



Fehlerbehebung bei Objekt- und Storage-Problemen

StorageGRID

NetApp
October 03, 2025

Inhalt

Fehlerbehebung bei Objekt- und Storage-Problemen	1
Bestätigen der Speicherorte von Objektdaten	1
Fehler beim Objektspeicher (Storage Volume)	3
Überprüfen der Objektintegrität	4
Was ist Hintergrundüberprüfung	4
Ändern der Hintergrundverifizierungsrate	5
Was ist die Vordergrundüberprüfung	8
Vordergrundüberprüfung wird ausgeführt	8
Fehlerbehebung verloren gegangene und fehlende Objektdaten	11
Untersuchung verlorener Objekte	12
Suche nach und Wiederherstellung möglicherweise verlorenen Objekten	17
Zurücksetzen verlorener und fehlender Objektanzahl	23
Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“	25
Fehlerbehebung beim SSTS-Alarm (Storage Status)	27
Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm)	31

Fehlerbehebung bei Objekt- und Storage-Problemen

Sie können verschiedene Aufgaben ausführen, um die Ursachen von Objekt- und Storage-Problemen zu ermitteln.

Bestätigen der Speicherorte von Objektdaten

Je nach Problem sollten Sie überprüfen, wo Objektdaten gespeichert werden. Beispielsweise möchten Sie überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und Objektdaten dort gespeichert werden, wo sie geplant sind.

Was Sie benötigen

- 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 allen Großbuchstaben ein.
 - **S3-Bucket und Objektschlüssel:** Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
 - **Swift Container und Objektname:** Wenn ein Objekt über die Swift-Schnittstelle aufgenommen wird, verwendet die Client-Anwendung eine Container- und Objektname-Kombination, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Wählen Sie **ILM > Objekt Metadaten Lookup** aus.
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.

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

source/testobject

Look Up

3. Klicken Sie Auf **Look Up**.

Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

- Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname 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-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIS": "2",
```

Verwandte Informationen

"Objektmanagement mit ILM"

"S3 verwenden"






"Verwenden Sie Swift"










Fehler beim Objektspeicher (Storage Volume)

Der zugrunde liegende Storage auf einem Storage-Node ist in Objektspeicher unterteilt. Diese Objektspeicher sind physische Partitionen, die als Bereitstellungspunkte für den Storage des StorageGRID Systems fungieren. 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		
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s		
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s		
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s		
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s		
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s		

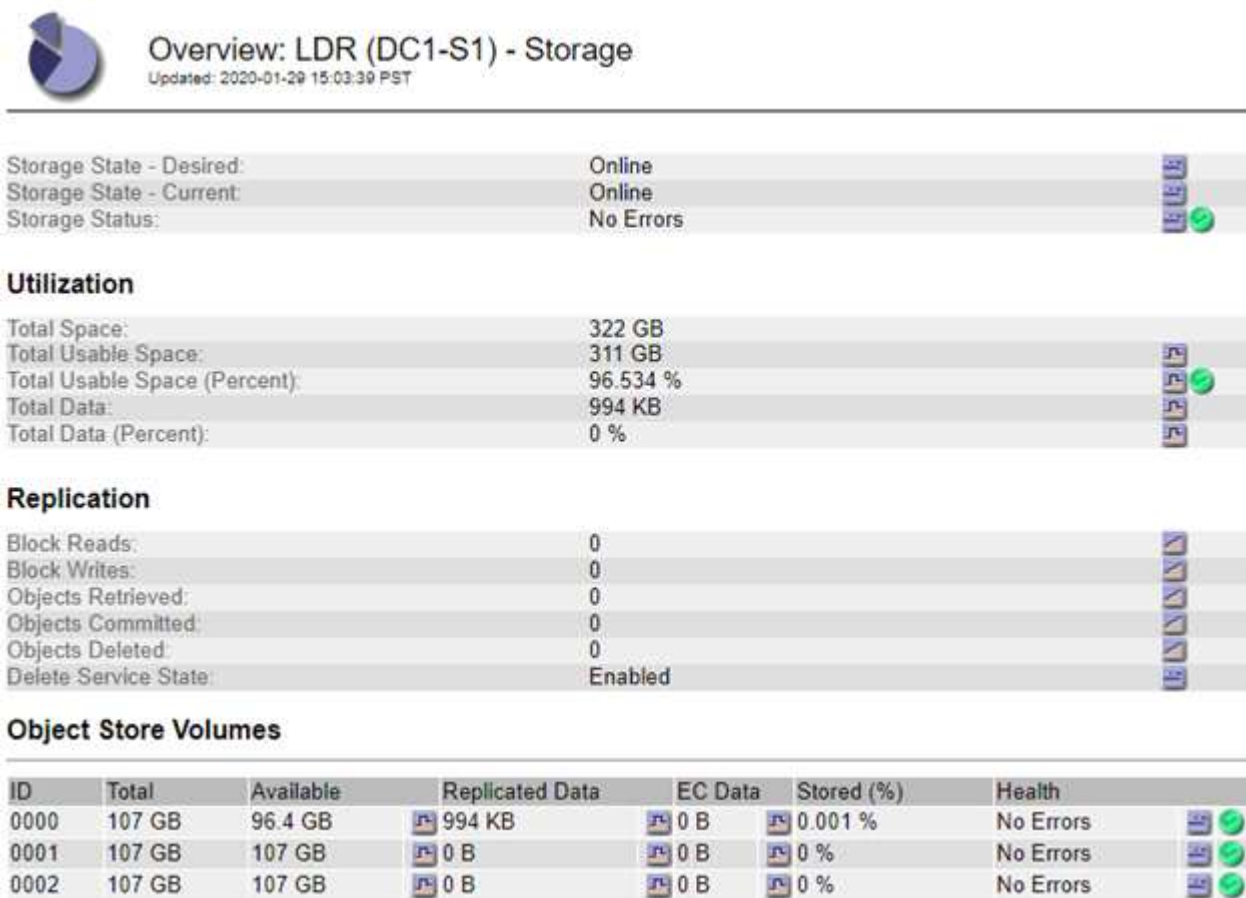
Volumes						
Mount Point	Device	Status	Size	Available	Write Cache Status	
/	croot	Online	21.00 GB	14.25 GB		Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB		Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB		Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB		Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB		Enabled

Object Stores						
ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB 	994.37 KB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Führen Sie die folgenden Schritte aus, um weitere Details zu jedem Storage-Node anzuzeigen:

1. Wählen Sie **Support > Tools > Grid Topology** Aus.

2. Wählen Sie **site** > **Storage Node** > **LDR** > **Storage** > **Übersicht** > **Haupt**.



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 Speicherknoten so bald wie möglich wieder voll zu machen. Wenn nötig, können Sie auf die Registerkarte **Konfiguration** gehen und den Speicherknoten in einen Read-only Zustand setzen, so dass das StorageGRID System ihn für den Datenabruf verwenden kann, während Sie sich auf eine vollständige Wiederherstellung des Servers vorbereiten.

Verwandte Informationen

["Verwalten Sie erholen"](#)

Überprüfen der Objektintegrität

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

Es gibt zwei Verifizierungsverfahren: Hintergrund- und Vordergrundüberprüfung. Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung wird automatisch ausgeführt und überprüft kontinuierlich die Korrektheit von Objektdaten. Die Vordergrundüberprüfung kann von einem Benutzer ausgelöst werden, um die Existenz (obwohl nicht die Korrektheit) 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 erstellt und gemäß der aktiven ILM-Richtlinie platziert. 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 isolierte 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 wiederhergestellt werden kann, wird das Attribut „Corrupt Copies detected (ECOR)“ um eins erhöht und es 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. 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 Alarmer (alt) im Zusammenhang mit der Hintergrundüberprüfung

Wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann (weil die Beschädigung verhindert, dass das Objekt identifiziert wird), wird die Warnung **Unerkannter beschädigter Gegenstand erkannt** ausgelöst.

Wenn die Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, da es keine andere Kopie finden kann, werden die Meldung **Objekte verloren** und der ältere Alarm VERLOREN GEGANGENE (verlorene Objekte) ausgelöst.

Ändern der Hintergrundverifizierungsrate

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 Topology** 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.

Overview Alarms Reports Configuration

Main Alarms

Configuration: LDR (DC2-S1-106-147) - Verification
Updated: 2019-04-24 16:13:44 PDT

Reset Missing Objects Count ☐

Foreground Verification

ID	Verify
0	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>

Background Verification

Verification Rate Adaptive ▼

Reset Corrupt Objects Count ☐

Quarantined Objects

Delete Quarantined Objects ☐

Apply Changes



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

1. Klicken Sie Auf **Änderungen Übernehmen**.
2. Überwachen der Ergebnisse der Hintergrundüberprüfung replizierter Objekte

- a. Gehen 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 aktive ILM-Richtlinie erfüllt.
- Wenn die Objektkennung nicht extrahiert werden kann (weil sie beschädigt wurde), wird die Metrik **korrupte Objekte nicht identifiziert** erhöht und die Warnung **nicht identifiziertes korruptes Objekt erkannt** ausgelöst.

- c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Ursache der Beschädigung zu ermitteln.
3. 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 Topology** 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).
4. Nachdem das StorageGRID System beschädigte Objekte automatisch wiederhergestellt hat, setzen Sie die Anzahl beschädigter Objekte zurück.
 - a. Wählen Sie **Support > Tools > Grid Topology** Aus.
 - b. Wählen Sie **Storage Node > LDR > Verifizierung > Konfiguration** aus.
 - c. Wählen Sie **Anzahl Der Beschädigten Objekte Zurücksetzen**.
 - d. Klicken Sie Auf **Änderungen Übernehmen**.
 5. 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.

1. Wählen Sie **Support > Tools > Grid Topology** Aus.
2. Wählen Sie **Storage Node > LDR > Verifizierung > Konfiguration**.
3. Wählen Sie **Gesperrte Objekte Löschen**.
4. Klicken Sie Auf **Änderungen Übernehmen**.

Was ist die Vordergrundüberprüfung

Vordergrundüberprüfung ist ein vom Benutzer initiiertes Prozess, der überprüft, ob alle erwarteten Objektdaten auf einem Storage-Node vorhanden sind. Vordergrundüberprüfung wird verwendet, um die Integrität eines Speichergeräts zu überprüfen.

Die Vordergrundüberprüfung ist eine schnellere Alternative zur Hintergrundüberprüfung, die die Existenz von Objektdaten auf einem Storage-Node, jedoch nicht die Integrität überprüft. Wenn bei der Überprüfung im Vordergrund festgestellt wird, dass viele Elemente fehlen, kann es zu Problemen mit dem gesamten oder einem Teil eines Speichergeräts, das mit dem Speicherknoten verknüpft ist, kommen.

Bei der Vordergrundüberprüfung werden sowohl replizierte Objektdaten als auch mit Erasure-Coding-Objektdaten überprüft:

- **Replizierte Objekte:** Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, die Kopie von an anderer Stelle im System gespeicherten Kopien zu ersetzen. Der Storage Node führt eine vorhandene Kopie durch eine ILM-Bewertung aus. Damit wird ermittelt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da die fehlende Kopie nicht mehr am erwarteten Standort vorhanden ist. Eine neue Kopie wird erstellt und platziert, um die aktive ILM-Richtlinie des Systems zu erfüllen. Diese neue Kopie kann nicht an demselben Speicherort abgelegt werden, an dem die fehlende Kopie gespeichert wurde.
- **Erasure-codierte Objekte:** Wenn ein Fragment eines Löschungskodierten Objekts gefunden wird, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Fragmente neu zu erstellen. Wenn das fehlende Fragment nicht wieder aufgebaut werden kann (weil zu viele Fragmente verloren sind), wird das Attribut Corrupt Copies detected (ECOR) um eins erhöht. ILM versucht anschließend, eine andere Kopie des Objekts zu finden, mit der das Unternehmen eine neue Kopie mit Verfahren zur Fehlerkorrektur erstellen kann.

Wenn bei der Vordergrundüberprüfung ein Problem mit dem Erasure Coding für ein Storage-Volume erkannt wird, wird bei der Vordergrundverifizierung eine Fehlermeldung angehalten, die das betroffene Volume identifiziert. Sie müssen ein Recovery-Verfahren für alle betroffenen Storage Volumes durchführen.

Wenn im Raster keine weiteren Kopien eines fehlenden replizierten Objekts oder eines beschädigten Erasure-codierten Objekts gefunden werden, werden die Meldung **Objekte verloren** und der Legacy-Alarm FÜR VERLORENE (verlorene Objekte) ausgelöst.

Vordergrundüberprüfung wird ausgeführt

Mit der Vordergrundüberprüfung können Sie die Existenz von Daten auf einem Speicherknoten überprüfen. Fehlende Objektdaten können darauf hindeuten, dass beim zugrunde liegenden Speichergerät ein Problem vorliegt.

Was Sie benötigen

- Sie haben sichergestellt, dass die folgenden Grid-Aufgaben nicht ausgeführt werden:
 - Grid Expansion: Add Server (GEXP), wenn ein Storage Node hinzugefügt wird
 - Storage Node Deaktivierungsfunktion (LDCM) auf demselben Storage-Node Wenn diese Grid-Aufgaben ausgeführt werden, warten Sie, bis sie abgeschlossen sind oder lassen Sie die Sperre frei.
- Sie haben sichergestellt, dass die Speicherung online ist. (Wählen Sie **Support > Tools > Grid Topology**. Wählen Sie dann **Storage Node > LDR > Storage > Übersicht > Haupt** aus. Vergewissern Sie sich, dass **Speicherstatus - Aktuell** online ist.)
- Sie haben sichergestellt, dass die folgenden Wiederherstellungsverfahren nicht auf demselben Speicherknoten ausgeführt werden:

- Recovery eines ausgefallenen Storage-Volumes
- Die Recovery eines Storage-Knotens mit einer fehlgeschlagenen Systemlaufwerk-Vordergrundüberprüfung bietet keine nützlichen Informationen, während Recovery-Verfahren ausgeführt werden.

Über diese Aufgabe

Vordergrundüberprüfung werden sowohl fehlende replizierte Objektdaten als auch fehlende, mit Erasure Coding versehenen Objektdaten überprüft:

- Wenn bei der Überprüfung im Vordergrund große Mengen fehlender Objektdaten festgestellt werden, liegt es wahrscheinlich vor, dass der Storage-Node analysiert und behoben werden muss.
- Wenn bei der Überprüfung im Vordergrund ein schwerwiegender Storage-Fehler bei der Datenlöschung festgestellt wird, werden Sie darüber informiert. Sie müssen die Wiederherstellung des Speichervolumens durchführen, um den Fehler zu beheben.

Sie können die Vordergrundüberprüfung so konfigurieren, dass alle Objektspeicher eines Storage Node oder nur bestimmte Objektspeichern überprüft werden.

Wenn die Vordergrundüberprüfung fehlende Objektdaten findet, versucht das StorageGRID-System, sie zu ersetzen. Wenn keine Ersatzkopie erstellt werden kann, kann der Alarm „VERLORENE Objekte“ ausgelöst werden.

Die Vordergrundüberprüfung generiert eine LDR-Vordergrundverifizierung, die je nach Anzahl der auf einem Storage-Node gespeicherten Objekte Tage- oder wochenlang dauern kann. Es ist möglich, mehrere Storage-Nodes gleichzeitig auszuwählen. Diese Grid-Aufgaben werden jedoch nicht gleichzeitig ausgeführt. Stattdessen werden sie in eine Warteschlange gestellt und bis zum Abschluss nacheinander ausgeführt. Wenn die Vordergrundüberprüfung auf einem Storage-Node ausgeführt wird, können Sie auf diesem Storage-Node keine andere Überprüfungsaufgabe im Vordergrund starten, obwohl die Option zum Überprüfen zusätzlicher Volumes für den Storage-Node möglicherweise verfügbar ist.

Wenn ein anderer Storage-Node als der, auf dem die Vordergrundüberprüfung ausgeführt wird, offline geschaltet wird, wird die Grid-Aufgabe weiter ausgeführt, bis das Attribut **% complete** 99.99 Prozent erreicht. Das Attribut **% complete** wird dann auf 50 Prozent zurückgestellt und wartet, bis der Speicherknoten wieder in den Online-Status zurückkehrt. Wenn der Status des Speicherknotens wieder online geschaltet wird, wird die Grid-Aufgabe für die Überprüfung des LDR-Vordergrunds fortgesetzt, bis sie abgeschlossen ist.

Schritte

1. Wählen Sie **Storage Node > LDR > Verifizierung** aus.
2. Wählen Sie **Konfiguration > Main**.
3. Aktivieren Sie unter **Vordergrundüberprüfung** das Kontrollkästchen für jede Speicher-Volume-ID, die Sie überprüfen möchten.

Overview


Alarms

Reports

Configuration

Main

Alarms



Configuration: LDR (dc1-cs1-99-82) - Verification

Updated: 2015-08-19 14:07:04 PDT

Reset Missing Objects Count ☐

Foreground Verification


ID	Verify
0	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>

Background Verification

Verification Rate

Adaptive

Reset Corrupt Objects Count ☐

Apply Changes 

4. Klicken Sie Auf **Änderungen Übernehmen**.

Warten Sie, bis die Seite automatisch aktualisiert und neu geladen wird, bevor Sie die Seite verlassen. Sobald die Aktualisierung abgeschlossen ist, stehen Objektspeicher zur Auswahl auf diesem Speicherknoten nicht mehr zur Verfügung.

Eine LDR-Vordergrundüberprüfungsraster-Aufgabe wird erstellt und ausgeführt, bis sie abgeschlossen, unterbrochen oder abgebrochen wird.

5. Fehlende Objekte oder fehlende Fragmente überwachen:

- Wählen Sie **Storage Node > LDR > Verifizierung** aus.
- Notieren Sie auf der Registerkarte Übersicht unter **Ergebnisse der Überprüfung** den Wert von **fehlenden Objekten erkannt**.

Hinweis: Der gleiche Wert wird auf der Seite Knoten als **Lost Objects** angegeben. Gehen Sie zu **Nodes > Storage Node** und wählen Sie die Registerkarte **Objects** aus.

Wenn die Anzahl der **fehlenden Objekte erkannt** groß ist (wenn Hunderte von fehlenden Objekten vorhanden sind), liegt wahrscheinlich ein Problem mit dem Speicher des Speicherknoten vor. Wenden Sie sich an den technischen Support.

- Wählen Sie **Storage Node > LDR > Erasure Coding** aus.
- Notieren Sie auf der Registerkarte Übersicht unter **Ergebnisse der Überprüfung** den Wert von **fehlenden Fragmenten erkannt**.

Wenn die Anzahl **fehlendes Fragment** groß ist (wenn hunderte von fehlenden Fragmenten vorhanden

sind), liegt wahrscheinlich ein Problem mit dem Speicher des Speicherknoten vor. Wenden Sie sich an den technischen Support.

Wenn die Vordergrundüberprüfung keine beträchtliche Anzahl an fehlenden replizierten Objektkopien oder eine beträchtliche Anzahl an fehlenden Fragmenten erkennt, funktioniert der Speicher normal.

6. Überwachen Sie den Abschluss der Vordergrundüberprüfungsraster-Aufgabe:

- a. Wählen Sie **Support > Tools > Grid Topology** Aus. Wählen Sie dann **site > Admin Node > CMN > Grid Task > Übersicht > Main**.
- b. Stellen Sie sicher, dass das Raster für die Vordergrundverifizierung fehlerfrei fortschreitet.

Hinweis: Bei Unterbrechung des Vordergrundverifizierungsgitters wird ein Alarm auf Notice-Ebene am Grid Task Status (SCAS) ausgelöst.

- c. Wenn die Rasteraufgabe mit einem angehalten wird `critical storage error`, Das betroffene Volumen wiederherstellen und dann die Vordergrundüberprüfung auf den verbleibenden Volumes ausführen, um auf zusätzliche Fehler zu überprüfen.

Achtung: Wenn die Aufgabe Vordergrundverifizierung mit der Meldung unterbricht `Encountered a critical storage error in volume volID`, Sie müssen das Verfahren für die Wiederherstellung eines fehlerhaften Speichervolume. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **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.

Verwandte Informationen

["Verwalten Sie erhalten"](#)

Fehlerbehebung verloren gegangene und fehlende Objektdaten

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 werden die Warnung **Objekte verloren** und der Alarm für verlorene Objekte (verlorene Objekte) ausgelöst, wie folgt:

- Wenn bei replizierten Kopien eine andere Kopie nicht abgerufen werden kann, gilt das Objekt als verloren,

und die Warnung und der Alarm werden ausgelöst.

- Wenn beim Löschen codierter 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 weitere Kopie gefunden wird, werden die Warnung und der Alarm 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.

Wenn Objekt-Daten ohne Kopien verloren gehen, gibt es keine Recovery-Lösung. Sie müssen jedoch den Zähler „Lost Object“ zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren.

Verwandte Informationen

["Untersuchung verlorener Objekte"](#)

["Zurücksetzen verlorener und fehlender Objektanzahl"](#)

Untersuchung verlorener Objekte

Wenn der Alarm * Objects lost* und der Alarm Legacy LOST Objects (Lost Objects) ausgelöst werden, müssen Sie sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Die Warnung **Objekte verloren** und der VERLORENE Alarm zeigen an, dass StorageGRID der Ansicht ist, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

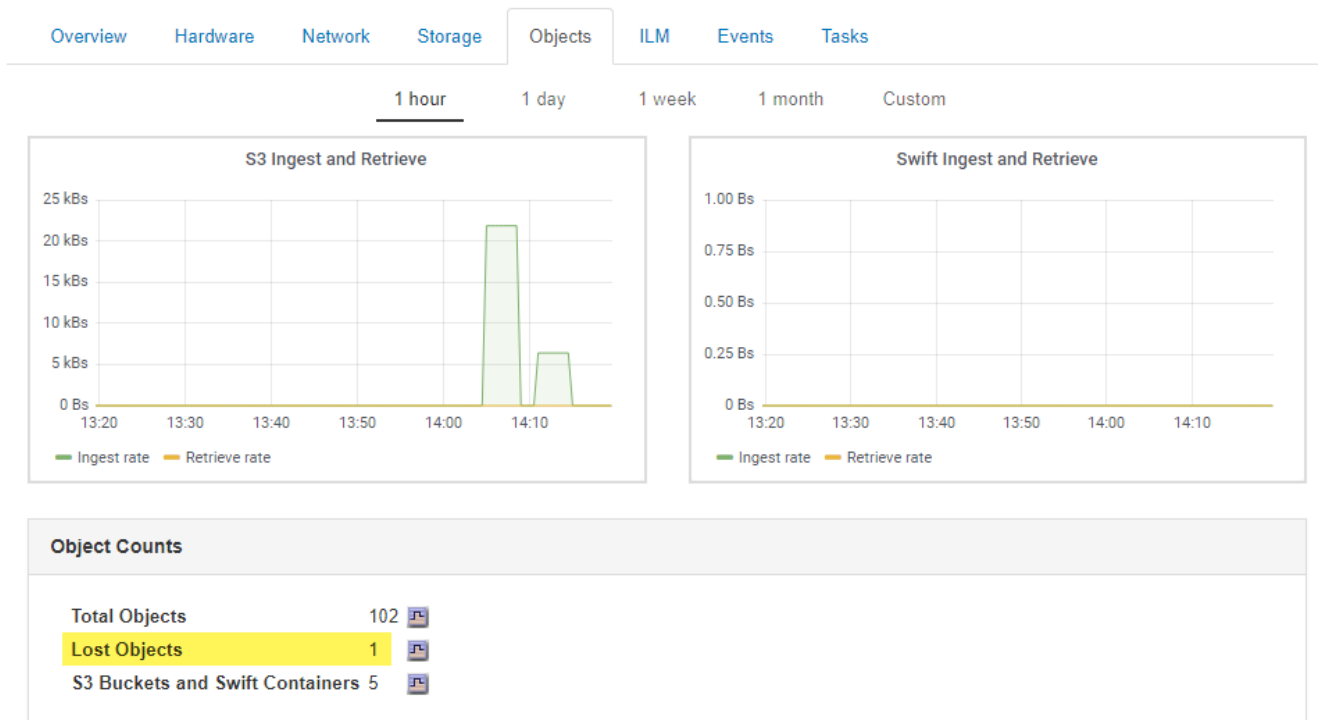
Untersuchen Sie verlorene Objektalarme oder -Warnmeldungen sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. In einigen Fällen können Sie ein verlorenes Objekt wiederherstellen, wenn Sie eine sofortige Aktion ausführen.

Die Anzahl der verlorenen Objekte kann im Grid Manager angezeigt werden.

Schritte

1. Wählen Sie **Knoten**.
2. Wählen Sie **Speicherknoten > Objekte** Aus.
3. Überprüfen Sie die Anzahl der in der Tabelle Objektanzahl angezeigten verlorenen Objekte.

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. Greifen Sie von einem Admin-Node aus auf das Audit-Protokoll zu, um die eindeutige Kennung (UUID) des Objekts zu bestimmen, das die Meldung **Objekte verloren** und DEN VERLORENEN Alarm 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. Geben Sie Ein: `cd /var/local/audit/export/`
 - 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] [AMID(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. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole.
- 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"
    },
    "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"
  }
]
}

```

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, kann der Alarm sicher ignoriert werden. Das Fehlen eines Objekts bedeutet, dass das Objekt absichtlich gelöscht wurde.</p>
Standorte 0	<p>Wenn im Ausgang Positionen aufgeführt sind, kann der Alarm Lost Objects 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>(Das Verfahren zum Auffinden potenziell verlorener Objekte erläutert, wie Sie die Node-ID verwenden, um den richtigen Storage-Node zu finden.)</p> <p>"Suche nach und Wiederherstellung möglicherweise verlorenen Objekten"</p> <p>Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um den Alarm und die Warnung zu löschen.</p>
Standorte = 0	<p>Wenn in der Ausgabe keine Positionen aufgeführt sind, fehlt das Objekt möglicherweise. Sie können versuchen, das Objekt selbst zu finden und wiederherzustellen, oder Sie können sich an den technischen Support wenden.</p> <p>"Suche nach und Wiederherstellung möglicherweise verlorenen Objekten"</p> <p>Vom technischen Support bitten Sie möglicherweise, zu bestimmen, ob ein Verfahren zur Storage-Recovery durchgeführt wird. Das heißt, wurde auf jedem Storage Node ein Befehl „<i>Repair-Data</i>“ ausgegeben, und läuft die Recovery noch? Weitere Informationen zum Wiederherstellen von Objektdaten auf einem Storage-Volume finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.</p>

Verwandte Informationen

["Verwalten Sie erholen"](#)

["Prüfung von Audit-Protokollen"](#)

Suche nach und Wiederherstellung möglicherweise verlorenen Objekten

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 „potentiell verloren“ identifiziert haben.

Was Sie benötigen

- Sie müssen über die UUID eines verlorenen Objekts verfügen, wie in „Untersuchung verlorener Objekte“ angegeben.
- Sie müssen 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 Audit-Protokolle befinden: `cd /var/local/audit/export/`
 - c. Verwenden Sie `grep`, um die mit dem potenziell verlorenen Objekt verknüpften Audit-Nachrichten zu extrahieren und sie an eine Ausgabedatei zu senden. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
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 messages_about_lost_objects.txt
```

Eine LLST-Überwachungsmeldung sieht wie diese 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):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

- 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.

- f. Suchen Sie den Speicherknoten für diese LDR-Knoten-ID.

Es gibt zwei Möglichkeiten, die Node-ID zum Suchen des Storage Node zu verwenden:

- Wählen Sie im Grid Manager die Option **Support > Tools > Grid Topology** aus. Wählen Sie dann **Data Center > Storage Node > LDR** aus. Die LDR-Knoten-ID befindet sich in der Node-Informationstabelle. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie den gefunden haben, der dieses LDR hostet.
- Laden Sie das Wiederherstellungspaket für das Grid herunter und entpacken Sie es. Das PAKET enthält ein Verzeichnis `ldocs`. Wenn Sie die Datei `index.html` öffnen, zeigt die Serverübersicht alle Knoten-IDs für alle Grid-Knoten an.

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'
```

Hinweis: Fügen Sie den Objektpfad immer in einzelne Anführungszeichen, um Sonderzeichen zu entkommen.

- Wenn der Objektpfad nicht gefunden wurde, geht 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 Schritt fort [Stellen Sie das Objekt in StorageGRID wieder her](#). Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.

1. 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:bycast 'file_path_of_object'`
 - b. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole. Geben Sie Ein: `telnet 0 1402`
 - 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 wird die aktive ILM-Richtlinie ausgelöst, die zusätzliche Kopien gemäß den Angaben in der Richtlinie erstellt.

Hinweis: Wenn der Speicherknoten, in dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf einen beliebigen Speicherknoten kopieren, der online ist. 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 das angezeigt `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'
```

Mit Schritt fortfahren [Überprüfen Sie, ob neue Standorte erstellt wurden](#)

1. 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`
2. 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: `cd /var/local/audit/export/`

- 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 >
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 messages_about_restored_object.txt
```

Eine ORLM-Überwachungsmeldung sieht wie diese Beispielmeldung 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 und die Volume-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.

b. Setzen Sie die Anzahl der verlorenen Objekte im Grid Manager zurück.

Verwandte Informationen

["Untersuchung verlorener Objekte"](#)

["Bestätigen der Speicherorte von Objektdaten"](#)

["Zurücksetzen verlorener und fehlender Objektanzahl"](#)

["Prüfung von Audit-Protokollen"](#)

Zurücksetzen verlorener und fehlender Objektanzahl

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

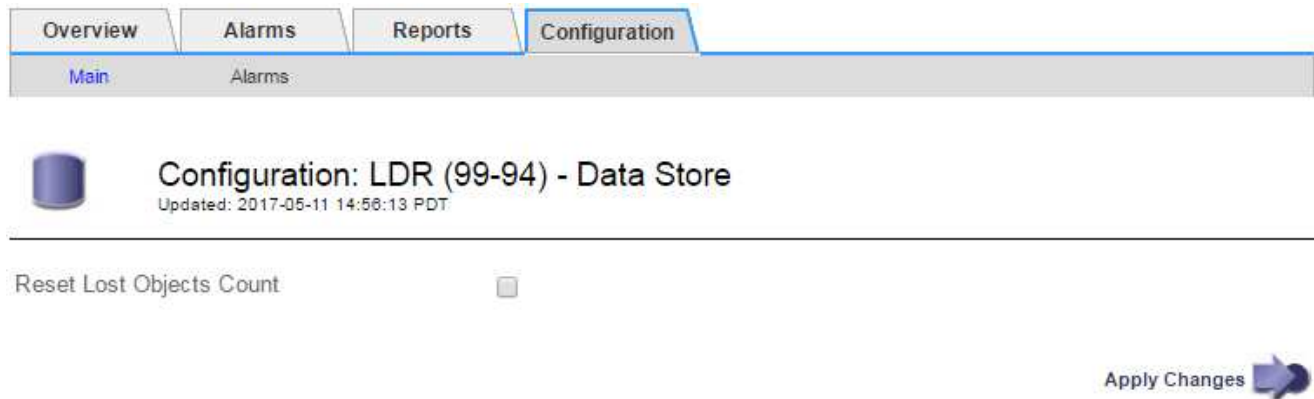
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **Support > Tools > Grid Topology > site > Storage Node > LDR > Data Store > Übersicht > Main**
- **Support > Tools > Grid Topology > 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 Topology** 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**.



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.
 - a. Wählen Sie **Site > Storage Node > LDR > Erasure Coding > Konfiguration** aus.
 - b. Wählen Sie **Reset reads Failure Count** und **Reset corrupte Kopien Detected Count** aus.
 - c. Klicken Sie Auf **Änderungen Übernehmen**.
 - d. Wählen Sie **Site > Storage Node > LDR > Verifizierung > Konfiguration**.
 - e. Wählen Sie **Anzahl der fehlenden Objekte zurücksetzen** und **Anzahl der beschädigten Objekte zurücksetzen**.
 - f. Wenn Sie sicher sind, dass keine isolierten Objekte erforderlich sind, können Sie **Quarantäne-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.

- g. Klicken Sie Auf **Änderungen Übernehmen**.

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

Verwandte Informationen

["StorageGRID verwalten"](#)

Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Der **Low Object Datenspeicher** wird ausgelöst, wenn die Gesamtzahl der replizierten und Erasure codierten Objektdaten auf einem Storage Node eine der Bedingungen erfüllt, die in der Warnungsregel konfiguriert sind.

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` Schätzung der Gesamtgröße der replizierten und Erasure-codierten 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 **Alarmer > Aktuell**.

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:

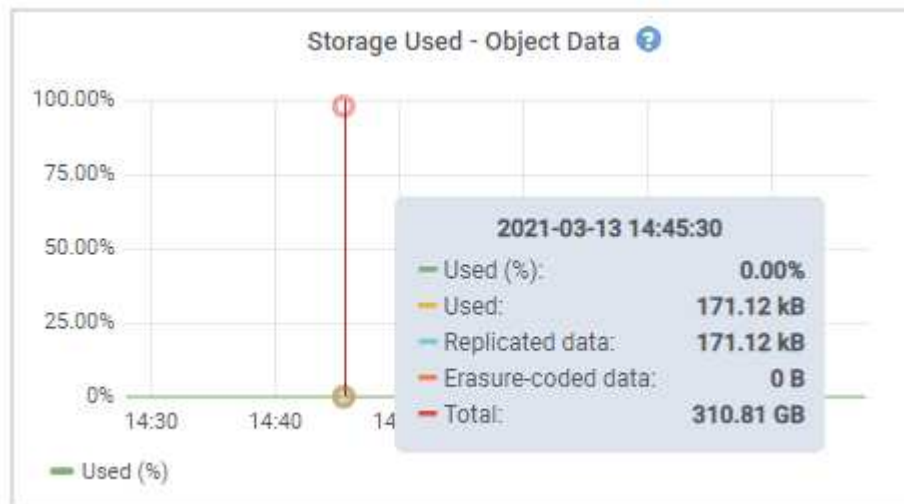
- Auslösezeit
- Der Name des Standorts und des Nodes
- Die aktuellen Werte der Metriken für diese Meldung

4. Wählen Sie **Nodes > Storage Node oder Standort > Storage** aus.

5. Bewegen Sie den Mauszeiger über das Diagramm „verwendete Daten – 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, ein Erweiterungsverfahren für zusätzliche Speicherkapazität durchführen.

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



Informationen zum Verwalten eines vollständigen Speicherknoten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

["Fehlerbehebung beim SSTS-Alarm \(Storage Status\)"](#)

["Erweitern Sie Ihr Raster"](#)

["StorageGRID verwalten"](#)

Fehlerbehebung beim SSTS-Alarm (Storage Status)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 Speicheroptionen Übersicht**) 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 > Alarmer (alt) > Aktuelle Alarmer**.
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 „Alarmer“ werden die aktiven Alarmer 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
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
Normal	SHLH (Health)						<input 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).

OverviewAlarmsReportsConfiguration

Main



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 **verfügbaren**-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.

Overview

Alarms

Reports

Configuration

Charts

Text

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

Attribute:

Total Usable Space

Quick Query:

Custom Query

Update

Vertical Scaling:

☒

Raw Data:

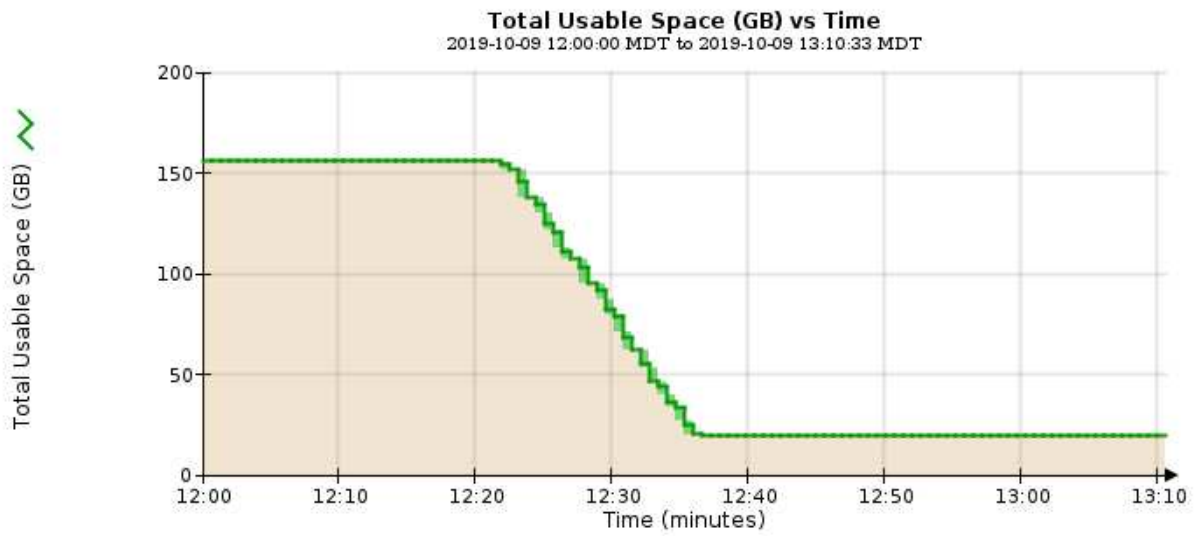
☐

Start Date:

2019/10/09 12:00:00

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.

Overview

Alarms

Reports

Configuration

Charts

Text

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

Attribute:

Total Usable Space (Percent)

Quick Query:

Custom Query

Update

Vertical Scaling:
☒

Raw Data:
☐

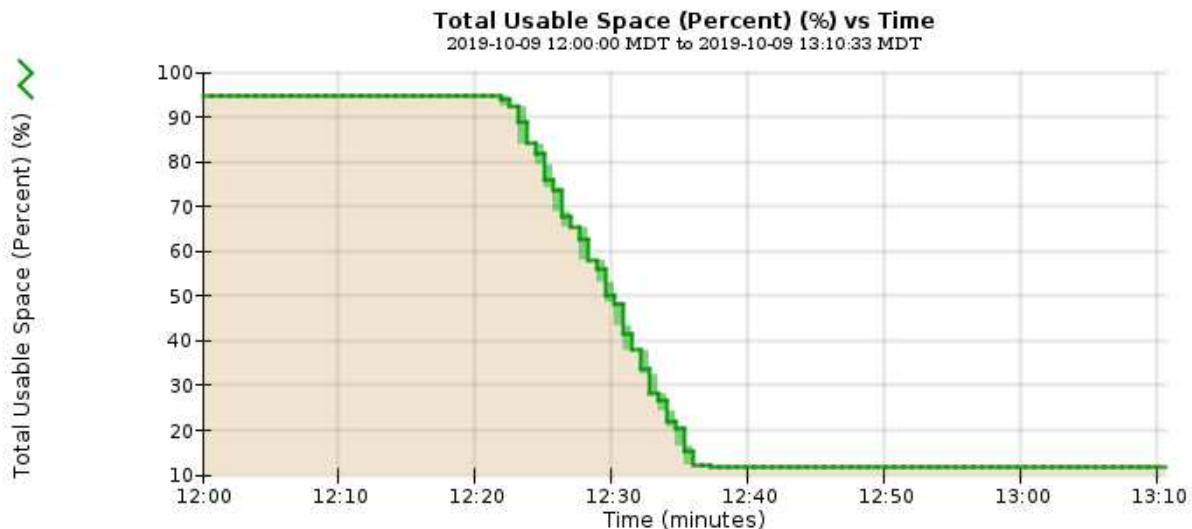
YYYY/MM/DD HH:MM:SS

Start Date:

2019/10/09 12:00:00

End Date:

2019/10/09 13:10:33



6. Bei Bedarf Erweiterung des StorageGRID Systems Storage-Kapazität hinzufügen.

Anweisungen zum Verwalten eines vollständigen Speicherknoten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

["Erweitern Sie Ihr Raster"](#)

["StorageGRID verwalten"](#)

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

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

Über diese Aufgabe

So kann beispielsweise ein S3-Multipart-Upload erfolgreich sein, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsmeldung nicht an den konfigurierten Endpunkt gesendet 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.

Weitere Informationen zur Fehlerbehebung bei Plattform-Services finden Sie in den Anweisungen für die Administration von StorageGRID. Möglicherweise müssen Sie über den Tenant Manager auf den Mandanten zugreifen, um einen Plattformdienstfehler zu beheben.

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. Klicken Sie auf **Ereignisanzahl 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.

Verwandte Informationen

["StorageGRID verwalten"](#)

["Verwenden Sie ein Mandantenkonto"](#)

["Referenz für Protokolldateien"](#)

["Ereignisanzahl wird zurückgesetzt"](#)

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.