



Fehlerbehebung für das StorageGRID-System

StorageGRID software

NetApp
January 15, 2026

Inhalt

Fehlerbehebung für das StorageGRID-System	1
Fehler in einem StorageGRID System beheben	1
Definieren Sie das Problem	1
Bewerten Sie das Risiko und die Auswirkungen auf das System	1
Datenerfassung	2
Analysieren von Daten	6
Checkliste für Eskalationsinformationen	6
Behebung von Objekt- und Storage-Problemen	8
Bestätigen Sie den Speicherort der Objektdaten	8
Fehler beim Objektspeicher (Storage Volume)	10
Überprüfen Sie die Objektintegrität	12
Fehlerbehebung bei S3 PUT Objektgröße zu groß Warnung	16
Fehlerbehebung bei verlorenen und fehlenden Objektdaten	18
Beheben Sie die Warnung „Niedrig Object Data Storage“	21
Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff	23
Behebung von Metadatenproblemen	26
Fehlerbehebung bei Zertifikatfehlern	28
Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche	30
Anmeldefehler beim Admin-Node	30
Probleme bei der Benutzeroberfläche	33
Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen	33
Fehler „422: Nicht verarbeitbare Entität“	34
Alarm bei MTU-Nichtübereinstimmung im Grid-Netzwerk	35
Node-Netzwerk-Frame-Fehlerwarnung	36
Fehler bei der Zeitsynchronisierung	38
Linux: Probleme mit der Netzwerkverbindung	38
Linux: Knotenstatus ist „verwaist“	39
Linux: Fehlerbehebung bei der IPv6-Unterstützung	40
Fehlerbehebung für einen externen Syslog-Server	42
Fehlerbehebung beim Load Balancer-Caching	45
Ermitteln, ob eine Anfrage ein Cache-Treffer war	45
Niedrige Cache-Trefferquote	46
Geringe Leistung	46

Fehlerbehebung für das StorageGRID-System

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.

Häufig können Sie Probleme selbst lösen. Unter Umständen 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 berichten, 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 nicht.
Sind Daten gefährdet?	Nein
Ist die Fähigkeit, Geschäfte zu führen, stark beeinträchtigt?	Ja, da Client-Applikationen keine Objekte im StorageGRID System speichern können und Daten nicht konsistent abgerufen werden können.

Datenerfassung

Nach dem 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 diese Daten 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 Warnmeldungen	<p>Mithilfe von Warnmeldungen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise zu den zugrunde liegenden Problemen geben, die das Problem verursachen könnten.</p> <p>Prüfen Sie die Liste der aktuellen Meldungen, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat.</p> <p>Prüfen Sie in der Vergangenheit ausgelöste Warnmeldungen, um zusätzliche Informationen zu erhalten.</p>	<ul style="list-style-type: none"> "Anzeige aktueller und aufgelöster Warnmeldungen"
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

Art der zu erfassenden Daten	Warum diese Daten sammeln	Anweisungen
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"
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 Objektverifizierungsvergängen" "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" "Starten Sie manuell ein AutoSupport-Paket" "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 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	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm Speicher verwendet - Objektdaten einen Zeitraum, in dem die Linie ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Speicherplatz jeden Tag verbraucht wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm „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 täglich belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Rate der S3-Operationen	Vorgänge/Sekunde	Wählen Sie im Grid Manager-Dashboard Leistung > S3-Vorgänge für Speicherknoten . Um die Aufnahme- und Abrufarten sowie die Anzahl für eine bestimmte Site oder einen bestimmten Knoten anzuzeigen, wählen Sie Knoten > Site oder Speicherknoten > Objekte . Positionieren Sie Ihren Cursor über dem S3-Aufnahme- und Abrufdiagramm.
ILM-Auswertungsrate	Objekte/Sekunde	Wählen Sie auf der Seite Knoten GRID > ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für Bewertungsrate für Ihr System zu schätzen.

Eigenschaft	Wert	Wie zu erhalten
ILM-Scan-Rate	Objekte/Sekunde	<p>Wählen Sie Knoten > grid > ILM.</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 Basislinienwert für Scan-Rate für Ihr System abzuschätzen.</p>
Objekte, die sich aus Client-Vorgängen in Warteschlange befinden	Objekte/Sekunde	<p>Wählen Sie Knoten > grid > ILM.</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 Basislinienwert für Objekte in der Warteschlange (von Client-Operationen) für Ihr System abzuschätzen.</p>
Durchschnittliche Abfragelatenz	Millisekunden	<p>Wählen Sie Knoten > Speicherknoten > Objekte. Zeigen Sie in der Abfragetabelle den Wert für die durchschnittliche Latenz an.</p>

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:

- Ermitteln Sie mithilfe der Warnmeldungen Points of Failure und Engpässe.
- Rekonstruieren Sie den Problemverlauf mithilfe des Alarmverlaufs und der 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 alleine 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	<p>Was sind die Problemsymptome? Wann hat das Problem begonnen? Passiert es konsequent oder intermittierend? Welche Zeiten hat es gelegentlich gegeben?</p> <p>Definieren Sie das Problem</p>

	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 als Teil 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? • Werden replizierte oder Erasure-Coded-Objekte von ILM erstellt? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das ausgewogene, strikte oder duale Commit-Aufnahmeverhalten?
	Log-Dateien und Systemdaten	<p>Sammeln Sie Protokolldateien und Systemdaten für Ihr System. Wählen Sie Support > Tools > Protokollsammlung.</p> <p>Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln.</p> <p>Wenn Sie Protokolle nur für ausgewählte Knoten sammeln, achten Sie darauf, mindestens einen Speicherknoten einzuschließen, der über den ADC-Dienst verfügt. Die ersten drei an einem Standort installierten Speicherknoten umfassen den ADC-Dienst.</p>
	Basisinformationen	<p>Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch</p> <p>Basispläne erstellen</p>
	Zeitachse der letzten Änderungen	<p>Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind.</p> <p>Erstellen Sie eine Zeitleiste der neusten Änderungen</p>
	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 dem Problem möchten Sie vielleicht "[Bestätigen Sie, wo Objektdaten gespeichert werden](#)". Beispielsweise möchten Sie überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und Objektdaten dort gespeichert werden, wo sie geplant sind.

Bevor Sie beginnen

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

Schritte

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

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

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

The screenshot shows a web-based application window titled "Object Metadata Lookup". Below the title, there is a sub-instruction: "Enter the identifier for any object stored in the grid to view its metadata.". There are two input fields: the first is labeled "Identifier" and contains the value "source/testobject"; the second is labeled "Version ID (optional)" and contains a long, randomly generated string of characters. At the bottom of the form is a blue rectangular button labeled "Look Up".

4. Wählen Sie **Look Up**.

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

- Systemmetadaten, einschließlich Objekt-ID (UUID), Version-ID (optional), Objektname, Name des Containers, Mandantenkontoname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien

- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FC0-31FF00C36056",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",
      "PAWS2": "2"
    }
  }
}
```

Fehler beim Objektspeicher (Storage Volume)

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

Sie können Objektspeicherinformationen für jeden Speicherknoten anzeigen. Wählen Sie **Knoten > Speicherknoten > Speicher**.

Disk devices

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

Volumes

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

Object stores

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

Je nach Art des Ausfalls können Fehler bei einem Speicher-Volume in dargestellt werden "[Warnmeldungen zu Storage-Volumes](#)". Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um den Speicherknoten so bald wie möglich wieder voll zu machen. Bei Bedarf können Sie auf die Registerkarte **Konfiguration** gehen "[Setzen Sie den Speicher-Node in einen schreibgeschützten Status](#)", damit das StorageGRID-System es für den Datenabruf nutzen kann, während Sie sich auf eine vollständige Wiederherstellung des Servers vorbereiten.

Überprüfen Sie die Objektintegrität

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

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

Was ist Hintergrundüberprüfung?

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

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

- **Replizierte Objekte:** Findet der Hintergrundverifizierungsvorgang ein beschädigtes Objekt, wird die beschädigte Kopie vom Speicherort entfernt und an anderer Stelle auf dem Speicherknoten isoliert. Anschließend wird eine neue, nicht beschädigte Kopie generiert und gemäß den aktiven ILM-Richtlinien abgelegt. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die ursprüngliche Kopie verwendet wurde.
- **Erasure-codierte Objekte:** Erkennt der Hintergrund-Verifizierungsprozess, dass ein Fragment eines Löschungscodierten Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Daten- und Paritätsfragmente neu zu erstellen. Wenn das beschädigte Fragment nicht neu erstellt werden kann, wird versucht, eine weitere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Bewertung durchgeführt, um eine Ersatzkopie des Objekts, das mit der Fehlerkorrektur codiert wurde, zu erstellen.

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

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

Warnmeldungen zur Hintergrundüberprüfung

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

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

Was ist Objektexistenz-Prüfung?

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

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

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

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

Überprüfung der Objektexistenz ausführen

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Berechtigung für Wartung oder Root-Zugriff](#)".
- Sie haben sichergestellt, dass die Speicherknoten, die Sie überprüfen möchten, online sind. Wählen Sie **Knoten** aus, um die Knotentabelle anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen der Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden 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

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

Schritte

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

Sie können nach Node-Namen oder Site suchen.

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

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

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

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

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

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

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

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

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

- Der Job ist abgeschlossen.

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



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

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

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

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

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 die Anzahl der erkannten fehlenden Objektkopien größer als Null ist und die Warnung „Möglicherweise verlorene Objekte“ nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Stellen Sie sicher, dass alle Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu verhindern.
- Wenn die Anzahl der erkannten fehlenden Objektkopien größer als Null ist und die Warnung „Möglicherweise verlorene Objekte“ ausgelöst wurde, kann die Datenintegrität beeinträchtigt sein. Wenden Sie sich an den technischen Support.
- Sie können potenziell verlorene Objektkopien untersuchen, indem Sie mit grep die LLST-Auditmeldungen extrahieren: `grep LLST audit_file_name`.

Dieses Verfahren ist ähnlich wie bei "[Untersuchung potenziell verlorener Objekte](#)", obwohl Sie für Objektkopien nach LLST anstatt OLST.

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

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

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

b. Legen Sie fest, welche Jobs für die erneute Ausführung bereit sind:

- Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.
- Überprüfen Sie für diese Jobs die Spalte Consistency Control auf Strong-site oder strong-global.

- c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **erneut ausführen**.
- d. Überprüfen Sie im Assistenten Jobs erneut ausführen die ausgewählten Knoten und Volumes sowie die Konsistenz.
- e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Rerun**.

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

Fehlerbehebung bei S3 PUT Objektgröße zu groß Warnung

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".

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

Schritte

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

- a. Eingabe ssh admin@primary_Admin_Node_IP
- b. Geben Sie das in der Datei aufgeführte Passwort ein Passwords.txt.
- c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: su -
- d. Geben Sie das in der Datei aufgeführte Passwort ein Passwords.txt.

Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von \$ zu #.

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

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

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

Option	Ziel
Externer Syslog-Server	/var/local/log/localaudit.log

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

Weitere Informationen finden Sie unter "[Protokollspeicherort auswählen](#)".

- f. Ermitteln Sie, welche Mandanten Objekte mit einer Größe von mehr als 5 gib verwenden.
 - i. Eingabe zgrep SPUT * | egrep "CSIZ\ (UI64\):[([5-9]\|[1-9]\ [0-9]\+)[0-9]\{9\}"
 - ii. Überprüfen Sie für jede Überwachungsmeldung in den Ergebnissen das Feld unter S3AI, um die Konto-ID des Mandanten zu ermitteln. Verwenden Sie die anderen Felder in der Meldung, um zu bestimmen, welche IP-Adresse vom Client, vom Bucket und vom Objekt verwendet wurde:

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

Beispiel für Ergebnisse des Audit-Protokolls

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"060X85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Wenn die Schreibvorgänge des Clients nicht normal sind, verwenden Sie die Mandanten-ID in der Warnmeldung, um den Mandanten zu identifizieren:
 - a. Gehen Sie zu **Support > Tools > Protokollsammlung**. Sammeln Sie Anwendungsprotokolle für den Speicherknoten in der Warnung. Geben Sie 15 Minuten vor und nach der Warnung an. Weitere

Informationen finden Sie unter "["Erfassen von Protokolldateien und Systemdaten"](#)".

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

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

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

Beispiel broadcast.log

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

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

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

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

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

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

Sie sollten alle Warnmeldungen zu potenziell verlorenen Objekten sofort untersuchen, um die Grundursache des Verlusts zu ermitteln und festzustellen, ob das Objekt möglicherweise noch in einem Offline- oder aus anderen Gründen derzeit nicht verfügbaren Speicherknoten vorhanden ist. Sehen ["Untersuchen Sie möglicherweise verlorene Objekte"](#). Aus Vorsicht kann es vorkommen, dass Benachrichtigungen über verlorene Gegenstände fälschlicherweise ausgelöst werden.

Für den Fall, dass Objektdaten ohne Kopien verloren gehen, gibt es keine Wiederherstellungslösung. Sie

müssen jedoch "[Setzen Sie den Zähler für potenziell verlorene Objekte zurück](#)" um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte verdecken.

Untersuchen Sie möglicherweise verlorene Objekte

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

Bevor Sie beginnen

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

Über diese Aufgabe

Die Warnung **Möglicherweise verlorene Objekte** weist darauf hin, dass gemäß den verfügbaren Informationen in StorageGRID keine Kopien eines Objekts im Grid vorhanden sind. Möglicherweise sind die 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.



Wenn mehr als 10 Objekte als verloren gemeldet werden, wenden Sie sich an den technischen Support. Führen Sie dieses Verfahren nicht selbst durch.

Schritte

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

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

4. Von einem Admin-Knoten aus, "[Rufen Sie das Überwachungsprotokoll auf](#)" So ermitteln Sie die eindeutige Kennung (UUID) des Objekts, das die Warnung „Möglicherweise verlorene Objekte“ 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 in der Datei aufgeführte Passwort ein `Passwords.txt`.
 - iii. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
 - iv. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`. Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von \$ zu #.
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden.

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

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

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

Weitere Informationen finden Sie unter "[Protokollspeicherort auswählen](#)".

- Verwenden Sie grep, um die Audit-Meldungen zu „Objekt verloren“ (OLST) zu extrahieren. Eingabe:
grep OLST audit_file_name
- 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]]
```

- Suchen Sie mit der UUID nach den Metadaten für das verlorene Objekt:

- Wählen Sie **ILM > Object Metadata Lookup**.
- Geben Sie die UUID ein, und wählen Sie **Look Up**.
- Überprüfen Sie die Speicherorte in den Metadaten, und ergreifen Sie die entsprechenden Maßnahmen:

Metadaten	Schlussfolgerung
Das Objekt-<object_identifier> wurde nicht gefunden	<p>Wenn das Objekt nicht gefunden wird, wird die Meldung „ERROR“ zurückgegeben.</p> <p>Wenn das Objekt nicht gefunden wird, Setzen Sie den Zähler für potenziell verlorene Objekte zurück, um die Warnung zu löschen. Das Fehlen eines Objekts weist darauf hin, dass das Objekt absichtlich gelöscht wurde.</p>

Metadaten	Schlussfolgerung
Standorte > 0	<p>Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung „Möglicherweise verlorene Objekte“ ein Fehlalarm 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>Wenn die Objekte vorhanden sind, Setzen Sie den Zähler für potenziell verlorene Objekte zurück, um die Warnung zu löschen.</p>
Standorte = 0	<p>Wenn in der Ausgabe keine Standorte aufgeführt sind, fehlt das Objekt möglicherweise. Wenden Sie sich an den technischen Support.</p> <p>Vom technischen Support bitten Sie möglicherweise, zu bestimmen, ob ein Verfahren zur Storage-Recovery durchgeführt wird. Siehe die Informationen über "Wiederherstellen von Objektdaten mit Grid Manager" und "Wiederherstellung von Objektdaten auf einem Storage-Volume".</p>

6. Nachdem Sie die Probleme mit verlorenen Objekten behoben haben, setzen Sie den Zähler für potenziell verlorene Objekte zurück, um sicherzustellen, dass es sich bei den Warnungen nicht um Fehlalarme handelt:
 - a. Wählen Sie **Knoten** aus.
 - b. Wählen Sie **Speicherknoten > Aufgaben**.
 - c. Wählen Sie im Abschnitt „Zähler potenziell verlorener Objekte zurücksetzen“ die Option „Zurücksetzen“ aus.

Beheben Sie die Warnung „Niedrig Object Data Storage“

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben ["Bestimmte Zugriffsberechtigungen"](#).

Über diese Aufgabe

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

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

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

In diesem Zustand:

- `storagegrid_storage_utilization_data_bytes` Ist eine Schätzung der Gesamtgröße replizierter und Erasure-Coded-Objektdaten für einen Storage Node.
- `storagegrid_storage_utilization_usable_space_bytes` Ist die Gesamtmenge des für einen Storage-Node verbleibenden Objektspeichers.

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 **Warnungen > Aktuell**.

Die Seite „Meldungen“ wird angezeigt.

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



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

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

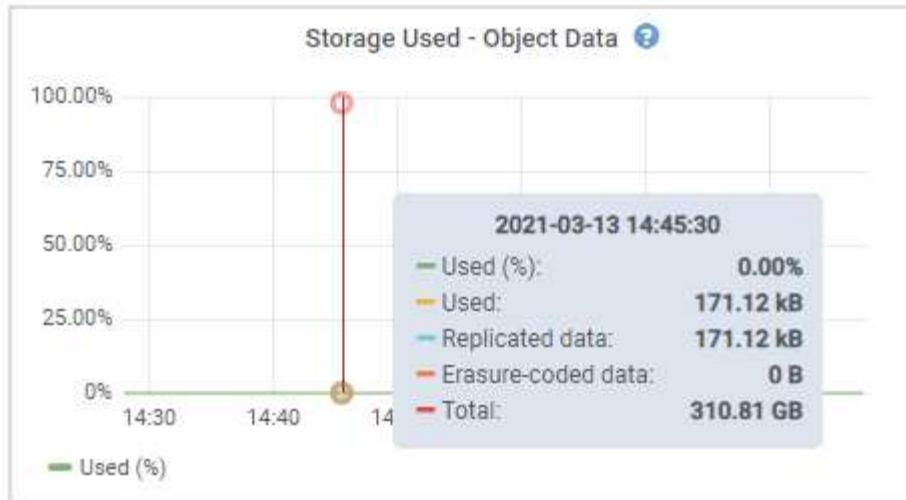
- Auslösezeit
- Der Name des Standorts und des Nodes
- Die aktuellen Werte der Metriken für diese Meldung

4. Wählen Sie **Knoten > Speicherknoten oder -site > Speicher**.

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

Die folgenden Werte werden angezeigt:

- **Used (%)**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Verwendet**: Die Menge des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Replizierte Daten**: Eine Schätzung der Menge der replizierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Erasure-codierte Daten**: Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt**: Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist die `storagegrid_storage_utilization_data_bytes` Metrik.



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

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

7. So bald wie möglich, "[Ergänzen Sie die Speicherkapazität](#)" in Ihr Raster.

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



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

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 früheren Versionen handelte es sich bei den drei "[Wasserzeichen für Storage-Volumes](#)" um globale Einstellungen — dieselben Werte gelten für jedes Speicher-Volume auf jedem Speicher-Node. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Storage Volume optimieren, basierend auf der Größe des Storage-Nodes und der relativen Kapazität des Volumes.

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

- Ihr System ist in der Nähe der Kapazität und kann keine neuen Daten akzeptieren, wenn optimierte Wasserzeichen angewendet wurden. StorageGRID ändert in diesem Fall keine Wasserzeichen-Einstellungen.
- Sie haben zuvor eine der Storage-Volume-Wasserzeichen auf einen benutzerdefinierten Wert gesetzt. StorageGRID überschreibt keine benutzerdefinierten Wasserzeichen-Einstellungen mit optimierten Werten. StorageGRID löst jedoch möglicherweise die Warnung **Low read-only Watermark override** aus, wenn Ihr

benutzerdefinierter Wert für das Speichervolumen-Softread-only-Wasserzeichen 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 der Warnmeldung gibt an, dass der benutzerdefinierte Wert des Speichervolumes mit weichem Lesezugriff kleiner ist als der minimale optimierte Wert für diesen Speicher-Node. 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 das Speichervolumen-Softread-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:

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

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

Beheben Sie die Meldung

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

Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Root-Zugriffsberechtigung](#)".

Über diese Aufgabe

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

Bewertung der Nutzung von Objektdaten für das gesamte Grid

Schritte

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

Anzeigen optimierter Storage-Wasserzeichen

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das schreibgeschützte weiche Wasserzeichen des Storage-Volumes berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

Schritte

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

```
storagegrid_storage_volume_minimum_optimized_soft_READONLY_watermark
```

In der letzten Spalte wird der minimale optimierte Wert des weichen schreibgeschützten Wasserzeichens für alle Speicher-Volumes auf jedem Storage Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das Speichervolume-Softread-only-Wasserzeichen, wird die Warnmeldung **Low read-only Watermark override** für den Speicherknoten 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 maximale optimierte Wert des weichen schreibgeschützten Wasserzeichens für alle Speicher-Volumes auf jedem Storage Node angezeigt.

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

Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können

Schritte

1. Wählen Sie **Knoten** aus.

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

Andernfalls erweitern Sie das Raster so schnell wie möglich. Entweder "[Storage-Volumes hinzufügen](#)" zu einem vorhandenen Knoten oder "[Neue Storage-Nodes hinzufügen](#)". Gehen Sie dann zu, um die Wasserzeicheneinstellungen zu [Verwenden Sie optimierte Wasserzeichen aktualisieren](#).
4. Wenn Sie weiterhin benutzerdefinierte Werte für die Wasserzeichen des Speichervolumes verwenden 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 abhängt), wenn der Node die Kapazität erreicht.

optimierte Wasserzeichen verwenden

Schritte

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

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

Behebung von Metadatenproblemen

Wenn Metadatenprobleme auftreten, werden Sie über die Ursache des Fehlers und über die empfohlenen Maßnahmen informiert. Sie müssen insbesondere neue Storage-Nodes hinzufügen, wenn die Warnmeldung zur Speicherung geringer Metadaten ausgelöst wird.

Bevor Sie beginnen

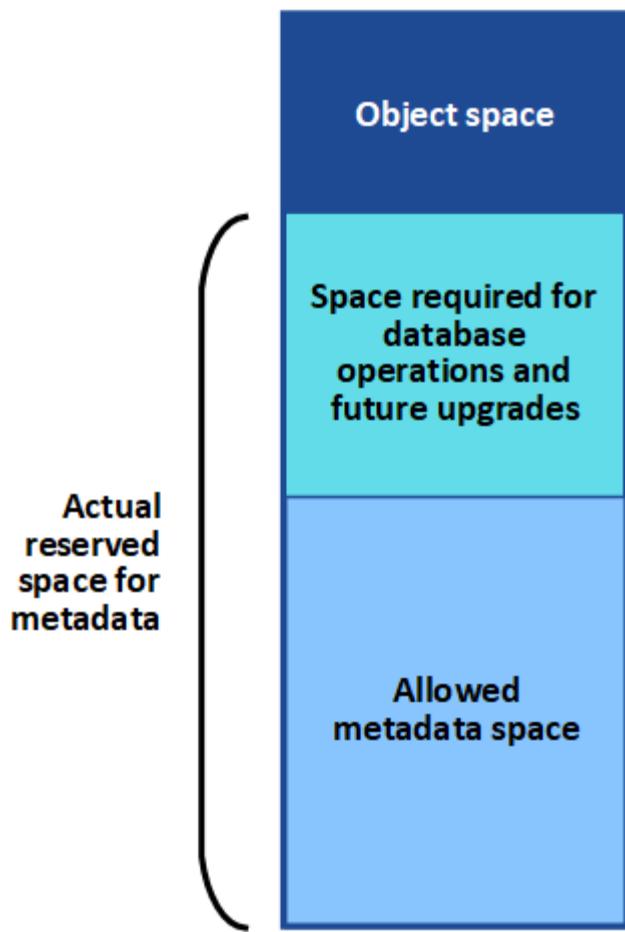
Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".

Über diese Aufgabe

Befolgen Sie die empfohlenen Aktionen für jede Metadatenbezogene Warnmeldung, die ausgelöst wird. Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

StorageGRID reserviert eine bestimmte Menge an Speicherplatz auf Volume 0 jedes Storage-Nodes für Objekt-Metadaten. Dieser als *actual reserved space* bekannte Speicherplatz wird in den für Objektmetadaten erlaubten Speicherplatz (den erlaubten Metadatenraum) und den für wichtige Datenbankvorgänge wie Data-Compaction und Repair erforderlichen Speicherplatz unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.

Volume 0



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

Sie können "[Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node](#)" Ihnen dabei helfen, Fehler vorherzusehen und zu korrigieren, 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:** Objektmetadaten verwenden 70% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie sollten so bald wie möglich neue Storage-Nodes hinzufügen.
- **Major:** Objektmetadaten verwenden 90% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie müssen sofort neue Storage-Nodes hinzufügen.



Wenn Objektmetadaten 90 % oder mehr des zulässigen Metadatenspeichers verwenden, wird eine Warnung im Dashboard 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.



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 **Warnungen > Aktuell**.
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 einem Standort Metadaten-Kapazität hinzufügen müssen, sollten Sie ebenfalls "[Erweitern Sie alle anderen Standorte](#)" die gleiche Anzahl von Storage-Nodes verwenden.

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.

Fehlerbehebung bei Zertifikatfehlern

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

Über diese Aufgabe

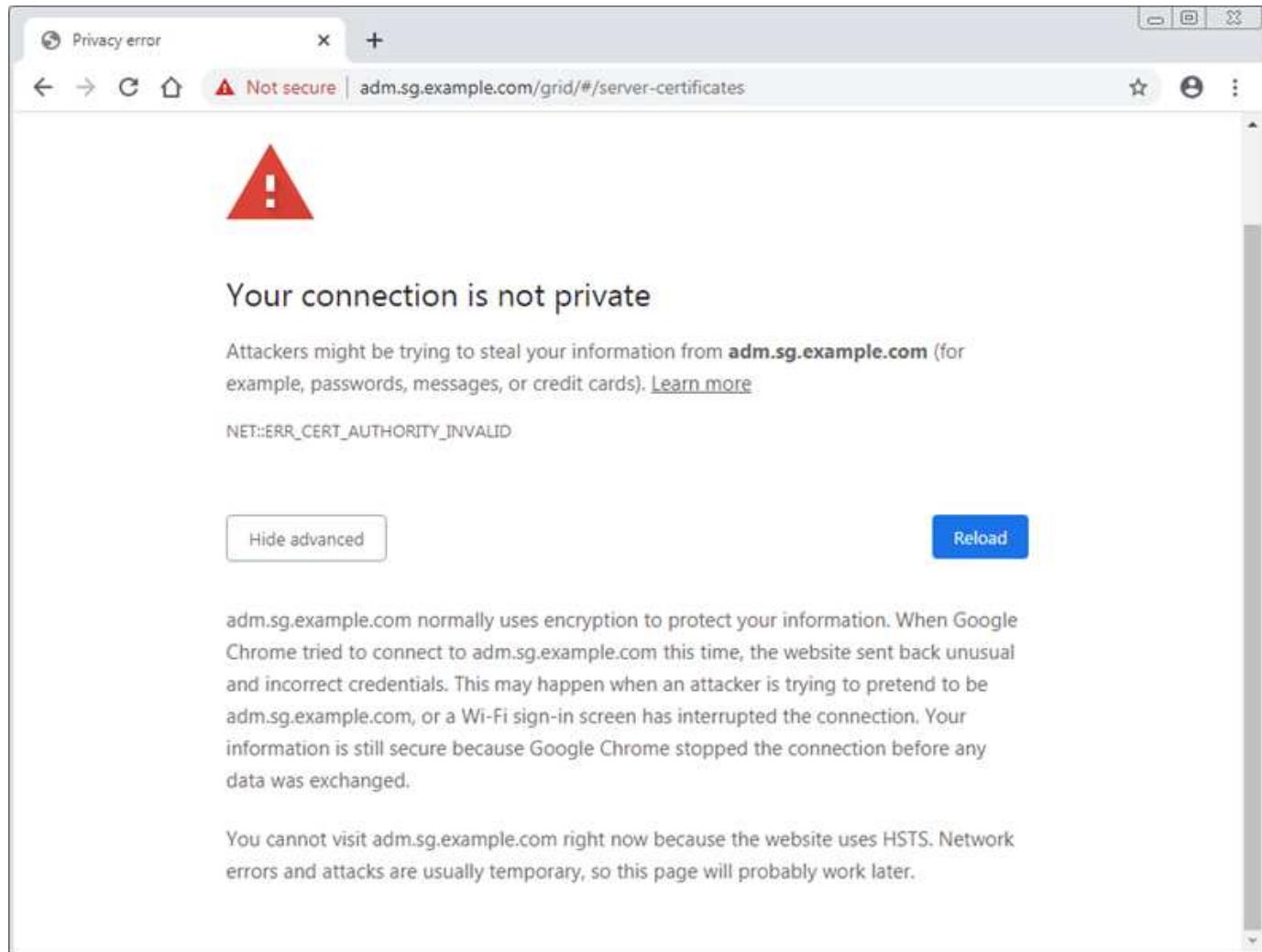
Zertifikatfehler können Probleme verursachen, wenn Sie versuchen, eine Verbindung mit StorageGRID mithilfe des Grid Managers, der Grid Management API, des Mandantenmanagers oder der Mandantenmanagement-API herzustellen. Zertifikatfehler können auch auftreten, wenn Sie versuchen, eine Verbindung mit einem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

Wenn Sie mit einem Domänennamen 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 der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnmeldung **Ablauf des Serverzertifikats für die Managementoberfläche** ausgelöst, wenn das Serverzertifikat abläuft.

Wenn Sie Clientzertifikate für die externe Prometheus-Integration verwenden, können Zertifikatfehler 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 Warnmeldung über ein abgelaufenes Zertifikat erhalten haben, greifen Sie auf die Zertifikatsdetails zu: . 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-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.

- Informationen zu einem Serverzertifikat finden Sie in den Schritten für "[Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#)".
 - Informationen zu einem Clientzertifikat finden Sie in den Schritten für "[Konfigurieren eines Client-Zertifikats](#)".
3. Versuchen Sie bei Serverzertifikatfehlern 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 **Konfiguration > Sicherheit > Zertifikate** und dann "[Wählen Sie die entsprechende Registerkarte Zertifikat aus](#)" um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
 - iii. In den Anweisungen zum Verwalten von StorageGRID finden Sie die Schritte für "[Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#)".

Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche

Sie können mehrere Aufgaben durchführen, um die Quelle von Problemen im Zusammenhang mit Administratorknoten und der StorageGRID-Benutzeroberfläche zu ermitteln.

Anmeldefehler beim Admin-Node

Wenn bei der Anmeldung bei einem StorageGRID-Administratorknoten ein Fehler auftritt, liegt möglicherweise ein Problem mit oder "[Trennt](#)", ein Problem mit "[Admin Node Services](#)", oder ein "[Problem mit der Cassandra-Datenbank](#)" auf verbundenen Speicherknoten vor "[Netzwerk](#)".

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die `Passwords.txt` Datei.
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".

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 über mehr als einen Administratorknoten verfügt, melden Sie sich von einem anderen Administratorknoten beim Grid-Manager an, um den Status eines nicht verfügbaren Administratorknotens zu überprüfen.

- Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **Knoten**, **Warnungen** und **Support** verwenden, um die Fehlerursache zu ermitteln.
- Wenn Sie nur einen Admin-Knoten haben oder sich immer noch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.

3. Ermitteln, ob die Hardware des Node offline ist

4. Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, lesen Sie die Schritte für "[Konfigurieren der Single Sign-On-Funktion](#)".

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 über einen 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. Prüfen von Warnmeldungen
 - ii. Wählen Sie **Konfiguration > Zugriffskontrolle > Identitätsföderation**.
 - 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 der lokale Benutzer sich nicht anmelden kann und Sie sicher sind, dass die Anmeldeinformationen korrekt sind, fahren Sie mit dem nächsten Schritt fort.

6. Verwenden Sie Secure Shell (SSH), um sich am Admin-Knoten anzumelden:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
- b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
- c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
- d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von \$ zu #.

7. Anzeigen des Status aller Dienste, die auf dem Grid-Knoten ausgeführt werden: `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. Verwenden Sie Lumberjack, um Protokolle zu sammeln: # /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
```

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

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

12. Melden Sie sich über den Admin-Knoten mit ssh bei jedem der ADC-Speicherknoten an, wobei die von Ihnen angegebenen IP-Adressen verwendet werden.
13. Anzeigen des Status aller Dienste, die auf dem Grid-Knoten ausgeführt werden: `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](#), um die Protokolle auf den Speicher-Nodes zu überprüfen.
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"](#).

Probleme bei der Benutzeroberfläche

Die Benutzeroberfläche des Grid-Managers oder des Mandantenmanagers reagiert nach der Aktualisierung der StorageGRID-Software möglicherweise nicht wie erwartet.

Schritte

1. Stellen Sie sicher, dass Sie einen [Unterstützter Webbrowser](#) verwenden.
2. 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.

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 „422: Nicht verarbeitbare Entität“

Der Fehler 422: Nicht verarbeitbare Entität kann aus verschiedenen Gründen 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
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</pre>	<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>

Fehlermeldung	Ursache und Korrekturmaßnahme
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	<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 für ausgehende TLS-Verbindungen verwenden "Von StorageGRID unterstützte Chiffren", wie in den Anweisungen zur Verwaltung von StorageGRID dargestellt.</p>

Alarm bei MTU-Nichtübereinstimmung im Grid-Netzwerk

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

- Der externe SSH-Zugriff ist standardmäßig blockiert. Falls erforderlich, "[Zugriff vorübergehend erlauben](#)".
- Führen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
 - Verwenden Sie die im Grid Manager angegebene Abfrage.
 - Navigieren Sie zur *primary Admin Node IP address/metrics/graph* folgenden Abfrage, und geben Sie sie ein: `node_network_mtu_bytes{device="eth0"}`
- "[Ändern Sie die MTU-Einstellungen](#)" Falls erforderlich, um sicherzustellen, dass sie für die Grid Network Interface (eth0) auf allen Knoten gleich sind.
 - Verwenden Sie für Linux- und VMware-basierte Nodes 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 Host-Schnittstelle konfigurierten Wert überschreitet, müssen Sie zuerst die Host-Schnittstelle so konfigurieren, dass der gewünschte MTU-Wert vorhanden ist, und dann mit dem `change-ip.py` Skript den MTU-Wert des Netzwerks im Container ändern.

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	Hilfescreen anzeigen und beenden.
-n node, --node node	Der Node. Die Standardeinstellung ist der lokale Knoten.

4. Wenn Sie externen SSH-Zugriff zugelassen haben, "[Zugriff blockieren](#)" wenn Sie die Aufgabe erledigt haben.

Node-Netzwerk-Frame-Fehlerwarnung

Node Network Reception Frame error Warnmeldungen können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerk-Hardware verursacht werden. Diese Warnmeldung wird eigenständig gelöscht, nachdem das zugrunde liegende Problem behoben wurde.

Über diese Aufgabe

Node Network Reception Frame error Warnmeldungen können durch die folgenden Probleme mit Netzwerk-Hardware verursacht werden, die mit StorageGRID verbunden wird:

- 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 potenziellen Ursachen dieser Warnung, wenn Sie Ihre Netzwerkkonfiguration beachten.
2. Führen Sie je nach Fehlerursache die folgenden Schritte aus:

FEC stimmt nicht überein



Diese Schritte gelten nur für **Node Network Reception Frame error**-Warnungen, die durch FEC-Nichtübereinstimmung auf StorageGRID-Geräten verursacht werden.

- a. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID-Gerät angeschlossen ist.
- b. Überprüfen Sie die physikalische Integrität der Kabel vom Gerät zum Switch.
- c. Wenn Sie die FEC-Einstellungen ändern möchten, um die Warnmeldung zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Verbindungsconfiguration“ des Installationsprogramms für das StorageGRID-Gerät für den Modus „automatisch“ konfiguriert ist (siehe die Anweisungen für Ihr Gerät):
 - "[SG6160](#)"
 - "[SGF6112](#)"
 - "[SG6000](#)"
 - "[SG5800](#)"
 - "[SG5700](#)"
 - "[SG110 und SG1100](#)"
 - "[SG100 und SG1000](#)"
- d. Ändern Sie die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

Sie können die 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 wird das Netzwerk in den Modus „kein FEC“ zurückfallen. Wenn FEC nicht aktiviert ist, sind die Anschlüsse anfälliger für Fehler, die durch elektrische Geräusche verursacht werden.



StorageGRID Appliances unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie keine FEC.

Switch-Port und MTU-NIC stimmen nicht überein

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

Die auf dem 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 als seine MTU ist, was mit dieser Konfiguration möglich ist, wird möglicherweise die Warnmeldung **Node Network Reception Frame error** ausgegeben. 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 gleich sein. Weitere Informationen finden Sie unter [Fehler bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU](#).



Siehe auch "[MTU-Einstellung ändern](#)".

Hohe Link-Fehlerraten

- a. Aktivieren Sie FEC, falls nicht bereits aktiviert.
- b. Stellen Sie sicher, dass Ihre Netzwerkkabel von guter Qualität sind und nicht beschädigt oder nicht ordnungsgemäß angeschlossen sind.
- c. Wenn 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.

NIC-Klingelpuffer überlaufen

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.

3. Überwachen Sie das Problem, und wenden Sie sich an den technischen Support, wenn die Meldung nicht gelöst wird.

Fehler bei der Zeitsynchronisierung

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 "[Angeben der externen NTP-Quelle](#)" Sie für eine StorageGRID-Installation auf Produktionsebene den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version vor Windows Server 2016 verwenden. 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.

Linux: Probleme mit der Netzwerkverbindung

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

Klonen VON MAC Adressen

In einigen Fällen können Netzwerkprobleme durch das Klonen von MAC-Adressen gelöst werden. Wenn Sie virtuelle Hosts verwenden, setzen Sie den Wert des MAC-Adressklonschlüssels für jedes Ihrer Netzwerke in Ihrer Knotenkonfigurationsdatei auf „true“. Diese Einstellung bewirkt, dass die MAC-Adresse des StorageGRID-Containers die MAC-Adresse des Hosts verwendet. Siehe die Anweisungen zu "[Erstellen Sie Knotenkonfigurationsdateien](#)" .

 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 finden Sie in der Anleitung für "[Aktivieren des MAC-Klonens](#)" .

Promiskuous Modus

Wenn Sie das Klonen von MAC-Adressen nicht verwenden möchten und lieber allen Schnittstellen erlauben möchten, Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen zu empfangen und zu übertragen, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene des virtuellen Switches und der Portgruppen für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen auf **Accept** gesetzt 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.

Weitere Informationen zur Verwendung des Promiscuous-Modus finden Sie in den Anweisungen für "[So konfigurieren Sie das Hostnetzwerk](#)" .

Linux: Knotenstatus ist „verwaist“

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`

Geben Sie für seconds 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

So zeigen Sie die IPv6-Adresse an, die einem Grid-Knoten zugewiesen wurde:

1. Wählen Sie **Knoten** und wählen Sie den Knoten aus.
2. Wählen Sie **zusätzliche IP-Adressen anzeigen** neben **IP-Adressen** auf der Registerkarte Übersicht aus.

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

Schritte

1. Melden Sie sich beim Host als Root 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 in der Dokumentation Ihres Betriebssystems nach, wie Sie die Einstellungen ändern `sysctl`. 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 Container: `exit`

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

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

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

7. Suchen Sie die folgenden 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 die Fehlermeldungen beschrieben, die möglicherweise mit einem externen Syslog-Server in Zusammenhang stehen, und Korrekturmaßnahmen werden aufgelistet.

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

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

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

- ["Überlegungen zur Verwendung eines externen Syslog-Servers"](#)
- ["Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server"](#)

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">1. Überprüfen Sie den eingegebenen Hostnamen. Wenn Sie eine IP-Adresse eingegeben haben, stellen Sie sicher, dass es sich um eine gültige IP-Adresse in der Schreibweise W.X.Y.Z („gepunktete Dezimalzahl“) handelt.2. Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind.3. 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">1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben.2. Vergewissern Sie sich, dass der Host für den syslog-Service einen Syslog-Daemon ausführt, der auf dem angegebenen Port abhört.3. 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 anzudeuten, 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-Netzwerksubnetz, 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-Netzwerksubnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese so konfiguriert sind, dass der Datenverkehr mithilfe der Netzwerkschnittstelle und des Gateways (Grid, Admin oder Client), über die Sie den Syslog-Server erreichen möchten, an den Syslog-Server weitergeleitet 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. <p>So lösen Sie dieses Problem:</p> <ol style="list-style-type: none"> 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 2. Wenn Sie TLS verwenden, vergewissern Sie sich, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 3. 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-Zertifikatbündel 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"> Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln. 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. Wenn Sie TLS verwenden, vergewissern Sie sich, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. Vergewissern Sie sich, dass das CA-Zertifikatbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat vom Syslog-Server kompatibel sind. 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"> Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Services ausgeführt werden. Starten Sie den falsch-Dienst auf den aufgeführten Knoten neu.

Fehlerbehebung beim Load Balancer-Caching

Informieren Sie sich über mögliche Probleme beim Load Balancer-Caching und wie Sie diese beheben können.

Ermitteln, ob eine Anfrage ein Cache-Treffer war

- Der X-Cache-Header wird in der Antwort auf vom Cache-Dienst verarbeitete Anfragen gesetzt. Mögliche Codes:
 - HIT: Das Objekt wurde aus dem Cache bereitgestellt
 - PARTIAL-HIT: Der Bucket/Schlüssel hatte einen Datensatz im Cache, aber nicht der gesamte angeforderte Bereich konnte aus dem Cache bereitgestellt werden
 - STALE: Der Bucket/Schlüssel hatte einen Datensatz im Cache, aber das Objekt wurde aktualisiert, seit es das letzte Mal aus dem Cache bereitgestellt wurde.
 - MISS: Das Objekt war nicht im Cache
- Der nginx-gw/endpoint-access.log.gz Der Datensatz für die Anfrage enthält „unix:/run/cache-svc/cache-svc.sock“ für Anfragen, die vom Cache verarbeitet werden.
- Der cache-svc/cache-svc.log meldet eine Meldung wie „Anforderung 320390: erfolgreich abgeschlossen (Cache-Treffer)“ oder „Anforderung 320375: erfolgreich abgeschlossen (Cache-Fehler)“. Suchen Sie den angeforderten Pfad, indem Sie nach anderen Datensätzen mit derselben Zeichenfolge

„Request <Nummer>“ suchen.

Niedrige Cache-Trefferquote

- Niedrige Cache-Trefferraten sind möglicherweise zu erwarten, wenn eine neue Arbeitslast hinzugefügt wird oder sich der Arbeitssatz ändert, auf den eine Arbeitslast zugreift. In diesen Situationen wird erwartet, dass die Trefferquote mit der Zeit steigt.
- Wenn mehrere Workloads Caching verwenden, sollten Sie das Hinzufügen von Richtlinien zur Verkehrsklassifizierung in Erwägung ziehen, um Teile der Workloads zu isolieren, die vom Cache bedient werden. Metriken zur Cache-Trefferquote sind pro Verkehrsklassifizierungsrichtlinie verfügbar. Wenn bei einigen Workloads keine guten Cache-Trefferquoten erzielt werden, sollten Sie erwägen, diese Workloads auf andere Endpunkte zu verschieben, bei denen das Caching nicht aktiviert ist.
- Bewerten Sie die Cache-Auslagerungsrate. Wenn der Cache zu klein für den Arbeitssatz ist, kommt es zu hohen Räumungsraten, was zu niedrigeren Trefferquoten führen kann.
- Unter FPVR sind möglicherweise Optionen zur Verbesserung der Trefferquoten bestimmter Workloads verfügbar.

Geringe Leistung

- Bewerten Sie die Cache-Trefferquote. Niedrige Cache-Trefferraten können zu einer geringen Gesamtleistung führen.
- Bewerten Sie die Cache-Auslagerungsrate. Während der Räumung werden einige Speicherressourcen zum Entfernen vorhandener Objekte von der Festplatte verwendet. Wenn der Räumungsprozess mit dem Zugriff auf neue Objekte nicht Schritt hält, kann das System die Schwellenwerte für das harte Wasserzeichen erreichen und beginnen, den Cache zu umgehen.
- Überprüfen Sie die Netzwerkbeschränkungen mithilfe der Diagnosefunktionen „Empfangsnutzung der Netzwerkschnittstellen“ und „Sendenutzung der Netzwerkschnittstellen“.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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