



Fehlerbehebung im StorageGRID System

StorageGRID software

NetApp
July 23, 2026

Inhalt

Fehlerbehebung im StorageGRID System	1
Fehlerbehebung in einem StorageGRID System	1
Das Problem definieren	1
Risiko und Auswirkungen auf das System bewerten	1
Daten sammeln	2
Daten analysieren	6
Checkliste für Eskalationsinformationen	6
Behebung von Objekt- und Speicherproblemen	8
Bestätigen Sie die Objektdatenspeicherorte in StorageGRID	8
Erfahren Sie mehr über Objektspeicher-Ausfälle für Speichervolumen in StorageGRID	10
Überprüfen Sie die Integrität der Objektdaten in StorageGRID	12
Beheben Sie die Warnung „S3 PUT object size too large“ in StorageGRID	16
Fehlerbehebung bei verlorenen und fehlenden Objektdaten	18
Beheben Sie die Warnung zum niedrigen Objektdaten-Speicher in StorageGRID	21
Beheben Sie die Warnung zur Wasserzeichenüberschreitung in StorageGRID	23
Beheben von Metadatenproblemen in StorageGRID	27
Beheben von Zertifikatsfehlern in StorageGRID	29
Beheben von Problemen mit dem Admin Node und der Benutzeroberfläche in StorageGRID	31
Anmeldefehler des Admin-Knotens	31
Probleme mit der Benutzeroberfläche	34
Beheben von Netzwerk-, Hardware- und Plattformproblemen in StorageGRID	34
Grid Network MTU-Nichtübereinstimmungswarnung	36
Warnung über einen Empfangsfehler im Knotennetzwerk	37
Zeitsynchronisationsfehler	39
Linux: Probleme mit der Netzwerkverbindung	39
Linux: Der Knotenstatus ist "verwaist"	40
Linux: Fehlerbehebung bei der IPv6-Unterstützung	41
Fehlerbehebung bei Fehlermeldungen des externen Syslog-Servers für StorageGRID	43
Erfahren Sie mehr über Caching-Probleme von Load-Balancern in StorageGRID	46
Feststellen, ob eine Anfrage ein Cache-Treffer war	46
Niedrige Cache-Trefferquote	47
Geringe Leistung	47

Fehlerbehebung im StorageGRID System

Fehlerbehebung in einem StorageGRID System

Sollten Sie bei der Verwendung eines StorageGRID Systems auf ein Problem stoßen, finden Sie in diesem Abschnitt Tipps und Hinweise zur Ermittlung und Behebung des Problems.

Oftmals können Sie Probleme selbst lösen; in manchen Fällen müssen Sie jedoch einige Probleme an den technischen Support eskalieren.

Das Problem definieren

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 sammeln könnten, um ein Problem zu definieren:

Frage	Beispielantwort
Was macht das StorageGRID-System bzw. was macht es nicht? Welche Symptome treten auf?	Clientanwendungen melden, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann hat das Problem begonnen?	Die Objektaufnahme wurde erstmals am 8. Januar 2020 gegen 14:50 Uhr abgelehnt.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Benachrichtigung durch die Client-Anwendung. Es wurden außerdem Benachrichtigungen per E-Mail empfangen.
Tritt das Problem regelmäßig auf oder nur gelegentlich?	Das Problem besteht weiterhin.
Wenn das Problem regelmäßig auftritt, welche Schritte führen dazu?	Das Problem tritt jedes Mal auf, wenn ein Client versucht, ein Objekt zu ingestieren.
Falls das Problem nur sporadisch auftritt, wann genau tritt es auf? Notieren Sie die Uhrzeiten aller Ihnen bekannten Vorfälle.	Das Problem ist nicht sporadisch.
Ist Ihnen dieses Problem schon einmal begegnet? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dies ist das erste Mal, dass ich dieses Problem sehe.

Risiko und Auswirkungen auf das System bewerten

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

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

Frage	Beispielantwort
Kann das StorageGRID System Inhalte aufnehmen?	Nr.
Können Clientanwendungen Inhalte abrufen?	Manche Objekte können abgerufen werden, andere nicht.
Sind die Daten gefährdet?	Nr.
Ist die Fähigkeit zur Geschäftstätigkeit stark beeinträchtigt?	Ja, weil Clientanwendungen keine Objekte im StorageGRID System speichern können und Daten nicht konsistent abgerufen werden können.

Daten sammeln

Nachdem Sie das Problem definiert und dessen Risiken und Auswirkungen bewertet haben, werden Daten für die Analyse gesammelt. Die Art der Daten, die am nützlichsten zu sammeln ist, hängt von der Art des Problems ab.

Art der zu erfassenden Daten	Warum werden diese Daten erfasst?	Anweisungen
Zeitleiste der letzten Änderungen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Eine Zeitleiste der letzten Änderungen erstellen
Benachrichtigungen überprüfen	Warnmeldungen können dabei unterstützen, die Ursache eines Problems schnell zu ermitteln, indem wichtige Hinweise auf die zugrunde liegenden Probleme gegeben werden, die das Problem verursachen könnten. In der Liste der aktuellen Warnmeldungen kann geprüft werden, ob StorageGRID die Ursache eines Problems identifiziert hat. Zusätzliche Erkenntnisse bieten die in der Vergangenheit ausgelösten Warnmeldungen.	• "Aktuelle und behobene Warnmeldungen"
Ausgangswerte festlegen	Informationen über die Normalwerte verschiedener Betriebskennzahlen sammeln. Diese Ausgangswerte und Abweichungen von diesen Ausgangswerten können wertvolle Hinweise liefern.	• Ausgangswerte festlegen

Art der zu erfassenden Daten	Warum werden diese Daten erfasst?	Anweisungen
Ingest- und Abruftests durchführen	Zur Fehlerbehebung bei Leistungsproblemen beim Importieren und Abrufen empfiehlt sich die Verwendung einer Workstation zum Speichern und Abrufen von Objekten. Ein Vergleich der Ergebnisse mit denen bei Nutzung der Clientanwendung ist möglich.	• "PUT- und GET-Leistung überwachen"
Prüfmeldungen überprüfen	Audit-Meldungen bieten die Möglichkeit, StorageGRID-Vorgänge im Detail nachzuvollziehen. Die Details in den Audit-Meldungen können bei der Fehlerbehebung vieler Arten von Problemen, einschließlich Leistungsproblemen, nützlich sein.	• "Prüfmeldungen überprüfen"
Objektstandorte und Speicherintegrität überprüfen	Wenn Speicherprobleme auftreten, sollte überprüft werden, ob die Objekte an den erwarteten Stellen abgelegt werden. Die Integrität der Objektdaten auf einem Storage Node sollte überprüft werden.	• "Überwachung von Objektverifizierungsoperationen" • "Objektdatenspeicherorte bestätigen" • "Objektintegrität verifizieren"
Daten für den technischen Support sammeln	Der technische Support kann Sie bitten, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um bei der Fehlerbehebung zu unterstützen.	• "Protokolldateien und Systemdaten sammeln" • "Ein AutoSupport-Paket manuell auslösen" • "Support-Metriken überprüfen"

Eine Zeitleiste der letzten Änderungen erstellen

Wenn ein Problem auftritt, sollte berücksichtigt werden, was sich in letzter Zeit geändert hat und wann diese Änderungen erfolgt sind.

- Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.
- Eine Zeitleiste der Änderungen kann dabei helfen zu erkennen, welche Änderungen möglicherweise für ein Problem verantwortlich sind und wie sich jede Änderung auf dessen Entwicklung ausgewirkt haben könnte.

Eine Tabelle der letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann jede Änderung erfolgte und alle relevanten Details zur Änderung, wie zum Beispiel Informationen darüber, was während der Durchführung der Änderung sonst noch geschah, kann erstellt werden:

Zeit des Wandels	Art der Änderung	Details
Beispiel: • Wann haben Sie die Knotenwiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Vorgang unterbrochen?	Was ist passiert? Was haben Sie getan?	Dokumentieren Sie alle relevanten Details zur Änderung. Zum Beispiel: • Einzelheiten zu den Netzwerkänderungen. • Welcher Hotfix installiert wurde. • Wie sich die Arbeitslasten der Kunden verändert haben. Achten Sie darauf, zu vermerken, ob mehr als eine Änderung gleichzeitig vorgenommen wurde. Wurde diese Änderung beispielsweise während eines laufenden Upgrades durchgeführt?

Beispiele für bedeutende Veränderungen in jüngster Zeit

Hier sind einige Beispiele für potenziell bedeutende Änderungen:

- Wurde das StorageGRID System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde das System kürzlich aktualisiert? Wurde ein Hotfix eingespielt?
- Wurden in letzter Zeit Hardware repariert oder ausgetauscht?
- Wurde die ILM Richtlinie aktualisiert?
- Hat sich die Arbeitslast des Kunden verändert?
- Hat sich die Client-Anwendung oder ihr Verhalten geändert?
- Haben Sie die Load Balancer geändert oder eine Hochverfügbarkeitsgruppe von Admin Nodes oder Gateway Nodes hinzugefügt oder entfernt?
- Wurden Aufgaben begonnen, deren Abschluss längere Zeit in Anspruch nehmen könnte? Beispiele hierfür sind:
 - Wiederherstellung eines ausgefallenen Storage Node
 - Stilllegung des Storage Node
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, wie zum Beispiel das Hinzufügen eines Mandanten oder die Änderung der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden die Plattformdienste kürzlich aktiviert oder geändert?
- Wurde Compliance kürzlich aktiviert?
- Wurden Cloud Storage Pools hinzugefügt oder entfernt?
- Wurden Änderungen an der Speicherkomprimierung oder Verschlüsselung vorgenommen?
- Gab es Änderungen an der Netzwerkinfrastruktur? Zum Beispiel VLANs, Router oder DNS.
- Wurden Änderungen an den NTP-Quellen vorgenommen?
- Wurden Änderungen an den Schnittstellen Grid, Admin oder Client Network vorgenommen?
- Wurden am StorageGRID System oder seiner Umgebung weitere Änderungen vorgenommen?

Ausgangswerte festlegen

Sie können Referenzwerte für Ihr System festlegen, indem Sie die Normalwerte verschiedener Betriebsparameter erfassen. In Zukunft können die aktuellen Werte mit diesen Referenzwerten verglichen werden, um abnormale Werte zu erkennen und zu beheben.

Eigenschaft	Wert	Bezugsmöglichkeiten
Durchschnittlicher Speicherverbrauch	GB verbraucht/Tag Prozent verbraucht/Tag	Gehen Sie zum Grid Manager. Auf der Seite „Knoten“ das gesamte Grid oder einen Standort auswählen und zur Registerkarte „Speicher“ wechseln. Im Diagramm „Speicherbelegung – Objektdaten“ lässt sich ein Zeitraum erkennen, in dem die Linie relativ stabil verläuft. Mit dem Mauszeiger über dem Diagramm lässt sich abschätzen, wie viel Speicher täglich verbraucht wird. Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenverbrauch	GB verbraucht/Tag Prozent verbraucht/Tag	Gehen Sie zum Grid Manager. Auf der Seite „Knoten“ das gesamte Grid oder einen Standort auswählen und zur Registerkarte „Speicher“ wechseln. Im Diagramm „Speicherbelegung – Objektmetadaten“ lässt sich ein Zeitraum erkennen, in dem die Linie relativ stabil verläuft. Mit dem Mauszeiger über dem Diagramm kann abgeschätzt werden, wie viel Metadaten Speicher täglich genutzt wird. Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Rate der S3-Operationen	Operationen pro Sekunde	Im Grid Manager Dashboard unter Performance > S3-Operationen für Storage Nodes auswählen. Die Aufnahme- und Abrufraten sowie -anzahlen für einen bestimmten Standort oder Knoten sind unter Knoten > site oder Storage Node > Objekte zu finden. Der Mauszeiger kann über das Diagramm für S3 Ingest und Retrieve positioniert werden.
ILM Bewertungsrate	Objekte/Sekunde	Auf der Seite „Knoten“ die Option grid > ILM auswählen. Im ILM-Warteschlangendiagramm lässt sich ein Zeitraum finden, in dem die Linie relativ stabil verläuft. Mit dem Cursor über dem Diagramm kann ein Basiswert für die Auswertungsrate des Systems abgeschätzt werden.

Eigenschaft	Wert	Bezugsmöglichkeiten
ILM Scanrate	Objekte/Sekunde	Wählen Sie Nodes > grid > ILM . Im ILM-Warteschlangendiagramm lässt sich ein Zeitraum finden, in dem die Linie relativ stabil ist. Mit dem Cursor über dem Diagramm kann ein Basiswert für die Scan rate des Systems abgeschätzt werden.
Objekte, die von Clientoperationen in die Warteschlange gestellt wurden	Objekte/Sekunde	Wählen Sie Nodes > grid > ILM . Im ILM-Warteschlangendiagramm lässt sich ein Zeitraum finden, in dem die Linie relativ stabil ist. Mit dem Cursor über dem Diagramm kann ein Basiswert für Objects queued (from client operations) für Ihr System abgeschätzt werden.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie Knoten > Speicherknoten > Objekte . In der Tabelle „Abfragen“ ist der Wert für die durchschnittliche Latenz ersichtlich.

Daten analysieren

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

Die Analyse ist problemabhängig, aber im Allgemeinen:

- Fehlerquellen und Engpässe lassen sich mithilfe der Warnmeldungen identifizieren.
- Die Problemhistorie lässt sich anhand des Alarmverlaufs und der Diagramme rekonstruieren.
- Mithilfe von Diagrammen lassen sich Anomalien erkennen und die Problemsituation mit dem Normalbetrieb vergleichen.

Checkliste für Eskalationsinformationen

Wenn Sie das Problem nicht selbst lösen können, wenden Sie sich an den technischen Support. Vor der Kontaktaufnahme mit dem technischen Support sollten die in der folgenden Tabelle aufgeführten Informationen bereitgestellt werden, um die Problemlösung zu erleichtern.

	Artikel	Hinweise
	Problemstellung	Welche Symptome des Problems treten auf? Wann hat das Problem begonnen? Tritt es durchgehend oder nur gelegentlich auf? Falls nur gelegentlich, zu welchen Zeiten ist es aufgetreten? Das Problem definieren

	Artikel	Hinweise
	Folgenabschätzung	Wie ist der Schweregrad des Problems? Welche Auswirkungen hat das auf die Client-Anwendung? • Hat der Client zuvor bereits erfolgreich eine Verbindung hergestellt? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	Wählen Sie Wartung > System > Lizenz . Die StorageGRID System-ID wird als Teil der aktuellen Lizenz angezeigt.
	Softwareversion	Oben im Grid Manager das Hilfesymbol auswählen und anschließend Über , um die StorageGRID Version anzuzeigen.
	Anpassung	Die Konfiguration Ihres StorageGRID Systems in einer Zusammenfassung. Beispielsweise können folgende Punkte aufgeführt werden: • Verwendet das Grid Speicherkomprimierung, Speicherverschlüsselung oder Compliance? • Erstellt ILM replizierte oder löschcodierte Objekte? Gewährleistet ILM Standortredundanz? Verwenden die ILM Regeln die Ingest-Verhaltensweisen Balanced, Strict oder Dual Commit?
	Protokolldateien und Systemdaten	Protokolldateien und Systemdaten für Ihr System sammeln. Support > Tools > Log collection auswählen. Sie können Protokolle für das gesamte Grid oder für ausgewählte Knoten sammeln. Wenn Sie Protokolle nur für ausgewählte Knoten erfassen, stellen Sie sicher, dass mindestens ein Storage Node den ADC-Service enthält. Die ersten drei Storage Nodes, die an einem Standort installiert werden, enthalten den ADC-Service.
	Basisinformationen	Basisinformationen zu Aufnahmeprozessen, Abrufprozessen und Speicherverbrauch erfassen. Ausgangswerte festlegen
	Zeitleiste der jüngsten Änderungen	Eine Zeitleiste, die alle kürzlich erfolgten Änderungen am System oder seiner Umgebung zusammenfasst. Eine Zeitleiste der letzten Änderungen erstellen

✓	Artikel	Hinweise
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie selbst Schritte unternommen haben, um das Problem zu diagnostizieren oder zu beheben, notieren Sie die durchgeführten Schritte und das Ergebnis.

Behebung von Objekt- und Speicherproblemen

Bestätigen Sie die Objektdatenspeicherorte in StorageGRID

Je nach Problem kann es sinnvoll sein, "[Bestätigen, wo die Objektdaten gespeichert werden](#)". Beispielsweise kann überprüft werden, ob die ILM Policy wie erwartet funktioniert und Objektdaten am vorgesehenen Ort gespeichert werden.

Bevor Sie beginnen

- Sie benötigen eine Objektkennung, die eine der folgenden sein kann:
 - UUID:** Die universell eindeutige Kennung des Objekts. Die UUID ist in Großbuchstaben anzugeben.
 - CBID:** Die eindeutige Kennung des Objekts in StorageGRID. Die CBID eines Objekts ist im Revisionsprotokoll zu finden. Die CBID muss in Großbuchstaben eingegeben werden.
 - S3-Bucket und Objektschlüssel:** Wenn ein Objekt über den "[S3 Schnittstelle](#)" importiert wird, verwendet die Clientanwendung eine Kombination aus Bucket und Objektschlüssel, um das Objekt zu speichern und zu identifizieren.

Schritte

1. **ILM > Objektmetatadensuche** auswählen.
2. Geben Sie die Kennung des Objekts im Feld **Kennung** ein.

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

3. Wenn eine bestimmte Version des Objekts gesucht wird, kann optional die Versions-ID eingegeben werden.

4. **Nach oben suchen** auswählen.

Sie "[Ergebnisse der Objektmetatadensuche](#)" erscheinen. Diese Seite listet folgende Arten von Informationen auf:

- Systemmetadaten, einschließlich der Objekt-ID (UUID), der Versions-ID (optional), des Objektnamens, des Namens des Containers, des Mandantenkontonamens oder der Mandantenkonto-ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Erstellung des Objekts sowie des Datums und der Uhrzeit der letzten Änderung des Objekts.
- Alle benutzerdefinierten Metadaten-Schlüssel-Wert-Paare, die dem Objekt zugeordnet sind.
- Bei S3-Objekten alle Objekt-Tag-Schlüssel-Wert-Paare, die dem Objekt zugeordnet sind.
- Für replizierte Objektkopien der aktuelle Speicherort jeder Kopie.
- Für mit Erasure-Codierung versehene Objektkopien ist der aktuelle Speicherort jedes Fragments.
- Bei Objektkopien in einem Cloud-Speicherpool ist der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und Multipart-Objekte eine Liste der Objektsegmente einschließlich Segmentkennungen und Datengrößen. Für Objekte mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten enthalten interne Systemmetadaten, deren Persistenz von Version zu Version nicht garantiert werden kann.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

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

```

Erfahren Sie mehr über Objektspeicher-Ausfälle für Speichervolumes in StorageGRID

Der zugrundeliegende Speicher eines Storage Node ist in Objektspeicher unterteilt. Objektspeicher werden auch als Speichervolumes bezeichnet.

Sie können Objektspeicherinformationen für jeden Storage Node anzeigen. **Knoten** > **Storage Node** > **Speicher** auswählen.

Disk devices

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

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	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 Fehlers können sich Störungen eines Speichervolumes in "[Speichervolumen-Warnungen](#)" widerspiegeln. Wenn ein Speichervolume ausfällt, sollte das ausgefallene Speichervolume repariert werden, damit der Speicherknoten so schnell wie möglich wieder vollständig funktionsfähig ist. Falls erforderlich, kann auf die Registerkarte **Konfiguration** gewechselt und "[Den Storage Node in einen schreibgeschützten Zustand versetzen](#)" ausgewählt werden, sodass das StorageGRID System es für den Datenabruf verwenden kann, während die vollständige Wiederherstellung des Servers vorbereitet wird.

Überprüfen Sie die Integrität der Objektdaten in StorageGRID

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

Es gibt zwei Verifizierungsprozesse: die Hintergrundverifizierung und die Objektexistenzprüfung (früher als Vordergrundverifizierung bezeichnet). Diese arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundverifizierung läuft automatisch und prüft kontinuierlich die Korrektheit der Objektdaten. Die Objektexistenzprüfung kann von einem Benutzer ausgelöst werden, um die Existenz (jedoch nicht die Korrektheit) von Objekten schneller zu überprüfen.

Was ist eine Hintergrundüberprüfung?

Der Hintergrundüberprüfungsprozess prüft automatisch und kontinuierlich Storage Nodes auf beschädigte Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Die Hintergrundverifizierung prüft die Integrität replizierter Objekte und Objekte mit Löschcodierung wie folgt:

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



Beschädigte Objektdaten werden in Quarantäne verschoben, anstatt aus dem System gelöscht zu werden, sodass sie weiterhin zugänglich sind. Weitere Informationen zum Zugriff auf in Quarantäne verschobene Objektdaten sind beim technischen Support erhältlich.

- **Erase-codierte Objekte:** Wenn der Hintergrundüberprüfungsprozess feststellt, dass ein Fragment eines erasure-codierten Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment am selben Storage Node mithilfe der verbleibenden Daten- und Paritätsfragmente wiederherzustellen. Kann das beschädigte Fragment nicht wiederhergestellt werden, wird versucht, eine andere Kopie des Objekts abzurufen. Ist das Abrufen erfolgreich, erfolgt eine ILM-Auswertung, um eine Ersatzkopie des erasure-codierten Objekts zu erstellen.

Der Hintergrundüberprüfungsprozess prüft ausschließlich Objekte auf Storage Nodes. Objekte in einem Cloud Storage Pool werden nicht geprüft. Objekte müssen älter als vier Tage sein, um für die Hintergrundüberprüfung in Frage zu kommen.

Die Hintergrundprüfung läuft kontinuierlich und ist so ausgelegt, dass sie den normalen Systembetrieb nicht beeinträchtigt. Die Hintergrundprüfung kann nicht angehalten werden. Allerdings kann die Hintergrundprüfrate erhöht werden, um den Inhalt eines Storage Node schneller zu überprüfen, falls ein Problem vermutet wird.

Warnmeldungen im Zusammenhang mit der Hintergrundüberprüfung

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

Wenn die Hintergrundprüfung ein beschädigtes Objekt nicht ersetzen kann, weil keine andere Kopie gefunden werden kann, wird die Warnung **Objects potentially lost** ausgelöst.

Was ist eine Objekt-Existenzprüfung?

Die Objektexistenzprüfung verifiziert, ob alle erwarteten replizierten Kopien von Objekten und Erasure-Coding-Fragmenten auf einem Storage Node vorhanden sind. Die Objektexistenzprüfung überprüft nicht die Objektdaten selbst (die Hintergrundverifizierung übernimmt dies); vielmehr bietet sie eine Möglichkeit zur Überprüfung der Integrität von Speichermedien, insbesondere wenn ein kürzlich aufgetretenes Hardwareproblem die Datenintegrität beeinträchtigt haben könnte.

Im Gegensatz zur Hintergrundprüfung, die automatisch erfolgt, muss ein Objektexistenzprüfungsauftrag manuell gestartet werden.

Die Objektexistenzprüfung liest die Metadaten jedes in StorageGRID gespeicherten Objekts und überprüft das Vorhandensein sowohl replizierter Objektkopien als auch von löschcodierten Objektfragmenten. Fehlende Daten werden wie folgt behandelt:

- **Replizierte Kopien:** Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, diese durch eine an anderer Stelle im System gespeicherte Kopie zu ersetzen. Der Storage Node führt eine vorhandene Kopie durch eine ILM-Evaluierung, wobei festgestellt wird, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da eine weitere Kopie fehlt. Eine neue Kopie wird erstellt und platziert, um die aktiven ILM-Richtlinien des Systems zu erfüllen. Diese neue Kopie wird möglicherweise nicht am selben Speicherort abgelegt, an dem die fehlende Kopie gespeichert war.
- **Erasure-codierte Fragmente:** Fehlt ein Fragment eines erasure-codierten Objekts, versucht StorageGRID automatisch, das fehlende Fragment am selben Storage Node mithilfe der verbleibenden Fragmente wiederherzustellen. Kann das fehlende Fragment nicht wiederhergestellt werden (weil zu viele Fragmente verloren gegangen sind), versucht ILM, eine weitere Kopie des Objekts zu finden, mit der ein neues erasure-codiertes Fragment generiert werden kann.

Objektexistenzprüfung ausführen

Sie erstellen und führen jeweils einen Objektexistenzprüfungsauftrag aus. Beim Erstellen eines Auftrags wählen Sie die Storage Nodes und Volumes aus, die Sie überprüfen möchten. Sie legen außerdem die Konsistenz für den Auftrag fest.

Bevor Sie beginnen

- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Sie haben die ["\\${post_edited_translations.segment}"](#).
- Sie haben sichergestellt, dass die Storage Nodes, die Sie überprüfen möchten, online sind. **Nodes** auswählen, um die Tabelle der Knoten anzuzeigen. Sicherstellen, dass neben dem Node-Name der Knoten, die Sie überprüfen möchten, keine Warnsymbole erscheinen.
- Sie haben sichergestellt, dass die folgenden Prozeduren **nicht** auf den zu überprüfenden Nodes ausgeführt werden:
 - Grid-Erweiterung zum Hinzufügen eines Storage Node
 - Stilllegung des Storage Node

- Wiederherstellung eines ausgefallenen Speichervolumens
- Wiederherstellung eines Storage Node mit ausgefallenem Systemlaufwerk
- EC Neuausrichtung
- Appliance Node-Klon

Die Überprüfung der Objektexistenz liefert während dieser Vorgänge keine nützlichen Informationen.

Über diese Aufgabe

Ein Auftrag zur Prüfung der Objektexistenz kann je nach Anzahl der Objekte im Grid, den ausgewählten Storage Nodes und Volumes sowie der gewählten Konsistenz Tage oder Wochen in Anspruch nehmen. Es kann jeweils nur ein Auftrag ausgeführt werden, jedoch können mehrere Storage Nodes und Volumes gleichzeitig ausgewählt werden.

Schritte

1. Wählen Sie **Wartung > Aufgaben > Objektexistenzprüfung**.
2. **Auftrag erstellen** auswählen. Der Assistent zum Erstellen eines Auftrags zur Objektexistenzprüfung wird angezeigt.
3. Wählen Sie die Knoten aus, die die zu überprüfenden Volumes enthalten. Zum Auswählen aller Online-Knoten das Kontrollkästchen **Node-Name** in der Spaltenüberschrift aktivieren.

Es ist möglich, nach Node-Name oder Standort zu suchen.

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

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

`${post_edited_translations.segment}`

6. Wählen Sie **Weiter**.
7. Die Konsistenz für die Aufgabe auswählen.

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

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **Alle** (Standard): Alle drei Kopien der Metadaten an jedem Standort.

Weitere Informationen zur Konsistenz sind in den Beschreibungen im Assistenten enthalten.

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

Es wird ein Job zur Überprüfung der Objektexistenz generiert und läuft so lange, bis eines der folgenden Ereignisse eintritt:

- Der Auftrag ist abgeschlossen.

- Sie pausieren oder brechen den Auftrag ab. Ein pausierter Auftrag kann fortgesetzt werden, ein abgebrochener jedoch nicht.
- Der Job hängt sich auf. Die Warnung **Objektexistenzprüfung ist hängen geblieben** wird ausgelöst. Es sind die in der Warnung angegebenen Korrekturmaßnahmen zu beachten.
- Der Auftrag schlägt fehl. Die Warnung **Objektexistenzprüfung fehlgeschlagen** wird ausgelöst. Es sind die in der Warnung angegebenen Korrekturmaßnahmen zu beachten.
- Es erscheint die Meldung „Dienst nicht verfügbar“ oder „Interner Serverfehler“. Nach einer Minute die Seite aktualisieren, um die Überwachung des Auftrags fortzusetzen.



Bei Bedarf können Sie die Seite zur Objektexistenzprüfung verlassen und zurückkehren, um die Überwachung des Auftrags fortzusetzen.

10. Während der Job läuft, kann auf der Registerkarte **Aktiver Job** der Wert für erkannte fehlende Objektkopien eingesehen werden.

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

Wenn die Anzahl der erkannten fehlenden Objektkopien größer als 100 ist, könnte ein Problem mit dem Storage Node-Speicher vorliegen.

11. Nach Abschluss des Auftrags sind alle weiteren erforderlichen Maßnahmen durchzuführen:

- Wenn die Anzahl der erkannten fehlenden Objektkopien null beträgt, wurden keine Probleme festgestellt. Es ist keine Aktion erforderlich.
- Wenn die Anzahl der erkannten fehlenden Objektkopien größer als null ist und die Warnung **Objects potentially lost** nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Es sollte überprüft werden, ob etwaige Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu verhindern.
- Wenn die Anzahl fehlender Objektkopien größer als null ist und die Warnung **Objects potentially lost** 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-Audit-Meldungen extrahieren: `grep LLST audit_file_name`.

Dieses Verfahren ähnelt dem für "[\\${post_edited_translations.segment}](#)", obwohl Sie bei Objektkopien nach LLST statt nach OLST suchen.

12. Wenn für den Auftrag die starke Standort- oder starke globale Konsistenz ausgewählt wurde, sollte etwa drei Wochen auf die Metadatenkonsistenz gewartet werden, danach kann der Auftrag erneut auf denselben Volumes ausgeführt werden.

Wenn StorageGRID genügend Zeit hatte, die Metadatenkonsistenz für die im Job enthaltenen Knoten und Volumes zu erreichen, kann das erneute Ausführen des Jobs fälschlicherweise als fehlend gemeldete Objektkopien entfernen oder dazu führen, dass zusätzliche Objektkopien überprüft werden, falls diese übersehen wurden.

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

b. Ermitteln, welche Aufträge zur erneuten Ausführung bereit sind:

- i. In der Spalte **Endzeit** lässt sich erkennen, welche Aufträge vor mehr als drei Wochen ausgeführt wurden.

- ii. In diesen Jobs die Spalte „Konsistenzkontrolle“ auf „strong-site“ oder „strong-global“ prüfen.
- c. Für jeden Job, der erneut ausgeführt werden soll, das Kontrollkästchen auswählen und anschließend **Erneut ausführen** wählen.
- d. Im Assistenten zum erneuten Ausführen von Aufträgen werden die ausgewählten Knoten und Volumes sowie die Konsistenz angezeigt.
- e. Wenn Sie bereit sind, die Aufträge erneut auszuführen, wählen Sie **Erneut ausführen**.

Die Registerkarte „Aktive Aufträge“ wird angezeigt. Alle ausgewählten Aufträge werden als ein Auftrag mit der Konsistenz strong-site erneut ausgeführt. Im Abschnitt „Details“ listet das Feld „Verwandte Aufträge“ die Auftrags-IDs der ursprünglichen Aufträge auf.

Beheben Sie die Warnung „S3 PUT object size too large“ in StorageGRID

Die Warnung „S3 PUT Objektgröße zu groß“ wird ausgelöst, wenn ein Mandant eine nicht-multipart PutObject-Operation versucht, die das S3-Größenlimit von 5 GiB überschreitet.

Bevor Sie beginnen

- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Du hast ["spezifische Zugriffsberechtigungen"](#).

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

Schritte

1. Zu **Konfiguration > Überwachung > Audit und Syslog-Server** wechseln.
2. Wenn die Client-Schreibvorgänge normal sind, kann auf das Revisionsprotokoll zugegriffen werden:
 - a. Eingeben `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
 - c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
 - d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von \$ zu #.

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

`${post_edited_translations.segment}`

Option	Ziel
<code>\${post_edited_translations.segment}</code>	<code>/var/local/log/localaudit.log</code>

Option	Ziel
Admin Nodes/lokale Knoten	- Admin Nodes (primäre und nicht-primäre): /var/local/audit/export/audit.log - Alle Knoten: Die /var/local/log/localaudit.log Datei ist in diesem Modus typischerweise leer oder fehlt.
Externer Syslog Server	/var/local/log/localaudit.log

Je nach Ihren Einstellungen für das Revisionsprotokoll-Ziel geben Sie Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

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

f. Ermittelt wird, welche Mandanten Objekte verwenden, die größer als 5 GiB sind.

- Eingeben `zgrep SPUT * | egrep "CSIZ\(UI64\) : ([5-9] | [1-9] [0-9]+) [0-9]{9}"`
- Für jede Revisionsprotokollmeldung in den Ergebnissen kann anhand des `S3AI`-Felds die Mandantenkonto-ID ermittelt werden. Die anderen Felder in der Meldung geben an, welche IP-Adresse vom Client, dem Bucket und dem Objekt verwendet wurde:

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

Beispielhafte Revisionsprotokoll-Ergebnisse

```
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):"06OX85M40Q90Y280B7YT"] [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. Falls Client-Schreibvorgänge nicht normal sind, kann die Mandanten-ID aus der Warnung zur Identifizierung des Mandanten verwendet werden:
 - a. Wechseln Sie zu **Support > Tools > Log collection**. Anwendungsprotokolle für den Storage Node in der Warnung sammeln. 15 Minuten vor und nach der Warnung angeben. Siehe "[Protokolldateien und Systemdaten sammeln](#)".
 - b. Die Datei extrahieren und zu `broadcast.log` wechseln:

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

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

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. Mieter werden darüber informiert, dass die maximale PutObject-Größe 5 GiB beträgt und für Objekte über 5 GiB Multipart-Uploads zu verwenden sind.
5. Die Benachrichtigung wird für eine Woche ignoriert, falls die Anwendung geändert wurde.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Erfahren Sie mehr über verlorene und fehlende Objektdaten in StorageGRID

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

Das StorageGRID System verwendet Standortinformationen in den Metadaten eines Objekts, um zu bestimmen, von welchem Ort das Objekt abgerufen wird. Wenn am erwarteten Ort keine Kopie des Objekts gefunden wird, versucht das System, eine weitere Kopie des Objekts von einer anderen Stelle im System abzurufen, sofern die ILM-Richtlinie eine Regel enthält, nach der zwei oder mehr Kopien des Objekts erstellt werden.

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

- Bei replizierten Kopien gilt: Kann keine weitere Kopie abgerufen werden, wird das Objekt als verloren betrachtet und die Warnung wird ausgelöst.
- Bei löschcodierten Kopien wird, falls eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, das Attribut Corrupt Copies Detected (ECOR) um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Wenn keine andere Kopie gefunden wird, wird die Warnung ausgelöst.

Alle Warnmeldungen zu **potenziell verlorenen Objekten** sollten umgehend untersucht werden, um die Ursache des Verlusts zu ermitteln und festzustellen, ob das Objekt möglicherweise noch auf einem offline befindlichen oder anderweitig derzeit nicht verfügbaren Storage Node existiert. Siehe "[Potenziell verlorene](#)".

Objekte untersuchen". Warnmeldungen zu verlorenen Objekten können vorsorglich fälschlicherweise ausgelöst werden.

Wenn Objektdaten ohne Kopien verloren gehen, gibt es keine Wiederherstellungsmöglichkeit. Es ist jedoch erforderlich, **"Zähler für potenziell verlorene Objekte zurücksetzen"** zu verhindern, dass bereits bekannte verlorene Objekte den Verlust neuer Objekte verdecken.

Beheben Sie die Warnung „Objekte möglicherweise verloren“ in StorageGRID

Wenn die Warnung **Objects potentially lost** ausgelöst wird, ist eine sofortige Untersuchung erforderlich. Informationen zu den betroffenen Objekten sollten gesammelt und der technische Support kontaktiert werden.

Bevor Sie beginnen

- Sie müssen mit einem **"unterstützte Webbrowser"** im Grid Manager angemeldet sein.
- Du hast **"spezifische Zugriffsberechtigungen"**.
- Sie müssen über die Datei `Passwords.txt` verfügen.

Über diese Aufgabe

Die Warnung „Objekte möglicherweise verloren“ bedeutet, dass laut den verfügbaren Informationen in StorageGRID keine Kopien eines Objekts im Grid vorhanden sind. Daten könnten dauerhaft verloren sein.

Benachrichtigungen über verlorene Objekte sollten umgehend untersucht werden. Möglicherweise sind Maßnahmen erforderlich, um weiteren Datenverlust zu verhindern. In einigen Fällen kann ein verlorenes Objekt wiederhergestellt werden, wenn schnell gehandelt wird.



Wenn mehr als 10 Objekte als verloren gemeldet werden, wenden Sie sich an den technischen Support. Dieses Verfahren sollte nicht eigenständig durchgeführt werden.

Schritte

1. Wählen Sie **Knoten**.
2. **Speicherknoten > Objekte** auswählen.
3. Die Anzahl der verlorenen Objekte in der Tabelle „Objektanzahl“ wird angezeigt.

Diese Zahl gibt die Gesamtzahl der Objekte an, die dieser Grid-Knoten im gesamten StorageGRID System als fehlend erkennt. Der Wert entspricht der Summe der Lost objects-Zähler der Data store-Komponente innerhalb der LDR- und DDS-Services.

4. Von einem Admin-Knoten aus **"auf das Revisionsprotokoll zugreifen"** lässt sich die eindeutige Kennung (UUID) des Objekts bestimmen, das die Warnung **Objects potentially lost** ausgelöst hat:
 - a. Anmeldung am Grid-Knoten:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
 - iii. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
 - iv. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein. Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Revisionsprotokolle befinden.

`${post_edited_translations.segment}`

Option	Ziel
<code>\${post_edited_translations.segment}</code>	<code>/var/local/log/localaudit.log</code>
Admin Nodes/lokale Knoten	• Admin Nodes (primäre und nicht-primäre): <code>/var/local/audit/export/audit.log</code> • Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Datei ist in diesem Modus typischerweise leer oder fehlt.
Externer Syslog Server	<code>/var/local/log/localaudit.log</code>

Je nach Ihren Einstellungen für das Revisionsprotokoll-Ziel geben Sie Folgendes ein: `cd /var/local/log` oder `/var/local/audit/export/`

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

- Verwenden Sie `grep`, um die Revisionsprotokollmeldungen Object Lost (OLST) zu extrahieren. Geben Sie Folgendes ein: `grep OLST audit_file_name`
- Beachten Sie den in der Nachricht enthaltenen UUID-Wert.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5] [UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"] [NOID(UI32):12288733] [VOL1(UI64):3222345986
] [RSLT(FC32):NONE] [AVER(UI32):10]
[ATIM(UI64):1581535134780426] [ATYP(FC32):OLST] [ANID(UI32):12448208] [A
MID(FC32):ILMX] [ATID(UI64):7729403978647354233]]
```

5. Die Metadaten des verlorenen Objekts können anhand der UUID ermittelt werden:

- ILM > Objektmetadatensuche** auswählen.
- Die UUID eingeben und **Nachschlagen** auswählen.
- Die Standorte in den Metadaten werden überprüft, und entsprechende Maßnahmen werden ergriffen:

Metadaten	Abschluss
Objekt <object_identifizier> nicht gefunden	Wird das Objekt nicht gefunden, wird die Meldung "ERROR": "" zurückgegeben. Wird das Objekt nicht gefunden, Zähler für potenziell verlorene Objekte zurücksetzen kann die Warnung gelöscht werden. Das Fehlen eines Objekts deutet darauf hin, dass das Objekt absichtlich gelöscht wurde.

Metadaten	Abschluss
Standorte > 0	Wenn in der Ausgabe Standorte aufgelistet sind, könnte die Warnung Objects potentially lost ein Fehlalarm sein. Bestätigen Sie, dass die Objekte vorhanden sind. Mit der in der Ausgabe aufgeführten Node ID und dem Dateipfad lässt sich bestätigen, dass sich die Objektdaten am angegebenen Speicherort befindet. Falls die Objekte existieren, Zähler für potenziell verlorene Objekte zurücksetzen kann die Warnung gelöscht werden.
Standorte = 0	Werden in der Ausgabe keine Standorte aufgeführt, fehlt das Objekt möglicherweise. Der technische Support sollte kontaktiert werden. Der technische Support könnte Sie bitten festzustellen, ob ein Storage-Wiederherstellungsverfahren im Gange ist. Siehe die Informationen zu "Wiederherstellung von Objektdaten mithilfe von Grid Manager" und "Wiederherstellen von Objektdaten auf einem Speichervolumen".

6. Nachdem Probleme mit verlorenen Objekten behoben wurden, sollte der Zähler für potenziell verlorene Objekte zurückgesetzt werden, damit Warnmeldungen keine Fehlalarme sind:
 - a. Wählen Sie **Knoten**.
 - b. **Speicherknoten** > **Aufgaben** auswählen.
 - c. `$_{post}_edited_translations.segment`

Beheben Sie die Warnung zum niedrigen Objektdaten-Speicher in StorageGRID

Die Warnung **Geringer Speicherplatz für Objektdaten** überwacht, wie viel Speicherplatz auf jedem Storage Node für die Speicherung von Objektdaten verfügbar ist.

Bevor Sie beginnen

- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Du hast ["spezifische Zugriffsberechtigungen"](#).

Über diese Aufgabe

Die Warnung **Geringer Speicherplatz für Objektdaten** wird ausgelöst, wenn die Gesamtmenge der replizierten und mit Erasure-Codierung versehenen Objektdaten auf einem Storage Node eine der in der Warnungsregel konfigurierten Bedingungen erfüllt.

Standardmäßig wird ein schwerwiegender Alarm ausgelöst, wenn diese Bedingung als wahr ausgewertet wird:

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

In diesem Zustand:

- `storagegrid_storage_utilization_data_bytes` ist eine Schätzung der Gesamtgröße der replizierten und löschcodierten Objektdaten für einen Speicherknoten.
- `storagegrid_storage_utilization_usable_space_bytes` ist die gesamte verbleibende Menge an Objektspeicherplatz für einen Storage Node.

Wenn eine schwerwiegende oder weniger schwerwiegende Warnung wegen **Geringem Objektdatenspeicher** ausgelöst wird, ist eine Speichererweiterung so bald wie möglich durchzuführen.

Schritte

1. **Benachrichtigungen > Aktuell** auswählen.

Die Seite „Benachrichtigungen“ erscheint.

2. In der Warntabelle kann bei Bedarf die Warngruppe **Niedriger Objektdatenspeicher** erweitert und die gewünschte Warnmeldung ausgewählt werden.



Wählen Sie die Benachrichtigung aus, nicht die Überschrift für eine Gruppe von Benachrichtigungen.

3. Die Angaben im Dialogfeld können überprüft werden, dabei ist Folgendes zu beachten:

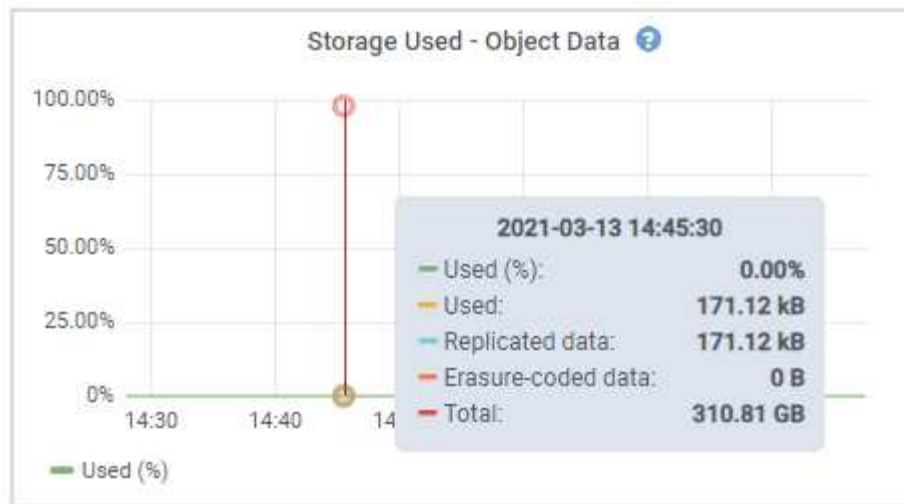
- Zeitausgelöst
- Name des Standorts und des Knotens
- Die aktuellen Werte der Kennzahlen für diese Warnung

4. **Knoten > Storage Node or Site > Speicher** auswählen.

5. Fahren Sie mit dem Cursor über das Diagramm „Storage Used - Object Data“.

Folgende Werte werden angezeigt:

- **Belegt (%)**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Verwendet**: Der Anteil des gesamten nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
- **Replizierte Daten**: Eine Schätzung der Menge an replizierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Erasure-coded data**: Eine Schätzung der Menge an erasure-coded Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt**: Die Gesamtmenge des nutzbaren Speicherplatzes auf diesem Knoten, Standort oder Grid. Der Wert „Belegt“ ist die `storagegrid_storage_utilization_data_bytes` Messgröße.



6. Mit den Zeitsteuerungen oberhalb des Diagramms lässt sich die Speichernutzung für verschiedene Zeiträume anzeigen.

Die Betrachtung der Speichernutzung im Zeitverlauf kann dabei helfen zu verstehen, wie viel Speicherplatz vor und nach Auslösung der Warnung genutzt wurde, und kann die Abschätzung ermöglichen, wie lange es dauern könnte, bis der verbleibende Speicherplatz des Knotens voll ist.

7. So schnell wie möglich ["Speicherkapazität hinzufügen"](#) zu Ihrem Grid.

Es besteht die Möglichkeit, Speichervolumes (LUNs) zu bestehenden Storage Nodes hinzuzufügen oder neue Storage Nodes hinzuzufügen.



Weitere Informationen finden sich unter ["Vollständige Speicherknoten verwalten"](#).

Beheben Sie die Warnung zur Wasserzeichenüberschreibung in StorageGRID

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, müssen Sie möglicherweise den Alarm **Low read-only watermark override** beheben. Nach Möglichkeit sollten Sie Ihr System aktualisieren, um die optimierten Werte zu verwenden.

In früheren Versionen waren die drei ["Speichervolumen Wasserzeichen"](#) globale Einstellungen, die gleichen Werte galten für jedes Speichervolume auf jedem Storage Node. Ab StorageGRID 11.6 kann die Software diese Wasserstände für jedes Speichervolume optimieren, basierend auf der Größe des Storage Node und der relativen Kapazität des Volumes.

Beim Upgrade auf StorageGRID 11.6 oder höher werden optimierte Read-only- und Read-write-Wasserzeichen automatisch auf alle Speichervolumes angewendet, es sei denn, eine der folgenden Bedingungen trifft zu:

- Ihr System ist nahezu ausgelastet und könnte keine neuen Daten mehr aufnehmen, wenn optimierte Wasserzeichen angewendet würden. StorageGRID wird in diesem Fall die Wasserzeicheneinstellungen nicht ändern.
- Sie haben zuvor für eines der Speichervolumen-Wasserzeichen einen benutzerdefinierten Wert festgelegt. StorageGRID überschreibt benutzerdefinierte Wasserzeicheneinstellungen nicht mit optimierten Werten. Allerdings kann StorageGRID die Warnung **Low read-only watermark override** auslösen, wenn Ihr

benutzerdefinierter Wert für das weiche, schreibgeschützte Wasserzeichen des Speichervolumens zu niedrig ist.

Informationen zur Warnmeldung

Wenn Sie benutzerdefinierte Werte für Speicher-Volume-Wasserzeichen verwenden, kann die Warnung **Low read-only watermark override** für einen oder mehrere Storage Nodes ausgelöst werden.

Jede Instanz der Warnung weist darauf hin, dass der benutzerdefinierte Wert für den Soft-Read-only-Wasserstand des Speicher-Volumes kleiner ist als der für diesen Storage Node optimierte Mindestwert. Bei weiterer Verwendung der benutzerdefinierten Einstellung kann es vorkommen, dass der Storage Node kritisch wenig Speicherplatz hat, bevor er sicher in den schreibgeschützten Zustand wechseln kann. Einige Speicher-Volumes können unzugänglich werden (automatisch ausgehängt), wenn der Node seine Kapazitätsgrenze erreicht.

Angenommen, Sie haben zuvor das Soft-Read-Only-Watermark für das Speichervolume auf 5 GB festgelegt. Nun wird angenommen, dass StorageGRID die folgenden optimierten Werte für die vier Speichervolumes im Storage Node A berechnet hat:

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

Die Warnung **Low read-only watermark override** wird für Storage Node A ausgelöst, da Ihr benutzerdefiniertes Wasserzeichen (5 GB) kleiner ist als der für alle Volumes in diesem Knoten optimierte Mindestwert (11 GB). Wenn die benutzerdefinierte Einstellung weiterhin verwendet wird, kann der Speicherplatz des Knotens kritisch knapp werden, bevor er sicher in den schreibgeschützten Zustand wechseln kann.

Die Warnung beheben

Führen Sie diese Schritte aus, wenn eine oder mehrere Warnmeldungen vom Typ **Low read-only watermark override** ausgelöst wurden. Diese Anweisungen können auch verwendet werden, wenn derzeit benutzerdefinierte Wasserzeicheneinstellungen genutzt werden und auf optimierte Einstellungen umgestellt werden soll, selbst wenn keine Warnmeldungen ausgelöst wurden.

Bevor Sie beginnen

- `${post_edited_translations.segment}`
- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Sie haben die ["Root-Zugriffsberechtigung"](#).

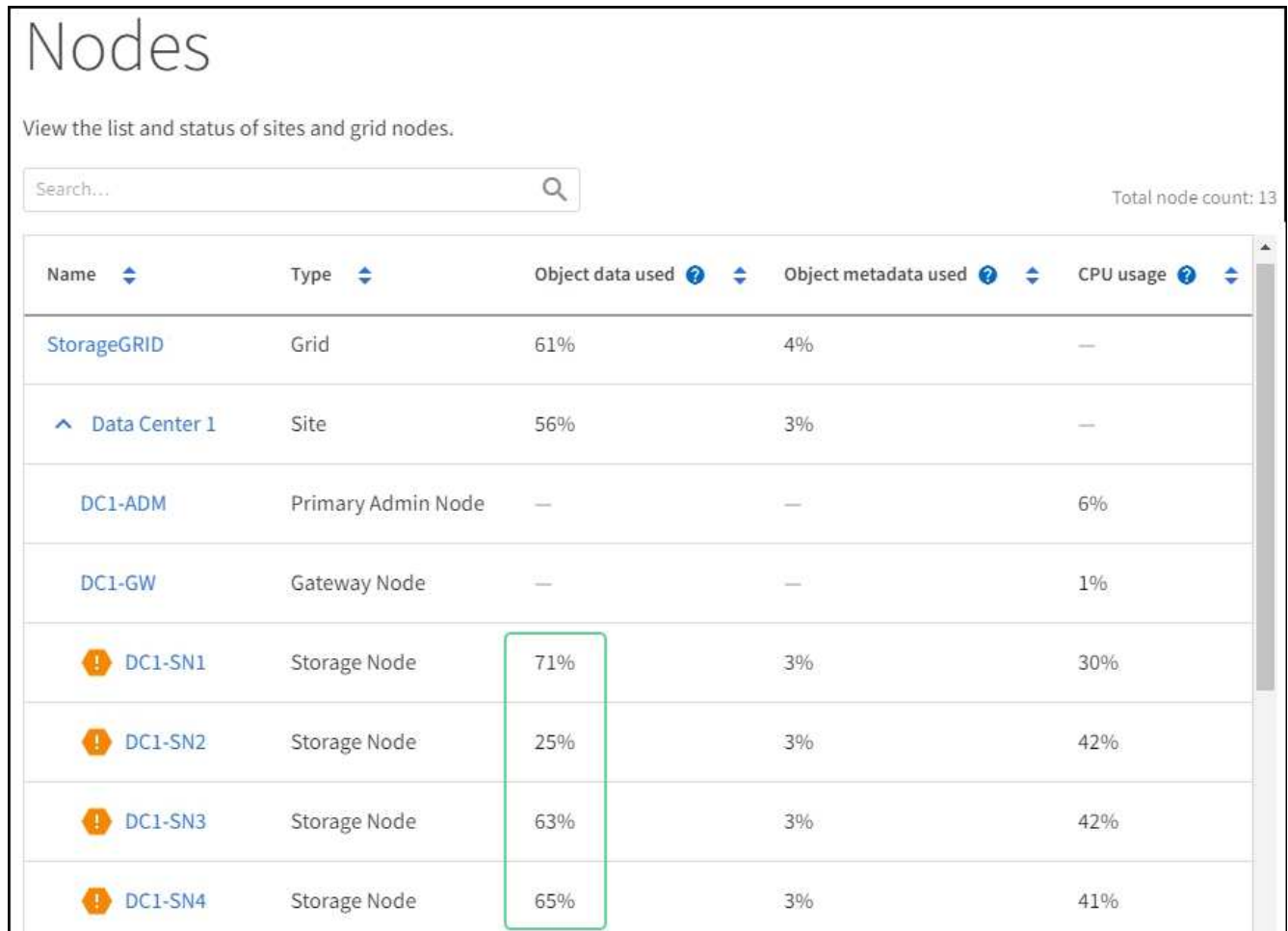
Über diese Aufgabe

Die Warnung **Low read-only watermark override** kann durch Aktualisierung der benutzerdefinierten Wasserzeicheneinstellungen auf die neuen Wasserzeichenüberschreibungen behoben werden. Wenn jedoch ein oder mehrere Storage Nodes nahezu voll sind oder spezielle ILM-Anforderungen bestehen, sollten zunächst die optimierten Speicherwasserzeichen betrachtet und festgestellt werden, ob deren Verwendung unbedenklich ist.

Bewertung der Objektdatennutzung für das gesamte Grid

Schritte

1. Wählen Sie **Knoten**.
2. Für jeden Standort im Grid die Liste der Knoten erweitern.
3. Die in der Spalte **Verwendete Objektdaten** angezeigten Prozentwerte für jeden Storage Node an jedem Standort sollten überprüft werden.



Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Führen Sie den entsprechenden Schritt aus:
 - a. Wenn keiner der Storage Nodes nahezu voll ist (zum Beispiel wenn alle Werte für **Object data used** unter 80 % liegen), können die Override-Einstellungen verwendet werden. Zu [Optimierte Wasserzeichen nutzen](#) wechseln.
 - b. Wenn ILM-Regeln ein striktes Aufnahmeverhalten verwenden oder bestimmte Speicherpools fast voll sind, sind die Schritte in [Optimierte Speicherwasserzeichen anzeigen](#) und [Es kann festgestellt werden, ob optimierte Wasserzeichen verwendet werden können](#). auszuführen.

Optimierte Speicherwasserzeichen anzeigen

StorageGRID verwendet zwei Prometheus-Metriken, um die optimierten Werte anzuzeigen, die für das Soft-Read-Only-Watermark des Speichervolumens berechnet wurden. Die minimalen und maximalen optimierten Werte für jeden Storage Node im Grid sind einsehbar.

Schritte

1. **Support > Tools > Metrics** auswählen.

2. Im Abschnitt Prometheus den Link auswählen, um auf die Prometheus Benutzeroberfläche zuzugreifen.

3. `${post_edited_translations.segment}`

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

Die letzte Spalte zeigt den minimalen optimierten Wert des weichen Grenzwerts für Schreibschutz für alle Speichervolumina auf jedem Storage Node. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für den weichen Grenzwert für Schreibschutz des Speichervolumens, wird die Warnmeldung **Low read-only watermark override** für den Storage Node ausgelöst.

4. Das empfohlene maximale Soft-Read-Only-Watermark wird angezeigt, wenn die folgende Prometheus-Metrik eingegeben und **Ausführen** ausgewählt wird:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

Die letzte Spalte zeigt den maximal optimierten Wert des Soft-Read-Only-Wasserzeichens für alle Storage Volumes auf jedem Storage Node.

5. Der maximal optimierte Wert für jeden Storage Node ist zu beachten.

Feststellen, ob optimierte Wasserzeichen verwendet werden können

Schritte

1. Wählen Sie **Knoten**.

2. Wiederholen Sie diese Schritte für jeden Online Storage Node:

a. **Speicherknoten > Speicher** auswählen.

b. Scrollen Sie nach unten zur Tabelle Objektspeicher.

c. Den **Verfügbar**-Wert für jeden Objektspeicher (Volume) mit dem maximal optimierten Wasserzeichen vergleichen, das für diesen Storage Node notiert wurde.

3. Wenn auf mindestens einem Volume jedes Online-Speicherknotens mehr Speicherplatz verfügbar ist als das maximal optimierte Wasserzeichen für diesen Knoten, zu [Optimierte Wasserzeichen nutzen](#) wechseln, um die optimierten Wasserzeichen zu verwenden.

Andernfalls sollte das Grid so bald wie möglich erweitert werden. Entweder ["Speichervolumen hinzufügen"](#) zu einem bestehenden Knoten oder ["Neue Storage Nodes hinzufügen"](#). Anschließend zur [Optimierte Wasserzeichen nutzen](#) wechseln, um die Wasserzeicheneinstellungen zu aktualisieren.

4. Wenn weiterhin benutzerdefinierte Werte für die Wasserzeichen des Speichervolumens verwendet werden sollen, ["Schweigen"](#) oder ["deaktivieren"](#) die Warnung **Low read-only watermark override** beachten.



Auf jedem Storage Node werden dieselben benutzerdefinierten Wasserzeichenwerte auf jedes Speichervolumen angewendet. Die Verwendung kleinerer als der empfohlenen Werte für die Wasserzeichen von Speichervolumen kann dazu führen, dass einige Speichervolumen nicht mehr zugänglich sind (automatisch ausgehängt werden), wenn der Node seine Kapazität erreicht.

Optimierte Wasserzeichen nutzen

Schritte

1. Wechseln Sie zu **Support > Sonstiges > Storage watermarks**.
2. Das Kontrollkästchen **Optimierte Werte verwenden** auswählen.
3. **Speichern** auswählen.

Für jedes Speichervolumen gelten nun optimierte Einstellungen für das Speichervolumen-Wasserzeichen, basierend auf der Größe des Storage Node und der relativen Kapazität des Volumens.

Beheben von Metadatenproblemen in StorageGRID

Bei Problemen mit Metadaten informieren Warnmeldungen über die Ursache der Probleme und empfohlene Maßnahmen. Insbesondere ist das Hinzufügen neuer Storage Nodes erforderlich, wenn die Warnmeldung „Low metadata storage“ ausgelöst wird.

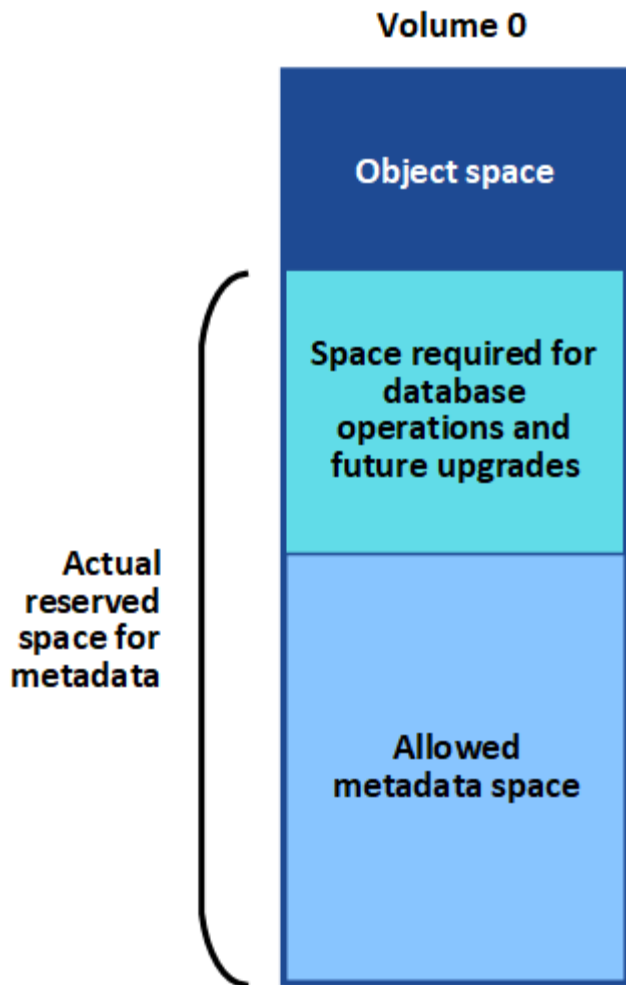
Bevor Sie beginnen

Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.

Über diese Aufgabe

Befolgen Sie die empfohlenen Maßnahmen für jede ausgelöste metadatenbezogene Warnung. Wenn die Warnung **Low metadata storage** ausgelöst wird, müssen neue Storage Nodes hinzugefügt werden.

StorageGRID reserviert auf Volume 0 jedes Storage Node einen bestimmten Speicherplatz für Objektmetadaten. Dieser Speicherplatz, der als *tatsächlich reservierter Speicherplatz* bezeichnet wird, ist unterteilt in den für Objektmetadaten vorgesehenen Speicherplatz (den zulässigen Metadatenspeicherplatz) und den für essentielle Datenbankoperationen wie Komprimierung und Reparatur benötigten Speicherplatz. Der zulässige Metadatenspeicherplatz bestimmt die Gesamtkapazität der Objekte.



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

Sie können ["Metadatenkapazität der Objekte für jeden Storage Node überwachen"](#) dazu beitragen, Fehler vorherzusehen und zu korrigieren, bevor sie auftreten.

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

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

- **Geringfügig:** Die Objektmetadaten belegen 70 % oder mehr des zulässigen Metadatenbereichs. Es wird empfohlen, so bald wie möglich neue Storage Nodes hinzuzufügen.
- **Schwerwiegend:** Die Objektmetadaten belegen 90 % oder mehr des zulässigen Metadaten Speichers. Es ist erforderlich, umgehend neue Storage Nodes hinzuzufügen.



Wenn Objektmetadaten 90 % oder mehr des zulässigen MetadatenSpeichers belegen, erscheint eine Warnung im Dashboard. Falls diese Warnung erscheint, ist es erforderlich, neue Storage Nodes umgehend hinzuzufügen. Objektmetadaten dürfen niemals mehr als 100 % des zulässigen Speicherplatzes belegen.

- **Kritisch:** Die Objektmetadaten belegen 100 % oder mehr des zulässigen MetadatenSpeichers und beginnen, den für essentielle Datenbankoperationen benötigten Speicherplatz zu verbrauchen. Die Aufnahme neuer Objekte muss gestoppt werden, und neue Storage Nodes müssen umgehend hinzugefügt werden.



Wenn die Größe von Volume 0 kleiner ist als die Speicheroption "Metadata Reserved Space" (zum Beispiel in einer Nicht-Produktionsumgebung), könnte die Berechnung für die Warnung **Geringer MetadatenSpeicher** ungenau sein.

Schritte

1. **Benachrichtigungen** > **Aktuell** auswählen.
2. In der Warntabelle kann bei Bedarf die Warngruppe **Geringer MetadatenSpeicher** erweitert und die spezifische Warnung ausgewählt werden, die angezeigt werden soll.
3. Die Details im Warndialogfeld können überprüft werden.
4. Wenn eine schwerwiegende oder kritische Warnung wegen **geringem MetadatenSpeicher** ausgelöst wurde, sollte eine Erweiterung durchgeführt werden, um sofort Storage Nodes hinzuzufügen.



Da StorageGRID an jedem Standort vollständige Kopien aller Objektmetadaten speichert, ist die Metadatenkapazität des gesamten Grids durch die Metadatenkapazität des kleinsten Standorts begrenzt. Wenn an einem Standort zusätzliche Metadatenkapazität benötigt wird, sollte auch "[Alle anderen Websites erweitern](#)" um die gleiche Anzahl an Storage Nodes erweitert werden.

Nach der Erweiterung verteilt StorageGRID die vorhandenen Objektmetadaten auf die neuen Knoten, wodurch die Gesamtkapazität des Grids für Metadaten erhöht wird. Es ist keine Benutzeraktion erforderlich. Die Warnung **Low metadata storage** wird aufgehoben.

Beheben von Zertifikatsfehlern in StorageGRID

Wenn beim Verbindungsversuch zu StorageGRID über einen Webbrowser, einen S3-Client oder ein externes Überwachungstool ein Sicherheits- oder Zertifikatsproblem auftritt, empfiehlt sich eine Überprüfung des Zertifikats.

Über diese Aufgabe

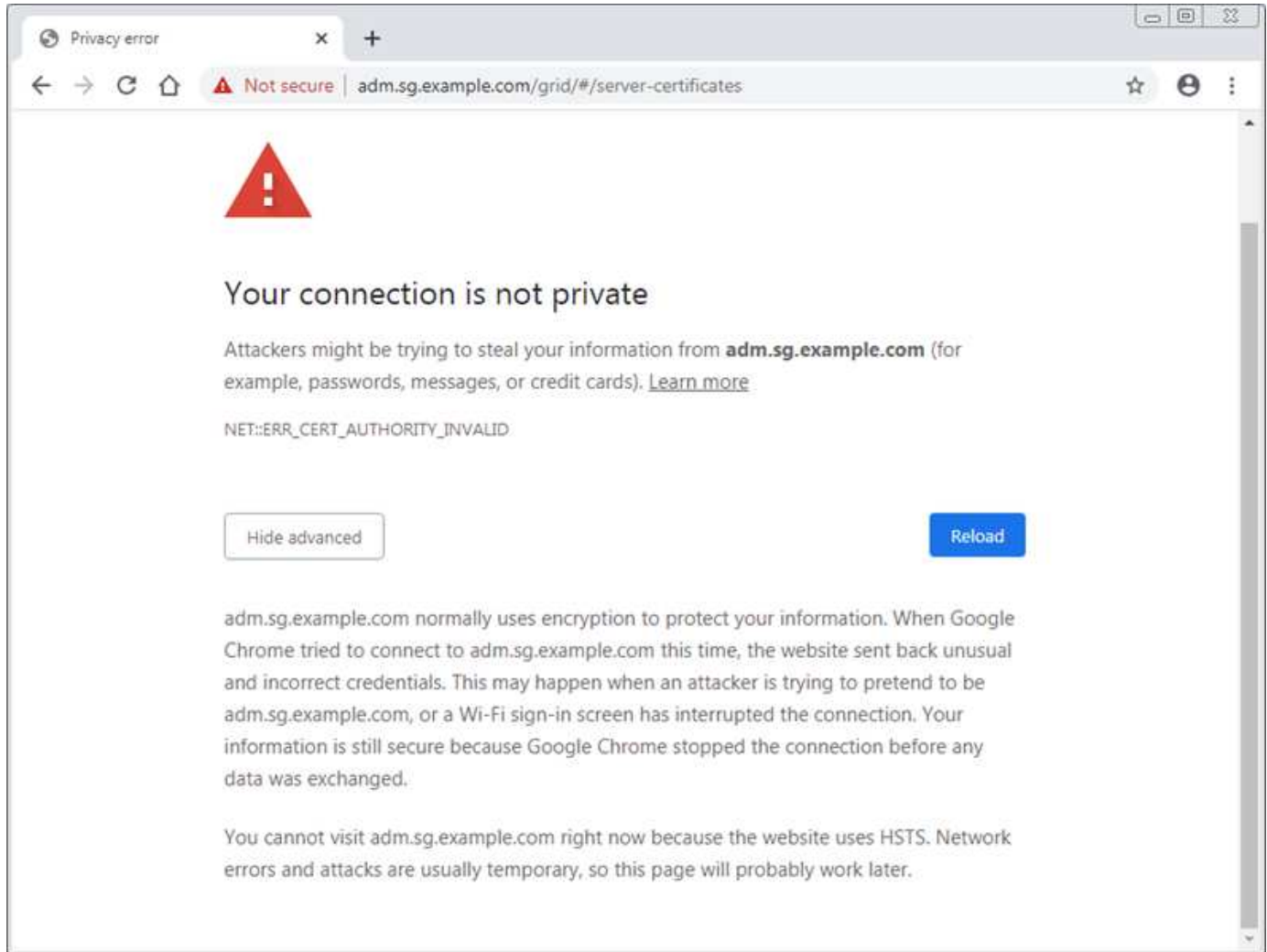
Zertifikatsfehler können Probleme verursachen, wenn Sie versuchen, über den Grid Manager, die Grid Management API, den Tenant Manager oder die Tenant Management API eine Verbindung zu StorageGRID herzustellen. Zertifikatsfehler können auch auftreten, wenn Sie versuchen, eine Verbindung mit einem S3 Client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

Wenn Sie über einen Domännennamen anstatt über eine IP-Adresse auf den Grid Manager oder Tenant Manager zugreifen, zeigt der Browser eine Zertifikatsfehlermeldung ohne Möglichkeit zur Umgehung an, wenn einer der folgenden Fälle eintritt:

- Ihr benutzerdefiniertes Managementoberfläche-Zertifikat läuft ab.

- Die Umstellung erfolgt von einem benutzerdefinierten Managementoberfläche-Zertifikat auf das Standardserverzertifikat.

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



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

Bei der Verwendung von Clientzertifikaten für die externe Prometheus-Integration können Zertifikatsfehler entweder durch das StorageGRID Managementoberfläche-Zertifikat oder durch Clientzertifikate verursacht werden. Die Warnung „Ablauf der auf der Seite Zertifikate konfigurierten Clientzertifikate“ wird ausgelöst, wenn ein Clientzertifikat demnächst abläuft.

Schritte

Wenn Sie eine Warnmeldung über ein abgelaufenes Zertifikat erhalten haben, können die Zertifikatsdetails aufgerufen werden: **Konfiguration > Sicherheit > Zertifikate** auswählen und dann "[die entsprechende Zertifikatsregisterkarte auswählen](#)".

1. Die Gültigkeitsdauer des Zertifikats prüfen. + Einige Webbrowser und S3-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.

2. Wenn das Zertifikat abgelaufen ist oder demnächst abläuft, sollte ein neues Zertifikat hochgeladen oder generiert werden.
 - Informationen zu einem Serverzertifikat bieten die Schritte unter "[Konfiguration eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#)".
 - Für ein Clientzertifikat siehe die Schritte für "[Konfiguration eines Clientzertifikats](#)".
3. Bei Serverzertifikatfehlern können eine oder beide der folgenden Optionen in Betracht gezogen werden:
 - Es ist sicherzustellen, dass der Subject Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass der SAN mit der IP-Adresse oder dem Hostnamen des Knotens übereinstimmt, zu dem eine Verbindung hergestellt wird.
 - Wenn versucht wird, eine Verbindung zu StorageGRID über einen Domännennamen herzustellen:
 - i. Um den Verbindungsfehler zu umgehen und auf den Grid Manager zuzugreifen, die IP-Adresse des Admin-Knotens anstelle des Domännennamens eingeben.
 - ii. Im Grid Manager **Konfiguration > Sicherheit > Zertifikate** auswählen und dann "[die entsprechende Zertifikatsregisterkarte auswählen](#)" verwenden, um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
 - iii. In den Anweisungen zur Administration von StorageGRID sind die Schritte für "[Konfiguration eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#)" aufgeführt.

Beheben von Problemen mit dem Admin Node und der Benutzeroberfläche in StorageGRID

Es stehen verschiedene Aufgaben zur Verfügung, die bei der Ermittlung der Ursache von Problemen im Zusammenhang mit Admin-Knoten und der StorageGRID Benutzeroberfläche unterstützen.

Anmeldefehler des Admin-Knotens

Wenn beim Anmelden an einem StorageGRID Admin Node ein Fehler auftritt, könnte Ihr System ein Problem mit einem "[Netzwerk](#)" oder "[Hardware](#)" Problem, ein Problem mit "[Admin Node Dienste](#)" oder ein "[Problem mit der Cassandra Datenbank](#)" auf verbundenen Storage Nodes haben.

Bevor Sie beginnen

- Sie sind mit einem "[unterstützte Webbrowser](#)" beim Grid Manager angemeldet.
- Sie haben die `Passwords.txt` Datei.
- Du hast "[spezifische Zugriffsberechtigungen](#)".

Über diese Aufgabe

Diese Richtlinien zur Fehlerbehebung gelten, wenn beim Anmelden an einem Admin-Knoten eine der folgenden Fehlermeldungen angezeigt wird:

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

- Unable to communicate with server. Reloading page...

Schritte

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

Wird der Fehler nicht automatisch behoben, folgt der nächste Schritt.

2. Wenn Ihr StorageGRID System mehr als einen Admin-Knoten hat, kann der Status eines nicht verfügbaren Admin-Knotens überprüft werden, indem Sie sich beim Grid Manager von einem anderen Admin-Knoten aus anmelden.
 - Wenn Sie sich anmelden können, stehen die Optionen **Dashboard**, **Knoten**, **Warnungen** und **Support** zur Verfügung, um die Ursache des Fehlers zu ermitteln.
 - Falls Sie nur einen Admin-Knoten haben oder sich immer noch nicht anmelden können, gehen Sie zum nächsten Schritt.
3. Es wird festgestellt, ob die Hardware des Knotens offline ist.
4. Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, finden Sie die Schritte für ["Konfiguration von Single Sign-On"](#).

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



Wenn SSO aktiviert ist, ist eine Anmeldung über einen eingeschränkten Port nicht möglich. Port 443 muss verwendet werden.

5. Es sollte festgestellt werden, ob das verwendete Konto zu einem Verbundbenutzer gehört.

Falls das Verbundbenutzerkonto nicht funktioniert, kann eine Anmeldung beim Grid Manager als lokaler Benutzer, wie zum Beispiel root, erfolgen.

- Wenn sich der lokale Benutzer anmelden kann:
 - i. Benachrichtigungen werden überprüft.
 - ii. **Konfiguration > Zugriffskontrolle > Identitätsföderation** auswählen.
 - iii. **Verbindung testen** kann verwendet werden, um die Verbindungseinstellungen für den LDAP-Server zu validieren.
 - iv. Falls der Test fehlschlägt, müssen etwaige Konfigurationsfehler behoben werden.
 - Wenn sich der lokale Benutzer nicht anmelden kann und Sie sicher sind, dass die Anmeldeinformationen korrekt sind, gehen Sie zum nächsten Schritt.
6. Secure Shell (SSH) zur Anmeldung am Admin-Knoten verwenden:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
 - b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
 - c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
 - d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von \$ zu #.

7. Status aller auf dem Grid-Knoten laufenden Dienste anzeigen: `storagegrid-status`

Es sollte sichergestellt sein, dass die Dienste nms, mi, nginx und mgmt api alle ausgeführt werden.

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

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

8. Bestätigen Sie, dass der nginx-gw Dienst läuft. # `service nginx-gw status`

9. Verwenden Sie Lumberjack, um Protokolle zu sammeln: # `/usr/local/sbin/lumberjack.rb`

Falls die Authentifizierung in der Vergangenheit fehlgeschlagen ist, können Sie mit den Lumberjack-Skriptoptionen `--start` und `--end` den entsprechenden Zeitraum festlegen. Details zu diesen Optionen bietet `lumberjack -h`.

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

10. Die folgenden Protokolle werden angezeigt:

° `/var/local/log/bycast.log`

- /var/local/log/bycast-err.log
- /var/local/log/nms.log
- **/*commands.txt

11. Falls keine Probleme mit dem Admin Node festgestellt werden konnten, kann einer der folgenden Befehle verwendet werden, um die IP-Adressen der drei Storage Nodes zu ermitteln, auf denen der ADC Service an Ihrem Standort ausgeführt wird. 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 Nodes nutzen den ADC-Dienst während des Authentifizierungsprozesses.

12. Vom Admin-Knoten aus per SSH bei jedem der ADC-Speicherknoten mit den ermittelten IP-Adressen anmelden.
13. Status aller auf dem Grid-Knoten laufenden Dienste anzeigen: `storagegrid-status`

Es sollte sichergestellt sein, dass die Dienste `idnt`, `acct`, `nginx` und `cassandra` alle ausgeführt werden.

14. Schritte [Verwenden Sie Lumberjack, um Protokolle zu sammeln](#). und [Protokolle anzeigen](#) werden wiederholt, um die Protokolle auf den Storage Nodes zu überprüfen.
15. Wenn das Problem nicht gelöst werden kann, sollte der technische Support kontaktiert werden.

Stellen Sie die gesammelten Protokolle dem technischen Support zur Verfügung. Siehe auch ["Referenz zu Protokolldateien"](#).

Probleme mit der Benutzeroberfläche

Die Benutzeroberfläche des Grid Managers oder des Tenant Managers reagiert nach einem Upgrade der StorageGRID Software möglicherweise nicht wie erwartet.

Schritte

1. Stellen Sie sicher, dass Sie ein ["unterstützte Webbrowser"](#) verwenden.
2. Leeren Sie den Cache Ihres Webbrowsers.

Durch das Leeren des Caches werden veraltete Ressourcen der vorherigen Version der StorageGRID Software entfernt, und die Benutzeroberfläche kann wieder korrekt funktionieren. Anleitungen dazu enthält die Dokumentation Ihres Webbrowsers.

Beheben von Netzwerk-, Hardware- und Plattformproblemen in StorageGRID

Es gibt verschiedene Aufgaben, die Sie durchführen können, um die Ursache von Problemen im Zusammenhang mit StorageGRID Netzwerk, Hardware und Plattform zu

ermitteln.

[[422-unprocessable-entity-errors]] == "422: Unprocessable Entity"-Fehler

Der Fehler 422: Nicht verarbeitbare Entität kann verschiedene Ursachen haben. Die Fehlermeldung gibt Aufschluss darüber, wodurch das Problem verursacht wurde.

Wenn eine der aufgeführten Fehlermeldungen angezeigt wird, sollte die empfohlene Maßnahme ergriffen werden.

Fehlermeldung	Grundursache 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>	Diese Meldung kann auftreten, wenn bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option TLS nicht verwenden für Transport Layer Security (TLS) ausgewählt wird. Die Option TLS nicht verwenden wird bei AD-Servern, die LDAP-Signierung erzwingen, nicht unterstützt. Es muss entweder die Option STARTTLS verwenden oder die Option LDAPS verwenden für TLS ausgewählt werden.

Fehlermeldung	Grundursache 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>	Diese Meldung erscheint, wenn versucht wird, eine nicht unterstützte Verschlüsselungsmethode zu verwenden, um eine Transport Layer Security (TLS)-Verbindung von StorageGRID zu einem externen System herzustellen, das für die Identitätsföderation oder Cloud Storage Pools verwendet wird. Die vom externen System angebotenen Verschlüsselungsverfahren sind zu prüfen. Das System muss eines der "Von StorageGRID unterstützte Chiffren" für ausgehende TLS-Verbindungen verwenden, wie in der Anleitung zur Administration von StorageGRID beschrieben.

Grid Network MTU-Nichtübereinstimmungswarnung

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

Über diese Aufgabe

Die Unterschiede in den MTU-Einstellungen könnten darauf hindeuten, dass einige, aber nicht alle eth0-Netzwerke für Jumbo-Frames konfiguriert sind. Eine MTU-Größenabweichung von mehr als 1000 kann Netzwerkleistungsprobleme verursachen.

Schritte

1. Der externe SSH-Zugriff ist standardmäßig blockiert. Falls erforderlich, ["vorübergehend Zugriff erlauben"](#).
2. Die MTU-Einstellungen für eth0 auf allen Knoten werden aufgelistet.
 - Die im Grid Manager bereitgestellte Abfrage kann verwendet werden.
 - Navigieren Sie zu *primary Admin Node IP address/metrics/graph* und geben Sie die folgende Abfrage ein: `node_network_mtu_bytes{device="eth0"}`
3. ["Die MTU-Einstellungen anpassen"](#) falls erforderlich, um sicherzustellen, dass sie für die Grid-Netzwerk-Schnittstelle (eth0) auf allen Knoten gleich sind.
 - Für Linux- und VMware-basierte Knoten kann folgender Befehl verwendet werden:
`/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

Hinweis: Auf Linux-basierten Knoten gilt: Falls der gewünschte MTU-Wert für das Netzwerk im Container den bereits auf der Host-Schnittstelle konfigurierten Wert überschreitet, muss zunächst die Host-Schnittstelle auf den gewünschten MTU-Wert konfiguriert werden und anschließend das

`change-ip.py` Skript verwendet werden, um den MTU-Wert des Netzwerks im Container zu ändern.

Die folgenden Argumente dienen zur Änderung der MTU auf Linux- oder VMware-basierten Knoten.

Positionsargumente	Beschreibung
<code>mtu</code>	Die einzustellende MTU. Muss im Bereich von 1280 bis 9216 liegen.
<code>network</code>	Die Netzwerke, auf die die MTU angewendet werden soll. Einer oder mehrere der folgenden Netzwerktypen sind einzubeziehen: • Grid • Administrator • Client

+

Optionale Argumente	Beschreibung
<code>-h, - help</code>	Hilfemeldung anzeigen und beenden.
<code>-n node, --node node</code>	Der Knoten. Standardmäßig ist der lokale Knoten.

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

Warnung über einen Empfangsfehler im Knotennetzwerk

Node network reception frame error-Warnmeldungen können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerkhardware verursacht werden. Diese Warnung wird automatisch aufgehoben, nachdem das zugrunde liegende Problem behoben wurde.

Über diese Aufgabe

Fehler beim Empfang von Frames im Knotennetzwerk können durch die folgenden Probleme mit der Netzwerkhardware verursacht werden, die mit StorageGRID verbunden ist:

- Vorwärtsfehlerkorrektur (FEC) ist erforderlich und wird nicht verwendet
- MTU-Fehler zwischen Switch Port und Netzwerkkarte
- Hohe Verbindungsfehlerraten
- NIC Ringpufferüberlauf

Schritte

1. Führen Sie die Schritte zur Fehlerbehebung für alle potenziellen Ursachen dieser Warnmeldung entsprechend Ihrer Netzwerkkonfiguration aus.
2. Führen Sie die folgenden Schritte entsprechend der Fehlerursache aus:

FEC Abweichung



Diese Schritte sind nur für **Node network reception frame error** Warnungen anwendbar, die durch FEC-Fehlanpassungen auf StorageGRID Geräten verursacht werden.

- a. Den FEC-Status des Ports im Switch prüfen, der an Ihre StorageGRID Appliance angeschlossen ist.
- b. Die physische Unversehrtheit der Kabel vom Gerät zum Switch überprüfen.
- c. Wenn Sie die FEC-Einstellungen ändern möchten, um die Warnung zu beheben, sollte zunächst sichergestellt werden, dass das Gerät auf der Seite „Link Configuration“ des StorageGRID Appliance Installer für den **Auto**-Modus 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 entsprechend an.

Die FEC-Einstellungen können auf StorageGRID Appliances nicht konfiguriert werden. Stattdessen versuchen die Appliances, die FEC-Einstellungen an den Switch-Ports, mit denen sie verbunden sind, zu erkennen und zu spiegeln. Wenn die Verbindungen auf Netzwerkgeschwindigkeiten von 25-GbE oder 100-GbE festgelegt werden, kann es vorkommen, dass Switch und Netzwerkkarte keine gemeinsame FEC-Einstellung aushandeln können. Ohne eine gemeinsame FEC-Einstellung fällt das Netzwerk in den „no-FEC“-Modus zurück. Wenn FEC nicht aktiviert ist, sind die Verbindungen anfälliger für Fehler durch elektrische Störungen.



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

MTU-Fehler zwischen Switch Port und Netzwerkkarte

Wenn die Warnung durch eine Diskrepanz zwischen Switch-Port und NIC-MTU verursacht wird, prüfen Sie, ob die auf dem Node konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port übereinstimmt.

Die auf dem Knoten konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung am Switch-Port, an den der Knoten angeschlossen ist. Wenn ein StorageGRID-Knoten einen Ethernet-Frame empfängt, der größer als seine MTU ist, was mit dieser Konfiguration möglich ist, kann die Warnung **Node network reception frame error** gemeldet werden. Wenn dies vermutet wird, sollte entweder die MTU des Switch-Ports an die MTU der StorageGRID-Netzwerkschnittstelle angepasst werden oder die MTU der StorageGRID-Netzwerkschnittstelle an die des Switch-Ports, abhängig von den End-to-End-MTU-Zielen oder -Anforderungen.



Für optimale Netzwerkleistung sollten alle Knoten mit ähnlichen MTU-Werten an ihren Grid-Netzwerk-Schnittstellen konfiguriert sein. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn es signifikante Unterschiede in den MTU-Einstellungen für das Grid-Netzwerk auf einzelnen Knoten gibt. Die MTU-Werte müssen nicht für alle Netzwerktypen identisch sein. Siehe [Fehlerbehebung bei der Warnung zur MTU-Fehlanpassung im Grid Network](#) für weitere Informationen.



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

Hohe Verbindungsfehlerraten

- a. FEC aktivieren, falls noch nicht aktiviert.
- b. Stellen Sie sicher, dass Ihre Netzwerkverkabelung von guter Qualität ist und weder beschädigt noch falsch angeschlossen ist.
- c. Wenn die Kabel nicht die Ursache des Problems zu sein scheinen, den technischen Support kontaktieren.



In einer Umgebung mit hohem elektrischem Rauschen können hohe Fehlerraten auftreten.

NIC Ringpufferüberlauf

Falls es sich bei dem Fehler um einen Überlauf des NIC-Ringpuffers handelt, wenden Sie sich an den technischen Support.

Der Ringpuffer kann überlaufen, wenn das StorageGRID System überlastet ist und Netzwerkereignisse nicht zeitnah verarbeiten kann.

3. Das Problem sollte überwacht werden, und der technische Support ist zu kontaktieren, falls die Warnmeldung nicht behoben wird.

Zeitsynchronisationsfehler

Möglicherweise treten Probleme mit der Zeitsynchronisation in Ihrem Grid auf.

Wenn Probleme mit der Zeitsynchronisierung auftreten, sollte überprüft werden, ob mindestens vier externe NTP-Quellen angegeben wurden, die jeweils eine Stratum 3- oder bessere Referenz liefern, und ob alle externen NTP-Quellen ordnungsgemäß funktionieren und von den StorageGRID Knoten erreichbar sind.



Bei einer "[Angabe der externen NTP-Quelle](#)" StorageGRID-Installation im Produktionsbetrieb sollte der Windows-Zeitdienst (W32Time) nicht unter einer Windows-Version vor Windows Server 2016 verwendet werden. Der Zeitdienst älterer Windows-Versionen ist nicht ausreichend genau und wird von Microsoft für den Einsatz in Umgebungen mit hohen Genauigkeitsanforderungen wie StorageGRID nicht unterstützt.

Linux: Probleme mit der Netzwerkverbindung

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

MAC Address Cloning

In manchen Fällen können Netzwerkprobleme durch die Verwendung von MAC-Adressenklonen behoben werden. Wenn virtuelle Hosts verwendet werden, ist der Wert des Schlüssels für das MAC-Adressenklonen für jedes Ihrer Netzwerke in der Knotenkonfigurationsdatei auf „true“ zu setzen. Mit dieser Einstellung verwendet der StorageGRID-Container die MAC-Adresse des Hosts. Siehe die Anweisungen zu ["Knotenkonfigurationsdateien erstellen"](#).



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

Weitere Informationen sind in der Anleitung für ["Aktivieren des MAC-Klonens"](#) enthalten.

Promiscuous Mode

Wenn Sie die MAC-Adressenklonierung nicht nutzen und stattdessen allen Schnittstellen erlauben möchten, Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen zu empfangen und zu senden, muss sichergestellt sein, dass die Sicherheitseigenschaften auf Ebene des virtuellen Switches und der Portgruppe für Promiscuous Mode, MAC Address Changes und Forged Transmits auf **Accept** gesetzt sind. Die auf dem virtuellen Switch festgelegten Werte können durch die Werte auf Portgruppenebene überschrieben werden, daher sollte sichergestellt sein, dass die Einstellungen an beiden Stellen identisch sind.

Weitere Informationen zur Verwendung des Promiscuous Mode finden sich in der Anleitung für ["wie das Host-Netzwerk konfiguriert wird"](#).

Linux: Der Knotenstatus ist "verwaist"

Ein Linux-Knoten im verwaisten Zustand deutet in der Regel darauf hin, dass entweder der storagegrid Service oder der StorageGRID Node Daemon, der den Container des Knotens steuert, unerwartet abgestürzt ist.

Über diese Aufgabe

Wenn ein Linux-Knoten meldet, dass er sich in einem verwaisten Zustand befindet, ist Folgendes zu beachten:

- Protokolle auf Fehler und Meldungen prüfen.
- Der Knoten wird erneut gestartet.
- Verwenden Sie gegebenenfalls Container-Engine-Befehle, um den vorhandenen Node Container zu stoppen.
- Der Knoten wird neu gestartet.

Schritte

1. Die Protokolle sowohl des Service-Daemons als auch des verwaisten Knotens auf offensichtliche Fehler oder Meldungen über ein unerwartetes Beenden prüfen.
2. Melden Sie sich am Host als Root oder mit einem Konto mit sudo-Berechtigung an.
3. Versuch, den Knoten erneut zu starten, indem Sie den folgenden Befehl ausführen: `$ sudo storagegrid node start node-name`

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

Wenn der Knoten verwaist ist, lautet die Antwort

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

4. Unter Linux die Container-Engine und alle zugehörigen storagegrid-node-Prozesse anhalten. Zum Beispiel: `sudo docker stop --time seconds container-name`

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

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

5. Der Knoten wird neu gestartet: `storagegrid node start node-name`

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

Linux: Fehlerbehebung bei der IPv6-Unterstützung

Möglicherweise muss die IPv6-Unterstützung im Kernel aktiviert werden, wenn StorageGRID-Knoten auf Linux-Hosts installiert wurden und festgestellt wird, dass den Knotencontainern nicht wie erwartet IPv6-Adressen zugewiesen wurden.

Über diese Aufgabe

Die einem Grid-Knoten zugewiesene IPv6-Adresse kann wie folgt angezeigt werden:

1. **Knoten** auswählen und den gewünschten Knoten auswählen.
2. Auf der Registerkarte „Übersicht“ neben „IP-Adressen“ die Option „Zusätzliche IP-Adressen anzeigen“ auswählen.

Falls die IPv6-Adresse nicht angezeigt wird und der Knoten auf einem Linux-Host installiert ist, sind die folgenden Schritte erforderlich, um die IPv6-Unterstützung im Kernel zu aktivieren.

Schritte

1. Melden Sie sich am Host als Root oder mit einem Konto mit sudo-Berechtigung an.
2. Führen Sie 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
```



Falls das Ergebnis nicht 0 ist, siehe die Dokumentation Ihres Betriebssystems zum Ändern der `sysctl` Einstellungen. Anschließend den Wert auf 0 ändern, bevor fortgefahren wird.

3. Wechsel in den StorageGRID Knotencontainer: `storagegrid node enter node-name`

4. Führen Sie 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, ist diese Vorgehensweise nicht anwendbar. Wenden Sie sich an den technischen Support.

5. Container verlassen: `exit`

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

6. Als Root die folgende Datei bearbeiten: `/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 Kommentarzeichen. Anschließend die Datei speichern und schließen.

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

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

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

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

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

Fehlerbehebung bei Fehlermeldungen des externen Syslog-Servers für StorageGRID

Die folgende Tabelle beschreibt die Fehlermeldungen, die im Zusammenhang mit der Verwendung eines externen Syslog-Servers auftreten können, und listet Korrekturmaßnahmen auf.

Diese Fehler werden vom Assistenten zum Konfigurieren des externen Syslog Servers angezeigt, wenn Probleme beim Senden von Testnachrichten auftreten, um zu überprüfen, ob der externe Syslog Server korrekt konfiguriert ist.

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

Weitere Informationen zum Senden von Audit-Informationen an einen externen Syslog-Server sind verfügbar unter:

- ["Überlegungen zur Verwendung eines externen Syslog Servers"](#)
- ["Logverwaltung und externen Syslog-Server konfigurieren"](#)

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Kann den Hostnamen nicht auflösen	Der von Ihnen eingegebene FQDN für den Syslog-Server konnte nicht in eine IP-Adresse aufgelöst werden. 1. Überprüfen Sie den eingegebenen Hostnamen. Falls Sie eine IP-Adresse eingegeben haben, stellen Sie sicher, dass es sich um eine gültige IP-Adresse im W.X.Y.Z-Format ("Punktdezimaldarstellung") handelt. 2. Es sollte überprüft werden, ob die DNS-Server korrekt konfiguriert sind. 3. Bestätigen Sie, dass jeder Node auf die IP-Adressen des DNS-Servers zugreifen kann.
Verbindung abgelehnt	Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde verweigert. Möglicherweise lauscht kein Dienst auf dem TCP- oder TLS-Port des Hosts, oder eine Firewall blockiert den Zugriff. 1. Überprüfen Sie, ob der korrekte FQDN oder die korrekte IP-Adresse, der korrekte Port und das korrekte Protokoll für den Syslog-Server eingegeben wurden. 2. Bestätigen Sie, dass auf dem Host für den Syslog-Dienst ein Syslog-Daemon ausgeführt wird, der auf dem angegebenen Port lauscht. 3. Bestätigen Sie, dass keine Firewall den Zugriff auf TCP/TLS-Verbindungen von den Nodes zur IP-Adresse und zum Port des Syslog-Servers blockiert.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Netzwerk nicht erreichbar	Der Syslog-Server befindet sich nicht in einem direkt angeschlossenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass er die Testnachrichten von den aufgelisteten Nodes nicht an den Syslog-Server weiterleiten konnte. 1. Prüfen Sie, ob der korrekte FQDN oder die korrekte IP-Adresse für den Syslog-Server eingegeben wurde. 2. Für jeden aufgeführten Node die Grid Network Subnet List, die Admin Networks Subnet Lists und die Client Network Gateways prüfen. Bestätigen, dass diese so konfiguriert sind, dass der Datenverkehr zum Syslog-Server über die erwartete Netzwerkschnittstelle und das entsprechende Gateway (Grid, Admin oder Client) geleitet wird.
Host nicht erreichbar	Der Syslog-Server befindet sich in einem direkt angeschlossenen Subnetz (Subnetz, das von den aufgeführten Nodes für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Nodes haben versucht, Testnachrichten zu senden, aber keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers erhalten. 1. Prüfen Sie, ob der korrekte FQDN oder die korrekte IP-Adresse für den Syslog-Server eingegeben wurde. 2. Es sollte überprüft werden, ob der Host, auf dem der Syslog-Dienst ausgeführt wird, erreichbar ist.
Zeitüberschreitung bei der Verbindung	Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber vom Syslog-Server wurde über einen längeren Zeitraum keine Antwort empfangen. Möglicherweise liegt eine Routing-Fehlkonfiguration vor oder eine Firewall verwirft den Datenverkehr, ohne eine Antwort zu senden (eine häufige Konfiguration). 1. Prüfen Sie, ob der korrekte FQDN oder die korrekte IP-Adresse für den Syslog-Server eingegeben wurde. 2. Für jeden aufgeführten Node die Grid Network Subnet List, die Admin Networks Subnet Lists und die Client Network Gateways prüfen. Bestätigen, dass diese so konfiguriert sind, dass der Datenverkehr zum Syslog-Server über die erwartete Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) geleitet wird. 3. Bestätigen Sie, dass keine Firewall den Zugriff auf TCP/TLS-Verbindungen von den aufgeführten Knoten zur IP-Adresse und zum Port des Syslog-Servers blockiert.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
Verbindung vom Partner geschlossen	Es wurde eine TCP-Verbindung zum Syslog-Server erfolgreich hergestellt, diese wurde jedoch später wieder geschlossen. Mögliche Gründe hierfür sind: • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gebootet. • Der Node und der Syslog-Server können unterschiedliche TCP/TLS-Einstellungen haben. • Möglicherweise schließt eine zwischengeschaltete Firewall inaktive TCP-Verbindungen. • Ein Nicht-Syslog-Server, der auf dem Syslog-Server-Port lauscht, könnte die Verbindung geschlossen haben. Zur Behebung dieses Problems: 1. Überprüfen Sie, ob der korrekte FQDN oder die korrekte IP-Adresse, der korrekte Port und das korrekte Protokoll für den Syslog-Server eingegeben wurden. 2. Wenn Sie TLS verwenden, vergewissern Sie sich, dass der Syslog-Server ebenfalls TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server ebenfalls TCP verwendet. 3. Es sollte überprüft werden, ob eine zwischengeschaltete Firewall so konfiguriert ist, dass sie inaktive TCP-Verbindungen schließt.
TLS-Zertifikatfehler	Das vom Syslog-Server empfangene Serverzertifikat war nicht kompatibel mit dem CA-Zertifikatspaket und dem Clientzertifikat, das Sie bereitgestellt haben. 1. Bestätigen Sie, dass das CA-Zertifikatspaket und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat auf dem Syslog-Server kompatibel sind. 2. <code>\${post_edited_translations.segment}</code>
Weiterleitung ausgesetzt	Syslog-Einträge werden nicht mehr an den Syslog-Server weitergeleitet und StorageGRID kann den Grund nicht erkennen. Die mit diesem Fehler bereitgestellten Debugging-Protokolle geben Aufschluss über die mögliche Ursache.

Fehlermeldung	Beschreibung und empfohlene Maßnahmen
TLS-Sitzung beendet	Der Syslog-Server hat die TLS-Sitzung beendet, und StorageGRID kann den Grund nicht erkennen. 1. Die mit diesem Fehler bereitgestellten Debugging-Protokolle geben Aufschluss über die mögliche Ursache. 2. Überprüfen Sie, ob der korrekte FQDN oder die korrekte IP-Adresse, der korrekte Port und das korrekte Protokoll für den Syslog-Server eingegeben wurden. 3. Wenn Sie TLS verwenden, vergewissern Sie sich, dass der Syslog-Server ebenfalls TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server ebenfalls TCP verwendet. 4. Bestätigen Sie, dass das CA-Zertifikatpaket und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat des Syslog-Servers kompatibel sind. 5. <code>\$_post_edited_translations.segment</code>
Abfrage der Ergebnisse fehlgeschlagen	Der für die Konfiguration und das Testen des Syslog-Servers verwendete Admin-Knoten kann keine Testergebnisse von den aufgelisteten Knoten anfordern. Möglicherweise ist mindestens ein Knoten ausgefallen. 1. Standardmäßige Schritte zur Fehlerbehebung stellen sicher, dass die Nodes online sind und alle erwarteten Services laufen. 2. Den miscd Dienst auf den aufgelisteten Nodes neu starten.

Erfahren Sie mehr über Caching-Probleme von Load-Balancern in StorageGRID

Informationen zu möglichen Problemen mit Load-Balancer-Caching und deren Fehlerbehebung.

Feststellen, ob eine Anfrage ein Cache-Treffer war

- Der X-Cache-Header wird in der Antwort auf Anfragen gesetzt, die vom Cache-Dienst verarbeitet werden. Mögliche Codes:
 - **HIT**: Das Objekt wurde aus dem Cache bereitgestellt
 - **PARTIAL-HIT**: Der Bucket/Schlüssel hatte zwar einen Eintrag im Cache, aber nicht der gesamte angeforderte Bereich konnte aus dem Cache bedient werden.
 - **STALE**: Der Bucket/Schlüssel hatte einen Eintrag im Cache, aber das Objekt wurde seit dem letzten Abruf aus dem Cache aktualisiert.
 - **MISS**: Das Objekt befand sich nicht im Cache
- Der ``nginx-gw/endpoint-access.log.gz`` Datensatz für die Anfrage enthält "unix:/run/cache-svc/cache-svc.sock" für Anfragen, die vom Cache verarbeitet werden.
- Die ``cache-svc/cache-svc.log`` meldet eine Nachricht wie „Anfrage 320390: erfolgreich abgeschlossen (Cache-Treffer)“ oder „Anfrage 320375: erfolgreich abgeschlossen (Cache-Miss)“. Der angeforderte Pfad lässt sich finden, indem nach anderen Einträgen mit derselben Zeichenfolge „Request <number>“ gesucht

wird.

Niedrige Cache-Trefferquote

- Niedrige Cache-Trefferquoten sind zu erwarten, wenn eine neue Arbeitslast hinzugefügt wird oder sich die von einer Arbeitslast genutzte Arbeitsmenge ändert. In diesen Situationen wird erwartet, dass die Trefferquote im Laufe der Zeit steigt.
- Wenn mehrere Workloads Caching nutzen, kann das Hinzufügen von Richtlinien zur Datenverkehrsklassifizierung dazu beitragen, die vom Cache bedienten Teile der Workloads zu isolieren. Cache-Trefferquotenmetriken sind pro Datenverkehrsklassifizierungsrichtlinie verfügbar. Wenn einige Workloads keine guten Cache-Trefferquoten aufweisen, kann das Verschieben dieser Workloads auf andere Endpunkte ohne aktiviertes Caching in Betracht gezogen werden.
- Die Cache-Verdrängungsrate wird bewertet. Wenn der Cache zu klein ist, um den Arbeitsdatensatz aufzunehmen, treten hohe Verdrängungsraten auf, was zu einer niedrigeren Trefferquote beitragen kann.
- Optionen zur Verbesserung der Trefferquote bestimmter Workloads könnten unter FPVR verfügbar sein.

Geringe Leistung

- Die Cache-Trefferquote bewerten. Niedrige Cache-Trefferquoten können zu einer niedrigen Gesamtleistung führen.
- Die Cache-Verdrängungsrate wird bewertet. Während der Verdrängung werden einige Speicherressourcen für das Entfernen vorhandener Objekte von der Festplatte verwendet. Hält der Verdrängungsprozess mit dem Zugriff auf neue Objekte nicht Schritt, kann das System die Hard-Watermark-Schwellenwerte erreichen und beginnt, den Cache zu umgehen.
- Netzwerkbeschränkungen lassen sich anhand der Diagnose „Network interfaces receive usage“ und „Network interfaces transmit usage“ überprüfen.

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

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

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

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

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

Markeninformationen

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