



Beheben von Objekt- und Speicherproblemen

StorageGRID software

NetApp
December 03, 2025

Inhalt

Beheben von Objekt- und Speicherproblemen	1
Bestätigen Sie die Speicherorte der Objektdaten	1
Fehler im Objektspeicher (Speichervolumen)	3
Überprüfen der Objektintegrität	5
Was ist eine Hintergrundüberprüfung?	6
Was ist eine Objektexistenzprüfung?	8
Fehlerbehebung bei der Warnung „S3 PUT-Objektgröße zu groß“	13
Fehlerbehebung bei verlorenen und fehlenden Objektdaten	15
Fehlerbehebung bei verlorenen und fehlenden Objektdaten	15
Untersuchen Sie verlorene Gegenstände	15
Suchen und Wiederherstellen potenziell verlorener Objekte	18
Zurücksetzen der Anzahl verlorener und fehlender Objekte	23
Fehlerbehebung bei der Warnung „Niedriger Objektdatenspeicher“	24
Fehlerbehebung bei Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“ ..	26
Verstehen Sie die Warnung	27
Beheben Sie die Warnung	27

Beheben von Objekt- und Speicherproblemen

Bestätigen Sie die Speicherorte der Objektdaten

Je nach Problem möchten Sie vielleicht "[Bestätigen Sie, wo die Objektdaten gespeichert werden](#)". Sie möchten beispielsweise überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und die Objektdaten am vorgesehenen Ort gespeichert werden.

Bevor Sie beginnen

- Sie müssen über eine Objektkennung verfügen. Dabei kann es sich um eine der folgenden handeln:
 - **UUID**: Die universell eindeutige Kennung des Objekts. Geben Sie die UUID in Großbuchstaben ein.
 - **CBID**: Die eindeutige Kennung des Objekts innerhalb von StorageGRID . Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in Großbuchstaben ein.
 - **S3-Bucket und Objektschlüssel**: Wenn ein Objekt über den "[S3-Schnittstelle](#)" verwendet die Clientanwendung eine Bucket- und Objektschlüsselkombination zum Speichern und Identifizieren des Objekts.

Schritte

1. Wählen Sie **ILM > Objektmetadaten**suche.
2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

Sie können eine UUID, CBID, einen S3-Bucket/Objektschlüssel oder einen Swift-Container/Objektnamen eingeben.

3. Wenn Sie eine bestimmte Version des Objekts suchen möchten, geben Sie die Versions-ID ein (optional).



4. Wählen Sie **Nachschlagen**.

Der "[Ergebnisse der Objektmetadaten](#)suche" erscheinen. Auf dieser Seite sind die folgenden Arten von Informationen aufgeführt:

- Systemmetadaten, einschließlich der Objekt-ID (UUID), der Versions-ID (optional), des Objektnamens, des Namens des Containers, des Mandantenkontonamens oder der ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Objekterstellung sowie des Datums und der Uhrzeit der letzten Objektänderung.
- Alle benutzerdefinierten Schlüssel-Wert-Paare der Benutzermetadaten, die mit dem Objekt verknüpft sind.

- Bei S3-Objekten alle mit dem Objekt verknüpften Schlüssel-Wert-Paare des Objekt-Tags.
- Bei replizierten Objektkopien der aktuelle Speicherort jeder Kopie.
- Bei Erasure-Coded-Objektkopien der aktuelle Speicherort jedes Fragments.
- Bei Objektkopien in einem Cloud Storage Pool der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte eine Liste von Objektsegmenten einschließlich Segmentkennungen und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten umfassen interne Systemmetadaten, deren Beibehaltung von Version zu Version nicht garantiert ist.

Das folgende Beispiel zeigt die Ergebnisse der Objektmetadatenuche für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

Fehler im Objektspeicher (Speichervolumen)

Der zugrunde liegende Speicher auf einem Speicherknoten ist in Objektspeicher unterteilt. Objektspeicher werden auch als Speichervolumen bezeichnet.

Sie können Objektspeicherinformationen für jeden Speicherknoten anzeigen. Objektspeicher werden unten auf der Seite **NODES** > **Storage Node** > **Storage** angezeigt.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sdC(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	1.55 MB 	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
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Mehr sehen "[Details zu jedem Speicherknoten](#)" , führen Sie die folgenden Schritte aus:

1. Wählen Sie **SUPPORT > Tools > Gittertopologie**.
2. Wählen Sie **site > Storage Node > LDR > Storage > Overview > Main**.



Overview: LDR (DC1-S1) - Storage
Updated: 2020-01-29 15:03:39 PST

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health	
0000	107 GB	96.4 GB	 994 KB	 0 B	 0.001 %	No Errors	
0001	107 GB	107 GB	 0 B	 0 B	 0 %	No Errors	
0002	107 GB	107 GB	 0 B	 0 B	 0 %	No Errors	

Abhängig von der Art des Fehlers können sich Fehler bei einem Speichervolumen in "[Speichervolumenwarnungen](#)" . Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um die volle Funktionalität des Speicherknotens so schnell wie möglich wiederherzustellen. Bei Bedarf können Sie auf die Registerkarte **Konfiguration** gehen und "[Versetzen Sie den Speicherknoten in einen schreibgeschützten Zustand](#)" damit das StorageGRID -System es zum Datenabruf verwenden kann, während Sie eine vollständige Wiederherstellung des Servers vorbereiten.

Überprüfen der Objektintegrität

Das StorageGRID -System überprüft die Integrität der Objektdaten auf Speicherknoten und sucht nach beschädigten und fehlenden Objekten.

Es gibt zwei Überprüfungsprozesse: Hintergrundüberprüfung und Objektexistenzprüfung (früher Vordergrundüberprüfung genannt). Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung läuft automatisch und prüft kontinuierlich die Richtigkeit der Objektdaten. Die Objektexistenzprüfung kann von einem Benutzer ausgelöst werden, um die Existenz (jedoch nicht die Richtigkeit) von Objekten schneller zu überprüfen.

Was ist eine Hintergrundüberprüfung?

Der Hintergrundüberprüfungsprozess prüft Speicherknoten automatisch und kontinuierlich auf beschädigte Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Bei der Hintergrundüberprüfung wird die Integrität replizierter und löschcodierter Objekte wie folgt überprüft:

- **Replizierte Objekte:** Wenn der Hintergrundüberprüfungsprozess ein beschädigtes repliziertes Objekt findet, wird die beschädigte Kopie von ihrem Speicherort entfernt und an einer anderen Stelle auf dem Speicherknoten unter Quarantäne gestellt. Anschließend wird eine neue, unbeschädigte Kopie erstellt und platziert, um die aktiven ILM-Richtlinien zu erfüllen. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die Originalkopie verwendet wurde.



Beschädigte Objektdaten werden unter Quarantäne gestellt und nicht aus dem System gelöscht, sodass weiterhin auf sie zugegriffen werden kann. Weitere Informationen zum Zugriff auf unter Quarantäne gestellte Objektdaten erhalten Sie beim technischen Support.

- **Erasure-Coded-Objekte:** Wenn der Hintergrundüberprüfungsprozess erkennt, dass ein Fragment eines Erasure-Coded-Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment an Ort und Stelle auf demselben Speicherknoten mithilfe der verbleibenden Daten- und Paritätsfragmente wiederherzustellen. Wenn das beschädigte Fragment nicht wiederhergestellt werden kann, wird versucht, eine weitere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Auswertung durchgeführt, um eine Ersatzkopie des löschcodierten Objekts zu erstellen.

Der Hintergrundüberprüfungsprozess prüft nur Objekte auf Speicherknoten. Es werden keine Objekte in einem Cloud-Speicherpool überprüft. Objekte müssen älter als vier Tage sein, um für die Hintergrundüberprüfung in Frage zu kommen.

Die Hintergrundüberprüfung läuft kontinuierlich und ist so konzipiert, dass sie die normalen Systemaktivitäten nicht beeinträchtigt. Die Hintergrundüberprüfung kann nicht gestoppt werden. Sie können jedoch die Hintergrundüberprüfungsrate erhöhen, um den Inhalt eines Speicherknotens schneller zu überprüfen, wenn Sie ein Problem vermuten.

Warnungen im Zusammenhang mit der Hintergrundüberprüfung

Wenn das System ein beschädigtes Objekt erkennt, das es nicht automatisch korrigieren kann (weil die Beschädigung die Identifizierung des Objekts verhindert), wird die Warnung **Unbekanntes beschädigtes Objekt erkannt** ausgelöst.

Wenn die Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, weil keine andere Kopie gefunden werden kann, wird die Warnung „Objekte verloren“ ausgelöst.

Ändern Sie die Hintergrundüberprüfungsrate

Sie können die Rate ändern, mit der die Hintergrundüberprüfung replizierte Objektdaten auf einem Speicherknoten prüft, wenn Sie Bedenken hinsichtlich der Datenintegrität haben.

Bevor Sie beginnen

- Sie müssen beim Grid Manager mit einem [unterstützter Webbrowser](#) .
- Du hast [spezifische Zugriffsberechtigungen](#) .

Informationen zu diesem Vorgang

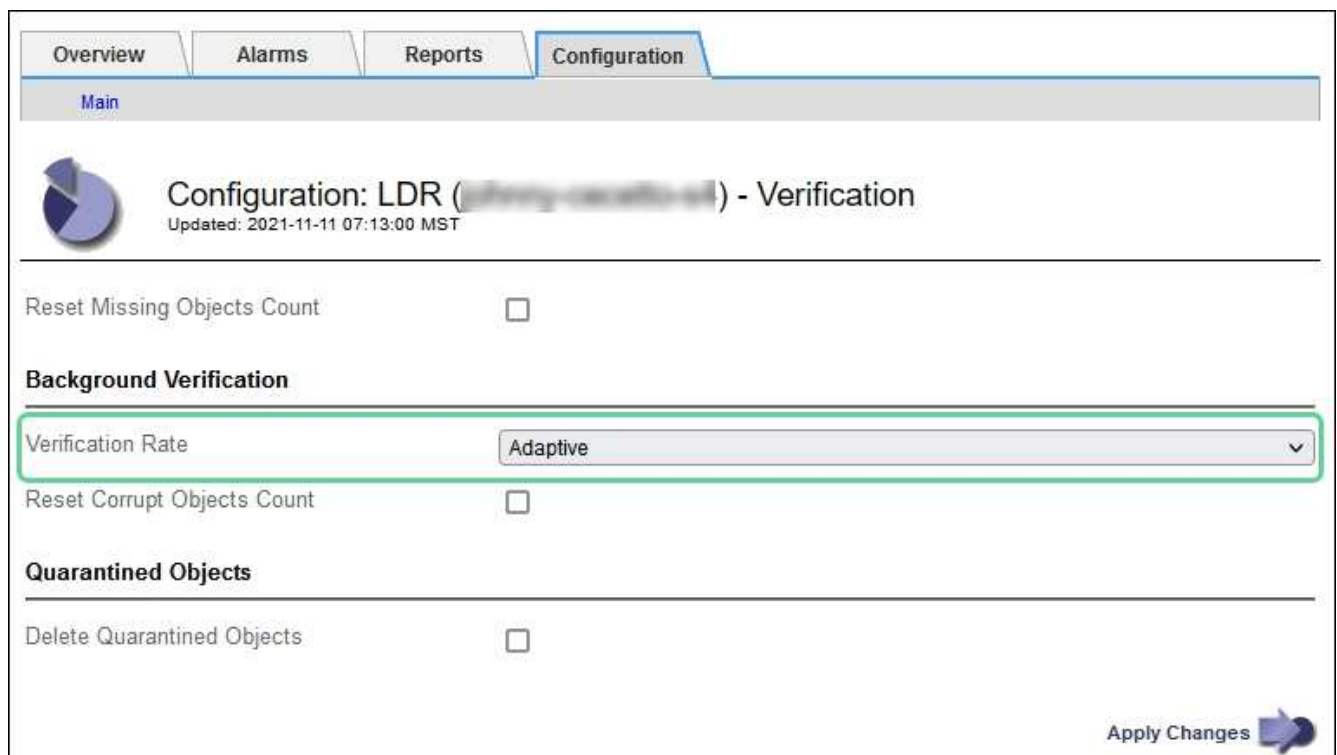
Sie können die Überprüfungsrate für die Hintergrundüberprüfung auf einem Speicherknoten ändern:

- **Adaptiv:** Standardeinstellung. Die Aufgabe ist für eine Überprüfung mit maximal 4 MB/s oder 10 Objekten/s ausgelegt (je nachdem, was zuerst überschritten wird).
- **Hoch:** Die Speicherüberprüfung erfolgt schnell, mit einer Geschwindigkeit, die normale Systemaktivitäten verlangsamen kann.

Verwenden Sie die hohe Überprüfungsrate nur, wenn Sie vermuten, dass ein Hardware- oder Softwarefehler die Objektdaten beschädigt haben könnte. Nachdem die Hintergrundüberprüfung mit hoher Priorität abgeschlossen ist, wird die Überprüfungsrate automatisch auf „Adaptiv“ zurückgesetzt.

Schritte

1. Wählen Sie **SUPPORT > Tools > Gittertopologie**.
2. Wählen Sie **Speicherknoten > LDR > Verifizierung**.
3. Wählen Sie **Konfiguration > Haupt**.
4. Gehen Sie zu **LDR > Verifizierung > Konfiguration > Haupt**.
5. Wählen Sie unter „Hintergrundüberprüfung“ **Überprüfungsrate > Hoch** oder **Überprüfungsrate > Adaptiv**.



The screenshot shows the 'Configuration' tab for 'LDR (Storage Controller) - Verification'. The 'Verification Rate' is set to 'Adaptive'. Below this, there are checkboxes for 'Reset Missing Objects Count', 'Reset Corrupt Objects Count', and 'Delete Quarantined Objects'. An 'Apply Changes' button is at the bottom right.

6. Klicken Sie auf **Änderungen übernehmen**.
7. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung für replizierte Objekte.
 - a. Gehen Sie zu **NODES > Storage Node > Objects**.
 - b. Überwachen Sie im Abschnitt „Überprüfung“ die Werte für **Beschädigte Objekte** und **Unidentifizierte beschädigte Objekte**.

Wenn bei der Hintergrundüberprüfung beschädigte replizierte Objektdaten gefunden werden, wird die Metrik **Beschädigte Objekte** erhöht und StorageGRID versucht, die Objektkennung wie folgt aus den Daten zu extrahieren:

- Wenn die Objektkennung extrahiert werden kann, erstellt StorageGRID automatisch eine neue

Kopie der Objektdaten. Die neue Kopie kann überall im StorageGRID -System erstellt werden, wo die aktiven ILM-Richtlinien erfüllt werden.

- Wenn die Objektkennung nicht extrahiert werden kann (weil sie beschädigt wurde), wird die Metrik **Beschädigte Objekte nicht identifiziert** erhöht und die Warnung **Unidentifiziertes beschädigtes Objekt erkannt** ausgelöst.

c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Grundursache der Beschädigung zu ermitteln.

8. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung für Erasure-Codierte Objekte.

Wenn bei der Hintergrundüberprüfung beschädigte Fragmente von Erasure-Coded-Objektdaten gefunden werden, wird das Attribut „Beschädigte Fragmente erkannt“ erhöht. StorageGRID stellt das Problem wieder her, indem das beschädigte Fragment an Ort und Stelle auf demselben Speicherknoten neu erstellt wird.

a. Wählen Sie **SUPPORT > Tools > Gittertopologie**.

b. Wählen Sie **Speicherknoten > LDR > Erasure Coding**.

c. Überwachen Sie in der Tabelle „Verifizierungsergebnisse“ das Attribut „Beschädigte Fragmente erkannt“ (ECCD).

9. Nachdem beschädigte Objekte automatisch vom StorageGRID System wiederhergestellt wurden, setzen Sie die Anzahl der beschädigten Objekte zurück.

a. Wählen Sie **SUPPORT > Tools > Gittertopologie**.

b. Wählen Sie **Speicherknoten > LDR > Verifizierung > Konfiguration**.

c. Wählen Sie **Anzahl beschädigter Objekte zurücksetzen**.

d. Klicken Sie auf **Änderungen übernehmen**.

10. Wenn Sie sicher sind, dass die unter Quarantäne gestellten Objekte nicht benötigt werden, können Sie sie löschen.



Wenn die Warnung „Objekte verloren“ ausgelöst wurde, möchte der technische Support möglicherweise auf unter Quarantäne gestellte Objekte zugreifen, um das zugrunde liegende Problem zu beheben oder eine Datenwiederherstellung zu versuchen.

a. Wählen Sie **SUPPORT > Tools > Gittertopologie**.

b. Wählen Sie **Speicherknoten > LDR > Verifizierung > Konfiguration**.

c. Wählen Sie **Unter Quarantäne gestellte Objekte löschen**.

d. Wählen Sie **Änderungen übernehmen**.

Was ist eine Objektexistenzprüfung?

Die Objektexistenzprüfung überprüft, ob alle erwarteten replizierten Kopien von Objekten und Erasure-Coded-Fragmenten auf einem Speicherknoten vorhanden sind. Bei der Objekt-Existenzprüfung werden nicht die Objektdaten selbst überprüft (dies geschieht durch die Hintergrundüberprüfung). Stattdessen bietet sie eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich aufgetretenes Hardwareproblem die Datenintegrität beeinträchtigt haben könnte.

Im Gegensatz zur Hintergrundüberprüfung, die automatisch erfolgt, müssen Sie einen Job zur Überprüfung der Objektexistenz manuell starten.

Die Objektexistenzprüfung liest die Metadaten für jedes in StorageGRID gespeicherte Objekt und überprüft die Existenz sowohl replizierter Objektkopien als auch löschcodierter Objektfragmente. Mit fehlenden Daten wird

wie folgt verfahren:

- **Replizierte Kopien:** Wenn eine Kopie der replizierten Objektdaten fehlt, versucht StorageGRID automatisch, die Kopie durch eine an anderer Stelle im System gespeicherte Kopie zu ersetzen. Der Speicherknoten führt eine vorhandene Kopie durch eine ILM-Auswertung aus, die ergibt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da eine andere Kopie fehlt. Eine neue Kopie wird erstellt und platziert, um die aktiven ILM-Richtlinien des Systems zu erfüllen. Diese neue Kopie wird möglicherweise nicht am selben Ort abgelegt, an dem die fehlende Kopie gespeichert war.
- **Erase-Coded-Fragmente:** Wenn ein Fragment eines Erasure-Coded-Objekts fehlt, versucht StorageGRID automatisch, das fehlende Fragment an Ort und Stelle auf demselben Speicherknoten mithilfe der verbleibenden Fragmente wiederherzustellen. Wenn das fehlende Fragment nicht wiederhergestellt werden kann (weil zu viele Fragmente verloren gegangen sind), versucht ILM, eine weitere Kopie des Objekts zu finden, mit der es ein neues Erasure-Coded-Fragment generieren kann.

Führen Sie eine Objekt-Existenzprüfung durch

Sie erstellen und führen jeweils einen Job zur Objektexistenzprüfung aus. Wenn Sie einen Job erstellen, wählen Sie die Speicherknoten und Volumes aus, die Sie überprüfen möchten. Sie wählen auch die Konsistenz für den Auftrag aus.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Sie haben die ["Wartungs- oder Root-Zugriffsberechtigung"](#) .
- Sie haben sichergestellt, dass die Speicherknoten, die Sie überprüfen möchten, online sind. Wählen Sie **NODES** aus, um die Knotentabelle anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen der Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden Prozeduren auf den Knoten, die Sie überprüfen möchten, **nicht** ausgeführt werden:
 - Netzerweiterung zum Hinzufügen eines Speicherknotens
 - Außerbetriebnahme von Speicherknoten
 - Wiederherstellung eines ausgefallenen Speichervolumes
 - Wiederherstellung eines Speicherknotens mit einem ausgefallenen Systemlaufwerk
 - EC-Neugewichtung
 - Appliance-Knotenklon

Die Objektexistenzprüfung liefert keine nützlichen Informationen, während diese Verfahren ausgeführt werden.

Informationen zu diesem Vorgang

Die Ausführung eines Objektexistenzprüfungsauftrags kann Tage oder Wochen dauern, abhängig von der Anzahl der Objekte im Raster, den ausgewählten Speicherknoten und Datenträgern und der ausgewählten Konsistenz. Sie können jeweils nur einen Job ausführen, aber Sie können mehrere Speicherknoten und Volumes gleichzeitig auswählen.

Schritte

1. Wählen Sie **WARTUNG > Aufgaben > Objektexistenzprüfung**.
2. Wählen Sie **Job erstellen**. Der Assistent „Job zur Objektexistenzprüfung erstellen“ wird angezeigt.
3. Wählen Sie die Knoten aus, die die Volumes enthalten, die Sie überprüfen möchten. Um alle Online-Knoten auszuwählen, aktivieren Sie das Kontrollkästchen **Knotenname** in der Spaltenüberschrift.

Sie können nach Knotennamen oder Site suchen.

Sie können keine Knoten auswählen, die nicht mit dem Raster verbunden sind.

4. Wählen Sie **Weiter**.

5. Wählen Sie für jeden Knoten in der Liste ein oder mehrere Volumes aus. Sie können anhand der Speichervolumennummer oder des Knotennamens nach Volumes suchen.

Um alle Volumes für jeden ausgewählten Knoten auszuwählen, aktivieren Sie das Kontrollkästchen **Speichervolume** in der Spaltenüberschrift.

6. Wählen Sie **Weiter**.

7. Wählen Sie die Konsistenz für den Auftrag aus.

Die Konsistenz bestimmt, wie viele Kopien der Objektmetadaten für die Objektexistenzprüfung verwendet werden.

- **Strong-Site**: Zwei Kopien der Metadaten an einer einzigen Site.
- **Stark-global**: Zwei Kopien der Metadaten an jedem Standort.
- **Alle** (Standard): Alle drei Kopien der Metadaten an jedem Standort.

Weitere Informationen zur Konsistenz finden Sie in den Beschreibungen im Assistenten.

8. Wählen Sie **Weiter**.

9. Überprüfen und bestätigen Sie Ihre Auswahl. Sie können **Zurück** auswählen, um zu einem vorherigen Schritt im Assistenten zu gelangen und Ihre Auswahl zu aktualisieren.

Ein Job zur Objektexistenzprüfung wird generiert und ausgeführt, bis eines der folgenden Ereignisse eintritt:

- Der Auftrag ist abgeschlossen.
- Sie pausieren oder brechen den Auftrag ab. Sie können einen Job fortsetzen, den Sie angehalten haben, aber Sie können einen Job nicht fortsetzen, den Sie abgebrochen haben.
- Der Job stockt. Die Warnung „Prüfung der Objektexistenz ist ins Stocken geraten“ wird ausgelöst. Befolgen Sie die für die Warnung angegebenen Korrekturmaßnahmen.
- Der Auftrag schlägt fehl. Die Warnung **Prüfung der Objektexistenz fehlgeschlagen** wird ausgelöst. Befolgen Sie die für die Warnung angegebenen Korrekturmaßnahmen.
- Es wird die Meldung „Dienst nicht verfügbar“ oder „Interner Serverfehler“ angezeigt. Aktualisieren Sie die Seite nach einer Minute, um den Auftrag weiter zu überwachen.



Bei Bedarf können Sie von der Seite zur Objektexistenzprüfung weg navigieren und zurückkehren, um die Überwachung des Auftrags fortzusetzen.

10. Zeigen Sie während der Ausführung des Auftrags die Registerkarte **Aktiver Auftrag** an und notieren Sie sich den Wert „Fehlende Objektkopien erkannt“.

Dieser Wert stellt die Gesamtzahl der fehlenden Kopien replizierter Objekte und löschcodierter Objekte mit einem oder mehreren fehlenden Fragmenten dar.

Wenn die Anzahl der erkannten fehlenden Objektkopien größer als 100 ist, liegt möglicherweise ein Problem mit dem Speicher des Speicherknotens vor.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

Start time: 2021-11-10 14:43:02 MST

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Führen Sie nach Abschluss des Auftrags alle weiteren erforderlichen Aktionen aus:

- Wenn „Fehlende Objektkopien erkannt“ null ist, wurden keine Probleme gefunden. Es ist keine Aktion erforderlich.
- Wenn die Anzahl der erkannten fehlenden Objektkopien größer als Null ist und die Warnung **Objekte verloren** nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Stellen Sie sicher, dass alle Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu verhindern.
- Wenn die Anzahl der erkannten fehlenden Objektkopien größer als Null ist und die Warnung „Objekte verloren“ ausgelöst wurde, kann die Datenintegrität beeinträchtigt sein. Wenden Sie sich an den technischen Support.
- Sie können verlorene Objektkopien untersuchen, indem Sie mit grep die LLST-Auditmeldungen extrahieren: `grep LLST audit_file_name`.

Dieses Verfahren ist ähnlich wie bei ["Untersuchung verlorener Gegenstände"](#), obwohl Sie für Objektkopien nach LLST anstatt OLST.

12. Wenn Sie für den Job die starke Site- oder starke globale Konsistenz ausgewählt haben, warten Sie ungefähr drei Wochen, bis die Metadatenkonsistenz erreicht ist, und führen Sie den Job dann erneut auf denselben Volumes aus.

Wenn StorageGRID Zeit hatte, die Metadatenkonsistenz für die im Job enthaltenen Knoten und Volumes zu erreichen, kann eine erneute Ausführung des Jobs fälschlicherweise als fehlend gemeldete Objektkopien löschen oder dazu führen, dass zusätzliche Objektkopien überprüft werden, wenn diese fehlten.

- a. Wählen Sie **WARTUNG > Objektexistenzprüfung > Auftragsverlauf**.
- b. Bestimmen Sie, welche Jobs zur erneuten Ausführung bereit sind:
 - i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.
 - ii. Durchsuchen Sie für diese Jobs die Spalte „Konsistenzkontrolle“ nach „Strong-Site“ oder „Strong-Global“.
- c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **Erneut ausführen**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Delete | **Rerun** | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

☐	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
☒	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
☐	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Überprüfen Sie im Assistenten „Jobs erneut ausführen“ die ausgewählten Knoten und Volumes sowie die Konsistenz.
- e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Erneut ausführen**.

Die Registerkarte „Aktiver Job“ wird angezeigt. Alle von Ihnen ausgewählten Jobs werden als ein Job mit einer starken Site-Konsistenz erneut ausgeführt. Im Feld **Verwandte Jobs** im Abschnitt „Details“ werden die Job-IDs für die ursprünglichen Jobs aufgelistet.

Nach Abschluss

Wenn Sie weiterhin Bedenken hinsichtlich der Datenintegrität haben, gehen Sie zu **SUPPORT > Tools > Grid-Topologie > Site > Storage Node > LDR > Verifizierung > Konfiguration > Main** und erhöhen Sie die Hintergrundüberprüfungsrate. Die Hintergrundüberprüfung prüft die Richtigkeit aller gespeicherten Objektdaten und behebt alle gefundenen Probleme. Durch das möglichst schnelle Auffinden und Beheben potenzieller Probleme wird das Risiko eines Datenverlusts verringert.

Fehlerbehebung bei der Warnung „S3 PUT-Objektgröße zu groß“

Die Warnung „S3 PUT-Objektgröße zu groß“ wird ausgelöst, wenn ein Mandant einen nicht mehrteiligen PutObject-Vorgang versucht, der die S3-Größenbeschränkung von 5 GiB überschreitet.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .

Ermitteln Sie, welche Mandanten Objekte verwenden, die größer als 5 GiB sind, damit Sie sie benachrichtigen können.

Schritte

1. Gehen Sie zu **KONFIGURATION > Überwachung > Audit- und Syslog-Server**.
2. Wenn die Client-Schreibvorgänge normal sind, greifen Sie auf das Prüfprotokoll zu:

- a. Eingeben `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#` .

- e. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

Das Prüfprotokollverzeichnis und die entsprechenden Knoten hängen von Ihren Prüfzeleinstellungen ab.

Option	Ziel
Lokale Knoten (Standard)	<code>/var/local/log/localaudit.log</code>
Admin-Knoten/lokale Knoten	• Admin-Knoten (primär und nicht primär): <code>/var/local/audit/export/audit.log</code> • Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Die Datei ist in diesem Modus normalerweise leer oder fehlt.
Externer Syslog-Server	<code>/var/local/log/localaudit.log</code>

Geben Sie je nach Ihren Audit-Zieleinstellungen Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

Weitere Informationen finden Sie unter ["Auswählen von Zielen für Auditinformationen"](#) .

- f. Ermitteln Sie, welche Mandanten Objekte verwenden, die größer als 5 GiB sind.

- i. Eingeben `zgrep SPUT * | egrep "CSIZ(UI64\):( [5-9] | [1-9] [0-9]+) [0-9]{9}"`
- ii. Sehen Sie sich für jede Prüfnachricht in den Ergebnissen Folgendes an: `S3AI` Feld, um die Mandantenkonto-ID zu bestimmen. Verwenden Sie die anderen Felder in der Nachricht, um zu bestimmen, welche IP-Adresse vom Client, dem Bucket und dem Objekt verwendet wurde:

Code	Beschreibung
SAIP	Quell-IP
S3AI	Mandanten-ID
S3BK	Eimer
S3KY	Objekt
CSIZ	Größe (Bytes)

Beispiel für Audit-Protokollergebnisse

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Wenn Client-Schreibvorgänge nicht normal sind, verwenden Sie die Mandanten-ID aus der Warnung, um den Mandanten zu identifizieren:
 - a. Gehen Sie zu **SUPPORT > Tools > Protokolle**. Sammeln Sie Anwendungsprotokolle für den Speicherknoten in der Warnung. Geben Sie 15 Minuten vor und nach der Warnung an.
 - b. Extrahieren Sie die Datei und gehen Sie zu `bycast.log`:

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

- c. Suchen Sie im Protokoll nach `method=PUT` und identifizieren Sie den Client in der `clientIP` Feld.

Beispiel bycast.log


```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE  1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informieren Sie die Mieter, dass die maximale PutObject-Größe 5 GiB beträgt und dass für Objekte, die größer als 5 GiB sind, mehrteilige Uploads verwendet werden sollen.
5. Ignorieren Sie die Warnung eine Woche lang, wenn die Anwendung geändert wurde.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Objekte können aus verschiedenen Gründen abgerufen werden, darunter Leseanforderungen einer Clientanwendung, Hintergrundüberprüfungen replizierter Objektdaten, ILM-Neubewertungen und die Wiederherstellung von Objektdaten während der Wiederherstellung eines Speicherknotens.

Das StorageGRID -System verwendet Standortinformationen in den Metadaten eines Objekts, um zu bestimmen, von welchem Standort das Objekt abgerufen werden soll. Wenn am erwarteten Speicherort keine Kopie des Objekts gefunden wird, versucht das System, eine weitere Kopie des Objekts von einer anderen Stelle im System abzurufen, wobei davon ausgegangen wird, dass die ILM-Richtlinie eine Regel zum Erstellen von zwei oder mehr Kopien des Objekts enthält.

Wenn dieser Abruf erfolgreich ist, ersetzt das StorageGRID -System die fehlende Kopie des Objekts. Andernfalls wird die Warnung „Objekte verloren“ wie folgt ausgelöst:

- Wenn bei replizierten Kopien keine weitere Kopie abgerufen werden kann, gilt das Objekt als verloren und die Warnung wird ausgelöst.
- Wenn bei Erasure-Coded-Kopien eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, wird das Attribut „Corrupt Copies Detected“ (ECOR) um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Wenn keine andere Kopie gefunden wird, wird der Alarm ausgelöst.

Sie sollten alle Warnmeldungen zum Thema „Objektverlust“ sofort untersuchen, um die Grundursache des Verlusts zu ermitteln und festzustellen, ob das Objekt möglicherweise noch in einem Offline- oder anderweitig derzeit nicht verfügbaren Speicherknoten vorhanden ist. Sehen ["Untersuchen Sie verlorene Gegenstände"](#) .

Für den Fall, dass Objektdaten ohne Kopien verloren gehen, gibt es keine Wiederherstellungslösung. Sie müssen jedoch den Zähler für verlorene Objekte zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren. Sehen ["Zurücksetzen der Anzahl verlorener und fehlender Objekte"](#) .

Untersuchen Sie verlorene Gegenstände

Wenn die Warnung „Objekte verloren“ ausgelöst wird, müssen Sie dies sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Bevor Sie beginnen

- Sie müssen beim Grid Manager mit einem ["unterstützter Webbrowser"](#) .
- Du hast ["spezifische Zugriffsberechtigungen"](#) .
- Sie müssen über die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

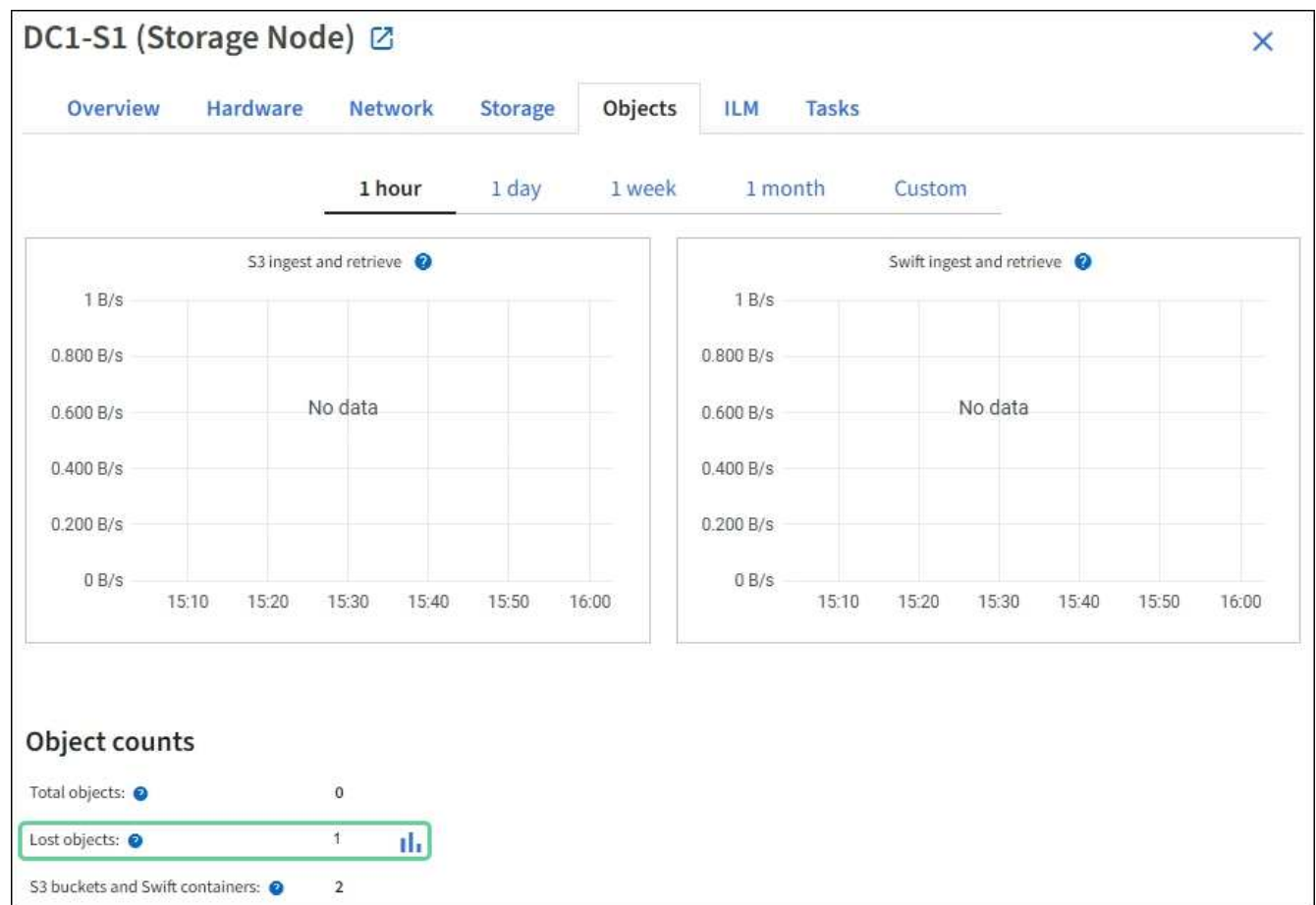
Die Warnung „Objekte verloren“ zeigt an, dass StorageGRID davon ausgeht, dass im Grid keine Kopien eines Objekts vorhanden sind. Möglicherweise sind die Daten dauerhaft verloren gegangen.

Gehen Sie Warnmeldungen zu verlorenen Gegenständen sofort nach. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu verhindern. In einigen Fällen können Sie einen verlorenen Gegenstand möglicherweise wiederherstellen, wenn Sie umgehend handeln.

Schritte

1. Wählen Sie **NODES**.
2. Wählen Sie **Speicherknoten > Objekte**.
3. Überprüfen Sie die Anzahl der verlorenen Objekte, die in der Objektanzahltafel angezeigt wird.

Diese Zahl gibt die Gesamtzahl der Objekte an, die dieser Grid-Knoten im gesamten StorageGRID System als fehlend erkennt. Der Wert ist die Summe der Zähler für verlorene Objekte der Datenspeicherkomponente innerhalb der LDR- und DDS-Dienste.



4. Von einem Admin-Knoten aus, ["Zugriff auf das Überwachungsprotokoll"](#) So ermitteln Sie die eindeutige Kennung (UUID) des Objekts, das die Warnung „Objekte verloren“ ausgelöst hat:
 - a. Melden Sie sich beim Grid-Knoten an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#`.
- b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

Das Prüfprotokollverzeichnis und die entsprechenden Knoten hängen von Ihren Prüfzeileinstellungen ab.

Option	Ziel
Lokale Knoten (Standard)	<code>/var/local/log/localaudit.log</code>
Admin-Knoten/lokale Knoten	• Admin-Knoten (primär und nicht primär): <code>/var/local/audit/export/audit.log</code> • Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Die Datei ist in diesem Modus normalerweise leer oder fehlt.
Externer Syslog-Server	<code>/var/local/log/localaudit.log</code>

Geben Sie je nach Ihren Audit-Zieleinstellungen Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

Weitere Informationen finden Sie unter "[Auswählen von Zielen für Auditinformationen](#)".

- c. Verwenden Sie `grep`, um die OLST-Auditmeldungen (Object Lost) zu extrahieren. Eingeben: `grep OLST audit_file_name`
- d. Beachten Sie den in der Nachricht enthaltenen UUID-Wert.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986]
[RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][AMID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Suchen Sie mithilfe der UUID nach den Metadaten für das verlorene Objekt:

- a. Wählen Sie **ILM > Objektmmdatensuche**.
- b. Geben Sie die UUID ein und wählen Sie **Nachschlagen**.
- c. Überprüfen Sie die Standorte in den Metadaten und ergreifen Sie die entsprechenden Maßnahmen:

Metadaten	Abschluss
Objekt <Objektkennung> nicht gefunden	Wenn das Objekt nicht gefunden wird, wird die Meldung „ERROR“ zurückgegeben. Wenn das Objekt nicht gefunden wird, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen. Das Fehlen eines Objekts weist darauf hin, dass das Objekt absichtlich gelöscht wurde.
Standorte > 0	Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung „Objekte verloren“ ein Fehlalarm sein. Bestätigen Sie, dass die Objekte vorhanden sind. Verwenden Sie die in der Ausgabe aufgeführte Knoten-ID und den Dateipfad, um zu bestätigen, dass sich die Objektdatei am aufgeführten Speicherort befindet. (Das Verfahren für "Suche nach möglicherweise verlorenen Gegenständen" erklärt, wie Sie die Knoten-ID verwenden, um den richtigen Speicherknoten zu finden.) Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen.
Standorte = 0	Wenn in der Ausgabe keine Standorte aufgeführt sind, fehlt das Objekt möglicherweise. Sie können versuchen, "Suchen und Wiederherstellen des Objekts" selbst oder Sie können sich an den technischen Support wenden. Der technische Support wird Sie möglicherweise bitten, festzustellen, ob gerade ein Speicherwiederherstellungsverfahren läuft. Informationen zu "Wiederherstellen von Objektdaten mit Grid Manager" Und "Wiederherstellen von Objektdaten auf einem Speichervolume".

Suchen und Wiederherstellen potenziell verlorener Objekte

Möglicherweise ist es möglich, Objekte zu finden und wiederherzustellen, die eine **Objekt verloren**-Warnung und einen älteren „Lost Objects“-Alarm (LOST) ausgelöst haben und die Sie als potenziell verloren identifiziert haben.

Bevor Sie beginnen

- Sie haben die UUID eines verlorenen Objekts, wie in "[Untersuchen Sie verlorene Gegenstände](#)".
- Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Sie können dieses Verfahren befolgen, um an anderer Stelle im Raster nach replizierten Kopien des verlorenen Objekts zu suchen. In den meisten Fällen wird der verlorene Gegenstand nicht gefunden. In einigen Fällen können Sie jedoch möglicherweise ein verlorenes repliziertes Objekt finden und wiederherstellen, wenn Sie umgehend Maßnahmen ergreifen.



Wenden Sie sich an den technischen Support, um Hilfe bei diesem Verfahren zu erhalten.

Schritte

1. Durchsuchen Sie von einem Admin-Knoten aus die Prüfprotokolle nach möglichen Objektstandorten:

a. Melden Sie sich beim Grid-Knoten an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

Das Prüfprotokollverzeichnis und die entsprechenden Knoten hängen von Ihren Prüfzeleinstellungen ab.

Option	Ziel
Lokale Knoten (Standard)	<code>/var/local/log/localaudit.log</code>
Admin-Knoten/lokale Knoten	• Admin-Knoten (primär und nicht primär): <code>/var/local/audit/export/audit.log</code> • Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Die Datei ist in diesem Modus normalerweise leer oder fehlt.
Externer Syslog-Server	<code>/var/local/log/localaudit.log</code>

Geben Sie je nach Ihren Audit-Zieleinstellungen Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

Weitere Informationen finden Sie unter "[Auswählen von Zielen für Auditinformationen](#)".

c. Verwenden Sie `grep`, um die "[Prüfmeldungen im Zusammenhang mit dem möglicherweise verlorenen Objekt](#)" und senden Sie sie an eine Ausgabedatei. Eingeben: `grep uuid-value audit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

d. Verwenden Sie `grep`, um die LLST-Auditmeldungen (Location Lost) aus dieser Ausgabedatei zu extrahieren. Eingeben: `grep LLST output_file_name`

Beispiel:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

Eine LLST-Auditnachricht sieht wie diese Beispielnachricht aus.

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
86871083190743409]]
```

e. Suchen Sie das PCLD-Feld und das NOID-Feld in der LLST-Nachricht.

Falls vorhanden, ist der Wert von PCLD der vollständige Pfad auf der Festplatte zur fehlenden replizierten Objektkopie. Der Wert von NOID ist die Knoten-ID des LDR, in dem eine Kopie des Objekts gefunden werden kann.

Wenn Sie einen Objektspeicherort finden, können Sie das Objekt möglicherweise wiederherstellen.

a. Suchen Sie den Speicherknoten, der dieser LDR-Knoten-ID zugeordnet ist. Wählen Sie im Grid Manager **SUPPORT > Tools > Grid-Topologie**. Wählen Sie dann **Data Center > Storage Node > LDR**.

Die Knoten-ID für den LDR-Dienst befindet sich in der Knoteninformationstabelle. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie denjenigen finden, der diesen LDR hostet.

2. Stellen Sie fest, ob das Objekt auf dem in der Prüfnachricht angegebenen Speicherknoten vorhanden ist:

a. Melden Sie sich beim Grid-Knoten an:

- i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
- iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

b. Stellen Sie fest, ob der Dateipfad für das Objekt vorhanden ist.

Verwenden Sie für den Dateipfad des Objekts den PCLD-Wert aus der LLST-Auditnachricht.

Geben Sie beispielsweise Folgendes ein:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6'
```



Setzen Sie den Objektpfad in Befehlen immer in einfache Anführungszeichen, um Sonderzeichen zu maskieren.

- Wenn der Objektpfad nicht gefunden wird, ist das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wurde, fahren Sie mit dem nächsten Schritt fort. Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.

3. Wenn der Objektpfad gefunden wurde, versuchen Sie, das Objekt in StorageGRID wiederherzustellen:

- Ändern Sie vom selben Speicherknoten aus den Besitz der Objektdatei, sodass sie von StorageGRID verwaltet werden kann. Eingeben: `chown ldr-user:bycast 'file_path_of_object'`
- Um auf die LDR-Konsole zuzugreifen, greifen Sie per Telnet auf den Localhost 1402 zu. Eingeben: `telnet 0 1402`
- Eingeben: `cd /proc/STOR`
- Eingeben: `Object_Found 'file_path_of_object'`

Geben Sie beispielsweise Folgendes ein:

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Ausgabe der `Object_Found` Der Befehl benachrichtigt das Raster über den Standort des Objekts. Außerdem werden dadurch die aktiven ILM-Richtlinien ausgelöst, die zusätzliche Kopien gemäß den Angaben in den einzelnen Richtlinien erstellen.



Wenn der Speicherknoten, auf dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf jeden Speicherknoten kopieren, der online ist. Platzieren Sie das Objekt in einem beliebigen /var/local/rangedb-Verzeichnis des Online-Speicherknotens. Geben Sie dann die `Object_Found` Befehl unter Verwendung dieses Dateipfads zum Objekt.

- Wenn das Objekt nicht wiederhergestellt werden kann, `Object_Found` Befehl schlägt fehl. Wenden Sie sich an den technischen Support.
- Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, wird eine Erfolgsmeldung angezeigt. Beispiel:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Fahren Sie mit dem nächsten Schritt fort.

4. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, überprüfen Sie, ob die neuen

Speicherorte erstellt wurden:

- a. Sign in beim Grid Manager an mit einem ["unterstützter Webbrowser"](#) .
 - b. Wählen Sie **ILM > Objektmetadatenuche**.
 - c. Geben Sie die UUID ein und wählen Sie **Nachschlagen**.
 - d. Überprüfen Sie die Metadaten und bestätigen Sie die neuen Standorte.
5. Suchen Sie von einem Admin-Knoten aus in den Prüfprotokollen nach der ORLM-Prüfnachricht für dieses Objekt, um zu bestätigen, dass das Information Lifecycle Management (ILM) die erforderlichen Kopien platziert hat.
- a. Melden Sie sich beim Grid-Knoten an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#` .
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden. Siehe [Unterschnitt 1. b](#) .
 - c. Verwenden Sie `grep`, um die mit dem Objekt verknüpften Prüfmeldungen in eine Ausgabedatei zu extrahieren. Eingeben: `grep uuid-value audit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt
```

- d. Verwenden Sie `grep`, um die ORLM-Auditmeldungen (Object Rules Met) aus dieser Ausgabedatei zu extrahieren. Eingeben: `grep ORLM output_file_name`

Beispiel:

```
Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
```

Eine ORLM-Auditnachricht sieht wie diese Beispielnachricht aus.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"***CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```


- a. Suchen Sie das LOCS-Feld in der Prüfnachricht.

Falls vorhanden, ist der Wert von CLDI in LOCS die Knoten-ID und die Volume-ID, auf der eine Objektkopie erstellt wurde. Diese Meldung zeigt an, dass das ILM angewendet wurde und dass zwei Objektkopien an zwei Stellen im Grid erstellt wurden.

6. "Setzen Sie die Anzahl verlorener und fehlender Objekte zurück"im Grid Manager.

Zurücksetzen der Anzahl verlorener und fehlender Objekte

Nachdem Sie das StorageGRID -System untersucht und überprüft haben, dass alle aufgezeichneten verlorenen Objekte dauerhaft verloren sind oder es sich um einen Fehlalarm handelt, können Sie den Wert des Attributs „Lost Objects“ auf Null zurücksetzen.

Bevor Sie beginnen

- Sie müssen beim Grid Manager mit einem "unterstützter Webbrowser" .
- Du hast "spezifische Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

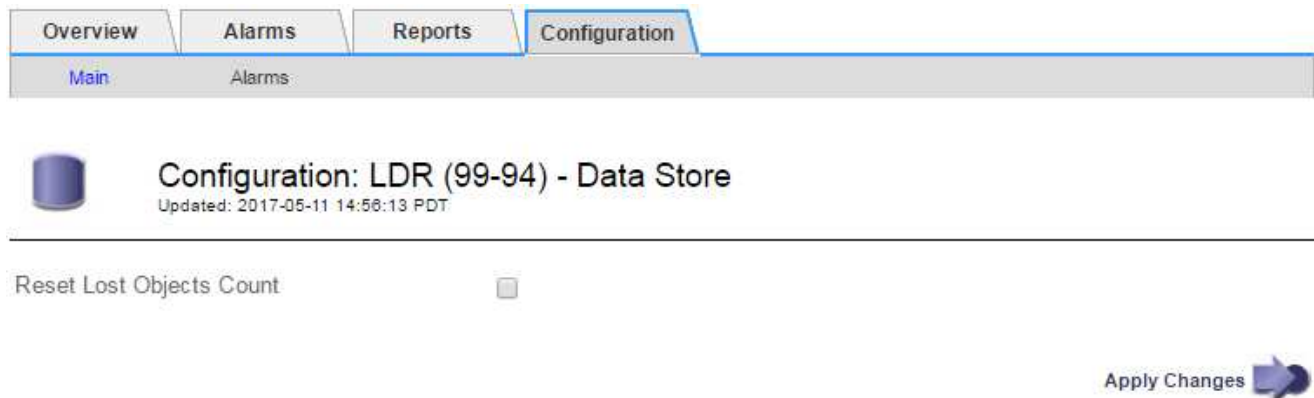
Sie können den Zähler für verlorene Objekte auf einer der folgenden Seiten zurücksetzen:

- **SUPPORT > Tools > Grid-Topologie > Site > Storage Node > LDR > Data Store > Übersicht > Main**
- **SUPPORT > Tools > Grid-Topologie > Site > Storage Node > DDS > Data Store > Übersicht > Main**

Diese Anweisungen zeigen das Zurücksetzen des Zählers von der Seite **LDR > Datenspeicher**.

Schritte

1. Wählen Sie **SUPPORT > Tools > Gittertopologie**.
2. Wählen Sie **Site > Storage Node > LDR > Data Store > Configuration** für den Storage Node, der die Warnung **Objects lost** oder den LOST-Alarm aufweist.
3. Wählen Sie **Anzahl verlorener Objekte zurücksetzen**.



4. Klicken Sie auf **Änderungen übernehmen**.

Das Attribut „Verlorene Objekte“ wird auf 0 zurückgesetzt und die Warnung „Objekte verloren“ sowie der Alarm „VERLOREN“ werden gelöscht. Dies kann einige Minuten dauern.

5. Optional können Sie andere zugehörige Attributwerte zurücksetzen, die beim Identifizieren des verlorenen Objekts möglicherweise erhöht wurden.
 - a. Wählen Sie **Site > Storage Node > LDR > Erasure Coding > Konfiguration**.
 - b. Wählen Sie **Anzahl Lesefehler zurücksetzen** und **Anzahl erkannter beschädigter Kopien zurücksetzen**.
 - c. Klicken Sie auf **Änderungen übernehmen**.
 - d. Wählen Sie **Site > Storage Node > LDR > Verifizierung > Konfiguration**.
 - e. Wählen Sie **Anzahl fehlender Objekte zurücksetzen** und **Anzahl beschädigter Objekte zurücksetzen**.
 - f. Wenn Sie sicher sind, dass die unter Quarantäne gestellten Objekte nicht benötigt werden, können Sie „Unter Quarantäne gestellte Objekte löschen“ auswählen.

Quarantäneobjekte werden erstellt, wenn bei der Hintergrundüberprüfung eine beschädigte replizierte Objektkopie identifiziert wird. In den meisten Fällen ersetzt StorageGRID das beschädigte Objekt automatisch und die unter Quarantäne gestellten Objekte können sicher gelöscht werden. Wenn jedoch die Warnung „Objekte verloren“ oder der Alarm „VERLOREN“ ausgelöst wird, möchte der technische Support möglicherweise auf die unter Quarantäne gestellten Objekte zugreifen.

- g. Klicken Sie auf **Änderungen übernehmen**.

Es kann einige Augenblicke dauern, bis die Attribute zurückgesetzt werden, nachdem Sie auf **Änderungen übernehmen** geklickt haben.

Fehlerbehebung bei der Warnung „Niedriger Objektdatenspeicher“

Die Warnung **Geringer Objektdatenspeicher** überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Speicherknoten verfügbar ist.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Du hast ["spezifische Zugriffsberechtigungen"](#).

Informationen zu diesem Vorgang

Die Warnung **Geringer Objektdatenspeicher** wird ausgelöst, wenn die Gesamtmenge der replizierten und löschcodierten Objektdaten auf einem Speicherknoten eine der in der Warnregel konfigurierten Bedingungen erfüllt.

Standardmäßig wird eine wichtige Warnung ausgelöst, wenn diese Bedingung als wahr ausgewertet wird:

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In diesem Zustand:

- ``storagegrid_storage_utilization_data_bytes`` ist eine Schätzung der Gesamtgröße der replizierten und

erasure-coded Objektdaten für einen Speicherknoten.

- `storagegrid\_storage\_utilization\_usable\_space\_bytes` ist die Gesamtmenge des für einen Speicherknoten verbleibenden Objektspeicherplatzes.

Wenn eine größere oder kleinere Warnung „Geringer Objektdatenspeicher“ ausgelöst wird, sollten Sie so schnell wie möglich eine Erweiterungsprozedur durchführen.

Schritte

1. Wählen Sie **WARNUNGEN > Aktuell**.

Die Seite „Warnungen“ wird angezeigt.

2. Erweitern Sie in der Tabelle der Warnungen bei Bedarf die Warnungsgruppe **Niedriger Objektdatenspeicher** und wählen Sie die Warnung aus, die Sie anzeigen möchten.



Wählen Sie die Warnung aus, nicht die Überschrift für eine Gruppe von Warnungen.

3. Überprüfen Sie die Details im Dialogfeld und beachten Sie Folgendes:

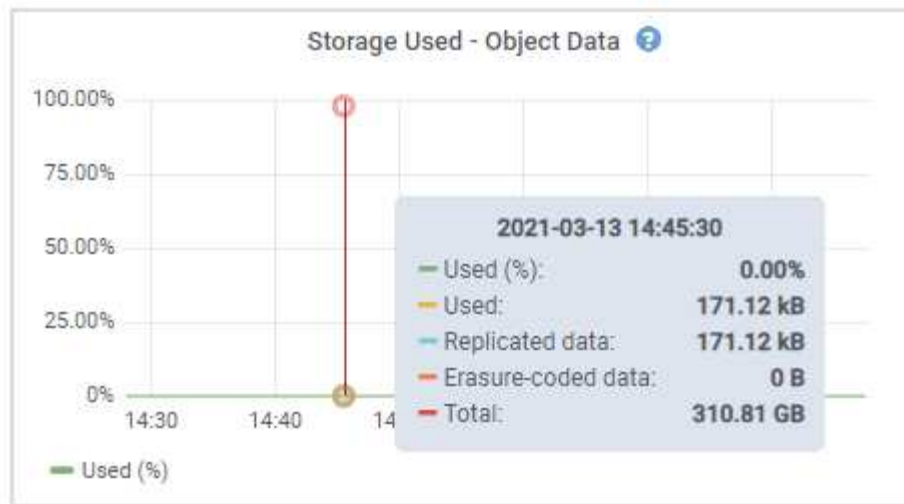
- Zeitgesteuert
- Der Name der Site und des Knotens
- Die aktuellen Werte der Metriken für diese Warnung

4. Wählen Sie **NODES > Speicherknoten oder -Site > Speicher**.

5. Positionieren Sie den Cursor über dem Diagramm „Speicherplatznutzung – Objektdaten“.

Es werden folgende Werte angezeigt:

- **Verwendet (%)**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Verwendet**: Die Menge des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Replizierte Daten**: Eine Schätzung der Menge der replizierten Objektdaten auf diesem Knoten, dieser Site oder diesem Raster.
- **Löschcodierte Daten**: Eine Schätzung der Menge der löschcodierten Objektdaten auf diesem Knoten, dieser Site oder diesem Raster.
- **Gesamt**: Die Gesamtmenge des nutzbaren Speicherplatzes auf diesem Knoten, dieser Site oder diesem Raster. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` metrisch.



6. Wählen Sie die Zeitsteuerungen über dem Diagramm aus, um die Speichernutzung über verschiedene Zeiträume anzuzeigen.

Durch die Betrachtung der Speichernutzung im Zeitverlauf können Sie besser nachvollziehen, wie viel Speicher vor und nach dem Auslösen der Warnung verwendet wurde. Außerdem können Sie so abschätzen, wie lange es dauern könnte, bis der verbleibende Speicherplatz des Knotens voll ist.

7. So schnell wie möglich, "[Speicherkapazität hinzufügen](#)" zu Ihrem Raster.

Sie können Speichervolumen (LUNs) zu vorhandenen Speicherknoten hinzufügen oder neue Speicherknoten hinzufügen.



Weitere Informationen finden Sie unter "[Vollständige Speicherknoten verwalten](#)".

Fehlerbehebung bei Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, müssen Sie möglicherweise die Warnung „Niedriges schreibgeschütztes Wasserzeichen überschreiben“ beheben. Wenn möglich, sollten Sie Ihr System aktualisieren, um die optimierten Werte zu verwenden.

In früheren Versionen waren die drei "[Speichervolumen-Wasserzeichen](#)" globale Einstellungen – dieselben Werte wurden auf jedes Speichervolumen auf jedem Speicherknoten angewendet. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Speichervolumen basierend auf der Größe des Speicherknotens und der relativen Kapazität des Volumens optimieren.

Wenn Sie auf StorageGRID 11.6 oder höher aktualisieren, werden optimierte schreibgeschützte und Lese-/Schreib-Wasserzeichen automatisch auf alle Speichervolumen angewendet, es sei denn, einer der folgenden Punkte trifft zu:

- Ihr System ist fast ausgelastet und könnte keine neuen Daten aufnehmen, wenn optimierte Wasserzeichen angewendet würden. StorageGRID ändert in diesem Fall die Wasserzeicheneinstellungen nicht.
- Sie haben zuvor eines der Wasserzeichen des Speichervolumens auf einen benutzerdefinierten Wert festgelegt. StorageGRID überschreibt benutzerdefinierte Wasserzeicheneinstellungen nicht durch

optimierte Werte. StorageGRID kann jedoch die Warnung **Niedriges schreibgeschütztes Wasserzeichen außer Kraft setzen** auslösen, wenn Ihr benutzerdefinierter Wert für das weiche schreibgeschützte Wasserzeichen des Speichervolumes zu klein ist.

Verstehen Sie die Warnung

Wenn Sie benutzerdefinierte Werte für Speichervolume-Wasserzeichen verwenden, wird möglicherweise für einen oder mehrere Speicherknoten die Warnung **Niedriges schreibgeschütztes Wasserzeichen außer Kraft setzen** ausgelöst.

Jede Instanz der Warnung zeigt an, dass der benutzerdefinierte Wert des weichen schreibgeschützten Wasserzeichens des Speichervolumes kleiner ist als der minimal optimierte Wert für diesen Speicherknoten. Wenn Sie weiterhin die benutzerdefinierte Einstellung verwenden, kann es passieren, dass der Speicherplatz des Speicherknotens kritisch knapp wird, bevor er sicher in den schreibgeschützten Zustand wechseln kann. Auf einige Speichervolumen kann möglicherweise nicht mehr zugegriffen werden (sie werden automatisch ausgehängt), wenn der Knoten seine Kapazitätsgrenze erreicht.

Angenommen, Sie haben das Soft-Read-Only-Wasserzeichen des Speichervolumes zuvor auf 5 GB festgelegt. Nehmen wir nun an, dass StorageGRID die folgenden optimierten Werte für die vier Speichervolumen im Speicherknoten A berechnet hat:

Band 0	12 GB
Band 1	12 GB
Band 2	11 GB
Band 3	15 GB

Die Warnung **Niedriger schreibgeschützter Wasserzeichen-Override** wird für Speicherknoten A ausgelöst, weil Ihr benutzerdefiniertes Wasserzeichen (5 GB) kleiner ist als der minimal optimierte Wert für alle Volumens in diesem Knoten (11 GB). Wenn Sie weiterhin die benutzerdefinierte Einstellung verwenden, kann der Speicherplatz des Knotens möglicherweise kritisch knapp werden, bevor er sicher in den schreibgeschützten Zustand wechseln kann.

Beheben Sie die Warnung

Führen Sie die folgenden Schritte aus, wenn eine oder mehrere Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“ ausgelöst wurden. Sie können diese Anweisungen auch verwenden, wenn Sie derzeit benutzerdefinierte Wasserzeicheneinstellungen verwenden und optimierte Einstellungen verwenden möchten, auch wenn keine Warnungen ausgelöst wurden.

Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind beim Grid Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Sie haben die ["Root-Zugriffsberechtigung"](#).

Informationen zu diesem Vorgang

Sie können die Warnung **Niedriger schreibgeschützter Wasserzeichen-Override** beheben, indem Sie die benutzerdefinierten Wasserzeicheneinstellungen auf die neuen Wasserzeichen-Overrides aktualisieren. Wenn

jedoch ein oder mehrere Speicherknoten fast voll sind oder Sie spezielle ILM-Anforderungen haben, sollten Sie sich zunächst die optimierten Speicherwasserzeichen ansehen und feststellen, ob deren Verwendung sicher ist.

Bewerten Sie die Objektdatennutzung für das gesamte Raster

Schritte

1. Wählen Sie **NODES**.
2. Erweitern Sie für jede Site im Raster die Liste der Knoten.
3. Überprüfen Sie die Prozentwerte, die in der Spalte **Verwendete Objektdaten** für jeden Speicherknoten an jedem Standort angezeigt werden.

Nodes

View the list and status of sites and grid nodes.

Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Führen Sie den entsprechenden Schritt aus:
 - a. Wenn keiner der Speicherknoten annähernd voll ist (z. B. alle Werte für **verwendete Objektdaten** kleiner als 80 % sind), können Sie mit der Verwendung der Überschreibungseinstellungen beginnen. Gehe zu [Verwenden Sie optimierte Wasserzeichen](#).
 - b. Wenn ILM-Regeln ein striktes Ingest-Verhalten verwenden oder wenn bestimmte Speicherpools fast voll sind, führen Sie die Schritte in [Optimierte Speicherwasserzeichen anzeigen](#) Und [Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können](#).

Optimierte Speicherwasserzeichen anzeigen

StorageGRID verwendet zwei Prometheus-Metriken, um die optimierten Werte anzuzeigen, die es für das Soft

Read-Only-Wasserzeichen des Speichervolumens berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Metriken**.
2. Wählen Sie im Abschnitt „Prometheus“ den Link zum Zugriff auf die Prometheus-Benutzeroberfläche aus.
3. Um das empfohlene minimale Soft-Read-Only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

Die letzte Spalte zeigt den minimal optimierten Wert des weichen schreibgeschützten Wasserzeichens für alle Speichervolumen auf jedem Speicherknoten. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das weiche schreibgeschützte Wasserzeichen des Speichervolumen, wird für den Speicherknoten die Warnung **Niedriges schreibgeschütztes Wasserzeichen außer Kraft setzen** ausgelöst.

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

Die letzte Spalte zeigt den maximal optimierten Wert des weichen schreibgeschützten Wasserzeichens für alle Speichervolumen auf jedem Speicherknoten.

5. Beachten Sie den maximal optimierten Wert für jeden Speicherknoten.

[[optimierte Wasserzeichen bestimmen]]Stellen Sie fest, ob Sie optimierte Wasserzeichen verwenden können

Schritte

1. Wählen Sie **NODES**.
2. Wiederholen Sie diese Schritte für jeden Online-Speicherknoten:
 - a. Wählen Sie **Speicherknoten > Speicher**.
 - b. Scrollen Sie nach unten zur Tabelle „Objektspeicher“.
 - c. Vergleichen Sie den **Verfügbar**-Wert für jeden Objektspeicher (Volume) mit dem maximal optimierten Wasserzeichen, das Sie für diesen Speicherknoten notiert haben.
3. Wenn mindestens ein Volume auf jedem Online-Speicherknoten mehr Speicherplatz zur Verfügung hat als das maximal optimierte Wasserzeichen für diesen Knoten, gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#) um mit der Verwendung der optimierten Wasserzeichen zu beginnen.

Andernfalls erweitern Sie das Netz so schnell wie möglich. Entweder ["Speichervolumen hinzufügen"](#) zu einem bestehenden Knoten oder ["neue Speicherknoten hinzufügen"](#). Gehen Sie dann zu [Verwenden Sie optimierte Wasserzeichen](#) um die Wasserzeicheneinstellungen zu aktualisieren.

4. Wenn Sie weiterhin benutzerdefinierte Werte für die Speichervolumen-Wasserzeichen verwenden müssen, ["Schweigen"](#) oder ["deaktivieren"](#) die Warnung **Niedriges schreibgeschütztes Wasserzeichen überschreiben**.



Auf jedem Speichervolume auf jedem Speicherknoten werden dieselben benutzerdefinierten Wasserzeichenwerte angewendet. Die Verwendung kleinerer Werte als empfohlen für Speichervolume-Wasserzeichen kann dazu führen, dass auf einige Speichervolumes nicht mehr zugegriffen werden kann (sie werden automatisch ausgehängt), wenn der Knoten seine Kapazitätsgrenze erreicht.

Verwenden Sie optimierte Wasserzeichen

Schritte

1. Gehen Sie zu **SUPPORT > Sonstiges > Speicherwasserzeichen**.
2. Aktivieren Sie das Kontrollkästchen **Optimierte Werte verwenden**.
3. Wählen Sie **Speichern**.

Für jedes Speichervolume gelten jetzt optimierte Wasserzeicheneinstellungen, basierend auf der Größe des Speicherknotens und der relativen Kapazität des Volumes.

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 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.