Fehlerbehebung beim StorageGRID -System

StorageGRID software

NetApp
December 03, 2025

Inhalt

Fehlerbehebung beim StorageGRID -System

Fehlerbehebung bei einem StorageGRID -System

Wenn bei der Verwendung eines StorageGRID -Systems ein Problem auftritt, finden Sie in den Tipps und Richtlinien in diesem Abschnitt Hilfe bei der Ermittlung und Lösung des Problems.

Oft können Sie Probleme selbst lösen. Bei manchen Problemen müssen Sie sich jedoch möglicherweise an den technischen Support wenden.

Definieren Sie das Problem

Der erste Schritt zur Lösung eines Problems besteht darin, das Problem klar zu definieren.

Diese Tabelle enthält Beispiele für die Arten von Informationen, die Sie zur Definition eines Problems sammeln können:

Frage	Beispielantwort
Was macht das StorageGRID -System bzw. was macht es nicht? Was sind die Symptome?	Clientanwendungen melden, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann begann das Problem?	Die Objektaufnahme wurde am 8. Januar 2020 gegen 14:50 Uhr erstmals verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Benachrichtigung durch Clientanwendung. Habe auch E-Mail-Benachrichtigungen erhalten.
Tritt das Problem ständig auf oder nur manchmal?	Das Problem besteht weiterhin.
Wenn das Problem regelmäßig auftritt, welche Schritte führen dazu, dass es auftritt?	Das Problem tritt jedes Mal auf, wenn ein Client versucht, ein Objekt aufzunehmen.
Wenn das Problem zeitweise auftritt, wann tritt es auf? Notieren Sie die Zeitpunkte aller Vorfälle, die Ihnen bekannt sind.	Das Problem tritt nicht zeitweise auf.
Ist Ihnen dieses Problem schon einmal begegnet? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dieses Problem ist mir zum ersten Mal begegnet.

Bewerten Sie das Risiko und die Auswirkungen auf das System

Nachdem Sie das Problem definiert haben, bewerten Sie dessen Risiko und Auswirkungen auf das StorageGRID -System. Beispielsweise bedeutet das Vorhandensein kritischer Warnungen nicht unbedingt, dass das System keine Kerndienste bereitstellt.

Diese Tabelle fasst die Auswirkungen des Beispielproblems auf den Systembetrieb zusammen:

Frage	Beispielantwort
Kann das StorageGRID -System Inhalte aufnehmen?	NEIN.
Können Clientanwendungen Inhalte abrufen?	Einige Objekte können abgerufen werden, andere nicht.
Sind Daten gefährdet?	NEIN.
Ist die Geschäftsfähigkeit stark beeinträchtigt?	Ja, da Clientanwendungen keine Objekte im StorageGRID -System speichern können und Daten nicht konsistent abgerufen werden können.

Daten sammeln

Nachdem Sie das Problem definiert und sein Risiko und seine Auswirkungen bewertet haben, sammeln Sie Daten für die Analyse. Welche Art von Daten am sinnvollsten zu erfassen ist, hängt von der Art des Problems ab.

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Erstellen Sie eine Zeitleiste der letzten Änderungen	Änderungen an Ihrem StorageGRID -System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Erstellen Sie eine Zeitleiste der letzten Änderungen
Benachrichtigungen überprüfen	Mithilfe von Warnmeldungen können Sie die Grundursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme liefern, die das Problem möglicherweise verursachen. Überprüfen Sie die Liste der aktuellen Warnungen, um festzustellen, ob StorageGRID die Grundursache eines Problems für Sie identifiziert hat. Überprüfen Sie in der Vergangenheit ausgelöste Warnungen, um zusätzliche Erkenntnisse zu erhalten.	• "Aktuelle und gelöste Warnmeldungen anzeigen"
Überwachen von Ereignissen	Zu den Ereignissen zählen alle Systemfehler oder Störungsereignisse für einen Knoten, einschließlich Fehlern wie Netzwerkfehlern. Überwachen Sie Ereignisse, um mehr über Probleme zu erfahren oder bei der Fehlerbehebung zu helfen.	• "Überwachen von Ereignissen"
Identifizieren Sie Trends mithilfe von Diagrammen und Textberichten	Trends können wertvolle Hinweise darauf liefern, wann Probleme erstmals auftraten, und Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	• "Verwenden Sie Diagramme und Grafiken" • "Verwenden Sie Textberichte"

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Festlegen von Basislinien	Sammeln Sie Informationen über die Normalwerte verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Basiswerten können wertvolle Hinweise liefern.	• Festlegen von Basislinien
Durchführen von Aufnahme- und Abruftests	Um Leistungsprobleme beim Aufnehmen und Abrufen zu beheben, verwenden Sie eine Workstation zum Speichern und Abrufen von Objekten. Vergleichen Sie die Ergebnisse mit denen, die Sie bei Verwendung der Clientanwendung sehen.	• "Überwachen Sie die PUT- und GET-Leistung"
Überprüfen von Auditmeldungen	Überprüfen Sie die Prüfmeldungen, um die StorageGRID -Vorgänge im Detail zu verfolgen. Die Details in den Prüfmeldungen können bei der Behebung vieler Arten von Problemen hilfreich sein, darunter auch Leistungsprobleme.	• "Überprüfen von Auditmeldungen"
Überprüfen Sie die Objektstandorte und Speicherintegrität	Wenn Sie Speicherprobleme haben, überprüfen Sie, ob die Objekte dort platziert werden, wo Sie es erwarten. Überprüfen Sie die Integrität der Objektdaten auf einem Speicherknoten.	• "Überwachen von Objektüberprüfungsvorgängen" • "Bestätigen Sie die Speicherorte der Objektdaten" • "Überprüfen der Objektintegrität"
Sammeln Sie Daten für den technischen Support	Der technische Support bittet Sie möglicherweise, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um bei der Behebung von Problemen zu helfen.	• "Erfassen von Protokolldateien und Systemdaten" • "Manuelles Auslösen eines AutoSupport -Pakets" • "Überprüfen der Supportmetriken"

Erstellen Sie eine Zeitleiste der letzten Änderungen

Wenn ein Problem auftritt, sollten Sie berücksichtigen, was sich kürzlich geändert hat und wann diese Änderungen aufgetreten sind.

- Änderungen an Ihrem StorageGRID -System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.
- Mithilfe einer Zeitleiste der Änderungen können Sie ermitteln, welche Änderungen möglicherweise für ein Problem verantwortlich sind und wie sich jede Änderung möglicherweise auf dessen Entwicklung ausgewirkt hat.

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält,

wann die einzelnen Änderungen vorgenommen wurden, sowie alle relevanten Details zu den Änderungen, z. B. Informationen darüber, was sonst noch während der Änderung geschah:

Zeit der Veränderung	Art der Änderung	Details
Beispiel: • Wann haben Sie mit der Knotenwiederherstellung begonnen? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Vorgang unterbrochen?	Was ist passiert? Was hast du gemacht?	Dokumentieren Sie alle relevanten Details zur Änderung. Beispiel: • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Wie sich die Arbeitslast der Clients verändert hat. Achten Sie darauf, ob mehrere Änderungen gleichzeitig vorgenommen wurden. Wurde diese Änderung beispielsweise während eines laufenden Upgrades vorgenommen?

Beispiele für bedeutende aktuelle Änderungen

Hier sind einige Beispiele für potenziell bedeutende Änderungen:

- Wurde das StorageGRID -System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde das System kürzlich aktualisiert? Wurde ein Hotfix angewendet?
- Wurde kürzlich Hardware repariert oder ausgetauscht?
- Wurde die ILM-Richtlinie aktualisiert?
- Hat sich die Arbeitsbelastung des Kunden geändert?
- Hat sich die Clientanwendung oder ihr Verhalten geändert?
- Haben Sie Load Balancer geändert oder eine Hochverfügbarkeitsgruppe von Admin-Knoten oder Gateway-Knoten hinzugefügt oder entfernt?
- Wurden Aufgaben begonnen, deren Erledigung möglicherweise viel Zeit in Anspruch nimmt? Beispiele hierfür sind:
  - Wiederherstellung eines ausgefallenen Speicherknotens
  - Außerbetriebnahme von Speicherknoten
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, z. B. das Hinzufügen eines Mandanten oder das Ändern der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattformdienste kürzlich aktiviert oder geändert?
- Wurde die Compliance vor Kurzem aktiviert?
- Wurden Cloud-Speicherpools hinzugefügt oder entfernt?
- Wurden Änderungen an der Speicherkomprimierung oder -verschlüsselung vorgenommen?
- Gab es Änderungen an der Netzwerkinfrastruktur? Zum Beispiel VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?

- Wurden sonstige Änderungen am StorageGRID -System oder seiner Umgebung vorgenommen?

Festlegen von Basislinien

Sie können Basiswerte für Ihr System festlegen, indem Sie die Normalwerte verschiedener Betriebswerte aufzeichnen. In Zukunft können Sie aktuelle Werte mit diesen Basiswerten vergleichen, um abnormale Werte zu erkennen und zu beheben.

Eigentum	Wert	So erhalten Sie
Durchschnittlicher Speicherverbrauch	Verbrauchte GB/Tag Prozent verbraucht/Tag	Gehen Sie zum Grid Manager. Wählen Sie auf der Seite „Knoten“ das gesamte Raster oder eine Site aus und wechseln Sie zur Registerkarte „Speicher“. Suchen Sie im Diagramm „Speichernutzung – Objektdaten“ einen Zeitraum, in dem die Linie relativ stabil ist. Bewegen Sie den Cursor über das Diagramm, um zu schätzen, wie viel Speicherplatz täglich verbraucht wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenverbrauch	Verbrauchte GB/Tag Prozent verbraucht/Tag	Gehen Sie zum Grid Manager. Wählen Sie auf der Seite „Knoten“ das gesamte Raster oder eine Site aus und wechseln Sie zur Registerkarte „Speicher“. Suchen Sie im Diagramm „Speicherplatznutzung – Objektmetadaten“ einen Zeitraum, in dem die Linie relativ stabil ist. Bewegen Sie den Cursor über das Diagramm, um zu schätzen, wie viel Metadatenspeicher täglich verbraucht wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Rate der S3/Swift-Operationen	Operationen/Sekunde	Wählen Sie im Grid Manager-Dashboard **Leistung** > **S3-Operationen** oder **Leistung** > **Swift-Operationen**. Um die Aufnahme- und Abrufraten sowie die Anzahl für eine bestimmte Site oder einen bestimmten Knoten anzuzeigen, wählen Sie **KNOTEN** > ***Site oder Speicherknoten*** > **Objekte**. Positionieren Sie Ihren Cursor über dem Ingest- und Retrieve-Diagramm für S3.

Eigentum	Wert	So erhalten Sie
Fehlgeschlagene S3/Swift-Operationen	Operationen	Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**. Zeigen Sie auf der Registerkarte „Übersicht“ im Abschnitt „API-Operationen“ den Wert für „S3-Operationen – Fehlgeschlagen“ oder „Swift-Operationen – Fehlgeschlagen“ an.
ILM-Auswertungsrate	Objekte/Sekunde	Wählen Sie auf der Seite „Knoten“ ***grid*** > **ILM** aus. Suchen Sie im ILM-Warteschlangendiagramm einen Zeitraum, in dem die Leitung relativ stabil ist. Positionieren Sie Ihren Cursor über dem Diagramm, um einen Basiswert für die **Bewertungsrate** für Ihr System zu schätzen.
ILM-Scanrate	Objekte/Sekunde	Wählen Sie **NODES** > ***grid*** > **ILM**. Suchen Sie im ILM-Warteschlangendiagramm einen Zeitraum, in dem die Leitung relativ stabil ist. Positionieren Sie Ihren Cursor über dem Diagramm, um einen Basiswert für die **Scanrate** für Ihr System zu schätzen.
Objekte aus Clientvorgängen in der Warteschlange	Objekte/Sekunde	Wählen Sie **NODES** > ***grid*** > **ILM**. Suchen Sie im ILM-Warteschlangendiagramm einen Zeitraum, in dem die Leitung relativ stabil ist. Positionieren Sie Ihren Cursor über dem Diagramm, um einen Basiswert für **in die Warteschlange gestellte Objekte (aus Clientvorgängen)** für Ihr System zu schätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie **NODES** > ***Storage Node*** > **Objects**. Zeigen Sie in der Abfragetabelle den Wert für die durchschnittliche Latenz an.

Daten analysieren

Verwenden Sie die gesammelten Informationen, um die Ursache des Problems und mögliche Lösungen zu ermitteln.

Die Analyse ist problemabhängig, aber im Allgemeinen gilt:

- Lokalisieren Sie mithilfe der Warnungen Fehlerpunkte und Engpässe.
- Rekonstruieren Sie den Problemverlauf mithilfe des Warnverlaufs und der Diagramme.
- Verwenden Sie Diagramme, um Anomalien zu finden und die Problemsituation mit dem Normalbetrieb zu vergleichen.

Checkliste für Eskalationsinformationen

Wenn Sie das Problem nicht selbst lösen können, wenden Sie sich an den technischen Support. Bevor Sie sich an den technischen Support wenden, sammeln Sie die in der folgenden Tabelle aufgeführten Informationen, um die Problemlösung zu erleichtern.

✔	Artikel	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann begann das Problem? Passiert das ständig oder zeitweise? Wenn es zeitweise auftritt, wann ist es aufgetreten? Definieren Sie das Problem
	Folgenabschätzung	Wie schwerwiegend ist das Problem? Welche Auswirkungen hat dies auf die Clientanwendung? • Hat der Client zuvor eine erfolgreiche Verbindung hergestellt? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID -System-ID	Wählen Sie **WARTUNG** > **System** > **Lizenz**. Die StorageGRID -System-ID wird als Teil der aktuellen Lizenz angezeigt.
	Softwareversion	Wählen Sie oben im Grid Manager das Hilfesymbol und dann **Info** aus, um die StorageGRID -Version anzuzeigen.
	Anpassung	Fassen Sie zusammen, wie Ihr StorageGRID -System konfiguriert ist. Listen Sie beispielsweise Folgendes auf: • Verwendet das Grid Speicherkomprimierung, Speicherverschlüsselung oder Compliance? • Erstellt ILM replizierte oder löschcodierte Objekte? Stellt ILM die Standortredundanz sicher? Verwenden ILM-Regeln die Aufnahmeverhalten „Balanced“, „Strict“ oder „Dual Commit“?

✔	Artikel	Hinweise
	Protokolldateien und Systemdaten	Sammeln Sie Protokolldateien und Systemdaten für Ihr System. Wählen Sie **SUPPORT** > **Tools** > **Protokolle**. Sie können Protokolle für das gesamte Raster oder für ausgewählte Knoten sammeln. Wenn Sie Protokolle nur für ausgewählte Knoten sammeln, achten Sie darauf, mindestens einen Speicherknoten einzuschließen, der über den ADC-Dienst verfügt. (Die ersten drei Speicherknoten an einem Standort umfassen den ADC-Dienst.) "Erfassen von Protokolldateien und Systemdaten"
	Basisinformationen	Sammeln Sie Basisinformationen zu Aufnahmevorgängen, Abrufvorgängen und Speicherverbrauch. Festlegen von Basislinien
	Zeitleiste der jüngsten Änderungen	Erstellen Sie eine Zeitleiste, die alle aktuellen Änderungen am System oder seiner Umgebung zusammenfasst. Erstellen Sie eine Zeitleiste der letzten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie selbst Schritte zur Diagnose oder Fehlerbehebung des Problems unternommen haben, dokumentieren Sie die durchgeführten Schritte und das Ergebnis.

Beheben von Objekt- und Speicherproblemen

Bestätigen Sie die Speicherorte der Objektdaten

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

Bevor Sie beginnen

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

Schritte

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

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

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

4. Wählen Sie **Nachschlagen**.

   Der"Ergebnisse der Objektmetadatensuche" erscheinen. Auf dieser Seite sind die folgenden Arten von Informationen aufgeführt:

   - Systemmetadaten, einschließlich der Objekt-ID (UUID), der Versions-ID (optional), des Objektnamens, des Namens des Containers, des Mandantenkontonamens oder der ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Objekterstellung sowie des Datums und der Uhrzeit der letzten Objektänderung.
   - Alle benutzerdefinierten Schlüssel-Wert-Paare der Benutzermetadaten, die mit dem Objekt verknüpft sind.
   - Bei S3-Objekten alle mit dem Objekt verknüpften Schlüssel-Wert-Paare des Objekt-Tags.
   - Bei replizierten Objektkopien der aktuelle Speicherort jeder Kopie.
   - Bei Erasure-Coded-Objektkopien der aktuelle Speicherort jedes Fragments.
   - Bei Objektkopien in einem Cloud Storage Pool der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
   - Für segmentierte Objekte und mehrteilige Objekte eine Liste von Objektsegmenten einschließlich Segmentkennungen und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
   - Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten umfassen interne Systemmetadaten, deren Beibehaltung von Version zu Version nicht garantiert ist.

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


Fehler im Objektspeicher (Speichervolumen)

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

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

Disk devices

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

Volumes

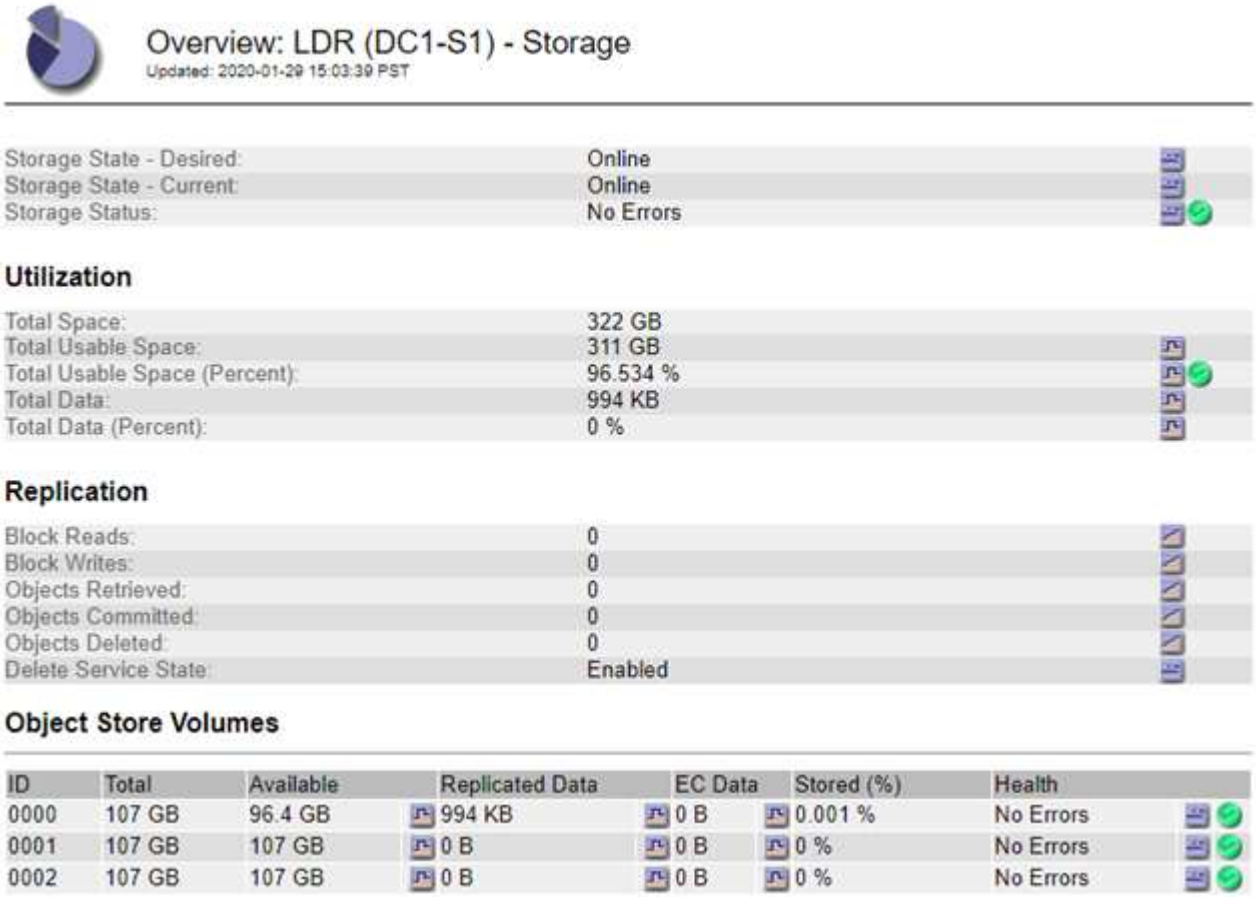
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Mehr sehen"Details zu jedem Speicherknoten" , führen Sie die folgenden Schritte aus:

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



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

Überprüfen der Objektintegrität

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

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

Was ist eine Hintergrundüberprüfung?

Der Hintergrundüberprüfungsprozess prüft Speicherknoten automatisch und kontinuierlich auf beschädigte

Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

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

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

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

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

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

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

Warnungen im Zusammenhang mit der Hintergrundüberprüfung

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

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

Ändern Sie die Hintergrundüberprüfungsrate

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

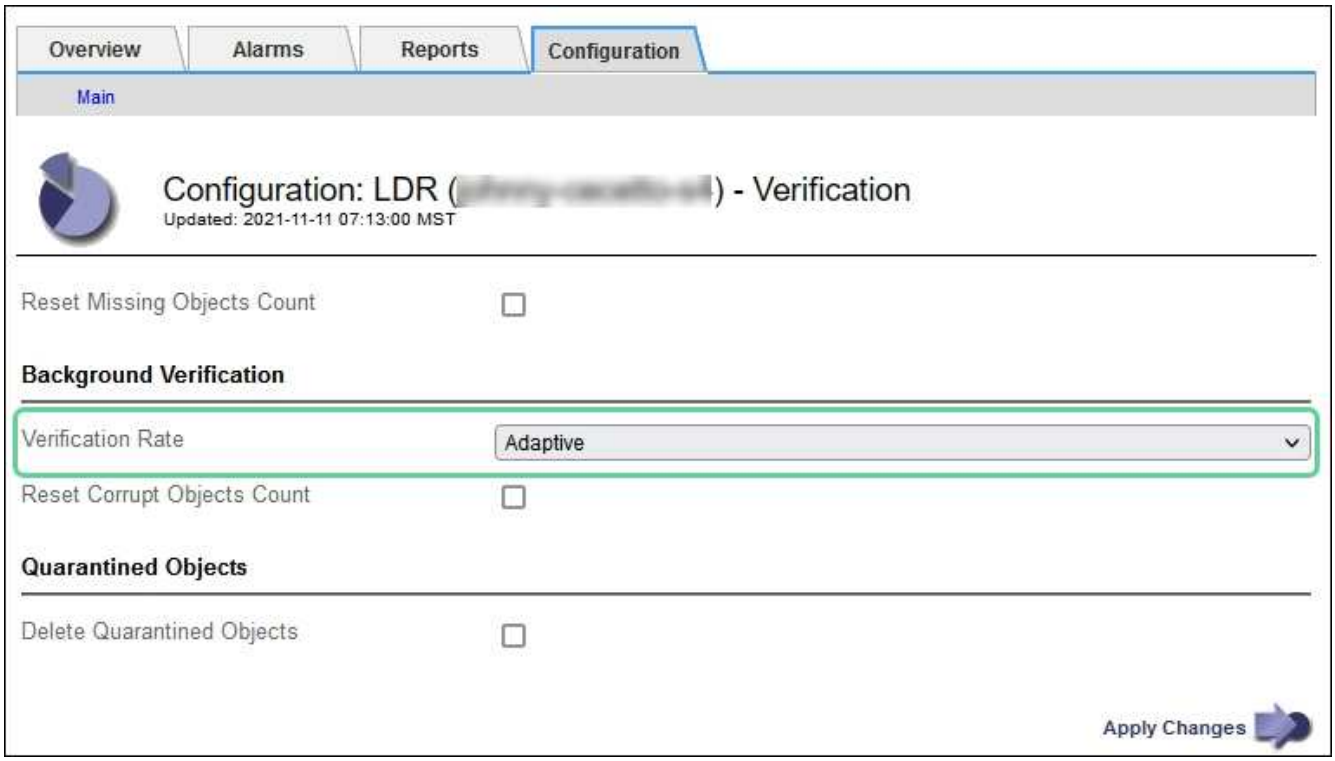
- Adaptiv: Standardeinstellung. Die Aufgabe ist für eine Überprüfung mit maximal 4 MB/s oder 10 Objekten/s ausgelegt (je nachdem, was zuerst überschritten wird).

- Hoch: Die Speicherüberprüfung erfolgt schnell, mit einer Geschwindigkeit, die normale Systemaktivitäten verlangsamen kann.

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

Schritte

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



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

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

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

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

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

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

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

   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***Speicherknoten*** > **LDR** > **Erasure Coding**.
   c. Überwachen Sie in der Tabelle „Verifizierungsergebnisse“ das Attribut „Beschädigte Fragmente erkannt“ (ECCD).

9. Nachdem beschädigte Objekte automatisch vom StorageGRID System wiederhergestellt wurden, setzen Sie die Anzahl der beschädigten Objekte zurück.
   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***Speicherknoten*** > **LDR** > **Verifizierung** > **Konfiguration**.
   c. Wählen Sie **Anzahl beschädigter Objekte zurücksetzen**.
   d. Klicken Sie auf **Änderungen übernehmen**.

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

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

    a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
    b. Wählen Sie ***Speicherknoten*** > **LDR** > **Verifizierung** > **Konfiguration**.
    c. Wählen Sie **Unter Quarantäne gestellte Objekte löschen**.
    d. Wählen Sie **Änderungen übernehmen**.

Was ist eine Objektexistenzprüfung?

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

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

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

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

Führen Sie eine Objekt-Existenzprüfung durch

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

Bevor Sie beginnen

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

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

Informationen zu diesem Vorgang

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

Schritte

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

   Sie können nach Knotennamen oder Site suchen.

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

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

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

6. Wählen Sie **Weiter**.
7. Wählen Sie die Konsistenz für den Auftrag aus.

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

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

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

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

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

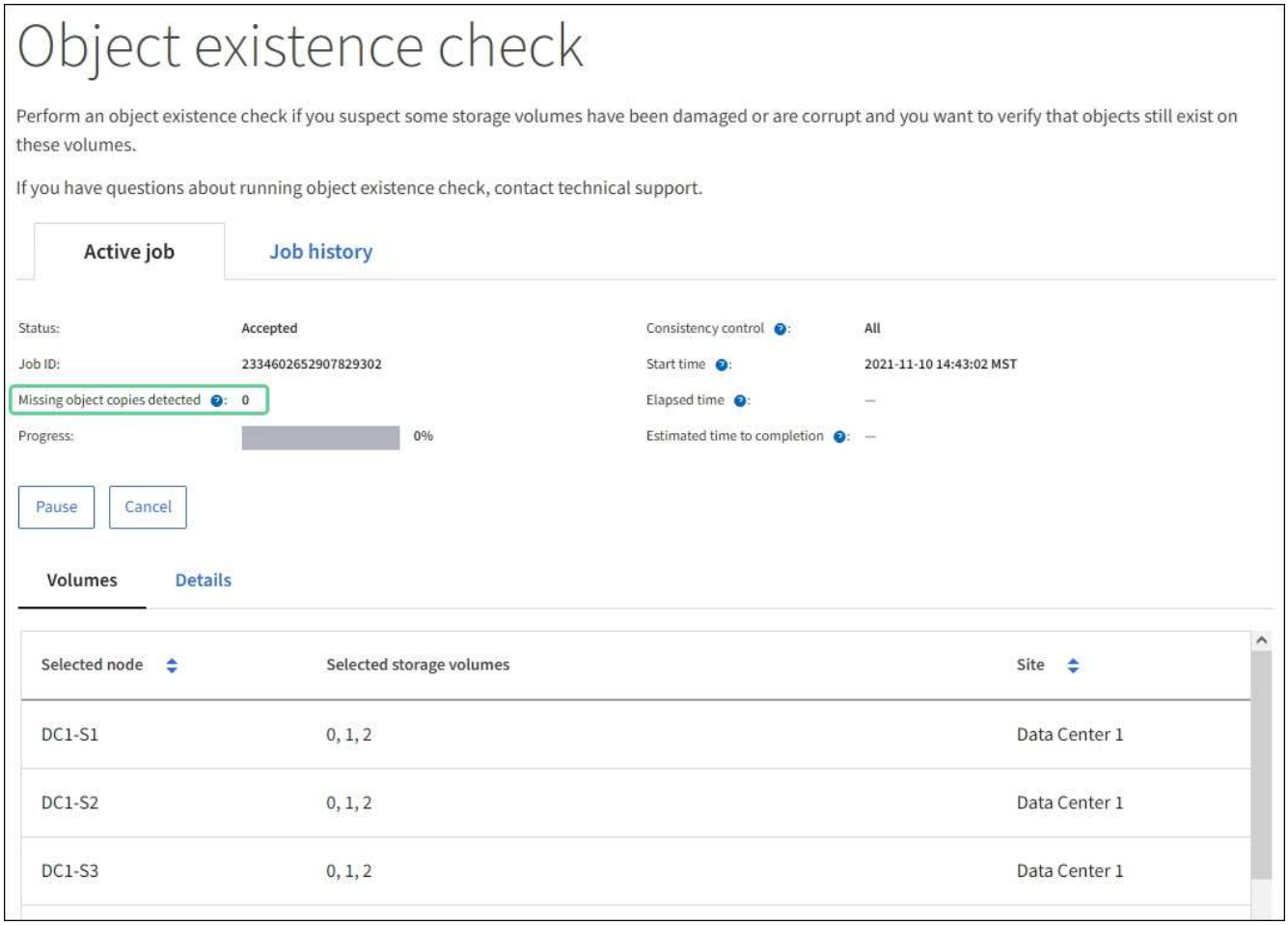
   - Der Auftrag ist abgeschlossen.
   - Sie pausieren oder brechen den Auftrag ab. Sie können einen Job fortsetzen, den Sie angehalten haben, aber Sie können einen Job nicht fortsetzen, den Sie abgebrochen haben.
   - Der Job stockt. Die Warnung „Prüfung der Objektexistenz ist ins Stocken geraten“ wird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

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

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

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

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



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

      Dieses Verfahren ist ähnlich wie bei"Untersuchung verlorener Gegenstände" , obwohl Sie für Objektkopien nach `LLST` anstatt `OLST` .

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

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

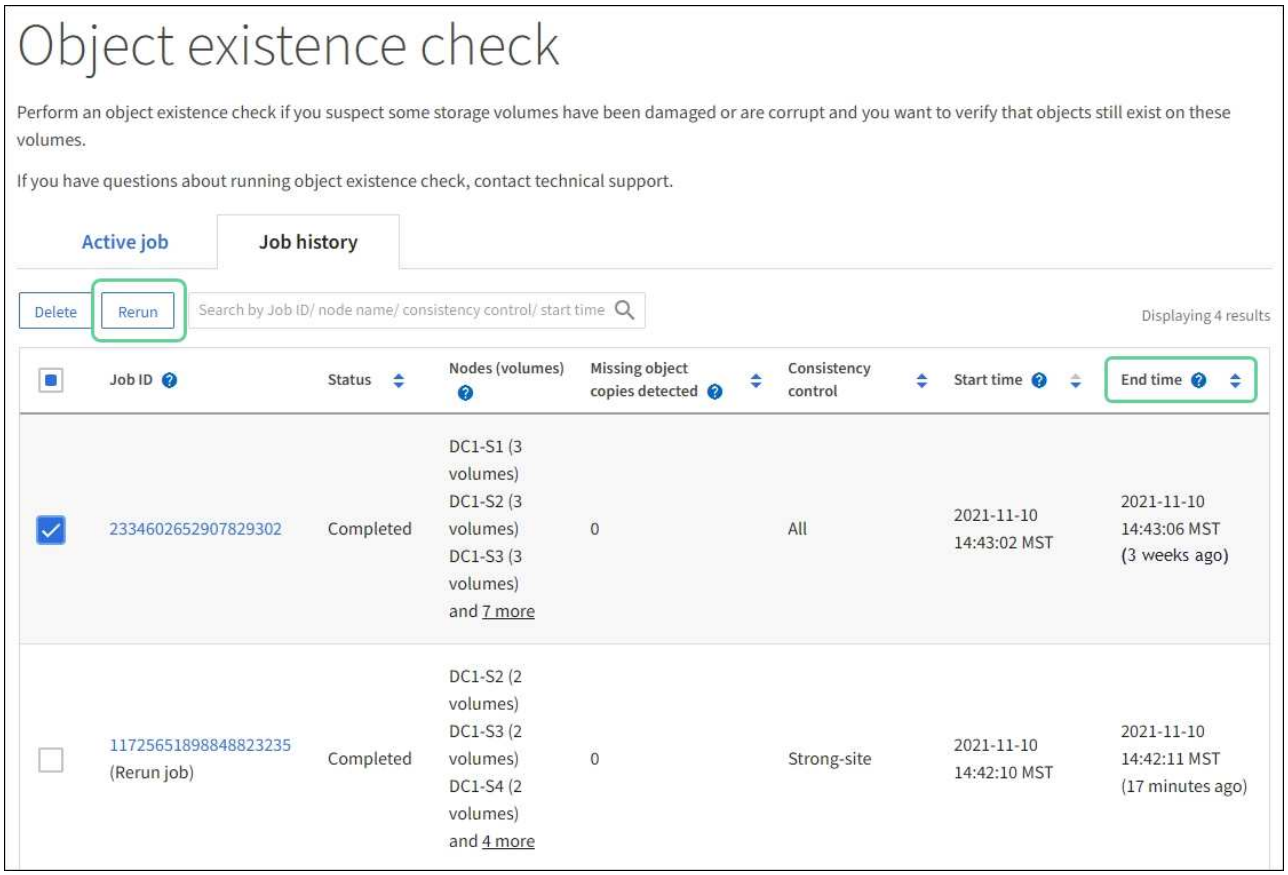
a. Wählen Sie **WARTUNG** > **Objektexistenzprüfung** > **Auftragsverlauf**.

b. Bestimmen Sie, welche Jobs zur erneuten Ausführung bereit sind:

   i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.

   ii. Durchsuchen Sie für diese Jobs die Spalte „Konsistenzkontrolle“ nach „Strong-Site“ oder „Strong-Global“.

c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **Erneut ausführen**.



d. Überprüfen Sie im Assistenten „Jobs erneut ausführen“ die ausgewählten Knoten und Volumes sowie die Konsistenz.

e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Erneut ausführen**.

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

Nach Abschluss

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

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

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

Bevor Sie beginnen

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

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

Schritte

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

   a. Eingeben `ssh admin@primary_Admin_Node_IP`

   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

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

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

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

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

   Weitere Informationen finden Sie unter"Auswählen von Zielen für Auditinformationen" .

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

      i. Eingeben `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

ii. Sehen Sie sich für jede Prüfnachricht in den Ergebnissen Folgendes an: `S3AI` Feld, um die Mandantenkonto-ID zu bestimmen. Verwenden Sie die anderen Felder in der Nachricht, um zu bestimmen, welche IP-Adresse vom Client, dem Bucket und dem Objekt verwendet wurde:

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

Beispiel für Audit-Protokollergebnisse

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"933908492661540043 43"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::9339084926615400 4343:root"][SBAI(CSTR):"9339084926615400 4343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Wenn Client-Schreibvorgänge nicht normal sind, verwenden Sie die Mandanten-ID aus der Warnung, um den Mandanten zu identifizieren:

   a. Gehen Sie zu **SUPPORT** > **Tools** > **Protokolle**. Sammeln Sie Anwendungsprotokolle für den Speicherknoten in der Warnung. Geben Sie 15 Minuten vor und nach der Warnung an.

   b. Extrahieren Sie die Datei und gehen Sie zu `bycast.log` :

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

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

      Beispiel bycast.log

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

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

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

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

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

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

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

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

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

Untersuchen Sie verlorene Gegenstände

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

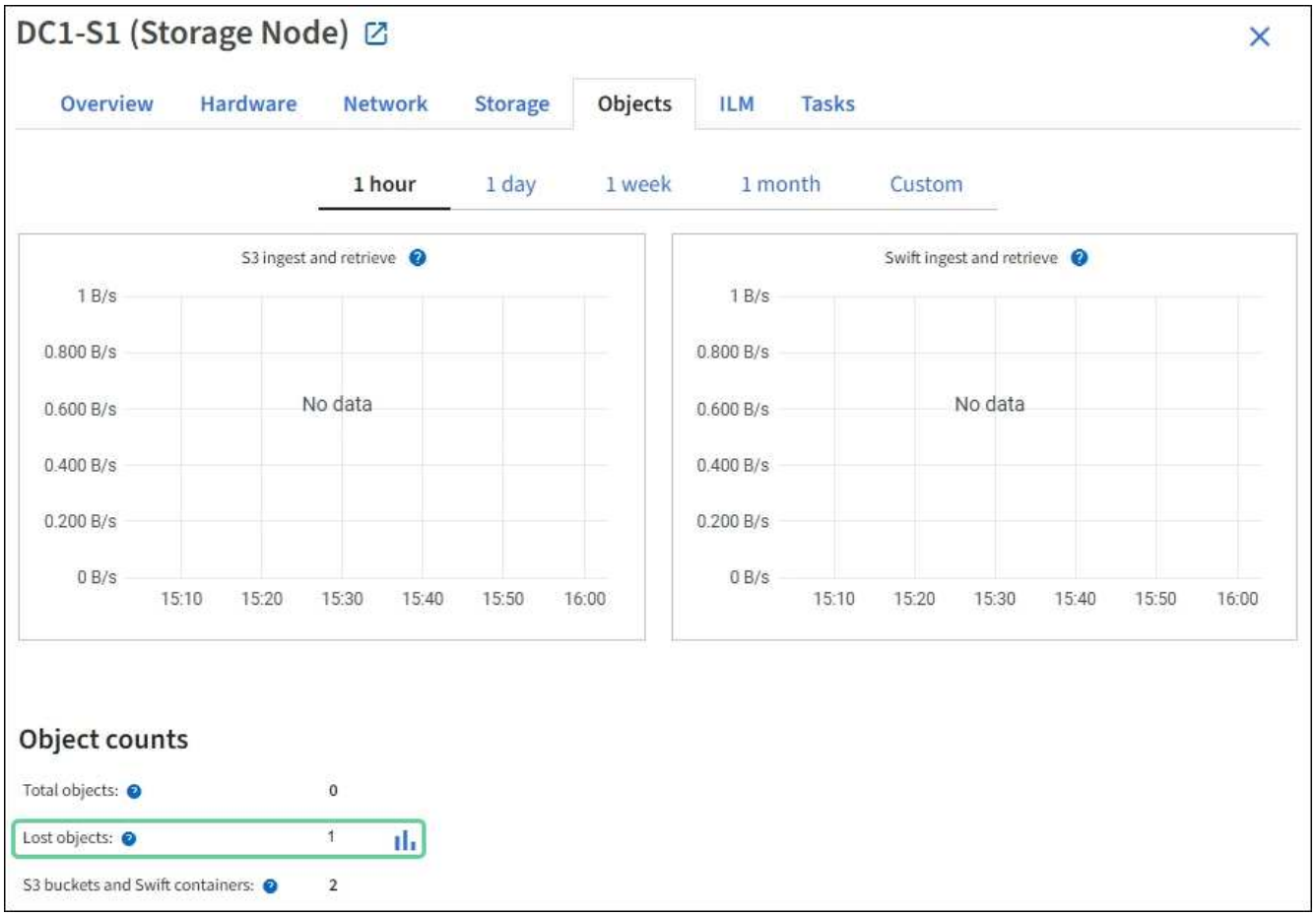
Die Warnung „Objekte verloren“ zeigt an, dass StorageGRID davon ausgeht, dass im Grid keine Kopien eines Objekts vorhanden sind. Möglicherweise sind die Daten dauerhaft verloren gegangen.

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

Schritte

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

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



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

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

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

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

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

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

Weitere Informationen finden Sie unter"Auswählen von Zielen für Auditinformationen" .

c. Verwenden Sie grep, um die OLST-Auditmeldungen (Object Lost) zu extrahieren. Eingeben: `grep OLST audit_file_name`

d. Beachten Sie den in der Nachricht enthaltenen UUID-Wert.

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

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

a. Wählen Sie **ILM** > **Objektmetadatensuche**.

b. Geben Sie die UUID ein und wählen Sie **Nachschlagen**.

c. Überprüfen Sie die Standorte in den Metadaten und ergreifen Sie die entsprechenden Maßnahmen:

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

Suchen und Wiederherstellen potenziell verlorener Objekte

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

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

Schritte

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

   a. Melden Sie sich beim Grid-Knoten an:

      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

      ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

      iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

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

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

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

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

      Weitere Informationen finden Sie unter"Auswählen von Zielen für Auditinformationen" .

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

      Beispiel:

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

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

      Beispiel:

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

Eine LLST-Auditnachricht sieht wie diese Beispielnachricht aus.

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

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

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

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

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

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

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

a. Melden Sie sich beim Grid-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

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

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

Geben Sie beispielsweise Folgendes ein:

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

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

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

3. Wenn der Objektpfad gefunden wurde, versuchen Sie, das Objekt in StorageGRID wiederherzustellen:
   a. Ändern Sie vom selben Speicherknoten aus den Besitz der Objektdatei, sodass sie von StorageGRID verwaltet werden kann. Eingeben: `chown ldr-user:bycast 'file_path_of_object'`
   b. Um auf die LDR-Konsole zuzugreifen, greifen Sie per Telnet auf den Localhost 1402 zu. Eingeben: `telnet 0 1402`
   c. Eingeben: `cd /proc/STOR`
   d. Eingeben: `Object_Found 'file_path_of_object'`

      Geben Sie beispielsweise Folgendes ein:

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

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

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

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

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

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

        Fahren Sie mit dem nächsten Schritt fort.

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

Speicherorte erstellt wurden:

a. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .

b. Wählen Sie **ILM** > **Objektmetadatensuche**.

c. Geben Sie die UUID ein und wählen Sie **Nachschlagen**.

d. Überprüfen Sie die Metadaten und bestätigen Sie die neuen Standorte.

5. Suchen Sie von einem Admin-Knoten aus in den Prüfprotokollen nach der ORLM-Prüfnachricht für dieses Objekt, um zu bestätigen, dass das Information Lifecycle Management (ILM) die erforderlichen Kopien platziert hat.

a. Melden Sie sich beim Grid-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei. Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

b. Wechseln Sie in das Verzeichnis, in dem sich die Überwachungsprotokolle befinden. SieheUnterschritt 1. b .

c. Verwenden Sie grep, um die mit dem Objekt verknüpften Prüfmeldungen in eine Ausgabedatei zu extrahieren. Eingeben: `grep uuid-value audit_file_name > output_file_name`

Beispiel:

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

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

Beispiel:

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

Eine ORLM-Auditnachricht sieht wie diese Beispielnachricht aus.

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

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

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

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

Zurücksetzen der Anzahl verlorener und fehlender Objekte

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

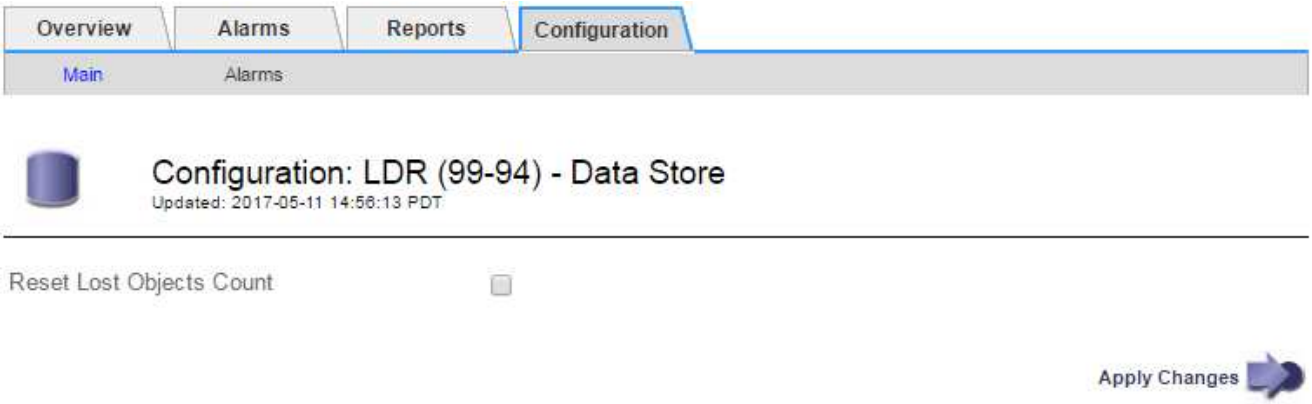
Sie können den Zähler für verlorene Objekte auf einer der folgenden Seiten zurücksetzen:

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

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

Schritte

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



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

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

5. Optional können Sie andere zugehörige Attributwerte zurücksetzen, die beim Identifizieren des verlorenen Objekts möglicherweise erhöht wurden.

   a. Wählen Sie ***Site*** > ***Storage Node*** > **LDR** > **Erasure Coding** > **Konfiguration**.

   b. Wählen Sie **Anzahl Lesefehler zurücksetzen** und **Anzahl erkannter beschädigter Kopien zurücksetzen**.

   c. Klicken Sie auf **Änderungen übernehmen**.

   d. Wählen Sie ***Site*** > ***Storage Node*** > **LDR** > **Verifizierung** > **Konfiguration**.

   e. Wählen Sie **Anzahl fehlender Objekte zurücksetzen** und **Anzahl beschädigter Objekte zurücksetzen**.

   f. Wenn Sie sicher sind, dass die unter Quarantäne gestellten Objekte nicht benötigt werden, können Sie „Unter Quarantäne gestellte Objekte löschen“ auswählen.

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

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

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

Fehlerbehebung bei der Warnung „Niedriger Objektdatenspeicher“

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

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

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

In diesem Zustand:

- `storagegrid_storage_utilization_data_bytes`ist eine Schätzung der Gesamtgröße der replizierten und erasure-coded Objektdaten für einen Speicherknoten.

- `storagegrid_storage_utilization_usable_space_bytes`ist die Gesamtmenge des für einen Speicherknoten verbleibenden Objektspeicherplatzes.

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

Schritte

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

   Die Seite „Warnungen“ wird angezeigt.

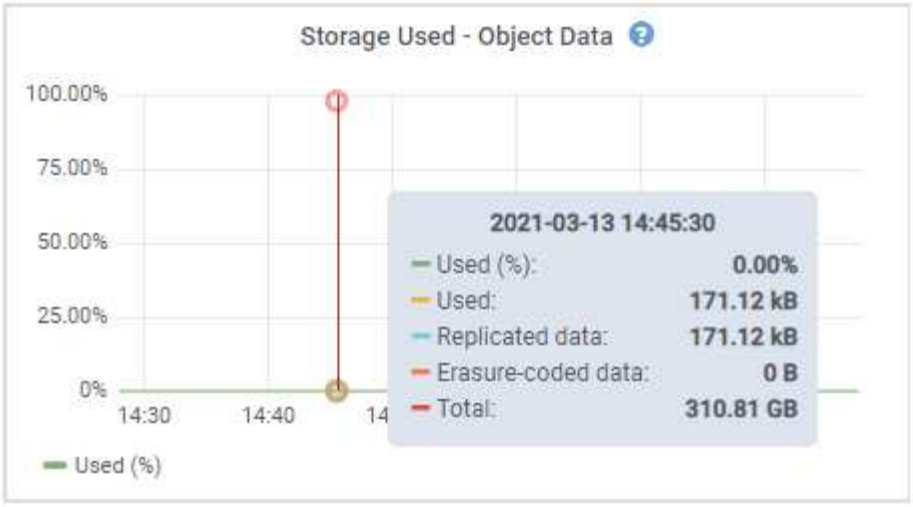
2. Erweitern Sie in der Tabelle der Warnungen bei Bedarf die Warnungsgruppe **Niedriger Objektdatenspeicher** und wählen Sie die Warnung aus, die Sie anzeigen möchten.

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

3. Überprüfen Sie die Details im Dialogfeld und beachten Sie Folgendes:
   - Zeitgesteuert
   - Der Name der Site und des Knotens
   - Die aktuellen Werte der Metriken für diese Warnung
4. Wählen Sie **NODES** > ***Speicherknoten oder -Site*** > **Speicher**.
5. Positionieren Sie den Cursor über dem Diagramm „Speicherplatznutzung – Objektdaten“.

   Es werden folgende Werte angezeigt:

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



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

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

7. So schnell wie möglich,"Speicherkapazität hinzufügen" zu Ihrem Raster.

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

   Weitere Informationen finden Sie unter "Vollständige Speicherknoten verwalten" .

Fehlerbehebung bei Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“

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

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

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

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

außer Kraft setzen auslösen, wenn Ihr benutzerdefinierter Wert für das weiche schreibgeschützte Wasserzeichen des Speichervolumes zu klein ist.

Verstehen Sie die Warnung

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

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

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

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

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

Beheben Sie die Warnung

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

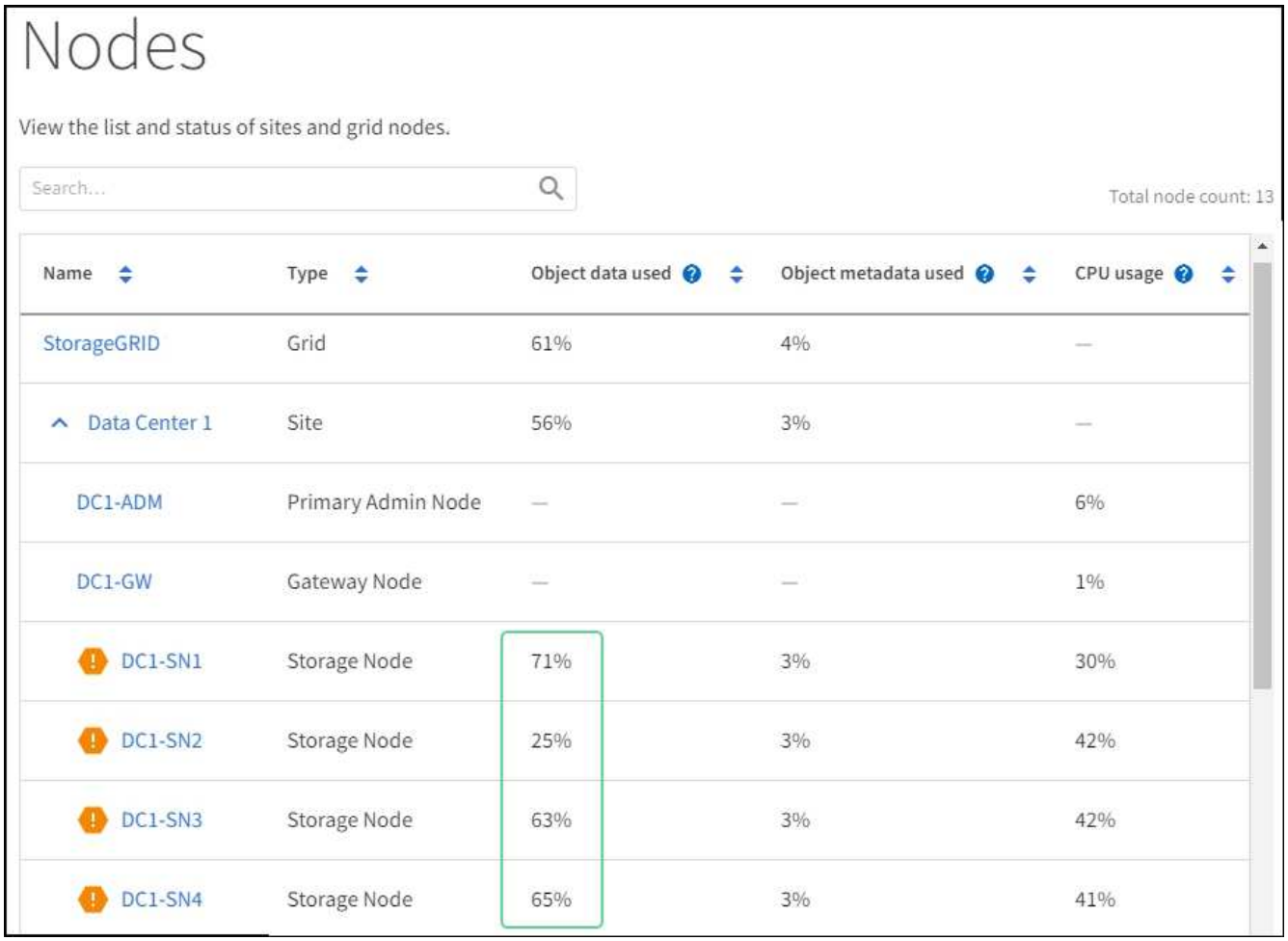
Sie können die Warnung **Niedriger schreibgeschützter Wasserzeichen-Override** beheben, indem Sie die benutzerdefinierten Wasserzeicheneinstellungen auf die neuen Wasserzeichen-Overrides aktualisieren. Wenn jedoch ein oder mehrere Speicherknoten fast voll sind oder Sie spezielle ILM-Anforderungen haben, sollten Sie sich zunächst die optimierten Speicherwasserzeichen ansehen und feststellen, ob deren Verwendung

sicher ist.

Bewerten Sie die Objektdatennutzung für das gesamte Raster

Schritte

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



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

Optimierte Speicherwasserzeichen anzeigen

StorageGRID verwendet zwei Prometheus-Metriken, um die optimierten Werte anzuzeigen, die es für das Soft Read-Only-Wasserzeichen des Speichervolumes berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

Schritte

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

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

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

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

Schritte

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

   Andernfalls erweitern Sie das Netz so schnell wie möglich. Entweder"Speichervolumes hinzufügen" zu einem bestehenden Knoten oder"neue Speicherknoten hinzufügen" . Gehen Sie dann zuVerwenden Sie optimierte Wasserzeichen um die Wasserzeicheneinstellungen zu aktualisieren.

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

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

Verwenden Sie optimierte Wasserzeichen

Schritte

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

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

Beheben von Metadatenproblemen

Wenn Metadatenprobleme auftreten, werden Sie durch Warnmeldungen über die Ursache der Probleme und empfohlene Maßnahmen informiert. Insbesondere müssen Sie neue Speicherknoten hinzufügen, wenn die Warnung „Geringer Metadatenspeicher“ ausgelöst wird.

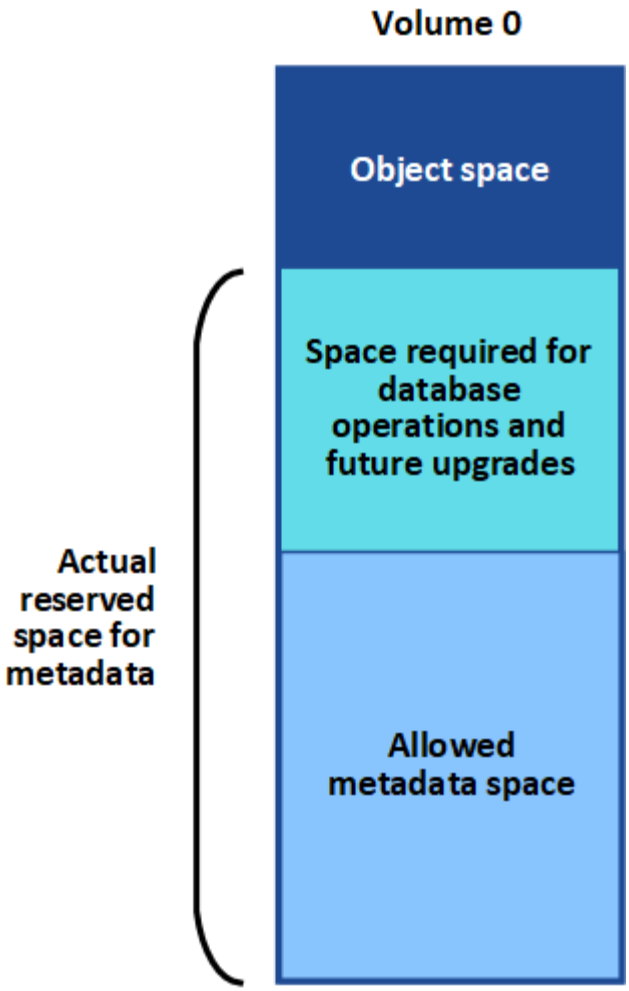
Bevor Sie beginnen

Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .

Informationen zu diesem Vorgang

Befolgen Sie die empfohlenen Maßnahmen für jede ausgelöste Metadatenwarnung. Wenn die Warnung **Geringer Metadatenspeicher** ausgelöst wird, müssen Sie neue Speicherknoten hinzufügen.

StorageGRID reserviert auf Volume 0 jedes Speicherknotens eine bestimmte Menge Speicherplatz für Objektmetadaten. Dieser Speicherplatz, der als *tatsächlich reservierter Speicherplatz* bezeichnet wird, ist unterteilt in den für Objektmetadaten zulässigen Speicherplatz (den zulässigen Metadatenspeicherplatz) und den für wesentliche Datenbankvorgänge wie Komprimierung und Reparatur erforderlichen Speicherplatz. Der zulässige Metadatenspeicherplatz bestimmt die Gesamtobjektkapazität.



Wenn Objektmetadaten mehr als 100 % des für Metadaten zulässigen Speicherplatzes beanspruchen, können Datenbankvorgänge nicht effizient ausgeführt werden und es treten Fehler auf.

Du kannst"Überwachen Sie die Objektmetadatenkapazität für jeden Speicherknoten" um Ihnen zu helfen, Fehler vorherzusehen und zu korrigieren, bevor sie auftreten.

StorageGRID verwendet die folgende Prometheus-Metrik, um zu messen, wie voll der zulässige Metadatenspeicher ist:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Wenn dieser Prometheus-Ausdruck bestimmte Schwellenwerte erreicht, wird die Warnung „Geringer Metadatenspeicher“ ausgelöst.

- **Geringfügig**: Objektmetadaten verwenden 70 % oder mehr des zulässigen Metadatenspeicherplatzes. Sie sollten so schnell wie möglich neue Speicherknoten hinzufügen.
- **Schwerwiegend**: Objektmetadaten verwenden 90 % oder mehr des zulässigen Metadatenspeichers. Sie müssen sofort neue Speicherknoten hinzufügen.

Wenn Objektmetadaten 90 % oder mehr des zulässigen Metadatenspeicherplatzes belegen, wird auf dem Dashboard eine Warnung angezeigt. Wenn diese Warnung erscheint, müssen Sie sofort neue Speicherknoten hinzufügen. Sie dürfen niemals zulassen, dass Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes belegen.

- **Kritisch**: Objektmetadaten verwenden 100 % oder mehr des zulässigen Metadatenspeicherplatzes und beginnen, den für wichtige Datenbankvorgänge erforderlichen Speicherplatz zu verbrauchen. Sie müssen die Aufnahme neuer Objekte stoppen und sofort neue Speicherknoten hinzufügen.

Wenn die Größe von Volume 0 kleiner ist als die Speicheroption „Reservierter Speicherplatz für Metadaten“ (z. B. in einer Nicht-Produktionsumgebung), ist die Berechnung für die Warnung „Geringer Metadatenspeicher“ möglicherweise ungenau.

Schritte

1. Wählen Sie **WARNUNGEN** > **Aktuell**.
2. Erweitern Sie in der Tabelle der Warnungen bei Bedarf die Warnungsgruppe **Geringer Metadatenspeicher** und wählen Sie die Warnung aus, die Sie anzeigen möchten.
3. Überprüfen Sie die Details im Warndialogfeld.
4. Wenn eine schwerwiegende oder kritische Warnung „Geringer Metadatenspeicher“ ausgelöst wurde, führen Sie sofort eine Erweiterung durch, um Speicherknoten hinzuzufügen.

Da StorageGRID an jedem Standort vollständige Kopien aller Objektmetadaten speichert, ist die Metadatenkapazität des gesamten Grids durch die Metadatenkapazität des kleinsten Standorts begrenzt. Wenn Sie die Metadatenkapazität einer Site erweitern müssen, sollten Sie auch"Erweitern Sie alle anderen Sites" durch die gleiche Anzahl von Speicherknoten.

Nachdem Sie die Erweiterung durchgeführt haben, verteilt StorageGRID die vorhandenen Objektmetadaten auf die neuen Knoten, wodurch die Gesamtmetadatenkapazität des Grids erhöht wird. Es ist keine Benutzeraktion erforderlich. Die Warnung **Geringer Metadatenspeicher** wird gelöscht.

Beheben von Zertifikatsfehlern

Wenn beim Versuch, über einen Webbrowser, einen S3-Client oder ein externes Überwachungstool eine Verbindung zu StorageGRID herzustellen, ein Sicherheits- oder Zertifikatsproblem auftritt, sollten Sie das Zertifikat überprüfen.

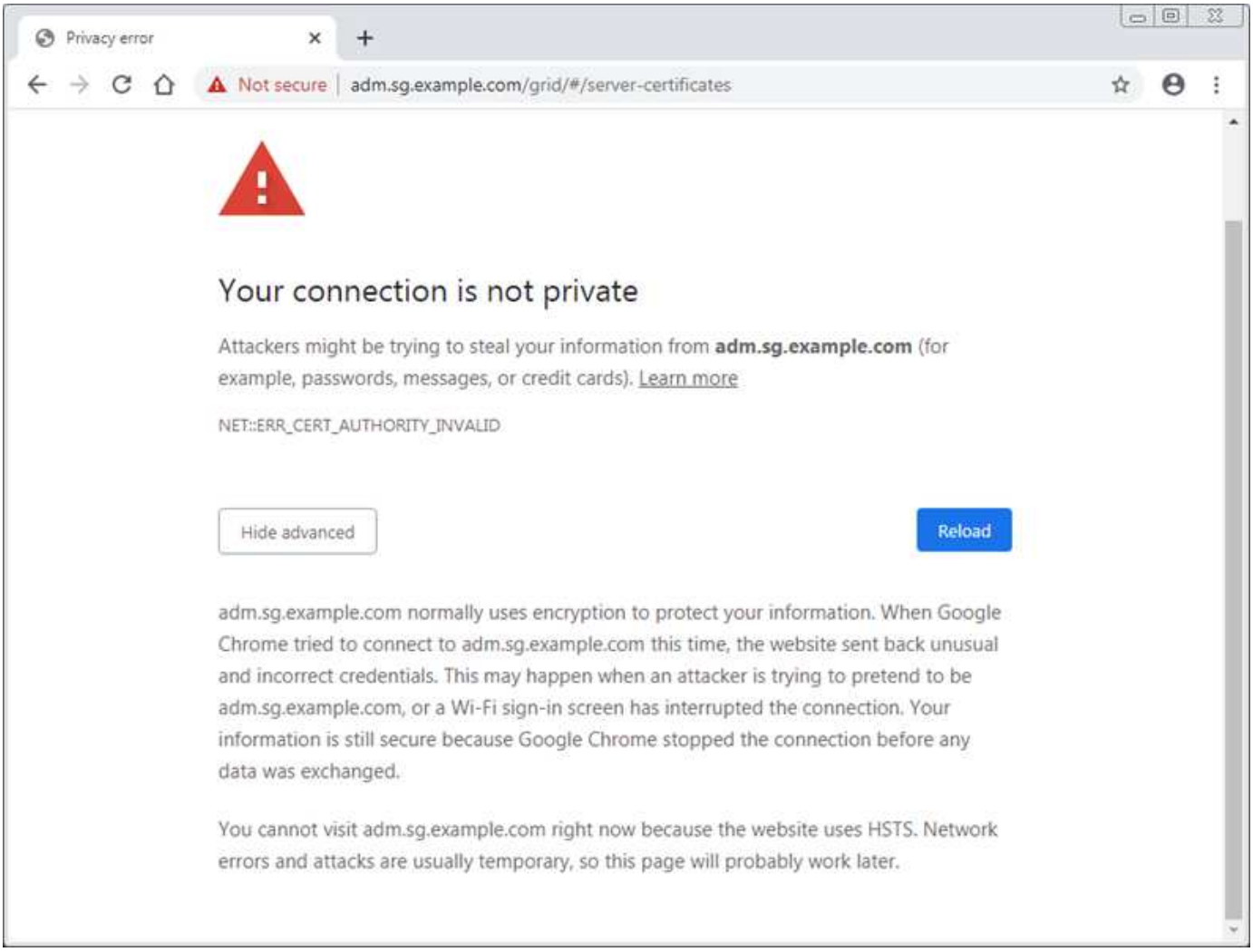
Informationen zu diesem Vorgang

Zertifikatsfehler können Probleme verursachen, wenn Sie versuchen, über den Grid Manager, die Grid Management API, den Tenant Manager oder die Tenant Management API eine Verbindung zu StorageGRID herzustellen. Zertifikatsfehler können auch auftreten, wenn Sie versuchen, eine Verbindung mit einem S3-Client oder einem externen Überwachungstool herzustellen.

Wenn Sie auf den Grid Manager oder Tenant Manager über einen Domänennamen statt einer IP-Adresse zugreifen, zeigt der Browser einen Zertifikatsfehler ohne Umgehungsoption an, wenn einer der folgenden Fälle eintritt:

- Ihr benutzerdefiniertes Verwaltungsschnittstellenzertifikat läuft ab.
- Sie kehren von einem benutzerdefinierten Verwaltungsschnittstellenzertifikat zum Standardserverzertifikat zurück.

Das folgende Beispiel zeigt einen Zertifikatsfehler, wenn das Zertifikat der benutzerdefinierten Verwaltungsschnittstelle abgelaufen ist:



Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn das Serverzertifikat bald abläuft.

Wenn Sie Client-Zertifikate für die externe Prometheus-Integration verwenden, können Zertifikatsfehler durch das Zertifikat der StorageGRID Verwaltungsschnittstelle oder durch Client-Zertifikate verursacht werden. Die Warnung **Ablauf der auf der Seite „Zertifikate“ konfigurierten Client-Zertifikate** wird ausgelöst, wenn ein Client-Zertifikat bald abläuft.

Schritte

Wenn Sie eine Warnmeldung über ein abgelaufenes Zertifikat erhalten haben, greifen Sie auf die Zertifikatsdetails zu: . Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann"Wählen Sie die entsprechende Zertifikatsregisterkarte aus" .

1. Überprüfen Sie die Gültigkeitsdauer des Zertifikats. + Einige Webbrowser und S3-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.
2. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein neues Zertifikat hoch oder generieren Sie ein neues.
    - Informationen zum Serverzertifikat finden Sie in den Schritten für"Konfigurieren eines

benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager" .

- Informationen zum Ein Client-Zertifikat finden Sie in den Schritten für"Konfigurieren eines Client-Zertifikats" .

3. Versuchen Sie bei Serverzertifikatsfehlern eine oder beide der folgenden Optionen:
   - Stellen Sie sicher, dass der Subject Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass der SAN mit der IP-Adresse oder dem Hostnamen des Knotens übereinstimmt, mit dem Sie eine Verbindung herstellen.
   - Wenn Sie versuchen, über einen Domänennamen eine Verbindung zu StorageGRID herzustellen:
     i. Geben Sie anstelle des Domänennamens die IP-Adresse des Admin-Knotens ein, um den Verbindungsfehler zu umgehen und auf den Grid Manager zuzugreifen.
     ii. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann"Wählen Sie die entsprechende Zertifikatsregisterkarte aus" um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
     iii. In den Anweisungen zur Verwaltung von StorageGRID finden Sie die Schritte für"Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager" .

Beheben von Problemen mit dem Admin-Knoten und der Benutzeroberfläche

Sie können verschiedene Aufgaben ausführen, um die Ursache von Problemen im Zusammenhang mit Admin-Knoten und der StorageGRID Benutzeroberfläche zu ermitteln.

Anmeldefehler beim Admin-Knoten

Wenn bei der Anmeldung bei einem StorageGRID Admin-Knoten ein Fehler auftritt, liegt möglicherweise ein Problem mit einem"Vernetzung" oder "Hardware" Problem, ein Problem mit"Admin-Knoten-Dienste" oder ein"Problem mit der Cassandra-Datenbank" auf verbundenen Speicherknoten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die `Passwords.txt` Datei.
- Du hast"spezifische Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Verwenden Sie diese Richtlinien zur Fehlerbehebung, wenn beim Versuch, sich bei einem Admin-Knoten anzumelden, eine der folgenden Fehlermeldungen angezeigt wird:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Schritte

1. Warten Sie 10 Minuten und versuchen Sie erneut, sich anzumelden.

   Wenn der Fehler nicht automatisch behoben wird, fahren Sie mit dem nächsten Schritt fort.

2. Wenn Ihr StorageGRID System über mehr als einen Admin-Knoten verfügt, versuchen Sie, sich von einem anderen Admin-Knoten aus beim Grid Manager anzumelden, um den Status eines nicht verfügbaren Admin-Knotens zu überprüfen.
   - Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **NODES**, **Alerts** und **SUPPORT** verwenden, um die Fehlerursache zu ermitteln.
   - Wenn Sie nur einen Admin-Knoten haben oder sich immer noch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Stellen Sie fest, ob die Hardware des Knotens offline ist.
4. Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, lesen Sie die Schritte für"Konfigurieren der einmaligen Anmeldung" .

   Möglicherweise müssen Sie SSO für einen einzelnen Admin-Knoten vorübergehend deaktivieren und erneut aktivieren, um etwaige Probleme zu beheben.

   > Wenn SSO aktiviert ist, können Sie sich nicht über einen eingeschränkten Port anmelden. Sie müssen Port 443 verwenden.

5. Stellen Sie fest, ob das von Ihnen verwendete Konto einem Verbundbenutzer gehört.

   Wenn das föderierte Benutzerkonto nicht funktioniert, versuchen Sie, sich beim Grid Manager als lokaler Benutzer, beispielsweise als Root, anzumelden.

   - Wenn sich der lokale Benutzer anmelden kann:
     i. Überprüfen Sie die Warnungen.
     ii. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Identitätsföderation**.
     iii. Klicken Sie auf **Verbindung testen**, um Ihre Verbindungseinstellungen für den LDAP-Server zu validieren.
     iv. Wenn der Test fehlschlägt, beheben Sie alle Konfigurationsfehler.
   - Wenn sich der lokale Benutzer nicht anmelden kann und Sie sicher sind, dass die Anmeldeinformationen korrekt sind, fahren Sie mit dem nächsten Schritt fort.
6. Verwenden Sie Secure Shell (ssh), um sich beim Admin-Knoten anzumelden:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

7. Zeigen Sie den Status aller auf dem Grid-Knoten ausgeführten Dienste an: `storagegrid-status`

   Stellen Sie sicher, dass alle NMS-, MI-, Nginx- und Mgmt-API-Dienste ausgeführt werden.

   Die Ausgabe wird sofort aktualisiert, wenn sich der Status eines Dienstes ändert.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Bestätigen Sie, dass der Dienst nginx-gw ausgeführt wird `# service nginx-gw status`
9. Verwenden Sie Lumberjack, um Protokolle zu sammeln: `# /usr/local/sbin/lumberjack.rb`

   Wenn die fehlgeschlagene Authentifizierung in der Vergangenheit aufgetreten ist, können Sie die Skriptoptionen --start und --end von Lumberjack verwenden, um den entsprechenden Zeitraum anzugeben. Verwenden Sie lumberjack -h, um Einzelheiten zu diesen Optionen zu erfahren.

   Die Ausgabe an das Terminal zeigt an, wohin das Protokollarchiv kopiert wurde.

10. Überprüfen Sie die folgenden Protokolle:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

- `**/*commands.txt`

11. Wenn Sie keine Probleme mit dem Admin-Knoten feststellen konnten, geben Sie einen der folgenden Befehle ein, um die IP-Adressen der drei Speicherknoten zu ermitteln, auf denen der ADC-Dienst an Ihrem Standort ausgeführt wird. Normalerweise sind dies die ersten drei Speicherknoten, die am Standort installiert wurden.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Admin-Knoten verwenden den ADC-Dienst während des Authentifizierungsprozesses.

12. Melden Sie sich vom Admin-Knoten aus per SSH bei jedem der ADC-Speicherknoten an, indem Sie die von Ihnen identifizierten IP-Adressen verwenden.
13. Zeigen Sie den Status aller auf dem Grid-Knoten ausgeführten Dienste an: `storagegrid-status`

    Stellen Sie sicher, dass alle Dienste idnt, acct, nginx und cassandra ausgeführt werden.

14. Schritte wiederholenVerwenden Sie Lumberjack, um Baumstämme zu sammeln UndProtokolle überprüfen um die Protokolle auf den Speicherknoten zu überprüfen.
15. Wenn Sie das Problem nicht lösen können, wenden Sie sich an den technischen Support.

    Stellen Sie dem technischen Support die gesammelten Protokolle zur Verfügung. Siehe auch "Referenz zu Protokolldateien".

Probleme mit der Benutzeroberfläche

Die Benutzeroberfläche für den Grid Manager oder den Tenant Manager reagiert nach der Aktualisierung der StorageGRID -Software möglicherweise nicht wie erwartet.

Schritte

1. Stellen Sie sicher, dass Sie ein"unterstützter Webbrowser" .
2. Leeren Sie den Cache Ihres Webbrowsers.

   Durch das Leeren des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID -Software verwendet wurden, und die Benutzeroberfläche kann wieder ordnungsgemäß funktionieren. Anweisungen finden Sie in der Dokumentation Ihres Webbrowsers.

Beheben von Netzwerk-, Hardware- und Plattformproblemen

Sie können verschiedene Aufgaben ausführen, um die Ursache von Problemen im Zusammenhang mit dem StorageGRID -Netzwerk, der Hardware und der Plattform zu ermitteln.

Fehler „422: Nicht verarbeitbare Entität“

Der Fehler 422: Unprocessable Entity kann aus verschiedenen Gründen auftreten. Überprüfen Sie die Fehlermeldung, um die Ursache Ihres Problems zu ermitteln.

Wenn Sie eine der aufgeführten Fehlermeldungen sehen, ergreifen Sie die empfohlene Maßnahme.

Fehlermeldung	Grundursache und Korrekturmaßnahmen

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires`
`binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Diese Meldung kann auftreten, wenn Sie beim Konfigurieren der Identitätsföderation mit Windows Active Directory (AD) die Option **TLS nicht verwenden** für Transport Layer Security (TLS) auswählen.
	
	Die Verwendung der Option **TLS nicht verwenden** wird für die Verwendung mit AD-Servern, die eine LDAP-Signatur erzwingen, nicht unterstützt. Sie müssen entweder die Option **STARTLS verwenden** oder die Option **LDAPS verwenden** für TLS auswählen.

Fehlermeldung	Grundursache und Korrekturmaßnahmen

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte Verschlüsselung zu verwenden, um eine Transport Layer Security (TLS)-Verbindung von StorageGRID zu einem externen System herzustellen, das zur Identifizierung der Föderation oder von Cloud-Speicherpools verwendet wird.
	
	Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eines der"Von StorageGRID unterstützte Chiffren" für ausgehende TLS-Verbindungen, wie in der Anleitung zur Administration von StorageGRID beschrieben.

MTU-Nichtübereinstimmungswarnung im Netznetzwerk

Die Warnung **MTU-Fehlanpassung im Grid-Netzwerk** wird ausgelöst, wenn die Einstellung der maximalen Übertragungseinheit (MTU) für die Grid-Netzwerkschnittstelle (eth0) zwischen den Knoten im Grid erheblich abweicht.

Informationen zu diesem Vorgang

Die Unterschiede in den MTU-Einstellungen könnten darauf hinweisen, dass einige, aber nicht alle eth0-Netzwerke für Jumbo Frames konfiguriert sind. Eine Nichtübereinstimmung der MTU-Größe von mehr als 1000 kann zu Problemen mit der Netzwerkleistung führen.

Schritte

1. Listen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
   - Verwenden Sie die im Grid Manager bereitgestellte Abfrage.
   - Navigieren Sie zu *`primary Admin Node IP address`*`/metrics/graph` und geben Sie die folgende Abfrage ein: `node_network_mtu_bytes{device="eth0"}`
2. "Ändern Sie die MTU-Einstellungen"nach Bedarf, um sicherzustellen, dass sie für die Grid-Netzwerkschnittstelle (eth0) auf allen Knoten gleich sind.
   - Verwenden Sie für Linux- und VMware-basierte Knoten den folgenden Befehl: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Beispiel: `change-ip.py -n node 1500 grid admin`

     Hinweis: Wenn auf Linux-basierten Knoten der gewünschte MTU-Wert für das Netzwerk im Container den bereits auf der Hostschnittstelle konfigurierten Wert überschreitet, müssen Sie zuerst die Hostschnittstelle so konfigurieren, dass sie den gewünschten MTU-Wert hat, und dann die `change-ip.py` Skript zum Ändern des MTU-Werts des Netzwerks im Container.

Verwenden Sie die folgenden Argumente zum Ändern der MTU auf Linux- oder VMware-basierten Knoten.

Positionsargumente	Beschreibung
`mtu`	Die einzustellende MTU. Muss im Bereich von 1280 bis 9216 liegen.
`network`	Die Netzwerke, auf die die MTU angewendet werden soll. Schließen Sie einen oder mehrere der folgenden Netzwerktypen ein: • Netz • Administrator • Kunde

+

Optionale Argumente	Beschreibung
`-h, – help`	Zeigen Sie die Hilfemeldung an und beenden Sie das Programm.
`-n node, --node node`	Der Knoten. Der Standard ist der lokale Knoten.

Knotennetzwerk-Empfangsframe-Fehlerwarnung

Fehler beim Empfang des Knotennetzwerk-Frames-Warnungen können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerkhardware verursacht werden. Diese Warnung wird von selbst gelöscht, nachdem das zugrunde liegende Problem behoben wurde.

Informationen zu diesem Vorgang

Fehler beim Empfang des Knotennetzwerk-Frames-Warnungen können durch die folgenden Probleme mit der Netzwerkhardware verursacht werden, die eine Verbindung zu StorageGRID herstellt:

- Vorwärtsfehlerkorrektur (FEC) ist erforderlich und wird nicht verwendet
- Switch-Port und NIC-MTU stimmen nicht überein
- Hohe Link-Fehlerraten
- NIC-Ringpufferüberlauf

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle möglichen Ursachen dieser Warnung in Ihrer Netzwerkkonfiguration.
2. Führen Sie je nach Fehlerursache folgende Schritte durch:

FEC-Fehlanpassung

Diese Schritte gelten nur für Warnungen vom Typ „Knotennetzwerk-Empfangsframefehler“*, die durch eine FEC-Nichtübereinstimmung auf StorageGRID -Geräten verursacht werden.

a. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID Gerät angeschlossen ist.
b. Überprüfen Sie die physische Integrität der Kabel vom Gerät zum Switch.
c. Wenn Sie die FEC-Einstellungen ändern möchten, um zu versuchen, die Warnung zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Link-Konfiguration“ des StorageGRID Appliance Installer für den Modus „**Auto**“ konfiguriert ist (siehe die Anweisungen für Ihr Gerät:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 und SG1100"
   - "SG100 und SG1000"
d. Ändern Sie die FEC-Einstellungen an den Switch-Ports. Die Ports der StorageGRID Appliance passen ihre FEC-Einstellungen nach Möglichkeit entsprechend an.

   Sie können keine FEC-Einstellungen auf StorageGRID -Geräten konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu ermitteln und zu spiegeln, mit denen sie verbunden sind. Wenn die Verbindungen auf Netzwerkgeschwindigkeiten von 25 GbE oder 100 GbE gezwungen werden, können Switch und NIC möglicherweise keine gemeinsame FEC-Einstellung aushandeln. Ohne eine gemeinsame FEC-Einstellung fällt das Netzwerk in den „No-FEC“-Modus zurück. Wenn FEC nicht aktiviert ist, sind die Verbindungen anfälliger für Fehler, die durch elektrisches Rauschen verursacht werden.

   StorageGRID Geräte unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie kein FEC.

Switch-Port und NIC-MTU stimmen nicht überein

Wenn die Warnung durch eine Nichtübereinstimmung von Switch-Port und NIC-MTU verursacht wird, überprüfen Sie, ob die auf dem Knoten konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port übereinstimmt.

Die auf dem Knoten konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung auf dem Switch-Port, mit dem der Knoten verbunden ist. Wenn ein StorageGRID Knoten einen Ethernet-Frame empfängt, der größer ist als seine MTU (was bei dieser Konfiguration möglich ist), wird möglicherweise die Warnung **Fehler beim Empfang des Frames im Knotennetzwerk** gemeldet. Wenn Sie glauben, dass dies der Fall ist, ändern Sie entweder die MTU des Switch-Ports, sodass sie mit der MTU der StorageGRID Netzwerkschnittstelle übereinstimmt, oder ändern Sie die MTU der StorageGRID -Netzwerkschnittstelle, sodass sie mit dem Switch-Port übereinstimmt, je nach Ihren End-to-End-MTU-Zielen oder -Anforderungen.

Für eine optimale Netzwerkleistung sollten alle Knoten mit ähnlichen MTU-Werten auf ihren Grid-Netzwerkschnittstellen konfiguriert werden. Die Warnung **MTU-Fehlanpassung des Grid-Netzwerks** wird ausgelöst, wenn es bei den MTU-Einstellungen für das Grid-Netzwerk auf einzelnen Knoten einen signifikanten Unterschied gibt. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein. Sehen Fehlerbehebung bei der Warnung „MTU-Fehlanpassung im Grid-Netzwerk“ für weitere Informationen.

Siehe auch "MTU-Einstellung ändern" .

Hohe Link-Fehlerraten

a. Aktivieren Sie FEC, falls noch nicht geschehen.
b. Stellen Sie sicher, dass Ihre Netzwerkverkabelung von guter Qualität ist und nicht beschädigt oder falsch angeschlossen ist.
c. Wenn die Kabel nicht das Problem zu sein scheinen, wenden Sie sich an den technischen Support.

In einer Umgebung mit starkem elektrischen Rauschen stellen Sie möglicherweise hohe Fehlerraten fest.

NIC-Ringpufferüberlauf

Wenn der Fehler auf einen Überlauf des NIC-Ringpuffers zurückzuführen ist, wenden Sie sich an den technischen Support.

Der Ringpuffer kann überlaufen, wenn das StorageGRID -System überlastet ist und Netzwerk-Ereignisse nicht rechtzeitig verarbeiten kann.

3. Beobachten Sie das Problem und wenden Sie sich an den technischen Support, wenn die Warnung nicht behoben wird.

Zeitsynchronisierungsfehler

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

Wenn bei der Zeitsynchronisierung Probleme auftreten, überprüfen Sie, ob Sie mindestens vier externe NTP-Quellen angegeben haben, die jeweils eine Stratum 3-Referenz oder besser bereitstellen, und ob alle externen NTP-Quellen normal funktionieren und von Ihren StorageGRID Knoten aus zugänglich sind.

Wann"Angabe der externen NTP-Quelle" Verwenden Sie für eine StorageGRID Installation auf Produktionsebene den Windows-Zeitdienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016. Der Zeitdienst früherer Windows-Versionen ist nicht genau genug und wird von Microsoft für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, nicht unterstützt.

Linux: Probleme mit der Netzwerkverbindung

Möglicherweise treten Probleme mit der Netzwerkkonnektivität für StorageGRID -Knoten auf, die auf Linux-Hosts gehostet werden.

Klonen von MAC-Adressen

In einigen Fällen können Netzwerkprobleme durch das Klonen von MAC-Adressen gelöst werden. Wenn Sie virtuelle Hosts verwenden, setzen Sie den Wert des MAC-Adressklonschlüssels für jedes Ihrer Netzwerke in Ihrer Knotenkonfigurationsdatei auf „true“. Diese Einstellung bewirkt, dass die MAC-Adresse des StorageGRID -Containers die MAC-Adresse des Hosts verwendet. Informationen zum Erstellen von Knotenkonfigurationsdateien finden Sie in den Anweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" .

> Erstellen Sie separate virtuelle Netzwerkschnittstellen zur Verwendung durch das Linux-Hostbetriebssystem. Die Verwendung derselben Netzwerkschnittstellen für das Linux-Hostbetriebssystem und den StorageGRID Container kann dazu führen, dass das Hostbetriebssystem nicht mehr erreichbar ist, wenn der Promiscuous-Modus auf dem Hypervisor nicht aktiviert wurde.

Weitere Informationen zum Aktivieren des MAC-Klonens finden Sie in den Anweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" .

Promiscuous-Modus

Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen das Empfangen und Senden von Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen erlauben möchten, stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppe für den Promiscuous-Modus, MAC-Adressänderungen und gefälschte Übertragungen auf **Akzeptieren** eingestellt sind. Die auf dem virtuellen Switch festgelegten Werte können durch die Werte auf Portgruppenebene überschrieben werden. Stellen Sie daher sicher, dass die Einstellungen an beiden Stellen identisch sind.

Weitere Informationen zur Verwendung des Promiscuous-Modus finden Sie in den Anweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" .

Linux: Knotenstatus ist „verwaist“

Ein Linux-Knoten in einem verwaisten Zustand weist normalerweise darauf hin, dass entweder der StorageGrid-Dienst oder der StorageGRID -Knoten-Daemon, der den Container des Knotens steuert, unerwartet beendet wurde.

Informationen zu diesem Vorgang

Wenn ein Linux-Knoten meldet, dass er sich in einem verwaisten Zustand befindet, sollten Sie:

- Überprüfen Sie die Protokolle auf Fehler und Nachrichten.
- Versuchen Sie, den Knoten erneut zu starten.
- Verwenden Sie bei Bedarf Container-Engine-Befehle, um den vorhandenen Knotencontainer zu stoppen.
- Starten Sie den Knoten neu.

Schritte

1. Überprüfen Sie die Protokolle sowohl für den Service-Daemon als auch für den verwaisten Knoten auf offensichtliche Fehler oder Meldungen über ein unerwartetes Beenden.
2. Melden Sie sich beim Host als Root oder mit einem Konto mit Sudo-Berechtigung an.
3. Versuchen Sie, den Knoten erneut zu starten, indem Sie den folgenden Befehl ausführen: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Wenn der Knoten verwaist ist, lautet die Antwort

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Stoppen Sie unter Linux die Container-Engine und alle steuernden StorageGrid-Node-Prozesse. Beispiel: `sudo docker stop --time secondscontainer-name`

   Für `seconds` Geben Sie die Anzahl der Sekunden ein, die Sie warten möchten, bis der Container stoppt (normalerweise 15 Minuten oder weniger). Beispiel:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Starten Sie den Knoten neu: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Fehlerbehebung bei der IPv6-Unterstützung

Möglicherweise müssen Sie die IPv6-Unterstützung im Kernel aktivieren, wenn Sie StorageGRID -Knoten auf Linux-Hosts installiert haben und feststellen, dass den Knotencontainern nicht wie erwartet IPv6-Adressen zugewiesen wurden.

Informationen zu diesem Vorgang

So zeigen Sie die einem Grid-Knoten zugewiesene IPv6-Adresse an:

1. Wählen Sie **NODES** und wählen Sie den Knoten aus.
2. Wählen Sie auf der Registerkarte „Übersicht“ neben „IP-Adressen“ die Option „Zusätzliche IP-Adressen anzeigen“ aus.

Wenn die IPv6-Adresse nicht angezeigt wird und der Knoten auf einem Linux-Host installiert ist, führen Sie diese Schritte aus, um die IPv6-Unterstützung im Kernel zu aktivieren.

Schritte

1. Melden Sie sich beim Host als Root oder mit einem Konto mit Sudo-Berechtigung an.
2. Führen Sie den folgenden Befehl aus: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Das Ergebnis sollte 0 sein.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

Wenn das Ergebnis nicht 0 ist, lesen Sie in der Dokumentation Ihres Betriebssystems nach, um `sysctl` Einstellungen. Ändern Sie dann den Wert auf 0, bevor Sie fortfahren.

3. Geben Sie den StorageGRID -Knotencontainer ein: `storagegrid node enter node-name`
4. Führen Sie den folgenden Befehl aus: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Das Ergebnis sollte 1 sein.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

Wenn das Ergebnis nicht 1 ist, gilt dieses Verfahren nicht. Wenden Sie sich an den technischen Support.

5. Verlassen Sie den Container: `exit`

```
root@DC1-S1:~ # exit
```

6. Bearbeiten Sie als Root die folgende Datei: `/var/lib/storagegrid/settings/sysctl.d/net.conf` .

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Suchen Sie die folgenden zwei Zeilen und entfernen Sie die Kommentar-Tags. Speichern und schließen Sie dann die Datei.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Führen Sie diese Befehle aus, um den StorageGRID Container neu zu starten:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Fehlerbehebung bei einem externen Syslog-Server

In der folgenden Tabelle werden die Fehlermeldungen beschrieben, die bei der Verwendung eines externen Syslog-Servers auftreten können, und es werden Korrekturmaßnahmen aufgelistet.

Diese Fehler werden vom Assistenten „Externen Syslog-Server konfigurieren“ angezeigt, wenn beim Senden von Testnachrichten zur Überprüfung der korrekten Konfiguration des externen Syslog-Servers Probleme auftreten.

Probleme zur Laufzeit können gemeldet werden durch"Fehler bei der Weiterleitung des externen Syslog-Servers" Alarm. Wenn Sie diese Warnung erhalten, befolgen Sie die Anweisungen in der Warnung, um die Testnachrichten erneut zu senden, damit Sie detaillierte Fehlermeldungen erhalten.

Weitere Informationen zum Senden von Audit-Informationen an einen externen Syslog-Server finden Sie unter:

- "Überlegungen zur Verwendung eines externen Syslog-Servers"
- "Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server"

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Kann den Hostnamen nicht auflösen	Der von Ihnen für den Syslog-Server eingegebene FQDN konnte nicht in eine IP-Adresse aufgelöst werden. 1. Überprüfen Sie den eingegebenen Hostnamen. Wenn Sie eine IP-Adresse eingegeben haben, stellen Sie sicher, dass es sich um eine gültige IP-Adresse in WXYZ-Notation („dotted decimal“) handelt. 2. Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind. 3. Bestätigen Sie, dass jeder Knoten auf die IP-Adressen für den DNS-Server zugreifen kann.
Verbindung abgelehnt	Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde abgelehnt. Möglicherweise lauscht kein Dienst auf dem TCP- oder TLS-Port des Hosts oder eine Firewall blockiert den Zugriff. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 2. Vergewissern Sie sich, dass auf dem Host für den Syslog-Dienst ein Syslog-Daemon ausgeführt wird, der den angegebenen Port überwacht. 3. Stellen Sie sicher, dass der Zugriff auf TCP/TLS-Verbindungen von den Knoten zur IP und zum Port des Syslog-Servers nicht durch eine Firewall blockiert wird.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Netzwerk nicht erreichbar	Der Syslog-Server befindet sich nicht in einem direkt angeschlossenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass er die Testnachrichten von den aufgelisteten Knoten nicht an den Syslog-Server weiterleiten konnte. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Knoten die Grid-Netzwerk-Subnetzliste, die Admin-Netzwerk-Subnetzlisten und die Client-Netzwerk-Gateways. Bestätigen Sie, dass diese so konfiguriert sind, dass der Datenverkehr über die erwartete Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) an den Syslog-Server weitergeleitet wird.
Host nicht erreichbar	Der Syslog-Server befindet sich in einem direkt angeschlossenen Subnetz (Subnetz, das von den aufgelisteten Knoten für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Knoten versuchten, Testnachrichten zu senden, erhielten jedoch keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie, ob der Host, auf dem der Syslog-Dienst ausgeführt wird, aktiv ist.
Verbindungs-Timeout	Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber vom Syslog-Server wurde lange Zeit keine Antwort empfangen. Möglicherweise liegt eine Routing-Fehlkonfiguration vor oder eine Firewall blockiert den Datenverkehr, ohne eine Antwort zu senden (eine häufige Konfiguration). 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Knoten die Grid-Netzwerk-Subnetzliste, die Admin-Netzwerk-Subnetzlisten und die Client-Netzwerk-Gateways. Bestätigen Sie, dass diese so konfiguriert sind, dass der Datenverkehr über die Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) an den Syslog-Server weitergeleitet wird, über die der Syslog-Server Ihrer Meinung nach erreicht werden soll. 3. Vergewissern Sie sich, dass der Zugriff auf TCP/TLS-Verbindungen von den aufgelisteten Knoten zur IP und zum Port des Syslog-Servers nicht durch eine Firewall blockiert wird.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Verbindung vom Partner geschlossen	Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, später jedoch geschlossen. Gründe hierfür können sein: • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gebootet. • Der Knoten und der Syslog-Server haben möglicherweise unterschiedliche TCP/TLS-Einstellungen. • Eine zwischengeschaltete Firewall schließt möglicherweise inaktive TCP-Verbindungen. • Ein Nicht-Syslog-Server, der den Syslog-Server-Port überwacht, hat möglicherweise die Verbindung geschlossen. So beheben Sie dieses Problem: 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 2. Wenn Sie TLS verwenden, stellen Sie sicher, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 3. Stellen Sie sicher, dass keine zwischengeschaltete Firewall so konfiguriert ist, dass sie inaktive TCP-Verbindungen schließt.
TLS-Zertifikatfehler	Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen bereitgestellten CA-Zertifikatpaket und Client-Zertifikat kompatibel. 1. Bestätigen Sie, dass das CA-Zertifikatpaket und das Client-Zertifikat (sofern vorhanden) mit dem Server-Zertifikat auf dem Syslog-Server kompatibel sind. 2. Bestätigen Sie, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Weiterleitung ausgesetzt	Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet und StorageGRID kann den Grund dafür nicht erkennen. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugprotokolle, um die Grundursache zu ermitteln.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
TLS-Sitzung beendet	Der Syslog-Server hat die TLS-Sitzung beendet und StorageGRID kann den Grund nicht erkennen. 1. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugprotokolle, um die Grundursache zu ermitteln. 2. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 3. Wenn Sie TLS verwenden, stellen Sie sicher, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 4. Bestätigen Sie, dass das CA-Zertifikatpaket und das Client-Zertifikat (sofern vorhanden) mit dem Server-Zertifikat des Syslog-Servers kompatibel sind. 5. Bestätigen Sie, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Ergebnisabfrage fehlgeschlagen	Der für die Konfiguration und das Testen des Syslog-Servers verwendete Admin-Knoten kann keine Testergebnisse von den aufgelisteten Knoten anfordern. Möglicherweise sind ein oder mehrere Knoten ausgefallen. 1. Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Dienste ausgeführt werden. 2. Starten Sie den Miscd-Dienst auf den aufgelisteten Knoten neu.