



Informationen zu StorageGRID

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/de-de/storagegrid-120/primer/index.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Inhalt

Informationen zu StorageGRID	1
Was ist StorageGRID?	1
StorageGRID Vorteile	2
Hybrid Clouds mit StorageGRID	3
Cloud-Storage-Pools	3
S3 Plattformdienste	3
ONTAP Datentiering mit FabricPool	3
StorageGRID Architektur und Netzwerktopologie	4
Bereitstellungstopologien	4
Systemarchitektur	5
Grid-Knoten und Dienste	7
StorageGRID Grid-Knoten und Services	7
Was ist ein StorageGRID Admin Node?	11
Was ist ein StorageGRID Storage Node?	13
Was ist ein StorageGRID Gateway Node?	19
Wie StorageGRID Daten verwaltet	20
Was ist ein StorageGRID Objekt	20
Objektlebenszyklus in StorageGRID	22
Wie StorageGRID die Objektaufnahme handhabt	23
Wie StorageGRID Objektkopien verwaltet	24
Wie StorageGRID den Objektabruf handhabt	27
Wie StorageGRID das Löschen von Objekten handhabt	28
Informationslebenszyklusmanagement in StorageGRID	30
StorageGRID erkunden	32
Erkunden Sie den StorageGRID Grid Manager	32
Erkunden Sie den StorageGRID Tenant Manager	37

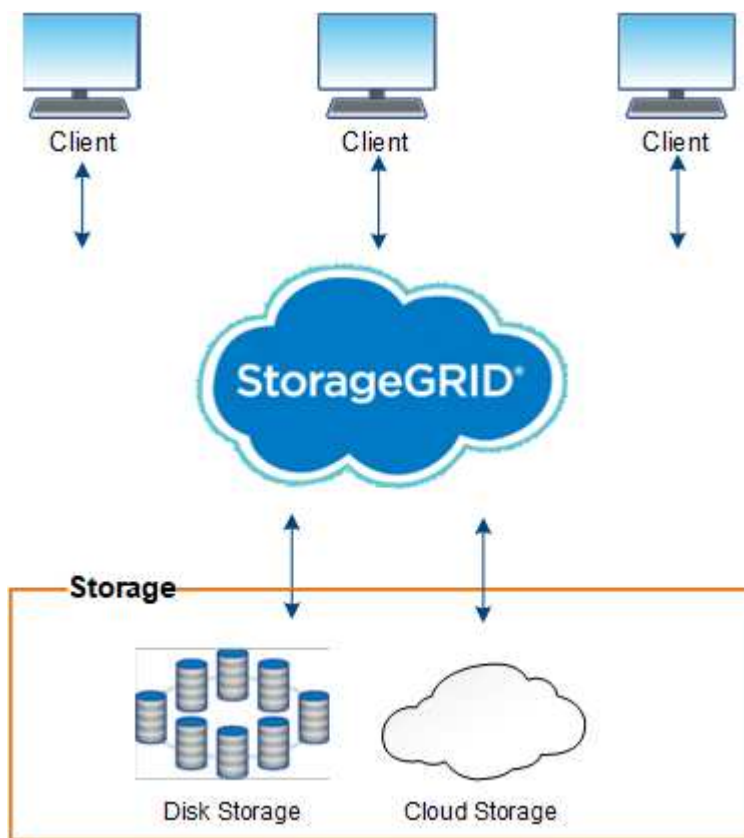
Informationen zu StorageGRID

Was ist StorageGRID?

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

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

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



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

StorageGRID Vorteile

Zu den Vorteilen des StorageGRID Systems gehören die folgenden:

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

Hybrid Clouds mit StorageGRID

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

Cloud-Storage-Pools

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

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



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

S3 Plattformdienste

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

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

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

ONTAP Datentiering mit FabricPool

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

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

Verwandte Informationen

- ["Was ist ein Cloud Storage Pool?"](#)
- ["Plattformdienste verwalten"](#)

- ["StorageGRID für FabricPool konfigurieren"](#)

StorageGRID Architektur und Netzwerktopologie

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

Informationen zu ["Grid-Node-Typen"](#).

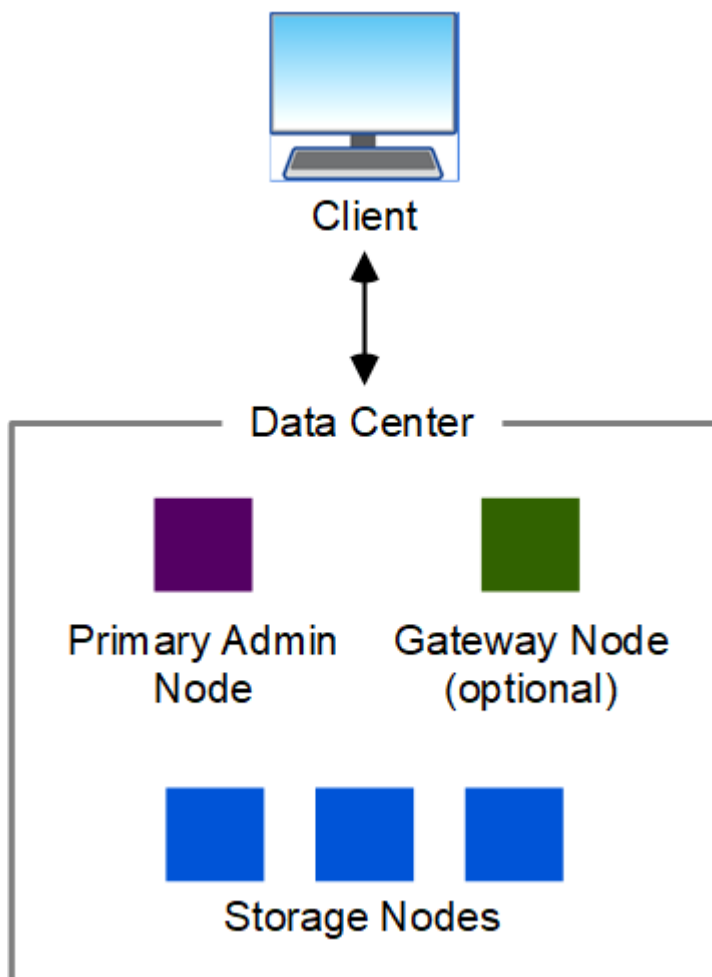
Weitere Informationen zur StorageGRID Netzwerktopologie, zu den Anforderungen und zur Grid-Kommunikation enthält die Dokumentation ["Netzwerkrichtlinien"](#).

Bereitstellungstopologien

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

Einzelstandort

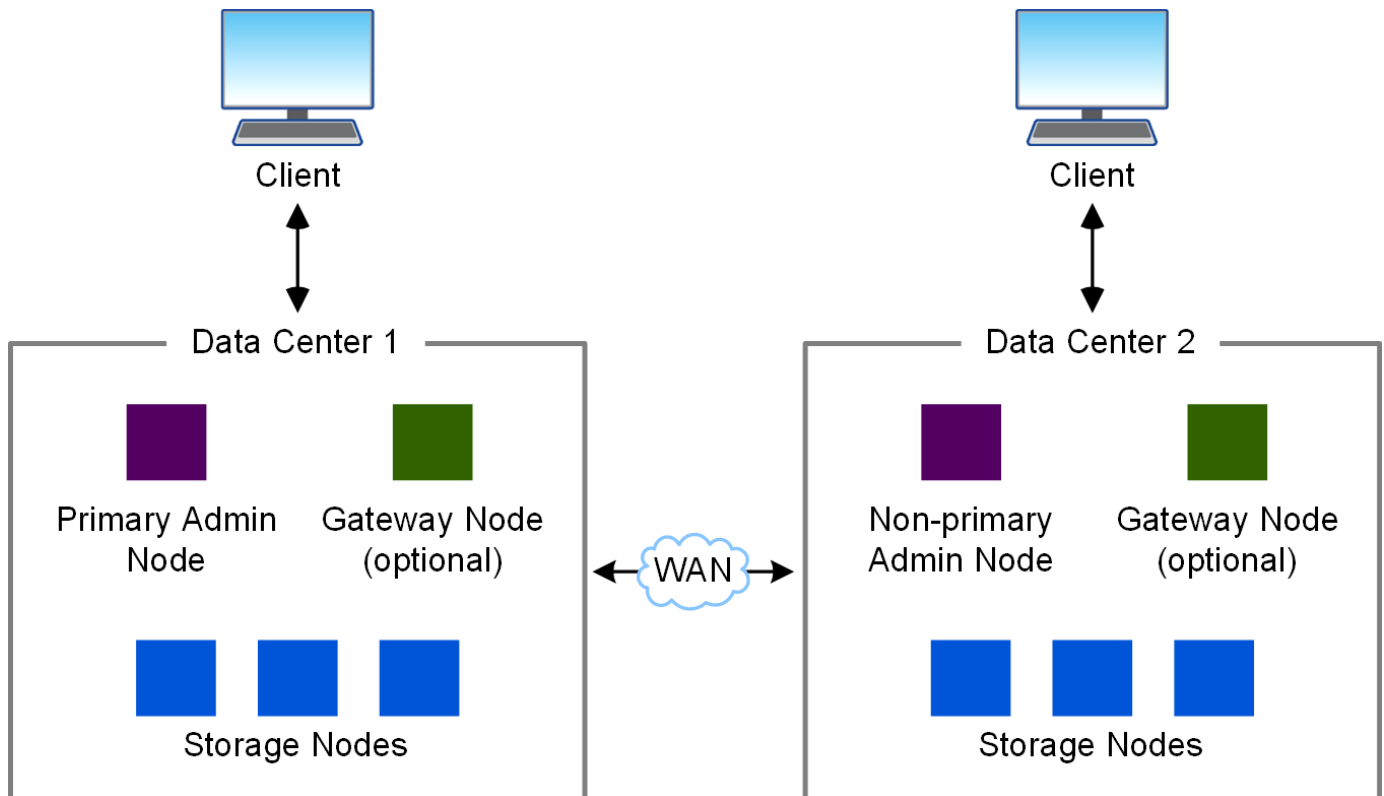
In einer Bereitstellung mit einem einzelnen Standort sind die Infrastruktur und der Betrieb des StorageGRID Systems zentralisiert.



Mehrere Standorte

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

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



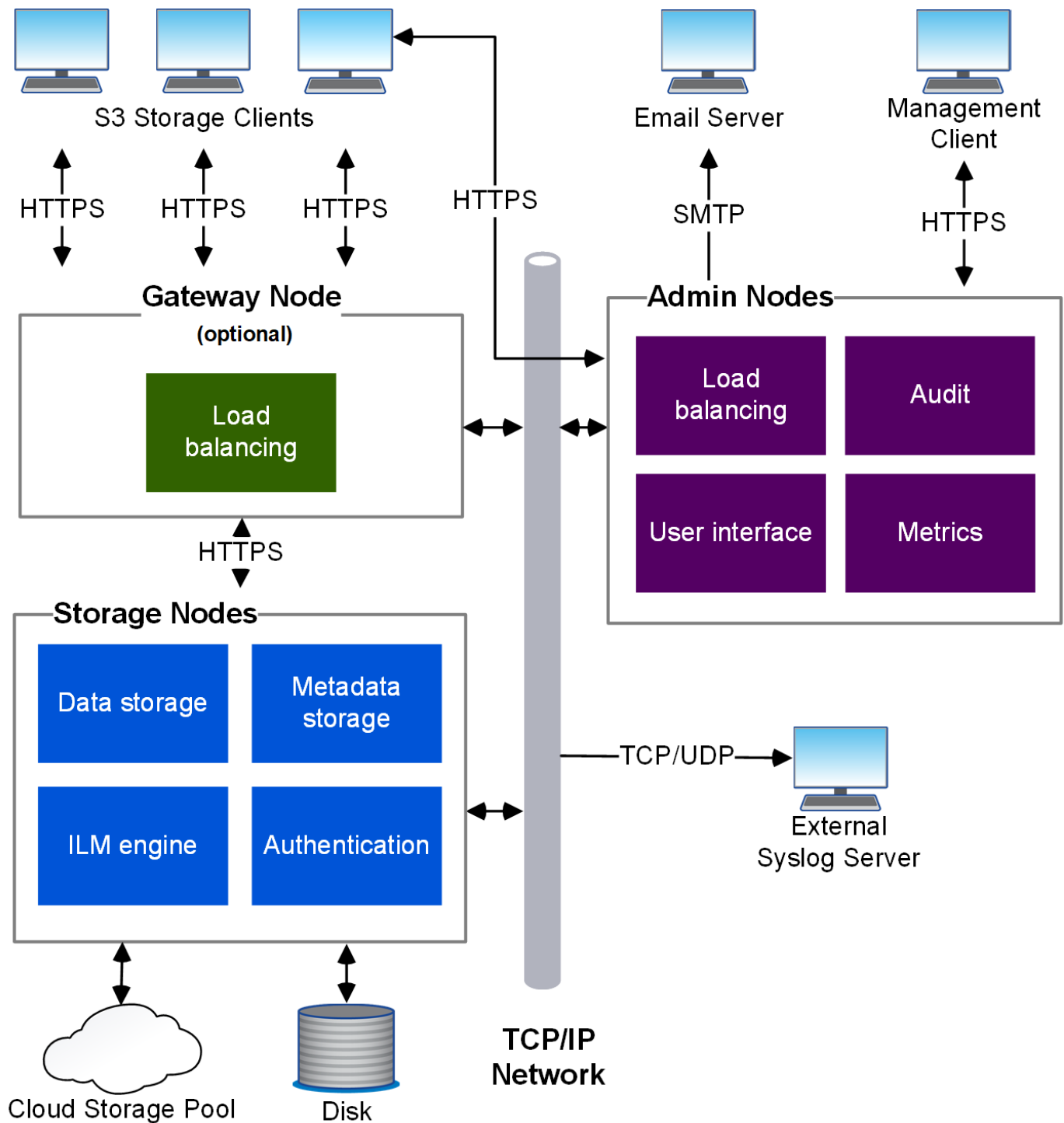
Innerhalb eines einzigen Rechenzentrums können auch mehrere logische Standorte existieren, um die Nutzung von verteilter Replikation und Erasure Coding für erhöhte Verfügbarkeit und Ausfallsicherheit zu ermöglichen.

Redundanz der Grid-Knoten

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

Systemarchitektur

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



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

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

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

Grid-Knoten und Dienste

StorageGRID Grid-Knoten und Services

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

Arten von Grid-Knoten

Das StorageGRID System verwendet drei Arten von Grid-Knoten:

Admin-Nodes

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

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

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

Speicher-knoten

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

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

Siehe ["Was ist ein Speicher-knoten?"](#)

Gateway-Nodes (optional)

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

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

Hardware- und Software-Nodes

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

StorageGRID Appliance Knoten

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

aufweisen.

Im Folgenden sind Informationen zu den verfügbaren Geräten aufgeführt:

- ["StorageGRID Appliance Dokumentation"](#)
- ["NetApp Hardware Universe"](#)

Softwarebasierte Knoten

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

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

StorageGRID Dienste

Im Folgenden befindet sich eine vollständige Liste der StorageGRID Dienste.

Service	Beschreibung	Standort
Account-Service-Forwarder	Bietet eine Schnittstelle für den Load Balancer Service, um den Account Service auf Remote-Hosts abzufragen, und stellt dem Load Balancer Service Benachrichtigungen über Änderungen der Load Balancer Endpoint-Konfiguration bereit.	Load Balancer Dienst auf Admin-Knoten und Gateway-Knoten
ADC (Administrativer Domänencontroller)	Pflegt Topologieinformationen, bietet Authentifizierungsdienste und beantwortet Anfragen der LDR- und CMN-Dienste.	Mindestens drei Speicherknoten mit dem ADC-Dienst an jedem Standort
AMS (Audit Management System)	Überwacht und protokolliert alle geprüften Systemereignisse und Transaktionen in einer Textprotokolldatei.	Admin-Nodes
Apache Tomcat	Webserver für Java-basierte Anwendungen.	Admin-Nodes
Avahi Daemon	Verarbeitet mDNS, das zur Namensauflösung und Diensterkennung innerhalb des lokalen Netzwerks verwendet wird.	Alle Knoten
Cache Service	Läuft auf Load Balancer-Knoten (Gateway) und verwaltet einen lokalen Cache für Objekthinhalte.	Gateway-Nodes
Cassandra	Verwaltet die verteilte Datenbank für Objektmeldaten.	Speicherknoten (außer Datenknoten)
Cassandra Reaper	Führt automatische Reparaturen an Objektmeldaten durch.	Speicherknoten

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

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

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

Was ist ein StorageGRID Admin Node?

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

Unterschiede zwischen primären und nicht-primären Admin Nodes

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

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

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

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

Bevorzugter Absender Admin Node

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

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

In diesen Fällen werden möglicherweise mehrere Benachrichtigungen gesendet:

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

Benachrichtigungen empfangen werden.

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



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

Primäre Dienste für Admin-Knoten

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

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

Was ist ein StorageGRID Storage Node?

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

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

Arten von Speicherknoten

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

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

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

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

Daten- und Metadaten Storage Node (kombiniert)

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

Speicherknoten nur für Metadaten

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

Nur-Metadaten-Speicherknoten haben spezifische Hardwareanforderungen:

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



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

reiner Datenspeicherknoten

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

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

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

Erforderliche Speicherknoten pro Grid und pro Standort

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

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

Primäre Dienste für Storage Nodes

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



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

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

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

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

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

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

Was ist ein StorageGRID Gateway Node?

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

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

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

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

Primäre Dienste für Gateway-Knoten

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

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

die mit dem LDR Service interagiert.

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

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

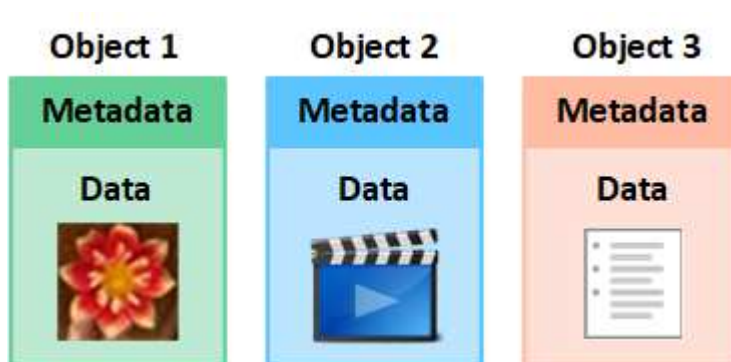
Wie StorageGRID Daten verwaltet

Was ist ein StorageGRID Objekt

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

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

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



Was sind Objektdaten?

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

Was sind Objektmetadaten?

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

Objektmetadaten enthalten unter anderem folgende Informationen:

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

der letzten Änderung des Objekts.

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

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

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

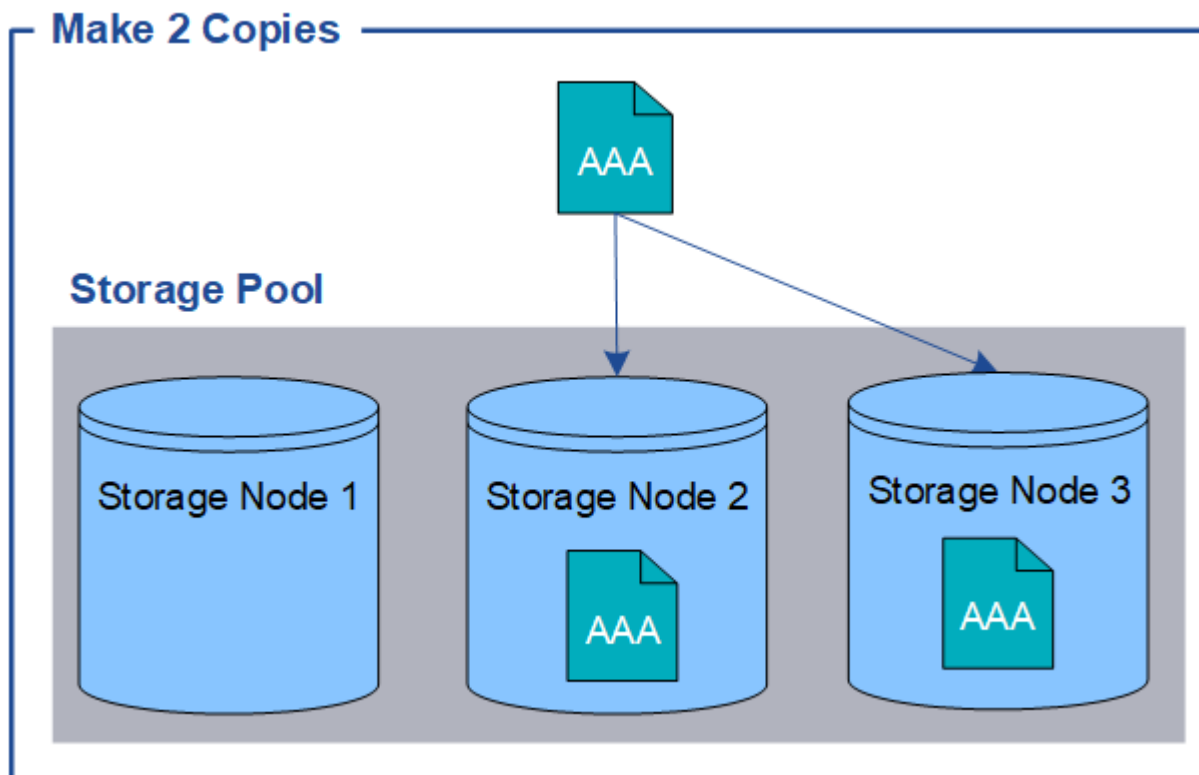
Wie werden Objektdaten geschützt?

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

Replication

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

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

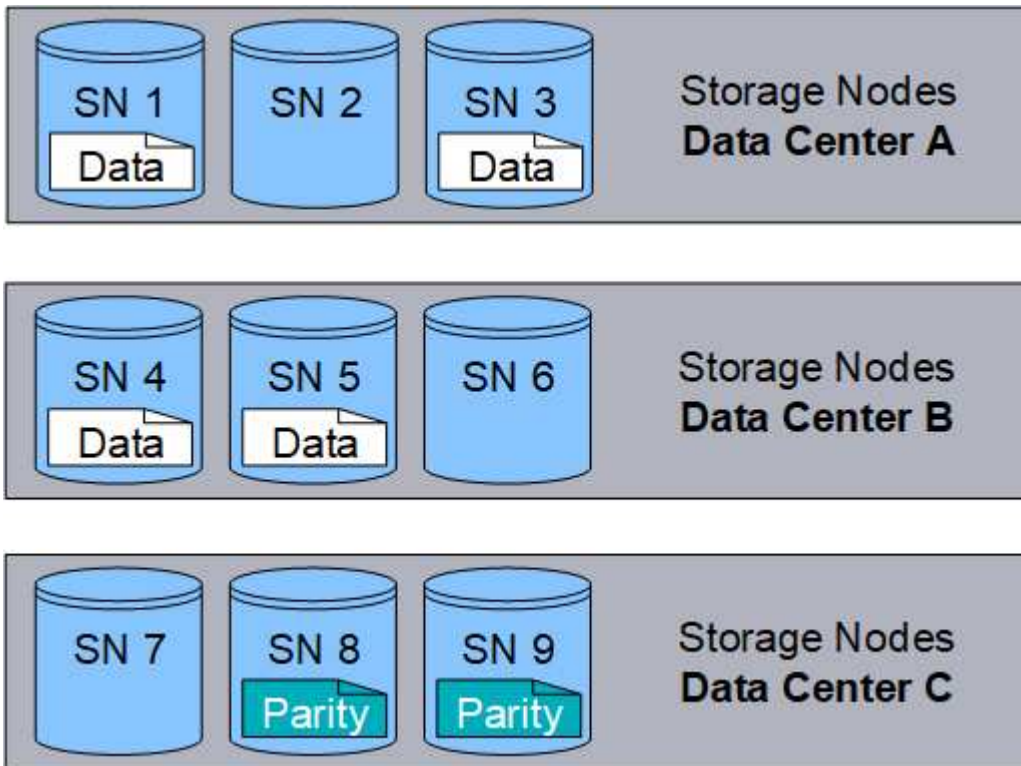


Erasure Coding

Wenn StorageGRID Objekte einer ILM-Regel zuordnet, die für die Erstellung von erasure-codierten Kopien konfiguriert ist, werden die Objektdaten in Datenfragmente zerlegt, zusätzliche Paritätsfragmente berechnet

und jedes Fragment auf einem anderen Storage Node gespeichert. Beim Zugriff auf ein Objekt wird es mithilfe der gespeicherten Fragmente wieder zusammengesetzt. Wenn ein Daten- oder Paritätsfragment beschädigt wird oder verloren geht, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten- und Paritätsfragmente rekonstruieren. ILM-Regeln und Erasure-Coding-Profil bestimmen das verwendete Erasure-Coding-Schema.

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



Verwandte Informationen

- ["Objekte mit ILM verwalten"](#)
- ["Informationslebenszyklusmanagement verwenden"](#)

Objektlebenszyklus in StorageGRID

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

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

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

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



Verwandte Informationen

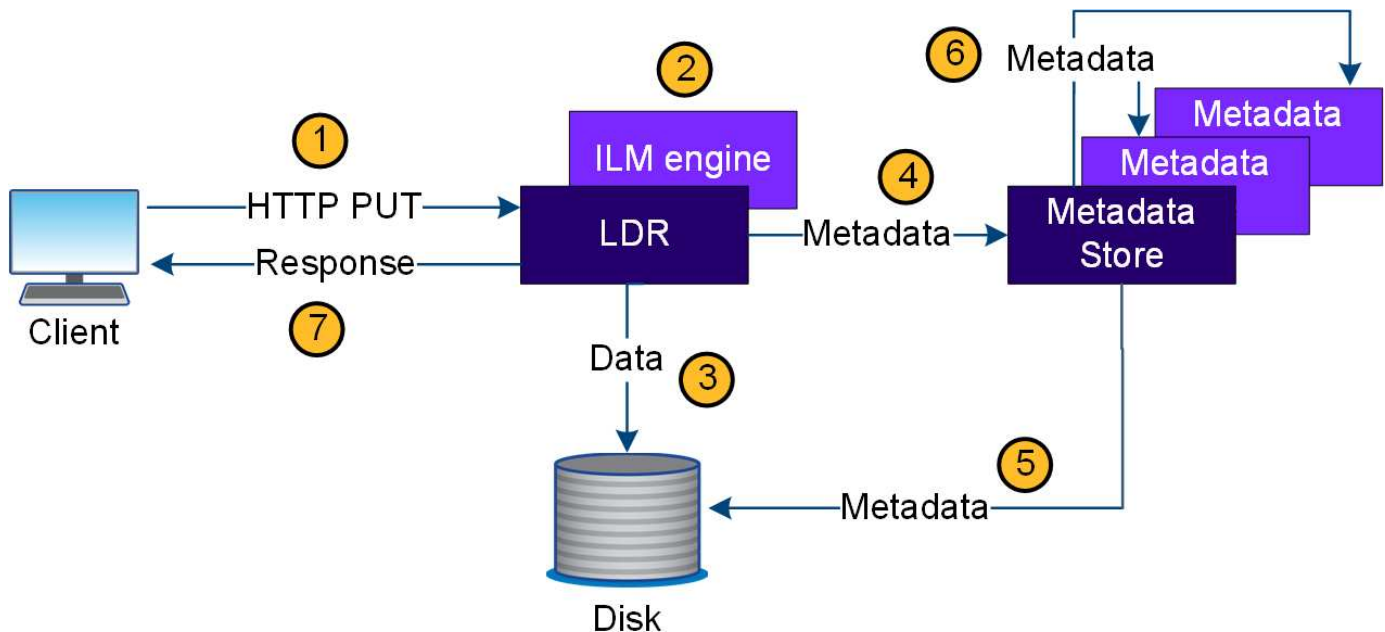
- ["Objekte mit ILM verwalten"](#)
- ["Informationslebenszyklusmanagement verwenden"](#)

Wie StorageGRID die Objektaufnahme handhabt

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

Datenfluss

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



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

2. Das Objekt wird anhand der ILM-Richtlinie des Systems bewertet.
3. Der LDR-Dienst speichert die Objektdaten als replizierte Kopie oder als löschcodierte Kopie. (Das Diagramm zeigt eine vereinfachte Darstellung der Speicherung einer replizierten Kopie auf der Festplatte.)
4. Der LDR-Dienst sendet die Objektmetadaten an den Metadatenpeicher.
5. Der Metadatenpeicher speichert die Objektmetadaten auf der Festplatte.
6. Der Metadatenpeicher verteilt Kopien der Objektmetadaten an andere Storage Nodes. Diese Kopien werden ebenfalls auf der Festplatte gespeichert.
7. Der LDR-Dienst gibt eine HTTP 200 OK-Antwort an den Client zurück, um zu bestätigen, dass das Objekt aufgenommen wurde.

Wie StorageGRID Objektkopien verwaltet

Objektdaten werden durch die aktiven ILM-Richtlinien und zugehörigen ILM-Regeln verwaltet. ILM-Regeln erstellen Replikate oder mit Erasure Coding versehene Kopien, um Objektdaten vor Verlust zu schützen.

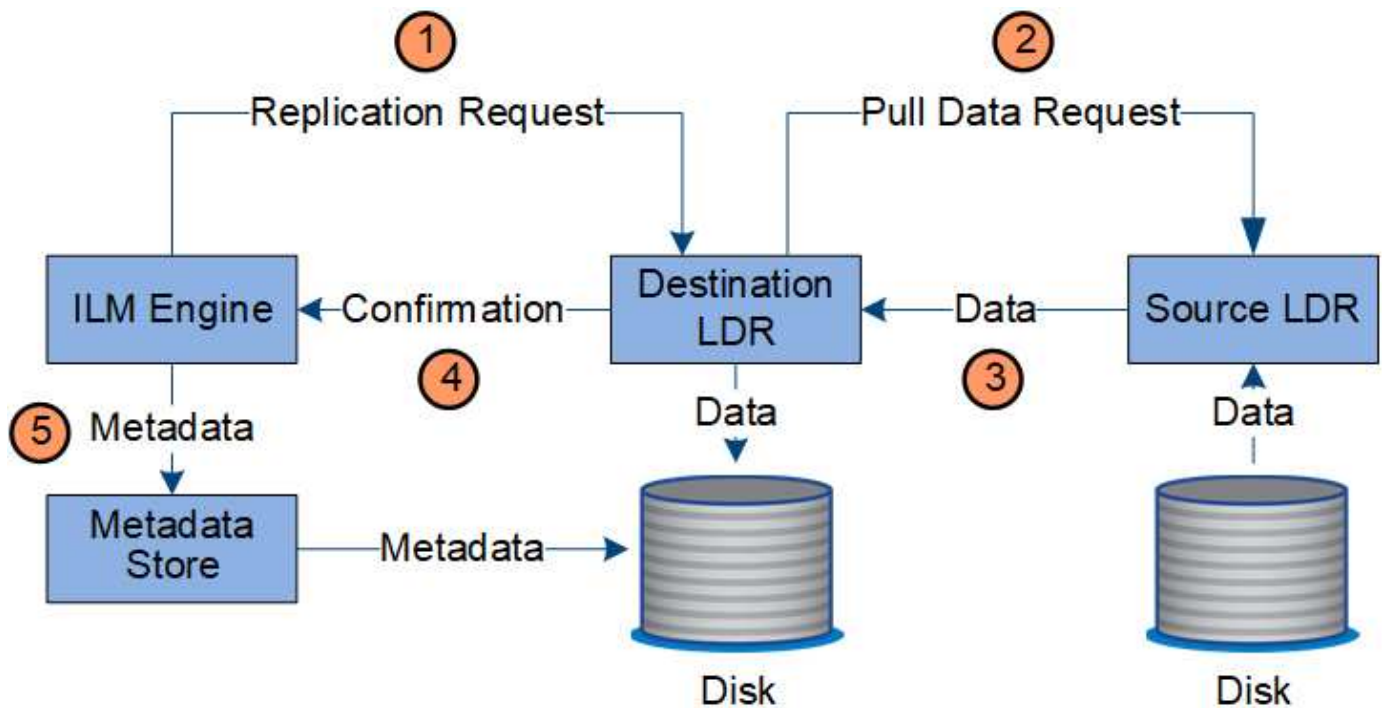
Je nach Lebenszyklus eines Objekts können unterschiedliche Arten oder Speicherorte von Objektkopien erforderlich sein. ILM-Regeln werden regelmäßig ausgewertet, um sicherzustellen, dass Objekte wie benötigt platziert werden.

Die Objektdaten werden vom LDR Service verwaltet.

Inhaltsschutz: Replikation

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

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

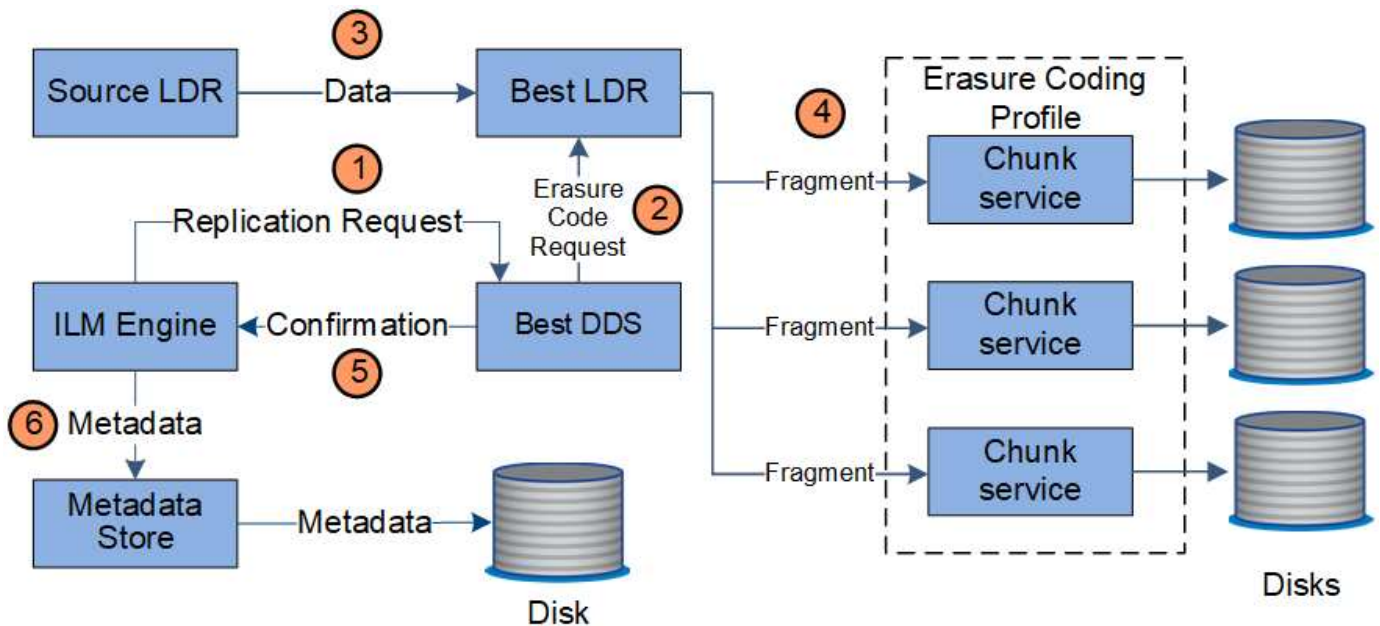


1. Die ILM-Engine fragt den ADC-Dienst ab, um den besten Ziel-LDR-Dienst innerhalb des durch die ILM-Regel festgelegten Speicherpools zu ermitteln. Anschließend sendet sie diesem LDR-Dienst einen Befehl zur Initiierung der Replikation.
2. Der Ziel-LDR-Dienst fragt den ADC-Dienst nach dem besten Quellstandort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

Inhaltsschutz: Erasure Coding

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

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

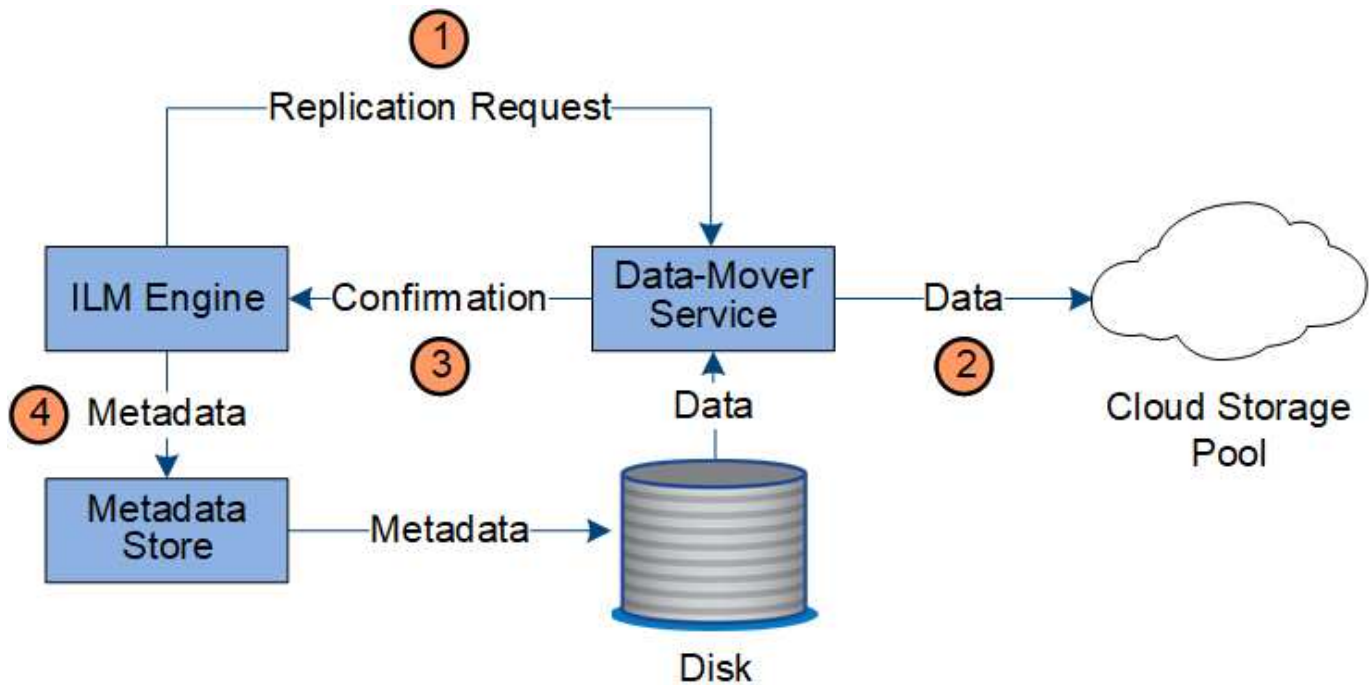


1. Die ILM-Engine fragt den ADC-Dienst ab, um zu bestimmen, welcher DDS-Dienst die Löschungs-codierung am besten durchführen kann. Nach der Bestimmung sendet die ILM-Engine eine „Initiate“-Anforderung an diesen Dienst.
2. Der DDS-Dienst weist einen LDR an, die Objektdaten mit einer Erasure-Codierung zu versehen.
3. Der Quell-LDR-Dienst sendet eine Kopie an den für das Erasure Coding ausgewählten LDR-Dienst.
4. Nachdem die entsprechende Anzahl an Parität- und Datenfragmenten erstellt wurde, verteilt der LDR-Dienst diese Fragmente auf die Storage Nodes (Chunk Services), aus denen der Speicherpool des Erasure-Coding-Profiles besteht.
5. Der LDR Service benachrichtigt die ILM Engine und bestätigt, dass die Objektdaten erfolgreich verteilt wurden.
6. Die ILM Engine aktualisiert den Metadaten-speicher mit Metadaten zum Objektstandort.

Inhaltsschutz: Cloud Storage Pool

Wenn die Inhaltsplatzierungsanweisungen einer ILM-Regel erfordern, dass eine replizierte Kopie der Objektdaten in einem Cloud Storage Pool gespeichert wird, werden die Objektdaten in den externen S3-Bucket oder Azure Blob Storage Container dupliziert, der für den Cloud Storage Pool angegeben wurde.

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



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

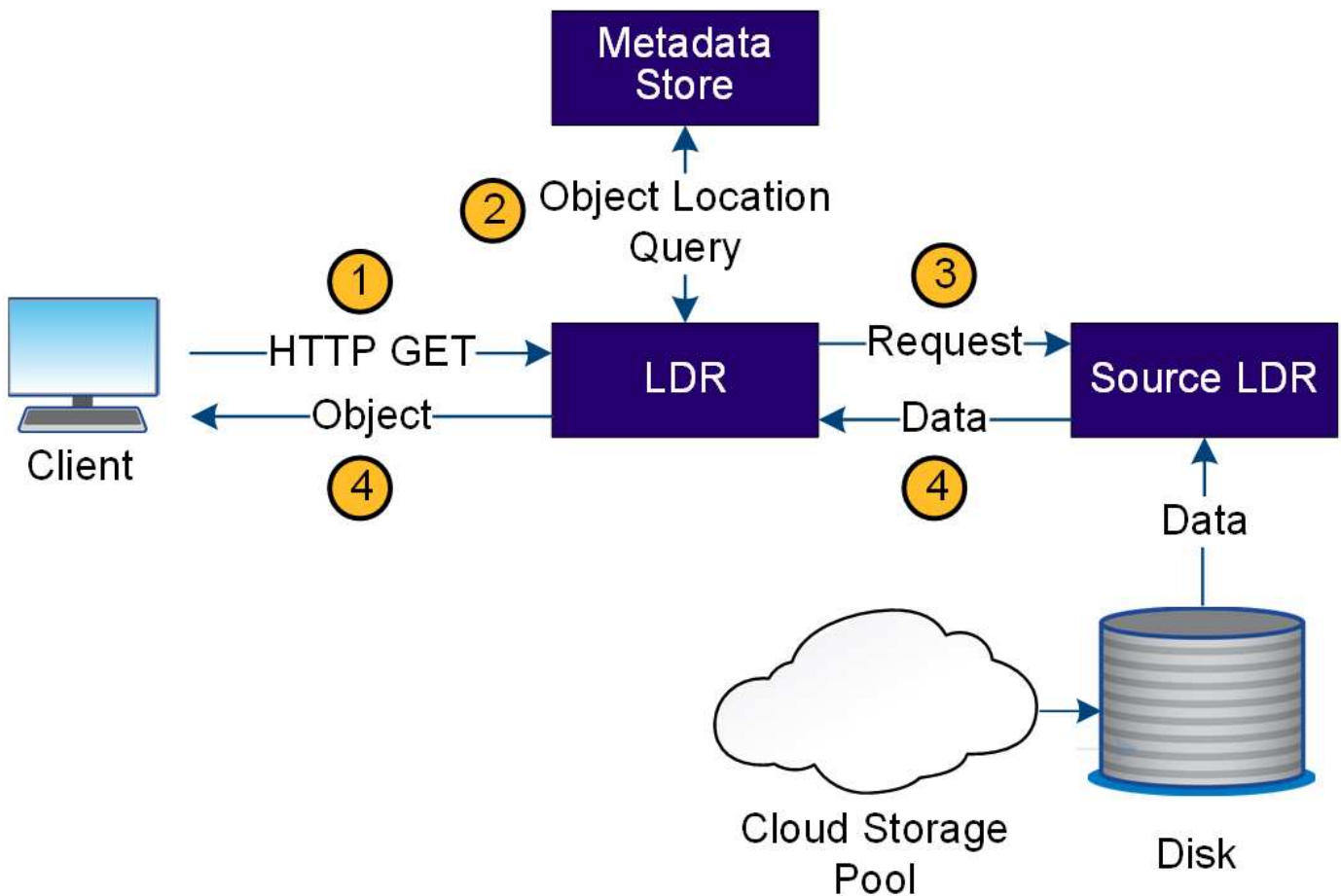
Wie StorageGRID den Objektabruf handhabt

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

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



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



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

Wie StorageGRID das Löschen von Objekten handhabt

Alle Objektkopien werden aus dem StorageGRID-System entfernt, wenn ein Client einen Löschvorgang durchführt oder die Lebensdauer des Objekts abläuft, wodurch die automatische Entfernung ausgelöst wird. Für die Objektlöschung existiert ein definierter Datenfluss.

Löschhierarchie

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

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

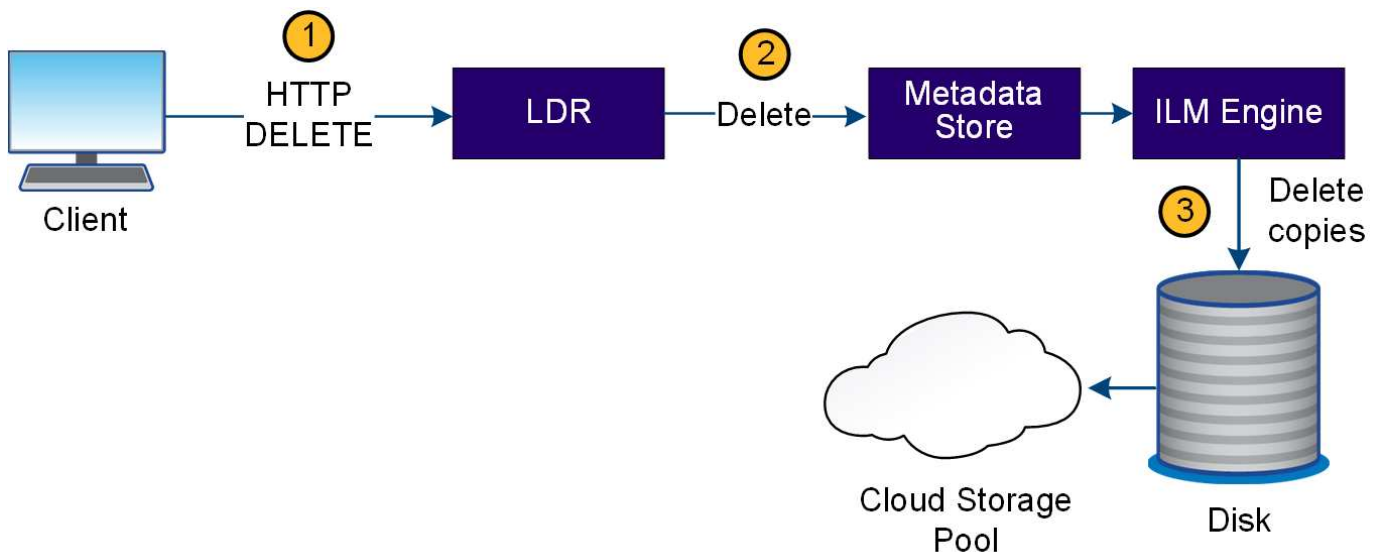
- Eine unter rechtlicher Sperre stehende Objektversion kann mit keiner Methode gelöscht werden.
 - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version mit keiner Methode gelöscht werden.
 - Objekte in Buckets mit aktivierter S3 Object Lock werden von ILM „dauerhaft“ aufbewahrt. Nach Ablauf des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Client-Anfrage oder durch das Ende des Bucket-Lebenszyklus gelöscht werden.
 - Wenn S3-Clients ein Standard-Retain-Until-Date für den Bucket festlegen, müssen sie kein Retain-Until-Date für jedes Objekt angeben.
- **Client-Löschanforderung:** Ein S3-Client kann eine Löschanforderung für ein Objekt stellen. Wenn ein Client ein Objekt löscht, werden alle Kopien des Objekts aus dem StorageGRID System entfernt.
 - **Objekte im Bucket löschen:** Tenant Manager-Benutzer können mit dieser Option alle Kopien der Objekte und Objektversionen in ausgewählten Buckets dauerhaft aus dem StorageGRID System entfernen.
 - **S3 Bucket Lifecycle:** S3-Clients können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Expiration-Aktion festlegt. Wenn ein Bucket-Lebenszyklus existiert, löscht StorageGRID automatisch alle Kopien eines Objekts, sobald das in der Expiration-Aktion angegebene Datum oder die Anzahl der Tage erreicht ist, es sei denn, der Client löscht das Objekt zuerst.
 - **ILM-Platzierungsanweisungen:** Unter der Annahme, dass für den Bucket keine S3-Objektsperre aktiviert ist und kein Bucket-Lebenszyklus existiert, löscht StorageGRID ein Objekt automatisch, wenn der letzte Zeitraum in der ILM-Regel abläuft und keine weiteren Platzierungen für das Objekt angegeben sind.



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

Siehe ["Wie Objekte gelöscht werden"](#) für weitere Informationen.

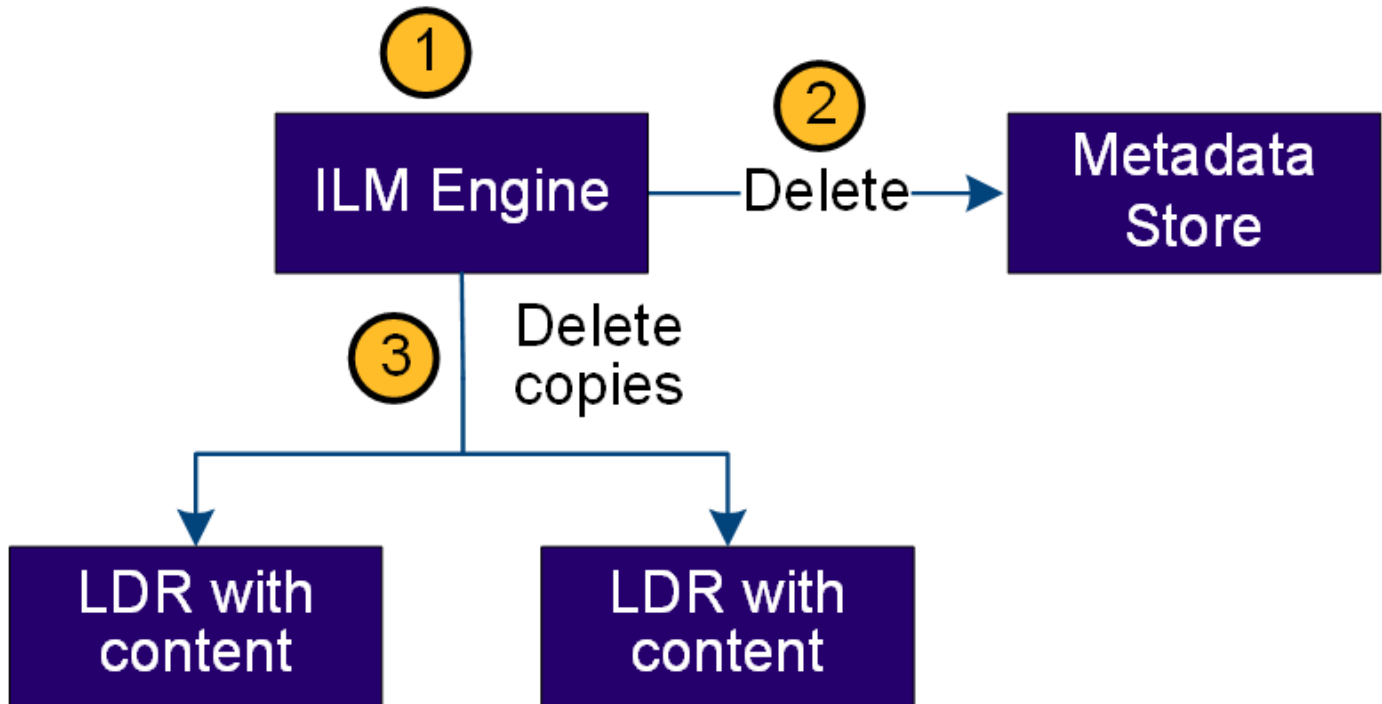
Datenfluss für das Löschen durch den Client



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

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

Datenfluss für ILM Löschvorgänge



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

Informationslebenszyklusmanagement in StorageGRID

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

Die ILM-Regeln definieren:

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

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

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

Beispiel einer ILM-Regel

Eine ILM Regel könnte beispielsweise Folgendes festlegen:

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

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

Wie eine ILM-Richtlinie Objekte auswertet

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

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

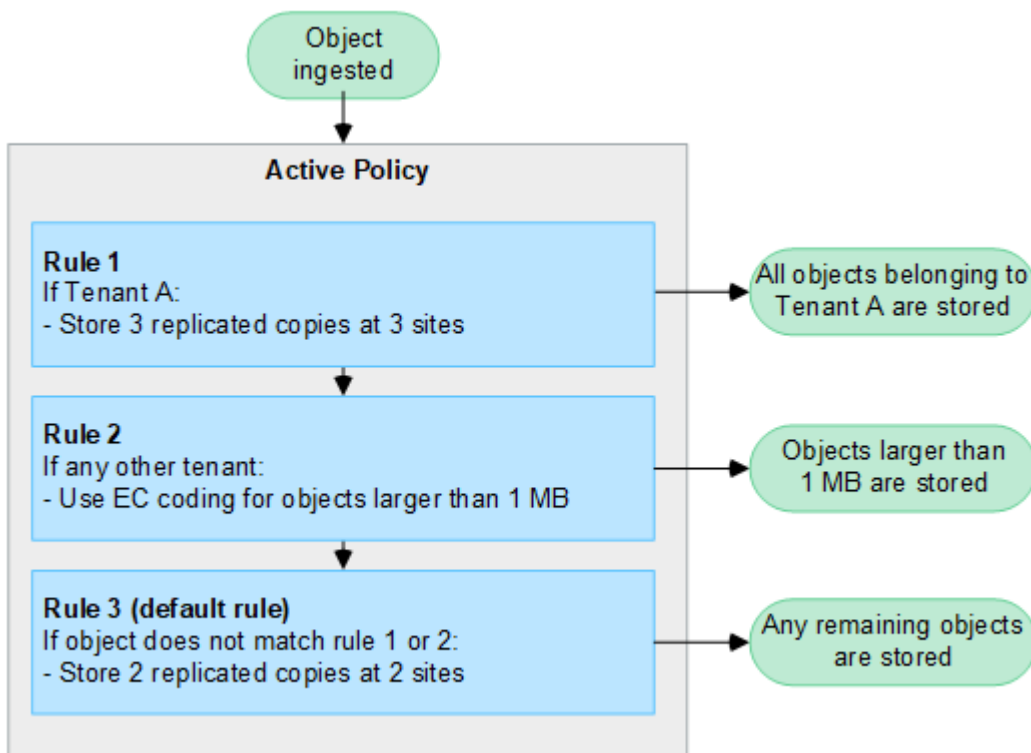
1. Wenn die Filter der ersten Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten dieser Regel aufgenommen und gemäß den Platzierungsanweisungen dieser Regel gespeichert.
2. Wenn die Filter der ersten Regel nicht mit dem Objekt übereinstimmen, wird das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

Beispiel einer ILM-Richtlinie

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

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

- Alle Objekte, die zu Tenant A gehören, abgleichen.
- Diese Objekte werden als drei replizierte Kopien an drei Standorten gespeichert.
- Objekte, die anderen Mandanten gehören, werden von Regel 1 nicht erfasst, daher erfolgt die Auswertung anhand von Regel 2.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
 - Alle Objekte anderer Mandanten werden abgeglichen, jedoch nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert.
 - Entspricht nicht Objekten mit einer Größe von 1 MB oder kleiner, daher werden diese Objekte anhand von Regel 3 ausgewertet.
- **Regel 3: 2 Kopien 2 Rechenzentren (Standard)**
 - Dies ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
 - Zwei replizierte Kopien aller Objekte, die nicht von Regel 1 oder Regel 2 erfasst werden (Objekte, die nicht zu Tenant A gehören und 1 MB oder kleiner sind), werden erstellt.



Verwandte Informationen

- ["Objekte mit ILM verwalten"](#)

StorageGRID erkunden

Erkunden Sie den StorageGRID Grid Manager

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



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

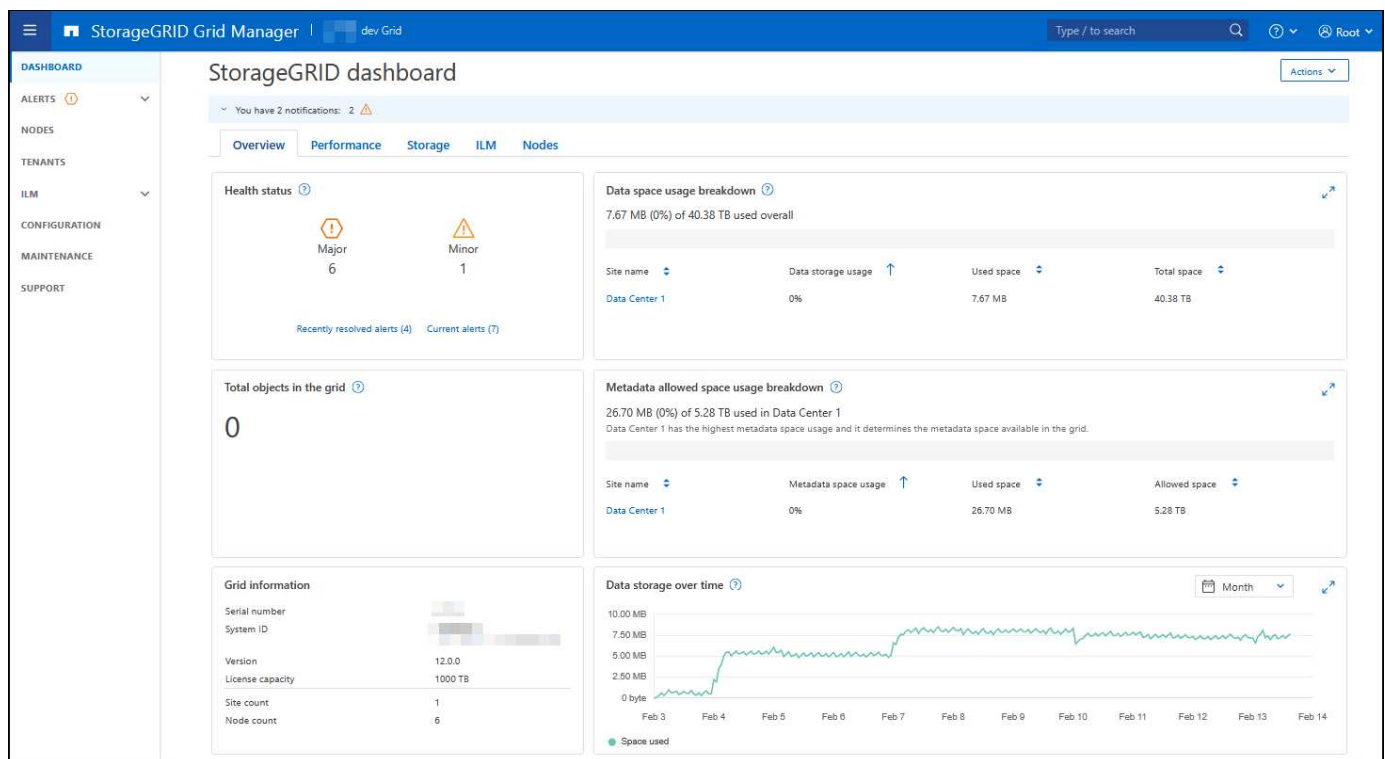
Wenn Sie sich im Grid Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Knoten her. Jedes StorageGRID System umfasst einen primären Admin-Knoten und beliebig viele nicht-primäre Admin-Knoten. Sie können sich mit jedem Admin-Knoten verbinden, und jeder Admin-Knoten zeigt eine ähnliche Ansicht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

Sie können mit einem ["unterstützte Webbrowser"](#) auf den Grid Manager zugreifen.

Grid Manager Dashboard

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

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



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

Suchfeld

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

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

suchen, beispielsweise nach Grid Nodes und Tenant Accounts.

Hilfemenü

Das Hilfemenü  bietet Zugriff auf:

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

Benachrichtigungsmenü

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

Im Menü „Benachrichtigungen“ können Sie Folgendes für "[Benachrichtigungen verwalten](#)" tun:

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

Nodes-Seite

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

Mandantenseite

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

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

ILM Menü

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

Im ILM-Menü lassen sich ILM anzeigen und verwalten:

- Regeln
- Richtlinien

- Richtlinien-Tags
- Storage Pools
- Storage-Grades
- Regionen
- Objektmetadatenabfrage

Konfigurationsmenü

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

Netzwerkaufgaben

Zu den Netzwerkaufgaben gehören:

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

Sicherheitsaufgaben

Zu den Sicherheitsaufgaben gehören:

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

Systemaufgaben

Zu den Systemaufgaben gehören:

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

Überwachungsaufgaben

Zu den Überwachungsaufgaben gehören:

- ["Protokollverwaltung konfigurieren"](#)
- ["SNMP Überwachung"](#)

Zugriffskontrollaufgaben

Zu den Aufgaben der Zugangskontrolle gehören:

- ["\\${post_edited_translations.segment}"](#)
- ["Administratorbenutzer verwalten"](#)
- Ändern Sie die ["Bereitstellungspassphrase"](#) oder ["Konsolenpasswörter für Nodes"](#)
- ["Identitätsföderation verwenden"](#)
- ["SSO konfigurieren"](#)

Wartungsmenü

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

Aufgaben

Zu den Wartungsaufgaben gehören:

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

System

Zu den Systemwartungsaufgaben, die Sie durchführen können, gehören:

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

- ["Upgrade von SANtricity OS auf SG5700 Storage Controllern mit Grid Manager"](#)

Netzwerk

Zu den Netzwerkwartungsaufgaben, die Sie durchführen können, gehören:

- ["DNS-Server konfigurieren"](#)
- ["Grid Network-Subnetze aktualisieren"](#)
- ["NTP Server verwalten"](#)

Support Menü

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

Tools

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

- ["Konfiguration von AutoSupport"](#)
- ["Diagnose ausführen"](#) zum aktuellen Zustand des Grid
- ["Protokolldateien und Systemdaten sammeln"](#)
- ["Support-Metriken überprüfen"](#)



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

Sonstige

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

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

Erkunden Sie den StorageGRID Tenant Manager

Das ["Tenant Manager"](#) ist die browserbasierte grafische Benutzeroberfläche, über die Mandantenbenutzer ihre Speicherkonten konfigurieren, verwalten und überwachen.



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

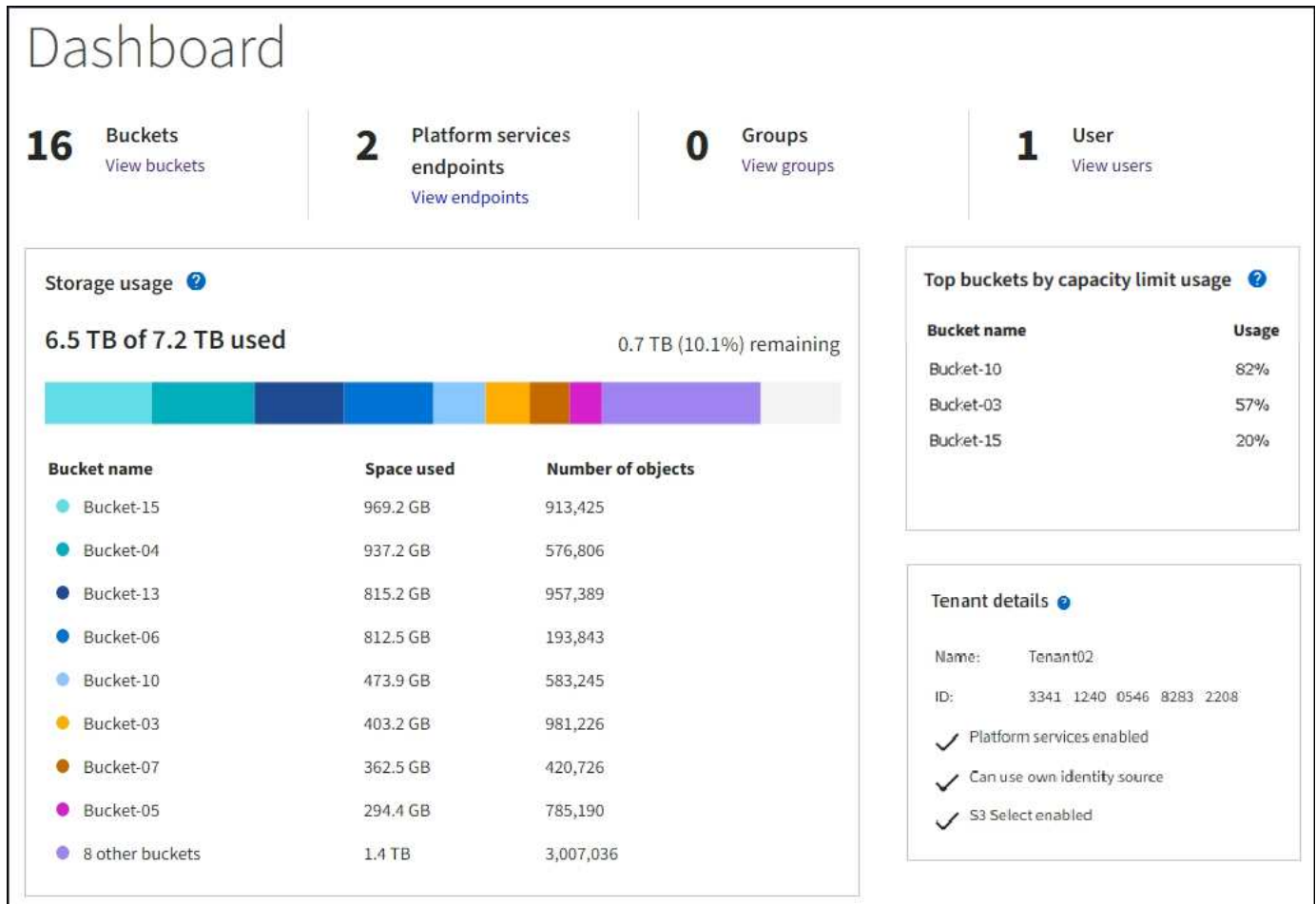
Wenn sich Mandantenbenutzer beim Tenant Manager anmelden, stellen sie eine Verbindung zu einem Admin Node her.

Tenant Manager Dashboard

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

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

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



Speichermenü (S3)

Dieses Menü ermöglicht S3 Benutzern Folgendes:

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

Meine Zugangsschlüssel

S3-Tenant-Benutzer können Zugriffsschlüssel wie folgt verwalten:

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



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

Buckets

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

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

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

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

Endpunkte für Plattformdienste

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

Grid Federation Verbindungen

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

Menü „Access Management“

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.