



Fehlerbehebung bei verlorenen und fehlenden Objektdaten

StorageGRID 11.8

NetApp
March 19, 2024

Inhalt

- Fehlerbehebung bei verlorenen und fehlenden Objektdaten 1
 - Fehlerbehebung bei verlorenen und fehlenden Objektdaten: Übersicht 1
 - Untersuchen Sie verlorene Objekte 1
 - Suche nach potenziell verlorenen Objekten und Wiederherstellung 6
 - Verlorene und fehlende Objektanzahl zurücksetzen 12

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 Löschvorgängen 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. Geben Sie Ein: `cd /var/local/log/`
- 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)": "MD5D0xBAC2A2617C1DFF7E959A76731E6EAF5E",
```

```

        "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, können Sie die Anzahl der verlorenen Objekte 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 Objects Lost 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 "Suche nach möglicherweise verlorenen Objekten" 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 verlorenen Objekte 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 "Suchen Sie das Objekt und stellen Sie es wieder her" 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 "Wiederherstellen von Objektdateien mit Grid Manager" Und "Wiederherstellung von Objektdateien auf einem Storage-Volume".</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 Audit-Protokolle befinden: `cd /var/local/log/`
 - 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 >
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 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) :
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.

- 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: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 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%DkRt78Ila#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: `cd /var/local/log/`

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 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 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.

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

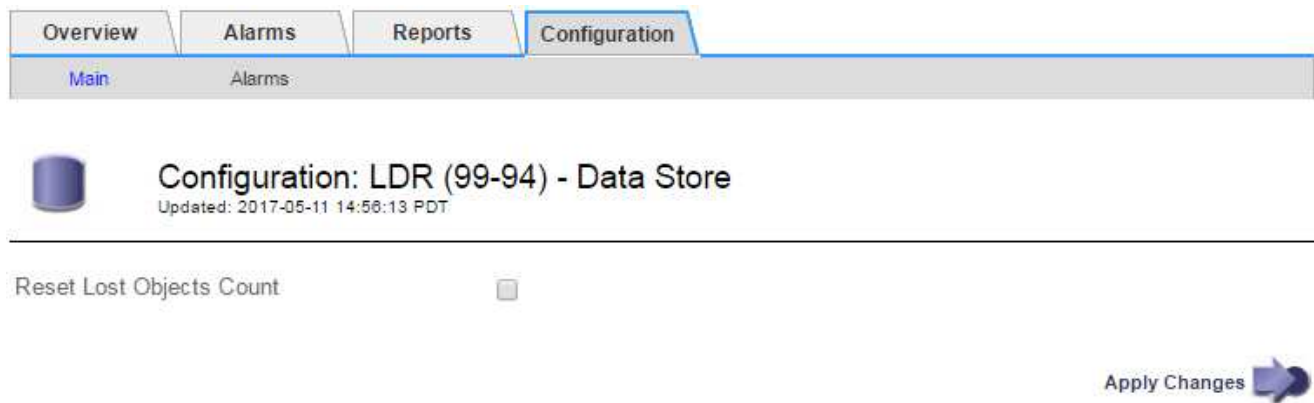
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **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**.



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** aus.
- e. Wählen Sie **Anzahl der fehlenden Objekte zurücksetzen** und **Anzahl der beschädigten Objekte zurücksetzen**.
- f. Wenn Sie sicher sind, dass isolierte Objekte nicht benötigt werden, können Sie **gesperrte 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.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.