



Managen Sie Storage-Nodes

StorageGRID

NetApp
October 03, 2025

Inhalt

Managen Sie Storage-Nodes	1
Allgemeines zum Verwalten von Storage-Nodes	1
Was ist ein Storage-Node?	1
Was ist der ADC-Dienst?	1
Was ist der DDS-Service?	2
Was ist der LDR-Service?	3
Storage-Optionen managen	5
Was ist Objektsegmentierung?	5
Was sind Wasserzeichen für Storage-Volumes?	6
Management von Objekt-Metadaten-Storage	10
Was sind Objekt-Metadaten?	10
Wie werden Objekt-Metadaten gespeichert?	10
Wo werden Objekt-Metadaten gespeichert?	11
Einstellung für reservierten Speicherplatz für Metadaten	11
Tatsächlich reservierter Speicherplatz für Metadaten	13
Beispiel für den tatsächlich reservierten Metadatenspeicherplatz	14
Zulässiger Metadatenspeicherplatz	14
Beispiel für zulässigen Metadatenspeicherplatz	15
Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität	16
Globale Einstellungen für gespeicherte Objekte konfigurieren	17
Gespeicherte Objektkomprimierung konfigurieren	17
Gespeicherte Objektverschlüsselung konfigurieren	18
Konfigurieren Sie die gespeicherte Objekt-Hashing	19
Konfigurationseinstellungen für Storage-Nodes	20
LDR	20
LDR-Datenspeicher	21
LDR-Speicher	21
LDR-Überprüfung	22
LDR Erasure Coding	22
LDR-Replizierung	23
Management vollständiger Storage-Nodes	24
Hinzufügen von Storage-Volumes	24
Hinzufügen von Shelves zur Storage-Erweiterung	24
Storage-Nodes Hinzufügen	24

Managen Sie Storage-Nodes

Allgemeines zum Verwalten von Storage-Nodes

Storage-Nodes stellen Festplattenkapazität und Services zur Verfügung. Das Verwalten von Storage-Nodes umfasst Folgendes:

- Management der Storage-Optionen
- Um zu verstehen, welche Wasserzeichen für das Storage-Volume sind und wie Sie mit Wasserzeichen-Überschreibungen steuern können, wann Storage-Nodes schreibgeschützt sind
- Monitoring und Management des Speicherplatzes, der für Objektmetadaten verwendet wird
- Globale Einstellungen für gespeicherte Objekte konfigurieren
- Konfigurationseinstellungen für Speicherknoten werden angewendet
- Verwalten vollständiger Speicherknoten

Was ist ein Storage-Node?

Storage-Nodes managen und speichern Objektdaten und Metadaten. Jedes StorageGRID System muss mindestens drei Storage-Nodes aufweisen. Wenn Sie über mehrere Standorte verfügen, muss jeder Standort im StorageGRID System auch drei Storage-Nodes aufweisen.

Ein Storage Node umfasst die Services und Prozesse, die zum Speichern, Verschieben, Überprüfen und Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind. Auf der Seite **NODES** können Sie detaillierte Informationen zu den Speicherknoten anzeigen.

Was ist der ADC-Dienst?

Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen miteinander. Der ADC-Service wird auf jedem der ersten drei Storage-Nodes an einem Standort gehostet.

Der ADC-Dienst verwaltet Topologiedaten, einschließlich Standort und Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden muss, kontaktiert er einen ADC-Service, um den besten Grid-Knoten für die Bearbeitung seiner Anforderung zu finden. Darüber hinaus behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung bei, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann. ADC-Informationen für einen Speicherknoten können Sie auf der Seite Grid Topology anzeigen (**SUPPORT Grid Topology**).

Zur Erleichterung von verteilten und isanded-Operationen synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Services und Topologie mit den anderen ADC-Diensten im StorageGRID-System.

Im Allgemeinen unterhalten alle Rasterknoten eine Verbindung zu mindestens einem ADC-Dienst. So wird sichergestellt, dass die Grid-Nodes immer auf die neuesten Informationen zugreifen. Wenn Grid-Nodes verbunden sind, speichern sie Zertifikate anderer Grid-Nodes', sodass die Systeme auch dann weiterhin mit bekannten Grid-Nodes funktionieren können, wenn ein ADC-Service nicht verfügbar ist. Neue Grid-Knoten können nur Verbindungen über einen ADC-Dienst herstellen.

Durch die Verbindung jedes Grid-Knotens kann der ADC-Service Topologiedaten erfassen. Die Informationen zu diesem Grid-Node umfassen die CPU-Last, den verfügbaren Festplattenspeicher (wenn der Storage vorhanden ist), unterstützte Services und die Standort-ID des Grid-Node. Andere Dienste fragen den ADC-Service nach Topologiedaten durch Topologieabfragen. Der ADC-Dienst reagiert auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID-System empfangen wurden.

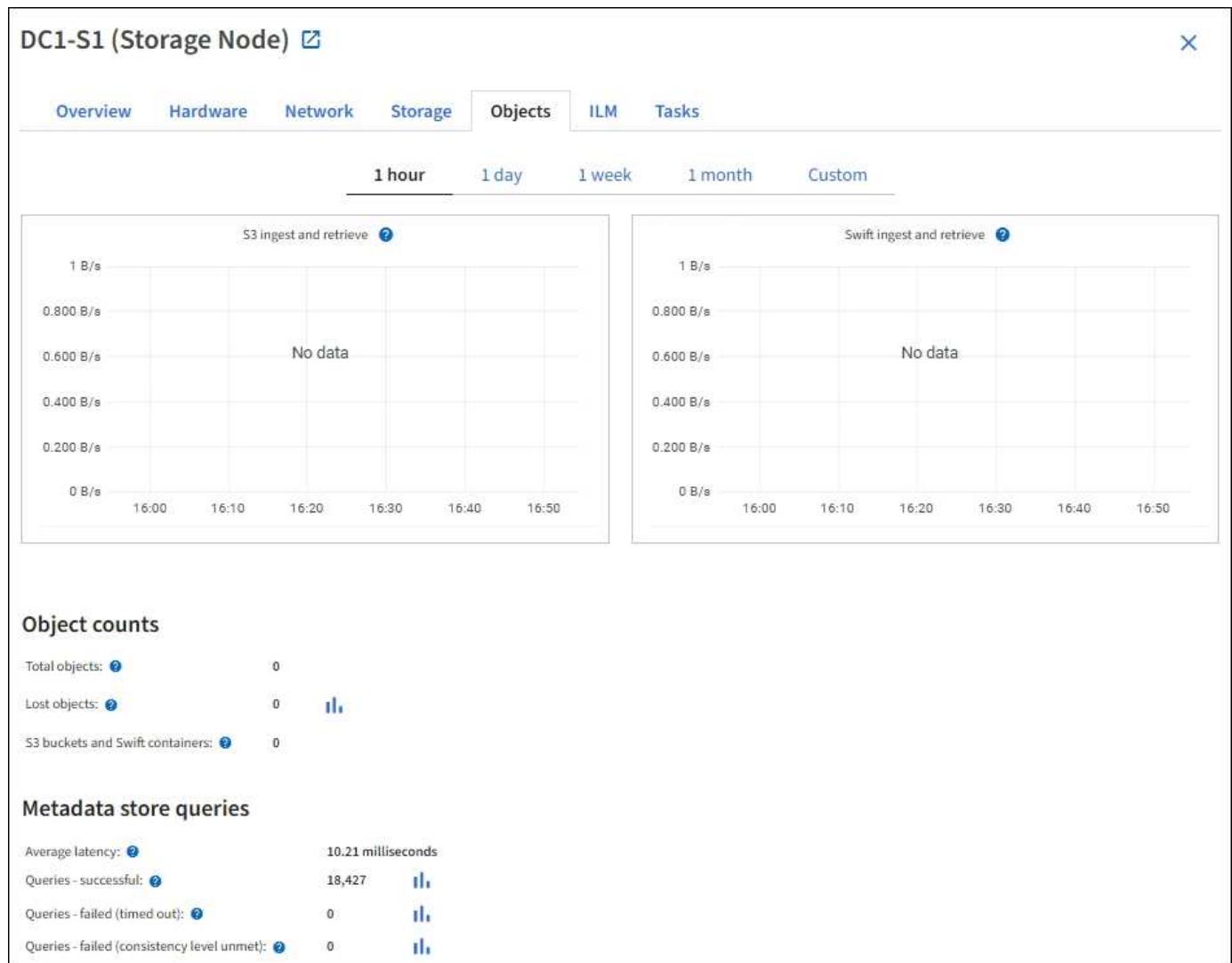
Was ist der DDS-Service?

Der DDS-Service (Distributed Data Store) wird von einem Storage-Node gehostet und führt Hintergrundaufgaben zu den im StorageGRID-System gespeicherten Objektmetadaten durch.

Anzahl der Objekte

Der DDS-Dienst verfolgt die Gesamtzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtzahl der über die unterstützten Schnittstellen (S3 oder Swift) des Systems aufgenommenen Objekte.

Die Gesamtzahl der Objekte wird auf der Registerkarte Objekte auf der Registerkarte Knoten für jeden Speicherknoten angezeigt.



Abfragen

Sie können die durchschnittliche Zeit für die Ausführung einer Abfrage zum Metadatenspeicher durch den

spezifischen DDS-Dienst, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtanzahl der fehlgeschlagenen Abfragen für ein Timeout-Problem identifizieren.

Vielleicht möchten Sie nach Abfrageinformationen suchen, um den Zustand des Metadatenspeichers, Cassandra, zu überwachen. Dies hat Auswirkungen auf die Aufnahme- und Abrufleistung des Systems. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl von verfügbaren Metadatenspeichern zum Zeitpunkt der Durchführung einer Abfrage durch den spezifischen DDS-Service.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen. Siehe [Führen Sie eine Diagnose aus](#).

Konsistenzgarantien und -Kontrollen

StorageGRID garantiert die Konsistenz zwischen Lese- und Schreibvorgängen bei neu erstellten Objekten. Jeder GET-Vorgang nach einem erfolgreich abgeschlossenen PUT-Vorgang kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschen bleiben irgendwann konsistent.

Was ist der LDR-Service?

Der Service Local Distribution Router (LDR) wird von jedem Speicherknoten gehostet und übernimmt den Content-Transport des StorageGRID-Systems. Der Content-Transport umfasst viele Aufgaben, einschließlich Datenspeicherung, Routing und Bearbeitung von Anfragen. Der LDR-Service erledigt den Großteil der harten Arbeit des StorageGRID-Systems durch die Handhabung von Datenübertragungslasten und Datenverkehrsfunktionen.

Der LDR-Service übernimmt folgende Aufgaben:

- Abfragen
- Information Lifecycle Management-Aktivitäten (ILM)
- Löschen von Objekten
- Objekt-Storage
- Objektdatenübertragung von einem anderen LDR-Service (Storage Node)
- Datenspeicher-Management
- Protokollschnittstellen (S3 und Swift)

Der LDR-Service managt auch die Zuordnung von S3- und Swift-Objekten zu den eindeutigen „Content Handles“ (UUIDs), die das StorageGRID System jedem aufgenommene Objekt zuweist.

Abfragen

LDR-Abfragen umfassen Abfragen zum Objektspeicherort während Abruf- und Archivierungsvorgängen. Sie können die durchschnittliche Zeit zum Ausführen einer Abfrage, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtzahl der Abfragen, die aufgrund eines Timeout-Problems fehlgeschlagen sind, identifizieren.

Sie können Abfrageinformationen prüfen, um den Zustand des Metadatenspeichers zu überwachen und die Aufnahme- und Abrufleistung des Systems zu beeinträchtigen. Wenn beispielsweise die Latenz für eine

durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl an verfügbaren Metadatenspeichern zum Zeitpunkt einer Abfrage durch den spezifischen LDR-Service.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen. Siehe [Führen Sie eine Diagnose aus](#).

ILM-Aktivität

Mithilfe der ILM-Metriken (Information Lifecycle Management) können Sie die Bewertung von Objekten für die ILM-Implementierung durchführen. Sie können diese Kennzahlen auf dem Dashboard oder auf **NODES Storage Node ILM** anzeigen.

Objektspeicher

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

Auf der Seite Knoten Speicher sehen Sie die Objektspeicher für einen Speicherknoten.

Object stores						
ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

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

Um sicherzustellen, dass selbst der Speicherplatz für replizierte Kopien genutzt wird, werden Objektdaten für ein bestimmtes Objekt auf Basis des verfügbaren Storage in einem Objektspeicher gespeichert. Wenn ein oder mehrere Objektspeichern die Kapazität voll haben, speichern die übrigen Objektspeicher weiterhin Objekte, bis kein Platz mehr auf dem Speicherknoten vorhanden ist.

Metadatensicherung

Objektmetadaten sind Informationen mit oder eine Beschreibung eines Objekts, z. B. Änderungszeit des Objekts oder der Storage-Standort. StorageGRID speichert Objekt-Metadaten in einer Cassandra-Datenbank, die über eine Schnittstelle zum LDR-Service verfügt.

Um Redundanz sicherzustellen und so vor Verlust zu schützen, werden an jedem Standort drei Kopien von Objekt-Metadaten aufbewahrt. Die Kopien werden gleichmäßig auf alle Storage-Nodes an jedem Standort

verteilt. Diese Replikation ist nicht konfigurierbar und wird automatisch ausgeführt.

Management von Objekt-Metadaten-Storage

Storage-Optionen managen

Storage-Optionen umfassen die Einstellungen für die Objektsegmentierung, die aktuellen Werte für Storage-Volume-Wasserzeichen und die Einstellung für reservierten Speicherplatz. Sie können auch die S3- und Swift-Ports anzeigen, die vom veralteten CLB-Dienst auf Gateway-Nodes und vom LDR-Service auf Storage-Nodes verwendet werden.

Informationen zu Port-Zuweisungen finden Sie unter [Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen](#).

Storage Options

Overview

Configuration

Storage Options Overview
Updated: 2021-11-23 11:01:41 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

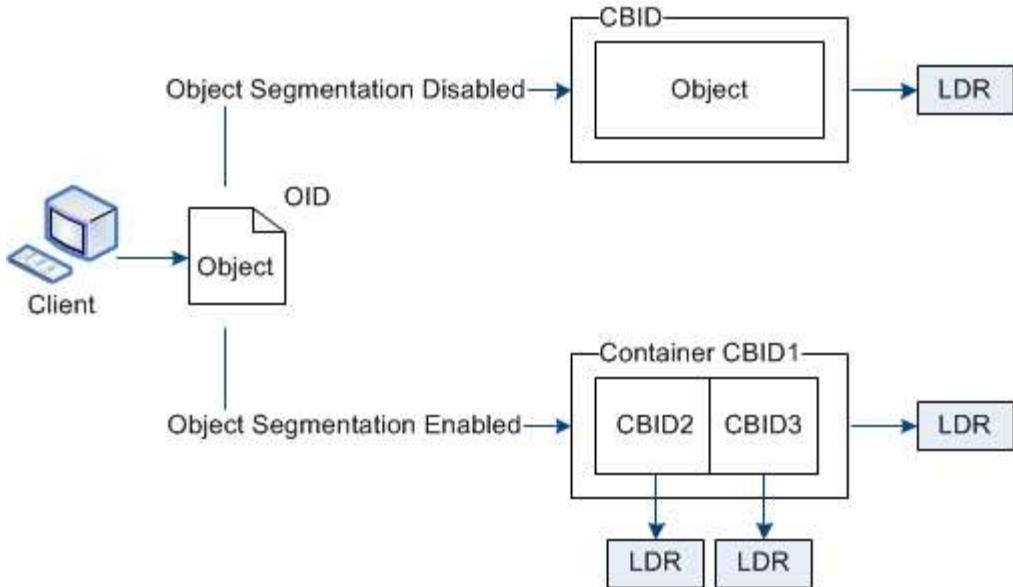
Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

Was ist Objektsegmentierung?

Objektsegmentierung ist der Vorgang, ein Objekt in eine Sammlung kleinerer Objekte mit fester Größe aufzuteilen, um die Speicherung und Ressourcennutzung für große Objekte zu optimieren. Auch beim S3-Multi-Part-Upload werden segmentierte Objekte erstellt, wobei ein Objekt die einzelnen Teile darstellt.

Wenn ein Objekt in das StorageGRID-System aufgenommen wird, teilt der LDR-Service das Objekt in Segmente auf und erstellt einen Segment-Container, der die Header-Informationen aller Segmente als Inhalt auflistet.



Beim Abruf eines Segment-Containers fasst der LDR-Service das ursprüngliche Objekt aus seinen Segmenten zusammen und gibt das Objekt dem Client zurück.

Der Container und die Segmente werden nicht notwendigerweise auf demselben Storage-Node gespeichert. Container und Segmente können auf jedem Storage-Node innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

Jedes Segment wird vom StorageGRID System unabhängig behandelt und trägt zur Anzahl der Attribute wie verwaltete Objekte und gespeicherte Objekte bei. Wenn ein im StorageGRID System gespeichertes Objekt beispielsweise in zwei Segmente aufgeteilt wird, erhöht sich der Wert von verwalteten Objekten nach Abschluss der Aufnahme um drei Segmente:

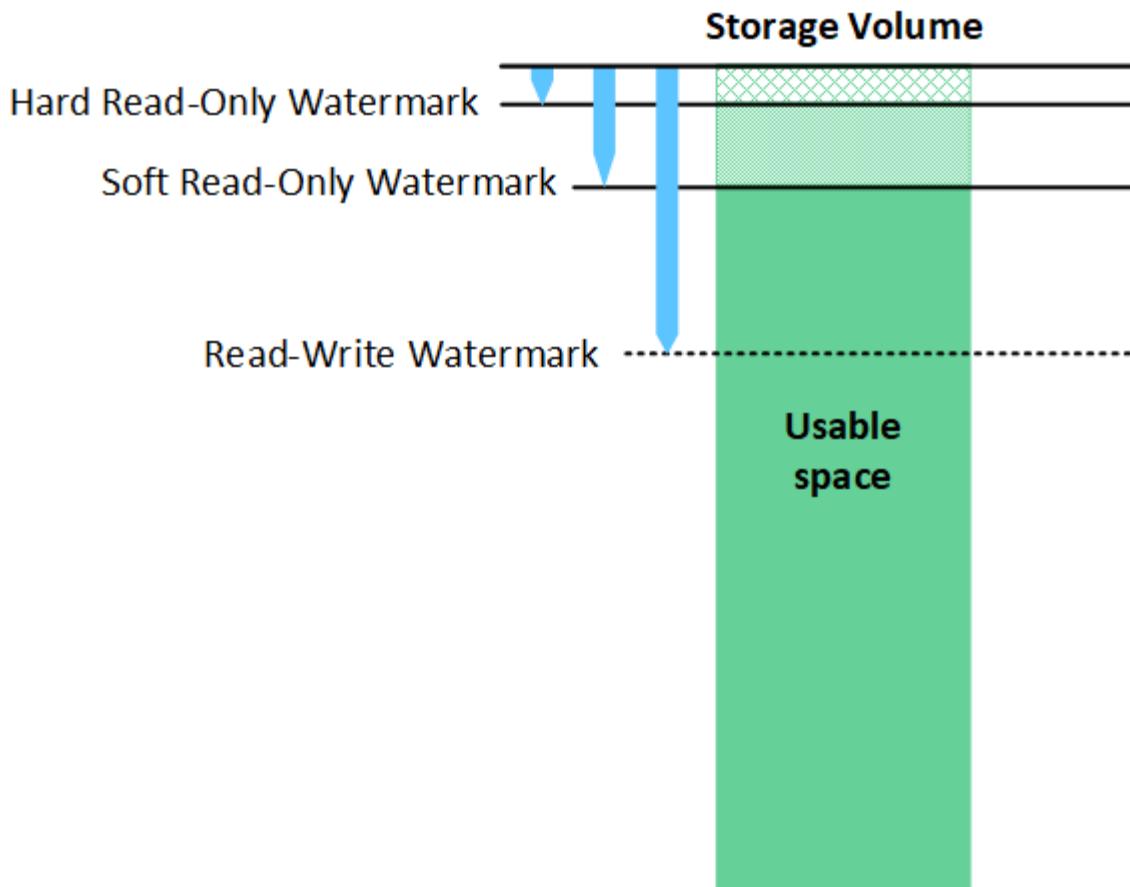
Segmentcontainer + Segment 1 + Segment 2 = drei gespeicherte Objekte

Die Performance beim Umgang mit großen Objekten lässt sich verbessern, indem Folgendes sichergestellt wird:

- Jedes Gateway und jeder Storage-Node verfügt über eine ausreichende Netzwerkbandbreite für den erforderlichen Durchsatz. Konfigurieren Sie beispielsweise separate Grid- und Client-Netzwerke auf 10-Gbit/s-Ethernet-Schnittstellen.
- Für den erforderlichen Durchsatz werden ausreichend Gateway und Storage-Nodes implementiert.
- Jeder Storage-Node verfügt über eine ausreichende Festplatten-I/O-Performance für den erforderlichen Durchsatz.

Was sind Wasserzeichen für Storage-Volumes?

StorageGRID verwendet drei Storage-Volume-Wasserzeichen, um sicherzustellen, dass Storage-Nodes sicher in einen schreibgeschützten Zustand überführt werden, bevor deren Speicherplatz kritisch knapp wird. Damit können Storage-Nodes, die aus einem schreibgeschützten Zustand migriert wurden, erneut Lese- und Schreibvorgänge werden.



Storage Volume-Wasserzeichen gelten nur für den Speicherplatz, der für replizierte und nach Datenkonsistenz (Erasure Coding) verwendet wird. Weitere Informationen über den Speicherplatz, der für Objekt-Metadaten auf Volume 0 reserviert ist, finden Sie unter [Management von Objekt-Metadaten-Storage](#).

Was ist das Soft Read-Only Watermark?

Das **Speichervolumen Soft Read-Only Watermark** ist das erste Wasserzeichen, das angibt, dass der für Objektdaten nutzbare Speicherplatz eines Speicherknoten voll wird.

Wenn jedes Volume in einem Storage-Node weniger freien Speicherplatz als das Soft Read-Only-Wasserzeichen dieses Volumes besitzt, wechselt der Storage-Node in den Modus *read-only*. Schreibgeschützter Modus bedeutet, dass der Storage Node für den Rest des StorageGRID Systems schreibgeschützte Dienste anbietet, aber alle ausstehenden Schreibanforderungen erfüllt.

Angenommen, jedes Volume in einem Speicherknoten hat einen Soft Read-Only-Wasserzeichen von 10 GB. Sobald jedes Volume weniger als 10 GB freien Speicherplatz hat, wechselt der Storage-Node in den Modus „Soft Read“.

Was ist die Hard Read-Only Watermark?

Das **Speichervolumen Hard Read-Only Watermark** ist das nächste Wasserzeichen, um anzuzeigen, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird.

Wenn der freie Speicherplatz auf einem Volume kleiner ist als das harte Read-Only-Wasserzeichen dieses Volumes, schlägt das Schreiben auf das Volume fehl. Schreibvorgänge auf anderen Volumes können jedoch fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes kleiner als ihre Hard Read-Only-

Wasserzeichen ist.

Angenommen, jedes Volume in einem Speicherknoten hat einen Hard Read-Only-Wasserzeichen von 5 GB. Sobald jedes Volume weniger als 5 GB freien Speicherplatz hat, akzeptiert der Speicherknoten keine Schreibanforderungen mehr.

Der Hard Read-Only-Wasserzeichen ist immer kleiner als der Soft Read-Only-Wasserzeichen.

Was ist der Read-Write-Wasserzeichen?

Das **Storage Volume Read-Write Watermark** gilt nur für Storage-Nodes, die in den schreibgeschützten Modus gewechselt sind. Er bestimmt, wann der Node wieder Lese-/Schreibzugriff werden kann. Wenn der freie Speicherplatz auf einem Speichervolumen in einem Speicherknoten größer ist als das Read-Write-Wasserzeichen dieses Volumes, wechselt der Knoten automatisch zurück in den Lese-Schreib-Zustand.

Angenommen, der Storage-Node ist in den schreibgeschützten Modus migriert. Nehmen Sie auch an, dass jedes Volume ein Read-Write-Wasserzeichen von 30 GB hat. Sobald der freie Speicherplatz eines beliebigen Volumes auf 30 GB ansteigt, wird der Node erneut zum Lesen/Schreiben.

Der Read-Write-Wasserzeichen ist immer größer als der Soft Read-Only-Wasserzeichen und der Hard Read-Only-Wasserzeichen.

Anzeigen von Wasserzeichen für Speichervolumen

Sie können die aktuellen Einstellungen für Wasserzeichen und die systemoptimierten Werte anzeigen. Wenn keine optimierten Wasserzeichen verwendet werden, können Sie festlegen, ob Sie die Einstellungen anpassen können oder sollten.

Was Sie benötigen

- Sie haben das Upgrade auf StorageGRID 11.6 abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Root-Zugriffsberechtigung.

Aktuelle Wasserzeichen-Einstellungen anzeigen

Im Grid Manager können Sie die aktuellen Einstellungen für Speicherwasserzeichen anzeigen.

Schritte

1. Wählen Sie **KONFIGURATION System Speicheroptionen**.
2. Sehen Sie sich im Abschnitt Speicherwasserzeichen die Einstellungen für die drei Überschreibungen der Speichervolumen an.

Storage Options

[Overview](#)

[Configuration](#)

[]
Storage Options Overview
Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

- Wenn die Wasserzeichen **0** überschreiben, sind alle drei Wasserzeichen für jedes Speichervolumen auf jedem Speicherknoten optimiert, basierend auf der Größe des Speicherknoten und der relativen Kapazität des Volumes.

Dies ist die Standardeinstellung und die empfohlene Einstellung. Sie sollten diese Werte nicht aktualisieren. Nach Bedarf können Sie optional [Anzeigen optimierter Speicherabdrücke](#).

- Wenn es sich bei den Wasserzeichen um nicht-0-Werte handelt, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Es wird nicht empfohlen, benutzerdefinierte Wasserzeichen zu verwenden. Befolgen Sie die Anweisungen für [Fehlerbehebung Warnungen bei niedriger Schreibschutzmarke überschreiben](#) Um zu bestimmen, ob Sie die Einstellungen anpassen können oder sollen.

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

- Wählen Sie **SUPPORT Tools Kennzahlen** aus.
- Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
- Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den

9

Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

4. Um das empfohlene maximale Softread-only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_maximum_optimized_soft_READONLY_watermark
```

In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

Management von Objekt-Metadaten-Storage

Die Kapazität der Objektmetadaten eines StorageGRID Systems steuert die maximale Anzahl an Objekten, die auf diesem System gespeichert werden können. Um sicherzustellen, dass Ihr StorageGRID System über ausreichend Platz zum Speichern neuer Objekte verfügt, müssen Sie wissen, wo und wie StorageGRID Objekt-Metadaten speichert.

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.

Für ein Objekt in StorageGRID enthalten die Objektmetadaten die folgenden Informationstypen:

- 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.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, Segment-IDs und Datengrößen.

Wie werden Objekt-Metadaten gespeichert?

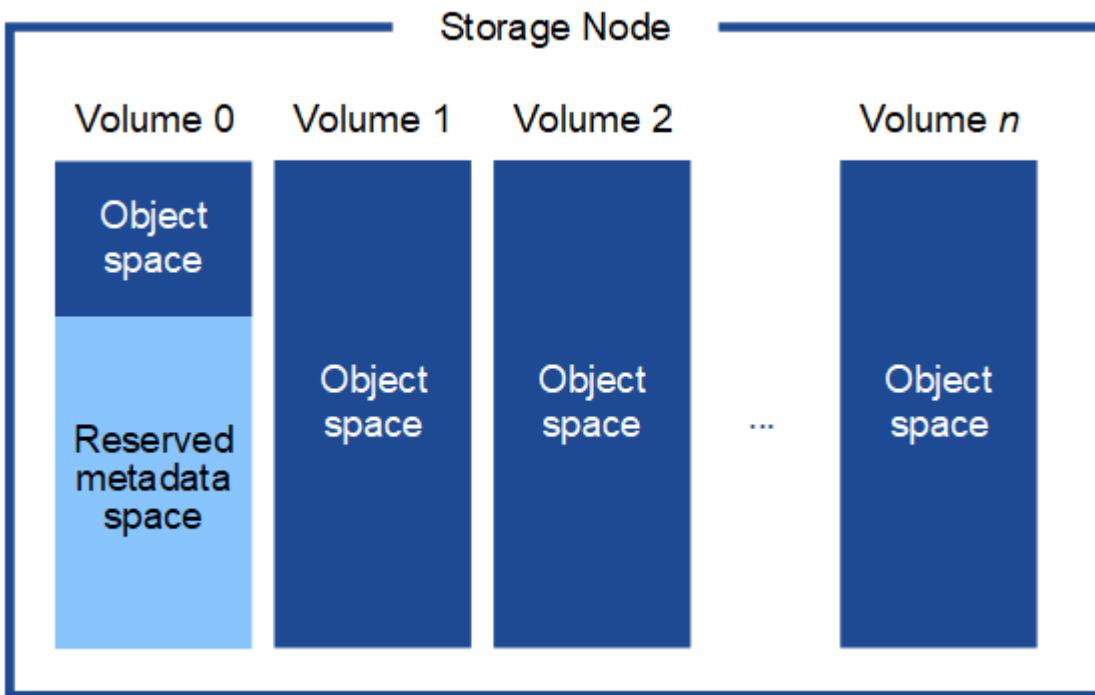
StorageGRID speichert Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert werden. Um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen, speichert StorageGRID drei Kopien der Metadaten für alle Objekte im System an jedem Standort. Die drei Kopien der Objektmetadaten werden gleichmäßig auf alle Storage-Nodes an jedem Standort verteilt.

Diese Abbildung zeigt die Speicherknoten an zwei Standorten. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten, die auf die Storage-Nodes an diesem Standort verteilt werden.



Wo werden Objekt-Metadaten gespeichert?

Diese Abbildung zeigt die Storage Volumes für einen einzelnen Storage-Node.



Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Sie verwendet den reservierten Speicherplatz zum Speichern von Objektmetadaten und zum Ausführen wichtiger Datenbankvorgänge. Alle übrigen Speicherplatz auf dem Storage Volume 0 und allen anderen Storage Volumes im Storage Node werden ausschließlich für Objektdaten (replizierte Kopien und nach Datenkonsistenz) verwendet.

Die Menge an Speicherplatz, die für Objektmetadaten auf einem bestimmten Storage-Node reserviert ist, hängt von einer Reihe von Faktoren ab, die im Folgenden beschrieben werden.

Einstellung für reservierten Speicherplatz für Metadaten

Die Einstellung *Metadaten Reserved Space* stellt die Menge an Speicherplatz dar, die für Metadaten auf Volume 0 jedes Storage-Node reserviert wird. Wie in der Tabelle dargestellt, basiert der Standardwert dieser Einstellung für StorageGRID 11.6 auf dem folgenden:

- Die Softwareversion, die Sie bei der Erstinstallation von StorageGRID verwendet haben.
- Die RAM-Menge auf jedem Storage-Node.

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz bei Metadaten für StorageGRID 11.6
11.5/11.6	128 GB oder mehr auf jedem Storage-Node im Grid	8 TB (8,000 GB)
	Weniger als 128 GB auf jedem Storage-Node im Grid	3 TB (3,000 GB)
11.1 bis 11.4	128 GB oder mehr auf jedem Speicherknoten an einem beliebigen Standort	4 TB (4,000 GB)
	Weniger als 128 GB auf jedem Speicherknoten an jedem Standort	3 TB (3,000 GB)
11.0 oder früher	Beliebiger Betrag	2 TB (2,000 GB)

So zeigen Sie die Einstellung für den reservierten Metadatenspeicherplatz für Ihr StorageGRID-System an:

1. Wählen Sie **KONFIGURATION System Speicheroptionen**.
2. Suchen Sie in der Tabelle Speicherwasserzeichen **Metadatenreservierter Speicherplatz**.



Storage Options Overview
Updated: 2021-12-10 13:53:01 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	8,000 GB

Im Screenshot beträgt der Wert **Metadaten reservierter Speicherplatz** 8,000 GB (8 TB). Dies ist die Standardeinstellung für eine neue StorageGRID 11.6-Installation, bei der jeder Speicherknoten 128 GB oder

mehr RAM hat.

Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur Einstellung „systemweiter reservierter Speicherplatz für Metadaten“ wird für jeden Storage-Node der tatsächliche reservierte Speicherplatz für Objektmetadaten ermittelt. Für jeden bestimmten Storage-Node hängt der tatsächliche reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Node und der systemweiten Einstellung **Metadaten reservierter Speicherplatz** ab.

Größe von Volume 0 für den Node	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht in der Produktion)	10% des Volumens 0
500 GB oder mehr	Die kleineren Werte: <ul style="list-style-type: none">• Lautstärke 0• Einstellung für reservierten Speicherplatz für Metadaten

So zeigen Sie den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Speicherknoten an:

1. Wählen Sie im Grid Manager **NODES Storage Node** aus.
2. Wählen Sie die Registerkarte **Storage** aus.
3. Bewegen Sie den Cursor über das Diagramm verwendete Speicherdaten — Objektmetadaten und suchen Sie den Wert **tatsächlich reserviert**.



Im Screenshot beträgt der **tatsächliche reservierte** Wert 8 TB. Dieser Screenshot ist für einen großen Speicherknoten in einer neuen StorageGRID 11.6 Installation. Da die Einstellung für den systemweiten reservierten Speicherplatz für Metadaten kleiner als das Volume 0 für diesen Storage-Node ist, entspricht der tatsächliche reservierte Speicherplatz für diesen Node der Einstellung für den reservierten Speicherplatz.

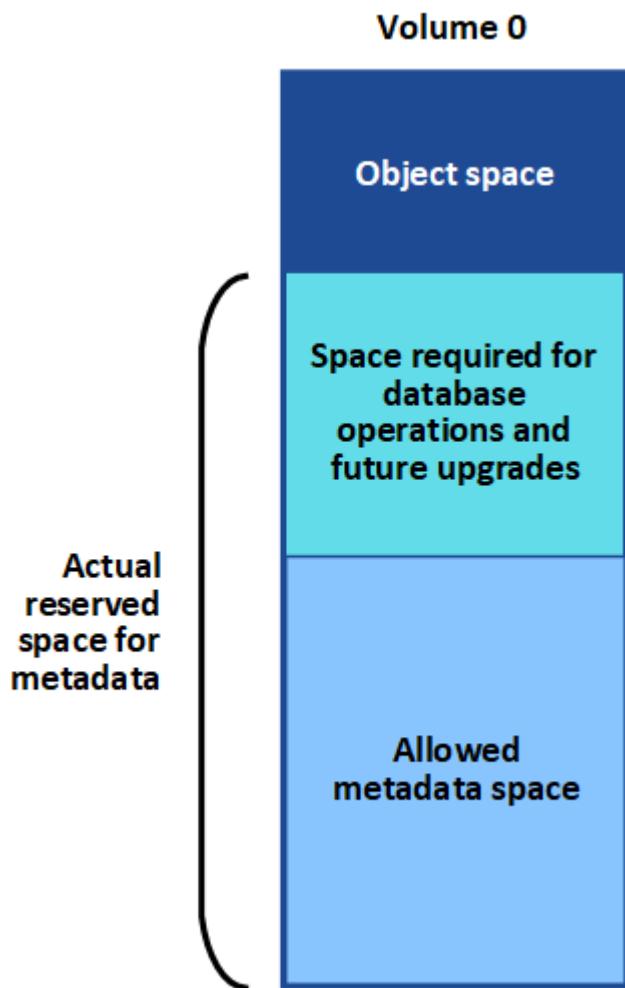
Beispiel für den tatsächlich reservierten Metadatenspeicherplatz

Angenommen, Sie installieren ein neues StorageGRID System unter Verwendung der Version 11.6. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für eine neue StorageGRID 11.6-Installation, wenn jeder Speicherknoten über mehr als 128 GB RAM verfügt.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)

Zulässiger Metadatenspeicherplatz

Der tatsächlich reservierte Speicherplatz jedes Storage-Node für Metadaten wird in den Speicherplatz für Objekt-Metadaten (den „zulässigen Metadatenspeicherplatz“) und den Platzbedarf für wichtige Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.

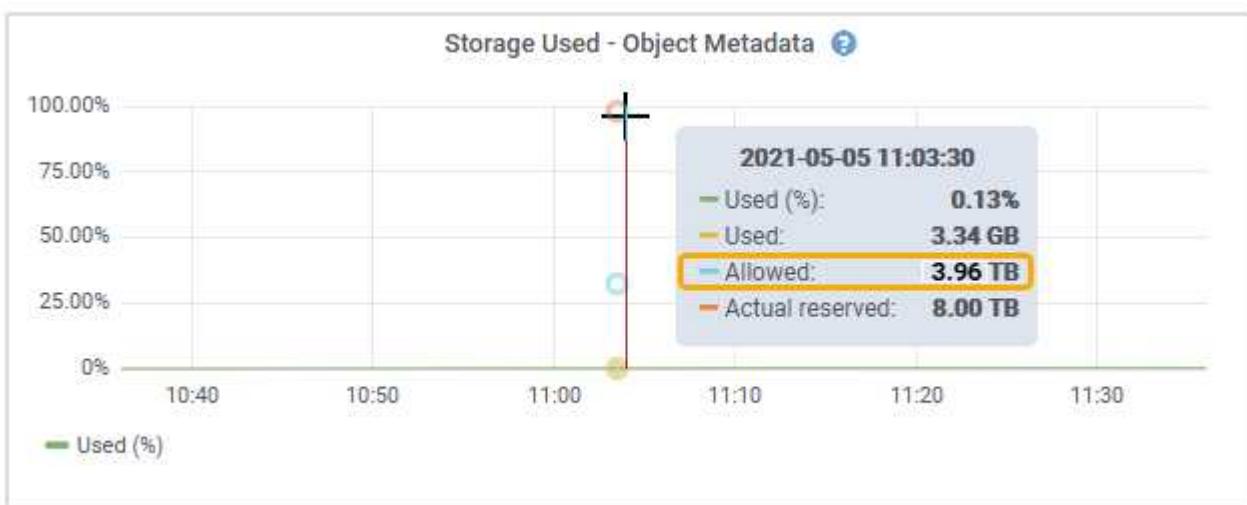


Die folgende Tabelle zeigt, wie StorageGRID den **zulässigen Metadatenspeicherplatz** für verschiedene Storage-Nodes berechnet, basierend auf der Speichermenge für den Node und dem tatsächlich reservierten Speicherplatz für Metadaten.

Speichermenge auf Speicherknoten			
lt; 128 GB	gt;= 128 GB		Tatsächlich reservierter Platz für Metadaten
lt;= 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.98 TB	gt; 4 TB

So zeigen Sie den zulässigen Metadatenspeicherplatz für einen Speicherknoten an:

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie den Speicherknoten aus.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Bewegen Sie den Cursor über das Diagramm verwendete Speicherdaten — Objektmetadaten und suchen Sie den Wert **zulässig**.



Im Screenshot beträgt der **zulässige**-Wert 3.96 TB, was der maximale Wert für einen Storage Node ist, dessen tatsächlicher reservierter Speicherplatz für Metadaten mehr als 4 TB beträgt.

Der **zulässige**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Beispiel für zulässigen Metadatenspeicherplatz

Angenommen, Sie installieren ein StorageGRID System mit Version 11.6. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für StorageGRID 11.6, wenn jeder Speicherknoten mehr als 128 GB RAM hat.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 3 TB, basierend auf der im angegebenen Berechnung [Tabelle für zulässigem Speicherplatz für Metadaten](#): (Tatsächlich reservierter Platz für Metadaten – 1 TB) × 60%, bis zu einem Maximum von 3.96 TB.

Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität

Wie oben beschrieben, verteilt StorageGRID Objektmetadaten gleichmäßig über Storage-Nodes an jedem Standort. Wenn ein Standort Storage-Nodes unterschiedlicher Größen enthält, bestimmt der kleinste Node am Standort die Metadaten-Kapazität des Standorts.

Beispiel:

- Sie haben ein Raster mit drei Storage Nodes unterschiedlicher Größe an einem einzigen Standort.
- Die Einstellung **Metadaten reservierter Platz** beträgt 4 TB.
- Die Storage-Nodes haben die folgenden Werte für den tatsächlich reservierten Metadatenspeicherplatz und den zulässigen Metadatenspeicherplatz.

Storage-Node	Größe von Volumen 0	Tatsächlich reservierter Metadatenspeicherplatz	Zulässiger Metadatenspeicherplatz
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Da Objektmetadaten gleichmäßig auf die Storage-Nodes an einem Standort verteilt werden, kann jeder Node in diesem Beispiel nur 1.32 TB Metadaten enthalten. Der zusätzlich zulässige Metadatenspeicherplatz von 0.66 TB für SN2 und SN3 kann nicht verwendet werden.



Da StorageGRID alle Objektmetadaten für ein StorageGRID System an jedem Standort speichert, wird die Gesamtkapazität der Metadaten eines StorageGRID Systems durch die Objektmetadaten des kleinsten Standorts bestimmt.

Und da die Objektmetadaten die maximale Objektanzahl steuern, wenn einem Node die Metadatenkapazität ausgeht, ist das Grid effektiv voll.

Verwandte Informationen

- Informationen zum Monitoring der Objektmetadaten für jeden Storage-Node finden Sie unter [Monitoring und Fehlerbehebung](#).
- Um die Kapazität der Objektmetadaten für Ihr System zu erhöhen, fügen Sie neue Storage-Nodes hinzu. Gehen Sie zu [Erweitern Sie Ihr Raster](#).

Globale Einstellungen für gespeicherte Objekte konfigurieren

Gespeicherte Objektkomprimierung konfigurieren

Über die Grid-Option „gespeicherte Objekte komprimieren“ lässt sich die Größe der in StorageGRID gespeicherten Objekte reduzieren, sodass Objekte weniger Storage belegen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Grid-Option „gespeicherte Objekte komprimieren“ ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, versucht StorageGRID, jedes Objekt beim Speichern mit verlustfreier Komprimierung zu komprimieren.



Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

Bevor Sie diese Option aktivieren, beachten Sie Folgendes:

- Die Komprimierung sollte nur aktiviert werden, wenn die gespeicherten Daten komprimierbar sind.
- Applikationen, die Objekte in StorageGRID speichern, komprimieren möglicherweise Objekte, bevor sie gespeichert werden. Wenn bereits eine Client-Applikation ein Objekt komprimiert hat, bevor sie in StorageGRID gespeichert wird, wird die Komprimierung gespeicherter Objekte die Größe eines Objekts nicht weiter verringert.
- Aktivieren Sie die Komprimierung nicht, wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn die Grid-Option „gespeicherte Objekte komprimieren“ aktiviert ist, sollten S3- und Swift-Client-Applikationen die AUSFÜHRUNG VON GET-Objektoperationen vermeiden, die einen Bereich von Bytes angeben. Diese Vorgänge „range Read“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. VORGÄNGE ZUM ABRUFEN von Objekten, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Optionen für gespeicherte Objekte das Kontrollkästchen **gespeicherte Objekte komprimieren**.

Stored Object Options



3. Wählen Sie **Speichern**.

Gespeicherte Objektverschlüsselung konfigurieren

Sie können gespeicherte Objekte verschlüsseln, wenn Sie sicherstellen möchten, dass die Daten bei einer Gefährdung eines Objektspeichers nicht in lesbare Form abgerufen werden können. Objekte sind standardmäßig nicht verschlüsselt.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme durch S3 oder Swift. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, aber es werden keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben aktuell verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.



Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

Gespeicherte Objekte können mit dem Verschlüsselungsalgorithmus AES-128 oder AES-256 verschlüsselt werden.

Die Einstellung „gespeicherte Objektverschlüsselung“ gilt nur für S3 Objekte, die nicht durch Verschlüsselung auf Bucket- oder Objektebene verschlüsselt wurden.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Ändern Sie im Abschnitt Speicherte Objektoptionen die gespeicherte Objektverschlüsselung in **Keine** (Standard), **AES-128** oder **AES-256**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  None AES-128 AES-256

Stored Object Hashing  SHA-1 SHA-256

3. Wählen Sie **Speichern**.

Konfigurieren Sie die gespeicherte Objekt-Hashing

Die Option „Speichertes Objekt-Hashing“ gibt den Hash-Algorithmus an, der zur Überprüfung der Objektintegrität verwendet wird.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Standardmäßig werden Objektdaten mit dem SHA-1-Algorithmus gehasht. Der SHA-256-Algorithmus erfordert zusätzliche CPU-Ressourcen und wird im Allgemeinen nicht für die Integritätsprüfung empfohlen.



Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Ändern Sie im Abschnitt „Optionen für gespeicherte Objekte“ die Option „gespeicherte Objekt-Hashing“ in **SHA-1** (Standardeinstellung) oder **SHA-256**.

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  None AES-128 AES-256

Stored Object Hashing  SHA-1 SHA-256

3. Wählen Sie **Speichern**.

Konfigurationseinstellungen für Storage-Nodes

Jeder Storage Node verwendet eine Reihe von Konfigurationseinstellungen und Zählern. Möglicherweise müssen Sie die aktuellen Einstellungen anzeigen oder Zähler zurücksetzen, um Alarme zu löschen (Legacy-System).



Mit Ausnahme der in der Dokumentation ausdrücklich enthaltenen Anweisungen sollten Sie sich mit dem technischen Support in Verbindung setzen, bevor Sie die Konfigurationseinstellungen für den Storage-Node ändern. Nach Bedarf können Sie Ereigniszähler zurücksetzen, um ältere Alarme zu löschen.

So greifen Sie auf die Konfigurationseinstellungen und Zähler eines Speicherknotens zu:

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site Storage Node** aus.
3. Erweitern Sie den Speicherknoten, und wählen Sie den Dienst oder die Komponente aus.
4. Wählen Sie die Registerkarte **Konfiguration**.

In den folgenden Tabellen sind die Konfigurationseinstellungen für Storage Node zusammengefasst.

LDR

Attributname	Codieren	Beschreibung
HTTP-Status	HSTE	<p>Der aktuelle Status des HTTP-Protokolls für S3, Swift und andere interne StorageGRID-Zugriffe:</p> <ul style="list-style-type: none">• Offline: Es sind keine Vorgänge zulässig. Jede Client-Anwendung, die versucht, eine HTTP-Sitzung für den LDR-Dienst zu öffnen, erhält eine Fehlermeldung. Aktive Sitzungen werden ordnungsgemäß geschlossen.• Online: Der Vorgang wird normal fortgesetzt
Automatisches Starten von HTTP	HTAS	<ul style="list-style-type: none">• Wenn diese Option ausgewählt ist, hängt der Zustand des Systems bei Neustart vom Zustand der LDR Storage-Komponente ab. Wenn die LDR Storage-Komponente beim Neustart schreibgeschützt ist, ist auch die HTTP-Schnittstelle schreibgeschützt. Wenn die LDR Storage Komponente Online ist, ist HTTP auch Online. Andernfalls bleibt die HTTP-Schnittstelle im Status Offline.• Wenn diese Option nicht aktiviert ist, bleibt die HTTP-Schnittstelle offline, bis sie explizit aktiviert ist.

LDR-Datenspeicher

Attributname	Codieren	Beschreibung
Anzahl Verlorener Objekte Zurücksetzen	RCOR	Setzen Sie den Zähler für die Anzahl der verlorenen Objekte dieses Dienstes zurück.

LDR-Speicher

Attributname	Codieren	Beschreibung
Storage-Zustand - Gewünscht	SSDS	<p>Eine vom Benutzer konfigurierbare Einstellung für den gewünschten Status der Speicherkomponente. Der LDR-Dienst liest diesen Wert und versucht, den durch dieses Attribut angegebenen Status zu entsprechen. Der Wert wird bei Neustarts dauerhaft verwendet.</p> <p>Mit dieser Einstellung können Sie beispielsweise dazu zwingen, dass Speicher schreibgeschützt wird, selbst wenn genügend Speicherplatz vorhanden ist. Dies kann bei der Fehlerbehebung hilfreich sein.</p> <p>Das Attribut kann einen der folgenden Werte annehmen:</p> <ul style="list-style-type: none"> • Offline: Wenn der gewünschte Status Offline ist, schaltet der LDR-Dienst die LDR Storage-Komponente offline. • Schreibgeschützt: Wenn der gewünschte Status schreibgeschützt ist, verschiebt der LDR-Service den Speicherstatus auf schreibgeschützt und hört auf, neue Inhalte zu akzeptieren. Beachten Sie, dass Inhalte möglicherweise noch für kurze Zeit im Speicherknoten gespeichert werden, bis offene Sitzungen geschlossen sind. • Online: Den Wert bei Online während des normalen Systembetriebs belassen. Der Speicherstatus – der aktuelle Status der Speicherkomponente wird durch den Service dynamisch festgelegt, basierend auf dem Zustand des LDR-Service, z. B. der Menge des verfügbaren Objektspeicherspeichers. Wenn der Speicherplatz knapp ist, ist die Komponente schreibgeschützt.
Zeitüberschreitung Bei Der Integritätsprüfung	SHCT	Die Zeitgrenze in Sekunden, innerhalb derer ein Integritätstest abgeschlossen werden muss, damit ein Speichervolumen als ordnungsgemäß angesehen wird. Ändern Sie diesen Wert nur, wenn Sie dazu vom Support aufgefordert werden.

LDR-Überprüfung

Attributname	Codieren	Beschreibung
Fehlende Objekte Zurücksetzen Anzahl	VCMI	Setzt die Anzahl der erkannten fehlenden Objekte zurück (OMIS). Nur nach Abschluss der Objektprüfung verwenden. Fehlende replizierte Objektdaten werden vom StorageGRID System automatisch wiederhergestellt.
Verifizierungsrate	VPRI	Legen Sie die Geschwindigkeit fest, mit der die Hintergrundüberprüfung durchgeführt wird. Weitere Informationen zur Konfiguration der Hintergrundverifizierungsrate finden Sie unter.
Anzahl Der Beschädigten Objekte Zurücksetzen	VCCR	Setzen Sie den Zähler für beschädigte, replizierte Objektdaten zurück, die während der Hintergrundüberprüfung gefunden wurden. Mit dieser Option können Sie den Alarmzustand der beschädigten Objekte löschen, die erkannt wurden (OCOR). Weitere Informationen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.
Objekte In Quarantäne Löschen	OQRT	<p>Löschen Sie beschädigte Objekte aus dem Quarantäneverzeichnis, setzen Sie die Anzahl der isolierten Objekte auf Null zurück und löschen Sie den Alarm „Quarantäne Objekte erkannt“ (OQRT). Diese Option wird verwendet, nachdem beschädigte Objekte vom StorageGRID-System automatisch wiederhergestellt wurden.</p> <p>Wenn ein Alarm „Lost Objects“ ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen. In manchen Fällen können isolierte Objekte für die Datenwiederherstellung oder das Debuggen der zugrunde liegenden Probleme, die die beschädigten Objektkopien verursacht haben, nützlich sein.</p>

LDR Erasure Coding

Attributname	Codieren	Beschreibung
Zurücksetzen Der Fehleranzahl Für Schreibvorgänge	RWF.	Setzen Sie den Zähler auf Schreibfehler von Objektdaten mit Erasure-Coding-Verfahren auf den Storage-Node zurück.
Anzahl Der Fehlgeschlagene Lesevorgänge Zurücksetzen	RSRF	Setzen Sie den Zähler für Leseausfälle von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.

Attributname	Codieren	Beschreibung
Zurücksetzen Löschen Fehleranzahl	RSDF	Setzen Sie den Zähler für Löschfehler von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.
Beschädigte Kopien Erkannte Anzahl Zurücksetzen	RSCC	Setzen Sie den Zähler für die Anzahl beschädigter Kopien von Objektdaten, die nach dem Erasure-Coding-Verfahren codiert wurden, auf dem Storage-Node zurück.
Beschädigte Fragmente Erkannte Anzahl Zurücksetzen	RCD	Setzen Sie den Zähler auf beschädigte Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage-Node zurück.
Fehlende Fragmente Erkannt Anzahl Zurücksetzen	RSMD	Setzen Sie den Zähler auf fehlende Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage Node zurück. Nur nach Abschluss der Objektprüfung verwenden.

LDR-Replizierung

Attributname	Codieren	Beschreibung
Fehleranzahl Inbound Replication Zurücksetzen	RICR	Setzen Sie den Zähler auf Fehler bei eingehender Replikation zurück. Dies kann verwendet werden, um den RIRF-Alarm (Inbound Replication — failed) zu löschen.
Fehleranzahl Für Ausgehende Replikation Zurücksetzen	ROCR	Setzen Sie den Zähler auf Fehler bei ausgehenden Replikationen zurück. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
Deaktivieren Sie Inbound Replication	DSIR	<p>Wählen Sie diese Option aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.</p> <p>Wenn die eingehende Replikation deaktiviert ist, können Objekte vom Speicherknoten zum Kopieren an andere Speicherorte im StorageGRID-System abgerufen werden, Objekte können jedoch nicht von anderen Speicherorten aus zu diesem Speicherknoten kopiert werden: Der LDR-Dienst ist schreibgeschützt.</p>

Attributname	Codieren	Beschreibung
Deaktivieren Sie Ausgehende Replikation	DSOR	<p>Wählen Sie diese Option aus, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abrufvorgänge) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.</p> <p>Wenn die ausgehende Replikation deaktiviert ist, können Objekte auf diesen Speicherknoten kopiert werden. Objekte können jedoch nicht vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der LDR-Service ist schreibgeschützt.</p>

Verwandte Informationen

[Monitoring und Fehlerbehebung](#)

Management vollständiger Storage-Nodes

Wenn Storage-Nodes die Kapazität erreichen, müssen Sie das StorageGRID System durch Hinzufügen eines neuen Storage erweitern. Es sind drei Optionen verfügbar: Das Hinzufügen von Storage Volumes, das Hinzufügen von Shelves zur Storage-Erweiterung und das Hinzufügen von Storage-Nodes.

Hinzufügen von Storage-Volumes

Jeder Storage-Node unterstützt eine maximale Anzahl an Storage-Volumes. Der definierte Höchstwert variiert je nach Plattform. Wenn ein Storage-Node weniger als die maximale Anzahl an Storage-Volumes enthält, können Sie Volumes hinzufügen, um seine Kapazität zu erhöhen. Siehe Anweisungen für [Erweitern eines StorageGRID Systems](#).

Hinzufügen von Shelves zur Storage-Erweiterung

Einige Storage-Nodes von StorageGRID Appliances, z. B. SG6060, können zusätzliche Storage-Shelves unterstützen. Bei StorageGRID Appliances mit Erweiterungsfunktionen, die nicht bereits auf die maximale Kapazität erweitert wurden, können Sie Storage-Shelves zur Steigerung der Kapazität hinzufügen. Siehe Anweisungen für [Erweitern eines StorageGRID Systems](#).

Storage-Nodes Hinzufügen

Sie können die Storage-Kapazität durch Hinzufügen von Storage-Nodes erhöhen. Beim Hinzufügen von Storage müssen die aktuell aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig berücksichtigt werden. Siehe Anweisungen für [Erweitern eines StorageGRID Systems](#).

Copyright-Informationen

Copyright © 2025 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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER 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.