



# **Behebung von Objekt- und Storage-Problemen**

**StorageGRID**

NetApp

December 03, 2025

# Inhalt

Behebung von Objekt- und Storage-Problemen . . . . .	1
Bestätigen Sie den Speicherort der Objektdaten . . . . .	1
Fehler beim Objektspeicher (Storage Volume) . . . . .	3
Überprüfen Sie die Objektintegrität . . . . .	5
Was ist Hintergrundüberprüfung? . . . . .	6
Was ist Objektexistenz-Prüfung? . . . . .	8
Fehlerbehebung bei S3 PUT Objektgröße zu groß Warnung . . . . .	13
Fehlerbehebung bei verlorenen und fehlenden Objektdaten . . . . .	15
Fehlerbehebung bei verlorenen und fehlenden Objektdaten: Übersicht . . . . .	15
Untersuchen Sie verlorene Objekte . . . . .	15
Suche nach potenziell verlorenen Objekten und Wiederherstellung . . . . .	21
Verlorene und fehlende Objektanzahl zurücksetzen . . . . .	27
Beheben Sie die Warnung „Niedrig Object Data Storage“ . . . . .	28
Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff . . . . .	30
Analysieren Sie die Meldung . . . . .	31
Beheben Sie die Meldung . . . . .	31
Fehlersuche im SSTS-Alarm (Storage Status) durchführen . . . . .	33
Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm) . . . . .	38

# Behebung von Objekt- und Storage-Problemen

## Bestätigen Sie den Speicherort der Objektdaten

Je nach dem Problem sollten Sie dies möglicherweise tun "["Bestätigen Sie, wo Objektdaten gespeichert werden"](#)". Beispielsweise möchten Sie überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und Objektdaten dort gespeichert werden, wo sie geplant sind.

### Bevor Sie beginnen

- Sie müssen über eine Objektkennung verfügen, die einer der folgenden sein kann:
  - **UUID:** Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.
  - **CBID:** Die eindeutige Kennung des Objekts in 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 durch das aufgenommen wird "["S3 Schnittstelle"](#)", Die Client-Anwendung verwendet eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
  - **Swift-Container und Objektname:** Wenn ein Objekt durch das aufgenommen wird "["Swift-Schnittstelle"](#)", Die Client-Anwendung verwendet eine Kombination aus Container und Objektnamen, um das Objekt zu speichern und zu identifizieren.

### Schritte

1. Wählen Sie **ILM > Object Metadata Lookup**.
2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

Sie können eine UUID, CBID, S3 Bucket/Objektschlüssel oder Swift Container/Objektname eingeben.

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

The screenshot shows a web-based 'Object Metadata Lookup' tool. At the top, the title 'Object Metadata Lookup' is displayed. Below it, a sub-instruction reads 'Enter the identifier for any object stored in the grid to view its metadata.' There are two input fields: 'Identifier' containing 'source/testobject' and 'Version ID (optional)' containing 'MEJGMkMyQzigtNEY5OC0xMUU3LTkzMExhRDAyNTAwQRK5N0Mx'. A large blue 'Look Up' button is positioned at the bottom of the form.

4. Wählen Sie **Look Up**.

Der "["Ergebnisse der Suche nach Objektmetadaten"](#)" Angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

- Systemmetadaten, einschließlich Objekt-ID (UUID), Version-ID (optional), Objektname, Name des Containers, Mandantenkontoname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie 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, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten 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-31FF00C36056",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",
      "PAWS2": "2"
    }
  }
}
```

## Fehler beim Objektspeicher (Storage Volume)

Der zugrunde liegende Storage auf einem Storage-Node ist in Objektspeicher unterteilt. Objektspeicher werden auch als Storage Volumes bezeichnet.

Sie können die 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

Um mehr zu sehen "[Details zu jedem Storage-Node](#)", Folgen Sie folgenden Schritten:

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site > Storage Node > LDR > Storage > Übersicht > Haupt**.

The screenshot shows the Storage Overview page for LDR (DC1-S1). It includes sections for Storage State, Utilization, Replication, and Object Store Volumes, each with detailed metrics and status indicators.

**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

Je nach Art des Ausfalls können Fehler bei einem Storage-Volume in einem Alarm über den Storage-Status oder den Zustand eines Objektspeicher gespiegelt werden. Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um den Speicherhüter so bald wie möglich wieder voll zu machen. Bei Bedarf können Sie auf die Registerkarte **Konfiguration** und gehen "[Setzen Sie den Speicher-Node in einen schreibgeschützten Status](#)" Damit das StorageGRID-System es für den Datenabruf nutzen kann, während Sie sich auf ein vollständiges Recovery des Servers vorbereiten.

## Überprüfen Sie die Objektintegrität

Das StorageGRID System überprüft die Integrität der Objektdaten auf Storage-Nodes und überprüft sowohl beschädigte als auch fehlende Objekte.

Es gibt zwei Verifizierungsverfahren: Hintergrundüberprüfung und Objektexistenz-Prüfung (früher als Vordergrundüberprüfung bezeichnet). Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung wird automatisch ausgeführt und überprüft kontinuierlich die Korrektheit von Objektdaten. Die Überprüfung der ObjektExistenz kann von einem Benutzer ausgelöst werden, um die Existenz (obwohl nicht die Richtigkeit) von Objekten schneller zu überprüfen.

## Was ist Hintergrundüberprüfung?

Die Hintergrundüberprüfung überprüft Storage Nodes automatisch und kontinuierlich auf beschädigte Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Bei der Hintergrundüberprüfung werden die Integrität replizierter Objekte und Objekte mit Erasure-Coding-Verfahren überprüft:

- **Replizierte Objekte:** Findet der Hintergrundverifizierungsvorgang ein beschädigtes Objekt, wird die beschädigte Kopie vom Speicherort entfernt und an anderer Stelle auf dem Speicherknoten isoliert. Anschließend wird eine neue, nicht beschädigte Kopie generiert und gemäß den aktiven ILM-Richtlinien abgelegt. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die ursprüngliche Kopie verwendet wurde.
-  Beschädigte Objektdaten werden nicht aus dem System gelöscht, sondern in Quarantäne verschoben, sodass weiterhin darauf zugegriffen werden kann. Weitere Informationen zum Zugriff auf gesperrte Objektdaten erhalten Sie vom technischen Support.
- **Erasure-codierte Objekte:** Erkennt der Hintergrund-Verifizierungsprozess, dass ein Fragment eines Löschungscodierten Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Daten- und Paritätsfragmente neu zu erstellen. Wenn das beschädigte Fragment nicht neu erstellt werden kann, wird versucht, eine weitere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Bewertung durchgeführt, um eine Ersatzkopie des Objekts, das mit der Fehlerkorrektur codiert wurde, zu erstellen.

Bei der Hintergrundüberprüfung werden nur Objekte auf Speicherknoten überprüft. Es überprüft keine Objekte auf Archiv-Nodes oder in einem Cloud-Speicherpool. Objekte müssen älter als vier Tage sein, um sich für die Hintergrundüberprüfung zu qualifizieren.

Die Hintergrundüberprüfung läuft mit einer kontinuierlichen Geschwindigkeit, die nicht auf normale Systemaktivitäten ausgerichtet ist. Die Hintergrundüberprüfung kann nicht angehalten werden. Sie können jedoch die Hintergrundverifizierungsrate erhöhen, um falls Sie vermuten, dass ein Problem vorliegt, den Inhalt eines Storage-Nodes schneller zu überprüfen.

## Warnmeldungen und Alarme (alt) im Zusammenhang mit der Hintergrundüberprüfung

Wenn das System ein beschädigtes Objekt erkennt, das nicht automatisch korrigiert werden kann (weil die Beschädigung verhindert, dass das Objekt identifiziert wird), wird die Warnmeldung **Unidentified Corrupt Object Detected** ausgelöst.

Wenn eine Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, weil es keine weitere Kopie finden kann, wird die Warnmeldung **Objects lost** ausgelöst.

## Ändern Sie die Hintergrundverifizierungsrate

Sie können die Rate ändern, mit der die Hintergrundüberprüfung replizierte Objektdaten auf einem Storage-Node überprüft, wenn Sie Bedenken hinsichtlich der Datenintegrität haben.

### Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".

### Über diese Aufgabe

Sie können die Verifizierungsrate für die Hintergrundüberprüfung eines Speicherknoten ändern:

- **Adaptiv:** Standardeinstellung. Die Aufgabe wurde entwickelt, um maximal 4 MB/s oder 10 Objekte/s zu überprüfen (je nachdem, welcher Wert zuerst überschritten wird).
- **Hoch:** Die Storage-Verifizierung verläuft schnell und kann zu einer Geschwindigkeit führen, die normale Systemaktivitäten verlangsamen kann.

Verwenden Sie die hohe Überprüfungsrate nur, wenn Sie vermuten, dass ein Hardware- oder Softwarefehler beschädigte Objektdaten aufweisen könnte. Nach Abschluss der Hintergrundüberprüfung mit hoher Priorität wird die Verifizierungsrate automatisch auf Adaptive zurückgesetzt.

#### Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Storage Node > LDR > Verifizierung** aus.
3. Wählen Sie **Konfiguration > Main**.
4. Gehen Sie zu **LDR > Verifizierung > Konfiguration > Main**.
5. Wählen Sie unter Hintergrundüberprüfung die Option **Verifizierungsrate > hoch** oder **Verifizierungsrate > adaptiv** aus.

The screenshot shows the 'Configuration: LDR' page with the 'Verification' tab selected. In the 'Background Verification' section, the 'Verification Rate' dropdown is highlighted with a green border and contains the value 'Adaptive'. There are also checkboxes for 'Reset Missing Objects Count' and 'Reset Corrupt Objects Count'. At the bottom right of the page is a blue 'Apply Changes' button with a right-pointing arrow.



Wenn Sie die Verifizierungsrate auf hoch setzen, wird der alte Alarm VPRI (Verification Rate) auf der Melderebene ausgelöst.

6. Klicken Sie Auf **Änderungen Übernehmen**.
7. Überwachen der Ergebnisse der Hintergrundüberprüfung replizierter Objekte
  - a. Wechseln Sie zu **NODES > Storage Node > Objects**.
  - b. Überwachen Sie im Abschnitt Überprüfung die Werte für **beschädigte Objekte** und **beschädigte Objekte nicht identifiziert**.

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

- Wenn die Objekt-ID extrahiert werden kann, erstellt StorageGRID automatisch eine neue Kopie der Objektdaten. Die neue Kopie kann an jedem beliebigen Ort im StorageGRID System erstellt werden, der die aktiven ILM-Richtlinien erfüllt.
  - Wenn der Objektbezeichner nicht extrahiert werden kann (weil er beschädigt wurde), wird die Metrik **korrupte Objekte nicht identifiziert** erhöht und die Warnung **nicht identifiziertes beschädigtes Objekt erkannt** ausgelöst.
- c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Ursache der Beschädigung zu ermitteln.
8. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung von Objekten, die mit Erasure Coding codiert wurden.

Wenn bei der Hintergrundüberprüfung beschädigte Fragmente von Objektdaten gefunden werden, die mit dem Erasure-Coding-Verfahren codiert wurden, wird das Attribut „beschädigte Fragmente erkannt“ erhöht. StorageGRID stellt sich wieder her, indem das beschädigte Fragment auf demselben Speicherknoten wiederhergestellt wird.

- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
  - b. Wählen Sie **Storage Node > LDR > Erasure Coding** aus.
  - c. Überwachen Sie in der Tabelle „Ergebnisse der Überprüfung“ das Attribut „beschädigte Fragmente erkannt“ (ECCD).
9. Nachdem das StorageGRID System beschädigte Objekte automatisch wiederhergestellt hat, setzen Sie die Anzahl beschädigter Objekte zurück.
- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
  - b. Wählen Sie **Storage Node > LDR > Verifizierung > Konfiguration**.
  - c. Wählen Sie **Anzahl Der Beschädigten Objekte Zurücksetzen**.
  - d. Klicken Sie Auf **Änderungen Übernehmen**.
10. Wenn Sie sicher sind, dass isolierte Objekte nicht erforderlich sind, können Sie sie löschen.



Wenn der Alarm **Objects lost** oder der Legacy-Alarm LOST (Lost Objects) ausgelöst wurde, möchte der technische Support möglicherweise auf isolierte Objekte zugreifen, um das zugrunde liegende Problem zu beheben oder eine Datenwiederherstellung zu versuchen.

- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- b. Wählen Sie **Storage Node > LDR > Verifizierung > Konfiguration**.
- c. Wählen Sie **Gesperrte Objekte Löschen**.
- d. Wählen Sie **Änderungen Anwenden**.

## Was ist Objektexistenz-Prüfung?

Die ObjektExistenz überprüft, ob alle erwarteten replizierten Kopien von Objekten und mit Erasure Coding verschlüsselten Fragmenten auf einem Storage Node vorhanden sind. Die Objektüberprüfung überprüft nicht die Objektdaten selbst (Hintergrundüberprüfung führt das durch); stattdessen bietet sie eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich auftretende Hardwareproblem die Datenintegrität beeinträchtigen könnte.

Im Gegensatz zur automatischen Hintergrundüberprüfung müssen Sie einen Auftrag zur Überprüfung der Objektexistenz manuell starten.

Die Objektexistenz prüft die Metadaten für jedes in StorageGRID gespeicherte Objekt und überprüft, ob es sich um replizierte Objektkopien sowie um Erasure Coding verschlüsselte Objektfragmente handelt. Fehlende Daten werden wie folgt behandelt:

- **Replizierte Kopien:** Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, die Kopie von einer an anderer Stelle im System gespeicherten Kopie zu ersetzen. Der Storage-Node führt eine vorhandene Kopie durch eine ILM-Evaluierung aus. Damit wird festgestellt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da eine weitere Kopie fehlt. Es wird eine neue Kopie erzeugt und abgelegt, um den aktiven ILM-Richtlinien des Systems zu entsprechen. Diese neue Kopie kann nicht an derselben Stelle platziert werden, an der die fehlende Kopie gespeichert wurde.
- **Erasure-codierte Fragmente:** Fehlt ein Fragment eines Objekts mit Löschungscode, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten mithilfe der verbleibenden Fragmente neu zu erstellen. Wenn das fehlende Fragment nicht neu aufgebaut werden kann (weil zu viele Fragmente verloren gegangen sind), versucht ILM, eine andere Kopie des Objekts zu finden, mit der es ein neues, lösercodiertes Fragment generieren kann.

## Überprüfung der ObjektExistenz ausführen

Sie erstellen und führen jeweils einen Job für die Überprüfung der Objektexistenz aus. Wenn Sie einen Job erstellen, wählen Sie die Storage-Nodes und Volumes aus, die Sie überprüfen möchten. Sie wählen auch die Konsistenz für den Job aus.

### Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Berechtigung für Wartung oder Root-Zugriff](#)".
- Sie haben sichergestellt, dass die zu prüfenden Speicherknoten online sind. Wählen Sie **NODES**, um die Tabelle der Knoten anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen für die Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden Verfahren auf den Knoten, die Sie überprüfen möchten, **nicht** ausgeführt werden:
  - Grid-Erweiterung, um einen Storage-Node hinzuzufügen
  - Deaktivierung des Storage Node
  - Recovery eines ausgesunkenen Storage-Volumes
  - Wiederherstellung eines Speicherknoten mit einem ausgesunkenen Systemlaufwerk
  - EC-Ausgleich
  - Appliance-Node-Klon

Die Objektprüfung bietet keine nützlichen Informationen, während diese Verfahren ausgeführt werden.

### Über diese Aufgabe

Ein Prüfauftrag für eine Objektexistenz kann Tage oder Wochen dauern, abhängig von der Anzahl der Objekte im Grid, den ausgewählten Storage-Nodes und Volumes und der ausgewählten Konsistenz. Sie können nur einen Job gleichzeitig ausführen, aber Sie können mehrere Speicherknoten und Volumes gleichzeitig auswählen.

### Schritte

1. Wählen Sie **WARTUNG > Aufgaben > Objekt Existenzprüfung**.
2. Wählen Sie **Job erstellen**. Der Assistent Job-Prüfung für Objektexistenz erstellen wird angezeigt.
3. Wählen Sie die Nodes aus, die die Volumes enthalten, die Sie überprüfen möchten. Um alle Online-Knoten auszuwählen, aktivieren Sie das Kontrollkästchen **Knotename** in der Spaltenüberschrift.

Sie können nach Node-Namen 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 mithilfe der Storage-Volume-Nummer oder des Node-Namens 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 Job aus.

Die Konsistenz legt fest, wie viele Kopien von Objektmetadaten für die Prüfung der Objektexistenz verwendet werden.

- **Strong-site**: Zwei Kopien von Metadaten an einem einzigen Standort.
- **Stark-global**: Zwei Kopien von Metadaten an jedem Standort.
- **Alle (Standard)**: Alle drei Kopien von Metadaten an jedem Standort.

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

8. Wählen Sie **Weiter**.
9. Ihre Auswahl überprüfen und überprüfen. Sie können **Zurück** auswählen, um zu einem vorherigen Schritt im Assistenten zu wechseln, um Ihre Auswahl zu aktualisieren.

Ein Job zur Überprüfung der Objektexistenz wird erstellt und wird ausgeführt, bis einer der folgenden Aktionen ausgeführt wird:

- Der Job ist abgeschlossen.
- Sie unterbrechen oder abbrechen den Job. Sie können einen angehaltenen Job fortsetzen, aber einen abgebrochenen Job nicht wieder aufnehmen.
- Der Job wird abgestellt. Die Warnung \* Objektexistenz ist blockiert\* wird ausgelöst. Befolgen Sie die für die Meldung angegebenen Korrekturmaßnahmen.
- Der Job schlägt fehl. Die Warnung \* Objektexistenz ist fehlgeschlagen\* wird ausgelöst. Befolgen Sie die für die Meldung angegebenen Korrekturmaßnahmen.
- Es wird die Meldung „Service nicht verfügbar“ oder „interner Serverfehler“ angezeigt. Aktualisieren Sie nach einer Minute die Seite, um mit der Überwachung des Jobs fortzufahren.



Sie können bei Bedarf von der Seite „Objektexistenz“ wegnavigieren und mit der Überwachung des Jobs fortfahren.

10. Zeigen Sie während der Ausführung des Jobs die Registerkarte **aktiver Job** an, und notieren Sie den Wert fehlender Objektkopien.

Dieser Wert stellt die Gesamtzahl der fehlenden Kopien replizierter Objekte und Objekte mit Erasure-Coding-Code mit einem oder mehreren fehlenden Fragmenten dar.

Wenn die Anzahl der erkannten fehlenden Objektkopien größer als 100 ist, kann es zu einem Problem mit dem Speicher des Speicherknotens kommen.

## 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.

The screenshot shows the 'Object existence check' interface. At the top, there are two tabs: 'Active job' (selected) and 'Job history'. Below the tabs, job details are displayed: Status: Accepted, Job ID: 2334602652907829302, Consistency control: All. A green box highlights 'Missing object copies detected: 0'. Progress bar: 0%. To the right, Start time: 2021-11-10 14:43:02 MST, Elapsed time: —, Estimated time to completion: —. Below the job details are two buttons: 'Pause' and 'Cancel'. At the bottom, there are two tabs: 'Volumes' (selected) and 'Details'. The 'Volumes' tab displays a table with three rows:

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. Nehmen Sie nach Abschluss des Jobs alle weiteren erforderlichen Maßnahmen vor:

- Wenn fehlende Objektkopien gefunden wurden, ist Null, dann wurden keine Probleme gefunden. Es ist keine Aktion erforderlich.
- Wenn fehlende Objektkopien erkannt sind größer als Null und die Warnung **Objekte verloren** nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Überprüfen Sie, ob Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu vermeiden.
- Wenn fehlende Objektkopien erkannt sind größer als Null und die Warnung **Objekte verloren** ausgelöst wurde, könnte die Datenintegrität beeinträchtigt werden. Wenden Sie sich an den technischen Support.
- Sie können verlorene Objektkopien untersuchen, indem Sie die LLST-Audit-Meldungen mit grep extrahieren: grep LLST audit\_file\_name.

Dieses Verfahren ähnelt dem Verfahren für "[Untersuchung verlorener Objekte](#)", Obwohl für Objektkopien Sie suchen LLST Statt OLST.

12. Wenn Sie die strong-site- oder strong-global-Konsistenz für den Job ausgewählt haben, warten Sie etwa drei Wochen auf die Metadatenkonsistenz, und führen Sie den Job erneut auf denselben Volumes aus.

Wenn StorageGRID Zeit hatte, konsistente Metadaten für die im Job enthaltenen Nodes und Volumes zu erzielen, konnte eine erneute Ausführung des Jobs fälschlicherweise gemeldete fehlende Objektkopien löschen oder zusätzliche Objektkopien veranlassen, dass sie nicht verwendet wurden.

- a. Wählen Sie **WARTUNG > Objekt Existenzprüfung > Jobverlauf**.
- b. Legen Sie fest, welche Jobs für die erneute Ausführung bereit sind:
  - i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.
  - ii. Überprüfen Sie für diese Jobs die Spalte Consistency Control auf Strong-site oder strong-global.
- c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **erneut ausführen**.

The screenshot shows a table of job results from an 'Object existence check'. The table has columns for Job ID, Status, Nodes (volumes), Missing object copies detected, Consistency control, Start time, and End time. Two rows are visible:

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 (3 weeks ago)	2021-11-10 14:43:06 MST
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 (17 minutes ago)	2021-11-10 14:42:11 MST

- 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 **Rerun**.

Die Registerkarte „aktiver Job“ wird angezeigt. Alle von Ihnen ausgewählten Jobs werden als ein Job an einer Konsistenz von strong-site erneut ausgeführt. In einem Feld mit \* Related Jobs\* im Bereich Details werden die Job-IDs für die ursprünglichen Jobs angezeigt.

#### Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **SUPPORT > Tools > Grid-Topologie > Site > Storage-Node > LDR > Verifizierung > Konfiguration > Main** und erhöhen Sie die Hintergrundverifizierungsrate. Die Hintergrundüberprüfung überprüft die Richtigkeit aller gespeicherten Objektdaten und repariert sämtliche gefundenen Probleme. Das schnelle Auffinden und Reparieren potenzieller Probleme verringert das Risiko von Datenverlusten.

# Fehlerbehebung bei S3 PUT Objektgröße zu groß Warnung

Die Warnmeldung S3 PUT Object size too Large wird ausgelöst, wenn ein Mandant versucht, einen nicht mehrteiligen PutObject-Vorgang auszuführen, der das S3-Größenlimit von 5 gib überschreitet.

## Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".

Legen Sie fest, welche Mandanten Objekte verwenden, die größer als 5 gib sind, damit Sie sie benachrichtigen können.

## Schritte

1. Gehen Sie zu **CONFIGURATION > Monitoring > Audit und Syslog-Server**.
2. Wenn die Schreibvorgänge des Clients normal sind, greifen Sie auf das Revisionsprotokoll zu:

- a. Eingabe ssh admin@*primary\_Admin\_Node\_IP*
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.

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

Das Verzeichnis der Überwachungsprotokolle und die entsprechenden Knoten hängen von den Einstellungen des Überwachungsziels ab.

Option	Ziel
Lokale Knoten (Standard)	/var/local/log/localaudit.log
Admin-Nodes/lokale Nodes	<ul style="list-style-type: none"><li>• Admin-Nodes (primär und nicht primär): /var/local/audit/export/audit.log</li><li>• Alle Knoten: Die /var/local/log/localaudit.log Datei ist in der Regel leer oder fehlt in diesem Modus.</li></ul>
Externer Syslog-Server	/var/local/log/localaudit.log

Geben Sie je nach den Einstellungen des Überwachungsziels Folgendes ein: cd /var/local/log  
Oder /var/local/audit/export/

Weitere Informationen finden Sie unter "[Wählen Sie Ziele für Audit-Informationen aus](#)".

- f. Ermitteln Sie, welche Mandanten Objekte mit einer Größe von mehr als 5 gib verwenden.
  - i. Eingabe `zgrep SPUT * | egrep "CSIZ\(\UI64\):([5-9]| [1-9][0-9]+)[0-9]{9}"`

- ii. Sehen Sie sich für jede Audit-Meldung in den Ergebnissen an S3AI Feld, um die Konto-ID des Mandanten zu bestimmen. Verwenden Sie die anderen Felder in der Meldung, um zu bestimmen, welche IP-Adresse vom Client, vom Bucket und vom Objekt verwendet wurde:

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

### Beispiel für Ergebnisse des Audit-Protokolls

```
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):"060X85M40Q90Y280B7YT"][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-
9B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):PUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Wenn die Schreibvorgänge des Clients nicht normal sind, verwenden Sie die Mandanten-ID in der Warnmeldung, um den Mandanten zu identifizieren:
- Gehen Sie zu **SUPPORT > Tools > Logs**. Sammeln Sie Anwendungsprotokolle für den Speicher-Node in der Warnmeldung. Geben Sie 15 Minuten vor und nach der Warnmeldung an.
  - Extrahieren Sie die Datei, und gehen Sie zu `broadcast.log`:

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

- Durchsuchen Sie das Protokoll nach `method=PUT` Und identifizieren Sie den Client im `clientIP` Feld.

### Beispiel broadcast.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 Mandanten, dass die maximale PutObject-Größe 5 GiB beträgt, und verwenden Sie mehrteilige Uploads für Objekte, die größer als 5 GiB sind.
5. Ignorieren Sie die Warnmeldung für eine Woche, wenn die Anwendung geändert wurde.

## Fehlerbehebung bei verlorenen und fehlenden Objektdaten

### Fehlerbehebung bei verlorenen und fehlenden Objektdaten: Übersicht

Objekte können aus verschiedenen Gründen abgerufen werden, darunter Leseanforderungen von einer Client-Applikation, Hintergrundverifizierungen replizierter Objektdaten, ILM-Neubewertungen und die Wiederherstellung von Objektdaten während der Recovery eines Storage Node.

Das StorageGRID System verwendet Positionsinformationen in den Metadaten eines Objekts, um von welchem Speicherort das Objekt abzurufen. Wenn eine Kopie des Objekts nicht am erwarteten Speicherort gefunden wird, versucht das System, eine andere Kopie des Objekts von einer anderen Stelle im System abzurufen, vorausgesetzt, die ILM-Richtlinie enthält eine Regel zum Erstellen von zwei oder mehr Kopien des Objekts.

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

- Wenn bei replizierten Kopien keine weitere Kopie abgerufen werden kann, gilt das Objekt als verloren, und die Warnmeldung wird ausgelöst.
- Wenn eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, wird das Attribut Corrupt Copies Detected (ECOR) für Kopien, die mit Löschtätigkeiten codiert wurden, um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Falls keine weitere Kopie gefunden wird, wird die Meldung ausgelöst.

Sie sollten alle **Objekte Lost**-Warnungen sofort untersuchen, um die Ursache des Verlusts zu ermitteln und zu ermitteln, ob das Objekt noch in einem Offline-oder anderweitig derzeit nicht verfügbar ist, Storage Node oder Archive Node. Siehe "[Untersuchen Sie verlorene Objekte](#)".

Wenn Objekt-Daten ohne Kopien verloren gehen, gibt es keine Recovery-Lösung. Sie müssen jedoch den Zähler „Lost Objects“ zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren. Siehe "[Verlorene und fehlende Objektanzahl zurücksetzen](#)".

### Untersuchen Sie verlorene Objekte

Wenn der Alarm **Objekte verloren** ausgelöst wird, müssen Sie sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

#### Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".
- Sie müssen die haben `Passwords.txt` Datei:

## Über diese Aufgabe

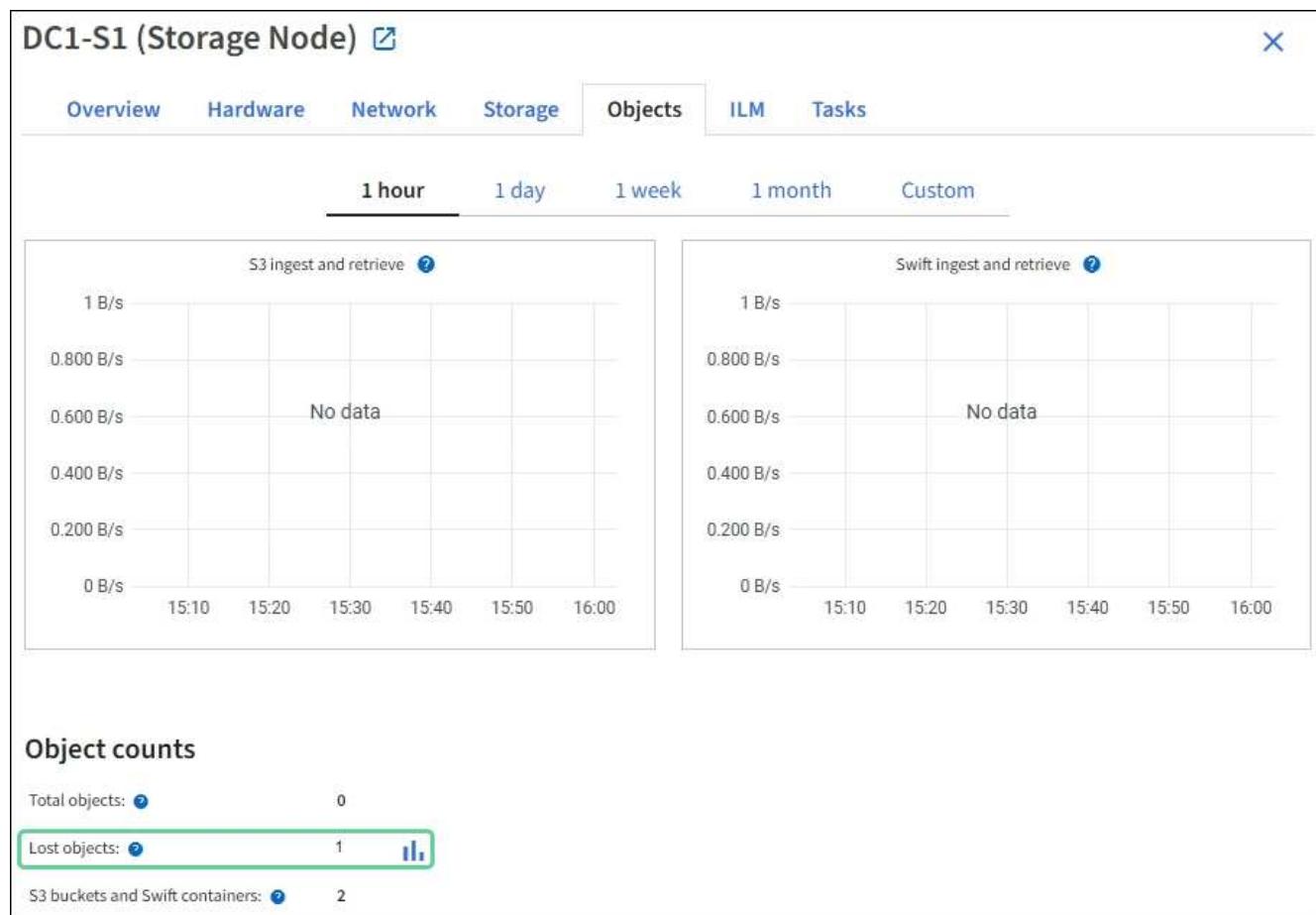
Die Warnung **Objects lost** zeigt an, dass StorageGRID glaubt, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

Untersuchen Sie verlorene Objektwarnungen sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. In einigen Fällen können Sie ein verlorenes Objekt wiederherstellen, wenn Sie eine sofortige Aktion ausführen.

## Schritte

1. Wählen Sie **KNOTEN**.
2. Wählen Sie **Speicherknoten > Objekte Aus**.
3. Überprüfen Sie die Anzahl der verlorenen Objekte, die in der Tabelle Objektanzahl angezeigt werden.

Diese Nummer gibt die Gesamtzahl der Objekte an, die dieser Grid-Node im gesamten StorageGRID-System als fehlend erkennt. Der Wert ist die Summe der Zähler Lost Objects der Data Store Komponente innerhalb der LDR- und DDS-Dienste.



4. Von einem Admin-Node, "[Rufen Sie das Überwachungsprotokoll auf](#)" So bestimmen Sie die eindeutige Kennung (UUID) des Objekts, das die Warnmeldung **Objects lost** ausgelöst hat:
  - a. Melden Sie sich beim Grid-Node an:

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

Das Verzeichnis der Überwachungsprotokolle und die entsprechenden Knoten hängen von den Einstellungen des Überwachungsziels ab.

Option	Ziel
Lokale Knoten (Standard)	<code>/var/local/log/localaudit.log</code>
Admin-Nodes/lokale Nodes	<ul style="list-style-type: none"> <li>• Admin-Nodes (primär und nicht primär): <code>/var/local/audit/export/audit.log</code></li> <li>• Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Datei ist in der Regel leer oder fehlt in diesem Modus.</li> </ul>
Externer Syslog-Server	<code>/var/local/log/localaudit.log</code>

Geben Sie je nach den Einstellungen des Überwachungsziels Folgendes ein: `cd /var/local/log`  
Oder `/var/local/audit/export/`

Weitere Informationen finden Sie unter "[Wählen Sie Ziele für Audit-Informationen aus](#)".

- c. Verwenden Sie grep, um die Audit-Meldungen zu „Objekt verloren“ (OLST) zu extrahieren. Geben Sie Ein: `grep OLST audit_file_name`
- d. Beachten Sie den in der Meldung 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] [A
MID(FC32):ILMX] [ATID(UI64):7729403978647354233]]
```

5. Verwenden Sie die `ObjectByUUID` Befehl zum Suchen des Objekts anhand seiner ID (UUID) und bestimmen Sie, ob die Daten gefährdet sind.
  - a. Verwenden Sie SSH, um sich bei einem beliebigen Storage-Node anzumelden. Rufen Sie dann die LDR-Konsole auf, indem Sie „telnet 0 1402“ eingeben.
  - b. Geben Sie Ein: `/proc/OBRP/ObjectByUUID UUID_value`

In diesem ersten Beispiel, das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 Hat zwei Standorte aufgelistet.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\ (Locations\")": \[
        \{
            "Location Type": "CLDI\ (Location online\")",
            "NOID\ (Node ID\")": "12448208",
            "VOLI\ (Volume ID\")": "3222345473",
            "Object File Path":

```

```
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78I1a\#3udu",
    "LTIM\ (Location timestamp)": "2020-02-
12T19:36:17.880569"
},
\{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12288733",
    "VOLI\ (Volume ID\)": "3222345984",
    "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\ (Location timestamp)": "2020-02-
12T19:36:17.934425"
}
]
```

Im zweiten Beispiel das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 Hat keine Standorte aufgelistet.

```

ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1dff7e959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}

```

- a. Überprüfen Sie die Ausgabe von /proc/OBRP/ObjectByUUID, und ergreifen Sie die entsprechenden Maßnahmen:

Metadaten	Schlussfolgerung
Kein Objekt gefunden ("FEHLER":")	<p>Wenn das Objekt nicht gefunden wird, wird die Meldung „FEHLER“:“ zurückgegeben.</p> <p>Wenn das Objekt nicht gefunden wird, können Sie die Anzahl der <b>verlorenen Objekte</b> zurücksetzen, um die Warnung zu löschen. Das Fehlen eines Objekts bedeutet, dass das Objekt absichtlich gelöscht wurde.</p>
Standorte > 0	<p>Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung <b>Objects Lost</b> falsch positiv sein.</p> <p>Vergewissern Sie sich, dass die Objekte vorhanden sind. Verwenden Sie die Knoten-ID und den Dateipfad, der in der Ausgabe aufgeführt ist, um zu bestätigen, dass sich die Objektdatei am aufgelisteten Speicherort befindet.</p> <p>(Verfahren für "<a href="#">Suche nach möglicherweise verlorenen Objekten</a>" Erläutert, wie Sie die Knoten-ID verwenden, um den richtigen Speicherknoten zu finden.)</p> <p>Wenn die Objekte vorhanden sind, können Sie die Anzahl der <b>verlorenen Objekte</b> zurücksetzen, um die Warnung zu löschen.</p>
Standorte = 0	<p>Wenn in der Ausgabe keine Positionen aufgeführt sind, fehlt das Objekt möglicherweise. Versuchen Sie es "<a href="#">Suchen Sie das Objekt und stellen Sie es wieder her</a>" Selbst oder Sie können sich an den technischen Support wenden.</p> <p>Vom technischen Support bitten Sie möglicherweise, zu bestimmen, ob ein Verfahren zur Storage-Recovery durchgeführt wird. Weitere Informationen finden Sie unter "<a href="#">Wiederherstellen von Objektdaten mit Grid Manager</a>" Und "<a href="#">Wiederherstellung von Objektdaten auf einem Storage-Volume</a>".</p>

## Suche nach potenziell verlorenen Objekten und Wiederherstellung

Möglicherweise können Objekte gefunden und wiederhergestellt werden, die einen Alarm „Lost Objects“ (LOST Objects – LOST) und einen „Object Lost“-Alarm ausgelöst haben und die Sie als „potenziell verloren“ identifiziert haben.

### Bevor Sie beginnen

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

### Über diese Aufgabe

Im Anschluss an dieses Verfahren können Sie sich nach replizierten Kopien des verlorenen Objekts an einer anderen Stelle im Grid suchen. In den meisten Fällen wird das verlorene Objekt nicht gefunden. In einigen Fällen können Sie jedoch ein verlorenes repliziertes Objekt finden und wiederherstellen, wenn Sie umgehend Maßnahmen ergreifen.



Wenden Sie sich an den technischen Support, wenn Sie Hilfe bei diesem Verfahren benötigen.

## Schritte

1. Suchen Sie in einem Admin-Knoten die Prüfprotokolle nach möglichen Objektspeichern:
  - a. Melden Sie sich beim Grid-Node an:
    - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
    - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
    - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
    - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.
  - b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden.

Das Verzeichnis der Überwachungsprotokolle und die entsprechenden Knoten hängen von den Einstellungen des Überwachungsziels ab.

Option	Ziel
Lokale Knoten (Standard)	<code>/var/local/log/localaudit.log</code>
Admin-Nodes/lokale Nodes	<ul style="list-style-type: none"><li>• Admin-Nodes (primär und nicht primär): <code>/var/local/audit/export/audit.log</code></li><li>• Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Datei ist in der Regel leer oder fehlt in diesem Modus.</li></ul>
Externer Syslog-Server	<code>/var/local/log/localaudit.log</code>

Geben Sie je nach den Einstellungen des Überwachungsziels Folgendes ein: `cd /var/local/log`  
Oder `/var/local/audit/export/`

Weitere Informationen finden Sie unter "["Wählen Sie Ziele für Audit-Informationen aus"](#)".

- c. Verwenden Sie grep, um den zu extrahieren "["Überwachungsmeldungen, die mit dem potenziell verlorenen Objekt verknüpft sind"](#)" Und senden Sie sie an eine Ausgabedatei. Geben Sie Ein: `grep uuid-valueaudit_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 Meldungen zum Lost Location (LLST) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep LLST output_file_name`

Beispiel:

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

Eine LLST-Überwachungsmeldung sieht wie in dieser Beispielmeldung 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 in der LLST-Meldung das Feld PCLD und das Feld NOID.

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, wo eine Kopie des Objekts gefunden werden kann.

Wenn Sie einen Speicherort für ein Objekt finden, kann das Objekt möglicherweise wiederhergestellt werden.

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

Die Knoten-ID für den LDR-Dienst befindet sich in der Tabelle Node Information. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie den gefunden haben, der dieses LDR hostet.

2. Stellen Sie fest, ob das Objekt auf dem in der Meldung „Audit“ angegebenen Speicherknoten vorhanden ist:

- a. Melden Sie sich beim Grid-Node an:

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

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

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

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

Geben Sie beispielsweise Folgendes ein:

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



Schließen Sie den Pfad der Objektdatei immer in einzelne Anführungszeichen ein, um Sonderzeichen zu umgehen.

- Wenn der Objektpfad nicht gefunden wird, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wird, 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:

- a. Ändern Sie vom gleichen Speicherknoten aus die Eigentumsrechte an der Objektdatei, so dass sie von StorageGRID gemanagt werden kann. Geben Sie Ein: chown ldr-user:broadcast 'file\_path\_of\_object'
- b. Verwenden Sie SSH, um sich bei einem beliebigen Storage-Node anzumelden. Rufen Sie dann die LDR-Konsole auf, indem Sie „telnet 0 1402“ eingeben.
- c. Geben Sie Ein: cd /proc/STOR
- d. Geben Sie Ein: Object\_Found 'file\_path\_of\_object'

Geben Sie beispielsweise Folgendes ein:

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

Ausstellen der Object\\_Found Durch den Befehl wird das Raster des Speicherorts des Objekts benachrichtigt. Zudem werden die aktiven ILM-Richtlinien ausgelöst. Anhand dieser Richtlinien werden zusätzliche Kopien erstellt, die in jeder Richtlinie angegeben sind.



Wenn der Speicher-Node, auf dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf jeden Online-Speicher-Node kopieren. Platzieren Sie das Objekt in einem beliebigen /var/local/rangedb-Verzeichnis des Online-Storage-Node. Geben Sie dann den aus Object\\_Found Befehl mit diesem Dateipfad zum Objekt.

- Wenn das Objekt nicht wiederhergestellt werden kann, wird der 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%DkRt78I1a#3udu'
```

Fahren Sie mit dem nächsten Schritt fort.

4. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, vergewissern Sie sich, dass neue Speicherorte erstellt wurden.

- a. Geben Sie Ein: cd /proc/OBRP

- b. Geben Sie Ein: ObjectByUUID UUID\_value

Das folgende Beispiel zeigt, dass es zwei Standorte für das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 gibt.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-BCCA72DD1311

{

    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1dff7e959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
}
```

```

"CLCO\ (Locations)": \[
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID)": "12448208",
        "VOLI\ (Volume ID)": "3222345473",
        "Object File Path":
        "/var/local/rangedb/1/p/17/11/00rH0%DkRt78IlA\#3udu",
        "LTIM\ (Location timestamp)": "2020-02-12T19:36:17.880569"
    \},
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID)": "12288733",
        "VOLI\ (Volume ID)": "3222345984",
        "Object File Path":
        "/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
        "LTIM\ (Location timestamp)": "2020-02-12T19:36:17.934425"
    }
]
}

```

- a. Melden Sie sich von der LDR-Konsole ab. Geben Sie Ein: exit
5. Durchsuchen Sie von einem Admin-Node aus die Prüfprotokolle für die ORLM-Überwachungsmeldung für dieses Objekt, um zu bestätigen, dass Information Lifecycle Management (ILM) Kopien nach Bedarf platziert hat.
  - a. Melden Sie sich beim Grid-Node an:
    - i. Geben Sie den folgenden Befehl ein: ssh admin@grid\_node\_IP
    - ii. Geben Sie das im aufgeführte Passwort ein Passwords.txt Datei:
    - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: su -
    - iv. Geben Sie das im aufgeführte Passwort ein Passwords.txt Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von \$ Bis #.
  - b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden. Siehe [Teilschritt 1, b.](#)
  - c. Verwenden Sie grep, um die mit dem Objekt verknüpften Überwachungsmeldungen in eine Ausgabedatei zu extrahieren. Geben Sie Ein: grep uuid-valueaudit\_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-Audit-Meldungen (Object Rules met) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: grep ORLM output\_file\_name

Beispiel:

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

Eine ORLM-Überwachungsmeldung sieht wie in dieser 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 FELD LOKS in der Überwachungsmeldung.

Wenn vorhanden, ist der Wert von CLDI in LOCS die Node-ID, in der eine Objektkopie erstellt wurde. Diese Meldung zeigt, dass das ILM angewendet wurde und dass an zwei Standorten im Grid zwei Objektkopien erstellt wurden.

6. ["Setzt die Anzahl der verlorenen und fehlenden Objekte zurück"](#) Im Grid-Manager.

## Verlorene und fehlende Objektanzahl zurücksetzen

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

### Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".

### Über diese Aufgabe

Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

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

Diese Anleitung zeigt das Zurücksetzen des Zählers von der Seite **LDR > Data Store**.

### Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Site > Storage Node > LDR > Data Store > Konfiguration** für den Speicherknoten, der die Meldung **Objekte verloren** oder DEN VERLORENEN Alarm hat.

### 3. Wählen Sie Anzahl Der Verlorenen Objekte Zurücksetzen.

Configuration: LDR (99-94) - Data Store  
Updated: 2017-05-11 14:56:13 PDT

Reset Lost Objects Count

Apply Changes ➔

### 4. Klicken Sie Auf Änderungen Übernehmen.

Das Attribut Lost Objects wird auf 0 zurückgesetzt und die Warnung **Objects lost** und DIE VERLORENE Alarmfunktion werden gelöscht, was einige Minuten dauern kann.

### 5. Setzen Sie optional andere zugehörige Attributwerte zurück, die beim Identifizieren des verlorenen Objekts möglicherweise erhöht wurden.

- Wählen Sie **Site > Storage Node > LDR > Erasure Coding > Konfiguration** aus.
- Wählen Sie **Reset reads Failure Count** und **Reset corrupte Kopien Detected Count** aus.
- Klicken Sie Auf **Änderungen Übernehmen**.
- Wählen Sie **Site > Storage Node > LDR > Verifizierung > Konfiguration** aus.
- Wählen Sie **Anzahl der fehlenden Objekte zurücksetzen** und **Anzahl der beschädigten Objekte zurücksetzen**.
- Wenn Sie sicher sind, dass isolierte Objekte nicht benötigt werden, können Sie **gesperzte Objekte löschen** auswählen.

Isolierte Objekte werden erstellt, wenn die Hintergrundüberprüfung eine beschädigte replizierte Objektkopie identifiziert. In den meisten Fällen ersetzt StorageGRID das beschädigte Objekt automatisch, und es ist sicher, die isolierten Objekte zu löschen. Wenn jedoch die Meldung **Objects lost** oder DER VERLORENE Alarm ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen.

- Klicken Sie Auf **Änderungen Übernehmen**.

Es kann einige Momente dauern, bis die Attribute zurückgesetzt werden, nachdem Sie auf **Änderungen anwenden** klicken.

## Beheben Sie die Warnung „Niedrig Object Data Storage“

Der Alarm \* Low Object Data Storage\* überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Storage Node verfügbar ist.

### Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

- Das ist schon "Bestimmte Zugriffsberechtigungen".

## Über diese Aufgabe

Die Warnmeldung **Low Object Data Storage** wird ausgelöst, wenn die Gesamtanzahl der replizierten und Erasure-coded Objektdaten auf einem Storage Node eine der in der Warnungsregel konfigurierten Bedingungen erfüllt.

Standardmäßig wird eine wichtige Warnmeldung ausgelöst, wenn diese Bedingung als „true“ bewertet 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 replizierter und Erasure-Coded-Objektdaten für einen Storage Node.
- `storagegrid_storage_utilization_usable_space_bytes` Ist die Gesamtmenge an verbleibendem Objekt-Speicherplatz für einen Storage-Node.

Wenn ein Major oder Minor **Low Object Data Storage**-Alarm ausgelöst wird, sollten Sie so schnell wie möglich eine Erweiterung durchführen.

## Schritte

### 1. Wählen Sie **ALERTS > Current**.

Die Seite „Meldungen“ wird angezeigt.

### 2. Erweitern Sie bei Bedarf aus der Warnmeldungstabelle die Warnungsgruppe **Low Object Data Storage** und wählen Sie die Warnung aus, die angezeigt werden soll.



Wählen Sie die Meldung und nicht die Überschrift einer Gruppe von Warnungen aus.

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

- Auslösezeit
- Der Name des Standorts und des Nodes
- Die aktuellen Werte der Metriken für diese Meldung

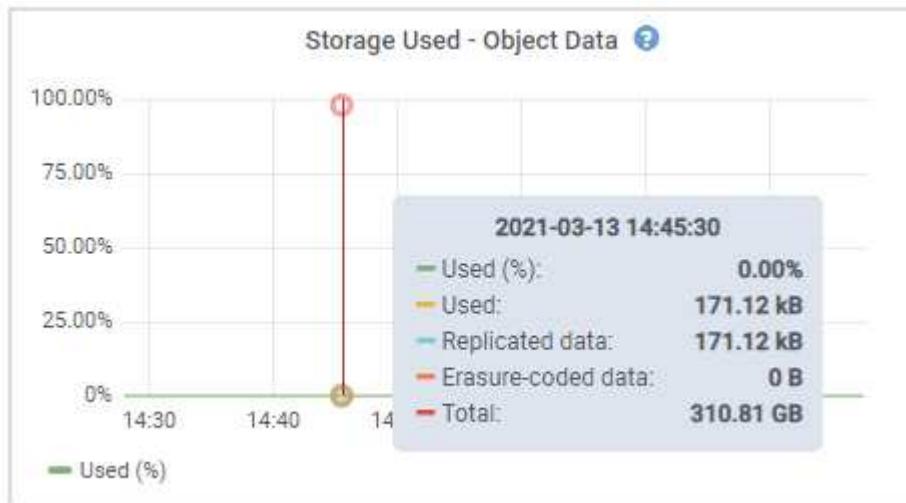
### 4. Wählen Sie **NODES > Storage Node oder Standort > Storage** aus.

### 5. Bewegen Sie den Cursor über die Grafik „verwendeter Speicher – Objektdaten“.

Die folgenden Werte werden angezeigt:

- **Used (%)**: 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, Standort oder Grid.

- **Erasure-codierte Daten:** Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt:** Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` Metrisch.



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

Mit einem Blick auf die Storage-Nutzung im Laufe der Zeit können Sie nachvollziehen, wie viel Storage vor und nach der Warnmeldung genutzt wurde, und Sie können schätzen, wie lange es dauern könnte, bis der verbleibende Speicherplatz des Node voll ist.

7. So bald wie möglich, "Ergänzen Sie die Speicherkapazität" Zu Ihrem Raster.

Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen.



Weitere Informationen finden Sie unter "["Management vollständiger Storage-Nodes"](#)".

#### **Verwandte Informationen**

["Fehlerbehebung des Storage Status \(SSTS\)-Alarms \(Legacy\)"](#)

## **Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff**

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, müssen Sie möglicherweise die Warnung **Low read-only Watermark override** auflösen. Wenn möglich, sollten Sie Ihr System aktualisieren, um mit den optimierten Werten zu beginnen.

In vorherigen Versionen, die drei "[Wasserzeichen für Storage-Volumes](#)" Wurden globale Einstellungen — dieselben Werte wurden auf jedes Storage Volume auf jedem Storage Node angewendet. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Storage Volume optimieren, basierend auf der Größe des Storage-Nodes und der relativen Kapazität des Volumes.

Wenn Sie ein Upgrade auf StorageGRID 11.6 oder höher durchführen, werden die optimierten Wasserzeichen für Lese- und Schreibzugriff automatisch auf alle Speicher-Volumes angewendet, es sei denn, eine der folgenden Aussagen trifft zu:

- Ihr System ist in der Nähe der Kapazität und kann keine neuen Daten akzeptieren, wenn optimierte Wasserzeichen angewendet wurden. StorageGRID ändert in diesem Fall keine Wasserzeichen-Einstellungen.
- Sie haben zuvor eine der Storage-Volume-Wasserzeichen auf einen benutzerdefinierten Wert gesetzt. StorageGRID überschreibt keine benutzerdefinierten Wasserzeichen-Einstellungen mit optimierten Werten. Allerdings kann StorageGRID die Warnung **Low read-only Watermark override** auslösen, wenn Ihr benutzerdefinierter Wert für das Speichervolumen Soft Read-Only Watermark zu klein ist.

## Analysieren Sie die Meldung

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, wird möglicherweise für einen oder mehrere Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

Jede Instanz des Alarms weist darauf hin, dass der benutzerdefinierte Wert des **Storage Volume Soft Read-Only Watermark** kleiner als der für diesen Speicherknoten optimierte Mindestwert ist. Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Speicherknoten möglicherweise kritisch wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergehen kann. Einige Speicher-Volumes sind möglicherweise nicht mehr zugänglich (automatisch abgehängt), wenn der Node die Kapazität erreicht.

Angenommen, Sie haben zuvor den **Speichervolumen Soft Read-Only-Wasserzeichen** auf 5 GB gesetzt. Nehmen Sie nun an, dass StorageGRID die folgenden optimierten Werte für die vier Storage-Volumes in Storage Node A berechnet hat:

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

Die Warnung **Low read-only Watermark override** wird für Storage Node A ausgelöst, da Ihr benutzerdefinierter Wasserzeichen (5 GB) kleiner als der für alle Volumes in diesem Knoten optimierte Mindestwert ist (11 GB). Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Node möglicherweise schwer mit wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergeht.

## Beheben Sie die Meldung

Befolgen Sie diese Schritte, wenn eine oder mehrere **Low Read-Only-Wasserzeichen überschreiben**-Warnungen ausgelöst wurden. Sie können diese Anweisungen auch verwenden, wenn Sie derzeit benutzerdefinierte Wasserzeichen-Einstellungen verwenden und optimierte Einstellungen auch dann verwenden möchten, wenn keine Warnungen ausgelöst wurden.

### Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "[Root-Zugriffsberechtigung](#)".

## Über diese Aufgabe

Sie können die Warnung **Low read-only Watermark override** lösen, indem Sie benutzerdefinierte Wasserzeichen-Einstellungen auf die neuen Wasserzeichen-Überschreibungen aktualisieren. Wenn jedoch ein oder mehrere Speicherknoten nahe voll sind oder Sie spezielle ILM-Anforderungen haben, sollten Sie zunächst die optimierten Speicherabdrücke anzeigen und feststellen, ob sie sicher verwendet werden können.

## Bewertung der Nutzung von Objektdaten für das gesamte Grid

### Schritte

1. Wählen Sie **KNOTEN**.
2. Erweitern Sie für jeden Standort im Raster die Liste der Nodes.
3. Überprüfen Sie die Prozentwerte, die in der Spalte **Objektdaten verwendet** für jeden Speicherknoten an jedem Standort angezeigt werden.
4. Befolgen Sie den entsprechenden Schritt:
  - a. Wenn keiner der Speicherknoten fast voll ist (zum Beispiel sind alle **Objektdaten verwendet** Werte kleiner als 80%), können Sie die Überschreibeinstellungen verwenden. Gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#).
  - b. Wenn ILM-Regeln ein striktes Aufnahmeverhalten verwenden oder bestimmte Storage-Pools nahezu voll sind, führen Sie die Schritte unter durch [Anzeigen optimierter Speicherabdrücke](#) Und [Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können](#).

### Anzeigen optimierter Storage-Wasserzeichen

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.

### Schritte

1. Wählen Sie **SUPPORT > Tools > Metriken**.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. 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 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.

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

#### Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können

##### Schritte

1. Wählen Sie **KNOTEN**.
2. Wiederholen Sie diese Schritte für jeden Online-Speicherknoten:
  - a. Wählen Sie **Storage-Node > Storage Aus**.
  - b. Scrollen Sie nach unten zur Tabelle „Objektspeichern“.
  - c. Vergleichen Sie den **verfügbar**-Wert für jeden Objektspeicher (Volumen) mit dem für diesen Speicherknoten angegebenen maximalen optimierten Wasserzeichen.
3. Wenn mindestens ein Volume auf jedem Online-Speicherknoten mehr Speicherplatz als das maximal optimierte Wasserzeichen für diesen Knoten hat, gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#). Um die optimierten Wasserzeichen zu verwenden.

Andernfalls erweitern Sie das Raster so schnell wie möglich. Entweder "[Storage-Volumes hinzufügen](#)" Zu einem vorhandenen Node oder "[Neue Storage-Nodes hinzufügen](#)". Fahren Sie dann mit fort [Verwenden Sie optimierte Wasserzeichen](#) Zum Aktualisieren der Einstellungen für Wasserzeichen.

4. Wenn Sie mit der Verwendung benutzerdefinierter Werte für die Speichervolumen-Wasserzeichen fortfahren müssen, "[Stille](#)" Oder "[Deaktivieren](#)" Die Warnung \* Low read-only Watermark override\*.



Auf jedes Storage Volume auf jedem Storage Node werden dieselben benutzerdefinierten Werte angewendet. Die Verwendung kleinerer Werte als empfohlen für Speichervolumen-Wasserzeichen kann dazu führen, dass einige Speicher-Volumes nicht mehr zugänglich sind (automatisch abhängig), wenn der Node die Kapazität erreicht.

#### optimierte Wasserzeichen verwenden

##### Schritte

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

Für jedes Storage Volume gelten nun optimierte Wasserzeichen, basierend auf der Größe des Storage Nodes und der relativen Kapazität des Volumes.

## Fehlersuche im SSTS-Alarm (Storage Status) durchführen

Der SSTS-Alarm (Storage Status) wird ausgelöst, wenn ein Speicherknoten über nicht genügend freien Speicherplatz für den Objektspeicher verfügt.

##### Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "[Unterstützter Webbrowser](#)".
- Das ist schon "[Bestimmte Zugriffsberechtigungen](#)".

## Über diese Aufgabe

Der SSTS-Alarm (Speicherstatus) wird auf Notice-Ebene ausgelöst, wenn die Menge an freiem Speicherplatz auf jedem Volume in einem Speicherknoten unter den Wert des Speichervolumen-Soft-Read-Only-Wasserzeichens (**KONFIGURATION > System > Speicheroptionen**) fällt.



## Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

Angenommen, das Speichervolumen-Soft-Read-Only-Wasserzeichen ist auf 10 GB gesetzt, das ist der Standardwert. Der SSTS-Alarm wird ausgelöst, wenn auf jedem Speicher-Volume im Storage-Node weniger als 10 GB nutzbarer Speicherplatz verbleibt. Wenn eines der Volumes über 10 GB oder mehr verfügbaren Speicherplatz verfügt, wird der Alarm nicht ausgelöst.

Wenn ein SSTS-Alarm ausgelöst wurde, können Sie diese Schritte ausführen, um das Problem besser zu verstehen.

### Schritte

1. Wählen Sie **SUPPORT > Alarne (alt) > Aktueller Alarm** aus.
2. Wählen Sie in der Spalte Service das Rechenzentrum, den Node und den Service aus, die dem SSTS-Alarm zugeordnet sind.

Die Seite Grid Topology wird angezeigt. Auf der Registerkarte „Alarne“ werden die aktiven Alarne für den ausgewählten Knoten und Dienst angezeigt.



## Alarms: LDR (DC1-S3-101-195) - Storage

Updated: 2019-10-09 12:52:43 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
<span style="color: yellow;">!</span> Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
<span style="color: yellow;">!</span> Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
<span style="color: green;">✓</span> Normal	SHLH (Health)						<input checked="" type="checkbox"/>

Apply Changes

In diesem Beispiel wurden sowohl die SSTS-Alarme (Speicherstatus) als auch die SAVP (Total Usable Space (Prozent)) auf der Notice-Ebene ausgelöst.



Typischerweise werden sowohl der SSTS-Alarm als auch der SAVP-Alarm etwa gleichzeitig ausgelöst. Ob jedoch beide Alarme ausgelöst werden, hängt von der Wasserzeichen-Einstellung in GB und der SAVP-Alarmeinstellung in Prozent ab.

- Um festzustellen, wie viel nutzbarer Speicherplatz tatsächlich verfügbar ist, wählen Sie **LDR > Storage > Übersicht** und suchen Sie das Attribut Total Usable Space (STAS).



## Overview: LDR (DC1-S1-101-193) - Storage

Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:	Online	
Storage State - Current:	Read-only	
Storage Status:	Insufficient Free Space	

### Utilization

Total Space:	164 GB	
Total Usable Space:	19.6 GB	
Total Usable Space (Percent):	11.937 %	
Total Data:	139 GB	
Total Data (Percent):	84.567 %	

### Replication

Block Reads:	0	
Block Writes:	2,279,881	
Objects Retrieved:	0	
Objects Committed:	88,882	
Objects Deleted:	16	
Delete Service State:	Enabled	

### Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	54.7 GB	2.93 GB	46.2 GB	0 B	84.486 %	No Errors
0001	54.7 GB	8.32 GB	46.3 GB	0 B	84.644 %	No Errors
0002	54.7 GB	8.36 GB	46.3 GB	0 B	84.57 %	No Errors

In diesem Beispiel bleiben nur 19.6 GB des 164 GB Speicherplatzes auf diesem Speicherknoten verfügbar. Beachten Sie, dass der Gesamtwert die Summe der **verfügbar**-Werte für die drei Objektspeicher-Volumes ist. Der SSTS-Alarm wurde ausgelöst, weil jedes der drei Speicher-Volumes weniger als 10 GB verfügbaren Speicherplatz hatte.

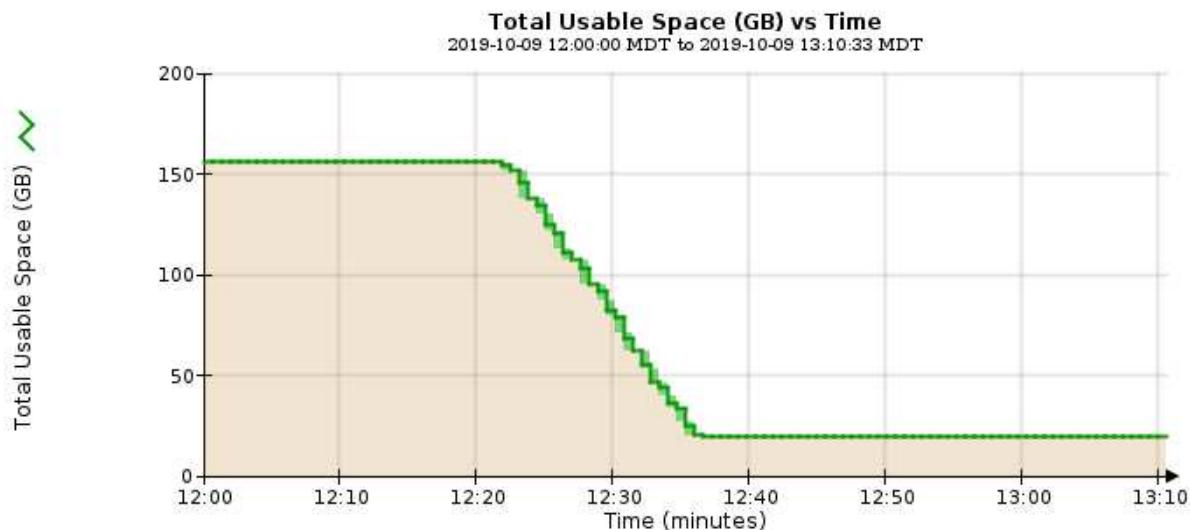
- Um zu verstehen, wie Speicher im Laufe der Zeit genutzt wurde, wählen Sie die Registerkarte **Berichte** und zeichnen den gesamten nutzbaren Speicherplatz in den letzten Stunden.

In diesem Beispiel sank der gesamte nutzbare Speicherplatz von etwa 155 GB bei 12:00 auf 20 GB bei 12:35, was der Zeit entspricht, zu der der SSTS-Alarm ausgelöst wurde.



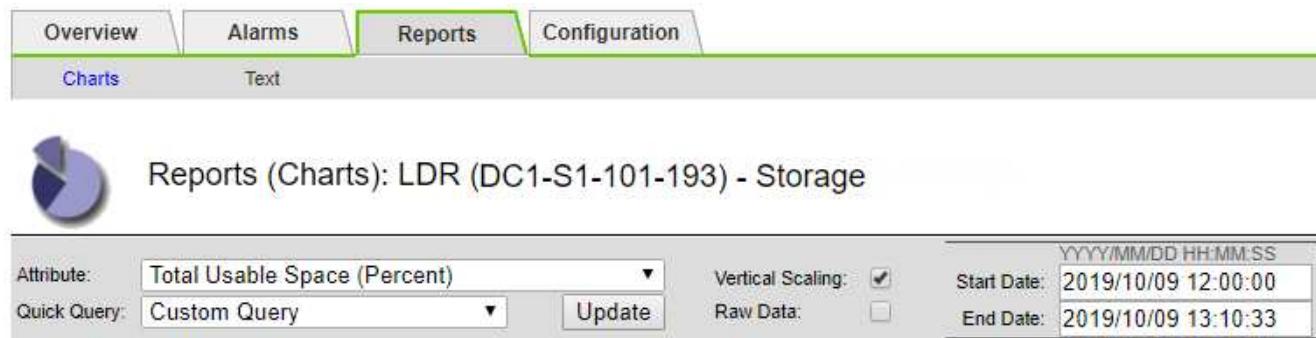
## Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	YYYY/MM/DD HH:MM:SS 2019/10/09 12:00:00
Quick Query:	Custom Query	Update	<input type="checkbox"/>	Raw Data:	End Date: 2019/10/09 13:10:33



5. Um zu verstehen, wie Speicher als Prozentsatz der Gesamtmenge genutzt wird, geben Sie den gesamten nutzbaren Speicherplatz (Prozent) in den letzten Stunden an.

In diesem Beispiel sank der nutzbare Gesamtspeicherplatz von 95 % auf etwa 10 % zur selben Zeit.



#### 6. Nach Bedarf "Ergänzen Sie die Speicherkapazität".

Siehe auch "[Management vollständiger Storage-Nodes](#)".

## Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm)

Der SMTT-Alarm (Total Events) wird im Grid Manager ausgelöst, wenn eine Plattformdienstmeldung an ein Ziel gesendet wird, das die Daten nicht akzeptieren kann.

### Über diese Aufgabe

Beispielsweise kann ein mehrteiliger S3-Upload erfolgreich sein, auch wenn die zugehörige Replizierungs- oder Benachrichtigung nicht an den konfigurierten Endpunkt geliefert werden kann. Alternativ kann eine Nachricht für die CloudMirror Replizierung nicht bereitgestellt werden, wenn die Metadaten zu lang sind.

Der SMTT-Alarm enthält eine Meldung „Letztes Ereignis“, die lautet: Failed to publish notifications for *bucket-name object key* Für das letzte Objekt, dessen Benachrichtigung fehlgeschlagen ist.

Ereignismeldungen sind auch in aufgeführt /var/local/log/bycast-err.log Protokolldatei. Siehe "[Referenz für Protokolldateien](#)".

Weitere Informationen finden Sie im "[Fehlerbehebung bei Plattform-Services](#)". Möglicherweise müssen Sie es "[Greifen Sie über den Tenant Manager auf den Mandanten zu](#)" So beheben Sie einen Plattformdienstfehler.

## Schritte

1. Um den Alarm anzuzeigen, wählen Sie **NODES > site > Grid Node > Events** aus.
2. Letztes Ereignis oben in der Tabelle anzeigen.  
Ereignismeldungen sind auch in aufgeführt /var/local/log/bycast-err.log.
3. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
4. Wählen Sie **Anzahl der Ereignisse zurücksetzen**.
5. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.
6. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts auszulösen.

## **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 VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERINER 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.