Erste Schritte

StorageGRID software

NetApp
November 04, 2025

Inhalt

Erste Schritte mit einem StorageGRID -System

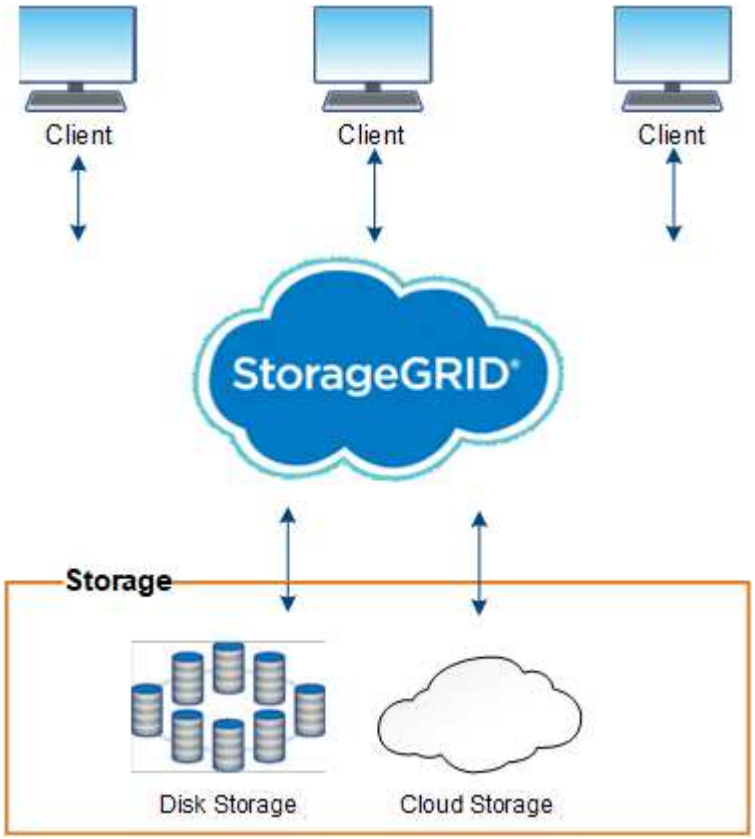
Erfahren Sie mehr über StorageGRID

Was ist StorageGRID?

NetApp® StorageGRID® ist eine softwaredefinierte Objektspeichersuite, die eine breite Palette von Anwendungsfällen in öffentlichen, privaten und hybriden Multicloud-Umgebungen unterstützt. StorageGRID bietet native Unterstützung für die Amazon S3-API und liefert branchenführende Innovationen wie automatisiertes Lebenszyklusmanagement, um unstrukturierte Daten über lange Zeiträume kostengünstig zu speichern, zu sichern, zu schützen und aufzubewahren.

StorageGRID bietet sicheren, dauerhaften Speicher für unstrukturierte Daten in großem Umfang. Integrierte, metadatengesteuerte Richtlinien zur Lebenszyklusverwaltung optimieren den Verbleib Ihrer Daten während ihrer gesamten Lebensdauer. Um die Kosten zu senken, werden Inhalte zur richtigen Zeit am richtigen Ort und auf der richtigen Speicherebene platziert.

StorageGRID besteht aus geografisch verteilten, redundanten, heterogenen Knoten, die sowohl in bestehende als auch in Clientanwendungen 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 ersetzt durch"ILM Cloud-Speicherpools" , die mehr Funktionalität bieten.

Vorteile von StorageGRID

Zu den Vorteilen des StorageGRID -Systems gehören:

- Ein massiv skalierbares und benutzerfreundliches, geografisch verteiltes Daten-Repository für unstrukturierte Daten.
- Standardprotokolle für die Objektspeicherung:
  - Amazon Web Services Simple Storage Service (S3)
  - OpenStack Swift

> Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.

- Hybrid Cloud aktiviert. Das richtlinienbasierte Information Lifecycle Management (ILM) speichert Objekte in öffentlichen Clouds, darunter Amazon Web Services (AWS) und Microsoft Azure. Die Dienste der StorageGRID -Plattform ermöglichen die Inhaltsreplikation, Ereignisbenachrichtigung und Metadatensuche von in öffentlichen Clouds gespeicherten Objekten.
- Flexibler Datenschutz zur Gewährleistung von Langlebigkeit und Verfügbarkeit. Daten können durch Replikation und mehrschichtige Löschcodierung geschützt werden. Die Überprüfung ruhender und übertragener Daten gewährleistet die Integrität für die langfristige Speicherung.
- Dynamisches Datenlebenszyklusmanagement zur Unterstützung der Verwaltung der Speicherkosten. Sie können ILM-Regeln erstellen, die den Datenlebenszyklus auf Objektebene verwalten und dabei Datenlokalität, Haltbarkeit, Leistung, Kosten und Aufbewahrungszeit anpassen.
- Hohe Verfügbarkeit der Datenspeicherung und einiger Verwaltungsfunktionen mit integriertem Lastenausgleich zur Optimierung der Datenlast über StorageGRID -Ressourcen hinweg.
- Unterstützung für mehrere Speichermandantenkonten, um die auf Ihrem System nach verschiedenen Entitäten gespeicherten Objekte zu trennen.
- Zahlreiche Tools zur Überwachung des Zustands Ihres StorageGRID -Systems, darunter ein umfassendes Warnsystem, ein grafisches Dashboard und detaillierte Statusinformationen für alle Knoten und Sites.
- Unterstützung für software- oder hardwarebasierte Bereitstellung. Sie können StorageGRID auf einem der folgenden Geräte bereitstellen:
  - Virtuelle Maschinen, die in VMware ausgeführt werden.
  - Container-Engines auf Linux-Hosts.
  - Von StorageGRID entwickelte Geräte.
    - Speichergeräte bieten Objektspeicher.
    - Service-Appliances bieten Netzverwaltungs- und Lastausgleichsdienste.
- Konform mit den relevanten Aufbewahrungsanforderungen dieser Verordnung:
  - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), die Börsenmitglieder, Makler oder Händler reguliert.
  - Regel 4511(c) der Financial Industry Regulatory Authority (FINRA), die sich den Format- und Medienanforderungen der SEC-Regel 17a-4(f) unterwirft.
  - Commodity Futures Trading Commission (CFTC) in Verordnung 17 CFR § 1.31(c)-(d), die den Handel mit Rohstoff-Futures regelt.
- Unterbrechungsfreie Upgrade- und Wartungsvorgänge. Behalten Sie den Zugriff auf Inhalte während Upgrade-, Erweiterungs-, Außerbetriebnahme- und Wartungsverfahren bei.

- Föderiertes Identitätsmanagement. Integriert sich zur Benutzerauthentifizierung in Active Directory, OpenLDAP oder Oracle Directory Service. 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

Verwenden Sie StorageGRID in einer Hybrid-Cloud-Konfiguration, indem Sie ein richtliniengesteuertes Datenmanagement implementieren, um Objekte in Cloud-Speicherpools zu speichern, StorageGRID -Plattformdienste nutzen und Daten mit NetApp FabricPool von ONTAP auf StorageGRID verschieben.

Cloud-Speicherpools

Mit Cloud-Speicherpools können Sie Objekte außerhalb des StorageGRID -Systems speichern. Beispielsweise möchten Sie möglicherweise selten aufgerufene Objekte in einen kostengünstigeren Cloud-Speicher verschieben, etwa Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archivzugriffsebene im Microsoft Azure Blob-Speicher. Oder Sie möchten möglicherweise ein Cloud-Backup von StorageGRID -Objekten verwalten, mit dem Sie Daten wiederherstellen können, die aufgrund eines Speichervolumes- oder Speicherknotenausfalls verloren gegangen sind.

Auch Speicher von Drittanbietern wird unterstützt, darunter Festplatten- und Bandspeicher.

> 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 Ihnen die Möglichkeit, Remotedienste als Endpunkte für die Objektreplikation, Ereignisbenachrichtigungen oder Suchintegration zu verwenden. Plattformdienste arbeiten unabhängig von den ILM-Regeln des Grids und sind für einzelne S3-Buckets aktiviert. Folgende Dienste werden unterstützt:

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

Sie können beispielsweise die CloudMirror-Replikation verwenden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und dann AWS-Dienste nutzen, um Analysen Ihrer Daten durchzuführen.

ONTAP -Daten-Tiering mit FabricPool

Sie können die Kosten für ONTAP -Speicher senken, indem Sie Daten mithilfe von FabricPool auf StorageGRID auslagern. FabricPool ermöglicht die automatische Zuordnung von Daten zu kostengünstigen Objektspeicherebenen, entweder vor Ort oder außerhalb.

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

Ähnliche Informationen

- "Was ist ein Cloud-Speicherpool?"
- "Plattformdienste verwalten"
- "Konfigurieren von StorageGRID für FabricPool"

StorageGRID -Architektur und Netzwerktopologie

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

Siehe die"Beschreibungen der Rasterknotentypen" .

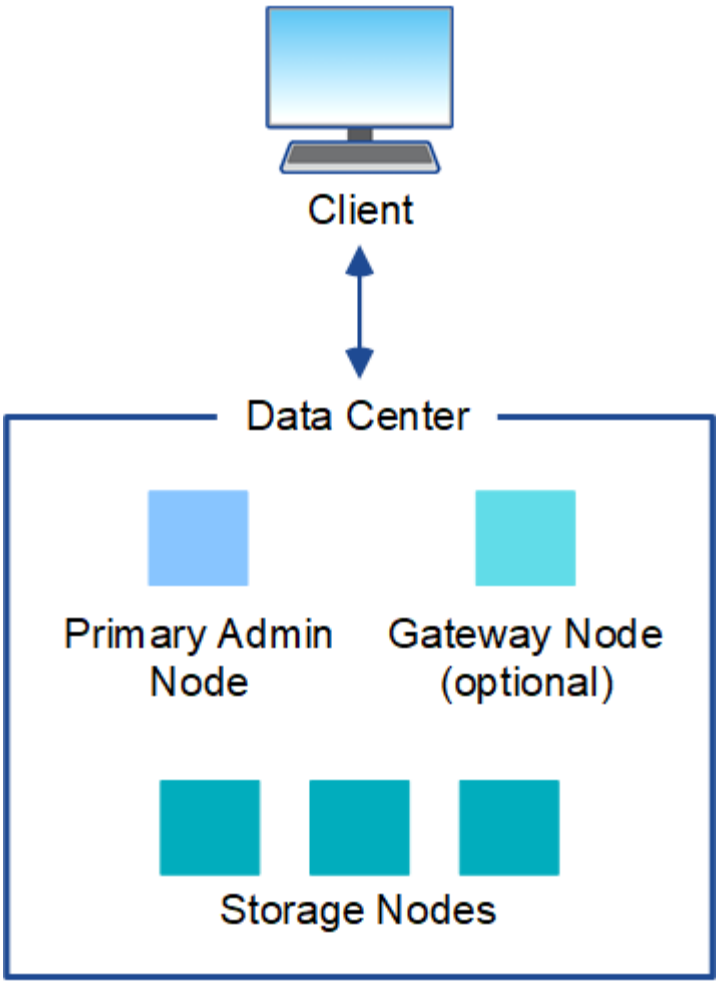
Weitere Informationen zur StorageGRID -Netzwerktopologie, den Anforderungen und der Grid-Kommunikation finden Sie im"Netzwerkrichtlinien" .

Bereitstellungstopologien

Das StorageGRID -System kann an einem einzelnen oder an mehreren Rechenzentrumsstandorten bereitgestellt werden.

Einzelne Site

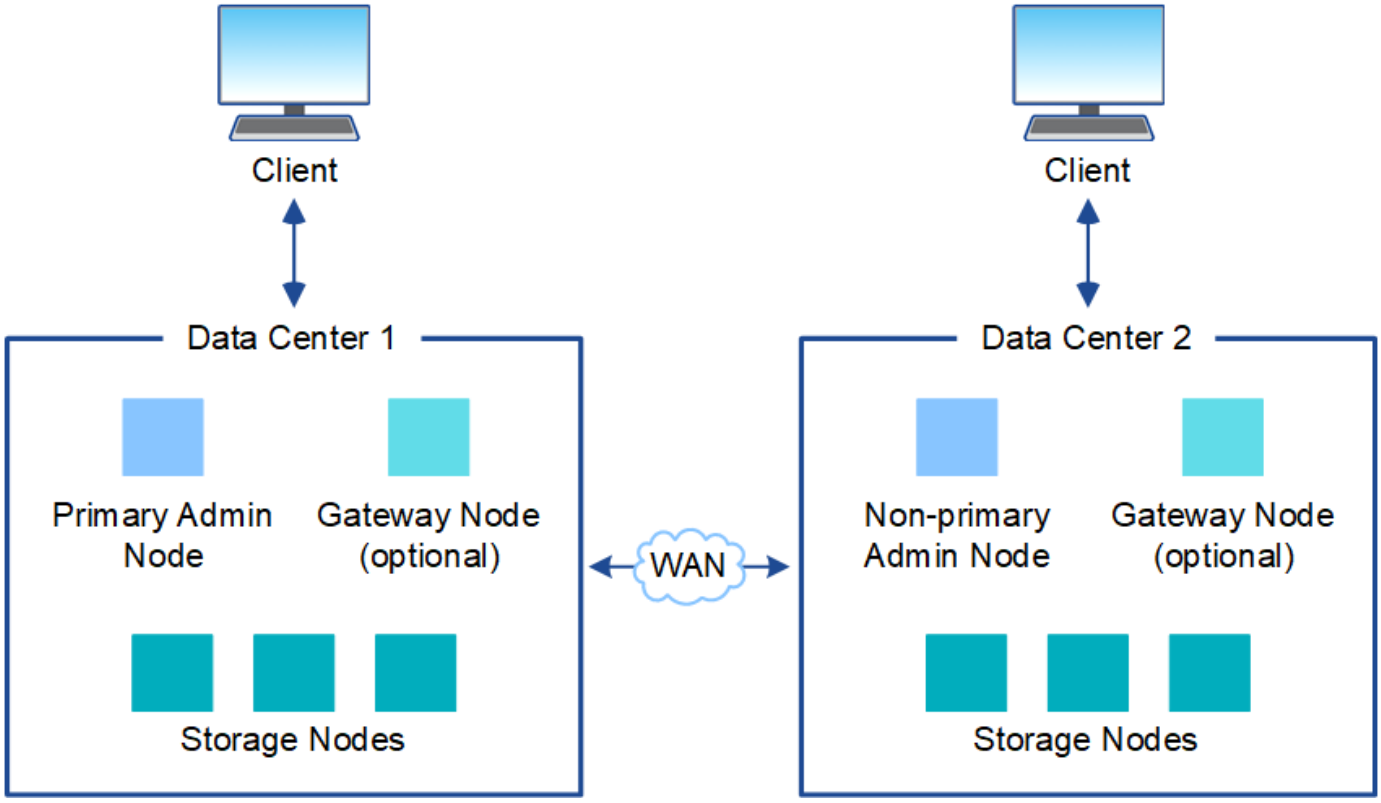
Bei einer Bereitstellung mit einem einzelnen Standort sind die Infrastruktur und der Betrieb des StorageGRID -Systems zentralisiert.



Mehrere Standorte

Bei einer Bereitstellung mit mehreren Standorten können an jedem Standort unterschiedliche Typen und Anzahlen von StorageGRID -Ressourcen installiert werden. Beispielsweise kann in einem Rechenzentrum mehr Speicherplatz erforderlich sein als in einem anderen.

Verschiedene Standorte liegen oft an geografisch unterschiedlichen Orten in unterschiedlichen Störungsbereichen, beispielsweise an einer Erdbebenverwerfungslinie oder in einem Überschwemmungsgebiet. Datenfreigabe und Notfallwiederherstellung werden durch die automatisierte Verteilung der Daten an andere Standorte erreicht.



Innerhalb eines einzigen Rechenzentrums können auch mehrere logische Standorte vorhanden sein, um die Verwendung von verteilter Replikation und Erasure Coding zur Erhöhung der Verfügbarkeit und Ausfallsicherheit zu ermöglichen.

Netzknotenredundanz

Bei einer Bereitstellung an einem oder mehreren Standorten können Sie aus Redundanzgründen optional mehr als einen Admin-Knoten oder Gateway-Knoten einschließen. Sie können beispielsweise mehr als einen Admin-Knoten an einem einzelnen Standort oder an mehreren Standorten installieren. Allerdings kann jedes StorageGRID -System nur einen primären Admin-Knoten haben.

Systemarchitektur

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

S3-Clients speichern und rufen Objekte in StorageGRID ab. Andere Clients werden zum Senden von E-Mail-Benachrichtigungen, zum Zugriff auf die StorageGRID -Verwaltungsschnittstelle und optional zum Zugriff auf die Audit-Freigabe verwendet.

S3-Clients können eine Verbindung zu einem Gateway-Knoten oder einem Admin-Knoten herstellen, um die Lastausgleichsschnittstelle zu Speicherknoten zu verwenden. Alternativ können S3-Clients über HTTPS eine direkte Verbindung zu Speicherknoten herstellen.

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

Netzknoten und Dienste

Netzknoten und Dienste

Der grundlegende Baustein eines StorageGRID -Systems ist der Grid-Knoten. Knoten enthalten Dienste, bei denen es sich um Softwaremodule handelt, die einem Grid-Knoten eine Reihe von Funktionen bereitstellen.

Arten von Gitterknoten

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

Admin-Knoten

Bereitstellung von Verwaltungsdiensten wie Systemkonfiguration, Überwachung und Protokollierung. Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Jedes Grid muss über einen primären Admin-Knoten verfügen und kann zur Redundanz über zusätzliche nicht-primäre Admin-Knoten verfügen. Sie können eine Verbindung zu jedem Admin-Knoten herstellen und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID Systems an. Wartungsverfahren müssen jedoch mithilfe des primären Admin-Knotens durchgeführt werden.

Admin-Knoten können auch zum Lastenausgleich des S3-Client-Verkehrs verwendet werden.

Sehen"Was ist ein Admin-Knoten?"

Speicherknoten

Verwalten und speichern Sie Objektdaten und Metadaten. Jeder Standort in Ihrem StorageGRID -System muss über mindestens drei Speicherknoten verfügen.

Sehen"Was ist ein Speicherknoten?"

Gateway-Knoten (optional)

Stellen Sie eine Lastausgleichsschnittstelle bereit, die Clientanwendungen zum Herstellen einer Verbindung mit StorageGRID verwenden können. Ein Load Balancer leitet Clients nahtlos zu einem optimalen Speicherknoten weiter, sodass der Ausfall von Knoten oder sogar einer ganzen Site transparent ist.

Sehen"Was ist ein Gateway-Knoten?"

Hardware- und Softwareknoten

StorageGRID Knoten können als StorageGRID Appliance-Knoten oder als softwarebasierte Knoten bereitgestellt werden.

StorageGRID -Geräteknoten

StorageGRID Hardwaregeräte sind speziell für die Verwendung in einem StorageGRID -System konzipiert. Einige Geräte können als Speicherknoten verwendet werden. Andere Appliances können als Admin-Knoten oder Gateway-Knoten verwendet werden. Sie können Appliance-Knoten mit softwarebasierten Knoten kombinieren oder vollständig entwickelte Grids mit ausschließlich Appliances bereitstellen, die nicht von externen Hypervisoren, Speichern oder Computerhardware abhängig sind.

Im Folgenden finden Sie Informationen zu den verfügbaren Geräten:

- "StorageGRID Appliance-Dokumentation"

- "NetApp Hardware Universe"

Softwarebasierte Knoten

Softwarebasierte Grid-Knoten können als virtuelle VMware-Maschinen oder innerhalb von Container-Engines auf einem Linux-Host bereitgestellt werden.

- Virtuelle Maschine (VM) in VMware vSphere: Siehe"Installieren Sie StorageGRID auf VMware" .
- Innerhalb einer Container-Engine auf Red Hat Enterprise Linux: Siehe"Installieren Sie StorageGRID unter Red Hat Enterprise Linux" .
- Innerhalb einer Container-Engine auf Ubuntu oder Debian: Siehe"Installieren Sie StorageGRID unter Ubuntu oder Debian" .

Verwenden Sie die "NetApp Interoperability Matrix Tool (IMT)" um die unterstützten Versionen zu ermitteln.

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

StorageGRID Dienste

Nachfolgend finden Sie eine vollständige Liste der StorageGRID -Dienste.

Service	Beschreibung	Standort
Kontodienst-Weiterleitung	Stellt eine Schnittstelle für den Load Balancer-Dienst bereit, um den Account-Dienst auf Remote-Hosts abzufragen, und sendet Benachrichtigungen über Konfigurationsänderungen des Load Balancer-Endpunkts an den Load Balancer-Dienst.	Load Balancer-Dienst auf Admin-Knoten und Gateway-Knoten
ADC (Administrativer Domänencontroller)	Verwaltet Topologieinformationen, stellt Authentifizierungsdienste bereit und antwortet auf Anfragen der LDR- und CMN-Dienste.	Mindestens drei Speicherknoten, die den ADC-Dienst an jedem Standort enthalten
AMS (Audit-Management-System)	Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textprotokolldatei.	Admin-Knoten
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch.	Speicherknoten
Chunk-Dienst	Verwaltet erasure-coded Daten und Paritätsfragmente.	Speicherknoten
CMN (Konfigurationsverwaltungsknoten)	Verwaltet systemweite Konfigurationen und Grid-Aufgaben. Jedes Grid verfügt über einen CMN-Dienst.	Primärer Admin-Knoten

Service	Beschreibung	Standort
DDS (Verteilter Datenspeicher)	Schnittstellen mit der Cassandra-Datenbank zur Verwaltung von Objektmetadaten.	Speicherknoten
DMV (Datenverschieber)	Verschiebt Daten zu Cloud-Endpunkten.	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-Knoten
Hohe Verfügbarkeit	Verwaltet hochverfügbare virtuelle IPs auf Knoten, die auf der Seite „Hochverfügbarkeitsgruppen“ konfiguriert sind. Dieser Dienst wird auch als Keepalived-Dienst bezeichnet.	Admin- und Gateway-Knoten
Identität (idnt)	Föderiert Benutzeridentitäten aus LDAP und Active Directory.	Speicherknoten, die den ADC-Dienst verwenden
Lambda-Schiedsrichter	Verwaltet S3 Select SelectObjectContent-Anfragen.	Alle Knoten
Lastenausgleich (nginx-gw)	Bietet Lastausgleich des S3-Verkehrs von Clients zu Speicherknoten. Der Load Balancer-Dienst kann über die Konfigurationsseite „Load Balancer-Endpunkte“ konfiguriert werden. Dieser Dienst ist auch als nginx-gw-Dienst bekannt.	Admin- und Gateway-Knoten
LDR (Lokaler Verteilungsrouter)	Verwaltet die Speicherung und Übertragung von Inhalten innerhalb des Grids.	Speicherknoten
MISCd Information Service Control Daemon	Bietet eine Schnittstelle zum Abfragen und Verwalten von Diensten auf anderen Knoten und zum Verwalten von Umgebungskonfigurationen auf dem Knoten, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Knoten
nginx	Fungiert als Authentifizierungs- 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

Service	Beschreibung	Standort
nginx-gw	Unterstützt den Load Balancer-Dienst.	Admin- und Gateway-Knoten
NMS (Netzwerkmanagementsystem)	Unterstützt die Überwachungs-, Berichts- und Konfigurationsoptionen, die über den Grid Manager angezeigt werden.	Admin-Knoten
Persistenz	Verwaltet Dateien auf der Root-Festplatte, die nach einem Neustart erhalten bleiben müssen.	Alle Knoten
Prometheus	Sammelt Zeitreihenmetriken von Diensten auf allen Knoten.	Admin-Knoten
RSM (Replizierte Zustandsmaschine)	Stellt sicher, dass Plattformdienstanfragen an die jeweiligen Endpunkte gesendet werden.	Speicherknoten, die den ADC-Dienst verwenden
SSM (Server Status Monitor)	Überwacht den Zustand der Hardware und meldet ihn an den NMS-Dienst.	Auf jedem Grid-Knoten ist eine Instanz vorhanden
Spurensammler	Führt eine Ablaufverfolgung durch, um Informationen für den technischen Support zu sammeln. Der Trace-Collector-Dienst verwendet die Open-Source-Software von Jaeger.	Admin-Knoten

Was ist ein Admin-Knoten?

Admin-Knoten bieten Verwaltungsdienste wie Systemkonfiguration, Überwachung und Protokollierung. Admin-Knoten können auch zum Lastenausgleich des S3-Client-Verkehrs verwendet werden. Jedes Grid muss über einen primären Admin-Knoten verfügen und kann aus Redundanzgründen eine beliebige Anzahl nicht-primärer Admin-Knoten haben.

Unterschiede zwischen primären und nicht-primären Admin-Knoten

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

Die Tabelle fasst die Funktionen primärer und nicht primärer Admin-Knoten zusammen.

Funktionen	Primärer Admin-Knoten	Nicht-primärer Admin-Knoten
Beinhaltet dieAMS Service	Ja	Ja

Funktionen	Primärer Admin-Knoten	Nicht-primärer Admin-Knoten
Beinhaltet dieCMN Service	Ja	Nein
Beinhaltet dieNMS Service	Ja	Ja
Beinhaltet diePrometheus Service	Ja	Ja
Beinhaltet dieSSM Service	Ja	Ja
Beinhaltet dieLastenausgleich UndHohe Verfügbarkeit Dienstleistungen	Ja	Ja
Unterstützt dieManagement-Anwendungsprogrammschnittstelle (MGMT-API)	Ja	Ja
Kann für alle netzwerkbezogenen Wartungsaufgaben verwendet werden, beispielsweise IP-Adressänderung und Aktualisierung von NTP-Servern	Ja	Nein
Kann nach der Erweiterung des Speicherknotens eine EC-Neuverteilung durchführen	Ja	Nein
Kann für die Volumenwiederherstellung verwendet werden	Ja	Ja
Kann Protokolldateien und Systemdaten von einem oder mehreren Knoten sammeln	Ja	Nein
Sendet Warnmeldungen, AutoSupport -Pakete und SNMP-Traps und informiert	Ja. Fungiert alsbevorzugter Absender .	Ja. Fungiert als Standby-Sender.

Admin-Knoten des bevorzugten Absenders

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

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

In diesen Fällen können mehrere Benachrichtigungen gesendet werden:

- Wenn Admin-Knoten voneinander isoliert werden, versuchen sowohl der bevorzugte Absender als auch die Standby-Absender, Benachrichtigungen zu senden, und es können mehrere Kopien der Benachrichtigungen empfangen werden.
- Wenn der Standby-Absender Probleme mit dem bevorzugten Absender erkennt und mit dem Senden von

Benachrichtigungen beginnt, kann der bevorzugte Absender möglicherweise seine Fähigkeit zum Senden von Benachrichtigungen wiedererlangen. In diesem Fall werden möglicherweise doppelte Benachrichtigungen gesendet. Der Standby-Absender stellt das Senden von Benachrichtigungen ein, wenn er beim bevorzugten Absender keine Fehler mehr erkennt.

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

Primäre Dienste für Admin-Knoten

Die folgende Tabelle zeigt die primären Dienste für Admin-Knoten. Allerdings sind in dieser Tabelle nicht alle Knotendienste aufgeführt.

Service	Tastenfunktion
Audit Management System (AMS)	Verfolgt Systemaktivitäten und Ereignisse.
Konfigurationsverwaltungsknoten (CMN)	Verwaltet die systemweite Konfiguration.
Hohe Verfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Knoten und Gateway-Knoten. **Hinweis:** Dieser Dienst ist auch auf Gateway-Knoten verfügbar.
Lastenausgleich	Bietet Lastausgleich des S3-Verkehrs von Clients zu Speicherknoten. **Hinweis:** Dieser Dienst ist auch auf Gateway-Knoten verfügbar.
Management-Anwendungsprogrammschnittstelle (mgmt-api)	Verarbeitet Anfragen von der Grid Management API und der Tenant Management API.
Netzwerkmanagementsystem (NMS)	Bietet Funktionen 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 Speicherknoten?

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 der Festplatte erforderlich sind.

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

Arten von Speicherknoten

Während der Installation können Sie den Typ des Speicherknotens auswählen, den Sie installieren möchten. Diese Typen sind für softwarebasierte Speicherknoten und für gerätebasierte Speicherknoten verfügbar, die die Funktion unterstützen:

- Kombinierter Daten- und Metadaten-Speicherknoten
- Nur-Metadaten-Speicherknoten
- Nur-Daten-Speicherknoten

Sie können den Speicherknotentyp in folgenden Situationen auswählen:

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

> ⓘ Sie können den Typ nicht mehr ändern, nachdem die Installation des Speicherknotens abgeschlossen ist.

Daten- und Metadaten-Speicherknoten (kombiniert)

Standardmäßig speichern alle neuen Speicherknoten sowohl Objektdaten als auch Metadaten. Dieser Speicherknotentyp wird als *kombinierter* Speicherknoten bezeichnet.

Nur-Metadaten-Speicherknoten

Die Verwendung eines Speicherknotens ausschließlich für Metadaten kann sinnvoll sein, wenn Ihr Grid eine sehr große Anzahl kleiner Objekte speichert. Durch die Installation dedizierter Metadatenkapazität wird ein besseres Gleichgewicht zwischen dem für eine sehr große Anzahl kleiner Objekte benötigten Speicherplatz und dem für die Metadaten dieser Objekte benötigten Speicherplatz erreicht. Darüber hinaus können reine Metadaten-Speicherknoten, die auf Hochleistungsgeräten gehostet werden, die Leistung steigern.

Für reine Metadaten-Speicherknoten gelten bestimmte Hardwareanforderungen:

- Bei Verwendung von StorageGRID -Geräten können reine Metadatenknoten nur auf SGF6112-Geräten mit zwölf 1,9-TB- oder zwölf 3,8-TB-Laufwerken konfiguriert werden.
- Bei der Verwendung softwarebasierter Knoten müssen die Knotenressourcen, die nur Metadaten enthalten, mit den vorhandenen Speicherknotenressourcen übereinstimmen. Beispiel:
  - Wenn die vorhandene StorageGRID Site SG6000- oder SG6100-Geräte verwendet, müssen die softwarebasierten Nur-Metadaten-Knoten die folgenden Mindestanforderungen erfüllen:
    - 128 GB RAM
    - 8-Kern-CPU
    - 8 TB SSD oder gleichwertiger Speicher für die Cassandra-Datenbank (rangedb/0)
  - Wenn die vorhandene StorageGRID Site virtuelle Speicherknoten mit 24 GB RAM, 8-Kern-CPU und 3 TB oder 4 TB Metadatenspeicher verwendet, sollten die softwarebasierten Nur-Metadaten-Knoten ähnliche Ressourcen verwenden (24 GB RAM, 8-Kern-CPU und 4 TB Metadatenspeicher (rangedb/0).
- Beim Hinzufügen einer neuen StorageGRID Site sollte die Gesamtmetadatenkapazität der neuen Site mindestens der vorhandenen StorageGRID Sites entsprechen und die neuen Site-Ressourcen sollten den Speicherknoten an vorhandenen StorageGRID Sites entsprechen.

Bei der Installation von reinen Metadatenknoten muss das Grid auch eine Mindestanzahl von Knoten zur

Datenspeicherung enthalten:

- Konfigurieren Sie für ein Single-Site-Grid mindestens zwei kombinierte oder reine Datenspeicherknoten.
- Konfigurieren Sie für ein Grid mit mehreren Standorten mindestens einen kombinierten oder Nur-Daten-Speicherknoten *pro Standort*.

> Obwohl reine Metadaten-Speicherknoten dieLDR-Dienst und S3-Clientanforderungen verarbeiten kann, wird die StorageGRID Leistung möglicherweise nicht gesteigert.

Nur-Daten-Speicherknoten

Die Verwendung eines Speicherknotens ausschließlich für Daten kann sinnvoll sein, wenn Ihre Speicherknoten unterschiedliche Leistungsmerkmale aufweisen. Um die Leistung potenziell zu steigern, könnten Sie beispielsweise ausschließlich Daten speichernde, hochleistungsfähige rotierende Festplatten-Speicherknoten zusammen mit ausschließlich Metadaten speichernden Hochleistungs-Speicherknoten einsetzen.

Beim Installieren von Nur-Daten-Knoten muss das Raster Folgendes enthalten:

- Mindestens zwei kombinierte oder reine Datenspeicherknoten *pro Raster*
- Mindestens ein kombinierter oder reiner Datenspeicherknoten *pro Site*
- Mindestens drei kombinierte oder reine Metadaten-Speicherknoten *pro Site*

Primäre Dienste für Speicherknoten

Die folgende Tabelle zeigt die primären Dienste für Speicherknoten. Allerdings sind in dieser Tabelle nicht alle Knotendienste aufgeführt.

> Einige Dienste, wie etwa der ADC-Dienst und der RSM-Dienst, sind normalerweise nur auf drei Speicherknoten an jedem Standort vorhanden.

Service	Tastenfunktion
Konto (acct)	Verwaltet Mieterkonten.

Service	Tastenfunktion
Administrativer Domänencontroller (ADC)	Behält die Topologie und die netzweite Konfiguration bei. **Hinweis**: Reine Datenspeicherknoten hosten den ADC-Dienst nicht. **Details** Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen untereinander. Der ADC-Dienst wird auf mindestens drei Speicherknoten an einem Standort gehostet. Der ADC-Dienst verwaltet Topologieinformationen, einschließlich des Standorts und der 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 besten Grid-Knoten zur Verarbeitung seiner Anfrage zu finden. Darüber hinaus behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID -Bereitstellung bei, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann. Um verteilte und isolierte Vorgänge zu ermöglichen, synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen zu Diensten und Topologie mit den anderen ADC-Diensten im StorageGRID System. Im Allgemeinen halten alle Grid-Knoten eine Verbindung zu mindestens einem ADC-Dienst aufrecht. Dadurch wird sichergestellt, dass die Grid-Knoten immer 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 weiter funktionieren, wenn ein ADC-Dienst nicht verfügbar ist. Neue Grid-Knoten können Verbindungen nur mithilfe eines ADC-Dienstes herstellen. Durch die Verbindung jedes Grid-Knotens kann der ADC-Dienst Topologieinformationen sammeln. Zu diesen Grid-Knoteninformationen gehören die CPU-Auslastung, der verfügbare Speicherplatz (sofern vorhanden), unterstützte Dienste und die Site-ID des Grid-Knotens. Andere Dienste fragen den ADC-Dienst über Topologieabfragen nach Topologieinformationen. Der ADC-Dienst antwortet auf jede Abfrage mit den neuesten Informationen, die er vom StorageGRID -System erhält.
Kassandra	Speichert und schützt Objektmetadaten. **Hinweis**: Reine Datenspeicherknoten hosten den Cassandra-Dienst nicht.
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch. **Hinweis**: Reine Datenspeicherknoten hosten den Cassandra Reaper-Dienst nicht.
Brocken	Verwaltet erasure-coded Daten und Paritätsfragmente.

Service	Tastenfunktion
Datenverschieber (dmv)	Verschiebt Daten in Cloud-Speicherpools.
Verteilter Datenspeicher (DDS)	Überwacht die Speicherung von Objektmetadaten. **Details** Jeder Speicherknoten umfasst den Distributed Data Store (DDS)-Dienst. Dieser Dienst interagiert mit der Cassandra-Datenbank, um Hintergrundaufgaben an den im StorageGRID System gespeicherten Objektmetadaten auszuführen. Der DDS-Dienst verfolgt die Gesamtzahl der in das StorageGRID System aufgenommenen Objekte sowie die Gesamtzahl der über jede der unterstützten Schnittstellen des Systems aufgenommenen Objekte (S3).
Identität (idnt)	Föderiert Benutzeridentitäten aus LDAP und Active Directory.

Service	Tastenfunktion
Lokaler Verteilungsrouter (LDR)	Verarbeitet Objektspeicherprotokollanforderungen und verwaltet Objektdaten auf der Festplatte.

Service	Tastenfunktion
Replizierte Zustandsmaschine (RSM)	Stellt sicher, dass Anfragen zu S3-Plattformdiensten an die jeweiligen Endpunkte gesendet werden.
Serverstatusmonitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein Gateway-Knoten?

Gateway-Knoten bieten eine dedizierte Lastausgleichsschnittstelle, die S3-Clientanwendungen zum Herstellen einer Verbindung mit StorageGRID verwenden können. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität maximiert, indem die Arbeitslast auf mehrere Speicherknoten verteilt wird. Gateway-Knoten sind optional.

Der StorageGRID Load Balancer-Dienst wird auf allen Admin-Knoten und allen Gateway-Knoten bereitgestellt. Es führt die Transport Layer Security (TLS)-Terminierung von Clientanforderungen durch, überprüft die Anforderungen und stellt neue sichere Verbindungen zu den Speicherknoten her. Der Load Balancer-Dienst leitet Clients nahtlos zu einem optimalen Speicherknoten weiter, sodass der Ausfall von Knoten oder sogar einer ganzen Site transparent ist.

Sie konfigurieren einen oder mehrere Load Balancer-Endpunkte, um den Port und das Netzwerkprotokoll (HTTPS oder HTTP) zu definieren, die eingehende und ausgehende Clientanforderungen für den Zugriff auf die Load Balancer-Dienste auf Gateway- und Admin-Knoten verwenden. Der Load Balancer-Endpunkt definiert außerdem den Clienttyp (S3), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten. Sehen "Überlegungen zum Lastenausgleich"

Bei Bedarf können Sie die Netzwerkschnittstellen mehrerer Gateway-Knoten und Admin-Knoten in einer Hochverfügbarkeitsgruppe (HA) zusammenfassen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast der Client-Anwendung verwalten. Sehen "Verwalten von Hochverfügbarkeitsgruppen (HA)"

Primäre Dienste für Gateway-Knoten

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

Service	Tastenfunktion
Hohe Verfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Knoten und Gateway-Knoten. **Hinweis:** Dieser Dienst ist auch auf Admin-Knoten zu finden.
Lastenausgleich	Bietet Layer-7-Lastausgleich des S3-Verkehrs von Clients zu Speicherknoten. Dies ist der empfohlene Lastausgleichsmechanismus. **Hinweis:** Dieser Dienst ist auch auf Admin-Knoten zu finden.

Grösstell der harten Arbeit des StorageGRID Systems, indem er Datenübertragungslasten und Datenverkehrsfunktionen handhabt.

Der LDR-Dienst übernimmt folgende Aufgaben:

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

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

Objektspeicher

Der zugrunde liegende Datenspeicher eines LDR-Dienstes ist in eine feste Anzahl von Objektspeichern (auch als Speichervolumes bezeichnet) unterteilt. Jeder Objektspeicher ist ein separater Einhängepunkt.

Die Objektspeicher in einem Speicherknoten werden durch eine Hexadezimalzahl von 0000 bis 002F identifiziert, die als Volume-ID bezeichnet wird. Im ersten Objektspeicher (Volume 0) ist Speicherplatz 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, darunter replizierte Kopien und löschcodierte

die mit dem LDR-Dienst 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 wird automatisch durchgeführt. Weitere Informationen finden Sie unter "Verwalten des

Service	Tastenfunktion
Serverstatusmonitor (SSM)	Überwacht das Betriebssystem und die zugrunde liegende Hardware.

Was ist ein Archivknoten?

Die Unterstützung für Archivknoten wurde entfernt.

Informationen zu Archivknoten finden Sie unter "Was ist ein Archivknoten (StorageGRID 11.8-Dokumentationsseite)" .

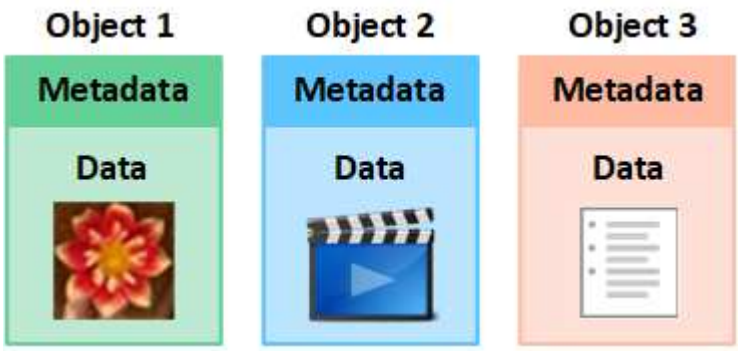
So verwaltet StorageGRID Daten

Was ist ein Objekt

Bei der Objektspeicherung ist die Speichereinheit ein Objekt und keine Datei oder ein Block. Im Gegensatz zur baumartigen Hierarchie eines Dateisystems oder Blockspeichers organisiert der Objektspeicher Daten in einem flachen, unstrukturierten Layout.

Durch die Objektspeicherung wird der physische Speicherort der Daten von der Methode entkoppelt, 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, beispielsweise 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 gesamten Grid zu verfolgen und den Lebenszyklus jedes Objekts im Laufe der Zeit zu verwalten.

Zu den Objektmetadaten gehören beispielsweise die folgenden Informationen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des Namens des S3-Buckets oder Swift-Containers, des Mandantenkontonamens oder der 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-Coded-Fragments.
- Alle mit dem Objekt verknüpften Benutzermetadaten.

Objektmetadaten sind anpassbar und erweiterbar, sodass sie für Anwendungen flexibel nutzbar sind.

Ausführliche Informationen dazu, wie und wo StorageGRID Objektmetadaten speichert, finden Sie unter"Verwalten des Objektmetadatenspeichers" .

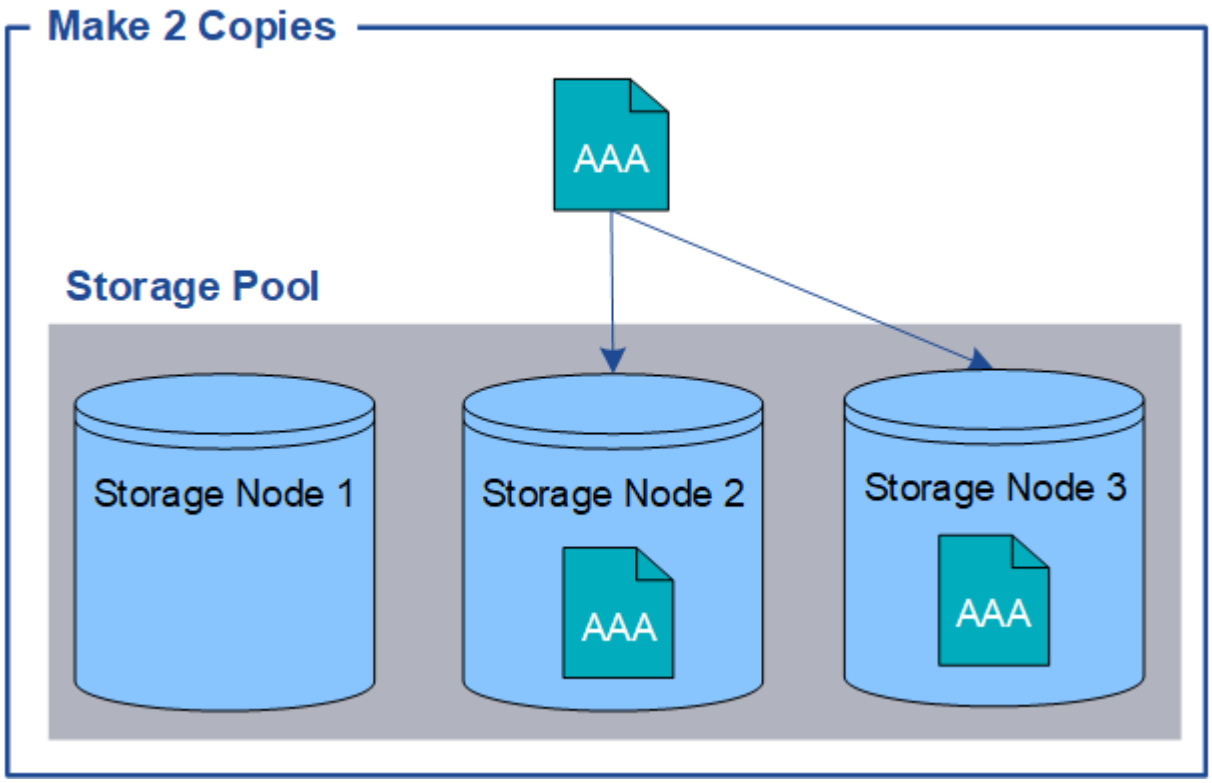
Wie werden Objektdaten geschützt?

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

Replikation

Wenn StorageGRID Objekte einer ILM-Regel (Information Lifecycle Management) zuordnet, die für die Erstellung replizierter Kopien konfiguriert ist, erstellt das System exakte Kopien der Objektdaten und speichert sie auf Speicherknoten oder Cloud-Speicherpools. ILM-Regeln bestimmen die Anzahl der erstellten Kopien, den Speicherort dieser Kopien und die Dauer ihrer Aufbewahrung durch das System. Wenn eine Kopie verloren geht, beispielsweise durch den Verlust eines Speicherknotens, ist das Objekt weiterhin verfügbar, wenn an anderer Stelle im StorageGRID -System eine Kopie davon vorhanden ist.

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

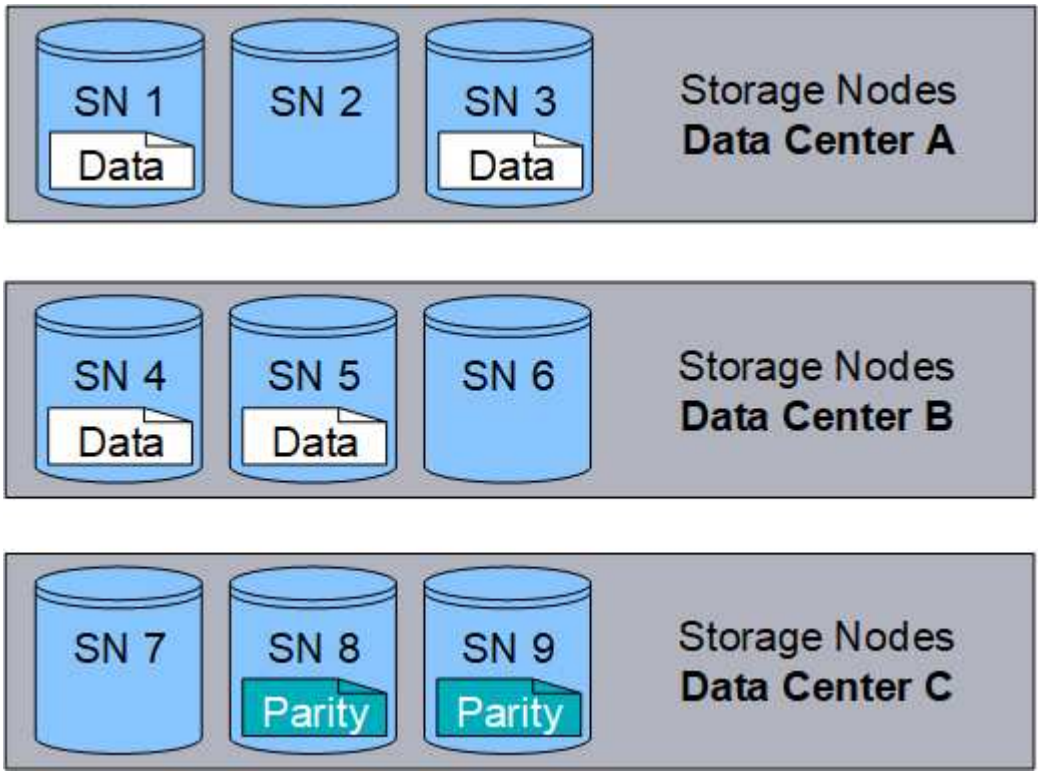


Löschcodierung

Wenn StorageGRID Objekte einer ILM-Regel zuordnet, die zum Erstellen von Erasure-Coded-Kopien konfiguriert ist, zerlegt es die Objektdaten in Datenfragmente, berechnet zusätzliche Paritätsfragmente und

speichert jedes Fragment auf einem anderen Speicherknoten. Beim Zugriff auf ein Objekt wird es anhand der gespeicherten Fragmente wieder zusammengesetzt. Wenn Daten oder ein Paritätsfragment beschädigt werden oder verloren gehen, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten und Paritätsfragmente wiederherstellen. ILM-Regeln und Erasure-Coding-Profile bestimmen das verwendete Erasure-Coding-Schema.

Das folgende Beispiel veranschaulicht die Verwendung 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 gleiche Datenfragmente aufgeteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Speicherknoten in drei Rechenzentren gespeichert, um Datenschutz bei Knotenausfällen oder Standortverlusten zu gewährleisten.



Ähnliche Informationen

- "Objekte mit ILM verwalten"
- "Nutzen Sie Information Lifecycle Management"

Das Leben eines Objekts

Das Leben eines Objekts besteht aus verschiedenen Phasen. Jede Phase stellt die Vorgänge dar, die mit dem Objekt durchgeführt werden.

Zum Lebenszyklus eines Objekts gehören die Vorgänge Aufnahme, Kopierverwaltung, Abrufen und Löschen.

- **Ingest**: Der Prozess einer S3-Clientanwendung, die 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 löschcodierter Kopien in StorageGRID, wie in den ILM-Regeln in den aktiven ILM-Richtlinien beschrieben. Während der Kopierverwaltungsphase schützt StorageGRID Objektdaten vor Verlust, indem es die angegebene Anzahl und Art von Objektkopien auf Speicherknoten oder in einem Cloud-Speicherpool erstellt und verwaltet.

- **Abrufen**: Der Prozess einer Client-Anwendung, die auf ein vom StorageGRID -System gespeichertes Objekt zugreift. Der Client liest das Objekt, das von einem Speicherknoten oder Cloud-Speicherpool abgerufen wird.
- **Löschen**: Der Vorgang zum Entfernen aller Objektkopien aus dem Raster. Objekte können entweder gelöscht werden, indem die Clientanwendung eine Löschanforderung an das StorageGRID -System sendet, oder als Ergebnis eines automatischen Prozesses, den StorageGRID ausführt, wenn die Lebensdauer des Objekts abläuft.

Ähnliche Informationen

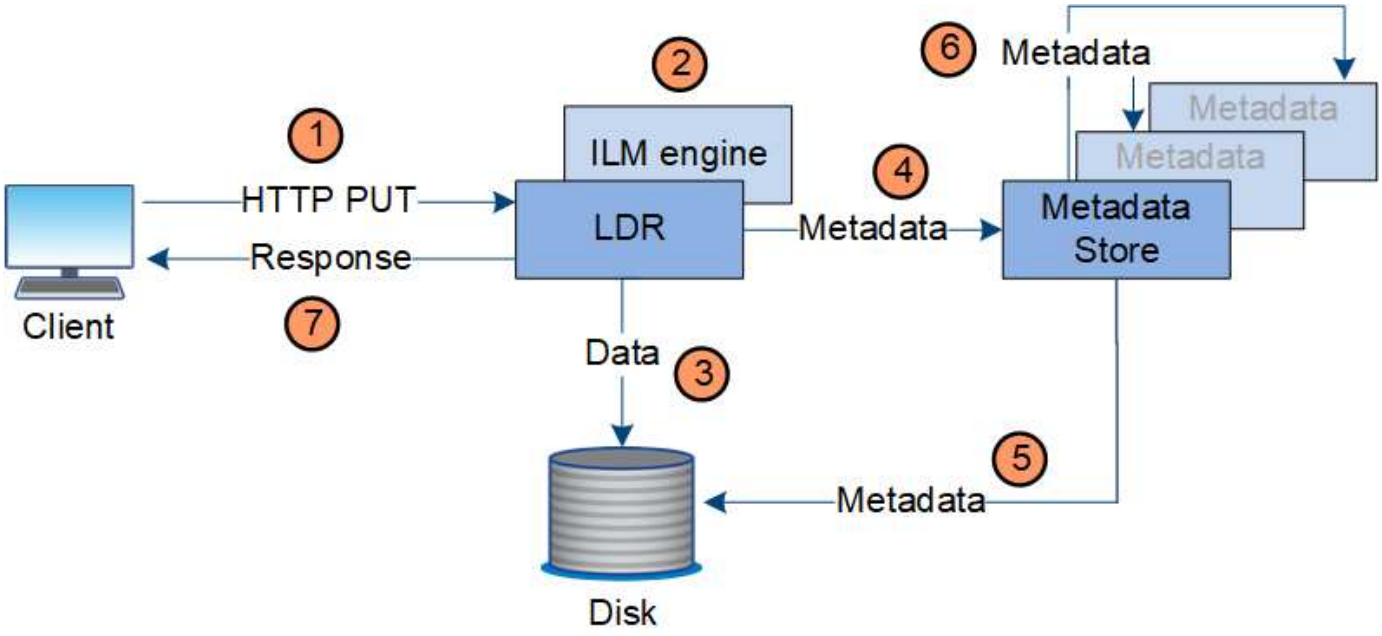
- "Objekte mit ILM verwalten"
- "Nutzen Sie Information Lifecycle Management"

Datenfluss erfassen

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

Datenfluss

Wenn ein Client ein Objekt in das StorageGRID -System einspeist, verarbeitet der LDR-Dienst auf den Speicherknoten die Anforderung 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 ausgewertet.
3. Der LDR-Dienst speichert die Objektdaten als replizierte Kopie oder als Erasure-Coded-Kopie. (Das Diagramm zeigt eine vereinfachte Version 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 überträgt Kopien von Objektmetadaten an andere Speicherknoten. Diese Kopien

werden auch auf der Festplatte gespeichert.

7. Der LDR-Dienst gibt eine HTTP 200 OK-Antwort an den Client zurück, um zu bestätigen, dass das Objekt aufgenommen wurde.

Kopierverwaltung

Objektdaten werden durch die aktiven ILM-Richtlinien und zugehörigen ILM-Regeln verwaltet. ILM-Regeln erstellen replizierte oder löschcodierte Kopien, um Objektdaten vor Verlust zu schützen.

Zu unterschiedlichen Zeitpunkten im Lebenszyklus eines Objekts können unterschiedliche Typen oder Speicherorte von Objektkopien erforderlich sein. ILM-Regeln werden regelmäßig ausgewertet, um sicherzustellen, dass Objekte wie erforderlich platziert werden.

Die Objektdaten werden vom LDR-Dienst verwaltet.

Inhaltsschutz: Replikation

Wenn die Anweisungen zur Inhaltsplatzierung einer ILM-Regel replizierte Kopien von Objektdaten erfordern, werden Kopien erstellt und von den Speicherknoten, aus denen der konfigurierte Speicherpool besteht, auf der Festplatte gespeichert.

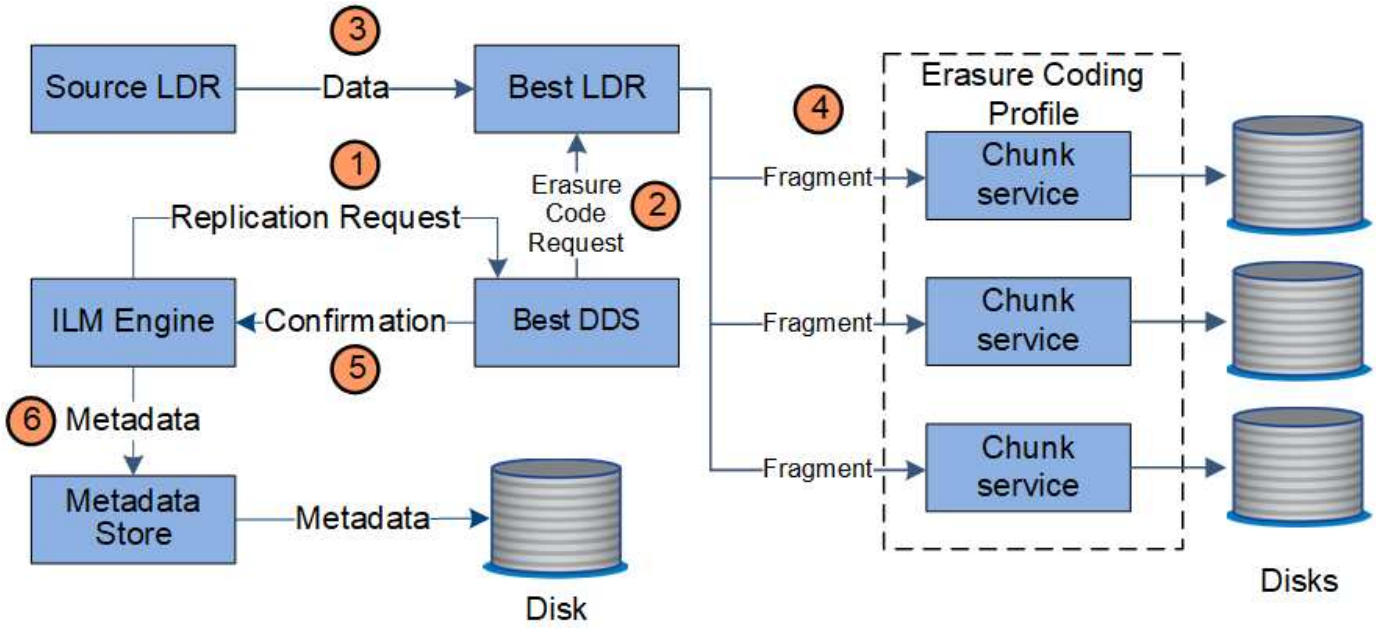
Die ILM-Engine im LDR-Dienst steuert die Replikation und stellt sicher, dass die richtige Anzahl von Kopien an den richtigen Orten und für die richtige Zeit gespeichert wird.

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

Inhaltsschutz: Erasure Coding

Wenn eine ILM-Regel Anweisungen zum Erstellen von Erasure-Coding-Kopien von Objektdaten enthält, zerlegt das entsprechende Erasure-Coding-Schema die Objektdaten in Daten- und Paritätsfragmente und verteilt diese Fragmente auf die im Erasure-Coding-Profil konfigurierten Speicherknoten.

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

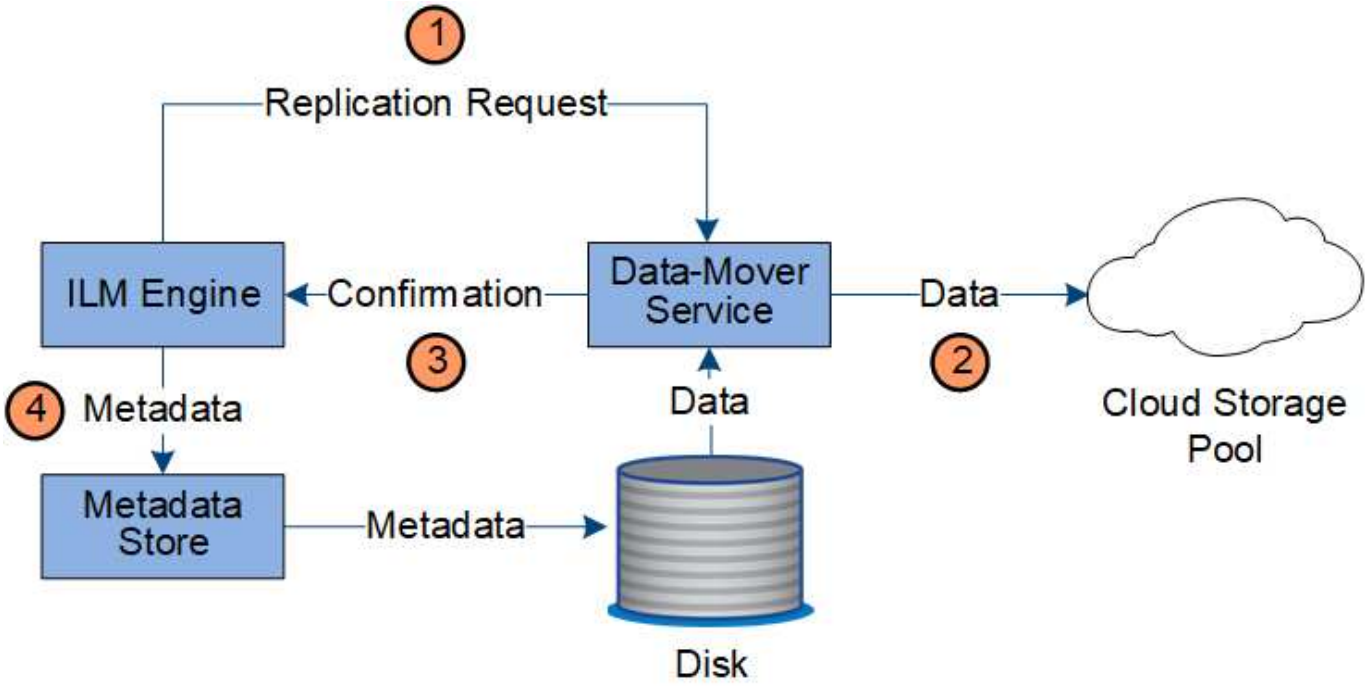


1. Die ILM-Engine fragt den ADC-Dienst ab, um zu ermitteln, welcher DDS-Dienst den Erasure-Coding-Vorgang am besten durchführen kann. Wenn dies festgestellt wird, sendet die ILM-Engine eine „Initialisierungs“-Anforderung an diesen Dienst.
2. Der DDS-Dienst weist einen LDR an, die Objektdaten mit einem Löschcode zu versehen.
3. Der Quell-LDR-Dienst sendet eine Kopie an den für die Erasure Coding ausgewählten LDR-Dienst.
4. Nachdem die entsprechende Anzahl an Paritäts- und Datenfragmenten erstellt wurde, verteilt der LDR-Dienst diese Fragmente auf die Speicherknoten (Chunk-Dienste), die den Speicherpool des Erasure-Coding-Profils bilden.
5. Der LDR-Dienst benachrichtigt die ILM-Engine und bestätigt, dass die Objektdaten erfolgreich verteilt wurden.
6. Die ILM-Engine aktualisiert den Metadatenspeicher mit Objektstandortmetadaten.

Inhaltsschutz: Cloud-Speicherpool

Wenn die Anweisungen zur Inhaltsplatzierung einer ILM-Regel erfordern, dass eine replizierte Kopie der Objektdaten in einem Cloud-Speicherpool gespeichert wird, werden die Objektdaten in den externen S3-Bucket oder Azure Blob-Speichercontainer dupliziert, der für den Cloud-Speicherpool angegeben wurde.

Die ILM-Engine, die eine Komponente des LDR-Dienstes ist, und der Data Mover-Dienst steuern die Bewegung von Objekten in den Cloud Storage Pool.



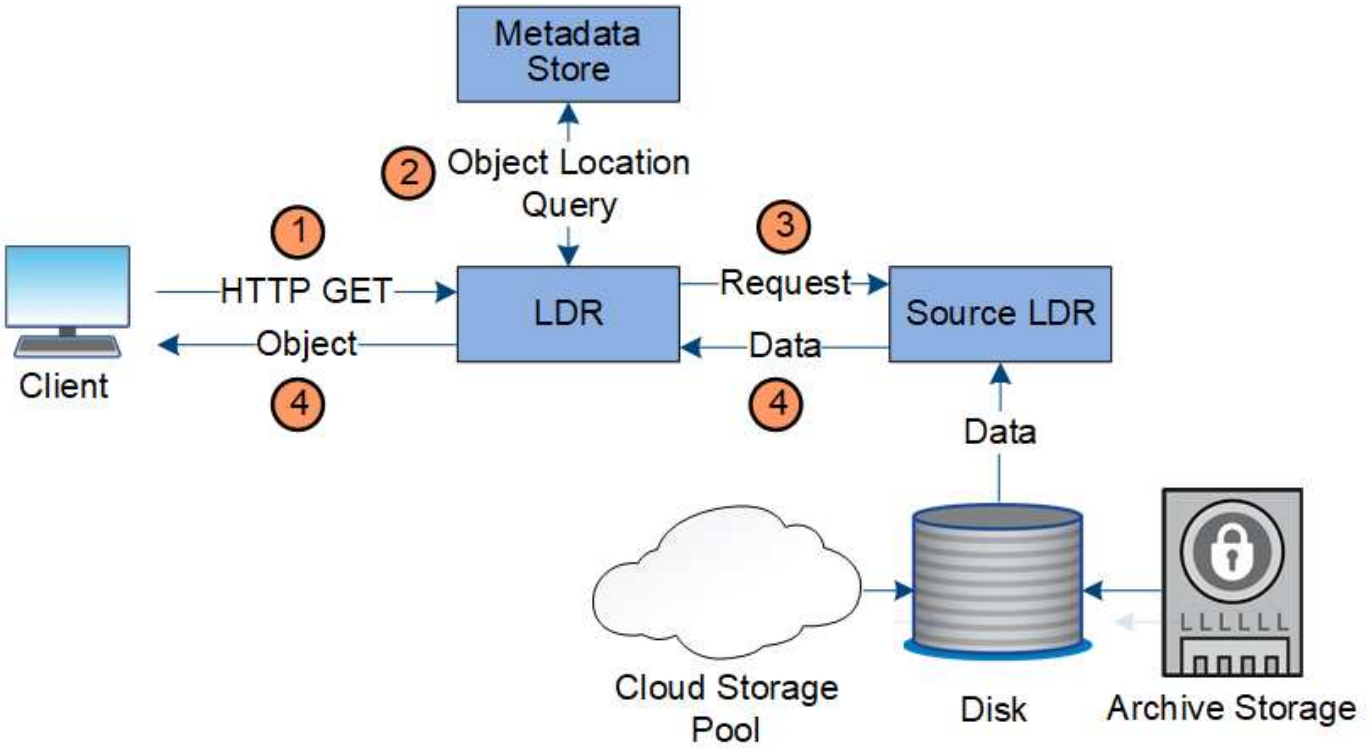
1. Die ILM-Engine wählt einen Data Mover-Dienst zur Replikation in den Cloud Storage Pool aus.
2. Der Data Mover-Dienst sendet die Objektdaten an den Cloud Storage Pool.
3. Der Data Mover-Dienst benachrichtigt die ILM-Engine, dass die Objektdaten gespeichert wurden.
4. Die ILM-Engine aktualisiert den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

Datenfluss abrufen

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 Speicherknoten oder, falls erforderlich, einem Cloud-Speicherpool zu verfolgen.

Der LDR-Dienst des Speicherknotens fragt den Metadatenspeicher nach dem Speicherort der Objektdaten ab und ruft sie vom Quell-LDR-Dienst ab. Der Abruf erfolgt vorzugsweise von einem Speicherknoten. Wenn das Objekt auf einem Speicherknoten nicht verfügbar ist, wird die Abrufanforderung an einen Cloud-Speicherpool weitergeleitet.

Wenn sich die einzige Objektkopie im AWS Glacier-Speicher oder in der Azure-Archivebene befindet, muss die Clientanwendung eine S3 RestoreObject-Anforderung ausgeben, um eine abrufbare Kopie im Cloud-Speicherpool wiederherzustellen.



1. Der LDR-Dienst empfängt eine Abrufanforderung von der Clientanwendung.
2. Der LDR-Dienst fragt den Metadatenspeicher nach dem Speicherort der Objektdaten und den Metadaten ab.
3. Der LDR-Dienst leitet die Abrufanforderung 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.

Datenfluss löschen

Alle Objektkopien werden aus dem StorageGRID -System entfernt, wenn ein Client einen Löschvorgang durchführt oder wenn die Lebensdauer des Objekts abläuft und dadurch seine automatische Entfernung ausgelöst wird. Für die Objektlöschung gibt es einen definierten Datenfluss.

Löschhierarchie

StorageGRID bietet mehrere Methoden zur Steuerung, wann Objekte aufbewahrt oder gelöscht werden. Objekte können auf Clientanforderung oder automatisch gelöscht werden. StorageGRID priorisiert alle S3-Objektsperreinstellungen immer gegenüber Client-Löschanforderungen, die wiederum Vorrang vor dem S3-Bucket-Lebenszyklus und ILM-Platzierungsanweisungen haben.

- **S3-Objektsperre**: Wenn die globale Einstellung „S3-Objektsperre“ für das Raster aktiviert ist, können S3-Clients Buckets mit aktivierter S3-Objektsperre erstellen und dann die S3-REST-API verwenden, um Einstellungen für die Aufbewahrungsdauer und die rechtliche Aufbewahrung für jede diesem Bucket hinzugefügte Objektversion festzulegen.
  - Eine Objektversion, die einer rechtlichen Sperre unterliegt, kann mit keiner Methode gelöscht werden.
  - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version mit keiner Methode gelöscht werden.

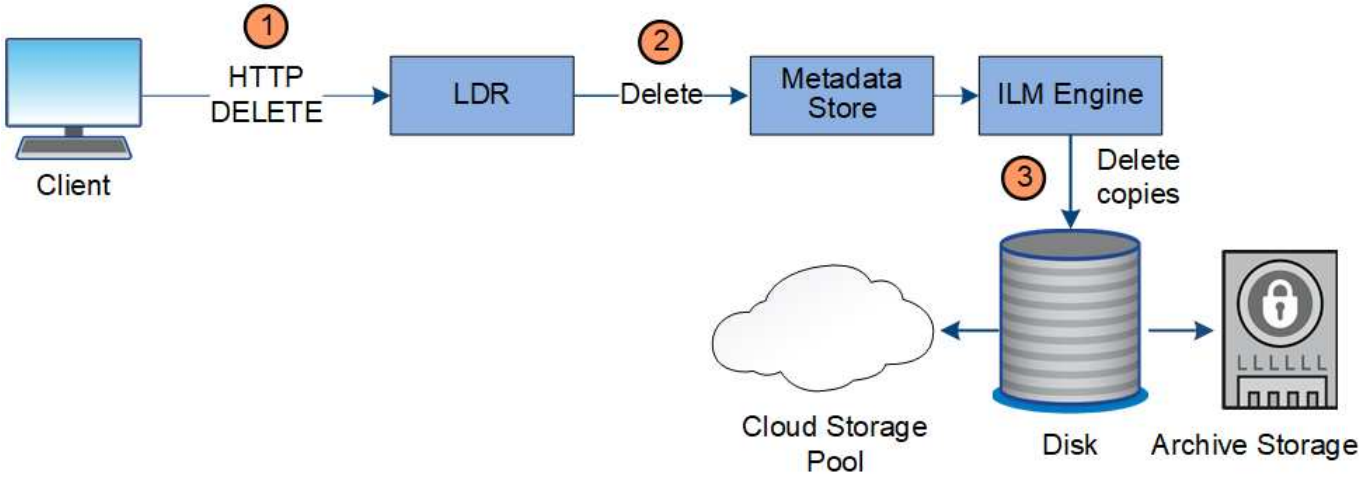
- Objekte in Buckets mit aktivierter S3-Objektsperre werden von ILM „für immer“ aufbewahrt. Nach Erreichen des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Clientanforderung oder den Ablauf des Bucket-Lebenszyklus gelöscht werden.
- Wenn S3-Clients ein Standard-Aufbewahrungsdatum auf den Bucket anwenden, müssen sie nicht für jedes Objekt ein Aufbewahrungsdatum 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 diese Option verwenden, um alle Kopien der Objekte und Objektversionen in ausgewählten Buckets dauerhaft aus dem StorageGRID System zu entfernen.
- **S3-Bucket-Lebenszyklus**: S3-Clients können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Ablaufaktion angibt. Wenn ein Bucket-Lebenszyklus vorhanden ist, löscht StorageGRID automatisch alle Kopien eines Objekts, wenn das in der Ablaufaktion angegebene Datum oder die Anzahl der Tage erreicht ist, es sei denn, der Client löscht das Objekt zuerst.
- **Anweisungen zur ILM-Platzierung**: Vorausgesetzt, für den Bucket ist die S3-Objektsperre nicht aktiviert und es gibt keinen Bucket-Lebenszyklus, löscht StorageGRID ein Objekt automatisch, wenn der letzte Zeitraum in der ILM-Regel endet und keine weiteren Platzierungen für das Objekt angegeben sind.

> Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Aktionen zum Ablauf des Lebenszyklus die ILM-Richtlinie für Objekte, die dem Lebenszyklusfilter entsprechen. Dies kann dazu führen, dass ein Objekt auch dann noch auf dem Raster verbleibt, wenn keine ILM-Anweisungen zum Platzieren des Objekts mehr vorliegen.

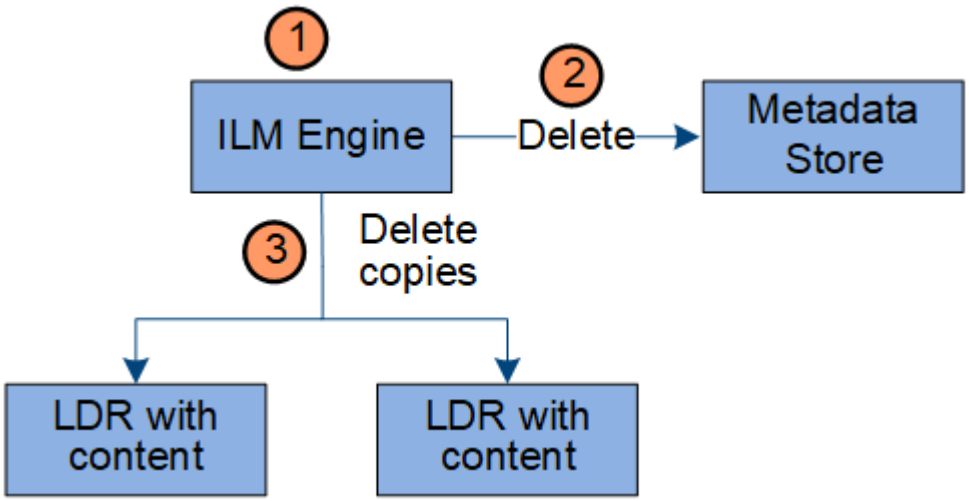
Sehen "So werden Objekte gelöscht" für weitere Informationen.

Datenfluss für Clientlöschungen



1. Der LDR-Dienst empfängt eine Löschanforderung von der Clientanwendung.
2. Der LDR-Dienst aktualisiert den Metadatenspeicher, sodass das Objekt für Clientanforderungen als gelöscht angezeigt wird, 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 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 Clientanforderungen gelöscht aussieht.
3. Die ILM-Engine entfernt alle Kopien des Objekts. Der Metadatenspeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Informationslebenszyklusmanagement

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

ILM-Regeln definieren:

- Welche Objekte sollen gespeichert werden? Eine Regel kann für alle Objekte gelten, oder Sie können Filter angeben, um zu ermitteln, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder Swift-Containern oder bestimmten Metadatenwerten verknüpft sind.
- Der Speichertyp und -ort. Objekte können auf Speicherknoten oder in Cloud-Speicherpools gespeichert werden.
- Der Typ der erstellten Objektkopien. Kopien können repliziert oder mit einem Erasure Code versehen werden.
- Bei replizierten Kopien die Anzahl der erstellten Kopien.
- Bei Erasure-Coding-Kopien das verwendete Erasure-Coding-Schema.
- Die Änderungen im Laufe der Zeit am Speicherort eines Objekts und an der Art der Kopien.
- Wie Objektdaten geschützt werden, wenn Objekte in das Raster aufgenommen werden (synchrone Platzierung 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. Um die Daten vor Verlust zu schützen, werden an jedem Standort automatisch drei Kopien der Objektmetadaten

verwaltet.

Beispiel einer ILM-Regel

Beispielsweise könnte eine ILM-Regel Folgendes festlegen:

- Gilt nur für die Objekte, die Mieter A gehören.
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Ort.
- Bewahren Sie die beiden Kopien „für immer“ auf, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte, bis sie durch eine Löschanforderung des Clients oder durch Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die Option „Ausgewogen“ für das Aufnahmeverhalten: Die Anweisung zur Platzierung an zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, beide erforderlichen Kopien sofort zu erstellen.

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

So bewertet eine ILM-Richtlinie Objekte

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

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

1. Wenn die Filter für die erste 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 für die erste Regel nicht mit dem Objekt übereinstimmen, wird das Objekt anhand jeder nachfolgenden Regel in der Richtlinie ausgewertet, bis eine Übereinstimmung gefunden wird.
3. Wenn keine Regeln mit einem Objekt übereinstimmen, werden das Aufnahmeverhalten und die Platzierungsanweisungen für die Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie und kann keine Filter verwenden. Es muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

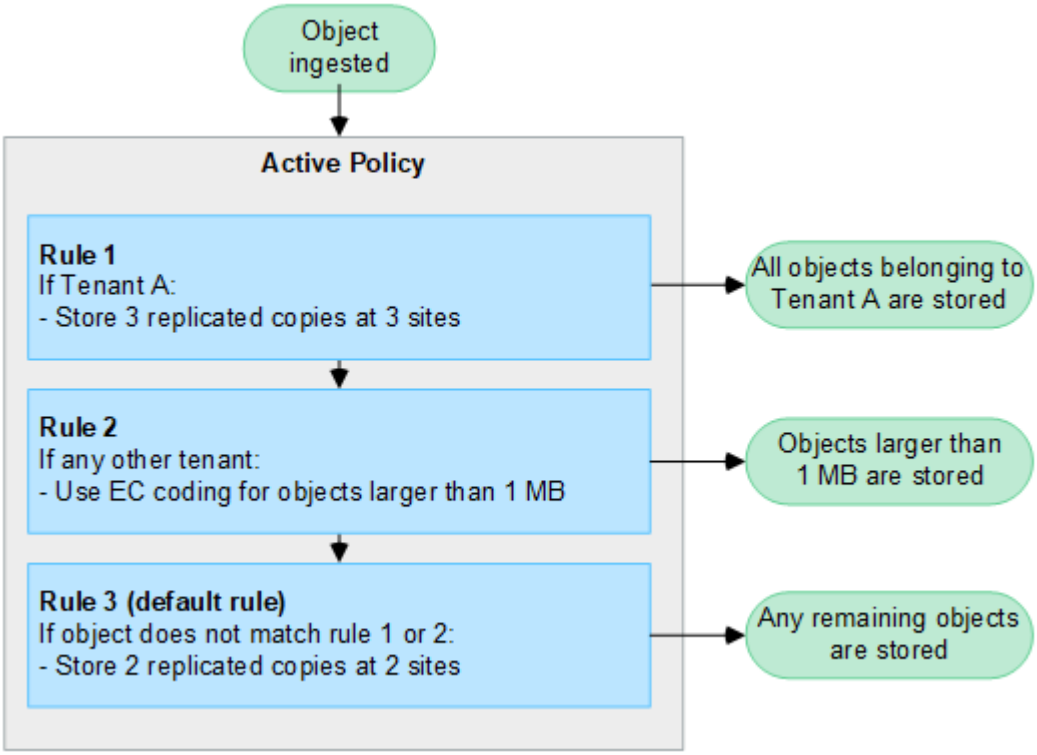
Beispiel einer ILM-Richtlinie

Beispielsweise könnte eine ILM-Richtlinie drei ILM-Regeln enthalten, die Folgendes festlegen:

- **Regel 1: Replikate für Mieter A**
  - Alle Objekte abgleichen, die zu Mieter A gehören.
  - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
  - Objekte, die anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie anhand von Regel 2 ausgewertet.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte anderer Mandanten werden abgeglichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mittels 6+3-Erasure-Coding an drei Standorten gespeichert.

- Stimmt nicht mit Objekten überein, die 1 MB oder kleiner sind. Daher werden diese Objekte anhand von Regel 3 ausgewertet.

- **Regel 3: 2 Kopien, 2 Rechenzentren** (Standard)
  - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und 1 MB oder kleiner sind).



Ähnliche Informationen

- "Objekte mit ILM verwalten"

Entdecken Sie StorageGRID

Entdecken Sie den Grid Manager

Der Grid Manager ist die browserbasierte grafische Benutzeroberfläche, mit der Sie Ihr StorageGRID -System konfigurieren, verwalten und überwachen können.

> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

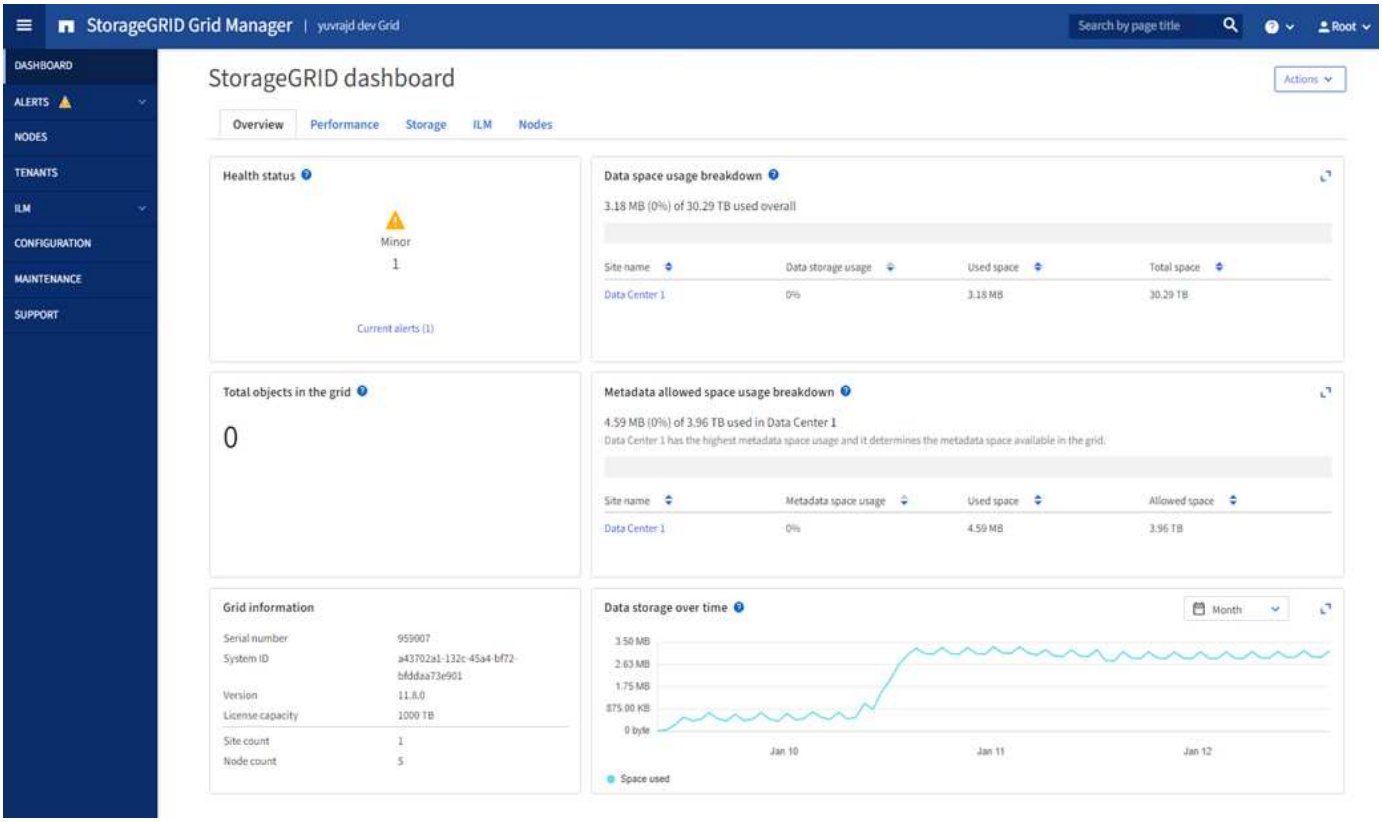
Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Jedes StorageGRID -System umfasst einen primären Admin-Knoten und eine beliebige Anzahl nicht-primärer Admin-Knoten. Sie können eine Verbindung zu jedem Admin-Knoten herstellen und jeder Admin-Knoten zeigt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

Sie können auf den Grid Manager zugreifen, indem Sie"unterstützter Webbrowser" .

Grid Manager-Dashboard

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

Das Dashboard enthält Informationen zu Systemzustand und -leistung, Speichernutzung, ILM-Prozessen, S3-Vorgängen und den Knoten im Grid. Du kannst"Konfigurieren Sie das Dashboard" indem Sie aus einer Sammlung von Karten auswählen, die die Informationen enthalten, die Sie zur effektiven Überwachung Ihres Systems benötigen.



Für eine Erklärung der auf jeder Karte angezeigten Informationen wählen Sie das Hilfesymbol für diese Karte.

Suchfeld

Über das Feld **Suchen** in der Kopfzeile können Sie schnell zu einer bestimmten Seite im Grid Manager navigieren. Sie können beispielsweise **km** eingeben, um auf die Seite des Schlüsselverwaltungsservers (KMS) zuzugreifen.

Mit der **Suche** können Sie Einträge in der Seitenleiste des Grid Managers und in den Menüs „Konfiguration“, „Wartung“ und „Support“ finden. Sie können auch nach Namen nach Elementen wie Grid-Knoten und Mandantenkonten suchen.

Hilfemenü

Das Hilfemenü bietet Zugriff auf:

- Der"FabricPool" Und"S3-Einrichtung" Zauberer
- Das StorageGRID Dokumentationszentrum für die aktuelle Version
- "API-Dokumentation"

- Informationen darüber, welche Version von StorageGRID aktuell installiert ist

Menü „Benachrichtigungen“

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

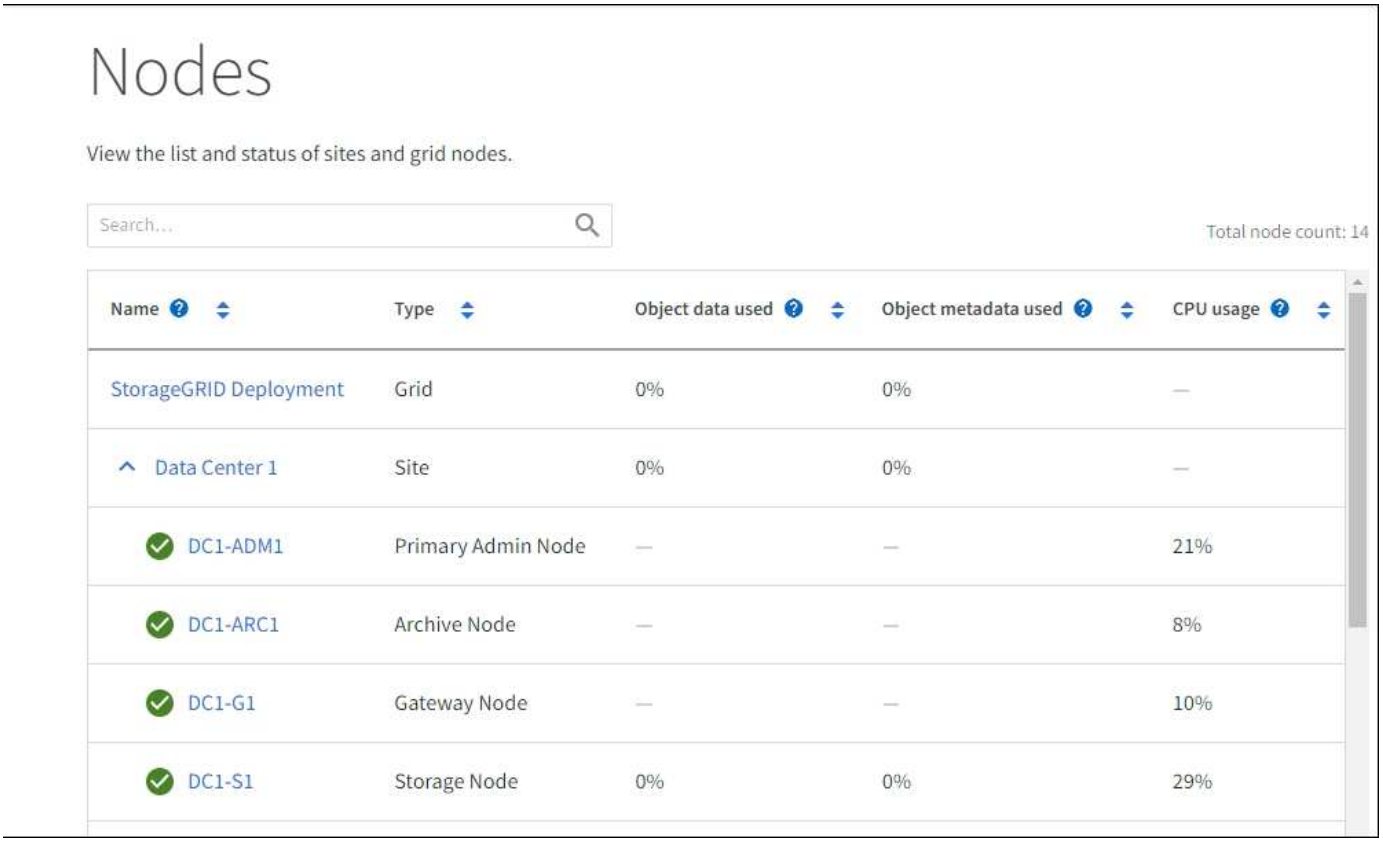
Im Menü „Alarme“ können Sie Folgendes tun:"Benachrichtigungen verwalten" :

- Aktuelle Warnungen überprüfen
- Überprüfen gelöster Warnungen
- Konfigurieren Sie Stummschaltungen, um Warnbenachrichtigungen zu unterdrücken
- Definieren Sie Warnregeln für Bedingungen, die Warnmeldungen auslösen
- Konfigurieren Sie den E-Mail-Server für Warnbenachrichtigungen

Knotenseite

Der"Knotenseite" zeigt Informationen zum gesamten Raster, zu jedem Standort im Raster und zu jedem Knoten an einem Standort an.

Auf der Nodes-Startseite werden kombinierte Metriken für das gesamte Raster angezeigt. Um Informationen zu einer bestimmten Site oder einem bestimmten Knoten anzuzeigen, wählen Sie die Site oder den Knoten aus.

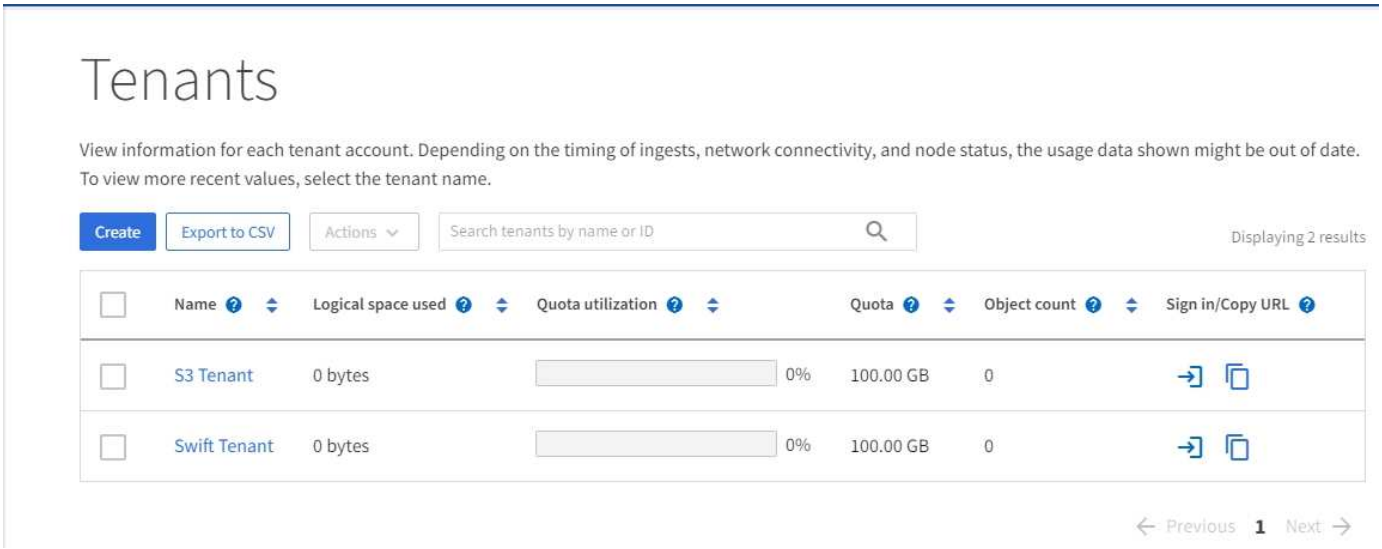


Mieterseite

Der"Mieterseite" ermöglicht es Ihnen,"Erstellen und Überwachen der Speichermandantenkonten" für Ihr StorageGRID System. Sie müssen mindestens ein Mandantenkonto erstellen, um festzulegen, wer Objekte

speichern und abrufen kann und welche Funktionen ihm zur Verfügung stehen.

Auf der Seite „Mandanten“ werden auch Nutzungsdetails für jeden Mandanten bereitgestellt, einschließlich der Menge des verwendeten Speichers und der Anzahl der Objekte. Wenn Sie beim Erstellen des Mandanten ein Kontingent festgelegt haben, können Sie sehen, wie viel von diesem Kontingent verwendet wurde.



ILM-Menü

Der"ILM-Menü" ermöglicht es Ihnen,"Konfigurieren Sie die Regeln und Richtlinien für das Information Lifecycle Management (ILM)." die die Haltbarkeit und Verfügbarkeit der Daten regeln. Sie können auch eine Objektkennung eingeben, um die Metadaten für dieses Objekt anzuzeigen.

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Speicherpools
- Lagerqualitäten
- Regionen
- Objektmetadatensuche

Konfigurationsmenü

Im Konfigurationsmenü können Sie Netzwerkeinstellungen, Sicherheitseinstellungen, Systemeinstellungen, Überwachungsoptionen und Zugriffskontrolloptionen festlegen.

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

- "Verwalten von Hochverfügbarkeitsgruppen"
- "Verwalten von Load Balancer-Endpunkten"
- "Konfigurieren von S3-Endpunktdomänennamen"

- "Verwalten von Richtlinien zur Verkehrsklassifizierung"
- "Konfigurieren von VLAN-Schnittstellen"

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

- "Sicherheitszertifikate verwalten"
- "Verwalten interner Firewall-Kontrollen"
- "Konfigurieren von Schlüsselverwaltungsservern"
- Konfigurieren von Sicherheitseinstellungen, einschließlich der"TLS- und SSH-Richtlinie" ,"Netzwerk- und Objektsicherheitsoptionen" , Und"Schnittstellensicherheitseinstellungen" .
- Konfigurieren der Einstellungen für eine"Speicherproxy" oder ein"Administrator-Proxy"

Systemaufgaben

Zu den Systemaufgaben gehören:

- Verwenden"Netzverbund" um Mandantenkontoinformationen zu klonen und Objektdaten zwischen zwei StorageGRID Systemen zu replizieren.
- Optional: Aktivieren Sie die"Gespeicherte Objekte komprimieren" Option.
- "Verwalten der S3-Objektsperre"
- Verstehen von Speicheroptionen wie"Objektsegmentierung" Und"Speichervolumen-Wasserzeichen" .
- "Verwalten von Erasure-Coding-Profilen" .

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- "Konfigurieren von Prüfmeldungen und Protokollzielen"
- "Verwenden der SNMP-Überwachung"

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugriffskontrolle gehören:

- "Verwalten von Administratorgruppen"
- "Verwalten von Administratorbenutzern"
- Ändern der"Bereitstellungspassphrase" oder"Passwörter für die Knotenkonsole"
- "Verwenden der Identitätsföderation"
- "Konfigurieren von SSO"

Wartungsmenü

Über das Wartungsmenü können Sie Wartungsaufgaben, Systemwartung und Netzwerkwartung durchführen.

Aufgaben

Zu den Wartungsaufgaben gehören:

- "Stilllegungsarbeiten"ungenutzte Netzknoten und Standorte zu entfernen
- "Expansionsvorgänge"um neue Grid-Knoten und Sites hinzuzufügen
- "Verfahren zur Wiederherstellung von Grid-Knoten"um einen ausgefallenen Knoten zu ersetzen und Daten wiederherzustellen
- "Prozeduren umbenennen"um die Anzeigenamen Ihres Rasters, Ihrer Sites und Knoten zu ändern
- "Operationen zur Objektexistenzprüfung"um die Existenz (jedoch nicht die Richtigkeit) von Objektdaten zu überprüfen
- Durchführen einer"Rollierender Neustart" um mehrere Grid-Knoten neu zu starten
- "Volume-Wiederherstellungsvorgänge"

System

Zu den Aufgaben der Systemwartung, die Sie durchführen können, gehören:

- "Anzeigen von StorageGRID -Lizenzinformationen"oder"Aktualisieren der Lizenzinformationen"
- Generieren und Herunterladen der"Wiederherstellungspaket"
- Durchführen von StorageGRID -Softwareupdates, einschließlich Software-Upgrades, Hotfixes und Updates der SANtricity OS-Software auf ausgewählten Geräten
  - "Upgrade-Verfahren"
  - "Hotfix-Verfahren"
  - "Aktualisieren Sie SANtricity OS auf SG6000-Speichercontrollern mit Grid Manager"
  - "Aktualisieren Sie SANtricity OS auf SG5700-Speichercontrollern mit Grid Manager"

Netzwerk

Zu den Aufgaben, die Sie zur Netzwerkwartung durchführen können, gehören:

- "Konfigurieren von DNS-Servern"
- "Aktualisieren von Grid-Netzwerk-Subnetzen"
- "Verwalten von NTP-Servern"

Support-Menü

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

Tools

Im Abschnitt „Tools“ des Support-Menüs können Sie:

- "Konfigurieren Sie AutoSupport"
- "Diagnose ausführen"zum aktuellen Zustand des Netzes
- "Zugriff auf den Grid-Topologie-Baum"um detaillierte Informationen zu Grid-Knoten, Diensten und Attributen anzuzeigen

- "Erfassen von Protokolldateien und Systemdaten"
- "Überprüfen der Supportmetriken"

> Die über die Option **Metriken** verfügbaren Tools sind für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig.

Alarme (alt)

Die Informationen zu Legacy-Alarmen wurden aus dieser Version der Dokumentation entfernt. Siehe "Verwalten von Warnungen und Alarmen (StorageGRID 11.8-Dokumentation)" .

Sonstige

Im Abschnitt „Sonstiges“ des Support-Menüs können Sie:

- Verwalten"Linkkosten"
- Sicht"Netzwerkmanagementsystem (NMS)" Einträge
- Verwalten"Speicherwasserzeichen"

Entdecken Sie den Tenant Manager

Der"Mietermanager" ist die browserbasierte grafische Benutzeroberfläche, auf die Mandantenbenutzer zugreifen, um ihre Speicherkonten zu konfigurieren, zu verwalten und zu überwachen.

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

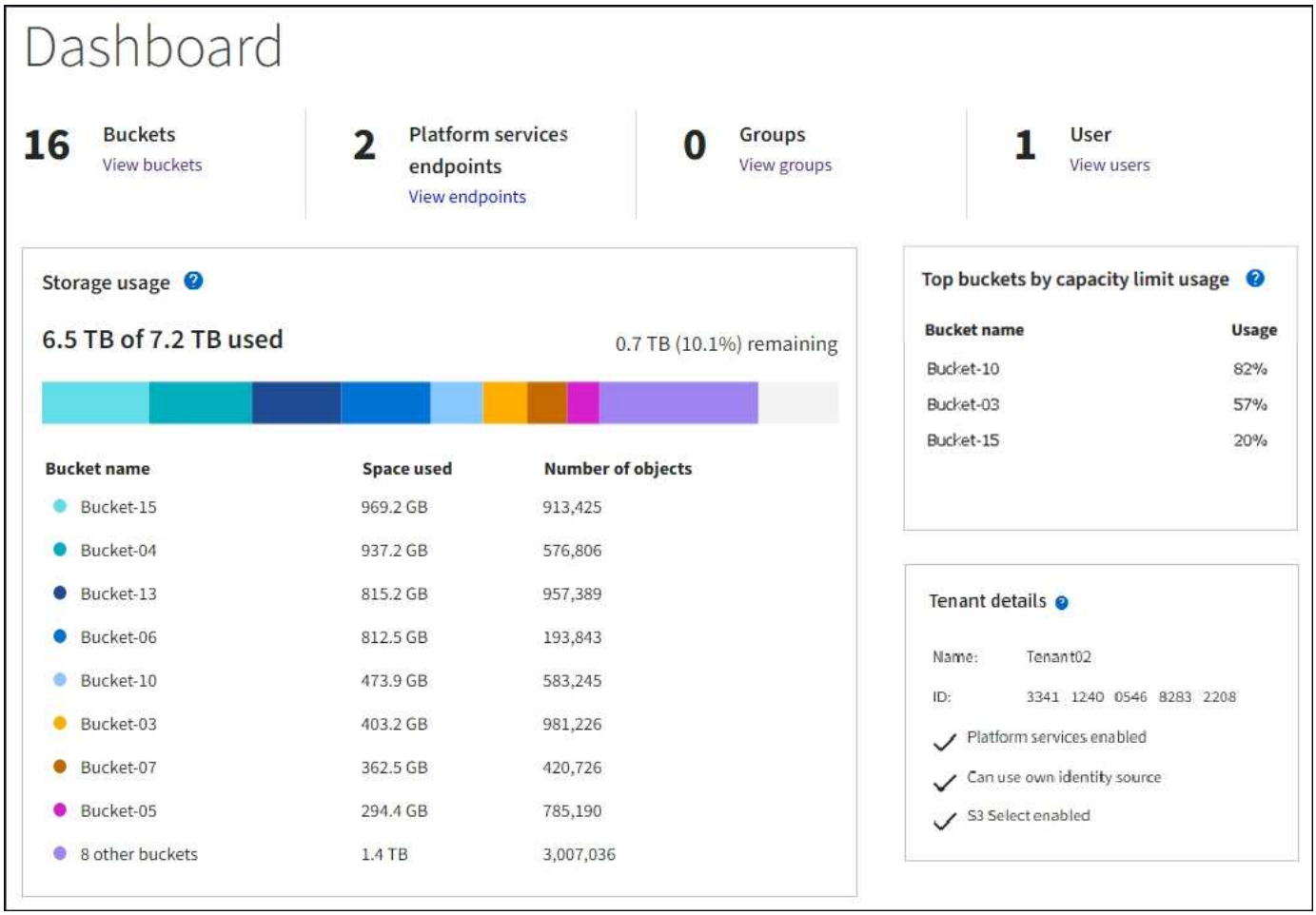
Wenn sich Mandantenbenutzer beim Mandantenmanager anmelden, stellen sie eine Verbindung zu einem Admin-Knoten her.

Mandantenmanager-Dashboard

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

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

Der über dem Balkendiagramm angezeigte Wert ist die Summe des für alle Buckets oder Container des Mandanten verwendeten Speicherplatzes. Wenn bei der Kontoerstellung die für den Mandanten maximal verfügbare Anzahl an Gigabyte, Terabyte oder Petabyte angegeben wurde, werden auch die Menge des verwendeten und verbleibenden Kontingents angezeigt.



Speichermenü (S3)

Das Speichermenü wird nur für S3-Mandantenkonten bereitgestellt. Über dieses Menü können S3-Benutzer Zugriffsschlüssel verwalten, Buckets erstellen, verwalten und löschen, Plattformdienst-Endpunkte verwalten und alle Grid-Föderationsverbindungen anzeigen, die sie verwenden dürfen.

Meine Zugriffsschlüssel

S3-Mandantenbenutzer können Zugriffsschlüssel wie folgt verwalten:

- Benutzer mit der Berechtigung „Eigene S3-Anmeldeinformationen verwalten“ können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung „Root-Zugriff“ können die Zugriffsschlüssel für das S3-Root-Konto, ihr eigenes Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten außerdem vollständigen Zugriff auf die Buckets und Objekte des Mandanten, sofern dies nicht ausdrücklich durch eine Bucket-Richtlinie deaktiviert wird.

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

Eimer

S3-Tenant-Benutzer mit den entsprechenden Berechtigungen können die folgenden Aufgaben für ihre Buckets ausführen:

- Buckets erstellen
- Aktivieren Sie S3 Object Lock für einen neuen Bucket (setzt voraus, dass S3 Object Lock für das StorageGRID -System aktiviert ist).
- Konsistenzwerte aktualisieren
- Aktivieren und Deaktivieren der Aktualisierung der letzten Zugriffszeit
- Aktivieren oder Aussetzen der Objektversionierung
- Standardaufbewahrung für S3 Object Lock aktualisieren
- Konfigurieren Sie Cross-Origin Resource Sharing (CORS)
- Alle Objekte in einem Bucket löschen
- Leere Buckets löschen
- Verwenden Sie die"S3-Konsole" zum Verwalten von Bucket-Objekten

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

- Konfigurieren Sie S3-Ereignisbenachrichtigungen, die an einen Zieldienst gesendet werden können, der den Amazon Simple Notification Service unterstützt.
- Konfigurieren Sie die CloudMirror-Replikation, die es dem Mandanten ermöglicht, Objekte automatisch in einen externen S3-Bucket zu replizieren.
- Konfigurieren Sie die Suchintegration, die Objektmetadaten an einen Zielsuchindex sendet, wenn ein Objekt erstellt oder gelöscht wird oder seine Metadaten oder Tags aktualisiert werden.

Plattformdienst-Endpunkte

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

Grid-Föderation-Verbindungen

Wenn ein Grid-Administrator die Verwendung einer Grid-Föderationsverbindung 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 Cross-Grid-Replikation aktiviert ist, und den letzten Fehler anzeigen, der aufgetreten ist, als Bucket-Daten in das andere Grid in der Verbindung repliziert wurden. Sehen "Grid-Föderation-Verbindungen anzeigen" .

Menü „Zugriffsverwaltung“

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

Verwenden Sie diese Richtlinien, um mehr über die Architektur und Netzwerktopologien

von StorageGRID zu erfahren und die Anforderungen für die Netzwerkkonfiguration und -bereitstellung kennenzulernen.

Zu dieser Anleitung

Diese Richtlinien enthalten Informationen, die Sie zum Erstellen der StorageGRID Netzwerkinfrastruktur verwenden können, bevor Sie StorageGRID -Knoten bereitstellen und konfigurieren. Verwenden Sie diese Richtlinien, um sicherzustellen, dass die Kommunikation zwischen allen Knoten im Grid und zwischen dem Grid und externen Clients und Diensten stattfinden kann.

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

- Speichern und Abrufen von Objektdaten
- Erhalten Sie E-Mail-Benachrichtigungen
- Greifen Sie auf die StorageGRID -Verwaltungsschnittstelle (Grid Manager und Tenant Manager) zu.
- Zugriff auf die Audit-Freigabe (optional)
- Bieten Sie Dienstleistungen an wie:
  - Netzwerkzeitprotokoll (NTP)
  - Domänennamensystem (DNS)
  - Schlüsselverwaltungsserver (KMS)

Das StorageGRID -Netzwerk muss entsprechend konfiguriert werden, um den Datenverkehr für diese und weitere Funktionen zu bewältigen.

Bevor Sie beginnen

Die Netzwerkkonfiguration für ein StorageGRID -System erfordert ein hohes Maß an Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerkrouting und Firewalls.

Machen Sie sich vor der Netzwerkkonfiguration mit der StorageGRID -Architektur vertraut, wie in"Erfahren Sie mehr über StorageGRID" .

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

Installieren von Appliance-Knoten

- "Installieren der Appliance-Hardware"

Installieren Sie softwarebasierte Knoten

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

Konfigurieren und Verwalten der StorageGRID -Software

- "StorageGRID verwalten"
- "Versionshinweise"

StorageGRID -Netzwerktypen

Die Grid-Knoten in einem StorageGRID -System verarbeiten *Grid-Verkehr*, *Admin-Verkehr* und *Client-Verkehr*. Sie müssen das Netzwerk entsprechend konfigurieren, um diese drei Arten von Datenverkehr zu verwalten und Kontrolle und Sicherheit zu gewährleisten.

Verkehrsarten

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

Sie können das Netzwerk auf folgende Arten konfigurieren:

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

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

Interne Ports sind nur über das Grid-Netzwerk zugänglich. Externe Ports sind von allen Netzwerktypen aus zugänglich. Diese Flexibilität bietet mehrere Optionen für die Gestaltung einer StorageGRID -Bereitstellung und die Einrichtung externer IP- und Portfilter in Switches und Firewalls. Sehen"interne Grid-Knoten-Kommunikation" Und"Externe Kommunikation" .

Netzwerkschnittstellen

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

Netzwerk	Schnittstellenname
Grid-Netzwerk (erforderlich)	eth0

Netzwerk	Schnittstellenname
Admin-Netzwerk (optional)	eth1
Client-Netzwerk (optional)	eth2

Einzelheiten zum Zuordnen virtueller oder physischer Ports zu Knotennetzwerkschnittstellen finden Sie in den Installationsanweisungen:

Softwarebasierte Knoten

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

Appliance-Knoten

- "SG6160 Speichergerät"
- "SGF6112 Speichergerät"
- "SG6000-Speichergerät"
- "SG5800 Speichergerät"
- "SG5700 Speichergerät"
- "SG110 und SG1100 Servicegeräte"
- "SG100 und SG1000 Servicegeräte"

Netzwerkinformationen für jeden Knoten

Sie müssen für jedes Netzwerk, das Sie auf einem Knoten aktivieren, Folgendes 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 Sie kein Gateway für ein Netzwerk konfigurieren möchten, sollten Sie die IP-Adresse als Gateway-Adresse verwenden.

Hochverfügbarkeitsgruppen

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

Netznetzwerk

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

StorageGRID unterstützt keine Netzwerkadressübersetzung (NAT) zwischen Knoten.

Das Grid-Netzwerk kann für den gesamten Admin-Verkehr und den gesamten Client-Verkehr verwendet werden, auch wenn das Admin-Netzwerk und das Client-Netzwerk konfiguriert sind. Das Grid-Netzwerk-Gateway ist das Standard-Gateway des Knotens, sofern für den Knoten nicht das Client-Netzwerk konfiguriert ist.

Beim Konfigurieren des Grid-Netzwerks müssen Sie sicherstellen, dass das Netzwerk vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt ist.

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

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

Admin-Netzwerk

Das Admin-Netzwerk ist optional. Nach der Konfiguration kann es für den Systemadministrations- und Wartungsverkehr verwendet werden. Das Admin-Netzwerk ist normalerweise ein privates Netzwerk und muss nicht zwischen Knoten geroutet werden können.

Sie können auswählen, für welche Grid-Knoten das Admin-Netzwerk aktiviert werden soll.

Wenn Sie das Admin-Netzwerk verwenden, muss der Verwaltungs- und Wartungsverkehr nicht über das Grid-Netzwerk laufen. Typische Verwendungszwecke des Admin-Netzwerks sind unter anderem:

- 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 Prüfprotokolle auf Admin-Knoten.
- Secure Shell Protocol (SSH)-Zugriff für Wartung und Support.

Das Admin-Netzwerk wird niemals für internen Grid-Verkehr verwendet. Es wird ein Admin-Netzwerk-Gateway bereitgestellt, das dem Admin-Netzwerk die Kommunikation mit mehreren externen Subnetzen ermöglicht. Das Admin-Netzwerk-Gateway wird jedoch nie als Standard-Gateway des Knotens verwendet.

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

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

Kundennetzwerk

Das Client-Netzwerk ist optional. Wenn es konfiguriert ist, wird es verwendet, um Clientanwendungen wie S3 Zugriff auf Grid-Dienste zu gewähren. Wenn Sie StorageGRID Daten einer externen Ressource zugänglich machen möchten (z. B. einem Cloud Storage Pool oder dem StorageGRID CloudMirror-Replikationsdienst), kann die externe Ressource auch das Client-Netzwerk verwenden. Grid-Knoten können mit jedem Subnetz kommunizieren, das über das Client-Netzwerk-Gateway erreichbar ist.

Sie können auswählen, auf welchen Grid-Knoten das Client-Netzwerk aktiviert werden soll. Es müssen sich nicht alle Knoten im selben Client-Netzwerk befinden und die Knoten kommunizieren niemals über das Client-Netzwerk miteinander. Das Client-Netzwerk ist erst betriebsbereit, wenn die Grid-Installation abgeschlossen ist.

Zur Erhöhung der Sicherheit können Sie festlegen, dass die Client-Netzwerkschnittstelle eines Knotens nicht vertrauenswürdig ist, sodass das Client-Netzwerk hinsichtlich der zulässigen Verbindungen restriktiver ist. Wenn die Client-Netzwerkschnittstelle eines Knotens nicht vertrauenswürdig ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie beispielsweise von der CloudMirror-Replikation verwendet werden, akzeptiert jedoch nur eingehende Verbindungen auf Ports, die explizit als Endpunkte des Lastenausgleichs konfiguriert wurden. Sehen"Verwalten von Firewall-Steuerelementen" Und"Konfigurieren von Load Balancer-Endpunkten" .

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Verkehr nicht über das Grid-Netzwerk laufen. Der Grid-Netzwerkverkehr kann auf ein sicheres, nicht routingfähiges Netzwerk aufgeteilt werden. Die folgenden Knotentypen werden häufig mit einem Client-Netzwerk konfiguriert:

- Gateway-Knoten, da diese Knoten Zugriff auf den StorageGRID Load Balancer-Dienst und S3-Client-Zugriff auf das Grid bieten.
- Speicherknoten, da diese Knoten Zugriff auf das S3-Protokoll sowie auf Cloud-Speicherpools und den CloudMirror-Replikationsdienst bieten.
- Admin-Knoten, um sicherzustellen, dass Mandantenbenutzer eine Verbindung zum Mandantenmanager herstellen können, ohne das Admin-Netzwerk verwenden zu müssen.

Beachten Sie Folgendes für das Client-Netzwerk-Gateway:

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

Optionale VLAN-Netzwerke

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

Um die Verwendung von VLANs zu unterstützen, müssen Sie eine oder mehrere Schnittstellen auf einem Knoten als Trunk-Schnittstellen am Switch konfigurieren. Sie können die Grid-Netzwerkschnittstelle (eth0) oder die Client-Netzwerkschnittstelle (eth2) als Trunk konfigurieren oder dem Knoten Trunk-Schnittstellen hinzufügen.

Wenn eth0 als Trunk konfiguriert ist, fließt der Grid-Netzwerkverkehr über die native Trunk-Schnittstelle, wie auf dem Switch konfiguriert. Wenn eth2 als Trunk konfiguriert ist und das Client-Netzwerk ebenfalls auf demselben Knoten konfiguriert ist, verwendet das Client-Netzwerk das native VLAN des Trunk-Ports, wie es auf dem Switch konfiguriert ist.

Über VLAN-Netzwerke wird nur eingehender Administratorverkehr unterstützt, wie er beispielsweise für SSH-, Grid Manager- oder Tenant Manager-Verkehr verwendet wird. Ausgehender Datenverkehr, wie er beispielsweise für NTP, DNS, LDAP, KMS und Cloud Storage Pools verwendet wird, wird über VLAN-Netzwerke nicht unterstützt.

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

Sehen"Konfigurieren von VLAN-Schnittstellen" für Anweisungen und Richtlinien.

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

Beispiele für Netzwerktopologien

Grid-Netzwerktopologie

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

Wenn Sie das Grid-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Knoten fest.

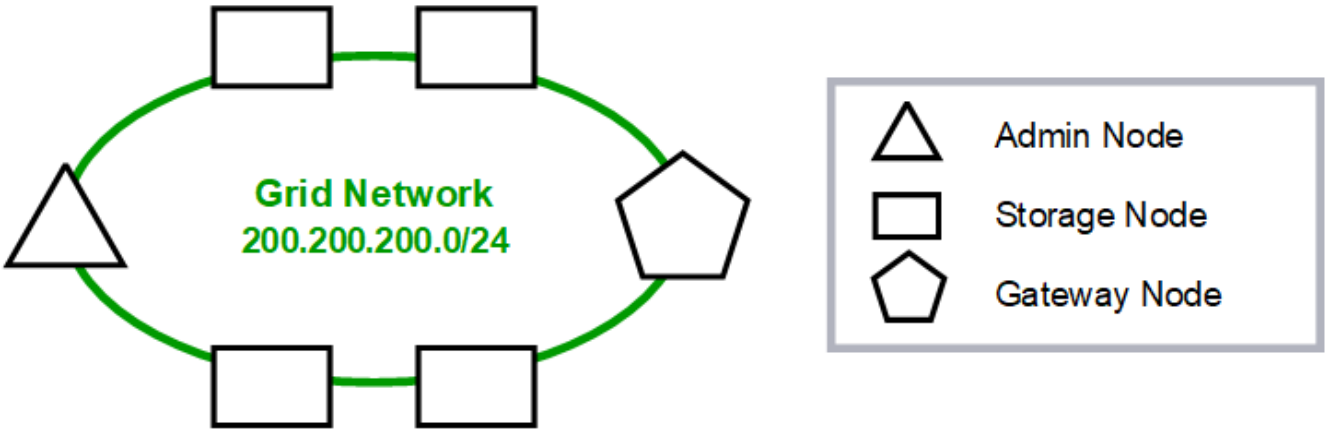
Während der Konfiguration müssen Sie alle Grid Network-Subnetze zur Grid Network Subnet List (GNSL) hinzufügen. Diese Liste enthält alle Subnetze für alle Sites und kann auch externe Subnetze enthalten, die Zugriff auf kritische Dienste wie NTP, DNS oder LDAP bieten.

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

In diesem Beispiel wird der gesamte Datenverkehr über dasselbe Netzwerk abgewickelt, einschließlich des Datenverkehrs im Zusammenhang mit S3-Clientanforderungen sowie Verwaltungs- und Wartungsfunktionen.

> Diese Topologie eignet sich für Einzelstandortbereitstellungen, die nicht extern verfügbar sind, für Proof-of-Concept- oder Testbereitstellungen oder wenn ein Lastenausgleich eines Drittanbieters als Clientzugriffsgrenze fungiert. Wenn möglich, sollte das Grid-Netzwerk ausschließlich für den internen Verkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk unterliegen zusätzlichen Firewall-Einschränkungen, die den externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Verkehr wird unterstützt, diese Verwendung 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

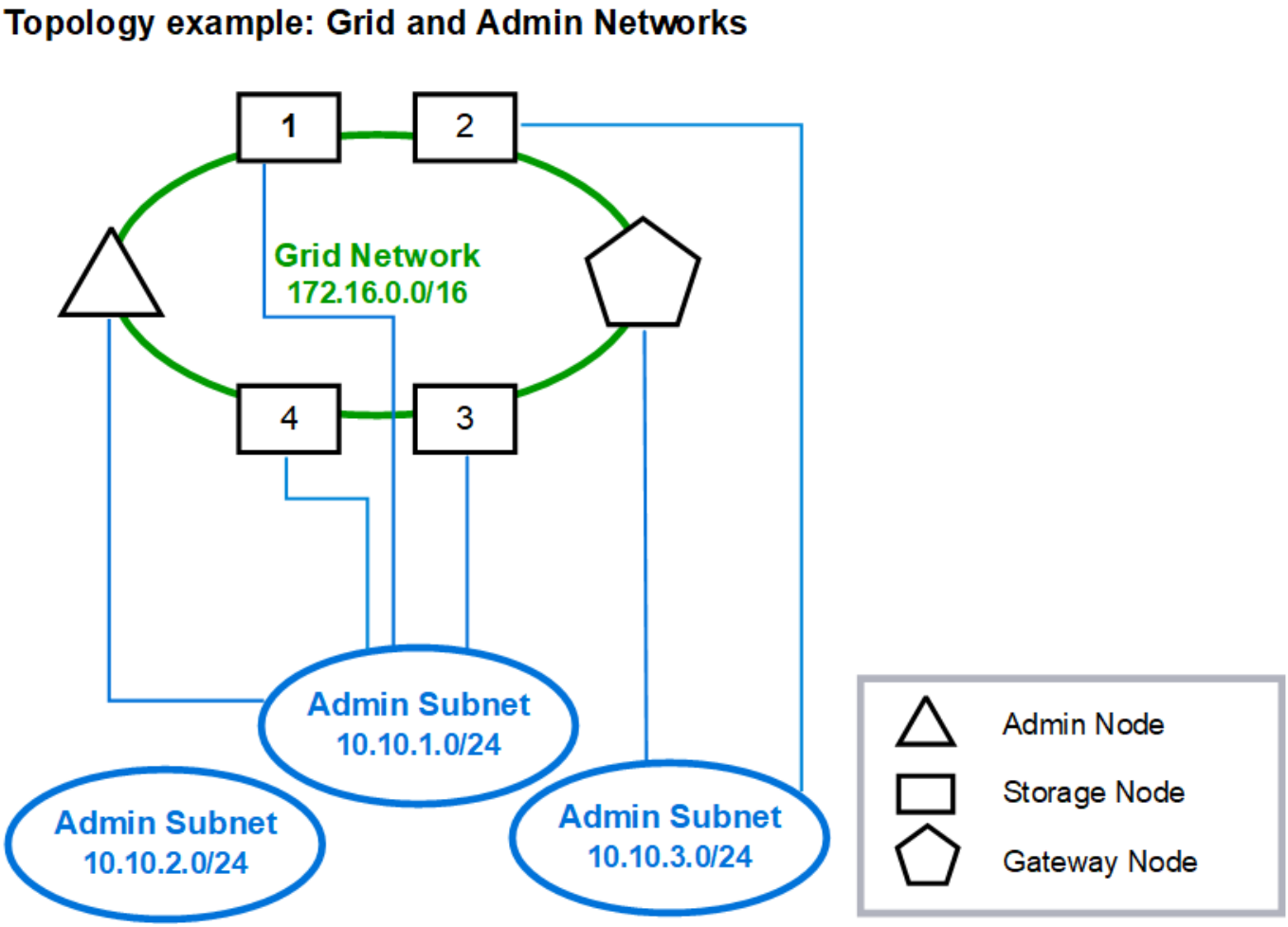
Admin-Netzwerktopologie

Ein Admin-Netzwerk ist optional. Eine Möglichkeit, ein Admin-Netzwerk und ein Grid-Netzwerk zu verwenden, besteht darin, für jeden Knoten ein routingfähiges Grid-Netzwerk und ein begrenztes Admin-Netzwerk zu konfigurieren.

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

Das Admin-Netzwerk kann für jeden Knoten eindeutig sein und aus mehreren Subnetzen bestehen. Jeder Knoten kann mit einer Admin External Subnet List (AESL) konfiguriert werden. Die AESL listet die über das Admin-Netzwerk erreichbaren Subnetze für jeden Knoten auf. Die AESL muss auch die Subnetze aller Dienste enthalten, auf die das Grid über das Admin-Netzwerk zugreift, z. B. NTP, DNS, KMS und LDAP. Für jedes Subnetz in der AESL werden statische Routen angewendet.

In diesem Beispiel wird das Grid-Netzwerk für den Datenverkehr im Zusammenhang mit S3-Clientanforderungen und Objektverwaltung verwendet, während das Admin-Netzwerk für Verwaltungsfunktionen verwendet wird.



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

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

System Generated

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

Client-Netzwerktopologie

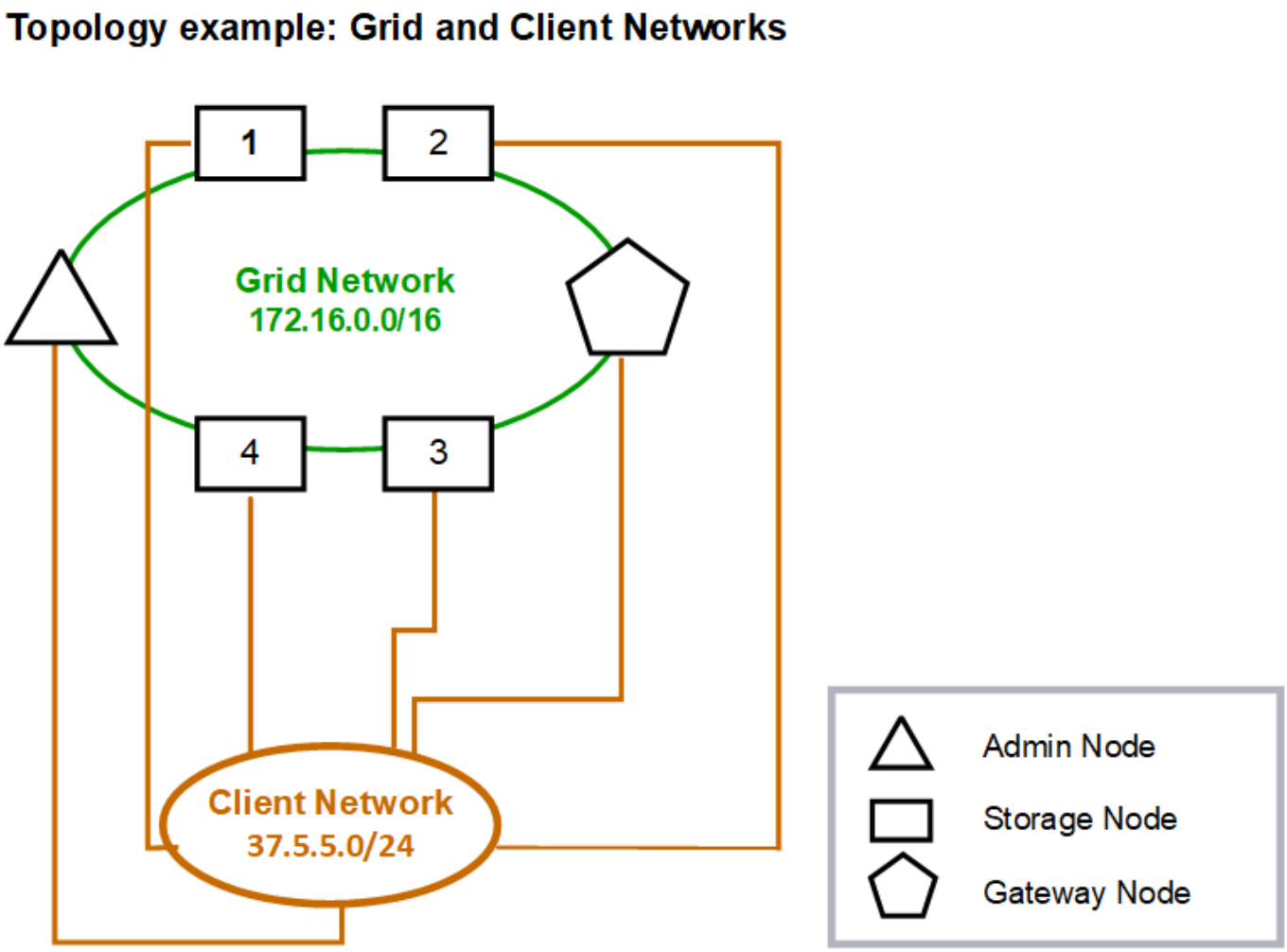
Ein Client-Netzwerk ist optional. Durch die Verwendung eines Client-Netzwerks kann der Client-Netzwerkverkehr (z. B. S3) vom internen Grid-Verkehr getrennt werden, wodurch die Grid-Vernetzung sicherer wird. Der Verwaltungsverkehr kann entweder vom Client- oder vom Grid-Netzwerk abgewickelt werden, wenn das Admin-Netzwerk nicht konfiguriert ist.

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

Wenn Sie während der Installation ein Client-Netzwerk für einen Knoten konfigurieren, wechselt das Standard-Gateway des Knotens nach Abschluss der Installation vom Grid-Netzwerk-Gateway zum Client-Netzwerk-Gateway. Wenn später ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway des Knotens auf die gleiche Weise.

In diesem Beispiel wird das Client-Netzwerk für S3-Client-Anfragen und für Verwaltungsfunktionen verwendet,

während das Grid-Netzwerk für interne Objektverwaltungsvorgänge 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

Ähnliche Informationen

"Knotennetzwerkkonfiguration ändern"

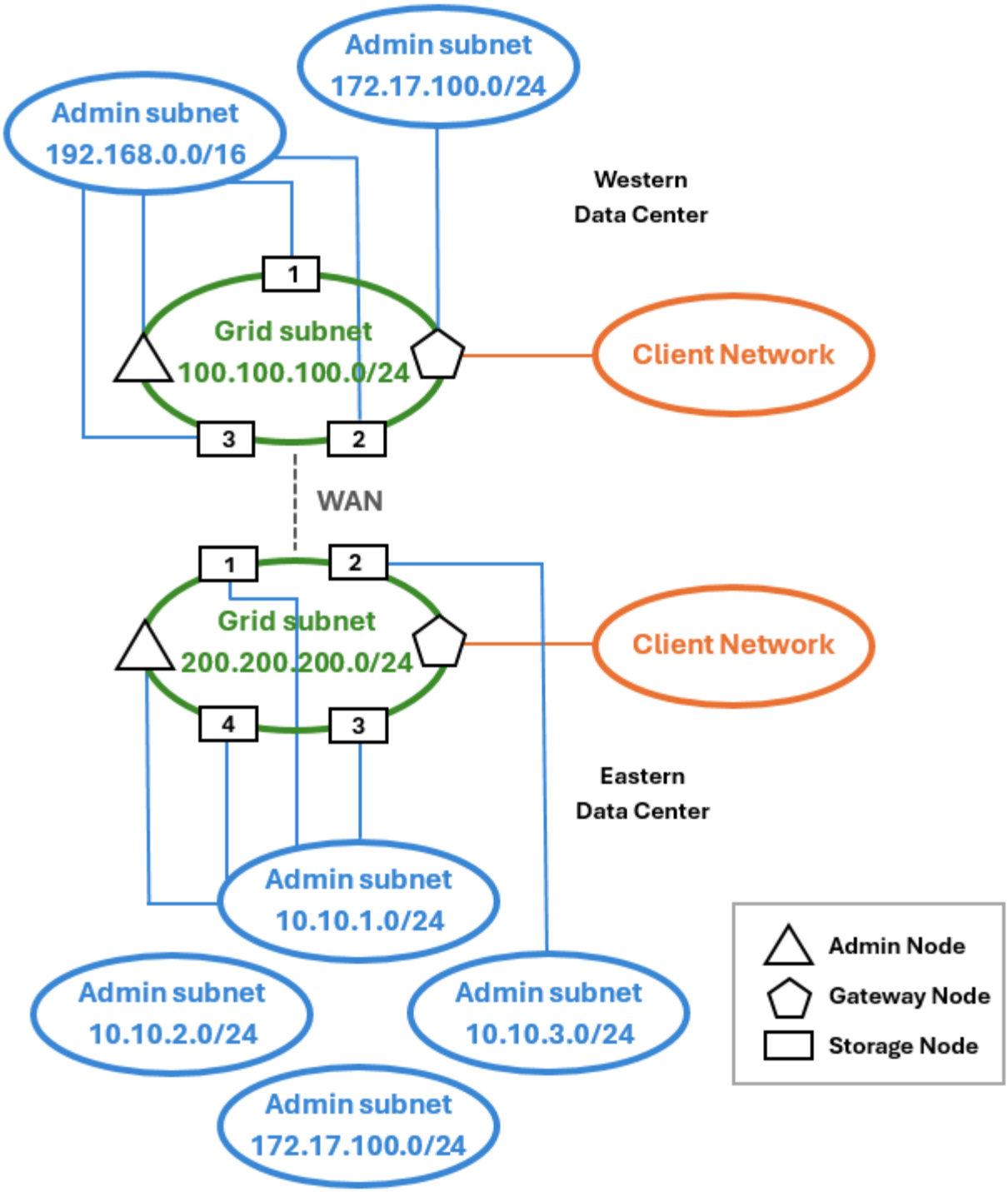
Topologie für alle drei Netzwerke

Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, begrenzten standortspezifischen Admin-Netzwerken und offenen Client-Netzwerken besteht. Die Verwendung von Load Balancer-Endpunkten und nicht vertrauenswürdigen Client-Netzwerken kann bei Bedarf zusätzliche Sicherheit bieten.

In diesem Beispiel:

- Das Grid-Netzwerk wird für den Netzwerkverkehr im Zusammenhang mit internen Objektverwaltungsvorgängen verwendet.
- Das Admin-Netzwerk wird für den Datenverkehr im Zusammenhang mit Verwaltungsfunktionen verwendet.
- Das Client-Netzwerk wird für den Datenverkehr im Zusammenhang mit S3-Client-Anfragen verwendet.

Topologiebeispiel: Grid-, Admin- und Client-Netzwerke



Netzwerkanforderungen

Sie müssen überprüfen, ob die aktuelle Netzwerkinfrastruktur und -konfiguration das geplante StorageGRID Netzwerkdesign unterstützen kann.

Allgemeine Netzwerkanforderungen

Alle StorageGRID Bereitstellungen müssen die folgenden Verbindungen unterstützen können.

Diese Verbindungen können über 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, normalerweise 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 aus erreichbar sein.
- **DNS-Serververbindungen**: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
- **LDAP/Active Directory-Serververbindungen**: Ausgehende TCP-Verbindung vom Identitätsdienst auf Speicherknoten.
- * AutoSupport*: Ausgehende TCP-Verbindung von den Admin-Knoten zu entweder `support.netapp.com` oder ein vom Kunden konfigurierter 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.

Wenn StorageGRID mithilfe der Standardroutingregeln keinen der bereitgestellten NTP- oder DNS-Server kontaktieren kann, versucht es automatisch, in allen Netzwerken (Grid, Admin und Client) Kontakt aufzunehmen, sofern die IP-Adressen der DNS- und NTP-Server angegeben sind. Wenn die NTP- oder DNS-Server in einem beliebigen Netzwerk erreichbar sind, erstellt StorageGRID automatisch zusätzliche Routing-Regeln, um sicherzustellen, dass dieses Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.

Obwohl Sie diese automatisch erkannten Hostrouten verwenden können, sollten Sie die DNS- und NTP-Routen im Allgemeinen manuell konfigurieren, um die Konnektivität sicherzustellen, falls die automatische Erkennung fehlschlägt.

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

Über VLAN-Schnittstellen werden nur S3-Clientverbindungen und SSH-, Grid Manager- und Tenant Manager-Verwaltungsverbindungen unterstützt. Ausgehende Verbindungen, beispielsweise 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.

Wide Area Networks (WANs) für mehrere Standorte

Bei der Konfiguration eines StorageGRID -Systems mit mehreren Standorten muss die WAN-Verbindung zwischen den Standorten eine Mindestbandbreite von 25 Mbit/Sekunde in jede Richtung aufweisen, bevor der Client-Verkehr berücksichtigt wird. Für die Datenreplikation oder Erasure Coding zwischen Standorten, die Erweiterung von Knoten oder Standorten, die Wiederherstellung von Knoten und andere Vorgänge oder Konfigurationen ist zusätzliche Bandbreite erforderlich.

Die tatsächlichen Mindestanforderungen an die WAN-Bandbreite hängen von der Clientaktivität und dem ILM-Schutzschema ab. Wenn Sie Hilfe bei der Schätzung der Mindestanforderungen für die WAN-Bandbreite

benötigen, wenden Sie sich an Ihren NetApp Professional Services-Berater.

Verbindungen für Admin-Knoten und Gateway-Knoten

Admin-Knoten müssen immer vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt werden. Sie müssen sicherstellen, dass kein nicht vertrauenswürdiger Client auf einen Admin-Knoten im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk zugreifen kann.

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

Verwenden der Netzwerkadressübersetzung (NAT)

Verwenden Sie keine Netzwerkadressübersetzung (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID Sites. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt geroutet werden können. Bei Bedarf können Sie jedoch NAT zwischen externen Clients und Grid-Knoten verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway-Knoten bereitzustellen. Die Verwendung von NAT zum Überbrücken eines öffentlichen Netzwerksegments wird nur unterstützt, wenn Sie eine Tunnelanwendung verwenden, die für alle Knoten im Grid transparent ist, d. h. die Grid-Knoten benötigen keine Kenntnis der öffentlichen IP-Adressen.

Netzwerkspezifische Anforderungen

Befolgen Sie die Anforderungen für jeden StorageGRID Netzwerktyp.

Netzwerk-Gateways und Router

- Wenn festgelegt, muss sich das Gateway für ein bestimmtes Netzwerk innerhalb des Subnetzes des jeweiligen Netzwerks befinden.
- Wenn Sie eine Schnittstelle mit statischer Adressierung konfigurieren, müssen Sie eine andere Gateway-Adresse als 0.0.0.0 angeben.
- Wenn Sie kein Gateway haben, empfiehlt es sich, die Gateway-Adresse auf die IP-Adresse der Netzwerkschnittstelle festzulegen.

Subnetze

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

Die folgenden Einschränkungen werden vom Grid Manager während der Bereitstellung erzwungen. Sie werden hier bereitgestellt, um bei der Netzwerkplanung vor der Bereitstellung zu helfen.

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

- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

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

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

- Das Grid-Netzwerk-Subnetz für jeden Knoten muss in der GNSL enthalten sein.
- Das Admin-Netzwerk-Subnetz darf sich nicht mit dem Grid-Netzwerk-Subnetz, dem Client-Netzwerk-Subnetz oder einem anderen Subnetz in der GNSL überschneiden.
- Die Subnetze in der AESL dürfen sich nicht mit Subnetzen in der GNSL überschneiden.
- Das Client-Netzwerk-Subnetz darf sich nicht mit dem Grid-Netzwerk-Subnetz, dem Admin-Netzwerk-Subnetz, einem anderen Subnetz in der GNSL oder einem anderen Subnetz in der AESL überschneiden.

Netznetzwerk

- Zum Zeitpunkt der Bereitstellung muss jeder Grid-Knoten an das Grid-Netzwerk angeschlossen sein und über die Netzwerkkonfiguration, die Sie bei der Bereitstellung des Knotens angeben, mit dem primären Admin-Knoten kommunizieren können.
- Während des normalen Netzbetriebs muss jeder Netzknoten in der Lage sein, über das Netznetzwerk mit allen anderen Netzknoten zu kommunizieren.

> Das Grid-Netzwerk muss zwischen den einzelnen Knoten direkt routebar sein. Die Netzwerkadressübersetzung (NAT) zwischen Knoten wird nicht unterstützt.

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, fügen Sie diese der Grid-Netzwerk-Subnetzliste (GNSL) hinzu. Für jedes Subnetz im GNSL werden auf allen Knoten statische Routen erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das native Trunk-VLAN das für den Grid-Netzwerkverkehr verwendete VLAN sein. Alle Grid-Knoten müssen über das native Trunk-VLAN zugänglich sein.

Admin-Netzwerk

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

Zu den typischen Verwendungszwecken des Admin-Netzwerks gehören Verwaltungsverbindungen, AutoSupport, KMS und Verbindungen zu kritischen Servern wie NTP, DNS und LDAP, wenn diese Verbindungen nicht über das Grid-Netzwerk oder das Client-Netzwerk bereitgestellt werden.

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

Sie müssen mindestens ein Subnetz im Admin-Netzwerk definieren, um eingehende Verbindungen von externen Subnetzen zu ermöglichen. Auf jedem Knoten werden für jedes Subnetz in der AESL automatisch statische Routen generiert.

Kundennetzwerk

Das Client-Netzwerk ist optional. Wenn Sie die Konfiguration eines Client-Netzwerks planen, beachten Sie die folgenden Überlegungen.

- Das Client-Netzwerk ist für die Unterstützung des Datenverkehrs von S3-Clients ausgelegt. Wenn konfiguriert, wird das Client-Netzwerk-Gateway zum Standard-Gateway des Knotens.
- Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur an explizit konfigurierten Load Balancer-Endpunkten akzeptieren. Sehen "Konfigurieren von Load Balancer-Endpunkten" .
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, überlegen Sie, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn dies konfiguriert ist, fließt der Client-Netzwerkverkehr über das native Trunk-VLAN, wie im Switch konfiguriert.

Ähnliche Informationen

"Knotennetzwerkkonfiguration ändern"

Bereitstellungsspezifische Netzwerküberlegungen

Linux-Bereitstellungen

Aus Gründen der Effizienz, Zuverlässigkeit und Sicherheit läuft das StorageGRID -System unter Linux als Sammlung von Container-Engines. Eine Container-Engine-bezogene Netzwerkkonfiguration ist in einem StorageGRID System nicht erforderlich.

Verwenden Sie für die Container-Netzwerkschnittstelle ein nicht gebundenes Gerät, z. B. ein VLAN oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Knotenkonfigurationsdatei an.

Verwenden Sie Bond- oder Bridge-Geräte nicht direkt als Container-Netzwerkschnittstelle. Dies könnte den Start des Knotens aufgrund eines Kernelproblems bei der Verwendung von Macvlan mit Bond- und Bridge-Geräten im Container-Namespace verhindern.

Siehe die Installationsanweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" Bereitstellungen.

Host-Netzwerkkonfiguration für Container-Engine-Bereitstellungen

Bevor Sie mit der StorageGRID -Bereitstellung auf einer Container-Engine-Plattform beginnen, legen Sie fest, welche Netzwerke (Grid, Admin, Client) jeder Knoten verwenden wird. Sie müssen sicherstellen, dass die Netzwerkschnittstelle jedes Knotens auf der richtigen virtuellen oder physischen Hostschnittstelle konfiguriert ist und dass jedes Netzwerk über ausreichend Bandbreite verfügt.

Physische Hosts

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

- Stellen Sie sicher, dass alle Hosts für jede Knotenschnittstelle dieselbe Hostschnittstelle verwenden. Diese Strategie vereinfacht die Hostkonfiguration und ermöglicht eine zukünftige Knotenmigration.
- Besorgen Sie sich eine IP-Adresse für den physischen Host selbst.

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

- Öffnen Sie die erforderlichen Ports zum Host.
- Wenn Sie VLAN-Schnittstellen in StorageGRID verwenden möchten, muss der Host über eine oder mehrere Trunk-Schnittstellen verfügen, die Zugriff auf die gewünschten VLANs bieten. Diese Schnittstellen können als eth0, eth2 oder als zusätzliche Schnittstellen an den Knotencontainer übergeben werden. Informationen zum Hinzufügen von Trunk- oder Zugriffsschnittstellen finden Sie im Folgenden:
  - **RHEL (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **RHEL, Ubuntu oder Debian (nach der Installation des Knotens)**:"Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen"

Empfehlungen zur Mindestbandbreite

Die folgende Tabelle enthält Empfehlungen zur minimalen LAN-Bandbreite für jeden StorageGRID Knotentyp und jeden Netzwerktyp. Sie müssen jedem physischen oder virtuellen Host eine ausreichende Netzwerkbandbreite bereitstellen, um die aggregierten Mindestbandbreitenanforderungen für die Gesamtzahl und den Typ der StorageGRID Knoten zu erfüllen, die Sie auf diesem Host ausführen möchten.

Knotentyp	**Netzwerktyp**		
	Netz	Administrator	Kunde
	Mindest-LAN-Bandbreite	Administrator	10 Gbit/s
1 Gbit/s	1 Gbit/s	Tor	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 nicht die SAN-Bandbreite, die für den Zugriff auf gemeinsam genutzten Speicher erforderlich ist. Wenn Sie gemeinsam genutzten Speicher verwenden, auf den über Ethernet (iSCSI oder FCoE) zugegriffen wird, sollten Sie auf jedem Host separate physische Schnittstellen bereitstellen, um ausreichend SAN-Bandbreite bereitzustellen. Um Engpässe zu vermeiden, sollte die SAN-Bandbreite für einen bestimmten Host in etwa der aggregierten Netzwerkbandbreite aller auf diesem Host ausgeführten Speicherknoten entsprechen.

Verwenden Sie die Tabelle, um die Mindestanzahl der auf jedem Host bereitzustellenden Netzwerkschnittstellen zu bestimmen, basierend auf der Anzahl und dem Typ der StorageGRID -Knoten, die Sie auf diesem Host ausführen möchten.

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

- Verbinden Sie das Grid und die Admin-Netzwerke auf dem Admin-Knoten (erfordert 10 + 1 = 11 Gbit/s)
- Verbinden Sie das Grid und die Client-Netzwerke mit dem Gateway-Knoten (erfordert 10 + 10 = 20 Gbit/s)
- Verbinden Sie das Grid-Netzwerk mit dem Speicherknoten (erfordert 10 Gbit/s)

In diesem Szenario sollten Sie mindestens 11 + 20 + 10 = 41 Gbit/s Netzwerkbandbreite bereitstellen. Diese kann durch zwei 40-Gbit/s-Schnittstellen oder fünf 10-Gbit/s-Schnittstellen erreicht werden, die möglicherweise zu Trunks zusammengefasst und dann von den drei oder mehr VLANs gemeinsam genutzt werden, die die Grid-, Admin- und Client-Subnetze lokal zum physischen Rechenzentrum mit dem Host übertragen.

Einige empfohlene Methoden zum Konfigurieren physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung Ihrer StorageGRID Bereitstellung finden Sie im Folgenden:

- "Konfigurieren des Hostnetzwerks (Red Hat Enterprise Linux)"
- "Konfigurieren Sie das Hostnetzwerk (Ubuntu oder Debian)."

Vernetzung und Ports für Plattformdienste und Cloud-Speicherpools

Wenn Sie StorageGRID -Plattformdienste oder Cloud Storage Pools verwenden möchten, müssen Sie Grid-Netzwerke und Firewalls konfigurieren, um sicherzustellen, dass die Zielendpunkte erreicht werden können.

Vernetzung für Plattformdienste

Wie beschrieben in"Plattformdienste für Mandanten verwalten" Und"Plattformdienste verwalten" Zu den Plattformdiensten gehören externe Dienste, die Suchintegration, Ereignisbenachrichtigung und CloudMirror-Replikation bereitstellen.

Plattformdienste erfordern Zugriff von Speicherknoten, die den StorageGRID ADC-Dienst hosten, auf die externen Dienstendpunkte. Beispiele für die Bereitstellung des Zugriffs sind:

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

Vernetzung für Cloud-Speicherpools

Cloud-Speicherpools erfordern außerdem Zugriff von Speicherknoten auf die Endpunkte, die vom verwendeten externen Dienst bereitgestellt werden, z. B. Amazon S3 Glacier oder Microsoft Azure Blob Storage. Weitere Informationen finden Sie unter"Was ist ein Cloud-Speicherpool?" .

Ports für Plattformdienste und Cloud Storage Pools

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

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

Beim Erstellen oder Bearbeiten des Endpunkts kann ein anderer Port angegeben werden. Sehen "Netzwerkportreferenz" .

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie außerdem"Konfigurieren der Speicherproxyeinstellungen" um das Senden von Nachrichten an externe Endpunkte zu ermöglichen, beispielsweise an einen Endpunkt im Internet.

VLANs und Plattformdienste und Cloud-Speicherpools

Sie können keine VLAN-Netzwerke für Plattformdienste oder Cloud-Speicherpools verwenden. Die Zielendpunkte müssen über das Grid-, Admin- oder Client-Netzwerk erreichbar sein.

Appliance-Knoten

Sie können die Netzwerkports auf StorageGRID -Geräten so konfigurieren, dass sie die Port-Bond-Modi verwenden, die Ihren Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

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

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

Informieren Sie sich über die Port-Bond-Modi für Ihr Gerät:

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

Netzwerkinstallation und -bereitstellung

Sie müssen verstehen, wie das Grid-Netzwerk und die optionalen Admin- und Client-Netzwerke während der Knotenbereitstellung und Grid-Konfiguration verwendet werden.

Erstmalige Bereitstellung eines Knotens

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

Ein Grid-Netzwerk mit konfiguriertem Gateway wird während der Bereitstellung zum Standard-Gateway für

einen Knoten. Das Standard-Gateway ermöglicht Grid-Knoten in separaten Subnetzen die Kommunikation mit dem primären Admin-Knoten, bevor das Grid konfiguriert wurde.

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

Automatische Knotenregistrierung mit primärem Admin-Knoten

Nachdem die Knoten bereitgestellt wurden, registrieren sie sich über das Grid-Netzwerk beim primären Admin-Knoten. Anschließend können Sie den Grid Manager, den `configure-storagegrid.py` Python-Skript oder die Installations-API zum Konfigurieren des Rasters und Genehmigen der registrierten Knoten. Während der Grid-Konfiguration können Sie mehrere Grid-Subnetze konfigurieren. Wenn Sie die Grid-Konfiguration abschließen, werden auf jedem Knoten statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway erstellt.

Deaktivieren des Admin-Netzwerks oder Client-Netzwerks

Wenn Sie das Admin-Netzwerk oder das Client-Netzwerk deaktivieren möchten, können Sie die Konfiguration während des Knotengenehmigungsprozesses entfernen oder nach Abschluss der Installation das Tool „IP ändern“ verwenden (siehe"Konfigurieren von IP-Adressen").

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Bereitstellung und Konfiguration des Grid-Knotens diese Richtlinien für DHCP-Adressierung und Netzwerkkonfigurationsänderungen.

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

  Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten.

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

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Sehen "Konfigurieren von IP-Adressen" .
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin-Knoten und anderen Grid-Knoten verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Netzwerkportreferenz

Interne Grid-Knoten-Kommunikation

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

NetApp empfiehlt, den ICMP-Verkehr (Internet Control Message Protocol) zwischen Grid-Knoten zu aktivieren. Das Zulassen von ICMP-Verkehr kann die Failover-Leistung verbessern, wenn ein Grid-Knoten nicht erreicht werden kann.

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

Richtlinien für Linux-basierte Knoten

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

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Richtlinien für VMware-basierte Knoten

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

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports neu zuordnen, wenn Sie Knoten mithilfe des VMware vSphere Web Client bereitstellen oder indem Sie bei der Automatisierung der Grid-Knotenbereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen zur Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter"Installieren Sie StorageGRID auf VMware" .

Richtlinien für Appliance-Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Sehen "Optional: Netzwerkports für das Gerät neu zuordnen" .

Interne StorageGRID Ports

Hafen	TCP oder UDP	Aus	Zu	Details
22	TCP	Primärer Admin-Knoten	Alle Knoten	Für Wartungsverfahren muss der primäre Admin-Knoten in der Lage sein, über SSH auf Port 22 mit allen anderen Knoten zu kommunizieren. Das Zulassen von SSH-Verkehr von anderen Knoten ist optional.
80	TCP	Geräte	Primärer Admin-Knoten	Wird von StorageGRID -Geräten verwendet, um mit dem primären Admin-Knoten zu kommunizieren und die Installation zu starten.

Hafen	TCP oder UDP	Aus	Zu	Details
123	UDP	Alle Knoten	Alle Knoten	Netzwerkzeitprotokolldienst. Jeder Knoten synchronisiert seine Zeit mit jedem anderen Knoten über NTP.
443	TCP	Alle Knoten	Primärer Admin-Knoten	Wird verwendet, um während der Installation und anderer Wartungsvorgänge den Status an den primären Admin-Knoten zu übermitteln.
1055	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
1139	TCP	Speicherknoten	Speicherknoten	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Knoten	Speicherknoten mit ADC	Berichterstellung, Prüfung und Konfiguration des internen Datenverkehrs.
1502	TCP	Alle Knoten	Speicherknoten	S3- und Swift-bezogener interner Datenverkehr.
1504	TCP	Alle Knoten	Admin-Knoten	NMS-Dienstberichterstattung und Konfiguration des internen Datenverkehrs.
1505	TCP	Alle Knoten	Admin-Knoten	AMS-Service-interner Verkehr.
1506	TCP	Alle Knoten	Alle Knoten	Serverstatus interner Datenverkehr.
1507	TCP	Alle Knoten	Gateway-Knoten	Interner Datenverkehr des Load Balancers.
1508	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr des Konfigurationsmanagements.
1511	TCP	Alle Knoten	Speicherknoten	Metadaten des internen Datenverkehrs.
5353	UDP	Alle Knoten	Alle Knoten	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.

Hafen	TCP oder UDP	Aus	Zu	Details
7001	TCP	Speicherknoten	Speicherknoten	Cassandra TLS-Clusterkommunikation zwischen Knoten.
7443	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Knoten	Appliance-Knoten	Interner Verkehr 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, Metriken und Netzwerkupdates.
10226	TCP	Speicherknoten	Primärer Admin-Knoten	Wird von StorageGRID -Geräten zum Weiterleiten von AutoSupport Paketen vom E-Series SANtricity System Manager an den primären Admin-Knoten verwendet.
10342	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
18000	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Datenverkehr des Kontodienstes.
18001	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Datenverkehr der Identity Federation.
18002	TCP	Admin-/Speicherknoten	Speicherknoten	Interner API-Verkehr im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Die Plattform bedient den internen Datenverkehr.

Hafen	TCP oder UDP	Aus	Zu	Details
18017	TCP	Admin-/Speicherknoten	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-/Speicherknoten	Speicherknoten	S3-bezogener interner Datenverkehr.
18083	TCP	Alle Knoten	Speicherknoten	Swift-bezogener interner Verkehr.
18086	TCP	Alle Knoten	Speicherknoten	Interner Verkehr im Zusammenhang mit dem LDR-Dienst.
18200	TCP	Admin-/Speicherknoten	Speicherknoten	Zusätzliche Statistiken zu Clientanfragen.
19000	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Verkehr des Keystone -Dienstes.

Ähnliche Informationen

"Externe Kommunikation"

Externe Kommunikation

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

Eingeschränkter Zugang zu Häfen

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, können Sie Folgendes tun:

- Verwenden"Load Balancer-Endpunkte" um den Zugriff auf benutzerdefinierte Ports zu ermöglichen.
- Ordnen Sie die Ports beim Bereitstellen von Knoten neu zu. Sie sollten die Endpunkte des Lastenausgleichs jedoch nicht neu zuordnen. Sehen Sie sich die Informationen zur Portneuzuordnung für Ihren StorageGRID Knoten an:
  - "Port-Neuzuordnungsschlüssel für StorageGRID unter Red Hat Enterprise Linux"
  - "Port-Neuzuordnungsschlüssel für StorageGRID unter Ubuntu oder Debian"

- "Ports für StorageGRID auf VMware neu zuordnen"
- "Optional: Netzwerkports für das Gerät neu zuordnen"

Für die externe Kommunikation verwendete Ports

Die folgende Tabelle zeigt die für den Datenverkehr in die Knoten verwendeten Ports.

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

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
22	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden.
25	TCP	SMTP	Admin-Knoten	E-Mail-Server	Wird für Warnungen und E-Mail-basierten AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 auf der Seite „E-Mail-Server“ überschreiben.
53	TCP/UDP	DNS	Alle Knoten	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Knoten	DHCP-Dienst	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient-Dienst wird für statisch konfigurierte Grids nicht ausgeführt.
68	UDP	DHCP	DHCP-Dienst	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-Knoten	Port 80 leitet für die Benutzeroberfläche des Admin-Knotens auf Port 443 um.
80	TCP	HTTP	Browser	Geräte	Port 80 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
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-Porteinstellung von 80 beim Erstellen eines Endpunkts überschreiben.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
80	TCP	HTTP	Speicherknoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTP verwenden. Grid-Administratoren können die Standard-HTTP-Porteinstellung von 80 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
111	TCP/UDP	RPCBind	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export (Portmap) verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
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-Polling verwendet. Alle Knoten stellen grundlegende Informationen bereit; Admin-Knoten stellen auch Warndaten bereit. Bei Konfiguration wird standardmäßig der UDP-Port 161 verwendet. **Hinweis:** Dieser Port ist nur erforderlich und wird nur in der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Knoten	Benachrichtigungsziele	Ausgehende SNMP-Benachrichtigungen und Traps werden standardmäßig an UDP-Port 162 gesendet. **Hinweis:** Dieser Port ist nur erforderlich, wenn SNMP aktiviert und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
389	TCP/UDP	LDAP	Speicherknoten mit ADC	Active Directory/LDAP	Wird zum Herstellen einer Verbindung mit einem Active Directory- oder LDAP-Server für die Identitätsföderation verwendet.
443	TCP	HTTPS	Browser	Admin-Knoten	Wird von Webbrowsern und Management-API-Clients verwendet, um auf den Grid Manager und den Tenant Manager zuzugreifen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.
443	TCP	HTTPS	Admin-Knoten	Active Directory	Wird von Admin-Knoten 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 Standard-HTTP-Porteinstellung 443 beim Erstellen eines Endpunkts überschreiben.
443	TCP	HTTPS	Speicherknoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTPS verwenden. Grid-Administratoren können die Standard-HTTPS-Porteinstellung 443 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
903	TCP	NFS	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export verwendet(`rpc.mountd`). **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
2022	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 22 anstelle von 2022 verwenden.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
2049	TCP	NFS	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export (NFS) verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
5353	UDP	mDNS	Alle Knoten	Alle Knoten	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
5696	TCP	KMIP	Gerät	KMS	Externer Datenverkehr des Key Management Interoperability Protocol (KMIP) von für die Knotenverschlüsselung konfigurierten Geräten zum Key Management Server (KMS), sofern auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer kein anderer Port angegeben ist.
8022	TCP	SSH	Service-Laptop	Alle Knoten	SSH auf Port 8022 gewährt Zugriff auf das Basisbetriebssystem auf Appliance- und virtuellen Knotenplattformen für Support und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare-Metal-)Knoten verwendet und muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
8443	TCP	HTTPS	Browser	Admin-Knoten	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
8443	TCP	HTTPS	Browser	Geräte	Wird von Webbrowsern und Verwaltungs-API-Clients verwendet, um auf das StorageGRID Appliance Installer zuzugreifen. **Hinweis**: Port 443 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
9022	TCP	SSH	Service-Laptop	Geräte	Gewährt Zugriff auf StorageGRID -Geräte im Vorkonfigurationsmodus für Support und Fehlerbehebung. Dieser Port muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
9091	TCP	HTTPS	Externer Grafana-Dienst	Admin-Knoten	Wird von externen Grafana-Diensten für den sicheren Zugriff auf den StorageGRID Prometheus-Dienst verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der zertifikatsbasierte 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 standardmäßige Kafka-Porteinstellung von 9092 beim Erstellen eines Endpunkts überschreiben.
9443	TCP	HTTPS	Browser	Admin-Knoten	Optional. Wird von Webbrowsern und Verwaltungs-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen.
18082	TCP	HTTPS	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18083	TCP	HTTPS	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18084	TCP	HTTP	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTP).
18085	TCP	HTTP	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTP).

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
23000-23999	TCP	HTTPS	Alle Knoten im Quellgrid für die Cross-Grid-Replikation	Admin-Knoten und Gateway-Knoten im Ziel-Grid für die Cross-Grid-Replikation	Dieser Portbereich ist für Grid-Föderation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden denselben Port.

Schnellstart für StorageGRID

Befolgen Sie diese allgemeinen Schritte, um ein beliebiges StorageGRID -System zu konfigurieren und zu verwenden.

1 Lernen, planen und Daten sammeln

Arbeiten Sie mit Ihrem NetApp Kundenbetreuer zusammen, um die Optionen zu verstehen und Ihr neues StorageGRID -System zu planen. Stellen Sie sich folgende Fragen:

- Wie viele Objektdaten werden Sie voraussichtlich zunächst und im Laufe der Zeit speichern?
- Wie viele Standorte benötigen Sie?
- Wie viele und welche Arten von Knoten benötigen Sie an jedem Standort?
- Welche StorageGRID Netzwerke werden Sie verwenden?
- Wer wird Ihr Raster zum Speichern von Objekten verwenden? Welche Anwendungen werden sie verwenden?
- Haben Sie besondere Sicherheits- oder Lageranforderungen?
- Müssen Sie gesetzliche oder behördliche Anforderungen erfüllen?

Optional können Sie mit Ihrem NetApp Professional Services-Berater zusammenarbeiten, um auf das NetApp ConfigBuilder-Tool zuzugreifen und eine Konfigurationsarbeitsmappe für die Installation und Bereitstellung Ihres neuen Systems auszufüllen. Sie können dieses Tool auch verwenden, um die Konfiguration beliebiger StorageGRID Geräte zu automatisieren. Sehen "Automatisieren Sie die Installation und Konfiguration von Geräten" .

Rezension"Erfahren Sie mehr über StorageGRID" und die"Netzwerkrichtlinien" .

2 Knoten installieren

Ein StorageGRID -System besteht aus einzelnen hardware- und softwarebasierten Knoten. Sie installieren zunächst die Hardware für jeden Appliance-Knoten und konfigurieren jeden Linux- oder VMware-Host.

Um die Installation abzuschließen, installieren Sie die StorageGRID -Software auf jedem Gerät oder

Softwarehost und verbinden die Knoten zu einem Grid. In diesem Schritt geben Sie Site- und Knotennamen, Subnetzdetails und die IP-Adressen für Ihre NTP- und DNS-Server an.

Erfahren Sie, wie:

- "Installieren der Appliance-Hardware"
- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

3 Sign in und Systemintegrität prüfen

Sobald Sie den primären Admin-Knoten installiert haben, können Sie sich beim Grid Manager anmelden. Von dort aus können Sie den allgemeinen Zustand Ihres neuen Systems überprüfen, AutoSupport und Warn-E-Mails aktivieren und S3-Endpunktdomänennamen einrichten.

Erfahren Sie, wie:

- "Sign in"
- "Überwachen Sie den Systemzustand"
- "Konfigurieren Sie AutoSupport"
- "E-Mail-Benachrichtigungen für Warnmeldungen einrichten"
- "Konfigurieren von S3-Endpunktdomänennamen"

4 Konfigurieren und Verwalten

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

Erfahren Sie, wie:

- "Steuern Sie den StorageGRID Zugriff"
- "Verwenden Sie den S3-Setup-Assistenten"
- "Verwenden des FabricPool -Setup-Assistenten"
- "Verwalten der Sicherheit"
- "Systemhärtung"

5 Einrichten von ILM

Sie steuern die Platzierung und Dauer jedes Objekts in Ihrem StorageGRID -System, indem Sie eine ILM-Richtlinie (Information Lifecycle Management) konfigurieren, die aus einer oder mehreren ILM-Regeln besteht. Die ILM-Regeln weisen StorageGRID an, wie Kopien von Objektdaten erstellt und verteilt und wie diese Kopien im Laufe der Zeit verwaltet werden.

Erfahren Sie, wie:"Objekte mit ILM verwalten"

6 Verwenden Sie StorageGRID

Nachdem die Erstkonfiguration abgeschlossen ist, können StorageGRID Mandantenkonten S3-Clientanwendungen verwenden, um Objekte aufzunehmen, abzurufen und zu löschen.

Erfahren Sie, wie:

- "Verwenden eines Mandantenkontos"
- "Verwenden Sie die S3 REST API"

7 Überwachen und Fehler beheben

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

Erfahren Sie, wie:

- "StorageGRID überwachen"
- "Fehlerbehebung bei StorageGRID"

8 Erweitern, pflegen und wiederherstellen

Sie können Knoten oder Sites hinzufügen, um die Kapazität oder Funktionalität Ihres Systems zu erweitern. Sie können auch verschiedene Wartungsverfahren durchführen, um Fehler zu beheben oder Ihr StorageGRID -System auf dem neuesten Stand und effizient zu halten.

Erfahren Sie, wie:

- "Erweitern eines Rasters"
- "Pflegen Sie Ihr Netz"
- "Knoten wiederherstellen"