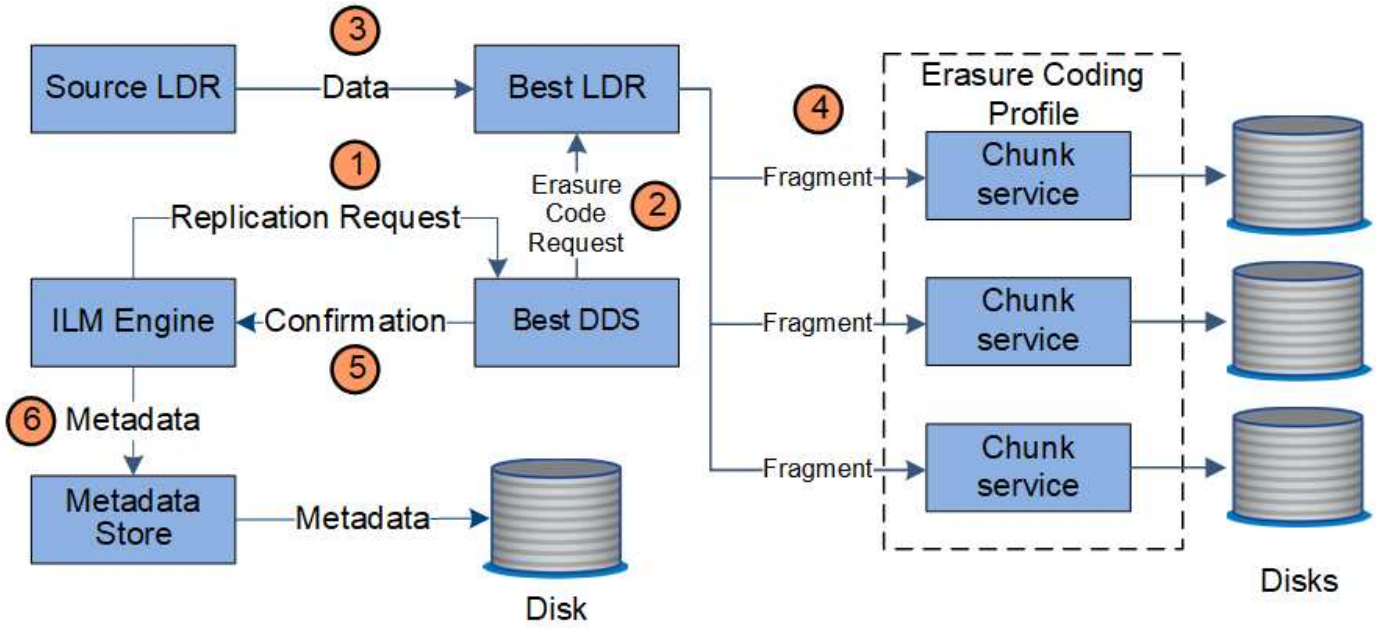


1. Die ILM-Engine fragt den ADC-Dienst ab, um den besten Ziel-LDR-Dienst innerhalb des durch die ILM-Regel festgelegten Speicherpools zu ermitteln. Anschließend sendet sie diesem LDR-Dienst einen Befehl zur Initiierung der Replikation.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellstandort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

Inhaltsschutz: Erasure Coding

Enthält eine ILM-Regel Anweisungen zum Erstellen von löschcodierten Kopien von Objektdaten, zerlegt das anwendbare Löschcodierungsverfahren die Objektdaten in Daten- und Paritätsfragmente und verteilt diese Fragmente auf die im Löschcodierungsprofil konfigurierten Storage Nodes.

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

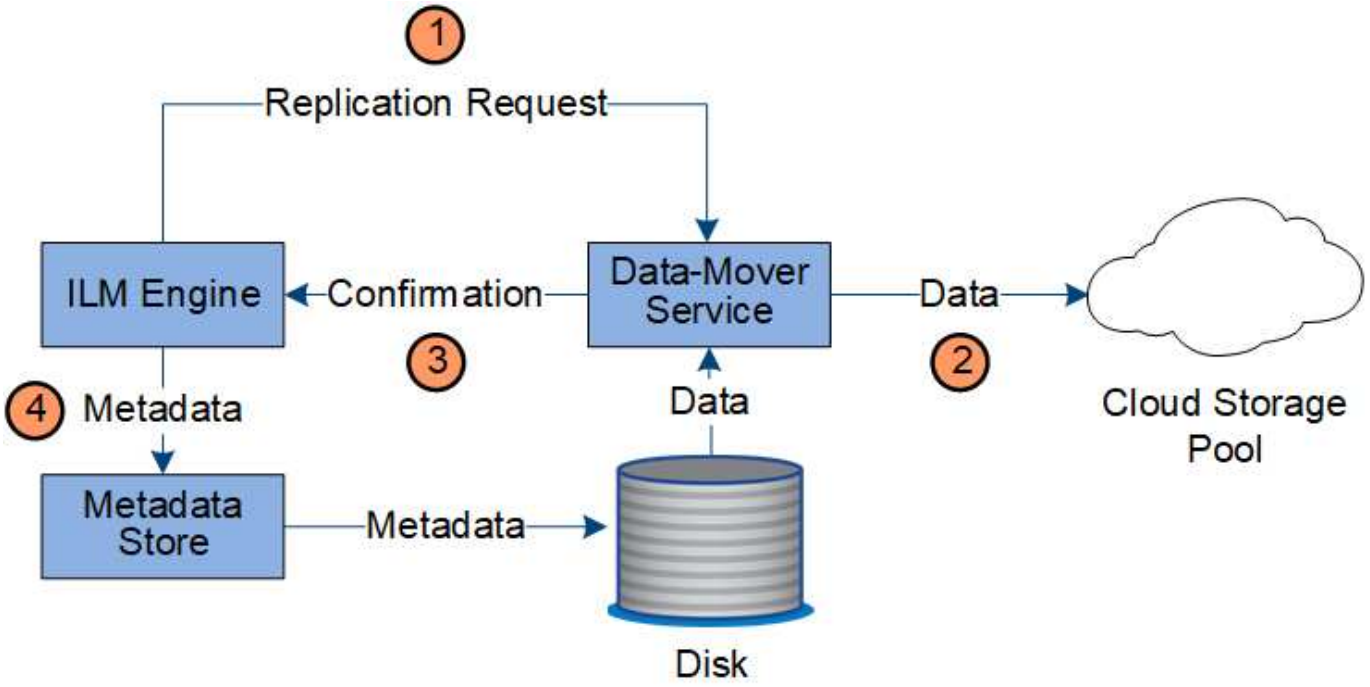


1. Die ILM-Engine fragt den ADC-Dienst ab, um zu bestimmen, welcher DDS-Dienst die Löschungscodierung am besten durchführen kann. Nach der Bestimmung sendet die ILM-Engine eine „Initiate“-Anforderung an diesen Dienst.
2. Der DDS-Dienst weist einen LDR an, die Objektdaten mit einer Erasure-Codierung zu versehen.
3. Der Quell-LDR-Dienst sendet eine Kopie an den für das Erasure Coding ausgewählten LDR-Dienst.
4. Nachdem die entsprechende Anzahl an Parität- und Datenfragmenten erstellt wurde, verteilt der LDR-Dienst 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 die Objektdaten erfolgreich verteilt wurden.
6. Die ILM Engine aktualisiert den Metadatenspeicher mit Metadaten zum Objektstandort.

Inhaltsschutz: Cloud Storage Pool

Wenn die Inhaltsplatzierungsanweisungen einer ILM-Regel erfordern, dass eine replizierte Kopie der Objektdaten in einem Cloud Storage Pool gespeichert wird, werden die 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-Dienstes ist, und der Data Mover Service steuern die Bewegung von Objekten in den Cloud Storage Pool.



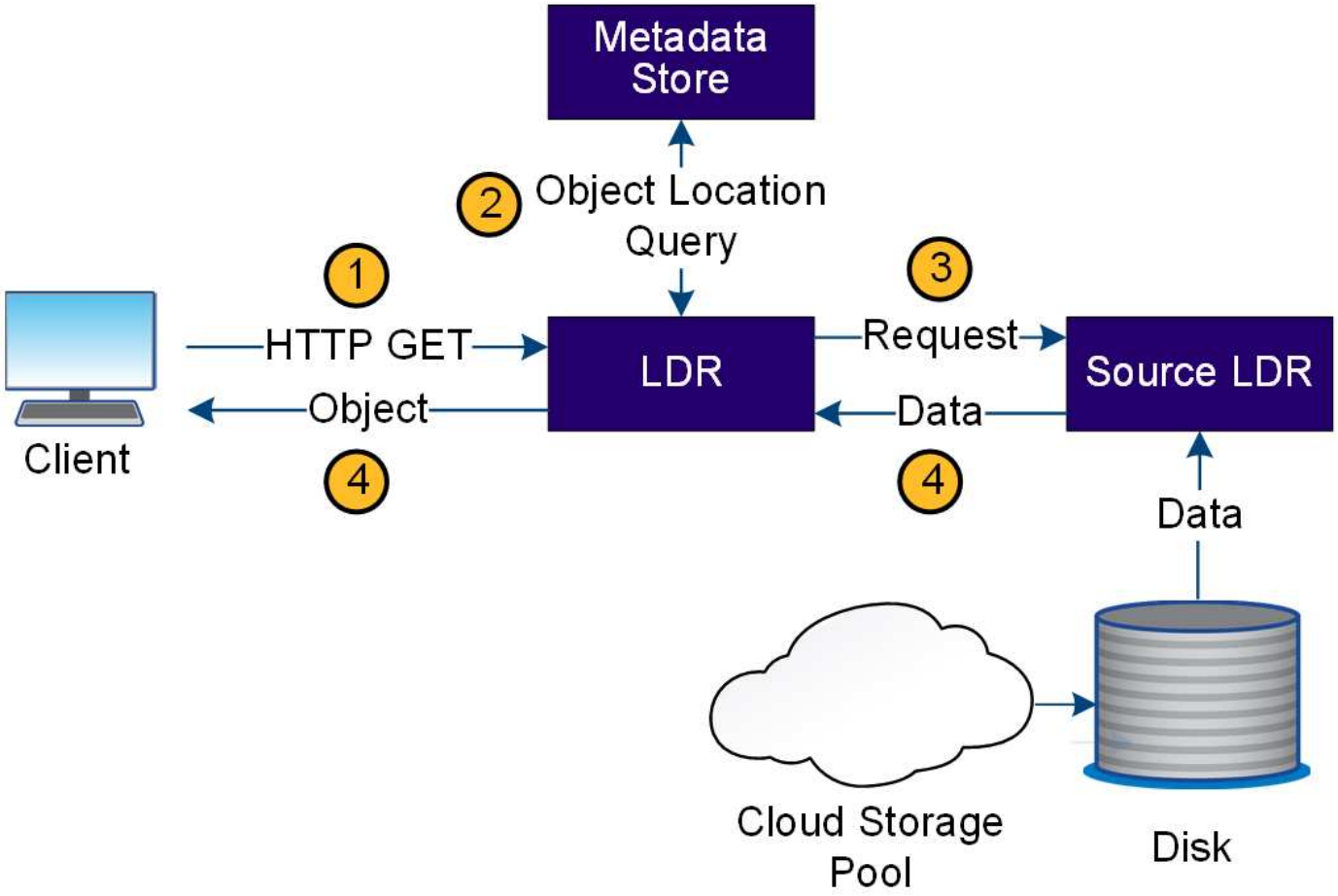
1. Die ILM Engine wählt einen Data Mover Service aus, der in den Cloud Storage Pool repliziert wird.
2. Der Data Mover Dienst sendet die Objektdaten an den Cloud Storage Pool.
3. Der Data Mover Dienst benachrichtigt die ILM Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM Engine aktualisiert den Metadatenspeicher mit Metadaten zum Objektstandort.

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 zu verfolgen.

Der LDR-Dienst des Storage Node fragt den Metadatenspeicher nach dem Speicherort der Objektdaten ab und ruft diese vom Quell-LDR-Dienst ab. Der Abruf erfolgt vorzugsweise von einem Storage Node. Ist das Objekt auf einem Storage Node nicht verfügbar, wird die Abrufanfrage an einen Cloud Storage Pool weitergeleitet.

Befindet sich die einzige Objektkopie im AWS Glacier Storage oder in der Azure Archive Tier, muss die Clientanwendung eine S3 RestoreObject-Anforderung stellen, um eine wiederherstellbare Kopie im Cloud Storage Pool wiederherzustellen.



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

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 abläuft, wodurch die automatische Entfernung ausgelöst wird. Für die Objektlöschung existiert ein definierter Datenfluss.

Löschhierarchie

StorageGRID bietet verschiedene Methoden zur Steuerung des Aufbewahrungs- oder Löschzeitpunkts von Objekten. Objekte können auf Client-Anfrage oder automatisch gelöscht werden. StorageGRID priorisiert stets alle S3 Object Lock-Einstellungen gegenüber Löschanforderungen des Clients, die wiederum Vorrang vor S3-Bucket-Lifecycle- und ILM-Platzierungsanweisungen haben.

- **S3 Object Lock**: Wenn die globale S3 Object Lock-Einstellung für das Grid aktiviert ist, können S3-Clients Buckets mit aktivierter S3 Object Lock erstellen und anschließend über die S3 REST API Aufbewahrungsfristen (retain-until-date) und rechtliche Aufbewahrung (legal hold) für jede Objektversion festlegen, die diesem Bucket hinzugefügt wird.

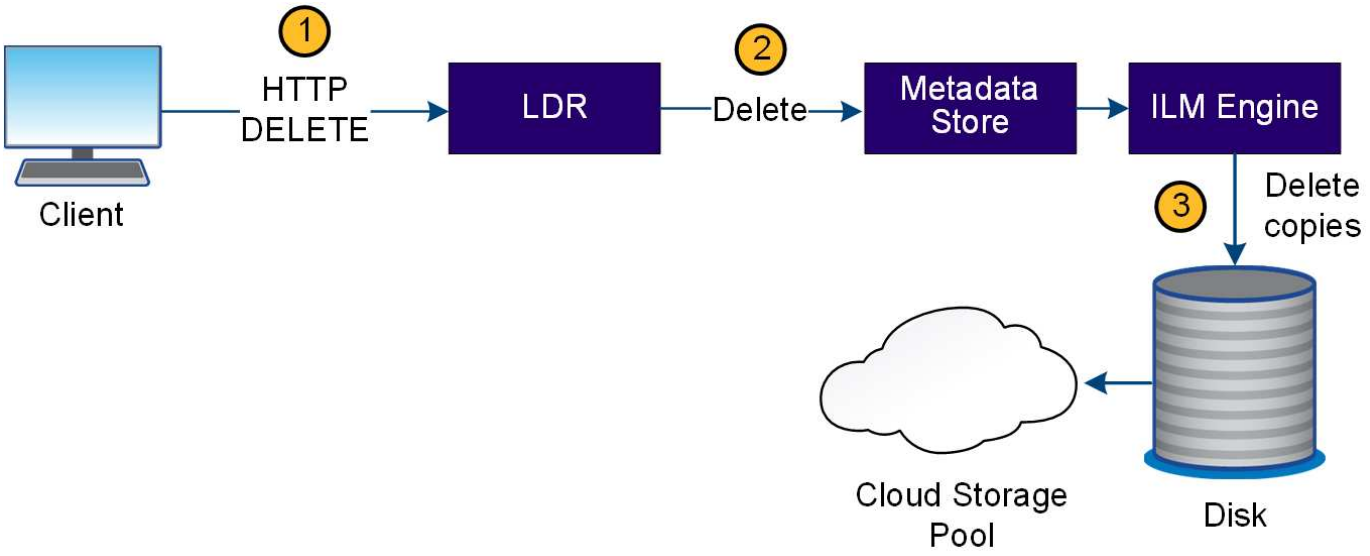
- Eine unter rechtlicher Sperre stehende Objektversion kann mit keiner Methode gelöscht werden.
- Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version mit keiner Methode gelöscht werden.
- Objekte in Buckets mit aktivierter S3 Object Lock werden von ILM „dauerhaft“ aufbewahrt. Nach Ablauf des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Client-Anfrage oder durch das Ende des Bucket-Lebenszyklus gelöscht werden.
- Wenn S3-Clients ein Standard-Retain-Until-Date für den Bucket festlegen, müssen sie kein Retain-Until-Date für jedes Objekt angeben.

- **Client-Löschanforderung**: Ein S3-Client kann eine Löschanforderung für ein Objekt stellen. Wenn ein Client ein Objekt löscht, werden alle Kopien des Objekts aus dem StorageGRID System entfernt.
- **Objekte im Bucket löschen**: Tenant Manager-Benutzer können mit dieser Option alle Kopien der Objekte und Objektversionen in ausgewählten Buckets dauerhaft aus dem StorageGRID System entfernen.
- **S3 Bucket Lifecycle**: S3-Clients können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Expiration-Aktion festlegt. Wenn ein Bucket-Lebenszyklus existiert, löscht StorageGRID automatisch alle Kopien eines Objekts, sobald das in der Expiration-Aktion angegebene Datum oder die Anzahl der Tage erreicht ist, es sei denn, der Client löscht das Objekt zuerst.
- **ILM-Platzierungsanweisungen**: Unter der Annahme, dass für den Bucket keine S3-Objektsperre aktiviert ist und kein Bucket-Lebenszyklus existiert, löscht StorageGRID ein Objekt automatisch, wenn der letzte Zeitraum in der ILM-Regel abläuft und keine weiteren Platzierungen für das Objekt angegeben sind.

> Wenn ein S3-Bucket-Lifecycle konfiguriert ist, überschreiben die Ablaufaktionen des Lifecycles die ILM-Richtlinie für Objekte, die dem Lifecycle-Filter entsprechen. Daher kann ein Objekt im Grid verbleiben, selbst nachdem alle ILM-Anweisungen zum Platzieren des Objekts abgelaufen sind.

Siehe "Wie Objekte gelöscht werden" für weitere Informationen.

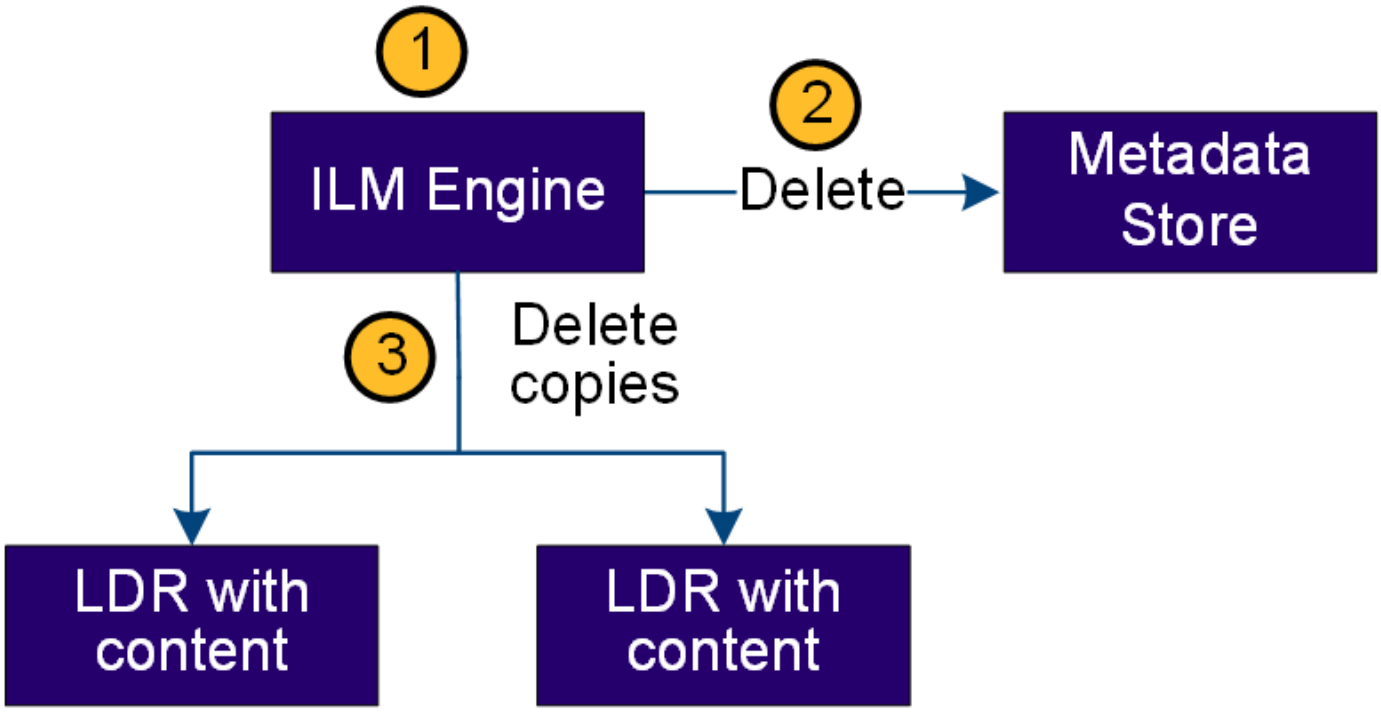
Datenfluss für das Löschen durch den Client



1. Der LDR Dienst empfängt eine Löschanforderung von der Clientanwendung.
2. Der LDR Service aktualisiert den Metadatenspeicher, sodass das Objekt für Clientanfragen als gelöscht erscheint, und weist die ILM Engine an, alle Kopien der Objektdaten zu entfernen.

3. Das Objekt wird aus dem System entfernt. Der Metadatenspeicher wird aktualisiert, um die Objektmetadaten zu entfernen.

Datenfluss für ILM Löschvorgänge



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

Informationslebenszyklusmanagement in StorageGRID

Mit Information Lifecycle Management (ILM) wird die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte im StorageGRID System gesteuert. ILM-Regeln bestimmen, wie StorageGRID Objekte im Zeitverlauf speichert. Eine oder mehrere ILM-Regeln werden konfiguriert und anschließend einer ILM-Richtlinie hinzugefügt. Ein Grid kann mehr als eine aktive Richtlinie gleichzeitig haben.

Die ILM-Regeln definieren:

- Welche Objekte gespeichert werden sollen. Eine Regel kann für alle Objekte gelten, oder es können Filter angegeben werden, um festzulegen, auf welche Objekte eine Regel angewendet wird. Beispielsweise kann eine Regel nur für Objekte gelten, die bestimmten Mandantenkonten, bestimmten S3 Buckets oder bestimmten Metadatenwerten zugeordnet sind.
- Speichertyp und Speicherort. Objekte können auf Speicherknoten oder in Cloud Storage Pools gespeichert werden.
- Die Art der erstellten Objektkopien. Kopien können repliziert oder mit Löschcodierung erstellt werden.
- Bei vervielfältigten Kopien die Anzahl der angefertigten Kopien.

- Bei löschcodierten Kopien das verwendete Löschcodierungsverfahren.
- Die Veränderungen im Laufe der Zeit hinsichtlich des Speicherorts eines Objekts und der Art der Kopien.
- Wie Objektdaten beim Einfügen von Objekten in das Grid geschützt werden (synchrones Placement oder Dual Commit).

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

Beispiel einer ILM-Regel

Eine ILM Regel könnte beispielsweise Folgendes festlegen:

- Gilt nur für Objekte, die zu Tenant A gehören.
- Zwei replizierte Kopien dieser Objekte werden erstellt und jede Kopie an einem anderen Standort gespeichert.
- Die beiden Kopien werden dauerhaft gespeichert, das bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen bewahrt StorageGRID diese Objekte auf, bis sie entweder durch eine Löschanforderung eines Clients oder durch das Ablaufen eines Bucket-Lebenszyklus gelöscht werden.
- Die Option „Ausgewogen“ für das Aufnahmeverhalten bewirkt, dass die Anweisung zur Platzierung an zwei Standorten angewendet wird, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, beide erforderlichen Kopien sofort zu erstellen.

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

Wie eine ILM-Richtlinie Objekte auswertet

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

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

1. Wenn die Filter der ersten Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten dieser Regel aufgenommen und gemäß den Platzierungsanweisungen dieser Regel gespeichert.
2. Wenn die Filter der ersten Regel nicht mit dem Objekt übereinstimmen, wird das Objekt mit jeder nachfolgenden Regel in der Richtlinie verglichen, bis eine Übereinstimmung gefunden wird.
3. Wenn keine Regel auf ein Objekt zutrifft, werden das Aufnahmeverhalten und die Platzierungsanweisungen der Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie und darf keine Filter verwenden. Sie muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

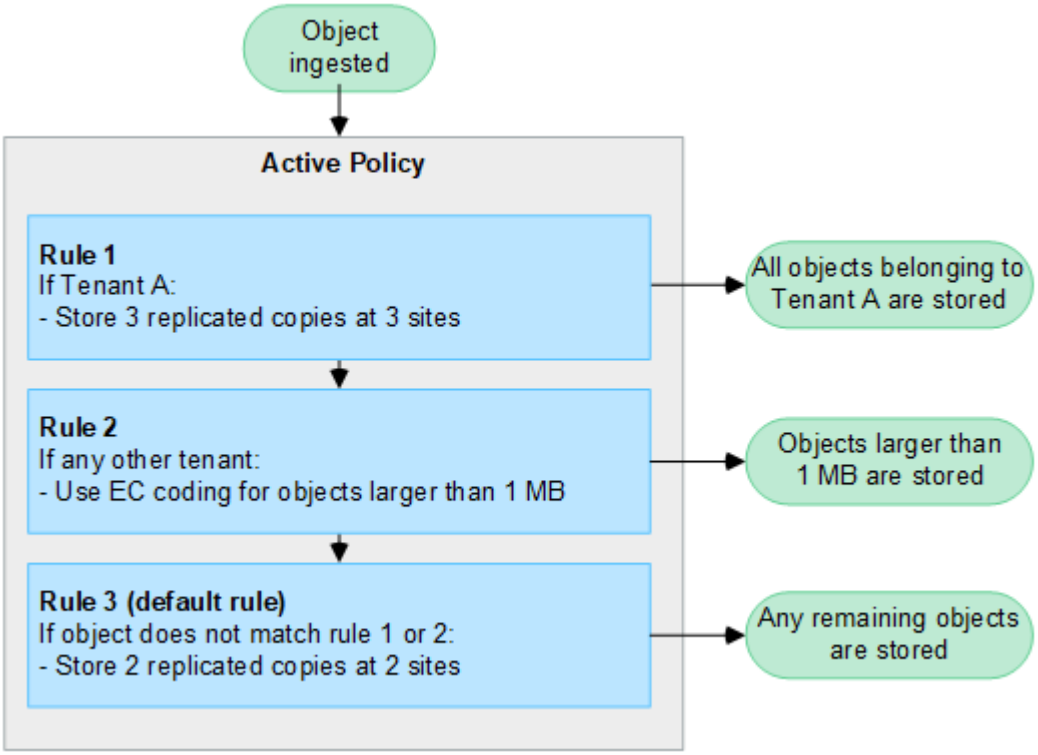
Beispiel einer ILM-Richtlinie

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

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

- Alle Objekte, die zu Tenant A gehören, abgleichen.
- Diese Objekte werden als drei replizierte Kopien an drei Standorten gespeichert.
- Objekte, die anderen Mandanten gehören, werden von Regel 1 nicht erfasst, daher erfolgt die Auswertung anhand von Regel 2.

- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte anderer Mandanten werden abgeglichen, jedoch 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 kleiner, daher werden diese Objekte anhand von Regel 3 ausgewertet.
- **Regel 3: 2 Kopien 2 Rechenzentren** (Standard)
  - Dies ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Zwei replizierte Kopien aller Objekte, die nicht von Regel 1 oder Regel 2 erfasst werden (Objekte, die nicht zu Tenant A gehören und 1 MB oder kleiner sind), werden erstellt.



Verwandte Informationen

- "Objekte mit ILM verwalten"

StorageGRID erkunden

Erkunden Sie den StorageGRID Grid Manager

Der Grid Manager ist die browserbasierte grafische Benutzeroberfläche, die die Konfiguration, Verwaltung und Überwachung Ihres StorageGRID Systems ermöglicht.

Der Grid Manager wird mit jeder neuen Version aktualisiert und entspricht möglicherweise nicht den Beispiel-Screenshots auf dieser Seite.

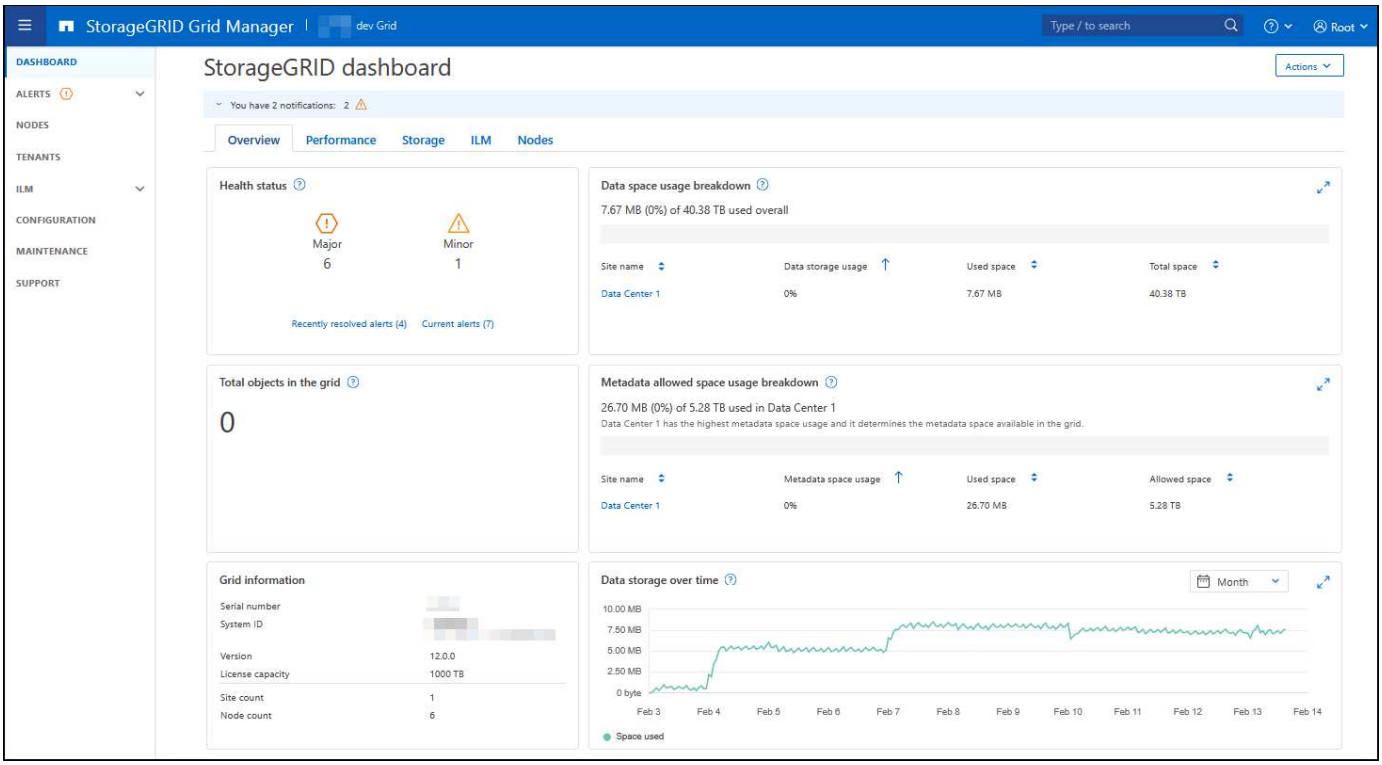
Wenn Sie sich im Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Jedes StorageGRID System umfasst einen primären Admin-Knoten und beliebig viele nicht-primäre Admin-Knoten. Sie können sich mit jedem Admin-Knoten verbinden, und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID Systems an.

Sie können mit einem "unterstützte Webbrowser" auf den Grid Manager zugreifen.

Grid Manager Dashboard

Wenn Sie sich zum ersten Mal im Grid Manager anmelden, kann das Dashboard genutzt werden, um "Systemaktivitäten überwachen" einen Überblick zu erhalten.

Das Dashboard enthält Informationen zum Systemzustand und zur Leistung, zur Speichernutzung, zu ILM-Prozessen, zu S3-Operationen und zu den Knoten im Grid. Es besteht die Möglichkeit, "Das Dashboard konfigurieren" aus einer Sammlung von Karten auszuwählen, die die benötigten Informationen für eine effektive Überwachung Ihres Systems enthalten.



Eine Erklärung der auf den einzelnen Karten angezeigten Informationen findet sich durch Auswahl des Hilfesymbols (?) für die jeweilige Karte.

Suchfeld

Das **Suchfeld** in der Kopfzeile ermöglicht eine schnelle Navigation zu einer bestimmten Seite im Grid Manager. Beispielsweise kann **km** eingegeben werden, um die Seite des Key management server (KMS) aufzurufen.

Sie können die **Suche** verwenden, um Einträge in der Seitenleiste des Grid Manager sowie in den Menüs „Konfiguration“, „Wartung“ und „Support“ zu finden. Es besteht außerdem die Möglichkeit, nach Namen zu suchen, beispielsweise nach Grid Nodes und Tenant Accounts.

Hilfemenü

Das Hilfemenü  bietet Zugriff auf:

- Die "FabricPool" und "S3 Setup" Assistenten
- Die StorageGRID Dokumentationsseite für die aktuelle Version
- "API-Dokumentation"
- Informationen darüber, welche Version von StorageGRID aktuell installiert ist

Benachrichtigungsmenü

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

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

- Aktuelle Warnmeldungen prüfen
- Gelöste Warnmeldungen überprüfen
- Stummschaltungen konfigurieren, um Warnmeldungen zu unterdrücken
- Alarmregeln für Bedingungen definieren, die Alarme auslösen
- Den E-Mail-Server für Benachrichtigungen konfigurieren

Nodes-Seite

Die "Nodes-Seite" zeigt Informationen über das gesamte Grid, jeden Standort im Grid und jeden Knoten an einem Standort an. Informationen zu einem bestimmten Standort oder Knoten werden angezeigt, wenn der entsprechende Standort oder Knoten ausgewählt wird.

Mandantenseite

Das "Mandantenseite" ermöglicht es, "Speichermandantenkonten erstellen und überwachen" für Ihr StorageGRID System zu nutzen. Mindestens ein Mandantenkonto muss erstellt werden, um festzulegen, wer Objekte speichern und abrufen kann und welche Funktionen diesen Personen zur Verfügung stehen.

Die Seite „Mandanten“ enthält außerdem Nutzungsdetails für jeden Mandanten, einschließlich des belegten Speicherplatzes und der Anzahl der Objekte. Wenn bei der Erstellung des Mandanten ein Kontingent festgelegt wurde, ist ersichtlich, wie viel dieses Kontingents bereits genutzt wurde.

ILM Menü

Das "ILM Menü" ermöglicht das "die Regeln und Richtlinien für das Information Lifecycle Management (ILM) konfigurieren" Festlegen von Richtlinien für Datenbeständigkeit und Datenverfügbarkeit. Es besteht außerdem die Möglichkeit, eine Objektkennung einzugeben, um die Metadaten für dieses Objekt anzuzeigen.

Im ILM-Menü lassen sich ILM anzeigen und verwalten:

- Regeln
- Richtlinien
- Richtlinien-Tags
- Storage Pools

- Storage-Grades
- Regionen
- Objektmetadatenabfrage

Konfigurationsmenü

Im Konfigurationsmenü lassen sich Netzwerkeinstellungen, Sicherheitseinstellungen, Systemeinstellungen, Überwachungsoptionen und Zugriffskontrolloptionen angeben.

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

- "Hochverfügbarkeitsgruppen verwalten"
- "Load Balancer Endpunkte verwalten"
- "S3-Endpunkt-Domänennamen konfigurieren"
- "Verkehrsklassifizierungsrichtlinien verwalten"
- "${post_edited_translations.segment}"
- "StorageGRID CORS für eine Managementoberfläche aktivieren"

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

- "Sicherheitszertifikate verwalten"
- "Interne Firewall-Steuerungen verwalten"
- "Schlüsselverwaltungsserver konfigurieren"
- Sicherheitseinstellungen konfigurieren, einschließlich "TLS und SSH-Richtlinie", "Netzwerk- und Objektsicherheitsoptionen", "Schnittstellen-Sicherheitseinstellungen" und "SSH-Zugriffsoptionen"
- Einstellungen für ein "Storage Proxy" oder ein "Admin-Proxy" konfigurieren

Systemaufgaben

Zu den Systemaufgaben gehören:

- Verwenden Sie "Grid-Föderation" zum Klonen von Mandantenkontoinformationen und zum Replizieren von Objektdaten zwischen zwei StorageGRID Systemen
- Optional kann die "Gespeicherte Objekte komprimieren" Option aktiviert werden.
- Optional kann die "Standardeinstellung für Bucket-Konsistenz"
- "S3 Object Lock verwalten"
- Speichereinstellungen wie "Speichervolumen Wasserzeichen" verstehen
- "Erasure-Coding-Profile verwalten"

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- "Protokollverwaltung konfigurieren"
- "SNMP Überwachung"

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugangskontrolle gehören:

- "${post_edited_translations.segment}"
- "Administratorbenutzer verwalten"
- Ändern Sie die "Bereitstellungspassphrase" oder "Konsolenpasswörter für Nodes"
- "Identitätsföderation verwenden"
- "SSO konfigurieren"

Wartungsmenü

Das Wartungsmenü ermöglicht die Durchführung von Wartungsaufgaben, Systemwartung und Netzwerkwartung.

Aufgaben

Zu den Wartungsaufgaben gehören:

- "Stilllegungsoperationen" zum Entfernen ungenutzter Grid-Nodes und Standorte
- "Erweiterungsvorgänge" neue Grid-Knoten und Standorte hinzufügen
- "Verfahren zur Wiederherstellung von Grid-Knoten" einen ausgefallenen Knoten ersetzen und Daten wiederherstellen
- "Umbenennungsverfahren"die Anzeigenamen Ihres Grids, Ihrer Standorte und Knoten zu ändern
- "Objektexistenzprüfungsoperationen"um die Existenz (jedoch nicht die Korrektheit) von Objektdaten zu überprüfen
- Einen "Rolling-Reboot"Neustart mehrerer Grid-Knoten durchführen
- "Volumenwiederherstellungsmaßnahmen"

System

Zu den Systemwartungsaufgaben, die Sie durchführen können, gehören:

- "${post_edited_translations.segment}" oder "Lizenzinformationen aktualisieren"
- Generieren und Herunterladen der "Wiederherstellungspaket"
- Durchführen von StorageGRID Softwareaktualisierungen, einschließlich Software-Upgrades, Hotfixes und Aktualisierungen der SANtricity OS Software auf ausgewählten Appliances
  - "Upgrade-Verfahren"
  - "Hotfix Verfahren"
  - "SANtricity OS auf SG6000 Storage Controllern mit Grid Manager aktualisieren"
  - "Upgrade von SANtricity OS auf SG5700 Storage Controllern mit Grid Manager"

Netzwerk

Zu den Netzwerkwartungsaufgaben, die Sie durchführen können, gehören:

- "DNS-Server konfigurieren"
- "Grid Network-Subnetze aktualisieren"
- "NTP Server verwalten"

Support Menü

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

Tools

Im Bereich „Tools“ des Support-Menüs sind folgende Aktionen möglich:

- "Konfiguration von AutoSupport"
- "Diagnose ausführen" zum aktuellen Zustand des Grid
- "Protokolldateien und Systemdaten sammeln"
- "Support-Metriken überprüfen"

> Die unter der Option **Metriken** verfügbaren Tools sind für den Einsatz durch den technischen Support vorgesehen. Einige Funktionen und Menüpunkte innerhalb dieser Tools sind absichtlich nicht funktionsfähig.

Sonstige

Im Abschnitt „Sonstiges“ des Support-Menüs sind folgende Aktionen möglich:

- Konfigurieren "E/A-Priorisierung"
- Konfigurieren "AutoSupport E-Mail-Einrichtung (Legacy)"
- Verwalten "Verbindungskosten"
- Service-IDs des Knotens anzeigen
- Verwalten "Speicherwasserzeichen"

Erkunden Sie den StorageGRID Tenant Manager

Das "Tenant Manager" ist die browserbasierte grafische Benutzeroberfläche, über die Mandantenbenutzer ihre Speicherkonten konfigurieren, verwalten und überwachen.

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

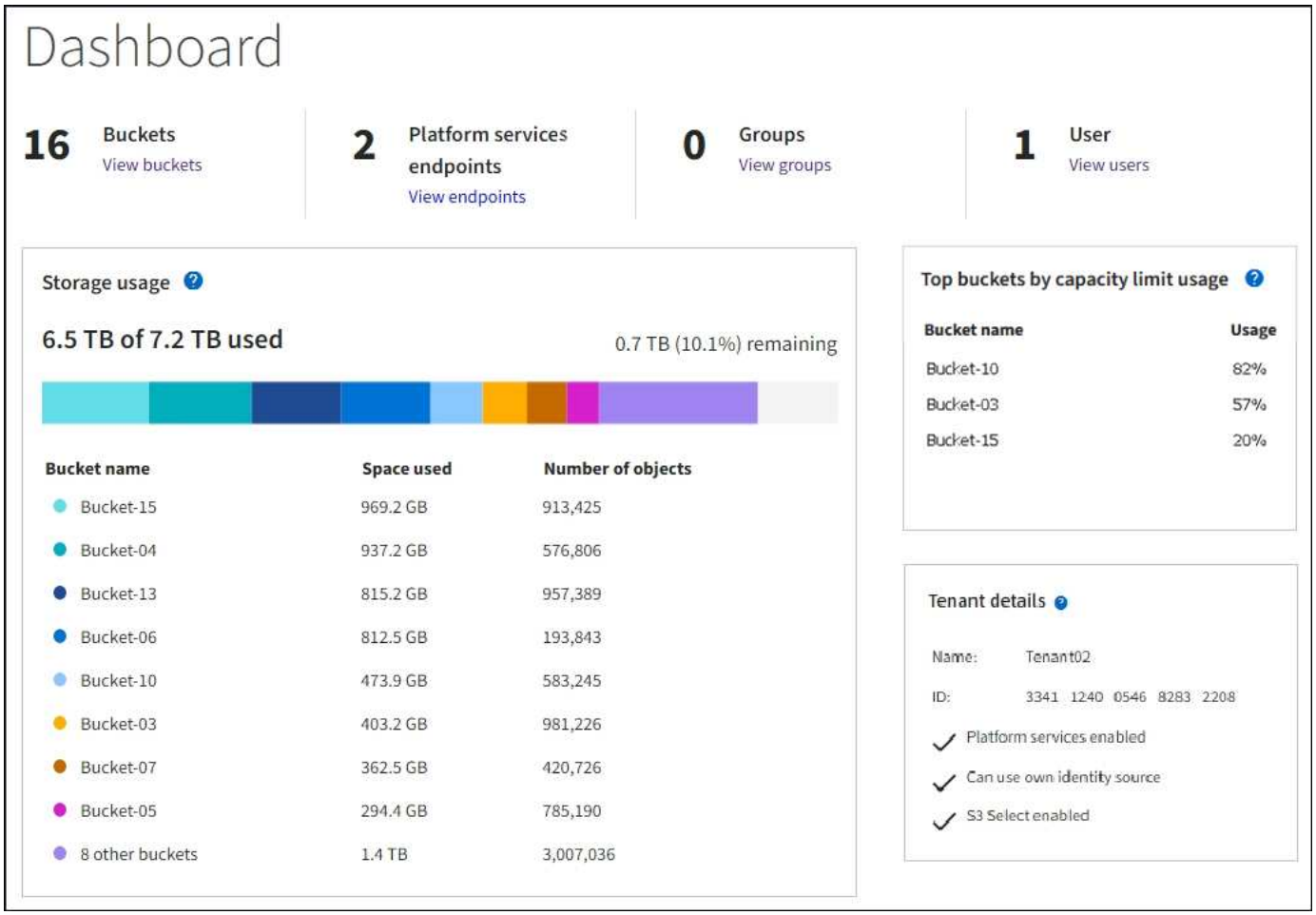
Wenn sich Mandantenbenutzer beim Tenant Manager anmelden, stellen sie eine Verbindung zu einem Admin Node her.

Tenant Manager Dashboard

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

Das Tenant Manager Dashboard ermöglicht es Mandantenbenutzern, die Speichernutzung auf einen Blick zu überwachen. Das Panel „Speichernutzung“ enthält eine Liste der größten S3 Buckets für den Mandanten. Der Wert „Belegter Speicherplatz“ entspricht der Gesamtmenge der Objektdaten im Bucket oder Container. Das Balkendiagramm stellt die relativen Größen dieser Buckets oder Container dar.

Der Wert über dem Balkendiagramm entspricht der Summe des Speicherplatzes aller Buckets oder Container des Mandanten. Wurde bei der Kontoerstellung die maximale Anzahl an Gigabyte, Terabyte oder Petabyte für den Mandanten festgelegt, werden auch der genutzte und der verbleibende Anteil des Kontingents angezeigt.



Speichermenü (S3)

Dieses Menü ermöglicht S3 Benutzern Folgendes:

- Zugriffsschlüssel verwalten
- Buckets erstellen, verwalten und löschen
- Plattform Services Endpunkte verwalten
- Alle Grid Federation Verbindungen, zu deren Nutzung sie berechtigt sind, anzeigen

Meine Zugangsschlüssel

S3-Tenant-Benutzer können Zugriffsschlüssel wie folgt verwalten:

- Benutzer, die über die Berechtigung "Eigene S3-Anmeldeinformationen verwalten" verfügen, können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit Root-Zugriffsberechtigung können die Zugriffsschlüssel für das S3-Root-Konto, ihr eigenes Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel gewähren außerdem vollen Zugriff auf die Buckets und Objekte des Mandanten, sofern dies nicht explizit durch eine Bucket-Richtlinie deaktiviert wird.

> Die Verwaltung der Zugriffsschlüssel für andere Benutzer erfolgt über das Menü Access management.

Buckets

S3-Tenant-Benutzer mit den entsprechenden Berechtigungen haben die Möglichkeit, die folgenden Aufgaben für ihre Buckets auszuführen:

- Buckets erstellen
- Aktivieren der S3-Objektsperre für einen neuen Bucket (setzt voraus, dass die S3-Objektsperre für das StorageGRID System aktiviert ist)
- Konsistenzwerte aktualisieren
- Aktivieren und Deaktivieren von Aktualisierungen der letzten Zugriffszeit
- Objektversionierung aktivieren oder aussetzen
- Standardaufbewahrungsdauer für S3 Object Lock aktualisieren
- Konfiguration der ursprungsübergreifenden Ressourcenteilung (CORS)
- Alle Objekte in einem Bucket löschen
- Leere Buckets löschen
- Die Funktion "S3 Konsole" dient zur Verwaltung von Bucket-Objekten.

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

- S3-Ereignisbenachrichtigungen konfigurieren, die an einen Zieldienst gesendet werden können, der den Amazon Simple Notification Service unterstützt.
- Die CloudMirror-Replikation konfigurieren, wodurch der Mandant Objekte automatisch in einen externen S3-Bucket replizieren kann.
- Die Suchintegration wird konfiguriert, sodass Objektmetadaten an einen Zielsuchindex gesendet werden, wenn ein Objekt erstellt oder gelöscht wird oder wenn dessen Metadaten oder Tags aktualisiert werden.

Endpunkte für Plattformdienste

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

Grid Federation Verbindungen

Wenn ein Grid-Administrator die Verwendung einer Grid-Federationsverbindung für das Mandantenkonto aktiviert hat, kann ein S3-Mandantenbenutzer mit Root-Zugriffsberechtigung den Verbindungsnamen anzeigen, auf die Bucket-Detailseite für jeden Bucket zugreifen, für den die Grid-übergreifende Replikation aktiviert ist, und den letzten Fehler einsehen, der bei der Replikation der Bucket-Daten in das andere Grid in der Verbindung aufgetreten ist. Siehe "Grid Federation Verbindungen anzeigen".

Menü „Access Management“

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

Netzwerkrichtlinien

Netzwerkrichtlinien für StorageGRID

Diese Richtlinien bieten Informationen zur StorageGRID Architektur und zu Netzwerktopologien sowie zu den Anforderungen an die Netzwerkkonfiguration und -bereitstellung.

Über diese Anweisungen

Diese Richtlinien liefern Informationen, mit denen die StorageGRID Netzwerkinfrastruktur vor der Bereitstellung und Konfiguration von StorageGRID Knoten erstellt werden kann. Diese Richtlinien tragen dazu bei, sicherzustellen, dass die Kommunikation zwischen allen Knoten im Grid sowie zwischen dem Grid und externen Clients und Diensten möglich ist.

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

- Objektdaten speichern und abrufen
- E-Mail-Benachrichtigungen empfangen
- Zugriff auf die StorageGRID Managementoberfläche (Grid Manager und Tenant Manager)
- Auf die Auditfreigabe zugreifen (optional)
- Dienstleistungen wie die folgenden werden bereitgestellt:
  - Network Time Protocol (NTP)
  - Domain Name System (DNS)
  - Schlüsselverwaltungsserver (KMS)

StorageGRID Netzwerkarchitektur muss entsprechend konfiguriert werden, um den Datenverkehr für diese Funktionen und mehr zu bewältigen.

Bevor Sie beginnen

Die Konfiguration der Netzwerkinfrastruktur eines StorageGRID Systems erfordert umfassende Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerkrouting und Firewalls.

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

Nachdem Sie festgelegt haben, welche StorageGRID Netzwerke Sie verwenden möchten und wie diese Netzwerke konfiguriert werden, können die StorageGRID Knoten gemäß den entsprechenden Anweisungen installiert und konfiguriert werden.

Appliance Knoten installieren

- "Gerätehardware installieren"

Softwarebasierte Knoten

- "StorageGRID auf softwarebasierten Knoten installieren"

StorageGRID Software konfigurieren und verwalten

- "StorageGRID verwalten"
- "Versionshinweise". Sie müssen sich mit Ihrem NetApp Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zuzugreifen.

StorageGRID Netzwerktypen

Die Grid-Knoten eines StorageGRID Systems verarbeiten Grid-Traffic, Admin-Traffic und Client-Traffic. Die Netzwerkkonfiguration muss entsprechend angepasst werden, um diese drei Arten von Traffic zu verwalten und Kontrolle sowie Sicherheit zu gewährleisten.

Verkehrsarten

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

Die Netzwerkkonfiguration ist auf folgende Weise möglich:

- Nur im Grid Network
- Grid und Admin Netzwerke
- Grid und Client Netzwerke
- Grid, Admin und Client Netzwerke

Das Grid Network ist obligatorisch und kann den gesamten Grid-Datenverkehr verwalten. Das Admin Network und das Client Network können bei der Installation einbezogen oder später hinzugefügt werden, um sich an geänderte Anforderungen anzupassen. Obwohl das Admin Network und das Client Network optional sind,

kann das Grid Network isoliert und gesichert werden, wenn diese Netzwerke für die Abwicklung des administrativen und des Client-Datenverkehrs verwendet werden.

Interne Ports sind nur über das Grid-Netzwerk erreichbar. Externe Ports sind von allen Netzwerktypen aus erreichbar. Diese Flexibilität bietet vielfältige Möglichkeiten für die Planung einer StorageGRID Bereitstellung und die Einrichtung externer IP- und Portfilter in Switches und Firewalls. Siehe "interne Grid-Knoten-Kommunikation" und "externe Kommunikation".

Netzwerkschnittstellen

StorageGRID Knoten sind über die folgenden spezifischen Schnittstellen mit den jeweiligen Netzwerken verbunden:

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

Weitere Informationen zur Zuordnung virtueller oder physischer Ports zu Knotennetzwerkschnittstellen finden Sie unter "StorageGRID auf softwarebasierten Knoten installieren".

Geräteknoten

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

Netzwerkinformationen für jeden Knoten

Für jedes Netzwerk, das Sie auf einem Knoten aktivieren, ist Folgendes zu konfigurieren:

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

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

Hochverfügbarkeitsgruppen

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

"Hochverfügbarkeitsgruppen verwalten".

Grid-Netzwerk

Das Grid Network ist erforderlich. Es wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das Grid Network stellt die Konnektivität zwischen allen Knoten im Grid über alle Standorte und Subnetze hinweg bereit. Alle Knoten im Grid Network müssen mit allen anderen Knoten kommunizieren können. Das Grid Network kann aus mehreren Subnetzen bestehen. Netzwerke mit kritischen Grid-Diensten, wie NTP, können ebenfalls als Grid-Subnetze hinzugefügt werden.

StorageGRID unterstützt keine Netzwerkadressübersetzung (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-Netzwerk-Gateway ist das Standardgateway des Knotens, es sei denn, für den Knoten ist das Client-Netzwerk konfiguriert.

Bei der Konfiguration des Grid-Netzwerks muss sichergestellt werden, dass das Netzwerk vor nicht vertrauenswürdigen Clients wie solchen im offenen Internet geschützt ist.

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

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

${post_edited_translations.segment}

Das Admin Network ist optional. Wenn es konfiguriert ist, kann es für Systemadministration und Wartungsdatenverkehr verwendet werden. Das Admin Network ist typischerweise ein privates Netzwerk und muss nicht zwischen den Knoten routbar sein.

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

Bei Verwendung des Admin Network muss der administrative und Wartungsdatenverkehr nicht über das Grid Network geleitet werden. Typische Anwendungsfälle des Admin Network sind die folgenden:

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

Das Admin Network wird niemals für internen Grid-Datenverkehr verwendet. Ein Admin Network Gateway ist vorhanden und ermöglicht dem Admin Network die Kommunikation mit mehreren externen Subnetzen. Das Admin Network Gateway wird jedoch niemals als Standard-Gateway des Knotens verwendet.

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

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

Client-Netzwerk

Das Clientnetzwerk ist optional. Wenn es konfiguriert ist, wird es verwendet, um Clientanwendungen wie S3 den Zugriff auf Grid-Dienste bereitzustellen. Wenn StorageGRID-Daten für eine externe Ressource (zum Beispiel einen Cloud Storage Pool oder den StorageGRID CloudMirror Replikationsdienst) zugänglich gemacht werden sollen, kann diese externe Ressource ebenfalls das Clientnetzwerk verwenden. Grid-Knoten können mit jedem Subnetz kommunizieren, das über das Clientnetzwerk-Gateway erreichbar ist.

Sie können auswählen, für welche Grid-Knoten das Client-Netzwerk aktiviert sein soll. Nicht alle Knoten müssen sich im selben Client-Netzwerk befinden, und die Knoten kommunizieren niemals über das Client-Netzwerk miteinander. Das Client-Netzwerk wird erst nach Abschluss der Grid-Installation betriebsbereit.

Zur Erhöhung der Sicherheit kann festgelegt werden, dass die Client Network-Schnittstelle eines Knotens als nicht vertrauenswürdig gilt, sodass das Client Network restriktiver hinsichtlich der zulässigen Verbindungen ist. Wenn die Client Network-Schnittstelle eines Knotens als nicht vertrauenswürdig eingestuft ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie beispielsweise von CloudMirror-Replikation verwendet werden, akzeptiert jedoch eingehende Verbindungen nur auf Ports, die explizit als Load Balancer-Endpunkte konfiguriert wurden. Siehe "Firewall-Steuerung verwalten" und "Load Balancer-Endpunkte konfigurieren".

Wenn ein Client Network verwendet wird, muss der Client-Datenverkehr nicht über das Grid Network laufen. Grid Network-Datenverkehr kann auf ein sicheres, nicht routbares Netzwerk getrennt werden. Die folgenden Knotentypen werden häufig mit einem Client Network konfiguriert:

- Gateway Nodes, da diese Nodes Zugriff auf den StorageGRID Load Balancer Service und S3-Clientzugriff auf das Grid bieten.
- Speicherknoten, da diese Knoten den Zugriff auf das S3-Protokoll und auf Cloud-Speicherpools sowie den CloudMirror Replikationsdienst ermöglichen.
- Admin-Knoten, damit Mandantenbenutzer eine Verbindung zum Tenant Manager herstellen können, ohne das Admin-Netzwerk nutzen zu müssen.

Beachten Sie Folgendes für das Client Network Gateway:

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

Optionale VLAN Netzwerke

Bei Bedarf können optional virtuelle LAN (VLAN) Netzwerke für Client-Datenverkehr und für bestimmte Arten von Administrator-Datenverkehr verwendet werden. Grid-Datenverkehr kann jedoch keine VLAN-Schnittstelle verwenden. Der interne StorageGRID Datenverkehr zwischen den Knoten muss immer das Grid-Netzwerk auf eth0 verwenden.

Um die Verwendung von VLANs zu unterstützen, muss eine oder mehrere Schnittstellen eines Knotens als Trunk-Schnittstellen am Switch konfiguriert werden. Die Grid Network-Schnittstelle (eth0) oder die Client Network-Schnittstelle (eth2) kann als Trunk konfiguriert werden, oder dem Knoten können Trunk-Schnittstellen

hinzugefügt werden.

Wenn eth0 als Trunk konfiguriert ist, fließt der Grid Network-Datenverkehr über die nativ-Schnittstelle des Trunks, wie am Switch konfiguriert. Analog dazu verwendet das Client Network, wenn eth2 als Trunk konfiguriert ist und das Client Network ebenfalls auf demselben Knoten konfiguriert ist, das native VLAN des Trunk-Ports, wie am Switch konfiguriert.

Über VLAN-Netzwerke wird ausschließlich eingehender Administrator-Datenverkehr unterstützt, beispielsweise für SSH, Grid Manager oder Tenant Manager. Ausgehender Datenverkehr, beispielsweise für NTP, DNS, LDAP, KMS und Cloud Storage Pools, wird über VLAN-Netzwerke nicht unterstützt.

> ⓘ VLAN-Schnittstellen können nur zu Admin-Knoten und Gateway-Knoten hinzugefügt werden. Eine VLAN-Schnittstelle kann nicht für den Client- oder Administratorzugriff auf Storage Nodes verwendet werden.

Siehe "${post_edited_translations.segment}" Anweisungen und Richtlinien.

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

Beispiele für Netzwerktopologien

Grid-Netzwerktopologie für StorageGRID

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

Bei der Konfiguration des Grid-Netzwerks werden die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle jedes Grid-Knotens festgelegt.

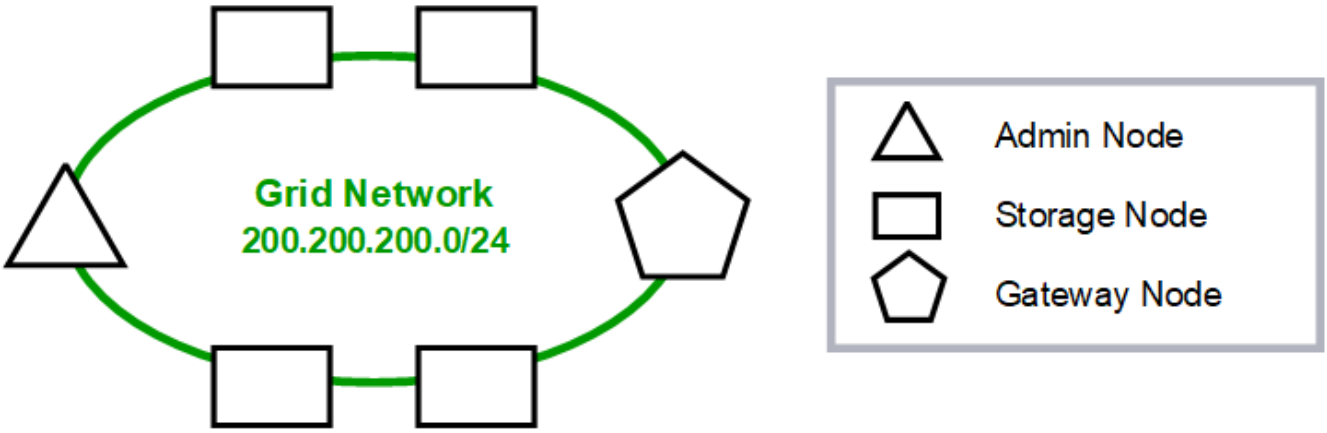
Während der Konfiguration müssen Sie alle Grid Network Subnetze zur Grid Network Subnetzliste (GNSL) hinzufügen. Diese Liste enthält alle Subnetze aller Standorte und kann auch externe Subnetze umfassen, die Zugriff auf wichtige Dienste wie NTP, DNS oder LDAP ermöglichen.

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

In diesem Beispiel nutzt der gesamte Datenverkehr dasselbe Netzwerk, einschließlich des Datenverkehrs im Zusammenhang mit S3-Clientanfragen sowie administrativen und Wartungsfunktionen.

> ⓘ Diese Topologie eignet sich für Einzelstandortbereitstellungen, die nicht extern verfügbar sind, für Proof-of-Concept- oder Testbereitstellungen oder wenn ein Load Balancer eines Drittanbieters als Clientzugriffsgrenze fungiert. Das Grid-Netzwerk sollte nach Möglichkeit ausschließlich für internen Datenverkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk verfügen über zusätzliche Firewall-Beschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Nutzung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, bietet jedoch weniger Schutzebenen.

Topology example: Grid Network only



Provisioned

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

System Generated

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

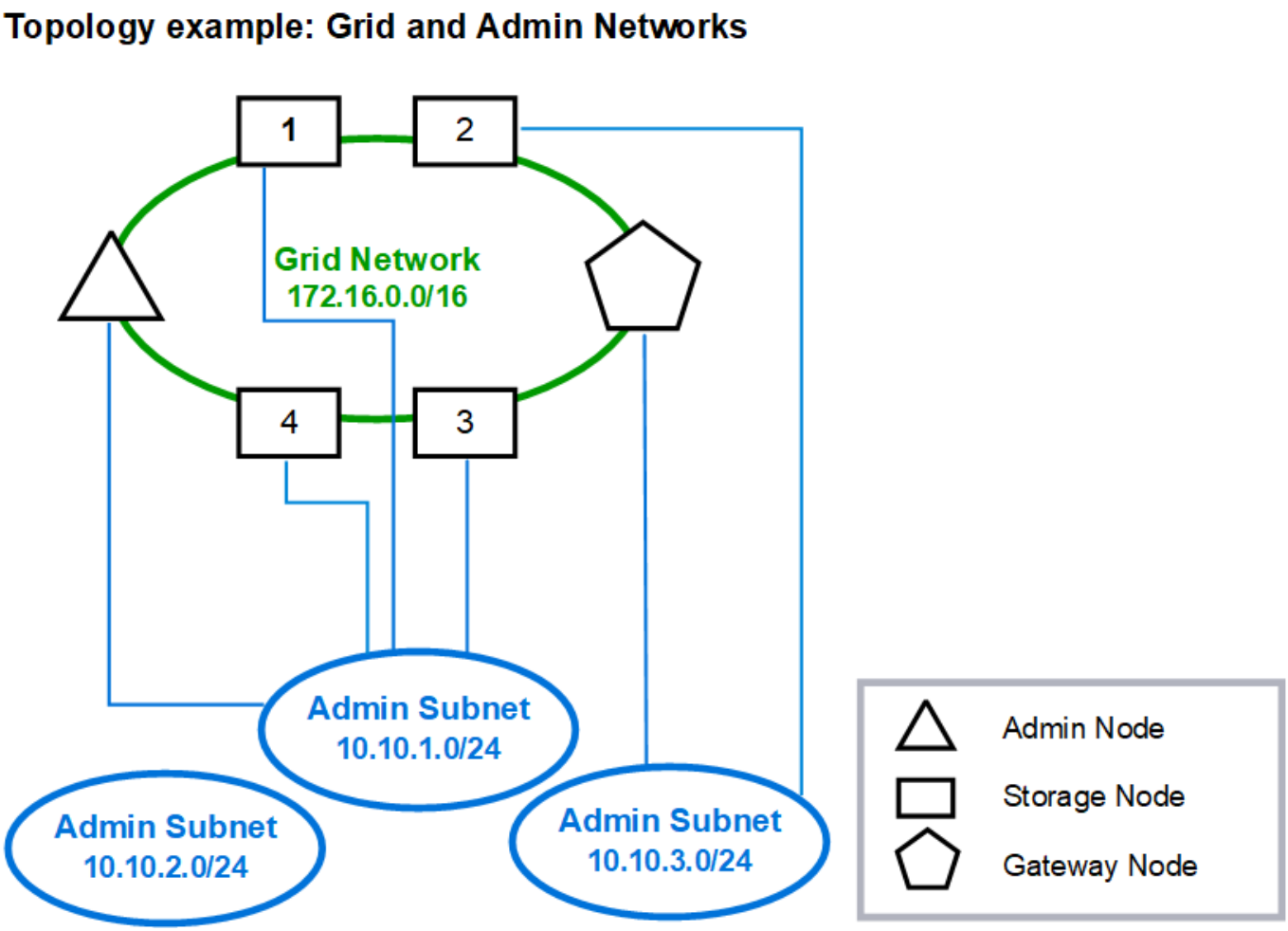
Admin-Netzwerktopologie für StorageGRID

Die Verwendung eines Admin Network ist optional. Eine Möglichkeit, ein Admin Network und ein Grid Network zu nutzen, besteht darin, für jeden Node ein routbares Grid Network und ein begrenztes Admin Network zu konfigurieren.

Bei der Konfiguration des Admin Network werden die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth1-Schnittstelle jedes Grid-Node festgelegt.

Das Admin Network kann für jeden Node einzigartig sein und aus mehreren Subnetzen bestehen. Jeder Node kann mit einer Admin External Subnet List (AESL) konfiguriert werden. Die AESL listet die Subnetze auf, die über das Admin Network für jeden Node erreichbar sind. Die AESL muss außerdem die Subnetze aller Services enthalten, auf die das Grid über das Admin Network zugreift, wie NTP, DNS, KMS und LDAP. Statische Routen werden für jedes Subnetz in der AESL angewendet.

In diesem Beispiel wird das Grid Network für den Datenverkehr im Zusammenhang mit S3-Clientanfragen und der Objektverwaltung verwendet, während das Admin Network für administrative Funktionen genutzt 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

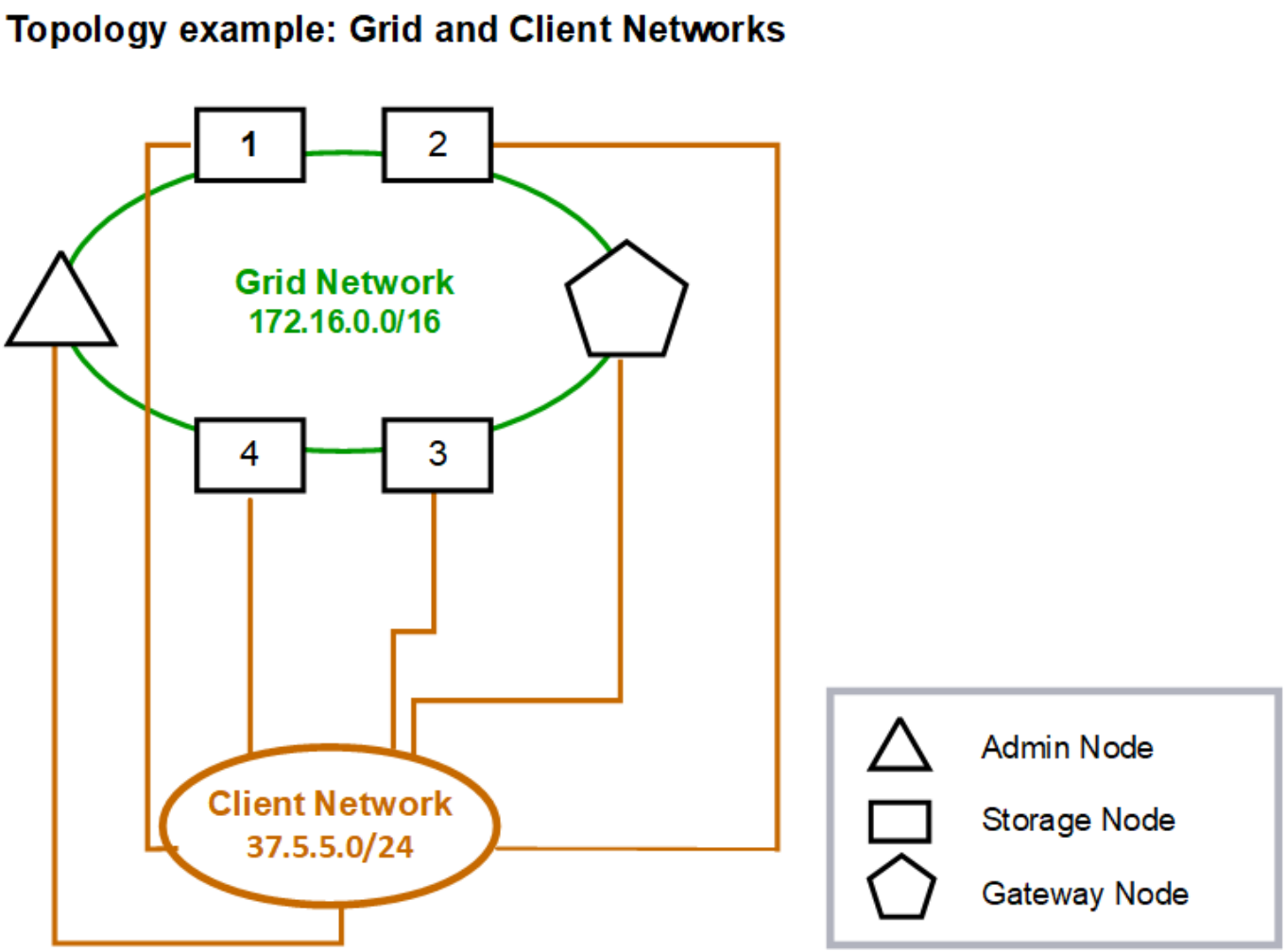
Die Einrichtung eines Client-Netzwerks ist optional. Durch die Verwendung eines Client-Netzwerks kann der Client-Netzwerkverkehr (zum Beispiel S3) vom internen Grid-Verkehr getrennt werden, was das Grid-Netzwerk sicherer macht. Administrativer Datenverkehr kann entweder über das Client- oder das Grid-Netzwerk erfolgen, wenn das Admin-Netzwerk nicht konfiguriert ist.

Bei der Konfiguration des Client Network werden die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth2-Schnittstelle des konfigurierten Node festgelegt. Das Client Network eines jeden Node kann unabhängig vom Client Network eines anderen Node sein.

Wenn während der Installation ein Clientnetzwerk für einen Knoten konfiguriert wird, wechselt das Standardgateway des Knotens nach Abschluss der Installation vom Grid Network Gateway zum Client Network Gateway. Wenn ein Clientnetzwerk später hinzugefügt wird, wechselt das Standardgateway des Knotens auf die gleiche Weise.

In diesem Beispiel wird das Client Network für S3-Client-Anfragen und für administrative Funktionen

verwendet, während das Grid Network für interne Objektmanagement-Operationen vorgesehen ist.



Provisioned

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

System Generated

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

Verwandte Informationen

"Netzwerkkonfiguration des Node ändern"

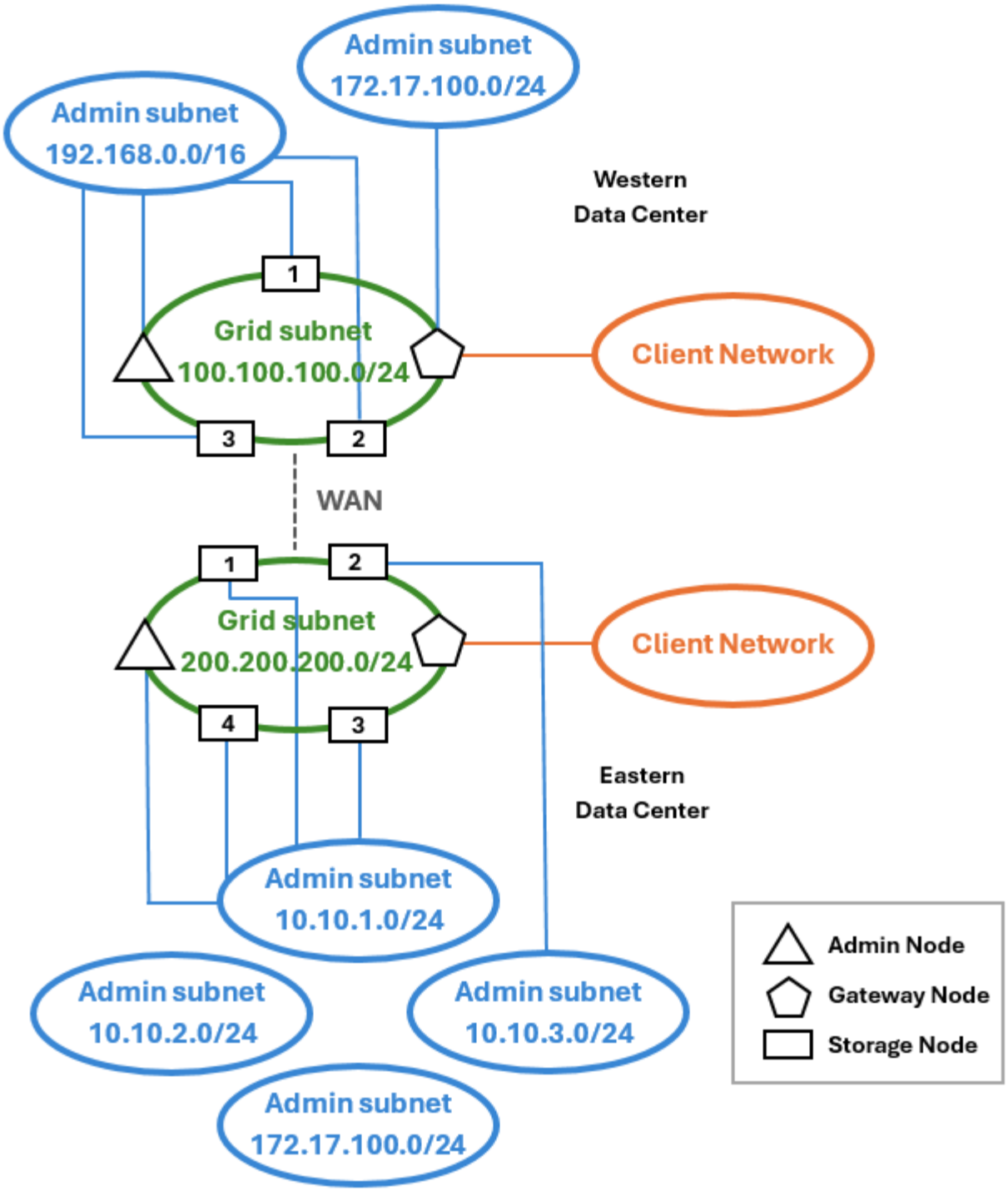
Netzwerktopologie für alle drei StorageGRID Netzwerke

Sie können alle drei Netzwerke zu einer Netzwerktopologie konfigurieren, die aus einem privaten Grid Network, abgegrenzten standortspezifischen Admin Networks und offenen Client Networks besteht. Die Verwendung von Load Balancer Endpunkten und nicht vertrauenswürdigen Client Networks kann bei Bedarf zusätzliche Sicherheit bieten.

In diesem Beispiel:

- Das Grid Network wird für Netzwerkverkehr im Zusammenhang mit internen Objektverwaltungsoperationen verwendet.
- Das Admin Network wird für Datenverkehr im Zusammenhang mit administrativen Funktionen verwendet.
- Das Client-Netzwerk wird für den Datenverkehr im Zusammenhang mit S3-Client-Anfragen verwendet.

Topologiebeispiel: Grid, Admin und Client Netzwerke



Netzwerkanforderungen für StorageGRID

Es ist zu überprüfen, ob die aktuelle Netzwerkinfrastruktur und -konfiguration das geplante StorageGRID Netzwerkdesign unterstützen kann.

Allgemeine Netzwerkanforderungen

Alle StorageGRID Bereitstellungen müssen die folgenden Verbindungen unterstützen können.

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

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

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

Kann StorageGRID keinen der bereitgestellten NTP- oder DNS-Server über die Standard-Routingregeln erreichen, wird automatisch versucht, über alle Netzwerke (Grid, Admin und Client) Kontakt aufzunehmen, sofern die IP-Adressen der DNS- und NTP-Server angegeben sind. Sind die NTP- oder DNS-Server über ein Netzwerk erreichbar, erstellt StorageGRID automatisch zusätzliche Routingregeln, damit dieses Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.

Obwohl Sie diese automatisch ermittelten Hostrouten nutzen können, sollte im Allgemeinen die manuelle Konfiguration der DNS- und NTP-Routen erfolgen, um die Konnektivität sicherzustellen, falls die automatische Ermittlung fehlschlägt.

Wenn Sie die optionalen Admin- und Clientnetzwerke während der Bereitstellung noch nicht konfigurieren möchten, können Sie diese Netzwerke konfigurieren, wenn Sie die Grid-Knoten während der Konfigurationsschritte genehmigen. Zusätzlich können Sie diese Netzwerke nach der Installation mit dem Tool „IP ändern“ konfigurieren (siehe "IP-Adressen konfigurieren").

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

Weitverkehrsnetze (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. Datenreplikation oder Erasure Coding zwischen Standorten, Knoten- oder Standorterweiterung, Knotenwiederherstellung und andere Vorgänge oder Konfigurationen erfordern zusätzliche Bandbreite.

Die tatsächlichen Mindestanforderungen an die WAN-Bandbreite hängen von der Clientaktivität und dem ILM-Schutzschema ab. Für Unterstützung bei der Abschätzung der Mindestanforderungen an die WAN-Bandbreite

steht Ihr NetApp Professional Services Berater zur Verfügung.

Verbindungen für Admin Nodes und Gateway Nodes

Admin Nodes müssen stets vor nicht vertrauenswürdigen Clients, wie zum Beispiel solchen aus dem offenen Internet, geschützt werden. Es muss sichergestellt sein, dass kein nicht vertrauenswürdiger Client auf einen Admin Node im Grid Network, im Admin Network oder im Client Network zugreifen kann.

Admin Nodes und Gateway Nodes, die zu Hochverfügbarkeitsgruppen hinzugefügt werden sollen, müssen mit einer statischen IP-Adresse konfiguriert sein. Weitere Informationen finden sich unter "Hochverfügbarkeitsgruppen verwalten".

Verwendung von Netzwerkadressübersetzung (NAT)

Keine Netzwerkadressübersetzung (NAT) im Grid Network zwischen Grid-Knoten oder zwischen StorageGRID Sites verwenden. Wenn private IPv4-Adressen für das Grid Network verwendet werden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt routbar sein. Falls erforderlich, kann jedoch NAT zwischen externen Clients und Grid-Knoten eingesetzt werden, beispielsweise um einer Gateway Node eine öffentliche IP-Adresse bereitzustellen. Die Verwendung von NAT zur Überbrückung eines öffentliches Netzwerk Segments wird nur unterstützt, wenn eine Tunneling-Anwendung eingesetzt wird, die für alle Knoten im Grid transparent ist, das heißt, die Grid-Knoten benötigen keine Kenntnis öffentlicher IP-Adressen.

Netzwerkspezifische Anforderungen für StorageGRID

Die Anforderungen für jeden StorageGRID Netzwerktyp sind zu beachten.

Netzwerk Gateways und Router

- Falls festgelegt, muss sich das Gateway für ein bestimmtes Netzwerk innerhalb des jeweiligen Subnetzes befinden.
- Wenn Sie eine Schnittstelle mit statischer Adressierung konfigurieren, muss eine andere Gateway-Adresse als 0.0.0.0 angegeben werden.
- Wenn kein Gateway vorhanden ist, gilt es als Best Practice, die Gateway-Adresse auf die IP-Adresse der Netzwerkschnittstelle zu setzen.

Subnetze

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

Die folgenden Einschränkungen werden vom Grid Manager während der Bereitstellung durchgesetzt. Sie sind hier zur Unterstützung der Netzwerkplanung vor der Bereitstellung aufgeführt.

- Die Subnetzmaske für eine Netzwerk-IP-Adresse darf nicht 255.255.255.254 oder 255.255.255.255 (/31 oder /32 in CIDR-Notation) sein.
- Das durch eine Netzwerkschnittstellen-IP-Adresse und Subnetzmaske (CIDR) definierte Subnetz darf sich nicht mit dem Subnetz einer anderen auf demselben Knoten konfigurierten Schnittstelle überschneiden.
- Für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines beliebigen Knotens sollten keine Subnetze verwendet werden, die die folgenden IPv4-Adressen enthalten:
  - 192.168.130.101
  - 192.168.130.121

- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4

  Beispielsweise sollten die folgenden Subnetzbereiche nicht für das Grid Network, das Admin Network oder das Client Network eines beliebigen Knotens verwendet werden:

- 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 Network Subnetz für jeden Knoten muss in die GNSL aufgenommen werden.
- Das Admin Network-Subnetz darf sich nicht mit dem Grid Network-Subnetz, dem Client Network-Subnetz oder einem Subnetz im GNSL überschneiden.
- Die Subnetze im AESL dürfen sich nicht mit Subnetzen im GNSL überschneiden.
- Das Client Network-Subnetz darf sich nicht mit dem Grid Network-Subnetz, dem Admin Network-Subnetz, einem beliebigen Subnetz im GNSL oder einem beliebigen Subnetz im AESL überschneiden.

Grid-Netzwerk

- Zur Implementierungszeit muss jeder Grid-Knoten an das Grid Network angeschlossen sein und mit dem primären Admin Node über die Netzwerkkonfiguration kommunizieren können, die bei der Bereitstellung des Knotens angegeben wird.
- Während des normalen Grid-Betriebs muss jeder Grid-Knoten in der Lage sein, über das Grid-Netzwerk mit allen anderen Grid-Knoten zu kommunizieren.

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

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, werden diese der Grid-Netzwerk-Subnetzliste (GNSL) hinzugefügt. Statische Routen werden auf allen Knoten für jedes Subnetz in der GNSL erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das native Trunk-VLAN dasjenige sein, das für den Grid-Netzwerkdatenverkehr verwendet wird. Alle Grid-Knoten müssen über das native Trunk-VLAN erreichbar sein.

${post_edited_translations.segment}

Das Admin-Netzwerk ist optional. Wenn ein Admin-Netzwerk konfiguriert werden soll, gelten die folgenden Anforderungen und Richtlinien.

Typische Anwendungsfälle des Admin Network sind Management-Verbindungen, AutoSupport, KMS und

Verbindungen zu kritischen Servern wie NTP, DNS und LDAP, sofern diese Verbindungen nicht über das Grid Network oder das Client Network bereitgestellt werden.

> Das Admin Network und AESL können für jeden Node einzigartig sein, solange die gewünschten Netzwerkdienste und Clients erreichbar sind.

> Sie müssen mindestens ein Subnetz im Admin Network definieren, um eingehende Verbindungen von externen Subnetzen zu ermöglichen. Statische Routen werden automatisch auf jedem Node für jedes Subnetz in der AESL generiert.

Client-Netzwerk

Das Clientnetzwerk ist optional. Bei der Konfiguration eines Clientnetzwerks sind die folgenden Punkte zu beachten.

- Das Client Network ist für die Unterstützung des Datenverkehrs von S3-Clients ausgelegt. Wenn konfiguriert, wird das Client Network Gateway zum Standardgateway des Knotens.
- Wenn Sie ein Client Network verwenden, kann StorageGRID vor feindlichen Angriffen geschützt werden, indem eingehender Client-Datenverkehr nur an explizit konfigurierten Load Balancer-Endpunkten akzeptiert wird. Siehe "Load Balancer-Endpunkte konfigurieren".
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, sollte berücksichtigt werden, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn konfiguriert, fließt der Client-Netzwerkdatenverkehr über das im Switch konfigurierte native VLAN des Trunks.

Verwandte Informationen

"Netzwerkkonfiguration des Node ändern"

Bereitstellungsspezifische Netzwerküberlegungen

Netzwerkkonfiguration für StorageGRID Linux-Bereitstellungen

Das StorageGRID System läuft aus Gründen der Effizienz, Zuverlässigkeit und Sicherheit unter Linux als Sammlung von Container-Engines. Eine container-engine-bezogene Netzwerkkonfiguration ist in einem StorageGRID System nicht erforderlich.

Für die Container-Netzwerkschnittstelle sollte ein Gerät ohne Bonding, wie ein VLAN oder ein virtuelles Ethernet-Paar (veth), verwendet werden. Dieses Gerät ist in der Knotenkonfigurationsdatei als Netzwerkschnittstelle anzugeben.

> Bond- oder Bridge-Geräte sollten nicht direkt als Container-Netzwerkschnittstelle verwendet werden. Dies könnte den Start des Knotens aufgrund eines Kernel-Problems bei der Verwendung von macvlan mit Bond- und Bridge-Geräten im Container-Namespace verhindern.

Siehe "Installationsanleitung".

Host-Netzwerkkonfiguration für Container Engine-Bereitstellungen

Vor Beginn der StorageGRID Implementierung auf einer Container-Engine-Plattform ist festzulegen, welche Netzwerke (Grid, Admin, Client) von den einzelnen Knoten verwendet werden. Es ist sicherzustellen, dass die Netzwerkschnittstelle jedes Knotens auf der korrekten 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-Knoten verwenden:

- Alle Hosts sollten für jede Knotenschnittstelle dieselbe Host-Schnittstelle verwenden. Diese Strategie vereinfacht die Host-Konfiguration und ermöglicht zukünftige Knotenmigrationen.
- Eine IP-Adresse für den physischen Host selbst erhalten.

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

- Die erforderlichen Ports zum Host müssen geöffnet werden.
- Wenn VLAN-Schnittstellen in StorageGRID verwendet werden sollen, muss der Host über eine oder mehrere Trunk-Schnittstellen verfügen, die den Zugriff auf die gewünschten VLANs ermöglichen. Diese Schnittstellen können dem Node-Container als eth0, eth2 oder als zusätzliche Schnittstellen zugewiesen werden. Zum Hinzufügen von Trunk- oder Access-Schnittstellen siehe Folgendes:
  - **Linux (vor der Installation des Node)**: "Knotenkonfigurationsdateien erstellen"
  - **Linux (nach der Installation des Nodes)**: "Trunk- oder Zugriffsschnittstellen zu einem Node hinzufügen"

> „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Installation. Eine Liste der unterstützten Versionen befindet sich unter "NetApp Interoperabilitätsmatrix Tool (IMT)".

Empfehlungen zur Mindestbandbreite

Die folgende Tabelle enthält die empfohlenen Mindestbandbreiten für das LAN für jeden StorageGRID-Knotentyp und jeden Netzwerktyp. Jeder physische oder virtuelle Host muss mit ausreichender Netzwerkbandbreite ausgestattet werden, um die aggregierten Mindestbandbreitenanforderungen für die Gesamtzahl und den Typ der StorageGRID-Knoten zu erfüllen, die auf diesem Host betrieben werden sollen.

Knotentyp	**Netzwerktyp**		
	Grid	Administrator	Client
	Minimale LAN Bandbreite	Administrator	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	Archiv	10 Gbit/s

Diese Tabelle enthält keine SAN Bandbreite, die für den Zugriff auf gemeinsam genutzten Speicher erforderlich ist. Bei gemeinsam genutztem Speicher, auf den über Ethernet (iSCSI oder FCoE) zugegriffen wird, sollten auf jedem Host separate physische Schnittstellen bereitgestellt werden, um ausreichende SAN Bandbreite zu gewährleisten. Um einen Engpass zu vermeiden, sollte die SAN Bandbreite eines Hosts in etwa der aggregierten Storage Node Netzwerkbandbreite aller auf diesem Host ausgeführten Storage Nodes entsprechen.

Anhand der Tabelle lässt sich die Mindestanzahl der auf jedem Host bereitzustellenden Netzwerkschnittstellen ermitteln, basierend auf der Anzahl und Art der StorageGRID Knoten, die auf diesem Host ausgeführt werden sollen.

Beispielsweise kann ein Admin Node, ein Gateway Node und ein Storage Node auf einem einzigen Host betrieben werden:

- Das Grid- und das Admin-Netzwerk werden auf dem Admin-Knoten verbunden (erfordert 10 + 1 = 11 Gbit/s)
- Das Grid- und das Client-Netzwerk am Gateway-Knoten verbinden (erfordert 10 + 10 = 20 Gbit/s)
- Das Grid Network am Storage Node verbinden (erfordert 10 Gbit/s)

In diesem Szenario ist eine Mindestbandbreite von 11 + 20 + 10 = 41 Gbit/s an Netzwerkbandbreite bereitzustellen, was durch zwei 40 Gbit/s-Schnittstellen oder fünf 10 Gbit/s-Schnittstellen erfüllt werden könnte, die gegebenenfalls zu Trunks zusammengefasst und dann von den drei oder mehr VLANs gemeinsam genutzt werden, welche die Grid-, Admin- und Client-Subnetze enthalten, die lokal im physischen Rechenzentrum liegen, in dem sich der Host befindet.

Einige empfohlene Methoden zur Konfiguration der physischen und Netzwerkressourcen auf den Hosts Ihres StorageGRID Clusters zur Vorbereitung Ihrer StorageGRID Bereitstellung sind unter "Das Hostnetzwerk konfigurieren" zu finden.

Netzwerk und Ports für Plattformdienste und Cloud Storage Pools

Wenn Sie StorageGRID Plattformdienste oder Cloud Storage Pools verwenden möchten, müssen Grid-Netzwerkfunktionen und Firewalls so konfiguriert werden, dass die Zielendpunkte erreichbar sind.

Vernetzung für Plattformdienste

Wie in "Plattformdienste für Mandanten verwalten" und "Plattformdienste verwalten" beschrieben, umfassen Plattformdienste externe Dienste, die Suchintegration, Ereignisbenachrichtigung und CloudMirror-Replikation bereitstellen.

Plattformdienste benötigen Zugriff von Speicherknoten, die den StorageGRID ADC Service hosten, auf die externen Dienstendpunkte. Beispiele für die Bereitstellung dieses Zugriffs sind:

- Auf den Speicherknoten mit ADC-Diensten werden eindeutige Admin-Netzwerke mit AESL-Einträgen konfiguriert, die zu den Zielendpunkten routen.
- Die vom Clientnetzwerk bereitgestellte Standardroute kann verwendet werden. Bei Nutzung der Standardroute besteht die Möglichkeit, mit "Funktion „Untrusted Client Network“" eingehende Verbindungen einzuschränken.

Netzwerk für Cloud Storage Pools

Cloud Storage Pools erfordern ebenfalls Zugriff von den Storage Nodes auf die von dem verwendeten externen Dienst bereitgestellten Endpunkte, wie etwa Amazon S3 Glacier oder Microsoft Azure Blob storage. Weitere Informationen sind unter "Was ist ein Cloud Storage Pool" zu finden.

Ports für Plattformdienste und Cloud Storage Pools

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

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

Beim Erstellen oder Bearbeiten des Endpunkts kann ein anderer Port angegeben werden. Siehe "Netzwerkport-Referenz".

Wenn Sie einen nicht transparenten Proxyserver verwenden, muss auch "Speicher-Proxy-Einstellungen konfigurieren" zugelassen werden, damit Nachrichten an externe Endpunkte wie einen Endpunkt im Internet gesendet werden können.

VLANs, Plattformdienste und Cloud Storage Pools

VLAN-Netzwerke können nicht für Plattformdienste oder Cloud Storage Pools verwendet werden. Die Zielendpunkte müssen über das Grid, Admin oder Client Network erreichbar sein.

Netzwerkkonfiguration für StorageGRID Appliance-Nodes

Sie können die Netzwerkports auf StorageGRID Appliances so konfigurieren, dass die Port-Bond-Modi verwendet werden, die Ihren Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

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

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

Informationen zu den Port-Bonding-Modi Ihres Geräts:

- "Port-Bond-Modi (SG6160)"
- "Port-Bond-Modi (SGF6112)"
- "Port-Bonding-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 Network sowie die optionalen Admin und Client

Networks während der Knotenbereitstellung und Grid-Konfiguration verwendet werden.

Erstmalige Bereitstellung eines Knotens

Bei der erstmaligen Bereitstellung eines Knotens muss der Knoten mit dem Grid Network verbunden werden, und es muss sichergestellt sein, dass er Zugriff auf den primären Admin Node hat. Wenn das Grid Network isoliert ist, kann das Admin Network auf dem primären Admin Node für Konfigurations- und Installationszugriffe von außerhalb des Grid Network konfiguriert werden.

Ein Grid-Netzwerk mit konfiguriertem Gateway wird während der Bereitstellung zum Standardgateway für einen Knoten. Das Standardgateway ermöglicht Grid-Knoten in separaten Subnetzen die Kommunikation mit dem primären Admin-Knoten, bevor das Grid konfiguriert wurde.

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

Automatische Knotenregistrierung beim primären Admin Node

Nach der Bereitstellung registrieren sich die Knoten über das Grid-Netzwerk beim primären Admin Node. Anschließend kann der Grid Manager, das `configure-storagegrid.py` Python-Skript oder die Installation API verwendet werden, um das Grid zu konfigurieren und die registrierten Knoten zu genehmigen. Während der Grid-Konfiguration können mehrere Grid-Subnetze konfiguriert werden. Statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway werden auf jedem Knoten erstellt, wenn die Grid-Konfiguration abgeschlossen ist.

Deaktivierung des Admin-Netzwerks oder des Client-Netzwerks

Wenn Sie das Admin Network oder das Client Network deaktivieren möchten, kann die Konfiguration während des Knotengenehmigungsprozesses entfernt werden, oder das Change IP Tool kann nach Abschluss der Installation verwendet werden (siehe "IP-Adressen konfigurieren").

Richtlinien nach der Installation für StorageGRID

Nach Abschluss der Bereitstellung und Konfiguration der Grid-Knoten gelten diese Richtlinien für die DHCP-Adressierung und Änderungen der Netzwerkkonfiguration.

- Wenn DHCP zur Zuweisung von IP-Adressen verwendet wurde, sollte für jede IP-Adresse in den verwendeten Netzwerken eine DHCP-Reservierung konfiguriert werden.

  DHCP kann nur während der Bereitstellungsphase eingerichtet werden. DHCP kann während der Konfiguration nicht eingerichtet werden.

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

- Die Verfahren zum Ändern der IP-Adresse sind erforderlich, wenn IP-Adressen, Subnetzmasken und Standardgateways für einen Grid-Knoten geändert werden sollen. Siehe "IP-Adressen konfigurieren".
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin Node und zu anderen Grid-Nodes verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen kann es erforderlich sein, diese Verbindungen erneut herzustellen.

Netzwerkport-Referenz

Interne Grid-Knotenkommunikation für StorageGRID

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

> NetApp empfiehlt, den Internet Control Message Protocol (ICMP)-Datenverkehr zwischen den Grid-Knoten zu aktivieren. Die Zulassung von ICMP-Datenverkehr kann die Failover-Leistung verbessern, wenn ein Grid-Knoten nicht erreichbar ist.

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

Richtlinien für Linux-basierte Knoten

Falls die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können Ports während der Implementierungszeit mithilfe eines Bereitstellungskonfigurationsparameters neu zugeordnet werden. Weitere Informationen zur Portneuzuordnung und zu Bereitstellungskonfigurationsparametern sind unter "StorageGRID auf softwarebasierten Knoten installieren" zu finden.

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf Bare-Metal-Hosts entfernen".

Richtlinien für VMware basierte Knoten

Die folgenden Ports sind nur zu konfigurieren, wenn Firewall-Beschränkungen definiert werden müssen, die außerhalb des VMware-Netzwerks liegen.

Falls die Netzwerkrichtlinien Ihres Unternehmens den Zugriff auf einen dieser Ports einschränken, können Ports bei der Bereitstellung von Knoten mithilfe des VMware vSphere Web Clients oder durch eine Konfigurationsdatei-Einstellung bei der Automatisierung der Grid-Knoten-Bereitstellung neu zugeordnet werden. Weitere Informationen zur Port-Neuzuordnung und zu den Bereitstellungskonfigurationsparametern enthält die Anleitung für "Installation von StorageGRID auf VMware".

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf Bare-Metal-Hosts entfernen".

Richtlinien für Geräteknoten

Falls die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können die Ports mithilfe des StorageGRID Appliance Installers neu zugeordnet werden. Siehe "Optional: Netzwerkports für das Appliance neu zuordnen".

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf StorageGRID Appliances entfernen".

StorageGRID interne Ports

Port	TCP oder UDP	Aus	Zu	Details
22	TCP	Primärer Admin-Knoten	Alle Knoten	Für Wartungsarbeiten muss der primäre Admin-Knoten über SSH auf Port 22 mit allen anderen Knoten kommunizieren können. Das Zulassen von SSH-Datenverkehr von anderen Knoten ist optional.
80	TCP	Appliances	Primärer Admin-Knoten	Wird von StorageGRID Appliances verwendet, um mit dem primären Admin-Node zu kommunizieren und die Installation zu starten.
123	UDP	Alle Knoten	Alle Knoten	Netzwerkzeitprotokolldienst. Jeder Knoten synchronisiert seine Zeit mithilfe von NTP mit jedem anderen Knoten.
443	TCP	Alle Knoten	Primärer Admin-Knoten	Wird verwendet, um den Status während der Installation und anderer Wartungsverfahren an den primären Admin Node zu übermitteln.
1055	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
1139	TCP	Speicherknoten	Speicherknoten	Interner Datenverkehr zwischen Storage Nodes.
1501	TCP	Alle Knoten	Speicherknoten mit ADC	Berichterstattung, Auditierung und Konfiguration des internen Datenverkehrs.
1502	TCP	Alle Knoten	Speicherknoten	S3-bezogener interner Datenverkehr.
1504	TCP	Alle Knoten	Admin-Nodes	NMS-Serviceberichte und Konfiguration des internen Datenverkehrs.
1505	TCP	Alle Knoten	Admin-Nodes	Interner Datenverkehr des AMS Service.
1506	TCP	Alle Knoten	Alle Knoten	Serverstatus interner Datenverkehr.
1507	TCP	Alle Knoten	Gateway-Nodes	Interner Datenverkehr des Load Balancer.
1508	TCP	Alle Knoten	Primärer Admin-Knoten	Konfigurationsmanagement interner Datenverkehr.

Port	TCP oder UDP	Aus	Zu	Details
1511	TCP	Alle Knoten	Speicherknoten	Interner Metadatenverkehr.
5353	UDP	Alle Knoten	Alle Knoten	Bietet den Multicast-DNS-Dienst (mDNS), der für vollständige Grid-IP-Änderungen und für die Ermittlung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
7001	TCP	Speicherknoten	Speicherknoten	Cassandra TLS-Clusterkommunikation zwischen Knoten.
7443	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, sonstige Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Knoten	Geräteknoten	Interner Datenverkehr im Zusammenhang mit dem Wartungsmodusverfahren.
9042	TCP	Speicherknoten	Speicherknoten	Cassandra Client-Port.
9999	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsverfahren, Kennzahlen und Netzwerkaktualisierungen.
10226	TCP	Speicherknoten	Primärer Admin-Knoten	Wird von StorageGRID Appliances für das Weiterleiten von AutoSupport-Paketen vom E-Series SANtricity System Manager an den primären Admin-Node verwendet.
10342	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
18000	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr des Kontodienstes.

Port	TCP oder UDP	Aus	Zu	Details
18001	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr der Identity Federation.
18002	TCP	Admin-/Storage-Nodes	Speicherknoten	Interner API-Datenverkehr im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr der Plattform-Services.
18017	TCP	Admin-/Storage-Nodes	Speicherknoten	Interner Datenverkehr des Data Mover Dienstes für Cloud Storage Pools.
18019	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr des Chunk-Dienstes für Erasure Coding und Replikation
18082	TCP	Admin-/Storage-Nodes	Speicherknoten	S3-bezogener interner Datenverkehr.
18086	TCP	Alle Knoten	Speicherknoten	Interner Datenverkehr im Zusammenhang mit dem LDR Service.
18200	TCP	Admin-/Storage-Nodes	Speicherknoten	Zusätzliche Statistiken zu Client-Anfragen.
19000	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr des Keystone-Dienstes.

Verwandte Informationen

"${post_edited_translations.segment}"

Externe Kommunikation für StorageGRID

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

Eingeschränkter Zugriff auf Ports

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, ist Folgendes

möglich:

- Verwenden Sie "Load Balancer Endpunkte", um den Zugriff auf benutzerdefinierte Ports zu ermöglichen.
- Ports sollten beim Bereitstellen von Knoten neu zugeordnet werden. Load-Balancer-Endpunkte sollten jedoch nicht neu zugeordnet werden. Informationen zur Portneuzuordnung für Ihren StorageGRID Knoten sind verfügbar:

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf StorageGRID Appliances entfernen" oder "Port-Remaps auf Bare-Metal-Hosts entfernen".

- "Port-Remap-Schlüssel für StorageGRID auf Red Hat Enterprise Linux"
- "Ports für StorageGRID auf VMware neu zuordnen"
- "Optional: Netzwerkports für das Appliance neu zuordnen"

Ports für externe Kommunikation

Die folgende Tabelle zeigt die Ports, die für den Datenverkehr in die Knoten verwendet werden.

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

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
22	TCP	SSH	Service Laptop	Alle Knoten	Für Prozeduren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional kann Port 2022 anstelle von 22 verwendet werden. **Hinweis**: Dieser Port ist nur erforderlich, wenn der SSH-Zugriff für bestimmte Wartungsarbeiten aktiviert werden muss.
25	TCP	SMTP	Admin-Nodes	E-Mail Server	Wird für Benachrichtigungen und E-Mail-basierte AutoSupport verwendet. Die Standardporteinstellung von 25 kann auf der Seite „E-Mail-Server“ überschrieben werden.
53	TCP/ UDP	DNS	Alle Knoten	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Knoten	DHCP-Service	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient Dienst wird für statisch konfigurierte Grids nicht ausgeführt.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
68	UDP	DHCP	DHCP-Service	Alle Knoten	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient Dienst wird nicht für Grids ausgeführt, die statische IP-Adressen verwenden.
80	TCP	HTTP	Browser	Admin-Nodes	Port 80 leitet für die Benutzeroberfläche des Admin Node auf Port 443 um.
80	TCP	HTTP	Browser	Appliances	Port 80 wird auf Port 8443 für den StorageGRID Appliance Installer umgeleitet.
80	TCP	HTTP	Speicherknoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTP verwenden. Mandanten können die Standard-HTTP-Port-Einstellung 80 beim Erstellen eines Endpunkts überschreiben.
80	TCP	HTTP	Speicherknoten	AWS	Cloud Storage Pools-Anfragen, die an AWS-Ziele gesendet werden, die HTTP verwenden. Grid-Administratoren können die standardmäßige HTTP-Port-Einstellung 80 beim Konfigurieren eines Cloud Storage Pools überschreiben.
123	UDP	NTP	Primäre NTP Knoten	Externes NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Knoten synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.
161	TCP/ UDP	SNMP	SNMP Client	Alle Knoten	Wird für SNMP-Abfragen verwendet. Alle Knoten liefern grundlegende Informationen; Admin Nodes liefern zusätzlich Warnmeldungen. Standardmäßig wird bei entsprechender Konfiguration UDP-Port 161 verwendet. **Hinweis:** Dieser Port ist nur erforderlich und wird auf der Knotenfirewall nur geöffnet, wenn SNMP konfiguriert ist. Wenn die Verwendung von SNMP vorgesehen ist, können alternative Ports konfiguriert werden. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID sind bei Ihrem NetApp Account Representative erhältlich.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
162	TCP/ UDP	SNMP-Benachrichtigungen	Alle Knoten	Benachrichtigungsziele	Ausgehende SNMP-Benachrichtigungen und Traps verwenden standardmäßig den UDP-Port 162. **Hinweis:** Dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn die Verwendung von SNMP vorgesehen ist, können alternative Ports konfiguriert werden. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID sind bei Ihrem NetApp Account Representative erhältlich.
389	TCP/ UDP	LDAP	Speicherknoten mit ADC	Active Directory/LDAP	Wird für die Verbindung mit einem Active Directory oder LDAP-Server für die Identitätsföderation 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 der Liste der privilegierten Adressen hinzugefügt. Siehe "Firewall-Steuerung konfigurieren" zur Konfiguration privilegierter IP-Adressen.
443	TCP	HTTPS	Admin-Nodes	Active Directory	Wird von Administratorknoten verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist.
443	TCP	HTTPS	Speicherknoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTPS verwenden. Mandanten können die Standardeinstellung für den HTTP-Port 443 beim Erstellen eines Endpunkts überschreiben.
443	TCP	HTTPS	Speicherknoten	AWS	Cloud Storage Pools-Anfragen, die an AWS-Ziele gesendet werden, die HTTPS verwenden. Grid-Administratoren können die standardmäßige HTTPS-Porteinstellung 443 beim Konfigurieren eines Cloud Storage Pools überschreiben.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
5353	UDP	mDNS	Alle Knoten	Alle Knoten	Bietet den Multicast-DNS-Dienst (mDNS), der für vollständige Grid-IP-Änderungen und für die Ermittlung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
5696	TCP	KMIP	Appliance	KMS	Key Management Interoperability Protocol (KMIP) externer Datenverkehr von Appliances, die für die Knotenverschlüsselung konfiguriert sind, zum Key Management Server (KMS), es sei denn, auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer ist ein anderer Port angegeben.
8443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann zur Trennung der Grid Manager und Tenant Manager Kommunikation verwendet werden. **Hinweis**: Wenn die Grid Manager-Ports 443 oder 8443 geschlossen werden, 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 der Liste der privilegierten Adressen hinzugefügt. Siehe "Firewall-Steuerung konfigurieren" zur Konfiguration privilegierter IP-Adressen.
8443	TCP	HTTPS	Browser	Appliances	Wird von Webbrowsern und Management-API-Clients verwendet, um auf den StorageGRID Appliance Installer zuzugreifen. **Hinweis**: Port 443 wird auf Port 8443 für den StorageGRID Appliance Installer umgeleitet.
9022	TCP	SSH	Service Laptop	Appliances	Gewährt Zugriff auf StorageGRID Appliances im Vorkonfigurationsmodus für Support- und Fehlerbehebung. Dieser Port muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
9091	TCP	HTTPS	Externer Grafana Dienst	Admin-Nodes	Wird von externen Grafana-Diensten für den sicheren Zugriff auf den StorageGRID Prometheus-Dienst verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist.
9092	TCP	Kafka	Speicherknoten mit ADC	Kafka Cluster	Wird für Plattformdienstnachrichten verwendet, die an einen Kafka-Cluster gesendet werden. Mandanten können die Standardeinstellung für den Kafka-Port 9092 beim Erstellen eines Endpunkts überschreiben.
9443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Grid Manager und Tenant Manager Kommunikation zu trennen.
18082	TCP	HTTPS	S3 Clients	Speicherknoten	S3-Client-Datenverkehr direkt zu Storage Nodes (HTTPS).
18084	TCP	HTTP	S3 Clients	Speicherknoten	S3-Client-Datenverkehr direkt zu Speicherknoten (HTTP).
23000-23999	TCP	HTTPS	Alle Knoten im Quellgrid für die gridübergreifende Replikation	Admin Nodes und Gateway Nodes im Ziel-Grid für die gridübergreifende Replikation	Dieser Portbereich ist für Grid-Federation-Verbindungen reserviert. Beide Grids einer Verbindung nutzen denselben Port.

Schnellstart für StorageGRID

Diese allgemeinen Schritte dienen zur Konfiguration und Nutzung eines beliebigen StorageGRID Systems.

Lernen, planen und Daten sammeln

Mit Ihrem NetApp Account Representative lassen sich die Optionen verstehen und die Planung Ihres neuen StorageGRID Systems vornehmen. Folgende Arten von Fragen sind zu berücksichtigen:

- Wie viele Objektdaten werden voraussichtlich anfänglich und im Laufe der Zeit gespeichert?
- Wie viele Standorte benötigen Sie?
- Wie viele und welche Arten von Knoten werden an jedem Standort benötigt?
- Welche StorageGRID Netzwerke werden verwendet?
- Wer wird Ihr Grid zur Speicherung von Objekten nutzen? Welche Anwendungen werden sie verwenden?
- Haben Sie besondere Sicherheits- oder Speicheranforderungen?
- Müssen Sie gesetzliche oder behördliche Anforderungen erfüllen?

Optional kann mit dem NetApp Professional Services Consultant zusammengearbeitet werden, um mit dem NetApp ConfigBuilder Tool eine Konfigurationsarbeitsmappe für die Installation und Bereitstellung des neuen Systems zu erstellen. Dieses Tool kann auch zur Automatisierung der Konfiguration beliebiger StorageGRID Appliances verwendet werden. Siehe "Automatisierung der Geräteinstallation und Konfiguration".

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

Knoten installieren

Ein StorageGRID System besteht aus einzelnen hardwarebasierten und softwarebasierten Knoten. Zunächst wird die Hardware für jeden Appliance-Knoten installiert und jeder Linux- oder VMware-Host konfiguriert.

Zur Vervollständigung der Installation wird die StorageGRID Software auf jedem Appliance- oder Software-Host installiert und die Knoten werden zu einem Grid verbunden. In diesem Schritt werden Standort- und Knotennamen, Subnetzdetails sowie die IP-Adressen für die NTP- und DNS-Server angegeben.

Informationen dazu, wie:

- "Gerätehardware installieren"
- "StorageGRID auf softwarebasierten Knoten installieren"

Anmelden und Systemzustand prüfen

Nach Abschluss der Grid-Installation können Sie sich beim Grid Manager anmelden. Von dort aus lässt sich der allgemeine Zustand Ihres neuen Systems überprüfen, AutoSupport und Benachrichtigungs-E-Mails aktivieren sowie S3-Endpunkt-Domänennamen einrichten.

Informationen dazu, wie:

- "Anmeldung beim Grid Manager"
- "Systemzustand überwachen"
- "Konfiguration von AutoSupport"
- "E-Mail-Benachrichtigungen für Warnmeldungen einrichten"
- "S3-Endpunkt-Domänennamen konfigurieren"

Konfiguration und Verwaltung

Die Konfigurationsaufgaben, die Sie für ein neues StorageGRID System durchführen müssen, hängen davon ab, wie Sie Ihr Grid nutzen. Mindestens werden der Systemzugriff eingerichtet, die FabricPool und S3

Assistenten verwendet und verschiedene Speicher- sowie Sicherheitseinstellungen verwaltet.

Informationen dazu, wie:

- "${post_edited_translations.segment}"
- "S3-Einrichtungsassistent verwenden"
- "Den FabricPool Einrichtungsassistenten verwenden"
- "Sicherheit verwalten"
- "Systemhärtung"

ILM einrichten

Sie steuern die Platzierung und Speicherdauer jedes Objekts in Ihrem StorageGRID System durch die Konfiguration einer Information Lifecycle Management (ILM) Richtlinie, die aus einer oder mehreren ILM-Regeln besteht. Die ILM-Regeln geben StorageGRID Anweisungen, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien im Laufe der Zeit verwaltet werden.

Informationen dazu, wie:"Objekte mit ILM verwalten"

StorageGRID verwenden

Nach Abschluss der Erstkonfiguration können StorageGRID-Mandantenkonten S3-Clientanwendungen verwenden, um Objekte aufzunehmen, abzurufen und zu löschen.

Informationen dazu, wie:

- "Ein Mandantenkonto verwenden"_
- "Die S3 REST API verwenden"

Überwachung und Fehlerbehebung

Sobald Ihr System eingerichtet und betriebsbereit ist, empfiehlt sich eine regelmäßige Überwachung der Aktivitäten sowie das Beheben von Warnmeldungen. Es besteht außerdem die Möglichkeit, einen externen Syslog Server zu konfigurieren, SNMP Monitoring zu nutzen oder zusätzliche Daten zu erfassen.

Informationen dazu, wie:

- "StorageGRID überwachen"
- "Fehlerbehebung StorageGRID"

Erweitern, warten und wiederherstellen

Sie können Knoten oder Standorte hinzufügen, um die Kapazität oder Funktionalität Ihres Systems zu erweitern. Es besteht außerdem die Möglichkeit, verschiedene Wartungsarbeiten durchzuführen, um Ausfälle zu beheben oder das StorageGRID System auf dem neuesten Stand zu halten und eine effiziente Leistung sicherzustellen.

Informationen dazu, wie:

- "Ein Grid erweitern"
- "Verwalten Sie Ihr Grid"
- "Knoten wiederherstellen"