



Fehler in einem StorageGRID System beheben

StorageGRID

NetApp
October 03, 2025

Inhalt

Fehler in einem StorageGRID System beheben	1
Fehler in einem StorageGRID System beheben	1
Überblick über die Problembestimmung	1
Behebung von Objekt- und Storage-Problemen	11
Bestätigen Sie den Speicherort der Objektdaten	11
Fehler beim Objektspeicher (Storage Volume)	13
Überprüfen Sie die Objektintegrität	15
Fehlerbehebung bei verlorenen und fehlenden Objektdaten	23
Beheben Sie die Warnung „Niedrig Object Data Storage“	35
Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff	37
Fehlersuche im SSTS-Alarm (Storage Status) durchführen	41
Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm)	45
Behebung von Metadatenproblemen	46
Beheben Sie die Warnmeldung zu niedrigen Metadaten-Storage	46
Fehlersuche im Alarm Services: Status - Cassandra (SVST) durchführen	48
Fehlerbehebung bei Cassandra-Fehlern außerhalb des Speichers (SMTT-Alarm)	52
Fehlerbehebung bei Zertifikatfehlern	53
Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche	54
Fehler bei der Anmeldung beheben	54
Fehlerbehebung bei Problemen mit der Benutzeroberfläche	58
Überprüfen Sie den Status eines nicht verfügbaren Admin-Knotens	58
Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen	58
Fehler bei „422: Unbearbeitbare Einheit“ beheben	59
Fehlerbehebung bei der MTU-Warnung für das Grid Network	60
Beheben Sie die Fehlerbehebung im NRER-Alarm (Network Receive Error)	61
Fehler bei der Zeitsynchronisierung beheben	63
Linux: Probleme mit der Netzwerkverbindung	63
Linux: Node-Status lautet „verwaiste“	64
Linux: Fehlerbehebung bei der IPv6-Unterstützung	65
Fehlerbehebung für einen externen Syslog-Server	67

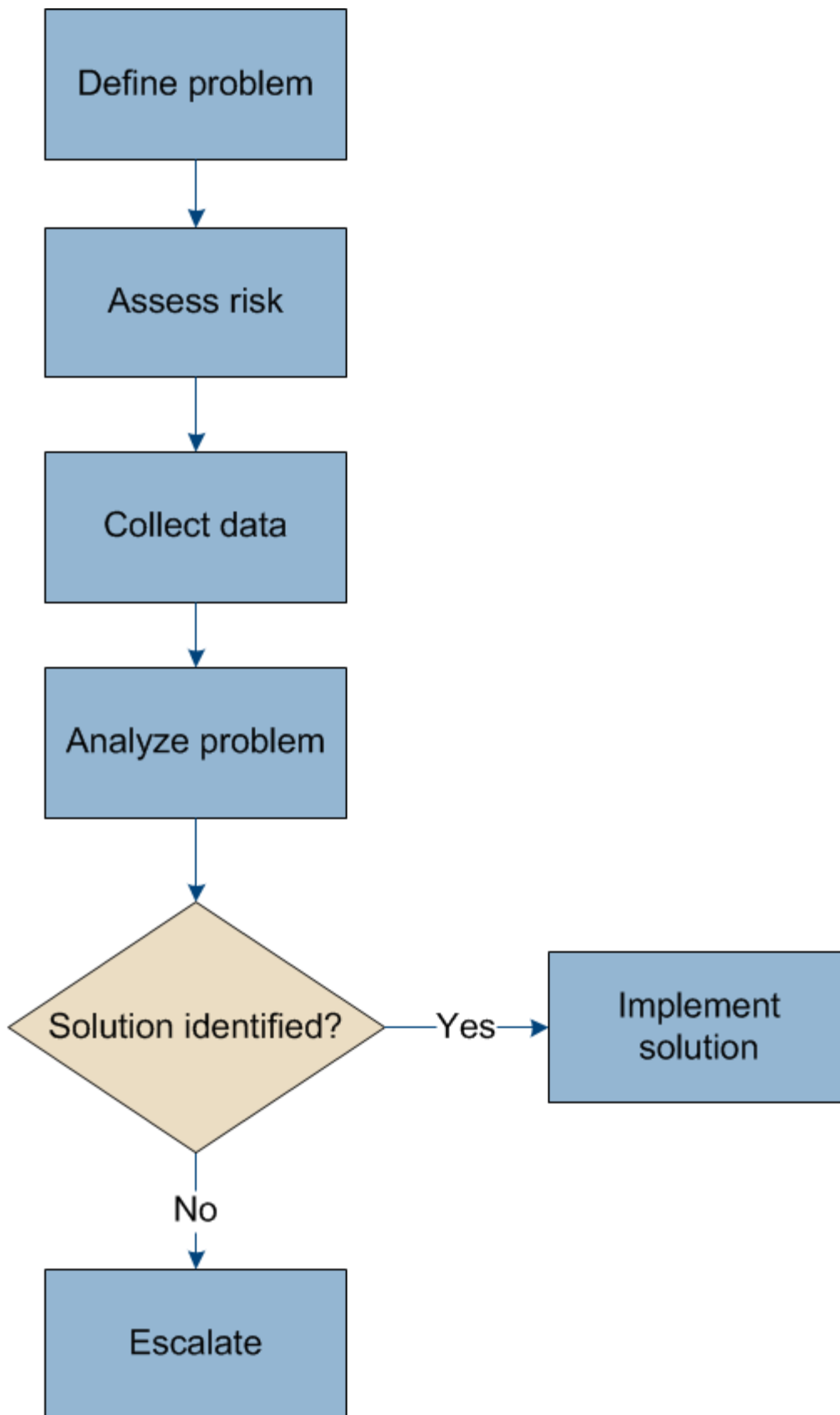
Fehler in einem StorageGRID System beheben

Fehler in einem StorageGRID System beheben

Wenn bei der Verwendung eines StorageGRID-Systems ein Problem auftritt, finden Sie in den Tipps und Richtlinien dieses Abschnitts Hilfe zum ermitteln und Beheben des Problems.

Überblick über die Problembestimmung

Wenn bei Ihnen ein Problem auftritt [Verwalten eines StorageGRID-Systems](#), Sie können den in dieser Abbildung beschriebenen Prozess verwenden, um das Problem zu identifizieren und zu analysieren. In vielen Fällen können Sie Probleme selbstständig lösen. In diesem Fall müssen Sie jedoch einige Probleme an den technischen Support eskalieren.



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 erfassen können, um ein Problem zu definieren:

Frage	Beispielantwort
Was macht das StorageGRID-System? Was sind die Symptome?	Client-Applikationen melden, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann hat das Problem begonnen?	Die Objektaufnahme wurde am 8. Januar 2020 um 14:50 Uhr verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Durch Client-Anwendung benachrichtigt. Auch Benachrichtigung per E-Mail erhalten.
Tritt das Problem konsequent oder nur in manchen Fällen auf?	Das Problem ist noch nicht behoben.
Wenn das Problem regelmäßig auftritt, welche Schritte dazu führen, 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 Zeiten der einzelnen Vorfälle, die Sie kennen.	Das Problem ist nicht intermittierend.
Haben Sie dieses Problem schon einmal gesehen? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dies ist das erste Mal, dass ich dieses Thema gesehen habe.

Bewerten Sie das Risiko und die Auswirkungen auf das System

Bewerten Sie nach Definition des Problems sein Risiko und die Auswirkungen auf das StorageGRID System. Beispielsweise bedeutet das Vorhandensein kritischer Warnmeldungen nicht zwangsläufig, dass das System keine Kernservices liefert.

In dieser Tabelle sind die Auswirkungen eines Beispielproblems auf Systemvorgänge zusammengefasst:

Frage	Beispielantwort
Kann das StorageGRID System Inhalte aufnehmen?	Nein
Können Client-Anwendungen Inhalte abrufen?	Einige Objekte können abgerufen werden, andere können nicht.
Sind Daten gefährdet?	Nein
Ist die Fähigkeit, Geschäfte zu führen, stark beeinträchtigt?	Ja, da Client-Applikationen keine Objekte auf dem StorageGRID System speichern und Daten nicht konsistent abgerufen werden können.

Datenerfassung

Nach der Definition des Problems und der Bewertung der Risiken und Auswirkungen können Sie Daten zur Analyse sammeln. Die Art der Daten, die am nützlichsten zu erfassen sind, hängt von der Art des Problems ab.

Art der zu erfassenden Daten	Warum diesen Dat sammeln	Anweisungen
Zeitplan der neuesten Änderungen erstellen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	<ul style="list-style-type: none">• Erstellen Sie eine Zeitleiste der neuesten Änderungen
Prüfen von Warnungen und Alarmen	<p>Mithilfe von Warnfunktionen und Alarmen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme geben.</p> <p>Überprüfen Sie die Liste der aktuellen Warnungen und Alarme, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat.</p> <p>Prüfen Sie die in der Vergangenheit ausgelösten Warnmeldungen und Alarme, um zusätzliche Einblicke zu erhalten.</p>	<ul style="list-style-type: none">• Anzeigen aktueller Warnmeldungen• Anzeigen von älteren Alarmen• Anzeigen von behobenen Warnmeldungen• Prüfen historischer Alarme und Alarmfrequenz (altes System)
Monitoring von Ereignissen	Ereignisse umfassen Systemfehler oder Fehlerereignisse für einen Node, einschließlich Fehler wie Netzwerkfehler. Überwachen Sie Ereignisse, um weitere Informationen zu Problemen zu erhalten oder um Hilfe bei der Fehlerbehebung zu erhalten.	<ul style="list-style-type: none">• Monitoring von Ereignissen
Identifizieren von Trends mithilfe von Diagrammen und Textberichten	Trends liefern wertvolle Hinweise darauf, wann Probleme zuerst auftraten, und können Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	<ul style="list-style-type: none">• Verwenden Sie Diagramme und Diagramme• Verwenden Sie Textberichte
Basispläne erstellen	Sammeln von Informationen über die normalen Stufen verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Grundlinien können wertvolle Hinweise liefern.	<ul style="list-style-type: none">• Basispläne erstellen
Durchführen von Einspeisung und Abruf von Tests	Zur Fehlerbehebung von Performance-Problemen bei Aufnahme und Abruf können Objekte auf einer Workstation gespeichert und abgerufen werden. Vergleichen Sie die Ergebnisse mit denen, die bei der Verwendung der Client-Anwendung angezeigt werden.	<ul style="list-style-type: none">• PUT- und GET-Performance werden überwacht

Art der zu erfassenden Daten	Warum diesen Dat sammeln	Anweisungen
Audit-Meldungen prüfen	Überprüfen Sie Audit-Meldungen, um StorageGRID Vorgänge im Detail zu befolgen. Die Details in Audit-Meldungen können bei der Behebung vieler Arten von Problemen, einschließlich von Performance-Problemen, nützlich sein.	<ul style="list-style-type: none"> • Audit-Meldungen prüfen
Überprüfen Sie Objektstandorte und Storage-Integrität	Wenn Sie Speicherprobleme haben, stellen Sie sicher, dass Objekte an der gewünschten Stelle platziert werden. Überprüfen Sie die Integrität von Objektdaten auf einem Storage-Node.	<ul style="list-style-type: none"> • Überwachen von Objektverifizierungsvorgängen • Bestätigen Sie den Speicherort der Objektdaten • Überprüfen Sie die Objektintegrität
Datenerfassung für technischen Support	Vom technischen Support werden Sie möglicherweise aufgefordert, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um Probleme zu beheben.	<ul style="list-style-type: none"> • Erfassen von Protokolldateien und Systemdaten • Senden Sie manuell eine AutoSupport Meldung aus • Prüfen von Support-Kennzahlen

Erstellen Sie eine Zeitleiste der neuesten 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.
- Durch eine Zeitleiste von Änderungen können Sie feststellen, welche Änderungen für ein Problem verantwortlich sein könnten und wie jede Änderung ihre Entwicklung beeinflusst haben könnte.

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann jede Änderung stattgefunden hat und welche relevanten Details über die Änderung angezeigt werden, und Informationen darüber, was während der Änderung noch passiert ist:

Zeit der Änderung	Art der Änderung	Details
<p>Beispiel:</p> <ul style="list-style-type: none"> • Wann haben Sie die Node-Wiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Prozess unterbrochen? 	<p>Was ist los? Was haben Sie gemacht?</p>	<p>Dokumentieren Sie alle relevanten Details zu der Änderung. Beispiel:</p> <ul style="list-style-type: none"> • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Änderungen bei Client-Workloads <p>Achten Sie darauf, zu beachten, ob mehrere Änderungen gleichzeitig durchgeführt wurden. Wurde diese Änderung beispielsweise vorgenommen, während ein Upgrade durchgeführt wurde?</p>

Beispiele für signifikante aktuelle Änderungen

Hier einige Beispiele für potenziell signifikante Änderungen:

- Wurde das StorageGRID System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde kürzlich ein Upgrade des Systems durchgeführt? Wurde ein Hotfix angewendet?
- Wurde irgendeine Hardware in letzter Zeit repariert oder geändert?
- Wurde die ILM-Richtlinie aktualisiert?
- Hat sich der Client-Workload geändert?
- Hat sich die Client-Applikation oder deren Verhalten geändert?
- Haben Sie den Lastausgleich geändert oder eine Hochverfügbarkeitsgruppe aus Admin-Nodes oder Gateway-Nodes hinzugefügt oder entfernt?
- Wurden Aufgaben gestartet, die ein sehr langer Zeitaufwand beanspruchen können? Beispiele:
 - Wiederherstellung eines fehlerhaften Speicherknotens
 - Ausmusterung von Storage-Nodes
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, beispielsweise beim Hinzufügen eines Mandanten oder bei der Änderung der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattform-Services kürzlich aktiviert oder geändert?
- Wurde die Compliance in letzter Zeit aktiviert?
- Wurden Cloud-Storage-Pools hinzugefügt oder entfernt?
- Wurden Änderungen an der Storage-Komprimierung oder -Verschlüsselung vorgenommen?
- Wurden Änderungen an der Netzwerkinfrastruktur vorgenommen? Beispiel: VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?
- Wurden Konfigurationsänderungen am Archiv-Node vorgenommen?

- Wurden weitere Änderungen am StorageGRID System bzw. an der zugehörigen Umgebung vorgenommen?

]Basispläne erstellen

Sie können Basislinien für Ihr System einrichten, indem Sie die normalen Ebenen verschiedener Betriebswerte erfassen. In Zukunft können Sie aktuelle Werte mit diesen Basiswerten vergleichen, um ungewöhnliche Werte zu erkennen und zu beheben.

Eigenschaft	Wert	Wie zu erhalten
Durchschnittlicher Storage-Verbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	<p>Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher.</p> <p>Suchen Sie im Diagramm Speicher verwendet - Objektdaten einen Zeitraum, in dem die Linie ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Storage täglich belegt wird</p> <p>Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.</p>
Durchschnittlicher Metadatenverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	<p>Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher.</p> <p>Suchen Sie im Diagramm „verwendete Speicher - Objektmetadaten“ einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Metadaten-Storage jeden Tag belegt wird</p> <p>Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.</p>

Eigenschaft	Wert	Wie zu erhalten
Geschwindigkeit von S3/Swift Operationen	Vorgänge/Sekunde	<p>Wechseln Sie im Grid Manager zum Fenster Dashboard. Sehen Sie sich im Abschnitt Protokollvorgänge die Werte für die S3-Rate und die Swift-Rate an.</p> <p>Wählen Sie NODES site oder Storage Node Objects aus, um die Einspeisungs- und Abrufraten und Zählungen für einen bestimmten Standort oder Knoten anzuzeigen. Halten Sie den Mauszeiger über das Diagramm Aufnahme und Abruf für S3 oder Swift.</p>
S3/Swift-Vorgänge sind fehlgeschlagen	Betrieb	Wählen Sie SUPPORT Tools Grid-Topologie aus. Zeigen Sie auf der Registerkarte Übersicht im Abschnitt API-Vorgänge den Wert für S3-Operationen an – Fehlgeschlagen oder Swift-Vorgänge – Fehlgeschlagen.
ILM-Auswertungsrates	Objekte/Sekunde	<p>Wählen Sie auf der Seite Knoten GRID ILM aus.</p> <p>Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um einen Basiswert für Evaluierungsrate für Ihr System zu schätzen.</p>
ILM-Scan-Rate	Objekte/Sekunde	<p>Wählen Sie NODES Grid ILM aus.</p> <p>Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basiswert für Scanrate für Ihr System zu schätzen.</p>

Eigenschaft	Wert	Wie zu erhalten
Objekte, die sich aus Client-Vorgängen in Warteschlange befinden	Objekte/Sekunde	Wählen Sie NODES Grid ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um einen Basiswert für Objekte in der Warteschlange (aus Client-Operationen) für Ihr System zu schätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie NODES Storage Node Objekte aus. Zeigen Sie in der Tabelle Abfragen den Wert für durchschnittliche Latenz an.

Analysieren von Daten


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


Die Analyse ist Problem-abhängig, aber im Allgemeinen:


- Erkennen von Fehlerpunkten und Engpässen mithilfe der Alarme.
- Rekonstruieren Sie den Problemverlauf mithilfe der Alarmhistorie und -Diagramme.
- Verwenden Sie Diagramme, um Anomalien zu finden und die Problemsituation mit dem normalen Betrieb 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, müssen Sie die in der folgenden Tabelle aufgeführten Informationen zur Erleichterung der Problembehebung nutzen.

	Element	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann hat das Problem begonnen? Passiert es konsequent oder intermittierend? Welche Zeiten hat es gelegentlich gegeben? Definieren Sie das Problem

	Element	Hinweise
	Folgenabschätzung	<p>Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation?</p> <ul style="list-style-type: none"> • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	Wählen Sie WARTUNG System Lizenz . Die StorageGRID System-ID wird im Rahmen der aktuellen Lizenz angezeigt.
	Softwareversion	Wählen Sie oben im Grid Manager das Hilfesymbol aus, und wählen Sie über , um die StorageGRID-Version anzuzeigen.
	Anpassbarkeit	<p>Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf:</p> <ul style="list-style-type: none"> • Verwendet das Grid Storage-Komprimierung, Storage-Verschlüsselung oder Compliance? • Erstellt ILM replizierte oder Erasure Coding Objekte? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das strenge, ausgewogene oder duale Ingest-Verhalten?
	Log-Dateien und Systemdaten	<p>Erfassen von Protokolldateien und Systemdaten für Ihr System Wählen Sie SUPPORT Tools Logs.</p> <p>Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln.</p> <p>Wenn Sie Protokolle nur für ausgewählte Knoten erfassen, müssen Sie mindestens einen Speicherknoten mit dem ADC-Service einschließen. (Die ersten drei Storage-Nodes an einem Standort enthalten den ADC-Service.)</p> <p>Erfassen von Protokolldateien und Systemdaten</p>
	Basisinformationen	<p>Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch</p> <p>Basispläne erstellen</p>

	Element	Hinweise
	Zeitachse der letzten Änderungen	Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind. Erstellen Sie eine Zeitleiste der neuesten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie Schritte zur Diagnose oder Behebung des Problems selbst ergriffen haben, achten Sie darauf, die Schritte und das Ergebnis zu notieren.

Behebung von Objekt- und Storage-Problemen

Bestätigen Sie den Speicherort der Objektdaten

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

Was Sie benötigen

- Sie müssen über eine Objektkennung verfügen, die einer der folgenden sein kann:
 - **UUID:** Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.
 - **CBID:** Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in allen Großbuchstaben ein.
 - **S3-Bucket und Objektschlüssel:** Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
 - **Swift Container und Objektname:** Wenn ein Objekt über die Swift-Schnittstelle aufgenommen wird, verwendet die Client-Anwendung eine Container- und Objektname-Kombination, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Wählen Sie **ILM Objekt-Metadaten-Lookup** aus.
2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

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

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

Object Metadata Lookup

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

Identifier

Version ID
(optional)

Look Up

4. Wählen Sie **Look Up**.

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

- Systemmetadaten, einschließlich Objekt-ID (UUID), Version-ID (optional), Objektname, Name des Containers, Mandantenkontoname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmeldaten 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": {
      "PAHS": "2",

```

Verwandte Informationen

[Objektmanagement mit ILM](#)

[S3 verwenden](#)

[Verwenden Sie Swift](#)

Fehler beim Objektspeicher (Storage Volume)

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

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

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sd(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	sd(8:16,sdb)	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd(8:32,sdc)	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde(8:48,sdd)	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf(8:64,sde)	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg(8:80,sdf)	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

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






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









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

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













Utilization

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

Replication

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

Object Store Volumes

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

Je nach Art des Ausfalls können Fehler bei einem Storage-Volume in einem Alarm über den Storage-Status oder den Zustand eines Objektspeicher gespiegelt werden. Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um den Speicherknoten so bald wie möglich wieder voll zu machen. Wenn nötig, können Sie auf die Registerkarte **Konfiguration** gehen und den Speicherknoten in einen Read-only Zustand setzen, so dass das StorageGRID System ihn für den Datenabruf verwenden kann, während Sie sich auf eine vollständige Wiederherstellung des Servers vorbereiten.

Verwandte Informationen

[Recovery und Wartung](#)

Überprüfen Sie die Objektintegrität

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

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

Was ist Hintergrundüberprüfung?

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

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

- **Replizierte Objekte:** Findet der Hintergrundverifizierungsvorgang ein beschädigtes Objekt, wird die beschädigte Kopie vom Speicherort entfernt und an anderer Stelle auf dem Speicherknoten isoliert. Anschließend wird eine neue, nicht beschädigte Kopie erstellt und gemäß der aktiven ILM-Richtlinie platziert. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die ursprüngliche Kopie verwendet wurde.



Beschädigte Objektdaten werden nicht aus dem System gelöscht, sondern in Quarantäne verschoben, sodass weiterhin darauf zugegriffen werden kann. Weitere Informationen zum Zugriff auf isolierte Objektdaten erhalten Sie vom technischen Support.

- **Erasure-codierte Objekte:** Erkennt der Hintergrund-Verifizierungsprozess, dass ein Fragment eines Löschungscodierten Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Daten- und Paritätsfragmente neu zu erstellen. Wenn das beschädigte Fragment nicht wiederhergestellt werden kann, wird versucht, eine andere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Bewertung durchgeführt, um eine Ersatzkopie des Objekts, das mit der Fehlerkorrektur codiert wurde, zu erstellen.

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

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

Warnmeldungen und Alarmer (alt) im Zusammenhang mit der Hintergrundüberprüfung

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

Wenn die Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, weil es keine andere Kopie finden kann, wird die Warnung **Objekte verloren** ausgelöst.

Ändern Sie die Hintergrundverifizierungsrate

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Sie können die Verifizierungsrate für die Hintergrundüberprüfung eines Speicherknoten ändern:

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

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

Schritte

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

The screenshot shows the 'Configuration: LDR () - Verification' page. The 'Configuration' tab is active. The 'Main' sub-tab is selected. The page title is 'Configuration: LDR () - Verification' with a timestamp 'Updated: 2021-11-11 07:13:00 MST'. The 'Background Verification' section contains a 'Verification Rate' dropdown menu set to 'Adaptive', which is highlighted with a green border. Other options include 'Reset Missing Objects Count', 'Reset Corrupt Objects Count', and 'Delete Quarantined Objects'. An 'Apply Changes' button with a right arrow icon is at the bottom right.



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

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

Wenn bei der Hintergrundüberprüfung beschädigte replizierte Objektdaten gefunden werden, wird die

Metrik **beschädigte Objekte** erhöht und StorageGRID versucht, die Objektkennung aus den Daten zu extrahieren, wie folgt:

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

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

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



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

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

Was ist Objektexistenz-Prüfung?

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

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

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

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

Überprüfung der ObjektExistenz ausführen

Sie erstellen und führen jeweils einen Job für die Überprüfung der Objektexistenz aus. Wenn Sie einen Job erstellen, wählen Sie die Speicherknoten und -Volumes aus, die Sie überprüfen möchten. Sie wählen auch das Consistency Control für den Job aus.

Was Sie benötigen

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

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

Über diese Aufgabe

Die Fertigstellung eines Objektes kann je nach Anzahl der Objekte im Raster, der ausgewählten Storage-Nodes und Volumes und der ausgewählten Konsistenzgruppe Tage oder Wochen dauern. Sie können nur einen Job gleichzeitig ausführen, aber Sie können mehrere Speicherknoten und Volumes gleichzeitig auswählen.

Schritte

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

Sie können nach Node-Namen oder Site suchen.

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

4. Wählen Sie **Weiter**.
5. Wählen Sie für jeden Knoten in der Liste ein oder mehrere Volumes aus. Sie können mithilfe der Storage-Volume-Nummer oder des Node-Namens nach Volumes suchen.

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

6. Wählen Sie **Weiter**.
7. Wählen Sie das Consistency Control für den Job aus.

Die Konsistenzkontrolle bestimmt, wie viele Kopien von Objektmetadaten für die Objektüberprüfung verwendet werden.

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

Weitere Informationen zur Consistency Control finden Sie in den Beschreibungen im Assistenten.

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

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

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



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

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

fehlender Objektkopien.

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

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

Object existence check

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

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

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

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

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

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

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

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

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

12. Wenn Sie für den Job die Kontrolle der Konsistenz vor Ort oder stark-global ausgewählt haben, warten Sie

ungefähr drei Wochen auf die Metadatenkonsistenz, und führen Sie den Job erneut auf denselben Volumes aus.

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

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

Object existence check

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

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

Active job | Job history

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

Displaying 4 results

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

- d. Überprüfen Sie im Assistenten für Rerun-Jobs die ausgewählten Knoten und Volumes und die Konsistenzsteuerung.
- e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Rerun**.

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

Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **SUPPORT Tools Grid-Topologie Site Storage-Node LDR Verifizierung Konfiguration Main** und erhöhen Sie die

Hintergrundverifizierungsrate. Die Hintergrundüberprüfung überprüft die Richtigkeit aller gespeicherten Objektdaten und repariert sämtliche gefundenen Probleme. Das schnelle Auffinden und Reparieren potenzieller Probleme verringert das Risiko von Datenverlusten.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

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

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

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

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

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

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

Verwandte Informationen

[Untersuchen Sie verlorene Objekte](#)

[Verlorene und fehlende Objektanzahl zurücksetzen](#)

Untersuchen Sie verlorene Objekte

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die `Passwords.txt` Datei:

Über diese Aufgabe

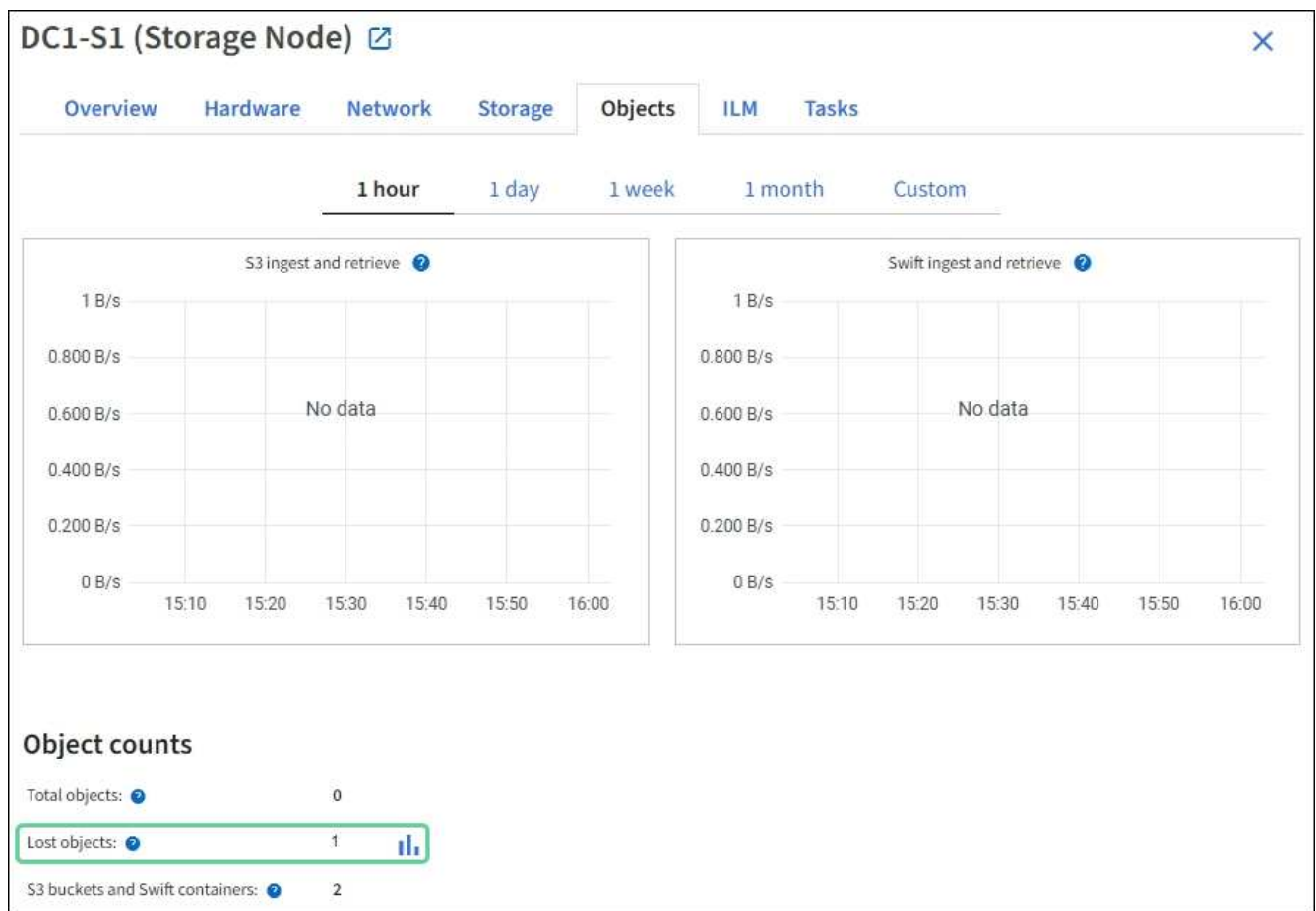
Die Warnung **Objects lost** zeigt an, dass StorageGRID glaubt, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

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

Schritte

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

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



4. Greifen Sie von einem Admin-Node aus auf das Audit-Protokoll zu, um die eindeutige Kennung (UUID) des Objekts zu bestimmen, das die Warnung **Objekte verloren** ausgelöst hat:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

- iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
- b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden. Geben Sie Ein: `cd /var/local/audit/export/`
- c. Verwenden Sie `grep`, um die Audit-Meldungen zu „Objekt verloren“ (OLST) zu extrahieren. Geben Sie Ein: `grep OLST audit_file_name`
- d. Beachten Sie den in der Meldung enthaltenen UUID-Wert.

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

5. Verwenden Sie die `ObjectByUUID` Befehl zum Suchen des Objekts anhand seiner ID (UUID) und bestimmen Sie, ob die Daten gefährdet sind.

- a. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole.
- b. Geben Sie Ein: `/proc/OBRP/ObjectByUUID UUID_value`

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

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

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
```

```

    "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
    "BSIZ(Content block size)": "5252084",
    "CVER(Content block version)": "196612",
    "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
    "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
    "ITME": "1581534970983000"
  },
  "CMSM": {
    "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
  },
  "AWS3": {
    "LOCC": "us-east-1"
  }
},
"CLCO\ (Locations\)": \[
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12448208",
    "VOLI\ (Volume ID\)": "3222345473",
    "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
    "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.880569"
  },
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12288733",
    "VOLI\ (Volume ID\)": "3222345984",
    "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.934425"
  }
]
}

```

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

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

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

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

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

Verwandte Informationen

[Prüfung von Audit-Protokollen](#)

Suche nach potenziell verlorenen Objekten und Wiederherstellung

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

Was Sie benötigen

- Sie müssen über die UUID eines verlorenen Objekts verfügen, wie in „Untersuchung verlorener Objekte“ angegeben.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

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



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

Schritte

1. Suchen Sie in einem Admin-Knoten die Prüfprotokolle nach möglichen Objektspeichern:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`
 - c. Verwenden Sie `grep`, um die mit dem potenziell verlorenen Objekt verknüpften Audit-Nachrichten zu extrahieren und sie an eine Ausgabedatei zu senden. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

Beispiel:

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

- d. Verwenden Sie `grep`, um die Meldungen zum Lost Location (LLST) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep LLST output_file_name`

Beispiel:

```
Admin: # grep LLST messages_about_lost_objects.txt
```

Eine LLST-Überwachungsmeldung sieht wie diese Beispielmeldung aus.

```
[AUDT:\[NOID\ (UI32\):12448208\[CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTYP(FC32):CLDI]
[PCLD\ (CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST] [RSLT(FC32):NONE] [AVER(UI32):10] [ATIM(UI64):
1581535134379225] [ATYP(FC32):LLST] [ANID(UI32):12448208] [AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

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

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

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

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

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

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

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

a. Melden Sie sich beim Grid-Node an:

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

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

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

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

Geben Sie beispielsweise Folgendes ein:

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

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

- Wenn der Objektpfad nicht gefunden wurde, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wurde, fahren Sie mit Schritt fort [Stellen Sie das Objekt in StorageGRID wieder her](#). Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.
 - a. Wenn der Objektpfad gefunden wurde, versuchen Sie, das Objekt in StorageGRID wiederherzustellen:
 - i. Ändern Sie vom gleichen Speicherknoten aus die Eigentumsrechte an der Objektdatei, so dass sie

von StorageGRID gemanagt werden kann. Geben Sie Ein: `chown ldr-user:bycast 'file_path_of_object'`

- ii. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole. Geben Sie Ein: `telnet 0 1402`
- iii. Geben Sie Ein: `cd /proc/STOR`
- iv. Geben Sie Ein: `Object_Found 'file_path_of_object'`

Geben Sie beispielsweise Folgendes ein:

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

Ausstellen der `Object_Found` Durch den Befehl wird das Raster des Speicherorts des Objekts benachrichtigt. Zudem wird die aktive ILM-Richtlinie ausgelöst, die zusätzliche Kopien gemäß den Angaben in der Richtlinie erstellt.

Hinweis: Wenn der Speicherknoten, in dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf einen beliebigen Speicherknoten kopieren, der online ist. Platzieren Sie das Objekt in einem beliebigen `/var/local/rangedb`-Verzeichnis des Online-Storage-Node. Geben Sie dann den aus `Object_Found` Befehl mit diesem Dateipfad zum Objekt.

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

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

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

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

- v. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, überprüfen Sie, ob neue Speicherorte erstellt wurden.
 - A. Geben Sie Ein: `cd /proc/OBRP`
 - B. Geben Sie Ein: `ObjectByUUID UUID_value`

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

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

```

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  },
  "CLCO\ (Locations\)": \[
    \{
      "Location Type": "CLDI\ (Location online\)",
      "NOID\ (Node ID\)": "12448208",
      "VOLI\ (Volume ID\)": "3222345473",
      "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
      "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.880569"
    },
    \{
      "Location Type": "CLDI\ (Location online\)",
      "NOID\ (Node ID\)": "12288733",
      "VOLI\ (Volume ID\)": "3222345984",
      "Object File Path":

```

```
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.934425"
  }
]
}
```

1. Melden Sie sich von der LDR-Konsole ab. Geben Sie Ein: `exit`
 - a. Durchsuchen Sie von einem Admin-Node aus die Prüfprotokolle für die ORLM-Überwachungsmeldung für dieses Objekt, um zu bestätigen, dass Information Lifecycle Management (ILM) Kopien nach Bedarf platziert hat.
2. Melden Sie sich beim Grid-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
3. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`
4. Verwenden Sie `grep`, um die mit dem Objekt verknüpften Überwachungsmeldungen in eine Ausgabedatei zu extrahieren. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

Beispiel:

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

5. Verwenden Sie `grep`, um die ORLM-Audit-Meldungen (Object Rules met) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep ORLM output_file_name`

Beispiel:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

Eine ORLM-Überwachungsmeldung sieht wie diese Beispielmeldung aus.

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

6. Suchen Sie das FELD LOKS in der Überwachungsmeldung.

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

Verwandte Informationen

[Untersuchen Sie verlorene Objekte](#)

[Verlorene und fehlende Objektanzahl zurücksetzen](#)

[Prüfung von Audit-Protokollen](#)

Verlorene und fehlende Objektanzahl zurücksetzen

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

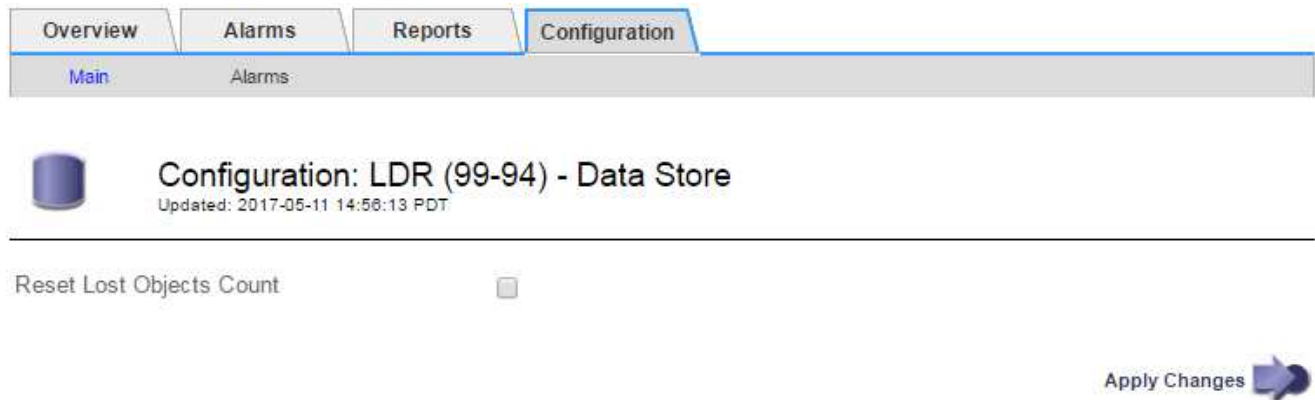
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

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

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

Schritte

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



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

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

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

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

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

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

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

Beheben Sie die Warnung „Niedrig Object Data Storage“

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die Warnung * Low Object Data Storage* wird ausgelöst, wenn die Gesamtzahl der replizierten und Erasure codierten Objektdaten auf einem Storage Node einer der Bedingungen entspricht, die in der Warnungsregel konfiguriert sind.

Standardmäßig wird eine wichtige Warnmeldung ausgelöst, wenn diese Bedingung als „true“ bewertet wird:

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

In diesem Zustand:

- `storagegrid_storage_utilization_data_bytes` Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten für einen Storage-Node
- `storagegrid_storage_utilization_usable_space_bytes` Ist die Gesamtmenge an verbleibendem Objekt-Speicherplatz für einen Storage-Node.

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

Schritte

1. Wählen Sie **ALERTS Current**.

Die Seite „Meldungen“ wird angezeigt.

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



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

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

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

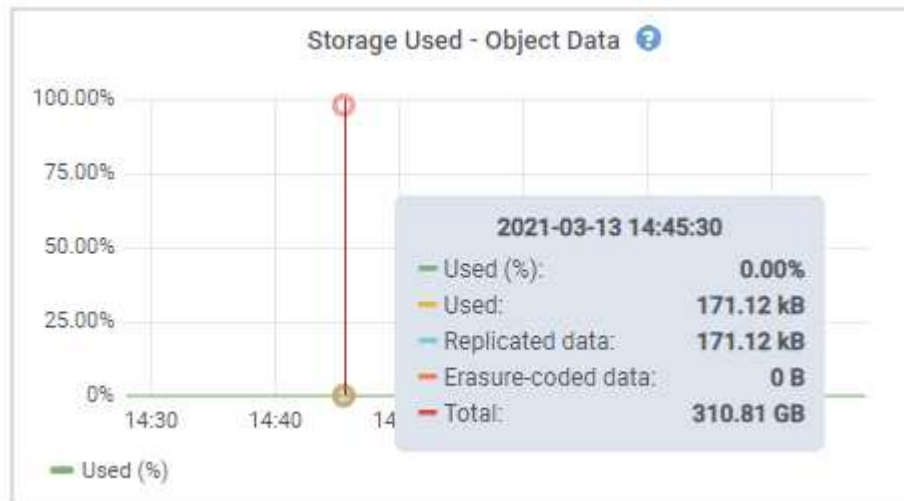
4. Wählen Sie **NODES Storage Node oder Standort Storage** aus.

5. Bewegen Sie den Mauszeiger über das Diagramm „verwendete Daten – Objektdaten“.

Die folgenden Werte werden angezeigt:

- **Used (%)**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Verwendet**: Die Menge des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Replizierte Daten**: Eine Schätzung der Menge der replizierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Erasure-codierte Daten**: Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.

- **Gesamt:** Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` Metrisch.



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

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

- So bald wie möglich, ein Erweiterungsverfahren für zusätzliche Speicherkapazität durchführen.

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



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

Verwandte Informationen

[Fehlersuche im SSTs-Alarm \(Storage Status\) durchführen](#)

[Erweitern Sie Ihr Raster](#)

[StorageGRID verwalten](#)

Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff

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

In vorherigen Versionen, die drei [Wasserzeichen für Storage-Volumes](#) Wurden globale Einstellungen #8212 durchgeführt. Dieselben Werte werden auf jedes Storage-Volume auf jedem Storage Node angewendet. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Storage Volume optimieren, basierend auf der Größe des Storage-Nodes und der relativen Kapazität des Volumes.

Wenn Sie ein Upgrade auf StorageGRID 11.6 durchführen, werden optimierte Read- und Write-Wasserzeichen automatisch auf alle Storage Volumes angewendet, sofern keine der folgenden Optionen zutrifft:

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

Analysieren Sie die Meldung

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

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

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

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

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

Beheben Sie die Meldung

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

Was Sie benötigen

- Sie haben das Upgrade auf StorageGRID 11.6 abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

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

Bewertung der Nutzung von Objektdaten für das gesamte Grid

1. Wählen Sie **KNOTEN**.
2. Erweitern Sie für jeden Standort im Raster die Liste der Nodes.
3. Überprüfen Sie die Prozentwerte, die in der Spalte **Objektdaten verwendet** für jeden Speicherknoten an jedem Standort angezeigt werden.
4. Wenn keiner der Speicherknoten fast voll ist (zum Beispiel sind alle **Objektdaten verwendet** Werte kleiner als 80%), können Sie die Überschreibeinstellungen verwenden. Gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#).



Es gibt einige Ausnahmen von dieser allgemeinen Regel. Wenn ILM-Regeln beispielsweise ein strenges Aufnahmeverhalten verwenden oder bestimmte Storage-Pools nahezu vollständig sind, sollten Sie zuerst die Schritte in durchführen [Anzeigen optimierter Speicherabdrücke](#) Und [ob Sie optimierte Wasserzeichen verwenden können](#).

5. Wenn mehrere Speicherknoten nahezu voll sind, führen Sie die Schritte unter aus [Anzeigen optimierter Speicherabdrücke](#) Und [ob Sie optimierte Wasserzeichen verwenden können](#).

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

1. Wählen Sie **SUPPORT Tools Kennzahlen** aus.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

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

Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können

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

Andernfalls [Erweitern Sie Ihr Raster](#) So bald wie möglich. Fügen Sie einem vorhandenen Node entweder Storage Volumes hinzu oder fügen Sie neue Storage-Nodes hinzu. Fahren Sie dann mit fort [Verwenden Sie optimierte Wasserzeichen](#) Zum Aktualisieren der Einstellungen für Wasserzeichen.

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



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

Verwenden Sie optimierte Wasserzeichen


1. Gehen Sie zu **KONFIGURATION System Speicheroptionen**.
2. Wählen Sie im Menü Speicheroptionen die Option **Konfiguration** aus.
3. Ändern Sie alle drei Wasserzeichen-Überschreibungen auf 0.
4. Wählen Sie **Änderungen Anwenden**.

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

Storage Options

Overview

Configuration



Storage Options Overview

Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

Fehlersuche im SSTS-Alarm (Storage Status) durchführen

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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



Storage Options Overview

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

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

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

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

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


Schritte




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


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

OverviewAlarmsReportsConfiguration

MainHistory

**Alarms: LDR (DC1-S3-101-195) - Storage**
Updated: 2019-10-09 12:52:43 MDT

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

Apply Changes 

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



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

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


Overview

Alarms

Reports

Configuration

Main



Overview: LDR (.DC1-S1-101-193) - Storage
Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:

Online

Storage State - Current:

Read-only

Storage Status:

Insufficient Free Space

Utilization

Total Space:

164 GB

Total Usable Space:

19.6 GB

Total Usable Space (Percent):

11.937 %

Total Data:

139 GB

Total Data (Percent):

84.567 %

Replication

Block Reads:

0

Block Writes:

2,279,881

Objects Retrieved:

0

Objects Committed:

88,882
















Objects Deleted:

16

Delete Service State:

Enabled

Object Store Volumes

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

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

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

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

Overview


Alarms

Reports

Configuration

Charts

Text



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

Attribute:

Total Usable Space

Quick Query:

Custom Query

Update

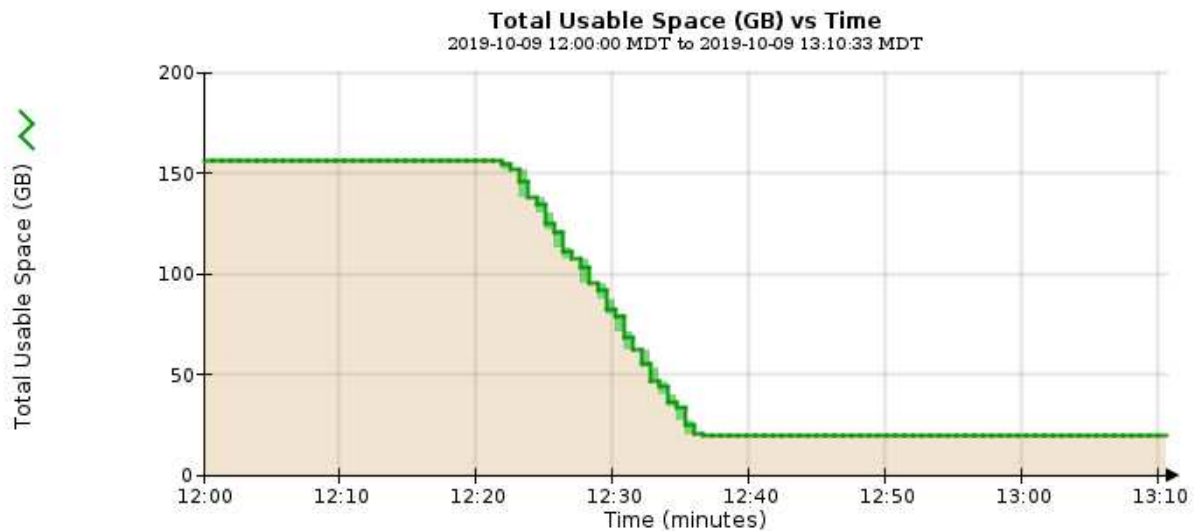
Vertical Scaling: ☒

Raw Data: ☐

YYYY/MM/DD HH:MM:SS

Start Date: 2019/10/09 12:00:00

End Date: 2019/10/09 13:10:33



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

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

Overview


Alarms

Reports

Configuration

Charts

Text



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

Attribute:

Total Usable Space (Percent)

Quick Query:

Custom Query

Update

Vertical Scaling:

☒

Raw Data:

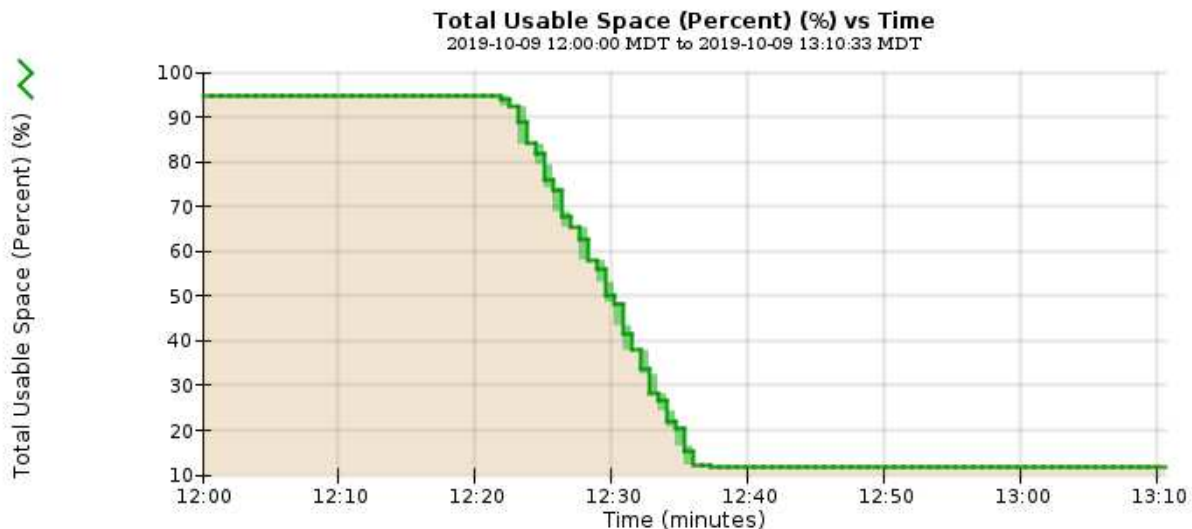
☐

Start Date:

2019/10/09 12:00:00

End Date:

2019/10/09 13:10:33



6. Fügen Sie bei Bedarf die Storage-Kapazität um hinzu [Erweitern des StorageGRID Systems](#).

Informationen zu Verfahren zum Verwalten eines vollständigen Speicherknoten finden Sie im [Anweisungen für die Administration von StorageGRID](#).

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

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

Über diese Aufgabe

So kann beispielsweise ein S3-Multipart-Upload erfolgreich sein, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsmeldung nicht an den konfigurierten Endpunkt gesendet werden kann. Alternativ kann eine Nachricht für die CloudMirror Replizierung nicht bereitgestellt werden, wenn die Metadaten zu lang sind.

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

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

Weitere Informationen zur Fehlerbehebung von Plattformdiensten finden Sie im [Anweisungen für die Administration von StorageGRID](#). Möglicherweise müssen Sie es [Greifen Sie über den Tenant Manager auf](#)

[den Mandanten zu](#) So beheben Sie einen Plattformdienstfehler.

Schritte

1. Um den Alarm anzuzeigen, wählen Sie **NODES site Grid Node Events** aus.
2. Letztes Ereignis oben in der Tabelle anzeigen.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

3. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
4. Wählen Sie **Anzahl der Ereignisse zurücksetzen**.
5. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.
6. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts auszulösen.

Behebung von Metadatenproblemen

Sie können mehrere Aufgaben durchführen, um die Ursache von Metadatenproblemen zu ermitteln.

Beheben Sie die Warnmeldung zu niedrigen Metadaten-Storage

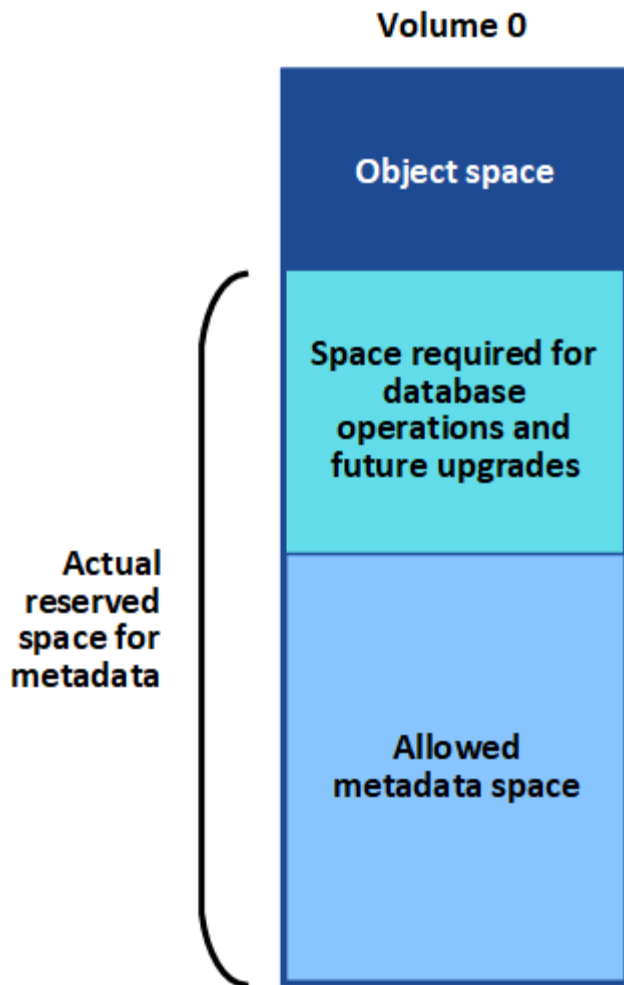
Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

Über diese Aufgabe

StorageGRID reserviert eine bestimmte Menge an Speicherplatz auf Volume 0 jedes Storage-Nodes für Objekt-Metadaten. Dieser Speicherplatz wird als tatsächlicher reservierter Speicherplatz bezeichnet und in den Speicherplatz für Objekt-Metadaten (zulässiger Metadatenspeicherplatz) und den für wichtige Datenbankvorgänge wie Data-Compaction und Reparatur erforderlichen Speicherplatz unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.



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

Das können Sie [Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node](#) Um Ihnen zu helfen, Fehler frühzeitig zu erkennen und zu beheben, bevor sie auftreten.

StorageGRID verwendet die folgende Prometheus Kennzahl, um den vollen Umfang des zulässigen Metadaten-Speicherplatzes zu messen:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Wenn dieser Prometheus-Ausdruck bestimmte Schwellenwerte erreicht, wird die Warnung **Low Metadaten Storage** ausgelöst.

- **Minor:** Objektmeldaten verwenden 70% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie sollten so bald wie möglich neue Storage-Nodes hinzufügen.
- **Major:** Objektmeldaten verwenden 90% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie müssen sofort neue Storage-Nodes hinzufügen.



Wenn Objektmetadaten 90 % oder mehr des zulässigen Metadaten-Speicherplatzes beanspruchen, wird im Dashboard eine Warnung angezeigt. Wenn diese Warnung angezeigt wird, müssen Sie sofort neue Speicherknoten hinzufügen. Es ist nicht zulässig, dass Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes nutzen.

- **Kritisch:** Objektmetadaten verbrauchen 100% oder mehr des zulässigen Metadaten-Speicherplatzes und verbrauchen den für wichtige Datenbankvorgänge erforderlichen Speicherplatz. Sie müssen die Aufnahme neuer Objekte beenden und sofort neue Speicherknoten hinzufügen.

In dem folgenden Beispiel belegen die Objektmetadaten mehr als 100 % des zulässigen Metadaten-Speicherplatzes. Hierbei handelt es sich um eine kritische Situation, die zu einem ineffizienten und ineffizienten Datenbankbetrieb und zu Fehlern führt.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.



Wenn die Größe von Volume 0 kleiner ist als die Option „Metadatenreservierter Speicherplatz“ (z. B. in einer nicht-Produktionsumgebung), kann die Berechnung für die Warnmeldung * Low Metadaten Storage* fehlerhaft sein.

Schritte

1. Wählen Sie **ALERTS Current**.
2. Erweitern Sie, falls erforderlich, aus der Warnmeldungstabelle die Warnungsgruppe **Low-Metadaten-Speicher** und wählen Sie die spezifische Warnung aus, die Sie anzeigen möchten.
3. Überprüfen Sie die Details im Dialogfeld „Warnung“.
4. Wenn eine wichtige oder kritische Warnung für * Storage-Systeme mit niedrigen Metadaten* ausgelöst wurde, führen Sie eine Erweiterung durch, um Storage-Nodes sofort hinzuzufügen.



Da StorageGRID komplette Kopien aller Objektmetadaten an jedem Standort speichert, wird die Metadaten-Kapazität des gesamten Grid durch die Metadaten-Kapazität des kleinsten Standorts begrenzt. Wenn Sie Metadaten an einem Standort hinzufügen müssen, sollten Sie auch [Erweitern Sie alle anderen Standorte](#) An die gleiche Anzahl von Storage-Nodes.

Nach der Erweiterung verteilt StorageGRID die vorhandenen Objekt-Metadaten neu auf die neuen Nodes, wodurch die allgemeine Metadaten des Grid erhöht werden. Es ist keine Benutzeraktion erforderlich. Die Warnung * Speicherung von niedrigen Metadaten* wird gelöscht.

Fehlersuche im Alarm Services: Status - Cassandra (SVST) durchführen

Der Alarm Services: Status – Cassandra (SVST) gibt an, dass Sie die Cassandra-Datenbank für einen Storage-Node möglicherweise neu aufbauen müssen. Cassandra dient als Metadatenspeicher für StorageGRID.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Wenn Cassandra länger als 15 Tage angehalten wird (z. B. ausgeschaltet), startet Cassandra nicht, wenn der Node wieder online geschaltet wird. Sie müssen die Cassandra-Datenbank für den betroffenen DDS-Dienst neu erstellen.

Das können Sie [Führen Sie eine Diagnose aus](#) Um zusätzliche Informationen über den aktuellen Status Ihres Rasters zu erhalten.



Wenn mindestens zwei der Cassandra-Datenbankdienste länger als 15 Tage ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Site Storage Node SSM Services Alarme Main**, um Alarme anzuzeigen.

Dieses Beispiel zeigt, dass der SVST-Alarm ausgelöst wurde.

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor	SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running		<input type="checkbox"/>

Auf der SSM Services-Hauptseite wird auch angezeigt, dass Cassandra nicht ausgeführt wird.

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC2-S1) - Services
Updated: 2017-03-30 09:53:53 MDT

Operating System: Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running	4	3.58 %	19.1 MB

3. Neustarten von Cassandra aus dem Storage-Node:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Geben Sie Ein: `/etc/init.d/cassandra status`
 - c. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: `/etc/init.d/cassandra restart`
4. Falls Cassandra nicht neu startet, bestimmen Sie, wie lange Cassandra ausgefallen ist. Wenn Cassandra länger als 15 Tage ausfällt, müssen Sie die Cassandra-Datenbank neu aufbauen.



Wenn zwei oder mehr der Cassandra-Datenbankdienste ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

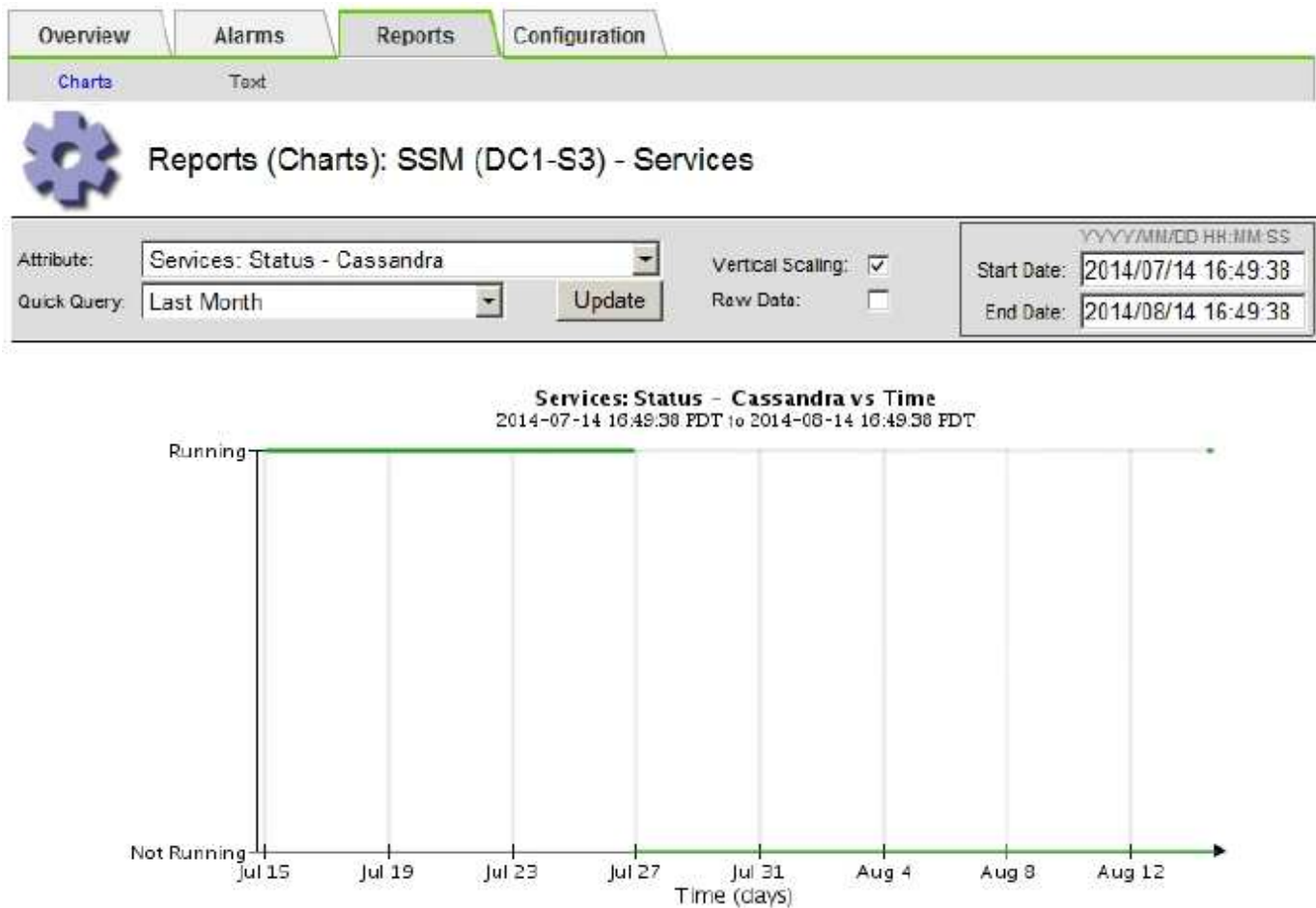
Sie können feststellen, wie lange Cassandra ausgefallen ist, indem Sie sie aufschreiben oder die Datei `servermanager.log` lesen.

5. Cassandra Diagramm:
 - a. Wählen Sie **SUPPORT Tools Grid-Topologie** aus. Wählen Sie dann **Site Storage Node SSM Services Berichte Diagramme** aus.
 - b. Wählen Sie **Attribut Service: Status - Cassandra**.
 - c. Geben Sie für **Startdatum** ein Datum ein, das mindestens 16 Tage vor dem aktuellen Datum liegt. Geben Sie für **Enddatum** das aktuelle Datum ein.

d. Klicken Sie Auf **Aktualisieren**.

e. Wenn Cassandra für mehr als 15 Tage nicht verfügbar ist, bauen Sie die Cassandra-Datenbank erneut aus.

Das folgende Diagramm zeigt, dass Cassandra seit mindestens 17 Tagen ausgefallen ist.



1. So prüfen Sie die Datei `servermanager.log` auf dem Speicherknoten:

a. Melden Sie sich beim Grid-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Geben Sie Ein: `cat /var/local/log/servermanager.log`

Der Inhalt der Datei `servermanager.log` wird angezeigt.

Wenn Cassandra länger als 15 Tage ausfällt, wird die folgende Meldung in der Datei `servermanager.log` angezeigt:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

- a. Stellen Sie sicher, dass der Zeitstempel dieser Nachricht der Zeitpunkt ist, zu dem Sie versucht haben, Cassandra wie in Schritt angegeben neu zu starten [Starten Sie Cassandra vom Storage-Node aus neu](#).

Für Cassandra gibt es mehrere Einträge; Sie müssen den letzten Eintrag finden.

- b. Wenn Cassandra länger als 15 Tage ausfällt, müssen Sie die Cassandra-Datenbank neu aufbauen.

Anweisungen hierzu finden Sie unter [Stellen Sie Storage Node länger als 15 Tage wieder her](#).

- c. Wenden Sie sich an den technischen Support, wenn die Alarmer nach dem Wiederaufbau von Cassandra nicht gelöscht werden.

Fehlerbehebung bei Cassandra-Fehlern außerhalb des Speichers (SMTT-Alarm)

Ein Alarm für Total Events (SMTT) wird ausgelöst, wenn die Cassandra-Datenbank einen Fehler außerhalb des Arbeitsspeichers hat. Wenn dieser Fehler auftritt, wenden Sie sich an den technischen Support, um das Problem zu bearbeiten.

Über diese Aufgabe

Wenn für die Cassandra-Datenbank ein Fehler außerhalb des Arbeitsspeichers auftritt, wird ein Heap Dump erstellt, ein SMTT-Alarm (Total Events) ausgelöst und die Anzahl der Cassandra Heap Out of Memory-Fehler wird um eins erhöht.

Schritte

1. Um das Ereignis anzuzeigen, wählen Sie **SUPPORT Tools Grid-Topologie Konfiguration**.
2. Stellen Sie sicher, dass die Anzahl der Cassandra Heap-Fehler bei einem Speicherfehler mindestens 1 beträgt.

Das können Sie [Führen Sie eine Diagnose aus](#) Um zusätzliche Informationen über den aktuellen Status Ihres Rasters zu erhalten.

3. Gehen Sie zu `/var/local/core/`, Komprimieren Sie die `Cassandra.hprof` Datei erstellen und an den technischen Support senden.
4. Erstellen Sie ein Backup der `Cassandra.hprof` Datei und löschen Sie sie aus dem `/var/local/core/` directory.

Diese Datei kann bis zu 24 GB groß sein, so sollten Sie sie entfernen, um Speicherplatz freizugeben.

5. Nachdem das Problem behoben wurde, aktivieren Sie das Kontrollkästchen **Zurücksetzen** für die Anzahl der Cassandra-Heap-Fehler aus dem Speicher. Wählen Sie dann **Änderungen anwenden**.



Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen.

Fehlerbehebung bei Zertifikatfehlern

Wenn beim Versuch, eine Verbindung mit StorageGRID über einen Webbrowser, einen S3- oder Swift-Client oder ein externes Monitoring-Tool herzustellen, ein Problem mit der Sicherheit oder dem Zertifikat auftritt, sollten Sie das Zertifikat überprüfen.

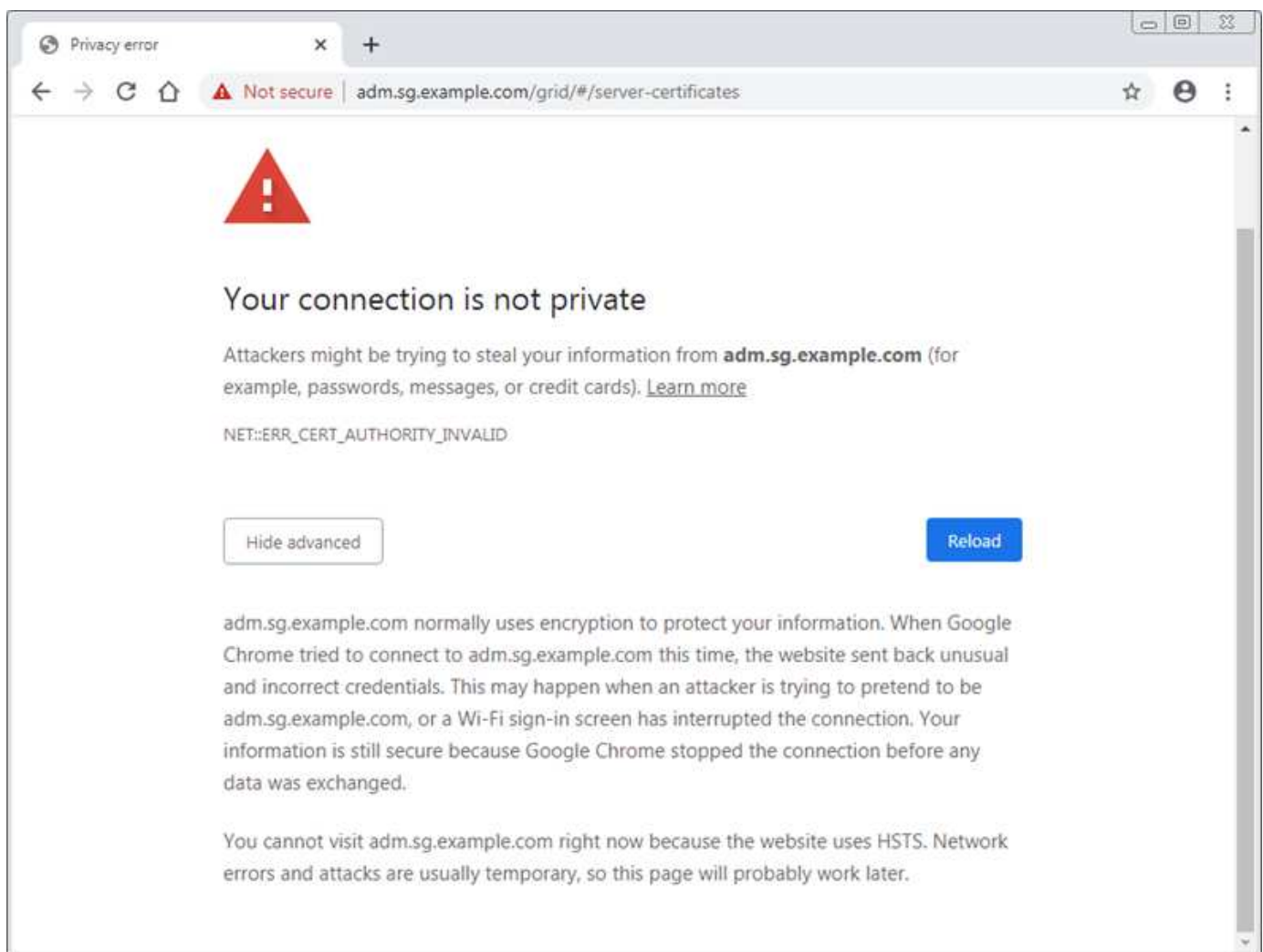
Über diese Aufgabe

Zertifikatfehler können Probleme verursachen, wenn Sie versuchen, eine Verbindung mit StorageGRID mithilfe des Grid Managers, der Grid Management API, des Mandantenmanagers oder der Mandantenmanagement-API herzustellen. Zertifikatfehler können auch auftreten, wenn Sie eine Verbindung mit einem S3- oder Swift-Client oder einem externen Monitoring-Tool herstellen.

Wenn Sie mit einem Domännennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für die benutzerdefinierte Managementoberfläche läuft ab.
- Sie werden von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Im folgenden Beispiel ist ein Zertifikatfehler angezeigt, wenn das Zertifikat der benutzerdefinierten Managementoberfläche abgelaufen ist:



Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn das Serverzertifikat abläuft.

Wenn Sie Clientzertifikate für die externe Prometheus-Integration verwenden, können Zertifikatsfehler durch das Zertifikat der StorageGRID-Verwaltungsschnittstelle oder durch Clientzertifikate verursacht werden. Die auf der Seite [Zertifikate](#)* konfigurierte Warnung *Ablauf von Clientzertifikaten wird ausgelöst, wenn ein Clientzertifikat abläuft.

Schritte

Wenn Sie eine Benachrichtigung über ein abgelaufenes Zertifikat erhalten haben, rufen Sie die Zertifikatsdetails auf: . Wählen Sie **KONFIGURATION Sicherheit Zertifikate** und dann [Wählen Sie die entsprechende Registerkarte Zertifikat aus](#).

1. Überprüfen Sie die Gültigkeitsdauer des Zertifikats. + einige Webbrowser und S3- oder Swift-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.
2. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein oder generieren Sie ein neues Zertifikat.
 - Ein Serverzertifikat finden Sie in den Schritten für [Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#).
 - Ein Client-Zertifikat finden Sie in den Schritten für [Konfigurieren eines Client-Zertifikats](#).
3. Versuchen Sie bei Serverzertifikatsfehlern oder beiden der folgenden Optionen:
 - Stellen Sie sicher, dass der Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass das SAN mit der IP-Adresse oder dem Hostnamen des Node übereinstimmt, mit dem Sie eine Verbindung herstellen.
 - Wenn Sie versuchen, eine Verbindung zu StorageGRID mit einem Domain-Namen herzustellen:
 - i. Geben Sie die IP-Adresse des Admin-Knotens anstelle des Domain-Namens ein, um den Verbindungsfehler zu umgehen und auf den Grid-Manager zuzugreifen.
 - ii. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und dann [Wählen Sie die entsprechende Registerkarte Zertifikat aus](#) So installieren Sie ein neues benutzerdefiniertes Zertifikat oder fahren mit dem Standardzertifikat fort.
 - iii. Lesen Sie in der Anleitung zum Verwalten von StorageGRID die Schritte für [Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#).

Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche

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

Fehler bei der Anmeldung beheben

Wenn beim Anmelden bei einem StorageGRID-Admin-Node ein Fehler auftritt, weist Ihr System möglicherweise ein Problem mit der Konfiguration des Identitätsverbunds auf, ein Netzwerk- oder Hardwareproblem, ein Problem mit den Admin-Node-Services oder ein Problem mit der Cassandra-Datenbank auf verbundenen Speicherknoten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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

- `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 melden Sie sich erneut an.

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

2. Wenn Ihr StorageGRID-System mehr als einen Admin-Knoten hat, melden Sie sich von einem anderen Admin-Knoten beim Grid-Manager an.
 - Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **NODES**, **Alerts** und **SUPPORT** verwenden, um die Ursache des Fehlers zu ermitteln.
 - Wenn Sie nur einen Admin-Node haben oder sich dennoch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Ermitteln, ob die Hardware des Node offline ist
4. Wenn SSO (Single Sign On) für Ihr StorageGRID-System aktiviert ist, lesen Sie in den Anweisungen zur Administration von StorageGRID die Schritte zur Konfiguration der Single Sign-On.

Unter Umständen müssen Sie SSO für einen einzelnen Admin-Node vorübergehend deaktivieren und erneut aktivieren, um Probleme zu beheben.



Wenn SSO aktiviert ist, können Sie sich nicht mit einem eingeschränkten Port anmelden. Sie müssen Port 443 verwenden.

5. Ermitteln Sie, ob das verwendete Konto einem föderierten Benutzer angehört.

Wenn das verbundene Benutzerkonto nicht funktioniert, melden Sie sich beim Grid Manager als lokaler Benutzer, z. B. als Root, an.

- Wenn sich der lokale Benutzer anmelden kann:
 - i. Überprüfen Sie alle angezeigten Alarmer.
 - ii. Wählen Sie **KONFIGURATION Zugangskontrolle Identitätsverbund**.
 - iii. Klicken Sie auf **Verbindung testen**, um die 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 sich 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:

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

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

7. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Stellen Sie sicher, dass die nms-, mi-, nginx- und Management-API-Services 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. Vergewissern Sie sich, dass der nginx-gw-Dienst ausgeführt wird # `service nginx-gw status`

9. Lumberjack zum Sammeln von Protokollen verwenden: # `/usr/local/sbin/lumberjack.rb`

Wenn die fehlgeschlagene Authentifizierung in der Vergangenheit stattgefunden hat, können Sie die Skriptoptionen `--start` und `--end` Lumberjack verwenden, um den entsprechenden Zeitbereich festzulegen. Verwenden Sie die `lumberjack -h` für Details zu diesen Optionen.

Die Ausgabe an das Terminal gibt an, wo das Protokollarchiv kopiert wurde.

10. folgende Protokolle prüfen:

- `/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, die den ADC-Dienst an Ihrem Standort ausführen. In der Regel handelt es sich dabei um die ersten drei Storage-Nodes, die am Standort installiert wurden.

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

```
# vi /var/local/gpt-data/specs/grid.xml
```

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

12. Melden Sie sich über den Admin-Node bei jedem der ADC-Speicherknoten an. Verwenden Sie dazu die IP-Adressen, die Sie identifiziert haben.

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

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

13. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Stellen Sie sicher, dass die Services `idnt`, `acct`, `nginx` und `cassandra` ausgeführt werden.

14. Wiederholen Sie die Schritte [Verwenden Sie Lumberjack, um Protokolle zu sammeln](#) Und [Protokolle prüfen](#) So prüfen Sie die Protokolle auf den Speicherknoten.

15. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Stellen Sie die Protokolle bereit, die Sie für den technischen Support gesammelt haben. Siehe auch [Referenz für Protokolldateien](#).

Fehlerbehebung bei Problemen mit der Benutzeroberfläche

Nach dem Upgrade auf eine neue Version der StorageGRID-Software sind möglicherweise Probleme mit dem Grid Manager oder dem Tenant Manager zu sehen.

Web-Oberfläche reagiert nicht wie erwartet

Der Grid-Manager oder der Mandantenmanager reagieren nach einem Upgrade der StorageGRID-Software möglicherweise nicht wie erwartet.

Wenn Probleme mit der Weboberfläche auftreten:

- Stellen Sie sicher, dass Sie ein verwenden [Unterstützter Webbrowser](#).



Die Browser-Unterstützung wurde für StorageGRID 11.5 geändert. Vergewissern Sie sich, dass Sie eine unterstützte Version verwenden.

- Löschen Sie den Cache Ihres Webbrowsers.

Beim Löschen des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID-Software verwendet werden, und die Benutzeroberfläche kann wieder ordnungsgemäß ausgeführt werden. Anweisungen hierzu finden Sie in der Dokumentation Ihres Webbrowsers.

Überprüfen Sie den Status eines nicht verfügbaren Admin-Knotens

Wenn das StorageGRID-System mehrere Administratorknoten enthält, können Sie den Status eines nicht verfügbaren Admin-Knotens mit einem anderen Admin-Knoten überprüfen.

Was Sie benötigen

Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Melden Sie sich bei einem verfügbaren Admin-Node mit einem bei Grid Manager an [Unterstützter Webbrowser](#).
2. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
3. Wählen Sie **Site nicht verfügbar Admin Node SSM Services Übersicht Main**.
4. Suchen Sie nach Diensten, die den Status nicht aktiv haben und die möglicherweise auch blau angezeigt werden.
5. Bestimmen Sie, ob Alarme ausgelöst wurden.
6. Ergreifen Sie die entsprechenden Maßnahmen, um das Problem zu lösen.

Verwandte Informationen

[StorageGRID verwalten](#)

Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen

Sie können verschiedene Aufgaben durchführen, um die Ursache von Problemen im

Zusammenhang mit dem StorageGRID Netzwerk-, Hardware- und Plattformproblemen zu ermitteln.

Fehler bei „422: Unbearbeitbare Einheit“ beheben

Der Fehler 422: Unbearbeitbare Einheit kann unter verschiedenen Umständen auftreten. Überprüfen Sie die Fehlermeldung, um festzustellen, welche Ursache Ihr Problem verursacht hat.

Wenn eine der aufgeführten Fehlermeldungen angezeigt wird, führen Sie die empfohlene Aktion durch.

Fehlermeldung	Ursache und Korrekturmaßnahme
<p>422: Unprocessable Entity</p> <p>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</p>	<p>Diese Meldung kann auftreten, wenn Sie bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option TLS nicht verwenden für Transport Layer Security (TLS) auswählen.</p> <p>Die Verwendung der Option keine Verwendung von TLS wird nicht für die Verwendung mit AD-Servern unterstützt, die LDAP-Signatur erzwingen. Sie müssen entweder die Option STARTTLS verwenden oder die Option LDAPS verwenden für TLS auswählen.</p>
<p>422: Unprocessable Entity</p> <p>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)</p>	<p>Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte Chiffre zu verwenden, um eine TLS-Verbindung (Transport Layer Security) von StorageGRID zu einem externen System herzustellen, das für Identify Federation oder Cloud Storage Pools verwendet wird.</p> <p>Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eine der von StorageGRID unterstützten Chiffren für ausgehende TLS-Verbindungen verwenden, wie in den Anleitungen zur StorageGRID-Verwaltung dargestellt.</p>

Fehlerbehebung bei der MTU-Warnung für das Grid Network

Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) über Knoten im Grid deutlich unterscheidet.

Über diese Aufgabe

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

Schritte

1. Führen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
 - Verwenden Sie die im Grid Manager angegebene Abfrage.
 - Navigieren Sie zu *primary Admin Node IP address/metrics/graph* Und geben Sie die folgende Abfrage ein: `node_network_mtu_bytes{interface='eth0'}`
2. Ändern Sie die MTU-Einstellungen nach Bedarf, um sicherzustellen, dass sie für die Grid Network Interface (eth0) auf allen Knoten identisch sind.
 - Informationen zu Appliance-Knoten finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.
 - 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 den verwenden `change-ip.py` Skript zum Ändern des MTU-Werts des Netzwerks im Container.

Verwenden Sie die folgenden Argumente, um die MTU auf Linux- oder VMware-basierten Knoten zu ändern.

Positionsargumente	Beschreibung
mtu	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
network	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: <ul style="list-style-type: none">• Raster• Admin• Client

+

Optionale Argumente	Beschreibung
-h, - help	Hilfemeldung anzeigen und beenden.
-n node, --node node	Der Node. Die Standardeinstellung ist der lokale Knoten.

Verwandte Informationen

[SG100- und SG1000-Services-Appliances](#)

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[SG5600 Storage Appliances](#)

Beheben Sie die Fehlerbehebung im NRER-Alarm (Network Receive Error)

NRER-Alarme (Network Receive Error) können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerk-Hardware verursacht werden. In einigen Fällen können NRER-Fehler ohne manuelles Eingreifen gelöscht werden. Wenn die Fehler nicht behoben werden, führen Sie die empfohlenen Maßnahmen durch.

Über diese Aufgabe

NRER-Alarme können durch die folgenden Probleme mit Netzwerk-Hardware verursacht werden, die eine Verbindung mit StorageGRID herstellt:

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

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle möglichen Ursachen des NRER-Alarms bei der Netzwerkkonfiguration.

- Wenn der Fehler durch eine nicht übereinstimmende FEC verursacht wird, führen Sie die folgenden Schritte aus:

Hinweis: Diese Schritte gelten nur für NRER-Fehler, die durch FEC-Diskrepanz auf StorageGRID-Geräten verursacht werden.

- i. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID-Gerät angeschlossen ist.
- ii. Überprüfen Sie die physikalische Integrität der Kabel vom Gerät zum Switch.
- iii. Wenn Sie die FEC-Einstellungen ändern möchten, um den NRER-Alarm zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Konfiguration verknüpfen“ des Installationsprogramms von StorageGRID-Geräten für den **Auto**-Modus konfiguriert ist (siehe Installations- und Wartungsanweisungen für Ihr Gerät). Ändern Sie dann die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

(Sie können FEC-Einstellungen auf StorageGRID-Geräten nicht konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu erkennen und zu spiegeln, an denen sie angeschlossen sind. Wenn die Verbindungen zu 25-GbE- oder 100-GbE-Netzwerkgeschwindigkeiten gezwungen sind, können Switch und NIC eine gemeinsame FEC-Einstellung nicht aushandeln. Ohne eine gemeinsame FEC-Einstellung kehrt das Netzwerk in den Modus „no-FEC“ zurück. Wenn FEC nicht aktiviert ist, sind die Anschlüsse anfälliger für Fehler, die durch elektrische Geräusche verursacht werden.)

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

- Wenn der Fehler durch einen Switch Port und eine nicht übereinstimmende NIC MTU verursacht wird, überprüfen Sie, ob die auf dem Node konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port identisch ist.

Die auf dem Node konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung am Switch-Port, mit dem der Node verbunden ist. Wenn ein StorageGRID-Knoten einen Ethernet-Frame empfängt, der größer ist als seine MTU, was mit dieser Konfiguration möglich ist, wird möglicherweise der NRR-Alarm gemeldet. Wenn Sie der Ansicht sind, dass dies geschieht, ändern Sie entweder die MTU des Switch Ports entsprechend der StorageGRID Netzwerkschnittstelle MTU oder ändern Sie die MTU der StorageGRID-Netzwerkschnittstelle je nach Ihren End-to-End-Zielen oder Anforderungen an den Switch-Port.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen identisch sein.



Informationen zum Ändern der MTU-Einstellung finden Sie im Installations- und Wartungshandbuch für Ihre Appliance.

- Wenn der Fehler durch hohe Verbindungsfehlerraten verursacht wird, führen Sie die folgenden Schritte aus:
 - i. Aktivieren Sie FEC, falls nicht bereits aktiviert.
 - ii. Stellen Sie sicher, dass Ihre Netzkabel von guter Qualität sind und nicht beschädigt oder nicht ordnungsgemäß angeschlossen sind.
 - iii. Falls die Kabel nicht das Problem darstellen, wenden Sie sich an den technischen Support.



In einer Umgebung mit hohem elektrischen Rauschen können hohe Fehlerraten festgestellt werden.

- Wenn es sich bei dem Fehler um einen NIC-Ringpuffer handelt, wenden Sie sich an den technischen Support.

Der Ruffuffer kann bei Überlastung des StorageGRID-Systems überlaufen werden und kann Netzwerkereignisse nicht zeitnah verarbeiten.

2. Nachdem Sie das zugrunde liegende Problem gelöst haben, setzen Sie den Fehlerzähler zurück.

- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- b. Wählen Sie **site Grid Node SSM Ressourcen Konfiguration Main**.

c. Wählen Sie **Empfangspunkt zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Verwandte Informationen

[Fehler bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU](#)

[Alarmreferenz \(Altsystem\)](#)

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[SG5600 Storage Appliances](#)

[SG100- und SG1000-Services-Appliances](#)

Fehler bei der Zeitsynchronisierung beheben

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

Wenn Probleme mit der Zeitsynchronisierung auftreten, stellen Sie sicher, dass Sie mindestens vier externe NTP-Quellen angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern, und dass alle externen NTP-Quellen normal funktionieren und von Ihren StorageGRID-Knoten zugänglich sind.



Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt.

Verwandte Informationen

[Recovery und Wartung](#)

Linux: Probleme mit der Netzwerkverbindung

Möglicherweise werden Probleme mit der Netzwerkverbindung für StorageGRID Grid-Nodes auftreten, die auf Linux-Hosts gehostet werden.

Klonen VON MAC Adressen

In einigen Fällen können Netzwerkprobleme mithilfe des Klonens von MAC-Adressen behoben werden. Wenn Sie virtuelle Hosts verwenden, legen Sie den Wert des MAC-Adressenklonens für jedes Ihrer Netzwerke in der Node-Konfigurationsdatei auf „true“ fest. Diese Einstellung bewirkt, dass die MAC-Adresse des StorageGRID-Containers die MAC-Adresse des Hosts verwendet. Informationen zum Erstellen von Node-Konfigurationsdateien finden Sie in den Anweisungen im Installationshandbuch für Ihre Plattform.



Erstellen Sie separate virtuelle Netzwerkschnittstellen, die vom Linux Host-Betriebssystem verwendet werden können. Die Verwendung derselben Netzwerkschnittstellen für das Linux-Hostbetriebssystem und den StorageGRID-Container kann dazu führen, dass das Host-Betriebssystem 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 im Installationshandbuch für Ihre Plattform.

Promiskuous Modus

Wenn Sie kein Klonen der MAC-Adresse verwenden möchten und lieber alle Schnittstellen Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen empfangen und übertragen möchten, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene der virtuellen Switch- und Portgruppen auf **Accept** für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen eingestellt sind. Die auf dem virtuellen Switch eingestellten Werte können von den Werten auf der Portgruppenebene außer Kraft gesetzt werden. Stellen Sie also sicher, dass die Einstellungen an beiden Stellen identisch sind.

Verwandte Informationen

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

Linux: Node-Status lautet „verwaiste“

Ein Linux-Node in einem verwaisten Status gibt in der Regel an, dass entweder der StorageGRID-Service oder der StorageGRID-Node-Daemon, der den Container steuert, unerwartet gestorben ist.

Über diese Aufgabe

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

- Überprüfen Sie die Protokolle auf Fehler und Meldungen.
- Versuchen Sie, den Node erneut zu starten.
- Verwenden Sie bei Bedarf Befehle der Container-Engine, um den vorhandenen Node-Container zu beenden.
- Starten Sie den Node neu.

Schritte

1. Überprüfen Sie die Protokolle sowohl für den Service-Daemon als auch für den verwaisten Node auf offensichtliche Fehler oder Meldungen zum unerwarteten Beenden.
2. Melden Sie sich beim Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung.
3. Versuchen Sie, den Node 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 Node verwaiste ist, wird die Antwort angezeigt

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

4. Stoppen Sie von Linux die Container-Engine und alle kontrollierenden storagegrid Node-Prozesse.
Beispiel: `sudo docker stop --time seconds container-name`

Für `seconds` Geben Sie die Anzahl der Sekunden ein, die Sie warten möchten, bis der Container angehalten wird (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 Sie bemerken, dass den Knoten-Containern keine IPv6-Adressen wie erwartet zugewiesen wurden.

Über diese Aufgabe

Die IPv6-Adresse, die einem Grid-Node zugewiesen wurde, wird in den folgenden Speicherorten im Grid Manager angezeigt:

- Wählen Sie **NODES** aus, und wählen Sie den Knoten aus. Wählen Sie dann auf der Registerkarte Übersicht neben **IP-Adressen** die Option **Mehr anzeigen** aus.

DC1-S2 (Storage Node)

Overview Hardware Network Storage Objects ILM Tasks

Node information

Name: DC1-S2
Type: Storage Node
ID: 352bd978-ff3e-45c5-aac1-24c7278206fa
Connection state: ✔ Connected
Storage used: Object data 0% Object metadata 0%
Software version: 11.6.0 (build 20210924.1557.00aSeb9)
IP addresses: 172.16.1.227 - eth0 (Grid Network)
10.224.1.227 - eth1 (Admin Network)
[Hide additional IP addresses](#)

Interface	IP address
eth0 (Grid Network)	172.16.1.227
eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532

- Wählen Sie **SUPPORT Tools Grid-Topologie** aus. Wählen Sie dann **Node SSM Ressourcen** aus. Wenn eine IPv6-Adresse zugewiesen wurde, wird sie unter der IPv4-Adresse im Abschnitt **Netzwerkadressen** aufgelistet.

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 an oder verwenden Sie ein Konto mit sudo-Berechtigung.
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 die Dokumentation zum Ändern des Betriebssystems `sysctl` Einstellungen. Ändern Sie dann den Wert in 0, bevor Sie fortfahren.

3. Geben Sie den StorageGRID-Node-Container 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 Behälter: `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 beiden Zeilen, und entfernen Sie die Kommentar-Tags. Speichern und schließen Sie anschließend die Datei.

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

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

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

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

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

Fehlerbehebung für einen externen Syslog-Server

In der folgenden Tabelle werden Fehlermeldungen des externen Syslog-Servers beschrieben und Korrekturmaßnahmen aufgeführt.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Hostname kann nicht aufgelöst werden	<p>Der für den Syslog-Server eingegebene FQDN konnte nicht in eine IP-Adresse aufgelöst werden.</p> <ol style="list-style-type: none">Überprüfen Sie den eingegebenen Hostnamen. Wenn Sie eine IP-Adresse eingegeben haben, stellen Sie sicher, dass es sich um eine gültige IP-Adresse in der Schreibweise W.X.Y.Z („gepunktete Dezimalstelle“) handelt.Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind.Vergewissern Sie sich, dass jeder Knoten auf die IP-Adressen des DNS-Servers zugreifen kann.
Verbindung abgelehnt	<p>Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde abgelehnt. Möglicherweise ist auf dem TCP- oder TLS-Port für den Host kein Service verfügbar, oder eine Firewall blockiert möglicherweise den Zugriff.</p> <ol style="list-style-type: none">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.Vergewissern Sie sich, dass der Host für den syslog-Service einen Syslog-Daemon ausführt, der auf dem angegebenen Port abhört.Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten auf die IP und den Port des Syslog-Servers blockiert.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Netzwerk nicht erreichbar	<p>Der Syslog-Server befindet sich nicht in einem direkt verbundenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass die Testmeldungen von den aufgeführten Knoten nicht an den Syslog-Server weitergeleitet werden konnten.</p> <ol style="list-style-type: none"> 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 Node die Liste des Grid-Netzwerksnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese konfiguriert sind, um Datenverkehr zum Syslog-Server über die erwartete Netzwerkschnittstelle und das erwartete Gateway (Grid, Administrator oder Client) zu leiten.
Host nicht erreichbar	<p>Der Syslog-Server befindet sich in einem direkt verbundenen Subnetz (Subnetz, das von den aufgeführten Knoten für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Knoten versuchten, Testmeldungen zu senden, erhielten aber keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers.</p> <ol style="list-style-type: none"> 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-Service ausgeführt wird, ausgeführt wird.
Zeitüberschreitung bei Verbindung	<p>Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber für lange Zeit wurde vom Syslog-Server keine Antwort empfangen. Möglicherweise gibt es eine Fehlkonfiguration bei Routing oder eine Firewall könnte den Datenverkehr ohne jede Antwort löschen (eine häufige Konfiguration).</p> <ol style="list-style-type: none"> 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 Node die Liste des Grid-Netzwerksnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese konfiguriert sind, um Datenverkehr über die Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) an den Syslog-Server weiterzuleiten, über den Sie erwarten, dass der Syslog-Server erreicht wird. 3. Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten blockiert, die in der IP und dem Port des Syslog-Servers aufgeführt sind.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Verbindung vom Partner geschlossen	<p>Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, wurde aber später geschlossen. Gründe hierfür sind u. a.:</p> <ul style="list-style-type: none"> • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gestartet. • Der Node und der Syslog-Server verfügen möglicherweise über unterschiedliche TCP/TLS-Einstellungen. • Bei einer Zwischenfirewall werden möglicherweise inaktive TCP-Verbindungen geschlossen. • Ein nicht-Syslog-Server, der auf dem Syslog-Server-Port hört, hat die Verbindung möglicherweise geschlossen. <ul style="list-style-type: none"> a. 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. b. Wenn Sie TLS verwenden, bestätigen Sie, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, bestätigen Sie, dass der Syslog-Server auch TCP verwendet. c. Überprüfen Sie, ob eine Zwischenfirewall nicht für das Schließen inaktiver TCP-Verbindungen konfiguriert ist.
Fehler beim TLS-Zertifikat	<p>Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen angegebenen CA-Zertifikatspaket und dem von Ihnen angegebenen Clientzertifikat kompatibel.</p> <ol style="list-style-type: none"> 1. Vergewissern Sie sich, dass das CA-Zertifikatsbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat auf dem Syslog-Server kompatibel sind. 2. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Weiterleitung angehalten	<p>Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet, und StorageGRID kann den Grund nicht erkennen.</p> <p>Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln.</p>

Fehlermeldung	Beschreibung und empfohlene Aktionen
TLS-Sitzung beendet	<p>Der Syslog-Server hat die TLS-Sitzung beendet und StorageGRID kann den Grund nicht erkennen.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, 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, bestätigen Sie, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, bestätigen Sie, dass der Syslog-Server auch TCP verwendet. 4. Vergewissern Sie sich, dass das CA-Zertifikatsbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat vom Syslog-Server kompatibel sind. 5. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Abfrage der Ergebnisse fehlgeschlagen	<p>Der für die Konfiguration und Tests des Syslog-Servers verwendete Admin-Node kann die Testergebnisse nicht von den aufgeführten Nodes anfordern. Mindestens ein Node ist ausgefallen.</p> <ol style="list-style-type: none"> 1. Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Services ausgeführt werden. 2. Starten Sie den falsch-Dienst auf den aufgeführten Knoten neu.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.