



Weitere Informationen zu StorageGRID

StorageGRID

NetApp
March 12, 2025

Inhalt

Weitere Informationen zu StorageGRID	1
Was ist StorageGRID?	1
Vorteile von StorageGRID	2
Hybrid Clouds mit StorageGRID	3
Cloud-Storage-Pools	3
S3-Plattform-Services	3
ONTAP Daten-Tiering mit FabricPool	3
StorageGRID Architektur und Netzwerktopologie	4
Implementierungstopologien	4
Systemarchitektur	6
Grid Nodes und Services	8
Grid Nodes und Services	8
Was ist ein Admin-Node?	11
Was ist ein Storage-Node?	13
Was ist ein Gateway Node?	19
Was ist ein Archivknoten?	20
Managen von Daten mit StorageGRID	20
Was ist ein Objekt	20
Das Leben eines Objekts	22
Datenfluss aufnehmen	23
Verwaltung von Kopien	24
Abrufen des Datenflusses	26
Löschen des Datenflusses	27
Informationslebenszyklus-Management	29
Entdecken Sie StorageGRID	31
Entdecken Sie den Grid Manager	31
Entdecken Sie den Tenant Manager	37

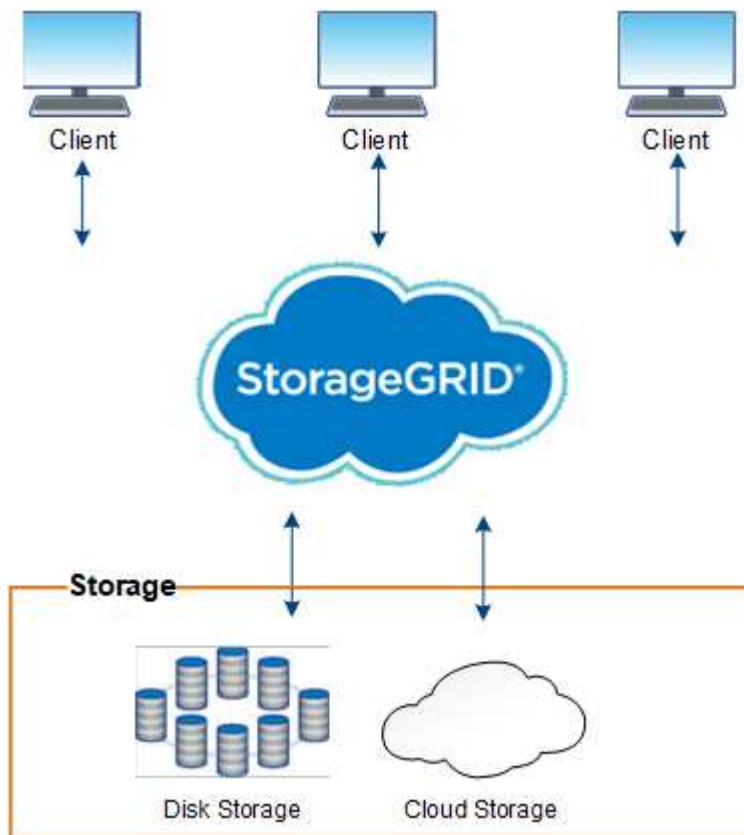
Weitere Informationen zu StorageGRID

Was ist StorageGRID?

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

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

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



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

Vorteile von StorageGRID

Das StorageGRID System bietet unter anderem folgende Vorteile:

- Extrem skalierbar und leicht zu verwendende Daten-Repositorys mit geografisch verteilten Standorten für unstrukturierte Daten
- Standard-Objekt-Storage-Protokolle:
 - Amazon Web Services Simple Storage Service (S3)
 - OpenStack Swift



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

- Hybrid Cloud-fähig: Richtlinienbasiertes Information Lifecycle Management (ILM) speichert Objekte in Public Clouds, einschließlich Amazon Web Services (AWS) und Microsoft Azure. StorageGRID Plattform-Services ermöglichen die Content-Replizierung, Ereignisbenachrichtigung und Metadatenuche von Objekten, die in Public Clouds gespeichert sind.
- Flexible Datensicherung für Langlebigkeit und Verfügbarkeit Die Daten lassen sich durch Replizierung und ein mehrstufiges Erasure Coding zur Fehlerkorrektur sichern. Überprüfung von Daten im Ruhezustand und auf der Übertragungsstrecke sorgt für Integrität für langfristige Aufbewahrung.
- Dynamisches Lifecycle Management für Daten zum Management der Storage-Kosten Sie können ILM-Regeln erstellen, die den Daten-Lebenszyklus auf Objektebene managen und Datenlokalität, Datenaufbewahrungszeit, Performance, Kosten anpassen. und Aufbewahrungszeit.
- Hochverfügbarkeit des Daten-Storage und einiger Managementfunktionen, mit integriertem Lastausgleich zur Optimierung der Datenlast über StorageGRID-Ressourcen hinweg.
- Unterstützung mehrerer Storage-Mandantenkonten, um die auf dem System gespeicherten Objekte durch unterschiedliche Einheiten zu trennen
- Zahlreiche Tools für das Monitoring des Systemzustands des StorageGRID Systems, einschließlich eines umfassenden Alarmsystems, einer grafischen Konsole und detaillierten Status für alle Knoten und Standorte
- Support für Software- oder hardwarebasierte Implementierung Sie können StorageGRID auf einer der folgenden Methoden implementieren:
 - Virtual Machines in VMware ausgeführt.
 - Container-Engines auf Linux Hosts
 - Speziell entwickelte StorageGRID Appliances
 - Storage Appliances bieten Objekt-Storage.
 - Services Appliances stellen Services für die Grid-Administration und den Lastausgleich bereit.
- Erfüllen der relevanten Speicheranforderungen dieser Vorschriften:
 - Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), die Börsenmitglieder, Broker oder Händler regelt.
 - Financial Industry Regulatory Authority (FINRA) Rule 4511(c), die die Format- und Medienanforderungen der SEC Rule 17a-4(f) vorgibt.
 - Commodity Futures Trading Commission (CFTC) in der Verordnung 17 CFR § 1.31(c)-(d), die den Handel mit Commodity Futures regelt.
- Unterbrechungsfreie Upgrades und Wartungsvorgänge Zugriff auf Inhalte bleibt während Upgrades,

Erweiterungen, Stilllegen und Wartungsarbeiten erhalten.

- Verbundenes Identitätsmanagement. Integration in Active Directory, OpenLDAP oder Oracle Directory Service zur Benutzerauthentifizierung. Unterstützt Single Sign-On (SSO) unter Verwendung des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen StorageGRID und Active Directory Federation Services (AD FS).

Hybrid Clouds mit StorageGRID

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

Cloud-Storage-Pools

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

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



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

S3-Plattform-Services

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

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

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

ONTAP Daten-Tiering mit FabricPool

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

Im Gegensatz zu manuellen Tiering-Lösungen senkt FabricPool durch das Automatisieren von Daten-Tiering die Gesamtbetriebskosten, um die Storage-Kosten zu senken. Durch Tiering in Public und Private Clouds einschließlich StorageGRID profitieren Sie von den Vorteilen der Wirtschaftlichkeit der Cloud.

Verwandte Informationen

- ["Was ist Cloud-Storage-Pool?"](#)
- ["Management von Plattform-Services"](#)
- ["Konfigurieren Sie StorageGRID für FabricPool"](#)

StorageGRID Architektur und Netzwerktopologie

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

Siehe ["Beschreibungen der Grid-Node-Typen"](#).

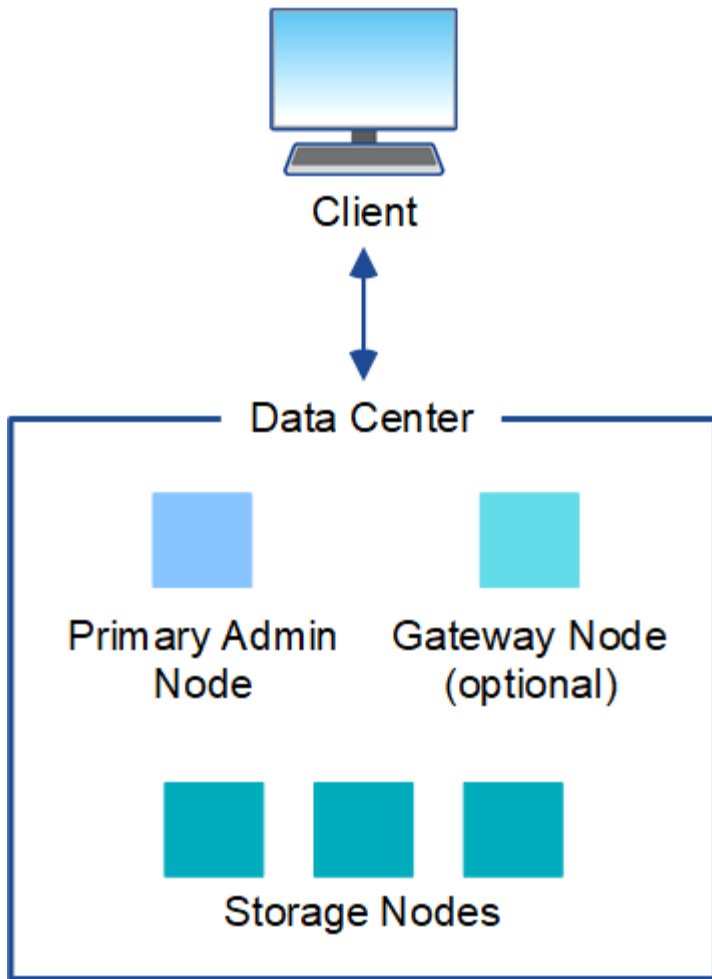
Weitere Informationen über die StorageGRID-Netzwerktopologie, -Anforderungen und -Netzkommunikation finden Sie im ["Netzwerkrichtlinien"](#).

Implementierungstopologien

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

Ein Standort

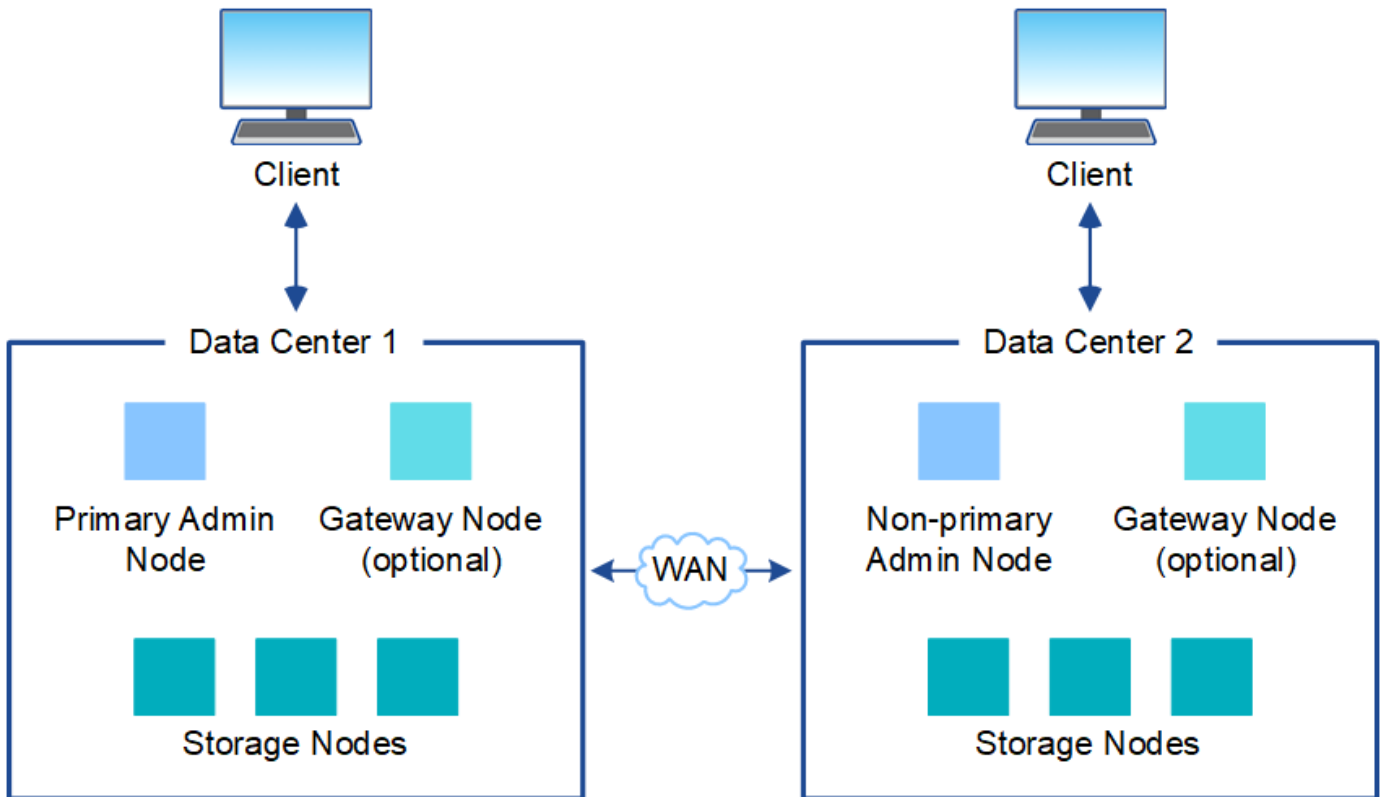
Bei einer Implementierung über einen einzigen Standort werden die Infrastruktur und der Betrieb des StorageGRID Systems zentralisiert.



Mehrere Standorte

In einer Implementierung mit mehreren Standorten können an jedem Standort unterschiedliche Typen und eine unterschiedliche Anzahl von StorageGRID Ressourcen installiert werden. So könnte beispielsweise mehr Storage für ein Datacenter als für ein anderes erforderlich sein.

Unterschiedliche Standorte befinden sich häufig an geografischen Standorten über unterschiedliche Ausfall-Domains, wie z. B. Erdbebenfehlerleitungen oder Überschwemmungsgebiete. Die Daten-Sharing und Disaster Recovery werden durch die automatische Verteilung der Daten an andere Standorte realisiert.



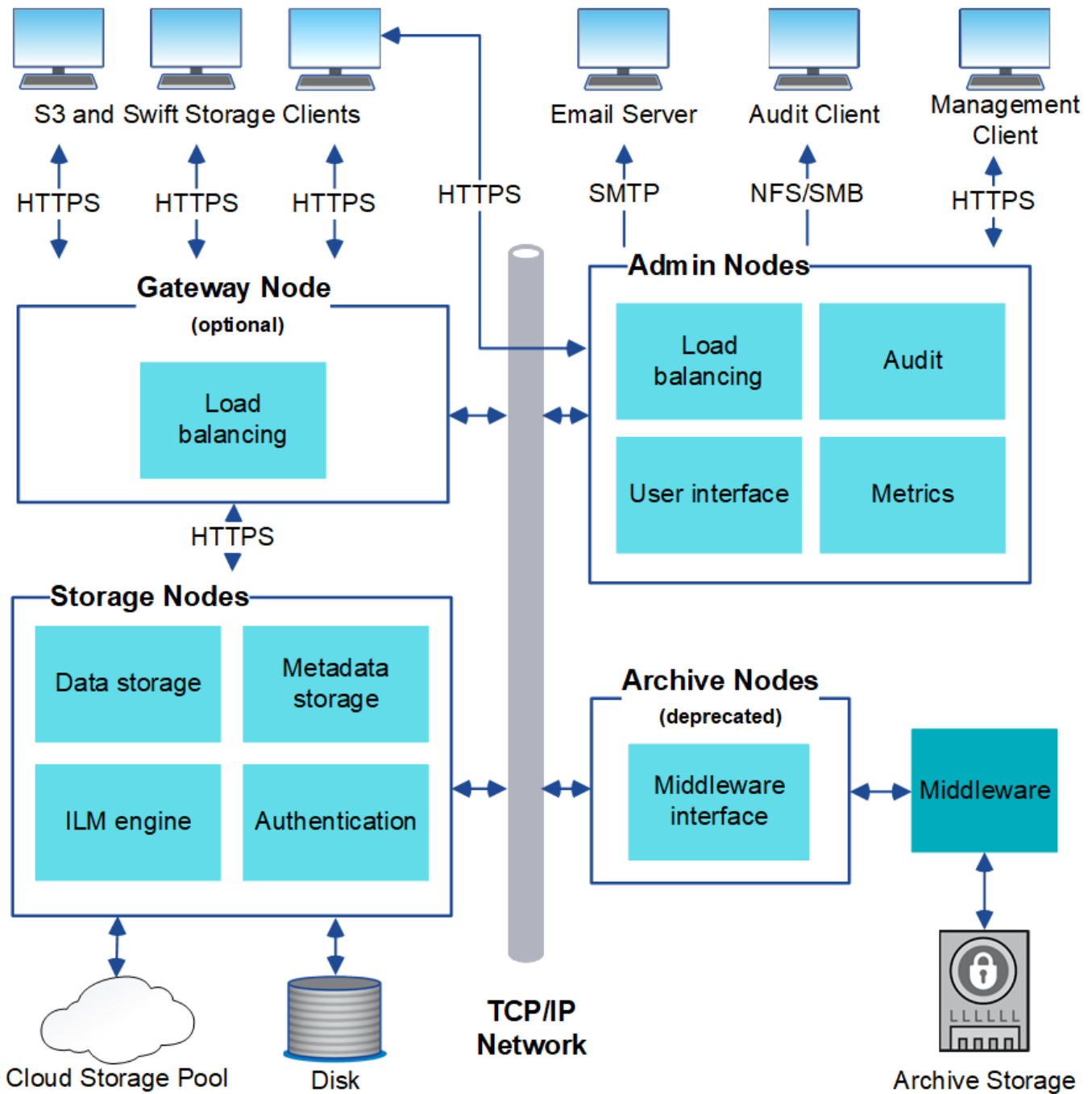
Darüber hinaus können mehrere logische Standorte innerhalb eines einzigen Datacenters eingesetzt werden, um die Verfügbarkeit und Ausfallsicherheit durch verteilte Replizierung und Erasure Coding zu verbessern.

Redundanz des Grid-Nodes

Bei einer Implementierung an einem Standort oder an mehreren Standorten können Sie optional mehrere Admin-Nodes oder Gateway-Nodes enthalten, um Redundanz zu gewährleisten. Sie können beispielsweise mehr als einen Admin-Node an einem einzelnen Standort oder an mehreren Standorten installieren. Allerdings kann jedes StorageGRID System nur einen primären Admin-Node haben.

Systemarchitektur

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



S3 Clients speichern Objekte in StorageGRID und rufen sie ab. Andere Clients werden verwendet, um E-Mail-Benachrichtigungen zu senden, auf die StorageGRID-Managementoberfläche zuzugreifen und optional auf die Audit-Freigabe zuzugreifen.

S3-Clients können eine Verbindung zu einem Gateway-Node oder einem Admin-Node herstellen, um die Load-Balancing-Schnittstelle zu Storage-Nodes zu verwenden. Alternativ können S3-Clients über HTTPS eine direkte Verbindung zu Storage-Nodes herstellen.

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

Grid Nodes und Services

Grid Nodes und Services

Der grundlegende Baustein eines StorageGRID Systems ist der Grid-Node. Nodes enthalten Services. Dies sind Softwaremodule, die einen Grid-Node mit einem Satz von Funktionen ausstatten.

Typen von Grid-Nodes

Das StorageGRID System nutzt vier Typen von Grid-Nodes:

Admin-Nodes

Bereitstellen von Managementservices wie Systemkonfiguration, Monitoring und Protokollierung Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Jedes Grid muss über einen primären Admin-Node verfügen und möglicherweise über zusätzliche nicht-primäre Admin-Nodes für Redundanz verfügen. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID-Systems an. Wartungsverfahren müssen jedoch mit dem primären Admin-Node durchgeführt werden.

Admin-Nodes können auch zum Lastausgleich für S3-Client-Traffic verwendet werden.

Siehe ["Was ist ein Admin-Node?"](#)

Storage-Nodes

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

Siehe ["Was ist ein Storage-Node?"](#)

Gateway-Nodes (optional)

Stellen Sie eine Schnittstelle für den Lastausgleich bereit, über die Client-Anwendungen eine Verbindung zu StorageGRID herstellen können. Ein Load Balancer leitet die Clients nahtlos an einen optimalen Storage Node weiter, sodass der Ausfall von Nodes oder sogar einem gesamten Standort transparent ist.

Siehe ["Was ist ein Gateway Node?"](#)

Hardware- und Software-Nodes

StorageGRID Nodes können als StorageGRID-Appliance-Nodes oder als softwarebasierte Nodes implementiert werden.

StorageGRID Appliance-Nodes

StorageGRID Hardware-Appliances wurden speziell für den Einsatz in einem StorageGRID System entwickelt. Einige Geräte können als Storage-Nodes verwendet werden. Andere Appliances können als Admin-Nodes oder Gateway-Nodes verwendet werden. Die Appliance-Nodes können mit softwarebasierten Nodes kombiniert oder vollständig entwickelten Appliance-Grids ohne Abhängigkeiten von externen Hypervisoren, Storage- oder Computing-Hardware implementiert werden.

Im Folgenden erfahren Sie mehr über die verfügbaren Appliances:

- ["StorageGRID Appliance-Dokumentation"](#)

- ["NetApp Hardware Universe"](#)

Softwarebasierte Nodes

Softwarebasierte Grid-Nodes können als VMware Virtual Machines oder in Container-Engines auf einem Linux-Host implementiert 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 auf Ubuntu oder Debian"](#).

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

Bei der Erstinstallation eines neuen softwarebasierten Storage-Knotens können Sie angeben, dass er nur für verwendet werden ["Speichern von Metadaten"](#)soll.

StorageGRID Services

Nachfolgend finden Sie eine vollständige Liste der StorageGRID Services.

Service	Beschreibung	Standort
Kontendienst-Forwarder	Stellt eine Schnittstelle für den Load Balancer-Service bereit, über die der Kontodienst auf Remote-Hosts abgefragt werden kann, und informiert über Änderungen bei der Konfiguration des Load Balancer-Endpunkts am Load Balancer-Service.	Load Balancer-Service auf Admin-Nodes und Gateway-Nodes
ADC (Administrative Domain Controller)	Verwaltet Topologiedaten, bietet Authentifizierungsservices und reagiert auf Anfragen aus den LDR- und CMN-Diensten.	Mindestens drei Storage Nodes, die den ADC-Dienst an jedem Standort enthalten
AMS (Audit Management System)	Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textdatei.	Admin-Nodes
Cassandra Reaper	Führt automatische Reparaturen von Objektmetadaten durch.	Storage-Nodes
Chunk-Service	Verwaltet Erasure-codierte Daten und Paritätsfragmente.	Storage-Nodes
CMN (Knoten für die Konfigurationsverwaltung)	Management systemweiter Konfigurationen und Grid-Aufgaben Jedes Grid hat einen CMN-Dienst.	Primärer Admin-Node

Service	Beschreibung	Standort
DDS (Distributed Data Store)	Schnittstellen zur Cassandra-Datenbank zum Management von Objektmetadaten	Storage-Nodes
DMV (Data Mover)	Verschiebt Daten in Cloud-Endpunkte	Storage-Nodes
Dynamische IP (dynap)	Überwacht das Raster auf dynamische IP-Änderungen und aktualisiert lokale Konfigurationen.	Alle Nodes
Grafana	Wird für die Darstellung von Kennzahlen im Grid Manager verwendet.	Admin-Nodes
Hochverfügbarkeit	Verwaltet virtuelle Hochverfügbarkeits-IPs auf Knoten, die auf der Seite „Hochverfügbarkeitsgruppen“ konfiguriert sind. Dieser Service wird auch als „Keepalived Service“ bezeichnet.	Admin- und Gateway-Nodes
Identität (idnt)	Föderiert Benutzeridentitäten von LDAP und Active Directory	Storage-Nodes, die den ADC-Dienst verwenden
Lambda-Schiedsrichter	Verwalten von S3 Select SelectObjectContent Requests.	Alle Nodes
Load Balancer (nginx-gw)	Bietet Lastausgleich für S3-Datenverkehr von Clients zu Storage-Nodes. Der Lastverteilungsservice kann über die Konfigurationsseite Load Balancer Endpoints konfiguriert werden. Dieser Service wird auch als nginx-gw-Service bezeichnet.	Admin- und Gateway-Nodes
LDR (Local Distribution Router)	Verwaltet die Speicherung und Übertragung von Inhalten innerhalb des Grids.	Storage-Nodes
MISCd Information Service Control Daemon	Stellt eine Schnittstelle zum Abfragen und Managen von Services auf anderen Nodes sowie zum Managen von Umgebungskonfigurationen auf dem Node bereit, beispielsweise zum Abfragen des Status von Services, die auf anderen Nodes ausgeführt werden.	Alle Nodes

Service	Beschreibung	Standort
Nginx	Fungiert als Authentifizierungs- und sicherer Kommunikationsmechanismus für verschiedene Grid Services (wie Prometheus und Dynamic IP), der die Möglichkeit zur Kommunikation mit Services auf anderen Knoten über HTTPS-APIs ermöglicht.	Alle Nodes
Nginx-gw	Schaltet den Lastverteilungsservice ein.	Admin- und Gateway-Nodes
NMS (Network Management System)	Gibt die Überwachungs-, Berichterstellungs- und Konfigurationsoptionen an, die über den Grid Manager angezeigt werden.	Admin-Nodes
Persistenz	Verwaltet Dateien auf dem Root-Laufwerk, die über einen Neustart bestehen müssen.	Alle Nodes
Prometheus	Erfasst Zeitreihungskennzahlen von Services auf allen Knoten.	Admin-Nodes
RSM (Replicated State Machine)	Stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden.	Storage-Nodes, die den ADC-Dienst verwenden
SSM (Server Status Monitor)	Überwacht Hardwarebedingungen und Berichte an den NMS-Service.	Auf jedem Grid-Node ist eine Instanz vorhanden
Trace-Kollektor	Führt eine Trace-Erfassung durch, um Informationen für den technischen Support zu sammeln. Der Trace Collector-Dienst verwendet die Open-Source-Jaeger-Software.	Admin-Nodes

Was ist ein Admin-Node?

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

Unterschiede zwischen primären und nicht primären Admin-Nodes

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

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

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

Administratorknoten des bevorzugten Absenders

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

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

In den folgenden Fällen können mehrere Benachrichtigungen gesendet werden:

- Wenn Admin-Knoten voneinander „islanded“ werden, versuchen sowohl der bevorzugte Sender als auch der Standby-Sender, Benachrichtigungen zu senden, und es können mehrere Kopien von

Benachrichtigungen empfangen werden.

- Wenn der Standby-Sender Probleme mit dem bevorzugten Sender erkennt und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Sender möglicherweise wieder Benachrichtigungen senden. In diesem Fall können doppelte Benachrichtigungen gesendet werden. Der Standby-Sender hört auf, Benachrichtigungen zu senden, wenn Fehler auf dem bevorzugten Sender nicht mehr erkannt werden.



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

Primäre Dienste für Admin-Nodes

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

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

Was ist ein Storage-Node?

Storage-Nodes managen und speichern Objektdaten und Metadaten. Storage-Nodes umfassen die Services und Prozesse, die zum Speichern, Verschieben, Überprüfen und

Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind.

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

Typen von Storage-Nodes

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

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

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

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



Sie können den Typ nach Abschluss der Installation des Storage-Node nicht mehr ändern.

Storage Node für Daten und Metadaten (kombiniert)

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

Storage-Node nur für Metadaten

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

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

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

Standorts mindestens den vorhandenen StorageGRID Standorten entsprechen, und neue Standortressourcen sollten den Storage-Nodes an den vorhandenen StorageGRID Standorten entsprechen.

Bei der Installation von nur Metadaten Nodes muss das Grid zudem eine Mindestanzahl an Nodes für den Storage enthalten:

- Konfigurieren Sie für ein Grid mit einem Standort mindestens zwei kombinierte oder reine Storage-Nodes.
- Konfigurieren Sie für ein Grid mit mehreren Standorten mindestens einen kombinierten oder nur-Daten-Storage-Node *pro Standort*.



Obwohl reine Metadaten-Storage-Nodes S3-Client-Anforderungen enthalten [LDR-Service](#) und verarbeiten können, erhöht sich die StorageGRID-Performance möglicherweise nicht.

Rein datenrein Storage-Node

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

Bei der Installation von reinen Datenknoten muss das Grid Folgendes enthalten:

- Mindestens zwei kombinierte oder rein datengeschützte Storage Nodes *pro Grid*
- Mindestens ein kombinierter oder nur-Daten-Storage Node *pro Standort*
- Mindestens drei kombinierte oder nur Metadaten-Storage-Nodes *pro Standort*

Primäre Services für Storage-Nodes

Die folgende Tabelle enthält die primären Services für Storage-Nodes. In dieser Tabelle werden jedoch nicht alle Node-Services aufgeführt.



Einige Services, wie z. B. der ADC-Service und der RSM-Service, bestehen in der Regel nur auf drei Storage-Nodes an jedem Standort.

Service	Tastenfunktion
Konto (Konto)	Management von Mandantenkonten.

Service	Tastenfunktion
Administrativer Domänen-Controller (ADC)	<p data-bbox="472 155 1159 191">Aufrechterhaltung der Topologie und Grid-Konfiguration</p> <p data-bbox="472 222 1333 258">Hinweis: Reine Daten-Speicher-Nodes hosten den ADC-Dienst nicht.</p> <p data-bbox="472 289 565 325">Details</p> <div data-bbox="472 331 1487 1514" style="border: 1px solid #ccc; padding: 10px;"> <p data-bbox="505 363 1382 464">Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen miteinander. Der ADC-Dienst wird auf mindestens drei Storage Nodes an einem Standort gehostet.</p> <p data-bbox="505 499 1451 772">Der ADC-Dienst verwaltet Topologiedaten, einschließlich Standort und Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden muss, kontaktiert er einen ADC-Service, um den besten Grid-Knoten für die Bearbeitung seiner Anforderung zu finden. Darüber hinaus behält der ADC-Service eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung bei, sodass jeder Grid-Node aktuelle Konfigurationsinformationen abrufen kann.</p> <p data-bbox="505 804 1430 940">Zur Erleichterung von verteilten und isanded-Operationen synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Services und Topologie mit den anderen ADC-Diensten im StorageGRID-System.</p> <p data-bbox="505 972 1442 1213">Im Allgemeinen unterhalten alle Rasterknoten eine Verbindung zu mindestens einem ADC-Dienst. So wird sichergestellt, dass die Grid-Nodes immer auf die neuesten Informationen zugreifen. Wenn sich Grid-Nodes verbinden, werden die Zertifikate anderer Grid-Nodes zwischengespeichert, sodass die Systeme mit bekannten Grid-Nodes weiterarbeiten können, selbst wenn ein ADC-Dienst nicht verfügbar ist. Neue Grid-Knoten können nur Verbindungen über einen ADC-Dienst herstellen.</p> <p data-bbox="505 1245 1451 1486">Durch die Verbindung jedes Grid-Knotens kann der ADC-Service Topologiedaten erfassen. Die Informationen zu diesem Grid-Node umfassen die CPU-Last, den verfügbaren Festplattenspeicher (wenn der Storage vorhanden ist), unterstützte Services und die Standort-ID des Grid-Node. Andere Dienste fragen den ADC-Service nach Topologiedaten durch Topologieabfragen. Der ADC-Dienst reagiert auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID-System empfangen wurden.</p> </div>
Cassandra	<p data-bbox="472 1562 976 1598">Speichert und sichert Objekt-Metadaten.</p> <p data-bbox="472 1629 1414 1665">Hinweis: Reine Daten-Storage-Nodes hosten den Cassandra-Service nicht.</p>
Cassandra Reaper	<p data-bbox="472 1709 1235 1745">Führt automatische Reparaturen von Objektmetadaten durch.</p> <p data-bbox="472 1776 1442 1843">Hinweis: Reine Daten-Storage-Nodes hosten den Cassandra Reaper-Service nicht.</p>
Chunk	<p data-bbox="472 1892 1175 1927">Verwaltet Erasure-codierte Daten und Paritätsfragmente.</p>

Service	Tastenfunktion
Data Mover (dmv)	Verschiebt Daten in Cloud-Storage-Pools
Verteilter Datenspeicher (DDS)	<p>Überwacht Objekt-Metadaten-Storage</p> <p>Details</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Jeder Storage Node umfasst den Distributed Data Store (DDS)-Service. Dieser Service ist mit der Cassandra-Datenbank verbunden, um Hintergrundaufgaben für die im StorageGRID-System gespeicherten Objektmetadaten auszuführen.</p> <p>Der DDS-Service verfolgt die Gesamtanzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtanzahl der über die unterstützten Schnittstellen (S3) des Systems aufgenommenen Objekte.</p> </div>
Identität (idnt)	Föderiert Benutzeridentitäten von LDAP und Active Directory

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

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

Was ist ein Gateway Node?

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

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

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

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

Primäre Dienste für Gateway-Nodes

In der folgenden Tabelle werden die primären Services für Gateway Nodes aufgeführt. In dieser Tabelle werden jedoch nicht alle Node-Services aufgeführt.

Service	Tastenfunktion
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. Hinweis: dieser Service befindet sich auch auf Admin Nodes.
Lastausgleich	Ermöglicht Layer-7-Lastausgleich für S3-Datenverkehr von Clients zu Storage-Nodes. Dies ist der empfohlene Lastausgleichmechanismus. Hinweis: dieser Service befindet sich auch auf Admin Nodes.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Replikation ist nicht konfigurierbar und wird automatisch ausgeführt. Weitere Informationen finden Sie unter ["Management von Objekt-Metadaten-Storage"](#).

Was ist ein Archivknoten?

Unterstützung für Archive Nodes wurde entfernt.

Informationen zu Archivknoten finden Sie unter "[Was ist ein Archiv-Node \(StorageGRID 11.8-Dokumentstandort\)?](#)".

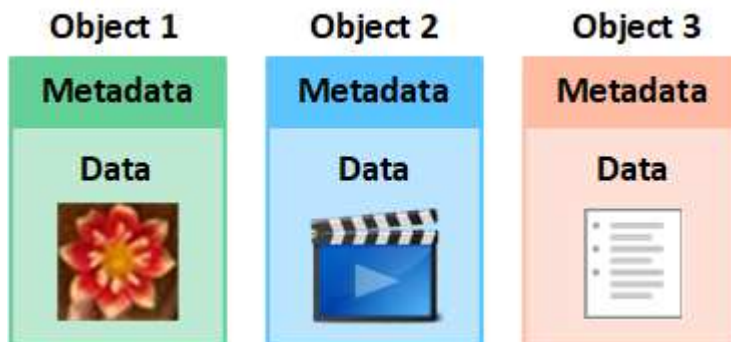
Managen von Daten mit StorageGRID

Was ist ein Objekt

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

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

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



Was sind Objektdaten?

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

Was sind Objekt-Metadaten?

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

Objektmetadaten enthalten Informationen wie die folgenden:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), dem Objektnamen, dem Namen des S3-Buckets oder Swift-Containers, dem Mandanten-Kontonamen oder -ID, der logischen Größe des Objekts, dem Datum und der Uhrzeit der ersten Erstellung des Objekts und Datum und Uhrzeit der letzten Änderung des Objekts.
- Der aktuelle Speicherort der einzelnen Objektkopien oder Fragmente, deren Löschen codiert wurde
- Alle dem Objekt zugeordneten Benutzer-Metadaten.

Objektmetadaten sind individuell anpassbar und erweiterbar und bieten dadurch Flexibilität für die Nutzung von Applikationen.

Detaillierte Informationen darüber, wie und wo StorageGRID Objektmetadaten speichert, finden Sie unter ["Management von Objekt-Metadaten-Storage"](#).

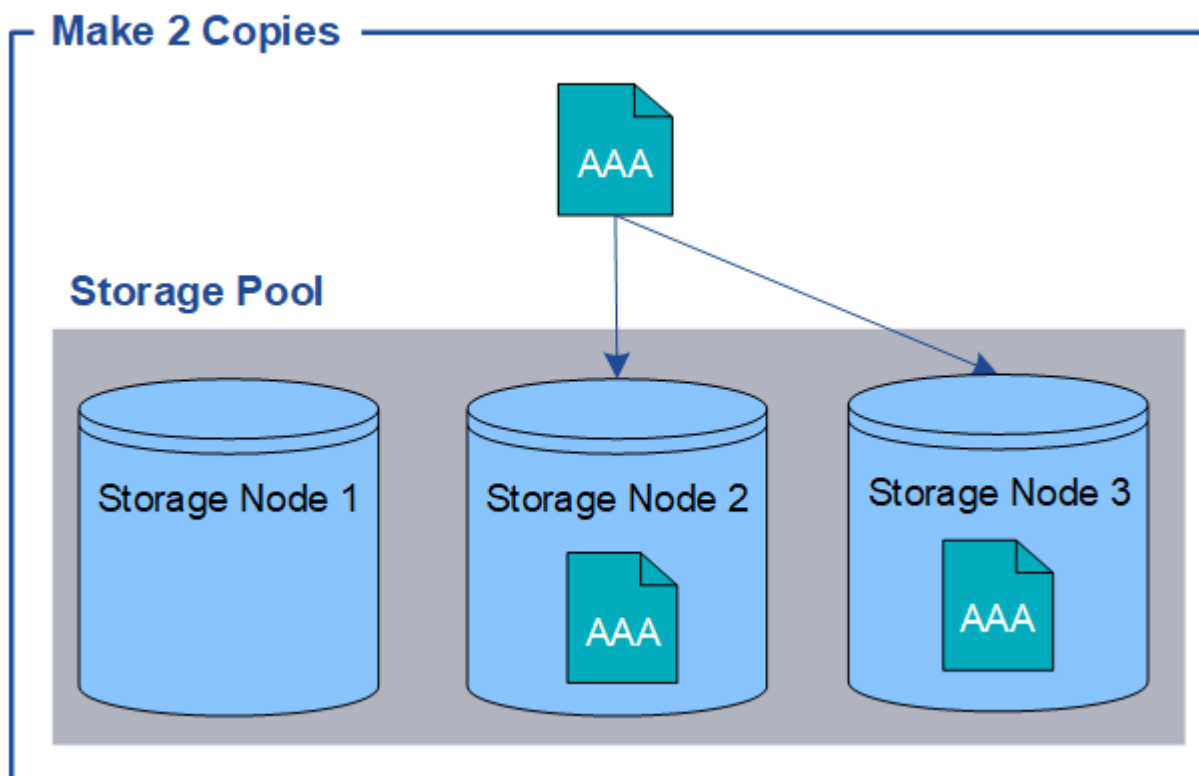
Wie werden Objektdaten gesichert?

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

Replizierung

Wenn StorageGRID Objekte einer ILM-Regel (Information Lifecycle Management) zuordnet, die zum Erstellen replizierter Kopien konfiguriert ist, erstellt das System exakte Kopien von Objektdaten und speichert diese auf Storage-Nodes oder Cloud Storage Pools. ILM-Regeln bestimmen die Anzahl der Kopien, die erstellt werden, wo diese Kopien gespeichert werden und wie lange sie vom System aufbewahrt werden. Falls eine Kopie verloren geht, beispielsweise aufgrund des Verlusts eines Storage-Nodes, ist das Objekt nach wie vor verfügbar, wenn eine Kopie davon an einer anderen Stelle im StorageGRID System vorhanden ist.

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

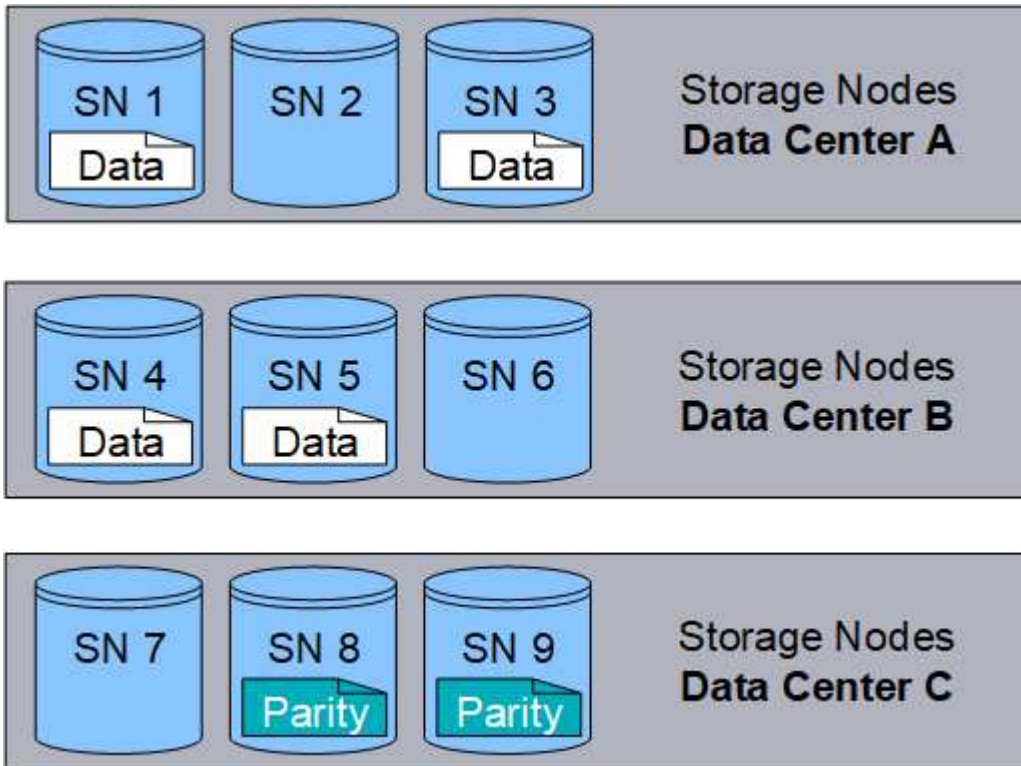


Erasure Coding

Wenn StorageGRID Objekte mit einer ILM-Regel übereinstimmt, die zur Erstellung von mit Datenkonsistenz versehenen Kopien konfiguriert ist, werden Objektdaten in Datenfragmente zerlegt, zusätzliche Paritätsfragmente berechnet und jedes Fragment auf einem anderen Storage Node gespeichert. Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Daten oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zum Erasure Coding diese Fragmente mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente neu erstellen. Das verwendete

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

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



Verwandte Informationen

- ["Objektmanagement mit ILM"](#)
- ["Verwenden Sie das Information Lifecycle Management"](#)

Das Leben eines Objekts

Das Leben eines Objekts besteht aus verschiedenen Etappen. Jede Phase stellt die Vorgänge dar, die mit dem Objekt auftreten.

Der Lebenszyklus eines Objekts umfasst das Aufnehmen, das Kopieren-Management, das Abrufen und Löschen von Objekten.

- **Ingest:** Der Prozess einer S3-Client-Anwendung, die ein Objekt über HTTP im StorageGRID-System speichert. In dieser Phase beginnt das StorageGRID-System mit der Verwaltung des Objekts.
- **Copy-Management:** Management replizierter und mit Erasure-Coded-Kopien in StorageGRID, wie in den ILM-Regeln der aktiven ILM-Richtlinien beschrieben. Während der Phase des Copy-Managements schützt StorageGRID Objektdaten vor Verlust, indem die angegebene Anzahl und der Typ der Objektkopien auf Storage Nodes oder in einem Cloud-Storage-Pool erstellt und aufrechterhalten wird.
- **Retrieve:** Der Prozess einer Client-Anwendung, die auf ein vom StorageGRID-System gespeichertes Objekt zugreift. Der Client liest das Objekt, das aus einem Storage Node oder Cloud Storage Pool abgerufen wird.

- **Löschen:** Der Vorgang, bei dem alle Objektkopien aus dem Raster entfernt werden. Objekte können entweder gelöscht werden, wenn eine Client-Applikation eine Löschanfrage an das StorageGRID System sendet, oder infolge eines automatischen Prozesses, der StorageGRID nach Ablauf der Nutzungsdauer des Objekts durchführt.



Verwandte Informationen

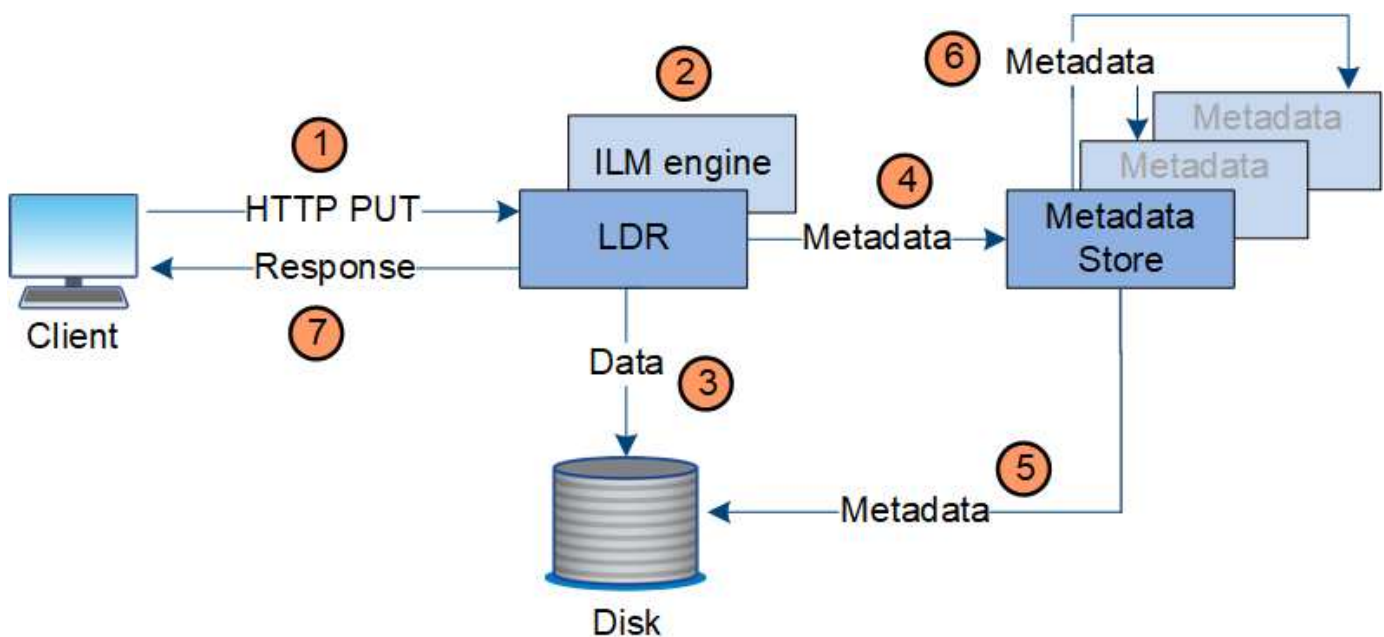
- ["Objektmanagement mit ILM"](#)
- ["Verwenden Sie das Information Lifecycle Management"](#)

Datenfluss aufnehmen

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

Datenfluss

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



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

4. Der LDR-Service sendet die Objektmetadaten an den Metadatenpeicher.
5. Der Metadaten-Speicher speichert die Objekt-Metadaten auf der Festplatte.
6. Der Metadatenpeicher überträgt Kopien von Objektmetadaten an andere Storage-Nodes. Diese Kopien werden auch auf der Festplatte gespeichert.
7. Der LDR-Dienst gibt eine HTTP 200 OK-Antwort an den Client zurück, um zu bestätigen, dass das Objekt aufgenommen wurde.

Verwaltung von Kopien

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

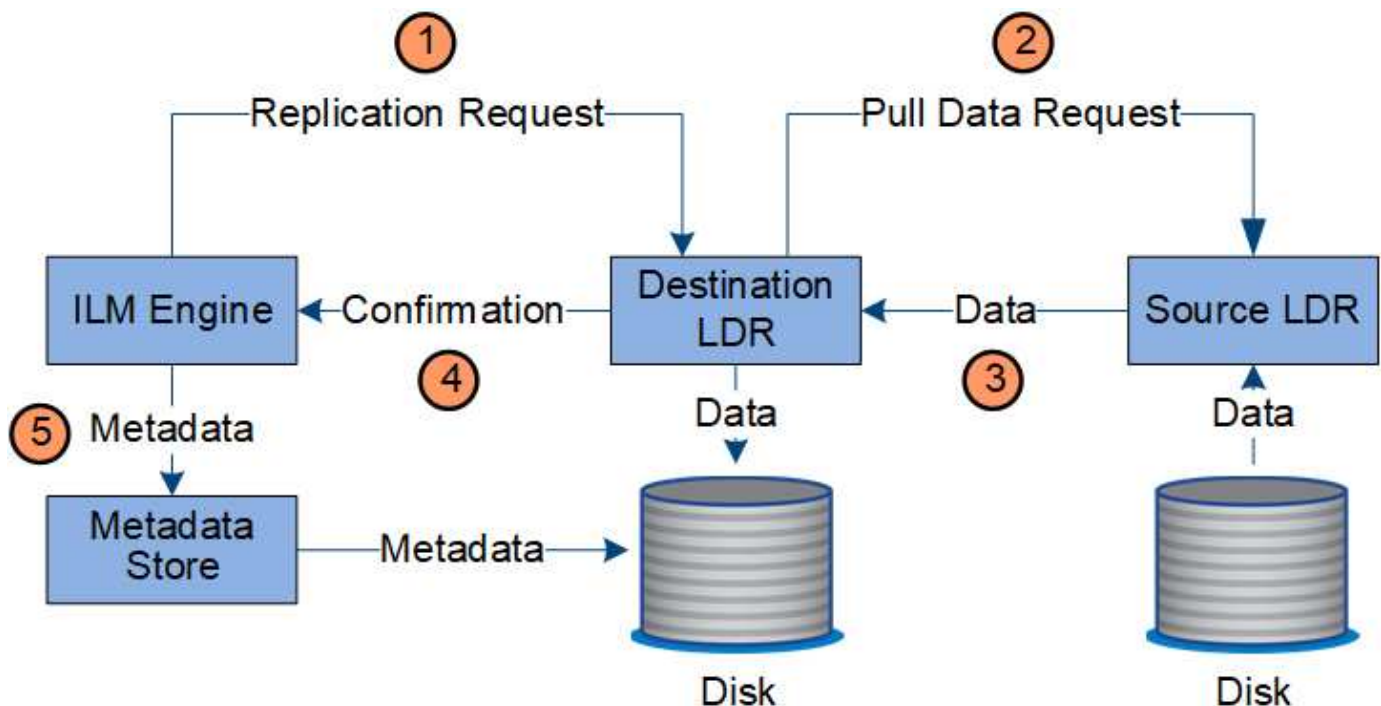
Unterschiedliche Typen und Standorte von Objektkopien können zu unterschiedlichen Zeiten der Lebensdauer des Objekts erforderlich sein. ILM-Regeln werden regelmäßig überprüft, um sicherzustellen, dass Objekte nach Bedarf platziert werden.

Objektdaten werden vom LDR-Service gemanagt.

Content-Schutz: Replikation

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

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



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

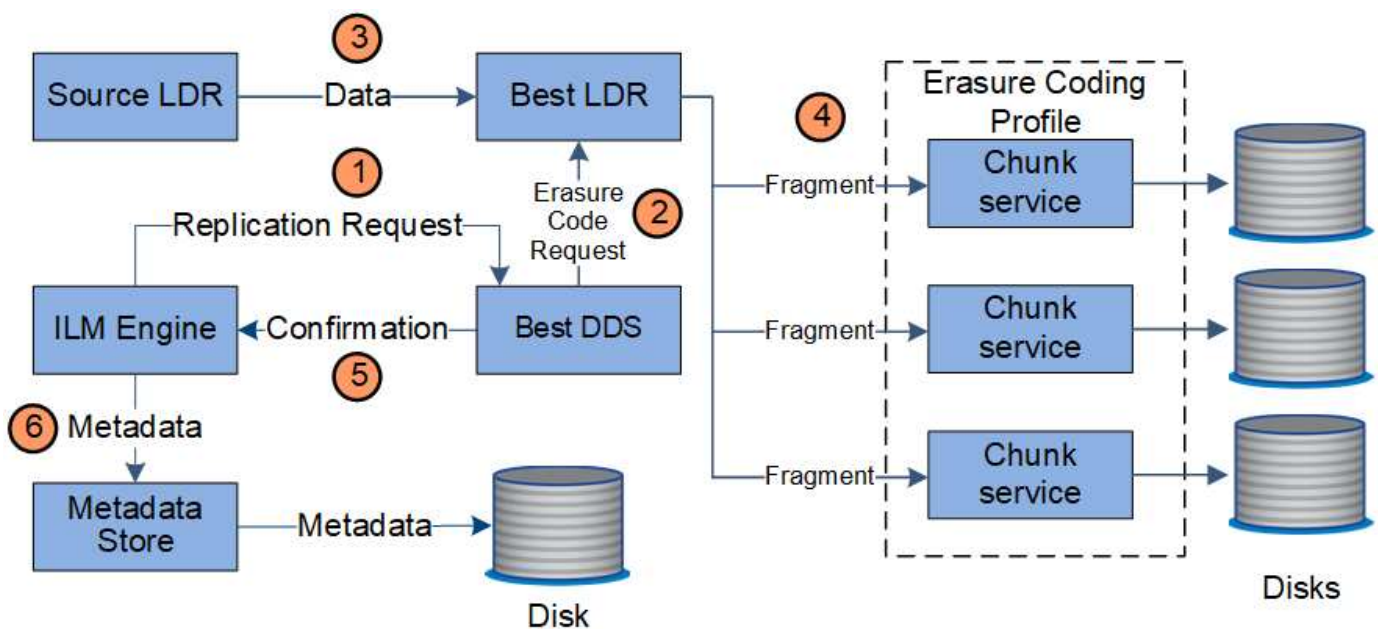
Replikation zu initiieren.

2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellspeicherort ab. Anschließend sendet er eine Replikationsanfrage an den Quell-LDR-Service.
3. Der Quell-LDR-Service sendet eine Kopie an den Ziel-LDR-Service.
4. Der Ziel-LDR-Service benachrichtigt die ILM Engine, dass die Objektdaten gespeichert wurden.
5. Die ILM-Engine aktualisiert den Metadatenpeicher mit Objektspeichermetadaten.

Content Protection: Erasure Coding

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

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



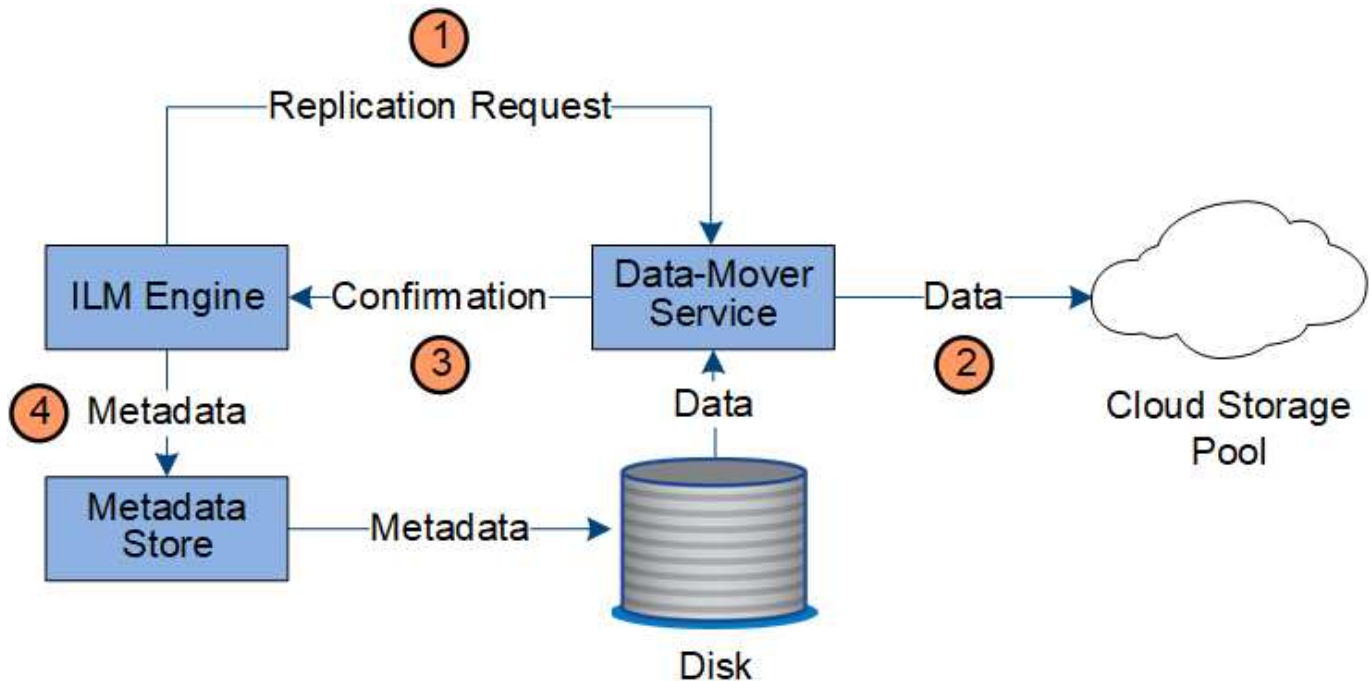
1. Die ILM-Engine fragt den ADC-Service ab, um zu bestimmen, welcher DDS-Service den Erasure Coding-Vorgang am besten ausführen kann. Wenn festgestellt, sendet die ILM-Engine eine „Initiierung“-Anforderung an diesen Service.
2. Der DDS-Dienst weist ein LDR an, den Code der Objektdaten zu löschen.
3. Der Quell-LDR-Service sendet eine Kopie an den für das Erasure Coding ausgewählten LDR-Service.
4. Nach der Erstellung der entsprechenden Anzahl von Parität und Datenfragmenten verteilt der LDR-Service diese Fragmente auf die Storage Nodes (Chunk-Services), aus denen der Speicherpool des Erasure-Coding-Profiles besteht.
5. Der LDR-Service benachrichtigt die ILM-Engine und bestätigt, dass Objektdaten erfolgreich verteilt werden.
6. Die ILM-Engine aktualisiert den Metadatenpeicher mit Objektspeichermetadaten.

Content-Sicherung: Cloud Storage Pool

Wenn für die Anweisungen zur Content-Platzierung einer ILM-Regel eine replizierte Kopie von Objektdaten in einem Cloud Storage-Pool gespeichert wird, werden Objektdaten in den externen S3-Bucket oder Azure Blob-

Storage-Container dupliziert, der für den Cloud Storage-Pool angegeben wurde.

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



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

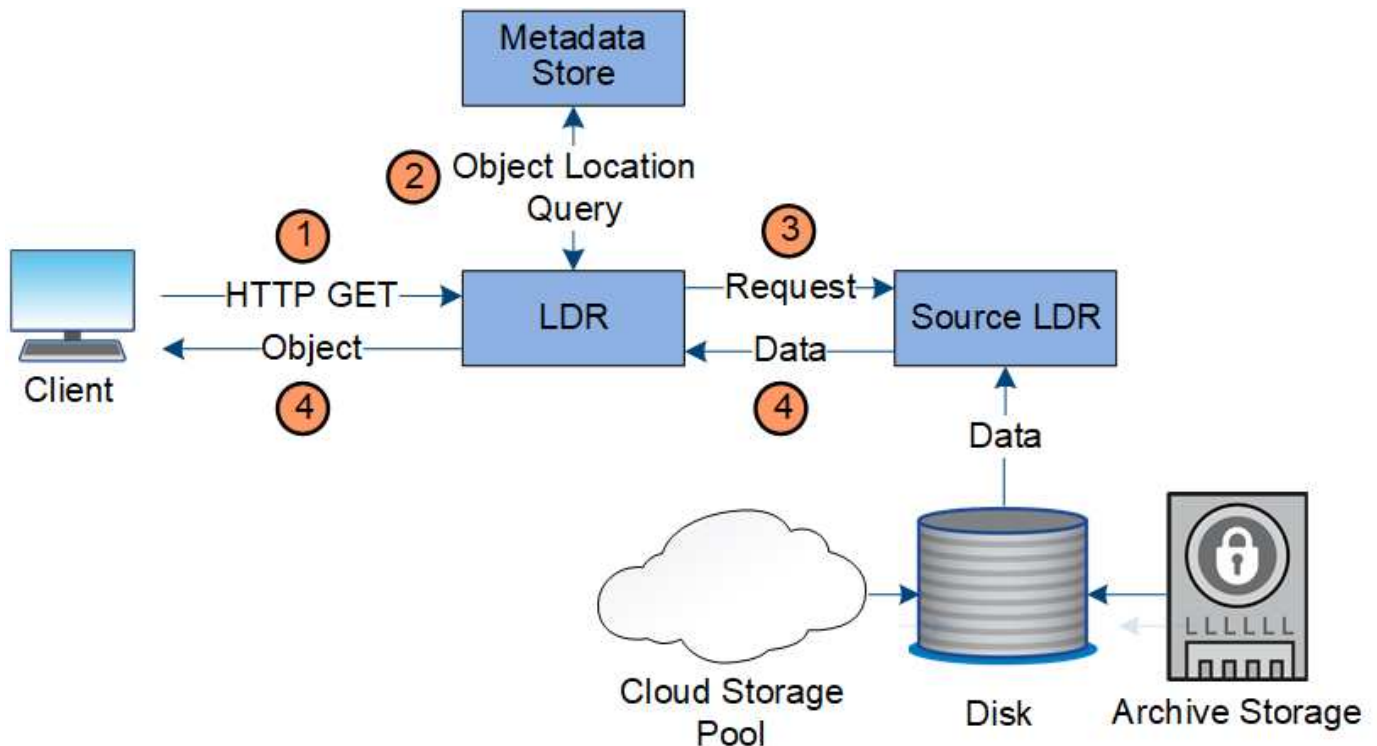
Abrufen des Datenflusses

Ein Abrufvorgang besteht aus einem definierten Datenfluss zwischen dem StorageGRID-System und dem Client. Das System verwendet Attribute, um den Abruf des Objekts von einem Storage Node oder, falls erforderlich, einem Cloud-Storage-Pool nachzuverfolgen.

Der LDR-Service des Storage Node fragt den Metadatenpeicher nach dem Speicherort der Objektdaten ab und ruft ihn vom Quell-LDR-Service ab. Bevorzugt wird der Abruf von einem Storage Node durchgeführt. Wenn das Objekt auf einem Storage-Node nicht verfügbar ist, wird die Abrufanforderung an einen Cloud-Speicherpool weitergeleitet.



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



1. Der LDR-Service erhält eine Abrufanforderung von der Client-Anwendung.
2. Der LDR-Service fragt den Metadatenpeicher nach dem Objektdatenstandort und den Metadaten ab.
3. Der LDR-Service leitet die Abfrage an den Quell-LDR-Service weiter.
4. Der Quell-LDR-Dienst gibt die Objektdaten aus dem abgefragten LDR-Dienst zurück und das System gibt das Objekt an die Client-Anwendung zurück.

Löschen des Datenflusses

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

Löschhierarchie

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

- **S3 Object Lock:** Wenn die globale S3 Object Lock-Einstellung für das Grid aktiviert ist, können S3-Clients Buckets mit aktivierter S3-Objektsperre erstellen und dann über die S3-REST-API Aufbewahrungseinstellungen für jede Objektversion festlegen, die diesem Bucket hinzugefügt wurde.
 - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.
 - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
 - Objekte in Buckets mit aktivierter S3 Objektsperre werden von ILM „ewig“ aufbewahrt. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder

den Ablauf des Bucket-Lebenszyklus gelöscht werden.

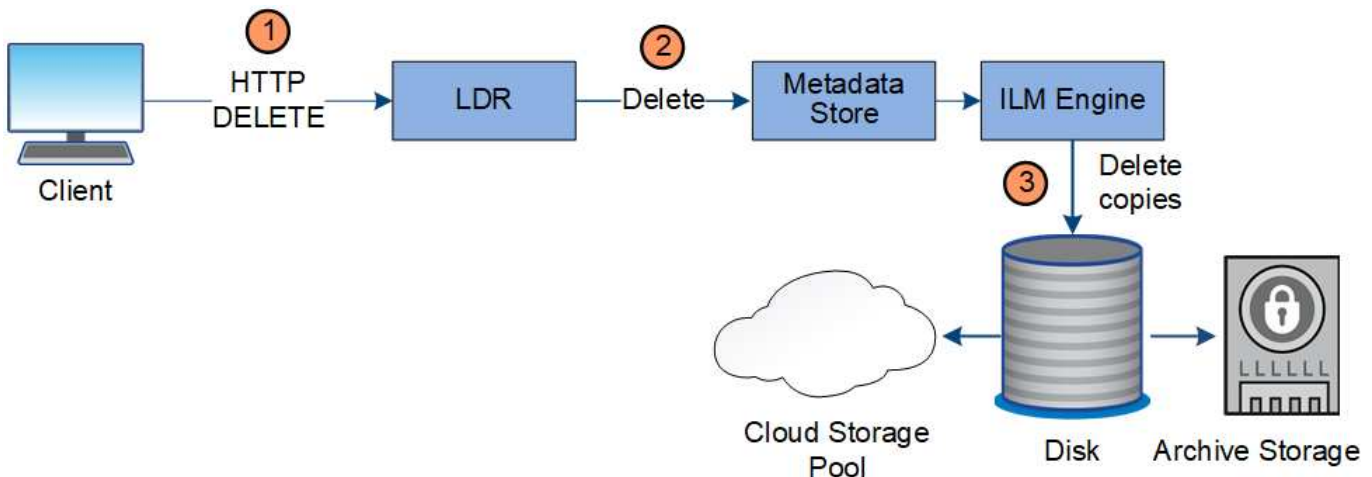
- Wenn S3-Clients ein Standarddatum für die Aufbewahrung bis auf den Bucket anwenden, müssen sie für jedes Objekt kein „bis zur Aufbewahrung“ angeben.
- **Client delete Request:** Ein S3-Client kann eine delete-Objekt-Anfrage ausgeben. Wenn ein Client ein Objekt löscht, werden alle Kopien des Objekts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



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

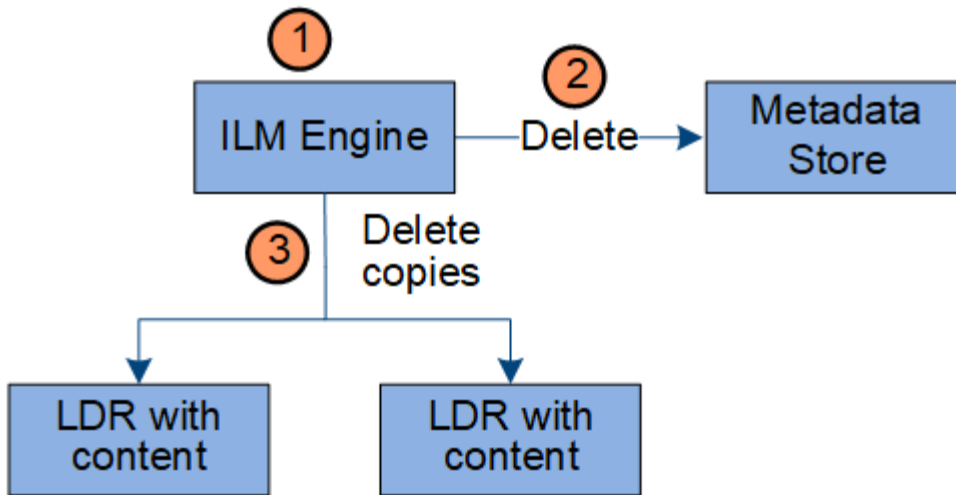
Weitere Informationen finden Sie unter ["So werden Objekte gelöscht"](#) .

Datenfluss für Clientlöschungen



1. Der LDR-Dienst erhält eine Löschanforderung von der Client-Anwendung.
2. Der LDR-Service aktualisiert den Metadatenpeicher, sodass das Objekt auf die Client-Anforderungen gelöscht wird, und weist die ILM-Engine an, alle Kopien von Objektdaten zu entfernen.
3. Das Objekt wurde aus dem System entfernt. Der Metadatenpeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Datenfluss für ILM-Löschungen



1. Die ILM-Engine legt fest, dass das Objekt gelöscht werden muss.
2. Die ILM-Engine benachrichtigt den Metadatenpeicher. Der Metadatenpeicher aktualisiert Objektmetadaten, sodass das Objekt auf Client-Anforderungen gelöscht aussieht.
3. Die ILM-Engine entfernt alle Kopien des Objekts. Der Metadatenpeicher wird aktualisiert, um Objektmetadaten zu entfernen.

Informationslebenszyklus-Management

Mithilfe von Information Lifecycle Management (ILM) können Sie die Platzierung, Dauer und das Aufnahmeverhalten für alle Objekte im StorageGRID System steuern. ILM-Regeln legen fest, wie StorageGRID Objekte im Laufe der Zeit speichert. Sie konfigurieren eine oder mehrere ILM-Regeln und fügen sie anschließend zu einer ILM-Richtlinie hinzu.

Ein Raster verfügt jeweils nur über eine aktive Richtlinie. Eine Richtlinie kann mehrere Regeln enthalten.

ILM-Regeln definieren:

- Welche Objekte sollten gespeichert werden. Eine Regel kann auf alle Objekte angewendet werden, oder Sie können Filter angeben, um zu identifizieren, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder Swift-Containern oder bestimmten Metadatenwerten verbunden sind.
- Speichertyp und -Standort. Objekte können auf Storage-Nodes oder in Cloud-Speicherpools gespeichert werden.
- Der Typ der Objektkopien, die erstellt wurden. Kopien können repliziert oder zur Fehlerkorrektur codiert werden.
- Für replizierte Kopien die Anzahl der Kopien, die erstellt werden.
- Für Kopien, die nach Erasure Coding codiert wurden, wird das Verfahren zur Fehlerkorrektur verwendet.
- Die Änderungen im Laufe der Zeit an dem Storage-Standort und den Koprototypen eines Objekts.
- Schutz von Objektdaten bei Aufnahme von Objekten in das Grid (synchrone Platzierung oder Dual-Commit)

Objekt-Metadaten werden nicht durch ILM-Regeln gemanagt. Stattdessen werden Objekt-Metadaten in einer Cassandra-Datenbank in einem sogenannten Metadaten-Speicher gespeichert. Drei Kopien von Objekt-

Metadaten werden automatisch an jedem Standort aufbewahrt, um die Daten vor Verlust zu schützen.

Beispiel für eine ILM-Regel

Eine ILM-Regel könnte beispielsweise Folgendes angeben:

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

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

Bewertung von Objekten durch eine ILM-Richtlinie

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

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

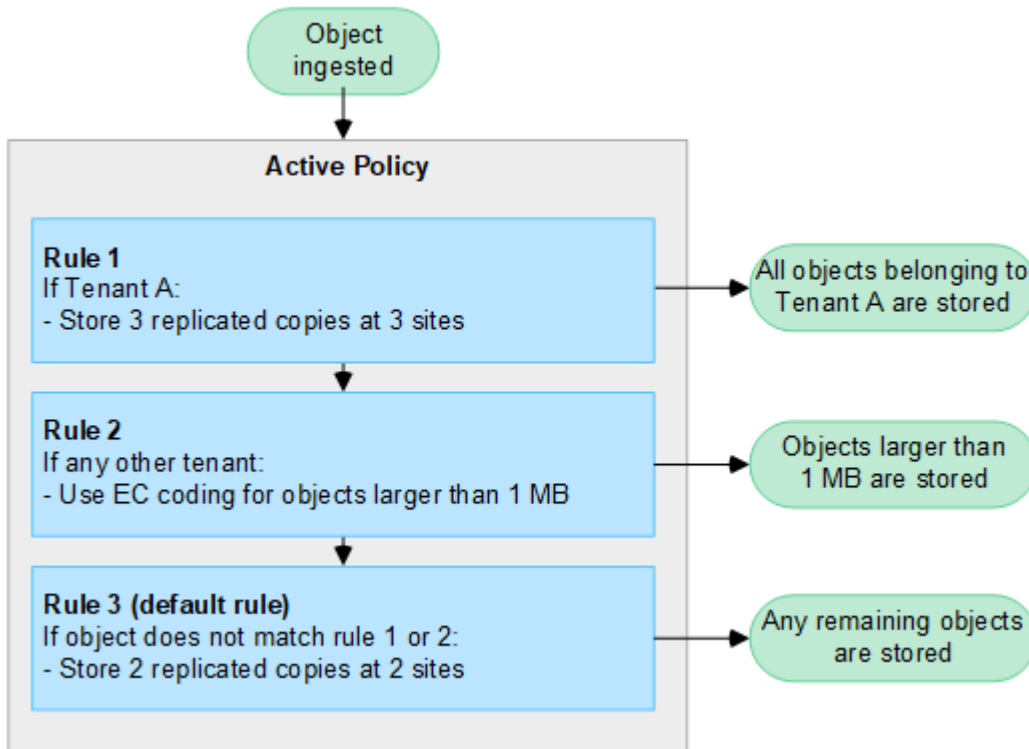
1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten der Regel aufgenommen und gemäß den Anweisungen zur Platzierung dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird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

Beispiel für eine ILM-Richtlinie

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

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

- Entspricht nicht Objekten mit einer Größe von 1 MB oder weniger, daher werden diese Objekte mit Regel 3 verglichen.
- **Regel 3: 2 Exemplare 2 Rechenzentren (Standard)**
 - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
 - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und mindestens 1 MB groß sind).



Verwandte Informationen

- ["Objektmanagement mit ILM"](#)

Entdecken Sie StorageGRID

Entdecken Sie den Grid Manager

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



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

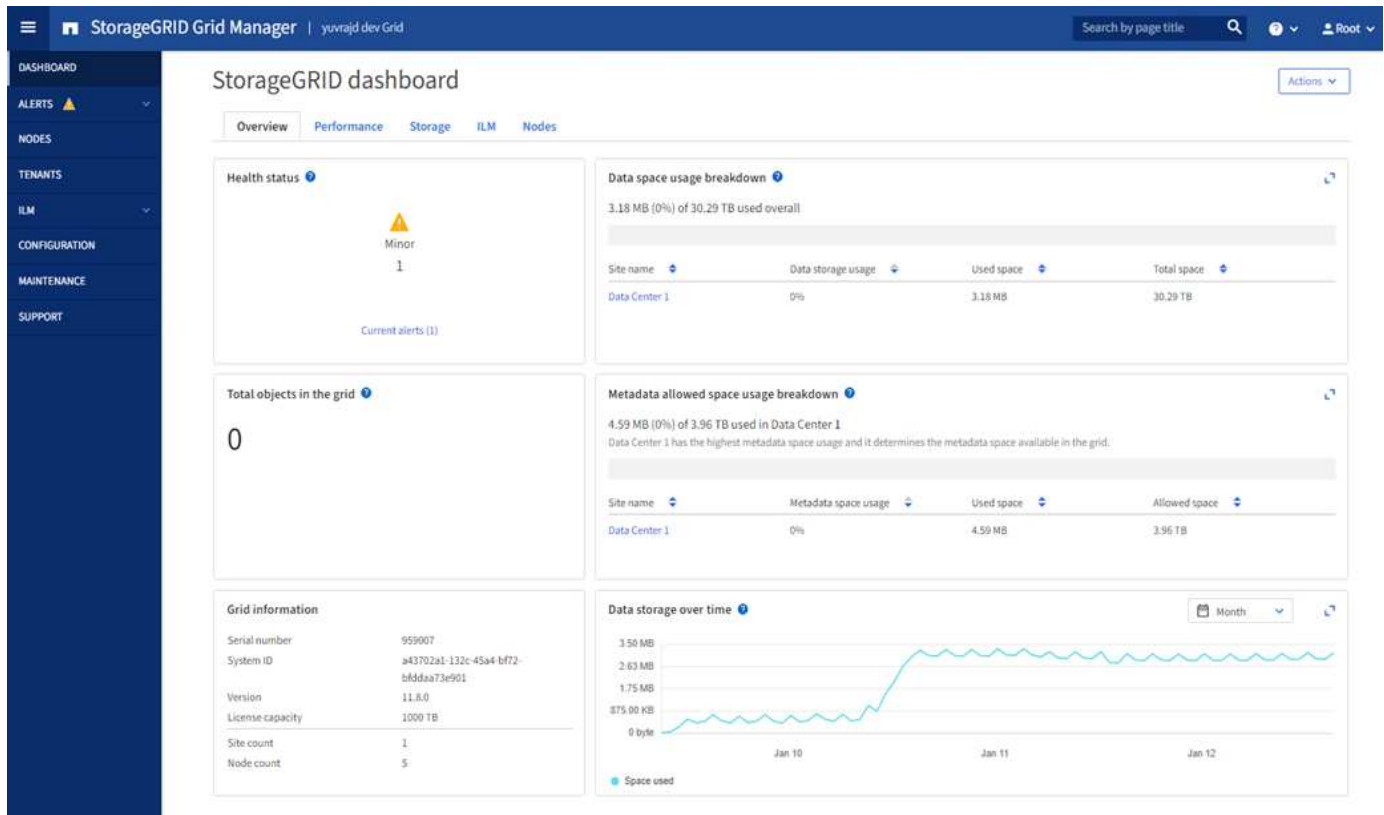
Wenn Sie sich beim Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Jedes StorageGRID System umfasst einen primären Admin-Node und eine beliebige Anzahl nicht primärer Admin-Nodes. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten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

Sie können den Grid-Manager über einen aufrufen ["Unterstützter Webbrowser"](#).

Grid Manager Dashboard

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

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



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

Suchfeld

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

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

Hilfe-Menü

Über das Hilfemenü können Sie auf Folgendes zugreifen:

- Der ["FabricPool"](#) und ["-S3-Einrichtung"](#) Assistent
- Das StorageGRID Dokumentationszentrum für die aktuelle Version

- ["API-Dokumentation"](#)
- Informationen darüber, welche Version von StorageGRID derzeit installiert ist

Menü „Meldungen“

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

Über das Menü „Alarme“ können Sie folgende Aktionen ausführen ["Managen von Warnmeldungen"](#):

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

Knoten Seite

Im ["Knoten Seite"](#) werden Informationen über das gesamte Raster, jeden Standort im Raster und jeden Node an einem Standort angezeigt.

Auf der Startseite Nodes werden die kombinierten Metriken für das gesamte Raster angezeigt. Um Informationen zu einem bestimmten Standort oder Node anzuzeigen, wählen Sie den Standort oder Node aus.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
▲ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Mandanten werden gestartet

["Mandanten werden gestartet"](#) Mit können Sie ["Erstellen und überwachen Sie die Konten von Storage-](#)

Mandanten für Ihr StorageGRID-System. Sie müssen mindestens ein Mandantenkonto erstellen, um anzugeben, wer Objekte speichern und abrufen kann und welche Funktionen ihnen zur Verfügung stehen.

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

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Create Export to CSV Actions Search tenants by name or ID

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	S3 Tenant	0 bytes	0%	100.00 GB	0	→ 📄
<input type="checkbox"/>	Swift Tenant	0 bytes	0%	100.00 GB	0	→ 📄

← Previous 1 Next →

ILM-Menü

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

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Storage-Pools
- Lagergütern
- Regionen
- Suche nach Objektmetadaten

Konfigurationsmenü

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

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

- "Verwalten von Hochverfügbarkeitsgruppen"
- "Verwalten von Endpunkten des Load Balancer"

- "Konfigurieren von S3-Endpunkt-Domännennamen"
- "Verwalten von Richtlinien für die Verkehrsklassifizierung"
- "Konfigurieren von VLAN-Schnittstellen"

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

- "Verwalten von Sicherheitszertifikaten"
- "Management interner Firewall-Kontrollen"
- "Konfigurieren von Verschlüsselungsmanagement-Servern"
- Konfigurieren von Sicherheitseinstellungen einschließlich "TLS- und SSH-Richtlinie", "Optionen für die Netzwerk- und Objektsicherheit" und "Sicherheitseinstellungen der Schnittstelle".
- Konfigurieren der Einstellungen für ein "Storage-Proxy" oder ein "Admin-Proxy"

Systemaufgaben

Zu den Systemaufgaben gehören:

- Verwenden "Grid-Verbund" zum Klonen von Mandantenkontoinformationen und zum Replizieren von Objektdaten zwischen zwei StorageGRID Systemen.
- Optional wird die Option aktiviert "Gespeicherte Objekte komprimieren".
- "Verwalten der S3-Objektsperre"
- Allgemeines zu Storage-Optionen wie "Objektsegmentierung" und "Wasserzeichen für Storage-Volumes".
- "Profile für das Erasure Coding managen".

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- "Konfigurieren von Überwachungsmeldungen und Protokollzielen"
- "Verwendung von SNMP-Überwachung"

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugriffssteuerung gehören:

- "Verwalten von Admin-Gruppen"
- "Verwalten von Administratorbenutzern"
- Ändern des "Provisionierungs-Passphrase" oder "Passwörter für die Node-Konsole"
- "Identitätsföderation verwenden"
- "SSO wird konfiguriert"

Menü Wartung

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

Aufgaben

Zu den Wartungsarbeiten gehören:

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

System

Sie können folgende Systemwartungsaufgaben ausführen:

- ["Anzeigen von StorageGRID-Lizenzinformationen"](#) Oder ["Lizenzinformationen werden aktualisiert"](#)
- Generieren und Herunterladen der ["Wiederherstellungspaket"](#)
- StorageGRID Software-Updates, einschließlich Software-Upgrades und Hotfixes, sowie Updates für die SANtricity OS Software auf ausgewählten Appliances
 - ["Upgrade-Verfahren"](#)
 - ["Hotfix-Verfahren"](#)
 - ["Aktualisieren Sie das SANtricity Betriebssystem auf SG6000 Storage Controllern mithilfe des Grid Manager"](#)
 - ["Aktualisieren Sie das SANtricity Betriebssystem auf SG5700 Storage Controllern mithilfe des Grid Manager"](#)

Netzwerk

Sie können folgende Aufgaben zur Netzwerkwartung ausführen:

- ["Konfigurieren von DNS-Servern"](#)
- ["Aktualisieren von Netzwerken"](#)
- ["Verwalten von NTP-Servern"](#)

Menü „Support“

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

Tools

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

- ["Konfigurieren Sie AutoSupport"](#)
- ["Führen Sie eine Diagnose aus"](#) Auf den aktuellen Zustand des Rasters

- ["Greifen Sie auf die Baumstruktur der Grid-Topologie zu"](#) So zeigen Sie detaillierte Informationen zu Grid-Nodes, Services und Attributen an
- ["Erfassen von Protokolldateien und Systemdaten"](#)
- ["Prüfen von Support-Kennzahlen"](#)



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

Alarmer (alt)

Die Informationen zu älteren Alarmen wurden aus dieser Version der Dokumentation entfernt. Siehe ["Verwaltung von Alarmen und Alarmen \(StorageGRID 11.8-Dokumentation\)"](#).

Sonstiges

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

- Managen ["Verbindungskosten"](#)
- Einträge ["Netzwerk-Management-System \(NMS\)"](#) anzeigen
- Managen ["Storage-Wasserzeichen"](#)

Entdecken Sie den Tenant Manager

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



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

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

Mandanten-Manager Dashboard

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

Über das Tenant Manager Dashboard können Mandantenbenutzer die Storage-Auslastung auf einen Blick überwachen. Im Bereich Storage-Nutzung finden Sie eine Liste der größten Buckets (S3) oder Container (Swift) für den Mandanten. Der Wert für „genutzter Speicherplatz“ ist die Gesamtmenge der Objektdaten im Bucket oder Container. Das Balkendiagramm stellt die relative Größe dieser Buckets oder Container dar.

Der über dem Balkendiagramm angezeigte Wert ist eine Summe des Speicherplatzes, der für alle Buckets oder Container des Mandanten verwendet wird. Wurde zum Zeitpunkt der Kontoerstellung die maximale Anzahl an Gigabyte, Terabyte oder Petabyte angegeben, so wird auch die Menge des verwendeten Kontingents und der verbleibenden Menge angezeigt.

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Speicherменü (S3)

Das Menü Storage wird nur für S3-Mandantenkonten angezeigt. In diesem Menü können S3 Benutzer Zugriffsschlüssel managen, Buckets erstellen, managen und löschen, Plattform-Services-Endpunkte managen und alle Grid-Verbindungen anzeigen, die sie verwenden dürfen.

Meine Zugriffsschlüssel

S3-Mandantenbenutzer können die Zugriffsschlüssel wie folgt managen:

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



Die Verwaltung der Zugriffstasten für andere Benutzer erfolgt über das Menü Access Management.

Buckets

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

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

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

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

Plattform-Services-Endpunkte

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

Netzverbundverbindungen

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

Öffnen Sie das Menü Management

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.