Überwachen und Fehler beheben

StorageGRID software

NetApp
December 03, 2025

Inhalt

Überwachen und beheben Sie Fehler eines StorageGRID -Systems

Überwachen Sie das StorageGRID -System

Überwachen Sie ein StorageGRID -System

Überwachen Sie Ihr StorageGRID System regelmäßig, um sicherzustellen, dass es die erwartete Leistung erbringt.

Bevor Sie beginnen

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

> Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben Folgendes:

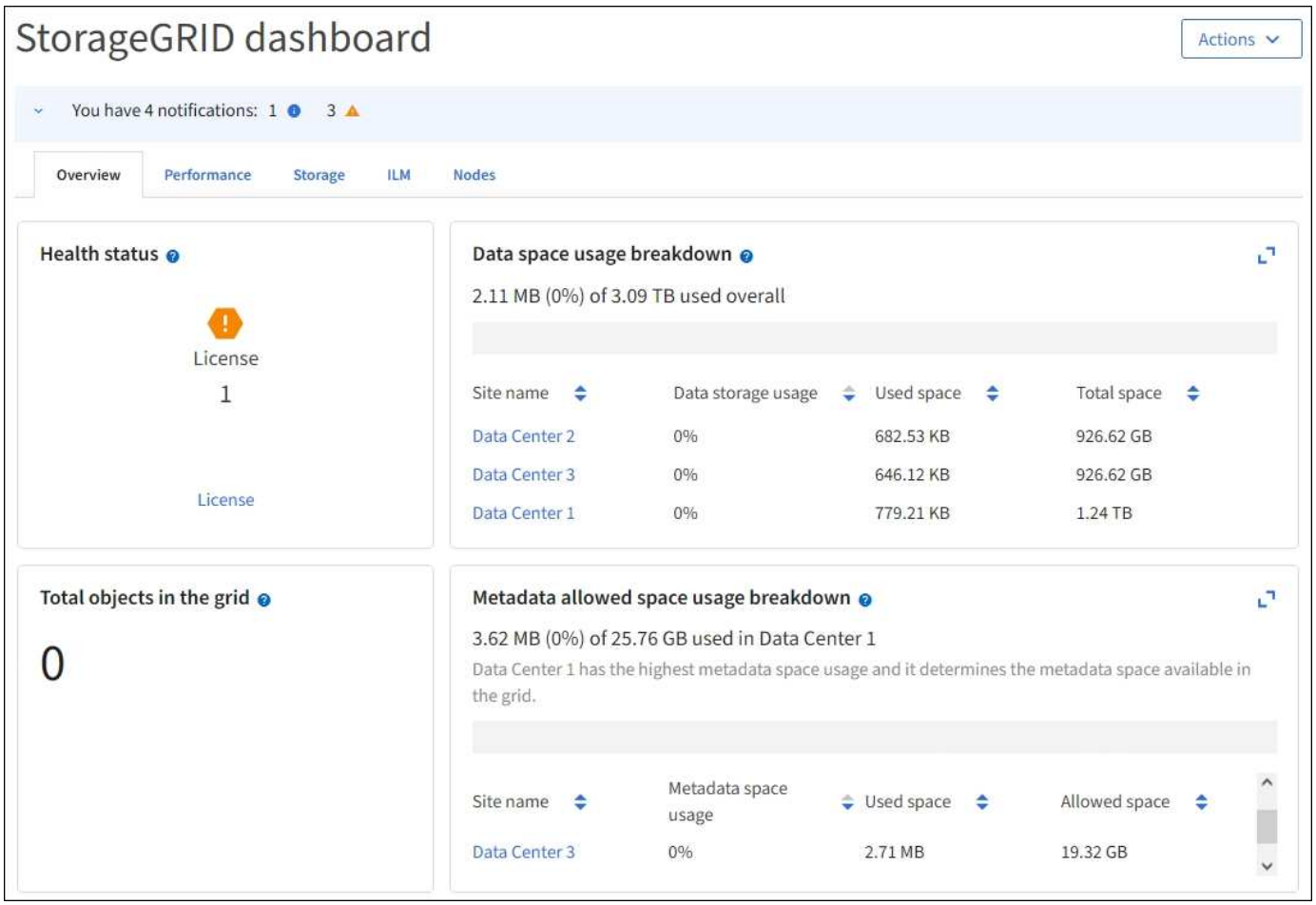
- "Anzeigen und Verwalten des Dashboards"
- "Anzeigen der Seite „Knoten“"
- "Überwachen Sie diese Aspekte des Systems regelmäßig:"
  - "Systemzustand"
  - "Speicherkapazität"
  - "Informationslebenszyklusmanagement"
  - "Netzwerk- und Systemressourcen"
  - "Mieteraktivität"
  - "Lastausgleichsvorgänge"
  - "Grid-Föderation-Verbindungen"
- "Verwalten von Warnungen"
- "Protokolldateien anzeigen"
- "Konfigurieren von Überwachungsmeldungen und Protokollzielen"
- "Verwenden Sie einen externen Syslog-Server"um Auditinformationen zu sammeln
- "Verwenden Sie SNMP zur Überwachung"
- "Erhalten Sie zusätzliche StorageGRID Daten", einschließlich Metriken und Diagnose

Anzeigen und Verwalten des Dashboards

Über das Dashboard können Sie die Systemaktivitäten auf einen Blick überwachen. Sie können benutzerdefinierte Dashboards erstellen, um Ihre StorageGRID-Implementierung zu überwachen.

Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.

Ihr Dashboard kann je nach Systemkonfiguration unterschiedlich sein.



Dashboard anzeigen

Das Dashboard besteht aus Registerkarten, die spezifische Informationen zum StorageGRID -System enthalten. Jede Registerkarte enthält Kategorien von Informationen, die auf Karten angezeigt werden.

Sie können das vom System bereitgestellte Dashboard unverändert verwenden. Darüber hinaus können Sie benutzerdefinierte Dashboards erstellen, die nur die Registerkarten und Karten enthalten, die für die Überwachung Ihrer StorageGRID-Implementierung relevant sind.

Die vom System bereitgestellten Dashboard-Registerkarten enthalten Karten mit den folgenden Arten von Informationen:

Registerkarte auf dem vom System bereitgestellten Dashboard	Enthält
Überblick	Allgemeine Informationen zum Raster, z. B. aktive Warnungen, Speicherplatznutzung und Gesamtzahl der Objekte im Raster.

Registerkarte auf dem vom System bereitgestellten Dashboard	Enthält
Performance	Speicherplatznutzung, im Laufe der Zeit verwendeter Speicher, S3-Vorgänge, Anforderungsdauer, Fehlerrate.
Storage	Nutzung des Mandantenkontingents und Nutzung des logischen Speicherplatzes. Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten.
ILM	Warteschlange und Auswertungsrate für das Informationslebenszyklusmanagement.
Nodes	CPU-, Daten- und Speichernutzung nach Knoten. S3-Operationen nach Knoten. Knoten-zu-Site-Verteilung.

Einige der Karten können zur besseren Anzeige maximiert werden. Wählen Sie das Maximierungssymbol in der oberen rechten Ecke der Karte. Um eine maximierte Karte zu schließen, wählen Sie das Symbol „Minimieren“ oder wählen Sie **Schließen**.

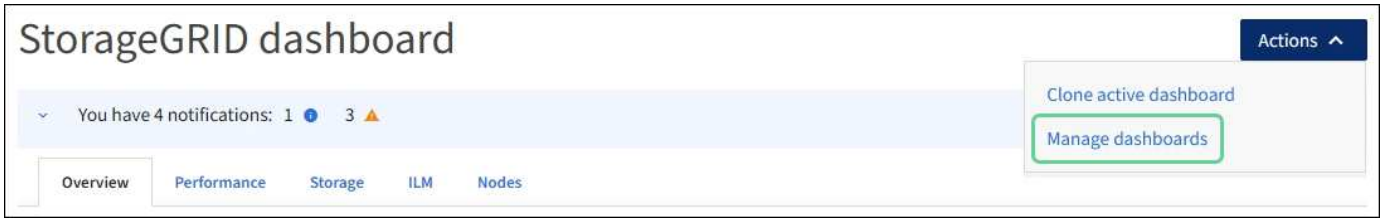
Dashboards verwalten

Wenn Sie Root-Zugriff haben (siehe"Berechtigungen der Administratorgruppe") können Sie die folgenden Verwaltungsaufgaben für Dashboards ausführen:

- Erstellen Sie ein benutzerdefiniertes Dashboard von Grund auf. Sie können benutzerdefinierte Dashboards verwenden, um zu steuern, welche StorageGRID -Informationen angezeigt werden und wie diese Informationen organisiert sind.
- Klonen Sie ein Dashboard, um benutzerdefinierte Dashboards zu erstellen.
- Legen Sie ein aktives Dashboard für einen Benutzer fest. Das aktive Dashboard kann das vom System bereitgestellte Dashboard oder ein benutzerdefiniertes Dashboard sein.
- Legen Sie ein Standard-Dashboard fest, das allen Benutzern angezeigt wird, sofern sie nicht ihr eigenes Dashboard aktivieren.
- Bearbeiten Sie einen Dashboard-Namen.
- Bearbeiten Sie ein Dashboard, um Registerkarten und Karten hinzuzufügen oder zu entfernen. Sie können mindestens 1 und höchstens 20 Registerkarten haben.
- Entfernen Sie ein Dashboard.

> Wenn Sie neben dem Root-Zugriff über eine andere Berechtigung verfügen, können Sie nur ein aktives Dashboard festlegen.

Um Dashboards zu verwalten, wählen Sie **Aktionen** > **Dashboards verwalten**.



Dashboards konfigurieren

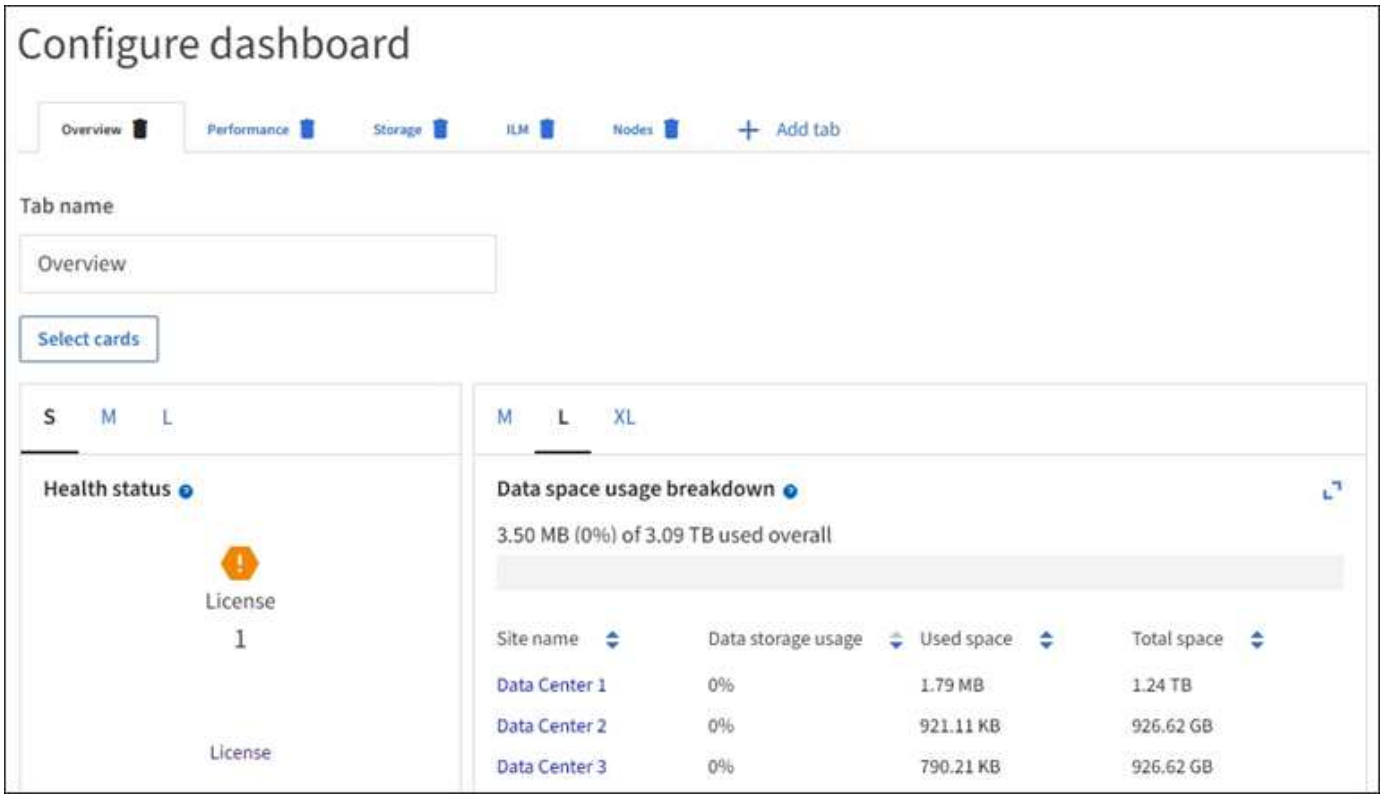
Um durch Klonen des aktiven Dashboards ein neues Dashboard zu erstellen, wählen Sie **Aktionen** > **Aktives Dashboard klonen**.

Um ein vorhandenes Dashboard zu bearbeiten oder zu klonen, wählen Sie **Aktionen** > **Dashboards verwalten**.

Das vom System bereitgestellte Dashboard kann nicht bearbeitet oder entfernt werden.

Beim Konfigurieren eines Dashboards können Sie:

- Registerkarten hinzufügen oder entfernen
- Benennen Sie Registerkarten um und geben Sie neuen Registerkarten eindeutige Namen
- Karten für jede Registerkarte hinzufügen, entfernen oder neu anordnen (ziehen)
- Wählen Sie die Größe für einzelne Karten, indem Sie oben auf der Karte **S**, **M**, **L** oder **XL** auswählen



Anzeigen der Seite „Knoten“

Anzeigen der Seite „Knoten“

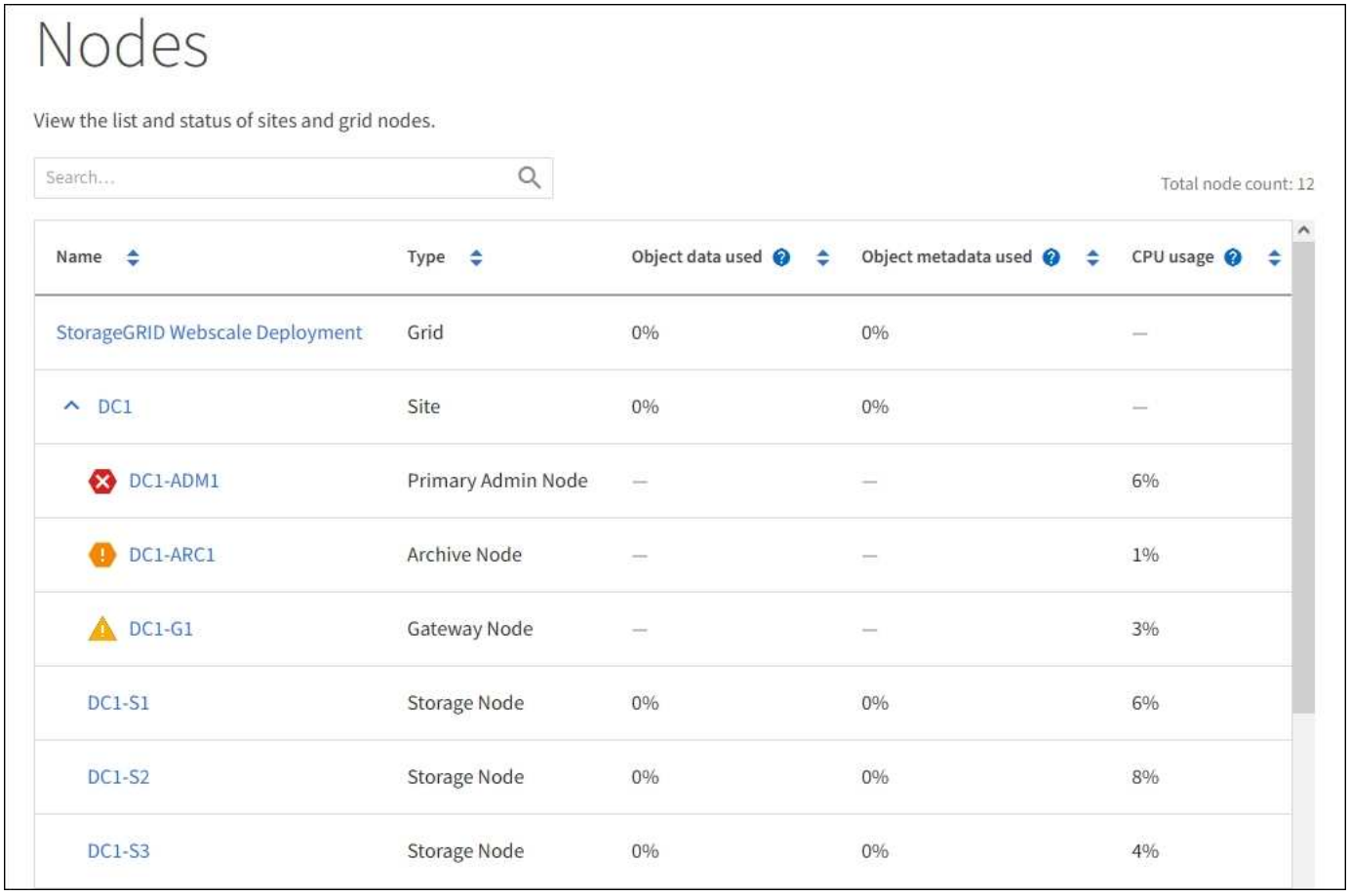
Wenn Sie detailliertere Informationen zu Ihrem StorageGRID -System benötigen, als das Dashboard bietet, können Sie auf der Seite „Knoten“ Metriken für das gesamte Grid, jeden Standort im Grid und jeden Knoten an einem Standort anzeigen.

In der Knotentabelle sind zusammenfassende Informationen für das gesamte Raster, jeden Standort und jeden Knoten aufgeführt. Wenn die Verbindung zu einem Knoten getrennt ist oder eine aktive Warnung vorliegt, wird neben dem Knotennamen ein Symbol angezeigt. Wenn der Knoten verbunden ist und keine aktiven Warnungen aufweist, wird kein Symbol angezeigt.

Wenn ein Knoten nicht mit dem Grid verbunden ist, beispielsweise während eines Upgrades oder in einem getrennten Zustand, sind bestimmte Metriken möglicherweise nicht verfügbar oder aus den Site- und Grid-Gesamtwerten ausgeschlossen. Nachdem ein Knoten die Verbindung zum Netz wiederhergestellt hat, warten Sie einige Minuten, bis sich die Werte stabilisiert haben.

Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.

Bei den gezeigten Screenshots handelt es sich um Beispiele. Ihre Ergebnisse können je nach Ihrer StorageGRID -Version variieren.



Verbindungsstatussymbole

Wenn ein Knoten vom Netz getrennt wird, wird neben dem Knotennamen eines der folgenden Symbole angezeigt.

Symbol	Beschreibung	Handlungsbedarf
	**Nicht verbunden – Unbekannt** Aus einem unbekannten Grund wird die Verbindung zu einem Knoten getrennt oder die Dienste auf dem Knoten fallen unerwartet aus. Beispielsweise könnte ein Dienst auf dem Knoten gestoppt worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Störung seine Netzwerkverbindung verloren haben. Möglicherweise wird auch die Warnung **Kommunikation mit Knoten nicht möglich** ausgelöst. Möglicherweise sind auch andere Warnungen aktiv.	Erfordert sofortige Aufmerksamkeit. "Wählen Sie jede Warnung aus" und befolgen Sie die empfohlenen Maßnahmen. Beispielsweise müssen Sie möglicherweise einen angehaltenen Dienst neu starten oder den Host für den Knoten neu starten. **Hinweis**: Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen können Sie den Status „Unbekannt“ ignorieren.
	**Nicht verbunden – Administrator-Ausfall** Aus einem erwarteten Grund ist der Knoten nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Möglicherweise sind auch eine oder mehrere Warnungen aktiv. Je nach zugrunde liegendem Problem gehen diese Knoten häufig ohne Eingriff wieder online.	Stellen Sie fest, ob dieser Knoten von Warnungen betroffen ist. Wenn eine oder mehrere Warnungen aktiv sind,"Wählen Sie jede Warnung aus" und befolgen Sie die empfohlenen Maßnahmen.

Wenn ein Knoten vom Netz getrennt wird, liegt möglicherweise eine Warnung vor, es wird jedoch nur das Symbol „Nicht verbunden“ angezeigt. Um die aktiven Warnungen für einen Knoten anzuzeigen, wählen Sie den Knoten aus.

Warnsymbole

Wenn für einen Knoten eine aktive Warnung vorliegt, wird neben dem Knotennamen eines der folgenden Symbole angezeigt:

Kritisch: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort angehen. Wenn das Problem nicht behoben wird, kann es zu Dienstunterbrechungen und Datenverlust kommen.

Schwerwiegend: Es liegt ein anormaler Zustand vor, der entweder den aktuellen Betrieb beeinträchtigt

oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten wichtige Warnungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder -Dienstes nicht stoppt.

⚠ **Geringfügig**: Das System funktioniert normal, es liegt jedoch ein anormaler Zustand vor, der die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn er anhält. Sie sollten kleinere Warnungen, die nicht von selbst verschwinden, überwachen und beheben, um sicherzustellen, dass sie nicht zu einem ernsteren Problem führen.

Details zu einem System, einer Site oder einem Knoten anzeigen

Um die in der Knotentabelle angezeigten Informationen zu filtern, geben Sie eine Suchzeichenfolge in das Feld **Suchen** ein. Sie können nach Systemnamen, Anzeigenamen oder Typ suchen (geben Sie beispielsweise **gat** ein, um schnell alle Gateway-Knoten zu finden).

So zeigen Sie die Informationen für das Raster, die Site oder den Knoten an:

- Wählen Sie den Rasternamen aus, um eine aggregierte Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen.
- Wählen Sie einen bestimmten Rechenzentrumsstandort aus, um eine aggregierte Zusammenfassung der Statistiken für alle Knoten an diesem Standort anzuzeigen.
- Wählen Sie einen bestimmten Knoten aus, um detaillierte Informationen zu diesem Knoten anzuzeigen.

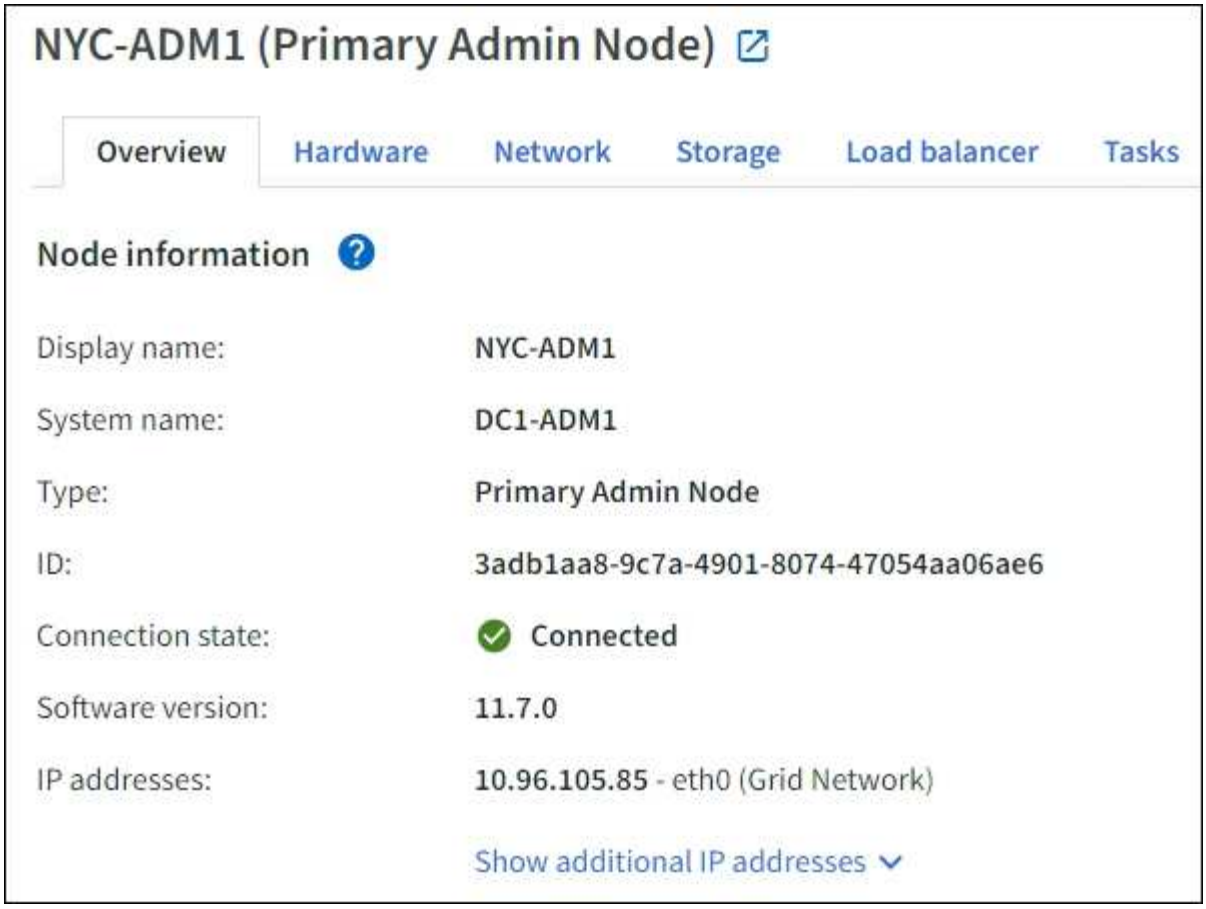
Anzeigen der Registerkarte „Übersicht“

Die Registerkarte „Übersicht“ bietet grundlegende Informationen zu jedem Knoten. Es werden auch alle Warnungen angezeigt, die derzeit den Knoten betreffen.

Die Registerkarte „Übersicht“ wird für alle Knoten angezeigt.

Knoteninformationen

Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden grundlegende Informationen zum Knoten aufgeführt.



Die Übersichtsinformationen für einen Knoten umfassen Folgendes:

- **Anzeigename** (wird nur angezeigt, wenn der Knoten umbenannt wurde): Der aktuelle Anzeigename für den Knoten. Verwenden Sie die"Raster, Sites und Knoten umbenennen" Verfahren zum Aktualisieren dieses Werts.
- **Systemname**: Der Name, den Sie während der Installation für den Knoten eingegeben haben. Systemnamen werden für interne StorageGRID -Vorgänge verwendet und können nicht geändert werden.
- **Typ**: Der Knotentyp – Admin-Knoten, primärer Admin-Knoten, Speicherknoten oder Gateway-Knoten.
- **ID**: Die eindeutige Kennung für den Knoten, die auch als UUID bezeichnet wird.
- **Verbindungsstatus**: Einer von drei Zuständen. Das Symbol für den schwerwiegendsten Zustand wird angezeigt.
  - **Unbekannt*** **: Aus einem unbekannten Grund ist der Knoten nicht mit dem Netz verbunden oder ein oder mehrere Dienste sind unerwartet ausgefallen. Beispielsweise ist die Netzwerkverbindung zwischen Knoten verloren gegangen, der Strom ist ausgefallen oder ein Dienst ist ausgefallen. Möglicherweise wird auch die Warnung *Kommunikation mit Knoten nicht möglich** ausgelöst. Möglicherweise sind auch andere Warnungen aktiv. Diese Situation erfordert sofortige Aufmerksamkeit.

    Bei verwalteten Herunterfahrvorgängen kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen können Sie den Status „Unbekannt“ ignorieren.

  - *Administrativ ausgefallen* : Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß

heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Möglicherweise sind auch eine oder mehrere Warnungen aktiv.

    - *Verbunden* : Der Knoten ist mit dem Netz verbunden.

- **Verwendeter Speicher**: Nur für Speicherknoten.
    - **Objektdaten**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der auf dem Speicherknoten verwendet wurde.
    - **Objektmetadaten**: Der Prozentsatz des insgesamt zulässigen Speicherplatzes für Objektmetadaten, der auf dem Speicherknoten verwendet wurde.
- **Softwareversion**: Die Version von StorageGRID , die auf dem Knoten installiert ist.
- **HA-Gruppen**: Nur für Admin-Knoten und Gateway-Knoten. Wird angezeigt, wenn eine Netzwerkschnittstelle auf dem Knoten in einer Hochverfügbarkeitsgruppe enthalten ist und ob diese Schnittstelle die primäre Schnittstelle ist.
- **IP-Adressen**: Die IP-Adressen des Knotens. Klicken Sie auf **Zusätzliche IP-Adressen anzeigen**, um die IPv4- und IPv6-Adressen und Schnittstellenzuordnungen des Knotens anzuzeigen.

Warnungen

Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle"Warnungen, die diesen Knoten derzeit betreffen und nicht stummgeschaltet wurden" . Wählen Sie den Warnungsnamen aus, um weitere Details und empfohlene Maßnahmen anzuzeigen.

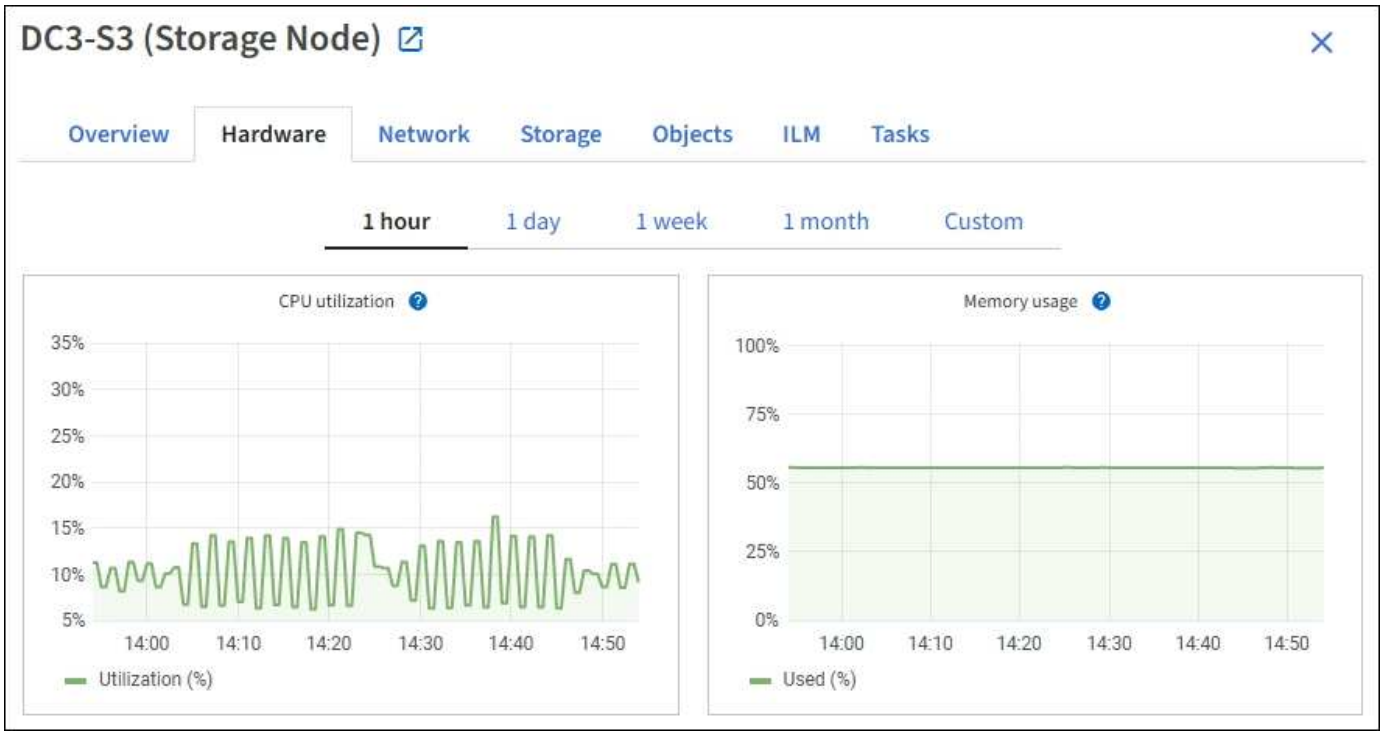
Benachrichtigungen sind auch enthalten für"Knotenverbindungszustände" .

Registerkarte „Hardware“ anzeigen

Auf der Registerkarte „Hardware“ werden die CPU-Auslastung und die Speichernutzung für jeden Knoten sowie zusätzliche Hardwareinformationen zu den Geräten angezeigt.

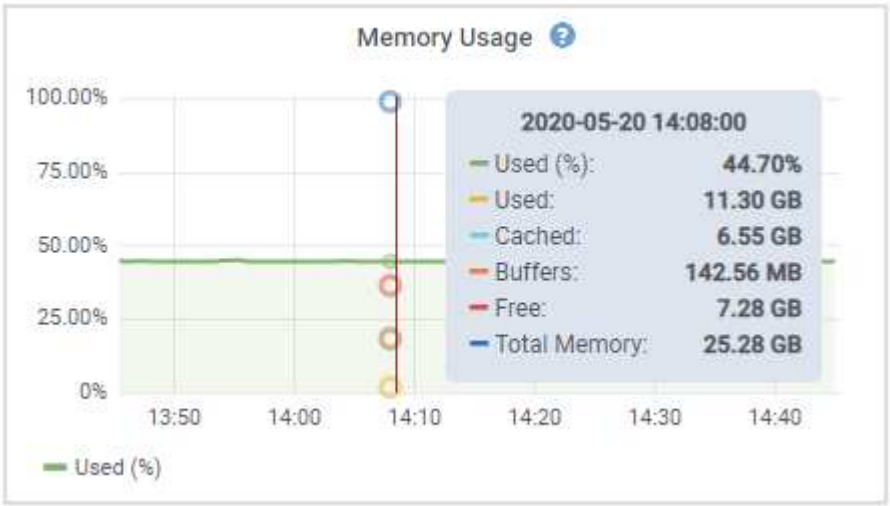
> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

Die Registerkarte „Hardware“ wird für alle Knoten angezeigt.



Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.

Um Details zur CPU-Auslastung und Speichernutzung anzuzeigen, positionieren Sie den Cursor über jedem Diagramm.



Wenn es sich bei dem Knoten um einen Appliance-Knoten handelt, enthält diese Registerkarte auch einen Abschnitt mit weiteren Informationen zur Appliance-Hardware.

Informationen zu Appliance-Speicherknoten anzeigen

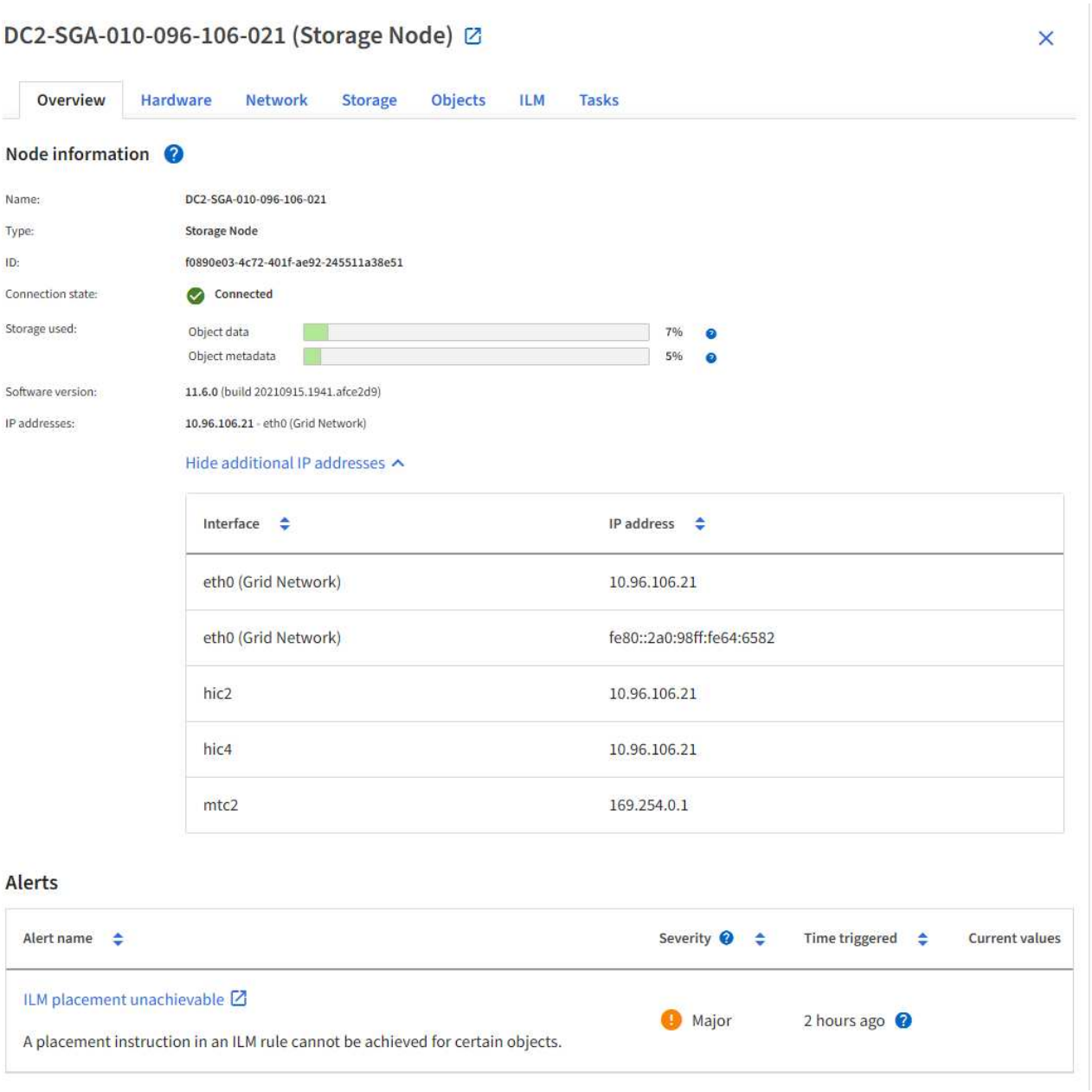
Auf der Seite „Knoten“ werden Informationen zum Dienstzustand und zu allen Rechen-, Festplatten- und Netzwerkressourcen für jeden Appliance-Speicherknoten aufgelistet. Sie können auch Speicher, Speicherhardware, Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen sowie Empfangs- und Sendedaten sehen.

Schritte

1. Wählen Sie auf der Seite „Knoten“ einen Appliance-Speicherknoten aus.
2. Wählen Sie **Übersicht**.

   Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden zusammenfassende Informationen zum Knoten angezeigt, z. B. Name, Typ, ID und Verbindungsstatus des Knotens. Die Liste der IP-Adressen enthält den Namen der Schnittstelle für jede Adresse wie folgt:

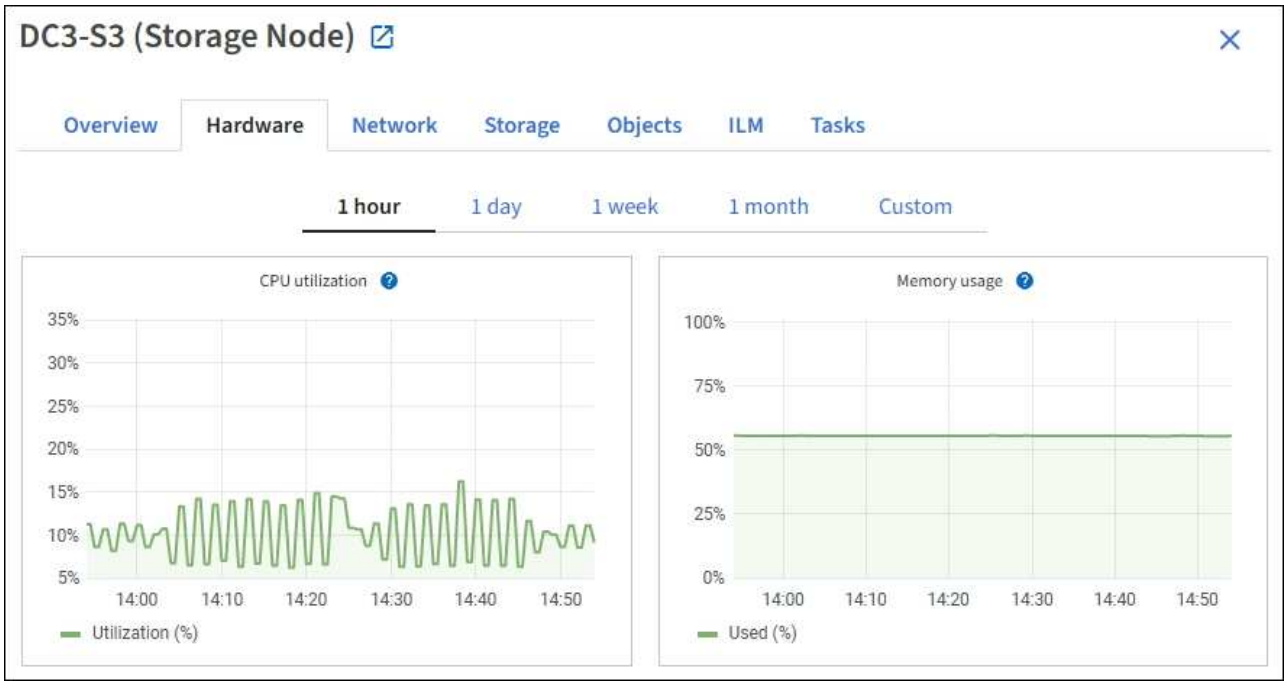
   - **eth**: Das Grid-Netzwerk, Admin-Netzwerk oder Client-Netzwerk.
   - **hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID Grid Network (eth0) und Client Network (eth2) verbunden werden.
   - **mtc**: Einer der physischen 1-GbE-Ports auf dem Gerät. Eine oder mehrere MTC-Schnittstellen werden verbunden, um die StorageGRID Admin Network-Schnittstelle (eth1) zu bilden. Sie können andere MTC-Schnittstellen für die temporäre lokale Konnektivität für einen Techniker im Rechenzentrum verfügbar lassen.



Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle aktiven Warnungen für den Knoten angezeigt.

3. Wählen Sie **Hardware** aus, um weitere Informationen zum Gerät anzuzeigen.

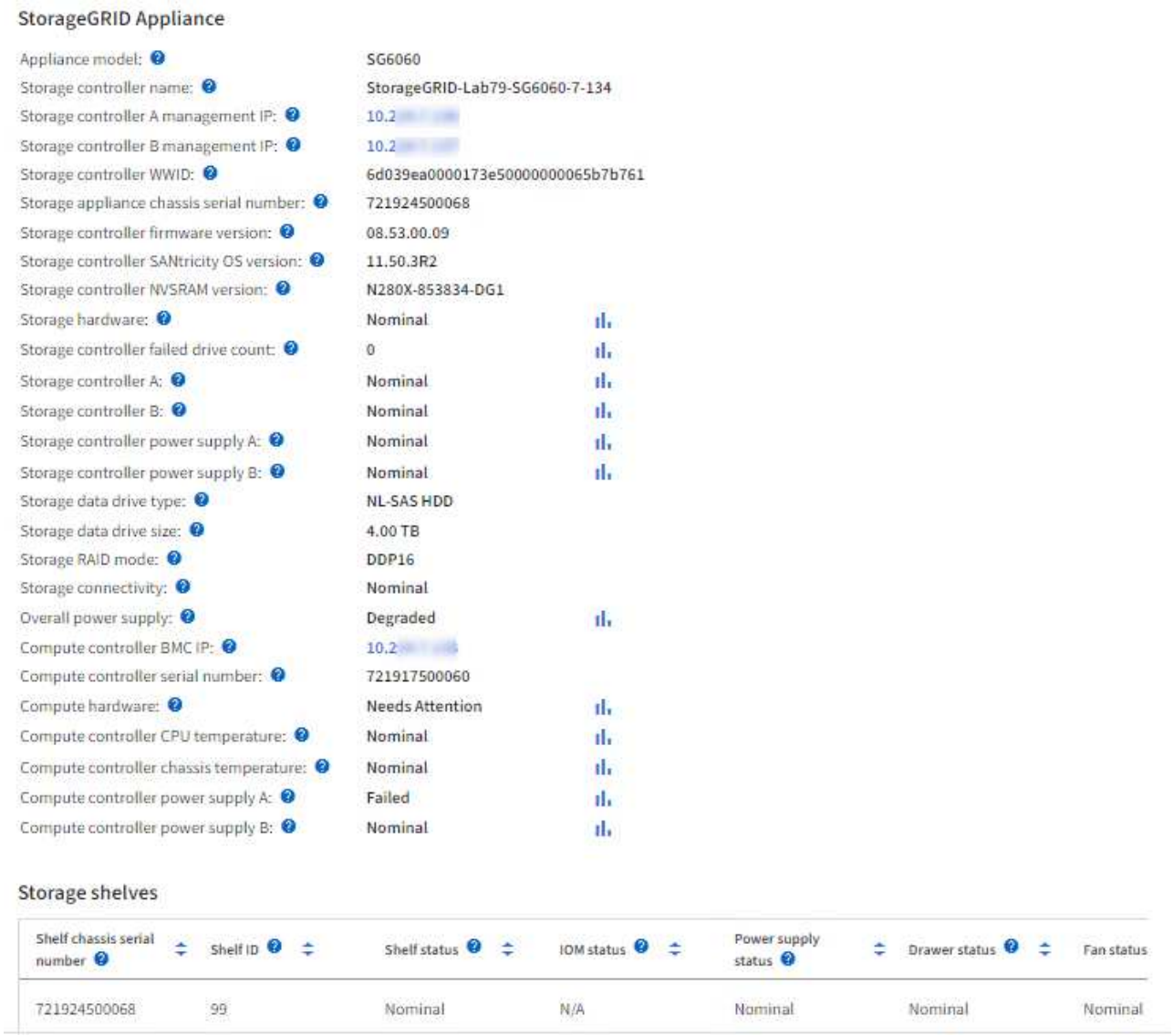
   a. Zeigen Sie die Diagramme zur CPU-Auslastung und zum Speicher an, um die Prozentsätze der CPU- und Speicherauslastung im Zeitverlauf zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.



b. Scrollen Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen wie den Modellnamen des Geräts, Controllernamen, Seriennummern und IP-Adressen sowie den Status jeder Komponente.

> Einige Felder, wie z. B. „Compute Controller BMC IP“ und „Compute Hardware“, werden nur für Geräte mit dieser Funktion angezeigt.

Komponenten für die Lagerregale und Erweiterungsregale, sofern diese Teil der Installation sind, werden in einer separaten Tabelle unterhalb der Gerätetabelle angezeigt.



Feld in der Appliance-Tabelle	Beschreibung
Gerätemodell	Die Modellnummer für dieses StorageGRID Gerät wird im SANtricity -Betriebssystem angezeigt.
Name des Speichercontrollers	Der Name für dieses StorageGRID Gerät wird im SANtricity -Betriebssystem angezeigt.
Speichercontroller A Verwaltungs-IP	IP-Adresse für Verwaltungsport 1 auf Speichercontroller A. Sie verwenden diese IP, um auf SANtricity OS zuzugreifen und Speicherprobleme zu beheben.
Verwaltungs-IP des Speichercontrollers B	IP-Adresse für Verwaltungsport 1 auf Speichercontroller B. Sie verwenden diese IP, um auf SANtricity OS zuzugreifen und Speicherprobleme zu beheben. Einige Gerätemodelle verfügen nicht über einen Speichercontroller B.

Feld in der Appliance-Tabelle	Beschreibung
WWID des Speichercontrollers	Die weltweite Kennung des Speichercontrollers, die im SANtricity -Betriebssystem angezeigt wird.
Seriennummer des Speichergerätgehäuses	Die Gehäuseseriennummer des Geräts.
Firmware-Version des Speichercontrollers	Die Version der Firmware auf dem Speichercontroller für dieses Gerät.
Speichercontroller SANtricity OS-Version	Die SANtricity OS-Version des Speichercontrollers A.
NVSRAM-Version des Speichercontrollers	NVSRAM-Version des Speichercontrollers, wie vom SANtricity System Manager gemeldet. Wenn beim SG6060 und SG6160 eine Nichtübereinstimmung der NVSRAM-Versionen zwischen den beiden Controllern vorliegt, wird die Version von Controller A angezeigt. Wenn Controller A nicht installiert oder betriebsbereit ist, wird die Version von Controller B angezeigt.
Speicherhardware	Der Gesamtstatus der Speichercontroller-Hardware. Wenn SANtricity System Manager den Status „Benötigt Aufmerksamkeit“ für die Speicherhardware meldet, meldet das StorageGRID -System ebenfalls diesen Wert. Wenn der Status „Benötigt Aufmerksamkeit“ lautet, überprüfen Sie zuerst den Speichercontroller mit SANtricity OS. Stellen Sie dann sicher, dass keine anderen Warnungen vorhanden sind, die für den Compute Controller gelten.
Anzahl der Laufwerksfehler des Speichercontrollers	Die Anzahl der Laufwerke, die nicht optimal sind.
Speichercontroller A	Der Status des Speichercontrollers A.
Speichercontroller B	Der Status des Speichercontrollers B. Einige Appliance-Modelle verfügen nicht über einen Speichercontroller B.
Speichercontroller-Netzteil A	Der Status des Netzteils A für den Speichercontroller.
Speichercontroller-Netzteil B	Der Status der Stromversorgung B für den Speichercontroller.
Speicherdatenlaufwerkstyp	Der Laufwerkstyp im Gerät, z. B. HDD (Festplatte) oder SSD (Solid-State-Laufwerk).

Feld in der Appliance-Tabelle	Beschreibung
Größe des Speicherdatenlaufwerks	Die effektive Größe eines Datenlaufwerks. Beim SG6160 wird auch die Größe des Cache-Laufwerks angezeigt. **Hinweis**: Für Knoten mit Erweiterungs-Shelfs verwenden Sie dieDatenlaufwerksgröße für jedes Regal stattdessen. Die effektive Laufwerksgröße kann je nach Regal unterschiedlich sein.
Speicher-RAID-Modus	Der für das Gerät konfigurierte RAID-Modus.
Speicherkonnektivität	Der Speicherkonnektivitätsstatus.
Gesamtstromversorgung	Der Status aller Stromversorgungen für das Gerät.
BMC -IP des Rechencontrollers	Die IP-Adresse des Baseboard Management Controller (BMC)-Ports im Compute Controller. Sie verwenden diese IP, um eine Verbindung zur BMC Schnittstelle herzustellen und die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird für Appliance-Modelle ohne BMC nicht angezeigt.
Seriennummer des Compute-Controllers	Die Seriennummer des Compute-Controllers.
Computerhardware	Der Status der Compute-Controller-Hardware. Dieses Feld wird für Appliance-Modelle ohne separate Rechen- und Speicherhardware nicht angezeigt.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute Controllers.
Gehäusetemperatur des Compute-Controllers	Der Temperaturstatus des Compute-Controllers.

+

Spalte in der Tabelle „Lagerregale“	Beschreibung
Seriennummer des Regalgehäuses	Die Seriennummer für das Lagerregalgehäuse.

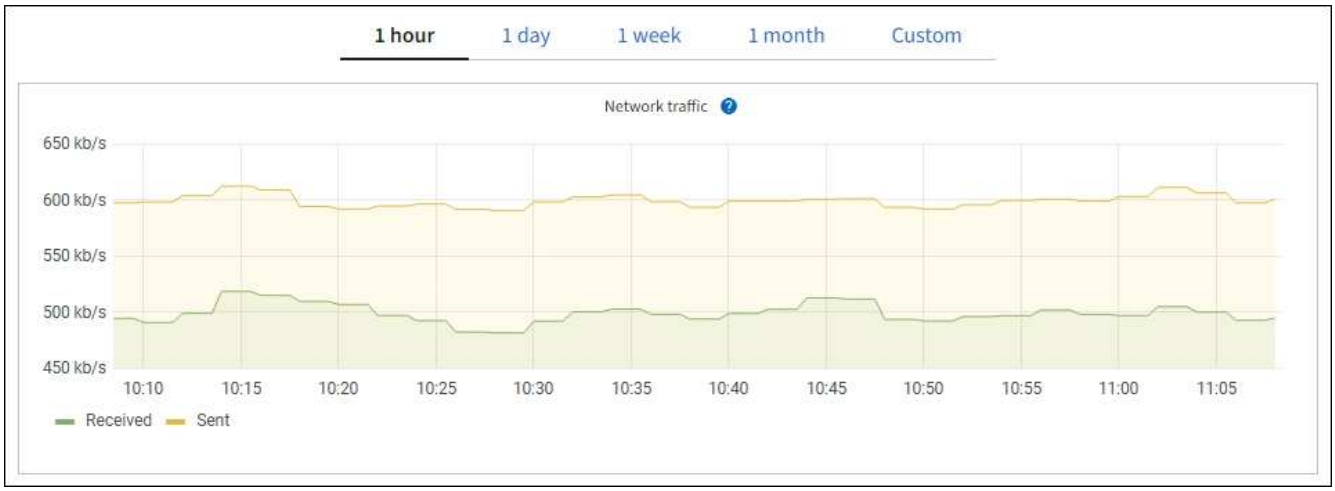
Spalte in der Tabelle „Lagerregale“	Beschreibung
Regal-ID	Die numerische Kennung für das Lagerregal. • 99: Speichercontroller-Regal • 0: Erstes Erweiterungsregal • 1: Zweites Erweiterungsregal **Hinweis:** Erweiterungsregale gelten nur für SG6060 und SG6160.
Regalstatus	Der Gesamtstatus des Lagerregals.
IOM-Status	Der Status der Eingabe-/Ausgabemodule (IOMs) in allen Erweiterungsregalen. N/A, wenn es sich nicht um ein Erweiterungsregal handelt.
Stromversorgungsstatus	Der Gesamtstatus der Stromversorgungen für das Speicherregal.
Schubladenstatus	Der Status der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Kühllüfter im Lagerregal.
Laufwerkssteckplätze	Die Gesamtzahl der Laufwerkssteckplätze im Speicherregal.
Datenlaufwerke	Die Anzahl der Laufwerke im Speicherregal, die zur Datenspeicherung verwendet werden.
Größe des Datenlaufwerks	Die effektive Größe eines Datenlaufwerks im Speicherregal.
Cache-Laufwerke	Die Anzahl der Laufwerke im Speicherregal, die als Cache verwendet werden.
Cache-Laufwerksgröße	Die Größe des kleinsten Cache-Laufwerks im Speicherregal. Normalerweise haben alle Cache-Laufwerke die gleiche Größe.
Konfigurationsstatus	Der Konfigurationsstatus des Speicherregals.

a. Bestätigen Sie, dass alle Status „Nominal“ sind.

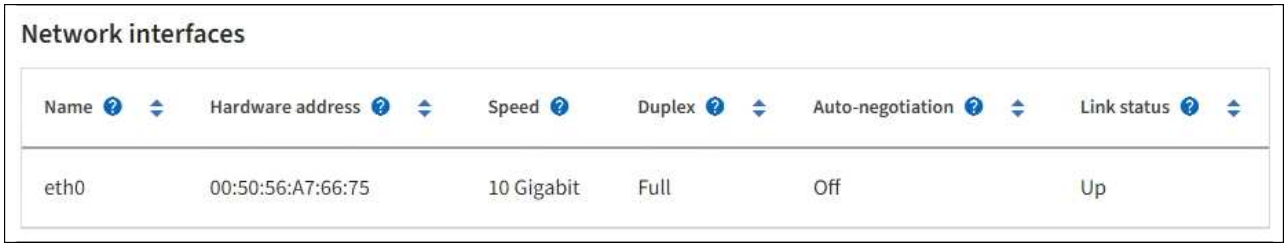
   Wenn ein Status nicht „Nominal“ ist, überprüfen Sie alle aktuellen Warnungen. Sie können auch SANtricity System Manager verwenden, um mehr über einige dieser Hardwarewerte zu erfahren. Lesen Sie die Anweisungen zur Installation und Wartung Ihres Geräts.

4. Wählen Sie **Netzwerk**, um Informationen zu jedem Netzwerk anzuzeigen.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs.



a. Lesen Sie den Abschnitt „Netzwerkschnittstellen“.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle „Netzwerkschnittstellen“, um zu bestimmen, ob die 10/25-GbE-Netzwerkports auf der Appliance für die Verwendung des Aktiv-/Sicherungsmodus oder des LACP-Modus konfiguriert wurden.

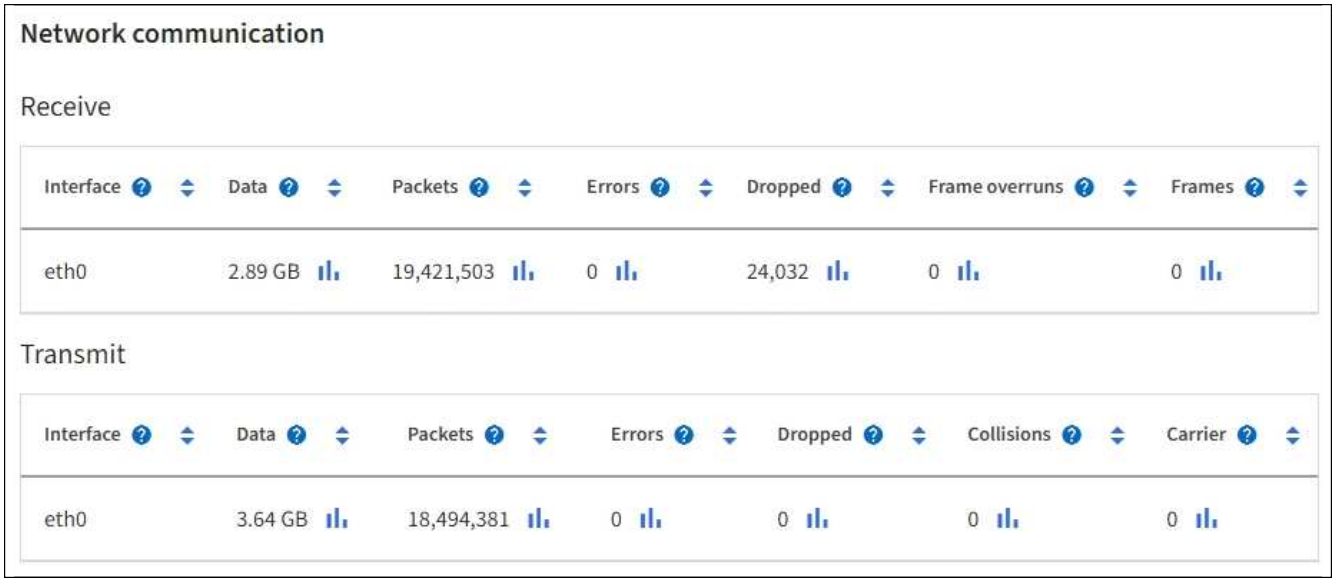
Bei den in der Tabelle angezeigten Werten wird davon ausgegangen, dass alle vier Links verwendet werden.

Link-Modus	Bond-Modus	Individuelle HIC-Verbindungsgeschwindigkeit (hic1, hic2, hic3, hic4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0,eth2)
Aggregat	LACP	25	100
Behoben	LACP	25	50
Behoben	Aktiv/Backup	25	25
Aggregat	LACP	10	40
Behoben	LACP	10	20
Behoben	Aktiv/Backup	10	10

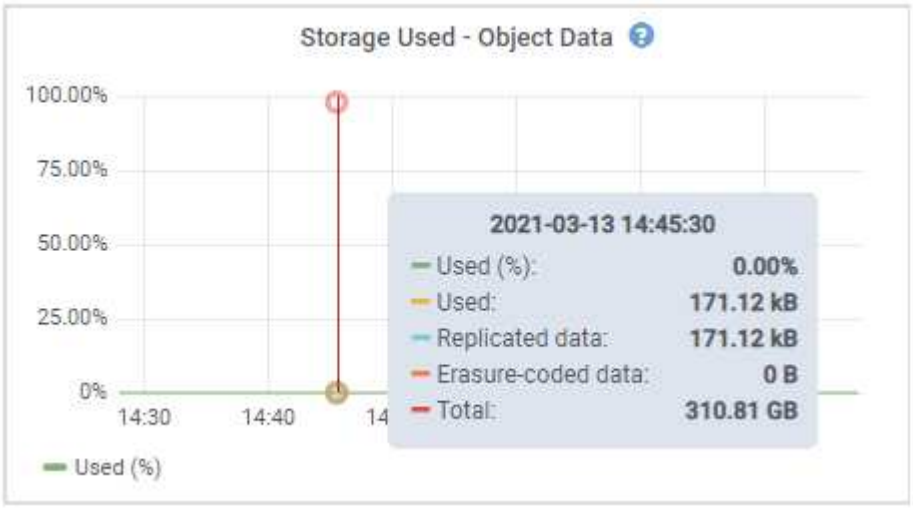
Sehen "Konfigurieren von Netzwerkverbindungen" Weitere Informationen zum Konfigurieren der 10/25-GbE-Ports.

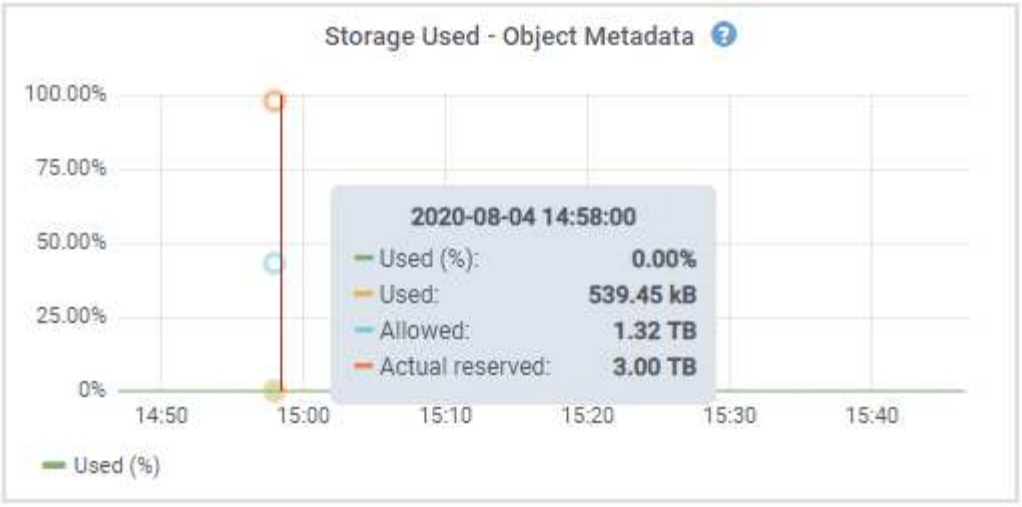
b. Lesen Sie den Abschnitt „Netzwerkkommunikation“.

   Die Empfangs- und Sendetabellen zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie weitere Empfangs- und Sendemetriken.



5. Wählen Sie **Speicher** aus, um Diagramme anzuzeigen, die den Prozentsatz des im Zeitverlauf für Objektdaten und Objektmetadaten verwendeten Speichers sowie Informationen zu Festplattengeräten, Volumes und Objektspeichern zeigen.

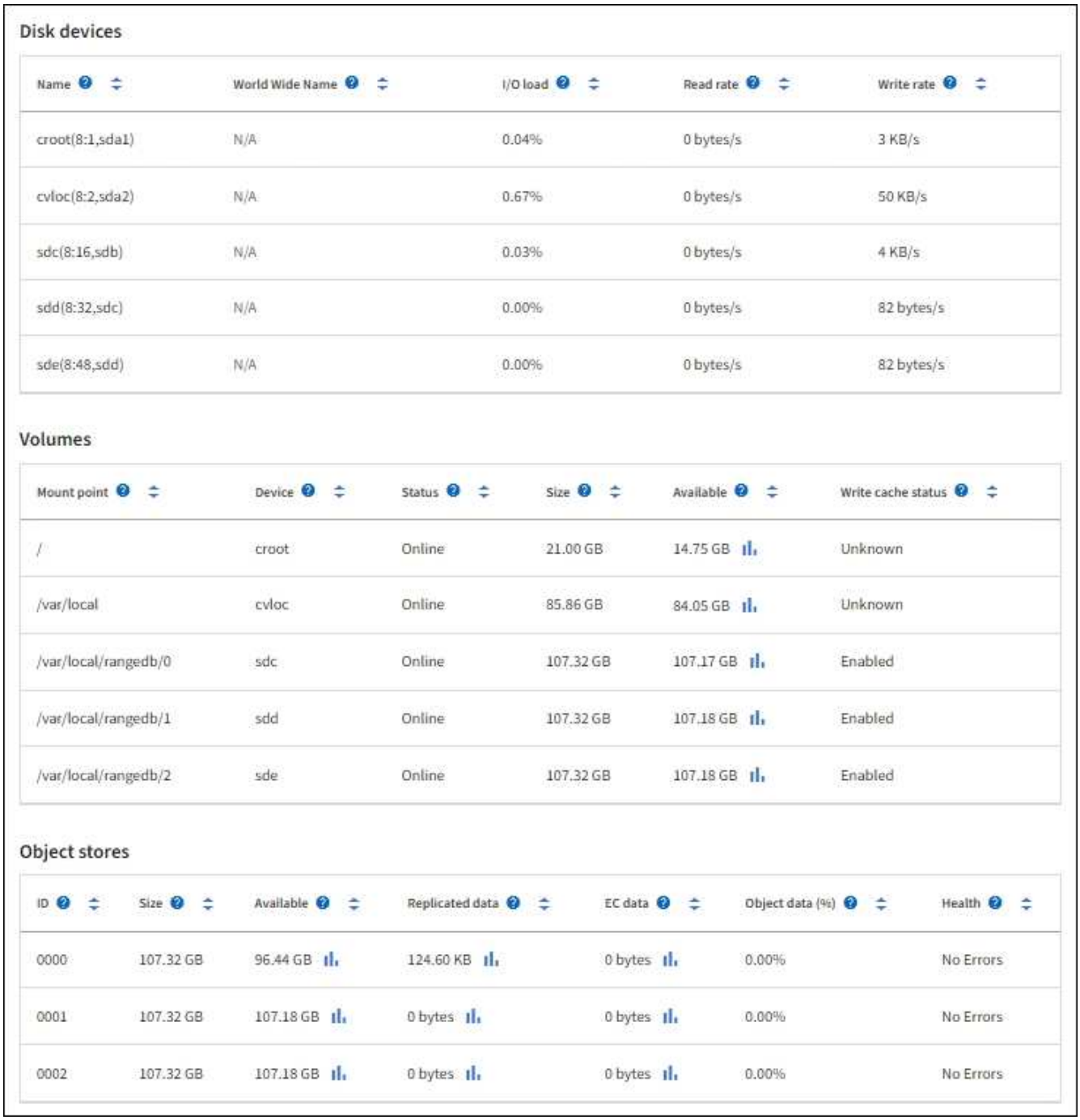




a. Scrollen Sie nach unten, um die Menge des verfügbaren Speichers für jedes Volume und jeden Objektspeicher anzuzeigen.

   Der weltweite Name für jede Festplatte entspricht der weltweiten Volume-Kennung (WWID), die angezeigt wird, wenn Sie die Standard-Volume-Eigenschaften in SANtricity OS anzeigen (der Verwaltungssoftware, die mit dem Speichercontroller des Geräts verbunden ist).

   Um Ihnen die Interpretation der Lese- und Schreibstatistiken für die Datenträger in Bezug auf Volume-Mount-Punkte zu erleichtern, entspricht der erste Teil des in der Spalte **Name** der Tabelle „Datenträgergeräte“ angezeigten Namens (also *sdc*, *sdd*, *sde* usw.) dem in der Spalte **Gerät** der Tabelle „Volumes“ angezeigten Wert.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	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

Informationen zu Appliance-Admin-Knoten und Gateway-Knoten anzeigen

Auf der Seite „Knoten“ werden Informationen zum Dienstzustand und zu allen Rechen-, Festplatten- und Netzwerkressourcen für jede Dienst-Appliance aufgelistet, die als Admin-Knoten oder Gateway-Knoten verwendet wird. Sie können auch Speicher, Speicherhardware, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen sowie Empfangs- und Sendedaten sehen.

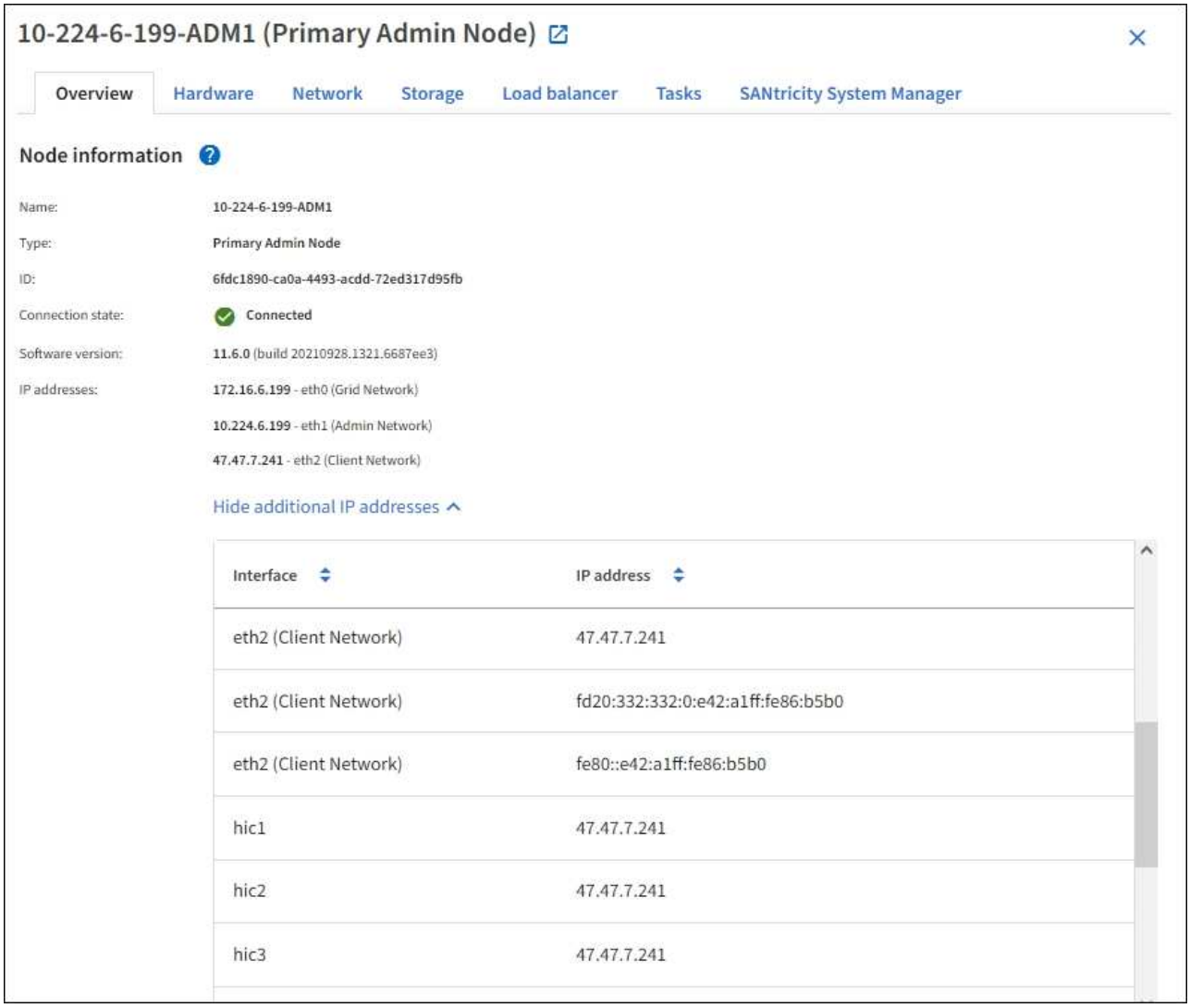
Schritte

1. Wählen Sie auf der Seite „Knoten“ einen Appliance-Admin-Knoten oder einen Appliance-Gateway-Knoten aus.
2. Wählen Sie **Übersicht**.

   Im Abschnitt „Knoteninformationen“ der Registerkarte „Übersicht“ werden zusammenfassende

Informationen zum Knoten angezeigt, z. B. Name, Typ, ID und Verbindungsstatus des Knotens. Die Liste der IP-Adressen enthält den Namen der Schnittstelle für jede Adresse wie folgt:

- **adllb** und **adlli**: Wird angezeigt, wenn Active/Backup-Bonding für die Admin-Netzwerkschnittstelle verwendet wird
- **eth**: Das Grid-Netzwerk, Admin-Netzwerk oder Client-Netzwerk.
- **hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID Grid Network (eth0) und Client Network (eth2) verbunden werden.
- **mtc**: Einer der physischen 1-GbE-Ports auf dem Gerät. Eine oder mehrere MTC-Schnittstellen werden zur Admin-Netzwerkschnittstelle (eth1) verbunden. Sie können andere MTC-Schnittstellen für die temporäre lokale Konnektivität für einen Techniker im Rechenzentrum verfügbar lassen.

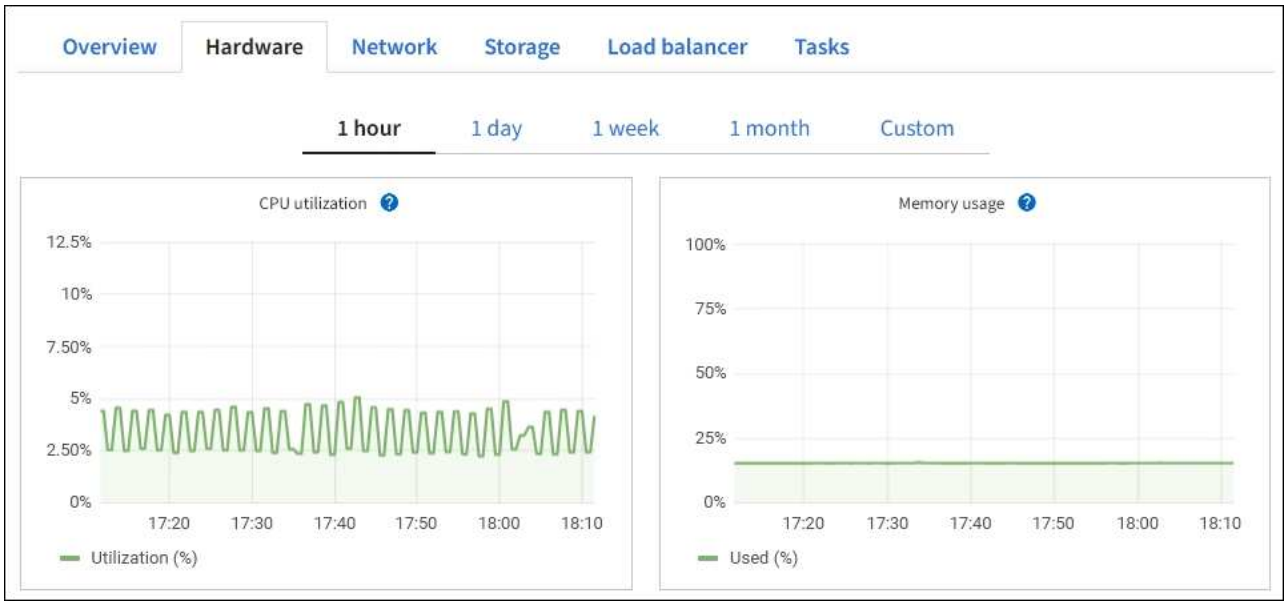


Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle aktiven Warnungen für den Knoten angezeigt.

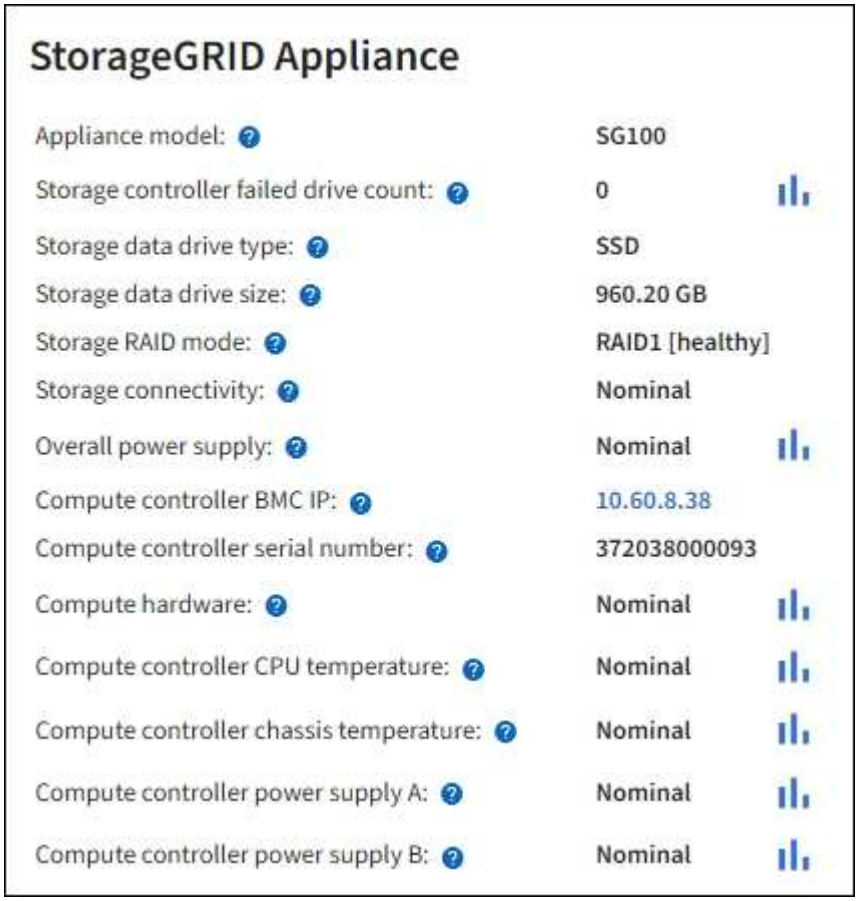
3. Wählen Sie **Hardware** aus, um weitere Informationen zum Gerät anzuzeigen.

   a. Zeigen Sie die Diagramme zur CPU-Auslastung und zum Speicher an, um die Prozentsätze der CPU- und Speicherauslastung im Zeitverlauf zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren

Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.



b. Scrollen Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen wie den Modellnamen, die Seriennummer, die Firmware-Version des Controllers und den Status jeder Komponente.



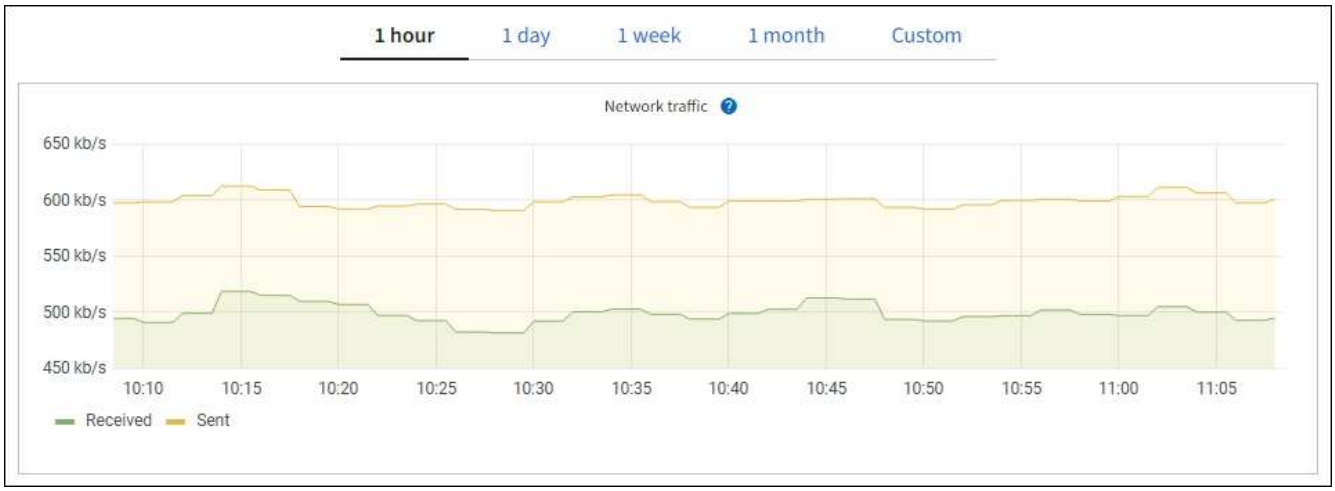
Feld in der Appliance-Tabelle	Beschreibung
Gerätemodell	Die Modellnummer für dieses StorageGRID Gerät.
Anzahl der Laufwerksfehler des Speichercontrollers	Die Anzahl der Laufwerke, die nicht optimal sind.
Speicherdatenlaufwerkstyp	Der Laufwerkstyp im Gerät, z. B. HDD (Festplatte) oder SSD (Solid-State-Laufwerk).
Größe des Speicherdatenlaufwerks	Die effektive Größe eines Datenlaufwerks.
Speicher-RAID-Modus	Der RAID-Modus für das Gerät.
Gesamtstromversorgung	Der Status aller Netzteile im Gerät.
BMC -IP des Rechencontrollers	Die IP-Adresse des Baseboard Management Controller (BMC)-Ports im Compute Controller. Sie können diese IP verwenden, um eine Verbindung zur BMC Schnittstelle herzustellen und die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird für Appliance-Modelle ohne BMC nicht angezeigt.
Seriennummer des Compute-Controllers	Die Seriennummer des Compute-Controllers.
Computerhardware	Der Status der Compute-Controller-Hardware.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute Controllers.
Gehäusetemperatur des Compute-Controllers	Der Temperaturstatus des Compute-Controllers.

a. Bestätigen Sie, dass alle Status „Nominal“ sind.

   Wenn ein Status nicht „Nominal“ ist, überprüfen Sie alle aktuellen Warnungen.

4. Wählen Sie **Netzwerk**, um Informationen zu jedem Netzwerk anzuzeigen.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs.



a. Lesen Sie den Abschnitt „Netzwerkschnittstellen“.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

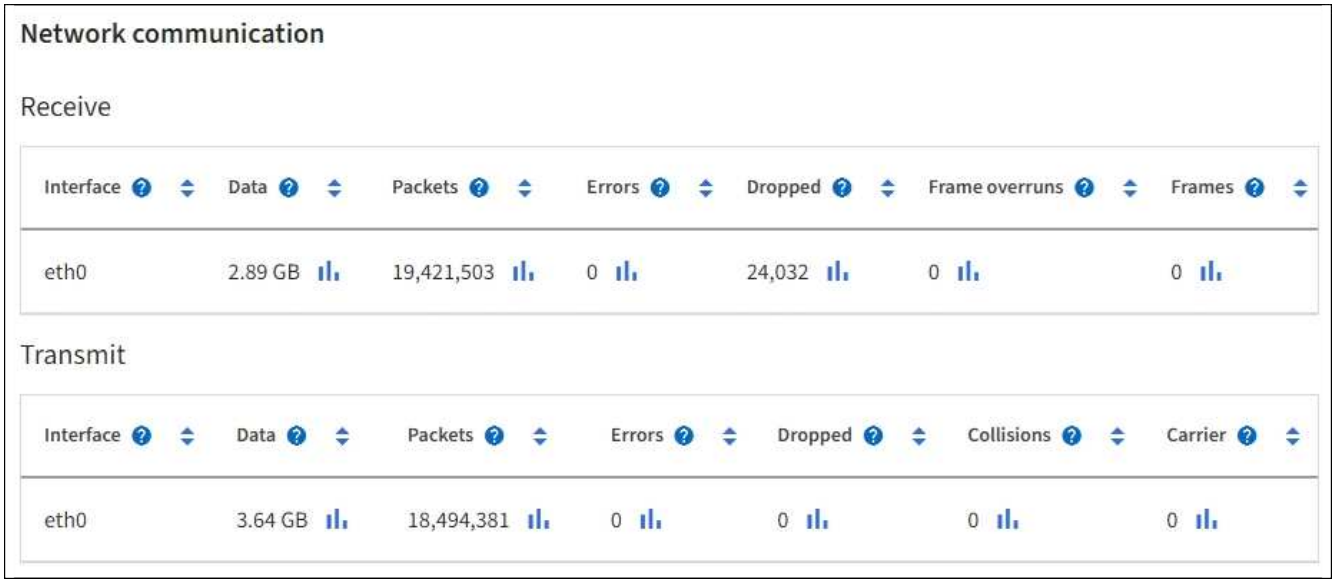
Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle „Netzwerkschnittstellen“, um zu bestimmen, ob die vier 40/100-GbE-Netzwerkports auf der Appliance für die Verwendung des Aktiv-/Sicherungsmodus oder des LACP-Modus konfiguriert wurden.

Bei den in der Tabelle angezeigten Werten wird davon ausgegangen, dass alle vier Links verwendet werden.

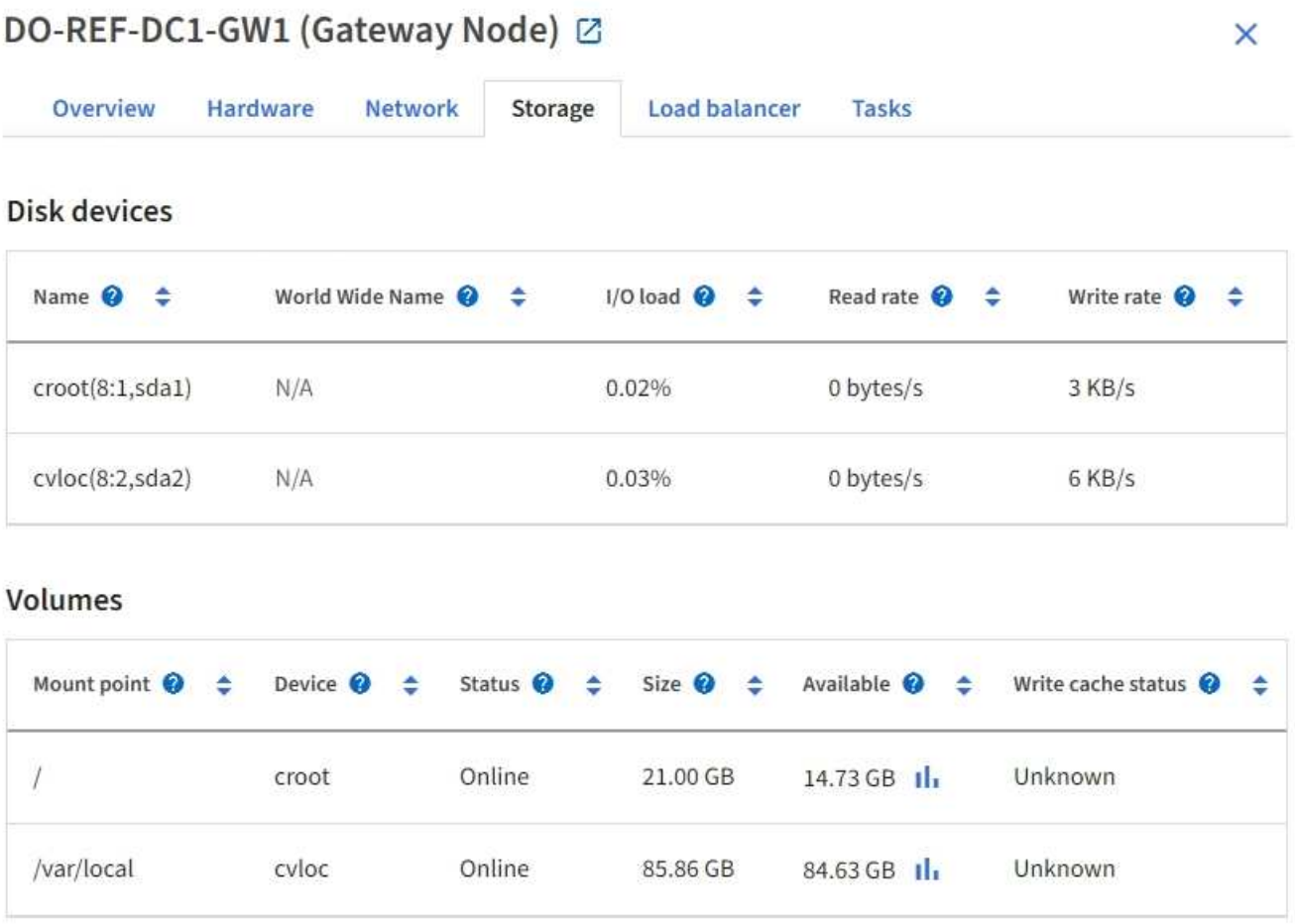
Link-Modus	Bond-Modus	Individuelle HIC-Verbindungsgeschwindigkeit (hic1, hic2, hic3, hic4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0, eth2)
Aggregat	LACP	100	400
Behoben	LACP	100	200
Behoben	Aktiv/Backup	100	100
Aggregat	LACP	40	160
Behoben	LACP	40	80
Behoben	Aktiv/Backup	40	40

b. Lesen Sie den Abschnitt „Netzwerkkommunikation“.

Die Empfangs- und Sendetabellen zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Sendemetriken.



5. Wählen Sie **Speicher** aus, um Informationen zu den Festplattengeräten und Volumes auf der Service-Appliance anzuzeigen.



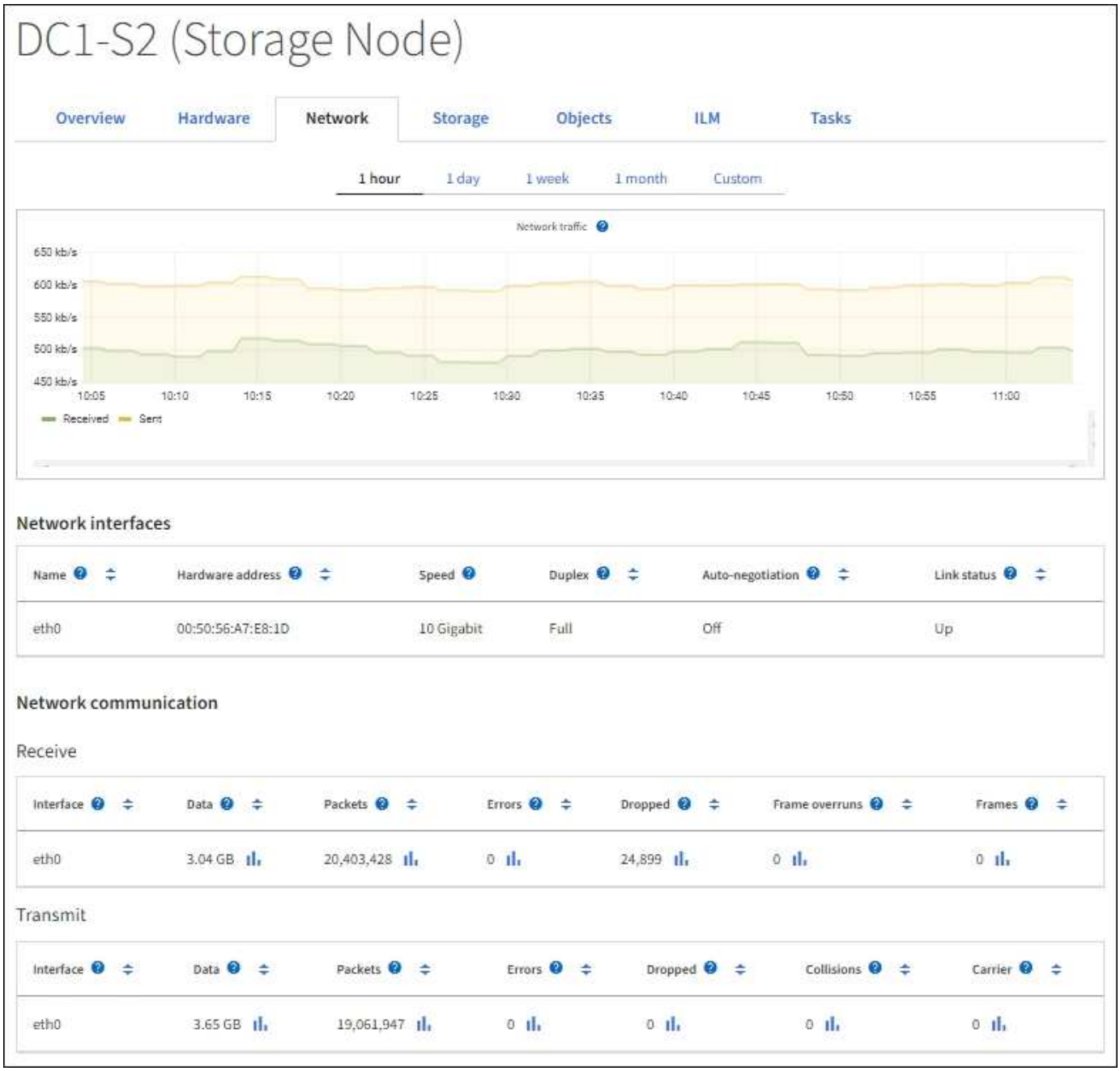
Anzeigen der Registerkarte „Netzwerk“

Auf der Registerkarte „Netzwerk“ wird ein Diagramm angezeigt, das den über alle Netzwerkschnittstellen auf dem Knoten, der Site oder dem Grid empfangenen und gesendeten Netzwerkverkehr darstellt.

Die Registerkarte „Netzwerk“ wird für alle Knoten, jeden Standort und das gesamte Raster angezeigt.

Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.

Für Knoten enthält die Tabelle „Netzwerkschnittstellen“ Informationen zu den physischen Netzwerkports jedes Knotens. Die Netzwerkkommunikationstabelle enthält Einzelheiten zu den Empfangs- und Sendevorgängen jedes Knotens und zu allen vom Treiber gemeldeten Fehlerzählern.



Ähnliche Informationen

"Überwachen Sie Netzwerkverbindungen und Leistung"

Registerkarte „Speicher“ anzeigen

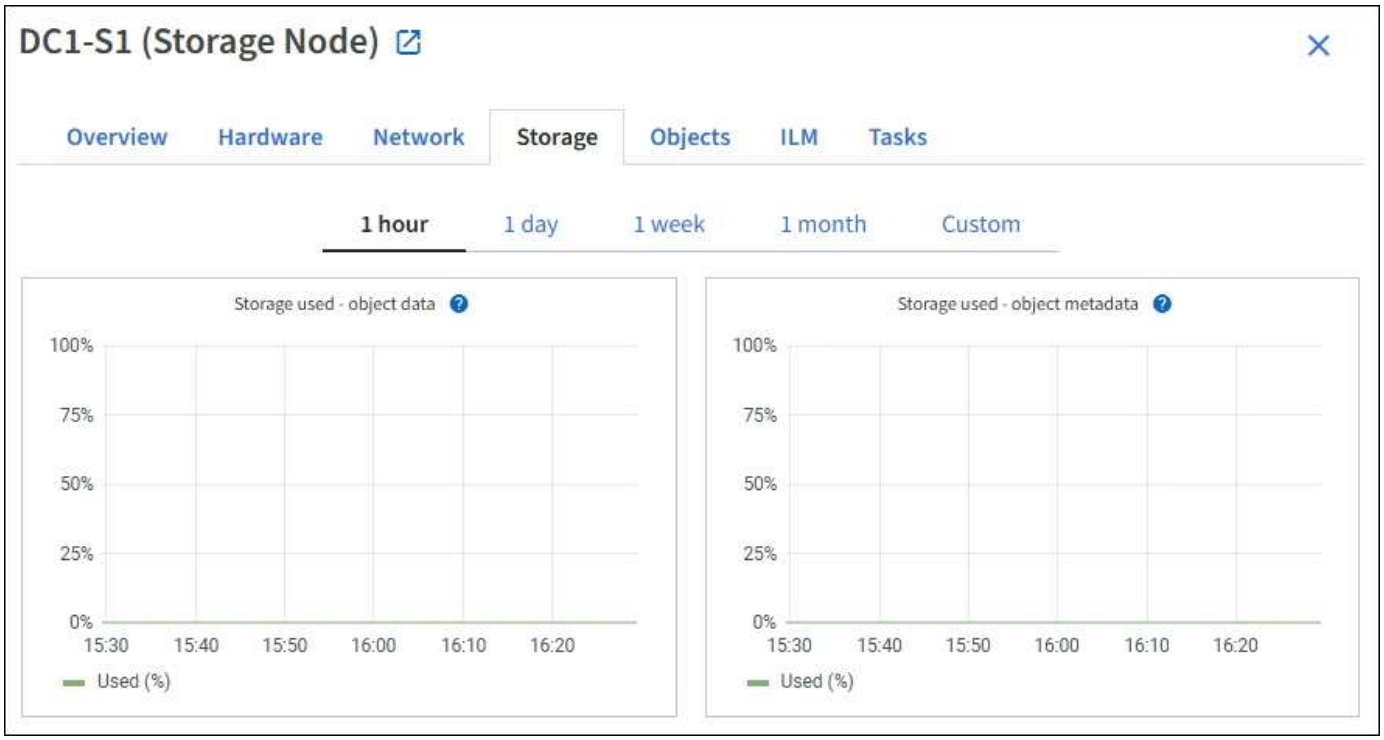
Auf der Registerkarte „Speicher“ werden die Speicherverfügbarkeit und andere Speichermetriken zusammengefasst.

Die Registerkarte „Speicher“ wird für alle Knoten, jeden Standort und das gesamte Raster angezeigt.

Diagramme zum verwendeten Speicher

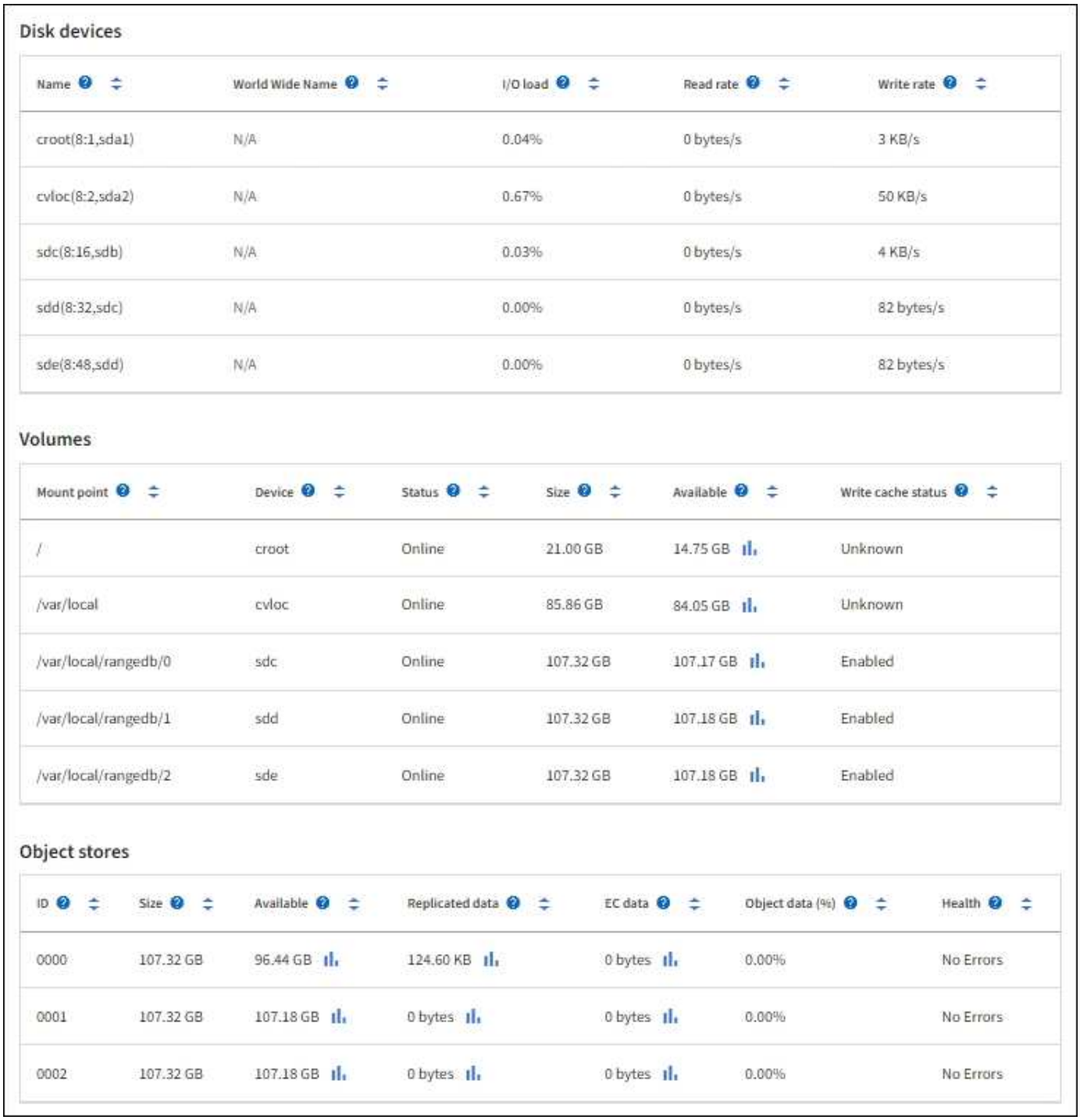
Für Speicherknoten, jeden Standort und das gesamte Raster enthält die Registerkarte „Speicher“ Diagramme, die zeigen, wie viel Speicher im Laufe der Zeit von Objektdaten und Objektmetadaten verwendet wurde.

Wenn ein Knoten nicht mit dem Grid verbunden ist, beispielsweise während eines Upgrades oder in einem getrennten Zustand, sind bestimmte Metriken möglicherweise nicht verfügbar oder aus den Site- und Grid-Gesamtwerten ausgeschlossen. Nachdem ein Knoten die Verbindung zum Netz wiederhergestellt hat, warten Sie einige Minuten, bis sich die Werte stabilisiert haben.



Tabellen für Festplattengeräte, Volumes und Objektspeicher

Für alle Knoten enthält die Registerkarte „Speicher“ Details zu den Festplattengeräten und Volumes auf dem Knoten. Für Speicherknoten enthält die Objektspeichertabelle Informationen zu jedem Speichervolumen.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	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

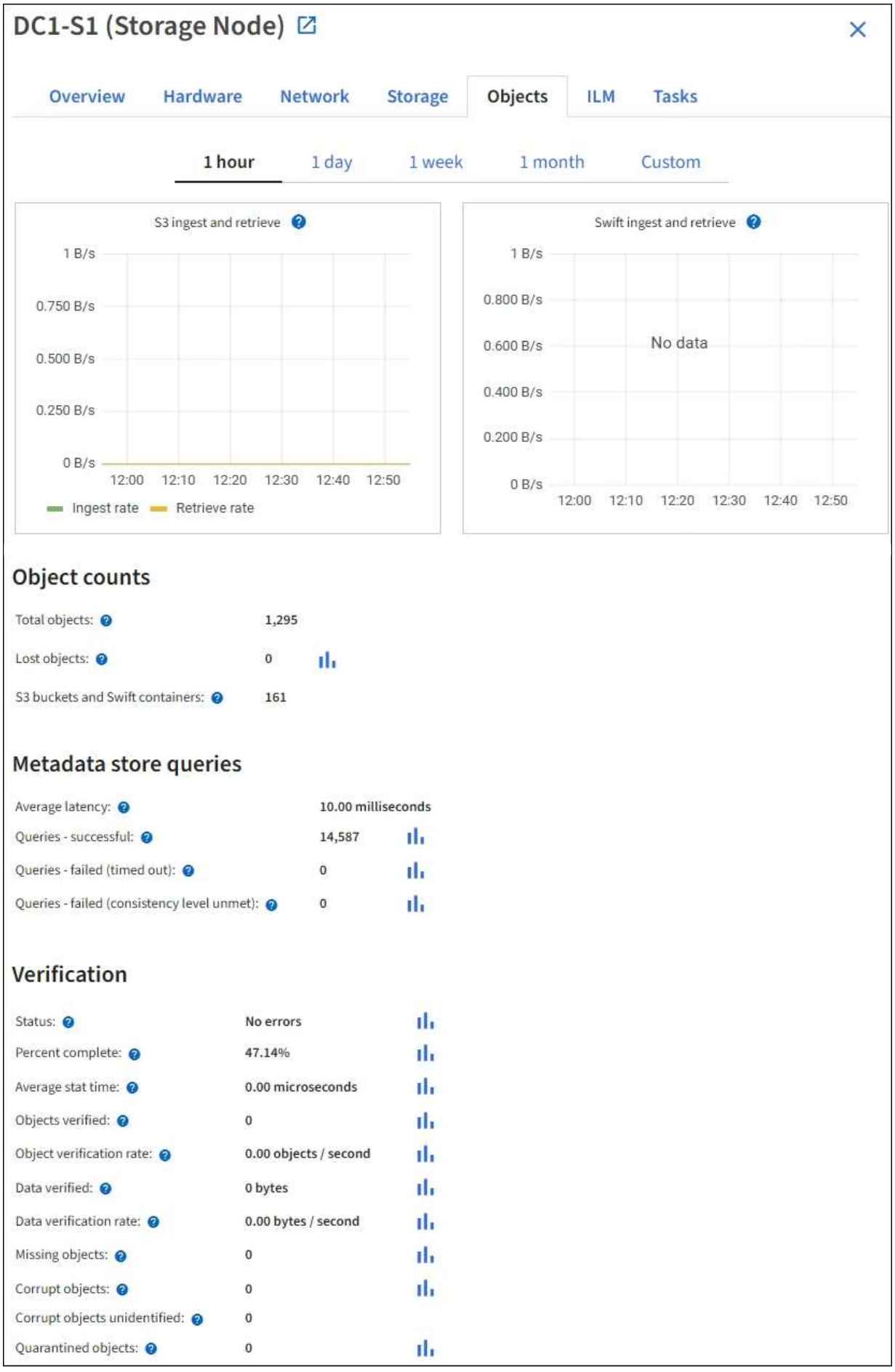
Ähnliche Informationen

"Überwachen der Speicherkapazität"

Anzeigen der Registerkarte „Objekte“

Die Registerkarte Objekte bietet Informationen über"S3-Aufnahme- und Abrufraten" .

Die Registerkarte „Objekte“ wird für jeden Speicherknoten, jede Site und das gesamte Raster angezeigt. Für Speicherknoten bietet die Registerkarte „Objekte“ auch Objektanzahlen und Informationen zu Metadatenabfragen und Hintergrundüberprüfungen.

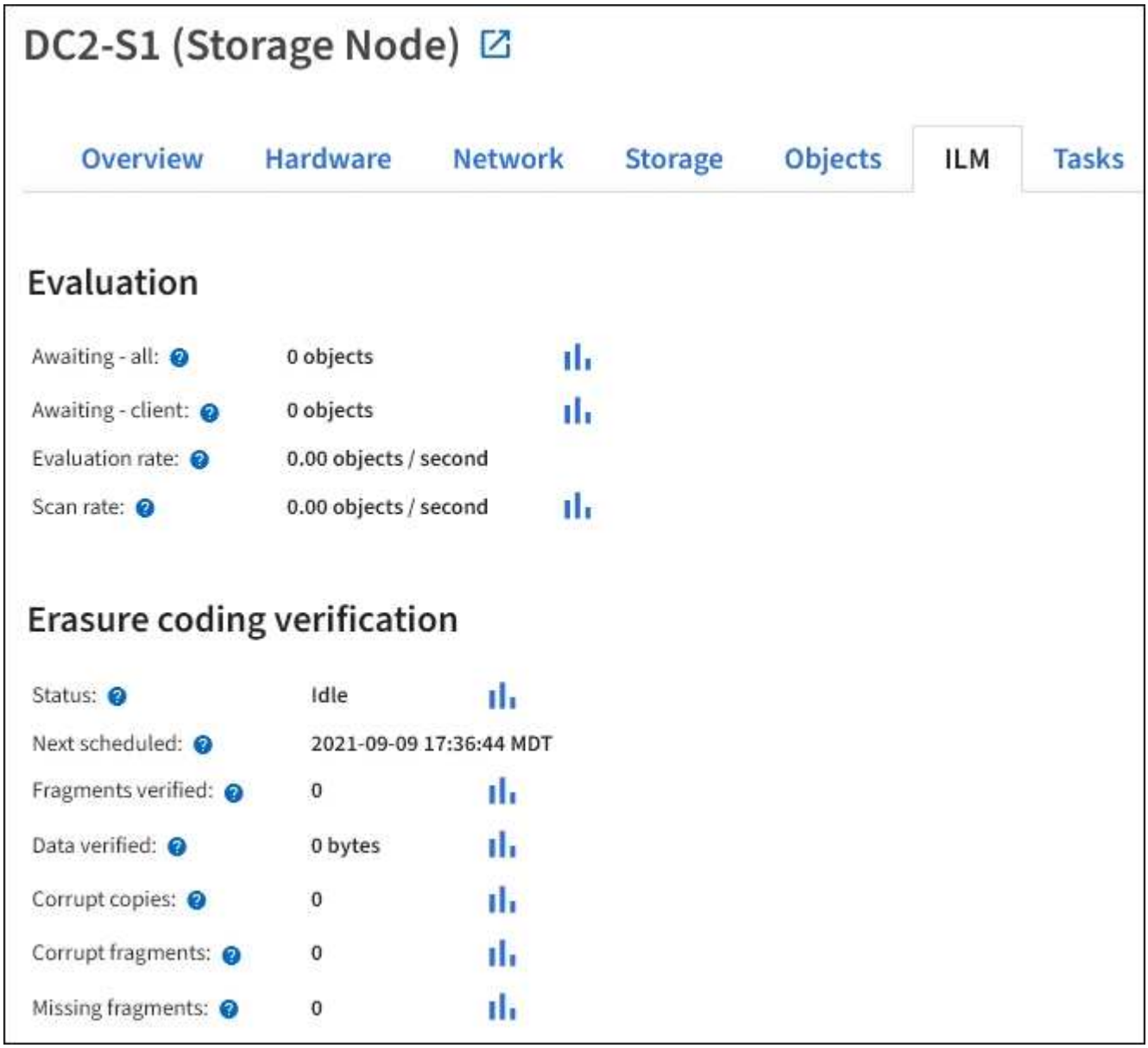

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

Anzeigen der Registerkarte „ILM“

Die Registerkarte „ILM“ bietet Informationen zu Vorgängen im Zusammenhang mit dem Information Lifecycle Management (ILM).

Die ILM-Registerkarte wird für jeden Speicherknoten, jeden Standort und das gesamte Raster angezeigt. Für jeden Standort und jedes Raster wird auf der Registerkarte „ILM“ ein Diagramm der ILM-Warteschlange im Zeitverlauf angezeigt. Für das Raster wird auf dieser Registerkarte auch die geschätzte Zeit angegeben, die zum Abschließen eines vollständigen ILM-Scans aller Objekte benötigt wird.

Für Speicherknoten bietet die Registerkarte „ILM“ Details zur ILM-Auswertung und Hintergrundüberprüfung für Erasure-Codierte Objekte.



Ähnliche Informationen

- "Überwachen Sie das Informationslebenszyklusmanagement"
- "StorageGRID verwalten"

Verwenden Sie die Registerkarte Aufgaben

Die Registerkarte „Aufgaben“ wird für alle Knoten angezeigt. Sie können diese Registerkarte verwenden, um einen Knoten umzubenennen oder neu zu starten oder um einen Appliance-Knoten in den Wartungsmodus zu versetzen.

Die vollständigen Anforderungen und Anweisungen für jede Option auf dieser Registerkarte finden Sie hier:

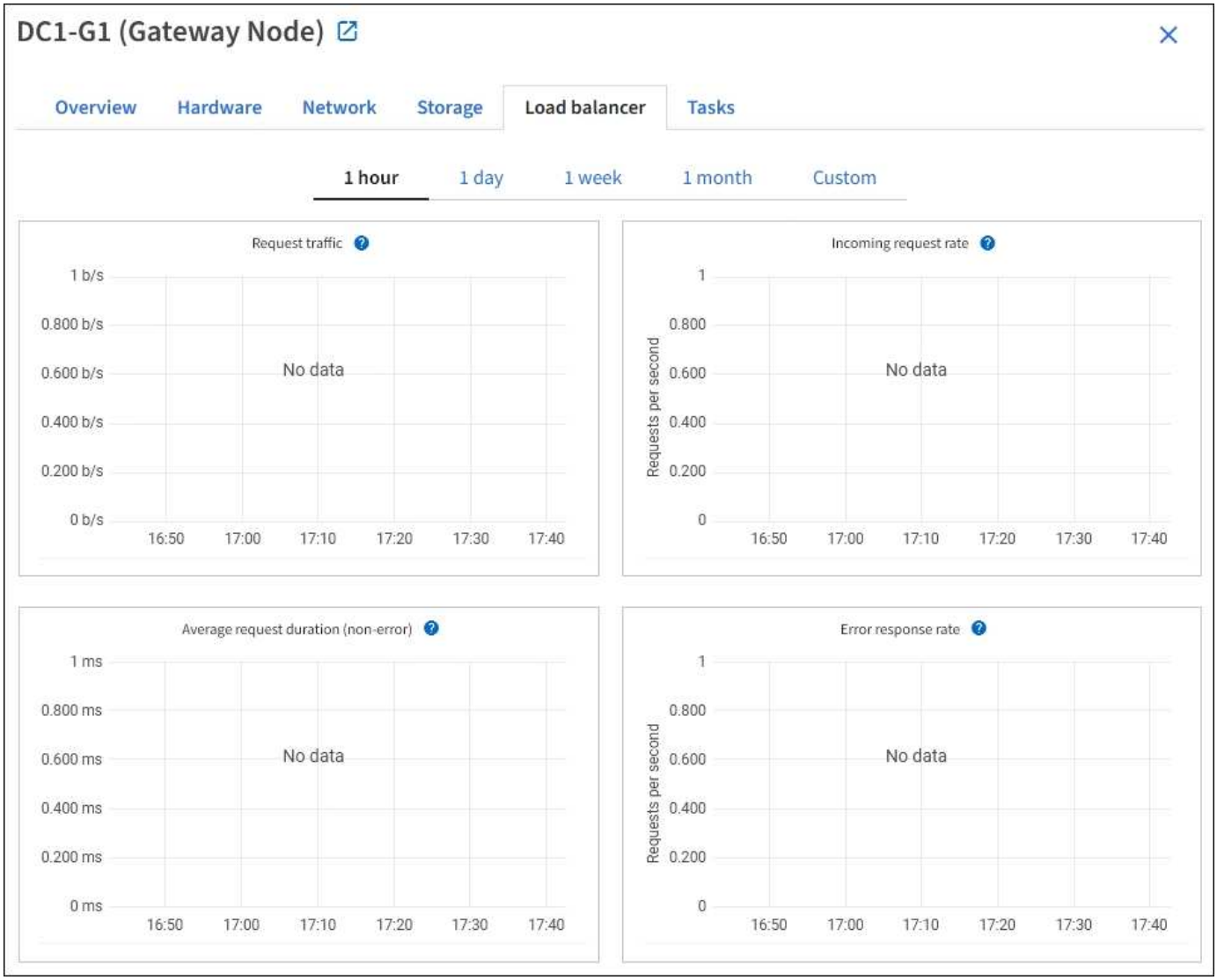
- "Raster, Sites und Knoten umbenennen"
- "Grid-Knoten neu starten"
- "Gerät in den Wartungsmodus versetzen"

Registerkarte „Load Balancer“ anzeigen

Die Registerkarte „Load Balancer“ enthält Leistungs- und Diagnosediagramme zum Betrieb des Load Balancer-Dienstes.

Die Registerkarte „Load Balancer“ wird für Admin-Knoten und Gateway-Knoten, jede Site und das gesamte Grid angezeigt. Für jeden Standort bietet die Registerkarte „Load Balancer“ eine aggregierte Zusammenfassung der Statistiken für alle Knoten an diesem Standort. Für das gesamte Raster bietet die Registerkarte „Load Balancer“ eine aggregierte Zusammenfassung der Statistiken für alle Sites.

Wenn über den Load Balancer-Dienst keine E/A ausgeführt wird oder kein Load Balancer konfiguriert ist, wird in den Diagrammen „Keine Daten“ angezeigt.



Verkehr anfordern

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt des Datendurchsatzes, der zwischen den Endpunkten des Lastenausgleichs und den Clients, die die Anfragen stellen, in Bits pro Sekunde übertragen wird.

> Dieser Wert wird nach Abschluss jeder Anfrage aktualisiert. Daher kann dieser Wert bei niedrigen Anforderungsraten oder sehr langlebigen Anforderungen vom Echtzeitdurchsatz abweichen. Sie können auf der Registerkarte „Netzwerk“ einen realistischeren Überblick über das aktuelle Netzwerkverhalten erhalten.

Rate eingehender Anfragen

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt der Anzahl neuer Anfragen pro Sekunde, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Dieser Wert wird aktualisiert, wenn die Header einer neuen Anfrage validiert wurden.

Durchschnittliche Anfragedauer (ohne Fehler)

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt der Anfragedauer, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Die Dauer jeder Anfrage beginnt, wenn ein Anfrageheader vom

Load Balancer-Dienst analysiert wird, und endet, wenn der vollständige Antworttext an den Client zurückgegeben wird.

Fehlerantwortrate

Dieses Diagramm bietet einen gleitenden 3-Minuten-Durchschnitt der Anzahl der pro Sekunde an Clients zurückgegebenen Fehlerantworten, aufgeschlüsselt nach Fehlerantwortcode.

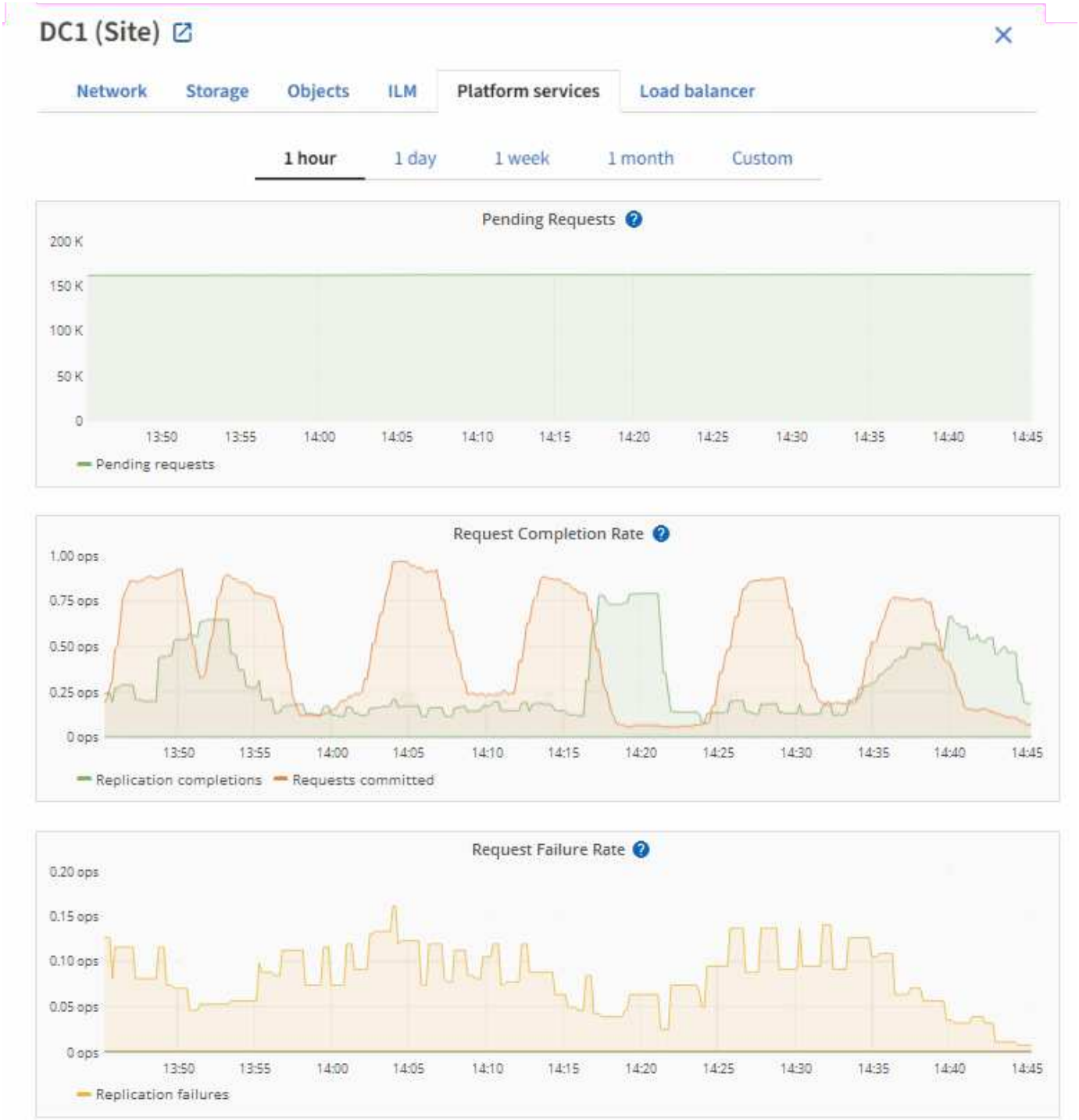
Ähnliche Informationen

- "Überwachen von Lastausgleichsvorgängen"
- "StorageGRID verwalten"

Registerkarte „Plattformdienste“ anzeigen

Die Registerkarte „Plattformdienste“ bietet Informationen zu allen S3-Plattformdienstvorgängen an einem Standort.

Die Registerkarte „Plattformdienste“ wird für jede Site angezeigt. Diese Registerkarte bietet Informationen zu S3-Plattformdiensten, wie z. B. CloudMirror-Replikation und Suchintegrationsdienst. Die Diagramme auf dieser Registerkarte zeigen Kennzahlen wie die Anzahl ausstehender Anfragen, die Anfrageabschlussrate und die Anfragefehlerrate an.



Weitere Informationen zu den S3-Plattformdiensten, einschließlich Details zur Fehlerbehebung, finden Sie im"Anweisungen zur Administration von StorageGRID" .

Anzeigen der Registerkarte „Laufwerke verwalten“

Über die Registerkarte „Laufwerke verwalten“ können Sie auf Details zugreifen und Fehlerbehebungs- und Wartungsaufgaben an Laufwerken in den Appliances durchführen, die diese Funktion unterstützen.

Über die Registerkarte „Laufwerke verwalten“ können Sie Folgendes tun:

- Anzeigen eines Layouts der Datenspeicherlaufwerke im Gerät
- Zeigen Sie eine Tabelle an, in der die einzelnen Laufwerksstandorte, Typen, Status, Firmware-Versionen und Seriennummern aufgeführt sind.
- Führen Sie an jedem Laufwerk Fehlerbehebungs- und Wartungsfunktionen durch

Um auf die Registerkarte Laufwerke verwalten zuzugreifen, müssen Sie über die"Speichergeräteadministrator oder Root-Zugriffsberechtigung" .

Informationen zur Verwendung der Registerkarte „Laufwerke verwalten“ finden Sie unter "Verwenden Sie die Registerkarte „Laufwerke verwalten“" .

Registerkarte „ SANtricity System Manager“ anzeigen (nur E-Serie)

Über die Registerkarte „SANtricity System Manager“ können Sie auf den SANtricity System Manager zugreifen, ohne den Verwaltungsport des Speichergeräts konfigurieren oder verbinden zu müssen. Auf dieser Registerkarte können Sie Hardwarediagnose- und Umgebungsinformationen sowie Probleme im Zusammenhang mit den Laufwerken überprüfen.

> Der Zugriff auf den SANtricity System Manager vom Grid Manager aus dient im Allgemeinen nur der Überwachung der Gerätehardware und der Konfiguration von E-Series AutoSupport. Viele Funktionen und Vorgänge im SANtricity System Manager, wie z. B. das Aktualisieren der Firmware, gelten nicht für die Überwachung Ihres StorageGRID Geräts. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Wartungsanweisungen für Ihr Gerät. Informationen zum Upgrade der SANtricity -Firmware finden Sie im "Wartungskonfigurationsverfahren" für Ihr Speichergerät.

> Die Registerkarte „SANtricity System Manager“ wird nur für Speichergeräteknoten angezeigt, die E-Series-Hardware verwenden.

Mit SANtricity System Manager können Sie Folgendes tun:

- Zeigen Sie Leistungsdaten wie Leistung auf Speicherarrayebene, E/A-Latenz, CPU-Auslastung des Speichercontrollers und Durchsatz an.
- Überprüfen Sie den Status der Hardwarekomponenten.
- Führen Sie Supportfunktionen aus, einschließlich der Anzeige von Diagnosedaten und der Konfiguration von E-Series AutoSupport.

> Informationen zur Verwendung von SANtricity System Manager zum Konfigurieren eines Proxys für E-Series AutoSupport finden Sie unter"Senden Sie E-Series AutoSupport -Pakete über StorageGRID" .

Um über Grid Manager auf SANtricity System Manager zuzugreifen, benötigen Sie die"Speichergeräteadministrator oder Root-Zugriffsberechtigung" .

> Sie müssen über die SANtricity -Firmware 8.70 oder höher verfügen, um über den Grid Manager auf den SANtricity System Manager zugreifen zu können.

Die Registerkarte zeigt die Homepage von SANtricity System Manager an.

Sie können den SANtricity System Manager-Link verwenden, um den SANtricity System Manager zur einfacheren Anzeige in einem neuen Browserfenster zu öffnen.

Um Details zur Leistung und Kapazitätsnutzung auf Speicher-Array-Ebene anzuzeigen, positionieren Sie den Cursor über jedem Diagramm.

Weitere Informationen zum Anzeigen der Informationen, die über die Registerkarte SANtricity System Manager zugänglich sind, finden Sie unter "Dokumentation zu NetApp E-Series und SANtricity" .

Regelmäßig zu überwachende Informationen

Was und wann zu überwachen ist

Auch wenn das StorageGRID -System weiterbetrieben werden kann, wenn Fehler auftreten oder Teile des Netzes nicht verfügbar sind, sollten Sie potenzielle Probleme überwachen und beheben, bevor sie die Effizienz oder Verfügbarkeit des Netzes beeinträchtigen.

Bevor Sie beginnen

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

Informationen zu Überwachungsaufgaben

Ein ausgelastetes System erzeugt große Mengen an Informationen. Die folgende Liste enthält Hinweise zu den wichtigsten Informationen, die kontinuierlich überwacht werden müssen.

Was zu überwachen ist	Frequenz
"Systemintegritätsstatus"	Täglich
Rate, mit der"Speicherknotenobjekt- und Metadatenkapazität" wird konsumiert	Wöchentlich
"Vorgänge zur Verwaltung des Informationslebenszyklus"	Wöchentlich
"Netzwerk- und Systemressourcen"	Wöchentlich
"Mieteraktivität"	Wöchentlich
"S3-Clientvorgänge"	Wöchentlich
"Lastausgleichsvorgänge"	Nach der Erstkonfiguration und nach allen Konfigurationsänderungen
"Grid-Föderation-Verbindungen"	Wöchentlich

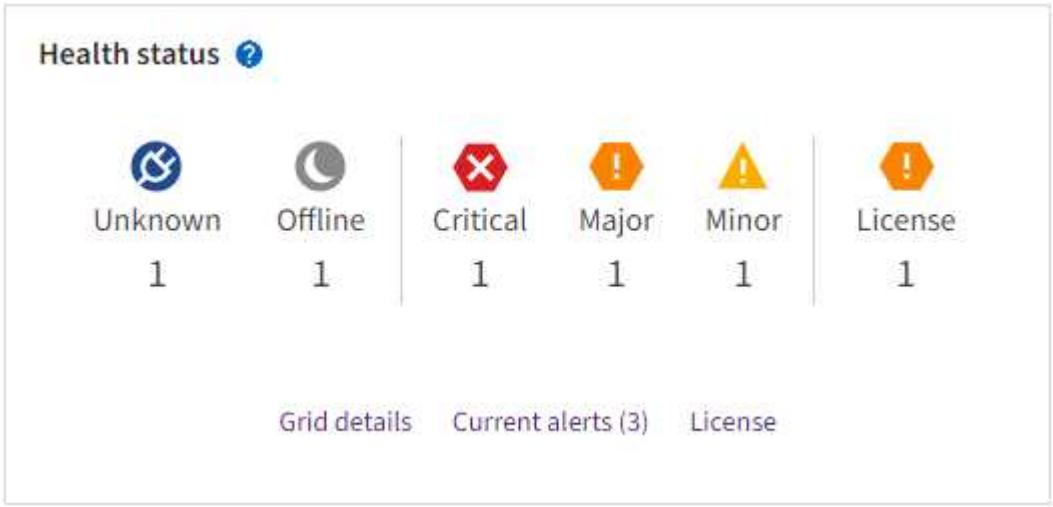
Überwachen Sie den Systemzustand

Überwachen Sie täglich den Gesamtzustand Ihres StorageGRID -Systems.

Informationen zu diesem Vorgang

Das StorageGRID -System kann weiterbetrieben werden, wenn Teile des Netzes nicht verfügbar sind. Bei den durch Warnungen angezeigten potenziellen Problemen handelt es sich nicht unbedingt um Probleme mit dem Systembetrieb. Untersuchen Sie die auf der Integritätsstatuskarte des Grid Manager-Dashboards zusammengefassten Probleme.

Um über Alarme informiert zu werden, sobald diese ausgelöst werden, können Sie "E-Mail-Benachrichtigungen für Warnungen einrichten" oder"SNMP-Traps konfigurieren" .



Wenn Probleme vorliegen, werden Links angezeigt, über die Sie weitere Details anzeigen können:

Link	Erscheint, wenn…
Rasterdetails	Alle Knoten sind getrennt (Verbindungsstatus „Unbekannt“ oder „Administrativ deaktiviert“).
Aktuelle Warnungen (Kritisch, Schwerwiegend, Geringfügig)	Warnungen sindderzeit aktiv .
Kürzlich gelöste Warnungen	In der letzten Woche ausgelöste Warnungensind nun gelöst .
Lizenz	Es gibt ein Problem mit der Softwarelizenz für dieses StorageGRID -System. Sie können "Aktualisieren Sie die Lizenzinformationen nach Bedarf" .

Überwachen Sie den Verbindungsstatus des Knotens

Wenn ein oder mehrere Knoten vom Netz getrennt werden, können kritische StorageGRID Vorgänge beeinträchtigt werden. Überwachen Sie den Verbindungsstatus der Knoten und beheben Sie etwaige Probleme umgehend.

Symbol	Beschreibung	Handlungsbedarf
	**Nicht verbunden – Unbekannt** Aus einem unbekannten Grund wird die Verbindung zu einem Knoten getrennt oder die Dienste auf dem Knoten fallen unerwartet aus. Beispielsweise könnte ein Dienst auf dem Knoten gestoppt worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Störung seine Netzwerkverbindung verloren haben. Möglicherweise wird auch die Warnung **Kommunikation mit Knoten nicht möglich** ausgelöst. Möglicherweise sind auch andere Warnungen aktiv.	Erfordert sofortige Aufmerksamkeit. Wählen Sie jede Warnung aus und befolgen Sie die empfohlenen Maßnahmen. Beispielsweise müssen Sie möglicherweise einen angehaltenen Dienst neu starten oder den Host für den Knoten neu starten. **Hinweis**: Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen können Sie den Status „Unbekannt“ ignorieren.
	**Nicht verbunden – Administrator-Ausfall** Aus einem erwarteten Grund ist der Knoten nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Möglicherweise sind auch eine oder mehrere Warnungen aktiv. Je nach zugrunde liegendem Problem gehen diese Knoten häufig ohne Eingriff wieder online.	Stellen Sie fest, ob dieser Knoten von Warnungen betroffen ist. Wenn eine oder mehrere Warnungen aktiv sind,Wählen Sie jeden Alarm aus und befolgen Sie die empfohlenen Maßnahmen.
	**Verbunden** Der Knoten ist mit dem Netz verbunden.	Keine Aktion erforderlich.

Aktuelle und gelöste Warnmeldungen anzeigen

Aktuelle Warnungen: Wenn eine Warnung ausgelöst wird, wird auf dem Dashboard ein Warnsymbol angezeigt. Auf der Seite „Knoten“ wird für den Knoten außerdem ein Warnsymbol angezeigt. Wenn"E-Mail-Benachrichtigungen sind konfiguriert" , wird auch eine E-Mail-Benachrichtigung gesendet, sofern der Alarm nicht stummgeschaltet wurde.

Behobene Warnungen: Sie können einen Verlauf der behobenen Warnungen suchen und anzeigen.

Optional haben Sie das Video angesehen: "Video: Übersicht über Warnungen"

Die folgende Tabelle beschreibt die im Grid Manager angezeigten Informationen für aktuelle und gelöste Warnungen.

Spaltenüberschrift	Beschreibung
Name oder Titel	Der Name der Warnung und ihre Beschreibung.
Schwere	Der Schweregrad der Warnung. Bei aktuellen Warnungen zeigt die Titelzeile, wenn mehrere Warnungen gruppiert sind, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten. **Kritisch**: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort angehen. Wenn das Problem nicht behoben wird, kann es zu Dienstunterbrechungen und Datenverlust kommen. **Schwerwiegend**: Es liegt ein anormaler Zustand vor, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten wichtige Warnungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder -Dienstes nicht stoppt. **Geringfügig**: Das System funktioniert normal, es liegt jedoch ein anormaler Zustand vor, der die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn er anhält. Sie sollten kleinere Warnungen, die nicht von selbst verschwinden, überwachen und beheben, um sicherzustellen, dass sie nicht zu einem ernsteren Problem führen.
Zeitgesteuert	**Aktuelle Warnungen**: Datum und Uhrzeit der Auslösung der Warnung in Ihrer Ortszeit und in UTC. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile die Zeiten für die jüngste Instanz der Warnung (*neueste*) und die älteste Instanz der Warnung (*älteste*) an. **Behobene Warnungen**: Wie lange es her ist, dass die Warnung ausgelöst wurde.
Site/Knoten	Der Name der Site und des Knotens, an dem der Alarm auftritt oder aufgetreten ist.

Spaltenüberschrift	Beschreibung
Status	Ob der Alarm aktiv, stummgeschaltet oder behoben ist. Wenn mehrere Warnungen gruppiert sind und im Dropdown-Menü „Alle Warnungen“ ausgewählt ist, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung aktiv sind und wie viele Instanzen stummgeschaltet wurden.
Zeit bis zur Lösung (nur gelöste Warnungen)	Wie lange es her ist, dass die Warnung behoben wurde.
Aktuelle Werte oder *Datenwerte*	Der Wert der Metrik, die zur Auslösung der Warnung geführt hat. Bei einigen Warnungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnung zu verstehen und zu untersuchen. Die für die Warnung **Geringer Objektdatenspeicher** angezeigten Werte umfassen beispielsweise den Prozentsatz des verwendeten Speicherplatzes, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Speicherplatzes. **Hinweis:** Wenn mehrere aktuelle Warnungen gruppiert sind, werden die aktuellen Werte nicht in der Titelzeile angezeigt.
Ausgelöste Werte (nur gelöste Warnungen)	Der Wert der Metrik, die zur Auslösung der Warnung geführt hat. Bei einigen Warnungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnung zu verstehen und zu untersuchen. Die für die Warnung **Geringer Objektdatenspeicher** angezeigten Werte umfassen beispielsweise den Prozentsatz des verwendeten Speicherplatzes, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Speicherplatzes.

Schritte

1. Wählen Sie den Link **Aktuelle Warnungen** oder **Behobene Warnungen** aus, um eine Liste der Warnungen in diesen Kategorien anzuzeigen. Sie können die Details einer Warnung auch anzeigen, indem Sie **Knoten** > ***Knoten*** > **Übersicht** auswählen und dann die Warnung aus der Tabelle „Warnungen“ auswählen.

   Aktuelle Warnungen werden standardmäßig wie folgt angezeigt:

   - Die zuletzt ausgelösten Warnungen werden zuerst angezeigt.
   - Mehrere Warnungen desselben Typs werden als Gruppe angezeigt.
   - Stummgeschaltete Warnungen werden nicht angezeigt.
   - Wenn für eine bestimmte Warnung auf einem bestimmten Knoten die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird nur die Warnung mit dem höchsten Schweregrad angezeigt. Das heißt, wenn Warnschwellenwerte für die Schweregrade „geringfügig“, „schwerwiegend“ und „kritisch“ erreicht werden, wird nur die kritische Warnung angezeigt.

     Die Seite „Aktuelle Warnungen“ wird alle zwei Minuten aktualisiert.

2. Um Gruppen von Warnungen zu erweitern, wählen Sie das Abwärtspfeilzeichen . Um einzelne Warnungen in einer Gruppe auszublenden, wählen Sie das Aufwärts-Caret , oder wählen Sie den Namen der Gruppe aus.
3. Um einzelne Warnungen statt Warnungsgruppen anzuzeigen, deaktivieren Sie das Kontrollkästchen **Warnungen gruppieren**.

4. Um aktuelle Warnungen oder Warnungsgruppen zu sortieren, wählen Sie die Aufwärts-/Abwärtspfeile in jeder Spaltenüberschrift.
   - Wenn **Gruppenwarnungen** ausgewählt ist, werden sowohl die Warnungsgruppen als auch die einzelnen Warnungen innerhalb jeder Gruppe sortiert. Beispielsweise möchten Sie möglicherweise die Warnungen in einer Gruppe nach **Auslösezeit** sortieren, um die aktuellste Instanz einer bestimmten Warnung zu finden.
   - Wenn **Gruppenwarnungen** gelöscht wird, wird die gesamte Liste der Warnungen sortiert. Sie möchten beispielsweise möglicherweise alle Warnungen nach **Knoten/Site** sortieren, um alle Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.
5. Um aktuelle Warnungen nach Status (**Alle Warnungen**, **Aktiv** oder **Stummgeschaltet**) zu filtern, verwenden Sie das Dropdown-Menü oben in der Tabelle.

   Sehen "Warnmeldungen stummschalten" .
6. So sortieren Sie gelöste Warnungen:
   - Wählen Sie einen Zeitraum aus dem Dropdown-Menü **Bei Auslösung** aus.
   - Wählen Sie einen oder mehrere Schweregrade aus dem Dropdown-Menü **Schweregrad** aus.
   - Wählen Sie aus dem Dropdown-Menü **Alarmregel** eine oder mehrere standardmäßige oder benutzerdefinierte Alarmregeln aus, um nach gelösten Alarmen zu filtern, die sich auf eine bestimmte Alarmregel beziehen.
   - Wählen Sie einen oder mehrere Knoten aus dem Dropdown-Menü **Knoten** aus, um nach gelösten Warnungen zu filtern, die sich auf einen bestimmten Knoten beziehen.
7. Um Details zu einer bestimmten Warnung anzuzeigen, wählen Sie die Warnung aus. Ein Dialogfeld enthält Details und empfohlene Maßnahmen für die von Ihnen ausgewählte Warnung.
8. (Optional) Wählen Sie für eine bestimmte Warnung „Diese Warnung stummschalten“ aus, um die Warnungsregel stummzuschalten, die die Auslösung dieser Warnung verursacht hat.

   Sie müssen über die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" um eine Warnregel stummzuschalten.

   > Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel stummzuschalten. Wenn eine Warnregel stummgeschaltet wird, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.
9. So zeigen Sie die aktuellen Bedingungen für die Warnregel an:
   a. Wählen Sie in den Alarmdetails **Bedingungen anzeigen** aus.

      Es wird ein Popup-Fenster angezeigt, in dem der Prometheus-Ausdruck für jeden definierten Schweregrad aufgelistet ist.

   b. Um das Popup zu schließen, klicken Sie irgendwo außerhalb des Popups.
10. Wählen Sie optional **Regel bearbeiten** aus, um die Warnregel zu bearbeiten, die zur Auslösung dieser Warnung geführt hat.

    Sie müssen über die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" , um eine Warnregel zu bearbeiten.

Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel zu bearbeiten. Wenn Sie Triggerwerte ändern, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

11. Um die Alarmdetails zu schließen, wählen Sie **Schließen**.

Überwachen der Speicherkapazität

Überwachen Sie den insgesamt verfügbaren nutzbaren Speicherplatz, um sicherzustellen, dass dem StorageGRID -System nicht der Speicherplatz für Objekte oder Objektmetadaten ausgeht.

StorageGRID speichert Objektdaten und Objektmetadaten getrennt und reserviert eine bestimmte Menge an Speicherplatz für eine verteilte Cassandra-Datenbank, die Objektmetadaten enthält. Überwachen Sie den Gesamtspeicherplatzverbrauch für Objekte und Objektmetadaten sowie Trends beim jeweiligen Speicherplatzverbrauch. Auf diese Weise können Sie das Hinzufügen von Knoten im Voraus planen und Dienstausfälle vermeiden.

Du kannst"Informationen zur Speicherkapazität anzeigen" für das gesamte Grid, für jeden Standort und für jeden Speicherknoten in Ihrem StorageGRID System.

Speicherkapazität für das gesamte Netz überwachen

Überwachen Sie die Gesamtspeicherkapazität Ihres Grids, um sicherzustellen, dass ausreichend freier Speicherplatz für Objektdaten und Objektmetadaten verbleibt. Wenn Sie wissen, wie sich die Speicherkapazität im Laufe der Zeit ändert, können Sie das Hinzufügen von Speicherknoten oder Speichervolumes besser planen, bevor die nutzbare Speicherkapazität des Grids verbraucht ist.

Über das Grid Manager-Dashboard können Sie schnell beurteilen, wie viel Speicher für das gesamte Grid und für jedes Rechenzentrum verfügbar ist. Die Seite „Knoten“ bietet detailliertere Werte für Objektdaten und Objektmetadaten.

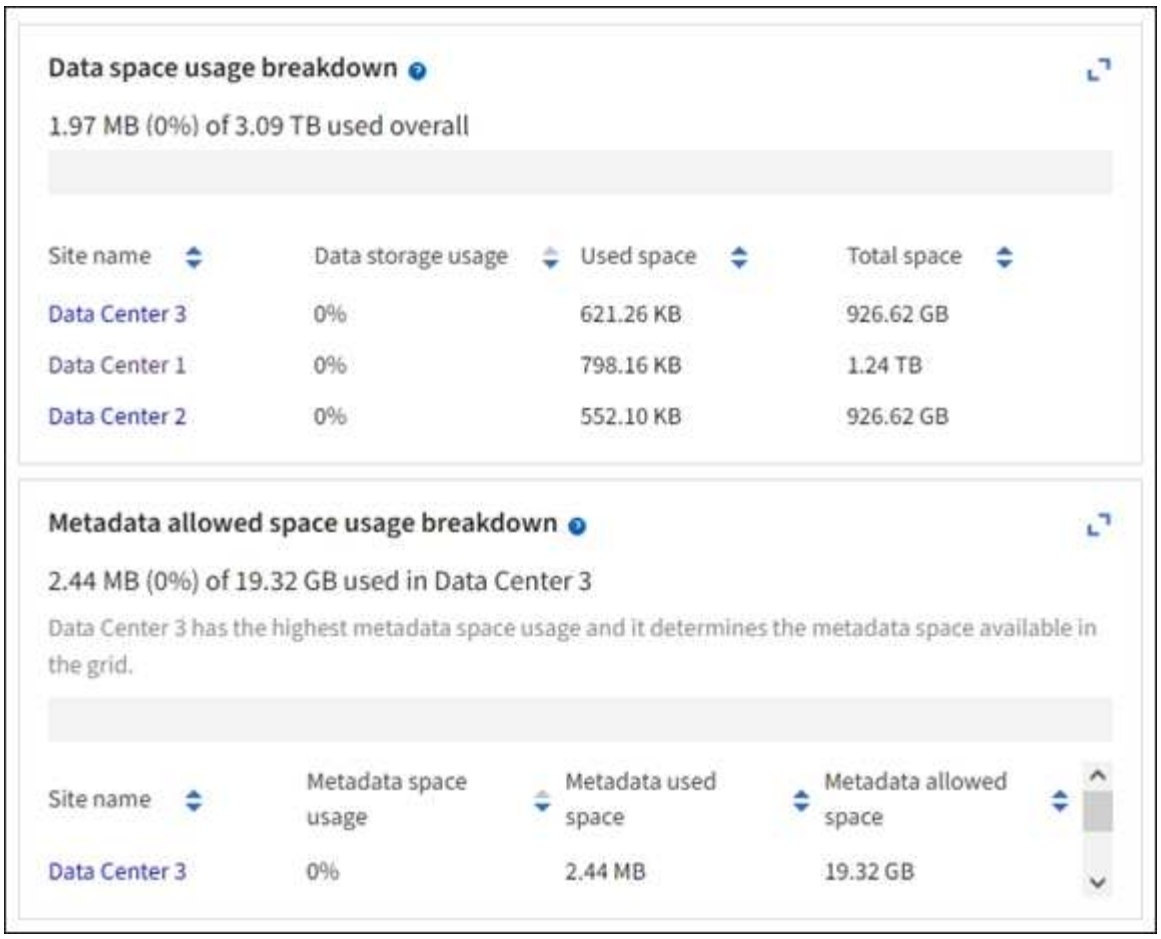
Schritte

1. Bewerten Sie, wie viel Speicher für das gesamte Grid und für jedes Rechenzentrum verfügbar ist.

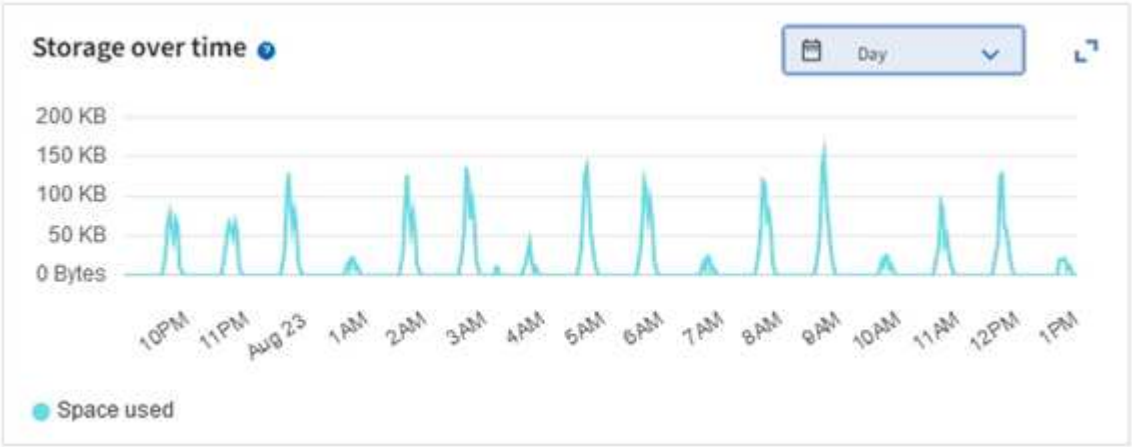
   a. Wählen Sie **Dashboard > Übersicht**.

   b. Beachten Sie die Werte auf den Karten „Aufschlüsselung der Datenspeicherplatznutzung“ und „Aufschlüsselung der zulässigen Metadatenspeicherplatznutzung“. Auf jeder Karte ist ein Prozentsatz der Speichernutzung, die Kapazität des verwendeten Speicherplatzes und der gesamte verfügbare oder pro Site zulässige Speicherplatz aufgeführt.

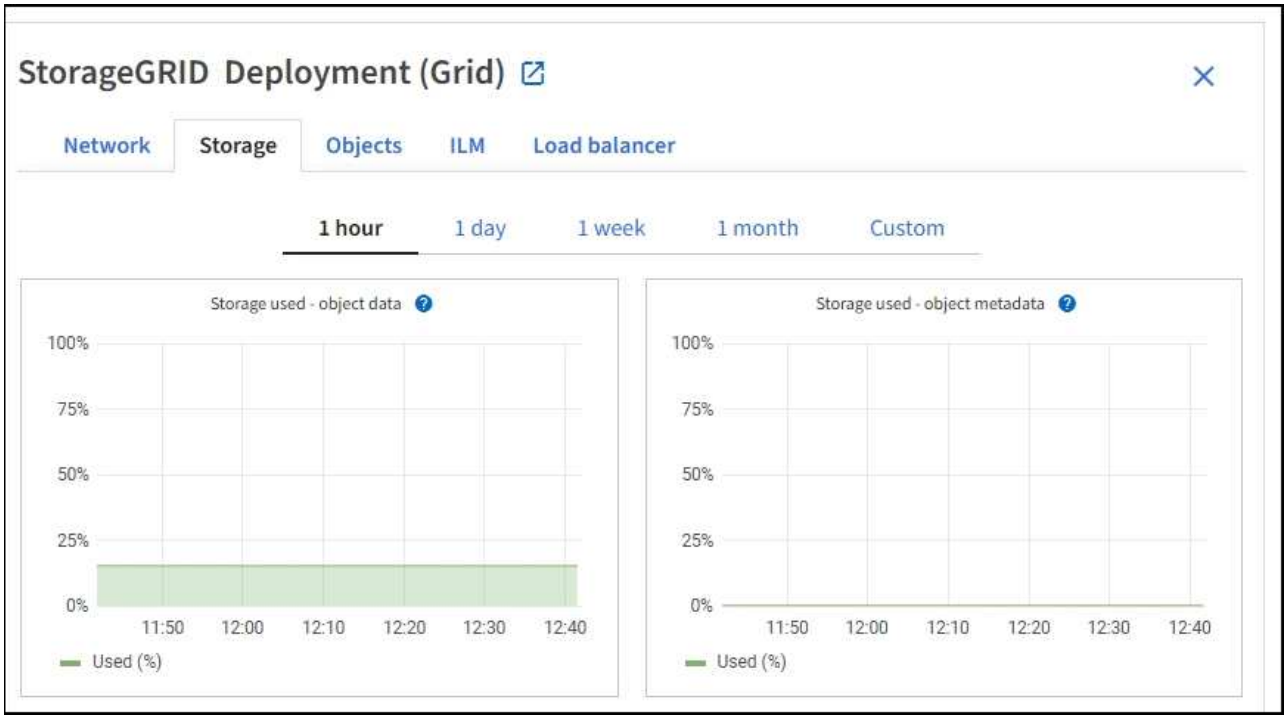
      Die Zusammenfassung umfasst keine Archivmedien.



a. Beachten Sie das Diagramm auf der Karte „Speicherung im Zeitverlauf“. Verwenden Sie das Dropdown-Menü für den Zeitraum, um zu ermitteln, wie schnell der Speicherplatz verbraucht wird.



2. Auf der Seite „Knoten“ finden Sie weitere Einzelheiten dazu, wie viel Speicherplatz verwendet wurde und wie viel Speicherplatz im Raster für Objektdaten und Objektmetadaten noch verfügbar ist.
   a. Wählen Sie **NODES**.
   b. Wählen Sie ***grid*** > **Speicher**.



c. Bewegen Sie den Cursor über die Diagramme **Verwendeter Speicher – Objektdaten** und **Verwendeter Speicher – Objektmetadaten**, um zu sehen, wie viel Objektspeicher und Objektmetadatenspeicher für das gesamte Raster verfügbar ist und wie viel im Laufe der Zeit verwendet wurde.

> Die Gesamtwerte für eine Site oder das Raster umfassen keine Knoten, die seit mindestens fünf Minuten keine Metriken gemeldet haben, beispielsweise Offline-Knoten.

3. Planen Sie eine Erweiterung, um Speicherknoten oder Speichervolumes hinzuzufügen, bevor die nutzbare Speicherkapazität des Grids verbraucht ist.

   Berücksichtigen Sie bei der Planung des Zeitpunkts einer Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Speicher dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, möchten Sie möglicherweise eine Erweiterung vornehmen, wenn vorhandene Speicherknoten zu etwa 70 % belegt sind, um die Anzahl der hinzuzufügenden Knoten zu reduzieren.

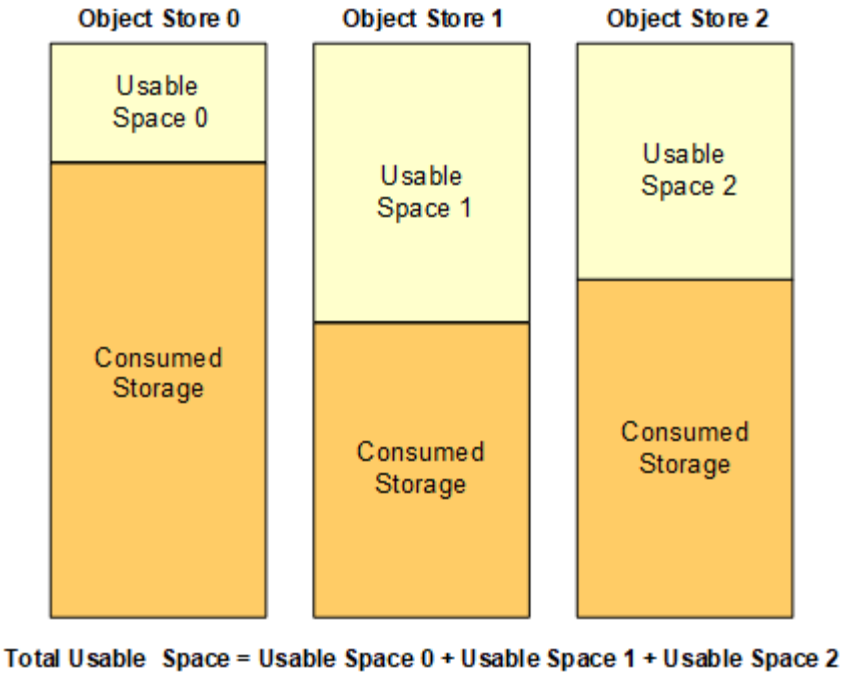
   Weitere Informationen zur Planung einer Speichererweiterung finden Sie im"Anleitung zur Erweiterung von StorageGRID" .

Überwachen Sie die Speicherkapazität für jeden Speicherknoten

Überwachen Sie den gesamten nutzbaren Speicherplatz für jeden Speicherknoten, um sicherzustellen, dass der Knoten über genügend Speicherplatz für neue Objektdaten verfügt.

Informationen zu diesem Vorgang

Der nutzbare Speicherplatz ist die Menge an Speicherplatz, die zum Speichern von Objekten zur Verfügung steht. Der gesamte nutzbare Speicherplatz für einen Speicherknoten wird berechnet, indem der verfügbare Speicherplatz aller Objektspeicher innerhalb des Knotens addiert wird.



Schritte

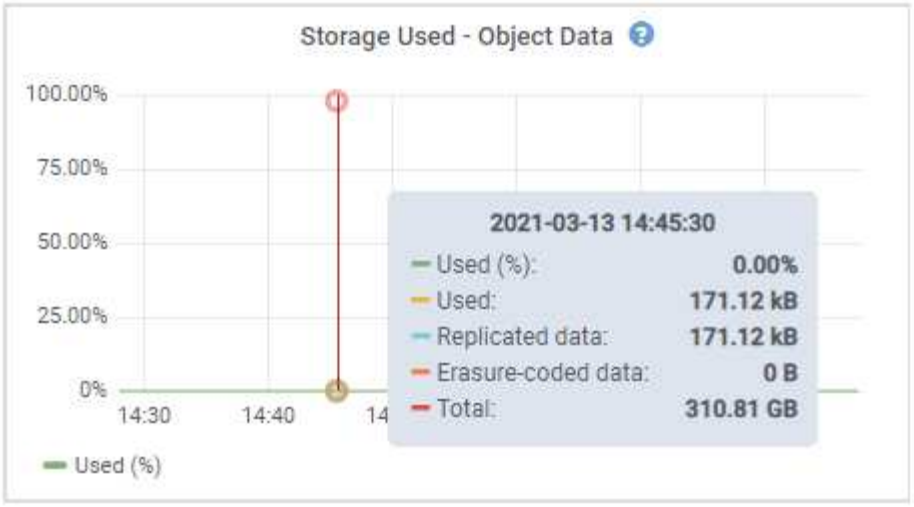
1. Wählen Sie **NODES** > ***Speicherknoten*** > **Speicher**.

   Die Diagramme und Tabellen für den Knoten werden angezeigt.

2. Positionieren Sie den Cursor über dem Datendiagramm „Speicherplatznutzung – Objekt“.

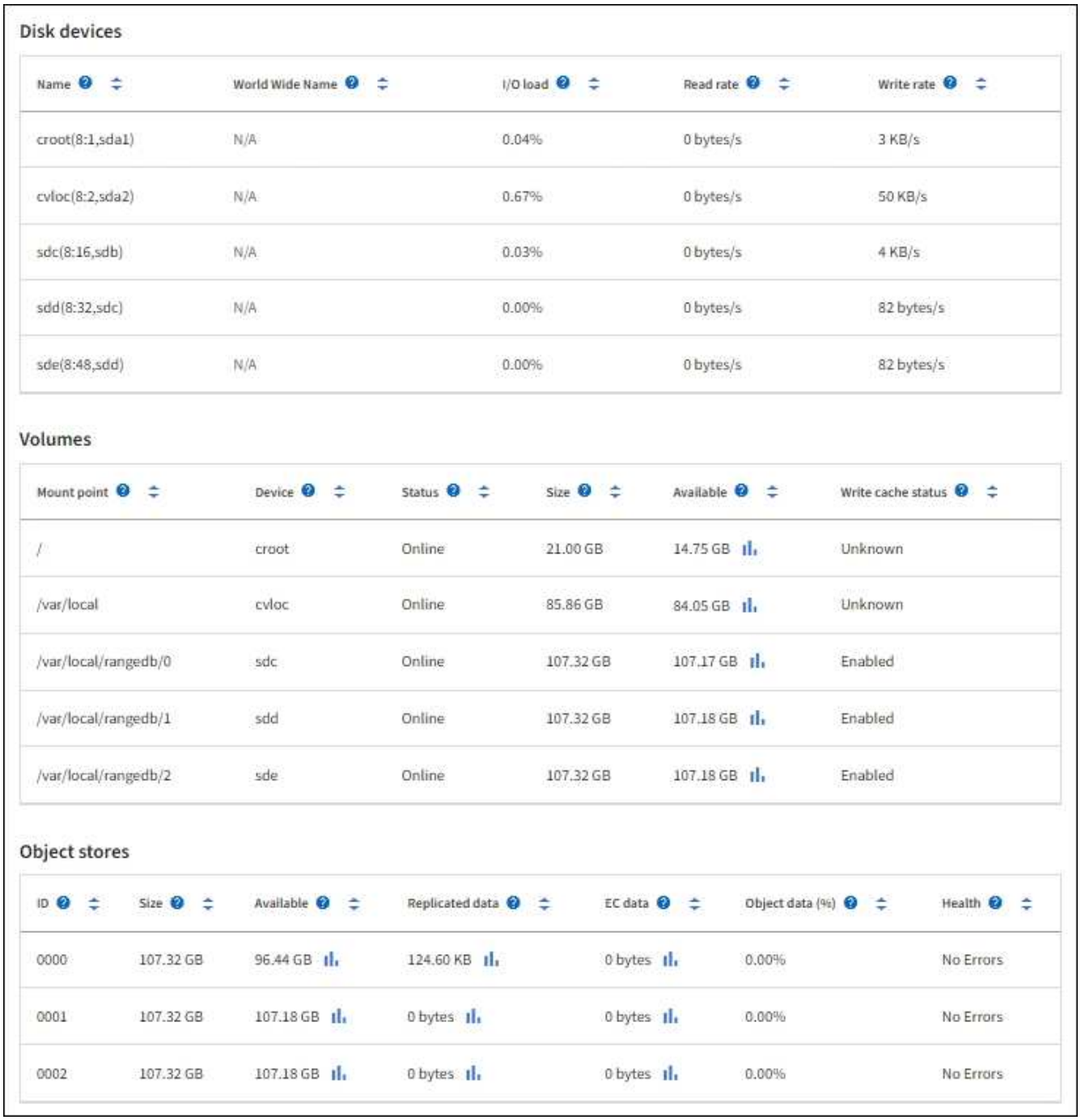
   Es werden folgende Werte angezeigt:

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



3. Überprüfen Sie die verfügbaren Werte in den Tabellen „Volumes“ und „Objektspeicher“ unter den Diagrammen.

Um Diagramme dieser Werte anzuzeigen, klicken Sie auf die Diagrammsymbole in den Spalten „Verfügbar“.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	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

4. Überwachen Sie die Werte im Laufe der Zeit, um die Rate abzuschätzen, mit der nutzbarer Speicherplatz verbraucht wird.
5. Um den normalen Systembetrieb aufrechtzuerhalten, fügen Sie Speicherknoten und Speichervolumes hinzu oder archivieren Sie Objektdaten, bevor der nutzbare Speicherplatz verbraucht ist.

   Berücksichtigen Sie bei der Planung des Zeitpunkts einer Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Speicher dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, möchten Sie möglicherweise eine Erweiterung vornehmen, wenn vorhandene Speicherknoten zu etwa 70 % belegt sind, um die Anzahl der hinzuzufügenden Knoten zu reduzieren.

Weitere Informationen zur Planung einer Speichererweiterung finden Sie im"Anleitung zur Erweiterung von

StorageGRID" .

Der"Geringe Objektdatenspeicherung" Eine Warnung wird ausgelöst, wenn auf einem Speicherknoten nicht genügend Speicherplatz zum Speichern von Objektdaten vorhanden ist.

Überwachen Sie die Objektmetadatenkapazität für jeden Speicherknoten

Überwachen Sie die Metadatennutzung für jeden Speicherknoten, um sicherzustellen, dass ausreichend Speicherplatz für wichtige Datenbankvorgänge verfügbar bleibt. Sie müssen an jedem Standort neue Speicherknoten hinzufügen, bevor die Objektmetadaten 100 % des zulässigen Metadatenspeicherplatzes überschreiten.

Informationen zu diesem Vorgang

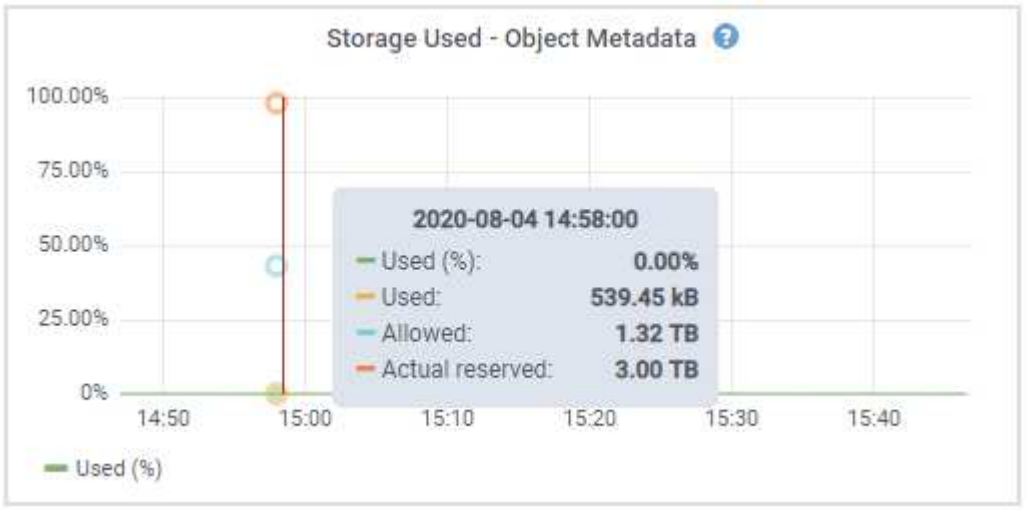
StorageGRID verwaltet an jedem Standort drei Kopien der Objektmetadaten, um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig auf alle Speicherknoten an jedem Standort verteilt, wobei der für Metadaten reservierte Speicherplatz auf Speichervolume 0 jedes Speicherknotens verwendet wird.

In einigen Fällen kann die Objektmetadatenkapazität des Grids schneller verbraucht werden als seine Objektspeicherkapazität. Wenn Sie beispielsweise normalerweise eine große Anzahl kleiner Objekte aufnehmen, müssen Sie möglicherweise Speicherknoten hinzufügen, um die Metadatenkapazität zu erhöhen, obwohl noch ausreichend Objektspeicherkapazität vorhanden ist.

Zu den Faktoren, die die Metadatennutzung erhöhen können, gehören unter anderem die Größe und Menge der Benutzermetadaten und Tags, die Gesamtzahl der Teile in einem mehrteiligen Upload und die Häufigkeit von Änderungen an ILM-Speicherorten.

Schritte

1. Wählen Sie **NODES** > ***Speicherknoten*** > **Speicher**.
2. Positionieren Sie den Cursor über dem Diagramm „Speicherplatznutzung – Objektmetadaten“, um die Werte für einen bestimmten Zeitpunkt anzuzeigen.



Gebraucht (%)

Der Prozentsatz des zulässigen Metadatenspeicherplatzes, der auf diesem Speicherknoten verwendet wurde.

Prometheus-Metriken: `storagegrid_storage_utilization_metadata_bytes` Und

`storagegrid_storage_utilization_metadata_allowed_bytes`

Gebraucht

Die Bytes des zulässigen Metadatenspeichers, die auf diesem Speicherknoten verwendet wurden.

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_bytes`

Erlaubt

Der für Objektmetadaten auf diesem Speicherknoten zulässige Speicherplatz. Um zu erfahren, wie dieser Wert für jeden Speicherknoten ermittelt wird, lesen Sie die"vollständige Beschreibung des zulässigen Metadatenbereichs" .

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_allowed_bytes`

Tatsächlich reserviert

Der tatsächliche Speicherplatz, der auf diesem Speicherknoten für Metadaten reserviert ist. Beinhaltet den zulässigen Speicherplatz und den erforderlichen Speicherplatz für wichtige Metadatenvorgänge. Um zu erfahren, wie dieser Wert für jeden Speicherknoten berechnet wird, lesen Sie die"vollständige Beschreibung des tatsächlich reservierten Speicherplatzes für Metadaten" .

Die Prometheus-Metrik wird in einer zukünftigen Version hinzugefügt.

Die Gesamtwerte für eine Site oder das Raster umfassen keine Knoten, die seit mindestens fünf Minuten keine Metriken gemeldet haben, beispielsweise Offline-Knoten.

3. Wenn der Wert **Verwendet (%)** 70 % oder höher ist, erweitern Sie Ihr StorageGRID -System, indem Sie jedem Standort Speicherknoten hinzufügen.

Die Warnung **Geringer Metadatenspeicher** wird ausgelöst, wenn der Wert **Verwendet (%)** bestimmte Schwellenwerte erreicht. Wenn die Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes belegen, können unerwünschte Ergebnisse auftreten.

Wenn Sie die neuen Knoten hinzufügen, gleicht das System die Objektmetadaten automatisch über alle Speicherknoten innerhalb der Site aus. Siehe die"Anleitung zur Erweiterung eines StorageGRID -Systems" .

Überwachen Sie Prognosen zur Speicherplatznutzung

Überwachen Sie die Speichernutzungsprognosen für Benutzerdaten und Metadaten, um abzuschätzen, wann Sie"ein Raster erweitern" .

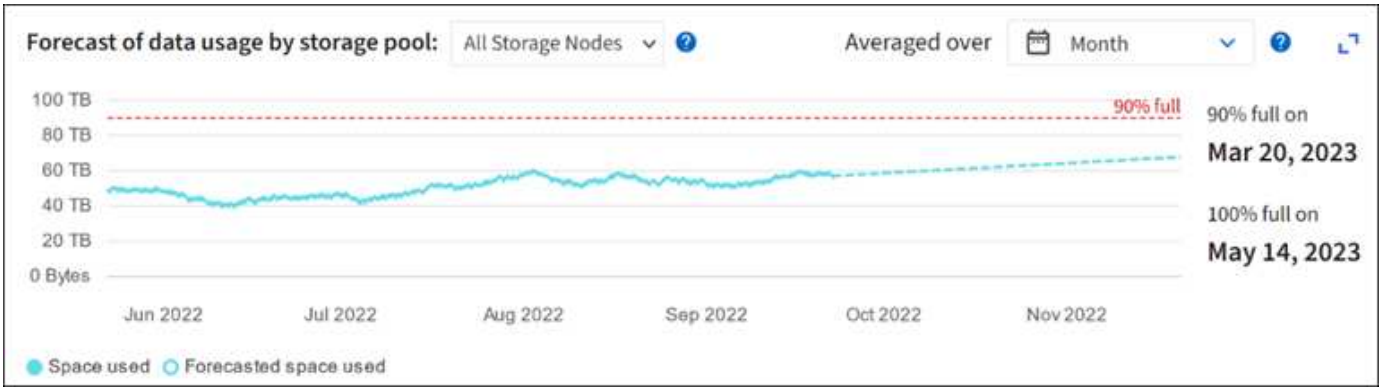
Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie im Pulldown-Menü „**Durchschnitt über**“ einen kürzeren Bereich aus, um nur die aktuellsten Aufnahmemuster anzuzeigen. Wenn Sie saisonale Muster erkennen, wählen Sie einen längeren Bereich.

Wenn Sie eine neue StorageGRID Installation haben, warten Sie, bis sich Daten und Metadaten angesammelt haben, bevor Sie die Prognosen zur Speicherplatznutzung auswerten.

Schritte

1. Wählen Sie im Dashboard **Speicher** aus.
2. Zeigen Sie die Dashboard-Karten, die Prognose der Datennutzung nach Speicherpool und die Prognose der Metadatennutzung nach Site an.

3. Verwenden Sie diese Werte, um abzuschätzen, wann Sie neue Speicherknoten zur Daten- und Metadatenspeicherung hinzufügen müssen.



Überwachen Sie das Informationslebenszyklusmanagement

Das Information Lifecycle Management (ILM)-System bietet Datenverwaltung für alle im Grid gespeicherten Objekte. Sie müssen die ILM-Vorgänge überwachen, um zu wissen, ob das Grid die aktuelle Last bewältigen kann oder ob mehr Ressourcen benötigt werden.

Informationen zu diesem Vorgang

Das StorageGRID -System verwaltet Objekte durch Anwendung der aktiven ILM-Richtlinien. Die ILM-Richtlinien und die zugehörigen ILM-Regeln bestimmen, wie viele Kopien erstellt werden, welche Art von Kopien erstellt werden, wo die Kopien abgelegt werden und wie lange jede Kopie aufbewahrt wird.

Die Objektaufnahme und andere objektbezogene Aktivitäten können die Rate überschreiten, mit der StorageGRID ILM auswerten kann. Dies führt dazu, dass das System Objekte in die Warteschlange stellt, deren ILM-Platzierungsanweisungen nicht nahezu in Echtzeit erfüllt werden können. Sie sollten überwachen, ob StorageGRID mit den Client-Aktionen Schritt hält.

Verwenden Sie die Dashboard-Registerkarte des Grid Managers

Schritte

Verwenden Sie die Registerkarte „ILM“ im Grid Manager-Dashboard, um ILM-Vorgänge zu überwachen:

1. Sign in .
2. Wählen Sie im Dashboard die Registerkarte „ILM“ aus und notieren Sie sich die Werte auf der Karte „ILM-Warteschlange (Objekte)“ und der Karte „ILM-Auswertungstarif“.

   Es ist mit vorübergehenden Spitzen in der ILM-Warteschlangenkarte (Objekte) auf dem Dashboard zu rechnen. Wenn die Warteschlange jedoch weiter zunimmt und nicht abnimmt, benötigt das Grid mehr Ressourcen, um effizient zu arbeiten: entweder mehr Speicherknoten oder, wenn die ILM-Richtlinie Objekte an entfernten Standorten platziert, mehr Netzwerkbandbreite.

Verwenden der NODES-Seite

Schritte

Untersuchen Sie außerdem ILM-Warteschlangen mithilfe der Seite **NODES**:

Die Diagramme auf der Seite **NODES** werden in einer zukünftigen StorageGRID Version durch die entsprechenden Dashboard-Karten ersetzt.

1. Wählen Sie **NODES**.
2. Wählen Sie ***Gridname*** > **ILM**.
3. Positionieren Sie den Cursor über dem ILM-Warteschlangendiagramm, um den Wert der folgenden Attribute zu einem bestimmten Zeitpunkt anzuzeigen:
   - **In die Warteschlange gestellte Objekte (aus Clientvorgängen)**: Die Gesamtzahl der Objekte, die aufgrund von Clientvorgängen (z. B. Aufnahme) auf eine ILM-Auswertung warten.
   - **In die Warteschlange gestellte Objekte (aus allen Vorgängen)**: Die Gesamtzahl der Objekte, die auf die ILM-Auswertung warten.
   - **Scanrate (Objekte/Sek.)**: Die Rate, mit der Objekte im Raster gescannt und für ILM in die Warteschlange gestellt werden.
   - **Auswertungsrate (Objekte/Sek.)**: Die aktuelle Rate, mit der Objekte im Grid anhand der ILM-Richtlinie ausgewertet werden.
4. Sehen Sie sich im Abschnitt „ILM-Warteschlange“ die folgenden Attribute an.

   Der ILM-Warteschlangenabschnitt ist nur für das Raster enthalten. Diese Informationen werden auf der ILM-Registerkarte für eine Site oder einen Speicherknoten nicht angezeigt.

   - **Scanzeitraum – geschätzt**: Die geschätzte Zeit, die zum Abschließen eines vollständigen ILM-Scans aller Objekte benötigt wird.

     Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde.

   - **Versuchte Reparaturen**: Die Gesamtzahl der Objektreparaturvorgänge für replizierte Daten, die versucht wurden. Dieser Zähler erhöht sich jedes Mal, wenn ein Speicherknoten versucht, ein Hochrisikoobjekt zu reparieren. Bei einer Netzüberlastung werden ILM-Reparaturen mit hohem Risiko priorisiert.

     Die gleiche Objektreparatur kann erneut inkrementiert werden, wenn die Replikation nach der Reparatur fehlgeschlagen ist.

   Diese Attribute können nützlich sein, wenn Sie den Fortschritt der Wiederherstellung des Storage Node-Volumes überwachen. Wenn die Anzahl der Reparaturversuche nicht mehr zunimmt und ein vollständiger Scan abgeschlossen wurde, ist die Reparatur wahrscheinlich abgeschlossen.

Überwachen Sie Netzwerk- und Systemressourcen

Die Integrität und Bandbreite des Netzwerks zwischen Knoten und Standorten sowie die Ressourcennutzung durch einzelne Grid-Knoten sind für einen effizienten Betrieb von entscheidender Bedeutung.

Überwachen Sie Netzwerkverbindungen und Leistung

Netzwerkkonnektivität und Bandbreite sind besonders wichtig, wenn Ihre ILM-Richtlinie (Information Lifecycle Management) replizierte Objekte zwischen Standorten kopiert oder löschcodierte Objekte mithilfe eines Schemas speichert, das Schutz vor Standortverlust bietet. Wenn das Netzwerk zwischen den Standorten nicht

verfügbar ist, die Netzwerklatenz zu hoch ist oder die Netzwerkbandbreite nicht ausreicht, können einige ILM-Regeln Objekte möglicherweise nicht an der erwarteten Stelle platzieren. Dies kann zu Aufnahmefehlern (wenn für ILM-Regeln die Option „Strenge Aufnahme“ ausgewählt ist) oder zu einer schlechten Aufnahmeleistung und ILM-Rückständen führen.

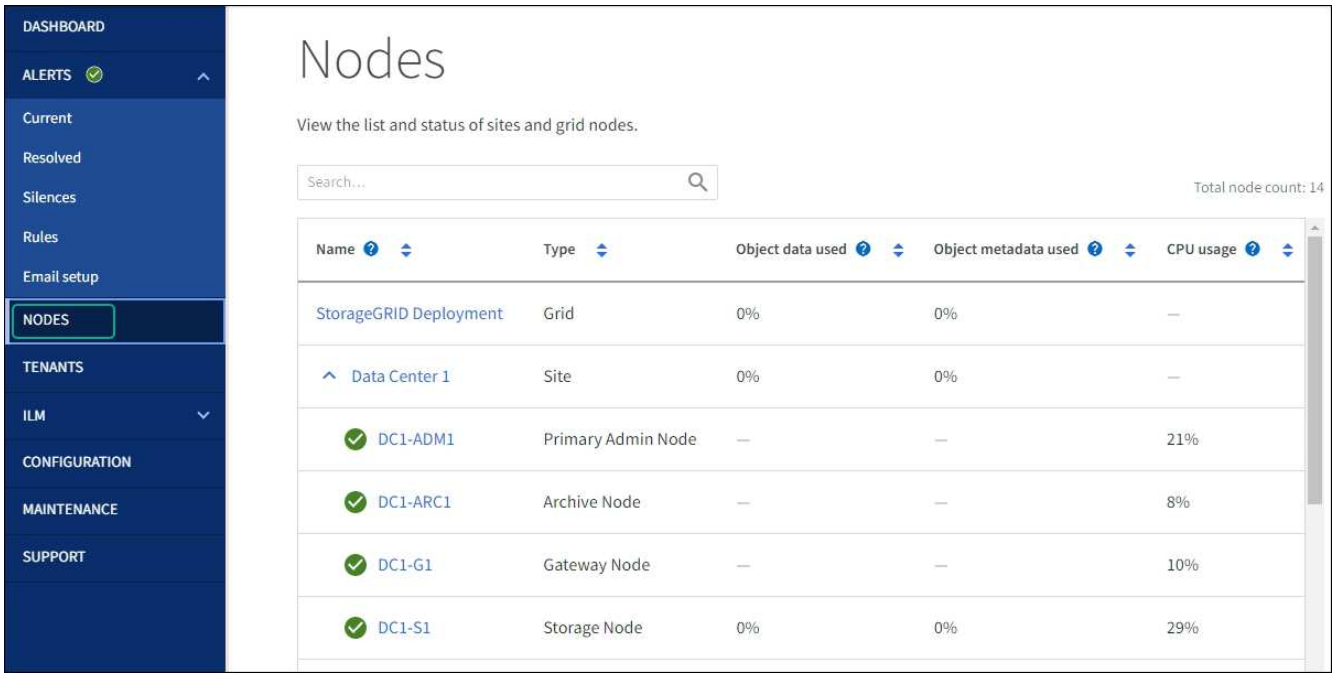
Verwenden Sie den Grid Manager, um die Konnektivität und Netzwerkleistung zu überwachen, damit Sie etwaige Probleme umgehend beheben können.

Darüber hinaus sollten Sie"Erstellen von Richtlinien zur Klassifizierung des Netzwerkverkehrs" damit Sie den Datenverkehr im Zusammenhang mit bestimmten Mandanten, Buckets, Subnetzen oder Load Balancer-Endpunkten überwachen können. Sie können bei Bedarf Richtlinien zur Verkehrsbeschränkung festlegen.

Schritte

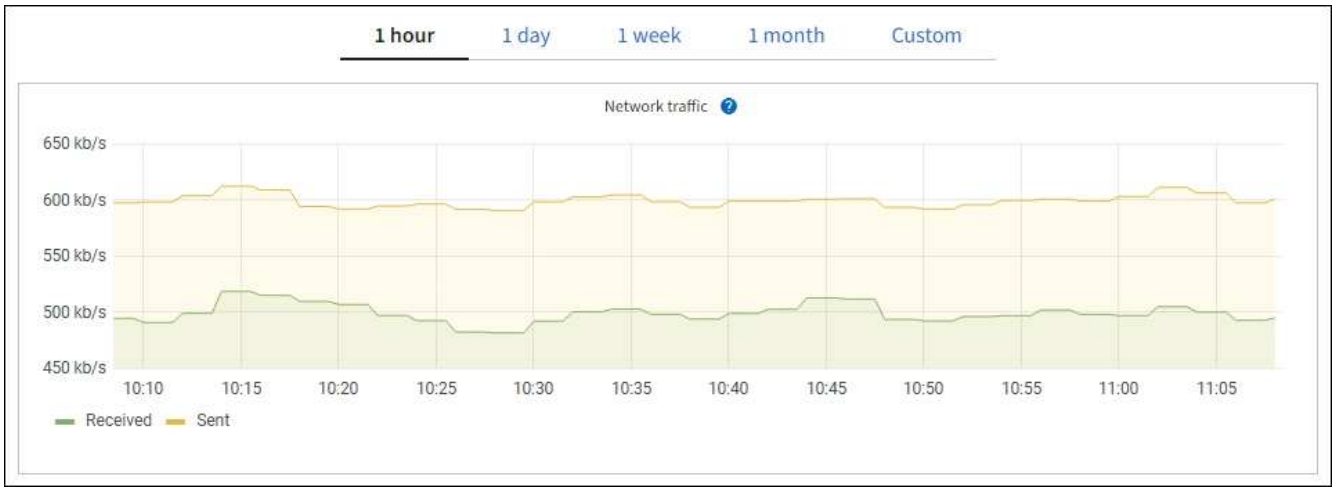
1. Wählen Sie **NODES**.

   Die Seite „Knoten“ wird angezeigt. Jeder Knoten im Raster wird im Tabellenformat aufgelistet.



2. Wählen Sie den Grid-Namen, einen bestimmten Rechenzentrumsstandort oder einen Grid-Knoten aus und wählen Sie dann die Registerkarte **Netzwerk**.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs für das gesamte Grid, den Rechenzentrumsstandort oder den Knoten.



a. Wenn Sie einen Grid-Knoten ausgewählt haben, scrollen Sie nach unten, um den Abschnitt **Netzwerkschnittstellen** der Seite zu überprüfen.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

b. Scrollen Sie für Grid-Knoten nach unten, um den Abschnitt **Netzwerkkommunikation** der Seite zu lesen.

Die Empfangs- und Sendetabellen zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Sendemetriken.

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

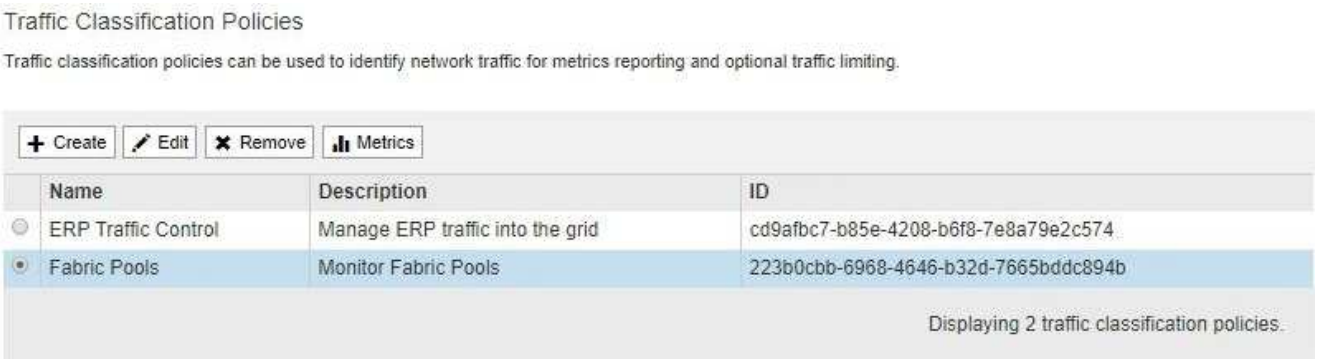
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

3. Verwenden Sie die mit Ihren Richtlinien zur Verkehrsklassifizierung verknüpften Metriken, um den Netzwerkverkehr zu überwachen.

a. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt und die vorhandenen Richtlinien werden in der Tabelle aufgelistet.



a. Um Diagramme anzuzeigen, die die mit einer Richtlinie verknüpften Netzwerkmetriken zeigen, wählen Sie das Optionsfeld links neben der Richtlinie aus und klicken Sie dann auf **Metriken**.

b. Sehen Sie sich die Diagramme an, um den mit der Richtlinie verbundenen Netzwerkverkehr zu verstehen.

   Wenn eine Datenverkehrsklassifizierungsrichtlinie darauf ausgelegt ist, den Netzwerkdatenverkehr zu begrenzen, analysieren Sie, wie oft der Datenverkehr begrenzt wird, und entscheiden Sie, ob die Richtlinie weiterhin Ihren Anforderungen entspricht. Von Zeit zu Zeit,"Passen Sie jede Verkehrsklassifizierungsrichtlinie nach Bedarf an" .

Ähnliche Informationen

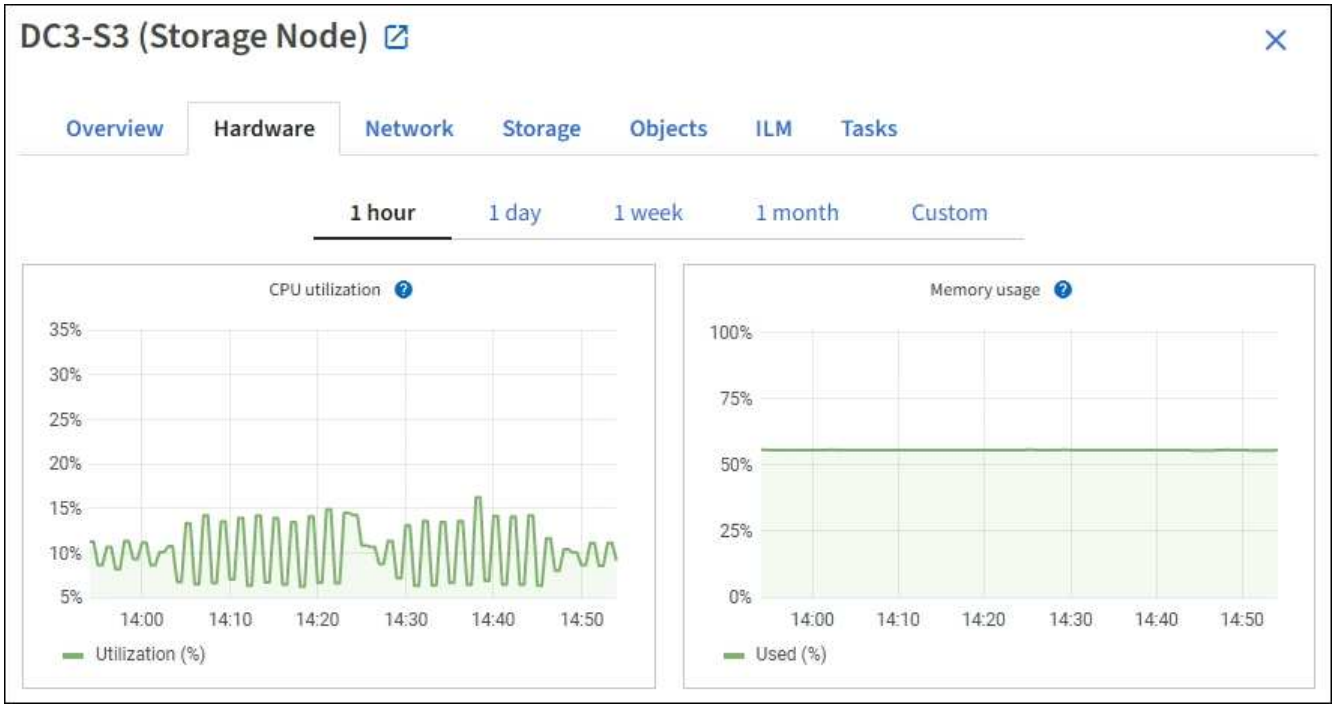
- "Anzeigen der Registerkarte „Netzwerk“"
- "Überwachen Sie den Verbindungsstatus des Knotens"

Überwachen von Ressourcen auf Knotenebene

Überwachen Sie einzelne Grid-Knoten, um deren Ressourcennutzungsgrade zu überprüfen. Wenn Knoten ständig überlastet sind, sind für einen effizienten Betrieb möglicherweise mehr Knoten erforderlich.

Schritte

1. Wählen Sie auf der Seite **NODES** den Knoten aus.
2. Wählen Sie die Registerkarte **Hardware**, um Diagramme zur CPU-Auslastung und Speichernutzung anzuzeigen.



3. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente über dem Diagramm oder der Grafik aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, in dem Sie Datums- und Zeitbereiche angeben können.
4. Wenn der Knoten auf einem Speichergerät oder einem Servicegerät gehostet wird, scrollen Sie nach unten, um die Komponententabellen anzuzeigen. Der Status aller Komponenten sollte „Nominal“ sein. Untersuchen Sie Komponenten mit einem anderen Status.

Ähnliche Informationen

- "Informationen zu Appliance-Speicherknoten anzeigen"
- "Informationen zu Appliance-Admin-Knoten und Gateway-Knoten anzeigen"

Überwachen Sie die Mieteraktivität

Alle S3-Client-Aktivitäten sind mit StorageGRID Mandantenkonten verknüpft. Mit dem Grid Manager können Sie die Speichernutzung oder den Netzwerkverkehr für alle oder einen bestimmten Mandanten überwachen. Sie können das Prüfprotokoll oder die Grafana-Dashboards verwenden, um detailliertere Informationen darüber zu sammeln, wie Mieter StorageGRID verwenden.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .

Alle Mieter anzeigen

Auf der Seite „Mieter“ werden grundlegende Informationen zu allen aktuellen Mieterkonten angezeigt.

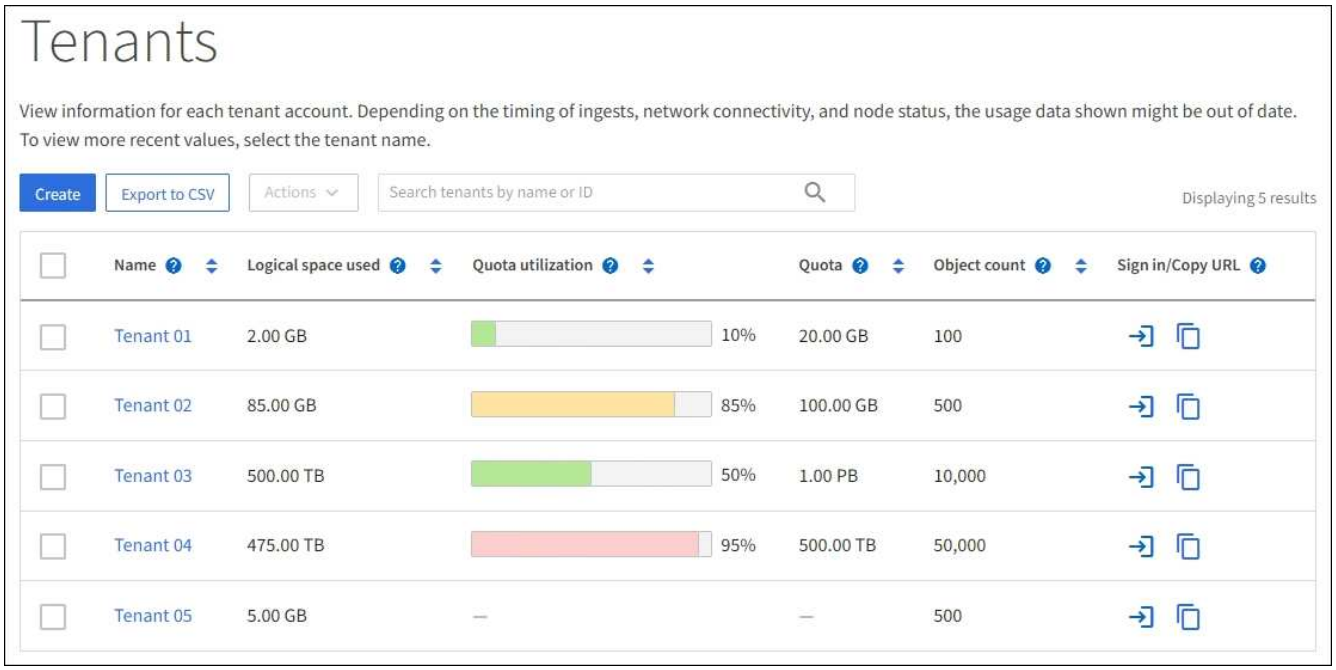
Schritte

1. Wählen Sie **MIETER** aus.

2. Überprüfen Sie die auf den Mieterseiten angezeigten Informationen.

   Für jeden Mandanten werden der verwendete logische Speicherplatz, die Kontingentnutzung, das Kontingent und die Objektanzahl aufgelistet. Wenn für einen Mandanten kein Kontingent festgelegt ist, enthalten die Felder „Kontingentnutzung“ und „Kontingent“ einen Bindestrich (—).

   > Bei den Angaben zum belegten Speicherplatz handelt es sich um Schätzwerte. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst.



3. Optional können Sie sich bei einem Mandantenkonto anmelden, indem Sie den Anmeldelink auswählen. in der Spalte * Sign in/ URL kopieren *.
4. Kopieren Sie optional die URL für die Anmeldeseite eines Mandanten, indem Sie den Link „URL kopieren“ auswählen. in der Spalte * Sign in/ URL kopieren *.
5. Wählen Sie optional **Exportieren nach CSV**, um eine `.csv` Datei mit den Nutzungswerten für alle Mandanten.

   Sie werden aufgefordert, die `.csv` Datei.

   Der Inhalt der `.csv` Die Datei sieht wie im folgenden Beispiel aus:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   Sie können das `.csv` Datei in einer Tabellenkalkulationsanwendung oder verwenden Sie sie in der Automatisierung.

6. Wenn keine Objekte aufgelistet sind, wählen Sie optional **Aktionen** > **Löschen** aus, um einen oder mehrere Mandanten zu entfernen. Sehen "Mieterkonto löschen" .

Sie können ein Mandantenkonto nicht entfernen, wenn das Konto Buckets oder Container enthält.

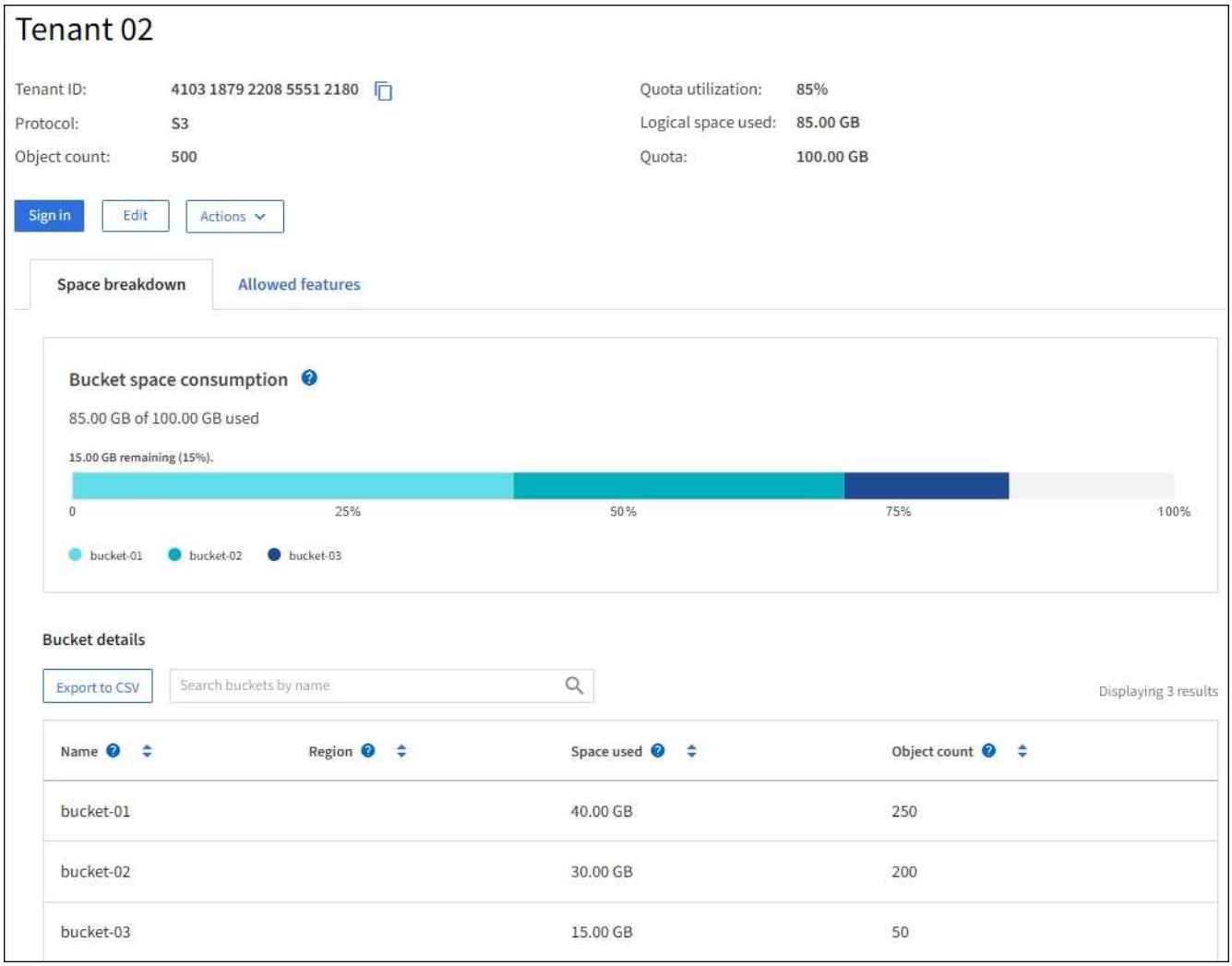
Einen bestimmten Mandanten anzeigen

Sie können Details zu einem bestimmten Mieter anzeigen.

Schritte

1. Wählen Sie den Mandantennamen auf der Seite „Mandanten“ aus.

   Die Seite mit den Mieterdetails wird angezeigt.



2. Sehen Sie sich die Mieterübersicht oben auf der Seite an.

   Dieser Abschnitt der Detailseite enthält zusammenfassende Informationen zum Mandanten, darunter die Objektanzahl des Mandanten, die Kontingentnutzung, den verwendeten logischen Speicherplatz und die Kontingenteinstellung.

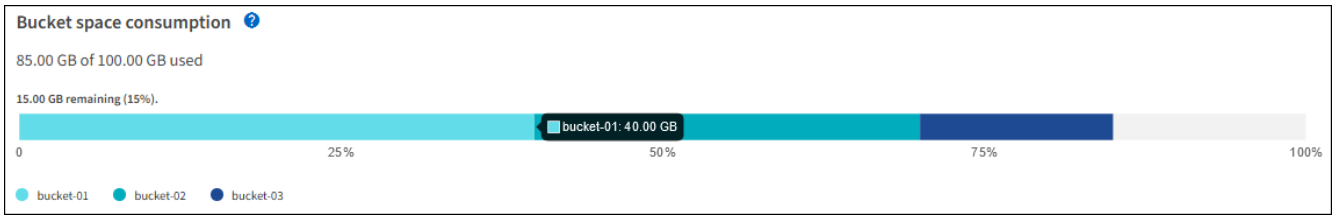
3. Überprüfen Sie auf der Registerkarte **Speicherplatzaufschlüsselung** das Diagramm **Speicherplatzverbrauch**.

   Dieses Diagramm zeigt den gesamten Speicherplatzverbrauch für alle S3-Buckets des Mandanten.

   Wenn für diesen Mandanten ein Kontingent festgelegt wurde, wird die Menge des verwendeten und

verbleibenden Kontingents als Text angezeigt (z. B. `85.00 GB of 100 GB used`). Wenn kein Kontingent festgelegt wurde, verfügt der Mandant über ein unbegrenztes Kontingent und der Text enthält nur die Menge des verwendeten Speicherplatzes (z. B. `85.00 GB used`). Das Balkendiagramm zeigt den Prozentsatz der Quote in jedem Bucket oder Container. Wenn der Mandant das Speicherkontingent um mehr als 1 % und mindestens 1 GB überschritten hat, zeigt das Diagramm das Gesamtkontingent und den Überschussbetrag an.

Sie können den Cursor über das Balkendiagramm bewegen, um den von jedem Bucket oder Container verwendeten Speicherplatz anzuzeigen. Sie können den Cursor über das Segment „Freier Speicherplatz“ bewegen, um die verbleibende Speicherquote anzuzeigen.



> Die Kontingentnutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. Beispielsweise überprüft StorageGRID das Kontingent, wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen ab, wenn der Mandant das Kontingent überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kontingent überschritten wurde. Wenn Objekte gelöscht werden, kann es sein, dass ein Mandant vorübergehend daran gehindert wird, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Die Berechnung der Kontingentnutzung kann 10 Minuten oder länger dauern.

> Die Kontingentnutzung eines Mandanten gibt die Gesamtmenge der Objektdaten an, die der Mandant in StorageGRID hochgeladen hat (logische Größe). Die Kontingentnutzung stellt nicht den Speicherplatz dar, der zum Speichern von Kopien dieser Objekte und ihrer Metadaten (physische Größe) verwendet wird.

> Sie können die Warnregel „Hohe Kontingentnutzung des Mandanten“ aktivieren, um festzustellen, ob Mandanten ihre Kontingente verbrauchen. Wenn diese Option aktiviert ist, wird diese Warnung ausgelöst, wenn ein Mandant 90 % seines Kontingents genutzt hat. Anweisungen hierzu finden Sie unter"Alarmregeln bearbeiten" .

4. Überprüfen Sie auf der Registerkarte **Speicherplatzaufschlüsselung** die **Bucket-Details**.

   Diese Tabelle listet die S3-Buckets für den Mandanten auf. Der verwendete Speicherplatz ist die Gesamtmenge der Objektdaten im Bucket oder Container. Dieser Wert stellt nicht den für ILM-Kopien und Objektmetadaten erforderlichen Speicherplatz dar.

5. Wählen Sie optional **In CSV exportieren** aus, um eine CSV-Datei mit den Nutzungswerten für jeden Bucket oder Container anzuzeigen und zu exportieren.

   Der Inhalt eines einzelnen S3-Tenants `.csv` Die Datei sieht wie im folgenden Beispiel aus:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

Sie können das `.csv` Datei in einer Tabellenkalkulationsanwendung oder verwenden Sie sie in der Automatisierung.

6. Wählen Sie optional die Registerkarte **Zugelassene Funktionen** aus, um eine Liste der Berechtigungen und Funktionen anzuzeigen, die für den Mandanten aktiviert sind. Sehen"Mieterkonto bearbeiten" wenn Sie eine dieser Einstellungen ändern müssen.
7. Wenn der Mandant über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, wählen Sie optional die Registerkarte **Grid-Föderation** aus, um mehr über die Verbindung zu erfahren.

   Sehen"Was ist Grid-Föderation?" Und"Verwalten der zulässigen Mandanten für die Grid-Föderation" .

Netzwerkverkehr anzeigen

Wenn für einen Mandanten Richtlinien zur Verkehrsklassifizierung gelten, überprüfen Sie den Netzwerkverkehr für diesen Mandanten.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt und die vorhandenen Richtlinien werden in der Tabelle aufgelistet.

2. Überprüfen Sie die Liste der Richtlinien, um diejenigen zu ermitteln, die für einen bestimmten Mieter gelten.
3. Um die mit einer Richtlinie verknüpften Metriken anzuzeigen, wählen Sie das Optionsfeld links neben der Richtlinie aus und wählen Sie **Metriken**.
4. Analysieren Sie die Diagramme, um festzustellen, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

Sehen "Verwalten von Richtlinien zur Datenverkehrsklassifizierung" für weitere Informationen.

Verwenden des Überwachungsprotokolls

Optional können Sie das Überwachungsprotokoll für eine detailliertere Überwachung der Aktivitäten eines Mandanten verwenden.

Sie können beispielsweise die folgenden Arten von Informationen überwachen:

- Bestimmte Clientvorgänge, wie z. B. PUT, GET oder DELETE
- Objektgrößen
- Die ILM-Regel für Objekte
- Die Quell-IP der Client-Anfragen

Prüfprotokolle werden in Textdateien geschrieben, die Sie mit einem Protokollanalysetool Ihrer Wahl analysieren können. Dadurch können Sie die Aktivitäten Ihrer Kunden besser nachvollziehen oder ausgefeilte Chargeback- und Abrechnungsmodelle implementieren.

Sehen "Überprüfen der Überwachungsprotokolle" für weitere Informationen.

Verwenden Sie Prometheus-Metriken

Verwenden Sie optional Prometheus-Metriken, um Berichte zur Mieteraktivität zu erstellen.

- Wählen Sie im Grid Manager **SUPPORT** > **Tools** > **Metriken**. Sie können vorhandene Dashboards wie S3 Overview verwenden, um Clientaktivitäten zu überprüfen.

> Die auf der Seite „Metriken“ verfügbaren Tools sind in erster Linie für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig.

- Wählen Sie oben im Grid Manager das Hilfesymbol und dann **API-Dokumentation** aus. Sie können die Metriken im Abschnitt „Metriken“ der Grid Management-API verwenden, um benutzerdefinierte Warnregeln und Dashboards für die Mieteraktivität zu erstellen.

Sehen "Überprüfen der Supportmetriken" für weitere Informationen.

Überwachen Sie S3-Clientvorgänge

Sie können die Aufnahme- und Abrufraten von Objekten sowie Metriken für Objektanzahl, Abfragen und Überprüfung überwachen. Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Clientanwendungen anzeigen, Objekte im StorageGRID -System zu lesen, zu schreiben und zu ändern.

Bevor Sie beginnen

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

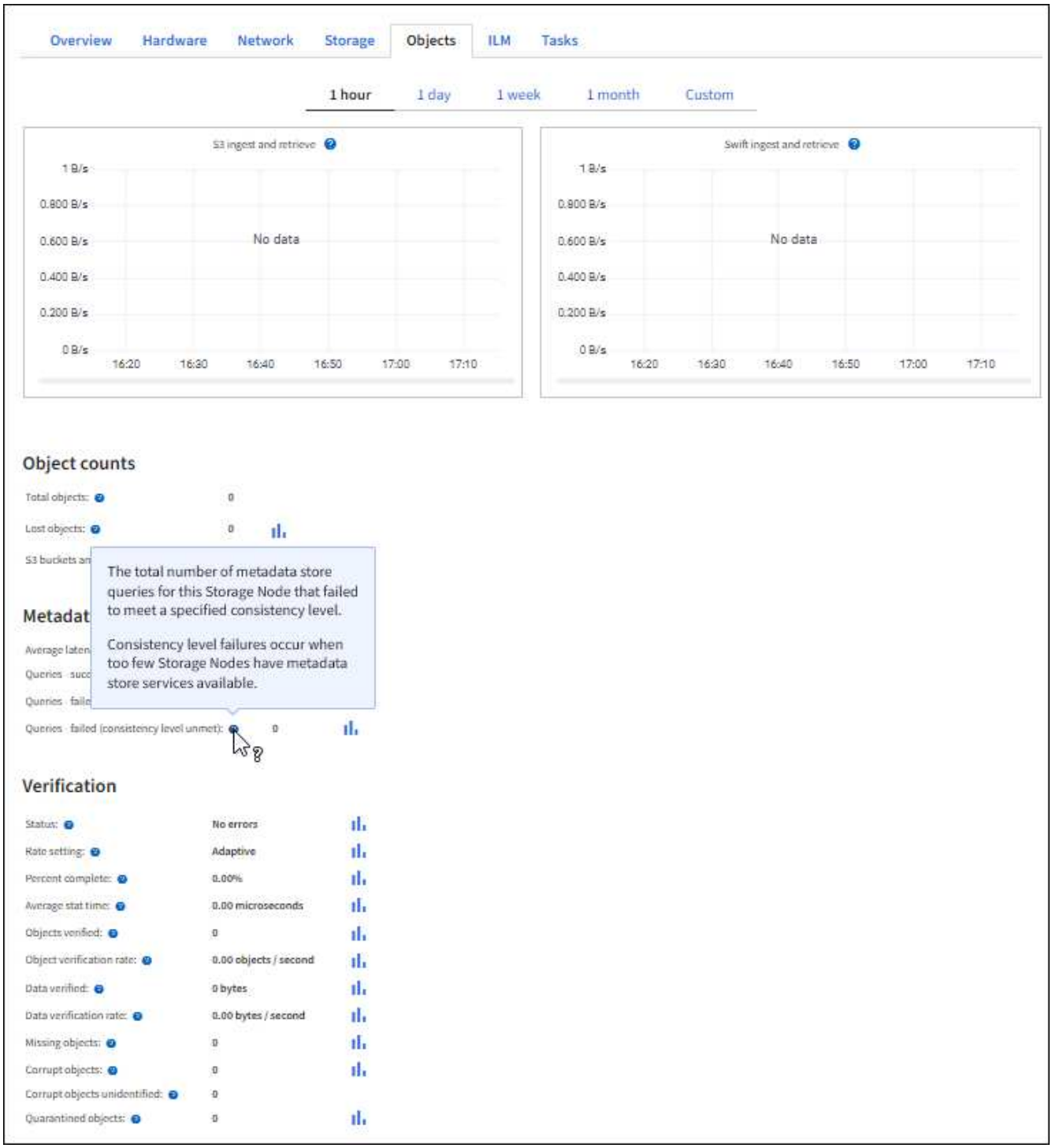
Schritte

1. Wählen Sie im Dashboard die Registerkarte **Leistung** aus.
2. Sehen Sie sich die S3-Diagramme an, die die Anzahl der von Speicherknoten ausgeführten Clientvorgänge und die Anzahl der von Speicherknoten empfangenen API-Anfragen während des ausgewählten Zeitraums zusammenfassen.
3. Wählen Sie **NODES**, um auf die Knotenseite zuzugreifen.
4. Wählen Sie auf der Nodes-Startseite (Rasterebene) die Registerkarte **Objekte** aus.

   Das Diagramm zeigt die S3-Aufnahme- und Abrufraten für Ihr gesamtes StorageGRID System in Bytes pro Sekunde und die Menge der aufgenommenen oder abgerufenen Daten. Sie können ein Zeitintervall auswählen oder ein benutzerdefiniertes Intervall anwenden.

5. Um Informationen zu einem bestimmten Speicherknoten anzuzeigen, wählen Sie den Knoten aus der Liste links aus und wählen Sie die Registerkarte **Objekte**.

   Das Diagramm zeigt die Aufnahme- und Abrufraten für den Knoten. Die Registerkarte enthält auch Metriken für Objektzählungen, Metadatenabfragen und Überprüfungsvorgänge.



Überwachen von Lastausgleichsvorgängen

Wenn Sie einen Load Balancer zum Verwalten von Clientverbindungen zu StorageGRID verwenden, sollten Sie die Load Balancing-Vorgänge überwachen, nachdem Sie das System zum ersten Mal konfiguriert haben und nachdem Sie Konfigurationsänderungen vorgenommen oder eine Erweiterung durchgeführt haben.

Informationen zu diesem Vorgang

Sie können den Load Balancer-Dienst auf Admin-Knoten oder Gateway-Knoten oder einen externen Load Balancer eines Drittanbieters verwenden, um Clientanforderungen auf mehrere Speicherknoten zu verteilen.

Nachdem Sie den Lastenausgleich konfiguriert haben, sollten Sie sicherstellen, dass die Vorgänge zum Aufnehmen und Abrufen von Objekten gleichmäßig auf die Speicherknoten verteilt werden. Durch gleichmäßig verteilte Anfragen wird sichergestellt, dass StorageGRID auch unter Last auf Clientanfragen reagiert und zur Aufrechterhaltung der Clientleistung beitragen kann.

Wenn Sie eine Hochverfügbarkeitsgruppe (HA) aus Gateway-Knoten oder Admin-Knoten im Active-Backup-Modus konfiguriert haben, verteilt nur ein Knoten in der Gruppe aktiv Client-Anfragen.

Weitere Informationen finden Sie unter "Konfigurieren von S3-Clientverbindungen" .

Schritte

1. Wenn S3-Clients über den Load Balancer-Dienst eine Verbindung herstellen, überprüfen Sie, ob Admin-Knoten oder Gateway-Knoten den Datenverkehr wie erwartet aktiv verteilen:
   a. Wählen Sie **NODES**.
   b. Wählen Sie einen Gateway-Knoten oder Admin-Knoten aus.
   c. Überprüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle „Primär“ hat.

      Knoten mit der Rolle „Primär“ und Knoten, die nicht zu einer HA-Gruppe gehören, sollten Anfragen aktiv an Clients verteilen.

   d. Wählen Sie für jeden Knoten, der aktiv Client-Anfragen verteilen soll, die Option"Registerkarte „Load Balancer“" .
   e. Überprüfen Sie das Diagramm des Load Balancer-Anforderungsverkehrs der letzten Woche, um sicherzustellen, dass der Knoten aktiv Anforderungen verteilt hat.

      Knoten in einer Active-Backup-HA-Gruppe können von Zeit zu Zeit die Backup-Rolle übernehmen. Während dieser Zeit verteilen die Knoten keine Clientanforderungen.

   f. Überprüfen Sie das Diagramm der eingehenden Anforderungsrate des Load Balancers für die letzte Woche, um den Objektdurchsatz des Knotens zu überprüfen.
   g. Wiederholen Sie diese Schritte für jeden Admin-Knoten oder Gateway-Knoten im StorageGRID System.
   h. Verwenden Sie optional Richtlinien zur Verkehrsklassifizierung, um eine detailliertere Analyse des vom Load Balancer-Dienst bereitgestellten Verkehrs anzuzeigen.
2. Stellen Sie sicher, dass diese Anfragen gleichmäßig auf die Speicherknoten verteilt werden.
   a. Wählen Sie ***Speicherknoten*** > **LDR** > **HTTP**.
   b. Überprüfen Sie die Anzahl der **derzeit eingerichteten eingehenden Sitzungen**.
   c. Wiederholen Sie dies für jeden Speicherknoten im Raster.

      Die Anzahl der Sitzungen sollte auf allen Speicherknoten ungefähr gleich sein.

Überwachen von Grid-Föderation-Verbindungen

Sie können grundlegende Informationen zu allen"Grid-Föderation-Verbindungen" , detaillierte Informationen zu einer bestimmten Verbindung oder Prometheus-Metriken zu Cross-Grid-Replikationsvorgängen. Sie können eine Verbindung von beiden Rastern aus überwachen.

Bevor Sie beginnen

- Sie sind beim Grid Manager auf einem der beiden Grids mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" für das Raster, bei dem Sie angemeldet sind.

Alle Verbindungen anzeigen

Auf der Seite „Grid-Föderation“ werden grundlegende Informationen zu allen Grid-Föderationsverbindungen und zu allen Mandantenkonten angezeigt, die Grid-Föderationsverbindungen verwenden dürfen.

Schritte

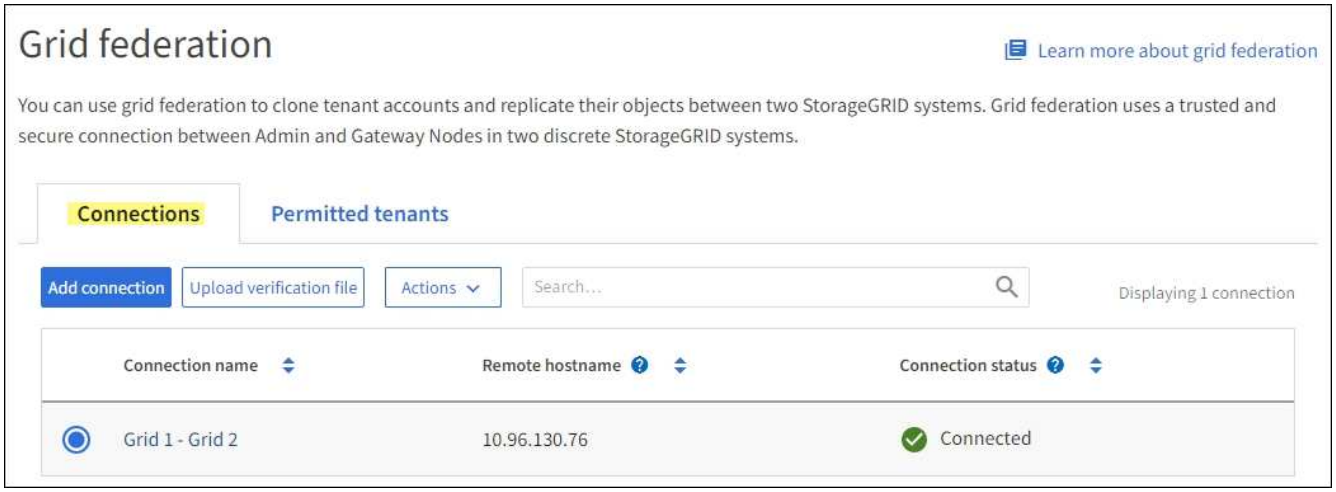
1. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.

   Die Seite „Grid-Föderation“ wird angezeigt.

2. Um grundlegende Informationen zu allen Verbindungen in diesem Raster anzuzeigen, wählen Sie die Registerkarte **Verbindungen**.

   Auf dieser Registerkarte können Sie:

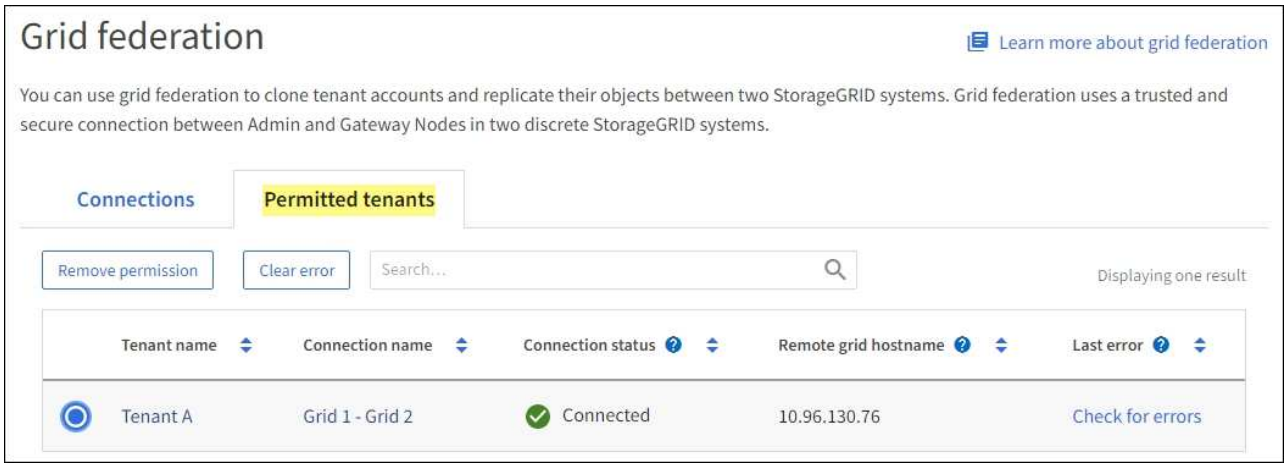
   - "Erstellen einer neuen Verbindung" .
   - Wählen Sie eine bestehende Verbindung aus, um"bearbeiten oder testen" .



3. Um grundlegende Informationen zu allen Mandantenkonten in diesem Raster anzuzeigen, die über die Berechtigung **Rasterföderationsverbindung verwenden** verfügen, wählen Sie die Registerkarte **Zugelassene Mandanten** aus.

   Auf dieser Registerkarte können Sie:

   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an" .
   - Zeigen Sie die Detailseite für jede Verbindung an. Sehen Anzeigen einer bestimmten Verbindung .
   - Wählen Sie einen zulässigen Mieter aus und"die Berechtigung entfernen" .
   - Suchen Sie nach Cross-Grid-Replikationsfehlern und beheben Sie gegebenenfalls den letzten Fehler. Sehen "Beheben von Grid-Föderationsfehlern" .



Eine bestimmte Verbindung anzeigen

Sie können Details zu einer bestimmten Grid-Föderation-Verbindung anzeigen.

Schritte

1. Wählen Sie auf der Grid-Föderationsseite eine der Registerkarten aus und wählen Sie dann den Verbindungsnamen aus der Tabelle aus.

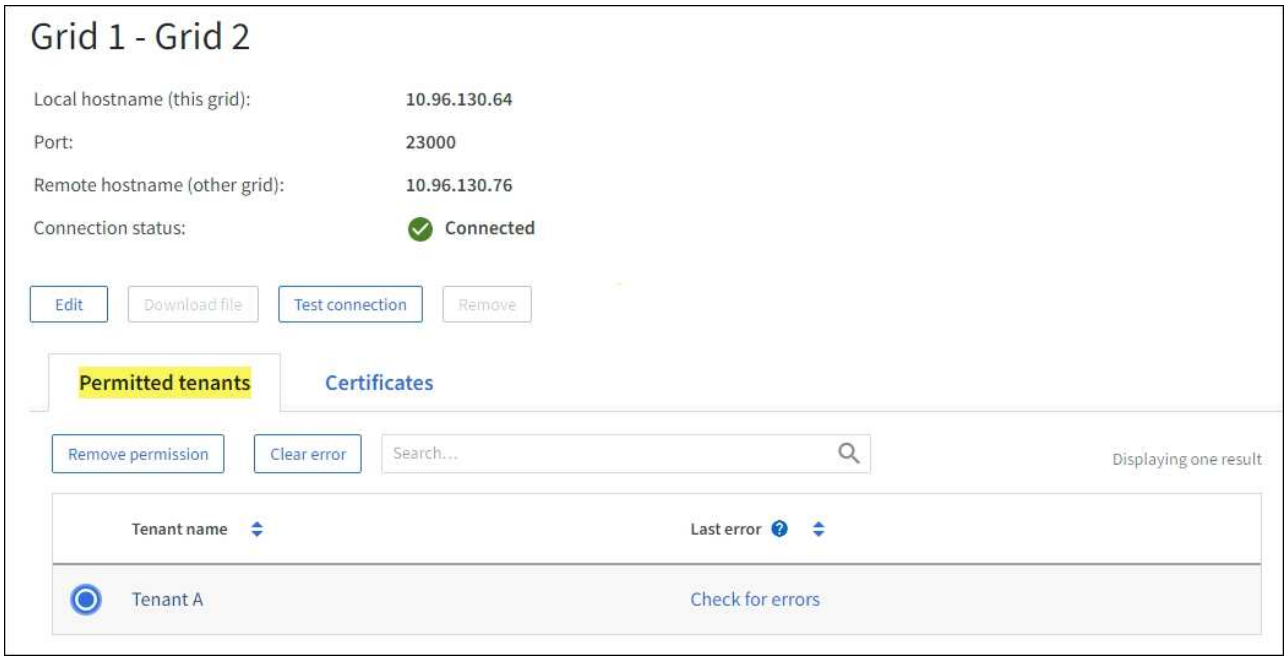
   Auf der Detailseite der Verbindung können Sie:

   - Sehen Sie sich grundlegende Statusinformationen zur Verbindung an, einschließlich der lokalen und Remote-Hostnamen, des Ports und des Verbindungsstatus.
   - Wählen Sie eine Verbindung zu"bearbeiten, testen oder entfernen" .

2. Wählen Sie beim Anzeigen einer bestimmten Verbindung die Registerkarte **Zulässige Mandanten** aus, um Details zu den zulässigen Mandanten für die Verbindung anzuzeigen.

   Auf dieser Registerkarte können Sie:

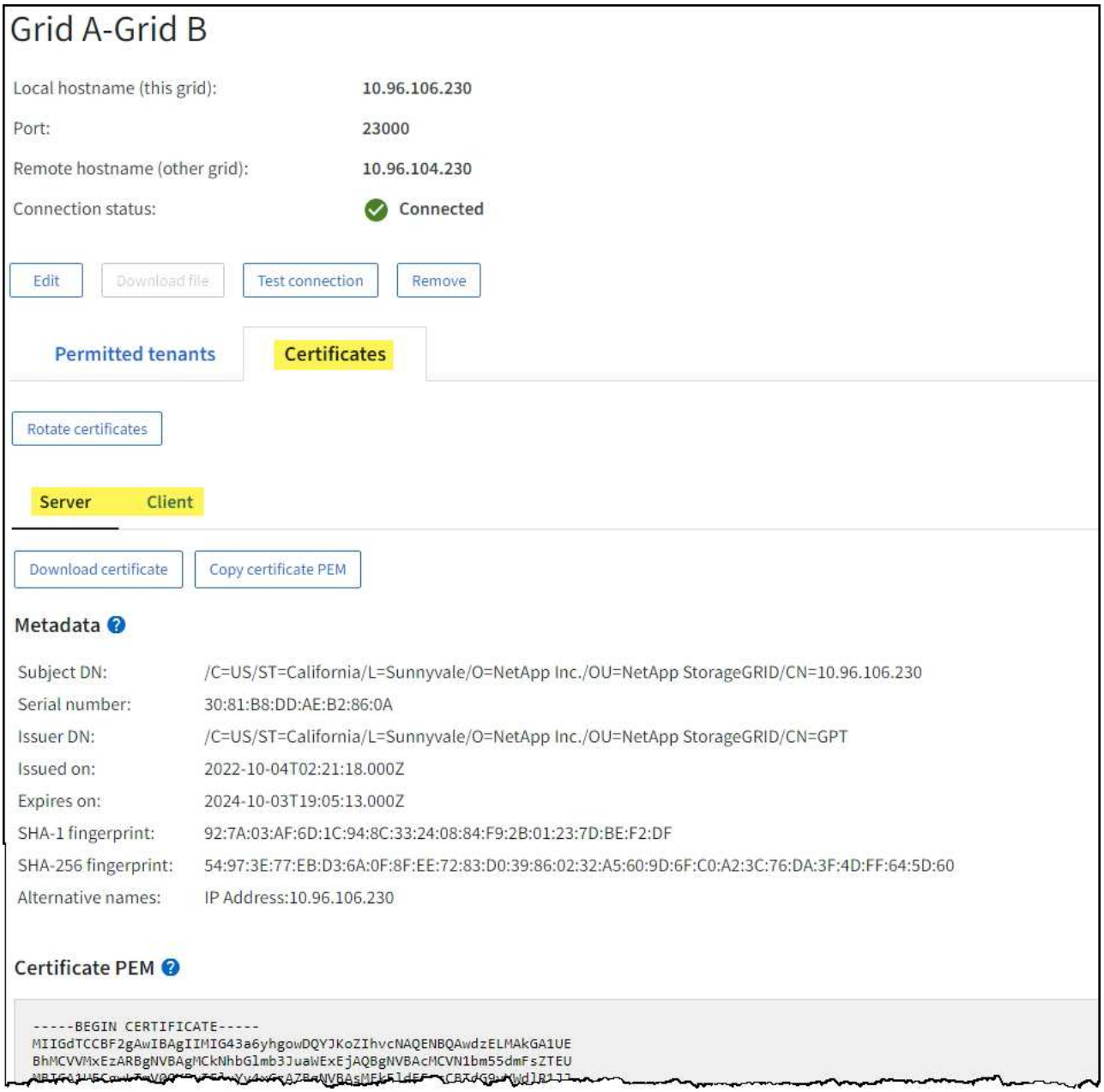
   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an" .
   - "Entfernen der Berechtigung eines Mandanten"um die Verbindung zu nutzen.
   - Suchen Sie nach Cross-Grid-Replikationsfehlern und beheben Sie den letzten Fehler. Sehen "Beheben von Grid-Föderationsfehlern" .



3. Wählen Sie beim Anzeigen einer bestimmten Verbindung die Registerkarte **Zertifikate** aus, um die vom System generierten Server- und Client-Zertifikate für diese Verbindung anzuzeigen.

   Auf dieser Registerkarte können Sie:

   - "Verbindungszertifikate rotieren" .
   - Wählen Sie **Server** oder **Client**, um das zugehörige Zertifikat anzuzeigen oder herunterzuladen oder das Zertifikat PEM zu kopieren.



Überprüfen der Cross-Grid-Replikationsmetriken

Sie können das Cross-Grid-Replication-Dashboard in Grafana verwenden, um Prometheus-Metriken zu Cross-Grid-Replikationsvorgängen in Ihrem Grid anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **SUPPORT** > **Tools** > **Metriken**.

   Die auf der Seite „Metriken“ verfügbaren Tools sind für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe die Liste der"häufig verwendete Prometheus-Metriken" .

2. Wählen Sie im Abschnitt „Grafana“ der Seite **Cross Grid Replication** aus.

   Ausführliche Anweisungen finden Sie unter"Überprüfen der Supportmetriken" .

3. Um die Replikation von Objekten, deren Replikation fehlgeschlagen ist, erneut zu versuchen, siehe"Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge" .

Verwalten von Warnungen

Verwalten von Warnungen

Das Warnsystem bietet eine benutzerfreundliche Schnittstelle zum Erkennen, Bewerten und Beheben von Problemen, die während des StorageGRID -Betriebs auftreten können.

Warnungen werden bei bestimmten Schweregraden ausgelöst, wenn die Bedingungen der Warnungsregel als wahr ausgewertet werden. Wenn eine Warnung ausgelöst wird, werden die folgenden Aktionen ausgeführt:

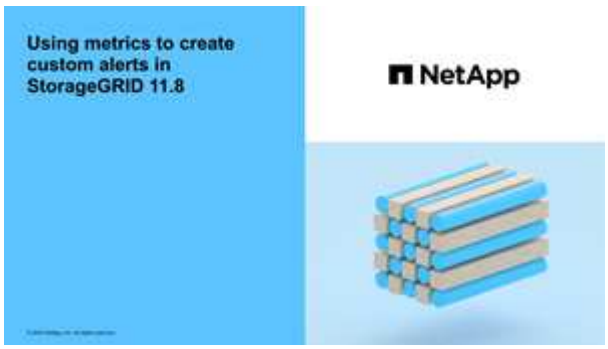
- Auf dem Dashboard im Grid Manager wird ein Symbol für den Schweregrad der Warnung angezeigt und die Anzahl der aktuellen Warnungen wird erhöht.
- Die Warnung wird auf der Übersichtsseite **NODES** und auf der Registerkarte **NODES** > ***node*** > **Übersicht** angezeigt.
- Vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und E-Mail-Adressen für die Empfänger angegeben, wird eine E-Mail-Benachrichtigung gesendet.
- Vorausgesetzt, Sie haben den StorageGRID SNMP-Agenten konfiguriert, wird eine SNMP-Benachrichtigung (Simple Network Management Protocol) gesendet.

Sie können benutzerdefinierte Warnungen erstellen, Warnungen bearbeiten oder deaktivieren und Warnbenachrichtigungen verwalten.

Weitere Informationen:

- Sehen Sie sich das Video an: "Video: Übersicht über Warnungen"

- Sehen Sie sich das Video an: "Video: Benutzerdefinierte Benachrichtigungen"



- Siehe die"Warnungsreferenz" .

Anzeigen von Warnregeln

Warnregeln definieren die Bedingungen, die auslösen"spezifische Warnungen" . StorageGRID enthält eine Reihe von Standard-Alarmregeln, die Sie unverändert verwenden oder ändern können, oder Sie können benutzerdefinierte Alarmregeln erstellen.

Sie können die Liste aller standardmäßigen und benutzerdefinierten Warnregeln anzeigen, um zu erfahren, welche Bedingungen die einzelnen Warnmeldungen auslösen und um zu sehen, ob Warnmeldungen deaktiviert sind.

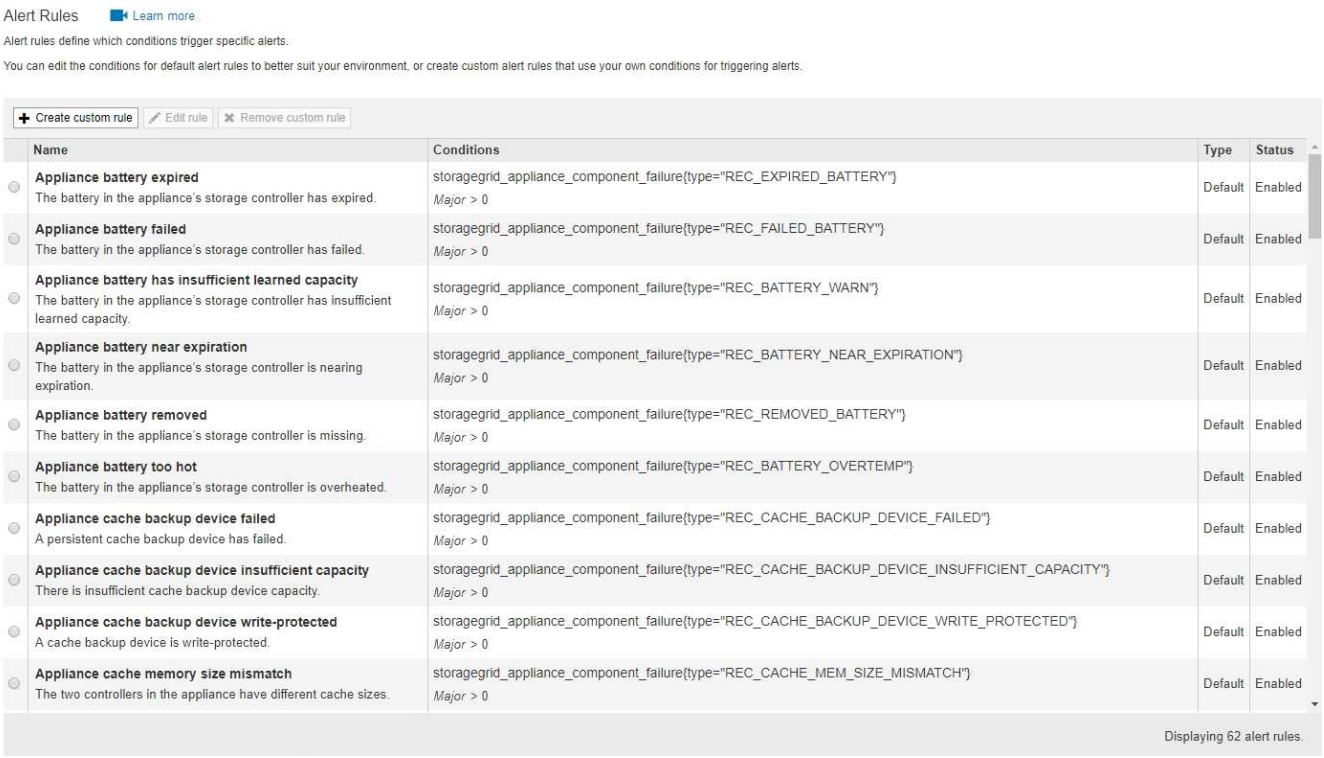
Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .
- Optional haben Sie das Video angesehen: "Video: Übersicht über Warnungen"

Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.



2. Überprüfen Sie die Informationen in der Tabelle mit den Warnregeln:

Spaltenüberschrift	Beschreibung
Name	Der eindeutige Name und die Beschreibung der Warnregel. Benutzerdefinierte Warnregeln werden zuerst aufgeführt, gefolgt von Standardwarnregeln. Der Name der Warnregel ist der Betreff für E-Mail-Benachrichtigungen.

Spaltenüberschrift	Beschreibung
Bedingungen	Die Prometheus-Ausdrücke, die bestimmen, wann dieser Alarm ausgelöst wird. Ein Alarm kann bei einem oder mehreren der folgenden Schweregrade ausgelöst werden, es ist jedoch nicht für jeden Schweregrad eine Bedingung erforderlich. • *Kritisch* : Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort angehen. Wenn das Problem nicht behoben wird, kann es zu Dienstunterbrechungen und Datenverlust kommen. • *Wesentlich* : Es liegt ein anormaler Zustand vor, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten wichtige Warnungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder -Dienstes nicht stoppt. • *Unerheblich* : Das System funktioniert normal, es liegt jedoch ein anormaler Zustand vor, der die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn er anhält. Sie sollten kleinere Warnungen, die nicht von selbst verschwinden, überwachen und beheben, um sicherzustellen, dass sie nicht zu einem ernsteren Problem führen.
Typ	Der Typ der Warnregel: • **Standard**: Eine mit dem System bereitgestellte Warnregel. Sie können eine Standardwarnregel deaktivieren oder die Bedingungen und die Dauer einer Standardwarnregel bearbeiten. Sie können eine Standardwarnregel nicht entfernen. • **Standard***: Eine Standardwarnregel, die eine bearbeitete Bedingung oder Dauer enthält. Bei Bedarf können Sie einen geänderten Zustand problemlos wieder auf den ursprünglichen Standard zurücksetzen. • **Benutzerdefiniert**: Eine von Ihnen erstellte Warnregel. Sie können benutzerdefinierte Warnregeln deaktivieren, bearbeiten und entfernen.
Status	Ob diese Warnregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnregeln werden nicht ausgewertet, daher werden keine Warnmeldungen ausgelöst.

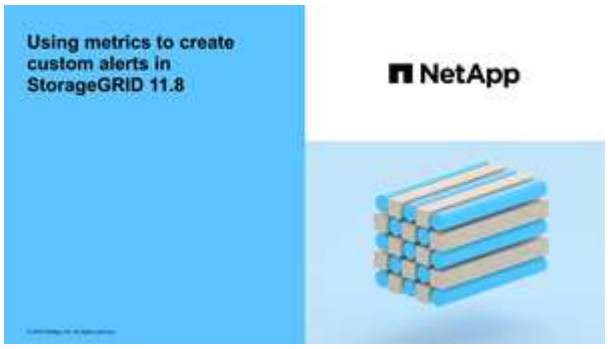
Erstellen Sie benutzerdefinierte Warnregeln

Sie können benutzerdefinierte Warnregeln erstellen, um Ihre eigenen Bedingungen zum Auslösen von Warnmeldungen festzulegen.

Bevor Sie beginnen

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

- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .
- Sie kennen die"häufig verwendete Prometheus-Metriken" .
- Sie verstehen die "Syntax von Prometheus-Abfragen" .
- Optional haben Sie das Video angesehen: "Video: Benutzerdefinierte Benachrichtigungen" .



Informationen zu diesem Vorgang

StorageGRID validiert keine benutzerdefinierten Warnungen. Wenn Sie benutzerdefinierte Warnregeln erstellen möchten, befolgen Sie diese allgemeinen Richtlinien:

- Sehen Sie sich die Bedingungen für die Standardwarnregeln an und verwenden Sie sie als Beispiele für Ihre benutzerdefinierten Warnregeln.
- Wenn Sie mehr als eine Bedingung für eine Warnregel definieren, verwenden Sie für alle Bedingungen denselben Ausdruck. Ändern Sie dann den Schwellenwert für jede Bedingung.
- Überprüfen Sie jede Bedingung sorgfältig auf Tipp- und Logikfehler.
- Verwenden Sie nur die in der Grid Management API aufgeführten Metriken.
- Beachten Sie beim Testen eines Ausdrucks mithilfe der Grid Management API, dass eine „erfolgreiche“ Antwort ein leerer Antworttext sein kann (keine Warnung ausgelöst). Um zu sehen, ob der Alarm tatsächlich ausgelöst wird, können Sie vorübergehend einen Schwellenwert auf einen Wert festlegen, von dem Sie derzeit erwarten, dass er zutrifft.

  Um beispielsweise den Ausdruck zu testen `node_memory_MemTotal_bytes < 24000000000` , führen Sie zuerst `node_memory_MemTotal_bytes >= 0` und stellen Sie sicher, dass Sie die erwarteten Ergebnisse erhalten (alle Knoten geben einen Wert zurück). Ändern Sie dann den Operator und den Schwellenwert wieder auf die beabsichtigten Werte und führen Sie die Ausführung erneut aus. Keine Ergebnisse zeigen an, dass für diesen Ausdruck keine aktuellen Warnungen vorliegen.

- Gehen Sie nicht davon aus, dass eine benutzerdefinierte Warnung funktioniert, es sei denn, Sie haben überprüft, dass die Warnung zum erwarteten Zeitpunkt ausgelöst wird.

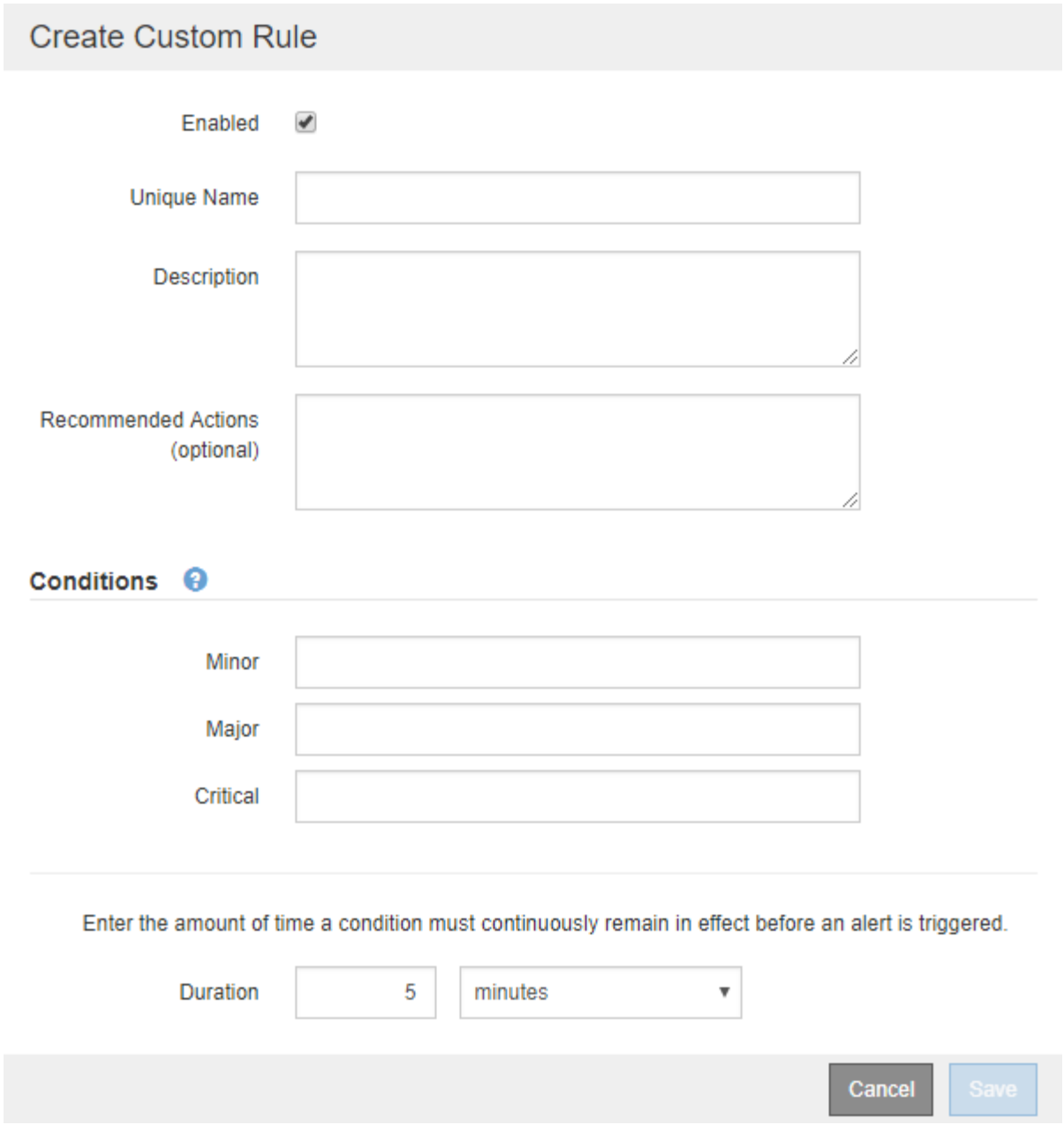
Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie **Benutzerdefinierte Regel erstellen**.

   Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.



3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktiviert**, um festzustellen, ob diese Warnregel derzeit aktiviert ist.

   Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

4. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Warnregel wird auf der Seite „Warnungen“ angezeigt und ist auch der Betreff für E-Mail-Benachrichtigungen. Namen für Warnregeln können zwischen 1 und 64 Zeichen lang sein.

Feld	Beschreibung
Beschreibung	Eine Beschreibung des auftretenden Problems. Die Beschreibung ist die Warnmeldung, die auf der Warnseite und in E-Mail-Benachrichtigungen angezeigt wird. Beschreibungen für Warnregeln können zwischen 1 und 128 Zeichen lang sein.
Empfohlene Maßnahmen	Optional die empfohlenen Maßnahmen, die ergriffen werden sollen, wenn diese Warnung ausgelöst wird. Geben Sie empfohlene Aktionen als einfachen Text ein (keine Formatierungscodes). Empfohlene Aktionen für Warnregeln können zwischen 0 und 1.024 Zeichen lang sein.

5. Geben Sie im Abschnitt „Bedingungen“ einen Prometheus-Ausdruck für einen oder mehrere Schweregrade der Warnung ein.

   Ein einfacher Ausdruck hat normalerweise die Form:

   ```
   [metric] [operator] [value]
   ```

   Ausdrücke können beliebig lang sein, werden in der Benutzeroberfläche jedoch in einer einzigen Zeile angezeigt. Mindestens ein Ausdruck ist erforderlich.

   Dieser Ausdruck bewirkt, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Knoten weniger als 24.000.000.000 Byte (24 GB) beträgt.

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Um verfügbare Metriken anzuzeigen und Prometheus-Ausdrücke zu testen, wählen Sie das Hilfesymbol und folgen Sie dem Link zum Abschnitt „Metriken“ der Grid Management API.

6. Geben Sie im Feld **Dauer** die Zeitspanne ein, die eine Bedingung kontinuierlich wirksam bleiben muss, bevor der Alarm ausgelöst wird, und wählen Sie eine Zeiteinheit aus.

   Um sofort einen Alarm auszulösen, wenn eine Bedingung erfüllt wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass vorübergehende Bedingungen Warnungen auslösen.

   Der Standardwert beträgt 5 Minuten.

7. Wählen Sie **Speichern**.

   Das Dialogfeld wird geschlossen und die neue benutzerdefinierte Warnregel wird in der Tabelle „Warnregeln“ angezeigt.

Alarmregeln bearbeiten

Sie können eine Warnregel bearbeiten, um die Auslösebedingungen zu ändern. Bei einer benutzerdefinierten Warnregel können Sie auch den Regelnamen, die Beschreibung und die empfohlenen Aktionen aktualisieren.

Bevor Sie beginnen

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

- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Wenn Sie eine Standardwarnregel bearbeiten, können Sie die Bedingungen für geringfügige, schwerwiegende und kritische Warnungen sowie die Dauer ändern. Wenn Sie eine benutzerdefinierte Warnregel bearbeiten, können Sie auch den Namen, die Beschreibung und die empfohlenen Aktionen der Regel bearbeiten.

> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel zu bearbeiten. Wenn Sie Triggerwerte ändern, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

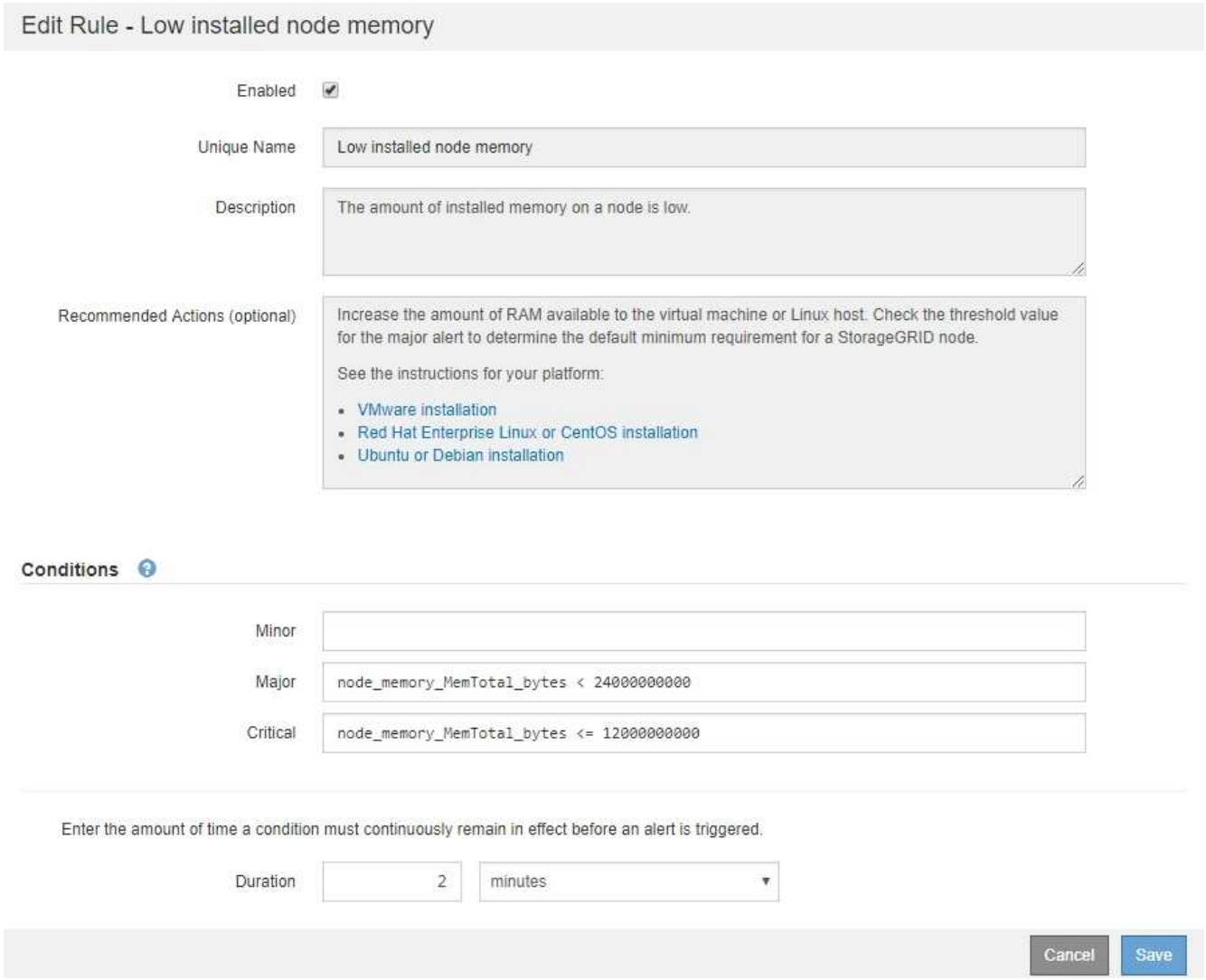
Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnregel aus, die Sie bearbeiten möchten.
3. Wählen Sie **Regel bearbeiten**.

   Das Dialogfeld „Regel bearbeiten“ wird angezeigt. Dieses Beispiel zeigt eine Standardwarnregel – die Felder „Eindeutiger Name“, „Beschreibung“ und „Empfohlene Aktionen“ sind deaktiviert und können nicht bearbeitet werden.



4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktiviert**, um festzustellen, ob diese Warnregel derzeit aktiviert ist.

   Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

   Wenn Sie die Warnregel für eine aktuelle Warnmeldung deaktivieren, müssen Sie einige Minuten warten, bis die Warnmeldung nicht mehr als aktive Warnmeldung angezeigt wird.

   Im Allgemeinen wird das Deaktivieren einer Standardwarnregel nicht empfohlen. Wenn eine Warnregel deaktiviert ist, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

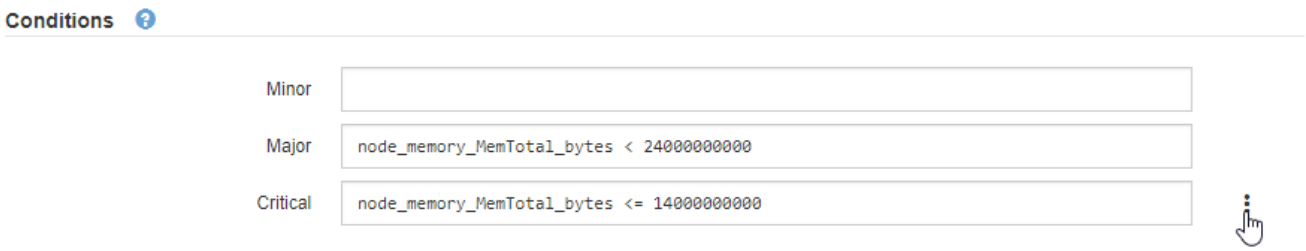
5. Aktualisieren Sie für benutzerdefinierte Warnregeln die folgenden Informationen nach Bedarf.

   Sie können diese Informationen für Standardwarnregeln nicht bearbeiten.

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Warnregel wird auf der Seite „Warnungen“ angezeigt und ist auch der Betreff für E-Mail-Benachrichtigungen. Namen für Warnregeln können zwischen 1 und 64 Zeichen lang sein.
Beschreibung	Eine Beschreibung des auftretenden Problems. Die Beschreibung ist die Warnmeldung, die auf der Warnseite und in E-Mail-Benachrichtigungen angezeigt wird. Beschreibungen für Warnregeln können zwischen 1 und 128 Zeichen lang sein.
Empfohlene Maßnahmen	Optional die empfohlenen Maßnahmen, die ergriffen werden sollen, wenn diese Warnung ausgelöst wird. Geben Sie empfohlene Aktionen als einfachen Text ein (keine Formatierungscodes). Empfohlene Aktionen für Warnregeln können zwischen 0 und 1.024 Zeichen lang sein.

6. Geben Sie im Abschnitt „Bedingungen“ den Prometheus-Ausdruck für einen oder mehrere Schweregrade der Warnung ein oder aktualisieren Sie ihn.

Wenn Sie eine Bedingung für eine bearbeitete Standardwarnregel auf ihren ursprünglichen Wert zurücksetzen möchten, wählen Sie die drei Punkte rechts neben der geänderten Bedingung aus.



Wenn Sie die Bedingungen für eine aktuelle Warnung aktualisieren, werden Ihre Änderungen möglicherweise erst implementiert, wenn die vorherige Bedingung behoben ist. Wenn das nächste Mal eine der Bedingungen für die Regel erfüllt ist, spiegelt die Warnung die aktualisierten Werte wider.

Ein einfacher Ausdruck hat normalerweise die Form:

```
[metric] [operator] [value]
```

Ausdrücke können beliebig lang sein, werden in der Benutzeroberfläche jedoch in einer einzigen Zeile angezeigt. Mindestens ein Ausdruck ist erforderlich.

Dieser Ausdruck bewirkt, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Knoten weniger als 24.000.000.000 Byte (24 GB) beträgt.

```
node_memory_MemTotal_bytes < 24000000000
```

7. Geben Sie im Feld **Dauer** die Zeitspanne ein, die eine Bedingung kontinuierlich wirksam bleiben muss,

bevor der Alarm ausgelöst wird, und wählen Sie die Zeiteinheit aus.

Um sofort einen Alarm auszulösen, wenn eine Bedingung erfüllt wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass vorübergehende Bedingungen Warnungen auslösen.

Der Standardwert beträgt 5 Minuten.

8. Wählen Sie **Speichern**.

   Wenn Sie eine Standardwarnregel bearbeitet haben, wird **Standard*** in der Spalte Typ angezeigt. Wenn Sie eine standardmäßige oder benutzerdefinierte Warnregel deaktiviert haben, wird in der Spalte **Status** **Deaktiviert** angezeigt.

Warnregeln deaktivieren

Sie können den aktivierten/deaktivierten Status für eine Standard- oder benutzerdefinierte Warnregel ändern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

> Im Allgemeinen wird das Deaktivieren einer Standardwarnregel nicht empfohlen. Wenn eine Warnregel deaktiviert ist, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnregel aus, die Sie deaktivieren oder aktivieren möchten.
3. Wählen Sie **Regel bearbeiten**.

   Das Dialogfeld „Regel bearbeiten“ wird angezeigt.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktiviert**, um festzustellen, ob diese Warnregel derzeit aktiviert ist.

   Wenn eine Warnregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

   > Wenn Sie die Warnregel für eine aktuelle Warnmeldung deaktivieren, müssen Sie einige Minuten warten, bis die Warnmeldung nicht mehr als aktive Warnmeldung angezeigt wird.

5. Wählen Sie **Speichern**.

   Deaktiviert wird in der Spalte **Status** angezeigt.

Entfernen benutzerdefinierter Warnregeln

Sie können eine benutzerdefinierte Warnregel entfernen, wenn Sie sie nicht mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **WARNUNGEN** > **Regeln**.

   Die Seite „Warnregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die benutzerdefinierte Warnregel aus, die Sie entfernen möchten.

   Sie können eine Standardwarnregel nicht entfernen.

3. Wählen Sie **Benutzerdefinierte Regel entfernen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **OK**, um die Warnregel zu entfernen.

   Alle aktiven Instanzen der Warnung werden innerhalb von 10 Minuten behoben.

Verwalten von Warnbenachrichtigungen

SNMP-Benachrichtigungen für Warnungen einrichten

Wenn StorageGRID beim Auftreten von Warnungen SNMP-Benachrichtigungen senden soll, müssen Sie den StorageGRID SNMP-Agenten aktivieren und ein oder mehrere Trap-Ziele konfigurieren.

Sie können die Option **KONFIGURATION** > **Überwachung** > **SNMP-Agent** im Grid Manager oder die SNMP-Endpunkte für die Grid Management-API verwenden, um den StorageGRID SNMP-Agenten zu aktivieren und zu konfigurieren. Der SNMP-Agent unterstützt alle drei Versionen des SNMP-Protokolls.

Informationen zur Konfiguration des SNMP-Agenten finden Sie unter"Verwenden Sie die SNMP-Überwachung" .

Nachdem Sie den StorageGRID SNMP-Agenten konfiguriert haben, können zwei Arten ereignisgesteuerter Benachrichtigungen gesendet werden:

- Traps sind vom SNMP-Agenten gesendete Benachrichtigungen, die keine Bestätigung durch das Verwaltungssystem erfordern. Traps dienen dazu, das Verwaltungssystem darüber zu informieren, dass in StorageGRID etwas passiert ist, beispielsweise dass ein Alarm ausgelöst wurde. Traps werden in allen drei Versionen von SNMP unterstützt.
- Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Wenn der SNMP-Agent innerhalb einer bestimmten Zeitspanne keine Bestätigung erhält, sendet er die Information erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist. Informs werden in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden gesendet, wenn ein Standard- oder benutzerdefinierter Alarm mit einem beliebigen Schweregrad ausgelöst wird. Um SNMP-Benachrichtigungen für einen Alarm zu unterdrücken, müssen Sie eine Stummschaltung für den Alarm konfigurieren. Sehen "Warnmeldungen stummschalten" .

Wenn Ihre StorageGRID -Bereitstellung mehrere Admin-Knoten umfasst, ist der primäre Admin-Knoten der bevorzugte Absender für Warnbenachrichtigungen, AutoSupport -Pakete sowie SNMP-Traps und -Informationen. Wenn der primäre Admin-Knoten nicht verfügbar ist, werden Benachrichtigungen vorübergehend von anderen Admin-Knoten gesendet. Sehen "Was ist ein Admin-Knoten?" .

E-Mail-Benachrichtigungen für Warnmeldungen einrichten

Wenn Sie beim Auftreten von Warnmeldungen E-Mail-Benachrichtigungen erhalten möchten, müssen Sie Informationen zu Ihrem SMTP-Server angeben. Sie müssen auch die E-Mail-Adressen der Empfänger von Warnbenachrichtigungen eingeben.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Das für Warnbenachrichtigungen verwendete E-Mail-Setup wird für AutoSupport Pakete nicht verwendet. Sie können jedoch für alle Benachrichtigungen denselben E-Mail-Server verwenden.

Wenn Ihre StorageGRID -Bereitstellung mehrere Admin-Knoten umfasst, ist der primäre Admin-Knoten der bevorzugte Absender für Warnbenachrichtigungen, AutoSupport -Pakete sowie SNMP-Traps und -Informationen. Wenn der primäre Admin-Knoten nicht verfügbar ist, werden Benachrichtigungen vorübergehend von anderen Admin-Knoten gesendet. Sehen "Was ist ein Admin-Knoten?" .

Schritte

1. Wählen Sie **WARNUNGEN** > **E-Mail-Setup**.

   Die Seite „E-Mail-Setup“ wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, um anzugeben, dass Benachrichtigungs-E-Mails gesendet werden sollen, wenn Warnungen konfigurierte Schwellenwerte erreichen.

   Die Abschnitte „E-Mail-Server (SMTP)“, „Transport Layer Security (TLS), E-Mail-Adressen“ und „Filter“ werden angezeigt.

3. Geben Sie im Abschnitt „E-Mail-Server (SMTP)“ die Informationen ein, die StorageGRID für den Zugriff auf Ihren SMTP-Server benötigt.

   Wenn Ihr SMTP-Server eine Authentifizierung erfordert, müssen Sie sowohl einen Benutzernamen als auch ein Kennwort angeben.

Feld	Eingeben
Mailserver	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des SMTP-Servers.

Feld	Eingeben
Hafen	Der für den Zugriff auf den SMTP-Server verwendete Port. Muss zwischen 1 und 65535 liegen.
Benutzername (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen zur Authentifizierung ein.
Passwort (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie das Kennwort zur Authentifizierung ein.

4. Geben Sie im Abschnitt „E-Mail-Adressen“ die E-Mail-Adressen des Absenders und aller Empfänger ein.
   a. Geben Sie für die **E-Mail-Adresse des Absenders** eine gültige E-Mail-Adresse an, die als Absenderadresse für Warnbenachrichtigungen verwendet werden soll.

      Beispiel: `storagegrid-alerts@example.com`

   b. Geben Sie im Abschnitt „Empfänger“ für jede E-Mail-Liste oder Person eine E-Mail-Adresse ein, die bei Auftreten einer Warnung eine E-Mail erhalten soll.

      Wählen Sie das Plus-Symbol ➕ um Empfänger hinzuzufügen.

5. Wenn für die Kommunikation mit dem SMTP-Server Transport Layer Security (TLS) erforderlich ist, wählen Sie im Abschnitt Transport Layer Security (TLS) die Option **TLS erforderlich** aus.
   a. Geben Sie im Feld **CA-Zertifikat** das CA-Zertifikat ein, das zur Überprüfung der Identität des SMTP-Servers verwendet wird.

      Sie können den Inhalt kopieren und in dieses Feld einfügen oder **Durchsuchen** auswählen und die Datei auswählen.

      Sie müssen eine einzelne Datei bereitstellen, die die Zertifikate jeder zwischengeschalteten ausstellenden Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

   b. Aktivieren Sie das Kontrollkästchen **Client-Zertifikat senden**, wenn Ihr SMTP-E-Mail-Server von E-Mail-Absendern die Bereitstellung von Client-Zertifikaten zur Authentifizierung erfordert.
   c. Geben Sie im Feld **Client-Zertifikat** das PEM-codierte Client-Zertifikat ein, das an den SMTP-Server gesendet werden soll.

      Sie können den Inhalt kopieren und in dieses Feld einfügen oder **Durchsuchen** auswählen und die Datei auswählen.

   d. Geben Sie im Feld **Privater Schlüssel** den privaten Schlüssel für das Client-Zertifikat in unverschlüsselter PEM-Kodierung ein.

      Sie können den Inhalt kopieren und in dieses Feld einfügen oder **Durchsuchen** auswählen und die Datei auswählen.

> ⓘ Wenn Sie die E-Mail-Einstellungen bearbeiten müssen, wählen Sie das Bleistiftsymbol um dieses Feld zu aktualisieren.

6. Wählen Sie im Abschnitt „Filter“ aus, welche Warnschweregrade zu E-Mail-Benachrichtigungen führen sollen, es sei denn, die Regel für eine bestimmte Warnmeldung wurde stummgeschaltet.

Schwere	Beschreibung
Geringfügig, schwerwiegend, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die geringfügige, schwerwiegende oder kritische Bedingung für eine Warnregel erfüllt ist.
Schwerwiegend, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die schwerwiegende oder kritische Bedingung für eine Warnregel erfüllt ist. Bei geringfügigen Warnungen werden keine Benachrichtigungen gesendet.
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur gesendet, wenn die kritische Bedingung für eine Warnregel erfüllt ist. Für kleinere oder größere Warnungen werden keine Benachrichtigungen gesendet.

7. Wenn Sie bereit sind, Ihre E-Mail-Einstellungen zu testen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **Test-E-Mail senden**.

      Es wird eine Bestätigungsmeldung angezeigt, die darauf hinweist, dass eine Test-E-Mail gesendet wurde.

   b. Überprüfen Sie die Posteingänge aller E-Mail-Empfänger und bestätigen Sie, dass eine Test-E-Mail empfangen wurde.

      Wenn die E-Mail nicht innerhalb weniger Minuten eingeht oder die Warnung **Fehler bei E-Mail-Benachrichtigung** ausgelöst wird, überprüfen Sie Ihre Einstellungen und versuchen Sie es erneut.

   c. Sign in und senden Sie eine Test-E-Mail, um die Konnektivität von allen Sites zu überprüfen.

      Wenn Sie Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Konnektivität zu überprüfen. Dies steht im Gegensatz zum Testen von AutoSupport -Paketen, bei dem alle Admin-Knoten die Test-E-Mail senden.

8. Wählen Sie **Speichern**.

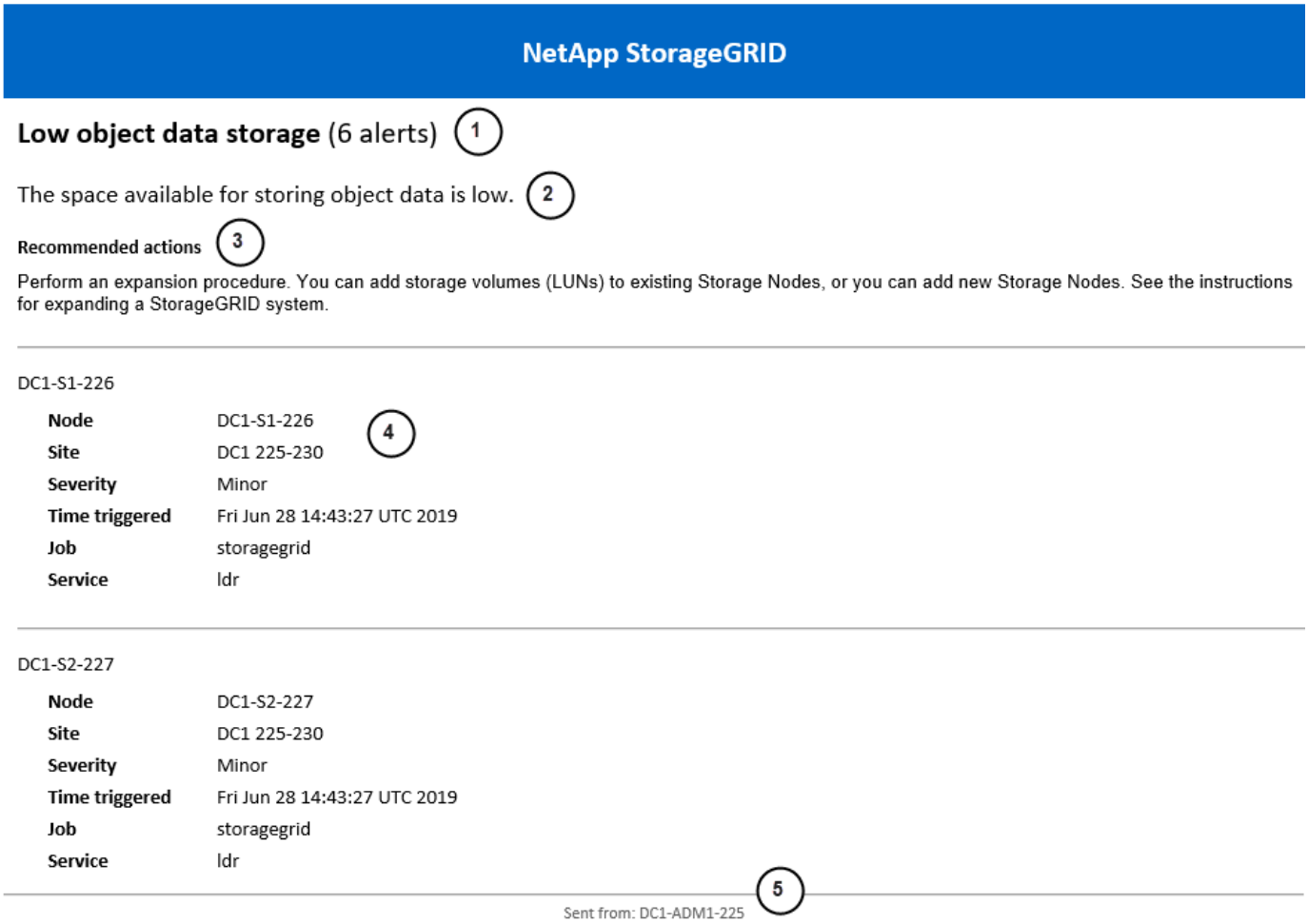
   Durch das Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Sie müssen **Speichern** auswählen.

   Die E-Mail-Einstellungen werden gespeichert.

In E-Mail-Benachrichtigungen enthaltene Informationen

Nachdem Sie den SMTP-E-Mail-Server konfiguriert haben, werden E-Mail-Benachrichtigungen an die angegebenen Empfänger gesendet, wenn eine Warnung ausgelöst wird, es sei denn, die Warnungsregel wird durch eine Stummschaltung unterdrückt. Sehen "Warnmeldungen stummschalten" .

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



Aufbieten, ausrufen, zurufen	Beschreibung
1	Der Name der Warnung, gefolgt von der Anzahl der aktiven Instanzen dieser Warnung.
2	Die Beschreibung der Warnung.
3	Alle empfohlenen Maßnahmen für die Warnung.
4	Details zu jeder aktiven Instanz der Warnung, einschließlich des betroffenen Knotens und der betroffenen Site, des Schweregrads der Warnung, der UTC-Zeit, zu der die Warnungsregel ausgelöst wurde, und des Namens des betroffenen Auftrags und Dienstes.
5	Der Hostname des Admin-Knotens, der die Benachrichtigung gesendet hat.

So werden Warnungen gruppiert

Um zu verhindern, dass beim Auslösen von Warnungen eine übermäßige Anzahl von E-Mail-Benachrichtigungen gesendet wird, versucht StorageGRID , mehrere Warnungen in derselben Benachrichtigung zu gruppieren.

In der folgenden Tabelle finden Sie Beispiele dafür, wie StorageGRID mehrere Warnungen in E-Mail-

Benachrichtigungen gruppiert.

Verhalten	Beispiel
Jede Warnmeldung gilt nur für Warnmeldungen mit demselben Namen. Wenn zwei Warnungen mit unterschiedlichen Namen gleichzeitig ausgelöst werden, werden zwei E-Mail-Benachrichtigungen gesendet.	• Alarm A wird auf zwei Knoten gleichzeitig ausgelöst. Es wird nur eine Benachrichtigung gesendet. • Alarm A wird auf Knoten 1 ausgelöst und Alarm B wird gleichzeitig auf Knoten 2 ausgelöst. Es werden zwei Benachrichtigungen gesendet – eine für jeden Alarm.
Wenn bei einer bestimmten Warnung auf einem bestimmten Knoten die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird nur für die Warnung mit dem höchsten Schweregrad eine Benachrichtigung gesendet.	• Alarm A wird ausgelöst und die Schwellenwerte für geringfügige, schwerwiegende und kritische Alarme werden erreicht. Für den kritischen Alarm wird eine Benachrichtigung gesendet.
Wenn zum ersten Mal ein Alarm ausgelöst wird, wartet StorageGRID 2 Minuten, bevor eine Benachrichtigung gesendet wird. Wenn während dieser Zeit andere Warnungen mit demselben Namen ausgelöst werden, gruppiert StorageGRID alle Warnungen in der ersten Benachrichtigung.	1. Alarm A wird um 08:00 Uhr auf Knoten 1 ausgelöst. Es wird keine Benachrichtigung gesendet. 2. Alarm A wird um 08:01 Uhr auf Knoten 2 ausgelöst. Es wird keine Benachrichtigung gesendet. 3. Um 08:02 Uhr wird eine Benachrichtigung gesendet, um beide Instanzen des Alarms zu melden.
Wenn ein weiterer Alarm mit demselben Namen ausgelöst wird, wartet StorageGRID 10 Minuten, bevor eine neue Benachrichtigung gesendet wird. Die neue Benachrichtigung meldet alle aktiven Warnungen (aktuelle Warnungen, die nicht stummgeschaltet wurden), auch wenn sie zuvor gemeldet wurden.	1. Alarm A wird um 08:00 Uhr auf Knoten 1 ausgelöst. Um 08:02 Uhr wird eine Benachrichtigung gesendet. 2. Alarm A wird um 08:05 Uhr auf Knoten 2 ausgelöst. Eine zweite Benachrichtigung wird um 08:15 Uhr (10 Minuten später) gesendet. Beide Knoten werden gemeldet.
Wenn mehrere aktuelle Warnungen mit demselben Namen vorliegen und eine dieser Warnungen behoben wird, wird keine neue Benachrichtigung gesendet, wenn die Warnung auf dem Knoten erneut auftritt, für den die Warnung behoben wurde.	1. Alarm A wird für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Alarm A wird für Knoten 2 ausgelöst. Eine zweite Benachrichtigung wird gesendet. 3. Alarm A wird für Knoten 2 behoben, bleibt aber für Knoten 1 aktiv. 4. Alarm A wird für Knoten 2 erneut ausgelöst. Es wird keine neue Benachrichtigung gesendet, da der Alarm für Knoten 1 noch aktiv ist.

Verhalten	Beispiel
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen des Alarms behoben oder die Alarmregel stummgeschaltet sind.	1. Alarm A wird am 8. März für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Alarm A wird nicht behoben oder stummgeschaltet. Weitere Benachrichtigungen werden am 15. März, 22. März, 29. März usw. gesendet.

Fehlerbehebung bei E-Mail-Benachrichtigungen

Wenn die Warnung **Fehler bei E-Mail-Benachrichtigung** ausgelöst wird oder Sie die E-Mail-Benachrichtigung zum Testalarm nicht erhalten können, führen Sie die folgenden Schritte aus, um das Problem zu beheben.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Schritte

1. Überprüfen Sie Ihre Einstellungen.
   a. Wählen Sie **WARNUNGEN** > **E-Mail-Setup**.
   b. Überprüfen Sie, ob die Einstellungen des E-Mail-Servers (SMTP) korrekt sind.
   c. Stellen Sie sicher, dass Sie gültige E-Mail-Adressen für die Empfänger angegeben haben.
2. Überprüfen Sie Ihren Spamfilter und stellen Sie sicher, dass die E-Mail nicht in einen Junk-Ordner verschoben wurde.
3. Bitten Sie Ihren E-Mail-Administrator um Bestätigung, dass E-Mails von der Absenderadresse nicht blockiert werden.
4. Erstellen Sie eine Protokolldatei für den Admin-Knoten und wenden Sie sich dann an den technischen Support.

   Der technische Support kann die Informationen in den Protokollen verwenden, um festzustellen, was schiefgelaufen ist. Beispielsweise kann die Datei „prometheus.log“ beim Herstellen einer Verbindung mit dem von Ihnen angegebenen Server einen Fehler anzeigen.

   Sehen "Erfassen von Protokolldateien und Systemdaten" .

Warnmeldungen stummschalten

Optional können Sie Stummschaltungen konfigurieren, um Warnbenachrichtigungen vorübergehend zu unterdrücken.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Verwalten von Warnungen oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Sie können Warnregeln für das gesamte Raster, eine einzelne Site oder einen einzelnen Knoten und für einen oder mehrere Schweregrade stummschalten. Jede Stille unterdrückt alle Benachrichtigungen für eine einzelne

Warnregel oder für alle Warnregeln.

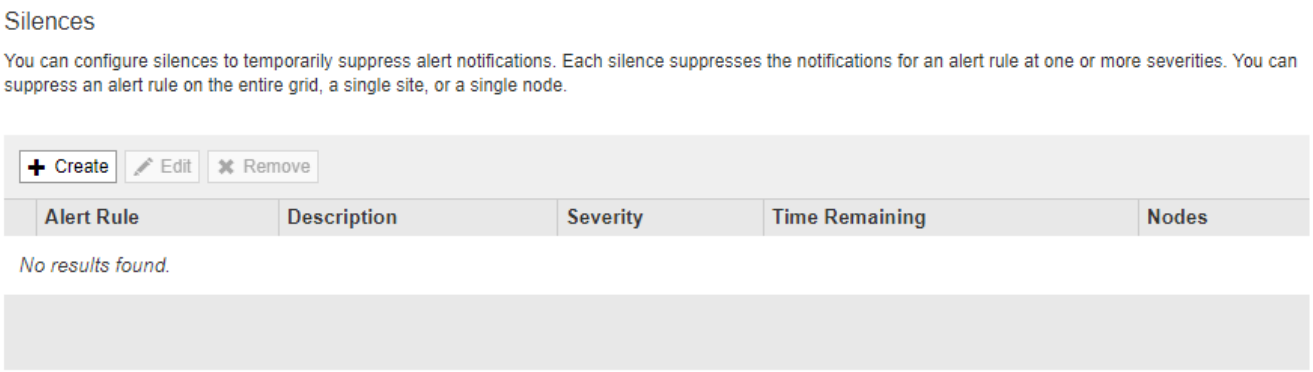
Wenn Sie den SNMP-Agenten aktiviert haben, werden durch Stummschalten auch SNMP-Traps und -Informationen unterdrückt.

> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel stummzuschalten. Wenn Sie eine Warnung stummschalten, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert.

Schritte

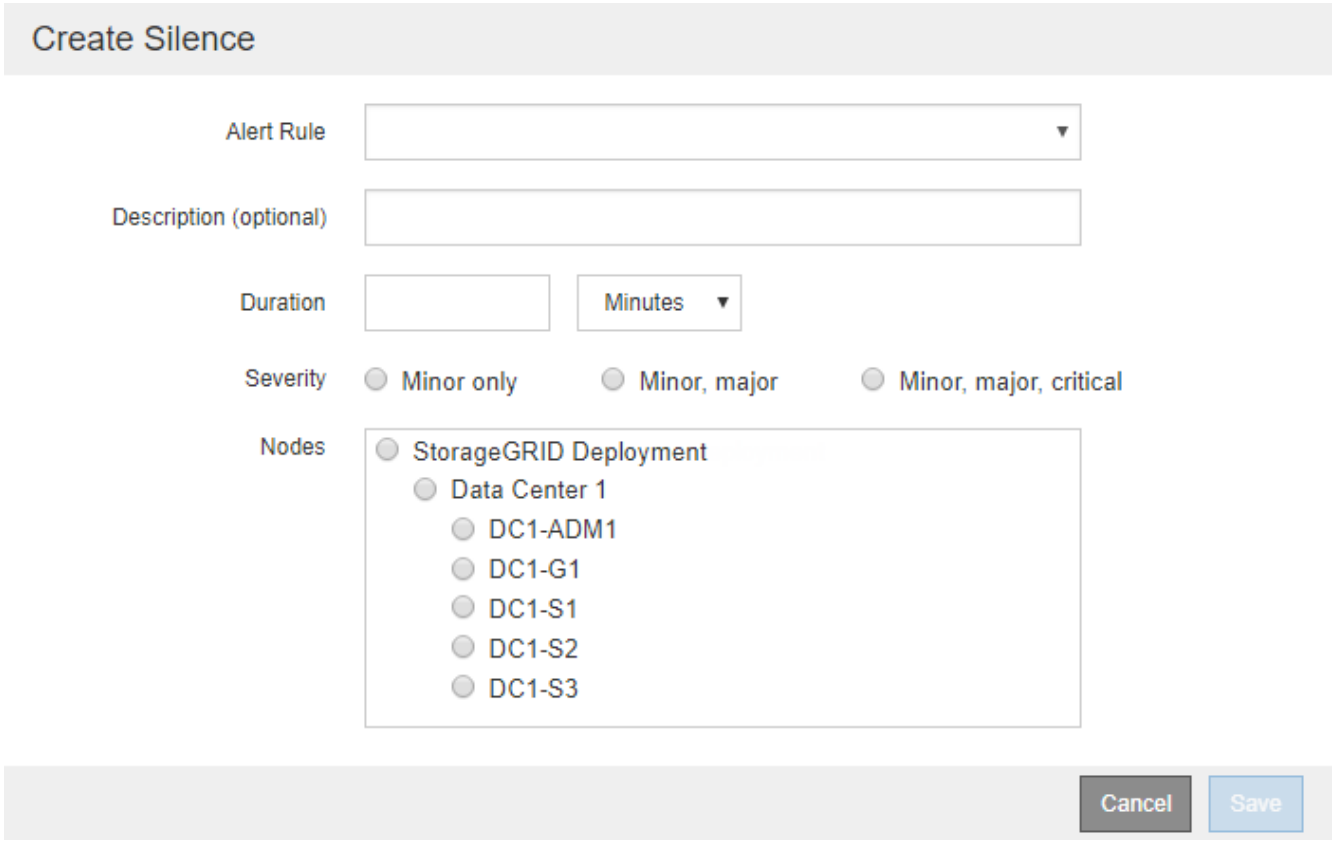
1. Wählen Sie **WARNUNGEN** > **Stummschaltungen**.

   Die Seite „Stille“ wird angezeigt.



2. Wählen Sie **Erstellen**.

   Das Dialogfeld „Stille erstellen“ wird angezeigt.



3. Wählen Sie die folgenden Informationen aus oder geben Sie sie ein:

Feld	Beschreibung
Warnregel	Der Name der Warnregel, die Sie stummschalten möchten. Sie können jede Standard- oder benutzerdefinierte Warnregel auswählen, auch wenn die Warnregel deaktiviert ist. **Hinweis:** Wählen Sie **Alle Regeln** aus, wenn Sie alle Warnregeln anhand der in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.
Beschreibung	Optional eine Beschreibung der Stille. Beschreiben Sie beispielsweise den Zweck dieser Stille.
Dauer	Wie lange diese Stille in Kraft bleiben soll, in Minuten, Stunden oder Tagen. Eine Sperre kann zwischen 5 Minuten und 1.825 Tagen (5 Jahren) wirksam sein. **Hinweis:** Sie sollten eine Warnregel nicht für einen längeren Zeitraum stummschalten. Wenn eine Warnregel stummgeschaltet wird, erkennen Sie ein zugrunde liegendes Problem möglicherweise erst, wenn es die Ausführung eines kritischen Vorgangs verhindert. Möglicherweise müssen Sie jedoch eine längere Stille verwenden, wenn eine Warnung durch eine bestimmte, absichtliche Konfiguration ausgelöst wird, wie dies beispielsweise bei den Warnungen „Link zur Service-Appliance unterbrochen“ und „Link zur Speicher-Appliance unterbrochen“ der Fall sein kann.
Schwere	Welcher oder welche Schweregrade der Warnungen sollten stummgeschaltet werden? Wenn der Alarm bei einem der ausgewählten Schweregrade ausgelöst wird, werden keine Benachrichtigungen gesendet.
Nodes	Auf welchen Knoten oder welche Knoten soll diese Stille angewendet werden? Sie können eine Warnregel oder alle Regeln für das gesamte Raster, eine einzelne Site oder einen einzelnen Knoten unterdrücken. Wenn Sie das gesamte Raster auswählen, gilt die Stille für alle Sites und alle Knoten. Wenn Sie einen Standort auswählen, gilt die Stille nur für die Knoten an diesem Standort. **Hinweis:** Sie können für jede Stille nicht mehr als einen Knoten oder mehr als eine Site auswählen. Sie müssen zusätzliche Stummschaltungen erstellen, wenn Sie dieselbe Warnregel auf mehreren Knoten oder mehreren Sites gleichzeitig unterdrücken möchten.

4. Wählen Sie **Speichern**.
5. Wenn Sie eine Stille ändern oder beenden möchten, bevor sie abläuft, können Sie sie bearbeiten oder entfernen.

Option	Beschreibung
Bearbeiten einer Stille	a. Wählen Sie **WARNUNGEN** > **Stummschaltungen**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille aus, die Sie bearbeiten möchten. c. Wählen Sie **Bearbeiten**. d. Ändern Sie die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten. e. Wählen Sie **Speichern**.
Eine Stille entfernen	a. Wählen Sie **WARNUNGEN** > **Stummschaltungen**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille aus, die Sie entfernen möchten. c. Wählen Sie **Entfernen**. d. Wählen Sie **OK**, um zu bestätigen, dass Sie diese Stille entfernen möchten. **Hinweis**: Wenn dieser Alarm ausgelöst wird, werden jetzt Benachrichtigungen gesendet (sofern sie nicht durch eine andere Stille unterdrückt werden). Wenn diese Warnung derzeit ausgelöst wird, kann es einige Minuten dauern, bis E-Mail- oder SNMP-Benachrichtigungen gesendet werden und die Seite „Warnungen“ aktualisiert wird.

Ähnliche Informationen

"Konfigurieren des SNMP-Agenten"

Warnungsreferenz

In dieser Referenz sind die Standardwarnungen aufgelistet, die im Grid Manager angezeigt werden. Empfohlene Maßnahmen finden Sie in der Warnmeldung, die Sie erhalten.

Bei Bedarf können Sie benutzerdefinierte Warnregeln erstellen, die zu Ihrem Systemverwaltungsansatz passen.

Einige der Standardwarnungen verwenden"Prometheus-Metriken" .

Gerätewarnungen

Name der Warnung	Beschreibung
Gerätebatterie leer	Die Batterie im Speichercontroller des Geräts ist leer.
Gerätebatterie defekt	Die Batterie im Speichercontroller des Geräts ist ausgefallen.

Name der Warnung	Beschreibung
Die Gerätebatterie hat nicht genügend gelernte Kapazität	Die Batterie im Speichercontroller des Geräts verfügt nicht über die erforderliche Kapazität.
Gerätebatterie fast leer	Die Batterie im Speichercontroller des Geräts ist fast leer.
Gerätebatterie entfernt	Die Batterie im Speichercontroller des Geräts fehlt.
Gerätebatterie zu heiß	Die Batterie im Speichercontroller des Geräts ist überhitzt.
Appliance- BMC Kommunikationsfehler	Die Kommunikation mit dem Baseboard Management Controller (BMC) ist verloren gegangen.
Fehler beim Boot-Gerät der Appliance erkannt	Es wurde ein Problem mit dem Startgerät in der Appliance erkannt.
Fehler beim Appliance-Cache-Sicherungsgerät	Ein persistentes Cache-Backup-Gerät ist ausgefallen.
Unzureichende Kapazität des Appliance-Cache-Sicherungsgeräts	Die Kapazität des Cache-Backup-Geräts ist nicht ausreichend.
Appliance-Cache-Sicherungsgerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt.
Nicht übereinstimmende Größe des Appliance-Cache-Speichers	Die beiden Controller in der Appliance haben unterschiedliche Cachegrößen.
Fehler der CMOS-Batterie des Geräts	Es wurde ein Problem mit der CMOS-Batterie im Gerät festgestellt.
Gehäusetemperatur des Appliance-Compute-Controllers zu hoch	Die Temperatur des Compute-Controllers in einem StorageGRID Gerät hat einen nominalen Schwellenwert überschritten.
CPU-Temperatur des Appliance-Compute-Controllers zu hoch	Die Temperatur der CPU im Compute Controller in einem StorageGRID -Gerät hat einen nominalen Schwellenwert überschritten.
Der Appliance-Compute-Controller erfordert Aufmerksamkeit	Im Compute-Controller eines StorageGRID Geräts wurde ein Hardwarefehler erkannt.
Netzteil A des Appliance-Compute-Controllers hat ein Problem	Netzteil A im Compute-Controller hat ein Problem.
Das Netzteil B des Appliance-Compute-Controllers hat ein Problem	Netzteil B im Compute-Controller hat ein Problem.

Name der Warnung	Beschreibung
Der Dienst zur Überwachung der Appliance-Compute-Hardware ist angehalten	Der Dienst, der den Status der Speicherhardware überwacht, ist ins Stocken geraten.
Das Appliance-DAS-Laufwerk überschreitet das Limit für pro Tag geschriebene Daten	Jeden Tag werden übermäßig viele Daten auf ein Laufwerk geschrieben, was zum Erlöschen der Garantie führen kann.
Fehler im DAS-Laufwerk der Appliance erkannt	Es wurde ein Problem mit einem DAS-Laufwerk (Direct Attached Storage) in der Appliance erkannt.
Appliance DAS-Laufwerkssuchleuchte leuchtet	Die Laufwerkslokalisierungsleuchte für ein oder mehrere DAS-Laufwerke (Direct Attached Storage) in einem Appliance-Speicherknoten leuchtet.
Neuerstellung des Appliance-DAS-Laufwerks	Ein Direct-Attached-Storage-Laufwerk (DAS) wird neu erstellt. Dies ist zu erwarten, wenn es vor Kurzem ersetzt oder entfernt/wieder eingesetzt wurde.
Gerätelüfterfehler erkannt	Es wurde ein Problem mit einer Lüftereinheit im Gerät festgestellt.
Appliance-Fibre-Channel-Fehler erkannt	Zwischen dem Speichercontroller und dem Compute-Controller der Appliance wurde ein Fibre-Channel-Verbindungsproblem erkannt
Appliance-Fibre-Channel-HBA-Portfehler	Ein Fibre Channel-HBA-Port fällt aus oder ist ausgefallen.
Appliance-Flash-Cache-Laufwerke nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal.
Geräteverbindung/Batteriebehälter entfernt	Der Verbindungs-/Batteriebehälter fehlt.
Appliance-LACP-Port fehlt	Ein Port auf einem StorageGRID -Gerät nimmt nicht an der LACP-Verbindung teil.
Fehler der Appliance-NIC erkannt	Es wurde ein Problem mit einer Netzwerkschnittstellenkarte (NIC) im Gerät erkannt.
Gesamtstromversorgung des Geräts beeinträchtigt	Die Leistung eines StorageGRID -Geräts weicht von der empfohlenen Betriebsspannung ab.
Kritische Warnung zur Appliance-SSD	Eine Appliance-SSD meldet eine kritische Warnung.

Name der Warnung	Beschreibung
Fehler beim Appliance-Speichercontroller A	Speichercontroller A in einem StorageGRID -Gerät ist ausgefallen.
Ausfall des Appliance-Speichercontrollers B	Speichercontroller B in einem StorageGRID Gerät ist ausgefallen.
Ausfall des Laufwerks des Appliance-Speichercontrollers	Ein oder mehrere Laufwerke in einem StorageGRID -Gerät sind ausgefallen oder nicht optimal.
Hardwareproblem mit dem Appliance-Speichercontroller	Die SANtricity -Software meldet „Benötigt Aufmerksamkeit“ für eine Komponente in einem StorageGRID Gerät.
Ausfall der Stromversorgung des Appliance-Speichercontrollers A	Netzteil A in einem StorageGRID -Gerät weicht von der empfohlenen Betriebsspannung ab.
Ausfall der Stromversorgung B des Appliance-Speichercontrollers	Netzteil B in einem StorageGRID -Gerät ist von der empfohlenen Betriebsspannung abgewichen.
Der Dienst zur Überwachung der Appliance-Speicherhardware ist angehalten	Der Dienst, der den Status der Speicherhardware überwacht, ist ins Stocken geraten.
Abgenutzte Regale für die Geräteablage	Der Status einer der Komponenten im Speicherregal für ein Speichergerät ist herabgestuft.
Gerätetemperatur überschritten	Die Nenn- oder Maximaltemperatur für den Speichercontroller der Appliance wurde überschritten.
Gerätetemperatursensor entfernt	Ein Temperatursensor wurde entfernt.
Appliance-UEFI-Sicherheitsstartfehler	Ein Gerät wurde nicht sicher gestartet.
Die Festplatten-E/A ist sehr langsam	Sehr langsame Festplatten-E/A können die Grid-Leistung beeinträchtigen.
Lüfterfehler des Speichergeräts erkannt	Es wurde ein Problem mit einer Lüftereinheit im Speichercontroller für eine Appliance erkannt.
Speicherkonnektivität des Speichergeräts beeinträchtigt	Es liegt ein Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller vor.
Auf das Speichergerät kann nicht zugegriffen werden	Auf ein Speichergerät kann nicht zugegriffen werden.

Audit- und Syslog-Warnmeldungen

Name der Warnung	Beschreibung
Audit-Protokolle werden der In-Memory-Warteschlange hinzugefügt	Der Knoten kann keine Protokolle an den lokalen Syslog-Server senden und die Warteschlange im Arbeitsspeicher füllt sich.
Fehler bei der Weiterleitung des externen Syslog-Servers	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten.
Große Prüfwarteschlange	Die Festplattenwarteschlange für Prüfmeldungen ist voll. Wenn dieser Zustand nicht behoben wird, können S3- oder Swift-Vorgänge fehlschlagen.
Protokolle werden der Warteschlange auf der Festplatte hinzugefügt	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten und die Warteschlange auf der Festplatte füllt sich.

Bucket-Benachrichtigungen

Name der Warnung	Beschreibung
FabricPool Bucket verfügt über eine nicht unterstützte Bucket-Konsistenzeinstellung	Ein FabricPool Bucket verwendet die Konsistenzebene „Verfügbar“ oder „Stark-Site“, die nicht unterstützt wird.
FabricPool Bucket verfügt über nicht unterstützte Versionseinstellungen	Für einen FabricPool Bucket sind Versionierung oder S3 Object Lock aktiviert, die nicht unterstützt werden.

Cassandra-Warnungen

Name der Warnung	Beschreibung
Cassandra-Autokompaktorfehler	Beim Cassandra-Autokompaktor ist ein Fehler aufgetreten.
Die Metriken des Cassandra-Autokompaktors sind veraltet	Die Metriken, die den Cassandra-Autokompaktor beschreiben, sind veraltet.
Cassandra-Kommunikationsfehler	Die Knoten, auf denen der Cassandra-Dienst ausgeführt wird, haben Probleme bei der Kommunikation untereinander.
Cassandra-Komprimierungen überlastet	Der Cassandra-Komprimierungsprozess ist überlastet.
Cassandra-Übergrößen-Schreibfehler	Ein interner StorageGRID -Prozess hat eine zu große Schreibanforderung an Cassandra gesendet.

Name der Warnung	Beschreibung
Cassandra-Reparaturmetriken veraltet	Die Metriken, die Cassandra-Reparaturjobs beschreiben, sind veraltet.
Cassandra-Reparaturfortschritt langsam	Die Reparatur der Cassandra-Datenbank schreitet nur langsam voran.
Cassandra-Reparaturdienst nicht verfügbar	Der Cassandra-Reparaturservice ist nicht verfügbar.
Cassandra-Tabellenbeschädigung	Cassandra hat eine Tabellenbeschädigung festgestellt. Cassandra wird automatisch neu gestartet, wenn eine Tabellenbeschädigung erkannt wird.

Cloud Storage Pool-Warnungen

Name der Warnung	Beschreibung
Verbindungsfehler beim Cloud-Speicherpool	Bei der Integritätsprüfung für Cloud Storage Pools wurden ein oder mehrere neue Fehler festgestellt.
Ablauf der IAM Roles Anywhere-Endentitätszertifizierung	Das Endentitätszertifikat von IAM Roles Anywhere läuft bald ab.

Warnungen zur Grid-übergreifenden Replikation

Name der Warnung	Beschreibung
Dauerhafter Fehler bei der Cross-Grid-Replikation	Bei der gitterübergreifenden Replikation ist ein Fehler aufgetreten, der zur Behebung einen Benutzereingriff erfordert.
Cross-Grid-Replikationsressourcen nicht verfügbar	Gridübergreifende Replikationsanforderungen stehen aus, weil eine Ressource nicht verfügbar ist.

DHCP-Warnmeldungen

Name der Warnung	Beschreibung
DHCP-Lease abgelaufen	Die DHCP-Lease einer Netzwerkschnittstelle ist abgelaufen.
DHCP-Lease läuft bald ab	Die DHCP-Lease einer Netzwerkschnittstelle läuft bald ab.
DHCP-Server nicht verfügbar	Der DHCP-Server ist nicht verfügbar.

Debug- und Trace-Warnungen

Name der Warnung	Beschreibung
Auswirkungen auf die Debugleistung	Wenn der Debug-Modus aktiviert ist, kann die Systemleistung negativ beeinflusst werden.
Trace-Konfiguration aktiviert	Wenn die Trace-Konfiguration aktiviert ist, kann die Systemleistung negativ beeinflusst werden.

E-Mail- und AutoSupport Benachrichtigungen

Name der Warnung	Beschreibung
AutoSupport -Nachricht konnte nicht gesendet werden	Das Senden der letzten AutoSupport -Nachricht ist fehlgeschlagen.
Fehler bei der Domänennamenauflösung	Der StorageGRID -Knoten konnte Domänennamen nicht auflösen.
Fehler bei der E-Mail-Benachrichtigung	Die E-Mail-Benachrichtigung für eine Warnung konnte nicht gesendet werden.
SNMP-Informationsfehler	Fehler beim Senden von SNMP-Informationsbenachrichtigungen an ein Trap-Ziel.
SSH- oder Konsolen-Login erkannt	In den letzten 24 Stunden hat sich ein Benutzer mit der Webkonsole oder SSH angemeldet.

Erasure Coding (EC)-Warnungen

Name der Warnung	Beschreibung
EC-Neuausgleichsfehler	Der EC-Neuausgleichsvorgang ist fehlgeschlagen oder wurde abgebrochen.
EC-Reparaturfehler	Ein Reparaturauftrag für EC-Daten ist fehlgeschlagen oder wurde abgebrochen.
EC-Reparatur ins Stocken geraten	Ein Reparaturauftrag für EC-Daten ist ins Stocken geraten.
Fehler bei der Überprüfung des Löschcodierungsfragments	Erasure-Coded-Fragmente können nicht mehr verifiziert werden. Beschädigte Fragmente können möglicherweise nicht repariert werden.

Warnungen zum Ablauf von Zertifikaten

Name der Warnung	Beschreibung
Ablauf des Admin Proxy CA-Zertifikats	Ein oder mehrere Zertifikate im CA-Paket des Admin-Proxyservers laufen bald ab.

Name der Warnung	Beschreibung
Ablauf des Client-Zertifikats	Ein oder mehrere Client-Zertifikate laufen bald ab.
Ablauf des globalen Serverzertifikats für S3 und Swift	Das globale Serverzertifikat für S3 und Swift läuft bald ab.
Ablauf des Load Balancer-Endpunktzertifikats	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen bald ab.
Ablauf des Serverzertifikats für die Verwaltungsschnittstelle	Das für die Verwaltungsschnittstelle verwendete Serverzertifikat läuft bald ab.
Ablauf des externen Syslog-CA-Zertifikats	Das zum Signieren des externen Syslog-Serverzertifikats verwendete Zertifikat der Zertifizierungsstelle (CA) läuft bald ab.
Ablauf des externen Syslog-Client-Zertifikats	Das Client-Zertifikat für einen externen Syslog-Server läuft bald ab.
Ablauf des Zertifikats des externen Syslog-Servers	Das vom externen Syslog-Server vorgelegte Serverzertifikat läuft bald ab.

Grid-Netzwerkwarnungen

Name der Warnung	Beschreibung
MTU-Nichtübereinstimmung im Netz	Die MTU-Einstellung für die Grid-Netzwerkschnittstelle (eth0) unterscheidet sich erheblich zwischen den Knoten im Grid.

Grid-Föderationswarnungen

Name der Warnung	Beschreibung
Ablauf des Netzverbundzertifikats	Ein oder mehrere Grid-Föderation-Zertifikate laufen bald ab.
Grid-Föderation-Verbindungsfehler	Die Grid-Föderation-Verbindung zwischen dem lokalen und dem Remote-Grid funktioniert nicht.

Warnungen bei hoher Auslastung oder hoher Latenz

Name der Warnung	Beschreibung
Hohe Java-Heap-Nutzung	Ein hoher Prozentsatz des Java-Heap-Speichers wird verwendet.
Hohe Latenz bei Metadatenabfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.

Identitätsföderationswarnungen

Name der Warnung	Beschreibung
Fehler bei der Synchronisierung der Identitätsföderation	Föderierte Gruppen und Benutzer können nicht aus der Identitätsquelle synchronisiert werden.
Fehler bei der Identitätsföderationssynchronisierung für einen Mandanten	Föderierte Gruppen und Benutzer können nicht aus der von einem Mandanten konfigurierten Identitätsquelle synchronisiert werden.

Warnungen zum Information Lifecycle Management (ILM)

Name der Warnung	Beschreibung
ILM-Platzierung nicht erreichbar	Für bestimmte Objekte ist eine Platzierungsanweisung in einer ILM-Regel nicht realisierbar.
Niedrige ILM-Scanrate	Die ILM-Scanrate ist auf weniger als 100 Objekte/Sekunde eingestellt.

Warnungen des Schlüsselverwaltungsservers (KMS)

Name der Warnung	Beschreibung
Ablauf des KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des Zertifikats des Schlüsselverwaltungsservers (KMS) verwendet wurde, läuft bald ab.
Ablauf des KMS-Clientzertifikats	Das Client-Zertifikat für einen Schlüsselverwaltungsserver läuft bald ab
KMS-Konfiguration konnte nicht geladen werden	Die Konfiguration für den Schlüsselverwaltungsserver ist vorhanden, konnte aber nicht geladen werden.
KMS-Konnektivitätsfehler	Ein Appliance-Knoten konnte keine Verbindung zum Schlüsselverwaltungsserver für seine Site herstellen.
Name des KMS-Verschlüsselungsschlüssels nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt.
Fehler bei der Rotation des KMS-Verschlüsselungsschlüssels	Alle Appliance-Volumes wurden erfolgreich entschlüsselt, aber ein oder mehrere Volumes konnten nicht auf den neuesten Schlüssel rotiert werden.
KMS ist nicht konfiguriert	Für diese Site ist kein Schlüsselverwaltungsserver vorhanden.

Name der Warnung	Beschreibung
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	Ein oder mehrere Volumes auf einer Appliance mit aktivierter Knotenverschlüsselung konnten mit dem aktuellen KMS-Schlüssel nicht entschlüsselt werden.
Ablauf des KMS-Serverzertifikats	Das vom Schlüsselverwaltungsserver (KMS) verwendete Serverzertifikat läuft bald ab.
KMS-Server-Konnektivitätsfehler	Ein Appliance-Knoten konnte keine Verbindung zu einem oder mehreren Servern im Schlüsselverwaltungsserver-Cluster für seine Site herstellen.

Load Balancer-Warnungen

Name der Warnung	Beschreibung
Erhöhte Zero-Request-Load-Balancer-Verbindungen	Ein erhöhter Prozentsatz der Verbindungen zu Load Balancer-Endpunkten wurde getrennt, ohne dass Anforderungen ausgeführt wurden.

Warnungen bei lokalem Zeitversatz

Name der Warnung	Beschreibung
Großer Zeitversatz der lokalen Uhr	Der Offset zwischen der lokalen Uhr und der Network Time Protocol (NTP)-Zeit ist zu groß.

Warnungen bei zu wenig Arbeitsspeicher oder Speicherplatz

Name der Warnung	Beschreibung
Geringe Festplattenkapazität für Überwachungsprotokolle	Der für Audit-Protokolle verfügbare Speicherplatz ist gering. Wenn dieser Zustand nicht behoben wird, können S3- oder Swift-Vorgänge fehlschlagen.
Wenig verfügbarer Knotenspeicher	Die auf einem Knoten verfügbare RAM-Menge ist gering.
Wenig freier Speicherplatz für Speicherpool	Der zum Speichern von Objektdaten im Speicherknoten verfügbare Speicherplatz ist gering.
Wenig installierter Knotenspeicher	Die Menge des auf einem Knoten installierten Speichers ist gering.
Geringe Speicherung von Metadaten	Der zum Speichern von Objektmetadaten verfügbare Speicherplatz ist gering.
Niedrige Metrik-Festplattenkapazität	Der für die Metrikdatenbank verfügbare Speicherplatz ist gering.

Name der Warnung	Beschreibung
Geringe Objektdatenspeicherung	Der zum Speichern von Objektdaten verfügbare Speicherplatz ist gering.
Niedrige schreibgeschützte Wasserzeichenüberschreibung	Die Soft-Read-Only-Wasserzeichenüberschreibung des Speichervolumes ist kleiner als das minimal optimierte Wasserzeichen für einen Speicherknoten.
Geringe Root-Disk-Kapazität	Der auf der Root-Festplatte verfügbare Speicherplatz ist gering.
Geringe Systemdatenkapazität	Der für /var/local verfügbare Speicherplatz ist gering. Wenn dieser Zustand nicht behoben wird, können S3- oder Swift-Vorgänge fehlschlagen.
Wenig freier Speicherplatz im temporären Verzeichnis	Im Verzeichnis /tmp ist nur noch wenig Speicherplatz verfügbar.

Knoten- oder Knotennetzwerkwarnungen

Name der Warnung	Beschreibung
Empfangsnutzung des Admin-Netzwerks	Die Empfangsnutzung im Admin-Netzwerk ist hoch.
Übertragungsnutzung des Admin-Netzwerks	Die Übertragungsnutzung im Admin-Netzwerk ist hoch.
Firewall-Konfigurationsfehler	Die Firewall-Konfiguration konnte nicht angewendet werden.
Management-Schnittstellenendpunkte im Fallback-Modus	Alle Endpunkte der Verwaltungsschnittstelle sind zu lange auf die Standardports zurückgefallen.
Knotennetzwerk-Konnektivitätsfehler	Beim Übertragen der Daten zwischen den Knoten sind Fehler aufgetreten.
Fehler beim Empfang des Knotennetzwerk-Frames	Ein hoher Prozentsatz der von einem Knoten empfangenen Netzwerk-Frames war fehlerhaft.
Knoten nicht mit NTP-Server synchronisiert	Der Knoten ist nicht mit dem Network Time Protocol (NTP)-Server synchronisiert.
Knoten nicht mit NTP-Server gesperrt	Der Knoten ist nicht an einen NTP-Server (Network Time Protocol) gebunden.
Nicht-Appliance-Knotennetzwerk ausgefallen	Ein oder mehrere Netzwerkgeräte sind ausgefallen oder getrennt.

Name der Warnung	Beschreibung
Verbindung zur Dienst-Appliance im Admin-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Verbindung der Services-Appliance auf Admin-Netzwerkport 1 unterbrochen	Der Admin-Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung zur Dienst-Appliance im Client-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 1 unterbrochen	Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 2 unterbrochen	Netzwerkport 2 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 3 unterbrochen	Netzwerkport 3 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung der Dienste-Appliance auf Netzwerkport 4 unterbrochen	Netzwerkport 4 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung zur Speicher-Appliance im Admin-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Verbindung zur Speicher-Appliance auf Admin-Netzwerk-Port 1 unterbrochen	Der Admin-Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Verbindung zur Speicher-Appliance im Client-Netzwerk unterbrochen	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 1 unterbrochen	Netzwerkport 1 auf dem Gerät ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 2 unterbrochen	Netzwerkport 2 auf dem Gerät ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 3 unterbrochen	Netzwerkport 3 auf dem Gerät ist ausgefallen oder getrennt.
Speichergerät-Verbindung auf Netzwerkport 4 unterbrochen	Netzwerkport 4 auf dem Gerät ist ausgefallen oder getrennt.

Name der Warnung	Beschreibung
Speicherknoten nicht im gewünschten Speicherzustand	Der LDR-Dienst auf einem Speicherknoten kann aufgrund eines internen Fehlers oder eines Volume-bezogenen Problems nicht in den gewünschten Zustand wechseln
TCP-Verbindungsnutzung	Die Anzahl der TCP-Verbindungen auf diesem Knoten nähert sich der maximalen Anzahl, die verfolgt werden kann.
Kommunikation mit Knoten nicht möglich	Ein oder mehrere Dienste reagieren nicht oder der Knoten kann nicht erreicht werden.
Unerwarteter Neustart des Knotens	Ein Knoten wurde innerhalb der letzten 24 Stunden unerwartet neu gestartet.

Objektwarnungen

Name der Warnung	Beschreibung
Objekt-Existenzprüfung fehlgeschlagen	Der Job zur Überprüfung der Objektexistenz ist fehlgeschlagen.
Objekt-Existenzprüfung angehalten	Der Job zur Überprüfung der Objektexistenz ist ins Stocken geraten.
Verlorene Gegenstände	Ein oder mehrere Objekte sind aus dem Raster verloren gegangen.
S3 PUT-Objektgröße zu groß	Ein Client versucht einen PUT-Objektvorgang, der die S3-Größenbeschränkungen überschreitet.
Unbekanntes beschädigtes Objekt erkannt	Im replizierten Objektspeicher wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte.

Warnungen zu Plattformdiensten

Name der Warnung	Beschreibung
Niedrige Kapazität für ausstehende Anfragen der Plattformdienste	Die Anzahl der ausstehenden Anfragen der Plattformdienste nähert sich der Kapazitätsgrenze.
Plattformdienste nicht verfügbar	An einem Standort sind zu wenige Speicherknoten mit dem RSM-Dienst aktiv oder verfügbar.

Speichervolumenwarnungen

Name der Warnung	Beschreibung
Speichervolumen erfordert Aufmerksamkeit	Ein Speichervolume ist offline und erfordert Aufmerksamkeit.

Name der Warnung	Beschreibung
Speichervolumen muss wiederhergestellt werden	Ein Speichervolume wurde wiederhergestellt und muss wiederhergestellt werden.
Speichervolume offline	Ein Speichervolume war länger als 5 Minuten offline.
Es wurde versucht, das Speichervolume erneut zu mounten.	Ein Speichervolume war offline und löste eine automatische Neubereitstellung aus. Dies könnte auf ein Laufwerksproblem oder Dateisystemfehler hinweisen.
Bei der Volume-Wiederherstellung konnte die Reparatur replizierter Daten nicht gestartet werden.	Die Reparatur replizierter Daten für ein repariertes Volume konnte nicht automatisch gestartet werden.

Warnungen zu StorageGRID -Diensten

Name der Warnung	Beschreibung
Nginx-Dienst mit Backup-Konfiguration	Die Konfiguration des Nginx-Dienstes ist ungültig. Es wird nun die vorherige Konfiguration verwendet.
nginx-gw-Dienst mit Backup-Konfiguration	Die Konfiguration des nginx-gw-Dienstes ist ungültig. Es wird nun die vorherige Konfiguration verwendet.
Zum Deaktivieren von FIPS ist ein Neustart erforderlich	Die Sicherheitsrichtlinie erfordert keinen FIPS-Modus, aber das NetApp Cryptographic Security Module ist aktiviert.
Neustart erforderlich, um FIPS zu aktivieren	Die Sicherheitsrichtlinie erfordert den FIPS-Modus, aber das NetApp Cryptographic Security Module ist deaktiviert.
SSH-Dienst mit Sicherungskonfiguration	Die Konfiguration des SSH-Dienstes ist ungültig. Es wird nun die vorherige Konfiguration verwendet.

Mieterwarnungen

Name der Warnung	Beschreibung
Hohe Auslastung des Mandantenkontingents	Ein hoher Prozentsatz des Kontingentplatzes wird genutzt. Diese Regel ist standardmäßig deaktiviert, da sie zu viele Benachrichtigungen verursachen könnte.

Häufig verwendete Prometheus-Metriken

Sehen Sie sich diese Liste häufig verwendeter Prometheus-Metriken an, um die Bedingungen in den Standardwarnregeln besser zu verstehen oder die Bedingungen für benutzerdefinierte Warnregeln zu erstellen.

Sie können auch Erhalten Sie eine vollständige Liste aller Metriken .

Einzelheiten zur Syntax von Prometheus-Abfragen finden Sie unter "Abfragen von Prometheus" .

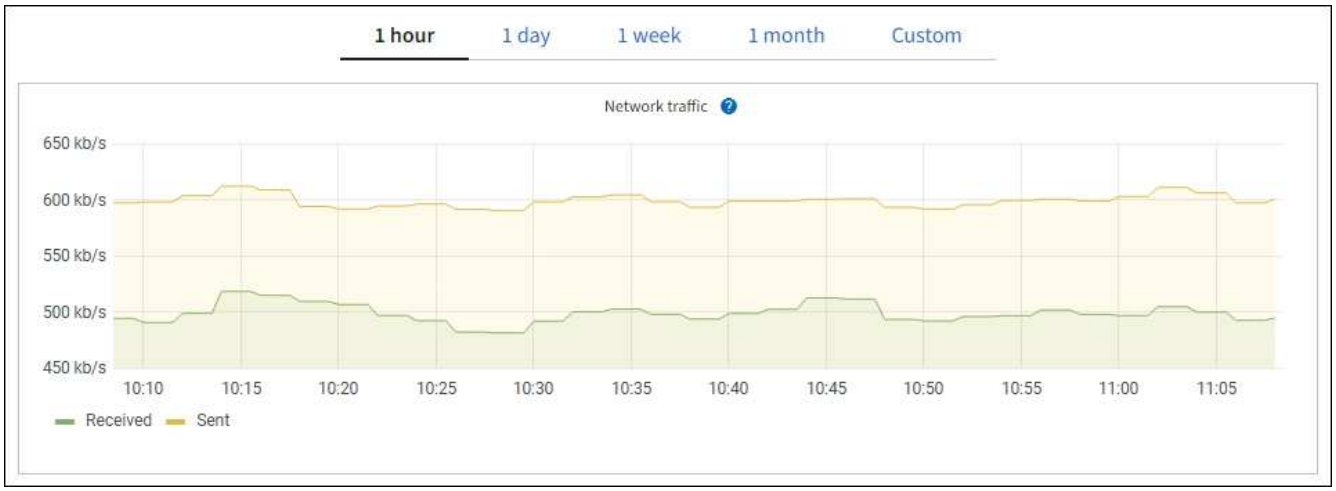
Was sind Prometheus-Metriken?

Prometheus-Metriken sind Zeitreihenmessungen. Der Prometheus-Dienst auf Admin-Knoten sammelt diese Metriken von den Diensten auf allen Knoten. Auf jedem Admin-Knoten werden Metriken gespeichert, bis der für Prometheus-Daten reservierte Speicherplatz voll ist. Wenn die `/var/local/mysql_ibdata/` Wenn das Volume die Kapazität erreicht, werden die ältesten Metriken zuerst gelöscht.

Wo werden Prometheus-Metriken verwendet?

Die von Prometheus gesammelten Metriken werden an mehreren Stellen im Grid Manager verwendet:

- **Knotenseite**: Die Grafiken und Diagramme auf den Registerkarten, die auf der Knotenseite verfügbar sind, verwenden das Grafana-Visualisierungstool, um die von Prometheus gesammelten Zeitreihenmetriken anzuzeigen. Grafana zeigt Zeitreihendaten in Diagramm- und Chartformaten an, während Prometheus als Backend-Datenquelle dient.



- **Warnungen**: Warnungen werden bei bestimmten Schweregraden ausgelöst, wenn Warnregelbedingungen, die Prometheus-Metriken verwenden, als wahr ausgewertet werden.
- **Grid Management API**: Sie können Prometheus-Metriken in benutzerdefinierten Warnregeln oder mit externen Automatisierungstools verwenden, um Ihr StorageGRID System zu überwachen. Eine vollständige Liste der Prometheus-Metriken ist über die Grid Management API verfügbar. (Wählen Sie oben im Grid Manager das Hilfesymbol und dann **API-Dokumentation** > **Metriken** aus.) Obwohl mehr als tausend Metriken verfügbar sind, wird nur eine relativ kleine Anzahl benötigt, um die kritischsten StorageGRID Vorgänge zu überwachen.

> Metriken, deren Namen „*private*“ enthalten, sind nur für den internen Gebrauch bestimmt und können zwischen StorageGRID Versionen ohne Vorankündigung geändert werden.

- Die Seite **SUPPORT** > **Tools** > **Diagnose** und die Seite **SUPPORT** > **Tools** > **Metriken**: Diese Seiten, die in erster Linie für den technischen Support vorgesehen sind, bieten mehrere Tools und Diagramme, die die Werte der Prometheus-Metriken verwenden.

> Einige Funktionen und Menüelemente auf der Seite „Metriken“ sind absichtlich nicht funktionsfähig und können sich ändern.

Liste der gängigsten Metriken

Die folgende Liste enthält die am häufigsten verwendeten Prometheus-Metriken.

> Metriken, deren Namen „*private*“ enthalten, sind nur für den internen Gebrauch bestimmt und können zwischen den StorageGRID Versionen ohne vorherige Ankündigung geändert werden.

alertmanager_notifications_failed_total
Die Gesamtzahl der fehlgeschlagenen Warnbenachrichtigungen.

node_filesystem_avail_bytes
Die Menge an Dateisystemspeicherplatz, die Nicht-Root-Benutzern in Bytes zur Verfügung steht.

node_memory_MemAvailable_bytes
Speicherinformationsfeld MemAvailable_bytes.

Knotennetzwerkträger
Trägerwert von `/sys/class/net/iface`.

node_network_receive_errs_total
Netzwerkgerätestatistik `receive_errs`.

node_network_transmit_errs_total
Netzwerkgerätestatistik `transmit_errs`.

storagegrid_administratively_down
Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Knoten oder die Dienste auf dem Knoten ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert.

storagegrid_appliance_compute_controller_hardware_status
Der Status der Compute-Controller-Hardware in einem Gerät.

storagegrid_appliance_failed_disks
Für den Speichercontroller in einem Gerät die Anzahl der Laufwerke, die nicht optimal sind.

storagegrid_appliance_storage_controller_hardware_status
Der Gesamtstatus der Speichercontroller-Hardware in einer Appliance.

storagegrid_content_buckets_and_containers
Die Gesamtzahl der diesem Speicherknoten bekannten S3-Buckets und Swift-Container.

storagegrid_content_objects
Die Gesamtzahl der diesem Speicherknoten bekannten S3- und Swift-Datenobjekte. Die Anzahl ist nur für Datenobjekte gültig, die von Clientanwendungen erstellt wurden, die über S3 mit dem System kommunizieren.

storagegrid_content_objects_lost
Die Gesamtzahl der Objekte, die dieser Dienst als im StorageGRID -System fehlend erkennt. Es sollten Maßnahmen ergriffen werden, um die Ursache des Verlusts zu ermitteln und festzustellen, ob eine Wiederherstellung möglich ist.

"Fehlerbehebung bei verlorenen und fehlenden Objektdaten"

storagegrid_http_sessions_incoming_attempted

Die Gesamtzahl der HTTP-Sitzungen, die mit einem Speicherknoten versucht wurden.

storagegrid_http_sessions_incoming_currently_established

Die Anzahl der HTTP-Sitzungen, die derzeit auf dem Speicherknoten aktiv (offen) sind.

storagegrid_http_sessions_incoming_failed

Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen werden konnten, entweder aufgrund einer fehlerhaften HTTP-Anforderung oder eines Fehlers bei der Verarbeitung eines Vorgangs.

storagegrid_http_sessions_incoming_successful

Die Gesamtzahl der HTTP-Sitzungen, die erfolgreich abgeschlossen wurden.

storagegrid_ilm_awaiting_background_objects

Die Gesamtzahl der Objekte auf diesem Knoten, die auf die ILM-Auswertung des Scans warten.

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

Die aktuelle Rate, mit der Objekte anhand der ILM-Richtlinie auf diesem Knoten ausgewertet werden.

storagegrid_ilm_awaiting_client_objects

Die Gesamtzahl der Objekte auf diesem Knoten, die auf die ILM-Auswertung von Clientvorgängen (z. B. Aufnahme) warten.

storagegrid_ilm_awaiting_total_objects

Die Gesamtzahl der Objekte, die auf die ILM-Auswertung warten.

storagegrid_ilm_scan_objects_per_second

Die Rate, mit der Objekte, die diesem Knoten gehören, gescannt und für ILM in die Warteschlange gestellt werden.

storagegrid_ilm_scan_period_estimated_minutes

Die geschätzte Zeit zum Abschließen eines vollständigen ILM-Scans auf diesem Knoten.

Hinweis: Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die diesem Knoten gehören.

storagegrid_load_balancer_endpoint_cert_expiry_time

Die Ablaufzeit des Load Balancer-Endpunktzertifikats in Sekunden seit der Epoche.

storagegrid_metadata_queries_average_latency_milliseconds

Die durchschnittliche Zeit, die zum Ausführen einer Abfrage des Metadatenspeichers über diesen Dienst benötigt wird.

storagegrid_network_received_bytes

Die Gesamtmenge der seit der Installation empfangenen Daten.

storagegrid_network_transmitted_bytes

Die Gesamtmenge der seit der Installation gesendeten Daten.

storagegrid_node_cpu_utilization_percentage

Der Prozentsatz der verfügbaren CPU-Zeit, die derzeit von diesem Dienst verwendet wird. Gibt an, wie ausgelastet der Dienst ist. Die Menge der verfügbaren CPU-Zeit hängt von der Anzahl der CPUs des Servers ab.

storagegrid_ntp_chosen_time_source_offset_milliseconds

Systematischer Zeitversatz durch eine ausgewählte Zeitquelle. Ein Offset wird eingeführt, wenn die Verzögerung zum Erreichen einer Zeitquelle nicht der Zeit entspricht, die die Zeitquelle benötigt, um den NTP-Client zu erreichen.

storagegrid_ntp_locked

Der Knoten ist nicht an einen Network Time Protocol (NTP)-Server gebunden.

storagegrid_s3_data_transfers_bytes_ingested

Die Gesamtmenge der von S3-Clients in diesen Speicherknoten aufgenommenen Daten seit der letzten Zurücksetzung des Attributs.

storagegrid_s3_data_transfers_bytes_retrieved

Die Gesamtmenge der von S3-Clients von diesem Speicherknoten abgerufenen Daten seit der letzten Zurücksetzung des Attributs.

storagegrid_s3_operations_failed

Die Gesamtzahl der fehlgeschlagenen S3-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen derjenigen, die durch einen S3-Autorisierungsfehler verursacht wurden.

storagegrid_s3_operations_successful

Die Gesamtzahl der erfolgreichen S3-Operationen (HTTP-Statuscode 2xx).

storagegrid_s3_operations_unauthorized

Die Gesamtzahl der fehlgeschlagenen S3-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind.

storagegrid_servercertificate_management_interface_cert_expiry_days

Die Anzahl der Tage bis zum Ablauf des Management Interface-Zertifikats.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Die Anzahl der Tage bis zum Ablauf des Object Storage API-Zertifikats.

storagegrid_service_cpu_seconds

Die kumulative Zeit, die die CPU seit der Installation von diesem Dienst verwendet wurde.

storagegrid_service_memory_usage_bytes

Die Menge an Arbeitsspeicher (RAM), die derzeit von diesem Dienst verwendet wird. Dieser Wert ist identisch mit dem Wert, der vom Linux-Dienstprogramm „top“ als RES angezeigt wird.

storagegrid_service_network_received_bytes

Die Gesamtmenge der von diesem Dienst seit der Installation empfangenen Daten.

storagegrid_service_network_transmitted_bytes

Die Gesamtmenge der von diesem Dienst gesendeten Daten.

storagegrid_service_restarts

Die Gesamtzahl der Neustarts des Dienstes.

storagegrid_service_runtime_seconds

Die Gesamtzeit, die der Dienst seit der Installation ausgeführt wurde.

storagegrid_service_uptime_seconds

Die Gesamtzeit, die der Dienst seit dem letzten Neustart ausgeführt wurde.

storagegrid_storage_state_current

Der aktuelle Status der Speicherdienste. Attributwerte sind:

- 10 = Offline
- 15 = Wartung
- 20 = Schreibgeschützt
- 30 = Online

storagegrid_storage_status

Der aktuelle Status der Speicherdienste. Attributwerte sind:

- 0 = Keine Fehler
- 10 = Im Übergang
- 20 = Nicht genügend freier Speicherplatz
- 30 = Datenträger nicht verfügbar
- 40 = Fehler

storagegrid_storage_utilization_data_bytes

Eine Schätzung der Gesamtgröße der replizierten und löschcodierten Objektdaten auf dem Speicherknoten.

storagegrid_storage_utilization_metadata_allowed_bytes

Der Gesamtspeicherplatz auf Volume 0 jedes Speicherknotens, der für Objektmetadaten zulässig ist. Dieser Wert ist immer kleiner als der tatsächliche Speicherplatz, der für Metadaten auf einem Knoten reserviert ist, da ein Teil des reservierten Speicherplatzes für wichtige Datenbankvorgänge (wie Komprimierung und Reparatur) und zukünftige Hardware- und Software-Upgrades benötigt wird. Der zulässige Speicherplatz für Objektmetadaten steuert die Gesamtobjektkapazität.

storagegrid_storage_utilization_metadata_bytes

Die Menge der Objektmetadaten auf Speichervolume 0 in Bytes.

storagegrid_storage_utilization_total_space_bytes

Die Gesamtmenge an Speicherplatz, die allen Objektspeichern zugewiesen ist.

storagegrid_storage_utilization_usable_space_bytes

Die Gesamtmenge des verbleibenden Objektspeicherplatzes. Berechnet durch Addition des verfügbaren Speicherplatzes für alle Objektspeicher auf dem Speicherknoten.

storagegrid_swift_data_transfers_bytes_ingested

Die Gesamtmenge der von Swift-Clients in diesen Speicherknoten aufgenommenen Daten seit der letzten

Zurücksetzung des Attributs.

storagegrid_swift_data_transfers_bytes_retrieved
Die Gesamtmenge der von Swift-Clients von diesem Speicherknoten abgerufenen Daten seit der letzten Zurücksetzung des Attributs.

storagegrid_swift_operations_failed
Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen derjenigen, die durch einen Swift-Autorisierungsfehler verursacht wurden.

storagegrid_swift_operations_successful
Die Gesamtzahl der erfolgreichen Swift-Operationen (HTTP-Statuscode 2xx).

storagegrid_swift_operations_unauthorized
Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind (HTTP-Statuscodes 401, 403, 405).

storagegrid_tenant_usage_data_bytes
Die logische Größe aller Objekte für den Mandanten.

storagegrid_tenant_usage_object_count
Die Anzahl der Objekte für den Mandanten.

storagegrid_tenant_usage_quota_bytes
Die maximale Menge an logischem Speicherplatz, der für die Objekte des Mandanten verfügbar ist. Wenn keine Kontingentmetrik angegeben ist, steht unbegrenzter Speicherplatz zur Verfügung.

Holen Sie sich eine Liste aller Metriken

Um die vollständige Liste der Metriken zu erhalten, verwenden Sie die Grid Management API.

1. Wählen Sie oben im Grid Manager das Hilfesymbol und dann **API-Dokumentation** aus.
2. Suchen Sie die **Metriken**-Operationen.
3. Führen Sie den `GET /grid/metric-names` Betrieb.
4. Laden Sie die Ergebnisse herunter.

Referenz zu Protokolldateien

Referenz zu Protokolldateien

StorageGRID bietet Protokolle, die zum Erfassen von Ereignissen, Diagnosemeldungen und Fehlerzuständen verwendet werden. Möglicherweise werden Sie gebeten, Protokolldateien zu sammeln und sie an den technischen Support weiterzuleiten, um bei der Fehlerbehebung zu helfen.

Die Protokolle sind wie folgt kategorisiert:

- "StorageGRID -Softwareprotokolle"
- "Bereitstellungs- und Wartungsprotokolle"
- "Über das bycast.log"

Die für jeden Protokolltyp bereitgestellten Details dienen nur als Referenz. Die Protokolle sind für die erweiterte Fehlerbehebung durch den technischen Support vorgesehen. Fortgeschrittene Techniken, bei denen der Problemverlauf mithilfe der Prüfprotokolle und der Anwendungsprotokolldateien rekonstruiert wird, gehen über den Rahmen dieser Anweisungen hinaus.

Zugriff auf die Protokolle

Um auf die Protokolle zuzugreifen, können Sie"Sammeln von Protokolldateien und Systemdaten" von einem oder mehreren Knoten als einzelnes Protokolldateiarchiv. Oder wenn der primäre Admin-Knoten nicht verfügbar ist oder einen bestimmten Knoten nicht erreichen kann, können Sie wie folgt auf einzelne Protokolldateien für jeden Grid-Knoten zugreifen:

1. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
2. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
3. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
4. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

Exportieren Sie Protokolle auf den Syslog-Server

Das Exportieren der Protokolle auf den Syslog-Server bietet folgende Möglichkeiten:

- Erhalten Sie eine Liste aller Grid Manager- und Tenant Manager-Anfragen sowie S3- und Swift-Anfragen.
- Bessere Transparenz bei S3-Anfragen, die Fehler zurückgeben, ohne die durch Audit-Protokollierungsmethoden verursachten Leistungseinbußen.
- Zugriff auf HTTP-Layer-Anfragen und Fehlercodes, die leicht zu analysieren sind.
- Bessere Transparenz bei Anfragen, die von Verkehrsklassifizierern beim Load Balancer blockiert wurden.

Informationen zum Exportieren der Protokolle finden Sie unter"Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Protokolldateikategorien

Das StorageGRID Protokolldateiarchiv enthält die für jede Kategorie beschriebenen Protokolle und zusätzliche Dateien, die Metriken und die Ausgabe von Debugbefehlen enthalten.

Archivspeicherort	Beschreibung
Prüfung	Während des normalen Systembetriebs generierte Prüfmeldungen.
Basis-Betriebssystem-Protokolle	Grundlegende Informationen zum Betriebssystem, einschließlich StorageGRID Image-Versionen.
Bündel	Globale Konfigurationsinformationen (Bundles).
Kassandra	Cassandra-Datenbankinformationen und Reaper-Reparaturprotokolle.

Archivspeicherort	Beschreibung
ec	VCS-Informationen zum aktuellen Knoten und EC-Gruppeninformationen nach Profil-ID.
Netz	Allgemeine Grid-Protokolle einschließlich Debug(`bycast.log`) Und `servermanager` Protokolle.
grid.json	Von allen Knoten gemeinsam genutzte Grid-Konfigurationsdatei. Zusätzlich, `node.json` ist spezifisch für den aktuellen Knoten.
hagroups	Metriken und Protokolle für Hochverfügbarkeitsgruppen.
installieren	`Gdu-server`und Protokolle installieren.
Lambda-Schiedsrichter	Protokolle im Zusammenhang mit der S3 Select-Proxy-Anforderung.
lumberjack.log	Debug-Meldungen im Zusammenhang mit der Protokollsammlung.
Metriken	Serviceprotokolle für Grafana, Jaeger, Node Exporter und Prometheus.
Sonstiges	Verschiedene Zugriffs- und Fehlerprotokolle.
MySQL	Die MariaDB-Datenbankkonfiguration und zugehörige Protokolle.
netto	Von netzwerkbezogenen Skripten und dem Dynip-Dienst generierte Protokolle.
nginx	Konfigurationsdateien und Protokolle für Load Balancer und Grid-Föderation. Enthält auch Grid Manager- und Tenant Manager-Verkehrsprotokolle.

Archivspeicherort	Beschreibung
nginx-gw	• `access.log`: Grid Manager und Tenant Manager fordern Protokollnachrichten an. ◦ Diesen Nachrichten vorangestellt ist `mgmt:` beim Exportieren mit Syslog. ◦ Das Format dieser Protokollnachrichten ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Eingehende Cross-Grid-Replikationsanforderungen. ◦ Diesen Nachrichten vorangestellt ist `cgr:` beim Exportieren mit Syslog. ◦ Das Format dieser Protokollnachrichten ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: S3- und Swift-Anfragen an Load Balancer-Endpunkte. ◦ Diesen Nachrichten vorangestellt ist `endpoint:` beim Exportieren mit Syslog. ◦ Das Format dieser Protokollnachrichten ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Bezieht sich auf die neue DNS-Check-Warnung.
ntp	NTP-Konfigurationsdatei und -Protokolle.
Verwaiste Objekte	Protokolle zu verwaisten Objekten.
Betriebssystem	Knoten- und Netzzustandsdatei, einschließlich Dienste `pid` .
andere	Protokolldateien unter `/var/local/log` die nicht in anderen Ordnern gesammelt werden.
Leistung	Leistungsinformationen zu CPU, Netzwerk und Festplatten-E/A.
Prometheus-Daten	Aktuelle Prometheus-Metriken, wenn die Protokollsammlung Prometheus-Daten enthält.
Bereitstellung	Protokolle im Zusammenhang mit dem Grid-Bereitstellungsprozess.
Floß	Protokolle vom Raft-Cluster, die in Plattformdiensten verwendet werden.

Archivspeicherort	Beschreibung
ssh	Protokolle im Zusammenhang mit der SSH-Konfiguration und dem SSH-Dienst.
SNMP	SNMP-Agentenkonfiguration zum Senden von SNMP-Benachrichtigungen.
Sockets-Daten	Socket-Daten für die Netzwerkfehlerbehebung.
system-commands.txt	Ausgabe von StorageGRID Containerbefehlen. Enthält Systeminformationen, beispielsweise zur Netzwerk- und Festplattennutzung.
Synchronisierungs-Wiederherstellungspaket	Bezieht sich auf die Aufrechterhaltung der Konsistenz des neuesten Wiederherstellungspakets auf allen Admin-Knoten und Speicherknoten, die den ADC-Dienst hosten.

StorageGRID -Softwareprotokolle

Sie können StorageGRID Protokolle zur Fehlerbehebung verwenden.

Wenn Sie Ihre Protokolle an einen externen Syslog-Server senden oder das Ziel der Audit-Informationen ändern möchten, wie z. B. die `bycast.log` Und `nms.log` , sehen"Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Allgemeine StorageGRID Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/bycast.log	Die primäre StorageGRID Fehlerbehebungsdatei. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events**.	Alle Knoten
/var/local/log/bycast-err.log	Enthält eine Teilmenge von `bycast.log` (Meldungen mit Schweregrad ERROR und CRITICAL). Außerdem werden im System KRITISCHE Meldungen angezeigt. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events**.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/core/	Enthält alle Core-Dump-Dateien, die bei einer abnormalen Programmbeendigung erstellt werden. Mögliche Ursachen sind Assertionsfehler, Verstöße oder Thread-Timeouts. **Hinweis**: Die Datei `/var/local/core/kexec_cmd` ist normalerweise auf Appliance-Knoten vorhanden und weist nicht auf einen Fehler hin.	Alle Knoten

Verschlüsselungsbezogene Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/ssh-config-generation.log	Enthält Protokolle im Zusammenhang mit der Generierung von SSH-Konfigurationen und dem Neuladen von SSH-Diensten.	Alle Knoten
/var/local/log/nginx/config-generation.log	Enthält Protokolle im Zusammenhang mit der Generierung von Nginx-Konfigurationen und dem Neuladen von Nginx-Diensten.	Alle Knoten
/var/local/log/nginx-gw/config-generation.log	Enthält Protokolle im Zusammenhang mit der Generierung von nginx-gw-Konfigurationen (und dem Neuladen von nginx-gw-Diensten).	Admin- und Gateway-Knoten
/var/local/log/update-cipher-configurations.log	Enthält Protokolle im Zusammenhang mit der Konfiguration von TLS- und SSH-Richtlinien.	Alle Knoten

Grid-Föderationsprotokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/update_grid_federation_config.log	Enthält Protokolle im Zusammenhang mit der Generierung von Nginx- und Nginx-GW-Konfigurationen für Grid-Föderationsverbindungen.	Alle Knoten

NMS-Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/nms.log	• Erfasst Benachrichtigungen vom Grid Manager und Tenant Manager. • Erfasst Ereignisse im Zusammenhang mit dem Betrieb des NMS-Dienstes. Zum Beispiel E-Mail-Benachrichtigungen und Konfigurationsänderungen. • Enthält XML-Bundle-Updates, die sich aus im System vorgenommenen Konfigurationsänderungen ergeben. • Enthält Fehlermeldungen im Zusammenhang mit dem einmal täglich durchgeführten Downsampling der Attribute. • Enthält Fehlermeldungen des Java-Webservers, beispielsweise Fehler bei der Seitengenerierung und HTTP-Status 500-Fehler.	Admin-Knoten
/var/local/log/nms.errlog	Enthält Fehlermeldungen im Zusammenhang mit MySQL-Datenbank-Upgrades. Enthält den Standardfehler-Stream (stderr) der entsprechenden Dienste. Es gibt eine Protokolldatei pro Dienst. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Admin-Knoten
/var/local/log/nms.requestlog	Enthält Informationen zu ausgehenden Verbindungen von der Management-API zu internen StorageGRID Diensten.	Admin-Knoten

Server Manager-Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/servermanager.log	Protokolldatei für die auf dem Server ausgeführte Server Manager-Anwendung.	Alle Knoten
/var/local/log/GridstatBackend.errlog	Protokolldatei für die Server Manager-GUI-Backend-Anwendung.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/gridstat.errlog	Protokolldatei für die Server Manager-GUI.	Alle Knoten

StorageGRID -Dienstprotokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/acct.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/adc.errlog	Enthält den Standardfehler-Stream (stderr) der entsprechenden Dienste. Es gibt eine Protokolldatei pro Dienst. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/ams.errlog		Admin-Knoten
/var/local/log/cassandra/system.log	Informationen zum Metadatenspeicher (Cassandra-Datenbank), die verwendet werden können, wenn beim Hinzufügen neuer Speicherknoten Probleme auftreten oder die Nodetool-Reparaturaufgabe hängen bleibt.	Speicherknoten
/var/local/log/cassandra-reaper.log	Informationen zum Cassandra Reaper-Dienst, der Reparaturen der Daten in der Cassandra-Datenbank durchführt.	Speicherknoten
/var/local/log/cassandra-reaper.errlog	Fehlerinformationen für den Cassandra Reaper-Dienst.	Speicherknoten
/var/local/log/chunk.errlog		Speicherknoten
/var/local/log/cmn.errlog		Admin-Knoten
/var/local/log/cms.errlog	Diese Protokolldatei ist möglicherweise auf Systemen vorhanden, die von einer älteren Version von StorageGRID aktualisiert wurden. Es enthält Legacy-Informationen.	Speicherknoten
/var/local/log/dds.errlog		Speicherknoten
/var/local/log/dmv.errlog		Speicherknoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/dynip*	Enthält Protokolle im Zusammenhang mit dem Dynip-Dienst, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Knoten
/var/local/log/grafana.log	Das mit dem Grafana-Dienst verknüpfte Protokoll, das zur Visualisierung von Metriken im Grid Manager verwendet wird.	Admin-Knoten
/var/local/log/hagroups.log	Das mit Hochverfügbarkeitsgruppen verknüpfte Protokoll.	Admin-Knoten und Gateway-Knoten
/var/local/log/hagroups_events.log	Verfolgt Statusänderungen, wie etwa den Übergang von BACKUP zu MASTER oder FAULT.	Admin-Knoten und Gateway-Knoten
/var/local/log/idnt.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/jaeger.log	Das mit dem Jaeger-Dienst verknüpfte Protokoll, das zur Ablaufverfolgung verwendet wird.	Alle Knoten
/var/local/log/kstn.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/lambda*	Enthält Protokolle für den S3 Select-Dienst.	Admin- und Gateway-Knoten Nur bestimmte Admin- und Gateway-Knoten enthalten dieses Protokoll. Siehe die"S3 Select-Anforderungen und -Einschränkungen für Admin- und Gateway-Knoten" .
/var/local/log/ldr.errlog		Speicherknoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/miscd/*.log	Enthält Protokolle für den MISCd-Dienst (Information Service Control Daemon), der eine Schnittstelle zum Abfragen und Verwalten von Diensten auf anderen Knoten und zum Verwalten von Umgebungskonfigurationen auf dem Knoten bereitstellt, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Knoten
/var/local/log/nginx/*.log	Enthält Protokolle für den Nginx-Dienst, der als Authentifizierungs- und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und Dynip) fungiert, um über HTTPS-APIs mit Diensten auf anderen Knoten kommunizieren zu können.	Alle Knoten
/var/local/log/nginx-gw/*.log	Enthält allgemeine Protokolle im Zusammenhang mit dem nginx-gw-Dienst, einschließlich Fehlerprotokollen und Protokollen für die eingeschränkten Admin-Ports auf Admin-Knoten.	Admin-Knoten und Gateway-Knoten
/var/local/log/nginx-gw/cgr-access.log.gz	Enthält Zugriffsprotokolle im Zusammenhang mit dem gitterübergreifenden Replikationsverkehr.	Admin-Knoten, Gateway-Knoten oder beides, basierend auf der Grid-Föderationskonfiguration. Wird nur im Zielraster für die rasterübergreifende Replikation gefunden.
/var/local/log/nginx-gw/endpoint-access.log.gz	Enthält Zugriffsprotokolle für den Load Balancer-Dienst, der den Lastenausgleich des S3-Verkehrs von Clients zu Speicherknoten bereitstellt.	Admin-Knoten und Gateway-Knoten
/var/local/log/persistenz*	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Stammfestplatte verwaltet, die über einen Neustart hinaus bestehen bleiben müssen.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/prometheus.log	Enthält für alle Knoten das Dienstprotokoll des Knotenexporters und das Dienstprotokoll des Ade-Exporter-Metriken. Enthält für Admin-Knoten auch Protokolle für die Dienste Prometheus und Alert Manager.	Alle Knoten
/var/local/log/raft.log	Enthält die Ausgabe der vom RSM-Dienst für das Raft-Protokoll verwendeten Bibliothek.	Speicherknoten mit RSM-Dienst
/var/local/log/rms.errlog	Enthält Protokolle für den Dienst Replicated State Machine Service (RSM), der für S3-Plattformdienste verwendet wird.	Speicherknoten mit RSM-Dienst
/var/local/log/ssm.errlog		Alle Knoten
/var/local/log/update-s3vs-domains.log	Enthält Protokolle im Zusammenhang mit der Verarbeitung von Updates für die Konfiguration der virtuell gehosteten S3-Domänennamen. Weitere Informationen finden Sie in den Anweisungen zum Implementieren von S3-Clientanwendungen.	Admin- und Gateway-Knoten
/var/local/log/update-snmp-firewall.*	Enthalten Protokolle zu den Firewall-Ports, die für SNMP verwaltet werden.	Alle Knoten
/var/local/log/update-sysl.log	Enthält Protokolle zu Änderungen an der Syslog-Konfiguration des Systems.	Alle Knoten
/var/local/log/update-traffic-classes.log	Enthält Protokolle im Zusammenhang mit Änderungen an der Konfiguration der Verkehrsklassifizierer.	Admin- und Gateway-Knoten
/var/local/log/update-utcn.log	Enthält Protokolle im Zusammenhang mit dem nicht vertrauenswürdigen Client-Netzwerkmodus auf diesem Knoten.	Alle Knoten

Ähnliche Informationen

- "Über das bycast.log"
- "Verwenden Sie die S3 REST-API"

Bereitstellungs- und Wartungsprotokolle

Sie können die Bereitstellungs- und Wartungsprotokolle zur Fehlerbehebung verwenden.

Dateiname	Hinweise	Gefunden auf
/var/local/log/install.log	Wird während der Softwareinstallation erstellt. Enthält eine Aufzeichnung der Installationsereignisse.	Alle Knoten
/var/local/log/expansion-progress.log	Im Zuge der Erweiterungsarbeiten entstanden. Enthält eine Aufzeichnung der Erweiterungsereignisse.	Speicherknoten
/var/local/log/pa-move.log	Erstellt während der Ausführung des `pa-move.sh` Skript.	Primärer Admin-Knoten
/var/local/log/pa-move-new_pa.log	Erstellt während der Ausführung des `pa-move.sh` Skript.	Primärer Admin-Knoten
/var/local/log/pa-move-old_pa.log	Erstellt während der Ausführung des `pa-move.sh` Skript.	Primärer Admin-Knoten
/var/local/log/gdu-server.log	Erstellt vom GDU-Dienst. Enthält Ereignisse im Zusammenhang mit Bereitstellungs- und Wartungsverfahren, die vom primären Admin-Knoten verwaltet werden.	Primärer Admin-Knoten
/var/local/log/send_admin_hw.log	Wird während der Installation erstellt. Enthält Debuginformationen zur Kommunikation eines Knotens mit dem primären Admin-Knoten.	Alle Knoten
/var/local/log/upgrade.log	Während des Software-Upgrades erstellt. Enthält eine Aufzeichnung der Software-Update-Ereignisse.	Alle Knoten

Über das bycast.log

Die Datei `/var/local/log/bycast.log` ist die primäre Fehlerbehebungsdatei für die StorageGRID -Software. Es gibt eine `bycast.log` Datei für jeden Rasterknoten. Die Datei enthält Nachrichten, die für diesen Grid-Knoten spezifisch sind.

Die Datei `/var/local/log/bycast-err.log` ist eine Teilmenge von `bycast.log` . Es enthält Meldungen mit den Schweregraden FEHLER und KRITISCH.

Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Dateirotation für bycast.log

Wenn die `bycast.log` Wenn die Datei 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet.

Die gespeicherte Datei wird umbenannt `bycast.log.1` und die neue Datei heißt `bycast.log` . Wenn das neue `bycast.log` erreicht 1 GB, `bycast.log.1` wird umbenannt und komprimiert und wird `bycast.log.2.gz` , Und `bycast.log` wird umbenannt `bycast.log.1` .

Die Rotationsgrenze für `bycast.log` sind 21 Dateien. Als die 22. Version des `bycast.log` Datei erstellt wird, wird die älteste Datei gelöscht.

Die Rotationsgrenze für `bycast-err.log` sind sieben Dateien.

> Wenn eine Protokolldatei komprimiert wurde, dürfen Sie sie nicht an denselben Speicherort dekomprimieren, an dem sie geschrieben wurde. Das Dekomprimieren der Datei an denselben Speicherort kann die Protokollrotationsskripte beeinträchtigen.

Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Ähnliche Informationen

"Erfassen von Protokolldateien und Systemdaten"

Nachrichten im bycast.log

Nachrichten in `bycast.log` werden von der ADE (Asynchronous Distributed Environment) geschrieben. ADE ist die Laufzeitumgebung, die von den Diensten jedes Grid-Knotens verwendet wird.

Beispiel einer ADE-Nachricht:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE-Nachrichten enthalten die folgenden Informationen:

Nachrichtensegment	Wert im Beispiel
Knoten-ID	12455685
ADE-Prozess-ID	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHR
UTC-Systemzeit	2019-05-05T27T17:10:29.784677 (JJJJ-MM-TTTHH:MM:SS.uuuuuu)
Schweregrad	FEHLER

Nachrichtensegment	Wert im Beispiel
Interne Trackingnummer	0906
Nachricht	SVMR: Integritätsprüfung auf Datenträger 3 ist mit der Begründung „TOUT“ fehlgeschlagen

Schweregrade der Nachrichten in bycast.log

Die Nachrichten in `bycast.log` werden Schweregrade zugewiesen.

Beispiel:

- **HINWEIS** – Ein Ereignis ist eingetreten, das aufgezeichnet werden sollte. Die meisten Protokollnachrichten befinden sich auf dieser Ebene.
- **WARNUNG** – Es ist ein unerwarteter Zustand aufgetreten.
- **FEHLER** – Es ist ein schwerwiegender Fehler aufgetreten, der den Betrieb beeinträchtigen wird.
- **KRITISCH** – Es ist ein anormaler Zustand aufgetreten, der den normalen Betrieb gestoppt hat. Sie sollten sich sofort um die zugrunde liegende Erkrankung kümmern.

Fehlercodes in `bycast.log`

Die meisten Fehlermeldungen in `bycast.log` enthalten Fehlercodes.

Die folgende Tabelle listet häufige nicht-numerische Codes in `bycast.log` Die genaue Bedeutung eines nicht numerischen Codes hängt vom Kontext ab, in dem er gemeldet wird.

Fehlercode	Bedeutung
SUCS	Kein Fehler
GERR	Unbekannt
CANC	Abgesagt
ABRT	Abgebrochen
TOUT	Time-out
INVL	Ungültig
NFND	Nicht gefunden
VERS	Version
KONF	Konfiguration

Fehlercode	Bedeutung
SCHEITERN	Fehlgeschlagen
ICPL	Unvollständig
ERLEDIGT	Erledigt
SUNV	Dienst nicht verfügbar

Die folgende Tabelle listet die numerischen Fehlercodes in `bycast.log` .

Fehlernummer	Fehlercode	Bedeutung
001	EPERM	Betrieb nicht zulässig
002	ENOENT	Keine solche Datei oder Verzeichnis
003	ESRCH	Kein solcher Prozess
004	EINTR	Unterbrochener Systemaufruf
005	EIO	E/A-Fehler
006	ENXIO	Kein solches Gerät oder keine solche Adresse
007	E2BIG	Argumentliste zu lang
008	ENOEXEC	Exec-Formatfehler
009	EBADF	Ungültige Dateinummer
010	ECHILD	Keine untergeordneten Prozesse
011	WIEDER	Versuchen Sie es erneut
012	ENOMEM	Nicht genügend Arbeitsspeicher
013	EACCES	Zugriff verweigert
014	EFAULT	Falsche Adresse
015	ENOTBLK	Blockgerät erforderlich
016	EBUSY	Gerät oder Ressource beschäftigt

Fehlernummer	Fehlercode	Bedeutung
017	EEXIST	Datei existiert
018	EXDEV	Geräteübergreifende Verknüpfung
019	ENODEV	Kein solches Gerät
020	ENOTDIR	Kein Verzeichnis
021	EISDIR	Ist ein Verzeichnis
022	EINVAL	Ungültiges Argument
023	ENFILE	Dateitabellenüberlauf
024	EMFILE	Zu viele geöffnete Dateien
025	ENOTTY	Keine Schreibmaschine
026	ETXTBSY	Textdatei belegt
027	EFBIG	Datei zu groß
028	ENOSPC	Kein Speicherplatz mehr auf dem Gerät
029	ESPEIPE	Unerlaubte Suche
030	EROFS	Schreibgeschütztes Dateisystem
031	EMLINK	Zu viele Links
032	EPIPE	Rohrbruch
033	EDOM	Mathematisches Argument außerhalb des Funktionsumfangs
034	ERANGE	Matheergebnis nicht darstellbar
035	EDEADLK	Es kommt zu einem Ressourcen-Deadlock
036	ENAMETOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperren verfügbar

Fehlernummer	Fehlercode	Bedeutung
038	ENOSYS	Funktion nicht implementiert
039	VERFÜHRUNG	Verzeichnis nicht leer
040	ELOOP	Zu viele symbolische Links gefunden
041		
042	ENOMSG	Keine Nachricht des gewünschten Typs
043	EIDRM	Kennung entfernt
044	EMHRNG	Kanalnummer außerhalb des gültigen Bereichs
045	EL2NSYNC	Ebene 2 nicht synchronisiert
046	EL3HLT	Level 3 gestoppt
047	EL3RST	Level 3 zurücksetzen
048	ELNRNG	Linknummer außerhalb des gültigen Bereichs
049	EUNATCH	Protokolltreiber nicht angeschlossen
050	ENOCSI	Keine CSI-Struktur verfügbar
051	EL2HLT	Level 2 gestoppt
052	EBADE	Ungültiger Umtausch
053	EBADR	Ungültiger Anforderungsdeskriptor
054	EXFULL	Austausch voll
055	ENOANO	Keine Anode
056	EBADRQC	Ungültiger Anforderungscode
057	EBADSLT	Ungültiger Steckplatz
058		
059	EBFONT	Ungültiges Schriftartdateiformat

Fehlernummer	Fehlercode	Bedeutung
060	ENOSTR	Gerät ist kein Stream
061	ENODATA	Keine Daten verfügbar
062	ETIME	Timer abgelaufen
063	ENOSR	Keine Stream-Ressourcen mehr vorhanden
064	ENONET	Maschine ist nicht im Netzwerk
065	ENOPKG	Paket nicht installiert
066	EREMOTE	Objekt ist remote
067	ENOLINK	Die Verbindung wurde getrennt
068	EADV	Fehler melden
069	ESRMNT	Srmount-Fehler
070	ECOMM	Kommunikationsfehler beim Senden
071	EPROTO	Protokollfehler
072	EMULTIHOP	Multihop versucht
073	EDOTDOT	RFS-spezifischer Fehler
074	EBADMSG	Keine Datennachricht
075	ÜBERLAUF	Wert zu groß für definierten Datentyp
076	ENOTUNIQ	Name im Netzwerk nicht eindeutig
077	EBADFD	Dateideskriptor in fehlerhaftem Zustand
078	EREMCHG	Remote-Adresse geändert
079	ELIBACC	Auf eine benötigte gemeinsam genutzte Bibliothek kann nicht zugegriffen werden
080	ELIBBAD	Zugriff auf eine beschädigte gemeinsam genutzte Bibliothek

Fehlernummer	Fehlercode	Bedeutung
081	ELIBSCN	
082	ELIBMAX	Versuch, zu viele gemeinsam genutzte Bibliotheken einzubinden
083	ELIBEXEC	Eine gemeinsam genutzte Bibliothek kann nicht direkt ausgeführt werden
084	EILSEQ	Unzulässige Bytefolge
085	ERESTART	Unterbrochener Systemaufruf sollte neu gestartet werden
086	ESTRPIPE	Streams-Pipe-Fehler
087	EUSERS	Zu viele Benutzer
088	ENOTSOCK	Socket-Operation auf Nicht-Socket
089	EDESTADDRREQ	Zieladresse erforderlich
090	EMSGSIZE	Nachricht zu lang
091	EPROTOTYP	Falscher Protokolltyp für Socket
092	ENOPROTOOPT	Protokoll nicht verfügbar
093	EPROTONOSUPPORT	Protokoll nicht unterstützt
094	ESOCKTNOSUPPORT	Socket-Typ wird nicht unterstützt
095	EOPNOTSUPP	Vorgang wird am Transportendpunkt nicht unterstützt
096	EPFNOSUPPORT	Protokollfamilie wird nicht unterstützt
097	EAFNOSUPPORT	Adressfamilie wird vom Protokoll nicht unterstützt
098	EADDRINUSE	Adresse bereits verwendet
099	EADDRNOTAVAIL	Die angeforderte Adresse kann nicht zugewiesen werden
100	ENETDOWN	Das Netzwerk ist ausgefallen

Fehlernummer	Fehlercode	Bedeutung
101	ENETUNREACH	Netzwerk ist nicht erreichbar
102	ENETRESET	Die Netzwerkverbindung wurde aufgrund eines Resets unterbrochen
103	ABGEBROCHEN	Software verursachte Verbindungsabbruch
104	ECONNRESET	Verbindung vom Peer zurückgesetzt
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Nach dem Herunterfahren des Transportendpunkts kann nicht gesendet werden
109	ETOOMANYREFS	Zu viele Referenzen: kann nicht zusammengefügt werden
110	ETIMEDOUT	Verbindungs-Timeout
111	ECONNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHOSTUNREACH	Keine Route zum Host
114	BEREITS	Vorgang läuft bereits
115	EINPROGRESS	Der Vorgang läuft derzeit
116		
117	EUCLEAN	Struktur muss gereinigt werden
118	ENOTNAM	Keine XENIX-Datei mit benanntem Typ
119	ENAVAIL	Keine XENIX-Semaphoren verfügbar
120	EISNAM	Ist eine benannte Typdatei

Fehlernummer	Fehlercode	Bedeutung
121	EREMOTEIO	Remote-E/A-Fehler
122	EDQUOT	Kontingent überschritten
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ABGESAGT	Vorgang abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEY ABGELAUFEN	Schlüssel ist abgelaufen
128	EKEY WIDERRUFEN	Schlüssel wurde widerrufen
129	EKEYABGELEHNT	Der Schlüssel wurde vom Dienst abgelehnt
130	EOWNERDEAD	Für robuste Mutexe: Besitzer gestorben
131	NICHT WIEDERHERSTELLBAR	Für robuste Mutexe: Zustand nicht wiederherstellbar

Konfigurieren von Überwachungsnachrichten und Protokollzielen

Überlegungen zur Verwendung eines externen Syslog-Servers

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID , den Sie zum Sammeln von Systemprüfungsinformationen an einem einzigen Ort verwenden können. Durch die Verwendung eines externen Syslog-Servers können Sie den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten. Für StorageGRID ist das Paketformat für ausgehende Syslog-Nachrichten mit RFC 3164 kompatibel.

Zu den Arten von Prüfinformationen, die Sie an den externen Syslog-Server senden können, gehören:

- Audit-Protokolle mit den während des normalen Systembetriebs generierten Audit-Meldungen
- Sicherheitsrelevante Ereignisse wie Anmeldungen und Eskalationen zum Root
- Anwendungsprotokolle, die möglicherweise angefordert werden, wenn es notwendig ist, einen Supportfall zu eröffnen, um ein aufgetretenes Problem zu beheben

Wann Sie einen externen Syslog-Server verwenden sollten

Ein externer Syslog-Server ist besonders nützlich, wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Anwendungen verwenden oder alle Auditdaten behalten möchten. Durch das Senden von Auditinformationen an einen externen Syslog-Server können Sie:

- Erfassen und verwalten Sie Auditinformationen wie Auditmeldungen, Anwendungsprotokolle und Sicherheitsereignisse effizienter.
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da Audit-Informationen direkt von den verschiedenen Speicherknoten an den externen Syslog-Server übertragen werden, ohne dass ein Admin-Knoten durchlaufen werden muss.

> Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit mehr als 8.192 Bytes am Ende der Nachricht abgeschnitten, um den allgemeinen Einschränkungen bei Implementierungen externer Syslog-Server zu entsprechen.

> Um die Möglichkeiten zur vollständigen Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers zu maximieren, können bis zu 20 GB lokale Protokolle mit Audit-Datensätzen gespeichert werden.(`localaudit.log`) werden auf jedem Knoten verwaltet.

So konfigurieren Sie einen externen Syslog-Server

Informationen zum Konfigurieren eines externen Syslog-Servers finden Sie unter"Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server" .

Wenn Sie die Verwendung des TLS- oder RELP/TLS-Protokolls konfigurieren möchten, benötigen Sie die folgenden Zertifikate:

- **Server-CA-Zertifikate**: Ein oder mehrere vertrauenswürdige CA-Zertifikate zur Überprüfung des externen Syslog-Servers in PEM-Kodierung. Wenn es weggelassen wird, wird das Standard-Grid-CA-Zertifikat verwendet.
- **Client-Zertifikat**: Das Client-Zertifikat zur Authentifizierung gegenüber dem externen Syslog-Server in PEM-Kodierung.
- **Privater Schlüssel des Clients**: Privater Schlüssel für das Client-Zertifikat in PEM-Kodierung.

> Wenn Sie ein Client-Zertifikat verwenden, müssen Sie auch einen privaten Client-Schlüssel verwenden. Wenn Sie einen verschlüsselten privaten Schlüssel angeben, müssen Sie auch die Passphrase angeben. Die Verwendung eines verschlüsselten privaten Schlüssels bietet keinen nennenswerten Sicherheitsvorteil, da Schlüssel und Passphrase gespeichert werden müssen. Aus Gründen der Einfachheit wird die Verwendung eines unverschlüsselten privaten Schlüssels empfohlen, sofern verfügbar.

So schätzen Sie die Größe des externen Syslog-Servers

Normalerweise ist Ihr Grid so dimensioniert, dass ein erforderlicher Durchsatz erreicht wird, der in S3-Operationen pro Sekunde oder Bytes pro Sekunde definiert ist. Beispielsweise besteht möglicherweise die Anforderung, dass Ihr Grid 1.000 S3-Operationen pro Sekunde oder 2.000 MB pro Sekunde an Objektaufnahmen und -abrufen verarbeiten muss. Sie sollten die Größe Ihres externen Syslog-Servers entsprechend den Datenanforderungen Ihres Grids anpassen.

Dieser Abschnitt enthält einige heuristische Formeln, mit deren Hilfe Sie die Rate und durchschnittliche Größe von Protokollnachrichten verschiedener Typen schätzen können, die Ihr externer Syslog-Server verarbeiten können muss, ausgedrückt in Bezug auf die bekannten oder gewünschten Leistungsmerkmale des Grids (S3-Operationen pro Sekunde).

Verwenden Sie S3-Operationen pro Sekunde in Schätzformeln

Wenn Ihr Grid für einen Durchsatz in Bytes pro Sekunde ausgelegt ist, müssen Sie diese Dimensionierung in S3-Operationen pro Sekunde umrechnen, um die Schätzformeln verwenden zu können. Um den Grid-Durchsatz zu konvertieren, müssen Sie zunächst Ihre durchschnittliche Objektgröße bestimmen. Dies können Sie mithilfe der Informationen in vorhandenen Prüfprotokollen und Metriken (sofern vorhanden) oder mithilfe Ihrer Kenntnisse über die Anwendungen tun, die StorageGRID verwenden. Wenn Ihr Grid beispielsweise so dimensioniert ist, dass ein Durchsatz von 2.000 MB/Sekunde erreicht wird und Ihre durchschnittliche Objektgröße 2 MB beträgt, dann ist Ihr Grid so dimensioniert, dass es 1.000 S3-Operationen pro Sekunde verarbeiten kann (2.000 MB / 2 MB).

> ⓘ Die Formeln zur Dimensionierung externer Syslog-Server in den folgenden Abschnitten stellen Schätzungen für den Normalfall dar (und nicht für den Worst-Case). Abhängig von Ihrer Konfiguration und Arbeitslast kann die Rate der Syslog-Nachrichten oder das Volumen der Syslog-Daten höher oder niedriger sein als in den Formeln vorhergesagt. Die Formeln dienen lediglich als Richtlinien.

Schätzformeln für Audit-Protokolle

Wenn Sie über keine anderen Informationen zu Ihrer S3-Arbeitslast verfügen als über die Anzahl der S3-Operationen pro Sekunde, die Ihr Grid voraussichtlich unterstützen wird, können Sie das Volumen der Prüfprotokolle, die Ihr externer Syslog-Server verarbeiten muss, mithilfe der folgenden Formeln schätzen, unter der Annahme, dass Sie die Prüfebenen auf den Standardwerten belassen (alle Kategorien auf „Normal“ eingestellt, außer „Speicher“, das auf „Fehler“ eingestellt ist):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 2.000 Syslog-Nachrichten pro Sekunde unterstützt und in der Lage sein, Prüfprotokolldaten mit einer Rate von 1,6 MB pro Sekunde zu empfangen (und normalerweise zu speichern).

Wenn Sie mehr über Ihre Arbeitsbelastung wissen, sind genauere Schätzungen möglich. Für Prüfprotokolle sind die wichtigsten zusätzlichen Variablen der Prozentsatz der S3-Operationen, die PUTs (vs. GETS) sind, und die durchschnittliche Größe in Bytes der folgenden S3-Felder (die in der Tabelle verwendeten 4-stelligen Abkürzungen sind Prüfprotokoll-Feldnamen):

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.

Code	Feld	Beschreibung
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Taste	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.

Verwenden wir P, um den Prozentsatz der S3-Operationen darzustellen, die PUTs sind, wobei 0 ≤ P ≤ 1 (also für eine 100 % PUT-Arbeitslast P = 1 und für eine 100 % GET-Arbeitslast P = 0).

Verwenden wir K, um die durchschnittliche Größe der Summe der S3-Kontonamen, des S3-Buckets und des S3-Schlüssels darzustellen. Angenommen, der S3-Kontoname lautet immer my-s3-account (13 Byte), Buckets haben Namen mit fester Länge wie /my/application/bucket-12345 (28 Byte) und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Byte). Dann beträgt der Wert von K 90 (13+13+28+36).

Wenn Sie Werte für P und K ermitteln können, können Sie das Volumen der Prüfprotokolle schätzen, die Ihr externer Syslog-Server verarbeiten muss. Verwenden Sie dazu die folgenden Formeln, vorausgesetzt, Sie belassen die Prüfebenen auf den Standardeinstellungen (alle Kategorien auf „Normal“ eingestellt, außer „Speicher“, das auf „Fehler“ eingestellt ist):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, Ihre Arbeitslast zu 50 % aus PUTs besteht und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte umfassen, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 1.500 Syslog-Nachrichten pro Sekunde unterstützt und in der Lage sein, Prüfprotokolldaten mit einer Rate von etwa 1 MB pro Sekunde zu empfangen (und normalerweise zu speichern).

Schätzformeln für nicht standardmäßige Prüfstufen

Die für Prüfprotokolle bereitgestellten Formeln gehen von der Verwendung der Standardeinstellungen für die Prüfebene aus (alle Kategorien sind auf „Normal“ eingestellt, mit Ausnahme von „Speicher“, das auf „Fehler“ eingestellt ist). Detaillierte Formeln zum Schätzen der Rate und der durchschnittlichen Größe von Überwachungsnachrichten für nicht standardmäßige Überwachungsebeneneinstellungen sind nicht verfügbar. Die folgende Tabelle kann jedoch für eine grobe Schätzung der Rate verwendet werden. Sie können die für Prüfprotokolle bereitgestellte Formel zur Berechnung der Durchschnittsgröße verwenden. Beachten Sie jedoch, dass dies wahrscheinlich zu einer Überschätzung führt, da die „zusätzlichen“ Prüfmeldungen im Durchschnitt kleiner sind als die Standardprüfmeldungen.

Zustand	Formel
Replikation: Audit-Levels alle auf Debug oder Normal eingestellt	Audit-Protokollrate = 8 x S3-Operationsrate
Erasure Coding: Audit-Levels alle auf Debug oder Normal eingestellt	Verwenden Sie dieselbe Formel wie für die Standardeinstellungen

Schätzformeln für Sicherheitsereignisse

Sicherheitsereignisse korrelieren nicht mit S3-Vorgängen und erzeugen normalerweise ein vernachlässigbares Volumen an Protokollen und Daten. Aus diesen Gründen werden keine Schätzformeln bereitgestellt.

Schätzformeln für Anwendungsprotokolle

Wenn Sie über keine anderen Informationen zu Ihrer S3-Arbeitslast verfügen als über die Anzahl der S3-Operationen pro Sekunde, die Ihr Grid voraussichtlich unterstützen wird, können Sie das Volumen der Anwendungsprotokolle, die Ihr externer Syslog-Server verarbeiten muss, mithilfe der folgenden Formeln schätzen:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 3.300 Anwendungsprotokolle pro Sekunde unterstützt und Anwendungsprotokolldaten mit einer Rate von etwa 1,2 MB pro Sekunde empfangen (und speichern) kann.

Wenn Sie mehr über Ihre Arbeitsbelastung wissen, sind genauere Schätzungen möglich. Bei Anwendungsprotokollen sind die wichtigsten zusätzlichen Variablen die Datensicherungsstrategie (Replikation vs. Erasure Coding), der Prozentsatz der S3-Operationen, die PUTs sind (vs. GETs/andere), und die durchschnittliche Größe der folgenden S3-Felder in Bytes (die in der Tabelle verwendeten 4-stelligen Abkürzungen sind die Namen der Prüfprotokollfelder):

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Taste	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.

Beispiele für Größenschätzungen

In diesem Abschnitt werden Beispielfälle erläutert, wie die Schätzformeln für Raster mit den folgenden Datenschutzmethoden verwendet werden können:

- Replikation

- Löschcodierung

Wenn Sie die Replikation zum Schutz Ihrer Daten verwenden

Lassen Sie P den Prozentsatz der S3-Operationen darstellen, die PUTs sind, wobei 0 ≤ P ≤ 1 (also für eine 100 % PUT-Arbeitslast P = 1 und für eine 100 % GET-Arbeitslast P = 0).

Lassen Sie K die durchschnittliche Größe der Summe der S3-Kontonamen, des S3-Buckets und des S3-Schlüssels darstellen. Angenommen, der S3-Kontoname lautet immer my-s3-account (13 Byte), Buckets haben Namen mit fester Länge wie /my/application/bucket-12345 (28 Byte) und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Byte). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie mithilfe der folgenden Formeln das Volumen der Anwendungsprotokolle schätzen, das Ihr externer Syslog-Server verarbeiten können muss.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, Ihre Arbeitslast zu 50 % aus PUTs besteht und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Bytes umfassen, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 1.800 Anwendungsprotokolle pro Sekunde unterstützt und Anwendungsdaten mit einer Rate von 0,5 MB pro Sekunde empfängt (und normalerweise speichert).

Wenn Sie Erasure Coding zum Datenschutz verwenden

Lassen Sie P den Prozentsatz der S3-Operationen darstellen, die PUTs sind, wobei 0 ≤ P ≤ 1 (also für eine 100 % PUT-Arbeitslast P = 1 und für eine 100 % GET-Arbeitslast P = 0).

Lassen Sie K die durchschnittliche Größe der Summe der S3-Kontonamen, des S3-Buckets und des S3-Schlüssels darstellen. Angenommen, der S3-Kontoname lautet immer my-s3-account (13 Byte), Buckets haben Namen mit fester Länge wie /my/application/bucket-12345 (28 Byte) und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Byte). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie mithilfe der folgenden Formeln das Volumen der Anwendungsprotokolle schätzen, das Ihr externer Syslog-Server verarbeiten können muss.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Wenn Ihr Grid beispielsweise für 1.000 S3-Operationen pro Sekunde ausgelegt ist, Ihre Arbeitslast zu 50 % aus PUTs besteht und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte umfassen, sollte Ihr externer Syslog-Server so dimensioniert sein, dass er 2.250 Anwendungsprotokolle pro Sekunde unterstützt und in der Lage sein, Anwendungsdaten mit einer Rate von 0,6 MB pro Sekunde zu empfangen (und normalerweise zu speichern).

Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server

Sie können eine Reihe von Einstellungen im Zusammenhang mit Prüfmeldungen konfigurieren. Sie können die Anzahl der aufgezeichneten Prüfmeldungen anpassen, alle HTTP-Anforderungsheader definieren, die Sie in die Prüfmeldungen zum Lesen und Schreiben des Clients aufnehmen möchten, einen externen Syslog-Server konfigurieren und angeben, wohin Prüfprotokolle, Sicherheitsereignisprotokolle und StorageGRID Softwareprotokolle gesendet werden.

Prüfmeldungen und -protokolle zeichnen Systemaktivitäten und Sicherheitsereignisse auf und sind wichtige Tools zur Überwachung und Fehlerbehebung. Alle StorageGRID -Knoten generieren Prüfmeldungen und Protokolle, um Systemaktivitäten und Ereignisse zu verfolgen.

Optional können Sie einen externen Syslog-Server konfigurieren, um Audit-Informationen remote zu speichern. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Prüfnachrichten auf die Leistung minimiert, ohne die Vollständigkeit der Prüfdaten zu verringern. Ein externer Syslog-Server ist besonders nützlich, wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Anwendungen verwenden oder alle Auditdaten behalten möchten. Sehen"Konfigurieren Sie Audit-Meldungen und einen externen Syslog-Server" für Details.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Wenn Sie planen, einen externen Syslog-Server zu konfigurieren, haben Sie die"Überlegungen zur Verwendung eines externen Syslog-Servers" und sichergestellt, dass der Server über genügend Kapazität zum Empfangen und Speichern der Protokolldateien verfügt.
- Wenn Sie einen externen Syslog-Server mit dem TLS- oder RELP/TLS-Protokoll konfigurieren möchten, verfügen Sie über die erforderlichen Server-CA- und Client-Zertifikate sowie den privaten Client-Schlüssel.

Ändern der Überwachungsmeldungsebenen

Sie können für jede der folgenden Nachrichtenkategorien im Überwachungsprotokoll eine andere Überwachungsebene festlegen:

Prüfungskategorie	Standardeinstellung	Weitere Informationen
System	Normal	"System-Audit-Meldungen"
Storage	Fehler	"Objektspeicher-Auditmeldungen"
Management	Normal	"Management-Audit-Nachricht"
Client liest	Normal	"Client liest Audit-Nachrichten"
Kunde schreibt	Normal	"Client schreibt Prüfmeldungen"
ILM	Normal	"ILM-Audit-Meldungen"

Prüfungskategorie	Standardeinstellung	Weitere Informationen
Cross-Grid-Replikation	Fehler	"CGRR: Cross-Grid-Replikationsanforderung"

Diese Standardeinstellungen gelten, wenn Sie StorageGRID ursprünglich mit Version 10.3 oder höher installiert haben. Wenn Sie ursprünglich eine frühere Version von StorageGRID verwendet haben, ist die Standardeinstellung für alle Kategorien auf „Normal“ eingestellt.

Bei Upgrades werden Konfigurationen auf Audit-Ebene nicht sofort wirksam.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**.
2. Wählen Sie für jede Kategorie von Prüfmeldungen eine Prüfebene aus der Dropdown-Liste aus:

Prüfebene	Beschreibung
Aus	Es werden keine Auditmeldungen aus dieser Kategorie protokolliert.
Fehler	Es werden nur Fehlermeldungen protokolliert – Prüfmeldungen, deren Ergebniscode nicht „erfolgreich“ (SUCS) war.
Normal	Es werden standardmäßige Transaktionsnachrichten protokolliert – die Nachrichten, die in diesen Anweisungen für die Kategorie aufgeführt sind.
Debuggen	Veraltet. Diese Ebene verhält sich genauso wie die normale Überwachungsebene.

   Zu den für eine bestimmte Ebene enthaltenen Nachrichten gehören auch diejenigen, die auf den höheren Ebenen protokolliert würden. Beispielsweise umfasst die Ebene „Normal“ alle Fehlermeldungen.

   Wenn Sie keine detaillierte Aufzeichnung der Client-Lesevorgänge für Ihre S3-Anwendungen benötigen, ändern Sie optional die Einstellung **Client Reads** in **Error**, um die Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu verringern.

3. Wählen Sie **Speichern**.

   Ein grünes Banner zeigt an, dass Ihre Konfiguration gespeichert wurde.

Definieren von HTTP-Anforderungsheadern

Sie können optional alle HTTP-Anforderungsheader definieren, die Sie in die Prüfnachrichten zum Lesen und Schreiben des Clients aufnehmen möchten. Diese Protokollheader gelten nur für S3-Anfragen.

Schritte

1. Definieren Sie im Abschnitt **Audit-Protokollheader** die HTTP-Anforderungsheader, die Sie in die Lese- und Schreib-Auditnachrichten des Clients aufnehmen möchten.

   Verwenden Sie ein Sternchen (*) als Platzhalter, um null oder mehr Zeichen abzugleichen. Verwenden Sie

die Escape-Sequenz (*), um ein wörtliches Sternchen zu finden.

2. Wählen Sie **Weitere Kopfzeile hinzufügen**, um bei Bedarf zusätzliche Kopfzeilen zu erstellen.

   Wenn in einer Anfrage HTTP-Header gefunden werden, werden diese in die Prüfnachricht unter dem Feld HTRH aufgenommen.

   > Anforderungsheader des Prüfprotokolls werden nur protokolliert, wenn die Prüfstufe für **Client-Lesevorgänge** oder **Client-Schreibvorgänge** nicht **Aus** ist.

3. Wählen Sie **Speichern**

   Ein grünes Banner zeigt an, dass Ihre Konfiguration gespeichert wurde.

Verwenden Sie einen externen Syslog-Server

Sie können optional einen externen Syslog-Server konfigurieren, um Prüfprotokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Ort außerhalb Ihres Grids zu speichern.

> Wenn Sie keinen externen Syslog-Server verwenden möchten, überspringen Sie diesen Schritt und gehen Sie zuAuswählen von Zielen für Auditinformationen .

> Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihren Anforderungen gerecht zu werden, können zusätzliche Konfigurationsoptionen angewendet werden, indem Sie `audit-destinations` Endpunkte, die sich im privaten API-Bereich des"Grid-Management-API" . Sie können die API beispielsweise verwenden, wenn Sie für unterschiedliche Knotengruppen unterschiedliche Syslog-Server verwenden möchten.

Syslog-Informationen eingeben

Greifen Sie auf den Assistenten „Externen Syslog-Server konfigurieren“ zu und geben Sie die Informationen ein, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. Wählen Sie auf der Seite „Audit- und Syslog-Server“ die Option „Externen Syslog-Server konfigurieren“ aus. Oder wählen Sie **Externen Syslog-Server bearbeiten**, wenn Sie zuvor einen externen Syslog-Server konfiguriert haben.

   Der Assistent „Externen Syslog-Server konfigurieren“ wird angezeigt.

2. Geben Sie im Schritt **Syslog-Informationen eingeben** des Assistenten im Feld **Host** einen gültigen vollqualifizierten Domänennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server ein.
3. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine Ganzzahl zwischen 1 und 65535 sein). Der Standardport ist 514.
4. Wählen Sie das Protokoll aus, das zum Senden von Audit-Informationen an den externen Syslog-Server verwendet wird.

   Die Verwendung von **TLS** oder **RELP/TLS** wird empfohlen. Sie müssen ein Serverzertifikat hochladen, um eine dieser Optionen zu verwenden. Durch die Verwendung von Zertifikaten können Sie die Verbindungen zwischen Ihrem Grid und dem externen Syslog-Server sichern. Weitere Informationen finden Sie unter "Sicherheitszertifikate verwalten" .

Alle Protokolloptionen erfordern die Unterstützung und Konfiguration des externen Syslog-Servers. Sie müssen eine Option wählen, die mit dem externen Syslog-Server kompatibel ist.

> Das Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls, um eine zuverlässige Übermittlung von Ereignismeldungen zu ermöglichen. Durch die Verwendung von RELP können Sie den Verlust von Prüfinformationen verhindern, wenn Ihr externer Syslog-Server neu gestartet werden muss.

5. Wählen Sie **Weiter**.
6. Wenn Sie **TLS** oder **RELP/TLS** ausgewählt haben, laden Sie die Server-CA-Zertifikate, das Client-Zertifikat und den privaten Client-Schlüssel hoch.
   a. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel, das/den Sie verwenden möchten.
   b. Wählen Sie das Zertifikat oder die Schlüsseldatei aus.
   c. Wählen Sie **Öffnen**, um die Datei hochzuladen.

      Neben dem Zertifikats- oder Schlüsseldateinamen wird ein grünes Häkchen angezeigt, das Sie darüber informiert, dass das Hochladen erfolgreich war.
7. Wählen Sie **Weiter**.

Syslog-Inhalte verwalten

Sie können auswählen, welche Informationen an den externen Syslog-Server gesendet werden sollen.

Schritte

1. Wählen Sie im Schritt **Syslog-Inhalt verwalten** des Assistenten alle Arten von Audit-Informationen aus, die Sie an den externen Syslog-Server senden möchten.
   - **Sende Audit-Protokolle**: Sendet StorageGRID -Ereignisse und Systemaktivitäten
   - **Sicherheitsereignisse senden**: Sendet Sicherheitsereignisse, beispielsweise wenn ein nicht autorisierter Benutzer versucht, sich anzumelden, oder wenn sich ein Benutzer als Root anmeldet
   - **Anwendungsprotokolle senden**: Sendet"Protokolldateien der StorageGRID -Software" nützlich für die Fehlerbehebung, einschließlich:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`(Nur Admin-Knoten)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - **Zugriffsprotokolle senden**: Sendet HTTP-Zugriffsprotokolle für externe Anfragen an Grid Manager, Tenant Manager, konfigurierte Load Balancer-Endpunkte und Grid-Föderationsanfragen von Remote-Systemen.
2. Wählen Sie mithilfe der Dropdown-Menüs den Schweregrad und die Einrichtung (Nachrichtentyp) für jede Kategorie von Prüfinformationen aus, die Sie senden möchten.

   Durch Festlegen von Schweregrad- und Einrichtungswerten können Sie die Protokolle auf anpassbare

Weise aggregieren, um die Analyse zu vereinfachen.

a. Wählen Sie für **Schweregrad Passthrough** oder einen Schweregradwert zwischen 0 und 7 aus.

   Wenn Sie einen Wert auswählen, wird der ausgewählte Wert auf alle Nachrichten dieses Typs angewendet. Informationen zu unterschiedlichen Schweregraden gehen verloren, wenn Sie den Schweregrad mit einem festen Wert überschreiben.

Schwere	Beschreibung
Durchreichen	Jede an das externe Syslog gesendete Nachricht muss denselben Schweregrad haben wie bei der lokalen Protokollierung auf dem Knoten: • Bei Prüfprotokollen ist der Schweregrad „Info“. • Bei Sicherheitsereignissen werden die Schweregrade von der Linux-Distribution auf den Knoten generiert. • Bei Anwendungsprotokollen variieren die Schweregrade je nach Problem zwischen „Info“ und „Hinweis“. Beispielsweise ergibt das Hinzufügen eines NTP-Servers und das Konfigurieren einer HA-Gruppe den Wert „Info“, während das absichtliche Stoppen des SSM- oder RSM-Dienstes den Wert „Notice“ ergibt. • Bei Zugriffsprotokollen ist der Schweregrad „Info“.
0	Notfall: System ist nicht nutzbar
1	Warnung: Sofortige Maßnahmen erforderlich
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber signifikanter Zustand
6	Informativ: Informationsnachrichten
7	Debug: Meldungen auf Debug-Ebene

b. Wählen Sie für **Einrichtung Passthrough** oder einen Einrichtungswert zwischen 0 und 23.

   Wenn Sie einen Wert auswählen, wird dieser auf alle Nachrichten dieses Typs angewendet. Informationen zu verschiedenen Einrichtungen gehen verloren, wenn Sie die Einrichtung mit einem festen Wert überschreiben.

Einrichtung	Beschreibung
Durchreichen	Jede an das externe Syslog gesendete Nachricht muss denselben Einrichtungswert haben wie bei der lokalen Protokollierung auf dem Knoten: • Bei Prüfprotokollen lautet die an den externen Syslog-Server gesendete Einrichtung „local7“. • Bei Sicherheitsereignissen werden die Einrichtungswerte von der Linux-Distribution auf den Knoten generiert. • Bei Anwendungsprotokollen weisen die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Einrichtungswerte auf: ◦ `bycast.log`: Benutzer oder Daemon ◦ `bycast-err.log`: Benutzer, Daemon, local3 oder local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Bei Zugriffsprotokollen lautet die an den externen Syslog-Server gesendete Einrichtung „local0“.
0	kern (Kernel-Nachrichten)
1	Benutzer (Nachrichten auf Benutzerebene)
2	mail
3	Daemon (Systemdaemons)
4	Auth (Sicherheits-/Autorisierungsnachrichten)
5	Syslog (intern von syslogd generierte Nachrichten)
6	lpr (Zeilendrucker-Subsystem)
7	Nachrichten (Netzwerk-Nachrichten-Subsystem)
8	UUCP
9	Cron (Uhr-Daemon)
10	Sicherheit (Sicherheits-/Autorisierungsnachrichten)

Einrichtung	Beschreibung
11	FTP
12	NTP
13	logaudit (Protokollprüfung)
14	logalert (Protokollalarm)
15	Uhr (Uhr-Daemon)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Wählen Sie **Weiter**.

Testnachrichten senden

Bevor Sie mit der Verwendung eines externen Syslog-Servers beginnen, sollten Sie alle Knoten in Ihrem Grid auffordern, Testnachrichten an den externen Syslog-Server zu senden. Sie sollten diese Testnachrichten verwenden, um Ihre gesamte Infrastruktur zur Protokollsammlung zu validieren, bevor Sie Daten an den externen Syslog-Server senden.

> Verwenden Sie die Konfiguration des externen Syslog-Servers erst, wenn Sie bestätigt haben, dass der externe Syslog-Server von jedem Knoten in Ihrem Grid eine Testnachricht empfangen hat und die Nachricht wie erwartet verarbeitet wurde.

Schritte

1. Wenn Sie keine Testnachrichten senden möchten, weil Sie sicher sind, dass Ihr externer Syslog-Server richtig konfiguriert ist und Prüfinformationen von allen Knoten in Ihrem Grid empfangen kann, wählen Sie **Überspringen und beenden**.

   Ein grünes Banner zeigt an, dass die Konfiguration gespeichert wurde.

2. Andernfalls wählen Sie **Testnachrichten senden** (empfohlen).

   Die Testergebnisse werden kontinuierlich auf der Seite angezeigt, bis Sie den Test beenden. Während der Test läuft, werden Ihre Prüfnachrichten weiterhin an Ihre zuvor konfigurierten Ziele gesendet.

3. Wenn Sie während der Syslog-Serverkonfiguration oder zur Laufzeit Fehler erhalten, korrigieren Sie diese und wählen Sie erneut **Testnachrichten senden**.

   Sehen"Fehlerbehebung bei einem externen Syslog-Server" um Ihnen bei der Behebung etwaiger Fehler zu helfen.

4. Warten Sie, bis ein grünes Banner angezeigt wird, das anzeigt, dass alle Knoten den Test bestanden haben.
5. Überprüfen Sie Ihren Syslog-Server, um festzustellen, ob Testnachrichten wie erwartet empfangen und verarbeitet werden.

   Wenn Sie UDP verwenden, überprüfen Sie Ihre gesamte Infrastruktur zur Protokollsammlung. Das UDP-Protokoll ermöglicht keine so strenge Fehlererkennung wie die anderen Protokolle.

6. Wählen Sie **Stoppen und beenden**.

   Sie werden zur Seite **Audit- und Syslog-Server** zurückgeleitet. Ein grünes Banner zeigt an, dass die Syslog-Serverkonfiguration gespeichert wurde.

   StorageGRID Auditinformationen werden erst an den externen Syslog-Server gesendet, wenn Sie ein Ziel auswählen, das den externen Syslog-Server enthält.

Auswählen von Zielen für Auditinformationen

Sie können angeben, wo Überwachungsprotokolle, Sicherheitsereignisprotokolle und"StorageGRID -Softwareprotokolle" gesendet werden.

StorageGRID verwendet standardmäßig lokale Knoten-Audit-Ziele und speichert die Audit-Informationen in `/var/local/log/localaudit.log` .

Bei der Verwendung `/var/local/log/localaudit.log` , die Audit-Protokolleinträge des Grid Managers und des Tenant Managers können an einen Speicherknoten gesendet werden. Welcher Knoten die aktuellsten Einträge hat, können Sie mithilfe der `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` Befehl.

Einige Ziele sind nur verfügbar, wenn Sie einen externen Syslog-Server konfiguriert haben.

Schritte

1. Wählen Sie auf der Seite „Audit- und Syslog-Server“ das Ziel für die Audit-Informationen aus.

   Nur lokale Knoten und **Externer Syslog-Server** bieten normalerweise eine bessere Leistung.

Option	Beschreibung
Nur lokale Knoten (Standard)	Prüfmeldungen, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden nicht an Admin-Knoten gesendet. Stattdessen werden sie nur auf den Knoten gespeichert, die sie generiert haben („der lokale Knoten“). Die auf jedem lokalen Knoten generierten Prüfinformationen werden gespeichert in `/var/local/log/localaudit.log` . **Hinweis**: StorageGRID entfernt regelmäßig lokale Protokolle in einer Rotation, um Speicherplatz freizugeben. Wenn die Protokolldatei für einen Knoten 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet. Die Rotationsgrenze für das Protokoll liegt bei 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Durchschnittlich werden auf jedem Knoten etwa 20 GB Protokolldaten gespeichert.
Admin-Knoten/lokale Knoten	Audit-Meldungen werden an das Audit-Protokoll auf den Admin-Knoten gesendet und Sicherheitsereignisprotokolle sowie Anwendungsprotokolle werden auf den Knoten gespeichert, die sie generiert haben. Die Auditinformationen werden in den folgenden Dateien gespeichert: • Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Die Datei ist normalerweise leer oder fehlt. Es kann sekundäre Informationen enthalten, beispielsweise eine zusätzliche Kopie einiger Nachrichten.
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf den lokalen Knoten gespeichert(`/var/local/log/localaudit.log`). Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option wird erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Knoten und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet(`/var/local/audit/export/audit.log`) auf Admin-Knoten, und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert(`/var/local/log/localaudit.log`). Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option wird erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.

2. Wählen Sie **Speichern**.

   Es wird eine Warnmeldung angezeigt.

3. Wählen Sie **OK**, um zu bestätigen, dass Sie das Ziel für Auditinformationen ändern möchten.

Ein grünes Banner zeigt an, dass die Audit-Konfiguration gespeichert wurde.

Neue Protokolle werden an die von Ihnen ausgewählten Ziele gesendet. Vorhandene Protokolle verbleiben an ihrem aktuellen Speicherort.

Verwenden Sie die SNMP-Überwachung

Verwenden Sie die SNMP-Überwachung

Wenn Sie StorageGRID mithilfe des Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den in StorageGRID enthaltenen SNMP-Agenten konfigurieren.

- "Konfigurieren des SNMP-Agenten"
- "Aktualisieren Sie den SNMP-Agenten"

Funktionen

Auf jedem StorageGRID Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Warnungen. Die MIB enthält außerdem Systembeschreibungsinformationen wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID Knoten unterstützt auch eine Teilmenge von MIB-II-Objekten.

Sehen"Zugriff auf MIB-Dateien" wenn Sie die MIB-Dateien auf Ihre Grid-Knoten herunterladen möchten.

Zunächst ist SNMP auf allen Knoten deaktiviert. Wenn Sie den SNMP-Agenten konfigurieren, erhalten alle StorageGRID Knoten dieselbe Konfiguration.

Der StorageGRID SNMP-Agent unterstützt alle drei Versionen des SNMP-Protokolls. Es bietet schreibgeschützten MIB-Zugriff für Abfragen und kann zwei Arten ereignisgesteuerter Benachrichtigungen an ein Verwaltungssystem senden:

Fallen

Traps sind vom SNMP-Agenten gesendete Benachrichtigungen, die keine Bestätigung durch das Verwaltungssystem erfordern. Traps dienen dazu, das Verwaltungssystem darüber zu informieren, dass in StorageGRID etwas passiert ist, beispielsweise dass ein Alarm ausgelöst wurde.

Traps werden in allen drei Versionen von SNMP unterstützt.

Informiert

Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Wenn der SNMP-Agent innerhalb einer bestimmten Zeitspanne keine Bestätigung erhält, sendet er die Information erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist.

Informs werden in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden in den folgenden Fällen gesendet:

- Bei jedem Schweregrad wird eine Standard- oder benutzerdefinierte Warnung ausgelöst. Um SNMP-Benachrichtigungen für einen Alarm zu unterdrücken, müssen Sie"Konfigurieren Sie eine Stille" für die Warnung. Warnmeldungen werden gesendet von"bevorzugter Absender-Admin-Knoten" .

Jeder Alarm wird basierend auf seinem Schweregrad einem von drei Trap-Typen zugeordnet: activeMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnungen, die diese Traps auslösen können, finden Sie im"Warnungsreferenz" .

SNMP-Versionsunterstützung

Die Tabelle bietet eine allgemeine Zusammenfassung der Unterstützung für jede SNMP-Version.

	SNMPv1	SNMPv2c	SNMPv3
Abfragen (GET und GETNEXT)	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen (Falle und Inform)	Nur Fallen	Fallen und Informationen	Fallen und Informationen
Benachrichtigungsauthentifizierung	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	USM-Benutzer für jedes Trap-Ziel

Einschränkungen

- StorageGRID unterstützt schreibgeschützten MIB-Zugriff. Lese-/Schreibzugriff wird nicht unterstützt.
- Alle Knoten im Grid erhalten die gleiche Konfiguration.
- SNMPv3: StorageGRID unterstützt den Transport Support Mode (TSM) nicht.
- SNMPv3: Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).
- SNMPv3: Das einzige unterstützte Datenschutzprotokoll ist AES.

Konfigurieren des SNMP-Agenten

Sie können den StorageGRID SNMP-Agenten so konfigurieren, dass er ein SNMP-Verwaltungssystem eines Drittanbieters für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwendet.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Der StorageGRID SNMP-Agent unterstützt SNMPv1, SNMPv2c und SNMPv3. Sie können den Agenten für eine oder mehrere Versionen konfigurieren. Für SNMPv3 wird nur die User Security Model (USM)-Authentifizierung unterstützt.

Alle Knoten im Grid verwenden dieselbe SNMP-Konfiguration.

Grundlegende Konfiguration festlegen

Aktivieren Sie als ersten Schritt den StorageGRID SMNP-Agenten und geben Sie grundlegende Informationen ein.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.

   Die SNMP-Agent-Seite wird angezeigt.

2. Um den SNMP-Agenten auf allen Grid-Knoten zu aktivieren, aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
3. Geben Sie im Abschnitt „Grundkonfiguration“ die folgenden Informationen ein.

Feld	Beschreibung
Systemkontakt	Optional. Der primäre Kontakt für das StorageGRID -System, der in SNMP-Nachrichten als sysContact zurückgegeben wird. Der Systemkontakt ist normalerweise eine E-Mail-Adresse. Dieser Wert gilt für alle Knoten im StorageGRID -System. **Systemkontakt** darf maximal 255 Zeichen lang sein.
Systemstandort	Optional. Der Standort des StorageGRID -Systems, der in SNMP-Nachrichten als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information sein, die zur Identifizierung des Standorts Ihres StorageGRID Systems nützlich ist. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Dieser Wert gilt für alle Knoten im StorageGRID -System. **Systemstandort** darf maximal 255 Zeichen lang sein.
Aktivieren Sie SNMP-Agent-Benachrichtigungen	• Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Trap- und Inform-Benachrichtigungen. • Wenn diese Option nicht ausgewählt ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.
Authentifizierungs-Traps aktivieren	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.

Community-Strings eingeben

Wenn Sie SNMPv1 oder SNMPv2c verwenden, füllen Sie den Abschnitt „Community-Strings“ aus.

Wenn das Verwaltungssystem die StorageGRID MIB abfragt, sendet es eine Community-Zeichenfolge. Wenn der Community-String mit einem der hier angegebenen Werte übereinstimmt, sendet der SNMP-Agent eine Antwort an das Verwaltungssystem.

Schritte

1. Geben Sie für **Nur-Lese-Community** optional eine Community-Zeichenfolge ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agentadressen zuzulassen.

   Um die Sicherheit Ihres StorageGRID -Systems zu gewährleisten, verwenden Sie nicht „public“ als Community-String. Wenn Sie dieses Feld leer lassen, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID Systems als Community-String.

   Jeder Community-String darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

2. Wählen Sie **Weitere Community-Zeichenfolge hinzufügen**, um zusätzliche Zeichenfolgen hinzuzufügen.

   Es sind bis zu fünf Zeichenfolgen zulässig.

Trap-Ziele erstellen

Verwenden Sie die Registerkarte „Trap-Ziele“ im Abschnitt „Weitere Konfigurationen“, um ein oder mehrere Ziele für StorageGRID -Trap- oder Inform-Benachrichtigungen zu definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Für die unterstützten MIB-II-Entitäten werden auch Standardbenachrichtigungen gesendet (z. B. ifDown und coldStart).

Schritte

1. Geben Sie im Feld **Standard-Trap-Community** optional die Standard-Community-Zeichenfolge ein, die Sie für SNMPv1- oder SNMPv2-Trap-Ziele verwenden möchten.

   Bei Bedarf können Sie bei der Definition eines bestimmten Trap-Ziels einen anderen („benutzerdefinierten“) Community-String angeben.

   Standard-Trap-Community darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

2. Um ein Trap-Ziel hinzuzufügen, wählen Sie **Erstellen**.
3. Wählen Sie aus, welche SNMP-Version für dieses Trap-Ziel verwendet werden soll.
4. Füllen Sie das Formular „Trap-Ziel erstellen“ für die von Ihnen ausgewählte Version aus.

SNMPv1

Wenn Sie SNMPv1 als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Muss Trap für SNMPv1 sein.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein vollqualifizierter Domänenname (FQDN) zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, sofern eine angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

SNMPv2c

Wenn Sie SNMPv2c als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Ob das Ziel für Fallen oder Informationen verwendet wird.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, sofern Sie nicht einen anderen Wert verwenden müssen.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, sofern eine angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

SNMPv3

Wenn Sie SNMPv3 als Version ausgewählt haben, füllen Sie diese Felder aus.

Feld	Beschreibung
Typ	Ob das Ziel für Fallen oder Informationen verwendet wird.
Gastgeber	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Hafen	Verwenden Sie 162, den Standardport für SNMP-Traps, sofern Sie nicht einen anderen Wert verwenden müssen.
Protokoll	Verwenden Sie UDP, das Standard-SNMP-Trap-Protokoll, es sei denn, Sie müssen TCP verwenden.
USM-Benutzer	Der USM-Benutzer, der für die Authentifizierung verwendet wird. • Wenn Sie **Trap** ausgewählt haben, werden nur USM-Benutzer ohne autoritative Engine-IDs angezeigt. • Wenn Sie **Informieren** ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt. • Wenn keine Benutzer angezeigt werden: i. Erstellen und speichern Sie das Trap-Ziel. ii. Gehe zuErstellen von USM-Benutzern und erstellen Sie den Benutzer. iii. Kehren Sie zur Registerkarte „Trap-Ziele“ zurück, wählen Sie das gespeicherte Ziel aus der Tabelle aus und wählen Sie **Bearbeiten**. iv. Wählen Sie den Benutzer aus.

5. Wählen Sie **Erstellen**.

   Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

Agentenadressen erstellen

Optional können Sie auf der Registerkarte „Agentenadressen“ im Abschnitt „Weitere Konfigurationen“ eine oder mehrere „Abhöradressen“ angeben. Dies sind die StorageGRID -Adressen, unter denen der SNMP-Agent Abfragen empfangen kann.

Wenn Sie keine Agentenadresse konfigurieren, ist die Standard-Abhöradresse der UDP-Port 161 in allen StorageGRID Netzwerken.

Schritte

1. Wählen Sie **Erstellen**.
2. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Internetprotokoll	Ob diese Adresse IPv4 oder IPv6 verwendet. Standardmäßig verwendet SNMP IPv4.
Transportprotokoll	Ob diese Adresse UDP oder TCP verwendet. Standardmäßig verwendet SNMP UDP.
StorageGRID Netzwerk	Auf welches StorageGRID -Netzwerk der Agent lauscht. • Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent überwacht alle drei Netzwerke auf Abfragen. • Netznetzwerk • Admin-Netzwerk • Kundennetzwerk **Hinweis**: Wenn Sie das Client-Netzwerk für unsichere Daten verwenden und eine Agentenadresse für das Client-Netzwerk erstellen, beachten Sie, dass auch der SNMP-Verkehr unsicher ist.
Hafen	Optional die Portnummer, auf der der SNMP-Agent lauschen soll. Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch jede beliebige nicht verwendete Portnummer eingeben. **Hinweis**: Wenn Sie den SNMP-Agenten speichern, öffnet StorageGRID automatisch die Agenten-Adressports auf der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

3. Wählen Sie **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

USM-Benutzer erstellen

Wenn Sie SNMPv3 verwenden, verwenden Sie die Registerkarte „USM-Benutzer“ im Abschnitt „Weitere Konfigurationen“, um die USM-Benutzer zu definieren, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

SNMPv3-*Inform*-Ziele müssen Benutzer mit Engine-IDs haben. Das SNMPv3-Trap-Ziel kann keine Benutzer mit Engine-IDs haben.

Diese Schritte gelten nicht, wenn Sie nur SNMPv1 oder SNMPv2c verwenden.

Schritte

1. Wählen Sie **Erstellen**.

2. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Benutzername	Ein eindeutiger Name für diesen USM-Benutzer. Benutzernamen dürfen maximal 32 Zeichen lang sein und keine Leerzeichen enthalten. Der Benutzername kann nach der Erstellung des Benutzers nicht mehr geändert werden.
Nur-Lese-MIB-Zugriff	Wenn diese Option ausgewählt ist, sollte dieser Benutzer nur Lesezugriff auf die MIB haben.
Autoritative Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, die maßgebliche Engine-ID für diesen Benutzer. Geben Sie 10 bis 64 Hex-Zeichen (5 bis 32 Bytes) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in Trap-Zielen für Informs ausgewählt werden. Dieser Wert ist für USM-Benutzer, die in Trap-Zielen für Traps ausgewählt werden, nicht zulässig. **Hinweis**: Dieses Feld wird nicht angezeigt, wenn Sie **Schreibgeschützter MIB-Zugriff** ausgewählt haben, da USM-Benutzer mit schreibgeschütztem MIB-Zugriff keine Engine-IDs haben können.
Sicherheitsstufe	Die Sicherheitsstufe für den USM-Benutzer: • **authPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Kennwort sowie ein Datenschutzprotokoll und ein Kennwort angeben. • **authNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Privatsphäre (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Kennwort angeben.
Authentifizierungsprotokoll	Immer auf SHA eingestellt, das einzige unterstützte Protokoll (HMAC-SHA-96).
Passwort	Das Kennwort, das dieser Benutzer zur Authentifizierung verwendet.
Datenschutzprotokoll	Wird nur angezeigt, wenn Sie **authPriv** ausgewählt und immer auf AES eingestellt haben, das einzige unterstützte Datenschutzprotokoll.
Passwort	Wird nur angezeigt, wenn Sie **authPriv** ausgewählt haben. Das Passwort, das dieser Benutzer aus Datenschutzgründen verwenden wird.

3. Wählen Sie **Erstellen**.

   Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

4. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, wählen Sie **Speichern**.

   Die neue SNMP-Agent-Konfiguration wird aktiv.

Aktualisieren Sie den SNMP-Agenten

Sie können SNMP-Benachrichtigungen deaktivieren, Community-Strings aktualisieren oder Agentenadressen, USM-Benutzer und Trap-Ziele hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Sehen"Konfigurieren des SNMP-Agenten" für Details zu jedem Feld auf der SNMP-Agent-Seite. Sie müssen unten auf der Seite **Speichern** auswählen, um alle auf den einzelnen Registerkarten vorgenommenen Änderungen zu übernehmen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.

   Die SNMP-Agent-Seite wird angezeigt.

2. Um den SNMP-Agenten auf allen Grid-Knoten zu deaktivieren, deaktivieren Sie das Kontrollkästchen **SNMP aktivieren** und wählen Sie **Speichern**.

   Wenn Sie den SNMP-Agenten erneut aktivieren, bleiben alle vorherigen SNMP-Konfigurationseinstellungen erhalten.

3. Aktualisieren Sie optional die Informationen im Abschnitt „Grundkonfiguration“:
   a. Aktualisieren Sie bei Bedarf den **Systemkontakt** und den **Systemstandort**.
   b. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, um zu steuern, ob der StorageGRID -SNMP-Agent Trap- und Inform-Benachrichtigungen sendet.

      Wenn dieses Kontrollkästchen deaktiviert ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.

   c. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Authentifizierungs-Traps aktivieren**, um zu steuern, ob der StorageGRID SNMP-Agent Authentifizierungs-Traps sendet, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.
4. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren oder fügen Sie optional eine **Nur-Lese-Community** im Abschnitt „Community-Strings“ hinzu.
5. Um Trap-Ziele zu aktualisieren, wählen Sie die Registerkarte Trap-Ziele im Abschnitt „Andere Konfigurationen“ aus.

   Verwenden Sie diese Registerkarte, um ein oder mehrere Ziele für StorageGRID Trap- oder Inform-Benachrichtigungen zu definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Für die unterstützten MIB-II-Entitäten werden auch Standardbenachrichtigungen gesendet (z. B. ifDown und coldStart).

Einzelheiten zu den einzugebenden Informationen finden Sie unter"Erstellen von Trap-Zielen" .

- Aktualisieren oder entfernen Sie optional die Standard-Trap-Community.

  Wenn Sie die Standard-Trap-Community entfernen, müssen Sie zunächst sicherstellen, dass alle vorhandenen Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

- Um ein Trap-Ziel hinzuzufügen, wählen Sie **Erstellen**.
- Um ein Trap-Ziel zu bearbeiten, wählen Sie das Optionsfeld und dann **Bearbeiten**.
- Um ein Trap-Ziel zu entfernen, wählen Sie das Optionsfeld und dann **Entfernen**.
- Um Ihre Änderungen zu übernehmen, wählen Sie unten auf der Seite **Speichern** aus.

6. Um Agentenadressen zu aktualisieren, wählen Sie die Registerkarte Agentenadressen im Abschnitt „Weitere Konfigurationen“ aus.

   Verwenden Sie diese Registerkarte, um eine oder mehrere „Abhöradressen“ anzugeben. Dies sind die StorageGRID -Adressen, unter denen der SNMP-Agent Abfragen empfangen kann.

   Einzelheiten zu den einzugebenden Informationen finden Sie unter"Agentenadressen erstellen" .

   - Um eine Agentenadresse hinzuzufügen, wählen Sie **Erstellen**.
   - Um eine Agentenadresse zu bearbeiten, wählen Sie das Optionsfeld und dann **Bearbeiten**.
   - Um eine Agentenadresse zu entfernen, wählen Sie das Optionsfeld und dann **Entfernen**.
   - Um Ihre Änderungen zu übernehmen, wählen Sie unten auf der Seite **Speichern** aus.

7. Um USM-Benutzer zu aktualisieren, wählen Sie im Abschnitt „Andere Konfigurationen“ die Registerkarte „USM-Benutzer“ aus.

   Verwenden Sie diese Registerkarte, um die USM-Benutzer zu definieren, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

   Einzelheiten zu den einzugebenden Informationen finden Sie unter"Erstellen von USM-Benutzern" .

   - Um einen USM-Benutzer hinzuzufügen, wählen Sie **Erstellen**.
   - Um einen USM-Benutzer zu bearbeiten, aktivieren Sie das Optionsfeld und wählen Sie **Bearbeiten**.

     Der Benutzername eines vorhandenen USM-Benutzers kann nicht geändert werden. Wenn Sie einen Benutzernamen ändern müssen, müssen Sie den Benutzer entfernen und einen neuen erstellen.

     > Wenn Sie die autoritative Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt beim Speichern der SNMP-Agent-Konfiguration ein Validierungsfehler auf.

   - Um einen USM-Benutzer zu entfernen, aktivieren Sie das Optionsfeld und wählen Sie **Entfernen**.

     > Wenn der von Ihnen entfernte Benutzer derzeit für ein Trap-Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt beim Speichern der SNMP-Agent-Konfiguration ein Validierungsfehler auf.

   - Um Ihre Änderungen zu übernehmen, wählen Sie unten auf der Seite **Speichern** aus.

8. Wenn Sie die SNMP-Agentenkonfiguration aktualisiert haben, wählen Sie **Speichern**.

Zugriff auf MIB-Dateien

MIB-Dateien enthalten Definitionen und Informationen zu den Eigenschaften verwalteter Ressourcen und Dienste für die Knoten in Ihrem Grid. Sie können auf MIB-Dateien zugreifen, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Netzes nützlich sein.

Sehen"Verwenden Sie die SNMP-Überwachung" Weitere Informationen zu SNMP- und MIB-Dateien.

Zugriff auf MIB-Dateien

Befolgen Sie diese Schritte, um auf die MIB-Dateien zuzugreifen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**.
2. Wählen Sie auf der SNMP-Agent-Seite die Datei aus, die Sie herunterladen möchten:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definiert die Warntabelle und Benachrichtigungen (Traps), auf die auf allen Admin-Knoten zugegriffen werden kann.
   - **ES-NETAPP-06-MIB.mib**: Definiert Objekte und Benachrichtigungen für Geräte auf Basis der E-Serie.
   - **MIB_1_10.zip**: Definiert Objekte und Benachrichtigungen für Appliances mit einer BMC Schnittstelle.

   Sie können auf jedem StorageGRID -Knoten auch am folgenden Speicherort auf MIB-Dateien zugreifen: `/usr/share/snmp/mibs`

3. So extrahieren Sie die StorageGRID OIDs aus der MIB-Datei:

   a. Holen Sie sich die OID des Stammverzeichnisses der StorageGRID -MIB:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Ergebnis: `.1.3.6.1.4.1.789.28669` (`28669` ist immer die OID für StorageGRID)

   a. Suchen Sie im gesamten Baum nach der StorageGRID -OID (mithilfe `paste` zum Verbinden von Zeilen):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

Der `snmptranslate` Der Befehl verfügt über viele Optionen, die zum Erkunden der MIB nützlich sind. Dieser Befehl ist auf jedem StorageGRID -Knoten verfügbar.

Inhalt der MIB-Datei

Alle Objekte befinden sich unter der StorageGRID -OID.

Objektname	Objekt-ID (OID)	Beschreibung
		Das MIB-Modul für NetApp StorageGRID Einheiten.

MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
activeAlertCount		Die Anzahl der aktiven Warnungen in der activeAlertTable.
aktiveAlarmtabelle		Eine Tabelle mit aktiven Warnungen in StorageGRID.
aktiveAlertId		Die ID der Warnung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
activeAlertName		Der Name der Warnung.
activeAlertInstance		Der Name der Entität, die die Warnung generiert hat, normalerweise der Knotenname.
activeAlertSeverity		Der Schweregrad der Warnung.
activeAlertStartTime		Datum und Uhrzeit der Auslösung des Alarms.

Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als Varbinds:

- aktiveAlertId
- activeAlertName
- activeAlertInstance
- activeAlertSeverity
- activeAlertStartTime

Benachrichtigungstyp	Objekt-ID (OID)	Beschreibung
aktiver MinorAlarm		Eine Warnung mit geringem Schweregrad
aktiver MajorAlert		Eine Warnung mit hohem Schweregrad
aktivKritischerAlarm		Eine Warnung mit kritischem Schweregrad

Sammeln Sie zusätzliche StorageGRID Daten

Verwenden Sie Diagramme und Grafiken

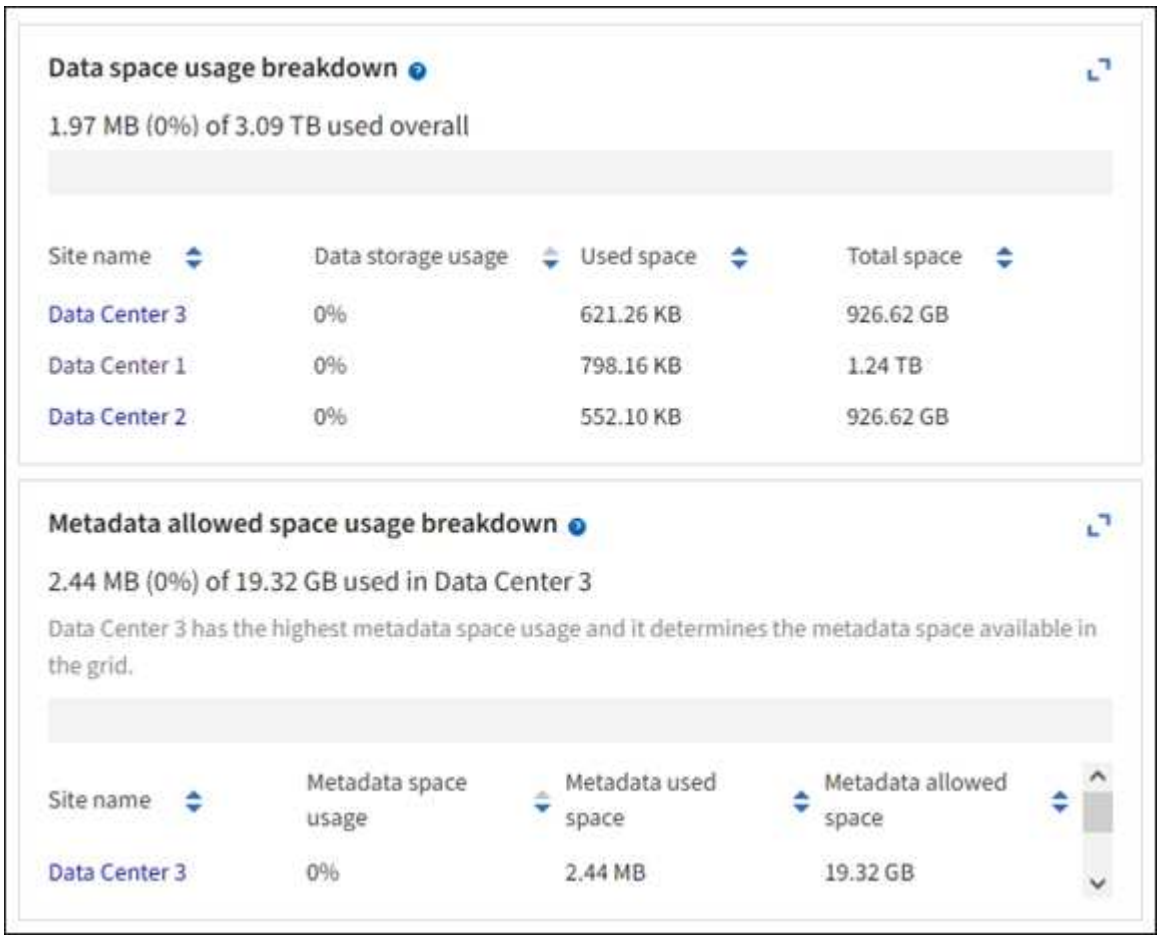
Mithilfe von Diagrammen und Berichten können Sie den Zustand des StorageGRID -Systems überwachen und Probleme beheben.

Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispiel-Screenshots auf dieser Seite überein.

Diagrammtypen

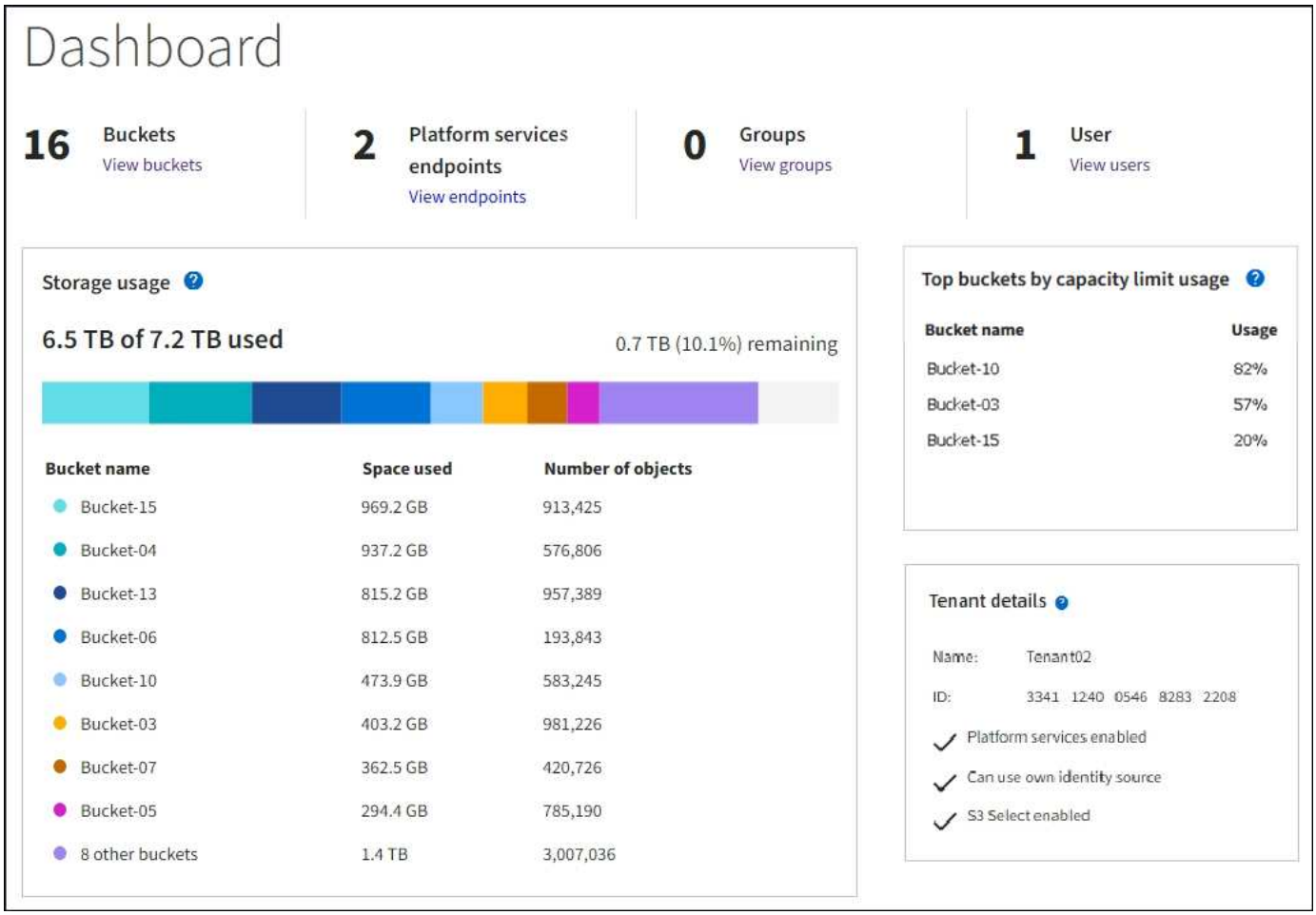
Diagramme und Grafiken fassen die Werte bestimmter StorageGRID -Metriken und -Attribute zusammen.

Das Grid Manager-Dashboard enthält Karten, die den verfügbaren Speicher für das Grid und jede Site zusammenfassen.



Das Speichernutzungsfenster im Tenant Manager-Dashboard zeigt Folgendes an:

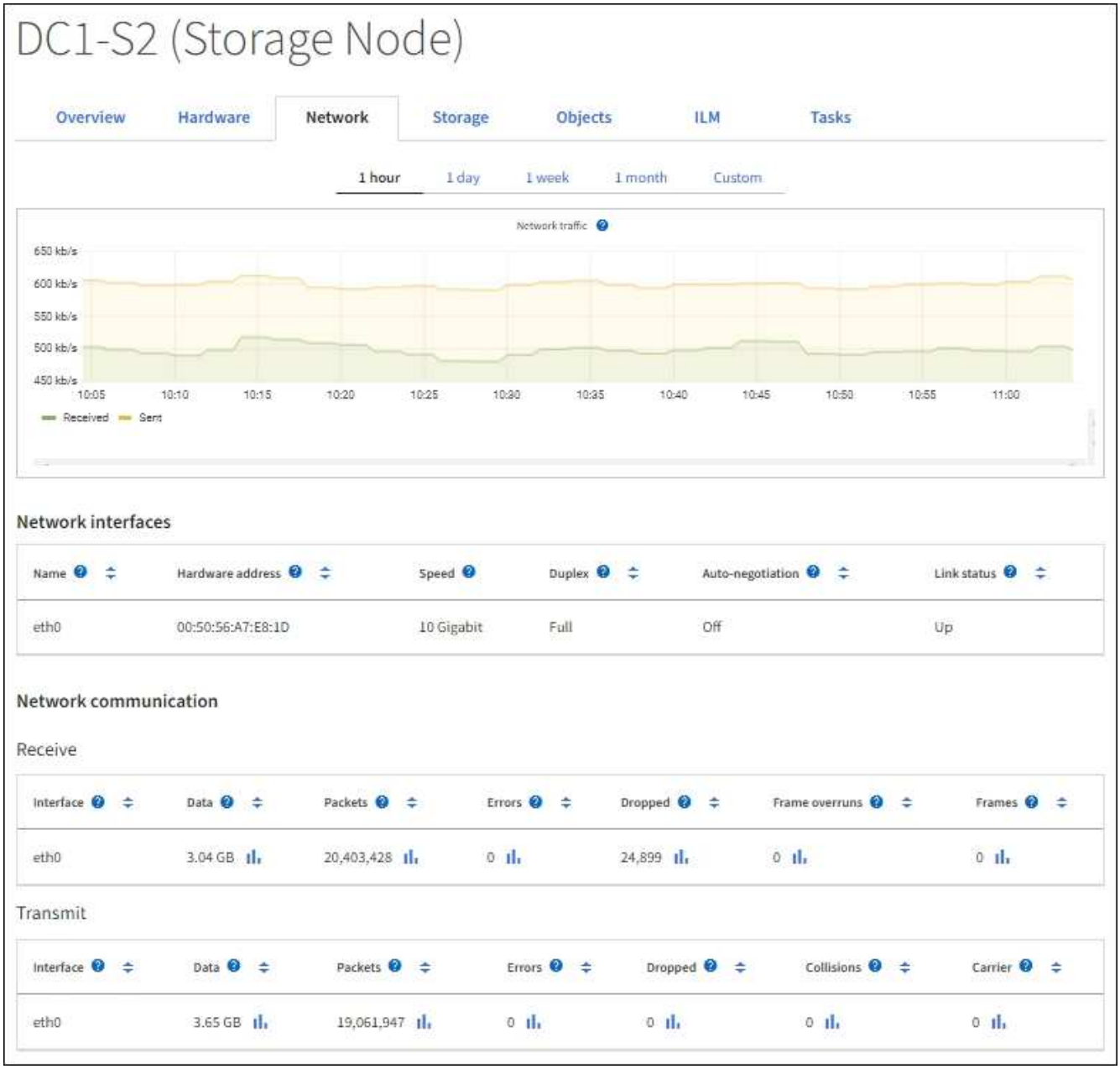
- Eine Liste der größten Buckets (S3) oder Container (Swift) für den Mandanten
- Ein Balkendiagramm, das die relativen Größen der größten Eimer oder Behälter darstellt
- Die insgesamt verwendete Speicherplatzmenge und, falls ein Kontingent festgelegt ist, die Menge und der Prozentsatz des verbleibenden Speicherplatzes



Darüber hinaus sind auf der Seite „Knoten“ und auf der Seite **SUPPORT** > **Tools** > **Grid-Topologie** Diagramme verfügbar, die zeigen, wie sich die Metriken und Attribute von StorageGRID im Laufe der Zeit ändern.

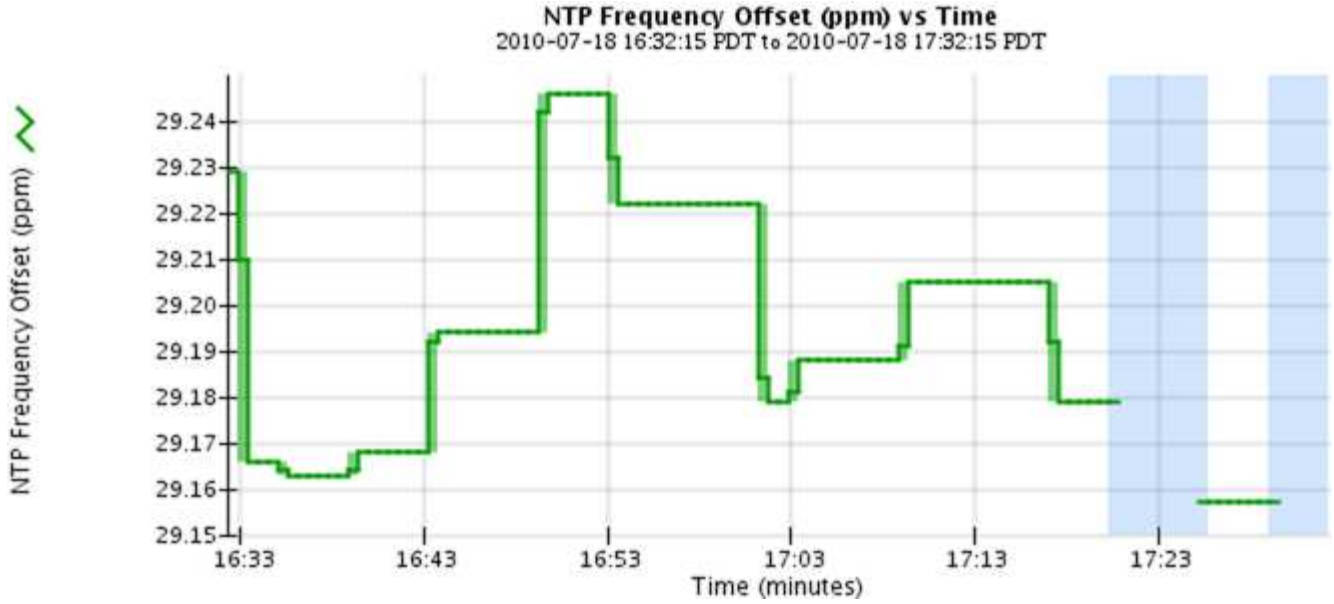
Es gibt vier Arten von Diagrammen:

- **Grafana-Diagramme**: Die auf der Knotenseite angezeigten Grafana-Diagramme werden verwendet, um die Werte der Prometheus-Metriken im Zeitverlauf darzustellen. Beispielsweise enthält die Registerkarte **NODES** > **Network** für einen Storage Node ein Grafana-Diagramm für den Netzwerkverkehr.

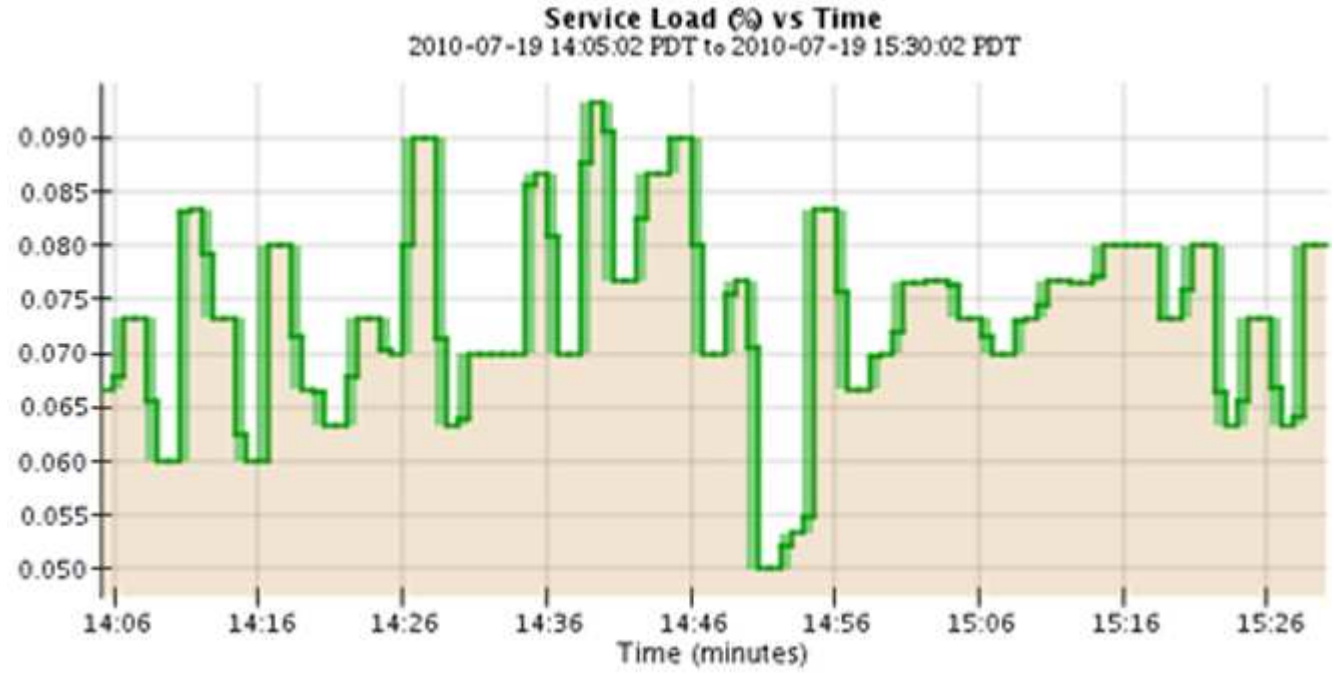


Grafana-Diagramme sind auch in den vorgefertigten Dashboards enthalten, die auf der Seite **SUPPORT** > **Tools** > **Metriken** verfügbar sind.

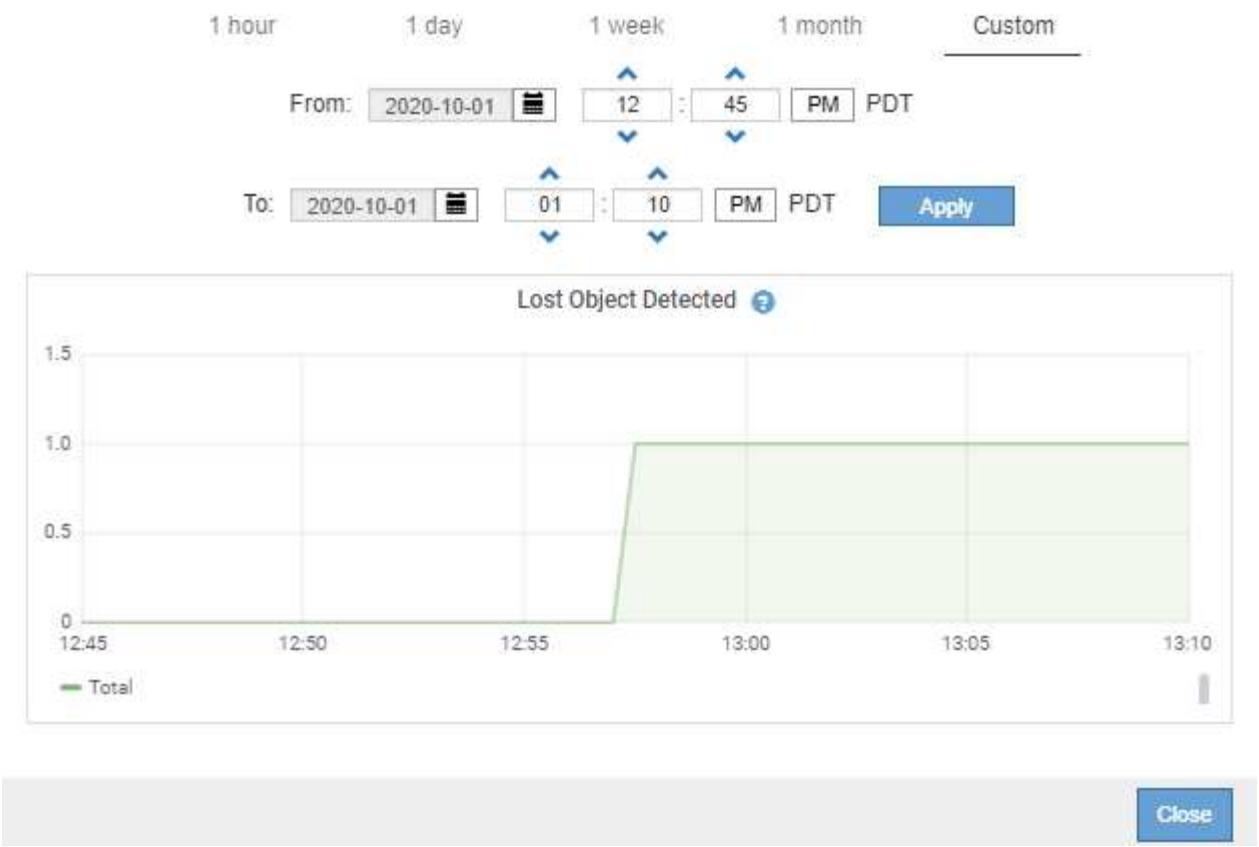
- **Liniendiagramme**: Verfügbar auf der Knotenseite und auf der Seite **SUPPORT** > **Tools** > **Gittertopologie** (wählen Sie das Diagrammsymbol nach einem Datenwert) werden Liniendiagramme verwendet, um die Werte von StorageGRID -Attributen darzustellen, die einen Einheitswert haben (z. B. NTP-Frequenzversatz in ppm). Die Wertänderungen werden in regelmäßigen Datenintervallen (Bins) über die Zeit aufgetragen.



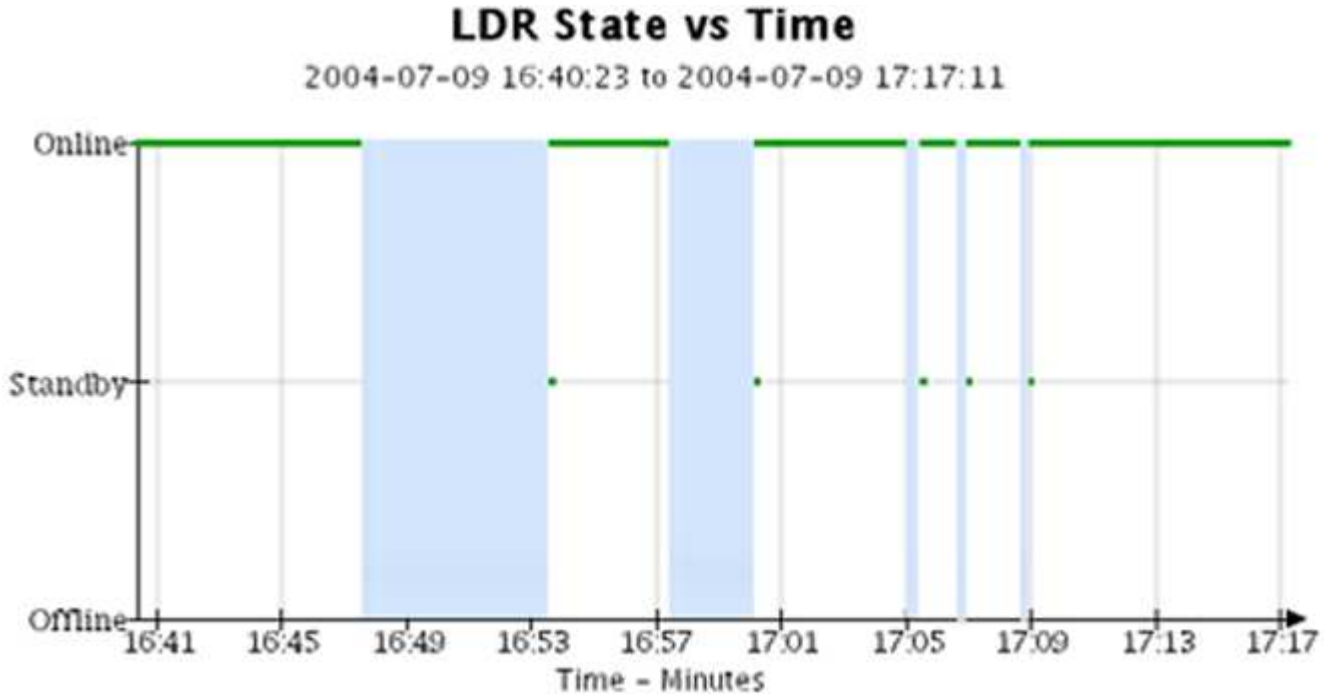
- **Flächendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **SUPPORT** > **Tools** > **Gittertopologie** (wählen Sie das Diagrammsymbol nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen wie Objektanzahlen oder Betriebslastwerte darzustellen. Flächendiagramme ähneln Liniendiagrammen, weisen jedoch unterhalb der Linie eine hellbraune Schattierung auf. Die Wertänderungen werden in regelmäßigen Datenintervallen (Bins) über die Zeit aufgetragen.



- Einige Diagramme sind mit einem anderen Diagrammsymbol gekennzeichnet und haben ein anderes Format:



- **Zustandsdiagramm**: Verfügbar auf der Seite **SUPPORT** > **Tools** > **Gittertopologie** (wählen Sie das Diagrammsymbol nach einem Datenwert) werden Zustandsdiagramme verwendet, um Attributwerte darzustellen, die unterschiedliche Zustände darstellen, wie z. B. einen Dienstzustand, der online, Standby oder offline sein kann. Zustandsgraphen ähneln Liniengraphen, der Übergang ist jedoch diskontinuierlich, d. h. der Wert springt von einem Zustandswert zum anderen.



Ähnliche Informationen

- "Anzeigen der Seite „Knoten“"
- "Den Netztopologie-Baum anzeigen"
- "Überprüfen der Supportmetriken"

Diagrammlegende

Die zum Zeichnen von Diagrammen verwendeten Linien und Farben haben eine bestimmte Bedeutung.

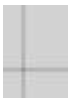
Beispiel	Bedeutung
	Die gemeldeten Attributwerte werden mithilfe dunkelgrüner Linien dargestellt.
	Eine hellgrüne Schattierung um dunkelgrüne Linien weist darauf hin, dass die tatsächlichen Werte in diesem Zeitbereich variieren und für eine schnellere Darstellung in „Binnings“ zusammengefasst wurden. Die dunkle Linie stellt den gewichteten Durchschnitt dar. Der hellgrüne Bereich gibt die Maximal- und Minimalwerte innerhalb des Behälters an. Für Flächendiagramme wird eine hellbraune Schattierung verwendet, um volumetrische Daten anzuzeigen.
	Leere Bereiche (keine dargestellten Daten) zeigen an, dass die Attributwerte nicht verfügbar waren. Der Hintergrund kann blau, grau oder eine Mischung aus Grau und Blau sein, je nach Status des Dienstes, der das Attribut meldet.
	Eine hellblaue Schattierung weist darauf hin, dass einige oder alle Attributwerte zu diesem Zeitpunkt unbestimmt waren. Das Attribut meldete keine Werte, weil sich der Dienst in einem unbekannten Zustand befand.
	Eine graue Schattierung weist darauf hin, dass einige oder alle Attributwerte zu diesem Zeitpunkt nicht bekannt waren, da der Dienst, der die Attribute meldete, administrativ nicht erreichbar war.
	Eine Mischung aus grauer und blauer Schattierung weist darauf hin, dass einige der Attributwerte zu diesem Zeitpunkt unbestimmt waren (weil sich der Dienst in einem unbekannten Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldete, administrativ nicht erreichbar war.

Diagramme und Grafiken anzeigen

Die Seite „Knoten“ enthält die Diagramme und Grafiken, auf die Sie regelmäßig zugreifen sollten, um Attribute wie Speicherkapazität und Durchsatz zu überwachen. In einigen Fällen, insbesondere bei der Zusammenarbeit mit dem technischen Support, können Sie über die Seite **SUPPORT** > **Tools** > **Grid-Topologie** auf zusätzliche Diagramme zugreifen.

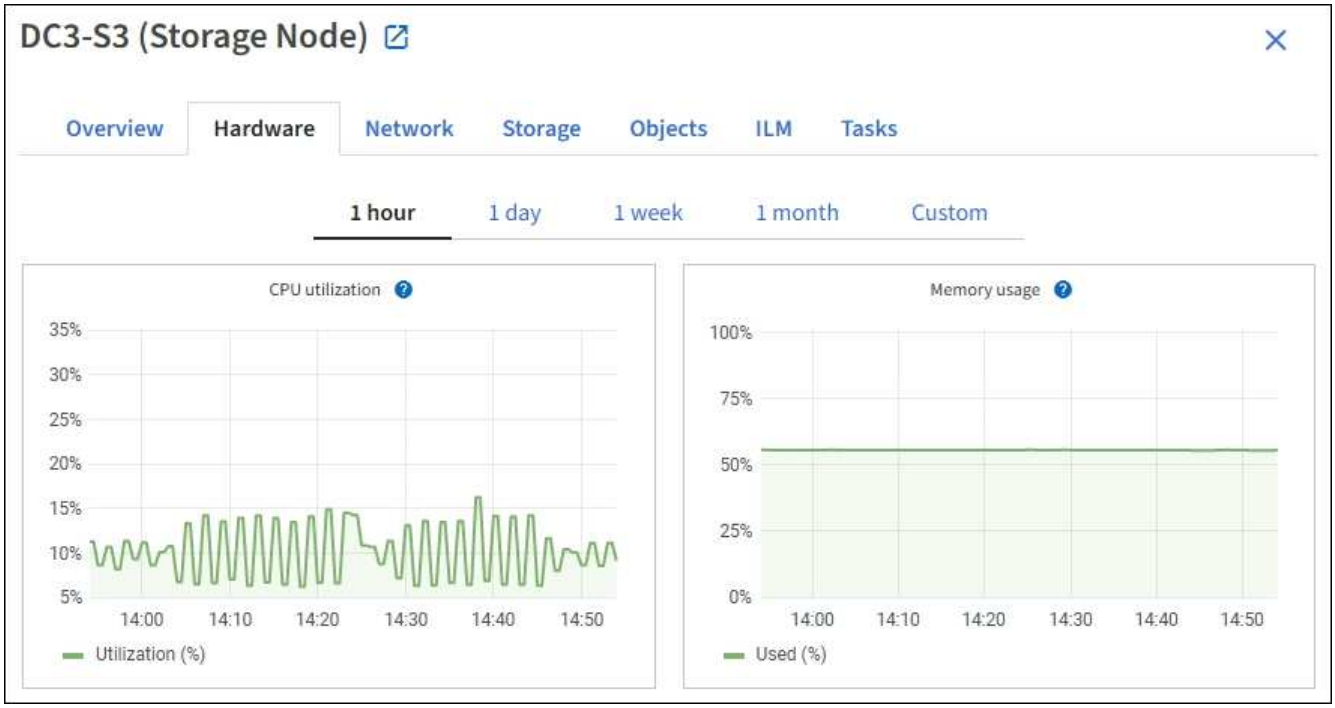
Bevor Sie beginnen

Sie müssen beim Grid Manager mit einem"unterstützter Webbrowser" .

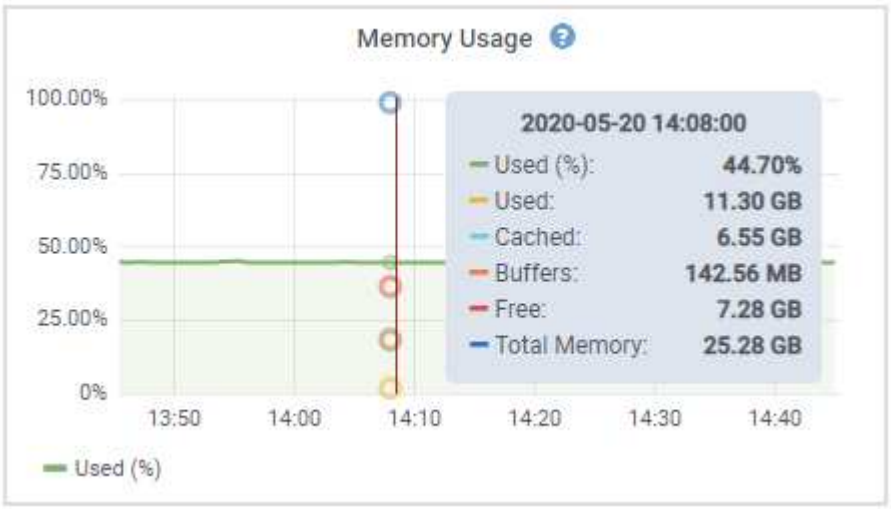
Schritte

1. Wählen Sie **NODES**. Wählen Sie dann einen Knoten, eine Site oder das gesamte Raster aus.
2. Wählen Sie die Registerkarte aus, zu der Sie Informationen anzeigen möchten.

Einige Registerkarten enthalten ein oder mehrere Grafana-Diagramme, mit denen die Werte der Prometheus-Metriken im Zeitverlauf dargestellt werden. Beispielsweise enthält die Registerkarte **KNOTEN** > **Hardware** für einen Knoten zwei Grafana-Diagramme.



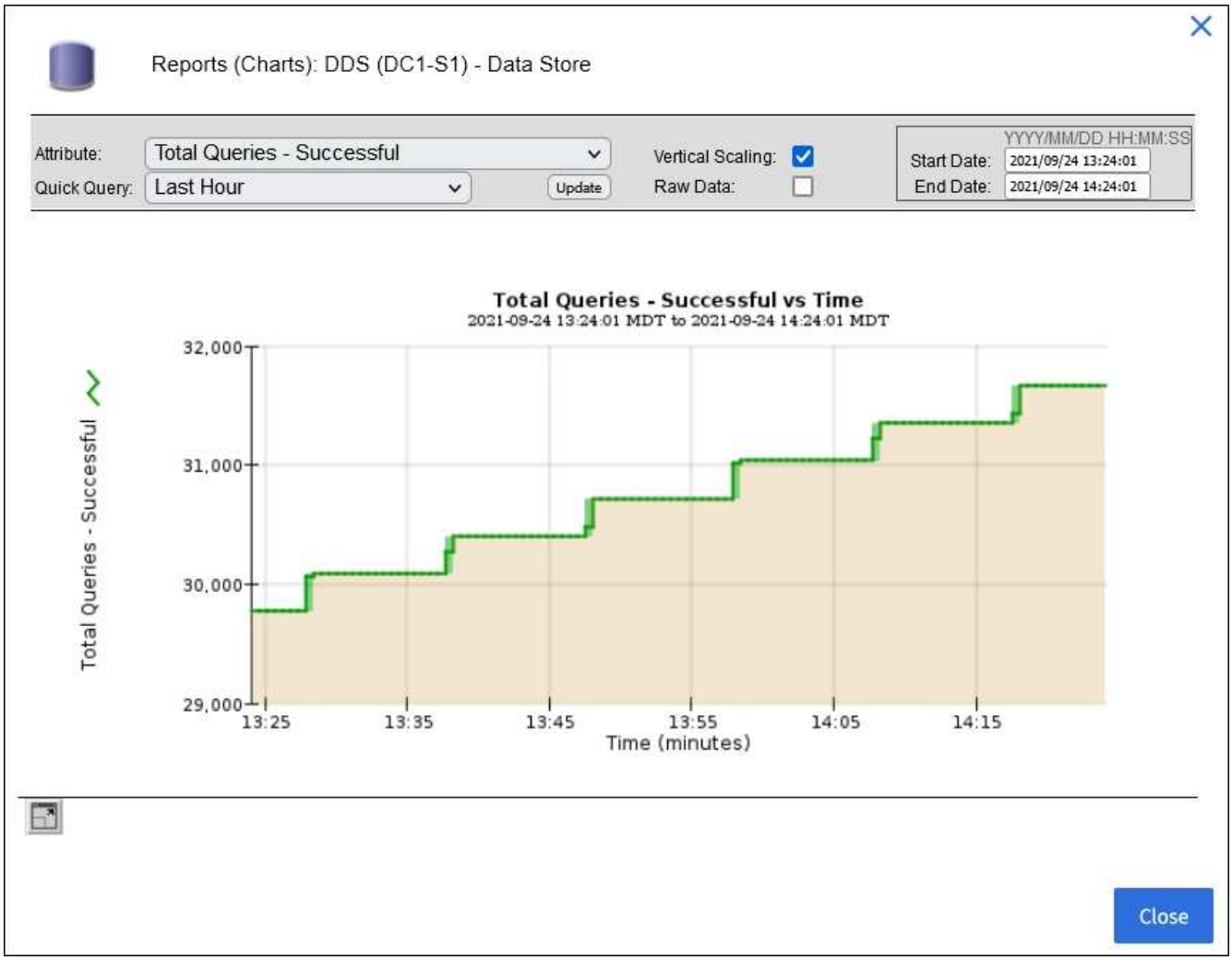
3. Optional können Sie den Cursor über dem Diagramm positionieren, um detailliertere Werte für einen bestimmten Zeitpunkt anzuzeigen.

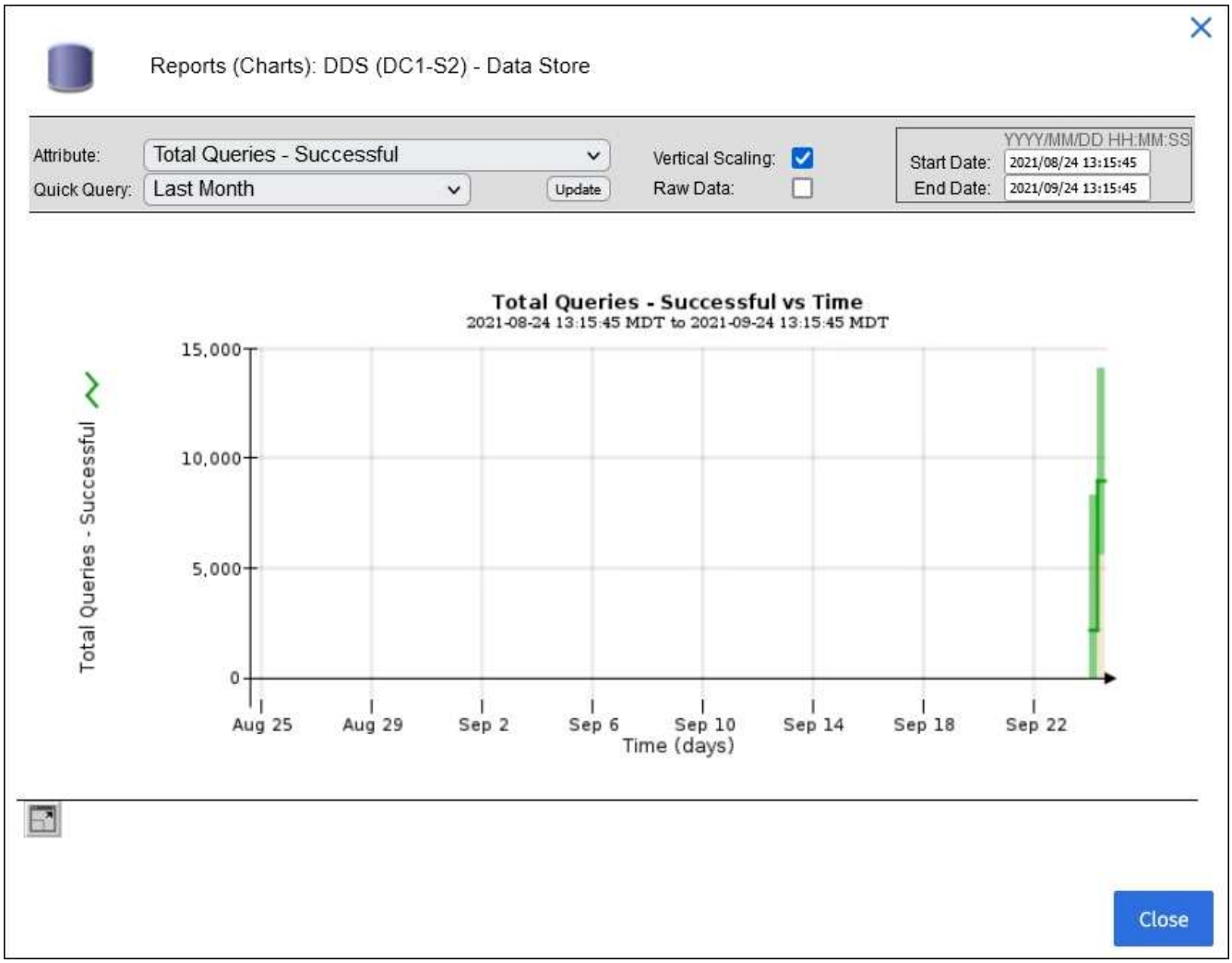


4. Bei Bedarf können Sie häufig ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Wählen Sie in der Tabelle auf der Seite „Knoten“ das Diagrammsymbol rechts neben dem Attributnamen.

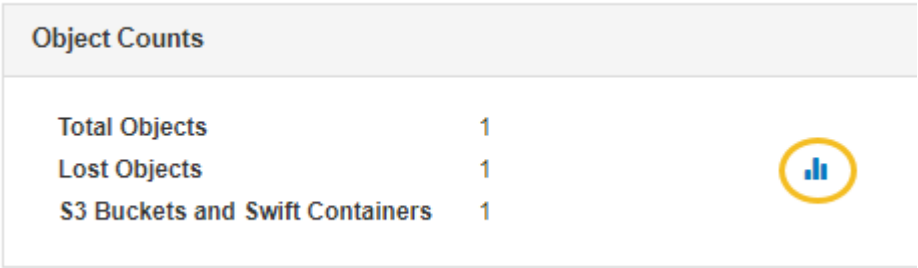
> Diagramme sind nicht für alle Metriken und Attribute verfügbar.

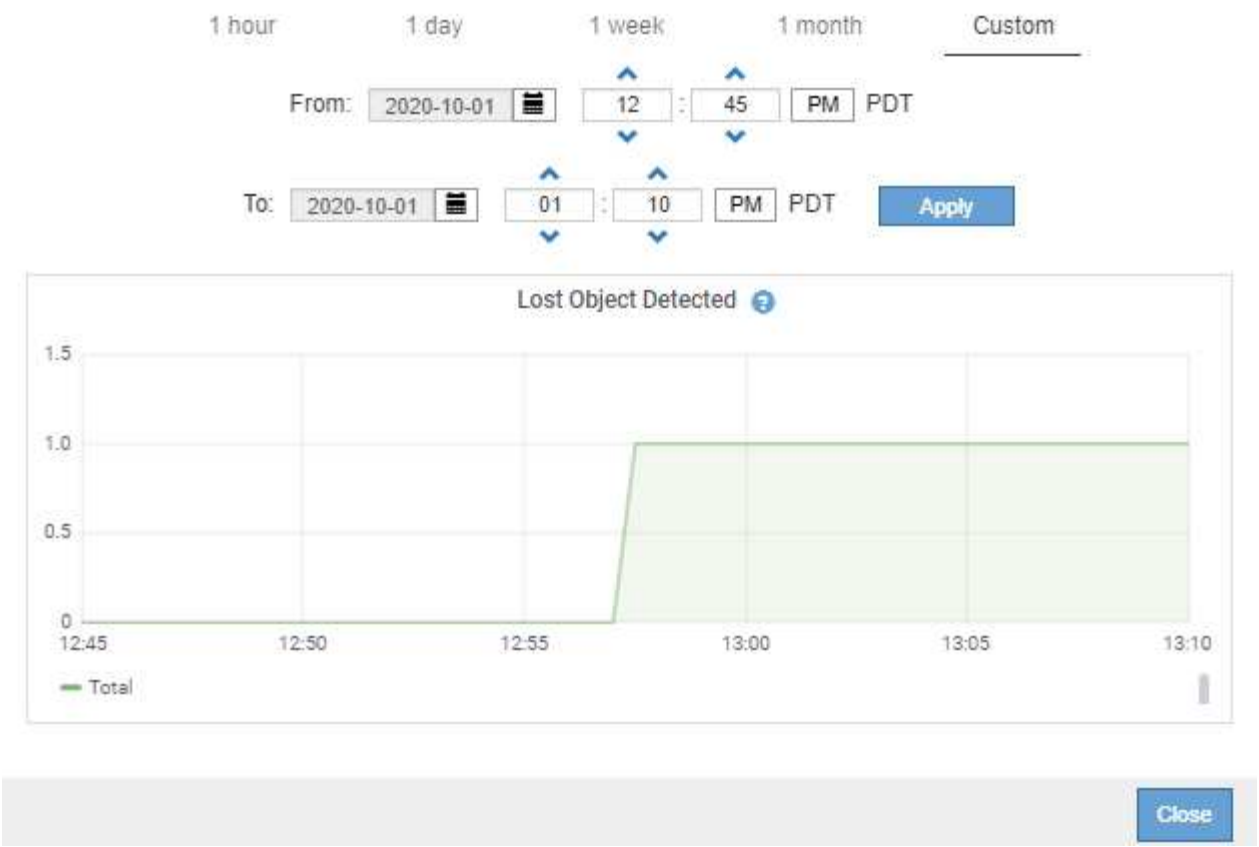
Beispiel 1: Auf der Registerkarte „Objekte“ für einen Speicherknoten können Sie das Diagrammsymbol auswählen um die Gesamtzahl der erfolgreichen Metadatenspeicherabfragen für den Speicherknoten anzuzeigen.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

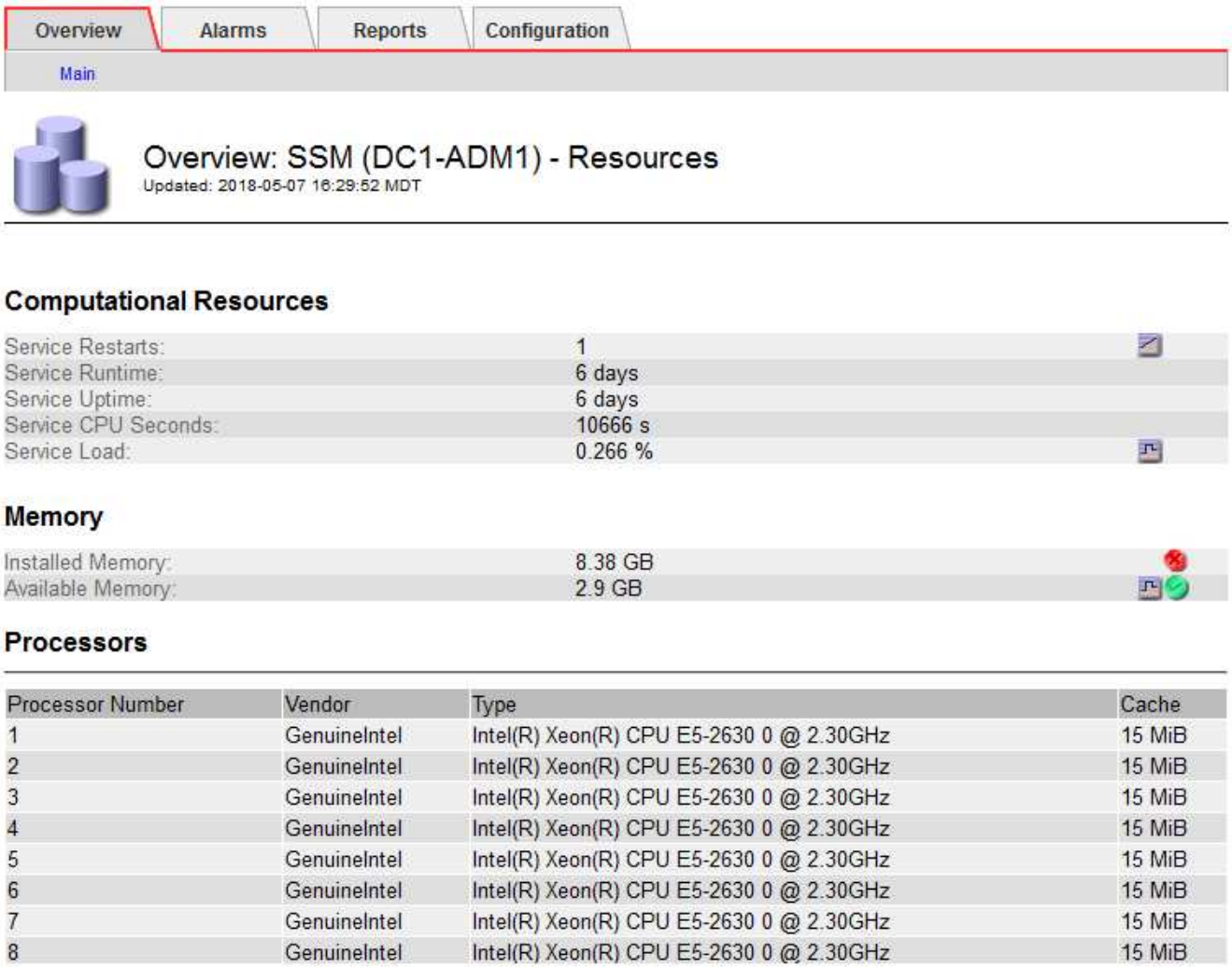


Beispiel 2: Auf der Registerkarte „Objekte“ für einen Speicherknoten können Sie das Diagrammsymbol auswählen um das Grafana-Diagramm mit der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte anzuzeigen.





5. Um Diagramme für Attribute anzuzeigen, die nicht auf der Knotenseite angezeigt werden, wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
6. Wählen Sie ***Grid-Knoten*** > ***Komponente oder Dienst*** > **Übersicht** > **Haupt**.



7. Wählen Sie das Diagrammsymbol neben dem Attribut.

   Die Anzeige wechselt automatisch zur Seite **Berichte** > **Diagramme**. Das Diagramm zeigt die Daten des Attributs für den letzten Tag.

Diagramme erstellen

Diagramme zeigen eine grafische Darstellung von Attributdatenwerten. Sie können über einen Rechenzentrumsstandort, einen Netzknoten, eine Komponente oder einen Dienst berichten.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***Rasterknoten*** > ***Komponente oder Dienst*** > **Berichte** > **Diagramme**.
3. Wählen Sie aus der Dropdown-Liste **Attribut** das Attribut aus, über das berichtet werden soll.
4. Um zu erzwingen, dass die Y-Achse bei Null beginnt, deaktivieren Sie das Kontrollkästchen **Vertikale Skalierung**.

5. Um Werte mit voller Genauigkeit anzuzeigen, aktivieren Sie das Kontrollkästchen **Rohdaten**. Um Werte auf maximal drei Dezimalstellen zu runden (z. B. für als Prozentsätze gemeldete Attribute), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie aus der Dropdown-Liste **Schnellabfrage** den Zeitraum aus, über den berichtet werden soll.

   Wählen Sie die Option „Benutzerdefinierte Abfrage“, um einen bestimmten Zeitraum auszuwählen.

   Das Diagramm wird nach einigen Augenblicken angezeigt. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein.

7. Wenn Sie „Benutzerdefinierte Abfrage“ ausgewählt haben, passen Sie den Zeitraum für das Diagramm an, indem Sie das **Startdatum** und das **Enddatum** eingeben.

   Verwenden Sie das Format *YYYY/MM/DDHH:MM:SS* in Ortszeit. Um dem Format zu entsprechen, sind führende Nullen erforderlich. Beispielsweise schlägt die Validierung bei 2017/4/6 7:30:00 fehl. Das richtige Format ist: 06.04.2017 07:30:00.

8. Wählen Sie **Aktualisieren**.

   Nach einigen Sekunden wird ein Diagramm erstellt. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein. Abhängig von der für die Abfrage eingestellten Zeitdauer wird entweder ein Rohtextbericht oder ein aggregierter Textbericht angezeigt.

Verwenden Sie Textberichte

Textberichte zeigen eine Textdarstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Abhängig vom Zeitraum, über den Sie berichten, werden zwei Arten von Berichten generiert: Rohtextberichte für Zeiträume unter einer Woche und aggregierte Textberichte für Zeiträume über einer Woche.

Rohtextberichte

Ein Rohtextbericht zeigt Details zum ausgewählten Attribut an:

- Empfangszeit: Lokales Datum und Uhrzeit, zu der ein Beispielwert der Daten eines Attributs vom NMS-Dienst verarbeitet wurde.
- Abtastzeit: Lokales Datum und Uhrzeit, zu der ein Attributwert abgetastet oder an der Quelle geändert wurde.
- Wert: Attributwert zum Zeitpunkt der Abtastung.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Aggregierte Textberichte

Ein aggregierter Textbericht zeigt Daten über einen längeren Zeitraum (normalerweise eine Woche) an als ein Rohtextbericht. Jeder Eintrag ist das Ergebnis der Zusammenfassung mehrerer Attributwerte (eine Ansammlung von Attributwerten) durch den NMS-Dienst im Laufe der Zeit in einen einzigen Eintrag mit Durchschnitts-, Maximal- und Minimalwerten, die aus der Ansammlung abgeleitet werden.

Jeder Eintrag zeigt die folgenden Informationen an:

- Aggregierte Zeit: Letztes lokales Datum und Uhrzeit, zu der der NMS-Dienst eine Reihe geänderter Attributwerte aggregiert (gesammelt) hat.
- Durchschnittswert: Der Durchschnitt des Attributwerts über den aggregierten Zeitraum.
- Mindestwert: Der Mindestwert über den aggregierten Zeitraum.
- Maximalwert: Der Maximalwert über den aggregierten Zeitraum.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Textberichte erstellen

Textberichte zeigen eine Textdarstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Sie können über einen Rechenzentrumsstandort, einen Netzknoten, eine Komponente oder einen Dienst berichten.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Bei Attributdaten, bei denen davon auszugehen ist, dass sie sich ständig ändern, werden diese Attributdaten vom NMS-Dienst (an der Quelle) in regelmäßigen Abständen abgetastet. Bei Attributdaten, die sich selten ändern (z. B. Daten, die auf Ereignissen wie Zustands- oder Statusänderungen basieren), wird bei einer Wertänderung ein Attributwert an den NMS-Dienst gesendet.

Die Art des angezeigten Berichts hängt vom konfigurierten Zeitraum ab. Standardmäßig werden aggregierte Textberichte für Zeiträume von mehr als einer Woche erstellt.

Grauer Text zeigt an, dass der Dienst während der Stichprobenentnahme administrativ nicht erreichbar war. Blauer Text zeigt an, dass sich der Dienst in einem unbekannten Zustand befand.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***Grid-Knoten*** > ***Komponente oder Dienst*** > **Berichte** > **Text**.
3. Wählen Sie aus der Dropdown-Liste **Attribut** das Attribut aus, über das berichtet werden soll.
4. Wählen Sie die Anzahl der Ergebnisse pro Seite aus der Dropdown-Liste **Ergebnisse pro Seite** aus.
5. Um Werte auf maximal drei Dezimalstellen zu runden (beispielsweise bei Attributen, die als Prozentsätze angegeben werden), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie aus der Dropdown-Liste **Schnellabfrage** den Zeitraum aus, über den berichtet werden soll.

   Wählen Sie die Option „Benutzerdefinierte Abfrage“, um einen bestimmten Zeitraum auszuwählen.

Der Bericht erscheint nach wenigen Augenblicken. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein.

7. Wenn Sie „Benutzerdefinierte Abfrage“ ausgewählt haben, müssen Sie den Berichtszeitraum anpassen, indem Sie das **Startdatum** und das **Enddatum** eingeben.

   Verwenden Sie das Format `YYYY/MM/DDHH:MM:SS` in Ortszeit. Um dem Format zu entsprechen, sind führende Nullen erforderlich. Beispielsweise schlägt die Validierung bei 2017/4/6 7:30:00 fehl. Das richtige Format ist: 06.04.2017 07:30:00.

8. Klicken Sie auf **Aktualisieren**.

   Nach wenigen Augenblicken wird ein Textbericht erstellt. Planen Sie für die tabellarische Darstellung großer Zeiträume mehrere Minuten ein. Abhängig von der für die Abfrage eingestellten Zeitdauer wird entweder ein Rohtextbericht oder ein aggregierter Textbericht angezeigt.

Textberichte exportieren

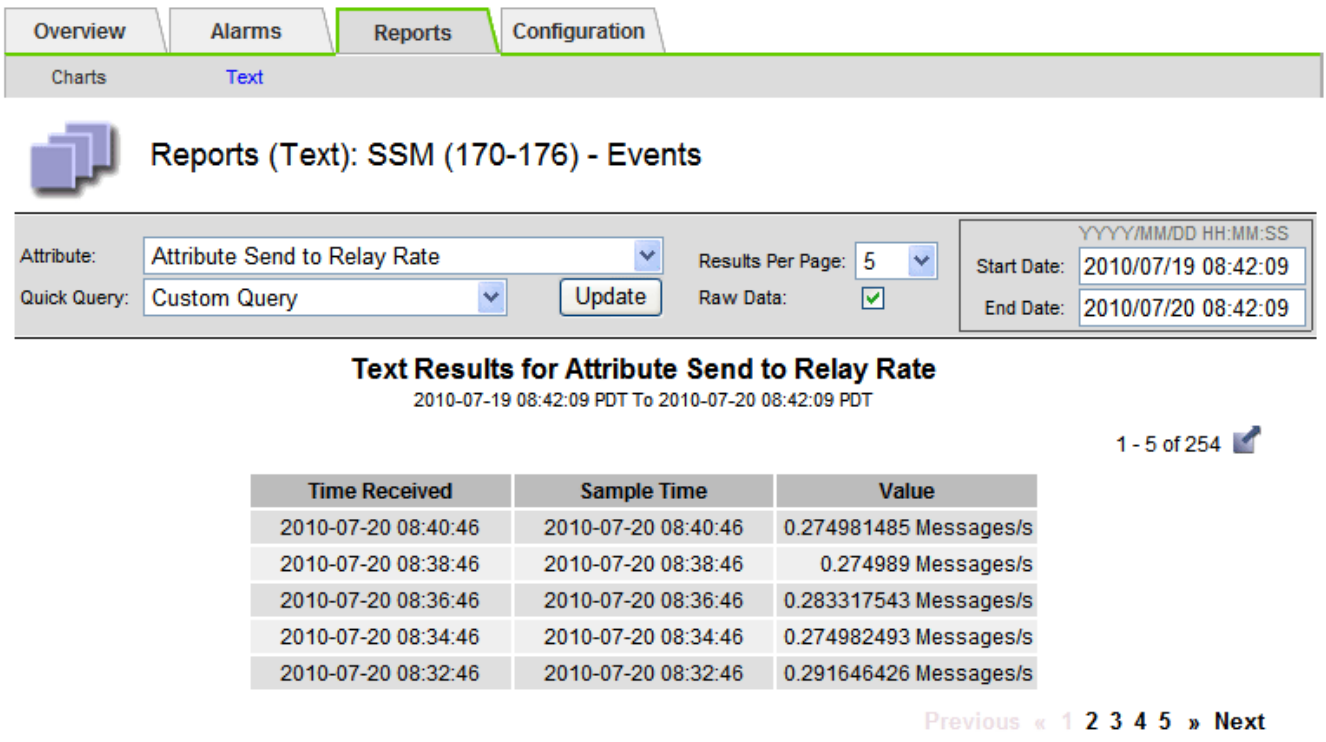
Exportierte Textberichte öffnen eine neue Browser-Registerkarte, in der Sie die Daten auswählen und kopieren können.

Informationen zu diesem Vorgang

Die kopierten Daten können dann in einem neuen Dokument (z. B. einer Tabelle) gespeichert und zur Analyse der Leistung des StorageGRID Systems verwendet werden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Erstellen Sie einen Textbericht.
3. Klicken Sie auf *Exportieren* .



Das Fenster „Textbericht exportieren“ wird geöffnet und zeigt den Bericht an.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Wählen Sie den Inhalt des Fensters „Textbericht exportieren“ aus und kopieren Sie ihn.

   Diese Daten können nun in ein Drittdokument, beispielsweise eine Tabellenkalkulation, eingefügt werden.

Überwachen Sie die PUT- und GET-Leistung

Sie können die Leistung bestimmter Vorgänge überwachen, beispielsweise das Speichern und Abrufen von Objekten, um Änderungen zu erkennen, die möglicherweise einer weiteren Untersuchung bedürfen.

Informationen zu diesem Vorgang

Um die PUT- und GET-Leistung zu überwachen, können Sie S3-Befehle direkt von einer Workstation aus ausführen oder die Open-Source-Anwendung S3tester verwenden. Mithilfe dieser Methoden können Sie die Leistung unabhängig von externen Faktoren von StorageGRID beurteilen, beispielsweise Problemen mit einer Clientanwendung oder Problemen mit einem externen Netzwerk.

Beachten Sie beim Testen von PUT- und GET-Vorgängen die folgenden Richtlinien:

- Verwenden Sie Objektgrößen, die mit den Objekten vergleichbar sind, die Sie normalerweise in Ihr Raster aufnehmen.
- Führen Sie Vorgänge sowohl für lokale als auch für Remote-Sites durch.

Nachrichten in der"Überwachungsprotokoll" geben die Gesamtzeit an, die zum Ausführen bestimmter Vorgänge erforderlich ist. Um beispielsweise die Gesamtverarbeitungszeit für eine S3-GET-Anforderung zu ermitteln, können Sie den Wert des TIME-Attributs in der SGET-Auditnachricht überprüfen. Sie finden das TIME-Attribut auch in den Audit-Nachrichten für die folgenden S3-Operationen: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Achten Sie bei der Analyse der Ergebnisse auf die durchschnittliche Zeit, die zur Erfüllung einer Anfrage benötigt wird, sowie auf den Gesamtdurchsatz, den Sie erreichen können. Wiederholen Sie dieselben Tests regelmäßig und zeichnen Sie die Ergebnisse auf, damit Sie Trends erkennen können, die möglicherweise

einer Untersuchung bedürfen.

- Du kannst "Laden Sie S3tester von GitHub herunter" .

Überwachen von Objektüberprüfungsvorgängen

Das StorageGRID -System kann die Integrität von Objektdaten auf Speicherknoten überprüfen und sowohl auf beschädigte als auch auf fehlende Objekte prüfen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Zwei"Verifizierungsprozesse" Arbeiten Sie zusammen, um die Datenintegrität sicherzustellen:

- Die **Hintergrundprüfung** läuft automatisch und überprüft kontinuierlich die Richtigkeit der Objektdaten.

  Bei der Hintergrundüberprüfung werden alle Speicherknoten automatisch und kontinuierlich überprüft, um festzustellen, ob beschädigte Kopien replizierter und löschcodierter Objektdaten vorhanden sind. Wenn Probleme gefunden werden, versucht das StorageGRID -System automatisch, die beschädigten Objektdaten durch Kopien zu ersetzen, die an anderer Stelle im System gespeichert sind. Für Objekte in einem Cloud-Speicherpool wird keine Hintergrundüberprüfung ausgeführt.

  > ⓘ Die Warnung **Unbekanntes beschädigtes Objekt erkannt** wird ausgelöst, wenn das System ein beschädigtes Objekt erkennt, das nicht automatisch korrigiert werden kann.

- Die **Objektexistenzprüfung** kann von einem Benutzer ausgelöst werden, um die Existenz (jedoch nicht die Richtigkeit) von Objektdaten schneller zu überprüfen.

  Die Objektexistenzprüfung überprüft, ob alle erwarteten replizierten Kopien von Objekten und Erasure-Coded-Fragmenten auf einem Speicherknoten vorhanden sind. Die Objektexistenzprüfung bietet eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich aufgetretenes Hardwareproblem die Datenintegrität beeinträchtigt haben könnte.

Sie sollten die Ergebnisse der Hintergrundüberprüfungen und Objektexistenzprüfungen regelmäßig überprüfen. Untersuchen Sie alle Fälle beschädigter oder fehlender Objektdaten sofort, um die Grundursache zu ermitteln.

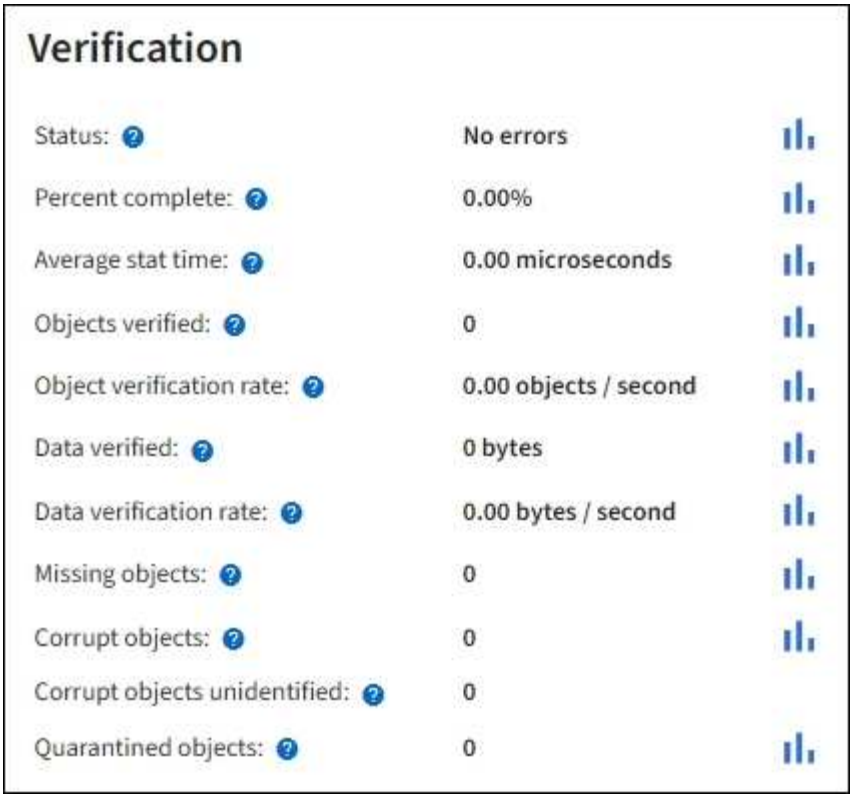
Schritte

1. Überprüfen Sie die Ergebnisse der Hintergrundüberprüfungen:

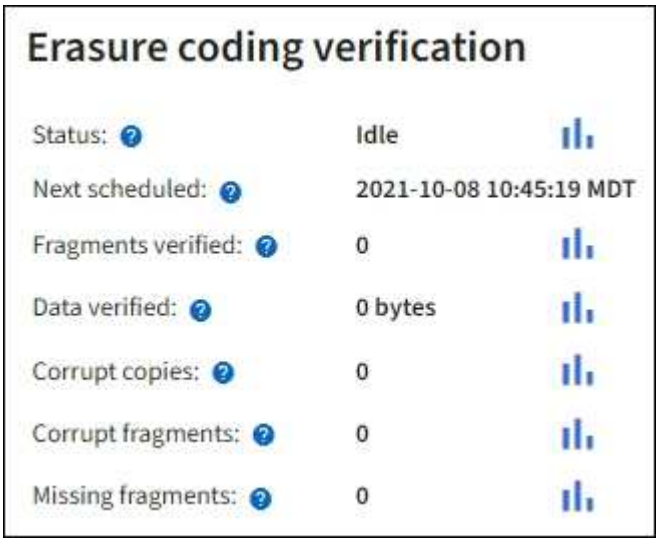
   a. Wählen Sie **NODES** > ***Storage Node*** > **Objects**.

   b. Überprüfen Sie die Überprüfungsergebnisse:

      - Um die Verifizierung der replizierten Objektdaten zu überprüfen, sehen Sie sich die Attribute im Abschnitt „Verifizierung“ an.

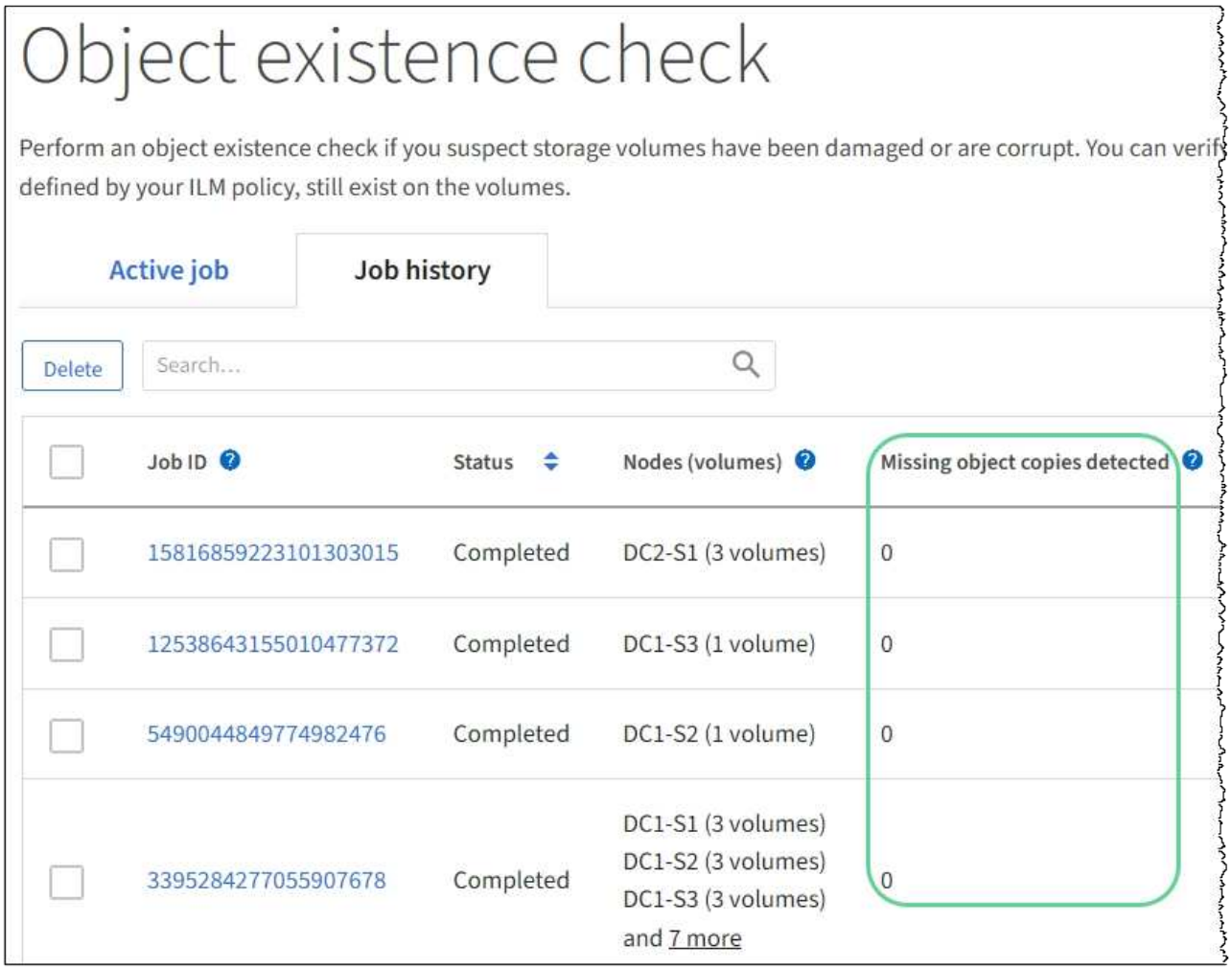


- Um die Erasure-Coding-Fragmentverifizierung zu überprüfen, wählen Sie ***Storage Node*** > **ILM** und sehen Sie sich die Attribute im Abschnitt „Erasure-Coding-Verifizierung“ an.



Wählen Sie das Fragezeichen neben dem Namen eines Attributs, um Hilfetext anzuzeigen.

2. Überprüfen Sie die Ergebnisse der Jobs zur Objektexistenzprüfung:
   a. Wählen Sie **WARTUNG** > **Objektexistenzprüfung** > **Auftragsverlauf**.
   b. Scannen Sie die Spalte „Fehlende Objektkopien erkannt“. Wenn bei einem Auftrag 100 oder mehr Objektkopien fehlen und die Warnung „Objekte verloren“ ausgelöst wurde, wenden Sie sich an den technischen Support.



Überwachen von Ereignissen

Sie können Ereignisse überwachen, die von einem Grid-Knoten erkannt werden, einschließlich benutzerdefinierter Ereignisse, die Sie erstellt haben, um Ereignisse zu verfolgen, die auf dem Syslog-Server protokolliert werden. Die im Grid Manager angezeigte Meldung „Letztes Ereignis“ bietet weitere Informationen zum aktuellsten Ereignis.

Ereignismeldungen werden auch aufgelistet in der `/var/local/log/bycast-err.log` Protokolldatei. Siehe die"Referenz zu Protokolldateien" .

Der SMTT-Alarm (Gesamtereignisse) kann wiederholt durch Probleme wie Netzwerkprobleme, Stromausfälle oder Upgrades ausgelöst werden. Dieser Abschnitt enthält Informationen zur Untersuchung von Ereignissen, damit Sie besser verstehen, warum diese Alarme aufgetreten sind. Wenn ein Ereignis aufgrund eines bekannten Problems aufgetreten ist, können die Ereigniszähler bedenkenlos zurückgesetzt werden.

Schritte

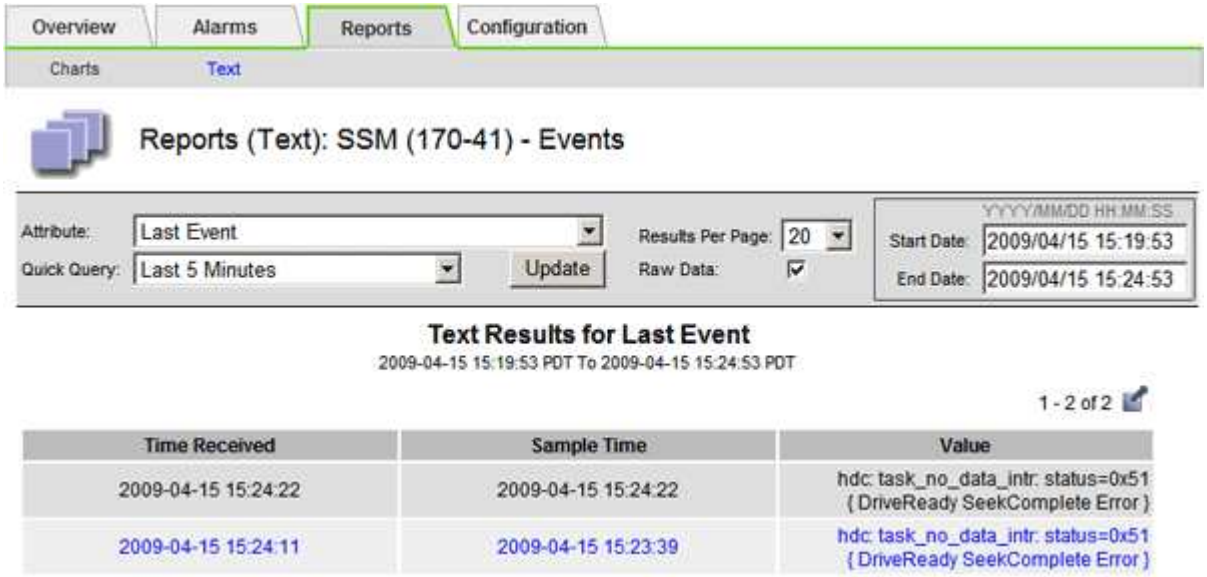
1. Überprüfen Sie die Systemereignisse für jeden Grid-Knoten:
   a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
   b. Wählen Sie ***site*** > ***grid node*** > **SSM** > **Events** > **Overview** > **Main**.
2. Erstellen Sie eine Liste früherer Ereignismeldungen, um in der Vergangenheit aufgetretene Probleme

einzugrenzen:

a. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
b. Wählen Sie ***site*** > ***grid node*** > **SSM** > **Events** > **Reports**.
c. Wählen Sie **Text** aus.

   Das Attribut **Letztes Ereignis** wird nicht angezeigt in der"Diagrammansicht" . So zeigen Sie es an:

d. Ändern Sie **Attribut** in **Letztes Ereignis**.
e. Wählen Sie optional einen Zeitraum für die **Schnellabfrage** aus.
f. Wählen Sie **Aktualisieren**.



Erstellen Sie benutzerdefinierte Syslog-Ereignisse

Mit benutzerdefinierten Ereignissen können Sie alle Kernel-, Daemon-, Fehler- und Benutzerereignisse auf kritischer Ebene verfolgen, die auf dem Syslog-Server protokolliert werden. Ein benutzerdefiniertes Ereignis kann nützlich sein, um das Auftreten von Systemprotokollmeldungen (und somit Netzwerksicherheitsereignissen und Hardwarefehlern) zu überwachen.

Informationen zu diesem Vorgang

Erwägen Sie die Erstellung benutzerdefinierter Ereignisse, um wiederkehrende Probleme zu überwachen. Die folgenden Überlegungen gelten für benutzerdefinierte Ereignisse.

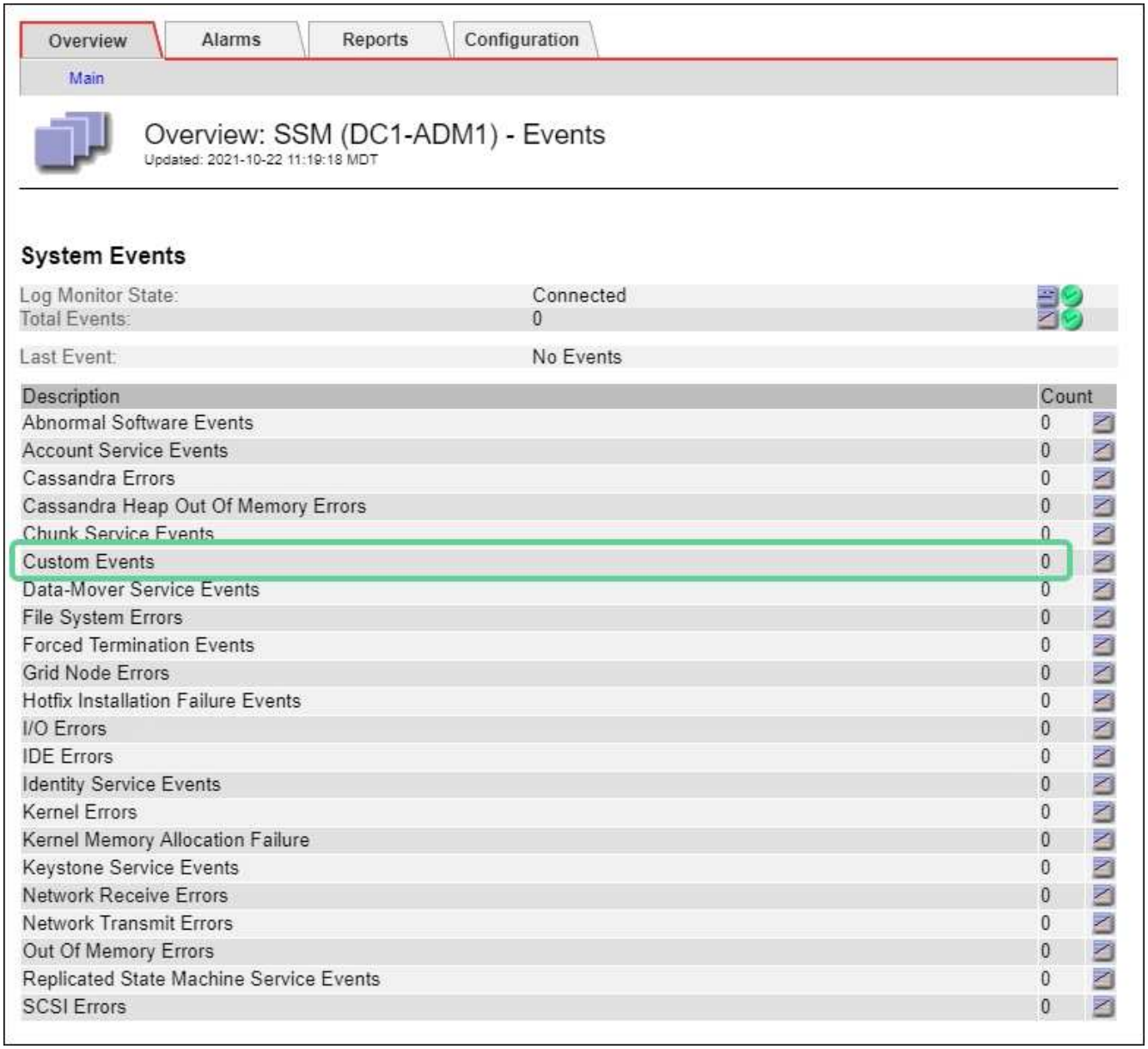
- Nachdem ein benutzerdefiniertes Ereignis erstellt wurde, wird jedes Vorkommen davon überwacht.
- Um ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern in der `/var/local/log/messages` Dateien müssen die Protokolle in diesen Dateien sein:
  - Vom Kernel generiert
  - Von Daemon oder Benutzerprogramm auf Fehler- oder kritischer Ebene generiert

Hinweis: Nicht alle Einträge in der `/var/local/log/messages` Dateien werden abgeglichen, sofern sie nicht die oben genannten Anforderungen erfüllen.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (Legacy)** > **Benutzerdefinierte Ereignisse**.
2. Klicken Sie auf *Bearbeiten* (oder *Einfügen* wenn dies nicht das erste Ereignis ist).
3. Geben Sie eine benutzerdefinierte Ereigniszeichenfolge ein, beispielsweise „Herunterfahren“
4. Wählen Sie **Änderungen übernehmen**.
5. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
6. Wählen Sie ***grid node*** > **SSM** > **Events**.
7. Suchen Sie den Eintrag für benutzerdefinierte Ereignisse in der Ereignistabelle und überwachen Sie den Wert für **Anzahl**.

   Wenn die Anzahl steigt, wird auf diesem Grid-Knoten ein von Ihnen überwachtes benutzerdefiniertes Ereignis ausgelöst.



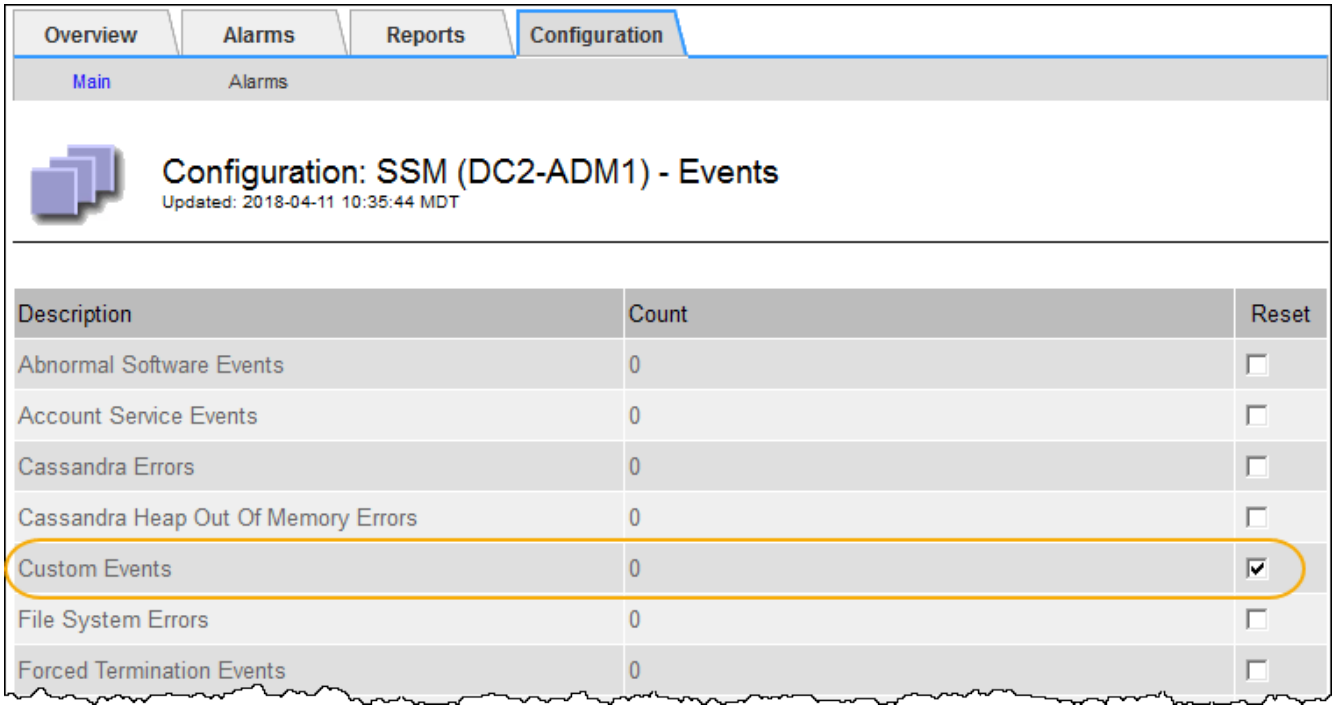
Setzt die Anzahl der benutzerdefinierten Ereignisse auf Null zurück

Wenn Sie den Zähler nur für benutzerdefinierte Ereignisse zurücksetzen möchten, müssen Sie die Seite „Grid-Topologie“ im Support-Menü verwenden.

Das Zurücksetzen eines Zählers führt dazu, dass der Alarm beim nächsten Ereignis ausgelöst wird. Wenn Sie dagegen einen Alarm bestätigen, wird dieser Alarm nur dann erneut ausgelöst, wenn der nächste Schwellenwert erreicht wird.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***grid node*** > **SSM** > **Events** > **Configuration** > **Main**.
3. Aktivieren Sie das Kontrollkästchen **Zurücksetzen** für benutzerdefinierte Ereignisse.



4. Wählen Sie **Änderungen übernehmen**.

Überprüfen von Auditmeldungen

Mithilfe von Audit-Meldungen können Sie die detaillierten Vorgänge Ihres StorageGRID Systems besser verstehen. Sie können Überwachungsprotokolle verwenden, um Probleme zu beheben und die Leistung zu bewerten.

Während des normalen Systembetriebs generieren alle StorageGRID -Dienste folgende Prüfmeldungen:

- Systemprüfungsmeldungen beziehen sich auf das Prüfsystem selbst, den Zustand der Grid-Knoten, die systemweite Aufgabenaktivität und die Sicherungsvorgänge der Dienste.
- Prüfmeldungen zum Objektspeicher beziehen sich auf die Speicherung und Verwaltung von Objekten innerhalb von StorageGRID, einschließlich der Speicherung und Abfrage von Objekten, Übertragungen von Grid-Knoten zu Grid-Knoten und Überprüfungen.
- Wenn eine S3-Clientanwendung eine Anforderung zum Erstellen, Ändern oder Abrufen eines Objekts stellt, werden Prüfmeldungen zum Lesen und Schreiben des Clients protokolliert.

- Management-Audit-Meldungen protokollieren Benutzeranfragen an die Management-API.

Jeder Admin-Knoten speichert Audit-Nachrichten in Textdateien. Die Audit-Freigabe enthält die aktive Datei (audit.log) sowie komprimierte Audit-Protokolle der vorherigen Tage. Jeder Knoten im Raster speichert außerdem eine Kopie der auf dem Knoten generierten Prüfinformationen.

Sie können direkt über die Befehlszeile des Admin-Knotens auf die Audit-Protokolldateien zugreifen.

StorageGRID kann standardmäßig Audit-Informationen senden, oder Sie können das Ziel ändern:

- StorageGRID verwendet standardmäßig lokale Knoten-Auditziele.
- Prüfprotokolleinträge von Grid Manager und Tenant Manager können an einen Speicherknoten gesendet werden.
- Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert.
- "Erfahren Sie mehr über die Konfiguration von Audit-Meldungen und Protokollzielen" .

Weitere Informationen zur Audit-Protokolldatei, zum Format der Audit-Meldungen, zu den Typen der Audit-Meldungen und zu den verfügbaren Tools zur Analyse der Audit-Meldungen finden Sie unter"Überprüfen der Überwachungsprotokolle" .

Erfassen von Protokolldateien und Systemdaten

Mit dem Grid Manager können Sie Protokolldateien und Systemdaten (einschließlich Konfigurationsdaten) für Ihr StorageGRID System abrufen.

Bevor Sie beginnen

- Sie müssen beim Grid Manager auf dem primären Admin-Knoten mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die Bereitstellungspassphrase verfügen.

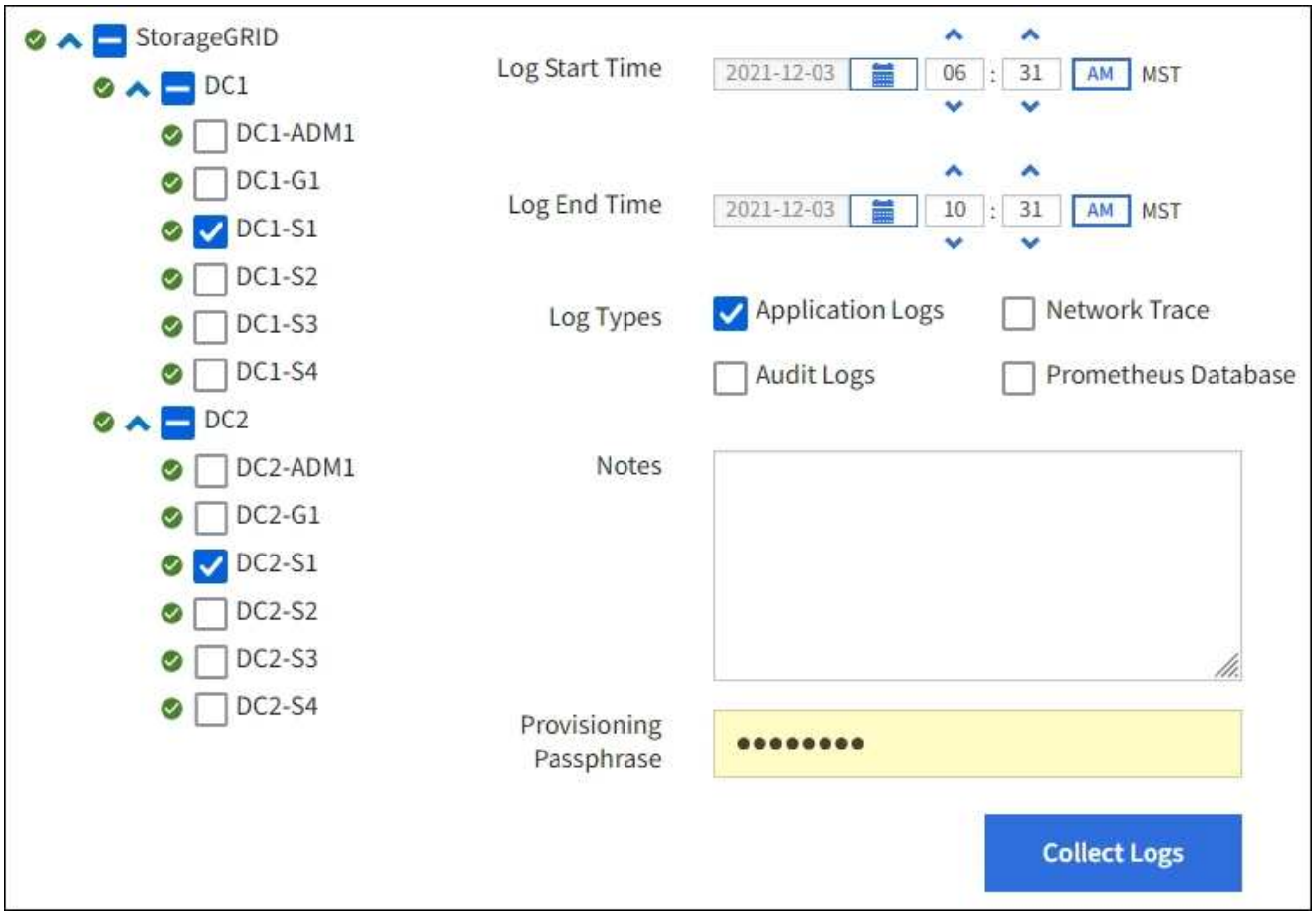
Informationen zu diesem Vorgang

Mit dem Grid Manager können Sie"Protokolldateien" , Systemdaten und Konfigurationsdaten von jedem Grid-Knoten für den von Ihnen ausgewählten Zeitraum. Daten werden gesammelt und in einer .tar.gz-Datei archiviert, die Sie dann auf Ihren lokalen Computer herunterladen können.

Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Protokolle**.



2. Wählen Sie die Grid-Knoten aus, für die Sie Protokolldateien sammeln möchten.

   Bei Bedarf können Sie Protokolldateien für das gesamte Grid oder einen gesamten Rechenzentrumsstandort sammeln.

3. Wählen Sie eine **Startzeit** und eine **Endzeit** aus, um den Zeitbereich der Daten festzulegen, die in die Protokolldateien aufgenommen werden sollen.

   Wenn Sie einen sehr langen Zeitraum auswählen oder Protokolle von allen Knoten in einem großen Raster sammeln, kann das Protokollarchiv zu groß werden, um auf einem Knoten gespeichert zu werden, oder zu groß, um zum Download auf dem primären Admin-Knoten gesammelt zu werden. In diesem Fall müssen Sie die Protokollerfassung mit einem kleineren Datensatz neu starten.

4. Wählen Sie die Protokolltypen aus, die Sie sammeln möchten.
   - **Anwendungsprotokolle**: Anwendungsspezifische Protokolle, die der technische Support am häufigsten zur Fehlerbehebung verwendet. Die gesammelten Protokolle sind eine Teilmenge der verfügbaren Anwendungsprotokolle.
   - **Audit-Protokolle**: Protokolle mit den während des normalen Systembetriebs generierten Audit-Meldungen.
   - **Netzwerkverfolgung**: Protokolle, die zum Debuggen des Netzwerks verwendet werden.
   - **Prometheus-Datenbank**: Zeitreihenmetriken von den Diensten auf allen Knoten.
5. Geben Sie optional Notizen zu den Protokolldateien ein, die Sie im Textfeld **Notizen** sammeln.

   Mithilfe dieser Hinweise können Sie dem technischen Support Informationen zu dem Problem geben, das Sie zum Sammeln der Protokolldateien veranlasst hat. Ihre Notizen werden einer Datei mit dem Namen

hinzugefügt `info.txt` , zusammen mit anderen Informationen zur Protokolldateisammlung. Der `info.txt` Die Datei wird im Protokolldatei-Archivpaket gespeichert.

6. Geben Sie die Bereitstellungspassphrase für Ihr StorageGRID -System in das Textfeld **Bereitstellungspassphrase** ein.
7. Wählen Sie **Protokolle sammeln**.

   Wenn Sie eine neue Anfrage senden, wird die vorherige Sammlung von Protokolldateien gelöscht.

   Auf der Seite „Protokolle“ können Sie den Fortschritt der Protokolldateierfassung für jeden Grid-Knoten überwachen.

   Wenn Sie eine Fehlermeldung bezüglich der Protokollgröße erhalten, versuchen Sie, Protokolle für einen kürzeren Zeitraum oder für weniger Knoten zu sammeln.

8. Wählen Sie **Herunterladen**, wenn die Protokolldateierfassung abgeschlossen ist.

   Die Datei *.tar.gz* enthält alle Protokolldateien von allen Grid-Knoten, bei denen die Protokollerfassung erfolgreich war. In der kombinierten *.tar.gz*-Datei befindet sich für jeden Grid-Knoten ein Protokolldateiarchiv.

Nach Abschluss

Sie können das Protokolldatei-Archivpaket bei Bedarf später erneut herunterladen.

Optional können Sie **Löschen** auswählen, um das Protokolldatei-Archivpaket zu entfernen und Speicherplatz freizugeben. Das aktuelle Protokolldatei-Archivpaket wird beim nächsten Sammeln von Protokolldateien automatisch entfernt.

Manuelles Auslösen eines AutoSupport -Pakets

Um den technischen Support bei der Behebung von Problemen mit Ihrem StorageGRID -System zu unterstützen, können Sie manuell das Senden eines AutoSupport Pakets auslösen.

Bevor Sie beginnen

- Sie müssen beim Grid Manager mit einem"unterstützter Webbrowser" .
- Sie müssen über Root-Zugriff oder die Berechtigung „Andere Rasterkonfiguration“ verfügen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport*.
2. Wählen Sie auf der Registerkarte **Aktionen** die Option **Benutzergesteuerten AutoSupport senden**.

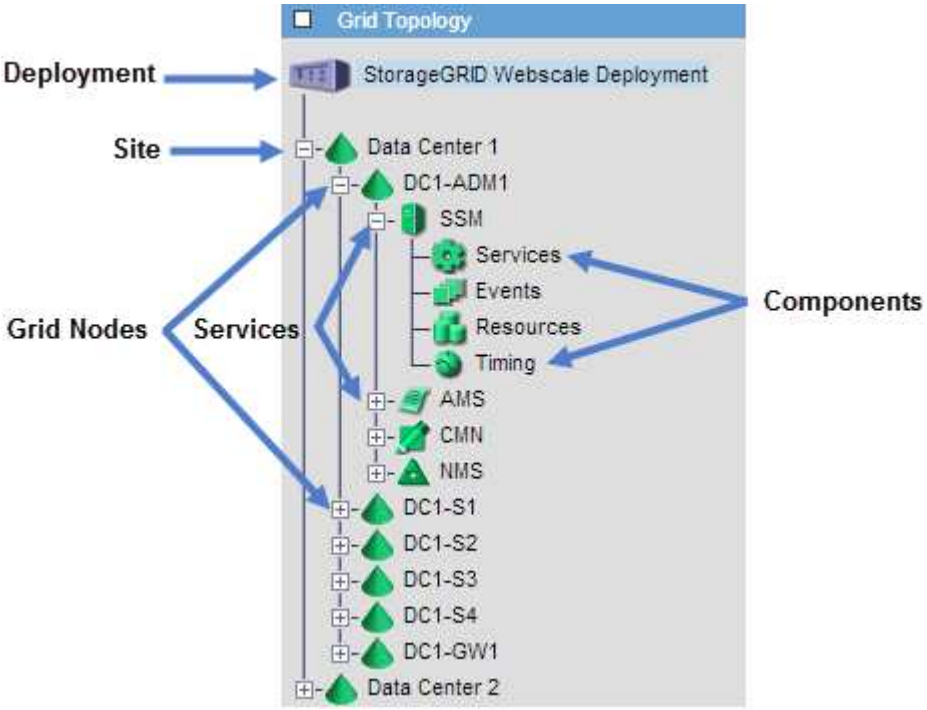
   StorageGRID versucht, ein AutoSupport Paket an die NetApp Support-Site zu senden. Wenn der Versuch erfolgreich ist, werden die Werte **Neuestes Ergebnis** und **Letzter erfolgreicher Zeitpunkt** auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, wird der Wert **Neuestes Ergebnis** auf „Fehlgeschlagen“ aktualisiert und StorageGRID versucht nicht, das AutoSupport Paket erneut zu senden.

   Aktualisieren Sie nach dem Senden eines vom Benutzer ausgelösten AutoSupport Pakets die AutoSupport -Seite in Ihrem Browser nach 1 Minute, um auf die aktuellsten Ergebnisse zuzugreifen.

Den Netztopologie-Baum anzeigen

Der Grid-Topologie-Baum bietet Zugriff auf detaillierte Informationen zu StorageGRID -Systemelementen, einschließlich Sites, Grid-Knoten, Diensten und Komponenten. In den meisten Fällen müssen Sie nur auf den Grid-Topologie-Baum zugreifen, wenn Sie in der Dokumentation dazu aufgefordert werden oder wenn Sie mit dem technischen Support zusammenarbeiten.

Um auf den Gittertopologie-Baum zuzugreifen, wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.



Um den Gittertopologie-Baum zu erweitern oder zu reduzieren, klicken Sie auf ⊞ oder ⊟ auf Site-, Knoten- oder Serviceebene. Um alle Elemente der gesamten Site oder in jedem Knoten zu erweitern oder zu reduzieren, halten Sie die Taste **<Strg>** gedrückt und klicken Sie.

StorageGRID -Attribute

Attribute melden Werte und Status für viele Funktionen des StorageGRID Systems. Attributwerte sind für jeden Rasterknoten, jeden Standort und das gesamte Raster verfügbar.

StorageGRID -Attribute werden an mehreren Stellen im Grid Manager verwendet:

- **Knotenseite**: Viele der auf der Knotenseite angezeigten Werte sind StorageGRID -Attribute. (Prometheus-Metriken werden auch auf den Knotenseiten angezeigt.)
- **Gittertopologiebaum**: Attributwerte werden im Gittertopologiebaum angezeigt (**SUPPORT** > **Tools** > **Gittertopologie**).
- **Ereignisse**: Systemereignisse treten auf, wenn bestimmte Attribute einen Fehler oder Störungszustand für einen Knoten aufzeichnen, einschließlich Fehlern wie Netzwerkfehlern.

Attributwerte

Die Attribute werden nach bestem Wissen und Gewissen gemeldet und sind annähernd richtig. Attributaktualisierungen können unter bestimmten Umständen verloren gehen, beispielsweise beim Absturz

eines Dienstes oder beim Ausfall und Wiederaufbau eines Grid-Knotens.

Darüber hinaus können Ausbreitungsverzögerungen die Meldung von Attributen verlangsamen. Aktualisierte Werte für die meisten Attribute werden in festen Intervallen an das StorageGRID System gesendet. Es kann mehrere Minuten dauern, bis eine Aktualisierung im System sichtbar ist, und zwei Attribute, die sich mehr oder weniger gleichzeitig ändern, können zu leicht unterschiedlichen Zeitpunkten gemeldet werden.

Überprüfen der Supportmetriken

Bei der Fehlerbehebung können Sie mit dem technischen Support zusammenarbeiten, um detaillierte Messwerte und Diagramme für Ihr StorageGRID System zu überprüfen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

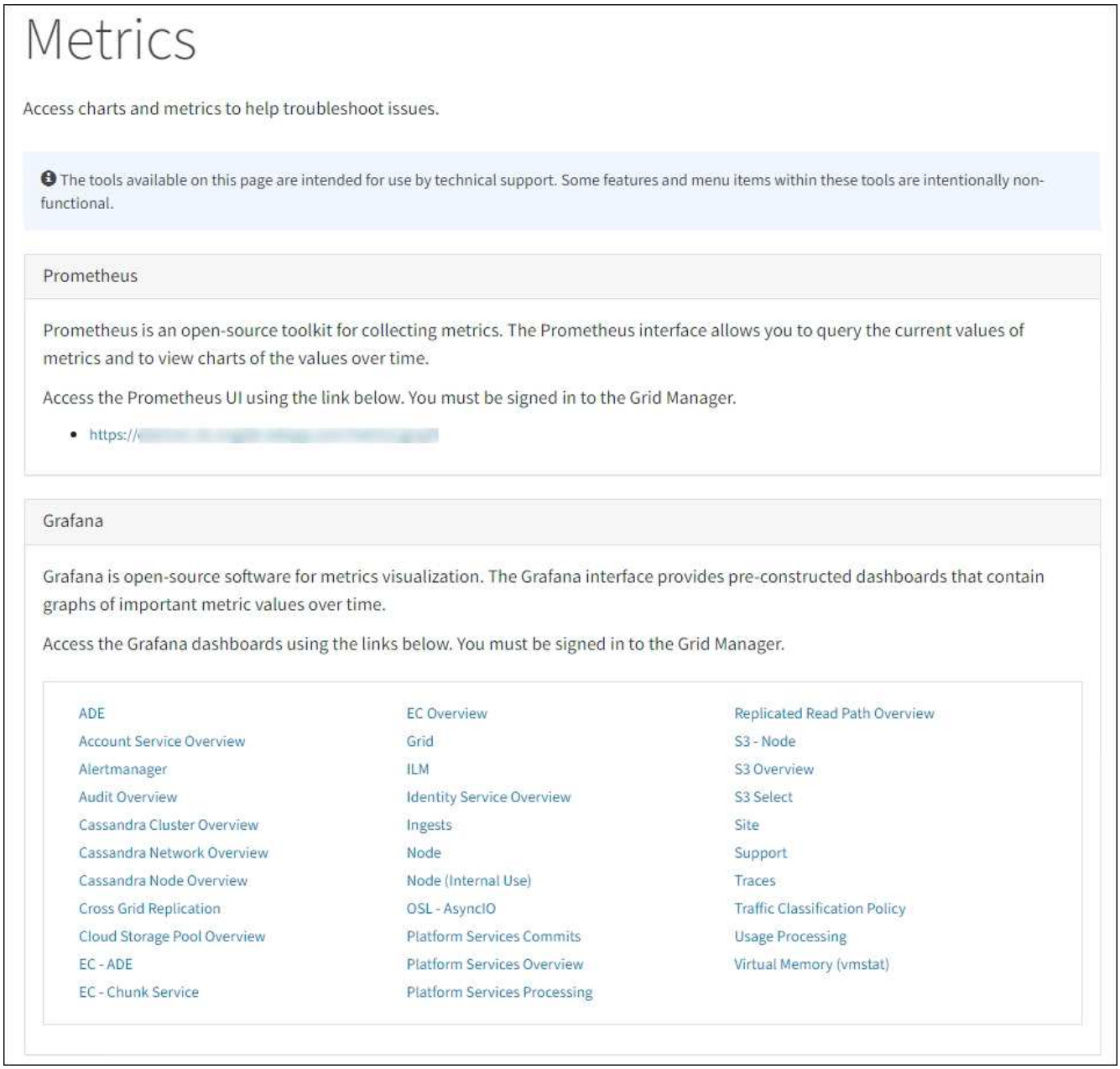
Über die Seite „Metriken“ können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist eine Open-Source-Software zum Sammeln von Metriken. Grafana ist eine Open-Source-Software zur Visualisierung von Metriken.

> ⓘ Die auf der Seite „Metriken“ verfügbaren Tools sind für die Verwendung durch den technischen Support vorgesehen. Einige Funktionen und Menüelemente dieser Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe die Liste der"häufig verwendete Prometheus-Metriken" .

Schritte

1. Wählen Sie gemäß den Anweisungen des technischen Supports **SUPPORT** > **Tools** > **Metriken**.

   Ein Beispiel für die Seite „Metriken“ wird hier angezeigt:



2. Um die aktuellen Werte der StorageGRID -Metriken abzufragen und Diagramme der Werte im Zeitverlauf anzuzeigen, klicken Sie auf den Link im Abschnitt „Prometheus“.

   Die Prometheus-Oberfläche wird angezeigt. Sie können diese Schnittstelle verwenden, um Abfragen zu den verfügbaren StorageGRID -Metriken auszuführen und StorageGRID -Metriken im Zeitverlauf grafisch darzustellen.

   > Metriken, deren Namen „*private*“ enthalten, sind nur für den internen Gebrauch bestimmt und können zwischen StorageGRID Versionen ohne Vorankündigung geändert werden.

3. Um auf vorgefertigte Dashboards mit Diagrammen der StorageGRID -Metriken im Zeitverlauf zuzugreifen, klicken Sie auf die Links im Abschnitt „Grafana“.

   Die Grafana-Schnittstelle für den von Ihnen ausgewählten Link wird angezeigt.

Diagnose ausführen

Bei der Fehlerbehebung können Sie mit dem technischen Support zusammenarbeiten, um eine Diagnose Ihres StorageGRID -Systems durchzuführen und die Ergebnisse zu überprüfen.

- "Überprüfen der Supportmetriken"
- "Häufig verwendete Prometheus-Metriken"

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Auf der Seite „Diagnose“ wird eine Reihe von Diagnoseprüfungen zum aktuellen Status des Rasters durchgeführt. Jede Diagnoseprüfung kann einen von drei Status haben:

- **Normal**: Alle Werte liegen im Normalbereich.
- **Achtung**: Einer oder mehrere Werte liegen außerhalb des Normalbereichs.
- **Achtung**: Einer oder mehrere Werte liegen deutlich außerhalb des Normalbereichs.

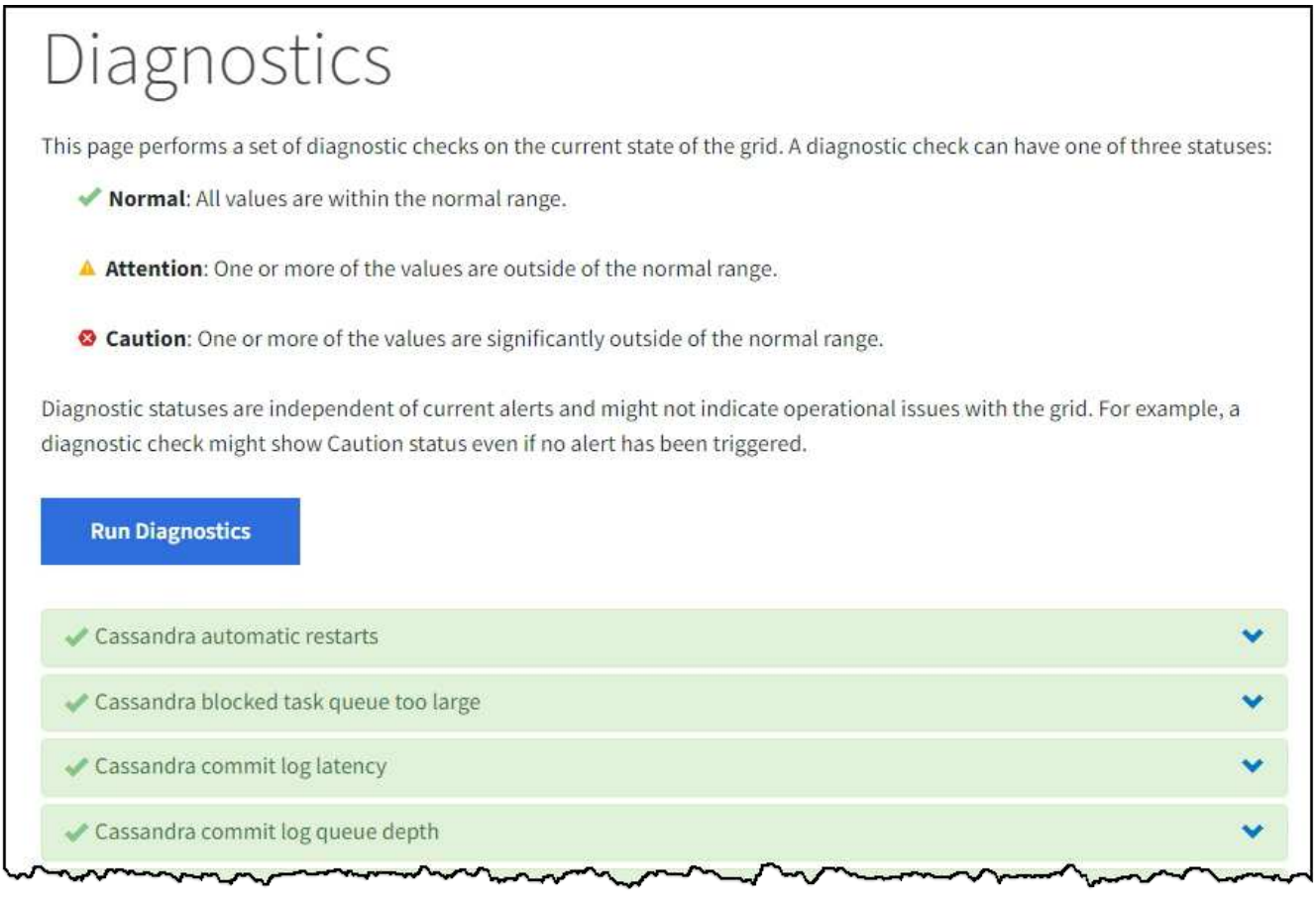
Diagnosestatus sind unabhängig von aktuellen Warnungen und weisen möglicherweise nicht auf Betriebsprobleme mit dem Netz hin. Beispielsweise kann eine Diagnoseprüfung den Status „Vorsicht“ anzeigen, auch wenn kein Alarm ausgelöst wurde.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Diagnose**.

   Die Seite „Diagnose“ wird angezeigt und listet die Ergebnisse für jede Diagnoseprüfung auf. Die Ergebnisse werden nach Schweregrad sortiert (Vorsicht, Achtung und dann Normal). Innerhalb jedes Schweregrads werden die Ergebnisse alphabetisch sortiert.

   In diesem Beispiel haben alle Diagnosen den Status „Normal“.



2. Um mehr über eine bestimmte Diagnose zu erfahren, klicken Sie irgendwo in die Zeile.

   Es werden Details zur Diagnose und ihren aktuellen Ergebnissen angezeigt. Die folgenden Details sind aufgeführt:

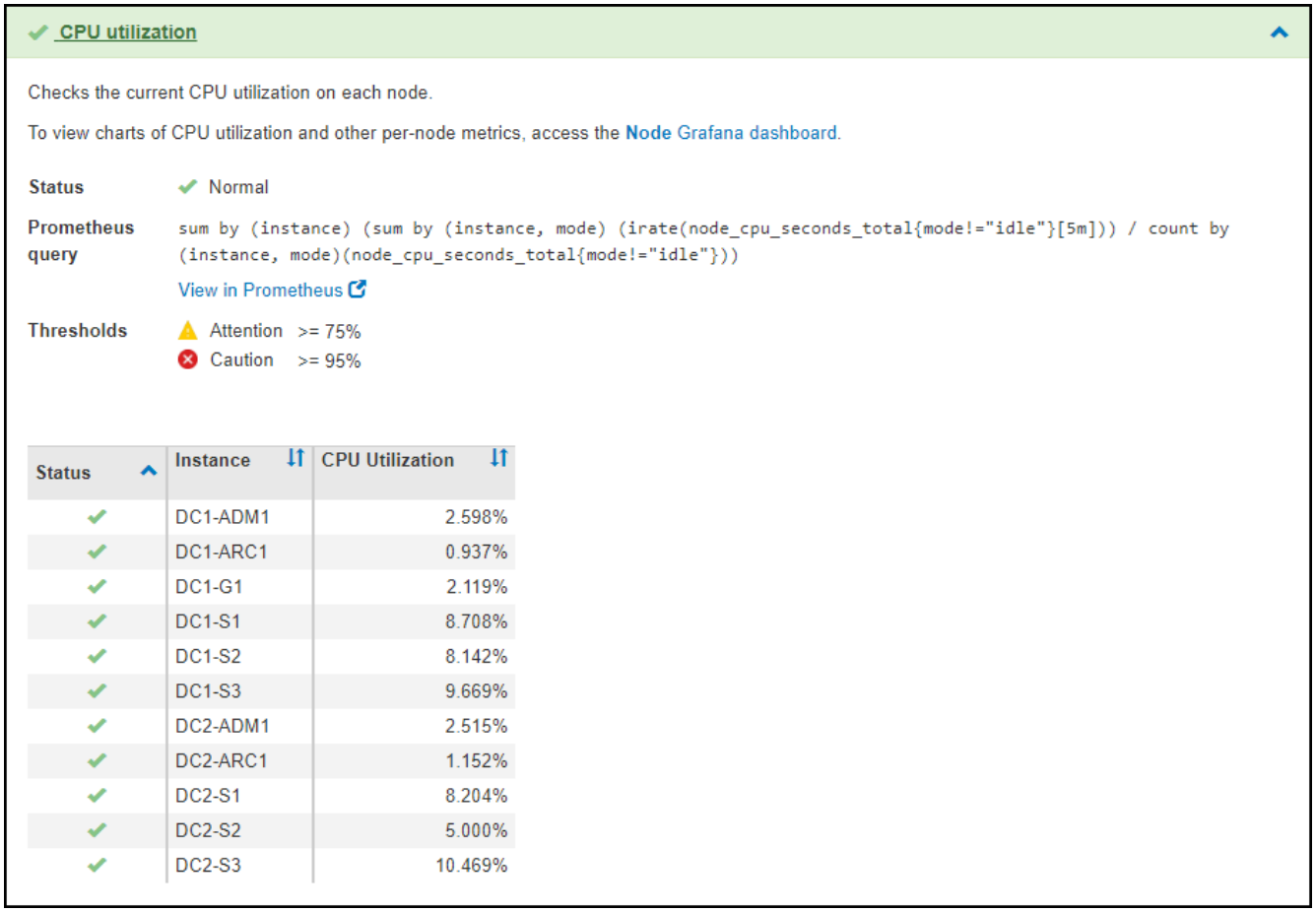
   - **Status**: Der aktuelle Status dieser Diagnose: Normal, Achtung oder Vorsicht.
   - **Prometheus-Abfrage**: Falls für die Diagnose verwendet, der Prometheus-Ausdruck, der zum

Generieren der Statuswerte verwendet wurde. (Nicht für alle Diagnosen wird ein Prometheus-Ausdruck verwendet.)

- **Schwellenwerte**: Sofern für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden abnormalen Diagnosestatus. (Schwellenwerte werden nicht für alle Diagnosen verwendet.)

  Sie können diese Schwellenwerte nicht ändern.

- **Statuswerte**: Eine Tabelle, die den Status und den Wert der Diagnose im gesamten StorageGRID -System anzeigt. In diesem Beispiel wird die aktuelle CPU-Auslastung für jeden Knoten in einem StorageGRID -System angezeigt. Alle Knotenwerte liegen unter den Schwellenwerten „Achtung“ und „Vorsicht“, sodass der Gesamtstatus der Diagnose „Normal“ ist.



3. **Optional**: Um Grafana-Diagramme im Zusammenhang mit dieser Diagnose anzuzeigen, klicken Sie auf den Link **Grafana-Dashboard**.

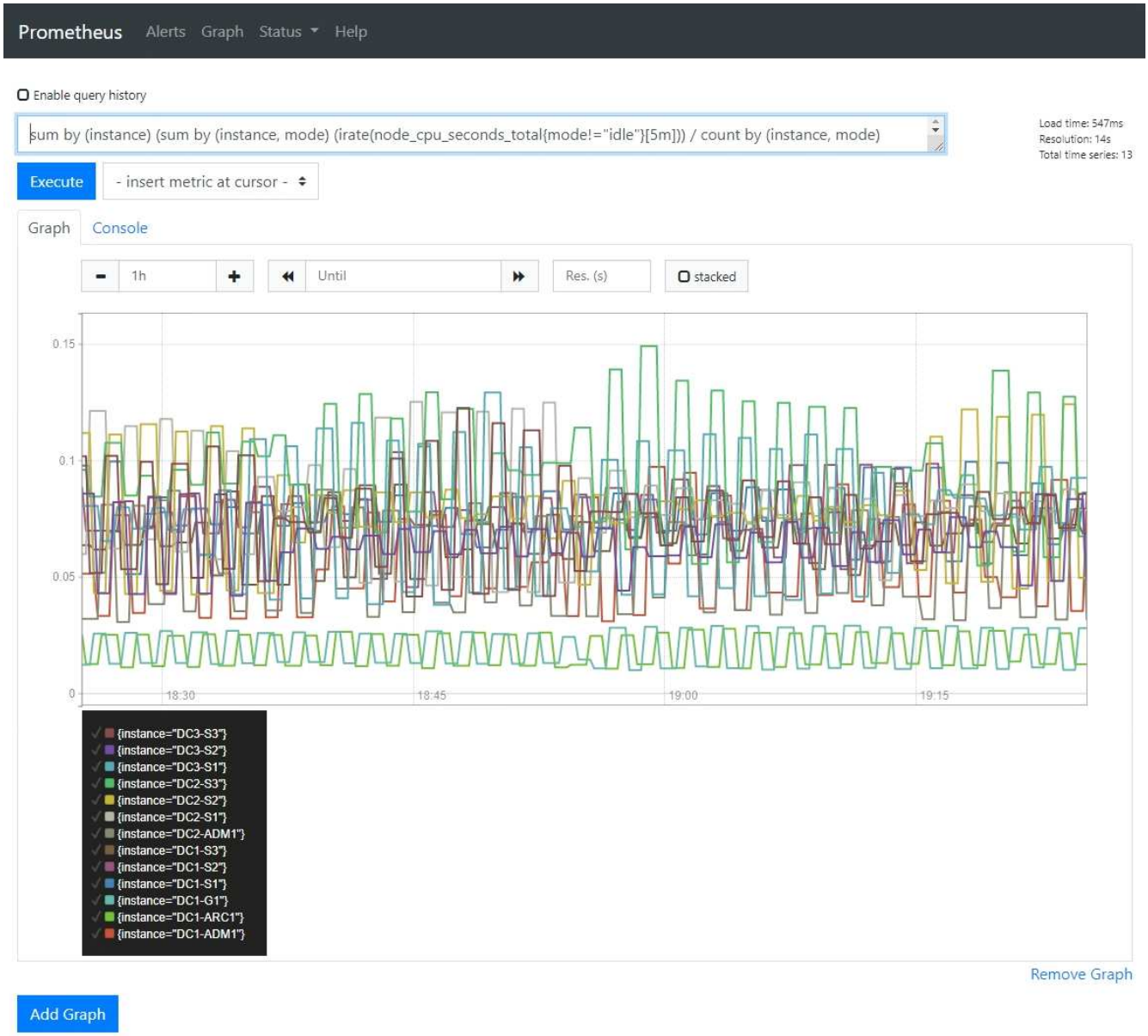
   Dieser Link wird nicht für alle Diagnosen angezeigt.

   Das zugehörige Grafana-Dashboard wird angezeigt. In diesem Beispiel wird das Knoten-Dashboard angezeigt, das die CPU-Auslastung im Zeitverlauf für diesen Knoten sowie andere Grafana-Diagramme für den Knoten anzeigt.

   Sie können auch über den Abschnitt „Grafana“ auf der Seite **SUPPORT** > **Tools** > **Metriken** auf die vorgefertigten Grafana-Dashboards zugreifen.

4. **Optional**: Um ein Diagramm des Prometheus-Ausdrucks im Zeitverlauf anzuzeigen, klicken Sie auf **In Prometheus anzeigen**.

   Es wird ein Prometheus-Diagramm des in der Diagnose verwendeten Ausdrucks angezeigt.



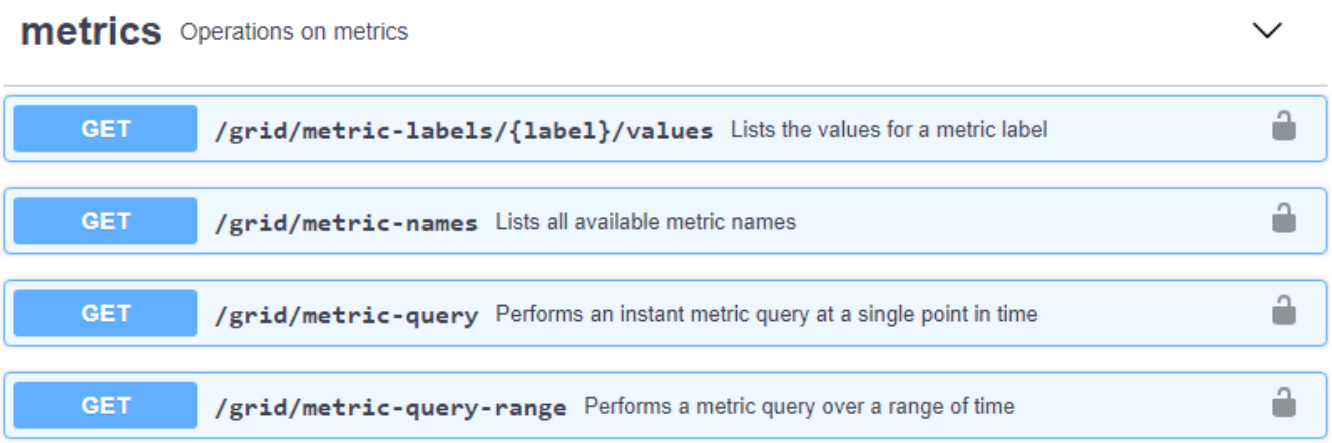
Erstellen Sie benutzerdefinierte Überwachungsanwendungen

Sie können benutzerdefinierte Überwachungsanwendungen und Dashboards mithilfe der StorageGRID -Metriken erstellen, die über die Grid Management API verfügbar sind.

Wenn Sie Metriken überwachen möchten, die nicht auf einer vorhandenen Seite des Grid Managers angezeigt werden, oder wenn Sie benutzerdefinierte Dashboards für StorageGRID erstellen möchten, können Sie die Grid Management-API verwenden, um StorageGRID -Metriken abzufragen.

Sie können auch mit einem externen Überwachungstool wie Grafana direkt auf Prometheus-Metriken zugreifen. Wenn Sie ein externes Tool verwenden, müssen Sie ein administratives Client-Zertifikat hochladen oder generieren, damit StorageGRID das Tool aus Sicherheitsgründen authentifizieren kann. Siehe die"Anweisungen zur Administration von StorageGRID" .

Um die Metrik-API-Operationen anzuzeigen, einschließlich der vollständigen Liste der verfügbaren Metriken, gehen Sie zum Grid Manager. Wählen Sie oben auf der Seite das Hilfesymbol und dann **API-Dokumentation** > **Metriken**
aus.



Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung gehen über den Rahmen dieser Dokumentation hinaus.

Fehlerbehebung beim StorageGRID -System

Fehlerbehebung bei einem StorageGRID -System

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

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

Definieren Sie das Problem

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

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

Frage	Beispielantwort
Was macht das StorageGRID -System bzw. was macht es nicht? Was sind die Symptome?	Clientanwendungen melden, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann begann das Problem?	Die Objektaufnahme wurde am 8. Januar 2020 gegen 14:50 Uhr erstmals verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Benachrichtigung durch Clientanwendung. Habe auch E-Mail-Benachrichtigungen erhalten.
Tritt das Problem ständig auf oder nur manchmal?	Das Problem besteht weiterhin.

Frage	Beispielantwort
Wenn das Problem regelmäßig auftritt, welche Schritte führen dazu, dass es auftritt?	Das Problem tritt jedes Mal auf, wenn ein Client versucht, ein Objekt aufzunehmen.
Wenn das Problem zeitweise auftritt, wann tritt es auf? Notieren Sie die Zeitpunkte aller Vorfälle, die Ihnen bekannt sind.	Das Problem tritt nicht zeitweise auf.
Ist Ihnen dieses Problem schon einmal begegnet? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dieses Problem ist mir zum ersten Mal begegnet.

Bewerten Sie das Risiko und die Auswirkungen auf das System

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

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

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

Daten sammeln

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

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Erstellen Sie eine Zeitleiste der letzten Änderungen	Änderungen an Ihrem StorageGRID -System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Erstellen Sie eine Zeitleiste der letzten Änderungen

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Benachrichtigungen überprüfen	Mithilfe von Warnmeldungen können Sie die Grundursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme liefern, die das Problem möglicherweise verursachen. Überprüfen Sie die Liste der aktuellen Warnungen, um festzustellen, ob StorageGRID die Grundursache eines Problems für Sie identifiziert hat. Überprüfen Sie in der Vergangenheit ausgelöste Warnungen, um zusätzliche Erkenntnisse zu erhalten.	• "Aktuelle und gelöste Warnmeldungen anzeigen"
Überwachen von Ereignissen	Zu den Ereignissen zählen alle Systemfehler oder Störungsereignisse für einen Knoten, einschließlich Fehlern wie Netzwerkfehlern. Überwachen Sie Ereignisse, um mehr über Probleme zu erfahren oder bei der Fehlerbehebung zu helfen.	• "Überwachen von Ereignissen"
Identifizieren Sie Trends mithilfe von Diagrammen und Textberichten	Trends können wertvolle Hinweise darauf liefern, wann Probleme erstmals auftraten, und Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	• "Verwenden Sie Diagramme und Grafiken" • "Verwenden Sie Textberichte"
Festlegen von Basislinien	Sammeln Sie Informationen über die Normalwerte verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Basiswerten können wertvolle Hinweise liefern.	• Festlegen von Basislinien
Durchführen von Aufnahme- und Abruftests	Um Leistungsprobleme beim Aufnehmen und Abrufen zu beheben, verwenden Sie eine Workstation zum Speichern und Abrufen von Objekten. Vergleichen Sie die Ergebnisse mit denen, die Sie bei Verwendung der Clientanwendung sehen.	• "Überwachen Sie die PUT- und GET-Leistung"
Überprüfen von Auditmeldungen	Überprüfen Sie die Prüfmeldungen, um die StorageGRID -Vorgänge im Detail zu verfolgen. Die Details in den Prüfmeldungen können bei der Behebung vieler Arten von Problemen hilfreich sein, darunter auch Leistungsprobleme.	• "Überprüfen von Auditmeldungen"

Art der zu erfassenden Daten	Warum diese Daten gesammelt werden	Anweisungen
Überprüfen Sie die Objektstandorte und Speicherintegrität	Wenn Sie Speicherprobleme haben, überprüfen Sie, ob die Objekte dort platziert werden, wo Sie es erwarten. Überprüfen Sie die Integrität der Objektdaten auf einem Speicherknoten.	• "Überwachen von Objektüberprüfungsvorgängen" • "Bestätigen Sie die Speicherorte der Objektdaten" • "Überprüfen der Objektintegrität"
Sammeln Sie Daten für den technischen Support	Der technische Support bittet Sie möglicherweise, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um bei der Behebung von Problemen zu helfen.	• "Erfassen von Protokolldateien und Systemdaten" • "Manuelles Auslösen eines AutoSupport -Pakets" • "Überprüfen der Supportmetriken"

Erstellen Sie eine Zeitleiste der letzten Änderungen

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

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

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann die einzelnen Änderungen vorgenommen wurden, sowie alle relevanten Details zu den Änderungen, z. B. Informationen darüber, was sonst noch während der Änderung geschah:

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

Beispiele für bedeutende aktuelle Änderungen

Hier sind einige Beispiele für potenziell bedeutende Änderungen:

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

Festlegen von Basislinien

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

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

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

Daten analysieren

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

Die Analyse ist problemabhängig, aber im Allgemeinen gilt:

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

Checkliste für Eskalationsinformationen

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

✔	Artikel	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann begann das Problem? Passiert das ständig oder zeitweise? Wenn es zeitweise auftritt, wann ist es aufgetreten? Definieren Sie das Problem
	Folgenabschätzung	Wie schwerwiegend ist das Problem? Welche Auswirkungen hat dies auf die Clientanwendung? • Hat der Client zuvor eine erfolgreiche Verbindung hergestellt? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID -System-ID	Wählen Sie **WARTUNG** > **System** > **Lizenz**. Die StorageGRID -System-ID wird als Teil der aktuellen Lizenz angezeigt.
	Softwareversion	Wählen Sie oben im Grid Manager das Hilfesymbol und dann **Info** aus, um die StorageGRID -Version anzuzeigen.
	Anpassung	Fassen Sie zusammen, wie Ihr StorageGRID -System konfiguriert ist. Listen Sie beispielsweise Folgendes auf: • Verwendet das Grid Speicherkomprimierung, Speicherverschlüsselung oder Compliance? • Erstellt ILM replizierte oder löschcodierte Objekte? Stellt ILM die Standortredundanz sicher? Verwenden ILM-Regeln die Aufnahmeverhalten „Balanced“, „Strict“ oder „Dual Commit“?
	Protokolldateien und Systemdaten	Sammeln Sie Protokolldateien und Systemdaten für Ihr System. Wählen Sie **SUPPORT** > **Tools** > **Protokolle**. Sie können Protokolle für das gesamte Raster oder für ausgewählte Knoten sammeln. Wenn Sie Protokolle nur für ausgewählte Knoten sammeln, achten Sie darauf, mindestens einen Speicherknoten einzuschließen, der über den ADC-Dienst verfügt. (Die ersten drei Speicherknoten an einem Standort umfassen den ADC-Dienst.) "Erfassen von Protokolldateien und Systemdaten"
	Basisinformationen	Sammeln Sie Basisinformationen zu Aufnahmevorgängen, Abrufvorgängen und Speicherverbrauch. Festlegen von Basislinien

✔	Artikel	Hinweise
	Zeitleiste der jüngsten Änderungen	Erstellen Sie eine Zeitleiste, die alle aktuellen Änderungen am System oder seiner Umgebung zusammenfasst. Erstellen Sie eine Zeitleiste der letzten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie selbst Schritte zur Diagnose oder Fehlerbehebung des Problems unternommen haben, dokumentieren Sie die durchgeführten Schritte und das Ergebnis.

Beheben von Objekt- und Speicherproblemen

Bestätigen Sie die Speicherorte der Objektdaten

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

Bevor Sie beginnen

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

Schritte

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

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

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

4. Wählen Sie **Nachschlagen**.

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

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

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


Fehler im Objektspeicher (Speichervolumen)

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

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

Disk devices

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

Volumes

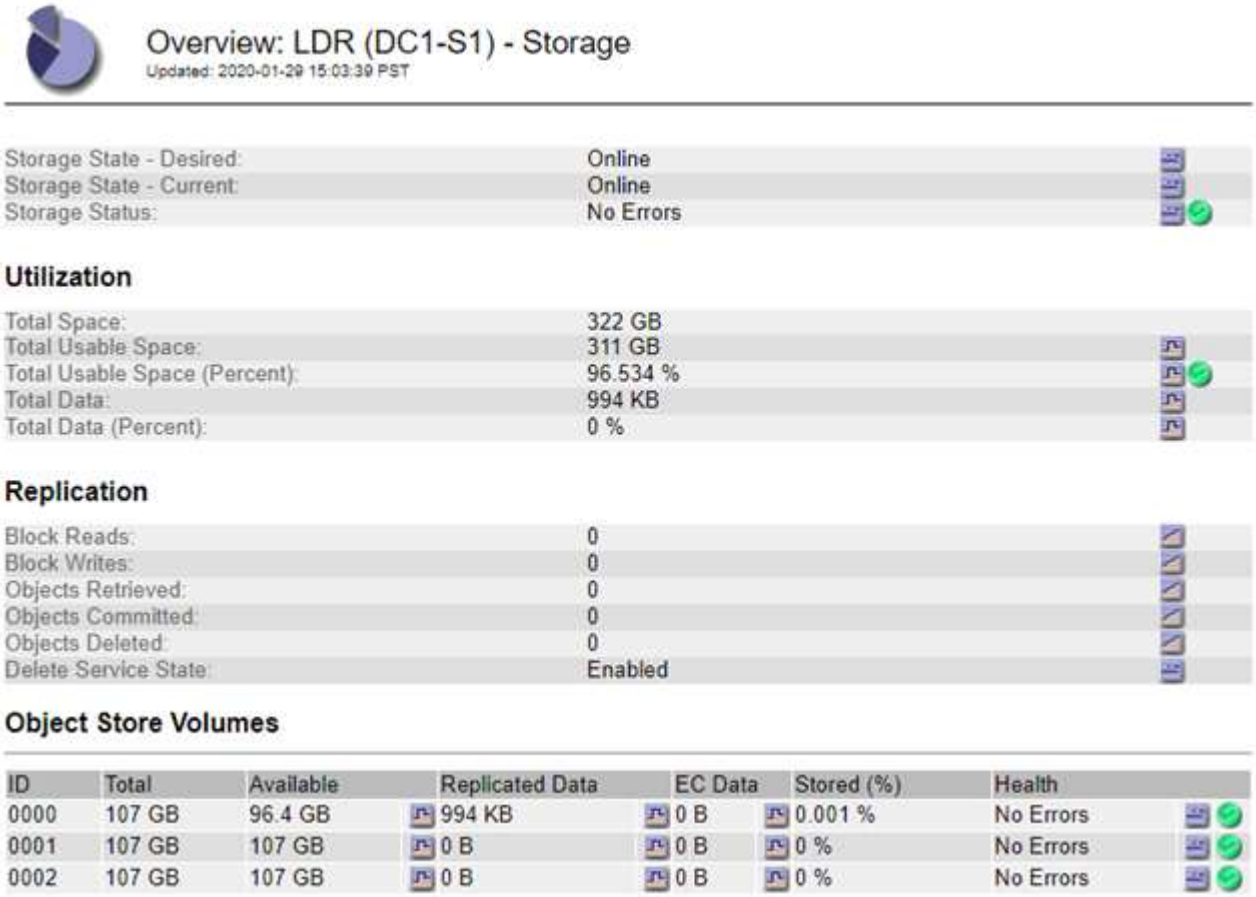
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

Object stores

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

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

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



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

Überprüfen der Objektintegrität

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

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

Was ist eine Hintergrundüberprüfung?

Der Hintergrundüberprüfungsprozess prüft Speicherknoten automatisch und kontinuierlich auf beschädigte

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

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

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

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

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

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

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

Warnungen im Zusammenhang mit der Hintergrundüberprüfung

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

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

Ändern Sie die Hintergrundüberprüfungsrate

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

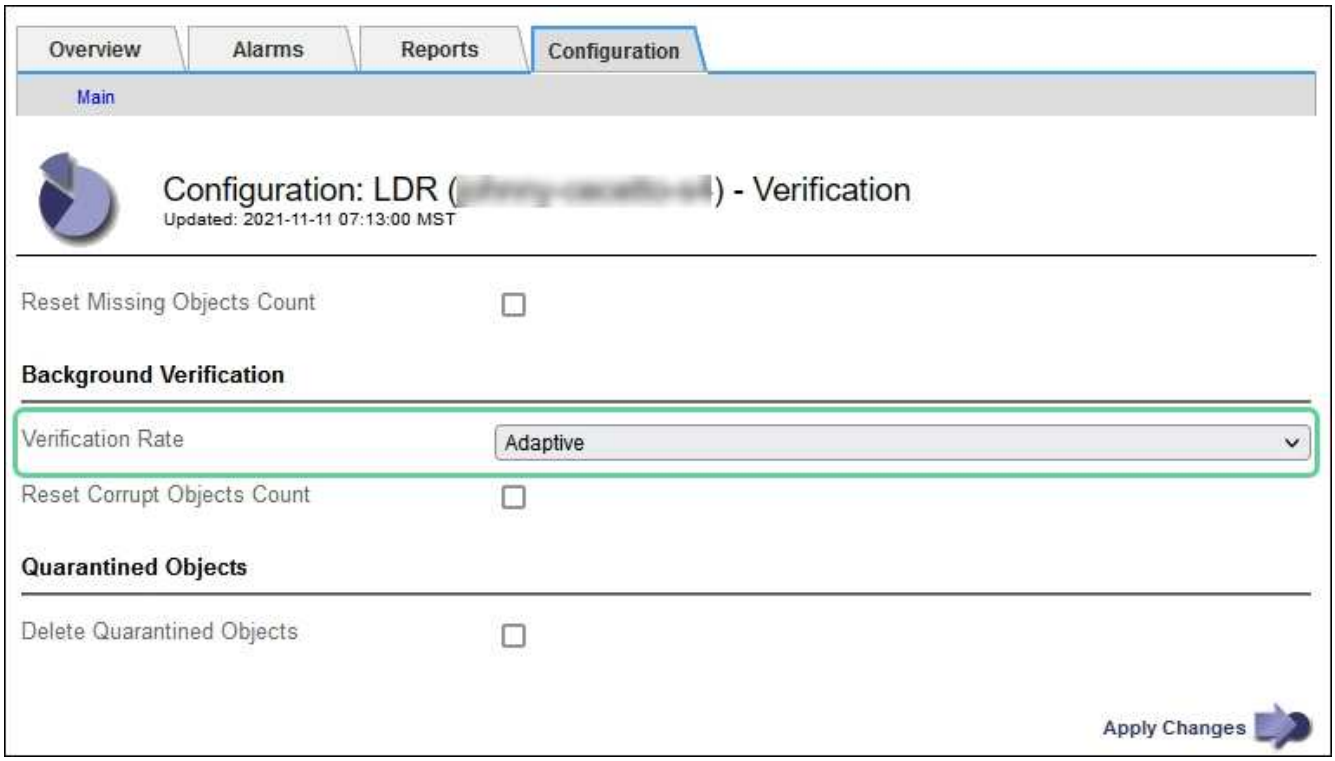
- Adaptiv: Standardeinstellung. Die Aufgabe ist für eine Überprüfung mit maximal 4 MB/s oder 10 Objekten/s ausgelegt (je nachdem, was zuerst überschritten wird).

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

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

Schritte

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



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

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

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

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

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

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

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

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

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

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

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

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

Was ist eine Objektexistenzprüfung?

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

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

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

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

Führen Sie eine Objekt-Existenzprüfung durch

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

Bevor Sie beginnen

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

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

Informationen zu diesem Vorgang

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

Schritte

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

   Sie können nach Knotennamen oder Site suchen.

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

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

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

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

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

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

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

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

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

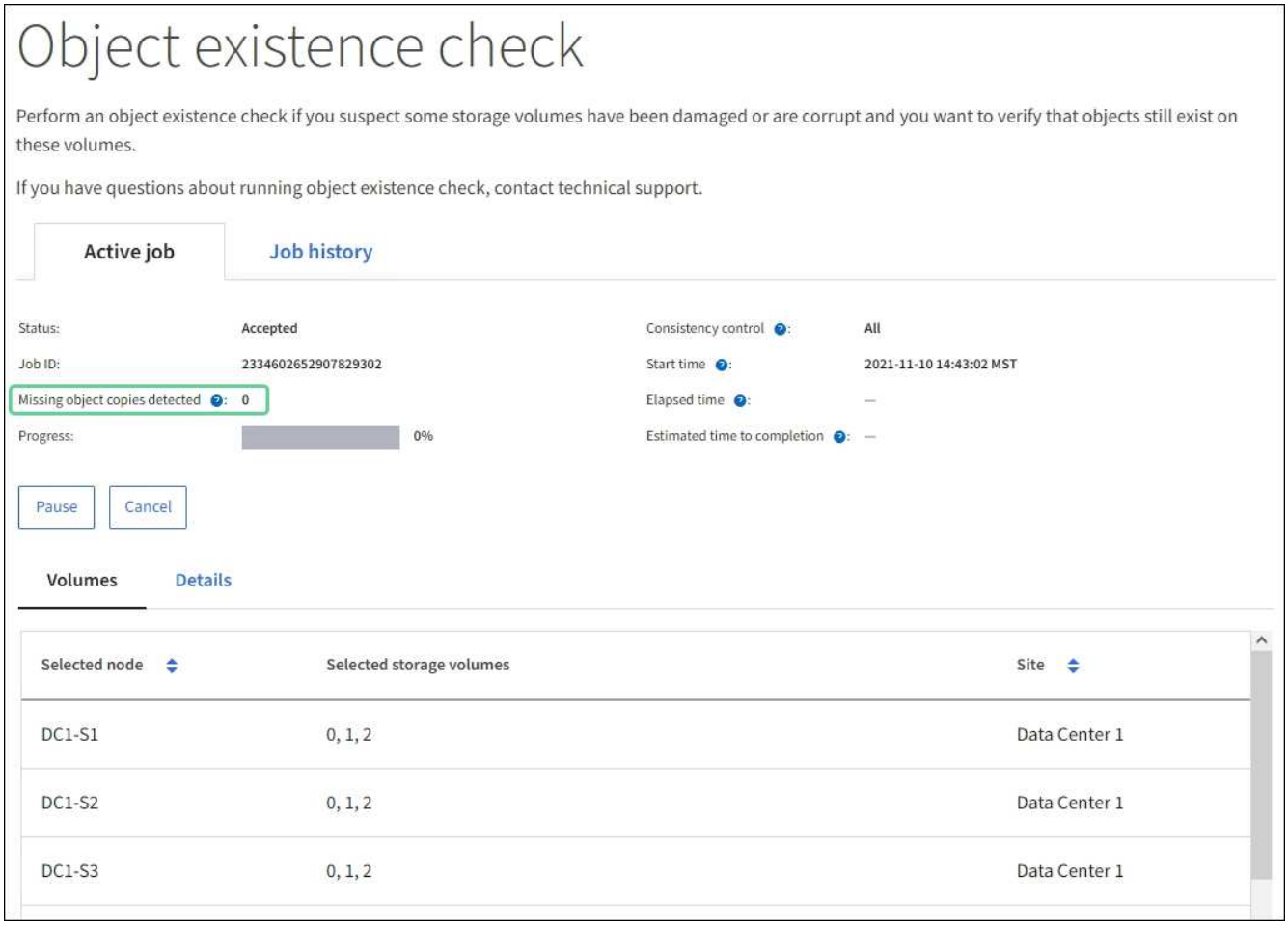
   - Der Auftrag ist abgeschlossen.
   - Sie pausieren oder brechen den Auftrag ab. Sie können einen Job fortsetzen, den Sie angehalten haben, aber Sie können einen Job nicht fortsetzen, den Sie abgebrochen haben.
   - Der Job stockt. Die Warnung „Prüfung der Objektexistenz ist ins Stocken geraten“ wird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

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

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

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

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



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

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

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

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

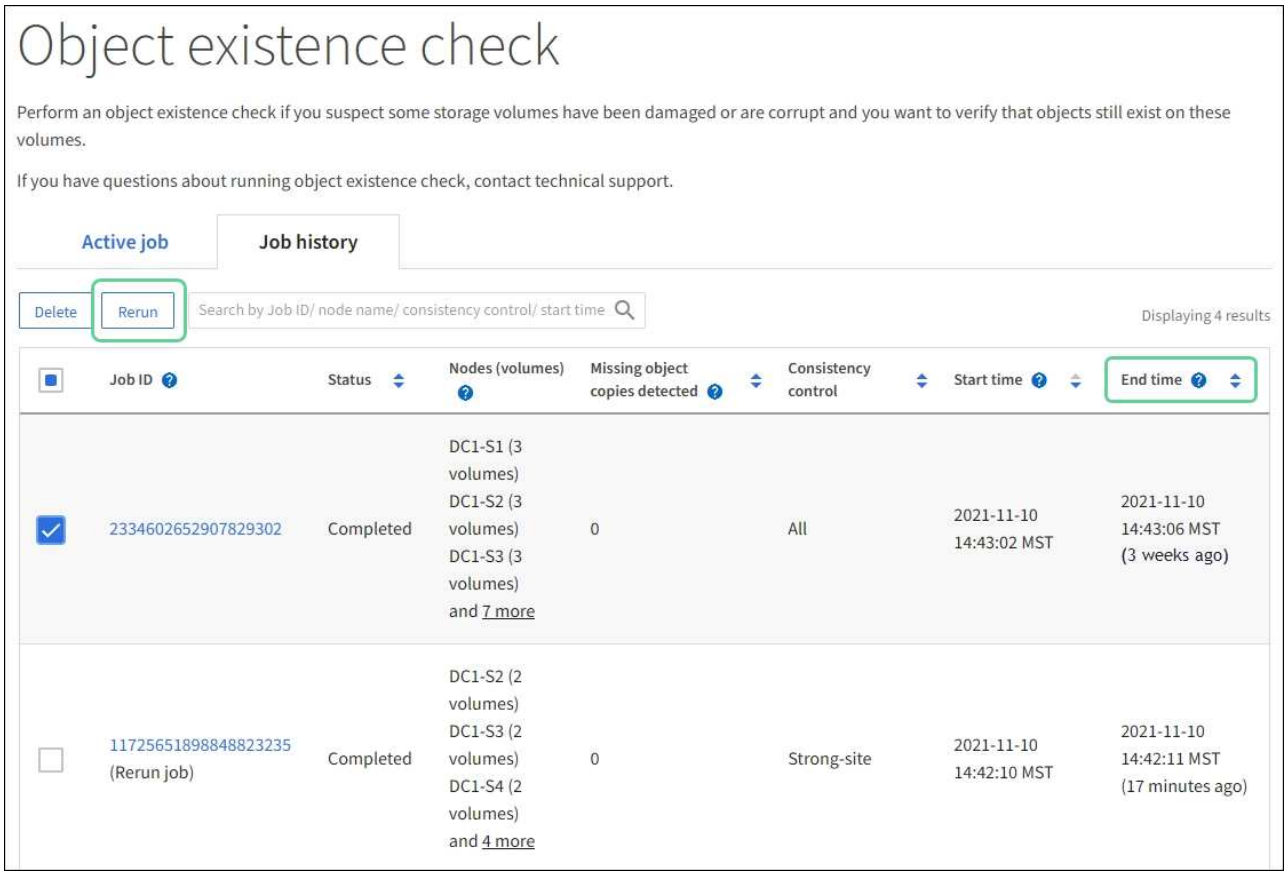
a. Wählen Sie **WARTUNG** > **Objektexistenzprüfung** > **Auftragsverlauf**.

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

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

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

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



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

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

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

Nach Abschluss

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

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

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

Bevor Sie beginnen

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

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

Schritte

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

   a. Eingeben `ssh admin@primary_Admin_Node_IP`

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

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

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

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

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

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

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

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

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

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

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

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

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

Beispiel für Audit-Protokollergebnisse

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

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

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

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

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

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

      Beispiel bycast.log

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

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

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

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

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

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

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

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

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

Untersuchen Sie verlorene Gegenstände

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

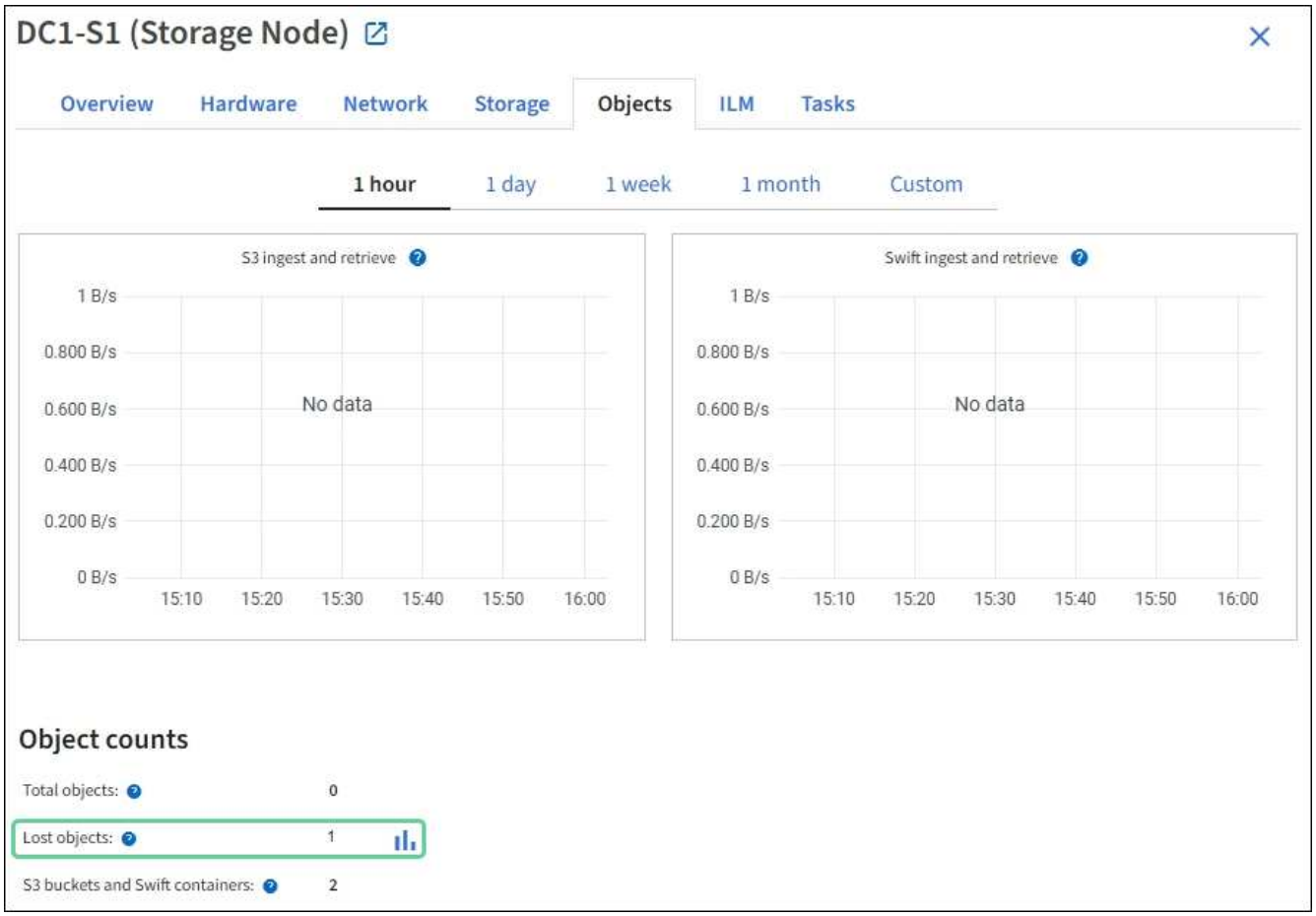
Die Warnung „Objekte verloren“ zeigt an, dass StorageGRID davon ausgeht, dass im Grid keine Kopien eines Objekts vorhanden sind. Möglicherweise sind die Daten dauerhaft verloren gegangen.

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

Schritte

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suchen und Wiederherstellen potenziell verlorener Objekte

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

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

Schritte

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

   a. Melden Sie sich beim Grid-Knoten an:

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

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

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

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

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

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

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

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

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

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

      Beispiel:

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

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

      Beispiel:

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

Eine LLST-Auditnachricht sieht wie diese Beispielnachricht aus.

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

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

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

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

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

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

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

a. Melden Sie sich beim Grid-Knoten an:

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

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

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

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

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

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

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

Geben Sie beispielsweise Folgendes ein:

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

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

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

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

      Geben Sie beispielsweise Folgendes ein:

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

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

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

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

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

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

      Fahren Sie mit dem nächsten Schritt fort.

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

Speicherorte erstellt wurden:

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

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

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

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

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

a. Melden Sie sich beim Grid-Knoten an:

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

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

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

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

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

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

Beispiel:

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

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

Beispiel:

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

Eine ORLM-Auditnachricht sieht wie diese Beispielnachricht aus.

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

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

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

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

Zurücksetzen der Anzahl verlorener und fehlender Objekte

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

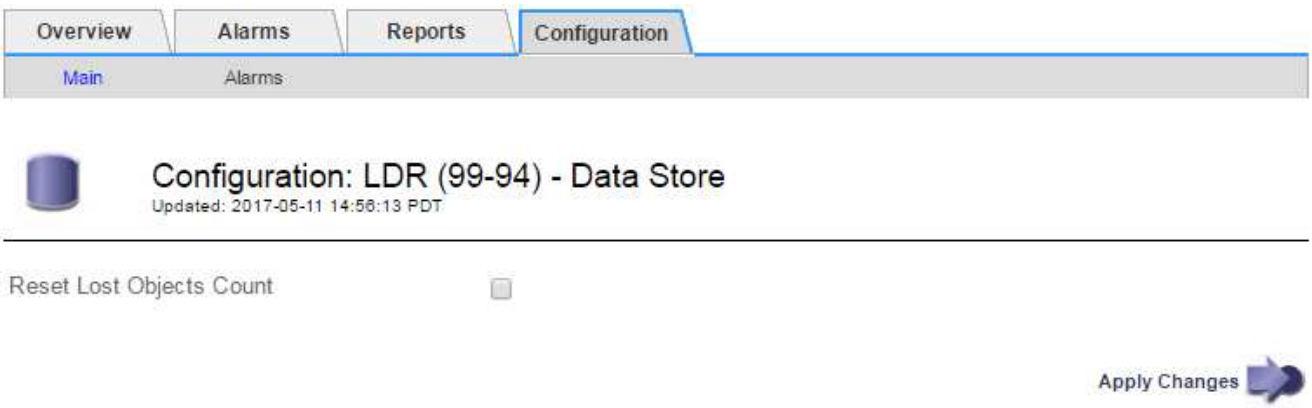
Sie können den Zähler für verlorene Objekte auf einer der folgenden Seiten zurücksetzen:

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

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

Schritte

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



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

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

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

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

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

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

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

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

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

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

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

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

Fehlerbehebung bei der Warnung „Niedriger Objektdatenspeicher“

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

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

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

In diesem Zustand:

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

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

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

Schritte

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

   Die Seite „Warnungen“ wird angezeigt.

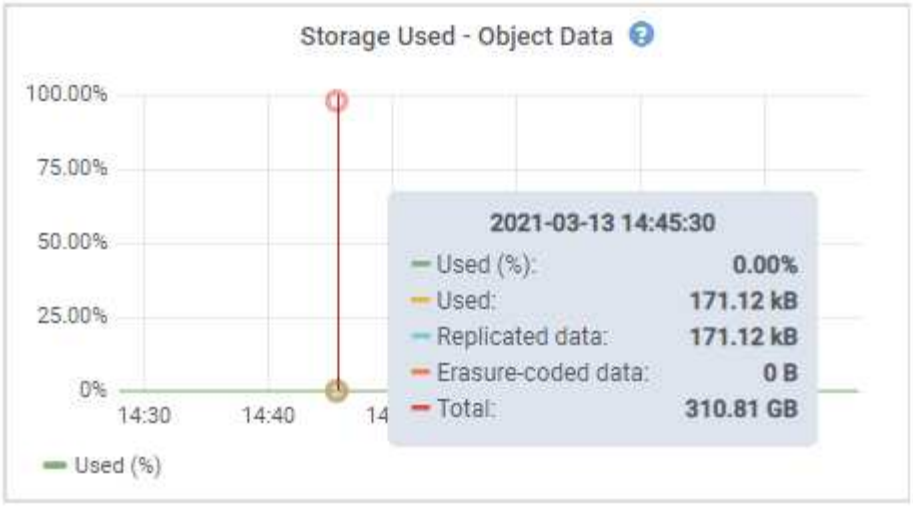
2. Erweitern Sie in der Tabelle der Warnungen bei Bedarf die Warnungsgruppe **Niedriger Objektdatenspeicher** und wählen Sie die Warnung aus, die Sie anzeigen möchten.

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

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

   Es werden folgende Werte angezeigt:

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



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

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

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

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

   Weitere Informationen finden Sie unter "Vollständige Speicherknoten verwalten" .

Fehlerbehebung bei Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens „Niedrig“

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

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

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

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

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

Verstehen Sie die Warnung

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

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

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

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

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

Beheben Sie die Warnung

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

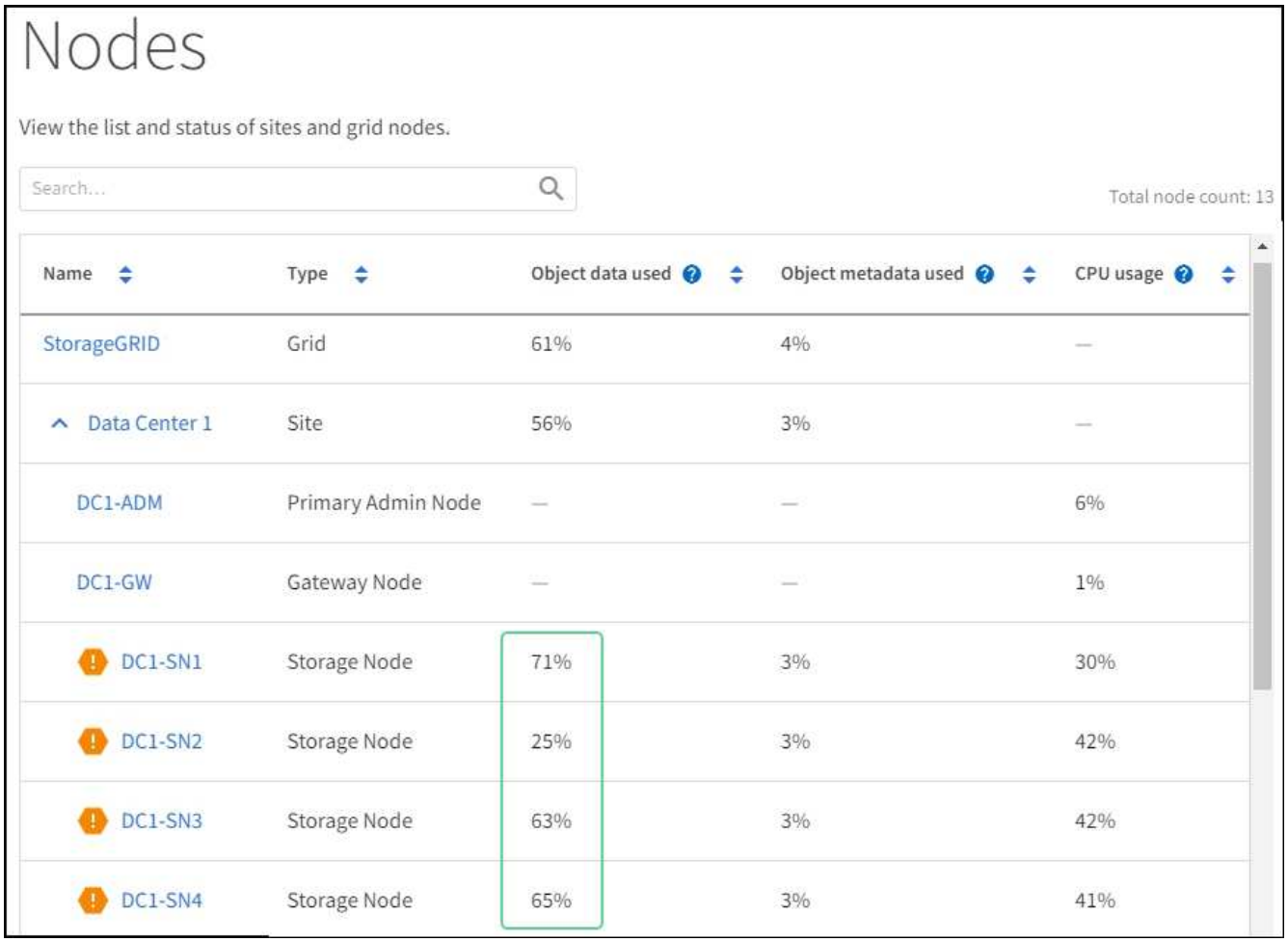
Sie können die Warnung **Niedriger schreibgeschützter Wasserzeichen-Override** beheben, indem Sie die benutzerdefinierten Wasserzeicheneinstellungen auf die neuen Wasserzeichen-Overrides aktualisieren. Wenn jedoch ein oder mehrere Speicherknoten fast voll sind oder Sie spezielle ILM-Anforderungen haben,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

sicher ist.

Bewerten Sie die Objektdatennutzung für das gesamte Raster

Schritte

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



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

Optimierte Speicherwasserzeichen anzeigen

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

Schritte

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

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

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

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

Schritte

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

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

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

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

Verwenden Sie optimierte Wasserzeichen

Schritte

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

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

Beheben von Metadatenproblemen

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

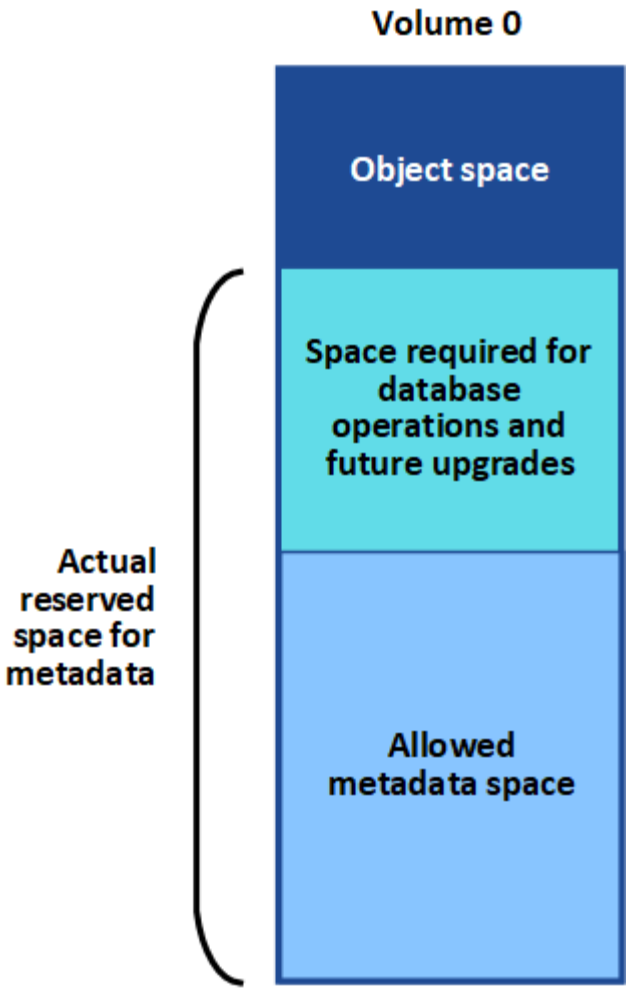
Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

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



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

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

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

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

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

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

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

Schritte

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

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

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

Beheben von Zertifikatsfehlern

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

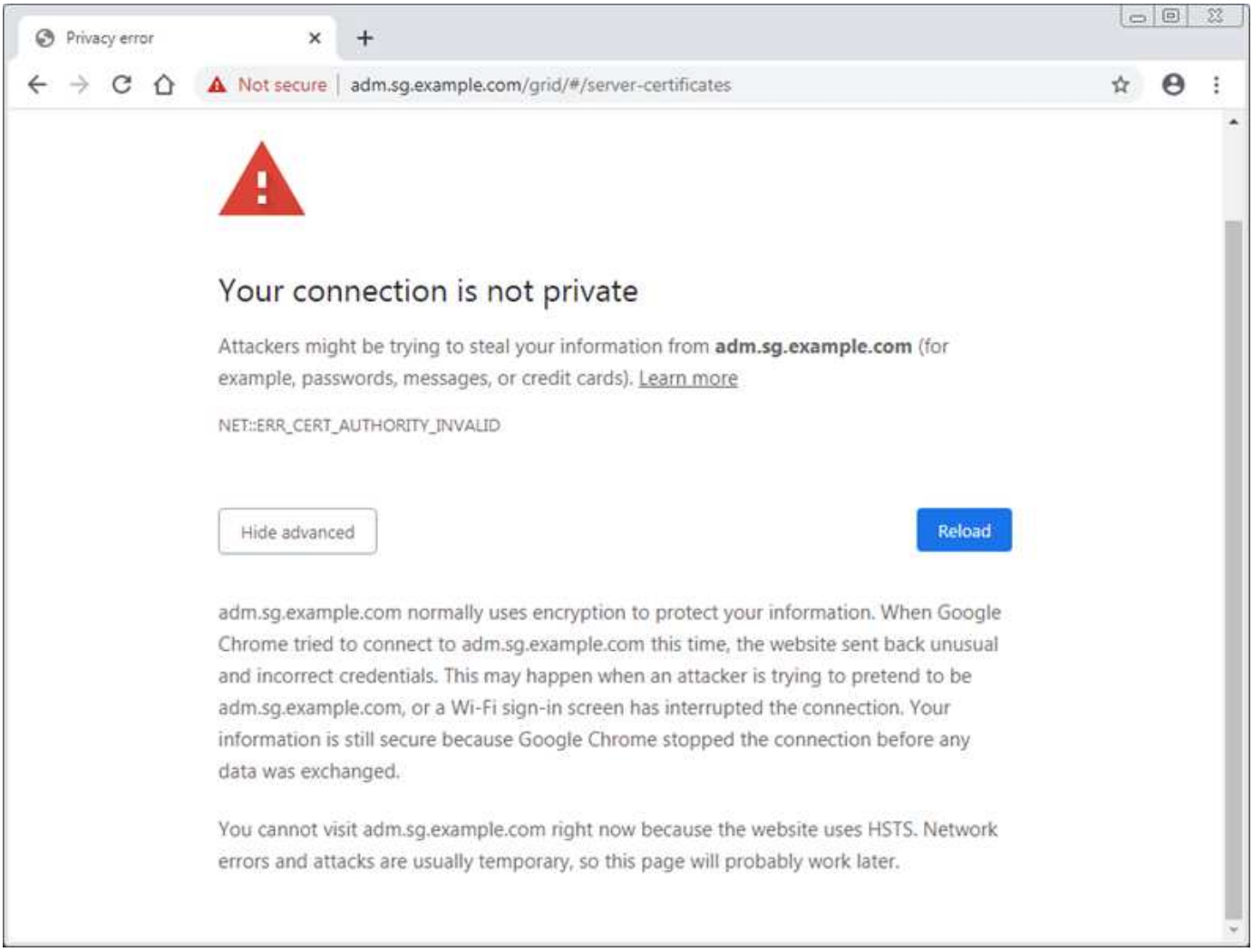
Informationen zu diesem Vorgang

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

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

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

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



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

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

Schritte

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

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

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

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

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

Beheben von Problemen mit dem Admin-Knoten und der Benutzeroberfläche

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

Anmeldefehler beim Admin-Knoten

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

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

Schritte

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

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

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

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

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

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

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

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

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .
7. Zeigen Sie den Status aller auf dem Grid-Knoten ausgeführten Dienste an: `storagegrid-status`

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

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

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

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

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

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

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

- `**/*commands.txt`

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

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

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

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

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

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

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

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

Probleme mit der Benutzeroberfläche

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

Schritte

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

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

Beheben von Netzwerk-, Hardware- und Plattformproblemen

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

Fehler „422: Nicht verarbeitbare Entität“

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

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

Fehlermeldung	Grundursache und Korrekturmaßnahmen

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

Fehlermeldung	Grundursache und Korrekturmaßnahmen

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

MTU-Nichtübereinstimmungswarnung im Netznetzwerk

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

Informationen zu diesem Vorgang

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

Schritte

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

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

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

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

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

+

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

Knotennetzwerk-Empfangsframe-Fehlerwarnung

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

Informationen zu diesem Vorgang

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

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

Schritte

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

FEC-Fehlanpassung

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

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

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

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

Switch-Port und NIC-MTU stimmen nicht überein

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

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

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

Siehe auch "MTU-Einstellung ändern" .

Hohe Link-Fehlerraten

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

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

NIC-Ringpufferüberlauf

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

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

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

Zeitsynchronisierungsfehler

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

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

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

Linux: Probleme mit der Netzwerkverbindung

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

Klonen von MAC-Adressen

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

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

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

Promiscuous-Modus

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

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

Linux: Knotenstatus ist „verwaist“

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

Informationen zu diesem Vorgang

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

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

Schritte

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

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

Wenn der Knoten verwaist ist, lautet die Antwort

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

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

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

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

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

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

Linux: Fehlerbehebung bei der IPv6-Unterstützung

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

Informationen zu diesem Vorgang

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

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

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

Schritte

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

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

Das Ergebnis sollte 0 sein.

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

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

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

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

Das Ergebnis sollte 1 sein.

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

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

5. Verlassen Sie den Container: `exit`

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

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

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

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

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

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

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

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

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

Fehlerbehebung bei einem externen Syslog-Server

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

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

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

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

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

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

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

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

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

Überprüfen der Überwachungsprotokolle

Prüfmeldungen und Protokolle

Diese Anweisungen enthalten Informationen zur Struktur und zum Inhalt von StorageGRID -Auditmeldungen und Auditprotokollen. Sie können diese Informationen verwenden, um den Prüfpfad der Systemaktivität zu lesen und zu analysieren.

Diese Anweisungen richten sich an Administratoren, die für die Erstellung von Berichten zur Systemaktivität und -nutzung verantwortlich sind, die eine Analyse der Prüfmeldungen des StorageGRID -Systems erfordern.

Um die Textprotokolldatei zu verwenden, müssen Sie Zugriff auf die konfigurierte Audit-Freigabe auf dem Admin-Knoten haben.

Informationen zum Konfigurieren von Überwachungsmeldungsebenen und zur Verwendung eines externen Syslog-Servers finden Sie unter"Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Nachrichtenfluss und -aufbewahrung prüfen

Alle StorageGRID -Dienste generieren während des normalen Systembetriebs Prüfmeldungen. Sie sollten verstehen, wie diese Prüfmeldungen durch das StorageGRID -System zum `audit.log` Datei.

Nachrichtenfluss prüfen

Audit-Nachrichten werden von Admin-Knoten und von den Speicherknoten verarbeitet, die über einen Administrative Domain Controller (ADC)-Dienst verfügen.

Wie im Flussdiagramm der Audit-Nachrichten dargestellt, sendet jeder StorageGRID Knoten seine Audit-Nachrichten an einen der ADC-Dienste am Rechenzentrumsstandort. Der ADC-Dienst wird für die ersten drei an jedem Standort installierten Speicherknoten automatisch aktiviert.

Jeder ADC-Dienst fungiert wiederum als Relay und sendet seine Sammlung von Audit-Nachrichten an jeden Admin-Knoten im StorageGRID -System, wodurch jeder Admin-Knoten eine vollständige Aufzeichnung der Systemaktivität erhält.

Jeder Admin-Knoten speichert Audit-Meldungen in Text-Logdateien; die aktive Logdatei trägt den Namen `audit.log`.

Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschvorgang, um sicherzustellen, dass keine Prüfmeldungen verloren gehen, bevor sie in das Prüfprotokoll geschrieben werden können.

Wenn ein Knoten eine Prüfnachricht generiert oder weiterleitet, wird die Nachricht in einer Prüfnachrichtenwarteschlange auf der Systemfestplatte des Grid-Knotens gespeichert. Eine Kopie der Nachricht wird immer in einer Audit-Nachrichtenwarteschlange aufbewahrt, bis die Nachricht in die Audit-Protokolldatei im Admin-Knoten geschrieben wird. `/var/local/log` Verzeichnis. Dadurch wird verhindert, dass während des Transports eine Prüfnachricht verloren geht.

Die Warteschlange der Prüfnachrichten kann aufgrund von Netzwerkverbindungsproblemen oder unzureichender Prüfkapazität vorübergehend größer werden. Wenn die Warteschlangen größer werden, verbrauchen sie mehr verfügbaren Speicherplatz in den einzelnen Knoten. `/var/local/` Verzeichnis. Wenn das Problem weiterhin besteht und das Prüfnachrichtenverzeichnis eines Knotens zu voll wird, priorisieren die einzelnen Knoten die Verarbeitung ihres Rückstands und sind vorübergehend für neue Nachrichten nicht verfügbar.

Insbesondere können die folgenden Verhaltensweisen auftreten:

- Wenn die `/var/local/log` Wenn das von einem Admin-Knoten verwendete Verzeichnis voll ist, wird der Admin-Knoten als für neue Prüfmeldungen nicht verfügbar gekennzeichnet, bis das Verzeichnis nicht mehr voll ist. S3-Client-Anfragen sind nicht betroffen. Der XAMS-Alarm (Unreachable Audit Repositories) wird ausgelöst, wenn ein Audit-Repository nicht erreichbar ist.
- Wenn die `/var/local/` Wenn das von einem Speicherknoten mit dem ADC-Dienst verwendete Verzeichnis zu 92 % gefüllt ist, wird der Knoten als für Prüfmeldungen nicht verfügbar gekennzeichnet, bis das Verzeichnis nur noch zu 87 % gefüllt ist. S3-Client-Anfragen an andere Knoten sind nicht betroffen. Der NRLY-Alarm (Available Audit Relays) wird ausgelöst, wenn Audit-Relays nicht erreichbar sind.

> ⓘ Wenn keine Storage Nodes mit dem ADC-Dienst verfügbar sind, speichern die Storage Nodes die Audit-Nachrichten lokal im `/var/local/log/localaudit.log` Datei.

- Wenn die `/var/local/` Das von einem Speicherknoten verwendete Verzeichnis ist zu 85 % gefüllt. Der Knoten lehnt S3-Client-Anfragen mit `503 Service Unavailable`.

Die folgenden Arten von Problemen können dazu führen, dass die Warteschlangen für

Überwachungsnachrichten sehr groß werden:

- Der Ausfall eines Admin-Knotens oder eines Speicherknotens mit dem ADC-Dienst. Wenn einer der Systemknoten ausfällt, kann es bei den übrigen Knoten zu einem Rückstau kommen.
- Eine anhaltende Aktivitätsrate, die die Prüfkapazität des Systems übersteigt.
- Der `/var/local/` Der Speicherplatz auf einem ADC-Speicherknoten wird aus Gründen voll, die nichts mit Prüfmeldungen zu tun haben. In diesem Fall akzeptiert der Knoten keine neuen Prüfnachrichten mehr und priorisiert seinen aktuellen Rückstand, was zu Rückständen auf anderen Knoten führen kann.

Alarm bei großer Audit-Warteschlange und Alarm bei in die Warteschlange gestellten Audit-Nachrichten (AMQS)

Damit Sie die Größe der Warteschlangen für Prüfnachrichten im Laufe der Zeit überwachen können, werden die Warnung „Große Prüfwarteschlange“ und der alte AMQS-Alarm ausgelöst, wenn die Anzahl der Nachrichten in einer Speicherknotenwarteschlange oder einer Admin-Knotenwarteschlange bestimmte Schwellenwerte erreicht.

Wenn die Warnung **Große Prüfwarteschlange** oder der alte AMQS-Alarm ausgelöst wird, überprüfen Sie zunächst die Systemlast. Wenn in letzter Zeit eine erhebliche Anzahl von Transaktionen stattgefunden hat, sollten sich die Warnung und der Alarm mit der Zeit auflösen und können ignoriert werden.

Wenn die Warnung oder der Alarm weiterhin besteht und an Schwere zunimmt, sehen Sie sich ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage hinweg stetig ansteigt, hat die Prüflast wahrscheinlich die Prüfkapazität des Systems überschritten. Reduzieren Sie die Client-Betriebsrate oder verringern Sie die Anzahl der protokollierten Prüfmeldungen, indem Sie die Prüfstufe für Client-Schreibvorgänge und Client-Lesevorgänge auf „Fehler“ oder „Aus“ ändern. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Doppelte Nachrichten

Das StorageGRID -System verfolgt einen konservativen Ansatz, wenn ein Netzwerk- oder Knotenausfall auftritt. Aus diesem Grund können im Überwachungsprotokoll doppelte Nachrichten vorhanden sein.

Zugriff auf die Überwachungsprotokolldatei

Der Audit-Share enthält die aktiven `audit.log` Datei und alle komprimierten Prüfprotokolldateien. Sie können direkt über die Befehlszeile des Admin-Knotens auf die Audit-Protokolldateien zugreifen.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

2. Wechseln Sie zum Verzeichnis mit den Audit-Protokolldateien:

```
cd /var/local/log
```

3. Zeigen Sie bei Bedarf die aktuelle oder eine gespeicherte Überwachungsprotokolldatei an.

Rotation der Überwachungsprotokolldateien

Audit-Protokolldateien werden auf einem Admin-Knoten gespeichert `/var/local/log` Verzeichnis. Die aktiven Audit-Protokolldateien heißen `audit.log` .

> Optional können Sie das Ziel der Überwachungsprotokolle ändern und Überwachungsinformationen an einen externen Syslog-Server senden. Wenn ein externer Syslog-Server konfiguriert ist, werden weiterhin lokale Protokolle von Prüfdatensätzen generiert und gespeichert. Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Einmal täglich wird der aktive `audit.log` Datei wird gespeichert und eine neue `audit.log` Datei wird gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format *`yyyy-mm-dd.txt`* . Wenn an einem Tag mehr als ein Prüfprotokoll erstellt wird, verwenden die Dateinamen das Datum, an dem die Datei gespeichert wurde, gefolgt von einer Zahl im Format *`yyyy-mm-dd.txt.n`* . Zum Beispiel, `2018-04-15.txt` Und `2018-04-15.txt.1` sind die erste und zweite Protokolldatei, die am 15. April 2018 erstellt und gespeichert wurden.

Nach einem Tag wird die gespeicherte Datei komprimiert und umbenannt, im Format *`yyyy-mm-dd.txt.gz`* , wodurch das ursprüngliche Datum erhalten bleibt. Im Laufe der Zeit führt dies dazu, dass der für Prüfprotokolle auf dem Admin-Knoten zugewiesene Speicherplatz verbraucht wird. Ein Skript überwacht den Speicherplatzverbrauch des Audit-Protokolls und löscht Protokolldateien nach Bedarf, um Speicherplatz im `/var/local/log` Verzeichnis. Prüfprotokolle werden basierend auf dem Datum ihrer Erstellung gelöscht, wobei die ältesten zuerst gelöscht werden. Sie können die Aktionen des Skripts in der folgenden Datei überwachen: `/var/local/log/manage-audit.log` .

Dieses Beispiel zeigt die aktive `audit.log` Datei, die Datei vom Vortag(`2018-04-15.txt`) und die komprimierte Datei für den Vortag(`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Audit-Protokolldateiformat

Audit-Protokolldateiformat

Die Audit-Protokolldateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Meldungen.

Jede Prüfnachricht enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Prüfnachricht ausgelöst hat (ATIM) im ISO 8601-Format, gefolgt von einem Leerzeichen:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, Wo *UUUUUU* sind Mikrosekunden.

- Die Prüfnachricht selbst, eingeschlossen in eckige Klammern und beginnend mit `AUDT` .

Das folgende Beispiel zeigt drei Audit-Meldungen in einer Audit-Protokolldatei (Zeilenumbrüche zur besseren Lesbarkeit hinzugefügt). Diese Nachrichten wurden generiert, als ein Mandant einen S3-Bucket erstellte und diesem Bucket zwei Objekte hinzufügte.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

In ihrem Standardformat sind die Prüfmeldungen in den Prüfprotokolldateien nicht einfach zu lesen oder zu interpretieren. Sie können die"Audit-Erklärtool" um vereinfachte Zusammenfassungen der Audit-Meldungen im Audit-Protokoll zu erhalten. Sie können die"Auditsummen-Tool" um zusammenzufassen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge dauerten.

Verwenden Sie das Audit-Explain-Tool

Sie können die `audit-explain` Tool zum Übersetzen der Audit-Meldungen im Audit-Protokoll in ein leicht lesbares Format.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Informationen zu diesem Vorgang

Der `audit-explain` Das auf dem primären Admin-Knoten verfügbare Tool bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Audit-Protokoll.

> Der `audit-explain` Das Tool ist in erster Linie für die Verwendung durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitung `audit-explain` Abfragen können eine große Menge an CPU-Leistung verbrauchen, was sich auf den Betrieb von StorageGRID auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-explain` Werkzeug. Diese vier"SPUT" Es wurden Prüfmeldungen generiert, als der S3-Mandant mit der Konto-ID 92484777680322627870 S3-PUT-Anfragen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und diesem Bucket drei Objekte hinzuzufügen.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Der `audit-explain` Das Tool kann Folgendes:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Verarbeiten Sie mehrere Dateien gleichzeitig. Beispiel:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Akzeptieren Sie Eingaben von einer Pipe, die es Ihnen ermöglicht, die Eingabe mithilfe der `grep` Befehl oder andere Mittel. Beispiel:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Da Audit-Protokolle sehr groß und langsam zu analysieren sein können, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen möchten, und ausführen `audit-explain` auf die Teile, statt auf die gesamte Datei.

> Der `audit-explain` Das Tool akzeptiert keine komprimierten Dateien als Pipe-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie deren Dateinamen als Befehlszeilenargumente an oder verwenden Sie die `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-explain -h
```

Schritte

1. Melden Sie sich beim primären Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .
2. Geben Sie den folgenden Befehl ein, wobei `/var/local/log/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   Der `audit-explain` Das Tool druckt für Menschen lesbare Interpretationen aller Nachrichten in der bzw. den angegebenen Dateien.

   > Um die Zeilenlänge zu reduzieren und die Lesbarkeit zu verbessern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel sehen möchten, verwenden Sie den Zeitstempel(`-t`) Option.

Verwenden Sie das Audit-Sum-Tool

Sie können die `audit-sum` Tool zum Zählen der Prüfnachrichten zum Schreiben, Lesen, Kopfzeilen und Löschen und zum Anzeigen der minimalen, maximalen und durchschnittlichen Zeit (oder Größe) für jeden Vorgangstyp.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie müssen über die `Passwords.txt` Datei.
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Informationen zu diesem Vorgang

Der `audit-sum` Das auf dem primären Admin-Knoten verfügbare Tool fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

> Der `audit-sum` Das Tool ist in erster Linie für die Verwendung durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitung `audit-sum` Abfragen können eine große Menge an CPU-Leistung verbrauchen, was sich auf den Betrieb von StorageGRID auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerten.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Der `audit-sum` Das Tool stellt Anzahl und Zeit für die folgenden S3-, Swift- und ILM-Auditmeldungen in einem Audit-Protokoll bereit.

> Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, wenn Funktionen veraltet sind. Wenn Sie auf einen Prüfcode stoßen, der hier nicht aufgeführt ist, überprüfen Sie die vorherigen Versionen dieses Themas auf ältere SG-Versionen. Beispiel: "StorageGRID 11.8 Dokumentation zum Verwenden des Auditsummentools" .

Code	Beschreibung	Siehe
IDEL	Von ILM initiiertes Löschen: Protokolliert, wenn ILM den Löschvorgang eines Objekts startet.	"IDEL: Von ILM initiiertes Löschen"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3 LÖSCHEN"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	"SHEA: S3 KOPF"

Code	Beschreibung	Siehe
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	"WDEL: Schnelles LÖSCHEN"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Container.	"WGET: Schnelles GET"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Containers zu überprüfen.	"WHEA: Schneller Kopf"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Containers.	"WPUT: Schnelles PUT"

Der `audit-sum` Das Tool kann Folgendes:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Verarbeiten Sie mehrere Dateien gleichzeitig. Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Akzeptieren Sie Eingaben von einer Pipe, die es Ihnen ermöglicht, die Eingabe mithilfe der `grep` Befehl oder andere Mittel. Beispiel:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Dieses Tool akzeptiert keine komprimierten Dateien als Pipe-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie deren Dateinamen als Befehlszeilenargumente an oder verwenden Sie die `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Sie können Befehlszeilenoptionen verwenden, um Vorgänge für Buckets getrennt von Vorgängen für Objekte

zusammenzufassen oder um Meldungszusammenfassungen nach Bucket-Name, Zeitraum oder Zieltyp zu gruppieren. Standardmäßig zeigen die Zusammenfassungen die minimale, maximale und durchschnittliche Betriebszeit an, Sie können jedoch die `size (-s)` Option, stattdessen die Objektgröße zu betrachten.

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-sum -h
```

Schritte

1. Melden Sie sich beim primären Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

2. Wenn Sie alle Nachrichten im Zusammenhang mit Schreib-, Lese-, Head- und Löschvorgängen analysieren möchten, führen Sie die folgenden Schritte aus:
   a. Geben Sie den folgenden Befehl ein, wobei `/var/local/log/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerten.

      ```
        message group           count     min(sec)        max(sec)
      average(sec)
        =============           =====     ========        ========
      ============
        IDEL                      274
        SDEL                   213371        0.004          20.934
      0.352
        SGET                   201906        0.010        1740.290
      1.132
        SHEA                    22716        0.005           2.349
      0.272
        SPUT                 1771398        0.011        1770.563
      0.487
      ```

      In diesem Beispiel sind SGET-Operationen (S3 GET) mit durchschnittlich 1,13 Sekunden am langsamsten, aber SGET- und SPUT-Operationen (S3 PUT) weisen beide lange Worst-Case-Zeiten von etwa 1.770 Sekunden auf.

   b. Um die 10 langsamsten Abrufvorgänge anzuzeigen, verwenden Sie den Befehl grep, um nur SGET-Nachrichten auszuwählen und die Option für die lange Ausgabe hinzuzufügen(`-l`), um Objektpfade

einzuschließen:

```
grep SGET audit.log | audit-sum -l
```

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, sodass Sie das Prüfprotokoll nach anderen Nachrichten durchsuchen können, die sich auf diese bestimmten Objekte beziehen.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
Anhand dieser Beispielausgabe können Sie erkennen, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von etwa 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe ist für die langsamen Abrufzeiten im schlimmsten Fall verantwortlich.

3. Wenn Sie bestimmen möchten, welche Objektgrößen in Ihr Raster aufgenommen und daraus abgerufen werden, verwenden Sie die Größenoption(`-s`):

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

In diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2,5 MB, die durchschnittliche Größe für SGET ist jedoch viel größer. Die Anzahl der SPUT-Nachrichten ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hindeutet, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufe gestern langsam waren:

   a. Führen Sie den Befehl für das entsprechende Überwachungsprotokoll aus und verwenden Sie die Option „Nach Zeit gruppieren“.(`-gt`), gefolgt vom Zeitraum (z. B. 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Diese Ergebnisse zeigen, dass der S3 GET-Verkehr zwischen 06:00 und 07:00 Uhr seinen Höhepunkt erreichte. Auch die Höchst- und Durchschnittszeiten sind zu diesen Zeiten erheblich höher und steigen nicht allmählich an, wenn die Anzahl steigt. Dies deutet darauf hin, dass irgendwo die Kapazität überschritten wurde, vielleicht im Netzwerk oder bei der Fähigkeit des Grids, Anfragen zu verarbeiten.

b. Um zu ermitteln, welche Objektgröße gestern stündlich abgerufen wurde, fügen Sie die Option „Größe“ hinzu(`-s`) zum Befehl:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Diese Ergebnisse deuten darauf hin, dass einige sehr große Abrufe stattfanden, als der gesamte Abrufverkehr seinen Höhepunkt erreichte.

c. Um weitere Details anzuzeigen, verwenden Sie die"Audit-Erklärtool" um alle SGET-Operationen während dieser Stunde zu überprüfen:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Wenn die Ausgabe des grep-Befehls voraussichtlich viele Zeilen umfasst, fügen Sie die `less` Befehl, um den Inhalt der Prüfprotokolldatei seitenweise (bildschirmweise) anzuzeigen.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen für Buckets langsamer sind als SPUT-Operationen für Objekte:

a. Beginnen Sie mit der `-go` Option, die Nachrichten für Objekt- und Bucket-Operationen separat gruppiert:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets andere Leistungsmerkmale aufweisen als SPUT-Operationen für Objekte.

b. Um zu ermitteln, welche Buckets die langsamsten SPUT-Operationen haben, verwenden Sie die `-gb` Option, die Nachrichten nach Bucket gruppiert:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Um zu bestimmen, welche Buckets die größte SPUT-Objektgröße haben, verwenden Sie sowohl die `-gb` und die `-s` Optionen:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Format der Prüfnachricht

Format der Prüfnachricht

Die innerhalb des StorageGRID -Systems ausgetauschten Prüfnachrichten enthalten für alle Nachrichten gemeinsame Standardinformationen und spezifische Inhalte, die das gemeldete Ereignis oder die gemeldete Aktivität beschreiben.

Wenn die zusammenfassenden Informationen der"Audit-Erklärung" Und"Auditsumme" Wenn die Tools nicht ausreichen, lesen Sie diesen Abschnitt, um das allgemeine Format aller Prüfmeldungen zu verstehen.

Nachfolgend sehen Sie ein Beispiel für eine Audit-Meldung, wie sie in der Audit-Protokolldatei erscheinen könnte:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Jede Prüfnachricht enthält eine Zeichenfolge von Attributelementen. Die gesamte Zeichenfolge ist in Klammern eingeschlossen(`[ ]`), und jedes Attributelement in der Zeichenfolge weist die folgenden Eigenschaften auf:

- In Klammern eingeschlossen `[ ]`
- Eingeführt durch die Zeichenfolge `AUDT` , was auf eine Prüfmeldung hinweist
- Ohne Trennzeichen (keine Kommas oder Leerzeichen) davor oder danach
- Beendet durch ein Zeilenvorschubzeichen `\n`

Jedes Element enthält einen Attributcode, einen Datentyp und einen Wert, die in diesem Format gemeldet werden:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Die Anzahl der Attributelemente in der Nachricht hängt vom Ereignistyp der Nachricht ab. Die Attributelemente sind in keiner bestimmten Reihenfolge aufgelistet.

Die folgende Liste beschreibt die Attributelemente:

- `ATTR`ist ein vierstelliger Code für das gemeldete Attribut. Es gibt einige Attribute, die allen Prüfmeldungen gemeinsam sind, und andere, die ereignisspezifisch sind.
- `type`ist eine vierstellige Kennung des Programmierdatentyps des Werts, z. B. UI64, FC32 usw. Der Typ ist in Klammern eingeschlossen `( ).
- `value`ist der Inhalt des Attributs, normalerweise ein numerischer oder Textwert. Auf Werte folgt immer ein Doppelpunkt(:`). Werte des Datentyps CSTR sind in doppelte Anführungszeichen " " eingeschlossen.

Datentypen

Zum Speichern von Informationen in Prüfmeldungen werden unterschiedliche Datentypen verwendet.

Typ	Beschreibung
UI32	Vorzeichenloser Long Integer (32 Bit); kann die Zahlen 0 bis 4.294.967.295 speichern.
UI64	Vorzeichenloser Double Long Integer (64 Bit); kann die Zahlen 0 bis 18.446.744.073.709.551.615 speichern.
FC32	Vierstellige Konstante; ein 32-Bit-Ganzzahlwert ohne Vorzeichen, der als vier ASCII-Zeichen dargestellt wird, z. B. „ABCD“.
IPAD	Wird für IP-Adressen verwendet.
CSTR	Ein Array mit variabler Länge aus UTF-8-Zeichen. Zeichen können mit den folgenden Konventionen maskiert werden: • Der Backslash ist \\. • Der Wagenrücklauf ist \r. • Doppelte Anführungszeichen sind \". • Zeilenvorschub (neue Zeile) ist \n. • Zeichen können durch ihre hexadezimalen Entsprechungen ersetzt werden (im Format \xHH, wobei HH der Hexadezimalwert ist, der das Zeichen darstellt).

Ereignisspezifische Daten

Jede Prüfmeldung im Prüfprotokoll zeichnet Daten auf, die für ein Systemereignis

spezifisch sind.

Im Anschluss an die Eröffnung `[AUDT:` Container, der die Nachricht selbst identifiziert, der nächste Satz von Attributen liefert Informationen über das Ereignis oder die Aktion, die in der Prüfnachricht beschrieben wird. Diese Attribute werden im folgenden Beispiel hervorgehoben:

2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]* **\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\] \[SACC\(CSTR\):"Konto"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\] \[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"Konto"\]\[S3BK\(CSTR\):"Bucket"\] \[S3KY\(CSTR\):"Objekt"\]\[CBID\(UI64\):0xCC128B9B9E428347\] \[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\]**[AVER(UI32):10] \[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ] \[ATID(UI64):15552417629170647261]]

Der `ATYP` Das Element (im Beispiel unterstrichen) identifiziert, welches Ereignis die Nachricht generiert hat. Diese Beispielnachricht enthält die"SHEA" Nachrichtencode ([ATYP(FC32):SHEA]), der angibt, dass er durch eine erfolgreiche S3-HEAD-Anforderung generiert wurde.

Gemeinsame Elemente in Prüfmeldungen

Alle Prüfmeldungen enthalten die gemeinsamen Elemente.

Code	Typ	Beschreibung
INMITTEN	FC32	Modul-ID: Eine vierstellige Kennung der Modul-ID, die die Nachricht generiert hat. Dies gibt das Codesegment an, innerhalb dessen die Prüfnachricht generiert wurde.
ANID	UI32	Knoten-ID: Die dem Dienst zugewiesene Grid-Knoten-ID, der die Nachricht generiert hat. Jedem Dienst wird bei der Konfiguration und Installation des StorageGRID -Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.
ASES	UI64	Audit-Sitzungskennung: In früheren Versionen gab dieses Element den Zeitpunkt an, zu dem das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit der Betriebssystem-Epoche (00:00:00 UTC am 1. Januar 1970) gemessen. **Hinweis:** Dieses Element ist veraltet und erscheint nicht mehr in Prüfmeldungen.
ASQN	UI64	Sequenzzähler: In früheren Versionen wurde dieser Zähler für jede generierte Prüfnachricht auf dem Grid-Knoten (ANID) erhöht und beim Neustart des Dienstes auf Null zurückgesetzt. **Hinweis:** Dieses Element ist veraltet und erscheint nicht mehr in Prüfmeldungen.

Code	Typ	Beschreibung
ATID	UI64	Trace-ID: Eine Kennung, die von allen Nachrichten gemeinsam genutzt wird, die durch ein einzelnes Ereignis ausgelöst wurden.
ATIM	UI64	Zeitstempel: Der Zeitpunkt, zu dem das Ereignis generiert wurde, das die Prüfnachricht ausgelöst hat, gemessen in Mikrosekunden seit der Betriebssystem-Epoche (00:00:00 UTC am 1. Januar 1970). Beachten Sie, dass die meisten verfügbaren Tools zum Konvertieren des Zeitstempels in lokales Datum und Uhrzeit auf Millisekunden basieren. Möglicherweise ist eine Rundung oder Kürzung des protokollierten Zeitstempels erforderlich. Die menschenlesbare Zeit, die am Anfang der Audit-Meldung im `audit.log` Datei ist das ATIM-Attribut im ISO 8601-Format. Datum und Uhrzeit werden dargestellt als *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , wobei die `T` ist ein Zeichenfolgenzeichen, das den Beginn des Zeitsegments des Datums angibt. *`UUUUUU`* sind Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine vierstellige Kennung des protokollierten Ereignisses. Dies bestimmt den „Nutzlast“-Inhalt der Nachricht: die enthaltenen Attribute.
BEHAUPTEN	UI32	Version: Die Version der Prüfnachricht. Im Zuge der Weiterentwicklung der StorageGRID -Software können neue Versionen von Diensten neue Funktionen für die Prüfberichterstattung enthalten. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst, um Nachrichten aus älteren Dienstversionen zu verarbeiten.
RSLT	FC32	Ergebnis: Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Wenn es für eine Nachricht nicht relevant ist, wird NONE statt SUCS verwendet, damit die Nachricht nicht versehentlich gefiltert wird.

Beispiele für Prüfnachrichten

Detaillierte Informationen finden Sie in jeder Prüfmeldung. Alle Prüfmeldungen verwenden dasselbe Format.

Nachfolgend sehen Sie ein Beispiel für eine Prüfmeldung, wie sie in der `audit.log` Datei:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Die Prüfnachricht enthält Informationen zum aufgezeichneten Ereignis sowie Informationen zur Prüfnachricht selbst.

Um zu ermitteln, welches Ereignis von der Prüfnachricht aufgezeichnet wird, suchen Sie nach dem ATYP-Attribut (unten hervorgehoben):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Der Wert des ATYP-Attributs ist SPUT. "SPUT" stellt eine S3 PUT-Transaktion dar, die die Aufnahme eines Objekts in einen Bucket protokolliert.

Die folgende Prüfmeldung zeigt auch den Bucket an, mit dem das Objekt verknüpft ist:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Um herauszufinden, wann das PUT-Ereignis aufgetreten ist, notieren Sie sich den Zeitstempel „Universal Coordinated Time“ (UTC) am Anfang der Prüfnachricht. Dieser Wert ist eine für Menschen lesbare Version des ATIM-Attributs der Prüfnachricht selbst:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM zeichnet die Zeit in Mikrosekunden seit Beginn der UNIX-Epoche auf. Im Beispiel ist der Wert `1405631878959669` entspricht Donnerstag, 17. Juli 2014, 21:17:59 UTC.

Prüfmeldungen und der Objektlebenszyklus

Wann werden Prüfmeldungen generiert?

Jedes Mal, wenn ein Objekt aufgenommen, abgerufen oder gelöscht wird, werden Prüfmeldungen generiert. Sie können diese Transaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

Die Verknüpfung der Prüfmeldungen erfolgt über protokollspezifische Kennungen.

Protokoll	Code
Verknüpfen von S3-Operationen	S3BK (Bucket), S3KY (Schlüssel) oder beides
Verknüpfen von Swift-Operationen	WCON (Container), WOBJ (Objekt) oder beides
Verknüpfung interner Vorgänge	CBID (interne Kennung des Objekts)

Zeitpunkt der Prüfmeldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Knoten, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der von den verschiedenen Diensten generierten Prüfmeldungen von der in den Beispielen in diesem Abschnitt gezeigten abweichen.

Objektaufnahmetransaktionen

Sie können Client-Ingest-Transaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

In den folgenden Tabellen sind nicht alle während einer Aufnahmetransaktion generierten Prüfmeldungen aufgeführt. Es sind nur die Nachrichten enthalten, die zum Verfolgen der Aufnahmetransaktion erforderlich sind.

S3-Ingest-Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3 PUT-Ingest-Transaktion wurde erfolgreich abgeschlossen.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Objektregeln erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Swift erfasst Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
WPUT	Schnelle PUT-Transaktion	Eine Swift PUT-Ingest-Transaktion wurde erfolgreich abgeschlossen.	CBID, WCON, WOBJ	"WPUT: Schnelles PUT"
ORLM	Objektregeln erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Beispiel: S3-Objektaufnahme

Die folgende Reihe von Prüfmeldungen ist ein Beispiel für die Prüfmeldungen, die generiert und im Prüfprotokoll gespeichert werden, wenn ein S3-Client ein Objekt in einen Speicherknoten (LDR-Dienst) einspeist.

In diesem Beispiel enthält die aktive ILM-Richtlinie die ILM-Regel „2 Kopien erstellen“.

> Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Prüfmeldungen aufgeführt. Es werden nur diejenigen aufgelistet, die sich auf die S3-Ingest-Transaktion (SPUT) beziehen.

In diesem Beispiel wird davon ausgegangen, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Nachricht wird generiert, um anzuzeigen, dass eine S3 PUT-Transaktion ausgegeben wurde, um ein Objekt in einem bestimmten Bucket zu erstellen.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Objektregeln erfüllt

Die ORLM-Nachricht gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Nachricht enthält die CBID des Objekts und den Namen der angewendeten ILM-Regel.

Bei replizierten Objekten enthält das LOCS-Feld die LDR-Knoten-ID und die Volume-ID der Objektstandorte.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Bei Erasure-Coding-Objekten enthält das LOCS-Feld die Erasure-Coding-Profil-ID und die Erasure-Coding-Gruppen-ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Das PATH-Feld enthält S3-Bucket- und Schlüsselinformationen oder Swift-Container- und Objektinformationen, je nachdem, welche API verwendet wurde.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Objektlöschtransaktionen

Sie können Objektlöschtransaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

In den folgenden Tabellen sind nicht alle während einer Löschtransaktion generierten Prüfmeldungen

aufgeführt. Es sind nur Nachrichten enthalten, die zum Verfolgen der Löschtransaktion erforderlich sind.

S3-Lösch-Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Es wurde eine Anforderung zum Löschen des Objekts aus einem Bucket gestellt.	CBID, S3KY	"SDEL: S3 LÖSCHEN"

Schnelles Löschen von Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
WDEL	Schnelles Löschen	Es wurde eine Anforderung zum Löschen des Objekts aus einem Container oder dem Container gestellt.	CBID, WOBJ	"WDEL: Schnelles LÖSCHEN"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt von einem Speicherknoten (LDR-Dienst) löscht, wird eine Prüfnachricht generiert und im Prüfprotokoll gespeichert.

> Im folgenden Beispiel sind nicht alle während einer Löschtransaktion generierten Prüfmeldungen aufgeführt. Es werden nur diejenigen aufgelistet, die sich auf die S3-Löschtransaktion (SDEL) beziehen.

SDEL: S3 Löschen

Das Löschen von Objekten beginnt, wenn der Client eine DeleteObject-Anforderung an einen LDR-Dienst sendet. Die Nachricht enthält den Bucket, aus dem das Objekt gelöscht werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Objektabruftransaktionen

Sie können Objektabruftransaktionen im Prüfprotokoll identifizieren, indem Sie S3-API-spezifische Prüfmeldungen suchen.

In den folgenden Tabellen sind nicht alle Prüfmeldungen aufgeführt, die während einer Abruftransaktion generiert werden. Es sind nur Nachrichten enthalten, die zum Verfolgen der Abruftransaktion erforderlich sind.

S3-Abruf-Audit-Nachrichten

Code	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 GET	Anforderung zum Abrufen eines Objekts aus einem Bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Audit-Nachrichten zum schnellen Abrufen

Code	Name	Beschreibung	Verfolgen	Siehe
WGET	Schnelles GET	Anforderung zum Abrufen eines Objekts aus einem Container.	CBID, WCON, WOBJ	"WGET: Schnelles GET"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Speicherknoten (LDR-Dienst) abruft, wird eine Prüfnachricht generiert und im Prüfprotokoll gespeichert.

Beachten Sie, dass im folgenden Beispiel nicht alle während einer Transaktion generierten Prüfmeldungen aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET: S3 GET

Der Objektabruf beginnt, wenn der Client eine GetObject-Anforderung an einen LDR-Dienst sendet. Die Nachricht enthält den Bucket, aus dem das Objekt abgerufen werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Wenn die Bucket-Richtlinie dies zulässt, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört. Die Prüfnachricht enthält Informationen zum Mandantenkonto des Bucket-Eigentümers, sodass Sie diese anonymen und kontoübergreifenden Anfragen verfolgen können.

In der folgenden Beispielnachricht sendet der Client eine GetObject-Anforderung für ein Objekt, das in einem Bucket gespeichert ist, das ihm nicht gehört. Die Werte für SBAI und SBAC zeichnen die Mandantenkonto-ID

und den Namen des Bucket-Eigentümers auf, die sich von der Mandantenkonto-ID und dem Namen des in S3AI und SACC aufgezeichneten Kunden unterscheiden.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Beispiel: S3 Select auf einem Objekt

Wenn ein S3-Client eine S3 Select-Abfrage für ein Objekt ausgibt, werden Prüfmeldungen generiert und im Prüfprotokoll gespeichert.

Beachten Sie, dass im folgenden Beispiel nicht alle während einer Transaktion generierten Prüfmeldungen aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3 Select-Transaktion (SelectObjectContent) beziehen.

Jede Abfrage führt zu zwei Prüfmeldungen: eine, die die Autorisierung der S3 Select-Anfrage durchführt (das S3SR-Feld ist auf „select“ gesetzt) und eine nachfolgende Standard-GET-Operation, die die Daten während der Verarbeitung aus dem Speicher abruft.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Metadaten-Update-Nachrichten

Audit-Nachrichten werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zur S3-Metadatenaktualisierung

Code	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3-Metadaten aktualisiert"

Beispiel: S3-Metadaten-Update

Das Beispiel zeigt eine erfolgreiche Transaktion zum Aktualisieren der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadaten-Update

Der S3-Client stellt eine Anfrage (SUPD), um die angegebenen Metadaten zu aktualisieren(`x-amz-meta-\*`) für das S3-Objekt (S3KY). In diesem Beispiel sind Anforderungsheader im Feld HTRH enthalten, da es als Audit-Protokollheader konfiguriert wurde (**KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**). Sehen "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Prüfmeldungen

Beschreibungen der Prüfnachrichten

Detaillierte Beschreibungen der vom System zurückgegebenen Prüfmeldungen finden Sie in den folgenden Abschnitten. Jede Prüfnachricht wird zunächst in einer Tabelle aufgelistet, in der verwandte Nachrichten nach der Aktivitätsklasse gruppiert werden, die die Nachricht darstellt. Diese Gruppierungen sind sowohl für das Verständnis der überwachten Aktivitätstypen als auch für die Auswahl des gewünschten Typs der Überwachungsnachrichtenfilterung nützlich.

Die Prüfmeldungen werden außerdem alphabetisch nach ihren vierstelligen Codes aufgelistet. Diese alphabetische Liste ermöglicht es Ihnen, Informationen zu bestimmten Nachrichten zu finden.

Die in diesem Kapitel verwendeten vierstelligen Codes sind die ATYP-Werte, die in den Prüfmeldungen zu finden sind, wie in der folgenden Beispielmeldung gezeigt:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Informationen zum Festlegen von Audit-Meldungsebenen, zum Ändern von Protokollzielen und zur Verwendung eines externen Syslog-Servers für Ihre Audit-Informationen finden Sie unter"Konfigurieren von

Überwachungsmeldungen und Protokollzielen"

Kategorien von Überwachungsnachrichten

System-Audit-Meldungen

Die Audit-Meldungen der Kategorie „Systemaudit“ werden für Ereignisse verwendet, die sich auf das Audit-System selbst, den Zustand von Grid-Knoten, die systemweite Aufgabenaktivität (Grid-Tasks) und Dienstsicherungsvorgänge beziehen.

Code	Nachrichtentitel und -beschreibung	Siehe
ECMC	Fehlendes Erasure-Coded-Datenfragment: Zeigt an, dass ein fehlendes Erasure-Coded-Datenfragment erkannt wurde.	"ECMC: Fehlendes Erasure-Coded-Datenfragment"
Kulturhauptstadt Europas	Beschädigtes Erasure-Coded-Datenfragment: Zeigt an, dass ein beschädigtes Erasure-Coded-Datenfragment erkannt wurde.	"ECOC: Beschädigtes Erasure-Coded-Datenfragment"
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Ein Verbindungsversuch mit Transport Layer Security (TLS) ist fehlgeschlagen.	"ETAF: Sicherheitsauthentifizierung fehlgeschlagen"
GNRG	GNDS-Registrierung: Ein Dienst hat Informationen über sich selbst im StorageGRID System aktualisiert oder registriert.	"GNRG: GNDS-Registrierung"
GNUR	GNDS-Abmeldung: Ein Dienst hat sich selbst vom StorageGRID System abgemeldet.	"GNUR: GNDS-Abmeldung"
GTED	Grid-Aufgabe beendet: Der CMN-Dienst hat die Verarbeitung der Grid-Aufgabe abgeschlossen.	"GTED: Grid-Aufgabe beendet"
GTST	Grid-Aufgabe gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid-Aufgabe begonnen.	"GTST: Grid-Aufgabe gestartet"
GTSU	Grid-Aufgabe übermittelt: Eine Grid-Aufgabe wurde an den CMN-Dienst übermittelt.	"GTSU: Grid-Aufgabe übermittelt"
LLST	Standort verloren: Diese Prüfmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"
OLST	Objekt verloren: Ein angefordertes Objekt kann im StorageGRID -System nicht gefunden werden.	"OLST: System hat verlorenes Objekt erkannt"

Code	Nachrichtentitel und -beschreibung	Siehe
SADD	Sicherheitsüberprüfung deaktivieren: Die Protokollierung von Überwachungsnachrichten wurde deaktiviert.	"SADD: Sicherheitsüberprüfung deaktivieren"
SADE	Sicherheitsaudit aktivieren: Die Protokollierung von Audit-Nachrichten wurde wiederhergestellt.	"SADE: Sicherheitsaudit aktivieren"
SVRF	Objektspeicherüberprüfung fehlgeschlagen: Ein Inhaltsblock hat die Überprüfung nicht bestanden.	"SVRF: Objektspeicherüberprüfung fehlgeschlagen"
SVRU	Object Store Verify Unknown: Im Objektspeicher wurden unerwartete Objektdaten erkannt.	"SVRU: Object Store Verify Unbekannt"
SYSD	Knotenstopp: Es wurde ein Herunterfahren angefordert.	"SYSD: Knotenstopp"
SYST	Knoten wird gestoppt: Ein Dienst hat einen ordnungsgemäßen Stopp eingeleitet.	"SYST: Knoten wird gestoppt"
SYSU	Knotenstart: Ein Dienst wurde gestartet. Die Art des vorherigen Herunterfahrens wird in der Nachricht angegeben.	"SYSU: Knotenstart"

Objektspeicher-Auditmeldungen

Die Audit-Meldungen der Kategorie „Objektspeicher-Audit“ werden für Ereignisse im Zusammenhang mit der Speicherung und Verwaltung von Objekten innerhalb des StorageGRID -Systems verwendet. Hierzu gehören die Speicherung und Abfrage von Objekten, Übertragungen von Grid-Knoten zu Grid-Knoten und Überprüfungen.

Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, wenn Funktionen veraltet sind. Wenn Sie auf einen Prüfcode stoßen, der hier nicht aufgeführt ist, überprüfen Sie die vorherigen Versionen dieses Themas auf ältere SG-Versionen. Beispiel: "StorageGRID 11.8 Objektspeicher-Auditmeldungen" .

Code	Beschreibung	Siehe
BROR	Bucket-Nur-Lese-Anforderung: Ein Bucket hat den Nur-Lese-Modus betreten oder verlassen.	"BROR: Bucket-Nur-Lese-Anforderung"
CBSE	Ende der Objektübertragung: Die Quelleinheit hat einen Datenübertragungsvorgang von Grid-Knoten zu Grid-Knoten abgeschlossen.	"CBSE: Objekt senden Ende"

Code	Beschreibung	Siehe
CBRE	Objektempfangsende: Die Zielentität hat einen Datenübertragungsvorgang von Grid-Knoten zu Grid-Knoten abgeschlossen.	"CBRE: Objektempfangsende"
CGRR	Cross-Grid-Replikationsanforderung: StorageGRID hat einen Cross-Grid-Replikationsvorgang versucht, um Objekte zwischen Buckets in einer Grid-Föderationsverbindung zu replizieren.	"CGRR: Cross-Grid-Replikationsanforderung"
EBDL	Löschen eines leeren Buckets: Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, der alle Objekte löscht (führt einen Vorgang zum Leeren des Buckets aus).	"EBDL: Leeren Bucket löschen"
EBKR	Anforderung zum Leeren des Buckets: Ein Benutzer hat eine Anforderung gesendet, den leeren Bucket ein- oder auszuschalten (d. h. Bucket-Objekte zu löschen oder das Löschen von Objekten zu beenden).	"EBKR: Leere Bucket-Anforderung"
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"SCMT: Object Store Commit-Anforderung"
SREM	Object Store Remove: Ein Inhaltsblock wurde aus einem Rasterknoten gelöscht und kann nicht mehr direkt angefordert werden.	"SREM: Objektspeicher entfernen"

Client liest Audit-Nachrichten

Wenn eine S3-Clientanwendung eine Anforderung zum Abrufen eines Objekts stellt, werden Prüfmeldungen zum Lesen des Clients protokolliert.

Code	Beschreibung	Verwendet von	Siehe
S3SL	S3 Select-Anforderung: Protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Nachricht kann Fehlermeldungs- und Fehlercodedetails enthalten. Die Anfrage war möglicherweise nicht erfolgreich.	S3-Client	"S3SL: S3-Auswahlanforderung"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfnachricht das Feld S3SR.	S3-Client	"SGET: S3 GET"

Code	Beschreibung	Verwendet von	Siehe
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	S3-Client	"SHEA: S3 KOPF"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Container.	Swift-Client	"WGET: Schnelles GET"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Containers zu überprüfen.	Swift-Client	"WHEA: Schneller Kopf"

Client schreibt Prüfmeldungen

Client-Schreibprüfmeldungen werden protokolliert, wenn eine S3-Clientanwendung eine Anforderung zum Erstellen oder Ändern eines Objekts stellt.

Code	Beschreibung	Verwendet von	Siehe
OVWR	Objektüberschreiben: Protokolliert eine Transaktion zum Überschreiben eines Objekts mit einem anderen Objekt.	S3- und Swift-Clients	"OVWR: Objektüberschreiben"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfnachricht das Feld S3SR.	S3-Client	"SDEL: S3 LÖSCHEN"
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zum Wiederherstellen eines Objekts aus dem AWS Glacier-Speicher in einem Cloud-Speicherpool.	S3-Client	"SPOS: S3 POST"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Prüfnachricht das Feld S3SR.	S3-Client	"SPUT: S3 PUT"
SUPD	S3-Metadaten aktualisiert: Protokolliert eine erfolgreiche Transaktion zum Aktualisieren der Metadaten für ein vorhandenes Objekt oder einen vorhandenen Bucket.	S3-Client	"SUPD: S3-Metadaten aktualisiert"

Code	Beschreibung	Verwendet von	Siehe
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	Swift-Client	"WDEL: Schnelles LÖSCHEN"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Containers.	Swift-Client	"WPUT: Schnelles PUT"

Management-Audit-Nachricht

Die Kategorie „Verwaltung“ protokolliert Benutzeranforderungen an die Verwaltungs-API.

Code	Nachrichtentitel und -beschreibung	Siehe
MGAU	Audit-Nachricht der Management-API: Ein Protokoll der Benutzeranforderungen.	"MGAU: Management-Audit-Nachricht"

ILM-Audit-Meldungen

Die Prüfmeldungen der Kategorie „ILM-Prüfung“ werden für Ereignisse im Zusammenhang mit Vorgängen im Zusammenhang mit dem Information Lifecycle Management (ILM) verwendet.

Code	Nachrichtentitel und -beschreibung	Siehe
IDEL	Von ILM initiiertes Löschen: Diese Prüfmeldung wird generiert, wenn ILM den Löschvorgang eines Objekts startet.	"IDEL: Von ILM initiiertes Löschen"
LKCU	Bereinigung überschriebener Objekte. Diese Prüfmeldung wird generiert, wenn ein überschriebenes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Bereinigung überschriebener Objekte"
ORLM	Objektregeln erfüllt: Diese Prüfmeldung wird generiert, wenn Objektdaten gemäß den ILM-Regeln gespeichert werden.	"ORLM: Objektregeln erfüllt"

Prüfnachrichtenreferenz

BROR: Bucket-Nur-Lese-Anforderung

Der LDR-Dienst generiert diese Prüfnachricht, wenn ein Bucket in den schreibgeschützten Modus wechselt oder diesen verlässt. Beispielsweise wechselt ein Bucket in den schreibgeschützten Modus, während alle Objekte gelöscht werden.

Code	Feld	Beschreibung
BKHD	Bucket-UUID	Die Bucket-ID.

Code	Feld	Beschreibung
BROV	Bucket-Schreibschutz-Anforderungswert	Ob der Bucket schreibgeschützt wird oder den schreibgeschützten Zustand verlässt (1 = schreibgeschützt, 0 = nicht schreibgeschützt).
BROS	Bucket-Schreibschutzgrund	Der Grund, warum der Bucket schreibgeschützt wird oder den schreibgeschützten Zustand verlässt. Beispiel: emptyBucket.
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, das die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.

CBRB: Objektempfang beginnt

Während des normalen Systembetriebs werden Inhaltsblöcke kontinuierlich zwischen verschiedenen Knoten übertragen, während auf Daten zugegriffen, diese repliziert und gespeichert werden. Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen initiiert wird, wird diese Nachricht von der Zielentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.
CTSS	Sequenzzählung starten	Gibt die erste angeforderte Sequenzanzahl an. Bei Erfolg beginnt die Übertragung ab dieser Sequenzzählung.

Code	Feld	Beschreibung
CTES	Erwartete Endsequenzanzahl	Gibt die zuletzt angeforderte Sequenzzählung an. Bei Erfolg gilt die Übertragung als abgeschlossen, wenn diese Sequenzanzahl empfangen wurde.
RSLT	Übertragungsstartstatus	Status zum Zeitpunkt des Überweisungsbeginns: SUCS: Übertragung erfolgreich gestartet.

Diese Prüfmeldung bedeutet, dass ein Knoten-zu-Knoten-Datenübertragungsvorgang für ein einzelnes Inhaltselement initiiert wurde, das durch seine Inhaltsblockkennung identifiziert wird. Der Vorgang fordert Daten von „Start Sequence Count“ bis „Expected End Sequence Count“ an. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und in Kombination mit Speicherüberwachungsmeldungen die Anzahl der Replikate zu überprüfen.

CBRE: Objektempfangsende

Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen abgeschlossen ist, wird diese Nachricht von der Zielentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.
CTSS	Sequenzzählung starten	Gibt die Sequenzanzahl an, bei der die Übertragung begonnen hat.
CTAS	Tatsächliche Endsequenzanzahl	Gibt die letzte erfolgreich übertragene Sequenzanzahl an. Wenn die tatsächliche Endsequenzanzahl mit der Startsequenzanzahl übereinstimmt und das Übertragungsergebnis nicht erfolgreich war, wurden keine Daten ausgetauscht.

Code	Feld	Beschreibung
RSLT	Übertragungsergebnis	Das Ergebnis des Übertragungsvorgangs (aus Sicht der sendenden Entität): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung verloren CTMO: Verbindungs-Timeout während des Aufbaus oder der Übertragung UNRE: Zielknoten-ID nicht erreichbar CRPT: Übertragung aufgrund des Empfangs beschädigter oder ungültiger Daten beendet

Diese Prüfmeldung bedeutet, dass ein Datenübertragungsvorgang von Knoten zu Knoten abgeschlossen wurde. Wenn das Übertragungsergebnis erfolgreich war, hat der Vorgang Daten von „Start Sequence Count“ nach „Actual End Sequence Count“ übertragen. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und Fehler zu lokalisieren, zu tabellieren und zu analysieren. In Kombination mit Speicherüberwachungsmeldungen kann es auch zum Überprüfen der Replikatanzahl verwendet werden.

CBSB: Objekt senden beginnen

Während des normalen Systembetriebs werden Inhaltsblöcke kontinuierlich zwischen verschiedenen Knoten übertragen, während auf Daten zugegriffen, diese repliziert und gespeichert werden. Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen initiiert wird, wird diese Nachricht von der Quellentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.

Code	Feld	Beschreibung
CTSS	Sequenzzählung starten	Gibt die erste angeforderte Sequenzanzahl an. Bei Erfolg beginnt die Übertragung ab dieser Sequenzzählung.
CTES	Erwartete Endsequenzanzahl	Gibt die zuletzt angeforderte Sequenzzählung an. Bei Erfolg gilt die Übertragung als abgeschlossen, wenn diese Sequenzanzahl empfangen wurde.
RSLT	Übertragungsstartstatus	Status zum Zeitpunkt des Überweisungsbeginns: SUCS: Übertragung erfolgreich gestartet.

Diese Prüfmeldung bedeutet, dass ein Knoten-zu-Knoten-Datenübertragungsvorgang für ein einzelnes Inhaltselement initiiert wurde, das durch seine Inhaltsblockkennung identifiziert wird. Der Vorgang fordert Daten von „Start Sequence Count“ bis „Expected End Sequence Count“ an. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und in Kombination mit Speicherüberwachungsmeldungen die Anzahl der Replikate zu überprüfen.

CBSE: Objekt senden Ende

Wenn die Übertragung eines Inhaltsblocks von einem Knoten zu einem anderen abgeschlossen ist, wird diese Nachricht von der Quellentität ausgegeben.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Knoten-zu-Knoten-Sitzung/Verbindung.
CBID	Inhaltsblockkennung	Die eindeutige Kennung des übertragenen Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung per Push oder Pull initiiert wurde: PUSH: Der Übertragungsvorgang wurde von der sendenden Entität angefordert. PULL: Der Übertragungsvorgang wurde von der empfangenden Entität angefordert.
CTSR	Quell-Entität	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zielentität	Die Knoten-ID des Ziels (Empfängers) der CBID-Übertragung.
CTSS	Sequenzzählung starten	Gibt die Sequenzanzahl an, bei der die Übertragung begonnen hat.

Code	Feld	Beschreibung
CTAS	Tatsächliche Endsequenzanzahl	Gibt die letzte erfolgreich übertragene Sequenzanzahl an. Wenn die tatsächliche Endsequenzanzahl mit der Startsequenzanzahl übereinstimmt und das Übertragungsergebnis nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis des Übertragungsvorgangs (aus Sicht der sendenden Entität): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung verloren CTMO: Verbindungs-Timeout während des Aufbaus oder der Übertragung UNRE: Zielknoten-ID nicht erreichbar CRPT: Übertragung aufgrund des Empfangs beschädigter oder ungültiger Daten beendet

Diese Prüfmeldung bedeutet, dass ein Datenübertragungsvorgang von Knoten zu Knoten abgeschlossen wurde. Wenn das Übertragungsergebnis erfolgreich war, hat der Vorgang Daten von „Start Sequence Count“ nach „Actual End Sequence Count“ übertragen. Sende- und Empfangsknoten werden durch ihre Knoten-IDs identifiziert. Diese Informationen können verwendet werden, um den Systemdatenfluss zu verfolgen und Fehler zu lokalisieren, zu tabellieren und zu analysieren. In Kombination mit Speicherüberwachungsmeldungen kann es auch zum Überprüfen der Replikatanzahl verwendet werden.

CGRR: Cross-Grid-Replikationsanforderung

Diese Nachricht wird generiert, wenn StorageGRID einen Cross-Grid-Replikationsvorgang versucht, um Objekte zwischen Buckets in einer Grid-Föderationsverbindung zu replizieren.

Code	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Bytes. Das CSIZ-Attribut wurde in StorageGRID 11.8 eingeführt. Dies kann dazu führen, dass Cross-Grid-Replikationsanforderungen, die ein Upgrade von StorageGRID 11.7 auf 11.8 umfassen, eine ungenaue Gesamtobjektgröße aufweisen.
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, dem der Bucket gehört, aus dem das Objekt repliziert wird.
GFID	Grid-Föderation-Verbindungs-ID	Die ID der Grid-Föderationsverbindung, die für die Grid-übergreifende Replikation verwendet wird.

Code	Feld	Beschreibung
OPER	CGR-Betrieb	Der Typ des Cross-Grid-Replikationsvorgangs, der versucht wurde: • 0 = Objekt replizieren • 1 = Mehrteiliges Objekt replizieren • 2 = Löschmarkierung replizieren
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das repliziert wurde.
RSLT	Ergebniscode	Gibt „Erfolgreich“ (SUCS) oder einen allgemeinen Fehler (GERR) zurück.

EBDL: Leeren Bucket löschen

Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, der alle Objekte löscht (und dabei einen Bucket-Leervorgang durchführt).

Code	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Bytes.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
RSLT	Ergebnis des Löschvorgangs	Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Wenn es für eine Nachricht nicht relevant ist, wird NONE statt SUCS verwendet, damit die Nachricht nicht versehentlich gefiltert wird.

EBKR: Leere Bucket-Anforderung

Diese Nachricht zeigt an, dass ein Benutzer eine Anforderung zum Ein- oder Ausschalten des leeren Buckets gesendet hat (d. h. zum Löschen von Bucket-Objekten oder zum Beenden des Löschens von Objekten).

Code	Feld	Beschreibung
BAUEN	Bucket-UUID	Die Bucket-ID.
EBJS	JSON-Konfiguration für leeren Bucket	Enthält das JSON, das die aktuelle Empty Bucket-Konfiguration darstellt.
S3AI	S3-Mandantenkonto-ID	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.

ECMC: Fehlendes Erasure-Coded-Datenfragment

Diese Prüfmeldung zeigt an, dass das System ein fehlendes Erasure-Coded-Datenfragment erkannt hat.

Code	Feld	Beschreibung
VCMC	VCS-ID	Der Name des VCS, das den fehlenden Block enthält.
MCID	Chunk-ID	Die Kennung des fehlenden Erasure-Codierten-Fragments.
RSLT	Ergebnis	Dieses Feld hat den Wert „NONE“. RSLT ist ein obligatorisches Nachrichtenfeld, ist für diese spezielle Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird „NONE“ anstelle von „SUCS“ verwendet.

ECOC: Beschädigtes Erasure-Coded-Datenfragment

Diese Prüfmeldung zeigt an, dass das System ein beschädigtes, löschcodiertes Datenfragment erkannt hat.

Code	Feld	Beschreibung
VCCO	VCS-ID	Der Name des VCS, das den beschädigten Block enthält.
VLID	Datenträger-ID	Das RangeDB-Volume, das das beschädigte Erasure-Coded-Fragment enthält.
CCID	Chunk-ID	Die Kennung des beschädigten Erasure-Code-Fragments.
RSLT	Ergebnis	Dieses Feld hat den Wert „NONE“. RSLT ist ein obligatorisches Nachrichtenfeld, ist für diese spezielle Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird „NONE“ anstelle von „SUCS“ verwendet.

ETAF: Sicherheitsauthentifizierung fehlgeschlagen

Diese Nachricht wird generiert, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Code	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung, über die die Authentifizierung fehlgeschlagen ist.
RUID	Benutzeridentität	Eine dienstabhängige Kennung, die die Identität des Remotebenutzers darstellt.
RSLT	Ursachencode	Der Grund für das Scheitern: SCNI: Der Aufbau einer sicheren Verbindung ist fehlgeschlagen. CERM: Zertifikat fehlte. CERT: Das Zertifikat war ungültig. CERE: Zertifikat ist abgelaufen. CERR: Zertifikat wurde widerrufen. CSGN: Die Zertifikatssignatur war ungültig. CSGU: Der Zertifikatsunterzeichner war unbekannt. UCRM: Benutzeranmeldeinformationen fehlten. UCRI: Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht zugelassen. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wenn eine Verbindung zu einem sicheren Dienst hergestellt wird, der TLS verwendet, werden die Anmeldeinformationen der Remote-Entität mithilfe des TLS-Profils und zusätzlicher, in den Dienst integrierter Logik überprüft. Wenn diese Authentifizierung aufgrund ungültiger, unerwarteter oder nicht zulässiger Zertifikate oder Anmeldeinformationen fehlschlägt, wird eine Prüfmeldung protokolliert. Dies ermöglicht Abfragen bei unberechtigten Zugriffsversuchen und anderen sicherheitsrelevanten Verbindungsproblemen.

Die Meldung kann durch eine falsche Konfiguration einer Remote-Entität oder durch Versuche verursacht werden, dem System ungültige oder nicht zulässige Anmeldeinformationen vorzulegen. Diese Prüfmeldung sollte überwacht werden, um Versuche zu erkennen, sich unbefugten Zugriff auf das System zu verschaffen.

GNRG: GNDS-Registrierung

Der CMN-Dienst generiert diese Prüfnachricht, wenn ein Dienst Informationen über sich selbst im StorageGRID System aktualisiert oder registriert hat.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • SUCS: Erfolgreich • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Knoten-ID	Die Knoten-ID des Dienstes, der die Aktualisierungsanforderung initiiert hat.
GNTP	Gerätetyp	Der Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Gerätemodellversion	Die Zeichenfolge, die die Gerätemodellversion des Grid-Knotens im DMDL-Paket identifiziert.
GNGP	Gruppe	Die Gruppe, zu der der Grid-Knoten gehört (im Kontext der Link-Kosten und der Rangfolge der Service-Abfragen).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Knotens.

Diese Nachricht wird immer dann generiert, wenn ein Grid-Knoten seinen Eintrag im Grid-Knoten-Paket aktualisiert.

GNUR: GNDS-Abmeldung

Der CMN-Dienst generiert diese Prüfnachricht, wenn ein Dienst nicht registrierte Informationen über sich selbst aus dem StorageGRID System hat.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • SUCS: Erfolgreich • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Knoten-ID	Die Knoten-ID des Dienstes, der die Aktualisierungsanforderung initiiert hat.

GTED: Grid-Aufgabe beendet

Diese Prüfmeldung zeigt an, dass der CMN-Dienst die Verarbeitung der angegebenen Rasteraufgabe abgeschlossen und die Aufgabe in die Verlaufstabelle verschoben hat. Wenn das Ergebnis SUCS, ABRT oder ROLF ist, wird eine entsprechende Prüfmeldung „Grid Task Started“ angezeigt. Die anderen Ergebnisse deuten darauf hin, dass die Verarbeitung dieser Grid-Aufgabe nie begonnen hat.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über ihren Lebenszyklus. **Hinweis:** Die Aufgaben-ID wird zum Zeitpunkt der Generierung einer Rasteraufgabe zugewiesen, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Rasteraufgabe mehrmals übermittelt wird. In diesem Fall reicht das Feld „Aufgaben-ID“ nicht aus, um die Prüfmeldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: • SUCS: Die Rasteraufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne Rollback-Fehler beendet. • ROLF: Die Grid-Aufgabe wurde beendet und konnte den Rollback-Prozess nicht abschließen. • CANC: Die Grid-Aufgabe wurde vom Benutzer abgebrochen, bevor sie gestartet wurde. • EXPR: Die Grid-Aufgabe ist abgelaufen, bevor sie gestartet wurde. • IVLD: Die Rasteraufgabe war ungültig. • AUTH: Die Grid-Aufgabe war nicht autorisiert. • DUPL: Die Rasteraufgabe wurde als Duplikat abgelehnt.

GTST: Grid-Aufgabe gestartet

Diese Prüfmeldung zeigt an, dass der CMN-Dienst mit der Verarbeitung der angegebenen Grid-Aufgabe begonnen hat. Die Prüfnachricht folgt unmittelbar auf die Nachricht „Grid Task Submitted“ für Grid-Aufgaben, die vom internen Grid Task Submission-Dienst initiiert und für die automatische Aktivierung ausgewählt wurden. Für Rasteraufgaben, die in die Tabelle „Ausstehend“ übermittelt werden, wird diese Nachricht generiert, wenn der Benutzer die Rasteraufgabe startet.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Dieses Feld identifiziert eine generierte Rasteraufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über ihren Lebenszyklus. **Hinweis:** Die Aufgaben-ID wird zum Zeitpunkt der Generierung einer Rasteraufgabe zugewiesen, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Rasteraufgabe mehrmals übermittelt wird. In diesem Fall reicht das Feld „Aufgaben-ID“ nicht aus, um die Prüfmeldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: • SUCS: Die Grid-Task wurde erfolgreich gestartet.

GTSU: Grid-Aufgabe übermittelt

Diese Prüfnachricht zeigt an, dass eine Rasteraufgabe an den CMN-Dienst übermittelt wurde.

Code	Feld	Beschreibung
TSID	Aufgaben-ID	Identifiziert eine generierte Rasteraufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über ihren Lebenszyklus. **Hinweis:** Die Aufgaben-ID wird zum Zeitpunkt der Generierung einer Rasteraufgabe zugewiesen, nicht zum Zeitpunkt der Übermittlung. Es ist möglich, dass eine bestimmte Rasteraufgabe mehrmals übermittelt wird. In diesem Fall reicht das Feld „Aufgaben-ID“ nicht aus, um die Prüfmeldungen „Übermittelt“, „Gestartet“ und „Beendet“ eindeutig zu verknüpfen.
TTYP	Aufgabentyp	Der Typ der Rasteraufgabe.
TWER	Aufgabenversion	Eine Zahl, die die Version der Rasteraufgabe angibt.
TDSC	Aufgabenbeschreibung	Eine für Menschen lesbare Beschreibung der Rasteraufgabe.
Mehrwertsteuer	Gültig nach Zeitstempel	Der früheste Zeitpunkt (UINT64 Mikrosekunden ab 1. Januar 1970 – UNIX-Zeit), zu dem die Grid-Aufgabe gültig ist.
VBTS	Gültig vor Zeitstempel	Der späteste Zeitpunkt (UINT64 Mikrosekunden ab 1. Januar 1970 – UNIX-Zeit), zu dem die Grid-Aufgabe gültig ist.
TSRC	Quelle	Die Quelle der Aufgabe: • TXTB: Die Grid-Aufgabe wurde über das StorageGRID -System als signierter Textblock übermittelt. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submission Service übermittelt.
ACTV	Aktivierungstyp	Die Art der Aktivierung: • AUTO: Die Rasteraufgabe wurde zur automatischen Aktivierung übermittelt. • PEND: Die Rasteraufgabe wurde in die ausstehende Tabelle übermittelt. Dies ist die einzige Möglichkeit für die TXTB-Quelle.

Code	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Einreichung: • SUCS: Die Rasteraufgabe wurde erfolgreich übermittelt. • FEHLGESCHLAGEN: Die Aufgabe wurde direkt in die Verlaufstabelle verschoben.

IDEL: Von ILM initiiertes Löschen

Diese Nachricht wird generiert, wenn ILM den Löschvorgang eines Objekts startet.

Die IDEL-Nachricht wird in einer der folgenden Situationen generiert:

- **Für Objekte in konformen S3-Buckets**: Diese Nachricht wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, weil seine Aufbewahrungsfrist abgelaufen ist (vorausgesetzt, die Einstellung zum automatischen Löschen ist aktiviert und die rechtliche Aufbewahrungsfrist ist deaktiviert).
- **Für Objekte in nicht konformen S3-Buckets**. Diese Nachricht wird generiert, wenn ILM mit dem Löschen eines Objekts beginnt, weil in den aktiven ILM-Richtlinien derzeit keine Platzierungsanweisungen für das Objekt gelten.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die CBID des Objekts.
CMPA	Compliance: Automatisches Löschen	Nur für Objekte in konformen S3-Buckets. 0 (falsch) oder 1 (wahr) gibt an, ob ein konformes Objekt automatisch gelöscht werden soll, wenn seine Aufbewahrungsfrist endet, es sei denn, der Bucket unterliegt einer rechtlichen Sperre.
CMPL	Compliance: Gesetzliche Aufbewahrungspflicht	Nur für Objekte in konformen S3-Buckets. 0 (falsch) oder 1 (wahr), gibt an, ob der Bucket derzeit einer rechtlichen Sperre unterliegt.
CMPR	Compliance: Aufbewahrungsfrist	Nur für Objekte in konformen S3-Buckets. Die Länge der Aufbewahrungsdauer des Objekts in Minuten.
CTME	Compliance: Aufnahmezeit	Nur für Objekte in konformen S3-Buckets. Die Aufnahmezeit des Objekts. Sie können zu diesem Wert die Aufbewahrungsdauer in Minuten hinzufügen, um festzulegen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	Marker-Versions-ID löschen	Die Versions-ID der Löschmarkierung, die beim Löschen eines Objekts aus einem versionierten Bucket erstellt wird. Operationen an Buckets schließen dieses Feld nicht ein.

Code	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.
LOCS	Standorte	Der Speicherort der Objektdaten innerhalb des StorageGRID -Systems. Der Wert für LOCS ist "", wenn das Objekt keine Standorte hat (z. B. wenn es gelöscht wurde). CLEC: für Erasure-Coding-Objekte die Erasure-Coding-Profil-ID und die Erasure-Coding-Gruppen-ID, die auf die Daten des Objekts angewendet wird. CLDI: für replizierte Objekte die LDR-Knoten-ID und die Volume-ID des Objektstandorts. CLNL: ARC-Knoten-ID des Objektstandorts, wenn die Objektdaten archiviert sind.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	• Wenn ein Objekt in einem konformen S3-Bucket automatisch gelöscht wird, weil seine Aufbewahrungsfrist abgelaufen ist, ist dieses Feld leer. • Wenn das Objekt gelöscht wird, weil derzeit keine Platzierungsanweisungen mehr für das Objekt gelten, wird in diesem Feld die menschenlesbare Bezeichnung der letzten ILM-Regel angezeigt, die für das Objekt galt.
SGRP	Site (Gruppe)	Falls vorhanden, wurde das Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das Objekt aufgenommen wurde.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das gelöscht wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

LKCU: Bereinigung überschriebener Objekte

Diese Meldung wird generiert, wenn StorageGRID ein überschriebenes Objekt entfernt, das zuvor bereinigt werden musste, um Speicherplatz freizugeben. Ein Objekt wird überschrieben, wenn ein S3-Client ein Objekt in einen Pfad schreibt, der bereits ein Objekt enthält. Der Entfernungsprozess erfolgt automatisch und im Hintergrund.

Code	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.
LTYP	Art der Bereinigung	*Nur zur internen Verwendung.*
LUID	Entfernte Objekt-UUID	Die Kennung des Objekts, das entfernt wurde.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell eindeutige Kennung	Die Kennung des noch vorhandenen Objekts. Dieser Wert ist nur verfügbar, wenn das Objekt nicht gelöscht wurde.

LKDM: Bereinigung durchgesickerter Objekte

Diese Nachricht wird generiert, wenn ein durchgesickerter Block bereinigt oder gelöscht wurde. Ein Chunk kann Teil eines replizierten Objekts oder eines erasure-encoded Objekts sein.

Code	Feld	Beschreibung
CLOC	Chunk-Standort	Der Dateipfad des durchgesickerten Blocks, der gelöscht wurde.

CTYP	Chunk-Typ	Art des Chunks:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

Code	Feld	Beschreibung

LTYP	Lecktyp	Die fünf Arten von Lecks, die erkannt werden können:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Chunk-Erstellungszeit	Zeitpunkt der Erstellung des durchgesickerten Chunks.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts, zu dem der Block gehört.
CBID	Inhaltsblockkennung	CBID des Objekts, zu dem der durchgesickerte Block gehört.
CSIZ	Inhaltsgröße	Die Größe des Blocks in Bytes.

LLST: Standort verloren

Diese Nachricht wird generiert, wenn kein Speicherort für eine Objektkopie (repliziert oder löschcodiert) gefunden werden kann.

Code	Feld	Beschreibung
CBIL	CBID	Das betroffene CBID.
ECPR	Erasure-Coding-Profil	Für löschcodierte Objektdaten. Die ID des verwendeten Erasure-Coding-Profils.
LTYP	Ortstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für erasure-coded Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten

Code	Feld	Beschreibung
NOID	Quellknoten-ID	Die Knoten-ID, auf der die Standorte verloren gegangen sind.
PCLD	Pfad zum replizierten Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten auf der Festplatte. Wird nur zurückgegeben, wenn LTYP den Wert CLDI hat (d. h. für replizierte Objekte). Nimmt die Form an `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Ergebnis	Immer KEINE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.
TSRC	Auslösende Quelle	USER: Vom Benutzer ausgelöst SYST: System ausgelöst
UUID	Universell eindeutige ID	Die Kennung des betroffenen Objekts im StorageGRID -System.

MGAU: Management-Audit-Nachricht

Die Kategorie „Verwaltung“ protokolliert Benutzeranforderungen an die Verwaltungs-API. Jede HTTP-Anforderung, die keine GET- oder HEAD-Anforderung an eine gültige API-URI ist, protokolliert eine Antwort, die den Benutzernamen, die IP und den Anforderungstyp an die API enthält. Ungültige API-URIs (wie z. B. /api/v3-authorize) und ungültige Anfragen an gültige API-URIs werden nicht protokolliert.

Code	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domänenname	Der Hostdomänenname.
MPAT	PATH anfordern	Der Anforderungspfad.
MPQP	Abfrageparameter anfordern	Die Abfrageparameter für die Anfrage.

Code	Feld	Beschreibung
MRBD	Anforderungstext	Der Inhalt des Anforderungstexts. Während der Antworttext standardmäßig protokolliert wird, wird der Anforderungstext in bestimmten Fällen protokolliert, wenn der Antworttext leer ist. Da die folgenden Informationen im Antworttext nicht verfügbar sind, werden sie für die folgenden POST-Methoden aus dem Anforderungstext übernommen: • Benutzername und Konto-ID in **POST-Autorisierung** • Neue Subnetzkonfiguration in **POST /grid/grid-networks/update** • Neue NTP-Server in **POST /grid/ntp-servers/update** • Außer Betrieb genommene Server-IDs in **POST /grid/servers/decommission** **Hinweis:** Vertrauliche Informationen werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen maskiert (z. B. ein Passwort).
MRMD	Anforderungsmethode	Die HTTP-Anforderungsmethode: • POST • SETZEN • LÖSCHEN • PATCH
MRSC	Antwortcode	Der Antwortcode.
UVP	Antworttext	Der Inhalt der Antwort (der Antworttext) wird standardmäßig protokolliert. **Hinweis:** Vertrauliche Informationen werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen maskiert (z. B. ein Passwort).
MSIP	Quell-IP-Adresse	Die IP-Adresse des Clients (Quelle).
MUUN	Benutzer-URN	Der URN (Uniform Resource Name) des Benutzers, der die Anfrage gesendet hat.
RSLT	Ergebnis	Gibt „Erfolgreich“ (SUCS) oder den vom Backend gemeldeten Fehler zurück.

OLST: System hat verlorenes Objekt erkannt

Diese Nachricht wird generiert, wenn der DDS-Dienst keine Kopien eines Objekts im StorageGRID -System finden kann.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die CBID des verlorenen Objekts.
NOID	Knoten-ID	Falls verfügbar, der letzte bekannte direkte oder nahegelegene Standort des verlorenen Objekts. Es ist möglich, nur die Knoten-ID ohne Volume-ID zu haben, wenn die Volume-Informationen nicht verfügbar sind.
WEG	S3-Bucket/Schlüssel	Falls verfügbar, der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.
UUID	Universell eindeutige ID	Die Kennung des verlorenen Objekts innerhalb des StorageGRID -Systems.
VOLI	Datenträger-ID	Falls verfügbar, die Volume-ID des Speicherknotens für den letzten bekannten Standort des verlorenen Objekts.

ORLM: Objektregeln erfüllt

Diese Nachricht wird generiert, wenn das Objekt gemäß den ILM-Regeln erfolgreich gespeichert und kopiert wurde.

> ⓘ Die ORLM-Meldung wird nicht generiert, wenn ein Objekt erfolgreich durch die Standardregel „2 Kopien erstellen“ gespeichert wurde und eine andere Regel in der Richtlinie den erweiterten Filter „Objektgröße“ verwendet.

Code	Feld	Beschreibung
BAUEN	Schaufelkopf	Bucket-ID-Feld. Wird für interne Vorgänge verwendet. Erscheint nur, wenn STAT PRGD ist.
CBID	Inhaltsblockkennung	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Bytes.

Code	Feld	Beschreibung
LOCS	Standorte	Der Speicherort der Objektdaten innerhalb des StorageGRID -Systems. Der Wert für LOCS ist "", wenn das Objekt keine Standorte hat (z. B. wenn es gelöscht wurde). CLEC: für Erasure-Coding-Objekte die Erasure-Coding-Profil-ID und die Erasure-Coding-Gruppen-ID, die auf die Daten des Objekts angewendet wird. CLDI: für replizierte Objekte die LDR-Knoten-ID und die Volume-ID des Objektstandorts. CLNL: ARC-Knoten-ID des Objektstandorts, wenn die Objektdaten archiviert sind.
WEG	S3-Bucket/Schlüssel	Der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	Die für Menschen lesbare Bezeichnung für die auf dieses Objekt angewendete ILM-Regel.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Behälter CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur für segmentierte und mehrteilige Objekte verfügbar.
STAT	Status	Der Status des ILM-Vorgangs. FERTIG: ILM-Vorgänge für das Objekt wurden abgeschlossen. DFER: Das Objekt wurde für eine zukünftige ILM-Neubewertung markiert. PRGD: Das Objekt wurde aus dem StorageGRID -System gelöscht. NLOC: Die Objektdaten sind im StorageGRID -System nicht mehr auffindbar. Dieser Status kann darauf hinweisen, dass alle Kopien der Objektdaten fehlen oder beschädigt sind.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.

Code	Feld	Beschreibung
VSID	Versions-ID	Die Versions-ID eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

Die ORLM-Audit-Nachricht kann für ein einzelnes Objekt mehr als einmal ausgegeben werden. Es wird beispielsweise immer dann ausgegeben, wenn eines der folgenden Ereignisse eintritt:

- ILM-Regeln für das Objekt werden dauerhaft erfüllt.
- Die ILM-Regeln für das Objekt werden für diese Epoche erfüllt.
- Das Objekt wurde durch ILM-Regeln gelöscht.
- Der Hintergrundüberprüfungsprozess erkennt, dass eine Kopie der replizierten Objektdaten beschädigt ist. Das StorageGRID -System führt eine ILM-Auswertung durch, um das beschädigte Objekt zu ersetzen.

Ähnliche Informationen

- "Objektaufnahmetransaktionen"
- "Objektlöschtransaktionen"

OVWR: Objektüberschreiben

Diese Nachricht wird generiert, wenn ein externer (vom Client angeforderter) Vorgang dazu führt, dass ein Objekt durch ein anderes Objekt überschrieben wird.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des zu überschreibenden Objekts in Bytes.
OCBD	Inhaltsblockkennung (vorherig)	Die CBID für das vorherige Objekt.
UUID	Universell eindeutige ID (neu)	Die Kennung des neuen Objekts innerhalb des StorageGRID -Systems.
OUID	Universell eindeutige ID (vorher)	Die Kennung für das vorherige Objekt innerhalb des StorageGRID -Systems.
WEG	S3-Objektpfad	Der S3-Objektpfad, der sowohl für das vorherige als auch für das neue Objekt verwendet wird

Code	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der Objektüberschreibungstransaktion. Ergebnis ist immer: SUCS: Erfolgreich
SGRP	Site (Gruppe)	Falls vorhanden, wurde das überschriebene Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das überschriebene Objekt aufgenommen wurde.

S3SL: S3-Auswahlanforderung

Diese Nachricht protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Nachricht kann Fehlermeldungs- und Fehlercodedetails enthalten. Die Anfrage war möglicherweise nicht erfolgreich.

Code	Feld	Beschreibung
BYSC	Gescannte Bytes	Anzahl der von Speicherknoten gescannten (empfangenen) Bytes. BYSC und BYPR sind wahrscheinlich unterschiedlich, wenn das Objekt komprimiert ist. Wenn das Objekt komprimiert ist, enthält BYSC die komprimierte Byteanzahl und BYPR die Bytes nach der Dekomprimierung.
BYPR	Verarbeitete Bytes	Anzahl der verarbeiteten Bytes. Gibt an, wie viele Bytes der „gescannten Bytes“ tatsächlich von einem S3 Select-Job verarbeitet oder bearbeitet wurden.
BYRT	Zurückgegebene Bytes	Anzahl der Bytes, die ein S3 Select-Job an den Client zurückgegeben hat.
REPR	Verarbeitete Datensätze	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job von Speicherknoten empfangen hat.
RERT	Zurückgegebene Datensätze	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job an den Client zurückgegeben hat.
JOFI	Auftrag abgeschlossen	Gibt an, ob die Verarbeitung des S3 Select-Jobs abgeschlossen ist oder nicht. Wenn dieser Wert falsch ist, konnte der Auftrag nicht abgeschlossen werden und die Fehlerfelder enthalten wahrscheinlich Daten. Der Kunde hat möglicherweise nur Teilergebnisse oder gar keine Ergebnisse erhalten.
REID	Anforderungs-ID	Kennung für die S3 Select-Anfrage.
EXTM	Ausführungszeit	Die Zeit in Sekunden, die für die Ausführung des S3 Select-Jobs benötigt wurde.

Code	Feld	Beschreibung
ERMG	Fehlermeldung	Fehlermeldung, die der S3 Select-Job generiert hat.
ERTY	Fehlertyp	Fehlertyp, der vom S3 Select-Job generiert wurde.
ERST	Fehler-Stacktrace	Fehler-Stacktrace, den der S3 Select-Job generiert hat.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat.
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen.

SADD: Sicherheitsüberprüfung deaktivieren

Diese Nachricht zeigt an, dass der ursprüngliche Dienst (Knoten-ID) die Protokollierung von Prüfnachrichten deaktiviert hat. Prüfnachrichten werden nicht mehr erfasst oder übermittelt.

Code	Feld	Beschreibung
AETM	Enable-Methode	Die zum Deaktivieren der Überwachung verwendete Methode.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Deaktivieren der Überwachungsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.

Die Meldung impliziert, dass die Protokollierung zuvor aktiviert war, jetzt aber deaktiviert wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemleistung zu verbessern. Nach der Massenaktivität wird die Überwachung wiederhergestellt (SADE) und die Möglichkeit, die Überwachung zu deaktivieren, wird dann dauerhaft blockiert.

SADE: Sicherheitsaudit aktivieren

Diese Nachricht zeigt an, dass der ursprüngliche Dienst (Knoten-ID) die Protokollierung

von Prüfnachrichten wiederhergestellt hat. Prüfnachrichten werden wieder erfasst und übermittelt.

Code	Feld	Beschreibung
AETM	Enable-Methode	Die Methode, die zum Aktivieren der Prüfung verwendet wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Aktivieren der Überwachungsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird NONE anstelle von SUCS verwendet.

Die Meldung impliziert, dass die Protokollierung zuvor deaktiviert war (SADD), jetzt aber wiederhergestellt wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemleistung zu verbessern. Nach der Massenaktivität wird die Überwachung wiederhergestellt und die Möglichkeit zum Deaktivieren der Überwachung dauerhaft blockiert.

SCMT: Objektspeicher-Commit

Grid-Inhalte werden erst verfügbar gemacht oder als gespeichert erkannt, wenn sie festgeschrieben (d. h. dauerhaft gespeichert) wurden. Dauerhaft gespeicherte Inhalte wurden vollständig auf die Festplatte geschrieben und haben die zugehörigen Integritätsprüfungen bestanden. Diese Nachricht wird ausgegeben, wenn ein Inhaltsblock gespeichert wird.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des Inhaltsblocks, der dauerhaft gespeichert wird.
RSLT	Ergebniscode	Status zum Zeitpunkt der Speicherung des Objekts auf der Festplatte: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und überprüft wurde und nun angefordert werden kann. Damit kann der Datenfluss innerhalb des Systems verfolgt werden.

SDEL: S3 LÖSCHEN

Wenn ein S3-Client eine DELETE-Transaktion ausgibt, wird eine Anforderung zum Entfernen des angegebenen Objekts oder Buckets oder zum Entfernen einer Bucket-/Objekt-Unterressource gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
DMRK	Marker-Versions-ID löschen	Die Versions-ID der Löschmarkierung, die beim Löschen eines Objekts aus einem versionierten Bucket erstellt wird. Operationen an Buckets schließen dieses Feld nicht ein.
GFID	Grid Federation-Verbindungs-ID	Die Verbindungs-ID der Grid-Föderationsverbindung, die einer Grid-übergreifenden Replikationslöschanforderung zugeordnet ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation-Quellkonto-ID	Die Konto-ID des Mandanten im Quellraster für eine rasterübergreifende Replikationslöschanforderung. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). `` `x-amz-bypass-governance-retention`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist.
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der DELETE-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich

Code	Feld	Beschreibung
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SGRP	Site (Gruppe)	Falls vorhanden, wurde das Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das Objekt aufgenommen wurde.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.

Code	Feld	Beschreibung
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUDM	Universell eindeutige Kennung für eine Löschmarkierung	Die Kennung einer Löschmarkierung. In den Prüfprotokollmeldungen ist entweder UUDM oder UUID angegeben, wobei UUDM eine Löschmarkierung angibt, die als Ergebnis einer Objektlöschanforderung erstellt wurde, und UUID ein Objekt angibt.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, das gelöscht wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SGET: S3 GET

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anforderung zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket oder zum Entfernen einer Bucket-/Objekt-Unterressource gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.

Code	Feld	Beschreibung
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
LITÄT	ListObjectsV2	Es wurde eine Antwort im *v2-Format* angefordert. Weitere Einzelheiten finden Sie unter "AWS ListObjectsV2" . Nur für GET-Bucket-Operationen.
NCHD	Anzahl der Kinder	Enthält Schlüssel und allgemeine Präfixe. Nur für GET-Bucket-Operationen.
RANG	Bereichsablesung	Nur für Bereichslesevorgänge. Gibt den Bytebereich an, der von dieser Anforderung gelesen wurde. Der Wert nach dem Schrägstrich (/) gibt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend.

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
Türkische Republik Nordzypern	Abgeschnitten oder nicht abgeschnitten	Auf „False“ setzen, wenn alle Ergebnisse zurückgegeben wurden. Auf „true“ setzen, wenn weitere Ergebnisse zur Rückgabe verfügbar sind. Nur für GET-Bucket-Operationen.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines angeforderten Objekts. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SHEA: S3 KOPF

Wenn ein S3-Client eine HEAD-Transaktion ausgibt, wird eine Anforderung gestellt, um die Existenz eines Objekts oder Buckets zu überprüfen und die Metadaten zu einem Objekt abzurufen. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des geprüften Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). ``
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines angeforderten Objekts. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SPOS: S3 POST

Wenn ein S3-Client eine POST-Objektanforderung ausgibt, wird diese Nachricht vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). (Für SPOS nicht zu erwarten).
RSLT	Ergebniscode	Ergebnis der RestoreObject-Anforderung. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend. Für einen S3-Auswahlvorgang auf „Auswählen“ einstellen.

Code	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SRCF	Unterressourcenkonfiguration	Informationen wiederherstellen.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines angeforderten Objekts. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anforderung zum Erstellen

eines neuen Objekts oder Buckets oder zum Entfernen einer Bucket-/Objekt-Unterressource gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern in der Anfrage vorhanden (auf die ersten 1024 Zeichen gekürzt).
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
GFID	Grid Federation-Verbindungs-ID	Die Verbindungs-ID der Grid-Föderationsverbindung, die einer PUT-Anforderung für die Grid-übergreifende Replikation zugeordnet ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation-Quellkonto-ID	Die Konto-ID des Mandanten im Quellraster für eine PUT-Anforderung zur rasterübergreifenden Replikation. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). `` `x-amz-bypass-governance-retention`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist.
LKEN	Objektsperre aktiviert	Wert des Anforderungsheaders `x-amz-bucket-object-lock-enabled` , falls in der Anfrage vorhanden.

Code	Feld	Beschreibung
LKLH	Objektsperre – Rechtliche Aufbewahrung	Wert des Anforderungsheaders `x-amz-object-lock-legal-hold` , falls in der PutObject-Anforderung vorhanden.
LKMD	Objektsperr-Aufbewahrungsmodus	Wert des Anforderungsheaders `x-amz-object-lock-mode` , falls in der PutObject-Anforderung vorhanden.
LKRU	Objektsperre – Aufbewahrung bis Datum	Wert des Anforderungsheaders `x-amz-object-lock-retain-until-date` , falls in der PutObject-Anforderung vorhanden. Die Werte sind auf einen Zeitraum von 100 Jahren ab dem Datum der Einnahme des Objekts begrenzt.
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
S3SR	S3-Unterressource	Der Bucket oder die Objekt-Subressource, an der gearbeitet wird, falls zutreffend.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.

Code	Feld	Beschreibung
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SRCF	Unterressourcenkonfiguration	Die neue Unterressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
ULID	ID hochladen	Nur in SPUT-Nachrichten für CompleteMultipartUpload-Vorgänge enthalten. Zeigt an, dass alle Teile hochgeladen und zusammengebaut wurden.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.
VSST	Versionsstatus	Der neue Versionsstatus eines Buckets. Es werden zwei Zustände verwendet: „aktiviert“ oder „ausgesetzt“. Operationen an Objekten schließen dieses Feld nicht ein.

SREM: Objektspeicher entfernen

Diese Nachricht wird ausgegeben, wenn Inhalte aus dem permanenten Speicher entfernt werden und nicht mehr über reguläre APIs zugänglich sind.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des aus dem permanenten Speicher gelöschten Inhaltsblocks.
RSLT	Ergebniscode	Gibt das Ergebnis der Inhaltsentfernungsvorgänge an. Der einzige definierte Wert ist: SUCS: Inhalt aus dem persistenten Speicher entfernt

Diese Prüfmeldung bedeutet, dass ein bestimmter Inhaltsblock aus einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Mithilfe der Nachricht kann der Fluss gelöschter Inhalte innerhalb des Systems verfolgt werden.

SUPD: S3-Metadaten aktualisiert

Diese Nachricht wird von der S3-API generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert. Die Meldung wird vom Server ausgegeben, wenn die Aktualisierung der Metadaten erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Operationen an Buckets schließen dieses Feld nicht ein.
CNCH	Konsistenzkontrollkopf	Der Wert des HTTP-Anforderungsheaders „Consistency-Control“, sofern in der Anforderung vorhanden, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Operationen an Buckets schließen dieses Feld nicht ein.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `` `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld). ``

Code	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer: SUCS: erfolgreich
S3AI	S3-Mandantenkonto-ID (Absender der Anfrage)	Die Mandantenkonto-ID des Benutzers, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3AK	S3-Zugriffsschlüssel-ID (Absender der Anfrage)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anfrage gesendet hat. Ein leerer Wert zeigt einen anonymen Zugriff an.
S3BK	S3-Bucket	Der Name des S3-Buckets.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen an Buckets schließen dieses Feld nicht ein.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Leer für anonyme Anfragen.
SAIP	IP-Adresse (Absender der Anfrage)	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandantenkonto-ID des Eigentümers des Ziel-Buckets. Wird verwendet, um kontoübergreifenden oder anonymen Zugriff zu identifizieren.
SUSR	S3-Benutzer-URN (Absender der Anfrage)	Die Mandantenkonto-ID und der Benutzername des Benutzers, der die Anfrage stellt. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Leer für anonyme Anfragen.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.

Code	Feld	Beschreibung
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
VSID	Versions-ID	Die Versions-ID der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Vorgänge an Buckets und Objekten in Buckets ohne Versionierung schließen dieses Feld nicht ein.

SVRF: Objektspeicherüberprüfung fehlgeschlagen

Diese Meldung wird immer dann ausgegeben, wenn ein Inhaltsblock den Überprüfungsprozess nicht besteht. Jedes Mal, wenn replizierte Objektdaten von der Festplatte gelesen oder auf die Festplatte geschrieben werden, werden mehrere Überprüfungen und Integritätsprüfungen durchgeführt, um sicherzustellen, dass die an den anfordernden Benutzer gesendeten Daten mit den ursprünglich in das System aufgenommenen Daten identisch sind. Wenn eine dieser Prüfungen fehlschlägt, stellt das System die beschädigten replizierten Objektdaten automatisch unter Quarantäne, um zu verhindern, dass sie erneut abgerufen werden.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des Inhaltsblocks, dessen Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Art des Überprüfungsfehlers: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Die Prüfung des Hash-basierten Nachrichtenauthentifizierungscodes (HMAC) ist fehlgeschlagen. EHSH: Unerwarteter Hash für verschlüsselten Inhalt. PHSH: Unerwarteter Hash des Originalinhalts. SEQC: Falsche Datensequenz auf der Festplatte. PERR: Ungültige Struktur der Datenträgerdatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.

Diese Nachricht sollte genau beobachtet werden. Fehler bei der Inhaltsüberprüfung können auf bevorstehende Hardwarefehler hinweisen.

Um festzustellen, welcher Vorgang die Nachricht ausgelöst hat, sehen Sie sich den Wert des AMID-Felds (Modul-ID) an. Beispielsweise gibt ein SVFY-Wert an, dass die Nachricht vom Storage Verifier-Modul generiert wurde, also durch Hintergrundüberprüfung, und STOR gibt an, dass die Nachricht durch Inhaltsabruf ausgelöst wurde.

SVRU: Object Store Verify Unbekannt

Die Speicherkomponente des LDR-Dienstes scannt kontinuierlich alle Kopien der replizierten Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Code	Feld	Beschreibung
FPTH	Dateipfad	Der Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert „NONE“. RSLT ist ein obligatorisches Nachrichtenfeld, für diese Nachricht jedoch nicht relevant. Damit diese Nachricht nicht gefiltert wird, wird „NONE“ anstelle von „SUCS“ verwendet.

Die Prüfmeldung „SVRU: Object Store Verify Unknown“ sollte genau überwacht werden. Dies bedeutet, dass im Objektspeicher unerwartete Kopien von Objektdaten erkannt wurden. Diese Situation sollte sofort untersucht werden, um festzustellen, wie diese Kopien erstellt wurden, da dies auf bevorstehende Hardwarefehler hinweisen kann.

SYSD: Knotenstopp

Wenn ein Dienst ordnungsgemäß beendet wird, wird diese Meldung generiert, um anzuzeigen, dass das Herunterfahren angefordert wurde. Normalerweise wird diese Nachricht erst nach einem anschließenden Neustart gesendet, da die Warteschlange der Prüfnachrichten vor dem Herunterfahren nicht gelöscht wird. Suchen Sie nach der SYST-Nachricht, die zu Beginn der Herunterfahrsequenz gesendet wurde, wenn der Dienst nicht neu gestartet wurde.

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Die Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren.

Die Meldung gibt nicht an, ob der Hostserver gestoppt wird, sondern nur der Berichtsdienst. Das RSLT eines SYSD kann kein „schmutziges“ Herunterfahren anzeigen, da die Meldung nur bei „sauberen“ Herunterfahren generiert wird.

SYST: Knoten wird gestoppt

Wenn ein Dienst ordnungsgemäß beendet wird, wird diese Meldung generiert, um anzuzeigen, dass das Herunterfahren angefordert wurde und dass der Dienst seine Herunterfahrsequenz eingeleitet hat. Mit SYST kann ermittelt werden, ob das Herunterfahren angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das normalerweise nach dem Neustart des Dienstes gesendet wird).

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Die Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren.

Die Meldung gibt nicht an, ob der Hostserver gestoppt wird, sondern nur der Berichtsdienst. Der RSLT-Code einer SYST-Nachricht kann kein „schmutziges“ Herunterfahren anzeigen, da die Nachricht nur bei „sauberen“ Herunterfahren generiert wird.

SYSU: Knotenstart

Wenn ein Dienst neu gestartet wird, wird diese Meldung generiert, um anzuzeigen, ob das vorherige Herunterfahren sauber (befohlen) oder ungeordnet (unerwartet) war.

Code	Feld	Beschreibung
RSLT	Sauberes Herunterfahren	Die Art der Abschaltung: SUCS: Das System wurde ordnungsgemäß heruntergefahren. DSDN: Das System wurde nicht sauber heruntergefahren. VRGN: Das System wurde nach der Serverinstallation (oder Neuinstallation) zum ersten Mal gestartet.

Die Meldung gibt nicht an, ob der Hostserver gestartet wurde, sondern nur, ob der Berichtsdienst gestartet wurde. Diese Nachricht kann verwendet werden, um:

- Erkennen Sie Diskontinuitäten im Prüfpfad.
- Stellen Sie fest, ob ein Dienst während des Betriebs ausfällt (da die verteilte Natur des StorageGRID -Systems diese Ausfälle maskieren kann). Der Server Manager startet einen ausgefallenen Dienst automatisch neu.

WDEL: Schnelles LÖSCHEN

Wenn ein Swift-Client eine DELETE-Transaktion ausgibt, wird eine Anforderung zum Entfernen des angegebenen Objekts oder Containers gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Bytes. Vorgänge an Containern umfassen dieses Feld nicht.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der DELETE-Transaktion. Ergebnis ist immer: SUCS: Erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
SGRP	Site (Gruppe)	Falls vorhanden, wurde das Objekt an der angegebenen Site gelöscht, die nicht die Site ist, an der das Objekt aufgenommen wurde.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.

Code	Feld	Beschreibung
WCON	Schneller Container	Der Name des Swift-Containers.
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

WGET: Schnelles GET

Wenn ein Swift-Client eine GET-Transaktion ausgibt, wird eine Anforderung zum Abrufen eines Objekts, zum Auflisten der Objekte in einem Container oder zum Auflisten der Container in einem Konto gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Ergebnis ist immer SUCS: erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.

Code	Feld	Beschreibung
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.
WCON	Schneller Container	Der Name des Swift-Containers. Bei Vorgängen mit Konten ist dieses Feld nicht enthalten.
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

WHEA: Schneller Kopf

Wenn ein Swift-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, um die Existenz eines Kontos, Containers oder Objekts zu überprüfen und alle relevanten Metadaten abzurufen. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Vorgänge an Konten und Containern umfassen dieses Feld nicht.

Code	Feld	Beschreibung
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
RSLT	Ergebniscode	Ergebnis der HEAD-Transaktion. Ergebnis ist immer: SUCS: erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.
WCON	Schneller Container	Der Name des Swift-Containers. Bei Vorgängen mit Konten ist dieses Feld nicht enthalten.
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Konten und Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.

WPUT: Schnelles PUT

Wenn ein Swift-Client eine PUT-Transaktion ausgibt, wird eine Anforderung zum Erstellen eines neuen Objekts oder Containers gestellt. Diese Nachricht wird vom Server ausgegeben, wenn die Transaktion erfolgreich war.

Code	Feld	Beschreibung
CBID	Inhaltsblockkennung	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, wird dieses Feld auf 0 gesetzt. Vorgänge an Containern umfassen dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Bytes. Vorgänge an Containern umfassen dieses Feld nicht.
HTRH	HTTP-Anforderungsheader	Liste der protokollierten HTTP-Anforderungsheadernamen und -werte, wie während der Konfiguration ausgewählt. `X-Forwarded-For`wird automatisch eingefügt, wenn es in der Anfrage vorhanden ist und wenn die `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungsabsenders (SAIP-Auditfeld).
MTME	Letzte Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Ergebnis ist immer: SUCS: erfolgreich
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Clientanwendung, die die Anfrage gestellt hat.
ZEIT	Zeit	Gesamtverarbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige IP-Adresse des Load Balancers	Wenn die Anfrage von einem vertrauenswürdigen Layer 7-Load Balancer weitergeleitet wurde, die IP-Adresse des Load Balancers.
UUID	Universell eindeutige Kennung	Die Kennung des Objekts innerhalb des StorageGRID -Systems.
WACC	Swift-Konto-ID	Die eindeutige Konto-ID, wie sie vom StorageGRID -System angegeben wird.
WCON	Schneller Container	Der Name des Swift-Containers.

Code	Feld	Beschreibung
WOBJ	Swift-Objekt	Die Swift-Objektkennung. Vorgänge an Containern umfassen dieses Feld nicht.
WUSR	Swift-Kontobenutzer	Der Benutzername des Swift-Kontos, der den Kunden, der die Transaktion durchführt, eindeutig identifiziert.