Monitoring und Fehlerbehebung

StorageGRID software

NetApp
January 15, 2026

This PDF was generated from https://docs.netapp.com/de-de/storagegrid/monitor/index.html on January 15, 2026. Always check docs.netapp.com for the latest.

Inhalt

Überwachung und Fehlerbehebung für ein StorageGRID System

Überwachen Sie das StorageGRID-System

Überwachen Sie ein StorageGRID System

Überwachen Sie Ihr StorageGRID-System regelmäßig, um sicherzustellen, dass es erwartungsgemäß funktioniert.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

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

Über diese Aufgabe

In diesen Anweisungen wird beschrieben, wie Sie:

- "Das Dashboard anzeigen und verwalten"
- "Zeigen Sie die Seite Knoten an"
- "Überwachen Sie diese Aspekte des Systems regelmäßig:"
  - "Systemzustand"
  - "Storage-Kapazität"
  - "Informationslebenszyklus-Management"
  - "Netzwerk- und Systemressourcen"
  - "Mandantenaktivität"
  - "Lastverteilung"
  - "Netzverbundverbindungen"
- "Verwalten von Meldungen"
- "Anzeigen von Protokolldateien"
- "Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server"
- "Verwenden Sie einen externen Syslog-Server" Zur Erfassung von Audit-Informationen
- "Verwenden Sie SNMP für die Überwachung"
- "E/A-Priorisierung ändern"um die relativen Prioritäten für E/A-Operationen zu ändern

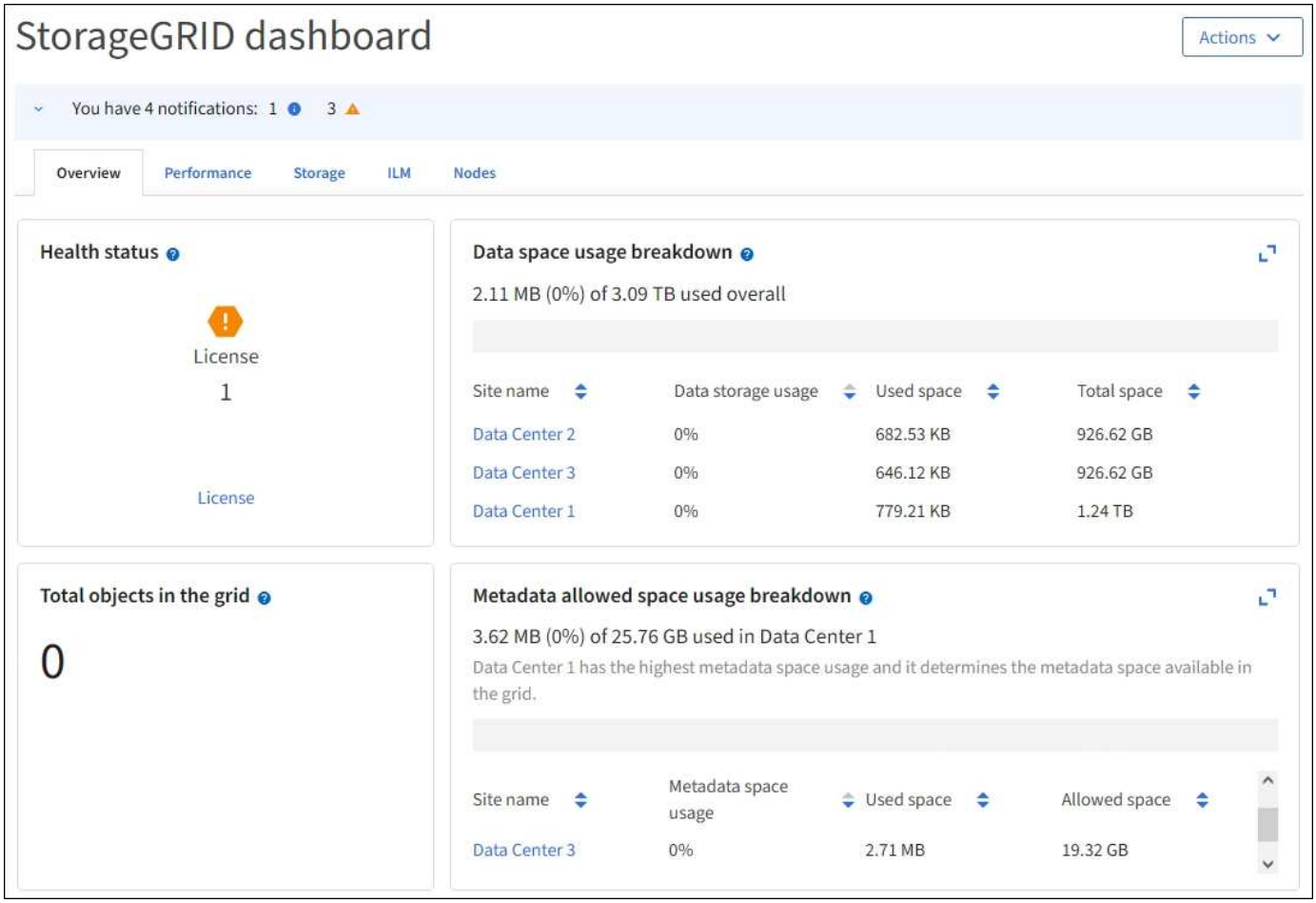
Das Dashboard anzeigen und verwalten

Über das Dashboard können Sie Systemaktivitäten auf einen Blick überwachen. Sie können benutzerdefinierte Dashboards erstellen, um die Implementierung von

StorageGRID zu überwachen.

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

Ihr Dashboard kann je nach Systemkonfiguration unterschiedlich sein.



Dashboard anzeigen

Die Konsole besteht aus Registerkarten mit spezifischen Informationen zum StorageGRID System. Jede Registerkarte enthält Informationskategorien, die auf Karten angezeigt werden.

Sie können das vom System bereitgestellte Dashboard wie dargestellt verwenden. Außerdem können Sie benutzerdefinierte Dashboards erstellen, die nur die Registerkarten und Karten enthalten, die für die Überwachung Ihrer Implementierung von StorageGRID relevant sind.

Die vom System bereitgestellten Dashboard-Registerkarten enthalten Karten mit den folgenden Informationstypen:

Im vom System bereitgestellten Dashboard	Enthält
Überblick	Allgemeine Informationen über das Raster, wie aktive Warnmeldungen, Speicherplatznutzung und Gesamtobjekte in der Tabelle.
Performance	Speichernutzung, verwendeter Storage im Zeitverlauf, S3-Vorgänge, Anfragedauer, Fehlerrate.
Storage	Nutzung von Mandantenkontingenten und logischer Speicherplatznutzung. Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten.
ILM	Information Lifecycle Management-Warteschlange und Evaluierungsrate.
Knoten	CPU-, Daten- und Arbeitsspeicherverbrauch pro Node S3-Vorgänge pro Node. Verteilung von Knoten zu Standort.

Einige der Karten können für eine einfachere Anzeige maximiert werden. Wählen Sie das Symbol Maximieren in der oberen rechten Ecke der Karte. Um eine maximierte Karte zu schließen, wählen Sie das Minimieren-Symbol oder wählen **Schließen**.

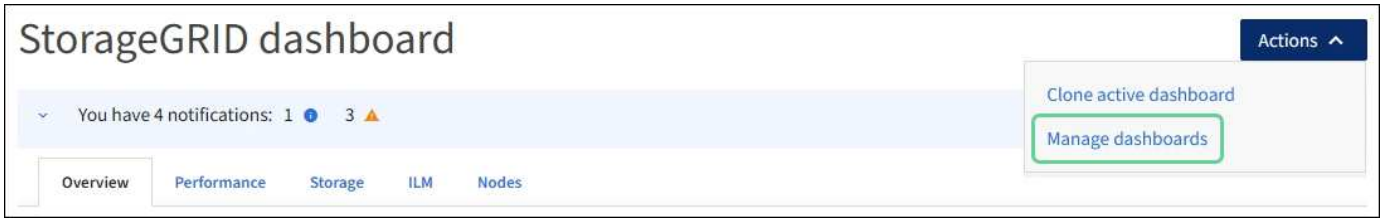
Managen von Dashboards

Wenn Sie Root-Zugriff haben (siehe "Berechtigungen für Admin-Gruppen"), 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 zur Erstellung benutzerdefinierter Dashboards.
- Legen Sie ein aktives Dashboard für einen Benutzer fest. Das aktive Dashboard kann entweder das vom System bereitgestellte Dashboard oder ein benutzerdefiniertes Dashboard sein.
- Legen Sie ein Standard-Dashboard fest, das allen Benutzern angezeigt wird, es sei denn, sie aktivieren ihr eigenes Dashboard.
- Bearbeiten Sie einen Dashboard-Namen.
- Bearbeiten Sie ein Dashboard, um Registerkarten und Karten hinzuzufügen oder zu entfernen. Sie können mindestens 1 und maximal 20 Registerkarten haben.
- Entfernen Sie ein Dashboard.

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

Um Dashboards zu verwalten, wählen Sie **actions** > **Manage Dashboards**.



Dashboards konfigurieren

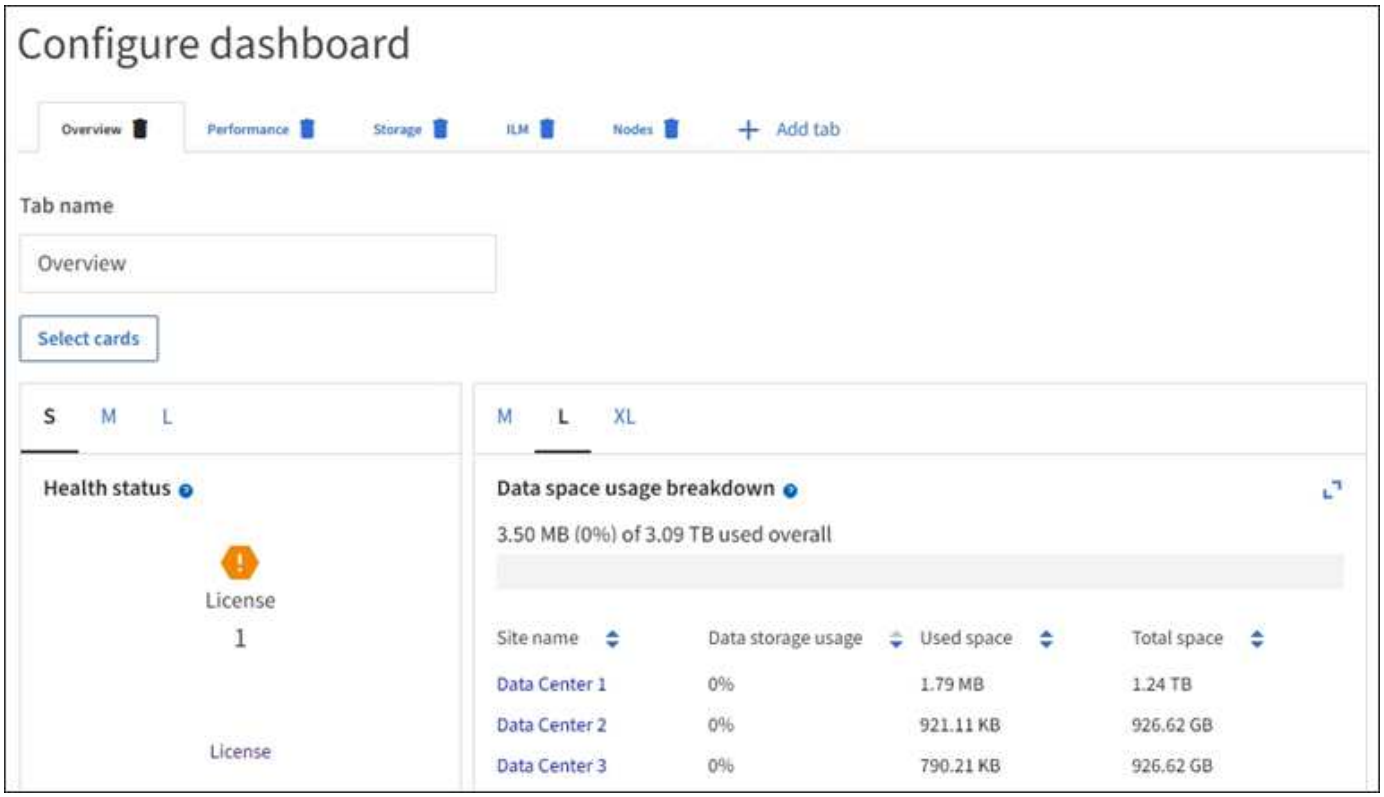
Um ein neues Dashboard durch Klonen des aktiven Dashboards zu erstellen, wählen Sie **actions** > **Clone Active Dashboard**.

Um ein vorhandenes Dashboard zu bearbeiten oder zu klonen, wählen Sie **actions** > **Manage Dashboards**.

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

Folgende Möglichkeiten stehen beim Konfigurieren eines Dashboards zur Verfügung:

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



Zeigen Sie die Seite Knoten an

Zeigen Sie die Seite Knoten an

Wenn Sie detailliertere Informationen über das StorageGRID-System benötigen, als das

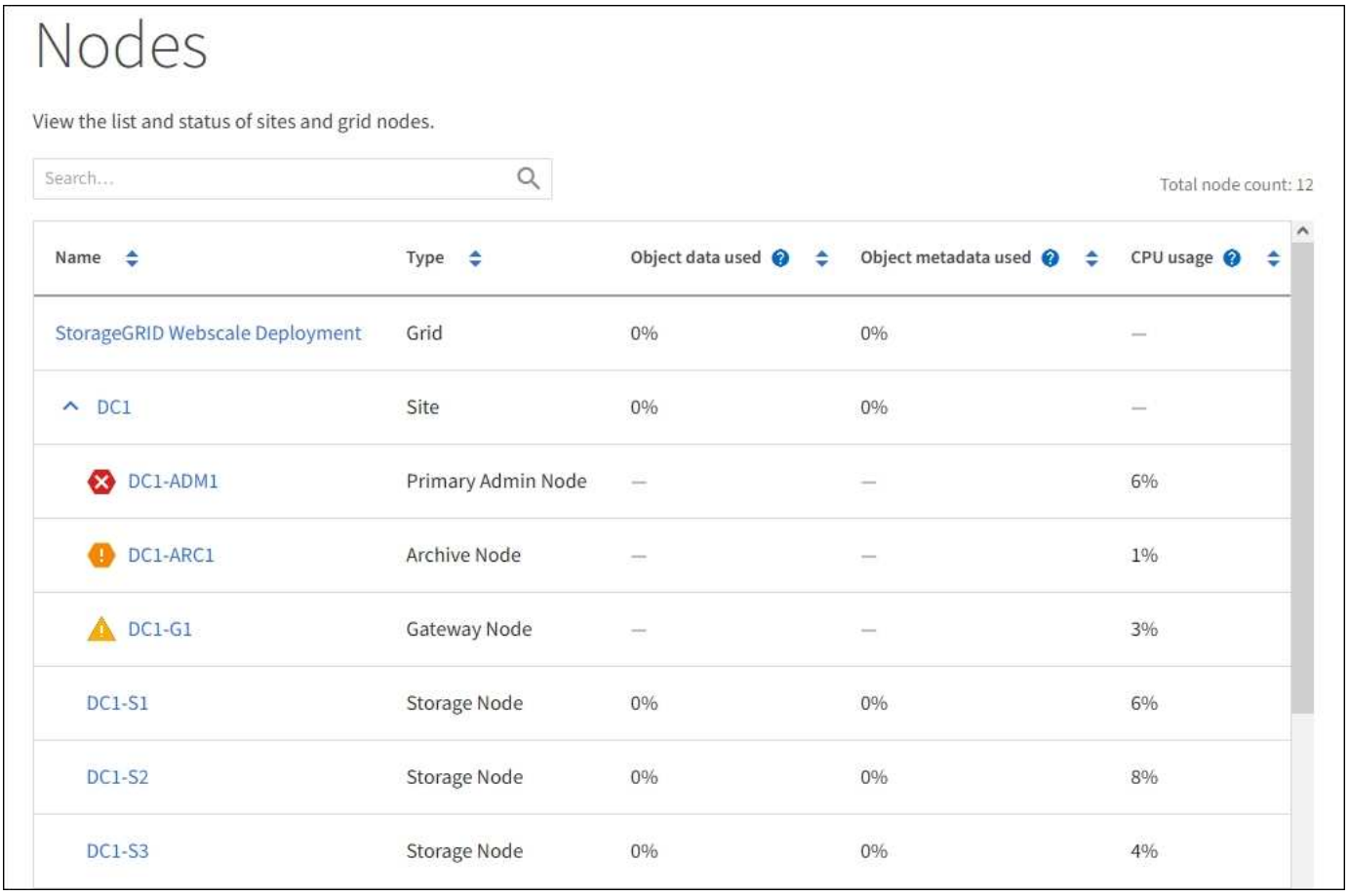
Dashboard bietet, können Sie auf der Seite Nodes Metriken für das gesamte Grid, jeden Standort im Raster und jeden Node an einem Standort anzeigen.

In der Tabelle Nodes werden Zusammenfassungsinformationen für das gesamte Raster, jeden Standort und jeden Node aufgeführt. Wenn ein Knoten getrennt ist oder eine aktive Warnmeldung hat, wird neben dem Knotennamen ein Symbol angezeigt. Wenn der Knoten verbunden ist und keine aktiven Warnmeldungen enthält, wird kein Symbol angezeigt.

Wenn ein Knoten nicht mit dem Raster verbunden ist, z. B. während eines Upgrades oder eines getrennten Status, sind bestimmte Metriken möglicherweise nicht verfügbar oder von den Gesamtsummen des Standorts und des Rasters ausgeschlossen. Nachdem sich ein Node wieder mit dem Grid verbunden hat, warten Sie einige Minuten, bis sich die Werte stabilisieren.

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

Die gezeigten Screenshots sind Beispiele. Die Ergebnisse können je nach StorageGRID-Version variieren.



Symbole für Verbindungsstatus

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

Symbol	Beschreibung	Handeln erforderlich
	Nicht verbunden - Unbekannt Aus einem unbekannten Grund ist die Verbindung zu einem Node unterbrochen, oder Dienste auf dem Node wurden unerwartet heruntergefahren. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren. Die Warnung * kann nicht mit Node* kommunizieren. Andere Warnmeldungen können ebenfalls aktiv sein.	Erfordert sofortige Aufmerksamkeit. "Wählen Sie jede Warnmeldung aus" Und befolgen Sie die empfohlenen Maßnahmen. Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten. **Hinweis**: Ein Knoten kann während des verwalteten Herunterfahrens als Unbekannt erscheinen. In diesen Fällen können Sie den Status Unbekannt ignorieren.
	Nicht verbunden - Administrativ unten Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise auch aktiv. Aufgrund des zugrunde liegenden Problems sind diese Nodes oft ohne Eingriff wieder online.	Ermitteln Sie, ob Warnmeldungen Auswirkungen auf diesen Node haben. Wenn eine oder mehrere Warnungen aktiv sind, "Wählen Sie jede Warnmeldung aus" und befolgen Sie die empfohlenen Maßnahmen.

Wenn ein Knoten vom Raster getrennt wird, liegt möglicherweise eine zugrunde liegende Warnmeldung vor, aber nur das Symbol „nicht verbunden“ wird angezeigt. Um die aktiven Warnmeldungen für einen Node anzuzeigen, wählen Sie den Node aus.

Warnungssymbole

Wenn eine aktive Warnmeldung für einen Node vorhanden ist, wird neben dem Node-Namen eines der folgenden Symbole angezeigt:

Kritisch: Es existiert eine anormale Bedingung, die den normalen Betrieb eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen.

Major: Es gibt einen anormalen Zustand, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für einen kritischen Alarm nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet.

⚠ **Minor**: Das System funktioniert normal, aber es gibt einen ungewöhnlichen Zustand, der die Fähigkeit des Systems beeinflussen könnte, wenn es weitergeht. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.

Zeigt Details zu einem System, Standort oder Node an

Um die in der Tabelle Knoten angezeigten Informationen zu filtern, geben Sie einen Suchstring in das Feld **Suche** ein. Sie können nach Systemnamen, Anzeigenamen oder Typ suchen (z. B. **gat** eingeben, um alle Gateway-Knoten schnell zu finden).

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

- Wählen Sie den Grid-Namen aus, um eine Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen.
- Wählen Sie einen bestimmten Datacenter-Standort aus, um eine aggregierte Zusammenfassung der Statistiken für alle Nodes an diesem Standort anzuzeigen.
- Wählen Sie einen bestimmten Node aus, um detaillierte Informationen zu diesem Node anzuzeigen.

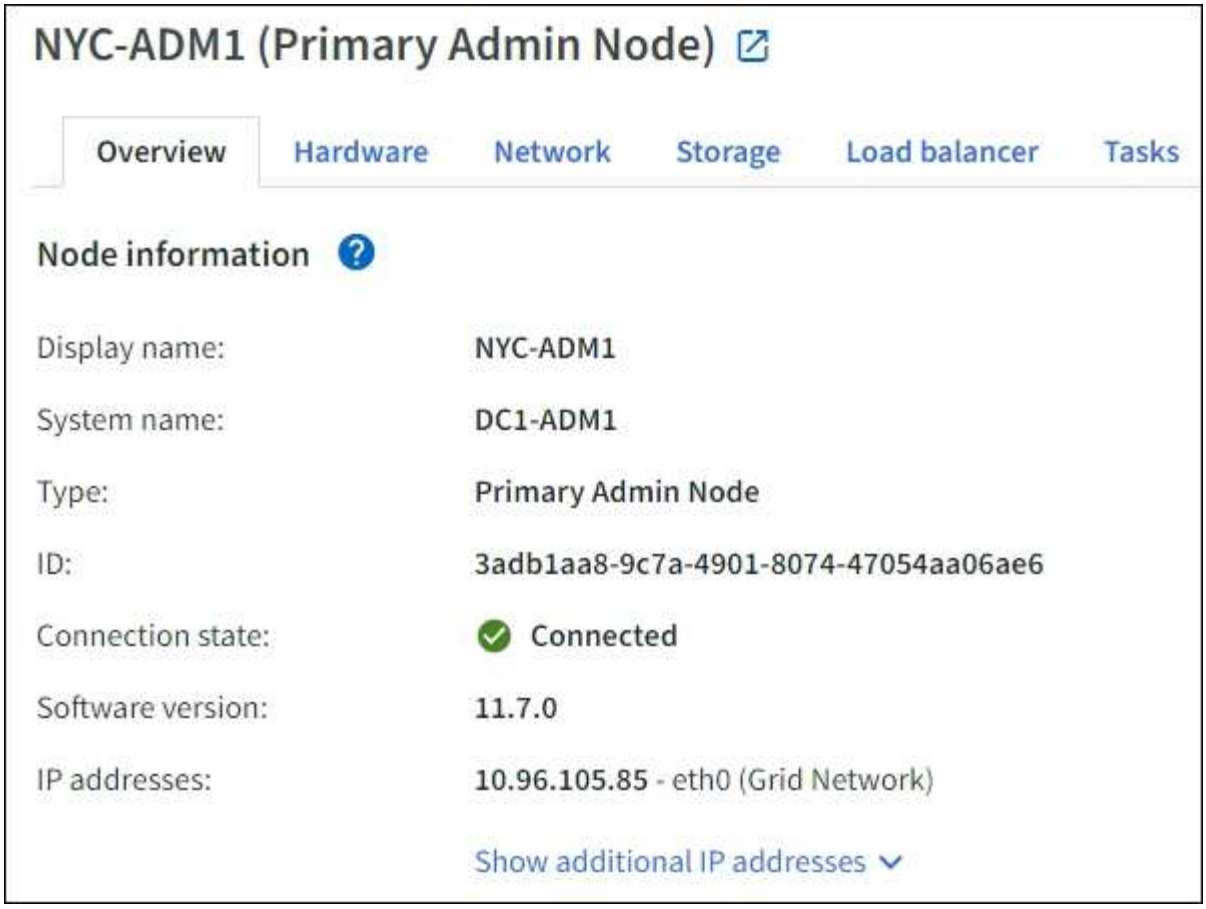
Zeigen Sie die Registerkarte Übersicht an

Die Registerkarte Übersicht enthält grundlegende Informationen zu den einzelnen Knoten. Es werden zudem alle Meldungen angezeigt, die derzeit den Node betreffen.

Die Registerkarte Übersicht wird für alle Knoten angezeigt.

Node-Informationen

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 das "Benennen Sie Raster, Standorte und Nodes um" Verfahren, um diesen Wert zu aktualisieren.
- **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 Typ des Knotens — Admin-Knoten, primärer Admin-Knoten, Speicher-Knoten 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 schwersten Zustand wird angezeigt.
  - **Unbekannt**: aus einem unbekannten Grund ist der Knoten nicht mit dem Grid verbunden, oder ein oder mehrere Dienste sind unerwartet ausgefallen. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen, der Strom ist ausgefallen oder ein Dienst ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.

    Ein Node wird möglicherweise während des verwalteten Herunterfahrens als „Unbekannt“ angezeigt. In diesen Fällen können Sie den Status Unbekannt ignorieren.

  - **Administrativ unten**: der Knoten ist aus einem erwarteten Grund nicht mit dem Raster verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist

möglicherweise auch aktiv.

- **Connected** : der Knoten ist mit dem Raster 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, die auf dem Speicherknoten verwendet wurden.
- **Software-Version**: Die Version von StorageGRID, die auf dem Knoten installiert ist.
- **HA-Gruppen**: Nur für Admin-Node und Gateway-Nodes. 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.

Meldungen

Im Abschnitt Warnungen der Registerkarte Übersicht werden alle aufgelistet"Warnmeldungen, die sich derzeit auf diesen Knoten auswirken, die nicht stummgeschaltet wurden". Wählen Sie den Namen der Warnmeldung aus, um weitere Details und empfohlene Aktionen anzuzeigen.

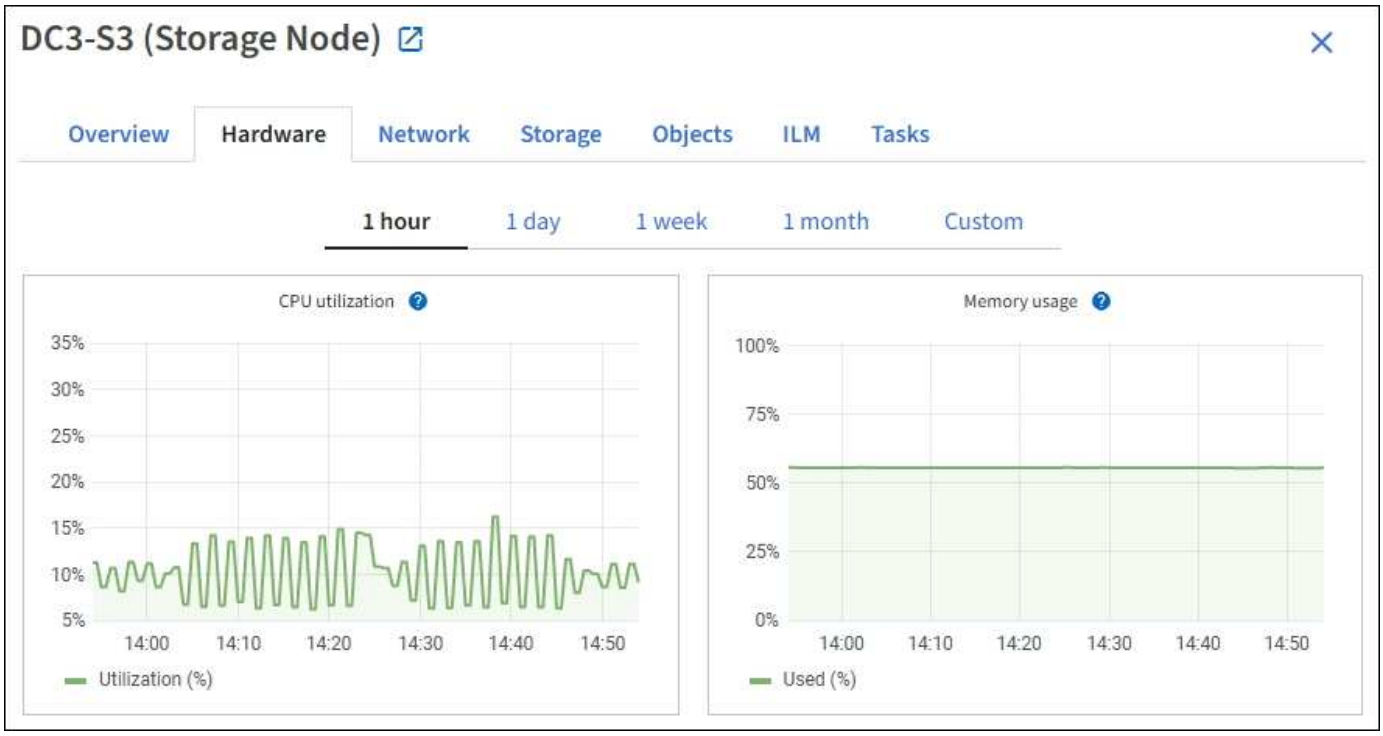
Warnungen sind auch für enthalten"Status der Node-Verbindung".

Zeigen Sie die Registerkarte Hardware an

Auf der Registerkarte Hardware werden für jeden Node CPU-Auslastung und Arbeitsspeicherauslastung sowie zusätzliche Hardware-Informationen über Appliances angezeigt.

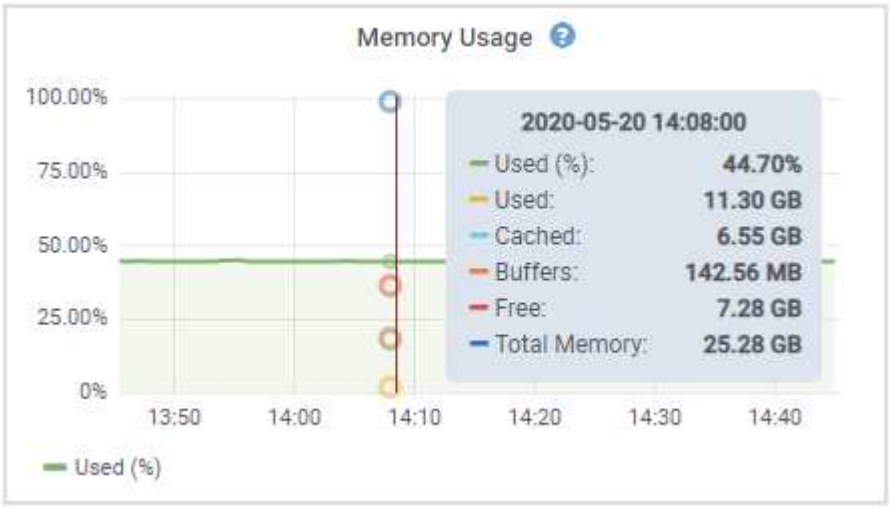
> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispielbildern auf dieser Seite überein.

Die Registerkarte Hardware wird für alle Nodes angezeigt.



Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.

Um Details zur CPU-Auslastung und Speicherauslastung anzuzeigen, setzen Sie den Mauszeiger auf die einzelnen Diagramme.



Wenn der Knoten ein Appliance-Node ist, enthält diese Registerkarte auch einen Abschnitt mit weiteren Informationen zur Appliance-Hardware.

Zeigen Sie Informationen zu Appliance Storage Nodes an

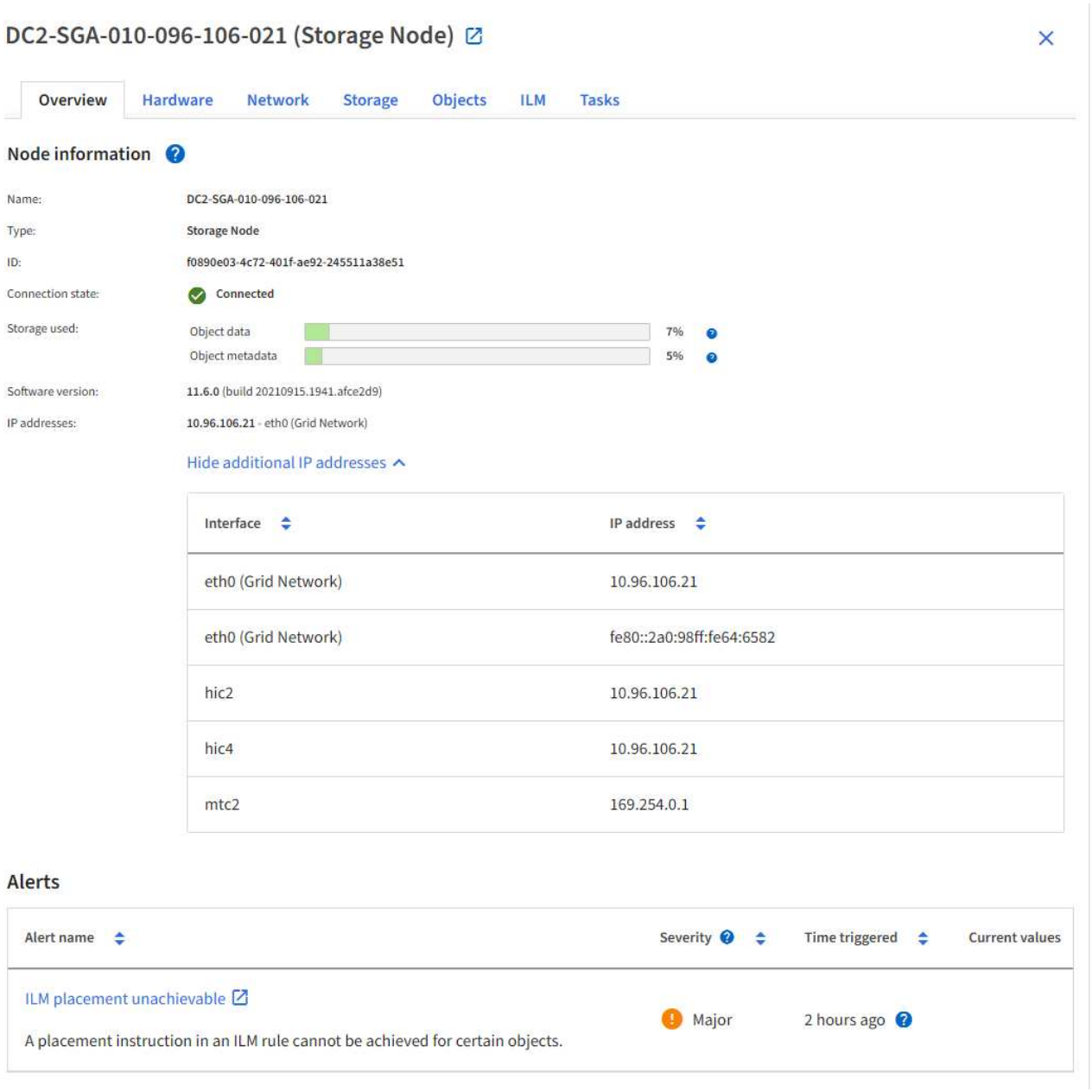
Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplattengeräte- und Netzwerkressourcen für jeden Appliance Storage Node aufgeführt. Außerdem können Sie den Arbeitsspeicher, die Storage-Hardware, die Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen und empfangen und übertragen Daten.

Schritte

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

   Im Abschnitt Node-Informationen auf der Registerkarte Übersicht werden zusammenfassende Informationen für den Node, z. B. Name, Typ, ID und Verbindungsstatus des Node, angezeigt. Die Liste der IP-Adressen umfasst den Namen der Schnittstelle für jede Adresse:

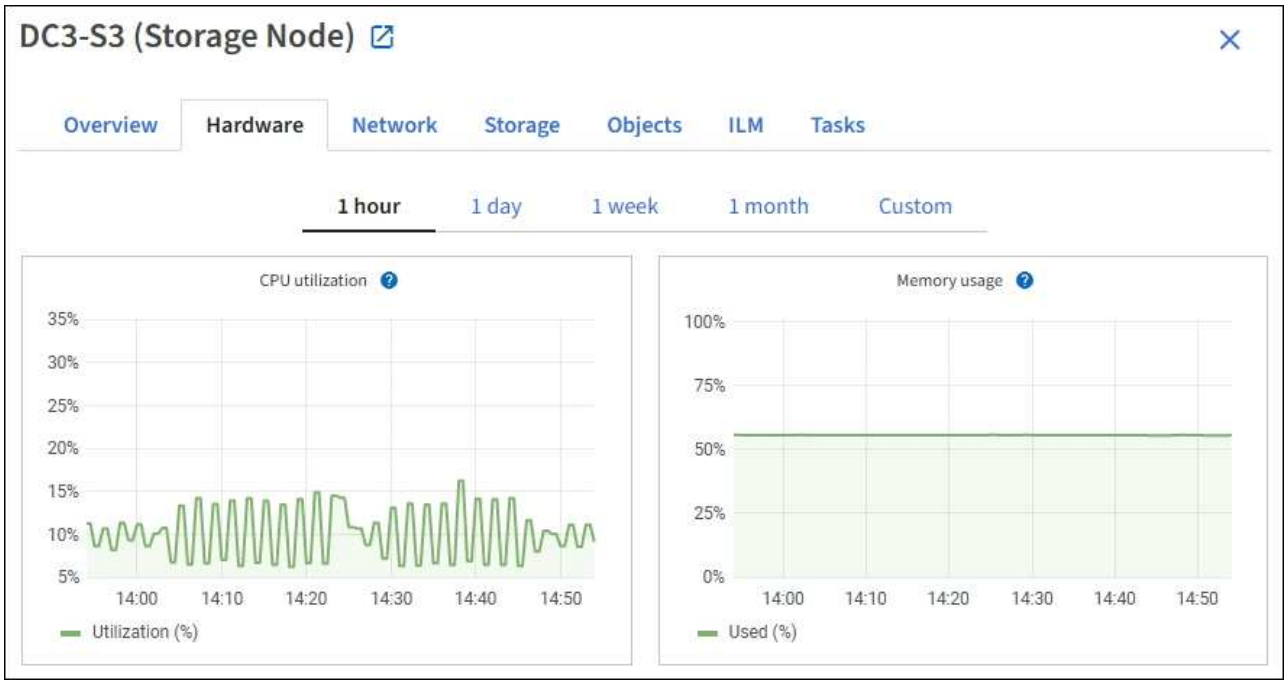
   - **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk.
   - **Hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID-Grid-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
   - **mtc**: Einer der physischen 1-GbE-Ports auf der Appliance. Eine oder mehrere mtc-Schnittstellen bilden die StorageGRID Admin-Netzwerkschnittstelle (eth1). Für den Techniker im Rechenzentrum können Sie andere mtc-Schnittstellen zur temporären lokalen Konnektivität zur Verfügung stellen.



Im Abschnitt „Meldungen“ der Registerkarte „Übersicht“ werden alle aktiven Meldungen für den Node angezeigt.

3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.

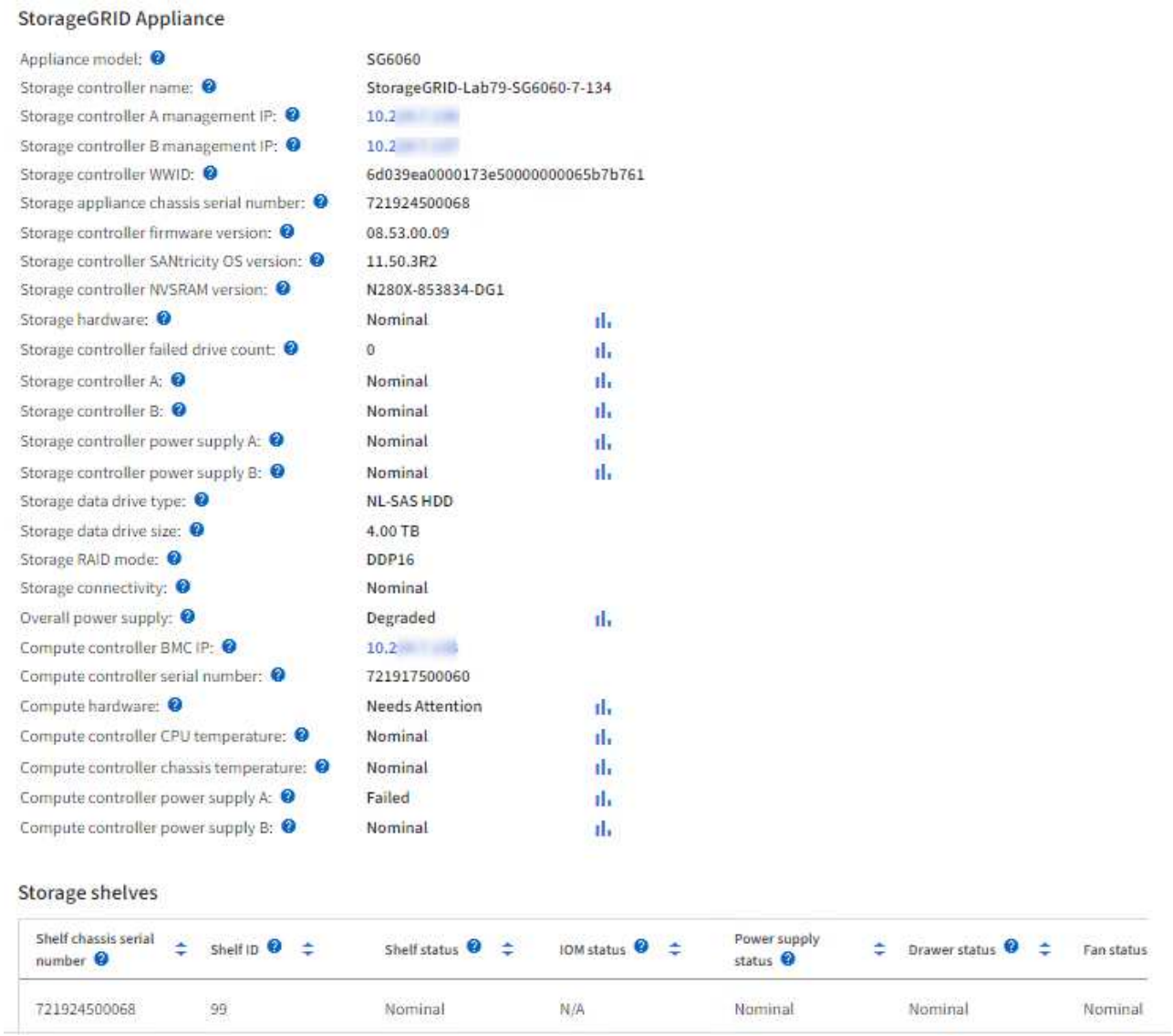
   a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, mit dem Sie Datum und Zeitbereiche festlegen können.



   b. Blättern Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen, z. B. den Modellnamen der Appliance, Controller-Namen, Seriennummern und IP-Adressen und den Status der einzelnen Komponenten.

> Einige Felder, wie BMC IP- und Computing-Hardware des Rechencontrollers, werden nur für Geräte mit dieser Funktion angezeigt.

   Komponenten für Storage-Shelfs und Erweiterungs-Shelfs, wenn sie Teil der Installation sind, werden in einer separaten Tabelle unter der Appliance-Tabelle aufgeführt.



Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance wird in SANtricity OS angezeigt.
Name des Storage Controllers	Der Name dieser StorageGRID-Appliance wird in SANtricity OS angezeigt.
Storage Controller A Management-IP	IP-Adresse für Management-Port 1 auf Storage Controller A. Sie verwenden diese IP, um auf das SANtricity OS zuzugreifen, um Storage-Probleme zu beheben.
Storage-Controller B Management-IP	IP-Adresse für Management-Port 1 auf Storage Controller B. Sie verwenden diese IP, um auf das SANtricity OS zuzugreifen, um Storage-Probleme zu beheben. Einige Appliance-Modelle besitzen keinen Storage Controller B.

Feld in der Appliance-Tabelle	Beschreibung
WWID des Storage Controller	Die weltweite Kennung des im SANtricity OS gezeigten Storage Controllers.
Seriennummer des Storage-Appliance-Chassis	Die Seriennummer des Gehäuses des Geräts.
Version der Storage Controller-Firmware	Die Version der Firmware auf dem Storage Controller für dieses Gerät.
SANtricity OS-Version des Storage-Controllers	Die SANtricity OS-Version von Storage Controller A
NVSRAM-Version des Storage-Controllers	NVSRAM-Version des Storage Controllers, wie vom SANtricity System Manager gemeldet. Wenn bei den SG6060 und SG6160 die NVSRAM-Version zwischen den beiden Controllern nicht übereinstimmt, wird die Version von Controller A angezeigt. Wenn Controller A nicht installiert oder betriebsbereit ist, wird die Version von Controller B angezeigt.
Storage-Hardware	Der Gesamtstatus der Hardware des Storage Controllers. Wenn SANtricity System Manager einen Status als Warnung für die Storage-Hardware meldet, meldet das StorageGRID System diesen Wert ebenfalls. Wenn der Status „erfordert Aufmerksamkeit“ lautet, überprüfen Sie zuerst den Storage Controller mit SANtricity OS. Stellen Sie dann sicher, dass keine weiteren Warnmeldungen für den Compute-Controller vorhanden sind.
Anzahl der Laufwerke bei Ausfall des Storage-Controllers	Die Anzahl der Laufwerke, die nicht optimal sind.
Storage Controller A	Der Status von Speicher-Controller A.
Storage Controller B	Der Status von Storage Controller B. einige Appliance-Modelle verfügen über keinen Storage Controller B.
Netzteil A für Storage-Controller	Der Status von Netzteil A für den Storage Controller.
Netzteil B für Storage Controller	Der Status von Netzteil B für den Speicher-Controller.
Typ des Speicherdatenspeichers	Der Laufwerkstyp in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).

Feld in der Appliance-Tabelle	Beschreibung
Größe der Speicherdatenlaufwerk	Die effektive Größe eines Datenlaufwerks. Beim SG6160 wird auch die Größe des Cache-Laufwerks angezeigt. **Hinweis**: Für Knoten mit Erweiterungs-Shelfs verwenden Sie stattdessen denDatenlaufwerk-Größe für jedes Shelf. Die effektive Laufwerksgröße kann je nach Shelf abweichen.
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.
Storage-Konnektivität	Der Status der Storage-Konnektivität.
Gesamtnetzteil	Der Status aller Netzteile für das Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird nicht für Gerätelodelle angezeigt, die keinen BMC enthalten.
Seriennummer des Computing-Controllers	Die Seriennummer des Compute-Controllers.
Computing-Hardware	Der Status der Compute-Controller-Hardware Dieses Feld wird nicht für Appliance-Modelle angezeigt, die über keine separate Computing-Hardware und Speicher-Hardware verfügen.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute-Controllers.
Temperatur im Computing-Controller-Chassis	Der Temperaturstatus des Compute-Controllers.

+

Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Seriennummer des Shelf Chassis	Die Seriennummer für das Storage Shelf-Chassis.

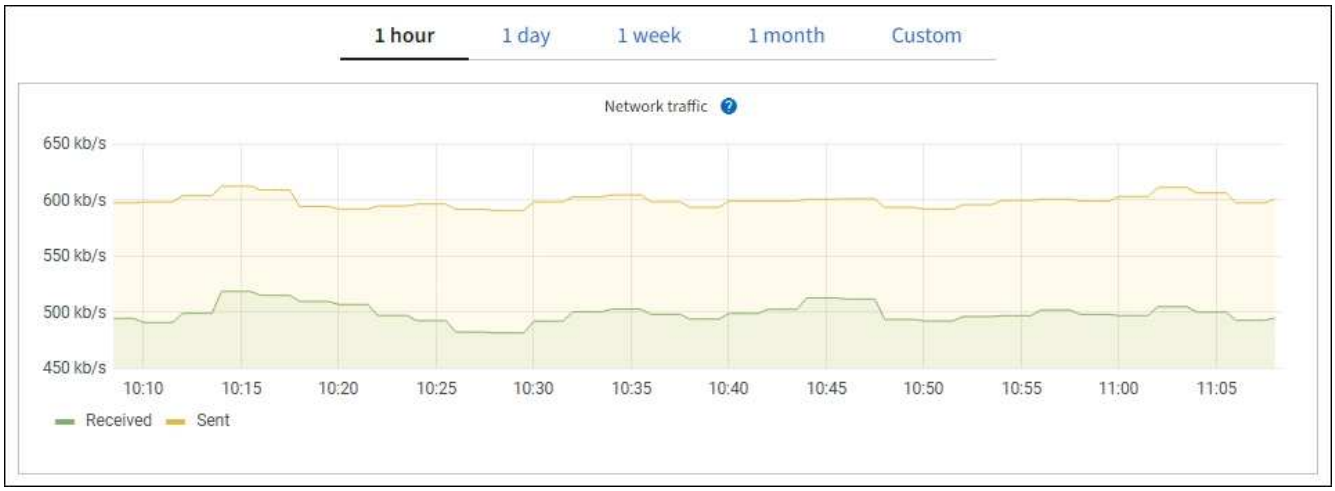
Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Shelf-ID	Die numerische Kennung für das Storage-Shelf. • 99: Storage Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf **Hinweis:** Erweiterungseinschübe gelten nur für die SG6060 und SG6160.
Der Shelf-Status	Der Gesamtstatus des Storage Shelf.
EAM-Status	Der Status der ein-/Ausgangsmodule (IOMs) in beliebigen Erweiterungs-Shelfs. K. A., wenn es sich nicht um ein Erweiterungs-Shelf handelt
Netzteilstatus	Der Gesamtstatus der Netzteile für das Storage Shelf.
Status der Schublade	Der Zustand der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Lüfter im Storage Shelf.
Laufwerksschächte	Die Gesamtzahl der Laufwerksschächte im Storage-Shelf.
Datenlaufwerke	Die Anzahl der Laufwerke im Storage Shelf, die für den Datenspeicher verwendet werden.
Größe des Datenlaufwerks	Die effektive Größe eines Datenlaufwerks im Storage Shelf.
Cache-Laufwerke	Die Anzahl der Laufwerke im Storage Shelf, die als Cache verwendet werden.
Größe des Cache-Laufwerks	Die Größe des kleinsten Cache-Laufwerks im Storage-Shelf. Normalerweise haben Cache-Laufwerke dieselbe Größe.
Konfigurationsstatus	Der Konfigurationsstatus des Storage Shelf.

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

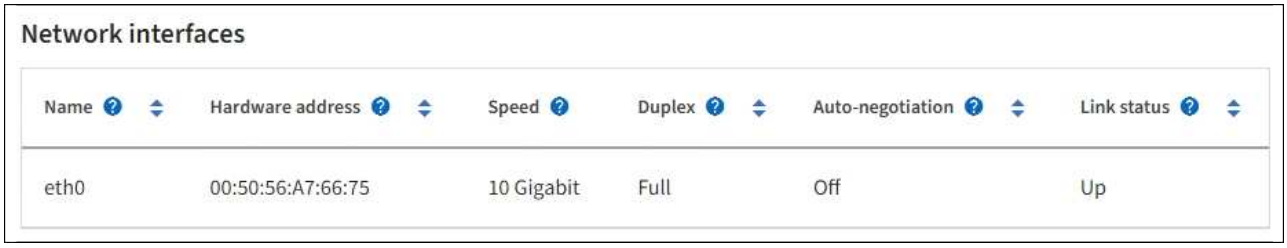
   Wenn ein Status nicht „nominal“ lautet, prüfen Sie alle aktuellen Warnmeldungen. Weitere Informationen zu einigen dieser Hardware-Werte finden Sie auch mit SANtricity System Manager. Informationen zur Installation und Wartung des Geräts finden Sie in den Anweisungen.

4. Wählen Sie **Netzwerk**, um Informationen für jedes Netzwerk anzuzeigen.

Das Diagramm „Netzwerkverkehr“ bietet eine Zusammenfassung des gesamten Netzwerkverkehr.



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 festzustellen, ob die 10/25-GbE-Netzwerkanschlüsse auf dem Gerät für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.

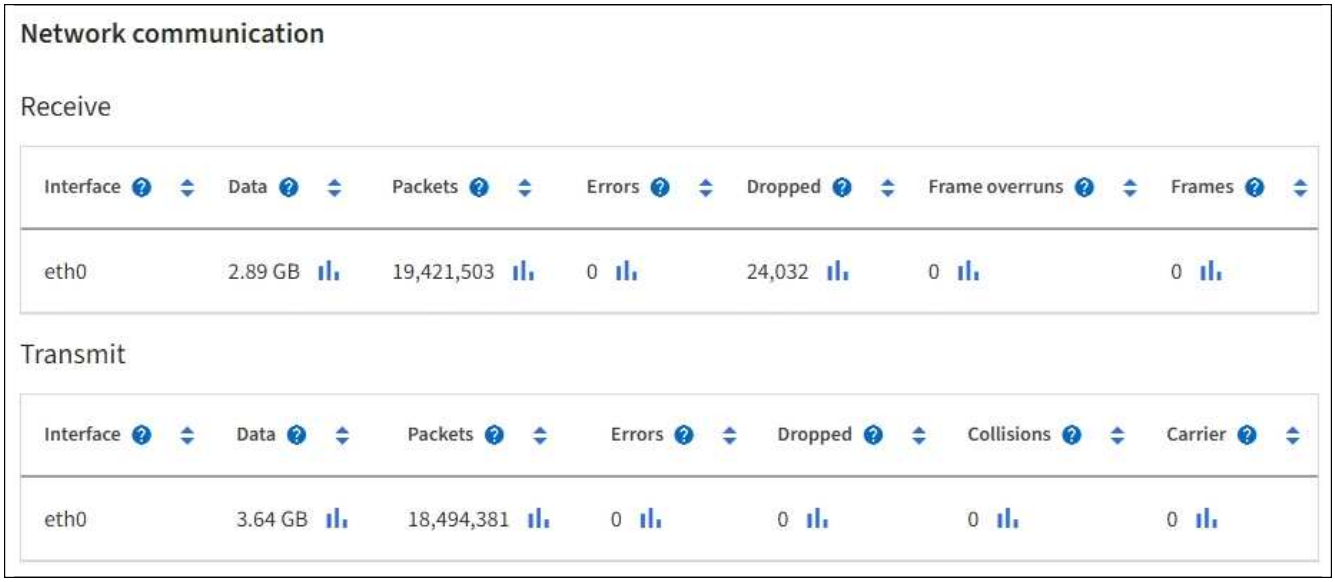
Die in der Tabelle aufgeführten Werte gehen davon aus, dass alle vier Links verwendet werden.

Verbindungsmodus	Bond-Modus	Einzelne HIC-Verbindungsgeschwindigkeit (Schluck1, 2, Schluck3, Schluck4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0,eth2)
Aggregat	LACP	25	100
Fest	LACP	25	50
Fest	Aktiv/Backup	25	25
Aggregat	LACP	10	40
Fest	LACP	10	20
Fest	Aktiv/Backup	10	10

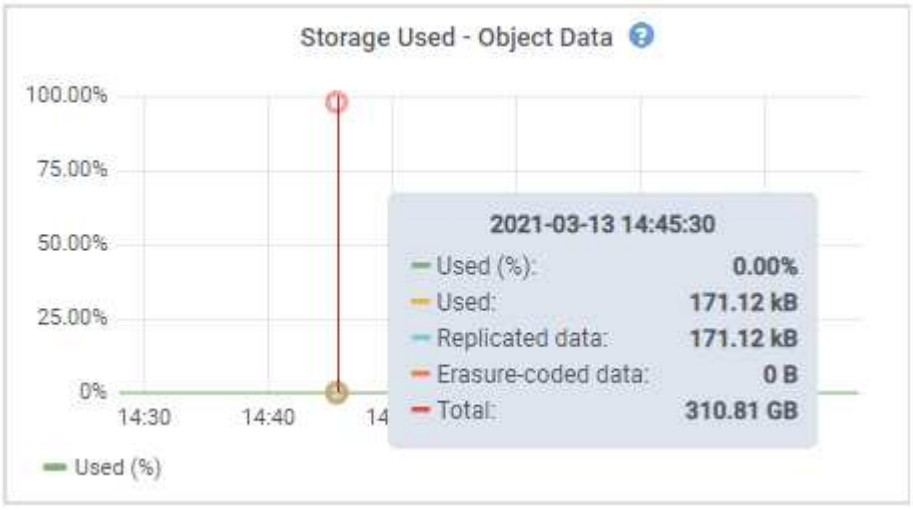
Weitere Informationen zum Konfigurieren der 10/25-GbE-Ports finden Sie unter "Netzwerkverbindungen konfigurieren".

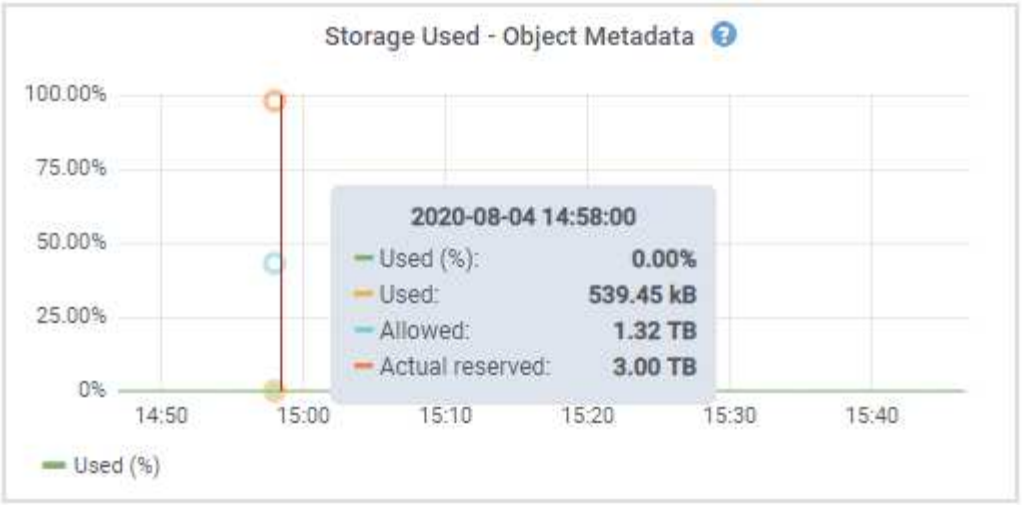
b. Lesen Sie den Abschnitt Netzwerkkommunikation.

   Die Tabellen „Empfangen und Senden“ zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Übertragungs-Metriken.



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

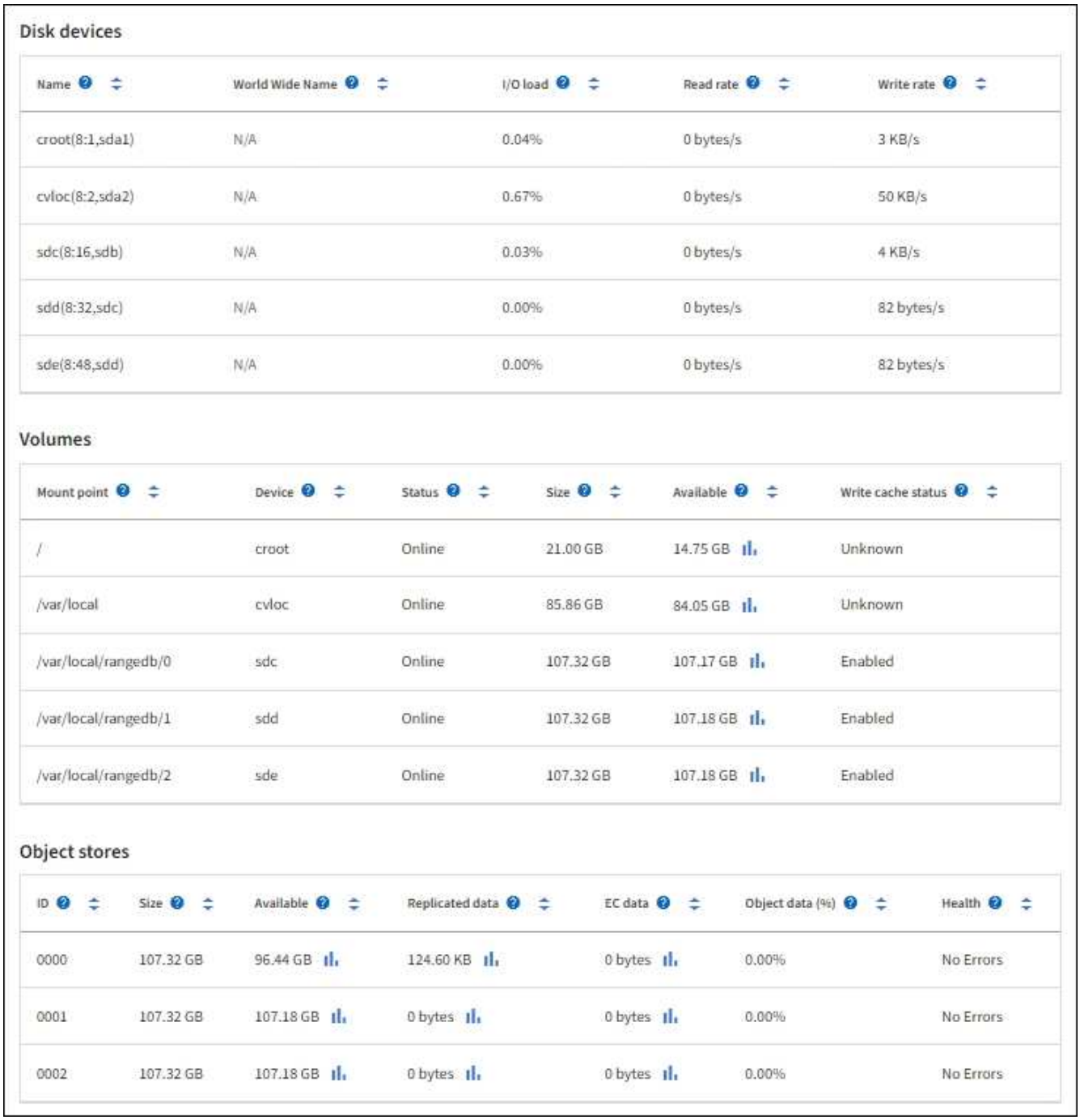




a. Blättern Sie nach unten, um die verfügbaren Speichermengen für jedes Volume und jeden Objektspeicher anzuzeigen.

   Der weltweite Name jeder Festplatte stimmt mit der WWID (World-Wide Identifier) des Volumes überein, die angezeigt wird, wenn Sie die Standard-Volume-Eigenschaften in SANtricity OS (der mit dem Storage Controller der Appliance verbundenen Managementsoftware) anzeigen.

   Um Ihnen bei der Auswertung von Datenträger-Lese- und Schreibstatistiken zu Volume-Mount-Punkten zu helfen, entspricht der erste Teil des Namens, der in der Spalte **Name** der Tabelle Disk Devices (d. h. *sdc*, *sdd*, *sde* usw.) in der Spalte **Gerät** der Tabelle Volumes angezeigt wird.



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

Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an

Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplatten- und Netzwerkressourcen für jede Service-Appliance, die als Admin-Node oder Gateway-Node verwendet wird, aufgeführt. Außerdem können Sie Arbeitsspeicher, Storage-Hardware, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen, Daten empfangen und übertragen.

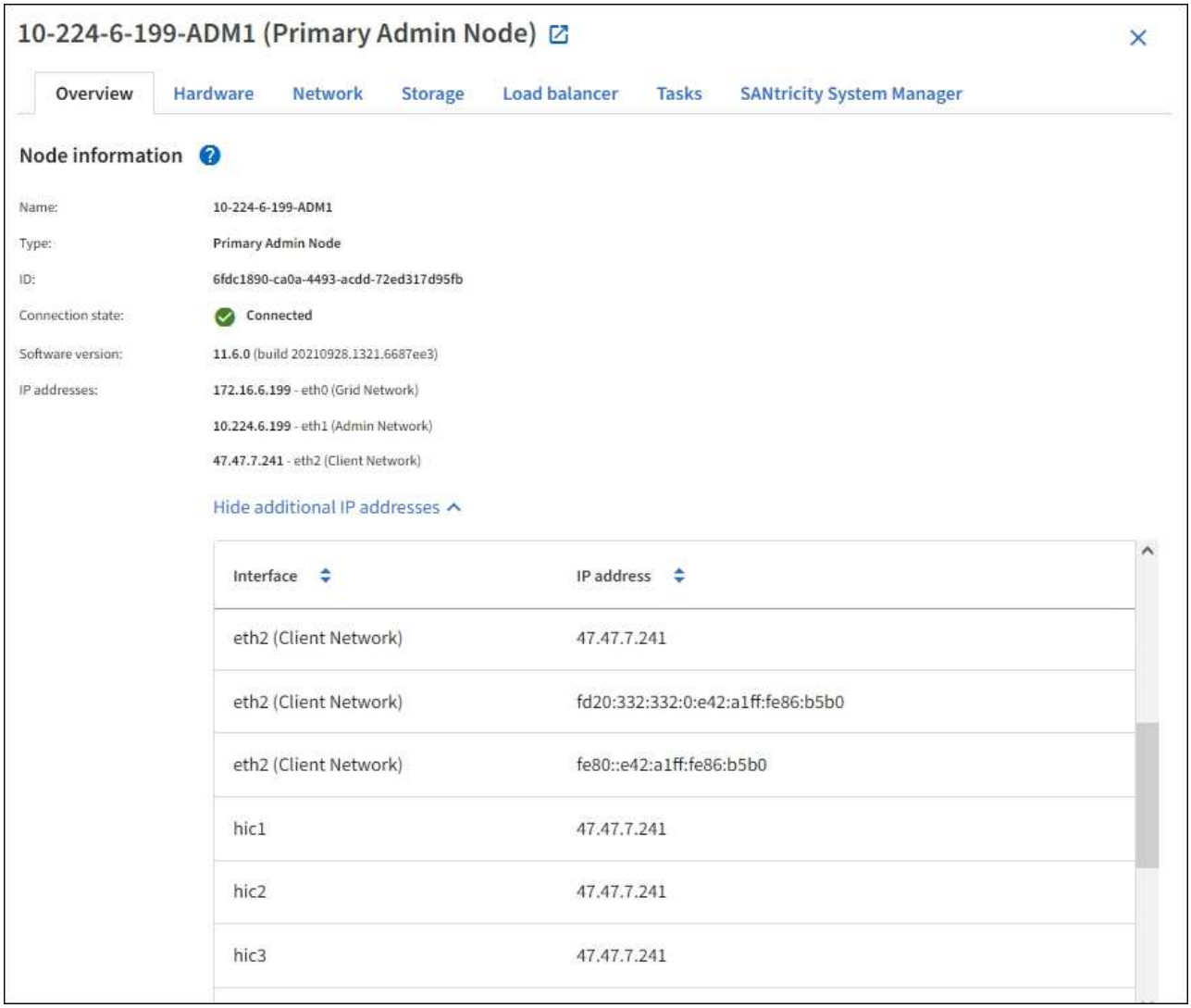
Schritte

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

   Im Abschnitt Node-Informationen auf der Registerkarte Übersicht werden zusammenfassende Informationen für den Node, z. B. Name, Typ, ID und Verbindungsstatus des Node, angezeigt. Die Liste

der IP-Adressen umfasst den Namen der Schnittstelle für jede Adresse:

- **Adlb** und **adlli**: Wird angezeigt, wenn Active/Backup Bonding für die Admin Network Interface verwendet wird
- **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das 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-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
- **mtc**: Einer der physischen 1-GbE-Ports auf der Appliance. Eine oder mehrere mtc-Schnittstellen bilden die Admin-Netzwerkschnittstelle (eth1). Für den Techniker im Rechenzentrum können Sie andere mtc-Schnittstellen zur temporären lokalen Konnektivität zur Verfügung stellen.

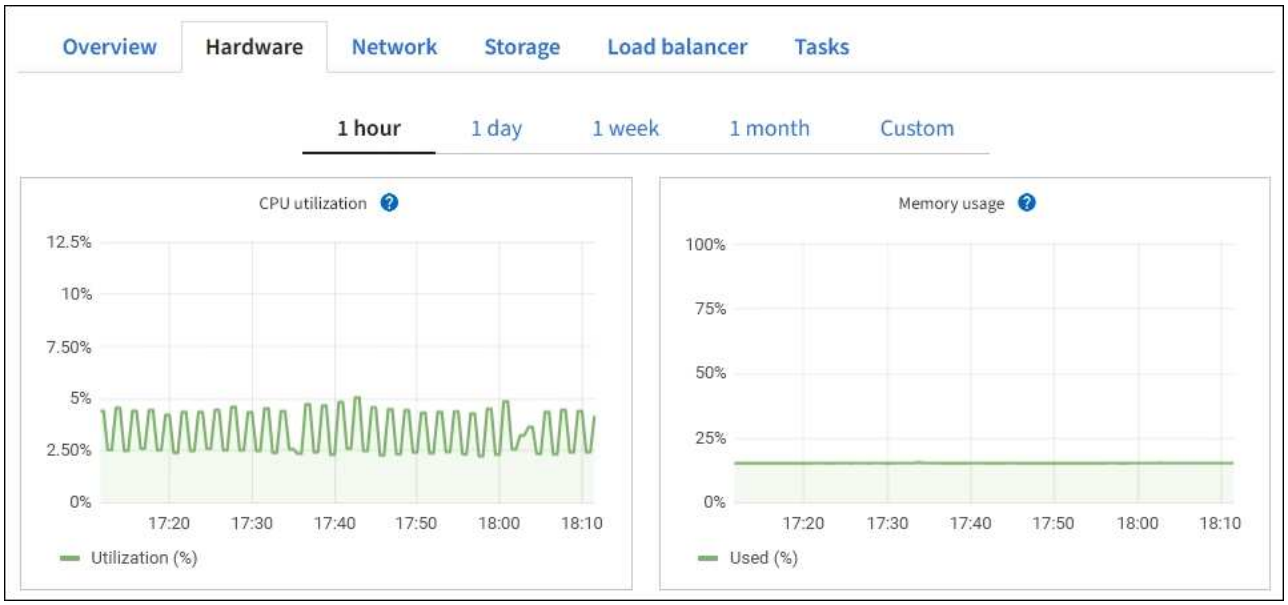


Im Abschnitt „Meldungen“ der Registerkarte „Übersicht“ werden alle aktiven Meldungen für den Node angezeigt.

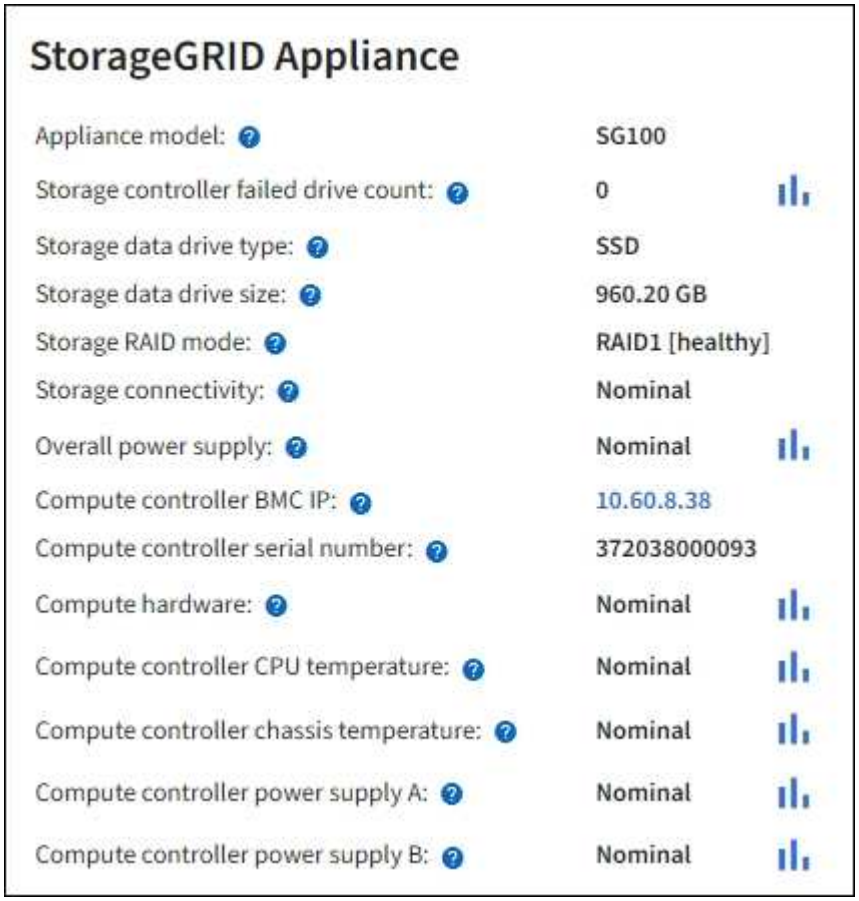
3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.

   a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.



b. Blättern Sie nach unten, um die Komponententabelle für das Gerät anzuzeigen. Diese Tabelle enthält Informationen, z. B. den Modellnamen, die Seriennummer, die Controller-Firmware-Version und den Status jeder Komponente.



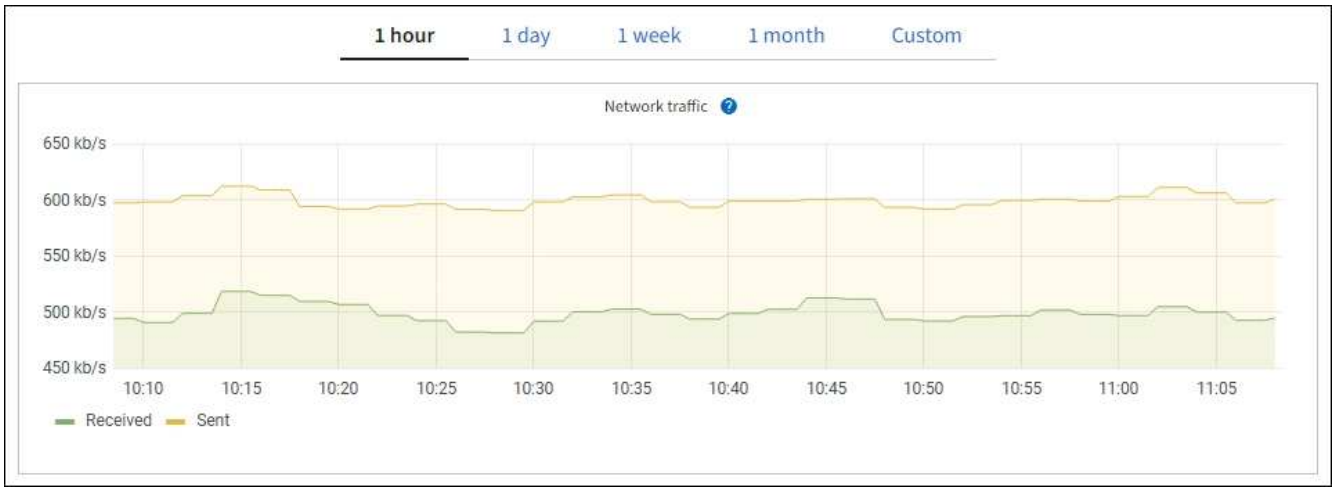
Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance.
Anzahl der Laufwerke bei Ausfall des Storage-Controllers	Die Anzahl der Laufwerke, die nicht optimal sind.
Typ des Speicherdatenspeichers	Der Laufwerkstyp in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe der Speicherdatenlaufwerk	Die effektive Größe eines Datenlaufwerks.
Storage RAID-Modus	Der RAID-Modus für die Appliance.
Gesamtnetzteil	Der Status aller Netzteile im Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird nicht für Gerätelodelle angezeigt, die keinen BMC enthalten.
Seriennummer des Computing-Controllers	Die Seriennummer des Compute-Controllers.
Computing-Hardware	Der Status der Compute-Controller-Hardware
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute-Controllers.
Temperatur im Computing-Controller-Chassis	Der Temperaturstatus des Compute-Controllers.

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

   Wenn ein Status nicht „nominal“ lautet, prüfen Sie alle aktuellen Warnmeldungen.

4. Wählen Sie **Netzwerk**, um Informationen für jedes Netzwerk anzuzeigen.

   Das Diagramm „Netzwerkverkehr“ bietet eine Zusammenfassung des gesamten Netzwerkverkehr.



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

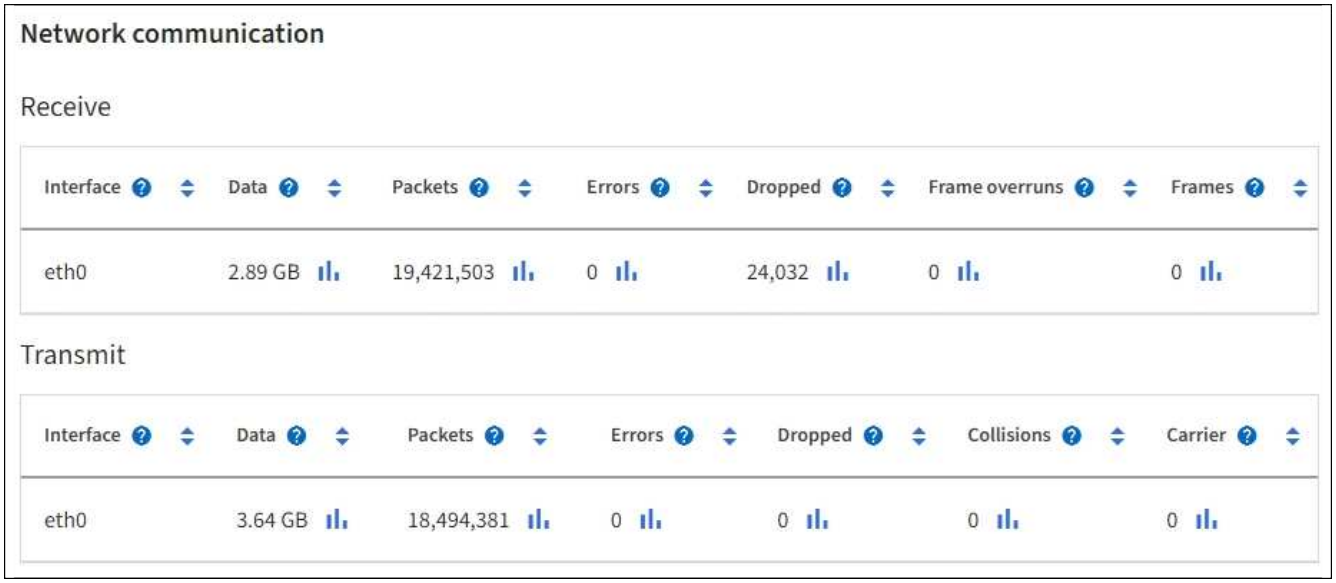
Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle Netzwerkschnittstellen, um festzustellen, ob die vier 40/100-GbE-Netzwerkanschlüsse auf der Appliance für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.

Die in der Tabelle aufgeführten Werte gehen davon aus, dass alle vier Links verwendet werden.

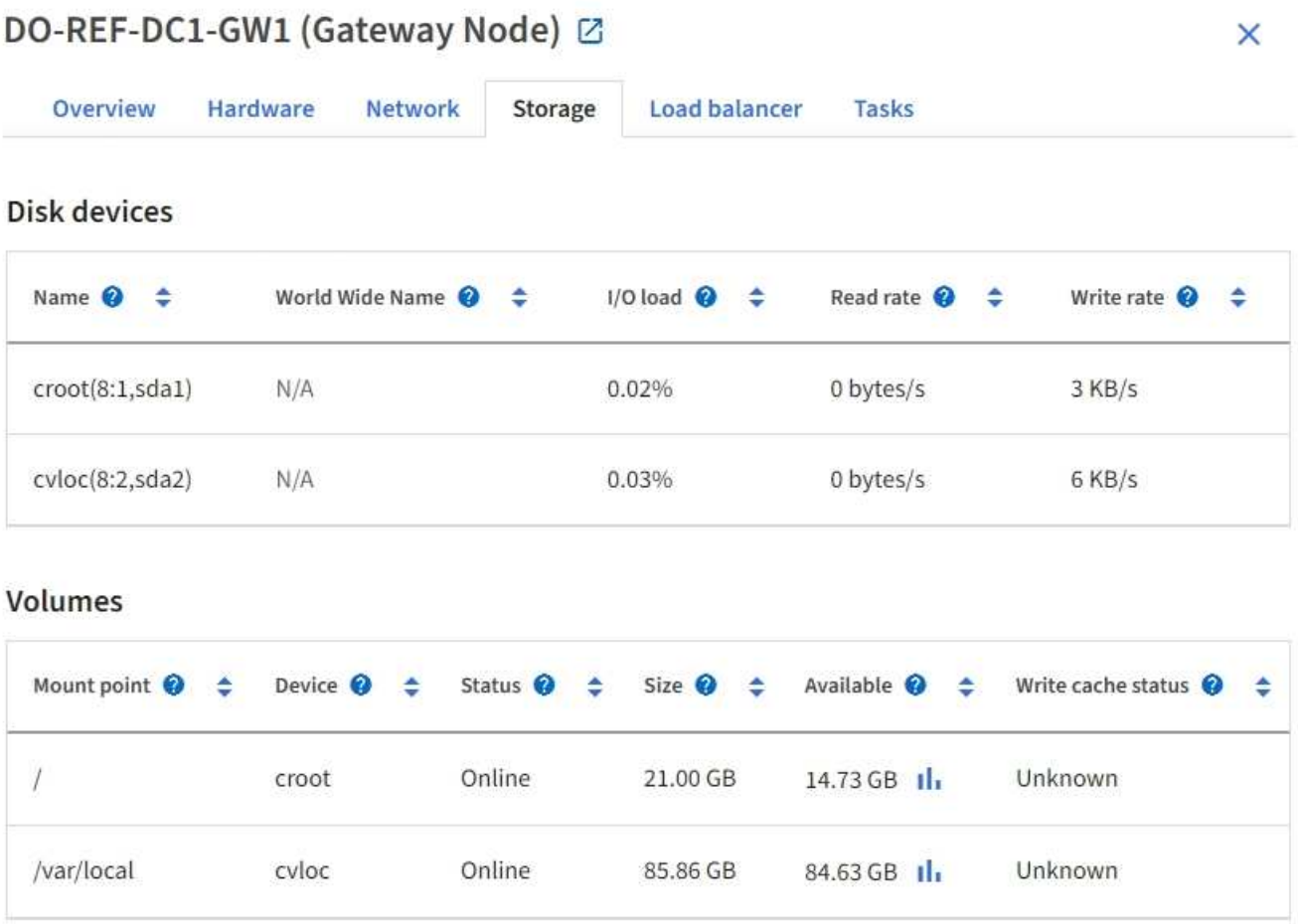
Verbindungsmodus	Bond-Modus	Einzelne HIC-Verbindungsgeschwindigkeit (Schluck1, 2, Schluck3, Schluck4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0, eth2)
Aggregat	LACP	100	400
Fest	LACP	100	200
Fest	Aktiv/Backup	100	100
Aggregat	LACP	40	160
Fest	LACP	40	80
Fest	Aktiv/Backup	40	40

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

Die Tabellen „Empfangen und Senden“ zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Übertragungstabellen.



5. Wählen Sie **Storage** aus, um Informationen zu den Festplattengeräten und Volumes auf der Services Appliance anzuzeigen.



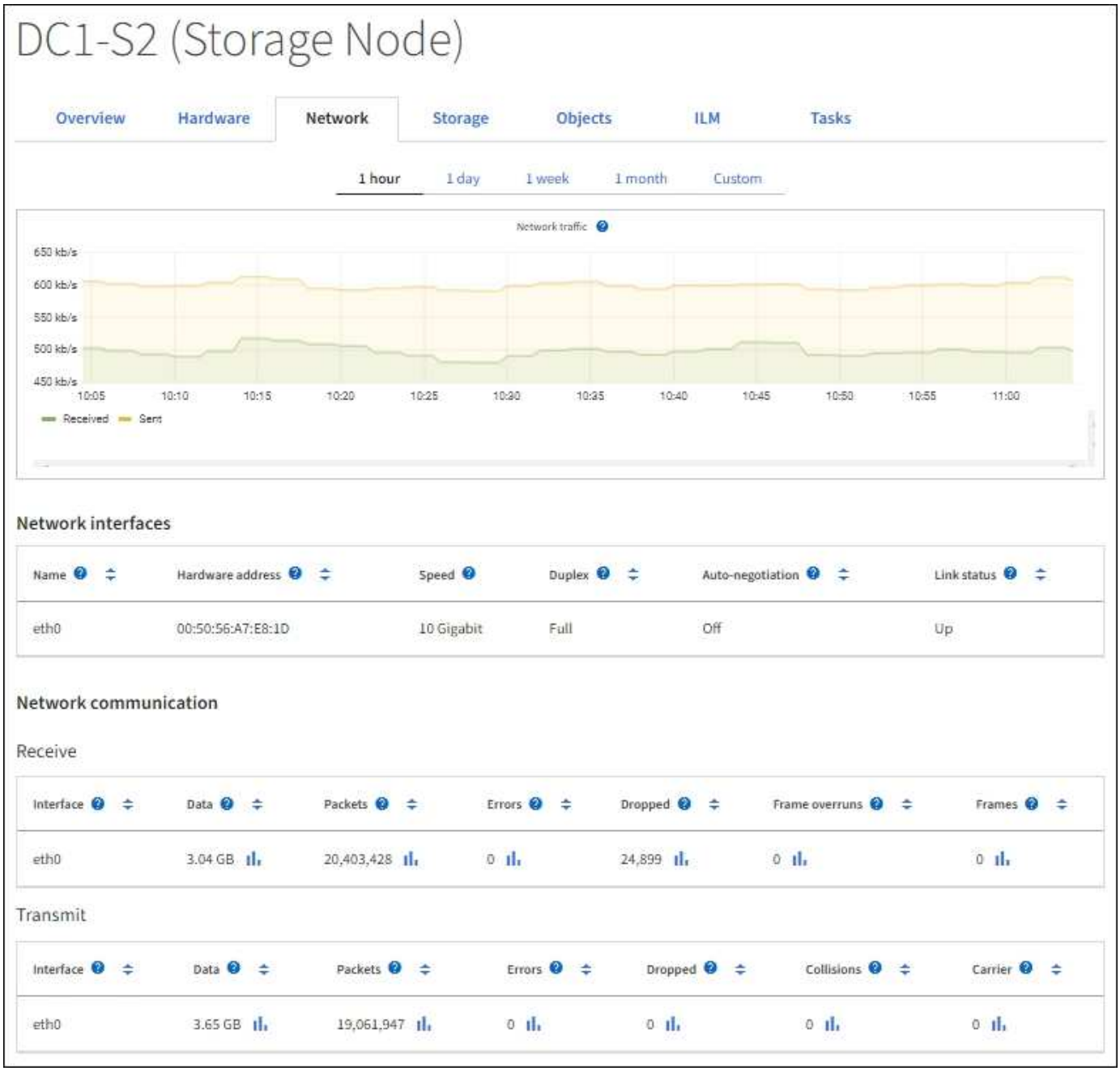
Zeigen Sie die Registerkarte Netzwerk an

Auf der Registerkarte Netzwerk wird ein Diagramm angezeigt, in dem der empfangene und gesendete Netzwerkdatenverkehr über alle Netzwerkschnittstellen auf dem Node, am Standort oder im Raster angezeigt wird.

Die Registerkarte Netzwerk wird für alle Nodes, jeden Standort und das gesamte Raster angezeigt.

Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.

Für Nodes bietet die Tabelle Netzwerkschnittstellen Informationen zu den physischen Netzwerkports jedes Node. Die Netzwerkkommunikationstabelle enthält Details zu den Empfangs- und Übertragungsvorgängen jedes Knotens sowie alle vom Treiber gemeldeten Fehlerzähler.



Verwandte Informationen

"Überwachen Sie Netzwerkverbindungen und Performance"

Öffnen Sie die Registerkarte „Speicher“

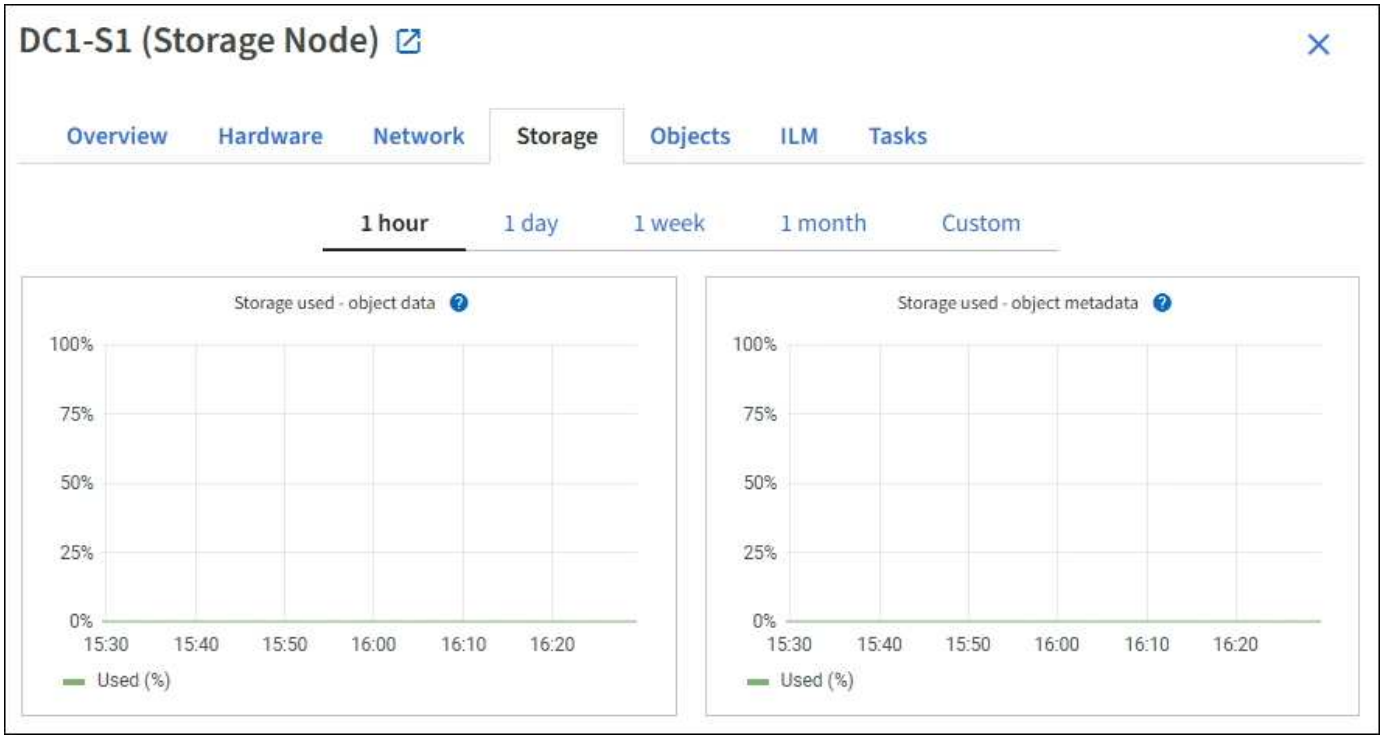
Die Registerkarte „Storage“ fasst Storage-Verfügbarkeit und andere Storage-Metriken zusammen.

Die Registerkarte Storage wird für alle Nodes, jeden Standort und das gesamte Raster angezeigt.

Verwendete Diagramme im Storage

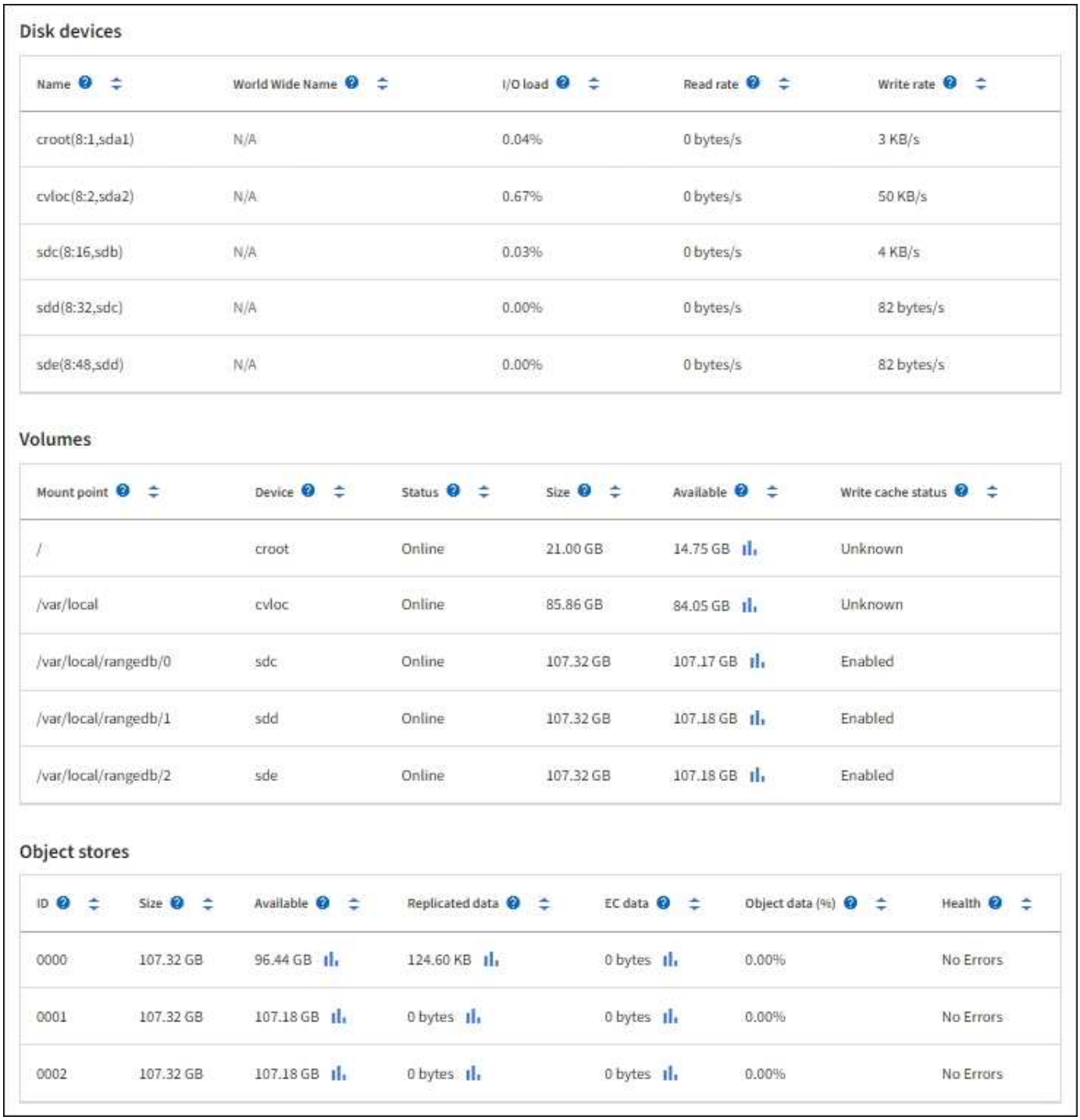
Für Storage-Nodes, jeden Standort und das gesamte Raster enthält die Registerkarte Storage Diagramme, die zeigen, wie viel Storage von Objektdaten und Objekt-Metadaten im Laufe der Zeit verwendet wurde.

Wenn ein Knoten nicht mit dem Raster verbunden ist, z. B. während eines Upgrades oder eines getrennten Status, sind bestimmte Metriken möglicherweise nicht verfügbar oder von den Gesamtsummen des Standorts und des Rasters ausgeschlossen. Nachdem sich ein Node wieder mit dem Grid verbunden hat, warten Sie einige Minuten, bis sich die Werte stabilisieren.



Festplattengeräte, Volumes und Objektspeichern Tabellen

Für alle Nodes enthält die Registerkarte Storage Details zu den Festplattengeräten und Volumes auf dem Node. Für Speicherknoten bietet die Objektspeichertabelle Informationen über jedes 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

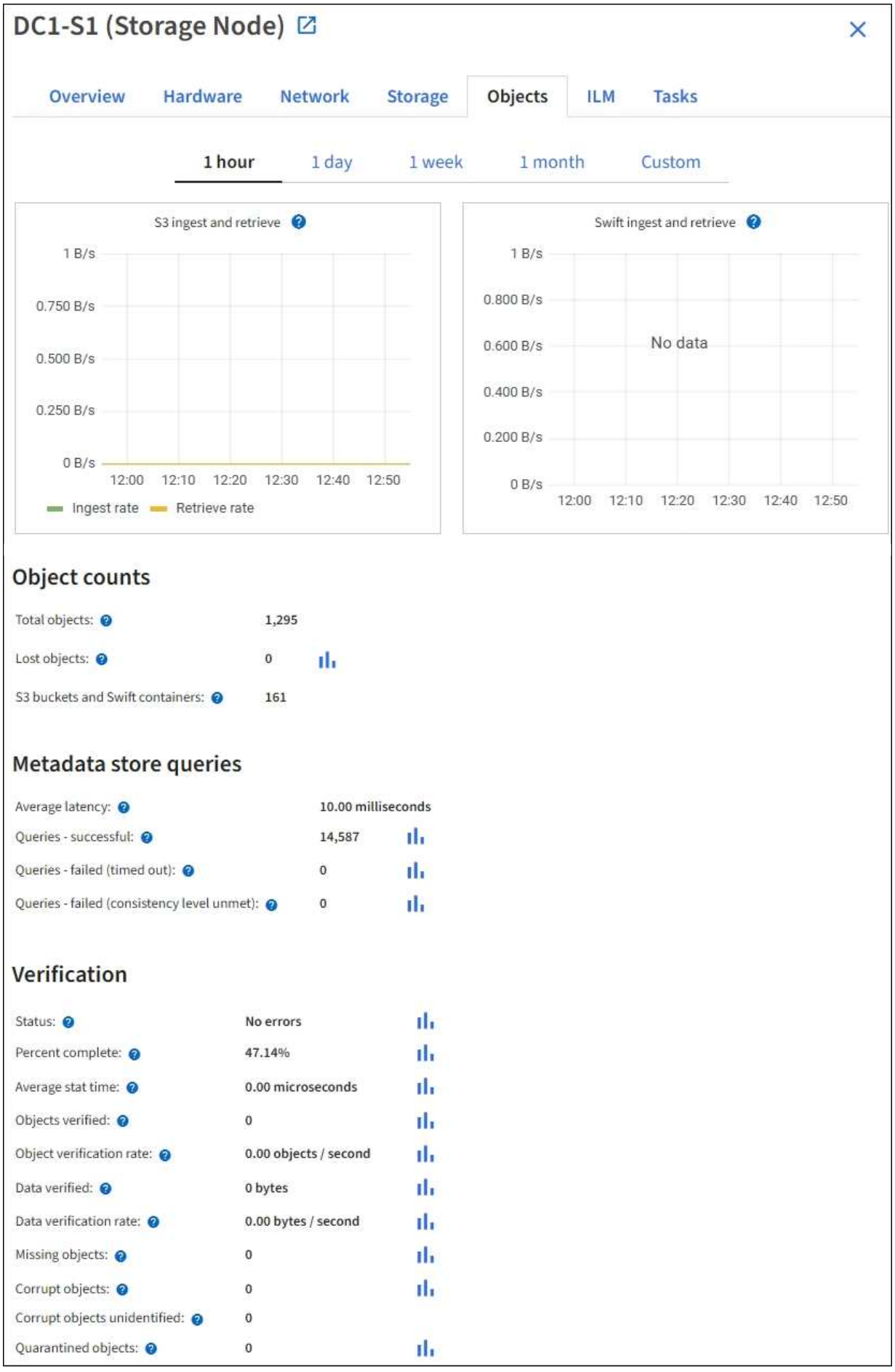
Verwandte Informationen

"Monitoring der Storage-Kapazität"

Zeigen Sie die Registerkarte Objekte an

Die Registerkarte Objekte enthält Informationen über "S3 Datenaufnahme- und -Abrufraten".

Für jeden Storage-Node, jeden Standort und das gesamte Raster wird die Registerkarte Objekte angezeigt. Für Storage-Nodes bietet die Registerkarte Objekte außerdem die Anzahl der Objekte und Informationen zu Metadatenabfragen und zur Hintergrundüberprüfung.

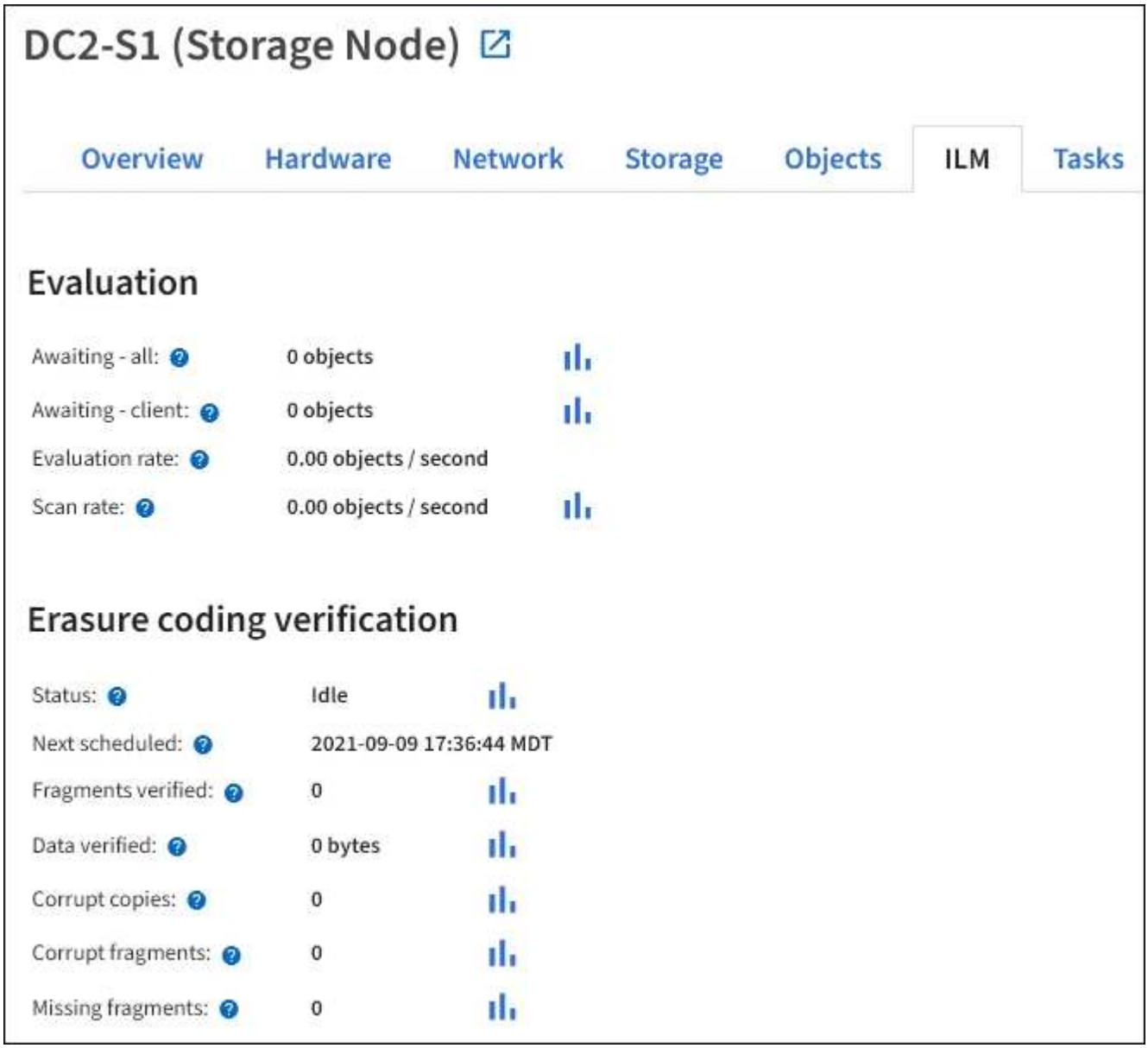

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 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

Zeigen Sie die Registerkarte ILM an

Die Registerkarte ILM bietet Informationen zu Operationen des Information Lifecycle Management (ILM).

Die ILM-Registerkarte wird für jeden Storage-Node, jeden Standort und das gesamte Grid angezeigt. Auf der Registerkarte ILM wird für jeden Standort und das Grid ein Diagramm der ILM-Warteschlange im Laufe der Zeit angezeigt. In dieser Registerkarte wird auch die voraussichtliche Zeit zum Abschluss eines vollständigen ILM-Scans aller Objekte bereitgestellt.

Für Storage-Nodes bietet die Registerkarte ILM Details zur ILM-Bewertung und zur Hintergrundüberprüfung von Objekten, die zur Fehlerkorrektur codiert wurden.



Verwandte Informationen

- "Überwachung des Information Lifecycle Management"
- "StorageGRID verwalten"

Zeigen Sie die Registerkarte Load Balancer an

Die Registerkarte Load Balancer enthält Performance- und Diagnosediagramme zum Betrieb des Load Balancer Service.

Die Registerkarte Load Balancer wird für Admin-Nodes und Gateway-Nodes, jeden Standort und das gesamte Raster angezeigt. Die Registerkarte Load Balancer bietet für jeden Standort eine zusammengefasste Zusammenfassung der Statistiken für alle Nodes an diesem Standort. Die Registerkarte Load Balancer bietet für das gesamte Raster eine zusammengefasste Zusammenfassung der Statistiken für alle Standorte.

Wenn kein I/O durch den Load Balancer-Service ausgeführt wird oder kein Load Balancer konfiguriert ist, wird in den Diagrammen „Keine Daten“ angezeigt.

Datenverkehr anfordern

Dieses Diagramm zeigt einen Mittelwert, der durch 3 Minuten bewegt wird und den Durchsatz der Daten zwischen den Endpunkten des Load Balancer und den Clients, die die Anforderungen erstellen, in Bits pro Sekunde übertragen wird.

Dieser Wert wird beim Abschluss jeder Anfrage aktualisiert. Aus diesem Grund kann sich der Wert von dem Echtzeitdurchsatz bei niedrigen Anfrageraten oder bei sehr langen Anforderungen unterscheiden. Auf der Registerkarte „Netzwerk“ finden Sie eine realistischere Ansicht des aktuellen Netzwerkverhaltens.

Eingehende Anfragerate

Dieses Diagramm zeigt einen 3-minütigen, sich bewegenden Durchschnitt der Anzahl neuer Anfragen pro Sekunde, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Dieser Wert wird aktualisiert, wenn die Kopfzeilen einer neuen Anfrage validiert wurden.

Durchschnittliche Anfragedauer (fehlerfrei)

Dieses Diagramm zeigt einen 3-minütigen versch. Durchschnitt der Anfragedauer und ist nach Anforderungstyp aufgeschlüsselt (GET, PUT, HEAD und DELETE). Jede Anforderungsdauer beginnt, wenn eine Anforderungs-Kopfzeile vom Lastbalancer-Dienst analysiert wird und endet, wenn der vollständige Antwortkörper an den Client zurückgesendet wird.

Fehlerantwortzrate

Dieses Diagramm zeigt einen Mittelwert, der durch 3 Minuten verschoben wird und der Anzahl der Fehlerantworten, die an Clients pro Sekunde zurückgegeben werden, aufgeschlüsselt nach dem Fehlercode.

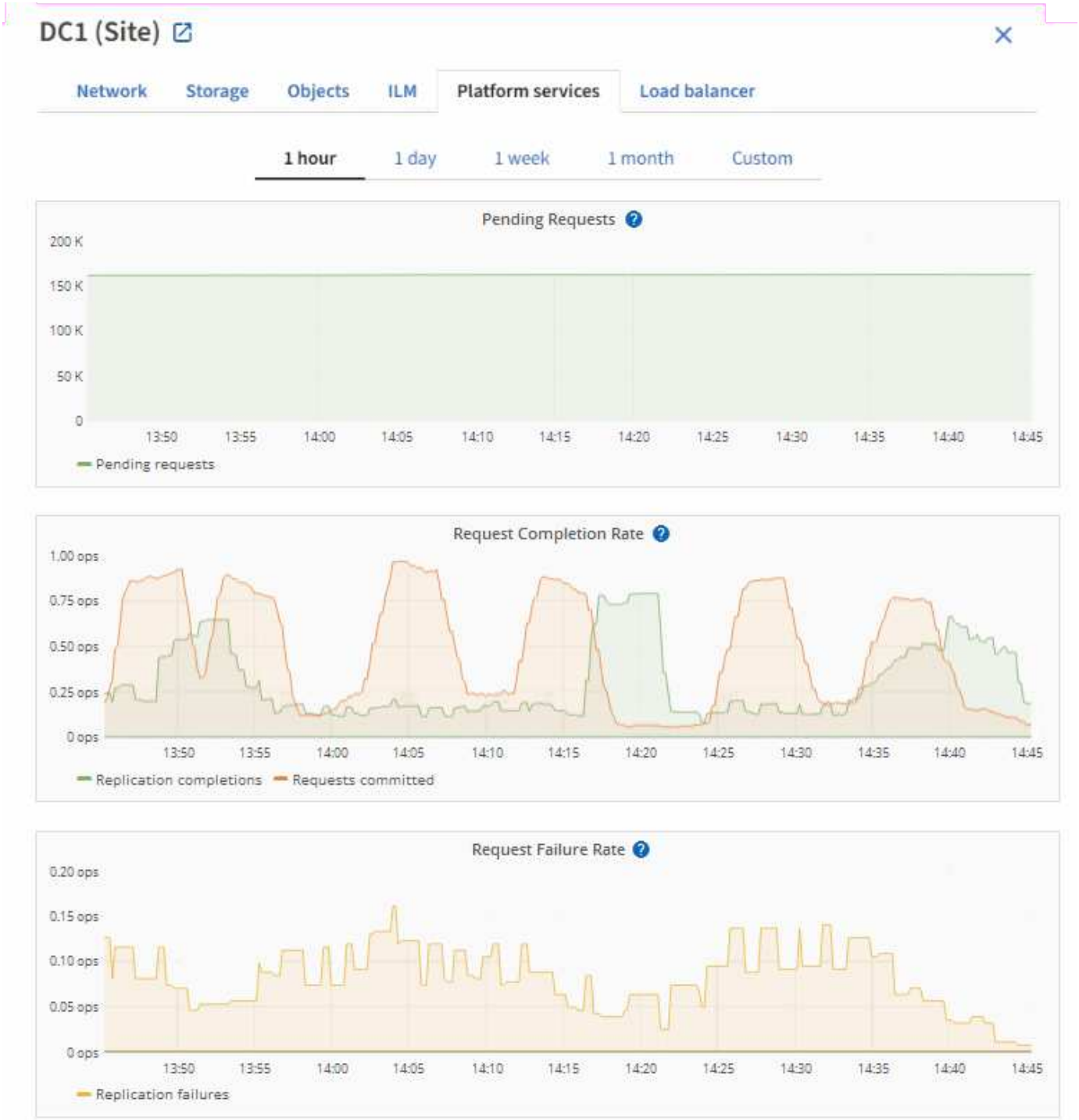
Verwandte Informationen

- "Monitoring von Lastverteilungsvorgängen"
- "StorageGRID verwalten"

Zeigen Sie die Registerkarte Plattformdienste an

Die Registerkarte Plattformdienste enthält Informationen über alle S3-Plattform-Servicevorgänge an einem Standort.

Die Registerkarte Plattformdienste wird für jede Site angezeigt. Diese Registerkarte enthält Informationen zu S3-Plattformdiensten wie CloudMirror-Replizierung und den Suchintegrationsdienst. In Diagrammen auf dieser Registerkarte werden Metriken angezeigt, z. B. die Anzahl der ausstehenden Anfragen, die Abschlussrate der Anfrage und die Rate bei Ausfällen von Anfragen.



Weitere Informationen zu S3-Plattformservices, einschließlich Details zur Fehlerbehebung, finden Sie im "Anweisungen für die Administration von StorageGRID".

Zeigen Sie die Registerkarte Laufwerke verwalten an

Auf der Registerkarte Laufwerke verwalten können Sie auf Details zugreifen und Fehlerbehebungs- und Wartungsaufgaben für Laufwerke in den Appliances durchführen, die diese Funktion unterstützen.

Auf der Registerkarte Laufwerke verwalten können Sie Folgendes tun:

- Zeigen Sie ein Layout der Datenspeicherlaufwerke in der Appliance an
- Zeigen Sie eine Tabelle an, in der die einzelnen Laufwerksorte, -Typen, -Status, -Firmware-Version und -Seriennummer aufgeführt sind
- Führen Sie auf jedem Laufwerk Fehlerbehebungs- und Wartungsfunktionen durch

Um auf die Registerkarte Laufwerke verwalten zuzugreifen, müssen Sie über die verfügen"Zugriffsberechtigung für den Administrator der Storage-Appliance oder den Root-Zugriff".

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

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

Über die Registerkarte „SANtricity System Manager“ können Sie auf SANtricity System Manager zugreifen, ohne den Managementport der Storage Appliance konfigurieren oder verbinden zu müssen. Sie können diese Registerkarte verwenden, um Informationen zur Hardware-Diagnose und -Umgebung sowie Probleme im Zusammenhang mit den Laufwerken zu überprüfen.

> Der Zugriff auf den SANtricity System Manager über den Grid Manager erlaubt in der Regel nur die Überwachung der Appliance-Hardware und die Konfiguration der E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, beispielsweise ein Firmware-Upgrade, gelten nicht für die Überwachung Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie stets die Hardware-Wartungsanweisungen für Ihr Gerät. Informationen zum Aktualisieren der SANtricity-Firmware finden Sie im "Verfahren zur Wartungskonfiguration" für Ihre Storage Appliance.

> Die Registerkarte SANtricity System Manager wird nur für Nodes von Storage-Appliances angezeigt, die die E-Series Hardware verwenden.

Mit SANtricity System Manager sind folgende Vorgänge möglich:

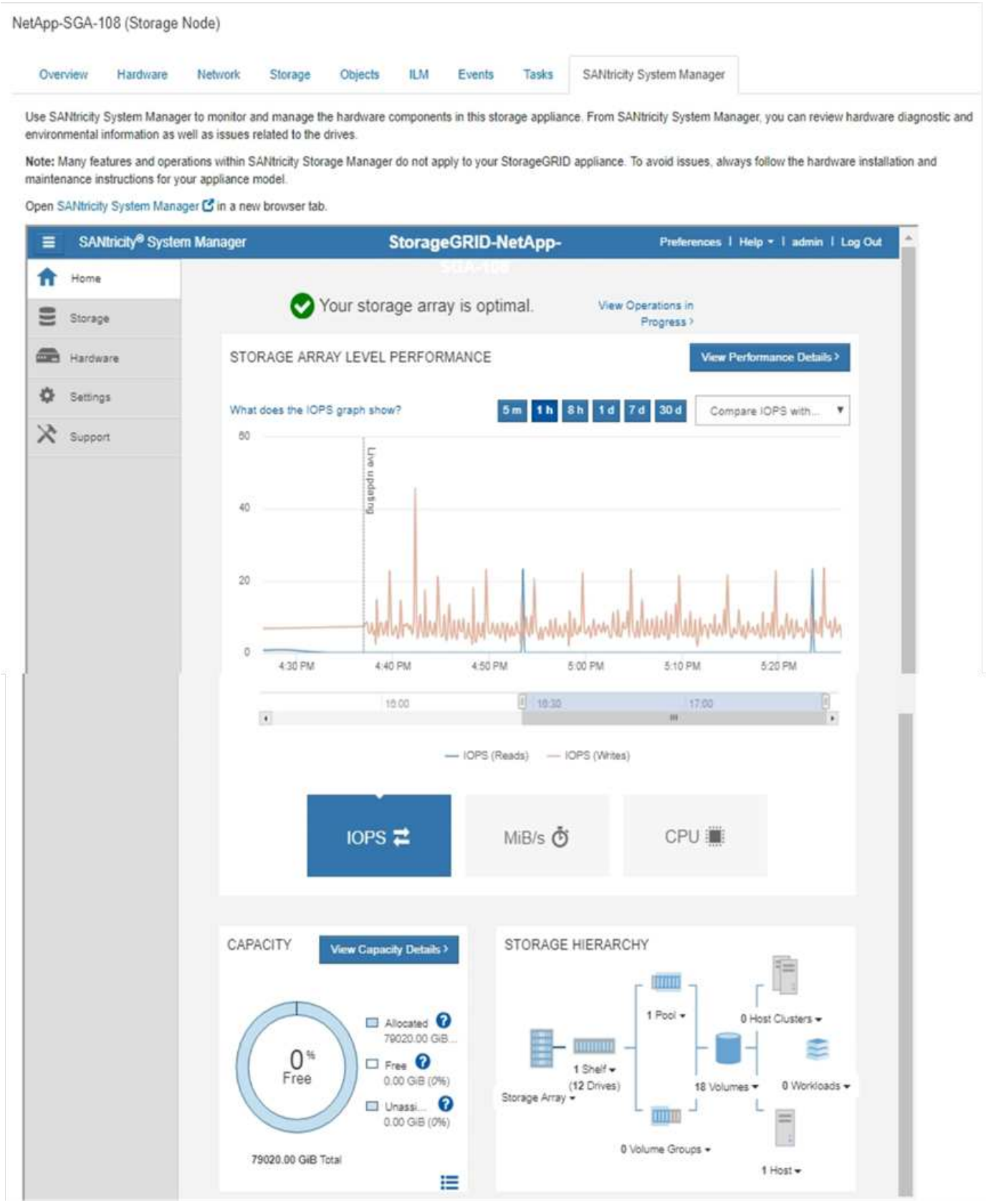
- Anzeige von Performance-Daten wie Performance auf Storage-Array-Ebene, I/O-Latenz, CPU-Auslastung des Storage-Controllers und Durchsatz
- Überprüfen Sie den Status der Hardwarekomponenten.
- Durchführung von Support-Funktionen, einschließlich Anzeige von Diagnosedaten und Konfiguration der E-Series AutoSupport

> Informationen zur Konfiguration eines Proxys für E-Series AutoSupport mit SANtricity System Manager finden Sie unter "Senden Sie E-Series AutoSupport-Pakete über StorageGRID".

Um über den Grid-Manager auf den SANtricity-Systemmanager zuzugreifen, muss die verfügen"Zugriffsberechtigung für den Administrator der Storage-Appliance oder den Root-Zugriff".

> Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mit dem Grid Manager auf SANtricity System Manager zuzugreifen.

Die Registerkarte zeigt die Startseite von SANtricity System Manager an.



Über den Link SANtricity System Manager können Sie den SANtricity System Manager in einem neuen Browser-Fenster öffnen und so die Ansicht erleichtern.

Wenn Sie Details zur Performance und Kapazitätsauslastung auf Speicher-Array-Ebene anzeigen möchten,

setzen Sie den Mauszeiger auf die einzelnen Diagramme.

Weitere Informationen zum Anzeigen der Informationen, auf die über die Registerkarte SANtricity-Systemmanager zugegriffen werden kann, finden Sie unter "NetApp E-Series und SANtricity Dokumentation".

Informationen, die regelmäßig überwacht werden müssen

Was und wann zu überwachen

Das StorageGRID System funktioniert auch dann weiter, wenn Fehler auftreten oder Teile des Grids nicht verfügbar sind, sollten Sie potenzielle Probleme überwachen und beheben, bevor sie die Effizienz oder Verfügbarkeit des Grids beeinträchtigen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über Überwachungsaufgaben

Ein überlastetes System generiert große Datenmengen. Die folgende Liste enthält Anleitungen zu den wichtigsten Informationen, die fortlaufend überwacht werden müssen.

Was überwacht werden soll	Frequenz
"Systemstatus"	Täglich
Rate, mit der "Objekt- und Metadatenkapazität des Storage-Node"verbraucht wird	Wöchentlich
"Information Lifecycle Management-Operationen"	Wöchentlich
"Netzwerk- und Systemressourcen"	Wöchentlich
"Mandantenaktivität"	Wöchentlich
"S3-Client-Vorgänge"	Wöchentlich
"Lastverteilung"	Nach der Erstkonfiguration und nach Konfigurationsänderungen
"Netzverbundverbindungen"	Wöchentlich

Systemzustand überwachen

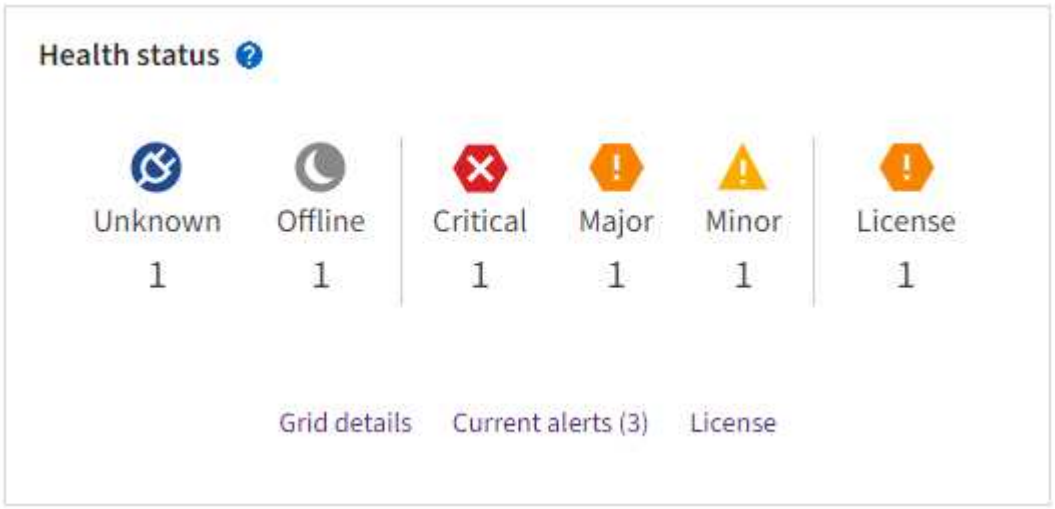
Überwachen Sie täglich den Gesamtzustand Ihres StorageGRID Systems.

Über diese Aufgabe

Das StorageGRID System kann weiter betrieben werden, wenn Teile des Grids nicht verfügbar sind. Potenzielle Probleme, die durch Warnmeldungen angezeigt werden, sind nicht unbedingt Probleme mit dem Systembetrieb. Untersuchen Sie die auf der Statuskarte „Systemzustand“ des Grid Manager-Dashboards

zusammengefassten Probleme.

Um Benachrichtigungen zu erhalten, sobald sie ausgelöst werden, können Sie "Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein" oder "Konfigurieren Sie SNMP-Traps".



Wenn Probleme bestehen, werden Links angezeigt, mit denen Sie weitere Details anzeigen können:

Verlinken	Wird angezeigt, wenn…
Grid-Details	Alle Knoten sind getrennt (Verbindungsstatus Unbekannt oder Administrativ inaktiv).
Aktuelle Warnmeldungen (kritisch, Haupt, Nebenfach)	Warnungen sind Derzeit aktiv.
Kürzlich behobene Warnmeldungen	In der vergangenen Woche ausgelöste Alarme Jetzt behoben.
Lizenz	Es liegt ein Problem mit der Softwarelizenz für dieses StorageGRID-System vor. Sie können "Aktualisieren Sie die Lizenzinformationen nach Bedarf".

Überwachen Sie die Status der Node-Verbindung

Wenn ein oder mehrere Nodes vom Grid getrennt werden, können kritische StorageGRID-Vorgänge beeinträchtigt werden. Überwachen Sie den Verbindungsstatus des Knotens, und beheben Sie alle Probleme umgehend.

Symbol	Beschreibung	Handeln erforderlich
	**Nicht verbunden - Unbekannt** Aus einem unbekannten Grund ist die Verbindung zu einem Node unterbrochen, oder Dienste auf dem Node wurden unerwartet heruntergefahren. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren. Die Warnung * kann nicht mit Node* kommunizieren. Andere Warnmeldungen können ebenfalls aktiv sein.	Erfordert sofortige Aufmerksamkeit. Wählen Sie jede Warnmeldung aus Und befolgen Sie die empfohlenen Maßnahmen. Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten. **Hinweis**: Ein Knoten kann während des verwalteten Herunterfahrens als Unbekannt erscheinen. In diesen Fällen können Sie den Status Unbekannt ignorieren.
	**Nicht verbunden - Administrativ unten** Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise auch aktiv. Aufgrund des zugrunde liegenden Problems sind diese Nodes oft ohne Eingriff wieder online.	Ermitteln Sie, ob Warnmeldungen Auswirkungen auf diesen Node haben. Wenn eine oder mehrere Warnungen aktiv sind, Wählen Sie jede Warnmeldung aus und befolgen Sie die empfohlenen Maßnahmen.
	• Verbunden* Der Knoten ist mit dem Raster verbunden.	Keine Aktion erforderlich.

Anzeige aktueller und aufgelöster Warnmeldungen

Aktuelle Alarme: Wenn ein Alarm ausgelöst wird, wird ein Warnsymbol auf dem Dashboard angezeigt. Auf der Seite Knoten wird auch ein Warnungssymbol für den Knoten angezeigt. Wenn "Benachrichtigungen für Warnmeldungen sind konfiguriert", wird auch eine E-Mail-Benachrichtigung gesendet, es sei denn, die Benachrichtigung wurde stummgeschaltet.

Aufgelöste Warnungen: Sie können einen Verlauf von Warnungen suchen und anzeigen, die behoben wurden.

Optional haben Sie das Video angesehen:

Übersicht über Warnungen

In der folgenden Tabelle werden die im Grid Manager angezeigten Informationen zu aktuellen und behobenen

Warnmeldungen beschrieben.

Spaltenüberschrift	Beschreibung
Name oder Titel	Der Name der Warnmeldung und deren Beschreibung.
Schweregrad	Der Schweregrad der Meldung. Wenn bei aktuellen Warnmeldungen mehrere Warnmeldungen gruppiert werden, zeigt die Titelzeile an, wie viele Instanzen dieser Warnmeldung bei jedem Schweregrad auftreten. **Kritisch**: Es existiert eine anormale Bedingung, die den normalen Betrieb eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. **Major**: Es gibt einen anormalen Zustand, der entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für einen kritischen Alarm nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. **Minor**: Das System funktioniert normal, aber es gibt einen ungewöhnlichen Zustand, der die Fähigkeit des Systems beeinflussen könnte, wenn es weitergeht. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
Auslösezeit	**Aktuelle Alarme**: Das Datum und die Uhrzeit, zu der der Alarm in Ihrer Ortszeit und in UTC ausgelöst wurde. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile Zeiten für die letzte Instanz der Warnmeldung (*neueste*) und die älteste Instanz der Warnmeldung (*älteste*) an. **Resolved Alerts**: Wie lange ist es her, dass der Alarm ausgelöst wurde.
Standort/Knoten	Der Name des Standorts und des Knotens, an dem die Warnung auftritt oder aufgetreten ist.
Status	Gibt an, ob die Warnmeldung aktiv, stummgeschaltet oder behoben ist. Wenn mehrere Warnungen gruppiert sind und **Alle Alarme** in der Dropdown-Liste ausgewählt ist, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung aktiv sind und wie viele Instanzen zum Schweigen gebracht wurden.
Behobene Zeit (nur behobene Warnmeldungen)	Wie lange zuvor wurde die Warnung behoben.

Spaltenüberschrift	Beschreibung
Aktuelle Werte oder *Datenwerte*	Der Wert der Metrik, der den Auslöser der Meldung verursacht hat. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Meldung mit * Objekt-Datenspeicher* enthalten beispielsweise den Prozentsatz des verwendeten Festplattenspeichers, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Festplattenspeichers. **Hinweis:** Wenn mehrere aktuelle Warnungen gruppiert werden, werden die aktuellen Werte nicht in der Titelzeile angezeigt.
Ausgelöste Werte (nur gelöste Warnmeldungen)	Der Wert der Metrik, der den Auslöser der Meldung verursacht hat. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Meldung mit * Objekt-Datenspeicher* enthalten beispielsweise den Prozentsatz des verwendeten Festplattenspeichers, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Festplattenspeichers.

Schritte

1. Wählen Sie den Link **Aktuelle Alarme** oder **gelöste Warnmeldungen** aus, um eine Liste der Warnungen in diesen Kategorien anzuzeigen. Sie können die Details für eine Warnmeldung auch anzeigen, indem Sie **Nodes** > ***Node*** > **Übersicht** auswählen und dann die Warnmeldung aus der Tabelle Alerts auswählen.

   Standardmäßig werden aktuelle Warnmeldungen wie folgt angezeigt:

   - Die zuletzt ausgelösten Warnmeldungen werden zuerst angezeigt.
   - Mehrere Warnmeldungen desselben Typs werden als Gruppe angezeigt.
   - Alarme, die stummgeschaltet wurden, werden nicht angezeigt.
   - Wenn für eine bestimmte Warnmeldung auf einem bestimmten Node die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird nur die schwerste Warnmeldung angezeigt. Wenn also Alarmschwellenwerte für kleinere, größere und kritische Schweregrade erreicht werden, wird nur die kritische Warnung angezeigt.

     Die Seite Aktuelle Warnmeldungen wird alle zwei Minuten aktualisiert.

2. Wählen Sie zum erweitern von Warengruppen das Menü aus. Um einzelne Warnungen in einer Gruppe auszublenden, wählen Sie das up-Caret aus, oder wählen Sie den Namen der Gruppe aus.
3. Um einzelne Warnungen anstelle von Warengruppen anzuzeigen, deaktivieren Sie das Kontrollkästchen **Gruppenwarnungen**.
4. Um aktuelle Warnmeldungen oder Warnungsgruppen zu sortieren, wählen Sie die nach-oben-/nach-unten-Pfeile in jeder Spaltenüberschrift aus.
   - Wenn **Group Alerts** ausgewählt ist, werden sowohl die Warnungsgruppen als auch die einzelnen Alarme innerhalb jeder Gruppe sortiert. Sie können beispielsweise die Warnungen in einer Gruppe nach **Zeit ausgelöst** sortieren, um die aktuellste Instanz eines bestimmten Alarms zu finden.
   - Wenn **Group Alerts** gelöscht wird, wird die gesamte Liste der Alerts sortiert. Beispielsweise können Sie alle Warnungen nach **Node/Site** sortieren, um alle Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.
5. Um aktuelle Warnmeldungen nach Status (**Alle Alarme**, **aktiv** oder **quittiert**) zu filtern, verwenden Sie das

Dropdown-Menü oben in der Tabelle.

Siehe "Benachrichtigung über Stille".

6. So sortieren Sie behobene Warnmeldungen:
   - Wählen Sie im Dropdown-Menü **When Triggered** einen Zeitraum aus.
   - Wählen Sie eine oder mehrere Schweregrade aus dem Dropdown-Menü **Schweregrad** aus.
   - Wählen Sie im Dropdown-Menü **Warnregel** eine oder mehrere Standard- oder benutzerdefinierte Warnungsregeln aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einer bestimmten Alarmregel zusammenhängen.
   - Wählen Sie im Dropdown-Menü **Node** einen oder mehrere Knoten aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einem bestimmten Knoten verbunden sind.
7. Um Details für eine bestimmte Warnmeldung anzuzeigen, wählen Sie die Warnmeldung aus. Ein Dialogfeld enthält Details und empfohlene Aktionen für die ausgewählte Warnmeldung.
8. (Optional) Wählen Sie für einen bestimmten Alarm die Option Diese Warnung stummschalten, um die Alarmregel, die diese Warnung ausgelöst hat, stummzuschalten.

   Sie müssen über den verfügen"Managen von Warnmeldungen oder Root-Zugriffsberechtigungen", um eine Warnungsregel stumm zu schalten.

   > Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn eine Alarmregel stumm geschaltet ist, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang abgeschlossen wird.

9. So zeigen Sie die aktuellen Bedingungen für die Meldungsregel an:
   a. Wählen Sie aus den Warnungsdetails **Bedingungen anzeigen**.

      Es wird ein Popup-Fenster mit dem Prometheus-Ausdruck für jeden definierten Schweregrad angezeigt.

   b. Um das Popup-Fenster zu schließen, klicken Sie außerhalb des Popup-Dialogfenster auf eine beliebige Stelle.
10. Wählen Sie optional **Regel bearbeiten**, um die Warnungsregel zu bearbeiten, die diese Warnung ausgelöst hat.

    Sie müssen über den verfügen"Managen von Warnmeldungen oder Root-Zugriffsberechtigungen", um eine Warnungsregel zu bearbeiten.

    > Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnungsregel zu bearbeiten. Wenn Sie die Triggerwerte ändern, können Sie möglicherweise ein zugrunde liegendes Problem erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

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

Monitoring der Storage-Kapazität

Überwachen Sie den insgesamt verfügbaren nutzbaren Speicherplatz, um sicherzustellen, dass dem StorageGRID System der Speicherplatz für Objekte oder Objekt-Metadaten nicht knapp wird.

StorageGRID speichert Objektdaten und Objektmetadaten separat und behält eine bestimmte Menge an Speicherplatz für eine verteilte Cassandra-Datenbank mit Objekt-Metadaten bei. Überwachen Sie den Gesamtspeicherplatz für Objekte und Objekt-Metadaten sowie Trends für den Speicherplatz, der für jeden verbraucht wird. So können Sie das Hinzufügen von Nodes vorausschauender planen und Serviceausfälle vermeiden.

Sie können "Informationen zur Storage-Kapazität anzeigen" für das gesamte Grid, für jeden Standort und für jeden Storage-Node in Ihrem StorageGRID-System.

Überwachung der Speicherkapazität für das gesamte Grid

Überwachen Sie die Gesamt-Storage-Kapazität Ihres Grids, um sicherzustellen, dass ausreichend freier Speicherplatz für Objektdaten und Objektmetadaten verbleibt. Wenn Sie verstehen, wie sich die Storage-Kapazität im Laufe der Zeit verändert, können Sie Storage-Nodes oder Storage-Volumes planen, bevor die nutzbare Storage-Kapazität des Grid verbraucht wird.

Mithilfe des Grid Manager Dashboards können Sie schnell bewerten, wie viel Storage für das gesamte Grid und für jedes Datacenter verfügbar ist. Die Seite Knoten enthält detailliertere Werte für Objektdaten und Objektmetadaten.

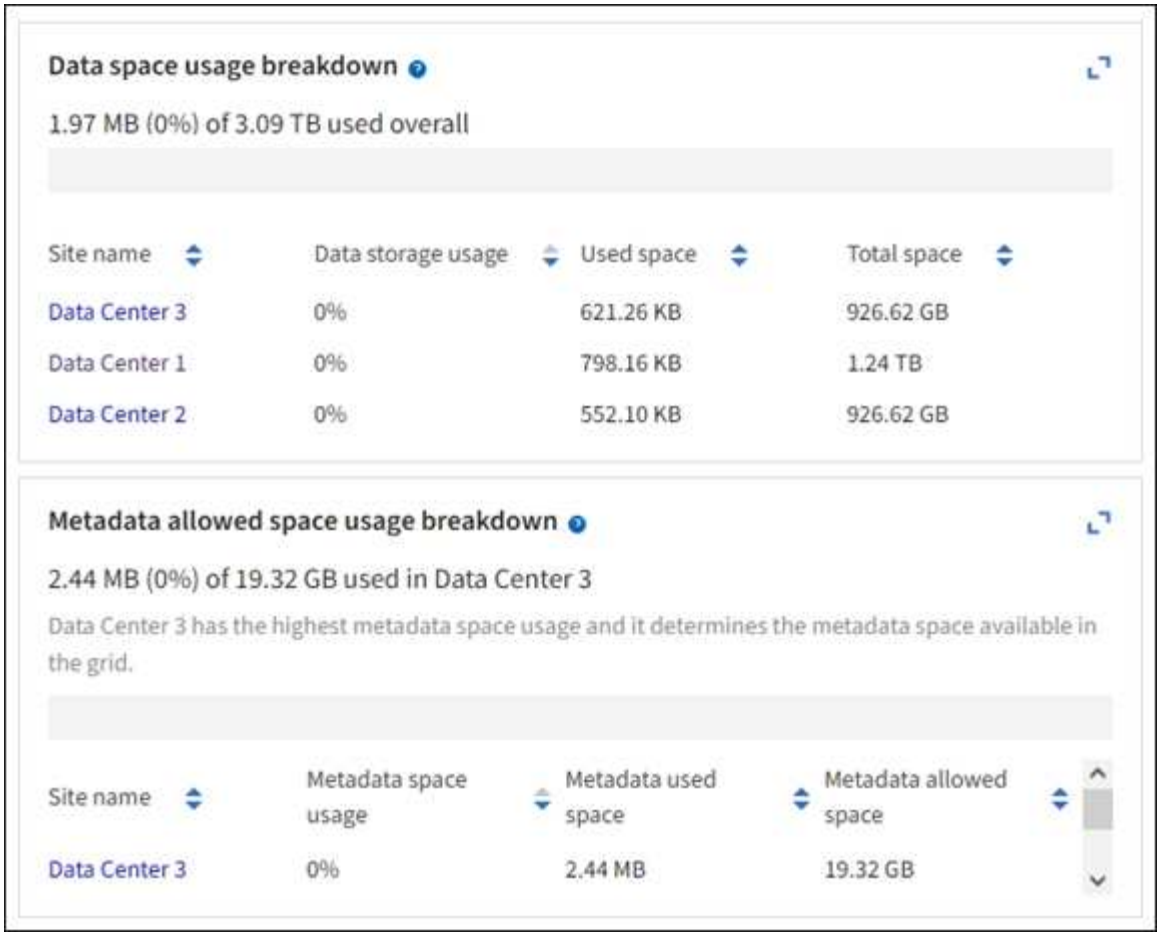
Schritte

1. Beurteilen Sie, wie viel Storage für das gesamte Grid und das jeweilige Datacenter verfügbar ist.

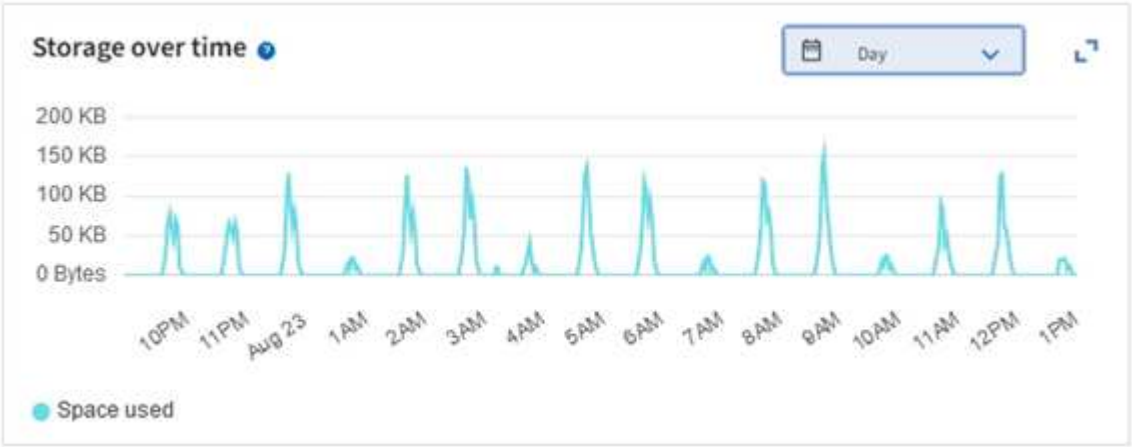
   a. Wählen Sie **Dashboard > Übersicht**.

   b. Beachten Sie die Werte für die Aufschlüsselung der Speicherplatznutzung und die Aufschlüsselung der Metadaten für die zulässige Speicherplatznutzung. Jede Karte listet einen Prozentsatz der Speichernutzung, die Kapazität des belegten Speicherplatzes und den gesamten verfügbaren oder von der Site erlaubten Speicherplatz auf.

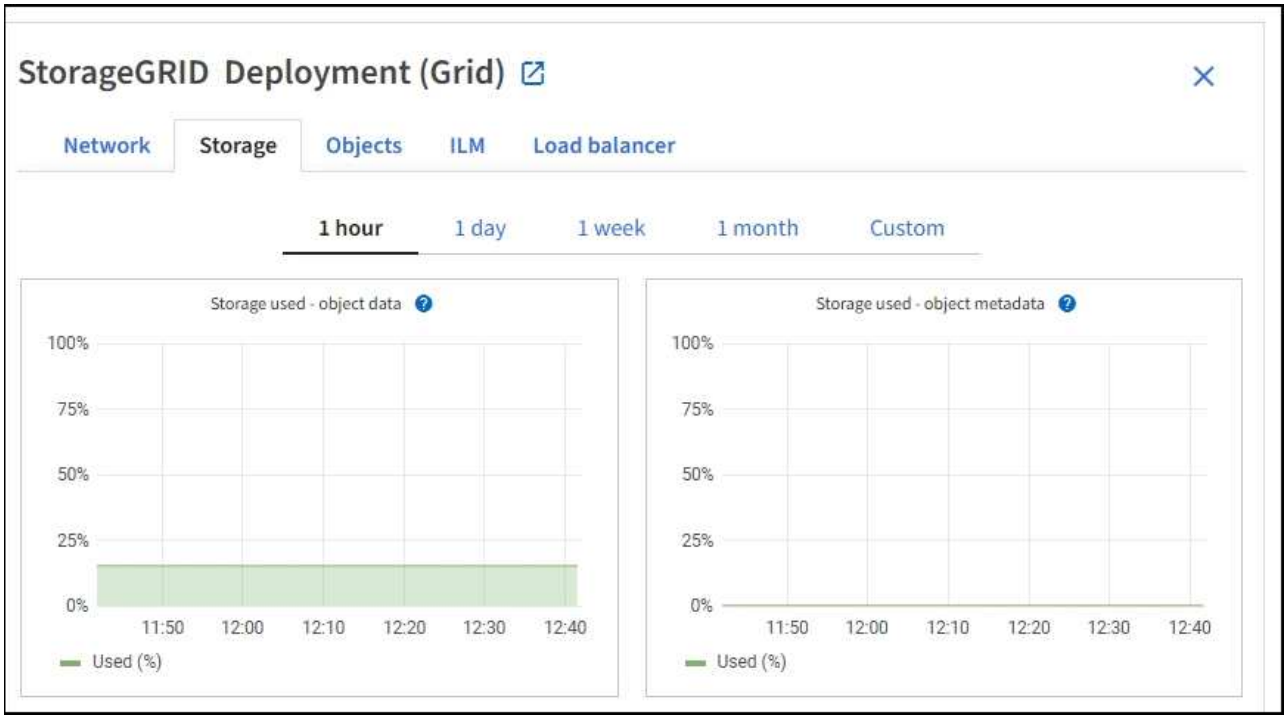
      Die Zusammenfassung enthält keine Archivierungsmedien.



a. Notieren Sie sich das Diagramm auf der Karte „Speicher im Zeitverlauf“. Anhand der Dropdown-Liste „Zeitraum“ können Sie ermitteln, wie schnell Storage verbraucht wird.



2. Auf der Seite Nodes finden Sie weitere Details dazu, wie viel Storage genutzt wurde und wie viel Storage für Objektdaten und Objektmetadaten im Grid verfügbar bleibt.
   a. Wählen Sie **Knoten** aus.
   b. Wählen Sie ***Grid*** > **Storage** aus.



c. Bewegen Sie den Cursor über die **Storage Used - Object Data** und die **Storage Used - Object metadata** Diagramme, um zu sehen, wie viel Objektspeicher und Objektmetadaten-Speicher für das gesamte Grid verfügbar sind und wie viel im Laufe der Zeit genutzt wurde.

> Die Gesamtwerte für einen Standort oder das Raster enthalten keine Knoten, die mindestens fünf Minuten lang keine Kennzahlen gemeldet haben, z. B. Offline-Nodes.

3. Planung, eine Erweiterung zum Hinzufügen von Storage-Nodes oder Storage-Volumes durchzuführen, bevor die nutzbare Storage-Kapazität des Grid genutzt wird

   Berücksichtigen Sie bei der Planung des Zeitplans für eine Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, wird es möglicherweise besser erweitert, wenn vorhandene Storage-Nodes ungefähr 70 % ausgelastet sind, um die Anzahl der hinzugefügten Nodes zu verringern.

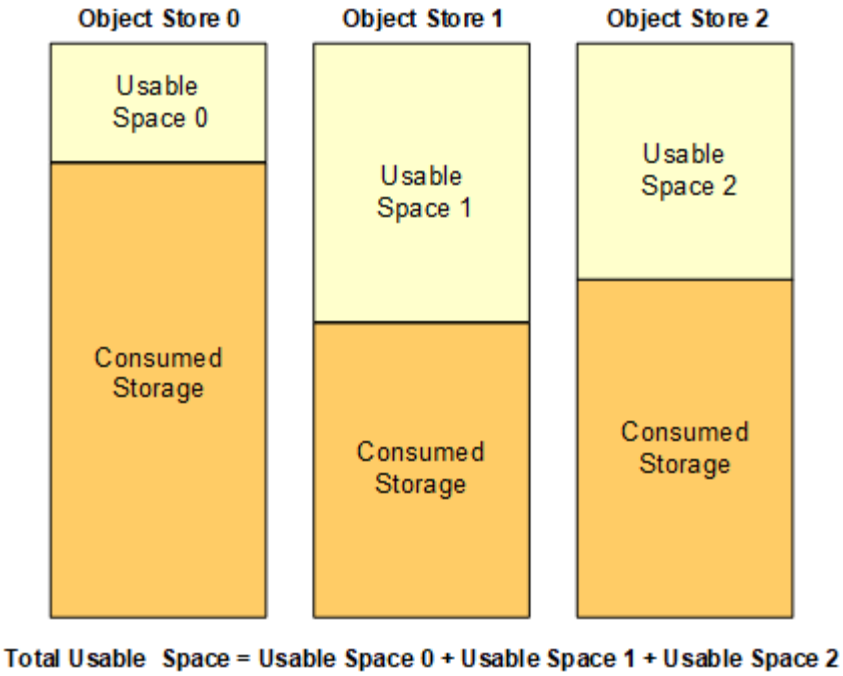
   Weitere Informationen zur Planung einer Speichererweiterung finden Sie im "Anweisungen zur Erweiterung von StorageGRID".

Überwachen Sie die Storage-Kapazität für jeden Storage-Node

Überwachen Sie den insgesamt nutzbaren Speicherplatz für jeden Storage-Node, um sicherzustellen, dass der Node über ausreichend Speicherplatz für neue Objektdaten verfügt.

Über diese Aufgabe

Der nutzbare Speicherplatz ist der Speicherplatz, der zum Speichern von Objekten zur Verfügung steht. Der insgesamt nutzbare Speicherplatz für einen Storage-Node wird berechnet, indem der verfügbare Speicherplatz in allen Objektspeichern innerhalb des Node hinzugefügt wird.



Schritte

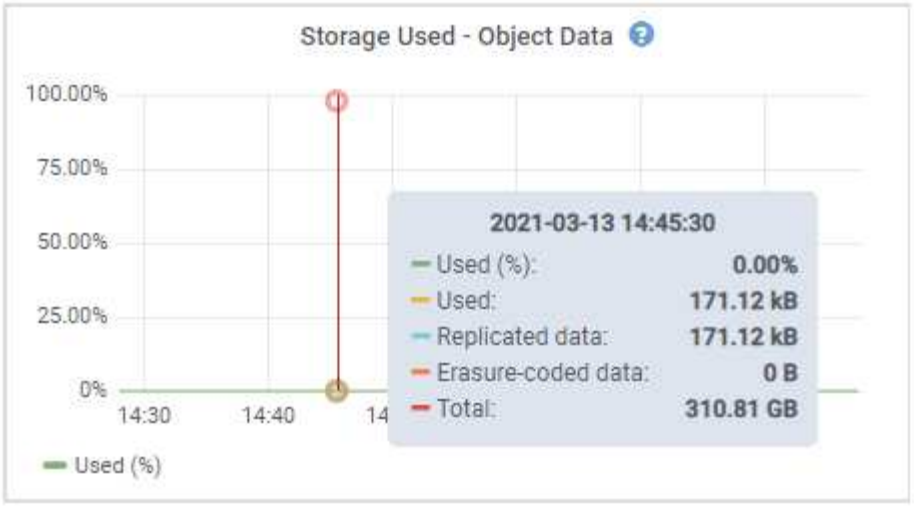
1. Wählen Sie **Knoten** > ***Speicherknoten*** > **Speicher**.

   Die Diagramme und Tabellen für den Node werden angezeigt.

2. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objektdaten.

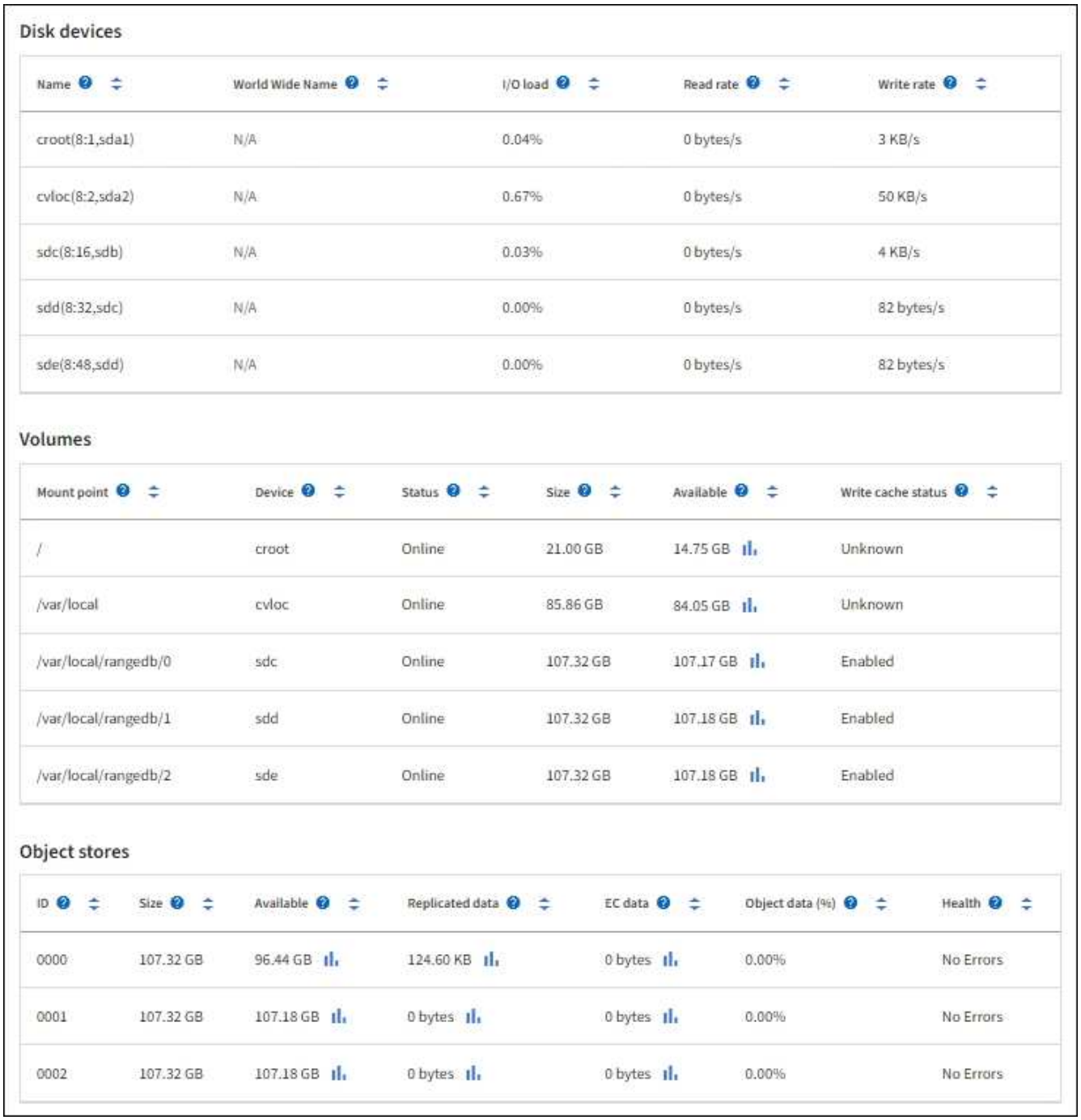
   Die folgenden Werte werden angezeigt:

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



3. Überprüfen Sie die verfügbaren Werte in den Tabellen Volumes und Objektspeichern unter den Diagrammen.

Um Diagramme dieser Werte anzuzeigen, klicken Sie in den verfügbaren Spalten auf die Diagrammsymbole.



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 Zeitbereich, um die Rate abzuschätzen, mit der der nutzbare Speicherplatz belegt wird.
5. Um normale Systemvorgänge aufrechtzuerhalten, fügen Sie Storage-Nodes hinzu, fügen Storage Volumes oder Archivdaten hinzu, bevor der nutzbare Speicherplatz verbraucht wird.

   Berücksichtigen Sie bei der Planung des Zeitplans für eine Erweiterung, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, wird es möglicherweise besser erweitert, wenn vorhandene Storage-Nodes ungefähr 70 % ausgelastet sind, um die Anzahl der hinzugefügten Nodes zu verringern.

Weitere Informationen zur Planung einer Speichererweiterung finden Sie im "Anweisungen zur Erweiterung

von StorageGRID".

Die "Niedriger Objekt-Storage" Warnmeldung wird ausgelöst, wenn nicht genügend Speicherplatz für das Speichern von Objektdaten auf einem Storage Node vorhanden ist.

Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node

Überwachen Sie die Metadatennutzung für jeden Storage-Node, um sicherzustellen, dass ausreichend Speicherplatz für wichtige Datenbankvorgänge verfügbar ist. Sie müssen an jedem Standort neue Storage-Nodes hinzufügen, bevor die Objektmetadaten 100 % des zulässigen Metadaten-Speicherplatzes übersteigen.

Über diese Aufgabe

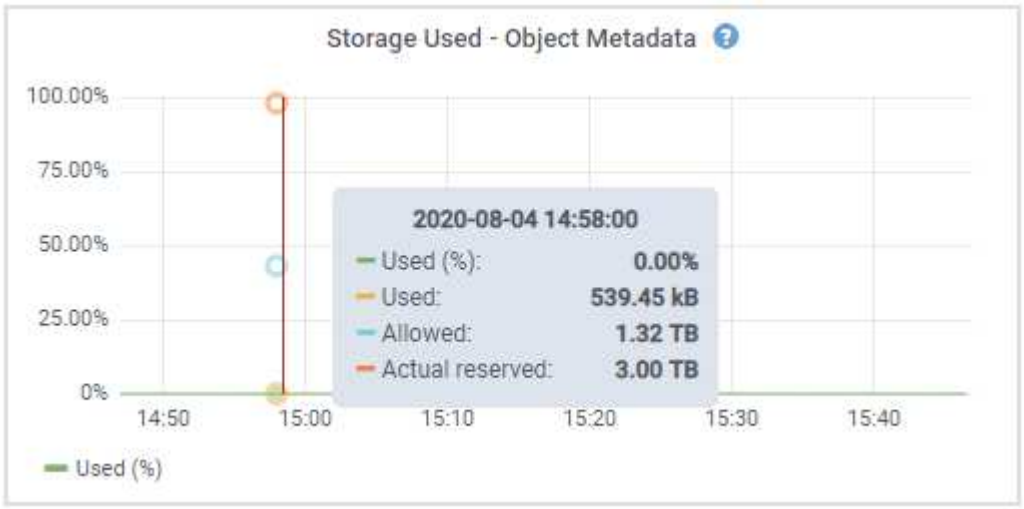
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage Volume 0 jedes Storage-Nodes verwendet.

In einigen Fällen wird die Kapazität der Objektmetadaten des Grid möglicherweise schneller belegt als die Kapazität des Objekt-Storage. Wenn Sie zum Beispiel normalerweise eine große Anzahl von kleinen Objekten aufnehmen, müssen Sie möglicherweise Storage-Nodes hinzufügen, um die Metadaten-Kapazität zu erhöhen, obwohl weiterhin ausreichend Objekt-Storage-Kapazität vorhanden ist.

Zu den Faktoren, die die Metadatennutzung steigern können, gehören die Größe und Menge der Metadaten und -Tags der Benutzer, die Gesamtzahl der Teile in einem mehrteiligen Upload und die Häufigkeit von Änderungen an den ILM-Speicherorten.

Schritte

1. Wählen Sie **Knoten** > ***Speicherknoten*** > **Speicher**.
2. Bewegen Sie den Mauszeiger über das Diagramm Speicher verwendet – Objekt-Metadaten, um die Werte für eine bestimmte Zeit anzuzeigen.



Nutzung (%)

Der Prozentsatz des zulässigen Metadaten-Speicherplatzes, der auf diesem Storage-Node verwendet wurde.

Prometheus Kennzahlen: `storagegrid_storage_utilization_metadata_bytes` Und `storagegrid_storage_utilization_metadata_allowed_bytes`

Verwendet

Die Bytes des zulässigen Metadaten-Speicherplatzes, der auf diesem Speicherknoten verwendet wurde.

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_bytes`

Zulässig

Der zulässige Speicherplatz für Objektmetadaten auf diesem Storage-Node. Wie dieser Wert für jeden Storage Node bestimmt wird, erfahren Sie im "Vollständige Beschreibung des zulässigen Metadatenspeichers".

Prometheus-Metrik: `storagegrid_storage_utilization_metadata_allowed_bytes`

Ist reserviert

Der tatsächliche Speicherplatz, der für Metadaten auf diesem Speicherknoten reserviert ist. Beinhaltet den zulässigen Speicherplatz und den erforderlichen Speicherplatz für wichtige Metadaten-Vorgänge. Wie dieser Wert für jeden Storage Node berechnet wird, erfahren Sie im "Vollständige Beschreibung des tatsächlich reservierten Speicherplatzes für Metadaten".

Prometheus Metrik wird in einer zukünftigen Version hinzugefügt.

Die Gesamtwerte für einen Standort oder das Raster enthalten keine Knoten, die mindestens fünf Minuten lang keine Kennzahlen gemeldet haben, z. B. Offline-Nodes.

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

Der Alarm * Low Metadaten Storage* wird ausgelöst, wenn der Wert **used (%)** bestimmte Schwellenwerte erreicht. Unerwünschte Ergebnisse können auftreten, wenn Objekt-Metadaten mehr als 100 % des zulässigen Speicherplatzes beanspruchen.

Wenn Sie die neuen Nodes hinzufügen, gleicht das System die Objektmetadaten automatisch auf alle Storage-Nodes am Standort aus. Siehe "Anweisungen zum erweitern eines StorageGRID-Systems".

Prognosen zur Speicherplatznutzung überwachen

Überwachen Sie die Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten, um abzuschätzen, wann Sie dies benötigen"Erweitern Sie ein Raster".

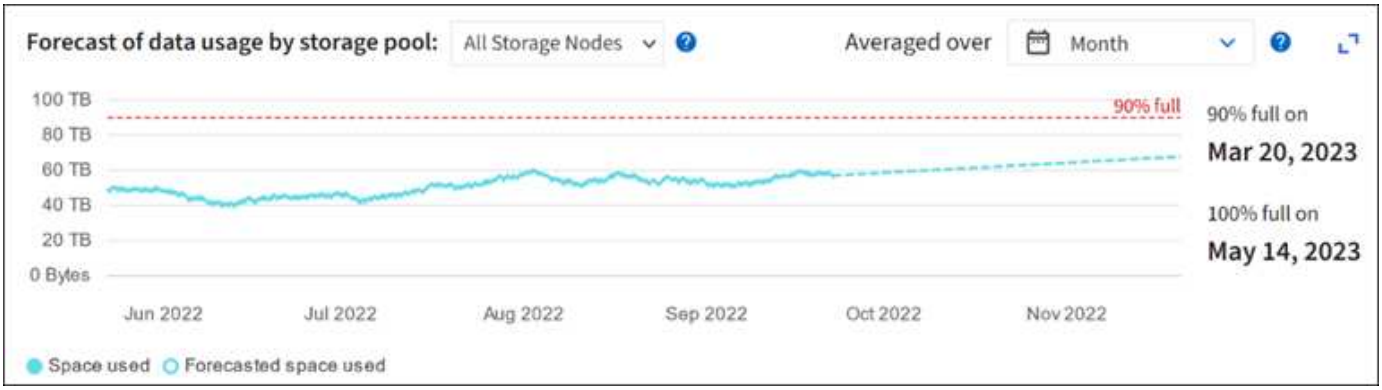
Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie einen kürzeren Bereich aus dem Pulldown-Menü **gemittelt über** aus, um nur die neuesten Aufnahmemuster wiederzugeben. Wenn Sie saisonale Muster bemerken, wählen Sie einen längeren Bereich aus.

Falls Sie eine neue StorageGRID-Installation besitzen, lassen Sie vor der Evaluierung der Prognosen zur Speicherplatznutzung zu, dass sich Daten und Metadaten anhäufen können.

Schritte

1. Wählen Sie auf dem Dashboard **Speicher**.
2. Sie können die Dashboard-Karten, Prognosen zur Datennutzung nach Storage-Pool und Prognosen zur Metadatennutzung nach Standort anzeigen.
3. Verwenden Sie diese Werte, um zu schätzen, wann Sie neue Storage-Nodes für den Daten- und

Metadatenspeicher hinzufügen müssen.



Überwachung des Information Lifecycle Management

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

Über diese Aufgabe

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

Die Objektaufnahme und andere objektbezogene Aktivitäten können die Geschwindigkeit übersteigen, mit der StorageGRID ILM-Prozesse evaluieren kann, sodass das System Objekte in eine Warteschlange einstellt, deren ILM-Platzierungsanweisungen nicht nahezu in Echtzeit erfüllt werden können. Sie sollten überprüfen, ob StorageGRID mit den Client-Aktionen Schritt hält.

Dashboard-Registerkarte des Grid Manager verwenden

Schritte

Überwachen Sie ILM-Vorgänge mithilfe der Registerkarte ILM im Grid Manager Dashboard:

1. Melden Sie sich beim Grid Manager an.
2. Wählen Sie im Dashboard die Registerkarte ILM aus und notieren Sie sich die Werte auf der ILM-Warteschlange (Objekte) und der ILM-Evaluierungsratenkarte.

   Es sind temporäre Spitzen in der ILM-Warteschlange (Objekte)-Karte auf dem Dashboard zu erwarten. Wenn die Warteschlange jedoch weiter wächst und nicht abnimmt, benötigt das Grid mehr Ressourcen, um effizient zu arbeiten: Entweder mehr Storage Nodes oder, wenn die ILM-Richtlinie Objekte an entfernten Standorten platziert, mehr Netzwerkbandbreite.

Verwenden der Seite „Knoten“

Schritte

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

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

1. Wählen Sie **Knoten** aus.
2. Wählen Sie ***Grid Name*** > **ILM** aus.
3. Bewegen Sie den Mauszeiger über das ILM-Warteschlangendiagramm, um den Wert der folgenden Attribute zu einem bestimmten Zeitpunkt anzuzeigen:
   - **Objekte in der Warteschlange (aus Client-Operationen)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aufgrund von Client-Operationen warten (z. B. Aufnahme).
   - **Objekte in der Warteschlange (aus allen Operationen)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten.
   - **Scan-Rate (Objects/sec)**: Die Geschwindigkeit, mit der Objekte im Raster gescannt und für ILM in die Warteschlange gestellt werden.
   - **Evaluationsrate (Objects/sec)**: Die aktuelle Rate, mit der Objekte anhand der ILM-Richtlinie im Grid ausgewertet werden.

   > Der Abschnitt zur ILM-Warteschlange ist nur für das Raster enthalten. Diese Informationen werden auf der Registerkarte ILM für einen Standort oder Storage Node nicht angezeigt.

4. Sehen Sie sich im Abschnitt ILM-Warteschlange die folgenden Attribute an.
   - **Scan-Zeitraum - geschätzt**: Die geschätzte Zeit, um einen vollständigen ILM-Scan aller Objekte durchzuführen.

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

   - **Reparaturversuche**: Die Gesamtzahl der Objektreparaturoperationen für replizierte Daten, die versucht wurden. Diese Zählung erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein Objekt mit hohem Risiko zu reparieren. Risikobehaftete ILM-Reparaturen werden priorisiert, wenn das Grid besetzt wird.

     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.

5. Alternativ senden Sie eine Prometheus-Abfrage für `storagegrid_ilm_scan_period_estimated_minutes` Und `storagegrid_ilm_repairs_attempted`.

Überwachen Sie Netzwerk- und Systemressourcen

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

Überwachen Sie Netzwerkverbindungen und Performance

Netzwerkkonnektivität und Bandbreite sind besonders wichtig, wenn Ihre Richtlinien für Information Lifecycle Management (ILM) replizierte Objekte zwischen Standorten kopieren oder Erasure Coding-codierte Objekte mit einem Schema speichern, das Site-Loss-Schutz bietet. Wenn das Netzwerk zwischen Standorten nicht verfügbar ist, die Netzwerklatenz zu hoch ist oder die Netzwerkbandbreite nicht ausreicht, können einige ILM-

Regeln Objekte möglicherweise nicht an den erwarteten Stellen platzieren. Dies kann zu Aufnahmeausfällen (wenn die strikte Aufnahmeoption für ILM-Regeln ausgewählt wird) oder zu schlechter Aufnahme-Performance und ILM-Rückprotokollen führen.

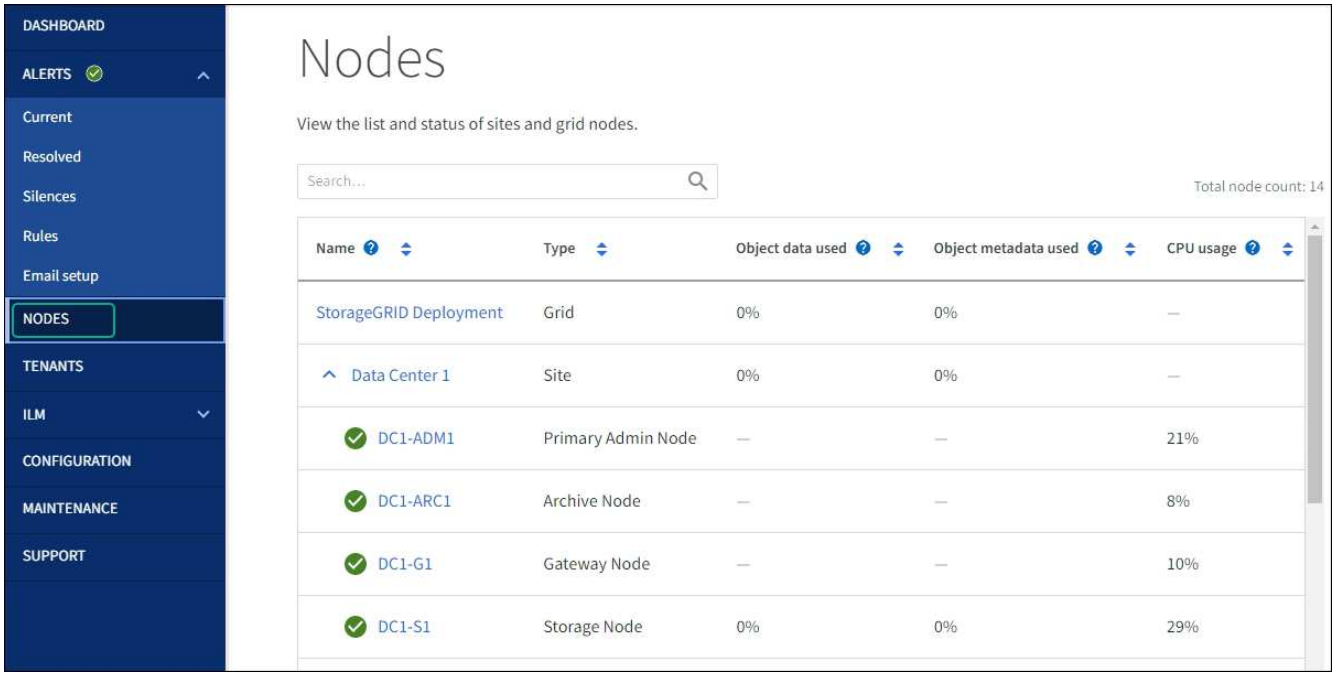
Überwachen Sie die Konnektivität und die Netzwerk-Performance mit dem Grid Manager, damit Sie bei Problemen umgehend auf Probleme reagieren können.

Denken Sie darüber hinaus daran"Erstellen von Klassifizierungsrichtlinien für den Netzwerkverkehr", dass Sie den Datenverkehr zu bestimmten Mandanten, Buckets, Subnetzen oder Endpunkten des Load Balancer überwachen können. Sie können Richtlinien zur Begrenzung des Datenverkehrs nach Bedarf festlegen.

Schritte

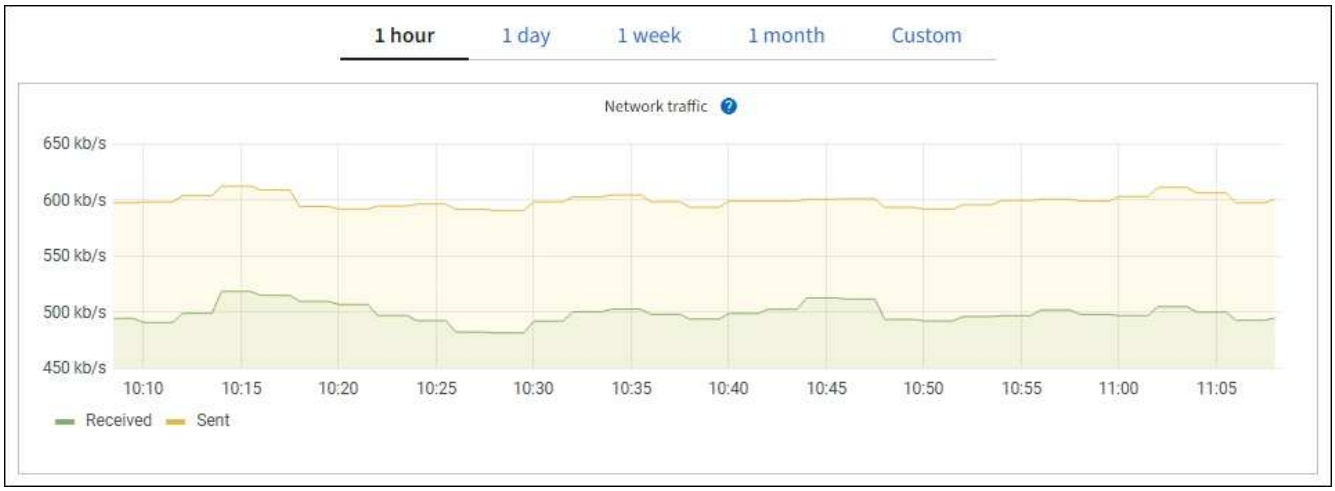
1. Wählen Sie **Knoten** aus.

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



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

   Das Diagramm „Netzwerk-Traffic“ bietet eine Zusammenfassung des gesamten Netzwerkverkehr für das gesamte Grid, den Datacenter-Standort oder für den Node.



a. Wenn Sie einen Rasterknoten ausgewählt haben, scrollen Sie nach unten, um den Abschnitt **Netzwerkschnittstellen** auf der Seite anzuzeigen.

Network interfaces

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

b. Blättern Sie bei Rasterknoten nach unten, um den Abschnitt **Netzwerkkommunikation** auf der Seite anzuzeigen.

Die Tabellen „Empfangen und Senden“ zeigen, wie viele Bytes und Pakete über jedes Netzwerk empfangen und gesendet wurden, sowie andere Empfangs- und Übertragungstabellen.

Network communication

Receive

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

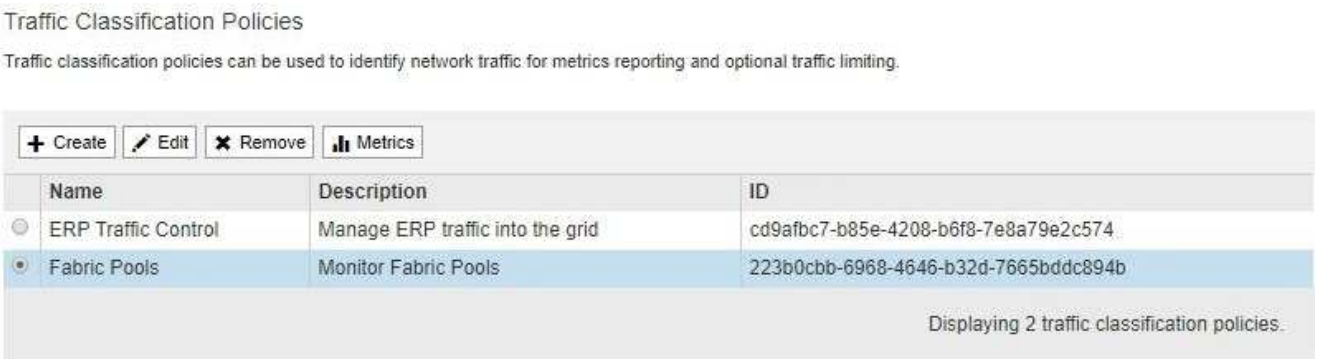
Transmit

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

3. Verwenden Sie die Metriken für Ihre Traffic-Klassifizierungsrichtlinien zur Überwachung des Netzwerkverkehrs.

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

Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



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

b. Überprüfen Sie die Diagramme, um den mit der Richtlinie verknüpften Netzwerkverkehr zu verstehen.

   Wenn eine Richtlinie zur Klassifizierung von Verkehrsströmen darauf ausgelegt ist, den Netzwerkverkehr zu begrenzen, analysieren Sie, wie oft der Datenverkehr begrenzt ist, und entscheiden Sie, ob die Richtlinie Ihre Anforderungen weiterhin erfüllt. Von Zeit zu Zeit, "Passen Sie jede Richtlinie zur Verkehrsklassifizierung nach Bedarf an".

Verwandte Informationen

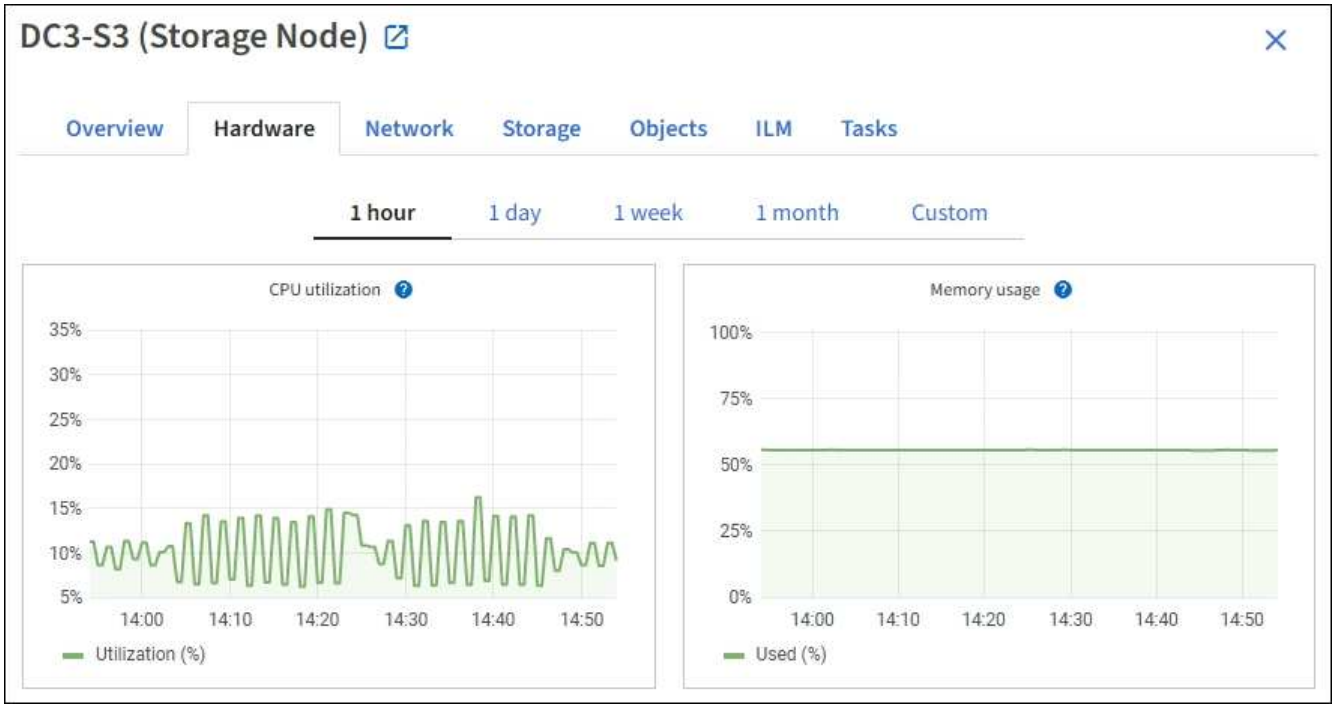
- "Zeigen Sie die Registerkarte Netzwerk an"
- "Überwachen Sie die Status der Node-Verbindung"

Monitoring von Ressourcen auf Node-Ebene

Überwachen Sie einzelne Grid-Nodes, um deren Ressourcenverbrauch zu prüfen. Sind Nodes konsistent überlastet, sind möglicherweise mehr Nodes erforderlich, um einen effizienten Betrieb zu gewährleisten.

Schritte

1. Wählen Sie auf der Seite **Knoten** den Knoten aus.
2. Wählen Sie die Registerkarte **Hardware** aus, um Grafiken der CPU-Auslastung und der Speicherauslastung anzuzeigen.



3. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms 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, mit dem Sie Datum und Zeitbereiche festlegen können.
4. Wenn der Node auf einer Storage Appliance oder einer Services Appliance gehostet wird, scrollen Sie nach unten, um die Komponententabellen anzuzeigen. Der Status aller Komponenten sollte „nominal“ lauten. Untersuchen Sie Komponenten, die einen anderen Status haben.

Verwandte Informationen

- "Zeigen Sie Informationen zu Appliance Storage Nodes an"
- "Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an"

Überwachen Sie die Mandantenaktivität

Alle S3-Client-Aktivitäten sind mit StorageGRID-Mandantenkonten verknüpft. Mit dem Grid Manager können Sie die Storage-Auslastung oder den Netzwerk-Traffic für alle Mandanten oder einen bestimmten Mandanten überwachen. Mithilfe des Revisionsprotokoll und Grafana-Dashboards können Sie detailliertere Informationen darüber sammeln, wie Mandanten StorageGRID verwenden.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Root-Zugriff oder Mandantenkonten".

Alle Mandanten anzeigen

Auf der Seite Tenants werden grundlegende Informationen für alle aktuellen Mandantenkonten angezeigt.

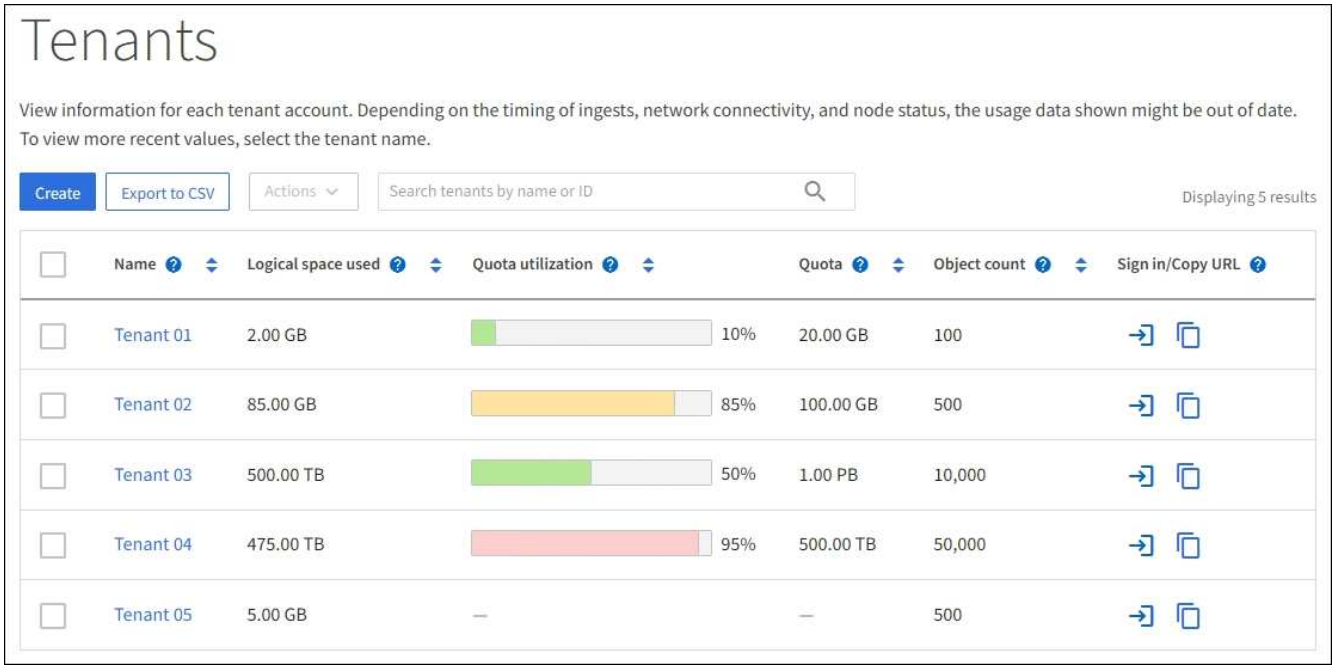
Schritte

1. Wählen Sie **Mandanten** aus.

2. Überprüfen Sie die auf den Mandanten-Seiten angezeigten Informationen.

   Für jeden Mandanten werden der genutzte logische Speicherplatz, die Kontingentnutzung, das Kontingent und die Objektanzahl aufgelistet. Wenn für einen Mandanten keine Quote festgelegt ist, enthalten die Felder Quota Usage und Quota einen Bindestrich (—).

   > Die logische Größe aller Objekte, die zu diesem Mandanten gehören, umfasst unvollständige und laufende mehrteilige Uploads. Die Größe umfasst nicht den zusätzlichen physischen Speicherplatz, der für ILM-Richtlinien verwendet wird. Bei den Werten für den belegten Speicherplatz handelt es sich um Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst.



3. Melden Sie sich optional bei einem Mandantenkonto an, indem Sie den Anmeldelink in der Spalte **Anmelden/URL kopieren** auswählen.
4. Kopieren Sie optional die URL für die Anmeldeseite eines Mandanten, indem Sie den Link URL kopieren in der Spalte **Anmelden/URL kopieren** auswählen.
5. Wählen Sie optional **Export to CSV**, um eine Datei mit den Nutzungswerten für alle Mandanten anzuzeigen und zu exportieren `.csv`.

   Sie werden aufgefordert, die Datei zu öffnen oder zu speichern `.csv`.

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

   Sie können die Datei in einer Tabellenkalkulationsanwendung öffnen `.csv` oder in der Automatisierung verwenden.

6. Wenn keine Objekte aufgelistet sind, wählen Sie optional **actions** > **Delete** aus, um einen oder mehrere Tenants zu entfernen. Siehe "Mandantenkonto löschen".

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

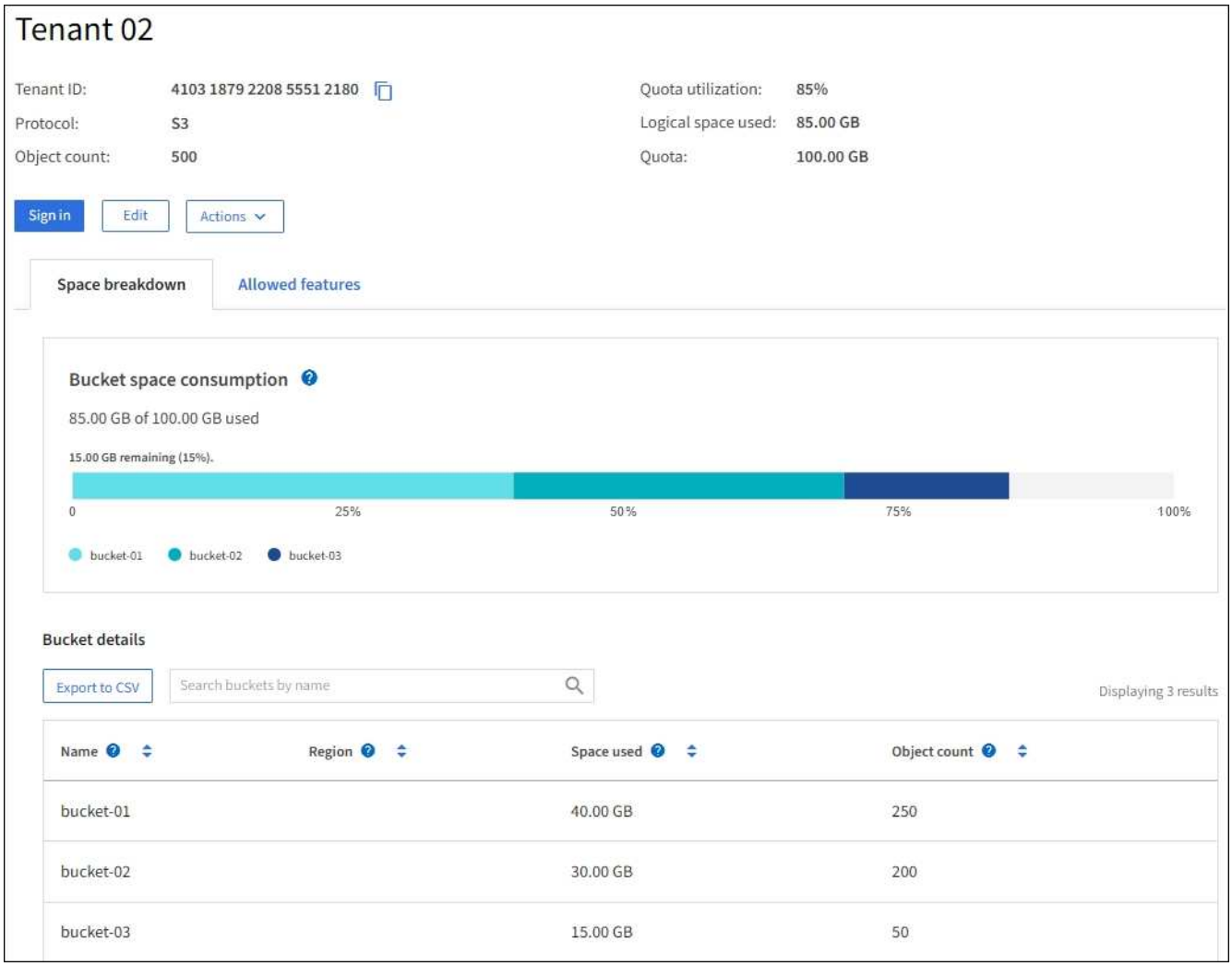
Zeigen Sie eine bestimmte Serviceeinheit an

Sie können Details zu einem bestimmten Mandanten anzeigen.

Schritte

1. Wählen Sie auf der Seite Tenants den Namen der Serviceeinheit aus.

   Die Seite mit den Mandantendetails wird angezeigt.



2. Überprüfen Sie oben auf der Seite die Übersicht über die Serviceeinheiten.

   Dieser Abschnitt der Detailseite enthält zusammenfassende Informationen für den Mandanten, einschließlich der Objektanzahl des Mandanten, der Kontingentnutzung, des verwendeten logischen Speicherplatzes und der Kontingenteinstellung.

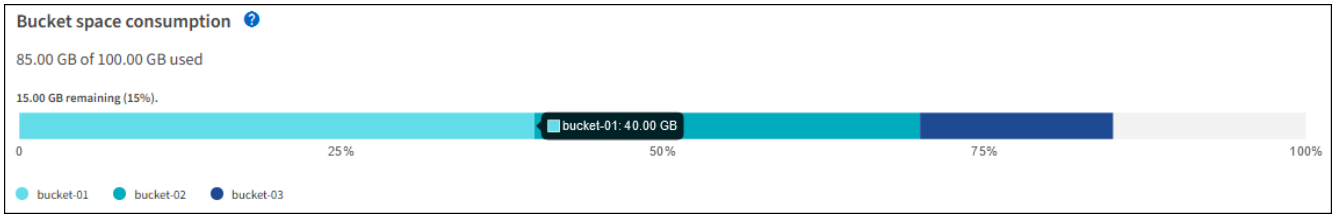
   > Die logische Größe aller Objekte, die zu diesem Mandanten gehören, umfasst unvollständige und laufende mehrteilige Uploads. Die Größe umfasst nicht den zusätzlichen physischen Speicherplatz, der für ILM-Richtlinien verwendet wird. Bei den Werten für den belegten Speicherplatz handelt es sich um Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst.

3. Sehen Sie sich auf der Registerkarte **Raumaufschlüsselung** das Diagramm **Speicherplatzverbrauch** an.

In diesem Diagramm wird der gesamte Speicherplatzverbrauch für alle S3-Buckets des Mandanten angezeigt.

Wenn für diesen Mandanten ein Kontingent festgelegt wurde, wird die Menge des verwendeten und verbleibenden Quotas im Text angezeigt (z. B. `85.00 GB of 100 GB used`). Wenn keine Quote festgelegt wurde, hat der Mieter eine unbegrenzte Quote, und der Text enthält nur eine Menge von Speicherplatz verwendet (zum Beispiel, `85.00 GB used`). Das Balkendiagramm zeigt den Prozentsatz der Quoten in jedem Bucket oder Container. Wenn der Mieter das Speicherkontingent um mehr als 1 % und mindestens 1 GB überschritten hat, zeigt das Diagramm das Gesamtkontingent und den Überschuss an.

Sie können den Cursor über das Balkendiagramm platzieren, um den von jedem Bucket oder Container verwendeten Speicher anzuzeigen. Sie können den Cursor über das Segment freier Speicherplatz platzieren, um die verbleibende Menge an Speicherplatz anzuzeigen.



Die Quotennutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. StorageGRID überprüft beispielsweise das Kontingent, wenn ein Mandant beginnt, Objekte hochzuladen und neue Einlässe zurückweist, wenn der Mieter die Quote überschritten hat. StorageGRID berücksichtigt jedoch bei der Bestimmung, ob das Kontingent überschritten wurde, nicht die Größe des aktuellen Uploads. Wenn Objekte gelöscht werden, kann ein Mandant vorübergehend daran gehindert werden, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Berechnungen der Kontingentnutzung können 10 Minuten oder länger dauern.

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

Sie können die Alarmregel **Tenant Quota Usage High** aktivieren, um festzustellen, ob Tenants ihre Quotas verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Anweisungen hierzu finden Sie unter "Bearbeiten von Meldungsregeln".

4. Überprüfen Sie auf der Registerkarte **Space Breakdown** die **Bucket Details**.

   In dieser Tabelle werden die S3-Buckets für den Mandanten aufgeführt. Der verwendete Speicherplatz ist die Gesamtgröße der Objektdaten im Bucket oder Container. Dieser Wert stellt nicht den Storage-Platzbedarf für ILM-Kopien und Objekt-Metadaten dar.

5. Wählen Sie optional **in CSV exportieren** aus, um eine .csv-Datei anzuzeigen und zu exportieren, die die Nutzungswerte für jeden Bucket oder Container enthält.

   Die Inhalte der Datei eines einzelnen S3-Mandanten `.csv` sehen 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 die Datei in einer Tabellenkalkulationsanwendung öffnen `.csv` oder in der Automatisierung verwenden.

6. Wählen Sie optional die Registerkarte **allowed Features** aus, um eine Liste der Berechtigungen und Funktionen anzuzeigen, die für den Mandanten aktiviert sind. Prüfen Sie"Mandantenkonto bearbeiten", ob Sie eine dieser Einstellungen ändern müssen.
7. Wenn der Mandant die Berechtigung **Grid Federation connection** verwenden hat, wählen Sie optional die Registerkarte **Grid Federation**, um mehr über die Verbindung zu erfahren.

   Siehe "Was ist Grid Federation?" und "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund".

Netzwerkverkehr anzeigen

Wenn Richtlinien zur Traffic-Klassifizierung für einen Mandanten vorhanden sind, überprüfen Sie den Netzwerkverkehr für diesen Mandanten.

Schritte

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

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.

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

Weitere Informationen finden Sie unter "Verwalten von Richtlinien zur Verkehrsklassifizierung" .

Verwenden Sie das Überwachungsprotokoll

Optional können Sie das Revisionsprotokoll für ein granulareres Monitoring der Aktivitäten eines Mandanten verwenden.

Sie können beispielsweise folgende Informationstypen überwachen:

- Bestimmte Client-Vorgänge, z. B. PUT, GET oder DELETE
- Objektgrößen
- Die ILM-Regel wurde auf Objekte angewendet
- Die Quell-IP von Client-Anforderungen

Audit-Protokolle werden in Textdateien geschrieben, die Sie mit einem Tool Ihrer Wahl analysieren können. Dadurch können Sie Kundenaktivitäten besser verstehen oder ausgereifte Chargeback- und Abrechnungsmodelle implementieren.

Weitere Informationen finden Sie unter "Prüfung von Audit-Protokollen" .

Verwenden Sie Prometheus-Kennzahlen

Optional können Sie mit den Prometheus-Kennzahlen Berichte über die Mandantenaktivität 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 den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig.

- Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**. Sie können die Kennzahlen im Abschnitt „Kennzahlen“ der Grid Management API verwenden, um benutzerdefinierte Alarmregeln und Dashboards für Mandantenaktivitäten zu erstellen.

Weitere Informationen finden Sie unter "Prüfen von Support-Kennzahlen" .

Monitoring von S3-Client-Vorgängen

Die Überwachung von Objekteraufnahmeraten und -Abruffraten sowie von Metriken für Objektanzahl, -Abfragen und -Verifizierung Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Client-Applikationen anzeigen, Objekte in StorageGRID zu lesen, zu schreiben und zu ändern.

Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

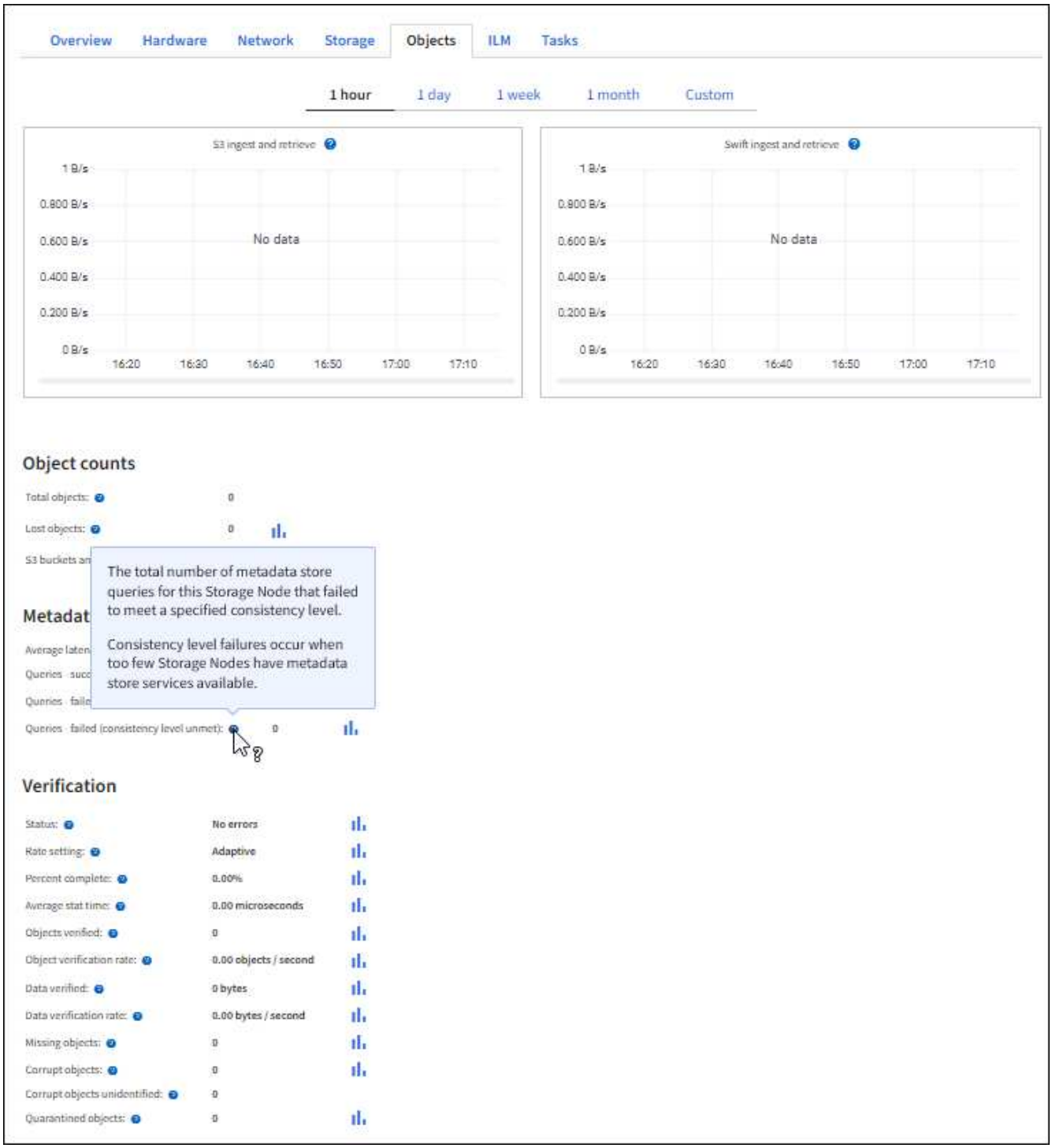
Schritte

1. Wählen Sie im Dashboard die Registerkarte **Performance** aus.
2. Beziehen Sie sich auf die S3-Diagramme, die die Anzahl der von Storage Nodes durchgeführten Clientvorgänge und die Anzahl der API-Anforderungen zusammenfassen, die von Storage Nodes während des ausgewählten Zeitraums empfangen wurden.
3. Wählen Sie **Knoten** aus, um auf die Knotenseite zuzugreifen.
4. Wählen Sie auf der Startseite Knoten (Rasterebene) die Registerkarte **Objekte** aus.

   Das Diagramm zeigt die S3-Aufnahme- und -Abrufraten Ihres gesamten StorageGRID Systems in Byte pro Sekunde sowie die Menge der aufgenommenen oder abgerufenen Daten. Sie können ein Zeitintervall auswählen oder ein benutzerdefiniertes Intervall anwenden.

5. Um Informationen zu einem bestimmten Storage Node anzuzeigen, wählen Sie den Knoten in der Liste auf der linken Seite aus, und wählen Sie die Registerkarte **Objects** aus.

   Im Diagramm werden die Aufnahme- und Abrufraten des Node angezeigt. Die Registerkarte enthält außerdem Kennzahlen für die Anzahl der Objekte, Metadatenabfragen und Verifizierungsvorgänge.



Monitoring von Lastverteilungsvorgängen

Wenn Sie zum Verwalten von Client-Verbindungen zu StorageGRID einen Load Balancer verwenden, sollten Sie die Lastausgleichvorgänge überwachen, nachdem Sie das System zunächst und nachdem Sie Konfigurationsänderungen vorgenommen oder eine Erweiterung durchgeführt haben.

Über diese Aufgabe

Sie können den Load Balancer-Dienst auf Admin-Nodes oder Gateway-Nodes oder einen externen Load Balancer von Drittanbietern verwenden, um Clientanforderungen über mehrere Storage-Nodes zu verteilen.

Nach der Konfiguration des Lastausgleichs sollten Sie bestätigen, dass Einspeisung und Abruf von Objekten gleichmäßig über Storage Nodes verteilt werden. Gleichmäßig verteilte Anfragen stellen sicher, dass StorageGRID weiterhin auf die Workload-Anforderungen reagiert und die Client-Performance erhalten kann.

Wenn Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) von Gateway Nodes oder Admin-Nodes im aktiv-Backup-Modus konfiguriert haben, verteilt nur ein Node in der Gruppe aktiv die Client-Anforderungen.

Weitere Informationen finden Sie unter "S3-Client-Verbindungen konfigurieren".

Schritte

1. Wenn sich S3-Clients über den Load Balancer-Service verbinden, überprüfen Sie, ob Admin-Nodes oder Gateway-Nodes den Datenverkehr aktiv wie erwartet verteilen:
   a. Wählen Sie **Knoten** aus.
   b. Wählen Sie einen Gateway-Node oder einen Admin-Node aus.
   c. Prüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle Primary hat.

      Nodes mit der Rolle „Primär“ und Nodes, die sich nicht in einer HA-Gruppe befinden, sollten Anforderungen aktiv an die Clients verteilen.

   d. Wählen Sie für jeden Knoten, der Clientanforderungen aktiv verteilen soll, die "Registerkarte Load Balancer".
   e. Überprüfen Sie die Tabelle für den Datenverkehr der Lastverteilungsanforderung für die letzte Woche, um sicherzustellen, dass der Knoten die Anforderungen aktiv verteilt hat.

      Nodes in einer aktiv-Backup-HA-Gruppe können die Backup-Rolle von Zeit zu Zeit übernehmen. Während dieser Zeit verteilen die Nodes keine Client-Anforderungen.

   f. Prüfen Sie das Diagramm der eingehenden Lastbalancer-Anfragerate für die letzte Woche, um den Objektdurchsatz des Nodes zu überprüfen.
   g. Wiederholen Sie diese Schritte für jeden Admin-Node oder Gateway-Node im StorageGRID-System.
   h. Optional können Sie mithilfe von Traffic-Klassifizierungsrichtlinien eine detailliertere Analyse des Datenverkehrs anzeigen, der vom Load Balancer Service bedient wird.
2. Stellen Sie sicher, dass diese Anfragen gleichmäßig auf Speicherknoten verteilt werden.
   a. Wählen Sie ***Storage Node*** > **LDR** > **HTTP** aus.
   b. Überprüfen Sie die Anzahl der **derzeit festgelegten eingehenden Sitzungen**.
   c. Wiederholen Sie diesen Vorgang für jeden Speicherknoten im Raster.

      Die Anzahl der Sitzungen sollte ungefähr auf allen Storage-Nodes gleich sein.

Überwachen von Netzverbundverbindungen

Sie können grundlegende Informationen über alle "Netzverbundverbindungen", detaillierte Informationen über eine bestimmte Verbindung oder Prometheus-Metriken über Grid-übergreifende Replikationsvorgänge überwachen. Sie können eine Verbindung von beiden Rastergitten aus überwachen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergitten mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung" für das Raster, bei dem Sie angemeldet sind.

Alle Verbindungen anzeigen

Die Seite Grid Federation enthält grundlegende Informationen zu allen Grid-Verbundverbindungen und zu allen Mandantenkonten, die für die Nutzung von Grid-Verbundverbindungen zugelassen sind.

Schritte

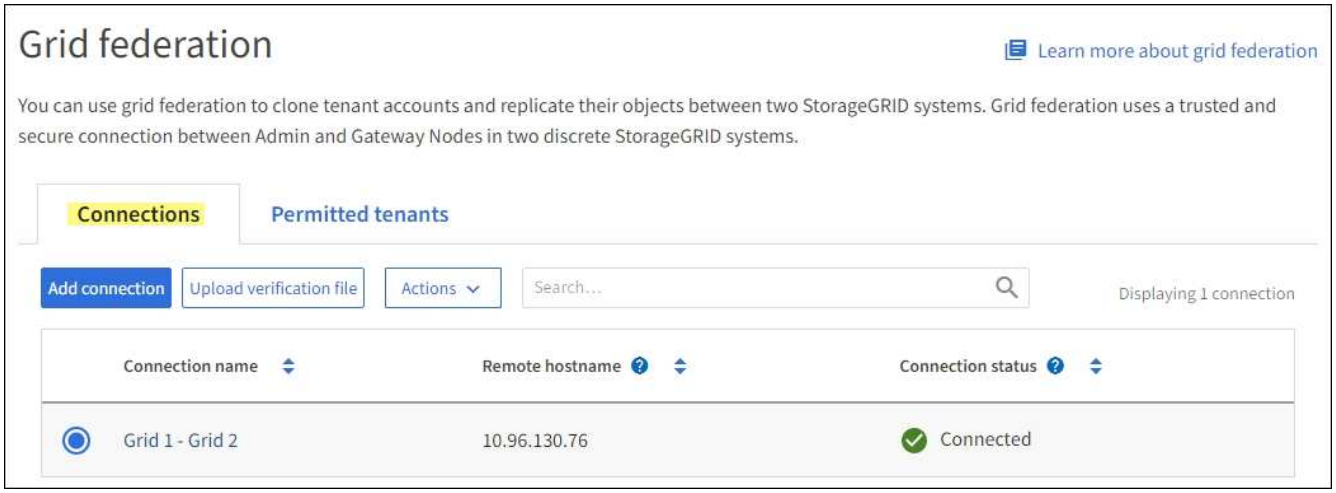
1. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.

   Die Seite Grid Federation wird angezeigt.

2. Um grundlegende Informationen für alle Verbindungen in diesem Raster anzuzeigen, wählen Sie die Registerkarte **Connections**.

   Über diese Registerkarte können Sie:

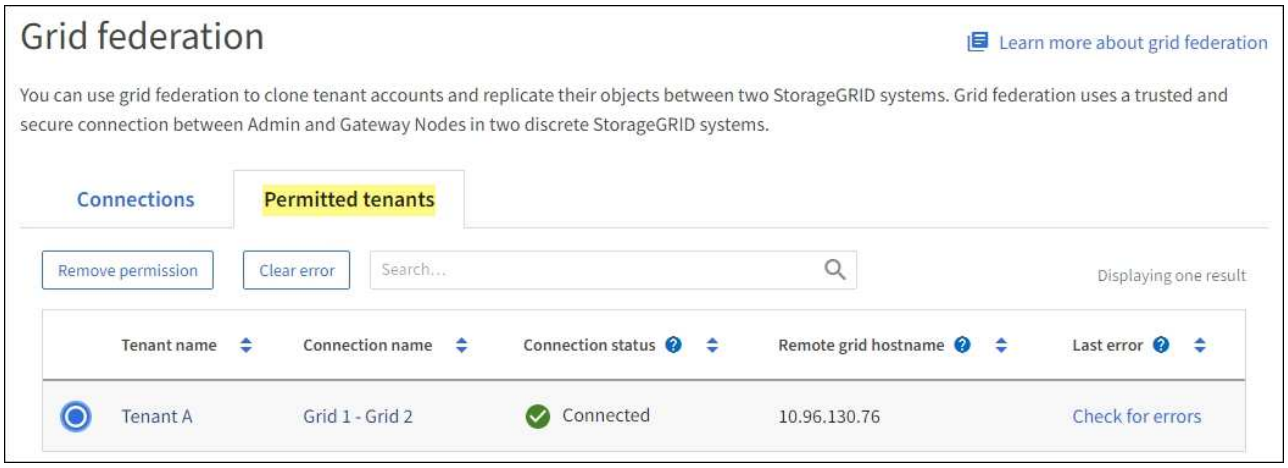
   - "Erstellen Sie eine neue Verbindung".
   - Wählen Sie eine vorhandene Verbindung zu "Bearbeiten oder testen".



3. Um grundlegende Informationen für alle Mandantenkonten in diesem Raster anzuzeigen, die über die Berechtigung **Grid Federation connection** verfügen, wählen Sie die Registerkarte **zulässige Mieter**.

   Über diese Registerkarte können Sie:

   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an".
   - Zeigen Sie die Detailseite für jede Verbindung an. Siehe Zeigen Sie eine bestimmte Verbindung an.
   - Wählen Sie einen zulässigen Mandanten und "Entfernen Sie die Berechtigung".
   - Überprüfen Sie die Grid-übergreifende Replikation, und löschen Sie ggf. den letzten Fehler. Siehe "Fehler beim Grid-Verbund beheben".



eine bestimmte Verbindung anzeigen

Sie können Details für eine bestimmte Grid Federation-Verbindung anzeigen.

Schritte

1. Wählen Sie auf der Seite Grid Federation eine der beiden Registerkarten aus, und wählen Sie dann den Verbindungsnamen aus der Tabelle aus.

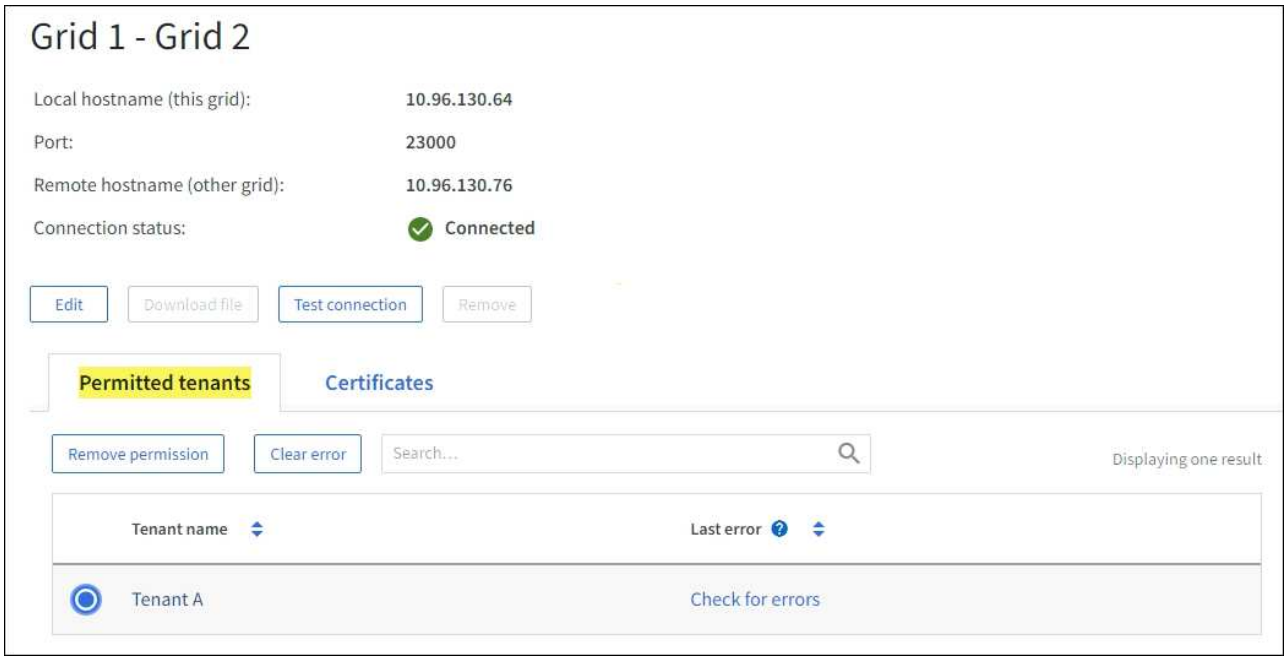
   Auf der Detailseite für die Verbindung können Sie:

   - Hier finden Sie grundlegende Statusinformationen zur Verbindung, einschließlich der lokalen und Remote-Hostnamen, des Ports und des Verbindungsstatus.
   - Wählen Sie eine Verbindung zu "Bearbeiten, testen oder entfernen".

2. Wenn Sie eine bestimmte Verbindung anzeigen, wählen Sie die Registerkarte **zulässige Mandanten**, um Details über die zulässigen Tenants für die Verbindung anzuzeigen.

   Über diese Registerkarte können Sie:

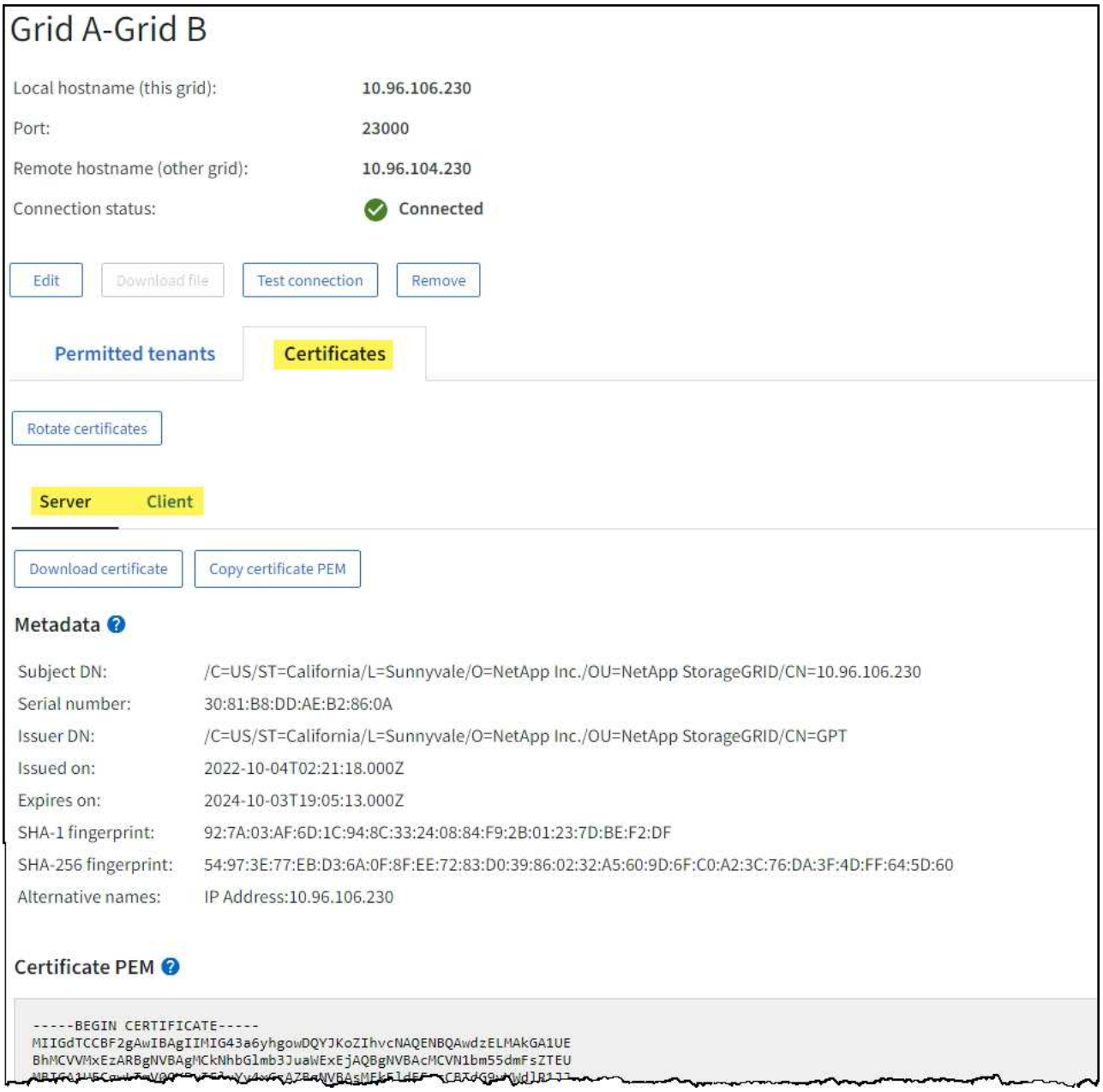
   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an".
   - "Entfernen Sie die Berechtigung eines Mandanten" Um die Verbindung zu verwenden.
   - Überprüfen Sie auf Grid-übergreifende Replikationsfehler, und löschen Sie den letzten Fehler. Siehe "Fehler beim Grid-Verbund beheben".



3. Wenn Sie eine bestimmte Verbindung anzeigen, wählen Sie die Registerkarte **Zertifikate**, um die vom System generierten Server- und Client-Zertifikate für diese Verbindung anzuzeigen.

   Über diese Registerkarte können Sie:

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



Grid-übergreifende Replizierungsmetriken prüfen

Über das Cross-Grid Replication Dashboard in Grafana können Sie Prometheus-Metriken zu Grid-übergreifenden Replikationsvorgängen auf Ihrem Grid anzeigen.

Schritte

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

   Die auf der Seite Metriken verfügbaren Tools sind für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe Liste von "Häufig verwendete Prometheus-Kennzahlen".

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

   Ausführliche Anweisungen finden Sie unter "Prüfen von Support-Kennzahlen".

3. Informationen zum erneuten Replizieren von Objekten, die nicht repliziert werden konnten, finden Sie unter "Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut".

Verwalten von Meldungen

Verwalten von Meldungen

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

Warnmeldungen werden auf bestimmten Schweregraden ausgelöst, wenn Alarmregelbedingungen als wahr bewertet werden. Wenn eine Meldung ausgelöst wird, treten die folgenden Aktionen auf:

- Im Grid Manager wird ein Symbol für den Schweregrad der Warnmeldung im Dashboard angezeigt, und die Anzahl der aktuellen Warnmeldungen wird erhöht.
- Die Warnung wird auf der Übersichtsseite **Knoten** und auf der Registerkarte **Knoten** > ***Knoten*** > **Übersicht** angezeigt.
- Es wird eine E-Mail-Benachrichtigung gesendet, vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und E-Mail-Adressen für die Empfänger bereitgestellt.
- Es wird eine SNMP-Benachrichtigung (Simple Network Management Protocol) gesendet, vorausgesetzt, Sie haben den StorageGRID SNMP-Agent konfiguriert.

Sie können benutzerdefinierte Warnmeldungen erstellen, Warnmeldungen bearbeiten oder deaktivieren und Warnmeldungen verwalten.

Weitere Informationen:

- Sehen Sie sich die Videos an:

  Übersicht über Warnungen

  Benutzerdefinierte Benachrichtigungen

- Weitere Informationen finden Sie im"Alerts Referenz" .

Zeigen Sie Alarmregeln an

Warnungsregeln definieren die Bedingungen, die auslösen "Spezifische Warnmeldungen". StorageGRID enthält eine Reihe von Standardwarnregeln, die Sie unverändert verwenden oder ändern können, oder Sie können individuelle Alarmregeln erstellen.

Sie können die Liste aller Standard- und benutzerdefinierten Warnungsregeln anzeigen, um zu erfahren, welche Bedingungen die einzelnen Warnmeldungen auslösen und feststellen, ob Meldungen deaktiviert sind.

Bevor Sie beginnen

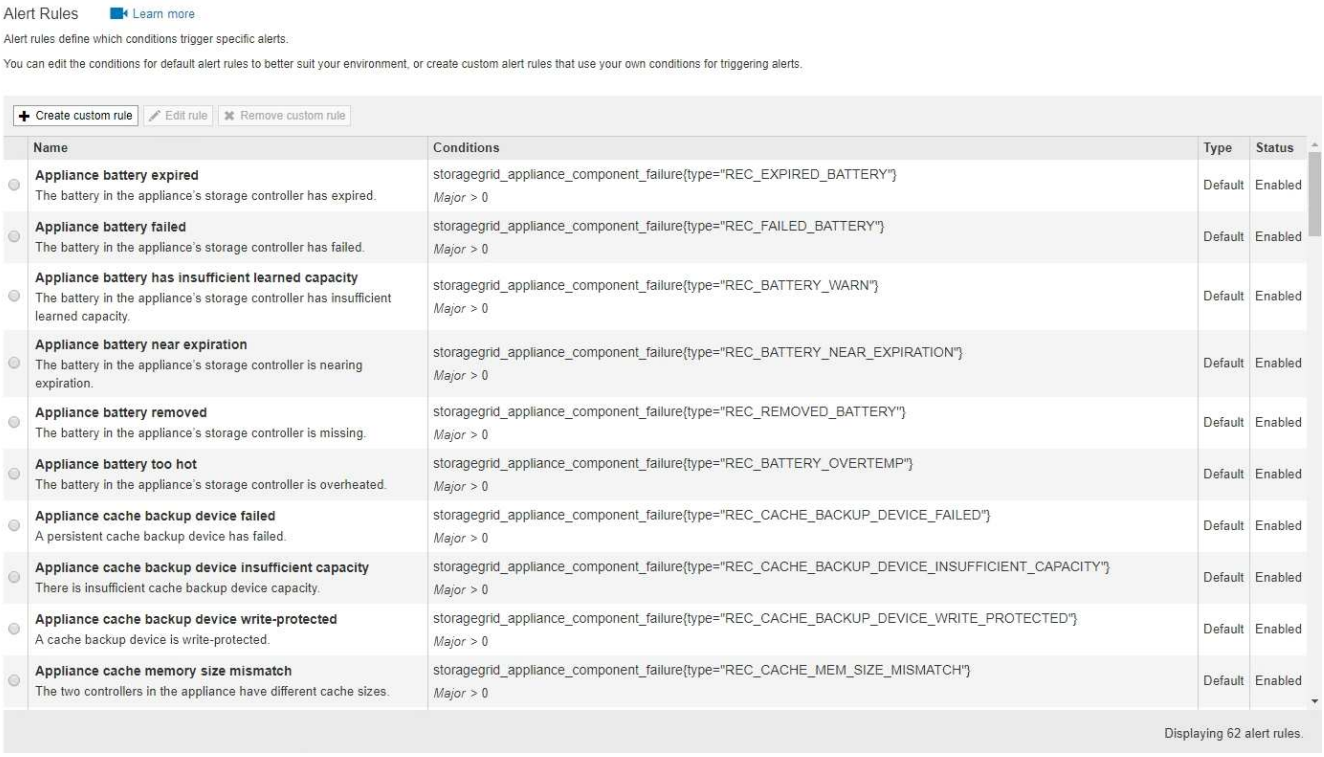
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".
- Optional haben Sie das Video angesehen:

  Übersicht über Warnungen

Schritte

1. Wählen Sie **Benachrichtigungen** > **Regeln**.

   Die Seite Alarmregeln wird angezeigt.



2. Die Informationen in der Tabelle mit den Alarmregeln prüfen:

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

Spaltenüberschrift	Beschreibung
Bestimmten Bedingungen	Die Prometheus Ausdrücke, die bestimmen, wann diese Warnung ausgelöst wird. Eine Meldung kann auf einem oder mehreren der folgenden Schweregrade ausgelöst werden, jedoch ist für jeden Schweregrad ein Zustand nicht erforderlich. • **Kritisch**: Es existiert eine anormale Bedingung, die den normalen Betrieb eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • **Major**: Es existiert eine anormale Bedingung, die entweder den aktuellen Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • **Minor**: das System funktioniert normal, aber es gibt einen abnormalen Zustand, der die Fähigkeit des Systems beeinflussen könnte, wenn es weitergeht. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
Typ	Der Typ der Warnregel: • **Standard**: Eine mit dem System bereitgestellte Warnregel. Sie können eine Standardwarnregel deaktivieren oder die Bedingungen und Dauer für eine Standardwarnregel bearbeiten. Eine Standard-Warnungsregel kann nicht entfernt werden. • **Standard***: Eine Standardwarnregel, die eine bearbeitete Bedingung oder Dauer enthält. Bei Bedarf können Sie eine geänderte Bedingung ganz einfach wieder auf die ursprüngliche Standardeinstellung zurücksetzen. • **Benutzerdefiniert**: Eine Alarmregel, die Sie erstellt haben. Sie können benutzerdefinierte Alarmregeln deaktivieren, bearbeiten und entfernen.
Status	Gibt an, ob diese Warnungsregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnungsregeln werden nicht ausgewertet, sodass keine Warnmeldungen ausgelöst werden.

Erstellen benutzerdefinierter Warnungsregeln

Sie können benutzerdefinierte Alarmregeln erstellen, um eigene Bedingungen für das Auslösen von Warnmeldungen zu definieren.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".
- Sie kennen die "Häufig verwendete Prometheus-Kennzahlen".
- Sie verstehen die "Syntax der Prometheus-Abfragen".
- Optional haben Sie das Video angesehen:

  Benutzerdefinierte Benachrichtigungen

Über diese Aufgabe

StorageGRID validiert keine benutzerdefinierten Warnmeldungen. Wenn Sie sich für die Erstellung benutzerdefinierter Warnungsregeln entscheiden, befolgen Sie die folgenden allgemeinen Richtlinien:

- Informieren Sie sich über die Bedingungen für die Standardwarnregeln und verwenden Sie sie als Beispiele für Ihre benutzerdefinierten Warnungsregeln.
- Wenn Sie mehrere Bedingungen für eine Warnungsregel definieren, verwenden Sie denselben Ausdruck für alle Bedingungen. Ändern Sie dann den Schwellenwert für jede Bedingung.
- Prüfen Sie jede Bedingung sorgfältig auf Tippfehler und Logikfehler.
- Verwenden Sie nur die in der Grid Management API aufgeführten Metriken.
- Beachten Sie beim Testen eines Ausdrucks mit der Grid Management API, dass eine „erfolgreiche“ Antwort möglicherweise ein leerer Antworttext ist (keine Warnung ausgelöst). Um zu überprüfen, ob die Meldung tatsächlich ausgelöst wird, können Sie vorübergehend einen Schwellenwert auf einen Wert festlegen, der Ihrer Meinung nach derzeit „true“ ist.

  Um zum Beispiel den Ausdruck zu testen `node_memory_MemTotal_bytes < 24000000000`, führen Sie zuerst aus `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 gewünschten Werte und führen Sie die Ausführung erneut aus. Keine Ergebnisse zeigen an, dass für diesen Ausdruck keine aktuellen Warnmeldungen vorhanden sind.

- Gehen Sie nicht davon aus, dass eine benutzerdefinierte Warnung funktioniert, es sei denn, Sie haben bestätigt, dass die Warnmeldung erwartungsgemäß ausgelöst wird.

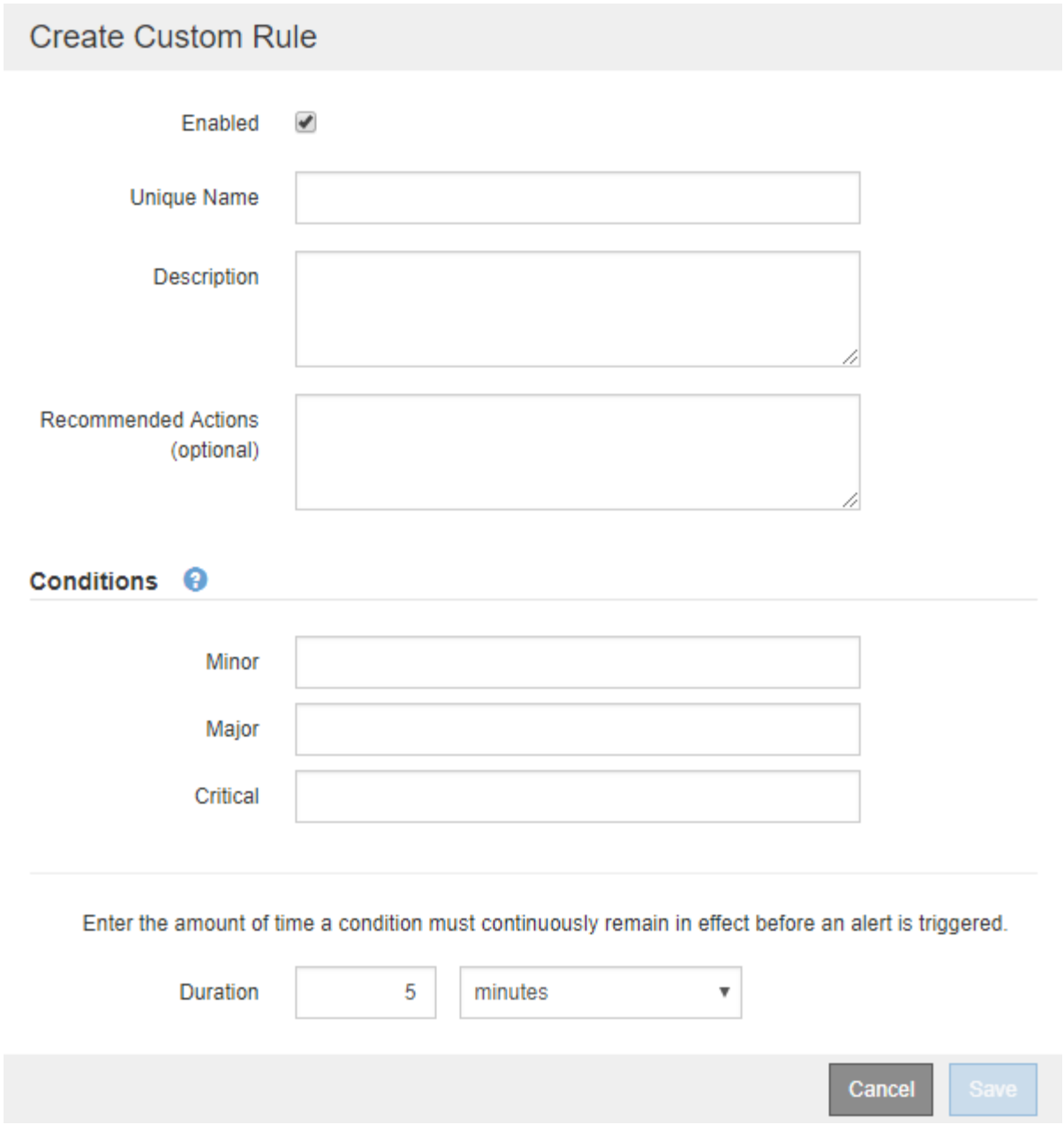
Schritte

1. Wählen Sie **Benachrichtigungen** > **Regeln**.

   Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie **eigene Regel erstellen**.

   Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.



3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **enabled**, um zu bestimmen, ob diese Warnungsregel aktuell aktiviert ist.

   Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.

4. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Alarmregel wird auf der Seite „Meldungen“ angezeigt und ist außerdem Betreff für E-Mail-Benachrichtigungen. Die Namen für Warnungsregeln können zwischen 1 und 64 Zeichen umfassen.

Feld	Beschreibung
Beschreibung	Eine Beschreibung des Problems. Die Beschreibung ist die auf der Seite „Meldungen“ und in E-Mail-Benachrichtigungen angezeigte Warnmeldung. Die Beschreibungen für Warnungsregeln können zwischen 1 und 128 Zeichen umfassen.
Empfohlene Maßnahmen	Optional sind die zu ergriffenen Maßnahmen verfügbar, wenn diese Meldung ausgelöst wird. Geben Sie empfohlene Aktionen als Klartext ein (keine Formatierungscodes). Die empfohlenen Aktionen für Warnungsregeln können zwischen 0 und 1,024 Zeichen liegen.

5. Geben Sie im Abschnitt Bedingungen einen Prometheus-Ausdruck für eine oder mehrere der Schweregrade für Warnmeldungen ein.

   Ein Grundausdruck ist in der Regel die Form:

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

   Ausdrücke können eine beliebige Länge haben, aber in einer einzigen Zeile in der Benutzeroberfläche angezeigt werden. 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 die verfügbaren Metriken anzuzeigen und Prometheus-Ausdrücke zu testen, wählen Sie das Hilfesymbol aus und folgen dem Link zum Abschnitt „Metriken“ der Grid Management API.

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

   Um sofort eine Warnung auszulösen, wenn eine Bedingung wahr wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass temporäre Bedingungen Warnungen auslösen.

   Die Standardeinstellung ist 5 Minuten.

7. Wählen Sie **Speichern**.

   Das Dialogfeld wird geschlossen, und die neue benutzerdefinierte Alarmregel wird in der Tabelle Alarmregeln angezeigt.

Bearbeiten von Meldungsregeln

Sie können eine Meldungsregel bearbeiten, um die Triggerbedingungen zu ändern. Für eine benutzerdefinierte Warnungsregel können Sie auch den Regelnamen, die Beschreibung und die empfohlenen Aktionen aktualisieren.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Über diese Aufgabe

Wenn Sie eine standardmäßige Warnungsregel bearbeiten, können Sie die Bedingungen für kleinere, größere und kritische Warnmeldungen sowie die Dauer ändern. Wenn Sie eine benutzerdefinierte Alarmregel bearbeiten, können Sie auch den Namen, die Beschreibung und die empfohlenen Aktionen der Regel bearbeiten.

> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnungsregel zu bearbeiten. Wenn Sie die Triggerwerte ändern, können Sie möglicherweise ein zugrunde liegendes Problem erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

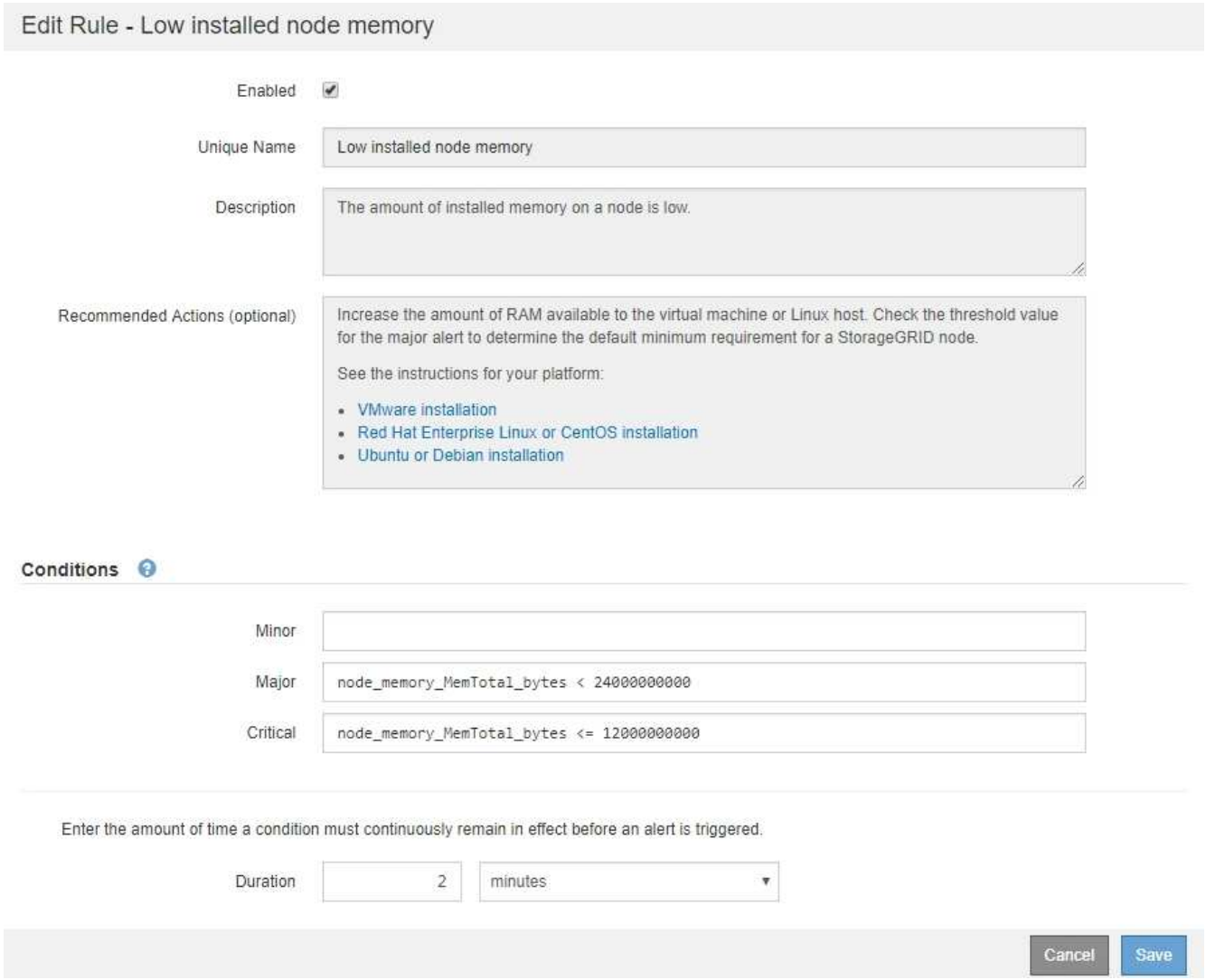
Schritte

1. Wählen Sie **Benachrichtigungen** > **Regeln**.

   Die Seite Alarmregeln wird angezeigt.

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

   Das Dialogfeld Regel bearbeiten wird angezeigt. Dieses Beispiel zeigt eine Standard-Alarmregel: Die Felder eindeutiger Name, Beschreibung und Empfohlene Aktionen sind deaktiviert und können nicht bearbeitet werden.



4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **enabled**, um zu bestimmen, ob diese Warnungsregel aktuell aktiviert ist.

   Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.

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

   Im Allgemeinen wird es nicht empfohlen, eine Standardwarnregel zu deaktivieren. Wenn eine Meldungsregel deaktiviert ist, kann ein zugrunde liegendes Problem möglicherweise erst erkannt werden, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

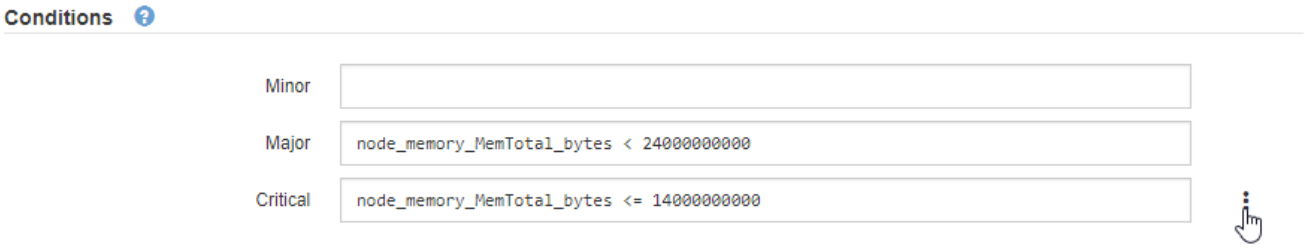
5. Aktualisieren Sie für benutzerdefinierte Warnungsregeln die folgenden Informationen, falls erforderlich.

   Sie können diese Informationen für Standard-Warnungsregeln nicht bearbeiten.

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Alarmregel wird auf der Seite „Meldungen“ angezeigt und ist außerdem Betreff für E-Mail-Benachrichtigungen. Die Namen für Warnungsregeln können zwischen 1 und 64 Zeichen umfassen.
Beschreibung	Eine Beschreibung des Problems. Die Beschreibung ist die auf der Seite „Meldungen“ und in E-Mail-Benachrichtigungen angezeigte Warnmeldung. Die Beschreibungen für Warnungsregeln können zwischen 1 und 128 Zeichen umfassen.
Empfohlene Maßnahmen	Optional sind die zu ergriffenen Maßnahmen verfügbar, wenn diese Meldung ausgelöst wird. Geben Sie empfohlene Aktionen als Klartext ein (keine Formatierungscodes). Die empfohlenen Aktionen für Warnungsregeln können zwischen 0 und 1,024 Zeichen liegen.

6. Geben Sie im Abschnitt Bedingungen den Prometheus-Ausdruck für eine oder mehrere Schweregrade für Warnmeldungen ein oder aktualisieren Sie diesen.

> 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 Meldung aktualisieren, werden Ihre Änderungen möglicherweise erst implementiert, wenn der vorherige Zustand behoben ist. Wenn das nächste Mal eine der Bedingungen für die Regel erfüllt ist, zeigt die Warnmeldung die aktualisierten Werte an.

Ein Grundausdruck ist in der Regel die Form:

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

Ausdrücke können eine beliebige Länge haben, aber in einer einzigen Zeile in der Benutzeroberfläche angezeigt werden. 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** den Zeitraum ein, den eine Bedingung kontinuierlich wirksam bleiben muss, bevor die Warnmeldung ausgelöst wird, und wählen Sie die Zeiteinheit aus.

Um sofort eine Warnung auszulösen, wenn eine Bedingung wahr wird, geben Sie **0** ein. Erhöhen Sie diesen Wert, um zu verhindern, dass temporäre Bedingungen Warnungen auslösen.

Die Standardeinstellung ist 5 Minuten.

8. Wählen Sie **Speichern**.

   Wenn Sie eine Standardwarnregel bearbeitet haben, wird in der Spalte Typ **Standard*** angezeigt. Wenn Sie eine Standard- oder benutzerdefinierte Alarmregel deaktiviert haben, wird in der Spalte **Status deaktiviertes** angezeigt.

Deaktivieren von Meldungsregeln

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Über diese Aufgabe

Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.

> Im Allgemeinen wird es nicht empfohlen, eine Standardwarnregel zu deaktivieren. Wenn eine Meldungsregel deaktiviert ist, kann ein zugrunde liegendes Problem möglicherweise erst erkannt werden, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

Schritte

1. Wählen Sie **Benachrichtigungen** > **Regeln**.

   Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnungsregel, die deaktiviert oder aktiviert werden soll.
3. Wählen Sie **Regel bearbeiten**.

   Das Dialogfeld Regel bearbeiten wird angezeigt.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **enabled**, um zu bestimmen, ob diese Warnungsregel aktuell aktiviert ist.

   Wenn eine Warnungsregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und es werden keine Warnungen ausgelöst.

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

5. Wählen Sie **Speichern**.

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

Entfernen Sie benutzerdefinierte Warnungsregeln

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Schritte

1. Wählen Sie **Benachrichtigungen** > **Regeln**.

   Die Seite Alarmregeln wird angezeigt.

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

   Eine Standard-Warnungsregel kann nicht entfernt werden.

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

   Ein Bestätigungsdialogfeld wird angezeigt.

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

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

Verwalten von Warnmeldungen

Einrichten von SNMP-Benachrichtigungen für Warnmeldungen

Wenn StorageGRID SNMP-Benachrichtigungen senden soll, wenn Warnmeldungen auftreten, müssen Sie den StorageGRID SNMP-Agent 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 zum Konfigurieren des SNMP-Agenten finden Sie unter "Verwenden Sie SNMP-Überwachung".

Nachdem Sie den StorageGRID SNMP-Agent konfiguriert haben, können zwei Arten von ereignisgesteuerten Benachrichtigungen gesendet werden:

- Traps sind Benachrichtigungen, die vom SNMP-Agenten gesendet werden und keine Bestätigung durch das Managementsystem erfordern. Traps dienen dazu, das Managementsystem über etwas innerhalb von StorageGRID zu informieren, wie z. B. eine Warnung, die ausgelöst wird. Traps werden in allen drei Versionen von SNMP unterstützt.
- Informationen sind ähnlich wie Traps, aber sie erfordern eine Bestätigung durch das Management-System. Wenn der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung erhält, wird die Benachrichtigung erneut gesendet, bis eine Bestätigung empfangen wurde oder der maximale Wiederholungswert erreicht wurde. Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

Trap- und Informieren-Benachrichtigungen werden gesendet, wenn eine Standard- oder benutzerdefinierte Warnung auf einem Schweregrad ausgelöst wird. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie eine Stille für die Warnung konfigurieren. Siehe "Benachrichtigung über Stille".

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Pakete und SNMP-Traps und -Benachrichtigungen. Wenn der primäre Admin-Node nicht mehr verfügbar ist, werden vorübergehend Benachrichtigungen von anderen Admin-Nodes gesendet. Siehe "Was ist ein Admin-Node?".

Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein

Wenn E-Mail-Benachrichtigungen gesendet werden sollen, wenn Warnmeldungen auftreten, müssen Sie Informationen über Ihren SMTP-Server angeben. Sie müssen auch E-Mail-Adressen für Empfänger von Benachrichtigungen eingeben.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Über diese Aufgabe

Die für Warnmeldungen verwendete E-Mail-Einrichtung wird für AutoSupport-Pakete nicht verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden.

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Pakete und SNMP-Traps und -Benachrichtigungen. Wenn der primäre Admin-Node nicht mehr verfügbar ist, werden vorübergehend Benachrichtigungen von anderen Admin-Nodes gesendet. Siehe "Was ist ein Admin-Node?".

Schritte

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

   Die Seite E-Mail-Einrichtung wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, um anzugeben, dass Benachrichtigungs-E-Mails gesendet werden sollen, wenn Benachrichtigungen 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	Eingabe
Mailserver	Der vollständig qualifizierte Domänenname (FQDN) oder die IP-Adresse des SMTP-Servers.

Feld	Eingabe
Port	Der Port, der für den Zugriff auf den SMTP-Server verwendet wird. Muss zwischen 1 und 65535 liegen.
Benutzername (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen ein, mit dem Sie sich authentifizieren möchten.
Kennwort (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie das Kennwort für die Authentifizierung ein.

4. Geben Sie im Abschnitt E-Mail-Adressen die E-Mail-Adressen für den Absender und für jeden Empfänger ein.
   a. Geben Sie für die **Absender E-Mail-Adresse** eine gültige E-Mail-Adresse an, die als Absenderadresse für Benachrichtigungen verwendet werden soll.

      Beispiel: `storagegrid-alerts@example.com`

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

      Wählen Sie das Plus-Symbol, um Empfänger hinzuzufügen.

5. Wenn Transport Layer Security (TLS) für die Kommunikation mit dem SMTP-Server 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 Identifizierung des SMTP-Servers verwendet wird.

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

      Sie müssen eine einzelne Datei bereitstellen, die die Zertifikate jeder Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

   b. Aktivieren Sie das Kontrollkästchen **Client-Zertifikat senden**, wenn Ihr SMTP-E-Mail-Server E-Mail-Absender benötigt, um Clientzertifikate für die Authentifizierung bereitzustellen.
   c. Geben Sie im Feld **Client Certificate** das PEM-codierte Clientzertifikat an, das an den SMTP-Server gesendet werden kann.

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

   d. Geben Sie im Feld **Private Key** den privaten Schlüssel für das Clientzertifikat in unverschlüsselter PEM-Codierung ein.

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

      Wenn Sie das E-Mail-Setup bearbeiten müssen, wählen Sie das Bleistiftsymbol aus, um dieses Feld zu aktualisieren.

6. Wählen Sie im Abschnitt Filter aus, welche Alarmschweregrade zu E-Mail-Benachrichtigungen führen soll, es sei denn, die Regel für eine bestimmte Warnung wurde stummgeschaltet.

Schweregrad	Beschreibung
Klein, groß, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die kleine, größere oder kritische Bedingung für eine Alarmregel erfüllt wird.
Kritisch	Wenn die Hauptbedingung für eine Warnmeldung erfüllt ist, wird eine E-Mail-Benachrichtigung gesendet. Benachrichtigungen werden nicht für kleinere Warnmeldungen gesendet.
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur gesendet, wenn die kritische Bedingung für eine Alarmregel erfüllt ist. Benachrichtigungen werden nicht für kleinere oder größere Warnmeldungen 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 angibt, dass eine Test-E-Mail gesendet wurde.

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

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

   c. Melden Sie sich bei anderen Admin-Knoten an und senden Sie eine Test-E-Mail, um die Verbindung von allen Standorten zu überprüfen.

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

8. Wählen Sie **Speichern**.

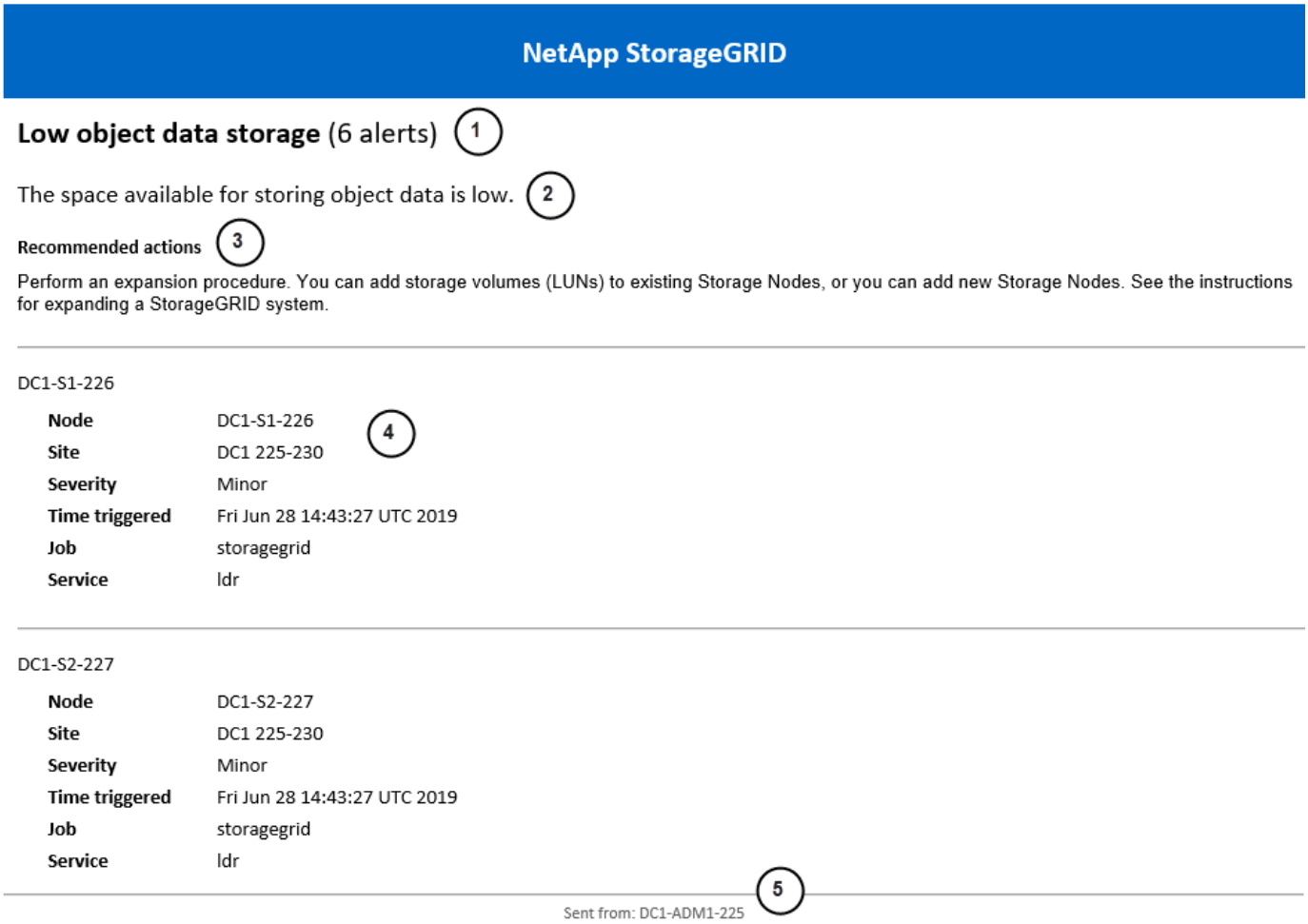
   Beim Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Sie müssen **Speichern** wählen.

   Die E-Mail-Einstellungen werden gespeichert.

Informationen, die in E-Mail-Benachrichtigungen für Warnmeldungen enthalten sind

Nachdem Sie den SMTP-E-Mail-Server konfiguriert haben, werden beim Auslösen einer Warnung E-Mail-Benachrichtigungen an die angegebenen Empfänger gesendet, es sei denn, die Alarmregel wird durch Stille unterdrückt. Siehe "Benachrichtigung über Stille".

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



Legende	Beschreibung
1	Der Name der Warnmeldung, gefolgt von der Anzahl der aktiven Instanzen dieser Warnmeldung.
2	Die Beschreibung der Warnmeldung.
3	Alle empfohlenen Aktionen für die Warnmeldung
4	Details zu jeder aktiven Instanz der Warnmeldung, einschließlich des betroffenen Node und Standorts, des Meldungsschweregrads, der UTC-Zeit, zu der die Meldungsregel ausgelöst wurde, und des Namens des betroffenen Jobs und Service.
5	Der Hostname des Admin-Knotens, der die Benachrichtigung gesendet hat.

Gruppierung von Warnungen

Um zu verhindern, dass bei der Auslösung von Warnmeldungen eine übermäßige Anzahl von E-Mail-Benachrichtigungen gesendet wird, versucht StorageGRID, mehrere Warnmeldungen in derselben Benachrichtigung zu gruppieren.

In der folgenden Tabelle finden Sie Beispiele, wie StorageGRID mehrere Warnmeldungen in E-Mail-Benachrichtigungen gruppiert.

Verhalten	Beispiel
Jede Warnbenachrichtigung gilt nur für Warnungen, die denselben Namen haben. Wenn zwei Benachrichtigungen mit verschiedenen Namen gleichzeitig ausgelöst werden, werden zwei E-Mail-Benachrichtigungen gesendet.	• Bei zwei Nodes wird gleichzeitig ein Alarm A ausgelöst. Es wird nur eine Benachrichtigung gesendet. • Bei Knoten 1 wird die Warnmeldung A ausgelöst, und gleichzeitig wird auf Knoten 2 die Warnmeldung B ausgelöst. Für jede Warnung werden zwei Benachrichtigungen gesendet.
Wenn für eine bestimmte Warnmeldung auf einem bestimmten Node die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird eine Benachrichtigung nur für die schwerste Warnmeldung gesendet.	• Die Warnmeldung A wird ausgelöst und die kleineren, größeren und kritischen Alarmschwellenwerte werden erreicht. Eine Benachrichtigung wird für die kritische Warnmeldung gesendet.
Bei der ersten Alarmauslösung wartet StorageGRID zwei Minuten, bevor eine Benachrichtigung gesendet wird. Wenn während dieser Zeit andere Warnmeldungen mit demselben Namen ausgelöst werden, gruppiert StorageGRID alle Meldungen in der ersten Benachrichtigung.	1. Alarm A wird auf Knoten 1 um 08:00 ausgelöst. Es wird keine Benachrichtigung gesendet. 2. Alarm A wird auf Knoten 2 um 08:01 ausgelöst. Es wird keine Benachrichtigung gesendet. 3. Um 08:02 Uhr wird eine Benachrichtigung gesendet, um beide Instanzen der Warnmeldung zu melden.
Falls eine weitere Benachrichtigung 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), selbst wenn sie zuvor gemeldet wurden.	1. Alarm A wird auf Knoten 1 um 08:00 ausgelöst. Eine Benachrichtigung wird um 08:02 Uhr gesendet. 2. Alarm A wird auf Knoten 2 um 08:05 ausgelöst. Eine zweite Benachrichtigung wird um 08:15 Uhr (10 Minuten später) versendet. Beide Nodes werden gemeldet.
Wenn mehrere aktuelle Warnmeldungen mit demselben Namen vorliegen und eine dieser Meldungen gelöst wird, wird eine neue Benachrichtigung nicht gesendet, wenn die Meldung auf dem Node, für den die Meldung behoben wurde, erneut auftritt.	1. Alarm A wird für Node 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Alarm A wird für Node 2 ausgelöst. Eine zweite Benachrichtigung wird gesendet. 3. Die Warnung A wird für Knoten 2 behoben, bleibt jedoch für Knoten 1 aktiv. 4. Für Node 2 wird erneut eine Warnmeldung A ausgelöst. Es wird keine neue Benachrichtigung gesendet, da die Meldung für Node 1 noch aktiv ist.
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnmeldung gelöst oder die Alarmregel stummgeschaltet wurde.	1. Am 8. März wird Alarm A für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Warnung A ist nicht gelöst oder stummgeschaltet. Weitere Benachrichtigungen erhalten Sie am 15. März, 22. März 29 usw.

Beheben Sie Warnmeldungen bei E-Mail-Benachrichtigungen

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Schritte

1. Überprüfen Sie Ihre Einstellungen.
   a. Wählen Sie **Benachrichtigungen** > **E-Mail-Setup**.
   b. Überprüfen Sie, ob die Einstellungen des SMTP-Servers (E-Mail) korrekt sind.
   c. Stellen Sie sicher, dass Sie gültige E-Mail-Adressen für die Empfänger angegeben haben.
2. Überprüfen Sie Ihren Spam-Filter, und stellen Sie sicher, dass die E-Mail nicht an einen Junk-Ordner gesendet wurde.
3. Bitten Sie Ihren E-Mail-Administrator, zu bestätigen, 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 anhand der in den Protokollen enthaltenen Informationen ermitteln, was schief gelaufen ist. Beispielsweise kann die Datei prometheus.log einen Fehler anzeigen, wenn Sie eine Verbindung zu dem von Ihnen angegebenen Server herstellen.

   Siehe "Erfassen von Protokolldateien und Systemdaten".

Benachrichtigung über Stille

Optional können Sie Stille konfigurieren, um Benachrichtigungen vorübergehend zu unterdrücken.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Über diese Aufgabe

Sie können Alarmregeln für das gesamte Grid, eine einzelne Site oder einen einzelnen Knoten und für einen oder mehrere Schweregrade stummschalten. Bei jeder Silence werden alle Benachrichtigungen für eine einzelne Warnungsregel oder für alle Warnungsregeln unterdrückt.

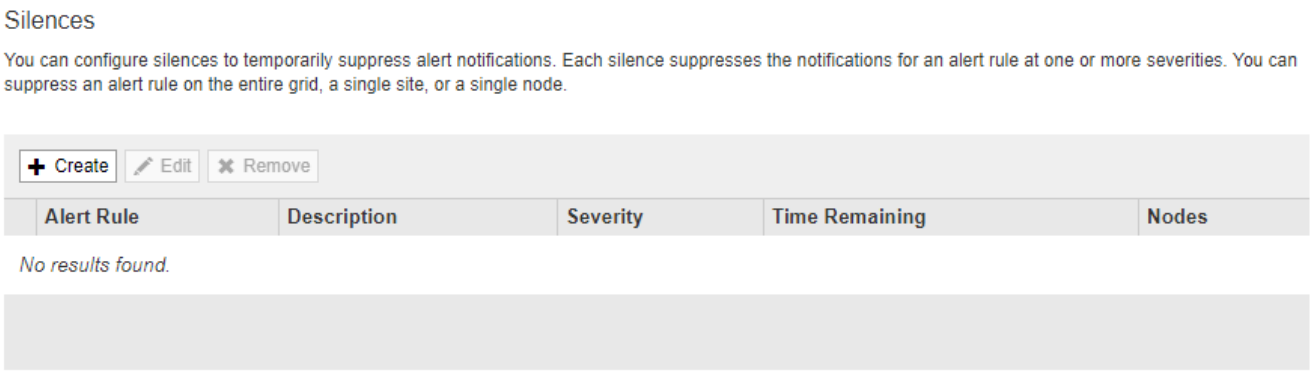
Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.

> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn Sie eine Warnmeldung stummschalten, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

Schritte

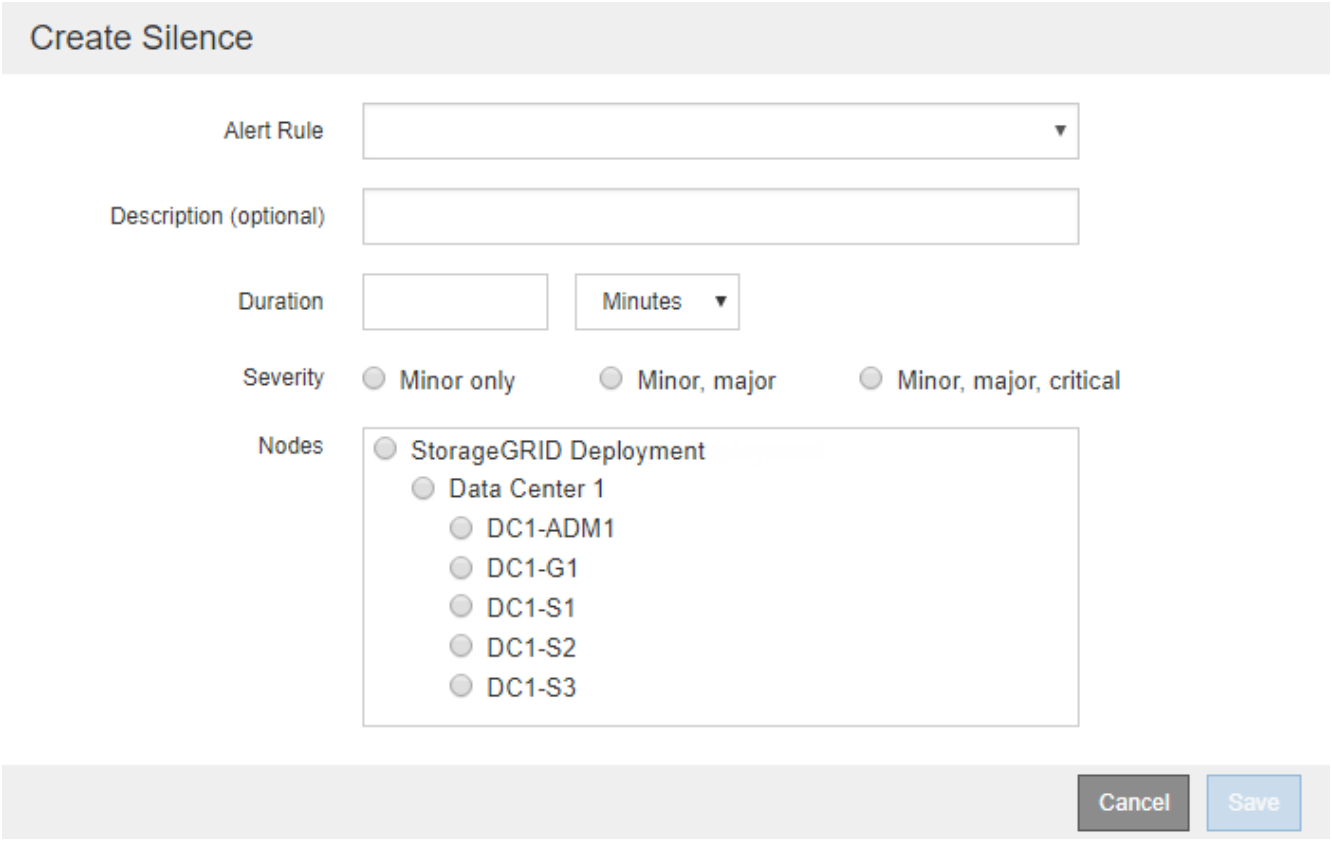
1. Wählen Sie **Warnungen** > **Stummschaltungen**.

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
Meldungsregel	Der Name der Alarmregel, die Sie stumm schalten möchten. Sie können eine beliebige Standard- oder benutzerdefinierte Warnungsregel auswählen, auch wenn die Alarmregel deaktiviert ist. **Hinweis:** Wählen Sie **Alle Regeln** aus, wenn Sie alle Alarmregeln mit den in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.

Feld	Beschreibung
Beschreibung	Optional eine Beschreibung der Stille. Beschreiben Sie zum Beispiel den Zweck dieser Stille.
Dauer	Wie lange Sie möchten, dass diese Stille in Minuten, Stunden oder Tagen wirksam bleibt. Eine Stille kann von 5 Minuten bis 1,825 Tage (5 Jahre) in Kraft sein. **Hinweis:** eine Alarmregel sollte nicht für längere Zeit stummgemacht werden. Wenn eine Alarmregel stumm geschaltet ist, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang abgeschlossen wird. Möglicherweise müssen Sie jedoch eine erweiterte Stille verwenden, wenn eine Warnung durch eine bestimmte, vorsätzliche Konfiguration ausgelöst wird, wie z. B. bei den **Services Appliance Link Down**-Alarmen und den **Storage Appliance Link down**-Alarmen.
Schweregrad	Welche Alarmschweregrade oder -Schweregrade stummgeschaltet werden sollten. Wenn die Warnung bei einem der ausgewählten Schweregrade ausgelöst wird, werden keine Benachrichtigungen gesendet.
Knoten	Auf welchen Knoten oder Knoten Sie diese Stille anwenden möchten. Sie können eine Meldungsregel oder alle Regeln im gesamten Grid, einer einzelnen Site oder einem einzelnen Node unterdrücken. Wenn Sie das gesamte Raster auswählen, gilt die Stille für alle Standorte und alle Knoten. Wenn Sie einen Standort auswählen, gilt die Stille nur für die Knoten an diesem Standort. **Hinweis:** Sie können nicht mehr als einen Knoten oder mehr als einen Standort für jede Stille auswählen. Sie müssen zusätzliche Stille erstellen, wenn Sie dieselbe Warnungsregel auf mehr als einem Node oder mehreren Standorten 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
Stille bearbeiten	a. Wählen Sie **Warnungen** > **Stummschaltungen**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille, 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**.

Option	Beschreibung
Entfernen Sie eine Stille	a. Wählen Sie **Warnungen** > **Stummschaltungen**. b. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie entfernen möchten. c. Wählen Sie **Entfernen**. d. Wählen Sie **OK**, um zu bestätigen, dass Sie diese Stille entfernen möchten. **Hinweis**: Benachrichtigungen werden jetzt gesendet, wenn diese Warnung ausgelöst wird (es sei denn, sie werden durch eine andere Stille unterdrückt). Wenn diese Warnmeldung derzeit ausgelöst wird, kann es einige Minuten dauern, bis E-Mail- oder SNMP-Benachrichtigungen gesendet werden und die Seite „Meldungen“ aktualisiert wird.

Verwandte Informationen

"Konfigurieren Sie den SNMP-Agent"

Alerts Referenz

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

Bei Bedarf können Sie benutzerdefinierte Alarmregeln erstellen, die Ihrem Systemmanagement entsprechen.

Einige der Standardwarnungen verwenden "Kennzahlen von Prometheus".

Appliance-Warnungen

Alarmname	Beschreibung
Akku des Geräts abgelaufen	Der Akku im Speicher-Controller des Geräts ist abgelaufen.
Akku des Geräts fehlgeschlagen	Der Akku im Speicher-Controller des Geräts ist ausgefallen.
Der Akku des Geräts weist nicht genügend Kapazität auf	Der Akku im Speicher-Controller des Geräts weist nicht genügend Kapazität auf.
Akku des Geräts befindet sich nahe dem Ablauf	Der Akku im Speicher-Controller des Geräts läuft langsam ab.
Akku des Geräts entfernt	Der Akku im Speicher-Controller des Geräts fehlt.
Der Akku des Geräts ist zu heiß	Die Batterie im Speicher-Controller des Geräts ist überhitzt.

Alarmname	Beschreibung
Fehler bei der BMC-Kommunikation des Geräts	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren.
Fehler des Gerät-Startgeräts erkannt	Es wurde ein Problem mit dem Startgerät in der Appliance festgestellt.
Fehler beim Sichern des Appliance-Cache	Ein persistentes Cache-Sicherungsgerät ist fehlgeschlagen.
Gerät-Cache-Backup-Gerät unzureichende Kapazität	Die Kapazität des Cache-Sicherungsgeräts ist nicht ausreichend.
Appliance Cache Backup-Gerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt.
Die Größe des Appliance-Cache-Speichers stimmt nicht überein	Die beiden Controller im Gerät haben unterschiedliche Cache-Größen.
Appliance-CMOS-Batteriefehler	Es wurde ein Problem mit der CMOS-Batterie im Gerät festgestellt.
Die Temperatur des Computing-Controller-Chassis des Geräts ist zu hoch	Die Temperatur des Computing-Controllers in einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.
Die CPU-Temperatur des Appliance-Compute-Controllers ist zu hoch	Die Temperatur der CPU im Computing-Controller einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.
Aufmerksamkeit für Compute-Controller ist erforderlich	Im Compute-Controller einer StorageGRID-Appliance wurde ein Hardwarefehler erkannt.
Ein Problem besteht in der Stromversorgung Des Computercontrollers A des Geräts	Bei Netzteil A im Compute-Controller ist ein Problem aufgetreten.
Das Netzteil B des Compute-Controllers ist ein Problem	Die Stromversorgung B im Compute-Controller hat ein Problem.
Der Service zur Überwachung der Computing-Hardware des Appliances ist ausgesetzt	Der Dienst, der den Status der Speicherhardware überwacht, ist blockiert.
Das-Laufwerk der Appliance überschreitet die Obergrenze für die pro Tag geschriebenen Daten	Jeden Tag wird eine übermäßige Menge an Daten auf ein Laufwerk geschrieben, wodurch die Gewährleistung erlöschen kann.

Alarmname	Beschreibung
Fehler des Appliance-das-Laufwerks erkannt	Bei einem Direct-Attached Storage (das)-Laufwerk in der Appliance wurde ein Problem festgestellt.
Das DAS-Laufwerk der Appliance befindet sich im falschen Steckplatz oder Knoten	Ein DAS-Laufwerk (Direct Attached Storage) befindet sich im falschen Steckplatz oder Knoten
Die LED für die das-Laufwerksfinder der Appliance leuchtet	Die Laufwerksfinder-LED für ein oder mehrere Direct-Attached Storage (das)-Laufwerke in einem Appliance-Storage-Node ist eingeschaltet.
Wiederherstellung des Appliance-das-Laufwerks	Ein Direct-Attached Storage (das)-Laufwerk wird neu erstellt. Dies wird erwartet, wenn es vor kurzem ersetzt oder entfernt/wieder eingesetzt wurde.
Fehler des Gerätelüfters erkannt	Es wurde ein Problem mit einer Lüftereinheit im Gerät festgestellt.
Fibre-Channel-Fehler des Geräts erkannt	Zwischen dem Appliance-Storage-Controller und dem Rechner-Controller wurde ein Fibre-Channel-Verbindungsproblem festgestellt
Fehler des Fibre-Channel-HBA-Ports des Geräts	Ein Fibre-Channel-HBA-Port ist ausgefallen oder ist ausgefallen.
Appliance Flash Cache Laufwerke sind nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal.
Geräteverbindung/Batteriebehälter entfernt	Der Verbindungs-/Batteriebehälter fehlt.
Geräte-LACP-Port fehlt	Ein Port auf einer StorageGRID-Appliance beteiligt sich nicht an der LACP-Verbindung.
Appliance-NIC-Fehler erkannt	Es wurde ein Problem mit einer Netzwerkkarte (NIC) im Gerät festgestellt.
Das gesamte Netzteil des Geräts ist heruntergestuft	Die Leistung eines StorageGRID-Geräts ist von der empfohlenen Betriebsspannung abweichen.
Appliance SANtricity OS-Softwareupdate erforderlich	Die SANtricity -Softwareversion ist niedriger als das empfohlene Minimum für diese Version von StorageGRID.
Kritische Warnung bei Appliance-SSD	Eine Appliance-SSD meldet eine kritische Warnung.
Ausfall des Appliance Storage Controller A	Der Speicher-Controller A in einer StorageGRID-Appliance ist ausgefallen.

Alarmname	Beschreibung
Fehler beim Speicher-Controller B des Geräts	Bei Speicher-Controller B in einer StorageGRID-Appliance ist ein Fehler aufgetreten.
Laufwerksausfall des Appliance-Storage-Controllers	Mindestens ein Laufwerk in einer StorageGRID-Appliance ist ausgefallen oder nicht optimal.
Hardwareproblem des Appliance Storage Controllers	SANtricity meldet, dass für eine Komponente einer StorageGRID Appliance ein Hinweis erforderlich ist.
Ausfall der Stromversorgung des Speicher-Controllers	Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abweichen.
Fehler bei Netzteil B des Speicher-Controllers	Stromversorgung B bei einem StorageGRID-Gerät hat von der empfohlenen Betriebsspannung abweichen.
Monitordienst der Appliance-Storage-Hardware ist ausgesetzt	Der Dienst, der den Status der Speicherhardware überwacht, ist blockiert.
Appliance Storage-Shelfs ist beeinträchtigt	Der Status einer der Komponenten im Storage Shelf für eine Storage Appliance ist beeinträchtigt.
Gerätetemperatur überschritten	Die nominale oder maximale Temperatur für den Lagercontroller des Geräts wurde überschritten.
Temperatursensor des Geräts entfernt	Ein Temperatursensor wurde entfernt.
Fehler beim sicheren Start der Appliance-UEFI	Ein Gerät wurde nicht sicher gestartet.
Die Festplatten-I/O ist sehr langsam	Sehr langsamer Festplatten-I/O kann die Grid-Performance beeinträchtigen.
Lüfterfehler des Speichergeräts erkannt	Es wurde ein Problem mit einer Lüftereinheit im Speicher-Controller für eine Appliance festgestellt.
Die Storage-Konnektivität der Storage-Appliance ist herabgesetzt	Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller.
Speichergerät nicht zugänglich	Auf ein Speichergerät kann nicht zugegriffen werden.

Audit- und Syslog-Warnmeldungen

Alarmname	Beschreibung
Audit-Protokolle werden der Warteschlange im Speicher hinzugefügt	Der Node kann Protokolle nicht an den lokalen Syslog-Server senden, und die Warteschlange im Speicher wird ausgefüllt.
Fehler bei der Weiterleitung des externen Syslog-Servers	Der Node kann Protokolle nicht an den externen Syslog-Server weiterleiten.
Große Audit-Warteschlange	Die Festplattenwarteschlange für Prüfmeldungen ist voll. Wenn dieser Zustand nicht behoben wird, können S3-Vorgänge fehlschlagen.
Protokolle werden der Warteschlange auf der Festplatte hinzugefügt	Der Node kann Protokolle nicht an den externen Syslog-Server weiterleiten, und die Warteschlange auf der Festplatte wird ausgefüllt.

Bucket-Warnmeldungen

Alarmname	Beschreibung
FabricPool Bucket hat die nicht unterstützte Bucket-Konsistenzeinstellung	Ein FabricPool-Bucket verwendet die verfügbare oder strong-site-Konsistenzstufe, die nicht unterstützt wird.
FabricPool Bucket hat nicht unterstützte Versionierung	In einem FabricPool Bucket ist die Versionierung oder die S3-Objektsperrung aktiviert, die nicht unterstützt werden.

Cassandra – Warnmeldungen

Alarmname	Beschreibung
Cassandra Auto-Kompaktor-Fehler	Beim Cassandra Auto-Kompaktor ist ein Fehler aufgetreten.
Cassandra Auto-Kompaktor-Kennzahlen veraltet	Die Kennzahlen, die den Cassandra Auto-Kompaktor beschreiben, sind veraltet.
Cassandra Kommunikationsfehler	Die Nodes, auf denen der Cassandra-Service ausgeführt wird, haben Probleme bei der Kommunikation untereinander.
Cassandra-Kompensation überlastet	Der Cassandra-Verdichtungsprozess ist überlastet.
Cassandra-Fehler bei der Übergröße des Schreibvorgangs	Bei einem internen StorageGRID-Prozess wurde eine zu große Schreibanforderung an Cassandra gesendet.
Veraltete Reparaturkennzahlen für Cassandra	Die Kennzahlen, die Cassandra-Reparaturaufträge beschreiben, sind veraltet.

Alarmname	Beschreibung
Cassandra Reparaturfortschritt langsam	Der Fortschritt der Cassandra-Datenbankreparaturen ist langsam.
Cassandra Reparaturservice nicht verfügbar	Der Cassandra-Reparaturservice ist nicht verfügbar.
Cassandra Tabelle beschädigt	Cassandra hat Tabellenbeschädigungen erkannt. Cassandra wird automatisch neu gestartet, wenn Tabellenbeschädigungen erkannt werden.

Warnmeldungen für Cloud-Storage-Pool

Alarmname	Beschreibung
Verbindungsfehler beim Cloud-Storage-Pool	Bei der Zustandsprüfung für Cloud-Storage-Pools wurde ein oder mehrere neue Fehler erkannt.
IAM Roles Anywhere End-Entity-Zertifizierung Ablauf	IAM-Rollen überall dort, wo das End-Entity-Zertifikat abläuft.

Warnmeldungen bei Grid-übergreifender Replizierung

Alarmname	Beschreibung
Dauerhafter Ausfall der Grid-übergreifenden Replizierung	Es ist ein gitterübergreifender Replikationsfehler aufgetreten, der vom Benutzer behoben werden muss.
Grid-übergreifende Replizierungsressourcen nicht verfügbar	Grid-übergreifende Replikationsanforderungen stehen aus, da eine Ressource nicht verfügbar ist.

DHCP-Warnungen

Alarmname	Beschreibung
DHCP-Leasing abgelaufen	Der DHCP-Leasingvertrag auf einer Netzwerkschnittstelle ist abgelaufen.
DHCP-Leasing läuft bald ab	Der DHCP-Lease auf einer Netzwerkschnittstelle läuft demnächst aus.
DHCP-Server nicht verfügbar	Der DHCP-Server ist nicht verfügbar.

Debug- und Trace-Warnungen

Alarmname	Beschreibung
Leistungsbeeinträchtigung debuggen	Wenn der Debug-Modus aktiviert ist, kann sich die Systemleistung negativ auswirken.
Trace-Konfiguration aktiviert	Wenn die Trace-Konfiguration aktiviert ist, kann die Systemleistung beeinträchtigt werden.

E-Mail- und AutoSupport-Benachrichtigungen

Alarmname	Beschreibung
Fehler beim Senden der AutoSupport-Nachricht	Die letzte AutoSupport-Meldung konnte nicht gesendet werden.
Auflösung des Domänennamens fehlgeschlagen	Der StorageGRID-Knoten konnte die Domänennamen nicht auflösen.
E-Mail-Benachrichtigung fehlgeschlagen	Die E-Mail-Benachrichtigung für eine Warnmeldung konnte nicht gesendet werden.
Ziel-Bucket für Protokollarchivierung nicht gefunden	Der Ziel-Bucket für die Protokollarchivierung fehlt, wodurch die Archivierung der Protokolle im Ziel-Bucket verhindert wird.
SNMP-Inform-Fehler	Fehler beim Senden von SNMP-Benachrichtigungen an ein Trap-Ziel.
Externer SSH-Zugriff aktiviert	Der externe SSH-Zugriff ist seit mehr als 24 Stunden aktiviert.
SSH- oder Konsole-Anmeldung erkannt	In den letzten 24 Stunden hat sich ein Benutzer über die Webkonsole oder SSH angemeldet.

Alarme für Erasure Coding (EC)

Alarmname	Beschreibung
EC-Ausgleichfehler	Das EC-Ausgleichverfahren ist fehlgeschlagen oder wurde gestoppt.
EC-Reparaturfehler	Ein Reparaturauftrag für EC-Daten ist fehlgeschlagen oder wurde angehalten.
EC-Reparatur blockiert	Ein Reparaturauftrag für EC-Daten ist blockiert.
Fehler bei der Verifizierung von Fragmenten, die nach der Löschung codiert wurden	Fragmente, die mit der Löschung codiert wurden, können nicht mehr verifiziert werden. Beschädigte Fragmente werden möglicherweise nicht repariert.

Ablauf von Zertifikatwarnungen

Alarmname	Beschreibung
Ablauf des Zertifikats der Administrator-Proxy-Zertifizierungsstelle	Mindestens ein Zertifikat im CA-Paket des Admin-Proxy-Servers läuft bald ab.
Ablauf des Client-Zertifikats	Mindestens ein Clientzertifikat läuft bald ab.
Ablauf des globalen Serverzertifikats für S3	Das globale Serverzertifikat für S3 läuft bald ab.
Ablauf des Endpunktzertifikats des Load Balancer	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen kurz vor dem Ablauf.
Ablauf des Serverzertifikats für die Verwaltungsschnittstelle	Das für die Managementoberfläche verwendete Serverzertifikat läuft bald ab.
Ablauf des externen Syslog CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des externen Syslog-Serverzertifikats verwendet wird, läuft in Kürze ab.
Ablauf des externen Syslog-Client-Zertifikats	Das Client-Zertifikat für einen externen Syslog-Server läuft kurz vor dem Ablauf.
Ablauf des externen Syslog-Serverzertifikats	Das vom externen Syslog-Server präsentierte Serverzertifikat läuft bald ab.

Warnmeldungen zum Grid-Netzwerk

Alarmname	Beschreibung
MTU-Diskrepanz bei dem Grid-Netzwerk	Die MTU-Einstellung für die Grid Network-Schnittstelle (eth0) unterscheidet sich deutlich von Knoten im Grid.

Warnmeldungen zu Grid-Verbund

Alarmname	Beschreibung
Ablauf des Netzverbundzertifikats	Ein oder mehrere Grid Federation-Zertifikate laufen demnächst ab.
Fehler bei der Verbindung mit dem Grid-Verbund	Die Netzverbundverbindung zwischen dem lokalen und dem entfernten Netz funktioniert nicht.

Warnmeldungen bei hoher Auslastung oder hoher Latenz

Alarmname	Beschreibung
Hohe Java-Heap-Nutzung	Es wird ein hoher Prozentsatz von Java Heap Space verwendet.
Hohe Latenz bei Metadatenanfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.

Warnmeldungen zur Identitätsföderation

Alarmname	Beschreibung
Synchronisierungsfehler bei der Identitätsföderation	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren.
Fehler bei der Synchronisierung der Identitätsföderation für einen Mandanten	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren, die von einem Mandanten konfiguriert wurde.

Warnmeldungen für Information Lifecycle Management (ILM)

Alarmname	Beschreibung
ILM-Platzierung nicht erreichbar	Für bestimmte Objekte kann keine Platzierung in einer ILM-Regel erzielt werden.
ILM-Scan-Rate niedrig	Die ILM-Scan-Rate ist auf weniger als 100 Objekte/Sekunde eingestellt.

KMS-Warnungen (Key Management Server)

Alarmname	Beschreibung
ABLAUF DES KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des KMS-Zertifikats (Key Management Server) verwendet wird, läuft bald ab.
ABLAUF DES KMS-Clientzertifikats	Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft demnächst ab
KMS-Konfiguration konnte nicht geladen werden	Es ist die Konfiguration für den Verschlüsselungsmanagement-Server vorhanden, konnte aber nicht geladen werden.
KMS-Verbindungsfehler	Ein Appliance-Node konnte keine Verbindung zum Schlüsselmanagementserver für seinen Standort herstellen.
DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt.

Alarmname	Beschreibung
DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen	Alle Appliance-Volumes wurden erfolgreich entschlüsselt, ein oder mehrere Volumes konnten jedoch nicht auf den neuesten Schlüssel gedreht werden.
KM ist nicht konfiguriert	Für diesen Standort ist kein Schlüsselverwaltungsserver vorhanden.
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	Ein oder mehrere Volumes auf einer Appliance mit aktivierter Node-Verschlüsselung konnten nicht mit dem aktuellen KMS-Schlüssel entschlüsselt werden.
Ablauf DES KMS-Serverzertifikats	Das vom KMS (Key Management Server) verwendete Serverzertifikat läuft in Kürze ab.
KMS-Serververbindungsfehler	Ein Appliance-Knoten konnte keine Verbindung zu einem oder mehreren Servern im Key Management Server-Cluster für seinen Standort herstellen.

Warnmeldungen zum Load Balancer

Alarmname	Beschreibung
Erhöhte Load Balancer-Verbindungen ohne Anforderung	Ein erhöhter Prozentsatz an Verbindungen zu Endpunkten des Lastausgleichs, die ohne Durchführung von Anfragen getrennt wurden.

Lokale Zeitversatz-Warnungen

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

Warnungen zu wenig Speicher oder zu wenig Speicherplatz

Alarmname	Beschreibung
Geringe Kapazität der Auditprotokoll-Festplatte	Der für Audit-Protokolle verfügbare Speicherplatz ist gering. Wenn dieser Zustand nicht behoben wird, können S3-Vorgänge fehlschlagen.
Niedriger verfügbarer Node-Speicher	Die RAM-Menge, die auf einem Knoten verfügbar ist, ist gering.
Wenig freier Speicherplatz für den Speicherpool	Der verfügbare Speicherplatz zum Speichern von Objektdaten im Storage Node ist gering.
Wenig installierter Node-Speicher	Der installierte Arbeitsspeicher auf einem Node ist gering.

Alarmname	Beschreibung
Niedriger Metadaten-Storage	Der zur Speicherung von Objektmetadaten verfügbare Speicherplatz ist gering.
Niedrige Kenngrößen für die Festplattenkapazität	Der für die Kennzahlendatenbank verfügbare Speicherplatz ist gering.
Niedriger Objekt-Storage	Der zum Speichern von Objektdaten verfügbare Platz ist gering.
Low Read-Only-Wasserzeichen überschreiben	Das weiche, schreibgeschützte Wasserzeichen des Speichervolumes liegt unter dem minimalen optimierten Wasserzeichen für einen Speicher-Node.
Niedrige Root-Festplattenkapazität	Der auf der Stammfestplatte verfügbare Speicherplatz ist gering.
Niedrige Datenkapazität des Systems	Der für /var/local verfügbare Speicherplatz ist gering. Wenn dieser Zustand nicht behoben wird, können S3-Vorgänge fehlschlagen.
Geringer Tmp-Telefonspeicherplatz	Der im Verzeichnis /tmp verfügbare Speicherplatz ist gering.

Warnmeldungen für das Node- oder Node-Netzwerk

Alarmname	Beschreibung
ADC-Quorum nicht erreicht	Speicherknoten mit ADC-Dienst ist offline. Erweiterungs- und Außerbetriebnahmevorgänge werden blockiert, bis das ADC-Quorum wiederhergestellt ist.
Admin-Netzwerk Nutzung erhalten	Die Empfangsauslastung im Admin-Netzwerk ist hoch.
Admin Netzwerk Übertragungsnutzung	Die Übertragungsnutzung im Admin-Netzwerk ist hoch.
Fehler bei der Firewall-Konfiguration	Firewall-Konfiguration konnte nicht angewendet werden.
Endpunkte der Managementoberfläche im Fallback-Modus	Alle Endpunkte der Managementoberfläche sind zu lange auf die Standardports zurückgefallen.
Fehler bei der Node-Netzwerkverbindung	Beim Übertragen der Daten zwischen den Nodes ist ein Fehler aufgetreten.
Node-Netzwerkannahme-Frame-Fehler	Bei einem hohen Prozentsatz der Netzwerkframes, die von einem Node empfangen wurden, gab es Fehler.

Alarmname	Beschreibung
Der Node ist nicht mit dem NTP-Server synchronisiert	Der Node ist nicht mit dem NTP-Server (Network Time Protocol) synchronisiert.
Der Node ist nicht mit dem NTP-Server gesperrt	Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt.
Nicht-Appliance-Knotennetzwerk ausgefallen	Mindestens ein Netzwerkgerät ist ausgefallen oder nicht verbunden.
Verbindung zur Service-Appliance im Admin-Netzwerk getrennt	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Services-Appliance-Verbindung am Admin-Netzwerkanschluss 1 getrennt	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden.
Verbindung zur Service-Appliance im Client-Netzwerk getrennt	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 1 getrennt	Netzwerkport 1 auf der Appliance ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 2 getrennt	Netzwerkport 2 auf der Appliance ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 3 getrennt	Netzwerkport 3 auf der Appliance ist ausgefallen oder getrennt.
Verbindung zur Service-Appliance auf Netzwerkport 4 getrennt	Netzwerkport 4 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Storage-Appliance im Admin-Netzwerk getrennt	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) ist ausgefallen oder getrennt.
Verknüpfung der Speicher-Appliance auf Admin-Netzwerk-Port 1 ausgefallen	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden.
Verbindung der SpeicherAppliance im Client-Netzwerk getrennt	Die Appliance-Schnittstelle zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung der Speicher-Appliance auf Netzwerkport 1 getrennt	Netzwerkport 1 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Speicher-Appliance auf Netzwerkport 2 getrennt	Netzwerkport 2 auf der Appliance ist ausgefallen oder getrennt.

Alarmname	Beschreibung
Verbindung der Speicher-Appliance auf Netzwerkport 3 getrennt	Netzwerkport 3 auf der Appliance ist ausgefallen oder getrennt.
Verbindung der Speicher-Appliance auf Netzwerkport 4 getrennt	Netzwerkport 4 auf der Appliance ist ausgefallen oder getrennt.
Storage-Node befindet sich nicht im gewünschten Speicherzustand	Der LDR-Service auf einem Storage Node kann aufgrund eines internen Fehlers oder eines Volume-bezogenen Problems nicht in den gewünschten Status wechseln
Verwendung der TCP-Verbindung	Die Anzahl der TCP-Verbindungen auf diesem Knoten nähert sich der maximalen Anzahl, die nachverfolgt werden kann.
Kommunikation mit Knoten nicht möglich	Mindestens ein Service reagiert nicht oder der Node kann nicht erreicht werden.
Unerwarteter Node-Neustart	Ein Node wurde in den letzten 24 Stunden unerwartet neu gebootet.

Objektwarnmeldungen

Alarmname	Beschreibung
Überprüfung der Objektexistenz fehlgeschlagen	Der Job für die Objektexistisprüfung ist fehlgeschlagen.
Prüfung der ObjektExistenz ist blockiert	Der Job zur Prüfung der ObjektExistenz ist blockiert.
Möglicherweise verlorene Objekte	Ein oder mehrere Objekte sind möglicherweise aus dem Raster verschwunden.
Verwaiste Objekte erkannt	Es wurden verwaiste Objekte erkannt.
S3 PUT Objekt size zu groß	Ein Client versucht, eine PUT-Objekt-Operation durchzuführen, die die S3-Größenlimits überschreitet.
Nicht identifizierte beschädigte Objekte erkannt	Im replizierten Objekt-Storage wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte.

Warnungen bei Objektbeschädigung

Alarmname	Beschreibung
Objektgröße stimmt nicht überein	Bei der Überprüfung der Objektexistenz wurde eine unerwartete Objektgröße erkannt.

Benachrichtigungen zu Plattform-Services

Alarmname	Beschreibung
Plattform-Services ausstehende Anforderungskapazität niedrig	Die Anzahl der ausstehenden Anfragen für Plattformdienste nähert sich der Kapazität.
Plattform-Services nicht verfügbar	Zu wenige Speicherknoten mit dem RSM-Service laufen oder sind an einem Standort verfügbar.

Warnmeldungen zu Storage-Volumes

Alarmname	Beschreibung
Das Storage-Volume muss beachtet werden	Ein Storage Volume ist offline und muss beachtet werden.
Das Speicher-Volume muss wiederhergestellt werden	Ein Speicher-Volume wurde wiederhergestellt und muss wiederhergestellt werden.
Das Storage-Volume ist offline	Ein Storage-Volume war seit mehr als 5 Minuten offline.
Versuch einer Neueinbindung des Speicher-Volumes	Ein Storage Volume war offline und löste eine automatische Neueinbindung aus. Dies kann auf ein Laufwerksproblem oder Dateisystemfehler hinweisen.
Die Volume-Wiederherstellung konnte die Reparatur replizierter Daten nicht starten	Die Reparatur replizierter Daten für ein repariertes Volume konnte nicht automatisch gestartet werden.

Warnmeldungen zu StorageGRID-Services

Alarmname	Beschreibung
Nginx-Dienst mit Backup-Konfiguration	Die Konfiguration des nginx-Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.
Nginx-gw-Dienst mit Backup-Konfiguration	Die Konfiguration des nginx-gw-Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.
Zum Deaktivieren von FIPS ist ein Neustart erforderlich	Die Sicherheitsrichtlinie erfordert keinen FIPS-Modus, aber es werden FIPS-Module verwendet.
Neustart erforderlich zur Aktivierung von FIPS	Die Sicherheitsrichtlinie erfordert den FIPS-Modus, aber es werden keine FIPS-Module verwendet.
SSH-Service unter Verwendung der Backup-Konfiguration	Die Konfiguration des SSH-Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.

Mandantenwarnmeldungen

Alarmname	Beschreibung
Hohe Kontingentnutzung für Mandanten	Ein hoher Prozentsatz des Quota-Speicherplatzes wird verwendet. Diese Regel ist standardmäßig deaktiviert, da sie möglicherweise zu viele Benachrichtigungen verursacht.

Häufig verwendete Prometheus-Kennzahlen

In dieser Liste der häufig verwendeten Prometheus-Kennzahlen können Sie die Bedingungen in den Standardwarnungsregeln besser verstehen oder die Bedingungen für benutzerdefinierte Warnungsregeln erstellen.

Sie können auch Holen Sie sich eine vollständige Liste aller Kennzahlen.

Details zur Syntax von Prometheus-Abfragen finden Sie unter "Prometheus Wird Abgefragt".

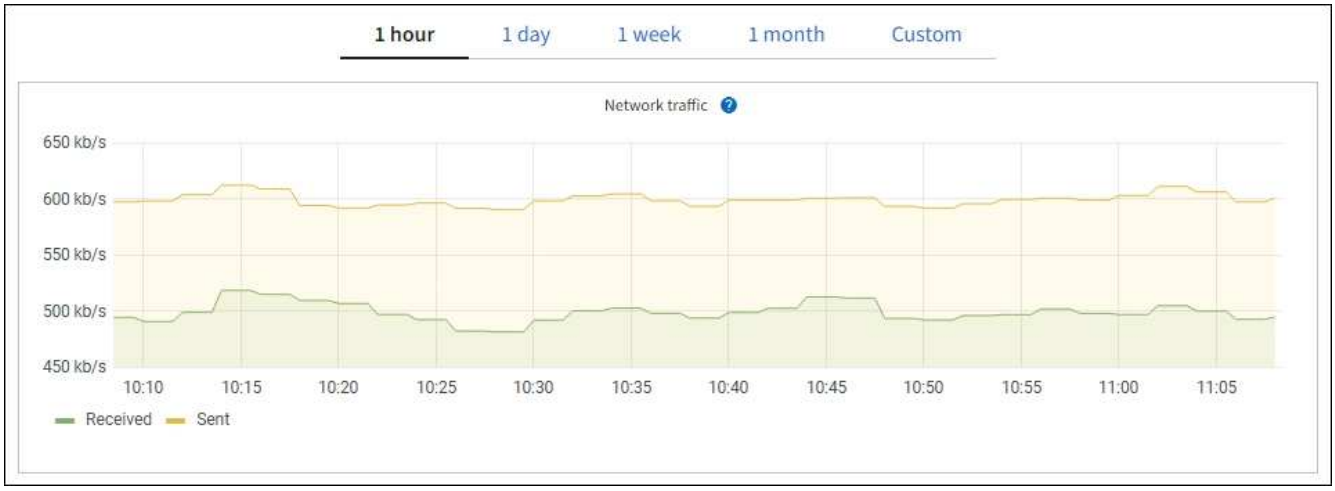
Was sind Prometheus-Kennzahlen?

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

Wo werden Prometheus-Kennzahlen verwendet?

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

- **Knoten Seite**: Die Grafiken und Diagramme auf den Registerkarten, die auf der Seite Knoten verfügbar sind, zeigen mit dem Grafana Visualization Tool die von Prometheus erfassten Zeitreihenmetriken an. Grafana zeigt Zeitserien-Daten im Diagramm- und Diagrammformat an, Prometheus dient als Back-End-Datenquelle.



- **Alerts**: Warnmeldungen werden auf bestimmten Schweregraden ausgelöst, wenn Alarmregelbedingungen, die Prometheus-Metriken verwenden, als wahr bewerten.
- **Grid Management API**: Sie können Prometheus-Kennzahlen in benutzerdefinierten Alarmregeln oder mit externen Automatisierungstools verwenden, um Ihr StorageGRID-System zu überwachen. Eine

vollständige Liste der Prometheus-Kennzahlen finden Sie über die Grid Management API. (Klicken Sie oben im Grid Manager auf das Hilfesymbol und wählen Sie **API-Dokumentation** > **metrics**.) Während mehr als tausend Kennzahlen zur Verfügung stehen, ist nur eine relativ kleine Zahl zur Überwachung der kritischsten StorageGRID Vorgänge erforderlich.

> Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen 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 häufigsten Kennzahlen

Die folgende Liste enthält die am häufigsten verwendeten Prometheus Kennzahlen.

> Metriken, die *private* in ihren Namen enthalten, sind nur für den internen Gebrauch und können ohne vorherige Ankündigung zwischen StorageGRID Versionen geändert werden.

Alertmanager_notifications_failed_total
Die Gesamtzahl der fehlgeschlagenen Warnmeldungen.

Node_Filesystem_verfügbare_Byte
Die Menge des Dateisystemspeichers, der nicht-Root-Benutzern in Byte zur Verfügung steht.

Node_Memory_MemAvailable_Bytes
Feld Speicherinformationen MemAvailable_Bytes.

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

Node_Network_receive_errs_total
Netzwerkgerätestatistik `receive_errs`.

Node_Network_transmit_errs_total
Netzwerkgerätestatistik `transmit_errs`.

storagegrid_administrativ_down
Der Node ist aus einem erwarteten Grund nicht mit dem Grid verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert.

storagegrid_Appliance_Compute_Controller_Hardware_Status
Der Status der Computing-Controller-Hardware in einer Appliance.

storagegrid_Appliance_failed_Disks
Für den Speicher-Controller in einer Appliance die Anzahl der Laufwerke, die nicht optimal sind.

storagegrid_Appliance_Storage_Controller_Hardware_Status

Der Gesamtstatus der Hardware eines Storage Controllers in einer Appliance.

storagegrid_Content_Buckets_und_Containern

Die Gesamtzahl der diesem Speicherknoten bekannten S3-Buckets.

storagegrid_Content_Objects

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

storagegrid_Content_Objects_Lost

Gesamtzahl der vom StorageGRID System erkannten Objekte, die von diesem Service als fehlend erkannt werden. Es sollten Maßnahmen ergriffen werden, um die Ursache des Schadens zu ermitteln und ob eine Erholung möglich ist.

"Fehlerbehebung bei verlorenen und fehlenden Objektdaten"

storagegrid_http_Sessions_Incoming_versuchte

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

storagegrid_http_Sessions_Incoming_derzeit_etabliertes

Die Anzahl der derzeit aktiven HTTP-Sitzungen (offen) auf dem Speicherknoten.

storagegrid_http_Sessions_INCOMING_FAILED

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

storagegrid_http_Sessions_Incoming_successful

Die Gesamtzahl der erfolgreich abgeschlossenen HTTP-Sitzungen.

storagegrid_ilm_awaiting_background_Objects

Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus dem Scan warten

storagegrid_ilm_awaiting_Client_Evaluation_Objects_per_Second

Die aktuelle Rate, mit der Objekte im Vergleich zur ILM-Richtlinie auf diesem Node bewertet werden.

storagegrid_ilm_awaiting_Client_Objects

Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus den Client-Vorgängen (z. B. Aufnahme) warten

storagegrid_ilm_awaiting_total_Objects

Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten

storagegrid_ilm_Scan_Objects_per_Second

Die Geschwindigkeit, mit der Objekte des Node gescannt und für ILM in der Warteschlange gestellt werden.

storagegrid_ilm_Scan_Period_Geschätzter_Minuten

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

Hinweis: Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die sich im Besitz dieses Knotens befinden.

storagegrid_Load_Balancer_Endpoint_cert_expiry_time

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

storagegrid_Metadatenabfragen_average_Latency_Millisekunden

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

storagegrid_Network_received_Byte

Die Gesamtmenge der seit der Installation empfangenen Daten.

storagegrid_Network_transmited_Byte

Die Gesamtmenge der seit der Installation gesendeten Daten.

storagegrid_Node_cpu_Utifficienty_percenty

Der Prozentsatz der verfügbaren CPU-Zeit, die derzeit von diesem Service genutzt wird. Gibt an, wie beschäftigt der Dienst ist. Die verfügbare CPU-Zeit hängt von der Anzahl der CPUs für den Server ab.

storagegrid_ntp_Chooed_time_source_Offset_Millisekunden

Systematischer Zeitversatz, der von einer ausgewählten Zeitquelle bereitgestellt wird. Offset wird eingeführt, wenn die Verzögerung zum Erreichen einer Zeitquelle nicht der Zeit entspricht, die für das Erreichen des NTP-Clients benötigt wird.

storagegrid_ntp_gesperrt

Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt.

storagegrid_s3_Data_Transfers_Bytes_aufgenommen

Die Gesamtmenge an Daten, die seit dem letzten Zurücksetzen des Attributs von S3-Clients auf diesen Storage-Node aufgenommen wurden.

storagegrid_s3_Data_Transfers_Bytes_abgerufen

Die Gesamtanzahl der Daten, die von S3-Clients von diesem Speicherknoten seit dem letzten Zurücksetzen des Attributs abgerufen wurden.

storagegrid_s3_Operations_fehlgeschlagen

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

storagegrid_s3_Operations_erfolgreich

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

storagegrid_s3_Operations_nicht autorisiert

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

storagegrid_Servercertifikat_Management_Interface_cert_expiry_days

Die Anzahl der Tage vor Ablauf des Managementschnittstelle-Zertifikats.

storagegrid_Serverzertifikat_Storage_API_endpunktes_cert_expiry_days

Die Anzahl der Tage, bevor das Objekt-Speicher-API-Zertifikat abläuft.

storagegrid_Service_cpu_Sekunden

Der kumulierte Zeitaufwand, die die CPU seit der Installation bei diesem Service verwendet hat.

storagegrid_Service_Memory_Usage_Byte

Die Speichermenge (RAM), die derzeit von diesem Dienst verwendet wird. Dieser Wert ist identisch mit dem, der vom Linux-Top-Dienstprogramm als RES angezeigt wird.

storagegrid_Service_Network_received_Byte

Die Gesamtanzahl der Daten, die seit der Installation von diesem Service eingehen.

storagegrid_Service_Network_transmited_Byte

Die Gesamtanzahl der von diesem Service gesendeten Daten.

storagegrid_Service_startet neu

Die Gesamtanzahl der Neustarts des Dienstes.

storagegrid_Service_Runtime_seconds

Die Gesamtzeit, die der Service seit der Installation ausgeführt hat.

storagegrid_Service_Uptime_Sekunden

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

storagegrid_Storage_State_current

Der aktuelle Status der Storage-Services. Attributwerte sind:

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

storagegrid_Storage_Status

Der aktuelle Status der Storage-Services. Attributwerte sind:

- 0 = Keine Fehler
- 10 = In Transition
- 20 = Nicht Genügend Freier Speicherplatz
- 30 = Volume(s) nicht verfügbar
- 40 = Fehler

storagegrid_Storage_Utilization_Data_Bytes

Eine Schätzung der Gesamtgröße der replizierten und Erasure-Coded-Objektdaten auf dem Storage Node.

storagegrid_Storage_Utiffici“_Metadata_allowed_Bytes

Der gesamte Speicherplatz auf Volume 0 jedes Storage-Node, der für Objekt-Metadaten zulässig ist. Dieser Wert ist immer kleiner als der tatsächlich für Metadaten auf einem Node reservierte Speicherplatz, da für grundlegende Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades ein Teil des reservierten Speicherplatzes benötigt wird. Der zulässige Speicherplatz für Objektmetadaten steuert die allgemeine Objektkapazität.

storagegrid_Storage_Utifficiendatiy_Metadata_Bytes

Die Menge der Objekt-Metadaten auf dem Storage-Volume 0 in Bytes.

storagegrid_Storage_Utifficienfficienals_total_space_Bytes

Der gesamte Speicherplatz, der allen Objektspeichern zugewiesen ist.

storagegrid_Storage_Utiable_space_Bytes

Die verbleibende Menge an Objekt-Storage. Berechnet durch Hinzufügen der verfügbaren Menge an Speicherplatz für alle Objektspeichern auf dem Storage-Node.

storagegrid_Tenant_Usage_Data_Byte

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, die für die Objekte des Mandanten verfügbar ist Wenn keine Quota-Metrik angegeben wird, steht eine unbegrenzte Menge an Speicherplatz zur Verfügung.

Eine Liste aller Kennzahlen abrufen

[[Alle Metriken abrufen]]um die vollständige Liste der Metriken zu erhalten, verwenden Sie die Grid Management API.

Schritte

1. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
2. Suchen Sie nach den **Metriken**-Vorgängen.
3. Führen Sie den `GET /grid/metric-names` Vorgang aus.
4. Ergebnisse herunterladen

Referenz für Protokolldateien

Referenz für Protokolldateien

StorageGRID stellt Protokolle bereit, die zum Erfassen von Ereignissen, Diagnosemeldungen und Fehlerbedingungen verwendet werden. Möglicherweise werden Sie gebeten, Protokolldateien zu sammeln und an den technischen Support zu leiten, um bei der Fehlerbehebung zu helfen.

Die Protokolle werden wie folgt kategorisiert:

- "StorageGRID-Softwareprotokolle"
- "Protokoll für Implementierung und Wartung"
- "Etwa bycast.log"

> Die Details, die für jeden Protokolltyp angegeben sind, dienen nur als Referenz. Die Protokolle sind für erweiterte Fehlerbehebung durch den technischen Support bestimmt. Fortschrittliche Techniken, die die Wiederherstellung des Problemverlaufs mit Hilfe der Audit-Protokolle und der Anwendung Log-Dateien beinhalten, liegen über den Umfang dieser Anweisungen hinaus.

Greifen Sie auf die Protokolle zu

Um auf die Protokolle zuzugreifen, können Sie"Erfassen von Protokolldateien und Systemdaten" von einem oder mehreren Knoten als einzelnes Protokolldateiarchiv. Alternativ können Sie wie folgt auf die einzelnen Protokolldateien für jeden Grid-Knoten zugreifen:

Schritte

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

Exportieren Sie Protokolle auf den Syslog-Server

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

- Erhalten Sie zusätzlich zu den S3-Anfragen eine Liste aller Grid Manager- und Tenant Manager-Anfragen.
- Besserer Einblick in S3-Anfragen, die Fehler zurückgeben, ohne die Auswirkungen auf die Performance, die durch Audit-Protokollierungsmethoden verursacht werden.
- Zugriff auf HTTP-Layer-Anforderungen und Fehlercodes, die einfach zu analysieren sind.
- Bessere Transparenz bei Anfragen, die von Traffic-Klassifikatoren am Load Balancer blockiert wurden.

Informationen zum Exportieren der Protokolle finden Sie unter"Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server" .

Kategorien von Protokolldateien

Das Archiv der StorageGRID-Protokolldatei enthält die für jede Kategorie beschriebenen Protokolle sowie zusätzliche Dateien, die Metriken und die Ausgabe des Debug-Befehls enthalten.

Speicherort der Archivierung	Beschreibung
Prüfung	Während des normalen Systembetriebs erzeugte Überwachungsmeldungen.
Protokolle von Base-os	Informationen zu Betriebssystemen, einschließlich StorageGRID-Image-Versionen
Pakete	Globale Konfigurationsinformationen (Bundles)
Cache-SVC	Cache-Dienstprotokolle (nur auf Gateway-Knoten).
cassandra	Cassandra Datenbankinformationen und Reaper Reparaturprotokolle.
eg	VCSs-Informationen über den aktuellen Knoten und EC-Gruppeninformationen nach Profil-ID.

Speicherort der Archivierung	Beschreibung
Raster	Allgemeine Grid-Protokolle einschließlich Debug(`bycast.log`) und `servermanager` Protokolle.
Grid.json	Die Grid-Konfigurationsdatei ist über alle Nodes hinweg freigegeben. Außerdem `node.json` ist spezifisch für den aktuellen Node.
Hagroups	Hochverfügbarkeitsgruppen – Kennzahlen und Protokolle
Installieren	`Gdu-server` Und Installationsprotokolle.
Lambda-Schiedsrichter	Protokolle in Verbindung mit der S3 Select Proxy-Anforderung.
durchgesickert	Protokolle vom Leakd-Dienst.
lumberjack.log	Debug-Meldungen im Zusammenhang mit Protokollerfassung.
Metriken	Service-Protokolle für Grafana, Jaeger, Node Exporter und Prometheus.
Falsch	Miscd-Zugriffs- und Fehlerprotokolle.
mysql	Die Konfiguration der MariaDB-Datenbank und die zugehörigen Protokolle.
Netz	Protokolle, die von netzwerkbezogenen Skripten und dem dynIP-Dienst erstellt werden.
Nginx	Konfigurationsdateien und Protokolle für den Load Balancer und den Grid Federation Beinhaltet außerdem Traffic-Protokolle: Grid Manager und Tenant Manager.

Speicherort der Archivierung	Beschreibung
Nginx-gw	• `access.log`: Grid Manager und Tenant Manager fordern Protokollmeldungen an. ◦ Diese Meldungen werden beim Exportieren mit syslog als Präfix festgelegt `mgmt:`. ◦ Das Format dieser Protokollmeldungen 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 Grid-übergreifende Replikationsanforderungen. ◦ Diese Meldungen werden beim Exportieren mit syslog als Präfix festgelegt `cgr:`. ◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: S3-Anfragen an Load Balancer-Endpunkte. ◦ Diese Meldungen werden beim Exportieren mit syslog als Präfix festgelegt `endpoint:`. ◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Im Zusammenhang mit der neuen DNS-Check-Warnung.
ntp	NTP-Konfigurationsdatei und -Protokolle
Verwaiste Objekte	Protokolle zu verwaisten Objekten.
betriebssystem	Knoten- und Grid-Statusdatei, einschließlich Services `pid`.
Andere	Protokolldateien unter `/var/local/log`, die nicht in anderen Ordnern gesammelt werden.
perf-	Performance-Informationen für CPU-, Netzwerk- und Festplatten-I/O.
prometheus-Data	Aktuelle Prometheus-Kennzahlen, wenn die Log-Sammlung Prometheus-Daten enthält.
Bereitstellung	Protokolle im Zusammenhang mit dem Grid-Bereitstellungsprozess.

Speicherort der Archivierung	Beschreibung
Floß	Protokolle aus dem in Plattformservices verwendeten Raft-Cluster.
ssh	Protokolle für SSH-Konfiguration und -Dienst.
snmp	SNMP-Agent-Konfiguration für das Senden von SNMP-Benachrichtigungen.
Steckdosen-Daten	Sockendaten für Netzwerk-Debug.
system-commands.txt	Ausgabe von StorageGRID-Containerbefehlen. Enthält Systeminformationen wie z. B. Netzwerk- und Festplattenverwendung.
Sync-Recovery-Paket	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 verwenden, um Probleme zu beheben.

> 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 der Protokollverwaltung" .

Allgemeine StorageGRID-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/bycast.log	Die primäre StorageGRID Fehlerbehebungsdatei.	Alle Nodes
/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.	Alle Nodes

Dateiname	Hinweise	Gefunden am
/Var/local/Core/	Enthält alle Core Dump-Dateien, die erstellt wurden, wenn das Programm normal beendet wird. Mögliche Ursachen sind Assertion Failures, Verstöße oder Thread Timeouts. **Hinweis**: Die Datei `/var/local/core/kexec_cmd` existiert normalerweise auf Appliance-Knoten und weist nicht auf einen Fehler hin.	Alle Nodes

Verschlüsselungsbezogene Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/ssh-config-generation.log	Enthält Protokolle zum Generieren von SSH-Konfigurationen und zum Neuladen von SSH-Services.	Alle Nodes
/Var/local/log/nginx/config-generation.log	Enthält Protokolle zum Generieren von nginx-Konfigurationen und zum Neuladen von nginx-Diensten.	Alle Nodes
/Var/local/log/nginx-gw/config-generation.log	Enthält Protokolle zur Erstellung von nginx-gw-Konfigurationen (und zum Neuladen von nginx-gw-Diensten).	Admin- und Gateway-Nodes
/Var/local/log/update-cipher-configurations.log	Enthält Protokolle zur Konfiguration von TLS- und SSH-Richtlinien.	Alle Nodes

Protokolle der Grid-Föderation

Dateiname	Hinweise	Gefunden am
/Var/local/log/update_grid_federation_config.log	Enthält Protokolle zur Erstellung von nginx- und nginx-gw-Konfigurationen für Netzverbundverbindungen.	Alle Nodes

NMS-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/nms.log	• Erfasst Benachrichtigungen vom Grid Manager und dem Tenant Manager. • Erfasst Ereignisse im Zusammenhang mit dem Betrieb des NMS-Dienstes. Beispielsweise E-Mail-Benachrichtigungen und Konfigurationsänderungen. • Enthält XML-Paketaktualisierungen, die aus Konfigurationsänderungen im System resultieren. • Enthält Fehlermeldungen zum Attribut Downsampling, das einmal täglich ausgeführt wird. • Enthält Java-Web-Server-Fehlermeldungen, z. B. Fehler beim Generieren der Seite und HTTP-Status 500-Fehler.	Admin-Nodes
/Var/local/log/nms.errlog	Enthält Fehlermeldungen bezüglich der MySQL-Datenbank-Upgrades. Enthält den Standardfehlerstrom (Stderr) der entsprechenden Dienste. Pro Dienst gibt es eine Protokolldatei. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Admin-Nodes
/Var/local/log/nms.requestlog	Enthält Informationen über ausgehende Verbindungen von der Management-API zu internen StorageGRID-Diensten.	Admin-Nodes

Server Manager-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/servermanager.log	Protokolldatei für die auf dem Server ausgeführte Server Manager-Anwendung.	Alle Nodes
/Var/local/log/GridstatBackend.errlog	Protokolldatei für die Back-End-Anwendung der Server Manager-GUI.	Alle Nodes
/Var/local/log/gridstat.errlog	Protokolldatei für die Benutzeroberfläche von Server Manager.	Alle Nodes

StorageGRID Serviceprotokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/acct.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/adc.errlog	Enthält den Standardfehlerstrom (Stderr) der entsprechenden Dienste. Pro Dienst gibt es eine Protokolldatei. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/ams.errlog		Admin-Nodes
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	Cache-Dienstprotokolle.	Gateway-Nodes
/Var/local/log/cassandra/system.log	Informationen für den Metadatenspeicher (Cassandra-Datenbank), die verwendet werden können, wenn Probleme beim Hinzufügen neuer Storage-Nodes auftreten oder wenn der nodetool-Reparaturauftrag abgestellt wird.	Storage-Nodes
/Var/local/log/cassandra-reaper.log	Informationen zum Cassandra Reaper Service, der Reparaturen der Daten in der Cassandra-Datenbank durchführt.	Storage-Nodes
/Var/local/log/cassandra-reaper.errlog	Fehlerinformationen für den Cassandra Reaper Service.	Storage-Nodes
/Var/local/log/chunk.errlog		Storage-Nodes
/Var/local/log/cmn.errlog		Admin-Nodes
/Var/local/log/cms.errlog	Diese Protokolldatei ist möglicherweise auf Systemen vorhanden, die von einer älteren StorageGRID-Version aktualisiert wurden. Er enthält Informationen zu Altsystemen.	Storage-Nodes
/Var/local/log/dds.errlog		Storage-Nodes
/Var/local/log/dmv.errlog		Storage-Nodes

Dateiname	Hinweise	Gefunden am
/Var/local/log/dynap*	Enthält Protokolle zum Dynap-Dienst, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Nodes
/Var/local/log/grafana.log	Das mit dem Grafana-Service verknüpfte Protokoll, das für die Visualisierung von Kennzahlen im Grid Manager verwendet wird.	Admin-Nodes
/Var/local/log/hagroups.log	Das Protokoll, das mit Hochverfügbarkeitsgruppen verknüpft ist.	Admin-Nodes und Gateway-Nodes
/Var/local/log/hagroups_events.log	Verfolgt Statusänderungen, beispielsweise den Übergang von BACKUP zu MASTER oder FEHLER.	Admin-Nodes und Gateway-Nodes
/Var/local/log/idnt.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/jaeger.log	Das Protokoll, das mit dem jaeger-Dienst verknüpft ist, das für die Trace-Erfassung verwendet wird.	Alle Nodes
/Var/local/log/kstn.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/Lambda*	Enthält Protokolle für den S3 Select-Service.	Admin- und Gateway-Nodes Dieses Protokoll enthält nur bestimmte Admin- und Gateway-Knoten. Siehe "S3 Select Anforderungen und Einschränkungen für Admin und Gateway Nodes".
/Var/local/log/ldr.errlog		Storage-Nodes

Dateiname	Hinweise	Gefunden am
/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 sowie zum Verwalten von Umgebungskonfigurationen auf dem Node bereitstellt, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Nodes
/Var/local/log/nginx/*.log	Enthält Protokolle für den nginx-Dienst, der als Authentifizierung 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 Nodes
/Var/local/log/nginx-gw/*.log	Enthält allgemeine Protokolle für den nginx-gw-Dienst, einschließlich Fehlerprotokolle und Protokolle für die eingeschränkten Admin-Ports auf Admin-Knoten.	Admin-Nodes und Gateway-Nodes
/Var/local/log/nginx-gw/cgr-access.log.gz	Enthält Zugriffsprotokolle für den Grid-übergreifenden Replikationsdatenverkehr.	Admin-Nodes, Gateway-Nodes oder beides, basierend auf der Grid-Federation-Konfiguration. Nur im Zielraster für die Grid-übergreifende Replikation gefunden.
/Var/local/log/nginx-gw/endpoint-access.log.gz	Die Lösung enthält Zugriffsprotokolle für den Load Balancer, der einen Lastausgleich für den S3-Datenverkehr von Clients zu Storage Nodes ermöglicht.	Admin-Nodes und Gateway-Nodes
/Var/local/log/persistence*	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Root-Festplatte verwaltet, die bei einem Neustart erhalten bleiben müssen.	Alle Nodes

Dateiname	Hinweise	Gefunden am
/Var/local/log/prometheus.log	Enthält für alle Knoten das Service-Protokoll für den Knoten-Exporter und das Kennzahlungsprotokoll der ade-Exporter. Für Admin-Knoten enthält auch Protokolle für die Prometheus- und Alert Manager-Dienste.	Alle Nodes
/Var/local/log/raft.log	Enthält die Ausgabe der Bibliothek, die vom RSM-Dienst für das Raft-Protokoll verwendet wird.	Storage-Nodes mit RSM-Service
/Var/local/log/RMS.errlog	Enthält Protokolle für den RSM-Service (Replicated State Machine Service), der für S3-Plattformservices verwendet wird.	Storage-Nodes mit RSM-Service
/Var/local/log/ssm.errlog		Alle Nodes
/Var/local/log/update-s3vs-domains.log	Enthält Protokolle zur Verarbeitung von Updates für die Konfiguration virtueller gehosteter S3-Domänennamen.Siehe Anweisungen für die Implementierung von S3-Client-Applikationen.	Admin- und Gateway-Nodes
/Var/local/log/Update-snmp-Firewall.*	Enthalten Protokolle im Zusammenhang mit den Firewall-Ports, die für SNMP verwaltet werden.	Alle Nodes
/Var/local/log/update-sysl.log	Enthält Protokolle in Bezug auf Änderungen an der Syslog-Konfiguration des Systems.	Alle Nodes
/Var/local/log/update-traffic-classes.log	Enthält Protokolle, die sich auf Änderungen an der Konfiguration von Traffic-Klassifikatoren beziehen.	Admin- und Gateway-Nodes
/Var/local/log/update-utcn.log	Enthält Protokolle, die sich auf diesem Knoten im Netzwerk des nicht vertrauenswürdigen Clients beziehen.	Alle Nodes

Verwandte Informationen

- "Etwa bycast.log"
- "S3-REST-API VERWENDEN"

Protokoll für Implementierung und Wartung

Sie können die Bereitstellungs- und Wartungsprotokolle verwenden, um Probleme zu beheben.

Dateiname	Hinweise	Gefunden am
/Var/local/log/install.log	Während der Softwareinstallation erstellt. Enthält eine Aufzeichnung der Installationsereignisse.	Alle Nodes
/Var/local/log/expansion-progress.log	Während Erweiterungsvorgängen erstellt. Enthält eine Aufzeichnung der Erweiterungereignisse.	Storage-Nodes
/Var/local/log/pa-move.log	Wird während der Ausführung des Skripts erstellt `pa-move.sh`.	Primärer Admin-Node
/Var/local/log/pa-move-new_pa.log	Wird während der Ausführung des Skripts erstellt `pa-move.sh`.	Primärer Admin-Node
/Var/local/log/pa-move-old_pa.log	Wird während der Ausführung des Skripts erstellt `pa-move.sh`.	Primärer Admin-Node
/Var/local/log/gdu-server.log	Erstellt durch den GDU-Dienst. Enthält Ereignisse im Zusammenhang mit Provisioning- und Wartungsverfahren, die vom primären Admin-Node verwaltet werden.	Admin-Nodes
/Var/local/log/send_admin_hw.log	Während der Installation erstellt. Enthält Debugging-Informationen zur Kommunikation eines Knotens mit dem primären Admin-Knoten.	Alle Nodes
/Var/local/log/upgrade.log	Wird während eines Software-Upgrades erstellt. Enthält eine Aufzeichnung der Softwareaktualisierungs-Ereignisse.	Alle Nodes

Etwa bycast.log

Die Datei `/var/local/log/bycast.log` ist die primäre Fehlerbehebungsdatei für die StorageGRID-Software. Für jeden Grid-Node gibt es eine `bycast.log` Datei. Die Datei enthält für diesen Grid-Node spezifische Meldungen.

Die Datei `/var/local/log/bycast-err.log` ist eine Teilmenge von `bycast.log`. Er enthält Meldungen mit dem Schweregrad „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 Sie die Protokollverwaltung und den externen Syslog-Server" .

Dateirotation für bycast.log

Wenn die `bycast.log` 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 wird benannt `bycast.log`. Wenn das neue `bycast.log` 1 GB erreicht, wird umbenannt und komprimiert, `bycast.log.1` um zu werden `bycast.log.2.gz`, und `bycast.log` wird umbenannt `bycast.log.1`.

Die Rotationsgrenze für `bycast.log` beträgt 21 Dateien. Wenn die 22. Version der `bycast.log` Datei erstellt wird, wird die älteste Datei gelöscht.

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

> Wenn eine Protokolldatei komprimiert wurde, dürfen Sie sie nicht auf den gleichen Speicherort dekomprimieren, an dem sie geschrieben wurde. Die Dekomprimierung der Datei an demselben Speicherort kann die Drehskripte des Protokolls 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 Sie die Protokollverwaltung und den externen Syslog-Server" .

Verwandte Informationen

"Erfassen von Protokolldateien und Systemdaten"

Nachrichten in bycast.log

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

Beispielmeldung für ADE:

```
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-Meldungen enthalten die folgenden Informationen:

Nachrichtensegment	Wert im Beispiel
Node-ID	12455685
PROZESS-ID WIRD ADDIEREN	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHF

Nachrichtensegment	Wert im Beispiel
UTC-Systemzeit	2019-05-05T27T17:10:29.784677 (JJJJ-MM-DDTHH:MM:SS.UUUUUU)
Schweregrad	FEHLER
Interne Tracking-Nummer	0906
Nachricht	SVMR: Integritätsprüfung auf Volume 3 mit Grund 'AUSWEG' fehlgeschlagen

Nachrichten-Schweregrade in bycast.log

Den Meldungen in `bycast.log` werden Schweregrade zugewiesen.

Beispiel:

- **HINWEIS** — ein Ereignis, das aufgezeichnet werden soll, ist aufgetreten. Die meisten Protokollmeldungen befinden sich auf dieser Ebene.
- **WARNUNG** — ein unerwarteter Zustand ist aufgetreten.
- **ERROR** — ein großer Fehler ist aufgetreten, der sich auf den Betrieb auswirkt.
- **KRITISCH** — Es ist ein anormaler Zustand aufgetreten, der den normalen Betrieb gestoppt hat. Sie sollten umgehend mit dem zugrunde liegenden Zustand beginnen.

Fehlercodes in `bycast.log`

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

In der folgenden Tabelle sind die allgemeinen nicht-numerischen Codes in aufgeführt `bycast.log`. Die genaue Bedeutung eines nicht-numerischen Codes hängt vom Kontext ab, in dem er gemeldet wird.

Fehlercode	Bedeutung
SUKZ	Kein Fehler
GERR	Unbekannt
STORNO	Storniert
ABRT	Abgebrochen
TOUT	Zeitüberschreitung
INVL	Ungültig
NFND	Nicht gefunden

Fehlercode	Bedeutung
ROVER	Version
CONF	Konfiguration
FEHLER	Fehlgeschlagen
ICPL	Unvollständig
FERTIG	Fertig
SUNV	Service nicht verfügbar

In der folgenden Tabelle sind die numerischen Fehlercodes in aufgeführt `bycast.log`.

Fehlernummer	Fehlercode	Bedeutung
001	EPERM	Vorgang nicht zulässig
002	ENOENT	Keine solche Datei oder Verzeichnis
003	ESRCH	Kein solcher Prozess
004	EINTR	Unterbrochener Systemanruf
005	EIO	I/O-Fehler
006	ENXIO	Dieses Gerät oder diese Adresse ist nicht vorhanden
007	E2BIG	Argumentliste zu lang
008	ENOEXEC	Fehler im Executive-Format
009	EBADF	Ungültige Dateinummer
010	ECHILD	Keine Kinderprozesse
011	EAGAIN	Versuchen Sie es erneut
012	ENOMEM	Nicht genügend Arbeitsspeicher
013	EACCES	Berechtigung verweigert
014	FAULT	Ungültige Adresse

Fehlernummer	Fehlercode	Bedeutung
015	ENOTBLK	Blockgerät erforderlich
016	EBUSY	Gerät oder Ressource beschäftigt
017	EEXIST	Datei vorhanden
018	EXDEV	Geräteübergreifende Verbindung
019	ENODEV	Kein solches Gerät
020	ENOTDIR	Kein Verzeichnis
021	EISDIR	Ist ein Verzeichnis
022	EINVAL	Ungültiges Argument
023	DATEI	Dateitabelle-Überlauf
024	EMFILE	Zu viele geöffnete Dateien
025	ENOTTY	Keine Schreibmaschine
026	ETXTBSY	Textdatei belegt
027	EFBIG	Datei zu groß
028	ENOSPC	Kein Platz mehr auf dem Gerät
029	ESPIPE	Illegale Suche
030	EROFS	Schreibgeschütztes Dateisystem
031	EMLINK	Zu viele Links
032	E-ROHR	Gebrochenes Rohr
033	EDOM	Math Argument aus Domäne der Funktion
034	ERANGE	Math Ergebnis nicht darstellbar
035	EDEADLK	Ressourcen-Deadlock würde eintreten
036	ENAMETOOOLONG	Dateiname zu lang

Fehlernummer	Fehlercode	Bedeutung
037	ENOLCK	Keine Datensatzsperren verfügbar
038	ENOSYS	Funktion nicht implementiert
039	ENOTEMPTY	Verzeichnis nicht leer
040	ELOOP	Es wurden zu viele symbolische Links gefunden
041		
042	ENOMSG	Keine Nachricht vom gewünschten Typ
043	EIDRM	Kennung entfernt
044	ECHRNG	Kanalnummer außerhalb des Bereichs
045	EL2NSYNC	Ebene 2 nicht synchronisiert
046	EL3HLT	Ebene 3 angehalten
047	EL3RST	Stufe 3 zurücksetzen
048	ELNRNG	Verbindungsnummer außerhalb des Bereichs
049	EUNATCH	Protokolltreiber nicht angeschlossen
050	ENOCSI	Keine CSI-Struktur verfügbar
051	EL2HLT	Ebene 2 angehalten
052	EBADE	Ungültiger Austausch
053	EBADR	Ungültiger Anforderungsdeskriptor
054	EXFULL	Exchange voll
055	ENOANO	Keine Anode
056	EBADRQC	Ungültiger Anforderungscode
057	EBADSLT	Ungültiger Steckplatz
058		

Fehlernummer	Fehlercode	Bedeutung
059	EBFONT	Schlechtes Schriftdateiformat
060	ENOSTR	Gerät kein Strom
061	ENODATA	Keine Daten verfügbar
062	ETIME	Timer abgelaufen
063	ENOSR	Aus Datenströmen: Ressourcen
064	ENONET	Die Maschine befindet sich nicht im Netzwerk
065	ENOPKG	Paket nicht installiert
066	EREMOTE	Das Objekt ist Remote
067	ENOLINK	Verbindung wurde getrennt
068	ADV	Fehler anzeigen
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	EOVERFLOW	Wert zu groß für definierten Datentyp
076	ENOTUNIQ	Name nicht eindeutig im Netzwerk
077	EBADFD	Dateideskriptor im schlechten Zustand
078	EREMCHG	Remote-Adresse geändert
079	ELIBACC	Kein Zugriff auf eine erforderliche freigegebene Bibliothek möglich

Fehlernummer	Fehlercode	Bedeutung
080	ELIBBAD	Zugriff auf eine beschädigte, gemeinsam genutzte Bibliothek
081	ELIBSCN	
082	ELIBMAX	Es wird versucht, zu viele gemeinsam genutzte Bibliotheken zu verbinden
083	ELIBEXEC	Eine gemeinsam genutzte Bibliothek kann nicht direkt exec
084	EILSEQ	Ungültige Byte-Sequenz
085	ERESTART	Unterbrochener Systemanruf sollte neu gestartet werden
086	ESTRPIPE	Leitungsfehler
087	EUSERS	Zu viele Benutzer
088	ENOTSOCK	Buchsenbetrieb an nicht-Socket
089	EDESTADDRREQ	Zieladresse erforderlich
090	EMSGSIZE	Nachricht zu lang
091	EPROTOTYPE	Protokoll falscher Typ für Socket
092	ENOPROTOOPT	Protokoll nicht verfügbar
093	EPROTONOSUPPORT	Protokoll nicht unterstützt
094	ESOCKTNOSUPPORT	Socket-Typ nicht unterstützt
095	EOPNOTSUPP	Der Vorgang wird auf dem Transportendpunkt nicht unterstützt
096	EPFNOSUPPORT	Protokollfamilie wird nicht unterstützt
097	EAFNOSUPPORT	Adressfamilie wird nicht durch Protokoll unterstützt
098	EADDRINUSE	Die Adresse wird bereits verwendet
099	EADDRNOTAVAIL	Angeforderte Adresse kann nicht zugewiesen werden

Fehlernummer	Fehlercode	Bedeutung
100	ENETDOWN	Netzwerk ausgefallen
101	ENETUNREACH	Netzwerk nicht erreichbar
102	ENETRESET	Die Verbindung wurde aufgrund von Reset unterbrochen
103	ECONNABORTED	Die Verbindung wurde durch die Software beendet
104	ECONNNRESET	Verbindungsrücksetzung durch Peer
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Senden nach dem Herunterfahren des Transportendpunkts nicht möglich
109	ETOMANYREFS	Zu viele Referenzen: Spleißen nicht möglich
110	ETIMEDOUT	Zeitüberschreitung bei Verbindung
111	ECONNNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHEOSTUNREACH	Keine Route zum Host
114	EALREADY	Der Vorgang wird bereits ausgeführt
115	EINPROGRESS	Vorgang wird jetzt ausgeführt
116		
117	EUCLEAN	Struktur muss gereinigt werden
118	ENOTNAM	Keine XENIX-Datei mit dem Namen
119	ENAVAIL	Keine XENIX-Semaphore verfügbar
120	EISNAM	Ist eine Datei mit dem Namen

Fehlernummer	Fehlercode	Bedeutung
121	EREMOTEIO	Remote-I/O-Fehler
122	EDQUOT	Kontingent überschritten
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ECANCELED	Vorgang Abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEYEXPIRED	Schlüssel abgelaufen
128	EKEYREVOKED	Schlüssel wurde widerrufen
129	EKEYREJECTED	Schlüssel wurde vom Dienst abgelehnt
130	EOWNERDEAD	Für robuste Mutexe: Besitzer starb
131	ENOTRECOVERABLE	Bei robusten Mutation: Status nicht wiederherstellbar

Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server

Überlegungen zur Verwendung eines externen Syslog-Servers

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID, mit dem Sie Audit-Informationen zum System an einem Ort sammeln können. Mithilfe eines externen Syslog-Servers können Sie den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten. Für StorageGRID ist das Format des ausgehenden Syslog-Nachrichtenpakets mit RFC 3164 kompatibel.

Folgende Arten von Audit-Informationen können Sie an den externen Syslog-Server senden:

- Prüfprotokolle mit den während des normalen Systembetriebs erzeugten Audit-Meldungen
- Sicherheitsbezogene Ereignisse wie Anmeldungen und Eskalationen im Root-Bereich
- Anwendungsprotokolle, die angefordert werden können, wenn ein Support-Fall geöffnet werden muss, um die Behebung eines aufgetretenen Problems zu beheben

Wann sollte ein externer Syslog-Server verwendet werden

Ein externer Syslog-Server ist besonders nützlich, wenn Sie ein großes Grid haben, mehrere Arten von S3 Applikationen verwenden oder alle Audit-Daten aufbewahren möchten. Durch das Senden von Audit-Informationen an einen externen Syslog-Server können Sie:

- Erfassen und managen Sie Audit-Informationen wie Audit-Nachrichten, Anwendungsprotokolle und Sicherheitsereignisse effizienter.
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da die Audit-Informationen direkt von den verschiedenen Storage-Knoten auf den externen Syslog-Server übertragen werden, ohne einen Admin-Knoten durchlaufen zu müssen.

> Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit mehr als 8,192 Byte am Ende der Nachricht abgeschnitten, um den üblichen Einschränkungen in externen Syslog-Server-Implementierungen zu entsprechen.

> Um die Optionen für die vollständige Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers (`localaudit.log`zu maximieren, werden auf jedem Knoten bis zu 20 GB lokale Protokolle von Audit-Datensätzen gepflegt.

So konfigurieren Sie einen externen Syslog-Server

Informationen zum Konfigurieren eines externen Syslog-Servers finden Sie unter"Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server" .

Wenn Sie das TLS- oder RELP/TLS-Protokoll konfigurieren möchten, müssen Sie über die folgenden Zertifikate verfügen:

- **Server-CA-Zertifikate**: Ein oder mehrere vertrauenswürdige CA-Zertifikate zur Überprüfung des externen Syslog-Servers in PEM-Codierung. Wenn nicht angegeben, wird das Standard-Grid-CA-Zertifikat verwendet.
- **Client-Zertifikat**: Das Client-Zertifikat zur Authentifizierung am externen Syslog-Server in PEM-Codierung.
- **Privater Client-Schlüssel**: Privater Schlüssel für das Client-Zertifikat in PEM-Codierung.

> Wenn Sie ein Clientzertifikat verwenden, müssen Sie auch einen privaten Clientschlüssel verwenden. Wenn Sie einen verschlüsselten privaten Schlüssel angeben, müssen Sie auch die Passphrase angeben. Die Verwendung eines verschlüsselten privaten Schlüssels bietet keine wesentlichen Sicherheitsvorteile, da Schlüssel und Passphrase gespeichert werden müssen. Aus Gründen der Einfachheit wird die Verwendung eines unverschlüsselten privaten Schlüssels empfohlen.

Wie schätzen Sie die Größe des externen Syslog-Servers ein

In der Regel wird das Grid so dimensioniert, dass es einen erforderlichen Durchsatz erzielt, der mit S3-Operationen pro Sekunde oder Byte pro Sekunde definiert wird. Möglicherweise müssen Sie z. B. angeben, dass Ihr Grid 1,000 S3-Operationen pro Sekunde oder 2,000 MB pro Sekunde der Objektingest und -Abruf verarbeiten muss. Sie sollten die Größe Ihres externen Syslog-Servers entsprechend den Datenanforderungen Ihres Grid festlegen.

Dieser Abschnitt enthält einige heuristische Formeln, mit denen Sie die Rate und die durchschnittliche Größe von Protokollmeldungen verschiedener Arten bewerten können, die Ihr externer Syslog-Server in der Lage sein muss, anhand der bekannten oder gewünschten Performance-Merkmale des Grid (S3-Operationen pro Sekunde) auszuführen.

In Schätzformeln S3-Operationen pro Sekunde verwenden

Wenn Ihr Grid für einen Durchsatz in Byte pro Sekunde ausgedrückt wurde, müssen Sie diese Größe in S3-Vorgänge pro Sekunde konvertieren, um die Abschätzung-Formeln zu verwenden. Um den Grid-Durchsatz zu konvertieren, müssen Sie zunächst die durchschnittliche Objektgröße festlegen, die Sie anhand der Informationen in vorhandenen Audit-Protokollen und -Metriken (falls vorhanden) durchführen können, oder indem Sie Ihre Kenntnisse über die Anwendungen nutzen, die StorageGRID verwenden. Beispiel: Wenn Ihr Grid einen Durchsatz von 2,000 MB/s erreicht hat und die durchschnittliche Objektgröße 2 MB beträgt, wurde das Grid so dimensioniert, dass es 1,000 S3-Operationen pro Sekunde (2,000 MB/2 MB) verarbeiten kann.

> Die Formeln für die externe Syslog-Server-Größenbemessung in den folgenden Abschnitten liefern allgemeine Schätzungen (und nicht die Schlimmstfall-Schätzungen). Je nach Konfiguration und Workload wird möglicherweise eine höhere oder niedrigere Rate von Syslog-Meldungen oder ein höheres Volumen an Syslog-Daten angezeigt als die Formel „Predict“. Die Formeln sind nur als Richtlinien zu verwenden.

Schätzformeln für Prüfprotokolle

Wenn Sie über keine Informationen zu Ihrem S3-Workload verfügen außer der Anzahl der S3-Vorgänge pro Sekunde, die Ihr Grid unterstützen soll, können Sie die Menge der Audit-Protokolle schätzen, die Ihr externer Syslog-Server anhand der folgenden Formeln verarbeiten muss. Unter der Annahme, dass Sie die Audit-Level auf die Standardwerte (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist):

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

Wenn Ihr Grid beispielsweise für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, sollte der externe Syslog-Server entsprechend angepasst werden und 2,000 Syslog-Nachrichten pro Sekunde unterstützen. Er sollte Audit-Protokolldaten von 1.6 MB pro Sekunde empfangen (und in der Regel speichern) können.

Wenn Sie mehr über Ihre Arbeitslast 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 der folgenden S3-Felder in Byte (4-stellige Abkürzungen in der Tabelle sind Namen von Audit-Protokollfeldern):

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
S3BK	S3 Bucket	Der S3-Bucket-Name

Codieren	Feld	Beschreibung
S3KY	S3 -Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.

Verwenden wir P, um den Prozentsatz der an Put-Vorgängen abzubilden, wobei 0 ≤ P ≤ 1 (für einen 100 % PUT-Workload, P = 1 und für einen 100 % GET-Workload, P = 0).

Verwenden wir K, um die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel darzustellen. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann ist der Wert von K 90 (13+13+28+36).

Wenn Sie Werte für P und K festlegen können, können Sie die Menge der Audit-Protokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss. Dabei wird davon ausgegangen, dass Sie die Audit-Level auf die Standardwerte setzen (alle Kategorien sind auf Normal gesetzt, außer Speicher, Die auf Fehler gesetzt ist):

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

Wenn Ihr Grid beispielsweise 1,000 S3-Operationen pro Sekunde angepasst ist, beträgt der Workload 50 % Put-Vorgänge sowie die S3-Kontonamen und Bucket-Namen Und Objektnamen durchschnittlich 90 Byte, Ihr externer Syslog-Server sollte Größe haben, um 1,500 Syslog-Nachrichten pro Sekunde zu unterstützen. Er sollte Audit-Protokolldaten mit einer Rate von ca. 1 MB pro Sekunde empfangen (und in der Regel speichern) können.

Schätzformeln für nicht standardmäßige Audit-Level

Die für Prüfprotokolle bereitgestellten Formeln setzen voraus, dass die standardmäßigen Einstellungen für die Revisionsstufe verwendet werden (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist). Detaillierte Formeln zur Schätzung der Rate und der durchschnittlichen Größe von Überwachungsmeldungen für nicht standardmäßige Überwachungseinstellungen sind nicht verfügbar. Die folgende Tabelle kann jedoch verwendet werden, um eine grobe Schätzung der Rate zu machen; Sie können die Formel für die durchschnittliche Größe von Audit-Protokollen verwenden, aber beachten Sie, dass sie wahrscheinlich zu einer Überschätzung führen wird, da die „zusätzlichen“ Audit-Meldungen im Durchschnitt kleiner sind als die standardmäßigen Audit-Meldungen.

Zustand	Formel
Replikation: Audit-Level alle auf Debug oder Normal eingestellt	Auditprotokollrate = 8 x S3-Betriebsrate
Verfahren zur Einhaltung von Datenkonsistenz: Für Audit-Level ist Debug oder Normal festgelegt	Verwenden Sie die gleiche Formel wie für die Standardeinstellungen

Schätzformeln für Sicherheitsereignisse

Sicherheitsereignisse werden nicht mit S3-Vorgängen in Beziehung gesetzt und erzeugen in der Regel eine vernachlässigbare Menge an Protokollen und Daten. Aus diesen Gründen werden keine Schätzformeln bereitgestellt.

Schätzformeln für Anwendungsprotokolle

Wenn neben der Anzahl der S3-Vorgänge pro Sekunde, die Ihr Grid unterstützen soll, keine Informationen zu Ihrem S3-Workload vorhanden sind, können Sie das Volumen der Anwendungen schätzen. Protokolle, die Ihr externer Syslog-Server verarbeiten muss, werden gemäß den folgenden Formeln verwendet:

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

Wenn Ihr Grid also für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, sollte der externe Syslog-Server entsprechend dimensioniert sein, um 3,300 Applikations-Logs pro Sekunde zu unterstützen und Applikations-Protokolldaten von etwa 1.2 MB pro Sekunde zu empfangen (und zu speichern).

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Für Anwendungsprotokolle sind die wichtigsten zusätzlichen Variablen die Datenschutzstrategie (Replikation vs. Erasure Coding), der Prozentsatz der S3-Operationen, die Put (vs. Gets/other) sind, und die durchschnittliche Größe der folgenden S3-Felder in Byte (4-stellige Abkürzungen, die in der Tabelle verwendet werden, sind Audit-Log-Feldnamen):

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
S3BK	S3 Bucket	Der S3-Bucket-Name
S3KY	S3 -Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.

Beispiel für eine Einschätzung der Dimensionierung

In diesem Abschnitt werden Beispielbeispiele erläutert, wie man die Schätzformeln für Raster mit den folgenden Methoden der Datensicherung verwendet:

- Replizierung
- Erasure Coding

Wenn Sie Replizierung für die Datensicherung verwenden

Stellen Sie P den Prozentsatz der an Put-Vorgängen dar, wobei 0 ≤ P ≤ 1 (für einen 100 % PUT-Workload, P = 1 und für einen 100 % GET-Workload, P = 0).

K darf die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Buckets und S3-Schlüssel repräsentieren. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten 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-Vorgänge pro Sekunde dimensioniert ist, beträgt der Workload 50 % und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte, sollte der externe Syslog-Server entsprechend angepasst werden, um 1800 Applikations-Logs pro Sekunde zu unterstützen, Und erhalten Applikationsdaten mit einer Rate von 0.5 MB pro Sekunde (und in der Regel auch dort).

Bei Verwendung von Erasure Coding zur Datensicherung

Stellen Sie P den Prozentsatz der an Put-Vorgängen dar, wobei 0 ≤ P ≤ 1 (für einen 100 % PUT-Workload, P = 1 und für einen 100 % GET-Workload, P = 0).

K darf die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Buckets und S3-Schlüssel repräsentieren. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten 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-Vorgänge pro Sekunde dimensioniert ist, beträgt der Workload 50 % Put, Ihre S3-Kontonamen, Bucket-Namen und Objektnamen sind durchschnittlich 90 Byte lang. Ihr externer Syslog-Server sollte so dimensioniert sein, dass er 2,250 Anwendungsprotokolle pro Sekunde unterstützt und Anwendungsdaten mit einer Rate von 0.6 MB pro Sekunde empfangen (und normalerweise speichern) kann.

Konfigurieren der Protokollverwaltung

Konfigurieren Sie nach Bedarf Prüfebenen, Protokollheader und den Speicherort von Prüfmeldungen und -protokollen.

Alle StorageGRID -Knoten generieren Prüfmeldungen und Protokolle, um Systemaktivitäten und Ereignisse zu

verfolgen. Prüfmeldungen und -protokolle sind wichtige Tools zur Überwachung und Fehlerbehebung.

Optional können Sie"Konfigurieren Sie einen externen Syslog-Server" um Auditinformationen 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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".
- Wenn Sie planen, einen externen Syslog-Server zu konfigurieren, haben Sie die folgenden Schritte überprüft und befolgt"Überlegungen zur Verwendung eines externen Syslog-Servers" .
- Wenn Sie einen externen Syslog-Server mit TLS- oder RELP/TLS-Protokoll konfigurieren möchten, verfügen Sie über die erforderlichen Server-CA- und Client-Zertifikate und den privaten Client-Schlüssel.

Meldungsebenen ändern

Sie können für jede der folgenden Meldungskategorien im Prüfprotokoll eine andere Überwachungsstufe festlegen:

Audit-Kategorie	Standardeinstellung	Weitere Informationen
System	Normal	"Systemaudits Meldungen"
Storage	Fehler	"Audit-Meldungen zu Objekt-Storage"
Vereinfachtes	Normal	"Management-Audit-Nachricht"
Client-Lesevorgänge	Normal	"Client liest Audit-Meldungen"
Client-Schreibvorgänge	Normal	"Audit-Meldungen des Clients schreiben"
ILM	Normal	"ILM-Prüfmeldungen"
Grid-übergreifende Replizierung	Fehler	"CGRR: Grid-übergreifende Replikationsanforderung"

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

Schritte

1. Wählen Sie **Konfiguration** > **Überwachung** > **Protokollverwaltung**.
2. Wählen Sie für jede Kategorie der Überwachungsmeldung eine Überwachungsstufe aus der Dropdown-Liste aus:

Audit-Level	Beschreibung
Aus	Es werden keine Überwachungsmeldungen aus der Kategorie protokolliert.
Fehler	Es werden nur Fehlermeldungen protokolliert – Prüfmeldungen, deren Ergebniscode nicht „erfolgreich“ (SUCS) war.
Normal	Standardtransaktionsmeldungen werden protokolliert – die in diesen Anweisungen für die Kategorie aufgeführten Nachrichten.
Debuggen	Veraltet. Dieser Level verhält sich mit dem normalen Prüfstand.

Die Meldungen, die für eine bestimmte Ebene enthalten sind, enthalten diejenigen, die auf den höheren Ebenen protokolliert werden würden. Die normale Ebene umfasst beispielsweise 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**.

Definieren Sie HTTP-Anforderungsheader

Sie können optional alle HTTP-Anforderungsheader definieren, die Sie in die Prüfnachrichten zum Lesen und Schreiben des Clients aufnehmen möchten.

Schritte

1. Definieren Sie im Abschnitt **Audit Protocol headers** die HTTP-Anforderungsheader, die Sie in die Audit-Nachrichten des Clients aufnehmen möchten.

   Verwenden Sie ein Sternchen (*) als Platzhalter, um Null oder mehr Zeichen zu entsprechen. Verwenden Sie die Escape-Sequenz (*), um mit einem wortwörtliche Sternchen überein.

2. Wählen Sie **Einen anderen Header hinzufügen** aus, um ggf. zusätzliche Header zu erstellen.

   Wenn HTTP-Header in einer Anfrage gefunden werden, sind sie in der Überwachungsmeldung unter dem Feld HTRH enthalten.

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

3. Wählen Sie **Speichern**

Konfigurieren des Protokollspeicherorts

Standardmäßig werden Prüfmeldungen und Protokolle auf den Knoten gespeichert, auf denen sie generiert werden. Sie werden regelmäßig rotiert und schließlich gelöscht, um zu verhindern, dass sie übermäßig viel Speicherplatz belegen. Wenn Sie Auditmeldungen und eine Teilmenge der Protokolle extern speichern möchten,Verwenden Sie einen externen Syslog-Server .

Wenn Sie die Protokolldateien intern speichern möchten, wählen Sie einen Mandanten und einen Bucket für die Protokollspeicherung aus und aktivieren Sie die Protokollarchivierung.

Verwenden Sie einen externen syslog-Server

Optional können Sie einen externen Syslog-Server konfigurieren, um Audit-Protokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Ort außerhalb des Grids zu speichern.

Wenn Sie keinen externen Syslog-Server verwenden möchten, überspringen Sie diesen Schritt und gehen Sie zuProtokollspeicherort auswählen .

Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können zusätzliche Konfigurationsoptionen über die Endpunkte angewendet werden `audit-destinations`, die sich im Abschnitt Private API des befinden"Grid Management API". Sie können beispielsweise die API verwenden, wenn Sie unterschiedliche Syslog-Server für verschiedene Knotengruppen verwenden möchten.

Geben Sie Syslog-Informationen ein

Greifen Sie auf den Assistenten zum Konfigurieren des externen Syslog-Servers zu und geben Sie die Informationen an, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. Wählen Sie auf der Registerkarte „Lokaler Knoten und externer 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 zum Konfigurieren des externen Syslog-Servers wird angezeigt.

2. Geben Sie für den Schritt **Enter syslog info** des Assistenten einen gültigen vollständig qualifizierten Domänennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server in das Feld **Host** 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 verwenden zu können. Mithilfe von Zertifikaten lassen sich die Verbindungen zwischen dem Grid und dem externen Syslog-Server sichern. Weitere Informationen finden Sie unter "Verwalten von Sicherheitszertifikaten".

   Für alle Protokolloptionen muss der externe Syslog-Server unterstützt und konfiguriert werden. Sie müssen eine Option wählen, die mit dem externen Syslog-Server kompatibel ist.

   Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls für eine zuverlässige Bereitstellung von Ereignismeldungen. Mithilfe von RELP können Sie den Verlust von Audit-Informationen 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 Sie verwenden möchten.
   b. Wählen Sie das Zertifikat oder die Schlüsseldatei aus.

c. Wählen Sie **Öffnen**, um die Datei hochzuladen.

   Neben dem Zertifikat- oder Schlüsseldateinamen wird eine grüne Prüfung angezeigt, die Sie darüber informiert, dass das Zertifikat erfolgreich hochgeladen wurde.

7. Wählen Sie **Weiter**.

Syslog-Inhalte managen

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

Schritte

1. Wählen Sie für den Schritt **syslog-Inhalt verwalten** des Assistenten jeden Typ von Audit-Informationen aus, die Sie an den externen syslog-Server senden möchten.
   - **Audit-Protokolle senden**: Sendet StorageGRID-Ereignisse und Systemaktivitäten
   - **Sicherheitsereignisse senden**: Sendet Sicherheitsereignisse, z. B. wenn ein nicht autorisierter Benutzer versucht sich anzumelden oder sich ein Benutzer als root anmeldet
   - **Senden von Anwendungsprotokollen**: Sendet "Protokolldateien der StorageGRID Software" nützliche Informationen für die Fehlersuche, einschließlich:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Nur Admin-Nodes)
     - `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 Federation-Anfragen von Remote-Systemen.
2. Verwenden Sie die Dropdown-Menüs, um den Schweregrad und die Einrichtung (Meldungstyp) für jede zu sendende Kategorie von Audit-Informationen auszuwählen.

   Durch das Festlegen von Schweregraden und Einrichtungswerten können Sie die Protokolle auf anpassbare Weise für eine einfachere Analyse zusammenfassen.

   a. Wählen Sie für **Severity Passthrough** aus, oder wählen Sie einen Schweregrad zwischen 0 und 7 aus.

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

Schweregrad	Beschreibung
Passthrough	Jede an das externe Syslog gesendete Nachricht hat denselben Schweregrad wie bei der lokalen Anmeldung am Knoten: • Für Prüfprotokolle lautet der Schweregrad „Info“. • Bei Sicherheitsereignissen werden die Schweregrade von der Linux-Distribution auf den Knoten generiert. • Bei Anwendungsprotokollen variieren die Schweregrade zwischen „Info“ und „Hinweis“, je nachdem, was das Problem ist. Wenn beispielsweise ein NTP-Server hinzugefügt und eine HA-Gruppe konfiguriert wird, wird der Wert „Info“ angezeigt, während der SSM- oder RSM-Service absichtlich angehalten wird, wird der Wert „Hinweis“ angezeigt. • Für Zugriffsprotokolle lautet der Schweregrad „Info“.
0	Notfall: System ist unbrauchbar
1	Warnung: Maßnahmen müssen sofort ergriffen werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber bedeutender Zustand
6	Information: Informationsmeldungen
7	Debug: Debug-Level-Meldungen

b. Wählen Sie für **Facilty Passthrough** aus, oder wählen Sie einen Wert zwischen 0 und 23 aus.

   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.

Anlage	Beschreibung
Passthrough	Jede Nachricht, die an das externe Syslog gesendet wird, hat denselben Einrichtungswert wie bei der lokalen Anmeldung am Knoten: • Für Audit-Protokolle lautet die an den externen Syslog-Server gesendete Einrichtung „local7“. • Bei Sicherheitsereignissen werden die Einrichtungswerte von der linux-Distribution auf den Knoten generiert. • Für Anwendungsprotokolle 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 • Für Zugriffsprotokolle lautet die an den externen Syslog-Server gesendete Einrichtung „local0“.
0	kern (Kernelmeldungen)
1	Benutzer (Meldungen auf Benutzerebene)
2	E-Mail
3	Daemon (Systemdemonen)
4	Auth (Sicherheits-/Autorisierungsmeldungen)
5	Syslog (intern erzeugte Nachrichten durch syslogd)
6	lpr (Liniendrucker-Subsystem)
7	nachrichten (Netzwerk-News-Subsystem)
8	UUCP
9	Cron (Clock Daemon)
10	Sicherheit (Sicherheits-/Autorisierungsmeldungen)

Anlage	Beschreibung
11	FTP
12	NTP
13	Logaudit (Protokollaudit)
14	Logalert (Protokollwarnung)
15	Uhr (Uhrzeitdaemon)
16	Local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Wählen Sie **Weiter**.

Versenden von Testmeldungen

Bevor Sie beginnen, einen externen Syslog-Server zu verwenden, sollten Sie anfordern, dass alle Knoten im Raster Testmeldungen an den externen Syslog-Server senden. Sie sollten diese Testmeldungen verwenden, um Sie bei der Validierung Ihrer gesamten Protokollierungs-Infrastruktur zu unterstützen, bevor Sie Daten an den externen Syslog-Server senden.

> Verwenden Sie die Konfiguration des externen Syslog-Servers erst, wenn Sie bestätigen, dass der externe Syslog-Server von jedem Knoten in Ihrem Raster eine Testmeldung erhalten hat und dass die Nachricht erwartungsgemäß verarbeitet wurde.

Schritte

1. Wenn Sie keine Testnachrichten senden möchten, weil Sie sicher sind, dass Ihr externer Syslog-Server korrekt konfiguriert ist und Audit-Informationen von allen Knoten in Ihrem Raster empfangen kann, wählen Sie **Überspringen und Beenden**.

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

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

   Die Testergebnisse werden kontinuierlich auf der Seite angezeigt, bis Sie den Test beenden. Während der Test läuft, werden Ihre Audit-Meldungen 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**.

   Weitere Informationen finden Sie unter, "Fehlerbehebung für einen externen Syslog-Server" um Sie bei der Behebung von Fehlern zu unterstützen.

4. Warten Sie, bis ein grünes Banner angezeigt wird, dass alle Nodes die Tests bestanden haben.
5. Überprüfen Sie den Syslog-Server, ob Testmeldungen empfangen und verarbeitet werden wie erwartet.

   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 **Stop and Finish**.

   Sie gelangen zurück zur Seite **Audit und Syslog Server**. Ein grünes Banner zeigt an, dass die Syslog-Server-Konfiguration gespeichert wurde.

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

Protokollspeicherort auswählen

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

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

Bei Verwendung von `/var/local/log/localaudit.log` werden die Audit-Protokolleinträge für Grid Manager und Tenant Manager möglicherweise an einen Storage Node gesendet. Mit dem Befehl finden Sie den Node mit den neuesten Einträgen `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`.

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

Schritte

1. Wählen Sie **Protokollspeicherort** > **Lokaler Knoten und externer Server**.
2. Um den Protokollspeicherort für die Protokolltypen zu ändern, wählen Sie eine andere Option.

   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. Um Protokolle über einen längeren Zeitraum zu speichern, Verwenden Sie einen Mandanten und einen Bucket zur Protokollspeicherung .
Admin-Nodes/lokale Nodes	Audit-Meldungen werden an das Überwachungsprotokoll auf Admin-Nodes gesendet, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden auf den Knoten gespeichert, die sie generiert haben. Die Audit-Informationen werden in folgenden Dateien gespeichert: • Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Datei ist normalerweise leer oder fehlt. Sie kann sekundäre Informationen enthalten, z. B. 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 Sieeinen externen Syslog-Server konfiguriert .
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 Sieeinen externen Syslog-Server konfiguriert .

3. Wählen Sie **Speichern**.

   Es wird eine Warnmeldung angezeigt.

4. Wählen Sie **OK**, um zu bestätigen, dass Sie das Ziel für die Audit-Informationen ändern möchten.

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

Verwenden Sie einen Eimer

Die Protokolle werden regelmäßig rotiert. Verwenden Sie einen S3-Bucket im selben Grid, um Protokolle über einen längeren Zeitraum zu speichern.

1. Wählen Sie **Protokollspeicherort** > **Bucket verwenden**.
2. Aktivieren Sie das Kontrollkästchen **Archivprotokolle aktivieren**.
3. Wenn der aufgeführte Mandant und Bucket nicht die sind, die Sie verwenden möchten, wählen Sie **Mandanten und Bucket ändern** und dann entweder **Mandanten und Bucket erstellen** oder **Mandanten und Bucket auswählen**.

   Mandanten und Bucket erstellen

   a. Geben Sie einen neuen Mandantennamen ein.
   b. Geben Sie ein Kennwort für den neuen Mandanten ein und bestätigen Sie es.
   c. Geben Sie einen neuen Bucket-Namen ein.
   d. Wählen Sie **Erstellen und aktivieren**.

   Wählen Sie Mandant und Bucket aus

   a. Wählen Sie aus dem Pulldown-Menü einen Mandantennamen aus.
   b. Wählen Sie einen Bucket aus dem Pulldown-Menü aus.
   c. Wählen Sie **Auswählen und aktivieren**.

4. Wählen Sie **Speichern**.

   Protokolle werden im von Ihnen angegebenen Mandanten und Bucket gespeichert. Der Objektschlüsselname für die Protokolle hat dieses Format:

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   Beispiel:

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```

Verwenden Sie SNMP-Überwachung

Verwenden Sie SNMP-Überwachung

Wenn Sie StorageGRID mit dem Simple Network Management Protocol (SNMP)

überwachen möchten, müssen Sie den SNMP-Agent konfigurieren, der in StorageGRID enthalten ist.

- "Konfigurieren Sie den SNMP-Agent"
- "Aktualisieren Sie den SNMP-Agent"

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder -Daemon ausgeführt, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Warnmeldungen. Die MIB enthält auch Informationen zur Systembeschreibung wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID-Knoten unterstützt auch eine Untergruppe von MIB-II-Objekten.

> Finden Sie "Zugriff auf MIB-Dateien" heraus, ob Sie die MIB-Dateien auf Ihrem Grid-Knoten herunterladen möchten.

Zunächst ist SNMP auf allen Knoten deaktiviert. Wenn Sie den SNMP-Agent konfigurieren, erhalten alle StorageGRID-Knoten die gleiche Konfiguration.

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

Traps

Traps sind Benachrichtigungen, die vom SNMP-Agenten gesendet werden und keine Bestätigung durch das Managementsystem erfordern. Traps dienen dazu, das Managementsystem über etwas innerhalb von StorageGRID zu informieren, wie z. B. eine Warnung, die ausgelöst wird.

Traps werden in allen drei Versionen von SNMP unterstützt.

Informiert

Informationen sind ähnlich wie Traps, aber sie erfordern eine Bestätigung durch das Management-System. Wenn der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung erhält, wird die Benachrichtigung erneut gesendet, bis eine Bestätigung empfangen oder der maximale Wiederholungswert erreicht wurde.

Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden in folgenden Fällen versendet:

- Eine Standardwarnung oder eine benutzerdefinierte Meldung wird für jeden Schweregrad ausgelöst. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie "Konfigurieren Sie eine Stille"für die Warnmeldung. Benachrichtigungen werden von der gesendet"Administratorknoten des bevorzugten Absenders".

  Jeder Alarm wird einem von drei Trap-Typen basierend auf dem Schweregrad des Alarms zugeordnet: ActiveMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnungen, die diese Traps auslösen können, finden Sie unter "Alerts Referenz".

Unterstützung von SNMP-Versionen

Die Tabelle bietet eine allgemeine Zusammenfassung der unterstützten SNMP-Versionen.

	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 (TRAP und INFORM)	Nur Traps	Traps und informiert	Traps und informiert
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 Nodes im Grid erhalten dieselbe 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 Sie den SNMP-Agent

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

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

Alle Knoten im Grid verwenden dieselbe SNMP-Konfiguration.

Geben Sie die Grundkonfiguration an

Aktivieren Sie als ersten Schritt den StorageGRID-SMNP-Agent und geben Sie grundlegende Informationen an.

Schritte

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

   Die Seite SNMP Agent wird angezeigt.

2. Um den SNMP-Agent 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** kann maximal 255 Zeichen lang sein.
Standort des Systems	Optional Der Speicherort des StorageGRID-Systems, der in SNMP-Nachrichten als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information sein, die hilfreich ist, um zu ermitteln, wo sich das StorageGRID System befindet. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Dieser Wert gilt für alle Knoten im StorageGRID-System. **Systemstandort** kann maximal 255 Zeichen lang sein.
Aktivieren Sie SNMP-Agentenbenachrichtigungen	• 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.
Aktivieren Sie Authentifizierungs-Traps	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er falsch authentifizierte Protokollmeldungen empfängt.

Geben Sie Community-Strings ein

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 die Community-Zeichenfolge einem der hier angegebenen Werte entspricht, sendet der SNMP-Agent eine Antwort an das Managementsystem.

Schritte

1. Geben Sie für **Read-Only Community** optional eine Community-Zeichenfolge ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agent-Adressen zu ermöglichen.

   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.

   Jede Community-Zeichenfolge darf maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

2. Wählen Sie **Add another Community string**, um zusätzliche Strings hinzuzufügen.

   Es sind bis zu fünf Zeichenfolgen zulässig.

Trap-Ziele erstellen

Verwenden Sie die Registerkarte Trap-Ziele im Abschnitt andere 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. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

Schritte

1. Geben Sie für das Feld **Default Trap Community** optional den Standard-Community-String ein, den Sie für SNMPv1- oder SNMPv2-Trap-Ziele verwenden möchten.

   Wenn Sie ein bestimmtes Trap-Ziel definieren, können Sie nach Bedarf eine andere (benutzerdefinierte) Community-Zeichenfolge bereitstellen.

   Default Trap Community kann maximal 32 Zeichen lang sein und darf keine Leerzeichen enthalten.

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

SNMPv1

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

Feld	Beschreibung
Typ	Muss Trap für SNMPv1 sein.
Host	Eine IPv4- oder IPv6-Adresse oder ein vollständig qualifizierter Domänenname (FQDN) für den Empfang des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, falls 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 darf keine Leerzeichen enthalten.

SNMPv2c

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

Feld	Beschreibung
Typ	Gibt an, ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, es sei denn, Sie müssen TCP verwenden.
Community-Zeichenfolge	Verwenden Sie die Standard-Trap-Community, falls 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 darf keine Leerzeichen enthalten.

SNMPv3

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

Feld	Beschreibung
Typ	Gibt an, ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, 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 maßgebliche Engine-IDs angezeigt. • Wenn Sie **Inform** 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. Gehen Sie zuUSM-Benutzer erstellen, 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.

Erstellen Sie Agentenadressen

Verwenden Sie optional die Registerkarte Agentenadressen im Abschnitt andere Konfigurationen, um eine oder mehrere „Listening-Adressen“ anzugeben. Dies sind die StorageGRID-Adressen, über die der SNMP-Agent Abfragen empfangen kann.

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

Schritte

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

Feld	Beschreibung
Internetprotokoll	Gibt an, 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	Welches StorageGRID-Netzwerk der Agent abhört. • Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent hört auf Abfragen in allen drei Netzwerken. • Grid-Netzwerk • Admin-Netzwerk • Client-Netzwerk **Hinweis**: Wenn Sie das Client-Netzwerk für unsichere Daten verwenden und eine Agentenadresse für das Client-Netzwerk erstellen, beachten Sie, dass der SNMP-Datenverkehr ebenfalls unsicher ist.
Port	Optional die Portnummer, die der SNMP-Agent abhören soll. Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben. **Hinweis**: Wenn Sie den SNMP-Agent speichern, öffnet StorageGRID automatisch die Agentenadressen-Ports 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.

Erstellen Sie USM-Benutzer

Wenn Sie SNMPv3 verwenden, definieren Sie auf der Registerkarte USM-Benutzer im Abschnitt andere Konfigurationen die USM-Benutzer, die zum Abfragen der MIB oder zum Empfangen von Traps und Informationen berechtigt sind.

> Für SNMPv3-Trap-Ziele wird empfohlen, für jeden Admin-Knoten einen USM-Benutzer zu erstellen. Wenn nicht jeder Admin-Knoten über einen USM-Benutzer verfügt, erhält Ihr Verwaltungssystem möglicherweise keine Benachrichtigungen mehr, wenn der primäre Admin-Knoten ausfällt.

SNMPv3 *Inform* Ziele müssen Benutzer mit Engine-IDs haben. 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 enthalten und dürfen keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht mehr geändert werden.
Schreibgeschützter MIB-Zugriff	Wenn diese Option ausgewählt ist, sollte dieser Benutzer Lesezugriff auf die MIB haben.
Maßgeblicher Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, ist die ID der autorisierenden Engine für diesen Benutzer. Geben Sie 10 bis 64 Hex-Zeichen (5 bis 32 Byte) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in Trap-Zielen für Informationen 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, die schreibgeschützten MIB-Zugriff haben, 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 Passwort sowie ein Datenschutzprotokoll und ein Passwort angeben. • **AuthNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort angeben.
Authentifizierungsprotokoll	Stellen Sie immer SHA ein, welches das einzige unterstützte Protokoll ist (HMAC-SHA-96).
Passwort	Das Kennwort, das dieser Benutzer zur Authentifizierung verwendet.

Feld	Beschreibung
Datenschutzprotokoll	Wird nur angezeigt, wenn Sie **authpriv** ausgewählt und immer auf AES gesetzt haben, das einzige unterstützte Datenschutzprotokoll.
Passwort	Wird nur angezeigt, wenn Sie **authpriv** ausgewählt haben. Das Passwort, das dieser Benutzer für den Datenschutz verwendet.

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-Agent

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

Weitere Informationen zu den einzelnen Feldern finden "Konfigurieren Sie den SNMP-Agent"Sie auf der Seite SNMP-Agent. Sie müssen unten auf der Seite **Speichern** auswählen, um alle Änderungen zu übernehmen, die Sie auf jeder Registerkarte vornehmen.

Schritte

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

   Die Seite SNMP Agent wird angezeigt.

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

   Wenn Sie den SNMP-Agent erneut aktivieren, bleiben alle früheren SNMP-Konfigurationseinstellungen erhalten.

3. Aktualisieren Sie optional die Informationen im Abschnitt Grundkonfiguration:
   a. Aktualisieren Sie bei Bedarf den * Systemkontakt* und **Systemstandort**.
   b. Aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Enable SNMP Agent notifications**, 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 **Enable Authentication Traps**, um zu steuern, ob der StorageGRID-SNMP-Agent Authentifizierungs-Traps sendet, wenn er falsch

authentifizierte Protokollmeldungen empfängt.

4. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren oder fügen Sie optional eine **schreibgeschützte Community** im Abschnitt Community Strings hinzu.
5. Um Trap-Ziele zu aktualisieren, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte Trap-Ziele aus.

   Auf dieser Registerkarte können Sie ein oder mehrere Ziele für StorageGRID-Trap- oder Informationsbenachrichtigungen definieren. Wenn Sie den SNMP-Agenten aktivieren und **Speichern** auswählen, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, wenn Warnungen ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

   Weitere Informationen zu den Eingeben finden Sie unter "Erstellen Sie Trap-Ziele".

   - Optional können Sie die Standard-Trap-Community aktualisieren oder entfernen.

     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 **Create**.
   - Um ein Trap-Ziel zu bearbeiten, aktivieren Sie das Optionsfeld und wählen **Bearbeiten**.
   - Um ein Trap-Ziel zu entfernen, aktivieren Sie das Optionsfeld und wählen Sie **Entfernen** aus.
   - Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der Seite.
6. Um die Agentenadressen zu aktualisieren, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte Agentenadressen aus.

   Verwenden Sie diese Registerkarte, um eine oder mehrere „Listening-Adressen“ anzugeben. Dies sind die StorageGRID-Adressen, über die der SNMP-Agent Abfragen empfangen kann.

   Weitere Informationen zu den Eingeben finden Sie unter "Erstellen Sie Agentenadressen".

   - Um eine Agentenadresse hinzuzufügen, wählen Sie **Create**.
   - Um eine Agentenadresse zu bearbeiten, aktivieren Sie das Optionsfeld und wählen **Bearbeiten**.
   - Um eine Agentenadresse zu entfernen, aktivieren Sie das Optionsfeld, und wählen Sie **Entfernen** aus.
   - Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der Seite.
7. Um USM-Benutzer zu aktualisieren, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

   Über diese Registerkarte können Sie USM-Benutzer definieren, die berechtigt sind, die MIB abzufragen oder Traps zu empfangen und zu informieren.

   Weitere Informationen zu den Eingeben finden Sie unter "USM-Benutzer erstellen".

   - Um einen USM-Benutzer hinzuzufügen, wählen Sie **Create**.
   - Um einen USM-Benutzer zu bearbeiten, wählen Sie das Optionsfeld und dann **Bearbeiten** aus.

     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 ID der autorisierenden Engine eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

- Um einen USM-Benutzer zu entfernen, wählen Sie das Optionsfeld und dann **Entfernen** aus.

  Wenn der Benutzer, den Sie entfernt haben, derzeit für ein Trap-Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen. Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

- Um Ihre Änderungen zu übernehmen, wählen Sie **Speichern** unten auf der Seite.

8. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, wählen Sie **Speichern**.

Zugriff auf MIB-Dateien

MIB-Dateien enthalten Definitionen und Informationen über die Eigenschaften der verwalteten Ressourcen und Dienste für die Knoten in der Tabelle. Sie können auf MIB-Dateien zugreifen, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Grids nützlich sein.

Weitere Informationen zu SNMP- und MIB-Dateien finden Sie unter"Verwenden Sie SNMP-Überwachung".

Zugriff auf MIB-Dateien

Gehen Sie wie folgt vor, um auf die MIB-Dateien zuzugreifen.

Schritte

1. Wählen Sie **Konfiguration** > **Überwachung** > **SNMP-Agent**.
2. Wählen Sie auf der Seite des SNMP-Agenten die Datei aus, die Sie herunterladen möchten:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definiert die Alarmtabelle und Benachrichtigungen (Traps), auf die auf allen Admin-Knoten zugegriffen werden kann.
   - **Es-NETAPP-06-MIB.mib**: Definiert Objekte und Benachrichtigungen für E-Series-basierte Appliances.
   - **MIB_1_10.zip**: Definiert Objekte und Benachrichtigungen für Geräte mit BMC-Schnittstelle.

     Sie können auch auf MIB-Dateien am folgenden Speicherort auf jedem StorageGRID-Knoten zugreifen: `/usr/share/snmp/mibs`

3. So extrahieren Sie die StorageGRID-OIDs aus der MIB-Datei:

   a. Erhalten Sie die OID des Stamms 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)

   b. Grep für die StorageGRID-OID in der gesamten Struktur (zum verbinden von Linien verwenden `paste`):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```

Der `snmptranslate` Befehl hat viele Optionen, die nützlich sind, um die MIB zu erforschen. Dieser Befehl ist auf jedem StorageGRID-Node verfügbar.

MIB-Dateiinhalte

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)	Typ	Zugang	MIB-Modul	Beschreibung
ActiveAlertCount		Integer32	Schreibgeschützt	NETAPP-STORAGEGRID-MIB	Die Anzahl der aktiven Warnungen in der activeAlertTable.
ActiveAlertTable		Sequenz von ActiveAlertEntry	Nicht zugänglich	NETAPP-STORAGEGRID-MIB	Eine Tabelle mit aktiven Warnmeldungen in StorageGRID.
aktiverAlarmeintrag		Sequenz	Nicht zugänglich	NETAPP-STORAGEGRID-MIB	Ein einzelner StorageGRID Alarm, indiziert nach Alarm-ID.
ActiveAlertId		Oktettzeichenfolge	Schreibgeschützt	NETAPP-STORAGEGRID-MIB	Die ID der Warnmeldung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
ActiveAlertName		Oktettzeichenfolge	Schreibgeschützt	NETAPP-STORAGEGRID-MIB	Der Name der Warnmeldung.
ActiveAlertInstance		Oktettzeichenfolge	Schreibgeschützt	NETAPP-STORAGEGRID-MIB	Der Name der Entität, die die Warnmeldung generiert hat, normalerweise der Knotenname.
ActiveAlertSchweregrad		Oktettzeichenfolge	Schreibgeschützt	NETAPP-STORAGEGRID-MIB	Der Schweregrad der Meldung.

Objektname	Objekt-ID (OID)	Typ	Zugang	MIB-Modul	Beschreibung
ActiveAlertStartTime		Datum und Uhrzeit	Schreibgeschützt	NETAPP-STORAGEGRID-MIB	Der Zeitpunkt, zu dem der Alarm ausgelöst wurde.

Erfassung zusätzlicher StorageGRID-Daten

PUT- und GET-Performance werden überwacht

Sie können die Performance bestimmter Vorgänge, z. B. Objektspeicher und -Abruf, überwachen, um Änderungen zu identifizieren, die möglicherweise weitere Untersuchungen erfordern.

Über diese Aufgabe

Zum Monitoring der PUT- und DER GET-Performance können S3-Befehle direkt von einer Workstation oder mit der Open-Source-S3tester-Applikation ausgeführt werden. Mit diesen Methoden können Sie die Leistung unabhängig von Faktoren bewerten, die außerhalb von StorageGRID liegen, z. B. Probleme mit einer Client-Applikation oder Probleme mit einem externen Netzwerk.

Wenn SIE Tests für PUT- und GET-Vorgänge durchführen, beachten Sie folgende Richtlinien:

- Objektgrößen sind vergleichbar mit den Objekten, die normalerweise in das Grid eingespeist werden.
- Durchführung von Vorgängen an lokalen und Remote Standorten

Meldungen im "Prüfprotokoll"geben die Gesamtzeit an, die für die Ausführung bestimmter Vorgänge benötigt wird. Um z. B. die Gesamtverarbeitungszeit für eine S3-GET-Anforderung zu bestimmen, können Sie den Wert des ZEITATTRIBUTS in der SGET-Audit-Nachricht prüfen. Das ZEITATTRIBUT finden Sie auch in den Audit-Meldungen für die folgenden S3-Operationen: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Bei der Analyse von Ergebnissen sollten Sie die durchschnittliche Zeit zur Erfüllung einer Anfrage sowie den Gesamtdurchsatz betrachten, den Sie erreichen können. Wiederholen Sie die gleichen Tests regelmäßig, und notieren Sie die Ergebnisse, damit Sie Trends identifizieren können, die eine Untersuchung erfordern könnten.

- Sie können "Laden Sie S3tester von Github herunter".

Überwachen von Objektverifizierungsvorgängen

Das StorageGRID System kann die Integrität von Objektdaten auf Storage-Nodes überprüfen und sowohl beschädigte als auch fehlende Objekte prüfen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".

Über diese Aufgabe

Zwei "Verifizierungsprozesse" arbeiten zusammen, um die Datenintegrität zu gewährleisten:

- **Hintergrundüberprüfung** läuft automatisch und überprüft kontinuierlich die Richtigkeit der Objektdaten.

Hintergrund-Verifizierung überprüft automatisch und kontinuierlich alle Storage-Nodes, um festzustellen, ob es beschädigte Kopien von replizierten und mit Erasure Coding verschlüsselten Objektdaten gibt. Falls Probleme gefunden werden, versucht das StorageGRID System automatisch, die beschädigten Objektdaten durch Kopien zu ersetzen, die an anderer Stelle im System gespeichert sind. Die Hintergrundüberprüfung wird nicht für Objekte in einem Cloud-Storage-Pool ausgeführt.

> Die Warnung **Unidentified Corrupt Object Detected** wird ausgelöst, wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann.

- **Objektexistenz-Prüfung** kann von einem Nutzer ausgelöst werden, um die Existenz (obwohl nicht die Richtigkeit) von Objektdaten schneller zu überprüfen.

  Die ObjektExistenz überprüft, ob alle erwarteten replizierten Kopien von Objekten und mit Erasure Coding verschlüsselten Fragmenten auf einem Storage Node vorhanden sind. Die Prüfung des Objektbestandes bietet eine Möglichkeit zur Überprüfung der Integrität von Speichergeräten, insbesondere dann, wenn kürzlich Probleme mit der Hardware die Datenintegrität beeinträchtigen könnten.

Sie sollten die Ergebnisse aus Hintergrundverifizierungen und Objektprüfungen regelmäßig überprüfen. Untersuchen Sie alle Instanzen beschädigter oder fehlender Objektdaten sofort, um die Ursache zu ermitteln.

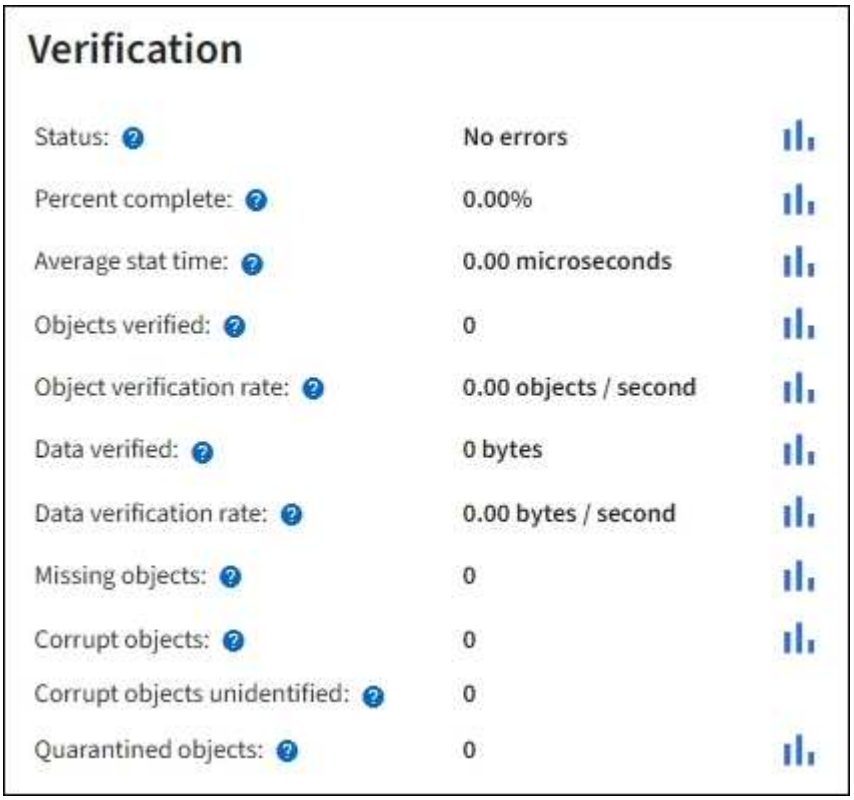
Schritte

1. Prüfen Sie die Ergebnisse aus Hintergrundverifizierungen:

   a. Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte**.

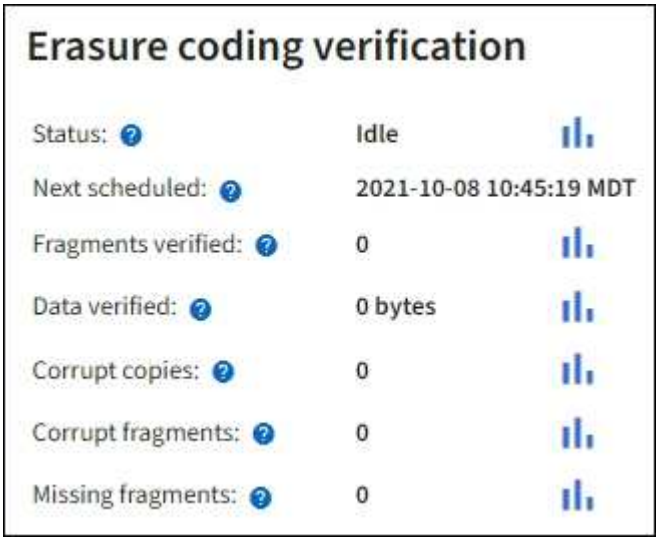
   b. Überprüfen Sie die Überprüfungsergebnisse:

      - Um die Verifizierung replizierter Objektdaten zu prüfen, sehen Sie sich die Attribute im Abschnitt Überprüfung an.



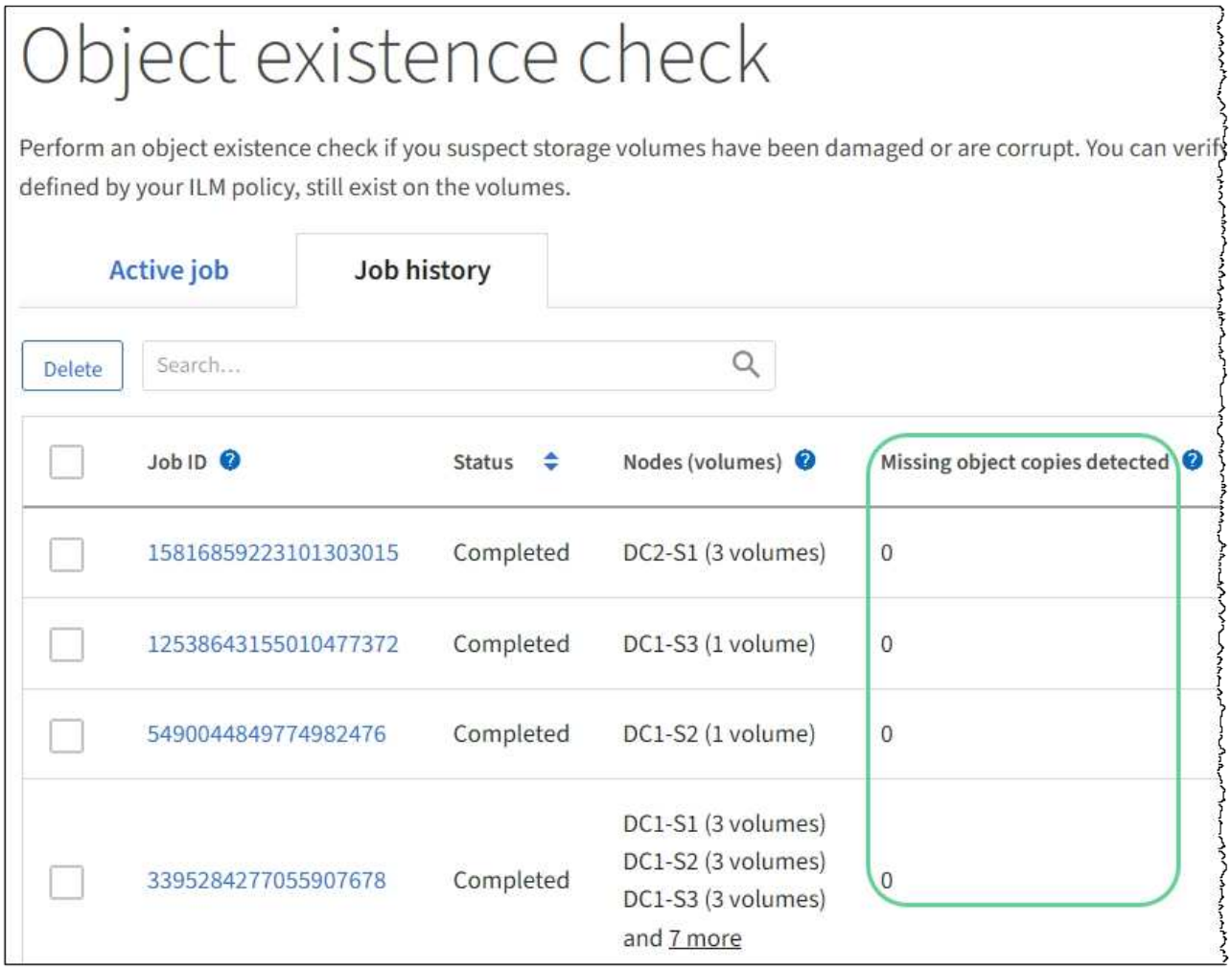
      - Um die Überprüfung von Fragment mit Löschungscode zu überprüfen, wählen Sie ***Storage Node*** >

ILM aus, und sehen Sie sich die Attribute im Abschnitt zur Verifizierung von Erasure-Coding an.



Wählen Sie das Fragezeichen neben dem Namen eines Attributs aus, um Hilfetext anzuzeigen.

2. Überprüfen Sie die Ergebnisse von Objektprüfaufträgen:
   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 „Möglicherweise verlorene Objekte“ ausgelöst wurde, wenden Sie sich an den technischen Support.



Audit-Meldungen prüfen

Audit-Meldungen helfen Ihnen, die detaillierten Vorgänge Ihres StorageGRID Systems besser zu verstehen. Sie können mithilfe von Audit-Protokollen Probleme beheben und die Performance bewerten.

Während des normalen Systembetriebs generieren alle StorageGRID Services wie folgt Audit-Meldungen:

- Systemaudits-Meldungen betreffen das Auditing des Systems selbst, den Status von Grid-Nodes, systemweite Task-Aktivitäten und Service-Backup-Vorgänge.
- Audit-Nachrichten zum Objekt-Storage beziehen sich auf die Storage- und das Management von Objekten in StorageGRID, einschließlich Objekt-Storage und -Abruf, Grid-Node- zu Grid-Node-Transfers und Verifizierungen.
- Audit-Meldungen zu Lese- und Schreibzugriffen von Clients werden protokolliert, wenn eine S3-Client-Applikation zum Erstellen, Ändern oder Abrufen eines Objekts fordert.
- Managementaudits protokollieren Benutzeranfragen an die Management-API.

Jeder Admin-Knoten speichert Audit-Meldungen in Textdateien. Die Revisionsfreigabe enthält die aktive Datei (Audit.log) sowie komprimierte Audit-Protokolle aus früheren Tagen. Jeder Node im Raster speichert auch eine Kopie der auf dem Node generierten Audit-Informationen.

Sie können über die Befehlszeile des Admin-Knotens direkt auf Audit-Log-Dateien zugreifen.

StorageGRID kann standardmäßig Audit-Informationen senden oder das Ziel ändern:

- StorageGRID ist standardmäßig auf lokale Node-Überwachungsziele eingestellt.
- Die Audit-Protokolleinträge von Grid Manager und Tenant Manager können an einen Storage Node gesendet werden.
- Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist.
- "Informationen zum Konfigurieren der Protokollverwaltung" .

Details zur Audit-Log-Datei, zum Format der Audit-Meldungen, zu den Typen der Audit-Meldungen und zu den verfügbaren Tools zur Analyse von Audit-Meldungen finden Sie unter "Prüfung von Audit-Protokollen".

Erfassen von Protokolldateien und Systemdaten

Sie können StorageGRID -Protokolldateien und Systemdaten, einschließlich Konfigurationsdaten, abrufen und an den technischen Support senden.

Bevor Sie beginnen

- Sie sind beim Grid Manager auf einem beliebigen Admin-Knoten mit einem"Unterstützter Webbrowser" .
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Verwenden Sie den Grid Manager, um"Log-Dateien" , Systemdaten und Konfigurationsdaten von jedem Grid-Knoten für den von Ihnen ausgewählten Zeitraum. Die Daten werden gesammelt und archiviert in einem `.tar.gz` Datei, die Sie dann auf Ihren lokalen Computer herunterladen oder an den technischen Support senden 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 Sie die Protokollverwaltung und den externen Syslog-Server" .

Schritte

1. Wählen Sie **Support** > **Tools** > **Protokollsammlung**. Es wird eine Tabelle mit Knoten angezeigt.
2. Wählen Sie die Grid-Knoten aus, für die Sie Protokolldateien sammeln möchten.

   Sie können nach Knotenname, Site und Knotentyp sortieren. Die Spalten „Site“ und „Knotentyp“ enthalten Filter zur Auswahl nach einzelnen Sites und Knotentypen.

3. Wählen Sie **Weiter**.
4. Wählen Sie den Datums- und Zeitbereich der Daten aus, 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 von einem Admin-Knoten zum Download abgerufen zu werden. Wenn eines dieser Szenarien eintritt, starten Sie die Protokollerfassung mit einem kleineren Datensatz neu.

5. 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.
6. Optional können Sie im Textfeld **Notizen** Notizen zu den Protokolldateien eingeben, die Sie erfassen.

   Mithilfe dieser Hinweise können Sie Informationen zum technischen Support über das Problem geben, das Sie zum Erfassen der Protokolldateien aufgefordert hat. Ihre Notizen werden zu einer Datei mit dem Namen, zusammen mit anderen Informationen über die Log-Datei-Sammlung hinzugefügt `info.txt`. Die `info.txt` Datei wird im Archivpaket der Protokolldatei gespeichert.

7. Geben Sie im Textfeld **Bereitstellungspassphrase** die Bereitstellungspassphrase für Ihr StorageGRID -System ein.
8. Wählen Sie **Protokolle sammeln**.

   Auf der Seite „Protokollsammlung“ können Sie den Fortschritt der Protokolldateisammlung für jeden Grid-Knoten überwachen.

   Wenn Sie eine Fehlermeldung über die Protokollgröße erhalten, versuchen Sie, Protokolle für einen kürzeren Zeitraum oder für weniger Nodes zu sammeln.

9. Wenn die Protokollerfassung fehlschlägt:
   - Wenn die Meldung „Protokollerfassung fehlgeschlagen“ angezeigt wird, können Sie die Protokollerfassung erneut versuchen oder die Sitzung ohne erneuten Versuch beenden.
   - Wenn die Meldung „Protokollerfassung teilweise fehlgeschlagen“ angezeigt wird, können Sie die Protokollerfassung erneut versuchen, die Sitzung beenden, die teilweise Protokolldatei herunterladen oder die teilweise Protokolldatei an AutoSupport senden.
10. Wenn die Protokolldateierfassung abgeschlossen ist:
    - Wählen Sie **Herunterladen**, um die `.tar.gz` Datei.
    - Wählen Sie **An AutoSupport senden**, um die `.tar.gz` Datei an den technischen Support.

      Der `.tar.gz` Die Datei enthält alle Protokolldateien aller Grid-Knoten, bei denen die Protokollerfassung erfolgreich war. Die kombinierte `.tar.gz` Die Datei enthält ein Protokolldateiarchiv für jeden Grid-Knoten.

    Gegenstand des AutoSupport Pakets ist `USER_TRIGGERED_SUPPORT_BUNDLE` .

11. Wählen Sie **Fertig**.

Der `.tar.gz` Die Datei wird gelöscht, wenn Sie **Fertig** auswählen. Stellen Sie sicher, dass Sie die Datei zuerst herunterladen oder senden.

Starten Sie manuell ein AutoSupport-Paket

Um den technischen Support bei der Fehlerbehebung in Ihrem StorageGRID System zu unterstützen, können Sie manuell ein AutoSupport Paket senden.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie verfügen über Root-Zugriff oder die Berechtigung „Andere Rasterkonfiguration“.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport*.
2. Wählen Sie auf der Registerkarte **Aktionen vom Benutzer ausgelöste 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.

3. Aktualisieren Sie nach 1 Minute die AutoSupport -Seite in Ihrem Browser, um auf die aktuellsten Ergebnisse zuzugreifen.

> Darüber hinaus können Sie"umfangreichere Logfiles und Systemdaten erfassen" und senden Sie sie an die NetApp Support Site.

Prüfen von Support-Kennzahlen

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte Metriken und Diagramme für Ihr StorageGRID System prüfen.

Bevor Sie beginnen

- Sie müssen im Grid-Manager mit einem angemeldet sein"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

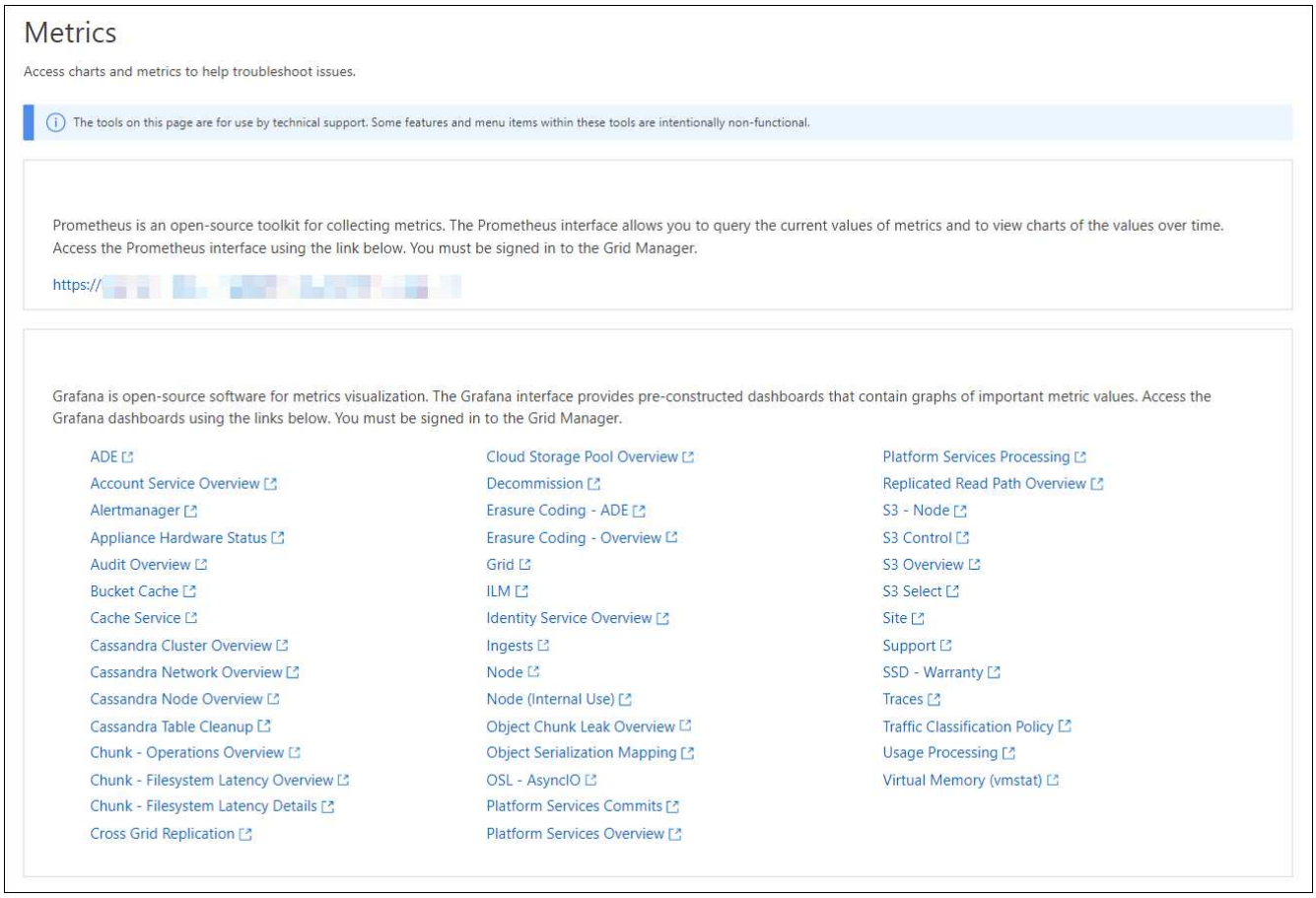
Auf der Seite Metriken können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist Open-Source-Software zum Sammeln von Kennzahlen. Grafana ist Open-Source-Software zur Visualisierung von Kennzahlen.

> Die auf der Seite Metriken verfügbaren Tools sind für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig und können sich ändern. Siehe Liste von "Häufig verwendete Prometheus-Kennzahlen".

Schritte

1. Wählen Sie gemäß den Anweisungen des technischen Supports **Support** > **Tools** > **Metriken**.

   Ein Beispiel für die Seite Metriken ist hier aufgeführt:



2. Um die aktuellen Werte der StorageGRID-Metriken abzufragen und Diagramme der Werte im Zeitverlauf anzuzeigen, klicken Sie im Abschnitt Prometheus auf den Link.

   Das Prometheus-Interface wird angezeigt. Sie können über diese Schnittstelle Abfragen für die verfügbaren StorageGRID-Metriken ausführen und StorageGRID-Metriken im Laufe der Zeit grafisch darstellen.

   > Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

3. Um über einen längeren Zeitraum auf vorkonfigurierte Dashboards mit Diagrammen zu StorageGRID-Kennzahlen zuzugreifen, klicken Sie im Abschnitt „Grafana“ auf die Links.

   Die Grafana-Schnittstelle für den ausgewählten Link wird angezeigt.

E/A-Priorisierung ändern

Durch die Priorisierung von Eingabe/Ausgabe (E/A) können Sie die relativen Prioritäten für E/A-Vorgänge im Grid ändern.

Standardmäßig wird dem PUT- und GET-E/A-Verkehr des Clients die höchste Priorität gegenüber Hintergrundaktivitäten wie dem Löschen von Erasure-Coded-Daten (EC) und der EC-Reparatur eingeräumt. Durch Erhöhen der Priorität der Bereinigung von Erasure-Coded-Daten (EC) und von EC-Reparaturaktivitäten können diese Aufgaben möglicherweise schneller abgeschlossen werden. Die Wirksamkeit von Änderungen der E/A-Priorisierung wird durch die Rate der Clientanforderungen, Schwankungen des Netzwerkverkehrs und andere laufende Netzwerkaufgaben beeinflusst.

Bevor Sie beginnen

- Überprüfen Sie die Seite zur E/A-Priorisierung, um festzustellen, welche Optionen sich auf Ihr Raster auswirken könnten.
- Bewerten Sie, ob der laufende Client-Verkehr längere Wartezeiten oder Client-Timeouts sicher bewältigen kann.

- Seien Sie darauf vorbereitet, die Auswirkungen der Priorisierungsänderung zu überwachen und bei Bedarf Anpassungen vorzunehmen. Diese Änderungen werden schnell umgesetzt, es kann jedoch Stunden dauern, bis ihre Wirkung sichtbar wird.

Schritte

1. Wählen Sie **Support** > **E/A-Priorisierung**.
2. (Optional) Ändern Sie die EC-Bereinigungs- und Reparaturpriorität für Hintergrundvorgänge, die EC-Daten bereinigen, von ihren Standardwerten.

   Verwenden Sie die standardmäßige niedrige EC-Bereinigungs- und Reparaturpriorität für Grids mit RAID-basierten Knoten.

3. Wählen Sie **Speichern**.
4. Überwachen Sie die"Metriken" um die Auswirkungen von Priorisierungsänderungen zu bewerten.

Führen Sie eine Diagnose aus

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support eine Diagnose auf Ihrem StorageGRID-System durchführen und die Ergebnisse überprüfen.

- "Prüfen von Support-Kennzahlen"
- "Häufig verwendete Prometheus-Kennzahlen"

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Die Seite Diagnose führt eine Reihe von diagnostischen Prüfungen zum aktuellen Status des Rasters durch. Jede diagnostische Prüfung kann einen von drei Zuständen haben:

- **Normal**: Alle Werte liegen im Normalbereich.
- **Achtung**: Ein oder mehrere der Werte liegen außerhalb des Normalbereichs.
- **Achtung**: Einer oder mehrere der Werte liegen deutlich außerhalb des Normalbereichs.

Diagnosestatus sind unabhängig von aktuellen Warnungen und zeigen möglicherweise keine betrieblichen Probleme mit dem Raster an. Beispielsweise wird bei einer Diagnose-Prüfung möglicherweise der Status „Achtung“ angezeigt, auch wenn keine Meldung ausgelöst wurde.

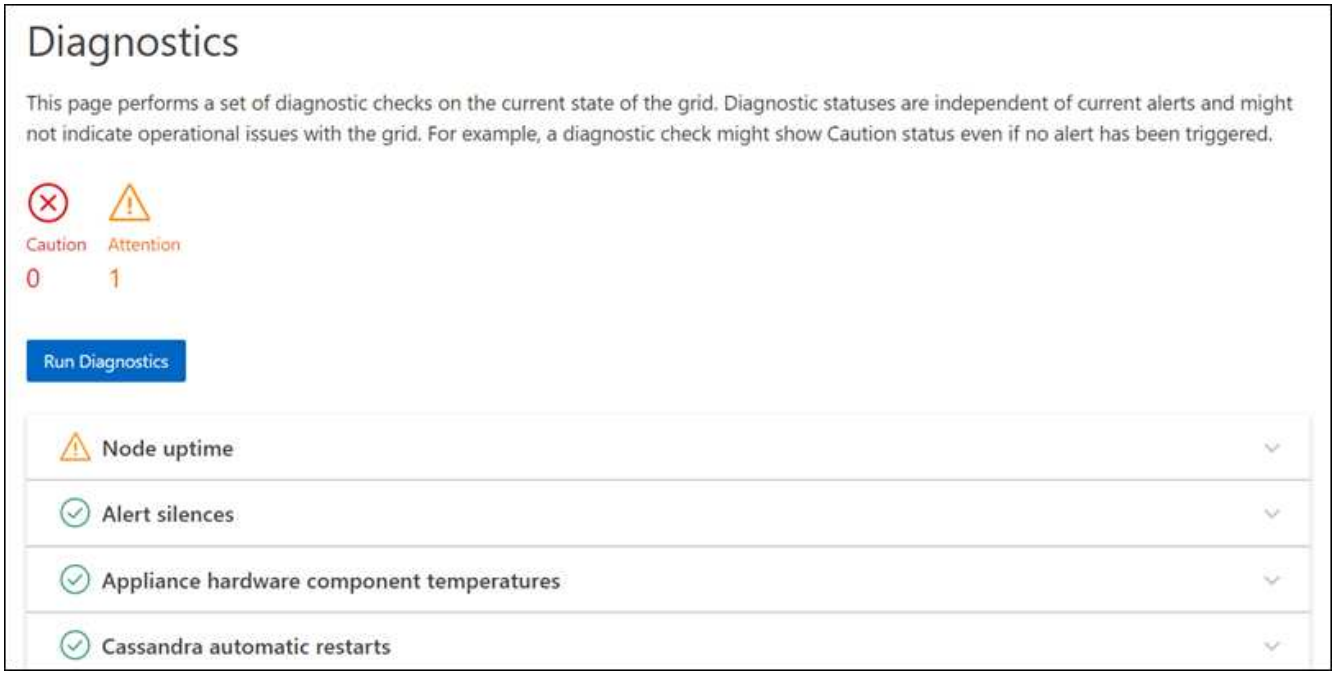
Schritte

1. Wählen Sie **Support** > **Tools** > **Diagnose**.

   Die Seite Diagnose wird angezeigt und zeigt die Ergebnisse für jede Diagnosetest an. Die Ergebnisse sind nach Schweregrad (Achtung, Achtung und dann normal) sortiert. Innerhalb jedes Schweregrads werden die Ergebnisse alphabetisch sortiert.

   In diesem Beispiel hat eine Diagnose den Status „Achtung“ und drei Diagnosen haben den Status

„Normal“.



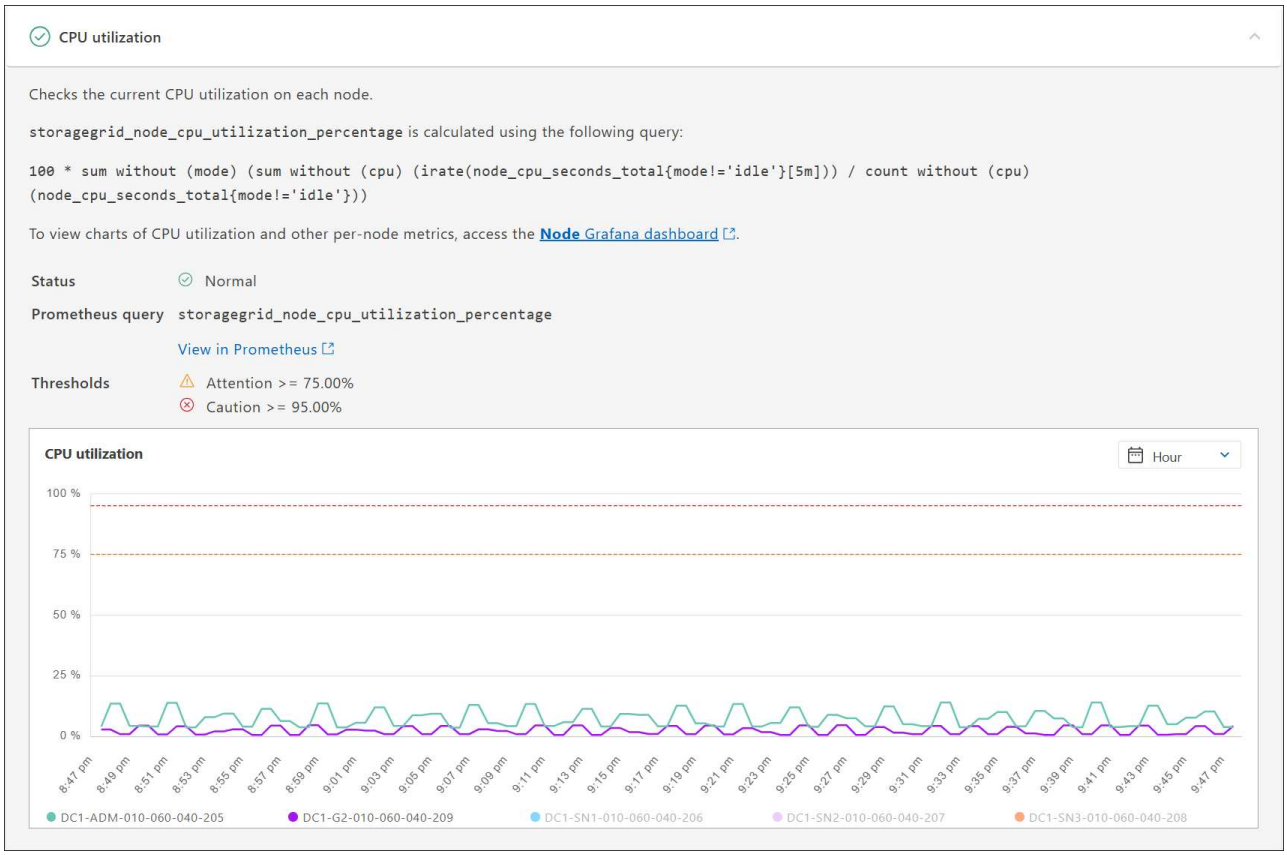
2. Wenn Sie mehr über eine bestimmte Diagnose erfahren möchten, klicken Sie auf eine beliebige Stelle in der Zeile.

   Details zur Diagnose und ihren aktuellen Ergebnissen werden angezeigt. Folgende Details sind aufgelistet:

   - **Status**: Der aktuelle Status dieser Diagnose: Normal, Achtung oder Achtung.
   - **Prometheus query**: Bei Verwendung für die Diagnose, der Prometheus Ausdruck, der verwendet wurde, um die Statuswerte zu generieren. (Ein Prometheus-Ausdruck wird nicht für alle Diagnosen verwendet.)
   - **Schwellenwerte**: Wenn für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden anormalen Diagnosestatus. (Schwellenwerte werden nicht für alle Diagnosen verwendet.)

     Sie können diese Schwellenwerte nicht ändern.

   - **Statuswerte**: Ein Diagramm und eine Tabelle (Tabelle nicht im Screenshot dargestellt), die den Status und den Wert der Diagnose im gesamten StorageGRID System anzeigen. 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, wählen Sie **Grafana-Dashboard**.

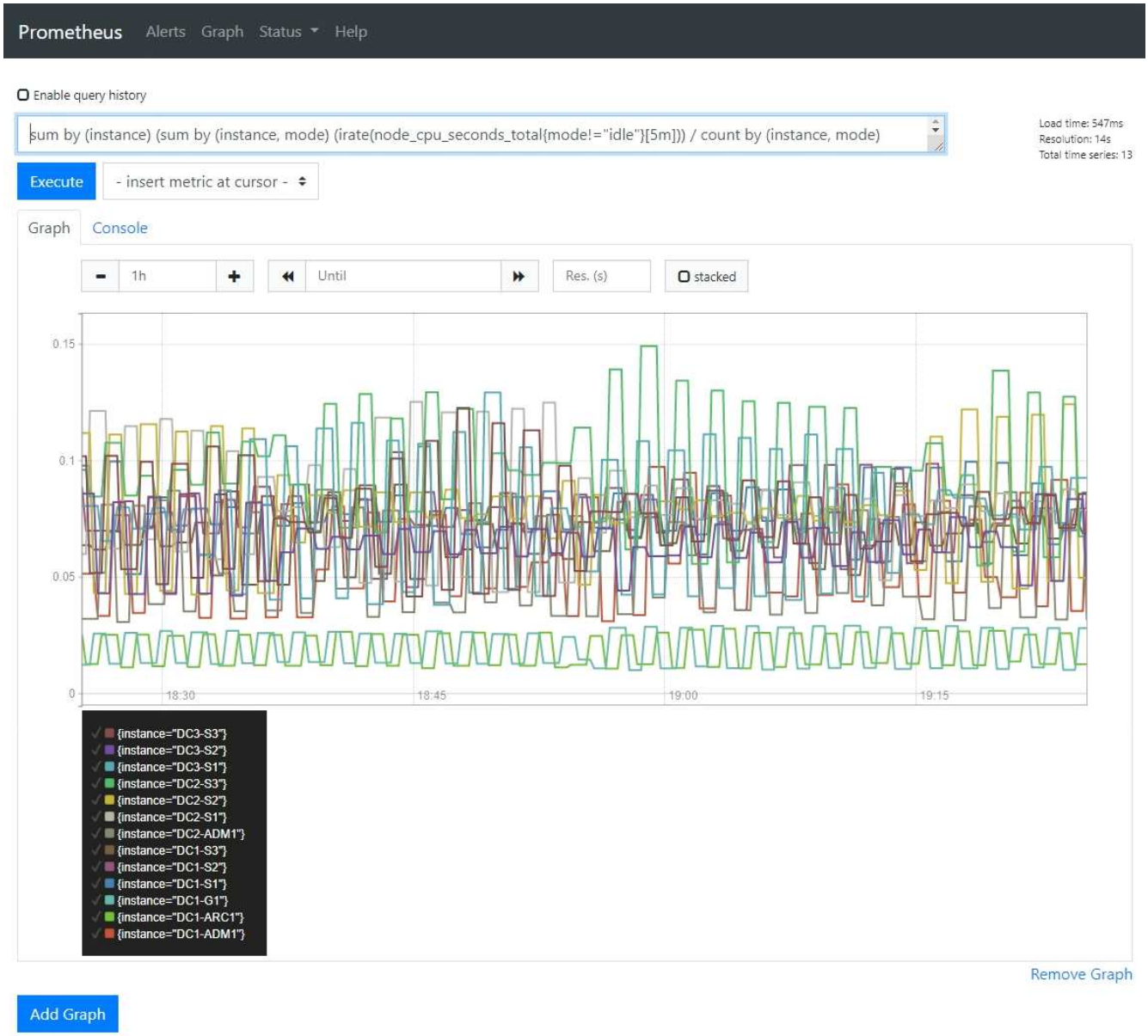
   Dieser Link wird nicht für alle Diagnosen angezeigt.

   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 über die Zeit zu sehen, klicken Sie auf **Anzeigen in Prometheus**.

   Es wird ein Prometheus-Diagramm des in der Diagnose verwendeten Ausdrucks angezeigt.



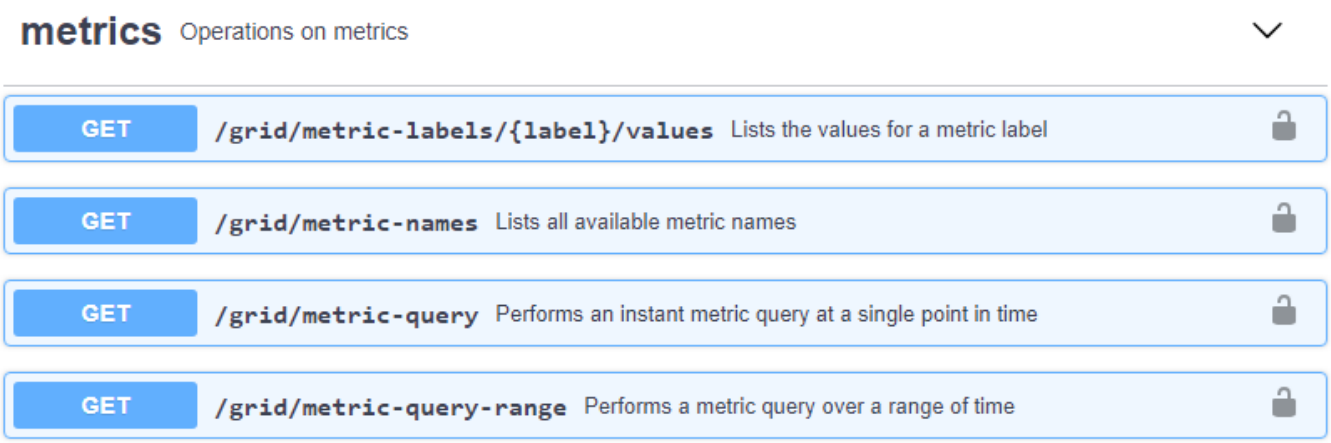
Erstellen benutzerdefinierter Überwachungsanwendungen

Mithilfe der StorageGRID-Kennzahlen der Grid-Management-API können Sie benutzerdefinierte Monitoring-Applikationen und Dashboards erstellen.

Wenn Sie Kennzahlen 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.

Über ein externes Monitoring-Tool wie Grafana können Sie auch direkt auf die Prometheus Metriken zugreifen. Zur Verwendung eines externen Tools müssen Sie ein Administrator-Clientzertifikat hochladen oder erstellen, damit StorageGRID das Tool für die Sicherheit authentifizieren kann. Siehe "Anweisungen für die Administration von StorageGRID".

Informationen zu den Kennzahlen-API-Vorgängen, einschließlich der vollständigen Liste der verfügbaren Metriken, finden Sie im Grid Manager. Wählen Sie oben auf der Seite das Hilfesymbol aus und wählen Sie **API-Dokumentation** > **metrics**.



Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung liegen über dem Umfang dieser Dokumentation hinaus.

Fehlerbehebung für das StorageGRID-System

Fehler in einem StorageGRID System beheben

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

Häufig können Sie Probleme selbst lösen. Unter Umständen müssen Sie jedoch einige Probleme an den technischen Support eskalieren.

Definieren Sie das Problem

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

Diese Tabelle enthält Beispiele für die Arten von Informationen, die Sie erfassen können, um ein Problem zu definieren:

Frage	Beispielantwort
Was macht das StorageGRID-System? Was sind die Symptome?	Client-Applikationen berichten, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann hat das Problem begonnen?	Die Objektaufnahme wurde am 8. Januar 2020 um 14:50 Uhr verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Durch Client-Anwendung benachrichtigt. Auch Benachrichtigung per E-Mail erhalten.
Tritt das Problem konsequent oder nur in manchen Fällen auf?	Das Problem ist noch nicht behoben.

Frage	Beispielantwort
Wenn das Problem regelmäßig auftritt, welche Schritte dazu führen, dass es auftritt	Das Problem tritt jedes Mal auf, wenn ein Client versucht, ein Objekt aufzunehmen.
Wenn das Problem zeitweise auftritt, wann tritt es auf? Notieren Sie die Zeiten der einzelnen Vorfälle, die Sie kennen.	Das Problem ist nicht intermittierend.
Haben Sie dieses Problem schon einmal gesehen? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dies ist das erste Mal, dass ich dieses Thema gesehen habe.

Bewerten Sie das Risiko und die Auswirkungen auf das System

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

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

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

Datenerfassung

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

Art der zu erfassenden Daten	Warum diese Daten sammeln	Anweisungen
Zeitplan der neuesten Änderungen erstellen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Erstellen Sie eine Zeitleiste der neuesten Änderungen

Art der zu erfassenden Daten	Warum diese Daten sammeln	Anweisungen
Prüfen von Warnmeldungen	Mithilfe von Warnmeldungen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise zu den zugrunde liegenden Problemen geben, die das Problem verursachen könnten. Prüfen Sie die Liste der aktuellen Meldungen, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat. Prüfen Sie in der Vergangenheit ausgelöste Warnmeldungen, um zusätzliche Informationen zu erhalten.	• "Anzeige aktueller und aufgelöster Warnmeldungen"
Basispläne erstellen	Sammeln von Informationen über die normalen Stufen verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Grundlinien können wertvolle Hinweise liefern.	• Basispläne erstellen
Durchführen von Einspeisung und Abruf von Tests	Zur Fehlerbehebung von Performance-Problemen bei Aufnahme und Abruf können Objekte auf einer Workstation gespeichert und abgerufen werden. Vergleichen Sie die Ergebnisse mit denen, die bei der Verwendung der Client-Anwendung angezeigt werden.	• "PUT- und GET-Performance werden überwacht"
Audit-Meldungen prüfen	Überprüfen Sie Audit-Meldungen, um StorageGRID Vorgänge im Detail zu befolgen. Die Details in Audit-Meldungen können bei der Behebung vieler Arten von Problemen, einschließlich von Performance-Problemen, nützlich sein.	• "Audit-Meldungen prüfen"
Überprüfen Sie Objektstandorte und Storage-Integrität	Wenn Sie Speicherprobleme haben, stellen Sie sicher, dass Objekte an der gewünschten Stelle platziert werden. Überprüfen Sie die Integrität von Objektdaten auf einem Storage-Node.	• "Überwachen von Objektverifizierungsvorgängen" • "Bestätigen Sie den Speicherort der Objektdaten" • "Überprüfen Sie die Objektintegrität"

Art der zu erfassenden Daten	Warum diese Daten sammeln	Anweisungen
Datenerfassung für technischen Support	Vom technischen Support werden Sie möglicherweise aufgefordert, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um Probleme zu beheben.	• "Erfassen von Protokolldateien und Systemdaten" • "Starten Sie manuell ein AutoSupport-Paket" • "Prüfen von Support-Kennzahlen"

Erstellen Sie eine Zeitleiste der neuesten Änderungen

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

- Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.
- Durch eine Zeitleiste von Änderungen können Sie feststellen, welche Änderungen für ein Problem verantwortlich sein könnten und wie jede Änderung ihre Entwicklung beeinflusst haben könnte.

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

Zeit der Änderung	Art der Änderung	Details
Beispiel: • Wann haben Sie die Node-Wiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Prozess unterbrochen?	Was ist los? Was haben Sie gemacht?	Dokumentieren Sie alle relevanten Details zu der Änderung. Beispiel: • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Änderungen bei Client-Workloads Achten Sie darauf, zu beachten, ob mehrere Änderungen gleichzeitig durchgeführt wurden. Wurde diese Änderung beispielsweise vorgenommen, während ein Upgrade durchgeführt wurde?

Beispiele für signifikante aktuelle Änderungen

Hier einige Beispiele für potenziell signifikante Änderungen:

- Wurde das StorageGRID System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde kürzlich ein Upgrade des Systems durchgeführt? Wurde ein Hotfix angewendet?
- Wurde irgendeine Hardware in letzter Zeit repariert oder geändert?
- Wurde die ILM-Richtlinie aktualisiert?

- Hat sich der Client-Workload geändert?
- Hat sich die Client-Applikation oder deren Verhalten geändert?
- Haben Sie den Lastausgleich geändert oder eine Hochverfügbarkeitsgruppe aus Admin-Nodes oder Gateway-Nodes hinzugefügt oder entfernt?
- Wurden Aufgaben gestartet, die ein sehr langer Zeitaufwand beanspruchen können? Beispiele:
  - Wiederherstellung eines fehlerhaften Speicherknotens
  - Ausmusterung von Storage-Nodes
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, beispielsweise beim Hinzufügen eines Mandanten oder bei der Änderung der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattform-Services kürzlich aktiviert oder geändert?
- Wurde die Compliance in letzter Zeit aktiviert?
- Wurden Cloud-Storage-Pools hinzugefügt oder entfernt?
- Wurden Änderungen an der Storage-Komprimierung oder -Verschlüsselung vorgenommen?
- Wurden Änderungen an der Netzwerkinfrastruktur vorgenommen? Beispiel: VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?
- Wurden weitere Änderungen am StorageGRID System bzw. an der zugehörigen Umgebung vorgenommen?

Basispläne erstellen

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

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

Eigenschaft	Wert	Wie zu erhalten
Durchschnittlicher Metadatenkverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm „verwendete Speicher - Objektmetadaten“ einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Metadaten-Storage täglich belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Rate der S3-Operationen	Vorgänge/Sekunde	Wählen Sie im Grid Manager-Dashboard **Leistung** > **S3-Vorgänge für Speicherknoten**. Um die Aufnahme- und 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 S3-Aufnahme- und Abrufdiagramm.
ILM-Auswertungsrate	Objekte/Sekunde	Wählen Sie auf der Seite Knoten ***GRID*** > **ILM** aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für **Bewertungsrate** für Ihr System zu schätzen.
ILM-Scan-Rate	Objekte/Sekunde	Wählen Sie **Knoten** > ***grid*** > **ILM**. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für **Scan-Rate** für Ihr System abzuschätzen.
Objekte, die sich aus Client-Vorgängen in Warteschlange befinden	Objekte/Sekunde	Wählen Sie **Knoten** > ***grid*** > **ILM**. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basislinienwert für **Objekte in der Warteschlange (von Client-Operationen)** für Ihr System abzuschätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte**. Zeigen Sie in der Abfragetabelle den Wert für die durchschnittliche Latenz an.

Analysieren von Daten

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

Die Analyse ist Problem-abhängig, aber im Allgemeinen:

- Ermitteln Sie mithilfe der Warnmeldungen Points of Failure und Engpässe.
- Rekonstruieren Sie den Problemverlauf mithilfe des Alarmverlaufs und der Diagramme.
- Verwenden Sie Diagramme, um Anomalien zu finden und die Problemsituation mit dem normalen Betrieb zu vergleichen.

Checkliste für Eskalationsinformationen

Wenn Sie das Problem nicht alleine lösen können, wenden Sie sich an den technischen Support. Bevor Sie sich an den technischen Support wenden, müssen Sie die in der folgenden Tabelle aufgeführten Informationen zur Erleichterung der Problembehebung nutzen.

✓	Element	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann hat das Problem begonnen? Passiert es konsequent oder intermittierend? Welche Zeiten hat es gelegentlich gegeben? Definieren Sie das Problem
	Folgenabschätzung	Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation? • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	Wählen Sie **Wartung** > **System** > **Lizenz**. Die StorageGRID -System-ID wird als Teil der aktuellen Lizenz angezeigt.
	Softwareversion	Wählen Sie oben im Grid Manager das Hilfesymbol aus, und wählen Sie **über**, um die StorageGRID-Version anzuzeigen.
	Anpassbarkeit	Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf: • Verwendet das Grid Storage-Komprimierung, Storage-Verschlüsselung oder Compliance? • Werden replizierte oder Erasure-Coded-Objekte von ILM erstellt? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das ausgewogene, strikte oder duale Commit-Aufnahmverhalten?

✔	Element	Hinweise
	Log-Dateien und Systemdaten	Sammeln Sie Protokolldateien und Systemdaten für Ihr System. Wählen Sie **Support** > **Tools** > **Protokollsammlung**. Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes 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 an einem Standort installierten Speicherknoten umfassen den ADC-Dienst.
	Basisinformationen	Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch Basispläne erstellen
	Zeitachse der letzten Änderungen	Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind. Erstellen Sie eine Zeitleiste der neuesten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie Schritte zur Diagnose oder Behebung des Problems selbst ergriffen haben, achten Sie darauf, die Schritte und das Ergebnis zu notieren.

Behebung von Objekt- und Storage-Problemen

Bestätigen Sie den Speicherort der Objektdaten

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

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **ILM** > **Object Metadata Lookup**.

2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

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

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

4. Wählen Sie **Look Up**.

   Die "Ergebnisse der Suche nach Objektmetadaten" wird angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

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

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


Fehler beim Objektspeicher (Storage Volume)

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

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

Disk devices

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

Volumes

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

Object stores

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

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

Überprüfen Sie die Objektintegrität

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

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

Was ist Hintergrundüberprüfung?

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

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

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

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

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

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

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

Warnmeldungen zur Hintergrundüberprüfung

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

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

Was ist Objektexistenz-Prüfung?

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

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

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

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

Überprüfung der ObjektExistenz ausführen

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".
- Sie haben sichergestellt, dass die Speicherknoten, die Sie überprüfen möchten, online sind. Wählen Sie **Knoten** aus, um die Knotentabelle anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen der Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden Verfahren auf den Knoten, die Sie überprüfen möchten, **nicht** ausgeführt werden:
  - Grid-Erweiterung, um einen Storage-Node hinzuzufügen
  - Deaktivierung des Storage Node

- Recovery eines ausgefallenen Storage-Volumes
- Wiederherstellung eines Speicherknoten mit einem ausgefallenen Systemlaufwerk
- EC-Ausgleich
- Appliance-Node-Klon

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

Über diese Aufgabe

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

Schritte

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

   Sie können nach Node-Namen oder Site suchen.

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

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

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

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

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

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

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

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

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

   - Der Job ist abgeschlossen.

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

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

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

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

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

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

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

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

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

    a. Wählen Sie **Wartung** > **Objektexistenzprüfung** > **Auftragsverlauf**.
    b. Legen Sie fest, welche Jobs für die erneute Ausführung bereit sind:
        i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.
        ii. Überprüfen Sie für diese Jobs die Spalte Consistency Control auf Strong-site oder strong-global.

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

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

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

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

Fehlerbehebung bei S3 PUT Objektgröße zu groß Warnung

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

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

Schritte

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

   a. Eingabe `ssh admin@primary_Admin_Node_IP`

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

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

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

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

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

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

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

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

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

Weitere Informationen finden Sie unter"Protokollspeicherort auswählen" .

f. Ermitteln Sie, welche Mandanten Objekte mit einer Größe von mehr als 5 gib verwenden.

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

ii. Überprüfen Sie für jede Überwachungsmeldung in den Ergebnissen das Feld unter `S3AI`, um die Konto-ID des Mandanten zu ermitteln. Verwenden Sie die anderen Felder in der Meldung, um zu bestimmen, welche IP-Adresse vom Client, vom Bucket und vom Objekt verwendet wurde:

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

Beispiel für Ergebnisse des Audit-Protokolls

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Wenn die Schreibvorgänge des Clients nicht normal sind, verwenden Sie die Mandanten-ID in der Warnmeldung, um den Mandanten zu identifizieren:

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

Informationen finden Sie unter "Erfassen von Protokolldateien und Systemdaten" .

b. Extrahieren Sie die Datei und gehen Sie zu `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 im `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 Mandanten, dass die maximale PutObject-Größe 5 gib beträgt, und verwenden Sie mehrteilige Uploads für Objekte, die größer als 5 gib sind.
5. Ignorieren Sie die Warnmeldung für eine Woche, wenn die Anwendung geändert wurde.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

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

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

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

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

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

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

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

Untersuchen Sie möglicherweise verlorene Objekte

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

Schritte

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

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

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

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

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

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

Weitere Informationen finden Sie unter"Protokollspeicherort auswählen" .

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

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

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

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

a. Wählen Sie **ILM** > **Object Metadata Lookup**.

b. Geben Sie die UUID ein, und wählen Sie **Look Up**.

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

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

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

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

Beheben Sie die Warnung „Niedrig Object Data Storage“

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

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

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

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

In diesem Zustand:

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

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

Schritte

1. Wählen Sie **Warnungen** > **Aktuell**.

   Die Seite „Meldungen“ wird angezeigt.

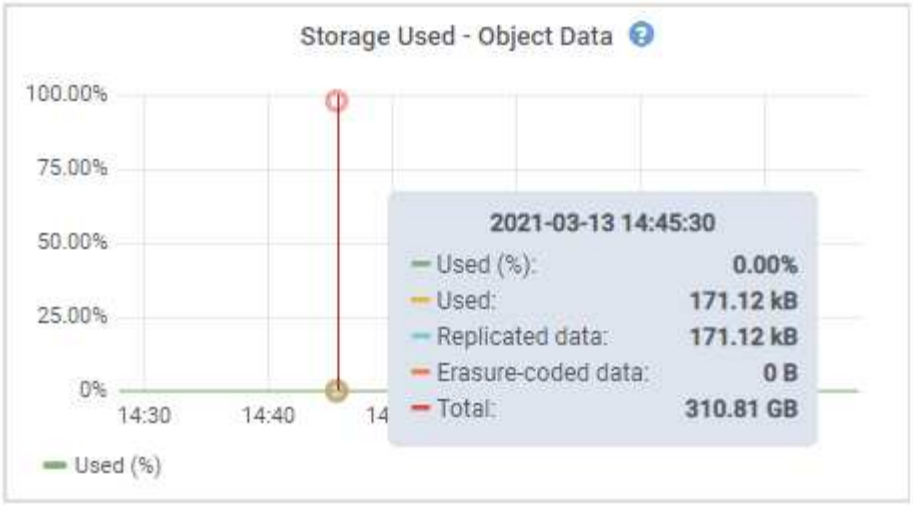
2. Erweitern Sie bei Bedarf aus der Warnmeldungstabelle die Warnungsgruppe **Low Object Data Storage** und wählen Sie die Warnung aus, die angezeigt werden soll.

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

3. Überprüfen Sie die Details im Dialogfeld, und beachten Sie Folgendes:
   - Auslösezeit
   - Der Name des Standorts und des Nodes
   - Die aktuellen Werte der Metriken für diese Meldung
4. Wählen Sie **Knoten** > ***Speicherknoten oder -site*** > **Speicher**.
5. Bewegen Sie den Cursor über die Grafik „verwendeter Speicher – Objektdaten“.

   Die folgenden Werte werden angezeigt:

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



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

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

7. So bald wie möglich, "Ergänzen Sie die Speicherkapazität" in Ihr Raster.

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

   Weitere Informationen finden Sie unter "Management vollständiger Storage-Nodes".

Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff

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

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

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

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

benutzerdefinierter Wert für das Speichervolumen-Softread-only-Wasserzeichen zu klein ist.

Analysieren Sie die Meldung

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

Jede Instanz der Warnmeldung gibt an, dass der benutzerdefinierte Wert des Speichervolumes mit weichem Lesezugriff kleiner ist als der minimale optimierte Wert für diesen Speicher-Node. Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Speicherknoten möglicherweise kritisch wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergehen kann. Einige Speicher-Volumes sind möglicherweise nicht mehr zugänglich (automatisch abgehängt), wenn der Node die Kapazität erreicht.

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

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

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

Beheben Sie die Meldung

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Bewertung der Nutzung von Objektdaten für das gesamte Grid

Schritte

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

Anzeigen optimierter Storage-Wasserzeichen

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

Schritte

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   In der letzten Spalte wird der maximale optimierte Wert des weichen schreibgeschützten Wasserzeichens für alle Speicher-Volumes auf jedem Storage Node angezeigt.

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

Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können

Schritte

1. Wählen Sie **Knoten** aus.

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

   Andernfalls erweitern Sie das Raster so schnell wie möglich. Entweder "Storage-Volumes hinzufügen" zu einem vorhandenen Knoten oder "Neue Storage-Nodes hinzufügen". Gehen Sie dann zu, um die Wasserzeicheneinstellungen zu Verwenden Sie optimierte Wasserzeichenaktualisieren.

4. Wenn Sie weiterhin benutzerdefinierte Werte für die Wasserzeichen des Speichervolumes verwenden müssen, "Stille" oder "Deaktivieren" die Warnung **Low read-only Watermark override**.

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

optimierte Wasserzeichen verwenden

Schritte

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

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

Behebung von Metadatenproblemen

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

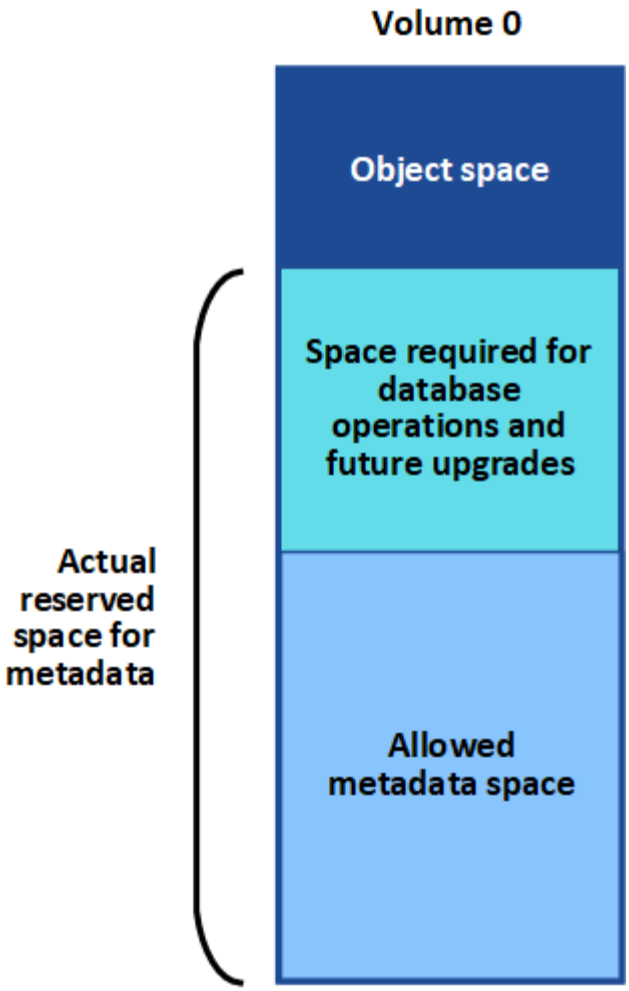
Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

Über diese Aufgabe

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

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



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

Sie können "Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node"Ihnen dabei helfen, Fehler vorherzusehen und zu korrigieren, bevor sie auftreten.

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

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

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

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

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

Schritte

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

Da StorageGRID komplette Kopien aller Objektmetadaten an jedem Standort speichert, wird die Metadaten-Kapazität des gesamten Grid durch die Metadaten-Kapazität des kleinsten Standorts begrenzt. Wenn Sie einem Standort Metadaten-Kapazität hinzufügen müssen, sollten Sie ebenfalls "Erweitern Sie alle anderen Standorte"die gleiche Anzahl von Storage-Nodes verwenden.

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

Fehlerbehebung bei Zertifikatfehlern

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

Über diese Aufgabe

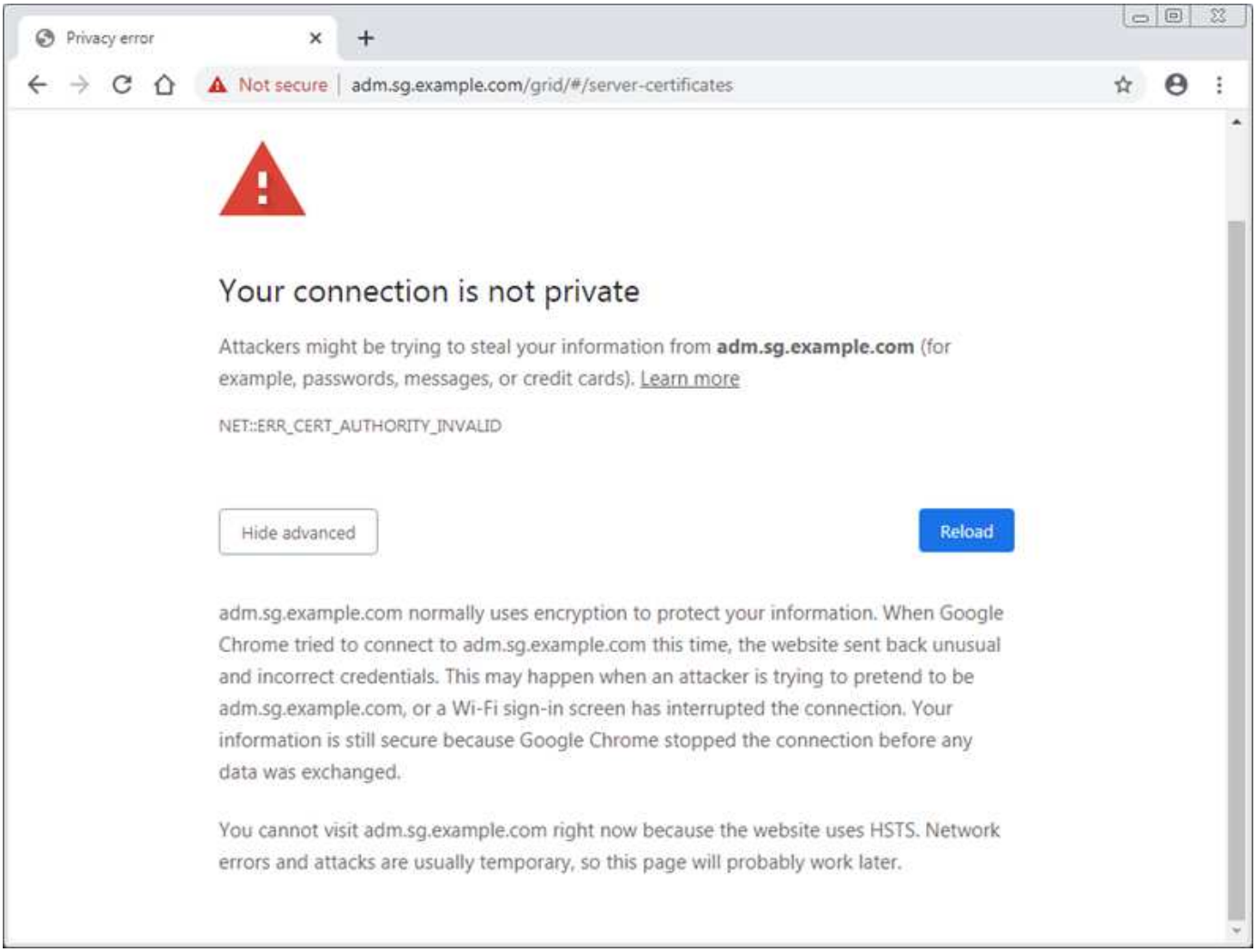
Zertifikatfehler können Probleme verursachen, wenn Sie versuchen, eine Verbindung mit StorageGRID mithilfe des Grid Managers, der Grid Management API, des Mandantenmanagers oder der Mandantenmanagement-API herzustellen. Zertifikatfehler können auch auftreten, wenn Sie versuchen, eine Verbindung mit einem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

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

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

Standardserverzertifikat zurückgesetzt.

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



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

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

Schritte

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

1. Überprüfen Sie die Gültigkeitsdauer des Zertifikats. + einige Webbrowser und S3-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.
2. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein oder generieren Sie ein neues Zertifikat.

- Informationen zu einem Serverzertifikat finden Sie in den Schritten für "Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager".
- Informationen zu einem Clientzertifikat finden Sie in den Schritten für "Konfigurieren eines Client-Zertifikats".

3. Versuchen Sie bei Serverzertifikatfehlern oder beiden der folgenden Optionen:
   - Stellen Sie sicher, dass der Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass das SAN mit der IP-Adresse oder dem Hostnamen des Node übereinstimmt, mit dem Sie eine Verbindung herstellen.
   - Wenn Sie versuchen, eine Verbindung zu StorageGRID mit einem Domain-Namen herzustellen:
     i. Geben Sie die IP-Adresse des Admin-Knotens anstelle des Domain-Namens ein, um den Verbindungsfehler zu umgehen und auf den Grid-Manager zuzugreifen.
     ii. Wählen Sie im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** und dann"Wählen Sie die entsprechende Registerkarte Zertifikat aus" um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
     iii. In den Anweisungen zum Verwalten von StorageGRID finden Sie die Schritte für "Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager".

Fehlerbehebung bei Problemen mit Admin-Node und Benutzeroberfläche

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

Anmeldefehler beim Admin-Node

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

1. Warten Sie 10 Minuten, und melden Sie sich erneut an.

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

2. Wenn Ihr StorageGRID-System über mehr als einen Administratorknoten verfügt, melden Sie sich von einem anderen Administratorknoten beim Grid-Manager an, um den Status eines nicht verfügbaren Administratorknotens zu überprüfen.
   - Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **Knoten**, **Warnungen** und **Support** verwenden, um die Fehlerursache zu ermitteln.
   - Wenn Sie nur einen Admin-Knoten haben oder sich immer noch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Ermitteln, ob die Hardware des Node offline ist
4. Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, lesen Sie die Schritte für"Konfigurieren der Single Sign-On-Funktion" .

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

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

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

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

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

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

7. Anzeigen des Status aller Dienste, die auf dem Grid-Knoten ausgeführt werden: `storagegrid-status`

   Stellen Sie sicher, dass die nms-, mi-, nginx- und Management-API-Services ausgeführt werden.

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

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

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

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

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

10. folgende Protokolle prüfen:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

- `**/*commands.txt`

11. Wenn Sie keine Probleme mit dem Admin-Knoten feststellen konnten, geben Sie einen der folgenden Befehle ein, um die IP-Adressen der drei Speicherknoten zu ermitteln, die den ADC-Dienst an Ihrem Standort ausführen. In der Regel handelt es sich dabei um die ersten drei Storage-Nodes, die am Standort installiert wurden.

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

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

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

12. Melden Sie sich über den Admin-Knoten mit ssh bei jedem der ADC-Speicherknoten an, wobei die von Ihnen angegebenen IP-Adressen verwendet werden.
13. Anzeigen des Status aller Dienste, die auf dem Grid-Knoten ausgeführt werden: `storagegrid-status`

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

14. Wiederholen Sie die Schritte Verwenden Sie Lumberjack, um Protokolle zu sammeln undProtokolle prüfen, um die Protokolle auf den Speicher-Nodes zu überprüfen.
15. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

    Stellen Sie die Protokolle bereit, die Sie für den technischen Support gesammelt haben. Siehe auch "Referenz für Protokolldateien".

Probleme bei der Benutzeroberfläche

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

Schritte

1. Stellen Sie sicher, dass Sie ein verwenden"Unterstützter Webbrowser".
2. Löschen Sie den Cache Ihres Webbrowsers.

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

Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen

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

Fehler „422: Nicht verarbeitbare Entität“

Der Fehler 422: Nicht verarbeitbare Entität kann aus verschiedenen Gründen auftreten. Überprüfen Sie die Fehlermeldung, um festzustellen, welche Ursache Ihr Problem verursacht hat.

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

Fehlermeldung	Ursache und Korrekturmaßnahme

`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 bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option **TLS nicht verwenden** für Transport Layer Security (TLS) auswählen.
	
	Die Verwendung der Option **keine Verwendung von TLS** wird nicht für die Verwendung mit AD-Servern unterstützt, die LDAP-Signatur erzwingen. Sie müssen entweder die Option **STARTTLS verwenden** oder die Option **LDAPS verwenden** für TLS auswählen.

Fehlermeldung	Ursache und Korrekturmaßnahme

`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 Chiffre zu verwenden, um eine TLS-Verbindung (Transport Layer Security) von StorageGRID zu einem externen System herzustellen, das für Identify Federation oder Cloud Storage Pools verwendet wird.
	
	Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eine der für ausgehende TLS-Verbindungen verwenden"Von StorageGRID unterstützte Chiffren", wie in den Anweisungen zur Verwaltung von StorageGRID dargestellt.

Alarm bei MTU-Nichtübereinstimmung im Grid-Netzwerk

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

Über diese Aufgabe

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

Schritte

1. Der externe SSH-Zugriff ist standardmäßig blockiert. Falls erforderlich,"Zugriff vorübergehend erlauben" .
2. Führen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
   - Verwenden Sie die im Grid Manager angegebene Abfrage.
   - Navigieren Sie zur *`primary Admin Node IP address`*`/metrics/graph` folgenden Abfrage, und geben Sie sie ein: `node_network_mtu_bytes{device="eth0"}`
3. "Ändern Sie die MTU-Einstellungen" Falls erforderlich, um sicherzustellen, dass sie für die Grid Network Interface (eth0) auf allen Knoten gleich sind.
   - Verwenden Sie für Linux- und VMware-basierte Nodes den folgenden Befehl: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

     Hinweis: Wenn auf Linux-basierten Knoten der gewünschte MTU-Wert für das Netzwerk im Container den bereits auf der Host-Schnittstelle konfigurierten Wert überschreitet, müssen Sie zuerst die Host-Schnittstelle so konfigurieren, dass der gewünschte MTU-Wert vorhanden ist, und dann mit dem `change-ip.py` Skript den MTU-Wert des Netzwerks im Container ändern.

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

Positionsargumente	Beschreibung
`mtu`	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
`network`	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: • Raster • Admin • Client

+

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

4. Wenn Sie externen SSH-Zugriff zugelassen haben,"Zugriff blockieren" wenn Sie die Aufgabe erledigt haben.

Node-Netzwerk-Frame-Fehlerwarnung

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

Über diese Aufgabe

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

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

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle potenziellen Ursachen dieser Warnung, wenn Sie Ihre Netzwerkkonfiguration beachten.
2. Führen Sie je nach Fehlerursache die folgenden Schritte aus:

FEC stimmt nicht überein

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

a. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID-Gerät angeschlossen ist.

b. Überprüfen Sie die physikalische Integrität der Kabel vom Gerät zum Switch.

c. Wenn Sie die FEC-Einstellungen ändern möchten, um die Warnmeldung zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Verbindungskonfiguration“ des Installationsprogramms für das StorageGRID-Gerät für den Modus „automatisch“ konfiguriert ist (siehe die Anweisungen für Ihr Gerät:

   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 und SG1100"
   - "SG100 und SG1000"

d. Ändern Sie die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

   Sie können die FEC-Einstellungen auf StorageGRID-Geräten nicht konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu erkennen und zu spiegeln, an denen sie angeschlossen sind. Wenn die Verbindungen zu 25-GbE- oder 100-GbE-Netzwerkgeschwindigkeiten gezwungen sind, können Switch und NIC eine gemeinsame FEC-Einstellung nicht aushandeln. Ohne eine gemeinsame FEC-Einstellung wird das Netzwerk in den Modus „kein FEC“ zurückfallen. Wenn FEC nicht aktiviert ist, sind die Anschlüsse anfälliger für Fehler, die durch elektrische Geräusche verursacht werden.

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

Switch-Port und MTU-NIC stimmen nicht überein

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

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

Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen gleich sein. Weitere Informationen finden Sie unter Fehler bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU .

Siehe auch "MTU-Einstellung ändern".

Hohe Link-Fehlerraten

a. Aktivieren Sie FEC, falls nicht bereits aktiviert.
b. Stellen Sie sicher, dass Ihre Netzwerkkabel von guter Qualität sind und nicht beschädigt oder nicht ordnungsgemäß angeschlossen sind.
c. Wenn die Kabel nicht das Problem darstellen, wenden Sie sich an den technischen Support.

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

NIC-Klingelpuffer überlaufen

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

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

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

Fehler bei der Zeitsynchronisierung

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

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

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

Linux: Probleme mit der Netzwerkverbindung

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

Klonen VON MAC Adressen

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

> ⓘ Erstellen Sie separate virtuelle Netzwerkschnittstellen, die vom Linux Host-Betriebssystem verwendet werden können. Die Verwendung derselben Netzwerkschnittstellen für das Linux-Hostbetriebssystem und den StorageGRID-Container kann dazu führen, dass das Host-Betriebssystem nicht mehr erreichbar ist, wenn der promiskuious-Modus auf dem Hypervisor nicht aktiviert wurde.

Weitere Informationen finden Sie in der Anleitung für"Aktivieren des MAC-Klonens" .

Promiskuous Modus

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

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

Linux: Knotenstatus ist „verwaist“

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

Über diese Aufgabe

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

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

Schritte

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

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

Wenn der Node verwaiste ist, wird die Antwort angezeigt

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

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

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

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

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

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

Linux: Fehlerbehebung bei der IPv6-Unterstützung

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

Über diese Aufgabe

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

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

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

Schritte

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

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

Das Ergebnis sollte 0 sein.

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

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

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

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

Das Ergebnis sollte 1 sein.

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

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

5. Verlassen Sie den Container: `exit`

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

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

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

7. Suchen Sie die folgenden beiden Zeilen, und entfernen Sie die Kommentar-Tags. Speichern und schließen Sie anschließend die Datei.

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

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

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

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

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

Fehlerbehebung für einen externen Syslog-Server

In der folgenden Tabelle werden die Fehlermeldungen beschrieben, die möglicherweise mit einem externen Syslog-Server in Zusammenhang stehen, und Korrekturmaßnahmen werden aufgelistet.

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

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

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

- "Überlegungen zur Verwendung eines externen Syslog-Servers"
- "Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server"

Fehlermeldung	Beschreibung und empfohlene Aktionen
Hostname kann nicht aufgelöst werden	Der 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 der Schreibweise W.X.Y.Z („gepunktete Dezimalzahl“) handelt. 2. Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind. 3. Vergewissern Sie sich, dass jeder Knoten auf die IP-Adressen des DNS-Servers zugreifen kann.
Verbindung abgelehnt	Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde abgelehnt. Möglicherweise ist auf dem TCP- oder TLS-Port für den Host kein Service verfügbar, oder eine Firewall blockiert möglicherweise den Zugriff. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 2. Vergewissern Sie sich, dass der Host für den syslog-Service einen Syslog-Daemon ausführt, der auf dem angegebenen Port abhört. 3. Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten auf die IP und den Port des Syslog-Servers blockiert.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Netzwerk nicht erreichbar	Der Syslog-Server befindet sich nicht in einem direkt verbundenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass die Testmeldungen von den aufgeführten Knoten nicht an den Syslog-Server weitergeleitet werden konnten. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Node die Liste des Grid-Netzwerksubnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese konfiguriert sind, um Datenverkehr zum Syslog-Server über die erwartete Netzwerkschnittstelle und das erwartete Gateway (Grid, Administrator oder Client) zu leiten.
Host nicht erreichbar	Der Syslog-Server befindet sich in einem direkt verbundenen Subnetz (Subnetz, das von den aufgeführten Knoten für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Knoten versuchten, Testmeldungen zu senden, erhielten aber keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers. 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie, ob der Host, auf dem der Syslog-Service ausgeführt wird, ausgeführt wird.
Zeitüberschreitung bei Verbindung	Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber für lange Zeit wurde vom Syslog-Server keine Antwort empfangen. Möglicherweise gibt es eine Fehlkonfiguration bei Routing oder eine Firewall könnte den Datenverkehr ohne jede Antwort löschen (eine häufige Konfiguration). 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Node die Liste des Grid-Netzwerksubnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese so konfiguriert sind, dass der Datenverkehr mithilfe der Netzwerkschnittstelle und des Gateways (Grid, Admin oder Client), über die Sie den Syslog-Server erreichen möchten, an den Syslog-Server weitergeleitet wird. 3. Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten blockiert, die in der IP und dem Port des Syslog-Servers aufgeführt sind.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Verbindung vom Partner geschlossen	Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, wurde aber später geschlossen. Gründe hierfür sind u. a.: • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gestartet. • Der Node und der Syslog-Server verfügen möglicherweise über unterschiedliche TCP/TLS-Einstellungen. • Bei einer Zwischenfirewall werden möglicherweise inaktive TCP-Verbindungen geschlossen. • Ein nicht-Syslog-Server, der auf dem Syslog-Server-Port hört, hat die Verbindung möglicherweise geschlossen. So lösen 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, vergewissern Sie sich, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 3. Überprüfen Sie, ob eine Zwischenfirewall nicht für das Schließen inaktiver TCP-Verbindungen konfiguriert ist.
Fehler beim TLS-Zertifikat	Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen angegebenen CA-Zertifikatspaket und dem von Ihnen angegebenen Clientzertifikat kompatibel. 1. Vergewissern Sie sich, dass das CA-Zertifikatbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat auf dem Syslog-Server kompatibel sind. 2. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Weiterleitung angehalten	Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet, und StorageGRID kann den Grund nicht erkennen. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln.

Fehlermeldung	Beschreibung und empfohlene Aktionen
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 Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln. 2. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 3. Wenn Sie TLS verwenden, vergewissern Sie sich, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, vergewissern Sie sich, dass der Syslog-Server auch TCP verwendet. 4. Vergewissern Sie sich, dass das CA-Zertifikatbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat vom Syslog-Server kompatibel sind. 5. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Abfrage der Ergebnisse fehlgeschlagen	Der für die Konfiguration und Tests des Syslog-Servers verwendete Admin-Node kann die Testergebnisse nicht von den aufgeführten Nodes anfordern. Mindestens ein Node ist ausgefallen. 1. Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Services ausgeführt werden. 2. Starten Sie den falsch-Dienst auf den aufgeführten Knoten neu.

Fehlerbehebung beim Load Balancer-Caching

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

Ermitteln, ob eine Anfrage ein Cache-Treffer war

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

Niedrige Cache-Trefferquote

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

Geringe Leistung

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

Prüfung von Audit-Protokollen

Audit-Meldungen und -Protokolle

Diese Anweisungen enthalten Informationen zur Struktur und zum Inhalt der StorageGRID-Prüfmeldungen und Prüfprotokolle. Sie können diese Informationen zum Lesen und Analysieren des Prüfprotokolls der Systemaktivität verwenden.

Diese Anweisungen richten sich an Administratoren, die für die Erstellung von Berichten zu Systemaktivitäten und -Nutzung verantwortlich sind, für die eine Analyse der Audit-Meldungen des StorageGRID Systems erforderlich ist.

Um die Text-Log-Datei verwenden zu können, müssen Sie auf die konfigurierte Revisionsfreigabe im Admin-Knoten zugreifen können.

Informationen zum Konfigurieren von Überwachungsmeldungsebenen und zur Verwendung eines externen Syslog-Servers finden Sie unter"Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server" .

Meldungsfluss und -Aufbewahrung von Audits

Alle StorageGRID-Services generieren während des normalen Systembetriebs Audit-Meldungen. Sie sollten verstehen, wie diese Meldungen über das StorageGRID-System in die Datei verschoben `audit.log` werden.

Die folgenden Workflows für Audit-Nachrichten und die Aufbewahrung von Audit-Nachrichten sind nur anwendbar, wenn StorageGRID für **Admin-Knoten/lokale Knoten** oder **Admin-Knoten und externen Syslog-Server** konfiguriert ist. Wenn StorageGRID für "Nur lokale Knoten" (Standard) oder "Externer Syslog-Server" konfiguriert ist, werden die Audit-Meldungen lokal auf jedem Knoten im `/var/local/log/localaudit.log` Datei und kann nicht von Admin-Knoten oder Speicherknoten verarbeitet werden.

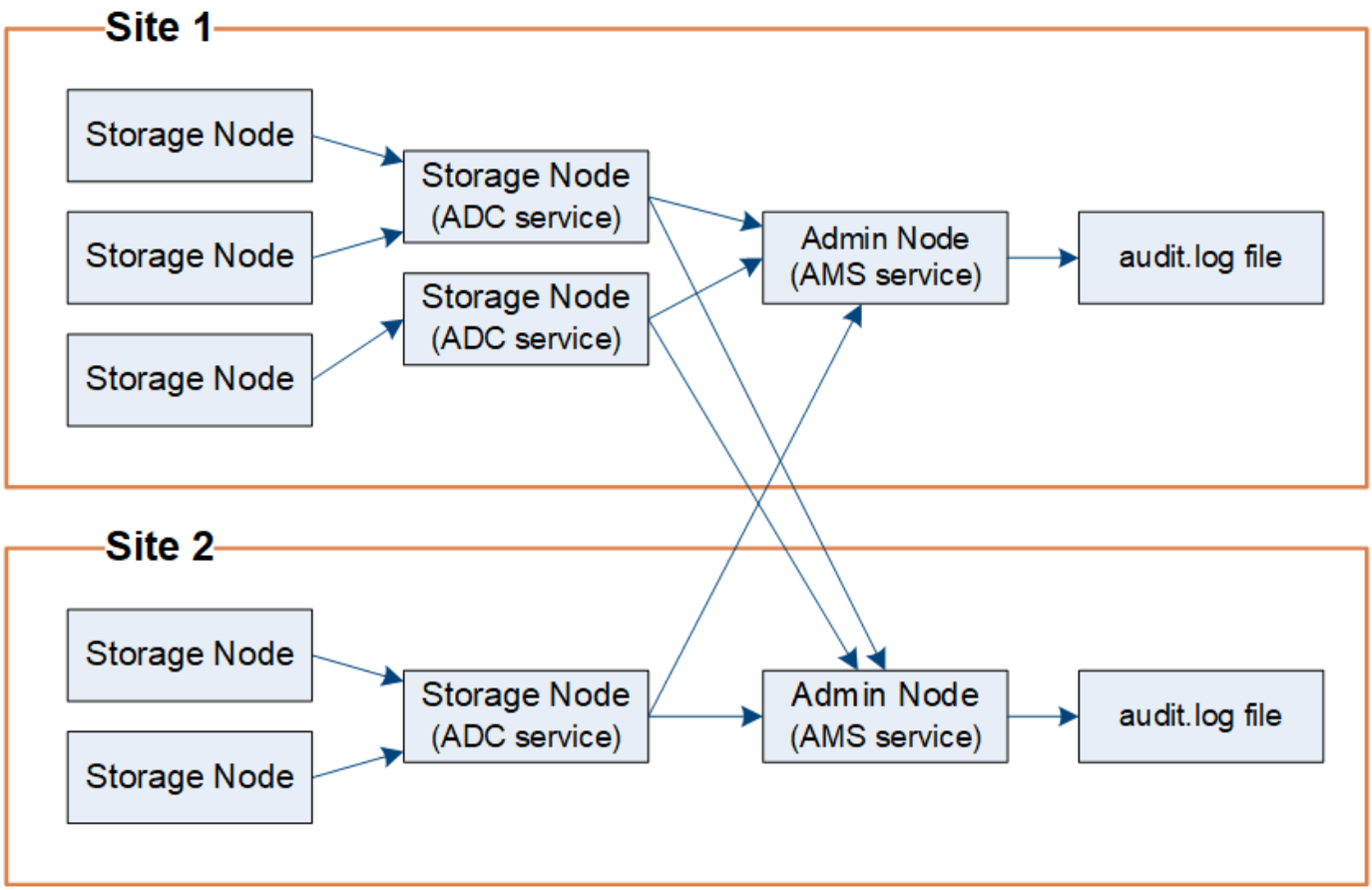
Audit-Nachrichtenfluss

Audit-Nachrichten werden von Admin-Knoten verarbeitet, wenn StorageGRID für **Admin-Knoten/lokale Knoten** oder **Admin-Knoten und externen Syslog-Server** konfiguriert ist, und von den Storage-Knoten, die über einen Administrative Domain Controller (ADC)-Dienst verfügen.

Wie im Überwachungsmeldung-Flow-Diagramm dargestellt, sendet jeder StorageGRID Node seine Audit-Meldungen an einen der ADC-Services am Datacenter-Standort. Der ADC-Dienst wird automatisch für die ersten drei Speicherknoten aktiviert, die an jedem Standort installiert sind.

Jeder ADC-Dienst fungiert wiederum als Relais und sendet seine Sammlung von Audit-Meldungen an jeden Admin-Knoten im StorageGRID-System, wodurch jeder Admin-Knoten einen vollständigen Datensatz der Systemaktivität erhält.

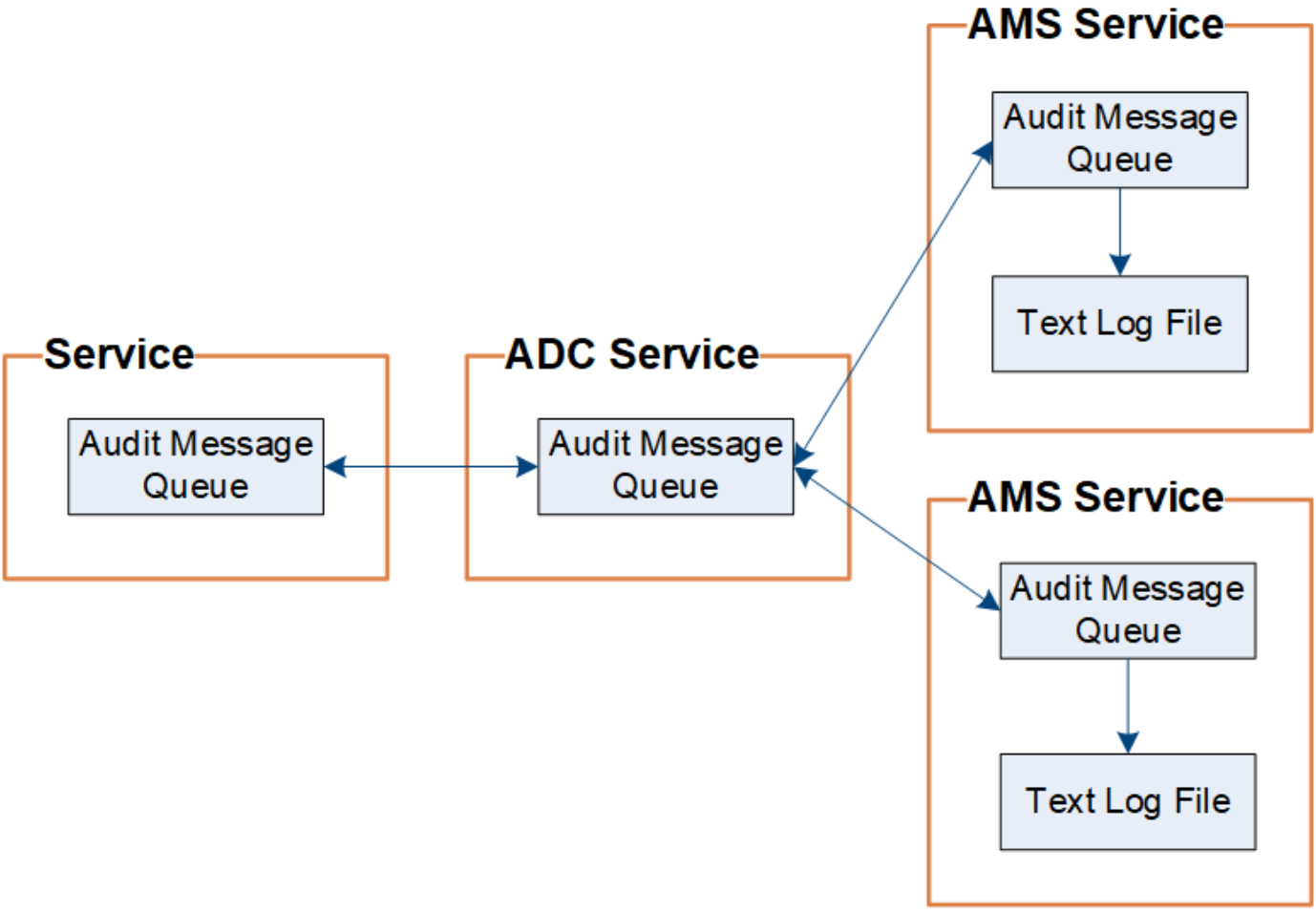
Jeder Admin-Knoten speichert Überwachungsmeldungen in Textprotokolldateien; die aktive Protokolldatei wird mit dem Namen `audit.log`.



Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschprozess, um sicherzustellen, dass keine Audit-Meldungen verloren gehen, bevor sie in das Audit-Protokoll geschrieben werden.

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/audit/export` 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.

Sie können insbesondere folgende Verhaltensweisen erkennen:

- Wenn die `/var/local/audit/export` 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 die Überwachung von Nachrichten 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 verfügbaren Storage-Nodes mit dem ADC-Dienst vorhanden sind, speichern die Storage-Nodes die Überwachungsmeldungen lokal in der `/var/local/log/localaudit.log` Datei.

- Wenn die `/var/local/` Das von einem Speicherknoten verwendete Verzeichnis ist zu 85 % gefüllt. Der Knoten beginnt, 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 Speicherknoten mit dem ADC-Dienst. Wenn einer der Systemknoten ausgefallen ist, werden die übrigen Knoten möglicherweise rückgemeldet.
- Eine nachhaltige Aktivitätsrate, die die Audit-Kapazität des Systems übersteigt.
- Der `/var/local/` Speicherplatz auf einem ADC-Speicherknoten wird aus Gründen voll, die nicht mit Überwachungsmeldungen in Verbindung stehen. In diesem Fall hört der Knoten auf, neue Überwachungsmeldungen zu akzeptieren und priorisiert seinen aktuellen Rückstand, was zu Backlogs auf anderen Knoten führen kann.

Großer Alarm für Überwachungswarteschlangen und Überwachungsmeldungen in Queued (AMQS)

Um Ihnen dabei zu helfen, die Größe der Überwachungsmeldungswarteschlangen im Laufe der Zeit zu überwachen, werden die Warnung **große Prüfwarteschlange** und der ältere AMQS-Alarm ausgelöst, wenn die Anzahl der Nachrichten in einer Speicherknotenwarteschlange oder Admin-Knoten-Warteschlange bestimmte Schwellenwerte erreicht.

Wenn der Alarm * Large Audit queue* oder der alte AMQS-Alarm ausgelöst wird, prüfen Sie zunächst die Auslastung des Systems – wenn eine beträchtliche Anzahl aktueller Transaktionen vorliegt, sollten sich die Warnung und der Alarm im Laufe der Zeit lösen 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 Sie die Protokollverwaltung und den externen Syslog-Server" .

Duplizieren von Nachrichten

Bei einem Netzwerk- oder Node-Ausfall ist das StorageGRID System konservativ. Aus diesem Grund können doppelte Nachrichten im Audit-Protokoll vorhanden sein.

Zugriff auf die Audit-Log-Datei

Die Audit-Freigabe enthält die aktive `audit.log` Datei und alle komprimierten Audit-Log-Dateien. Sie können über die Befehlszeile des Admin-Knotens direkt auf Audit-Log-Dateien zugreifen.

Der `audit.log` Die Datei bleibt leer, es sei denn, Sie konfigurieren StorageGRID für **Admin-Knoten/lokale Knoten** oder **Admin-Knoten und externen Syslog-Server**. Weitere Informationen finden Sie unter "Protokollspeicherort auswählen" .

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie müssen über die `Passwords.txt` Datei verfügen.
- 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 in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

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

2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:

   ```
   cd /var/local/audit/export/
   ```

3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

Drehung der Audit-Log-Dateien

Wenn StorageGRID für **Admin-Knoten/lokale Knoten** oder **Admin-Knoten und externen Syslog-Server** konfiguriert ist, werden die Audit-Protokolldateien auf dem Admin-Knoten gespeichert. `/var/local/audit/export/` 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 mit Prüfdatensätzen erstellt und gespeichert. Weitere Informationen finden Sie unter "Konfigurieren von Audit-Meldungen und externem Syslog-Server" .

Einmal täglich wird die aktive `audit.log` Datei gespeichert und eine neue `audit.log` Datei 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 Audit-Protokoll erstellt wird, verwenden die Dateinamen das Datum, an dem die Datei mit einer Zahl angehängt wurde, im Format *`yyyy-mm-dd.txt.n`*. Beispiel: `2018-04-15.txt` Und `2018-04-15.txt.1` sind die ersten und zweiten Protokolldateien, 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. Mit der Zeit wird der für Prüfprotokolle zugewiesene Admin-Knotenspeicher verbraucht. Ein Skript überwacht den Speicherplatzverbrauch des Audit-Protokolls und löscht Protokolldateien nach Bedarf, um Speicherplatz im `/var/local/audit/export/` Verzeichnis. Prüfprotokolle werden basierend auf dem Datum gelöscht, an dem sie erstellt wurden. Die ältesten Protokolle werden zuerst gelöscht. 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 des Vortages (`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
```

Format der Auditprotokolldatei

Format der Auditprotokolldatei

Die Audit-Log-Dateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Nachrichten.

Jede Überwachungsmeldung enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Meldung (ATIM) im ISO 8601-Format auslöste, gefolgt von einem Leerzeichen:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, Wo *UUUUUU* sind Mikrosekunden.

- Die Audit-Nachricht selbst, eingeschlossen in eckigen Klammern und beginnend mit `AUDT`.

Das folgende Beispiel zeigt drei Audit-Nachrichten in einer Audit-Log-Datei (Zeilenumbrüche zur Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, wenn ein Mandant einen S3-Bucket erstellt und diesem Bucket zwei Objekte hinzugefügt hat.

```
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):8439606722108456022]]

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 Überwachungsmeldungen in den Audit-Log-Dateien nicht einfach zu lesen oder zu interpretieren. Mit dem können Sie vereinfachte Zusammenfassungen der "Audit-Explain-Tool"Überwachungsmeldungen im Überwachungsprotokoll abrufen. Mithilfe des können Sie "Audit-Summe-Tool"zusammenfassen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

Verwenden Sie das Audit-Erklären-Tool

Sie können das Tool verwenden `audit-explain`, um die Audit-Meldungen im Audit-

Protokoll in ein leicht lesbares Format zu übersetzen.

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie müssen über die `Passwords.txt` Datei verfügen.
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

Das `audit-explain` Tool, das auf dem primären Admin-Knoten verfügbar ist, bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Audit-Protokoll.

> Das `audit-explain` Tool ist in erster Linie für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitungsabfragen `audit-explain` können eine hohe CPU-Leistung verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-explain` Tools. Diese vier "SPUT" Audit-Meldungen wurden generiert, als der S3-Mandant mit Konto-ID 92484777680322627870 S3-PUT-Anfragen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und drei Objekte zu diesem Bucket 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
```

Das `audit-explain` Tool kann Folgendes tun:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Mehrere Dateien gleichzeitig verarbeiten. Beispiel:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- Eingaben von einer Pipe akzeptieren, wodurch Sie die Eingabe mit dem Befehl oder anderen Mitteln filtern und vorverarbeiten `grep` können. Beispiel:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Da Audit-Protokolle sehr groß und langsam zu analysieren sind, können Sie Zeit sparen, indem Sie Teile filtern, die Sie auf den Teilen betrachten und ausführen möchten `audit-explain`, anstatt der gesamten Datei.

> Das `audit-explain` Tool akzeptiert keine komprimierten Dateien als Piped-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente ein, oder verwenden Sie das `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-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

   Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.
2. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   Das `audit-explain` Tool druckt menschenlesbare Interpretationen aller Meldungen in der angegebenen Datei oder Datei.

   > Um die Linienlänge zu verringern und die Lesbarkeit zu erleichtern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel sehen möchten, verwenden Sie die (`-t`Option timestamp).

Verwenden Sie das Audit-Sum-Tool

Mit dem Tool können `audit-sum` Sie die Audit-Meldungen schreiben, lesen, Kopf und löschen sowie die minimale, maximale und durchschnittliche Zeit (oder Größe) für jeden Operationsart anzeigen.

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben die `Passwords.txt` Datei.
- Sie kennen die IP-Adresse des primären Admin-Knotens.

Über diese Aufgabe

Das `audit-sum` auf dem primären Admin-Knoten verfügbare Tool fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

> Das `audit-sum` Tool ist in erster Linie für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitungsabfragen `audit-sum` können eine hohe CPU-Leistung verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

```
  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- 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 StorageGRID Versionen. Beispiel: "StorageGRID 11.8 Verwenden des Auditsummentools" .

Codieren	Beschreibung	Siehe
IDEL	ILM initiated Delete: Protokolliert, wenn ILM den Prozess des Löschens eines Objekts startet.	"IDEL: ILM gestartet Löschen"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3 LÖSCHEN"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten.	"SGET S3 ABRUFEN"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	"SHEA: S3 KOPF"

Codieren	Beschreibung	Siehe
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen.	"SPUT: S3 PUT"

Das `audit-sum` Tool kann Folgendes tun:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- Eingaben von einer Pipe akzeptieren, wodurch Sie die Eingabe mit dem Befehl oder anderen Mitteln filtern und vorverarbeiten `grep` können. 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
> ```

Mit Befehlszeilenoptionen können Operationen für Buckets separat von Operationen für Objekte zusammengefasst oder Nachrichtenübersichten nach Bucket-Namen, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden in den Zusammenfassungen die minimale, maximale und durchschnittliche Betriebsdauer angezeigt, Sie können jedoch die Option verwenden, um die `size (-s)` Objektgröße zu überprüfen.

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-sum -h
```

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

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

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

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

2. Wenn Sie alle Nachrichten analysieren möchten, die mit Schreibvorgängen, Lese-, Kopf- und Löschvorgängen zusammenhängen, führen Sie die folgenden Schritte aus:

   a. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

      ```
        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 (S3 GET) Vorgänge im Durchschnitt mit 1.13 Sekunden die langsamsten. SGET und SPUT (S3 PUT) Vorgänge weisen jedoch lange Schlimmstfallszeiten von etwa 1,770 Sekunden auf.

   b. Um die langsamsten 10 Abruffunktionen anzuzeigen, verwenden Sie den grep-Befehl, um nur SGET-Nachrichten auszuwählen und die Long-Ausgabeoption hinzuzufügen(`-l`, um Objektpfade einzuschließen:

      ```
      grep SGET audit.log | audit-sum -l
      ```

      Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, mit dem Sie das Audit-Protokoll für andere Meldungen zu diesen speziellen Objekten grep erstellen können.

```
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
```

+
Aus diesem Beispielausgang sehen Sie, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von ca. 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe berücksichtigt die langsamen Abrufzeiten im schlimmsten Fall.

3. Wenn Sie festlegen möchten, welche Größe von Objekten in Ihr Raster aufgenommen und aus diesem abgerufen werden soll, 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 deutlich größer. Die Anzahl der SPUT-Meldungen ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hinweist, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufvorgänge gestern langsam waren:

   a. Geben Sie den Befehl im entsprechenden Audit-Protokoll ein und verwenden Sie die Option Group-by-time (`-gt`), gefolgt von dem 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. Sowohl die maximale als auch die durchschnittliche Zeit sind in diesem Zeitraum erheblich höher und steigen nicht allmählich an, wenn die Anzahl zunimmt. Diese Messwerte deuten darauf hin, dass die Kapazität überschritten wurde, möglicherweise im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

b. Um zu bestimmen, welche Größe Objekte wurden abgerufen jede Stunde gestern, fügen Sie die Größe Option (`-s`), um den 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 zeigen, dass einige sehr große Rückrufe auftraten, als der gesamte Abrufverkehr seinen maximalen Wert hatte.

c. Weitere Informationen finden Sie im, "Audit-Explain-Tool"um alle SGET-Vorgänge während der betreffenden Stunde zu überprüfen:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Wenn die Ausgabe des grep-Befehls viele Zeilen enthalten soll, fügen Sie den Befehl hinzu, um den `less` Inhalt der Audit-Log-Datei jeweils eine Seite (ein Bildschirm) anzuzeigen.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen auf Buckets langsamer sind als SPUT-Vorgänge für Objekte:

a. Mit der Option wird gestartet `-go`, bei der Meldungen für Objekt- und Bucket-Vorgänge getrennt gruppiert werden:

```
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 unterschiedliche Leistungseigenschaften haben als SPUT-Operationen für Objekte.

b. Um zu ermitteln, welche Buckets die langsamsten SPUT-Vorgänge haben, verwenden Sie die `-gb` Option, welche Meldungen 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 ermitteln, welche Buckets die größte SPUT-Objektgröße aufweisen, verwenden Sie die `-gb` Optionen und `-s`:

```
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
```

Überwachungsmeldungsformat

Überwachungsmeldungsformat

Im StorageGRID-System ausgetauschte Audit-Meldungen enthalten Standardinformationen, die für alle Meldungen und spezifische Inhalte zur Beschreibung des Ereignisses oder der Aktivität üblich sind.

Wenn die zusammenfassenden Informationen, die von den und"Audit-Summe"-Tools bereitgestellt "Audit-Erklärung"werden, nicht ausreichen, finden Sie in diesem Abschnitt Informationen zum allgemeinen Format aller Überwachungsmeldungen.

Im Folgenden finden Sie eine Beispielmeldung, wie sie in der Audit-Log-Datei angezeigt werden kann:

```
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 Überwachungsmeldung enthält eine Zeichenfolge von Attributelementen. Der gesamte String ist in Klammern eingeschlossen (`[ ]`), und jedes Attribut-Element im String hat die folgenden Eigenschaften:

- In Klammern eingeschlossen `[ ]`
- Wird durch den String, der eine Audit-Nachricht anzeigt, eingeführt `AUDT`
- Ohne Trennzeichen (keine Kommata oder Leerzeichen) vor oder nach
- Beendet durch Zeilenvorschubzeichen `\n`

Jedes Element umfasst einen Attributcode, einen Datentyp und einen Wert, der in diesem Format angegeben wird:

```
[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 werden in keiner bestimmten Reihenfolge aufgeführt.

In der folgenden Liste werden die Attributelemente beschrieben:

- `ATTR` Ist ein vierstelliger Code für das gemeldete Attribut. Es gibt einige Attribute, die für alle Audit-Meldungen und andere, die ereignisspezifisch sind, gelten.
- `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, in der Regel ein numerischer Wert oder ein Textwert. Werte folgen immer einem Doppelpunkt (`:`). Die Werte des Datentyps CSTR sind von doppelten Anführungszeichen umgeben.

Datentypen

Verschiedene Datentypen werden zur Speicherung von Informationen in Audit-Meldungen verwendet.

Typ	Beschreibung
UI32	Unsigned long integer (32 Bit); es kann die Zahlen 0 bis 4,294,967,295 speichern.
UI64	Unsigned double long integer (64 Bit); es kann die Zahlen 0 bis 18,446,744,073,709,551,615 speichern.
FC32	4-Zeichen-Konstante; ein 32-Bit-Integer-Wert ohne Vorzeichen, der als vier ASCII-Zeichen wie „ABCD“ dargestellt wird.
IPAD	Wird für IP-Adressen verwendet.
CSTR	Ein Array mit variabler Länge von UTF-8 Zeichen. Zeichen können mit den folgenden Konventionen entgangen werden: • Backslash ist \\. • Der Schlittenrücklauf beträgt \r • Doppelte Anführungszeichen sind \". • Zeilenvorschub (neue Zeile) ist \n. • Zeichen können durch ihre hexadezimalen Äquivalente ersetzt werden (im Format \xHH, wobei HH der hexadezimale Wert ist, der das Zeichen darstellt).

Ereignisspezifische Daten

Jede Überwachungsmeldung im Prüfprotokoll zeichnet Daten auf, die für ein

Systemereignis spezifisch sind.

Nach dem öffnenden `[AUDT:` Container, der die Nachricht selbst identifiziert, liefern die nächsten Attribute Informationen über das Ereignis oder die Aktion, die in der Überwachungsmeldung beschrieben wird. Diese Attribute sind im folgenden Beispiel hervorgehoben:

2018-12-05T08:24:45.921845 **\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):„10.224.0 6002562159561246499.100 6002562159561246499“\[SCS3TR\(CSTR\):„6002562159561246499“**\\[SSB7BK\(CS3BK]\[SCSB7BK]:\][SCSB7BK]\[SCSB7BK]\][SCSB7BK]\[SCSB7BK]\[\]\[SCSB7BK]\[SCSB7BK]\[\]\[SCSB7BK]\[SCSBCSO CSOCSOCSOCSOCSOCSOCSOCSOKTR]:\]\][SCBK][SCBK][SCBK]\[SCBK]\[SCBK]\[SCSB1CSOCSLT\ [SCBK]\\\\\\\\\[SCSB1CSOCSOCSOCSO\\\\\\\\\ 30720\ 10 \ 1543998285921845\\\\ 12281045 \ 15552417629170647261

Das `ATYP` Element (im Beispiel unterstrichen) gibt an, welches Ereignis die Nachricht generiert hat. Diese Beispielnachricht enthält den "SHEA" Nachrichtencode ([ATYP(FC32):SHEA]), der angibt, dass er durch eine erfolgreiche S3-HEAD-Anforderung generiert wurde.

Gemeinsame Elemente in Audit-Meldungen

Alle Meldungen enthalten die allgemeinen Elemente.

Codieren	Typ	Beschreibung
INMITTEN	FC32	Modul-ID: Eine vierstellige Kennung der Modul-ID, die die Nachricht generiert hat. Dies gibt das Codesegment an, in dem die Überwachungsmeldung generiert wurde.
ANID	UI32	Node-ID: Die Grid-Node-ID, die dem Service zugewiesen wurde, der die Meldung generiert hat. Jedem Service wird bei Konfiguration und Installation des StorageGRID-Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.
ASES	UI64	Kennung der Auditsitzung: In vorherigen Releases gab dieses Element die Zeit an, zu der das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit der Betriebssystemepoche gemessen (00:00:00 UTC am 1. Januar 1970). **Hinweis:** Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ASQN	UI64	Sequenzanzahl: In vorherigen Releases wurde dieser Zähler für jede erzeugte Überwachungsmeldung auf dem Grid-Node (ANID) erhöht und beim Neustart des Dienstes auf Null zurückgesetzt. **Hinweis:** Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ATID	UI64	Trace-ID: Eine Kennung, die von den Nachrichten, die von einem einzelnen Ereignis ausgelöst wurden, gemeinsam genutzt wird.

Codieren	Typ	Beschreibung
ATIM	UI64	Zeitstempel: Die Zeit, zu der das Ereignis generiert wurde, das die Audit-Nachricht auslöste, gemessen in Mikrosekunden seit der Betriebssystemepoche (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 ein Aufrundung oder Verkürzung des protokollierten Zeitstempels erforderlich. Die vom Benutzer lesbare Zeit, die am Anfang der Überwachungsmeldung in der Datei angezeigt `audit.log` wird, ist das ATIM-Attribut im ISO 8601-Format. Datum und Uhrzeit werden als, dargestellt *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, wobei das ein literales Zeichenkette ist, das `T` den Beginn des Zeitsegments des Datums angibt. *`UUUUUU`* Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine vierstellige Kennung des zu protokollierenden Ereignisses. Dies regelt den "Nutzlastinhalt" der Nachricht: Die Attribute, die enthalten sind.
AVER	UI32	Version: Die Version der Audit-Nachricht. Wenn die StorageGRID Software weiterentwickelt wird, können neue Serviceversionen neue Funktionen in die Audit-Berichte integrieren. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst zur Verarbeitung von Meldungen aus älteren Serviceversionen.
RSLT	FC32	Ergebnis: Das Ergebnis von Ereignis, Prozess oder Transaktion. Wenn für eine Nachricht nicht relevant ist, WIRD KEINE verwendet, sondern SUCS, damit die Nachricht nicht versehentlich gefiltert wird.

Beispiele für Überwachungsnachrichten

Detaillierte Informationen finden Sie in jeder Audit-Nachricht. Alle Überwachungsmeldungen verwenden das gleiche Format.

Im Folgenden finden Sie ein Beispiel für eine Audit-Meldung, wie sie in der Datei angezeigt werden könnte `audit.log`:

```
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 Überwachungsmeldung enthält Informationen über das zu protokollierte Ereignis sowie Informationen über die Meldung selbst.

Um festzustellen, welches Ereignis durch die Überwachungsmeldung 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 Meldung des Audits zeigt auch den Bucket an, dem das Objekt zugeordnet 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 zu ermitteln, wann das PUT-Ereignis aufgetreten ist, notieren Sie den UTC-Zeitstempel (Universal Coordinated Time, Universal Coordinated Time, koordinierte Zeit) zu Beginn der Überwachungsmeldung. Dieser Wert ist eine vom Menschen lesbare Version des ATIM-Attributs der Überwachungsmeldung 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. In diesem Beispiel wird der Wert `1405631878959669` in Donnerstag, 17. Juli 2014 21:17:59 UTC übersetzt.

Überwachungsmeldungen und der Lebenszyklus von Objekten

Wann werden Audit-Meldungen generiert?

Audit-Nachrichten werden bei jeder Aufnahme, jedem Abruf oder jedem Löschen eines Objekts generiert. Sie können diese Transaktionen im Revisionsprotokoll identifizieren, indem Sie S3-API-spezifische Audit-Meldungen suchen.

Überwachungsmeldungen werden durch Kennungen verknüpft, die für jedes Protokoll spezifisch sind.

Protokoll	Codieren
Verknüpfen von S3-Vorgängen	S3BK (Eimer), S3KY (Schlüssel) oder beide
Verknüpfen interner Vorgänge	CBID (interne Kennung des Objekts)

Timing von Audit-Meldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Nodes, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der durch die verschiedenen Services erzeugten Audit-Meldungen von den Beispielen in diesem Abschnitt abweichen.

Objektaufnahme von Transaktionen

Sie können Client-Ingest-Transaktionen im Revisionsprotokoll identifizieren, indem Sie S3-API-spezifische Audit-Meldungen ermitteln.

In der folgenden Tabelle sind nicht alle während einer Aufnahmetransaktion generierten Prüfmeldungen aufgeführt. Es sind nur die Nachrichten enthalten, die zum Verfolgen der Aufnahmetransaktion erforderlich sind.

S3 Aufnahme von Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3-PUT-Aufnahmerate wurde erfolgreich abgeschlossen.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Beispiel: S3-Objektaufnahme

Die folgende Serie von Audit-Meldungen ist ein Beispiel für die im Revisionsprotokoll generierten und gespeicherten Audit-Meldungen, wenn ein S3-Client ein Objekt in einen Storage-Node (LDR-Service) einspeist.

In diesem Beispiel umfasst die aktive ILM-Richtlinie die ILM-Regel „2 Kopien erstellen“.

> Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Audit-Meldungen aufgeführt. Es werden nur solche aufgeführt, die sich auf die S3-Aufnahmetransaktion (SPUT) beziehen.

In diesem Beispiel wird vorausgesetzt, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Meldung gibt an, 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-Meldung gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Meldung enthält die CBID des Objekts und den Namen der verwendeten ILM-Regel.

Bei replizierten Objekten umfasst das Feld LOCS die LDR-Node-ID und 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]]
```

Für Objekte, die mit Erasure Coding codiert wurden, enthält das Feld LOCS die Profil-ID für Erasure Coding und die Gruppen-ID für Erasure Coding

```
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.

```
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]]
```

Löschen von Objekttransaktionen

Sie können Objektlöschtransaktionen im Revisionsprotokoll identifizieren, indem Sie S3-API-spezifische Audit-Meldungen suchen.

In den folgenden Tabellen sind nicht alle während einer Löschtransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die zum Verfolgen der Löschtransaktion erforderlich sind.

S3-Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Anforderung zum Löschen des Objekts aus einem Bucket gemacht.	CBID, S3KY	"SDEL: S3 LÖSCHEN"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt aus einem Storage-Node (LDR-Service) löscht, wird eine Überwachungsmeldung generiert und im Revisionsprotokoll gespeichert.

> Im folgenden Beispiel sind nicht alle während einer Löschtransaktion generierten Audit-Meldungen aufgeführt. Es werden nur diejenigen aufgelistet, die mit der S3-Löschtransaktion (SDEL) in Verbindung stehen.

SDEL: S3 Löschen

Das Löschen von Objekten beginnt, wenn der Client eine DeleteObject-Anforderung an einen LDR-Dienst sendet. Die Meldung 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]]
```

Abrufen von Objekttransaktionen

Sie können Transaktionen für den Abruf von Objekten im Revisionsprotokoll identifizieren, indem Sie S3-API-spezifische Audit-Meldungen suchen.

In der folgenden Tabelle 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 von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 ABRUFEN	Anforderung zum Abrufen eines Objekts aus einem Bucket	CBID, S3BK, S3KY	"SGET S3 ABRUFEN"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Storage-Node (LDR-Service) abruft, wird eine Audit-Meldung erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET S3 ABRUFEN

Der Objektabruf beginnt, wenn der Client eine GetObject-Anforderung an einen LDR-Dienst sendet. Die Meldung 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 ermöglicht, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört, Die Überwachungsmeldung enthält Informationen über das Mandantenkonto des Bucket-Inhabers, sodass Sie diese anonymen und Cross-Account-Anforderungen verfolgen können.

In der folgenden Beispielmeldung sendet der Client eine GetObject-Anforderung für ein Objekt, das in einem Bucket gespeichert ist, dem er nicht gehört. Die Werte für SBAI und SBAC zeichnen die Konto-ID und den Namen des Mandanten des Bucket-Besitzers auf. Diese Werte unterscheiden sich von der Konto-ID und dem Namen des in S3AI und SACC aufgezeichneten Clients.

```
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 Audit-Meldungen erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3 Select-Transaktion (SelectObjectContent) beziehen.

Jede Abfrage ergibt zwei Überwachungsmeldungen: Eine, die die Autorisierung der S3 Select-Anforderung ausführt (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]]
```

Nachrichten zum Metadatenupdate

Audit-Meldungen werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zu S3-Metadaten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten wurden aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3-Metadaten wurden aktualisiert"

Beispiel: S3-Metadatenaktualisierung

Das Beispiel zeigt eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadatenaktualisierung

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 Sie die Protokollverwaltung und den externen Syslog-Server" .

```
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]]
```

Audit-Meldungen

Beschreibungen von Audit-Meldungen

Detaillierte Beschreibungen der vom System zurückgegebenen Audit-Meldungen finden Sie in den folgenden Abschnitten. Jede Überwachungsmeldung wird zuerst in einer Tabelle aufgeführt, in der verwandte Nachrichten nach der Aktivitätsklasse gruppiert werden, für die die Meldung steht. Diese Gruppierungen sind sowohl für das Verständnis der Arten von Aktivitäten, die geprüft werden, als auch für die Auswahl der gewünschten Art der Filterung von Überwachungsnachrichten nützlich.

Die Überwachungsmeldungen werden auch alphabetisch nach ihren vier-Zeichen-Codes aufgelistet. Mit dieser alphabetischen Liste können Sie Informationen zu bestimmten Nachrichten finden.

Die in diesem Kapitel verwendeten vierstelligen Codes sind die ATYP-Werte, die in den Überwachungsmeldungen gefunden werden, wie in der folgenden Beispielmeldung dargestellt:

```
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 Sie die Protokollverwaltung und den externen Syslog-Server"

Kategorien von Überwachungsnachrichten

Systemaudits Meldungen

Die Audit-Meldungen, die zur Systemauditkategorie gehören, werden für Ereignisse im Zusammenhang mit dem Überwachungssystem selbst, Grid-Node-Status, systemweiter Aufgabenaktivität (Grid-Aufgaben) und Service-Backup-Vorgängen verwendet.

Codieren	Titel und Beschreibung der Nachricht	Siehe
ECMC	Fehlende Datenfragment mit Erasure-Code: Gibt an, dass ein fehlendes Datenfragment mit Erasure-Code erkannt wurde.	"ECMC: Fehlende Datenfragment mit Erasure-Code"
ECOC	Beschädigte Datenfragment mit Erasure-Code: Gibt an, dass ein beschädigtes Datenfragment mit Erasure-Code erkannt wurde.	"ECOC: Beschädigtes Datenfragment mit Erasure-Code"
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Verbindungsversuch mit TLS (Transport Layer Security) fehlgeschlagen.	"ETAF: Sicherheitsauthentifizierung fehlgeschlagen"
GNRG	GNDS Registrierung: Ein Dienst aktualisiert oder registriert Informationen über sich selbst im StorageGRID-System.	"GNRG: GNDS Registrierung"
GNUR	GNDS Unregistrierung: Ein Dienst hat sich vom StorageGRID-System nicht registriert.	"GNUR: GNDS Registrierung aufheben"
GTED	Grid Task beendet: Der CMN-Dienst hat die Verarbeitung der Grid-Aufgabe abgeschlossen.	"GTED: Grid Task beendet"
GTST	Grid Task gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid-Aufgabe begonnen.	"GTST: Grid Task gestartet"
GSU	Grid Task übermittelt: Eine Grid-Aufgabe wurde an den CMN-Dienst übermittelt.	"GTSU: Grid Task übermittelt"

Codieren	Titel und Beschreibung der Nachricht	Siehe
LLST	Standort verloren: Diese Überwachungsmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"
OLST	Objekt verloren: Ein angeforderter Gegenstand kann nicht innerhalb des StorageGRID Systems gefunden werden.	"OLST: System hat Lost Object erkannt"
SADD	Sicherheitsüberprüfung deaktivieren: Die Protokollierung von Überwachungsnachrichten wurde deaktiviert.	"SADD: Security Audit deaktiviert"
SADE	Sicherheitsüberprüfung aktivieren: Die Protokollierung von Prüfnachrichten wurde wiederhergestellt.	"SADE: Sicherheits-Audit aktivieren"
SVRF	Objektspeicherüberprüfung fehlgeschlagen: Überprüfung durch einen Inhaltsblock fehlgeschlagen.	"SVRF: Objektspeicherüberprüfung fehlgeschlagen"
SVRU	Objektspeicher Verify Unbekannt: Unerwartete Objektdaten im Objektspeicher erkannt.	"SVRU: Objektspeicher überprüfen Unbekannt"
SYSD	Knotenstopp: Es wurde ein Herunterfahren angefordert.	"SYSD: Knoten stoppen"
SYST	Knoten stoppen: Ein Dienst hat einen graziösen Stopp initiiert.	"SYST: Knoten wird angehalten"
SYSU	Node Start: Ein Dienst gestartet. In der Meldung wird der Charakter des vorherigen Herunterfahrens angezeigt.	"SYSU: Knoten Start"

Audit-Meldungen zu Objekt-Storage

Die Audit-Meldungen der Objekt-Storage-Audit-Kategorie werden für Ereignisse im Zusammenhang mit der Speicherung und Verwaltung von Objekten im StorageGRID System verwendet. Dazu zählen Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Verifizierungen.

Audit-Codes werden aus dem Produkt und der Dokumentation entfernt, da Funktionen veraltet sind. Wenn ein Audit-Code angezeigt wird, der hier nicht aufgeführt ist, überprüfen Sie die früheren Versionen dieses Themas auf ältere SG-Versionen. "Audit-Meldungen zu StorageGRID 11.8 Objekt-Storage"Beispiel: .

Codieren	Beschreibung	Siehe
BROR	Bucket Read Only Request: Ein Bucket wurde in den schreibgeschützten Modus eingegeben oder beendet.	"BROR: Bucket Read Only Request"
CBSES	Objekt Send End: Die Quelleinheit hat einen Grid-Node zum Grid-Node-Datentransfer abgeschlossen.	"CBSE: Objekt Senden Ende"
CBRE	Empfang des Objekts: Die Zieleinheit hat einen Grid-Node zum Datentransfer des Grid-Node abgeschlossen.	"CBRE: Das Objekt erhält das Ende"
CGRR	Grid-übergreifende Replizierungsanforderung: StorageGRID hat einen Grid-übergreifenden Replizierungsvorgang versucht, um Objekte zwischen Buckets in einer Grid-Verbundverbindung zu replizieren.	"CGRR: Grid-übergreifende Replikationsanforderung"
EBDL	Löschen von leeren Buckets: Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, das alle Objekte löscht (es wurde ein leerer Bucket-Vorgang durchgeführt).	"EBDL: Leerer Bucket löschen"
EBKR	Anforderung für leere Bucket: Ein Benutzer hat eine Anforderung gesendet, Leere Bucket ein- oder auszuschalten (d. h. Bucket-Objekte zu löschen oder das Löschen von Objekten zu stoppen).	"EBKR: Anforderung für leeren Bucket"
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"SCMT: Object Store Commit Request"
SREM	Objektspeicher Remove: Ein Inhaltsblock wurde von einem Grid-Knoten gelöscht und kann nicht mehr direkt angefordert werden.	"SREM: Objektspeicher Entfernen"

Client liest Audit-Meldungen

Gelesene Audit-Meldungen des Clients werden protokolliert, wenn eine S3-Client-Anwendung eine Anforderung zum Abrufen eines Objekts vornimmt.

Codieren	Beschreibung	Verwendet von	Siehe
S3SL	S3 Select-Anforderung: Protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Meldung kann Fehlermeldungen und Fehlercodedetails enthalten. Die Anforderung war möglicherweise nicht erfolgreich.	S3-Client	"S3SL: S3 Select Request"

Codieren	Beschreibung	Verwendet von	Siehe
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SGET S3 ABRUFEN"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	S3-Client	"SHEA: S3 KOPF"

Audit-Meldungen des Clients schreiben

Audit-Meldungen für den Client-Schreibvorgang werden protokolliert, wenn eine S3-Client-Anwendung eine Anforderung zum Erstellen oder Ändern eines Objekts stellt.

Codieren	Beschreibung	Verwendet von	Siehe
OVWR	Objekt-Überschreiben: Protokolliert eine Transaktion, um ein Objekt mit einem anderen Objekt zu überschreiben.	S3-Client	"OVWR: Objektüberschreibung"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SDEL: S3 LÖSCHEN"
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zur Wiederherstellung eines Objekts aus AWS Glacier Storage in einem Cloud Storage Pool.	S3-Client	"SPOS: S3-BEITRAG"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SPUT: S3 PUT"
SUPD	Aktualisierte S3 Metadaten: Protokolliert eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes Objekt oder Bucket.	S3-Client	"SUPD: S3-Metadaten wurden aktualisiert"

Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API.

Codieren	Titel und Beschreibung der Nachricht	Siehe
MGAU	Management-API-Audit-Nachricht: Ein Protokoll von Benutzeranfragen.	"MGAU: Management-Audit-Nachricht"

ILM-Prüfmeldungen

Die Audit-Meldungen der ILM-Audit-Kategorie werden für Ereignisse im Zusammenhang mit ILM-Vorgängen (Information Lifecycle Management) verwendet.

Codieren	Titel und Beschreibung der Nachricht	Siehe
IDEL	ILM-Initiated Delete: Diese Audit-Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.	"IDEL: ILM gestartet Löschen"
LKCU	Bereinigung Des Objekts Überschrieben. Diese Überwachungsmeldung wird erzeugt, wenn ein überschreibtes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Objektbereinigung überschrieben"
ORLM	Erfüllt Objektregeln: Diese Überwachungsmeldung wird generiert, wenn Objektdaten gemäß den ILM-Regeln gespeichert werden.	"ORLM: Objektregeln erfüllt"

Referenz für Überwachungsmeldung

BROR: Bucket Read Only Request

Der LDR-Service generiert diese Überwachungsmeldung, wenn ein Bucket in den schreibgeschützten Modus wechselt oder diesen beendet. Beispielsweise wechselt ein Bucket in den schreibgeschützten Modus, während alle Objekte gelöscht werden.

Codieren	Feld	Beschreibung
BKHD	Bucket-UUID	Die Bucket-ID.
BROV	Wert der schreibgeschützten Bucket-Anforderung	Gibt an, ob der Bucket schreibgeschützt ist oder den schreibgeschützten Status verlässt (1 = schreibgeschützt, 0 = nicht schreibgeschützt).
BROS	Grund für schreibgeschützten Bucket	Der Grund, warum der Bucket schreibgeschützt ist oder den schreibgeschützten Status verlässt. Beispiel: LeptyBucket.

Codieren	Feld	Beschreibung
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, das die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3 Bucket	Der S3-Bucket-Name

CBRB: Objekt empfangen beginnen

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn der Transfer eines Inhaltsblocks von einem Node zum anderen initiiert wird, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert

wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBRE: Das Objekt erhält das Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.

Codieren	Feld	Beschreibung
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung wurde aufgrund des Empfangs von beschädigten oder ungültigen Daten beendet

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

CBSB: Objektsendebeginn

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen initiiert wird, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.

Codieren	Feld	Beschreibung
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBSE: Objekt Senden Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.

Codieren	Feld	Beschreibung
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung wurde aufgrund des Empfangs von beschädigten oder ungültigen Daten beendet

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

CGRR: Grid-übergreifende Replikationsanforderung

Diese Meldung wird generiert, wenn StorageGRID versucht, Objekte zwischen Buckets in einer Grid-Federation-Verbindung in einem Grid-Replizierungsvorgang zu replizieren.

Codieren	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Byte. Das CSIZ-Attribut wurde in StorageGRID 11.8 eingeführt. Daher weisen Grid-übergreifende Replizierungsanforderungen für ein Upgrade auf StorageGRID 11.7 bis 11.8 möglicherweise eine ungenaue Gesamtobjektgröße auf.
S3AI	S3-Mandantenkonto-ID	Die ID des Mandantenkontos, dem der Bucket gehört, von dem das Objekt repliziert wird.

Codieren	Feld	Beschreibung
GFID	Verbindungs-ID des Grid-Verbunds	Die ID der Grid-Verbundverbindung, die für die Grid-übergreifende Replizierung verwendet wird.
BETR.	CGR-Betrieb	Der Typ des Grid-übergreifenden Replikationsvorgangs, der versucht wurde: • 0 = Objekt replizieren • 1 = Mehrteiliges Objekt replizieren • 2 = Löschmarkierung replizieren
S3BK	S3 Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens.
VSID	Version-ID	Die Versions-ID der spezifischen Version eines Objekts, das repliziert wurde.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder allgemeinen Fehler (GERR) zurück.

EBDL: Leerer Bucket löschen

Der ILM-Scanner hat ein Objekt in einem Bucket gelöscht, das alle Objekte löscht (und einen leeren Bucket-Vorgang durchgeführt).

Codieren	Feld	Beschreibung
CSIZ	Objektgröße	Die Größe des Objekts in Byte.
PFAD	S3-Bucket/Key	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 im StorageGRID System.
RSLT	Ergebnis des Löschvorgangs	Das Ergebnis eines Ereignisses, Prozesses oder einer Transaktion. Wenn für eine Nachricht nicht relevant ist, WIRD KEINE verwendet, sondern SUCS, damit die Nachricht nicht versehentlich gefiltert wird.

EBKR: Anforderung für leeren Bucket

Diese Meldung zeigt an, dass ein Benutzer eine Anforderung zum ein- und Ausschalten

von leeren Buckets gesendet hat (d. h. zum Löschen von Bucket-Objekten oder zum Beenden des Löschens von Objekten).

Codieren	Feld	Beschreibung
BUID	Bucket-UUID	Die Bucket-ID.
EBJS	Leere Bucket-JSON-Konfiguration	Enthält den JSON, der die aktuelle leere Bucket-Konfiguration darstellt.
S3AI	S3-Mandantenkonto-ID	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name

ECMC: Fehlende Datenfragment mit Erasure-Code

Diese Meldung zeigt an, dass das System ein fehlendes Datenfragment mit Löschungscode erkannt hat.

Codieren	Feld	Beschreibung
VCMC	VCS-ID	Der Name des VCS, der den fehlenden Teil enthält.
MCID	Block-ID	Der Bezeichner des fehlenden Fragments mit Löschungscode.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ECOC: Beschädigtes Datenfragment mit Erasure-Code

Diese Meldung zeigt an, dass das System ein korruptes Datenfragment mit Löschungscode erkannt hat.

Codieren	Feld	Beschreibung
VCCO	VCS-ID	Der Name des VCS, der den beschädigten Teil enthält.
VLID	Volume-ID	Das RangeDB-Volume, das das korrupte Fragment mit Löschungscode enthält.
CCID	Block-ID	Der Identifier des beschädigten Fragments zur Löschung.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ETAF: Sicherheitsauthentifizierung fehlgeschlagen

Diese Meldung wird erzeugt, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Codieren	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 Remote-Benutzers darstellt.
RSLT	Ursachencode	Der Grund für den Fehler: SCNI: Sichere Verbindungseinrichtung fehlgeschlagen. CERM: Zertifikat fehlt. Zertifikat: Zertifikat war ungültig. CERE: Das Zertifikat ist abgelaufen. CERR: Zertifikat wurde widerrufen. CSGN: Die Zertifikatsignatur war ungültig. CSGU: Zertifikatssignator war unbekannt. UCRM: Benutzerkennungen fehlten. UCRI: Die Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht zulässig. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wenn eine Verbindung zu einem sicheren Service hergestellt wird, der TLS verwendet, werden die Anmeldeinformationen der Remote-Einheit mithilfe des TLS-Profils und der zusätzlichen Logik, die in den Service integriert ist, überprüft. Wenn diese Authentifizierung aufgrund ungültiger, unerwarteter oder unzulässiger Zertifikate oder Anmeldeinformationen fehlschlägt, wird eine Überwachungsmeldung protokolliert. Dies ermöglicht Abfragen für nicht autorisierte Zugriffsversuche und andere sicherheitsrelevante Verbindungsprobleme.

Die Meldung kann dazu führen, dass eine Remoteineinheit eine falsche Konfiguration hat oder dass versucht

wird, ungültige oder unzulässige Anmeldedaten für das System vorzulegen. Diese Überwachungsmeldung sollte überwacht werden, um Versuche zu erkennen, unbefugten Zugriff auf das System zu erlangen.

GNRG: GNDS Registrierung

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst Informationen über sich selbst im StorageGRID-System aktualisiert oder registriert hat.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.
GNTP	Gerätetyp	Der Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Modellversion des Geräts	Der String, der die Gerätemodellversion des Grid-Knotens im DMDL-Bundle identifiziert.
GNGP	Gruppieren	Die Gruppe, zu der der Grid-Knoten gehört (im Zusammenhang mit Verbindungskosten und Service-Query-Ranking).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Node.

Diese Meldung wird generiert, wenn ein Grid-Knoten seinen Eintrag im Grid-Knoten-Paket aktualisiert.

GNUR: GNDS Registrierung aufheben

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst nicht registrierte Informationen über sich selbst vom StorageGRID-System enthält.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.

GTED: Grid Task beendet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst die Verarbeitung der

angegebenen Rasteraufgabe abgeschlossen hat und die Aufgabe in die Tabelle „Historisch“ verschoben hat. Wenn es sich um SUCS, ABRT oder ROLF handelt, wird eine entsprechende Überwachungsmeldung für die mit Grid Task gestartete Aufgabe angezeigt. Die anderen Ergebnisse zeigen, dass die Verarbeitung dieser Grid-Aufgabe nie gestartet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über den gesamten Lebenszyklus. **Hinweis:** die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: • SUCS: Die Grid-Aufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne Rollback-Fehler beendet. • ROLF: Die Grid-Aufgabe wurde beendet und konnte den Rollback-Vorgang nicht abschließen. • STORNO: Die Grid-Aufgabe wurde vom Benutzer vor dem Start abgebrochen. • EXPR: Der Grid-Task ist vor dem Start abgelaufen. • IVLD: Die Grid-Aufgabe war ungültig. • AUTH: Die Grid-Aufgabe war nicht zulässig. • DUPL: Die Grid-Aufgabe wurde als Duplikat abgelehnt.

GTST: Grid Task gestartet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst mit der Verarbeitung der angegebenen Grid-Aufgabe begonnen hat. Die Meldung „Audit“ folgt unmittelbar der Nachricht „Grid Task Submission Submitted“ für Grid-Aufgaben, die vom internen Grid Task Submission Service initiiert und für die automatische Aktivierung ausgewählt wurde. Für Grid-Aufgaben, die in die Tabelle „Ausstehend“ eingereicht werden, wird diese Meldung generiert, wenn der Benutzer die Grid-Aufgabe startet.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. **Hinweis:** die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: • SUCS: Die Grid-Aufgabe wurde erfolgreich gestartet.

GTSU: Grid Task übermittelt

Diese Überwachungsmeldung zeigt an, dass eine Grid-Aufgabe an den CMN-Dienst gesendet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Identifiziert eindeutig eine generierte Grid-Aufgabe und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. **Hinweis:** die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
TTYP	Aufgabentyp	Der Typ der Rasteraufgabe.
TVER	Aufgabenversion	Eine Zahl, die die Version der Grid-Aufgabe angibt.
TDSC	Aufgabenbeschreibung	Eine vom Menschen lesbare Beschreibung der Grid-Aufgabe.
VATS	Gültig Nach Zeitstempel	Die früheste Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX-Zeit), zu der die Grid-Aufgabe gültig ist.
VBTS	Gültig Vor Zeitstempel	Die letzte Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX Zeit), zu der die Grid-Aufgabe gültig ist.

Codieren	Feld	Beschreibung
TSRC	Quelle	Die Quelle der Aufgabe: • TXTB: Die Grid-Aufgabe wurde über das StorageGRID-System als signierter Textblock gesendet. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submit Service übermittelt.
ACTV	Aktivierungstyp	Die Art der Aktivierung: • AUTO: Die Grid-Aufgabe wurde zur automatischen Aktivierung eingereicht. • PEND: Die Grid-Aufgabe wurde in die ausstehende Tabelle übermittelt. Dies ist die einzige Möglichkeit für die TXTB-Quelle.
RSLT	Ergebnis	Das Ergebnis der Einreichung: • SUCS: Die Grid-Aufgabe wurde erfolgreich übermittelt. • FAIL: Die Aufgabe wurde direkt in die historische Tabelle verschoben.

IDEL: ILM gestartet Löschen

Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.

Die IDEL-Nachricht wird in einer der folgenden Situationen erzeugt:

- **Für Objekte in konformen S3-Buckets**: Diese Meldung wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, da der Aufbewahrungszeitraum abgelaufen ist (vorausgesetzt, die Einstellung zum automatischen Löschen ist aktiviert und die Legal Hold ist deaktiviert).
- **Für Objekte in nicht konformen S3 Buckets**. Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet, da derzeit keine Platzierungsanweisungen in den aktiven ILM-Richtlinien für das Objekt gelten.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CMPA	Compliance: Automatisches Löschen	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true) geben an, ob ein konformes Objekt automatisch gelöscht werden soll, wenn der Aufbewahrungszeitraum endet, es sei denn, der Bucket befindet sich unter einer gesetzlichen Aufbewahrungspflichten.
CMPL	Einhaltung: Gesetzliche Aufbewahrungspflichten	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true), die angeben, ob der Bucket derzeit unter einer gesetzlichen Aufbewahrungspflichten steht.

Codieren	Feld	Beschreibung
CMPR	Compliance: Aufbewahrungszeitraum	Nur für Objekte in S3-konformen Buckets. Die Länge der Aufbewahrungsdauer des Objekts in Minuten.
CTME	Compliance: Aufnahmezeit	Nur für Objekte in S3-konformen Buckets. Die Aufnahmezeit des Objekts. Sie können den Aufbewahrungszeitraum in Minuten zu diesem Wert hinzufügen, um zu bestimmen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Vorgänge in Buckets enthalten dieses Feld nicht.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte, die mit Erasure Coding codiert wurden, werden die Profil-ID und die Gruppen-ID der Erasure Coding-Gruppe verwendet, die auf die Objektdaten angewendet wird. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3-Bucket/Key	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 der Aufbewahrungszeitraum abgelaufen ist, ist dieses Feld leer. • Wenn das Objekt gelöscht wird, da derzeit keine Anweisungen zur Platzierung für das Objekt vorhanden sind, zeigt dieses Feld den vom Menschen lesbaren Namen der letzten ILM-Regel an, die auf das Objekt angewendet wurde.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.

Codieren	Feld	Beschreibung
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

LKCU: Objektbereinigung überschrieben

Diese Meldung wird generiert, wenn StorageGRID ein überschreibtes Objekt entfernt, das zuvor zur Freigabe von Speicherplatz erforderlich war. Ein Objekt wird überschrieben, wenn ein S3-Client ein Objekt auf einen Pfad schreibt, der bereits ein Objekt enthält. Die Entfernung erfolgt automatisch und im Hintergrund.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
LTYP	Art der Bereinigung	*Nur zur internen Verwendung.*
LUID	Objekt-UUID entfernt	Die Kennung des entfernten Objekts.
PFAD	S3-Bucket/Key	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: Leaked Object Cleanup

Diese Meldung wird generiert, wenn ein durchgesicktes Stück bereinigt oder gelöscht wurde. Ein Chunk kann Teil eines replizierten Objekts oder eines Erasure-Coding-Objekts sein.

Codieren	Feld	Beschreibung
KLOK	Chunk-Position	Der Dateipfad des durchgesickerten Blocks, der gelöscht wurde.

Codieren	Feld	Beschreibung

CTYP	Chunk-Typ	Typ des Chunk:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	Lecktyp	Die fünf Arten von Leckagen, 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	Die Zeit, zu der der durchgesickerte Block erstellt wurde.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts, zu dem das Chunk gehört.
CBID	Kennung Für Inhaltsblock	CBID des Objekts, zu dem der durchgesickerte Block gehört.
CSIZ	Inhaltsgröße	Die Größe des Chunk in Byte.

LLST: Standort verloren

Diese Meldung wird immer dann generiert, wenn ein Speicherort für eine Objektkopie (repliziert oder Erasure-coded) nicht gefunden werden kann.

Codieren	Feld	Beschreibung
CBIL	CBID	Die betroffene CBID.
ECPR	Erasure-Coding-Profil	Für Erasure-Coding-Objektdaten. Die ID des verwendeten Erasure-Coding-Profils.

Codieren	Feld	Beschreibung
LTYP	Positionstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für Erasure-codierte Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
PCLD	Pfad zu repliziertem Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten. Wird nur zurückgegeben, wenn LTYP einen Wert von CLDI (d.h. für replizierte Objekte) hat. Nimmt die Form an `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Ergebnis	Immer KEINE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
TSRC	Auslösequelle	BENUTZER: Benutzer ausgelöst SYST: System ausgelöst
UUID	Universally Unique ID	Die Kennung des betroffenen Objekts im StorageGRID-System.

MGAU: Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API. Jede HTTP-Anforderung, die keine GET- oder HEAD-Anforderung an einen gültigen API-URI ist, protokolliert eine Antwort, die den Benutzernamen, die IP und den Anforderungstyp an die API enthält. Ungültige API-URIs (z. B. /API/v3-authorize) und ungültige Anforderungen an gültige API-URIs werden nicht protokolliert.

Codieren	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domain-Name	Der Host-Domain-Name.
MPAT	AnfraPfad	Der Anfraspfad.
MPQP	Abfrageparameter anfordern	Die Abfrageparameter für die Anforderung.

Codieren	Feld	Beschreibung
MRBD	Text anfordern	Der Inhalt des Anforderungsinstanz. Während der Antwortkörper standardmäßig protokolliert wird, wird der Anforderungskörper in bestimmten Fällen protokolliert, wenn der Antwortkörper leer ist. Da die folgenden Informationen im Antwortkörper nicht verfügbar sind, werden sie von der Anforderungsstelle für die folgenden POST-Methoden übernommen: • Benutzername und Konto-ID in **POST authorize** • Neue Subnetze-Konfiguration in **POST /Grid/Grid-Networks/Update** • Neue NTP-Server in **POST /grid/ntp-Servers/Update** • Ausgemusterte Server-IDs in **POST /Grid/Servers/Decommission** **Hinweis:** sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MRMD	Anforderungsmethode	Die HTTP-Anforderungsmethode: • POST • PUT • Löschen • PATCH
MRSC	Antwortcode	Der Antwortcode.
MRSP	Antwortkörper	Der Inhalt der Antwort (der Antwortkörper) wird standardmäßig protokolliert. **Hinweis:** sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MSIP	Quell-IP-Adresse	Die Client (Quell-) IP-Adresse.
MUUN	User-URN	Der URN (einheitlicher Ressourcenname) des Benutzers, der die Anforderung gesendet hat.
RSLT	Ergebnis	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.

OLST: System hat Lost Object erkannt

Diese Meldung wird generiert, wenn der DDS-Dienst keine Kopien eines Objekts im StorageGRID-System finden kann.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des verlorenen Objekts.
NID	Node-ID	Falls verfügbar, die letzte bekannte direkte oder Nearline-Position des verlorenen Objekts. Es ist möglich, nur die Knoten-ID ohne eine Volume-ID zu haben, wenn die Volume-Informationen nicht verfügbar sind.
PFAD	S3-Bucket/Key	Falls verfügbar, sind der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
UUID	Universally Unique ID	Die Kennung des verlorenen Objekts im StorageGRID System.
VOLI	Volume-ID	Falls verfügbar, die Volume-ID des Storage Node für den letzten bekannten Speicherort des verlorenen Objekts.

ORLM: Objektregeln erfüllt

Diese Meldung wird generiert, wenn das Objekt erfolgreich gespeichert und wie durch die ILM-Regeln festgelegt kopiert wird.

> Die ORLM-Meldung wird nicht generiert, wenn ein Objekt erfolgreich mit der Regel 2 Kopien erstellen gespeichert wird, wenn eine andere Regel in der Richtlinie den erweiterten Filter Objektgröße verwendet.

Codieren	Feld	Beschreibung
BUID	Bucket-Header	Bucket-ID-Feld Wird für interne Vorgänge verwendet. Wird nur angezeigt, wenn STAT PRGD ist.
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.

Codieren	Feld	Beschreibung
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte, die mit Erasure Coding codiert wurden, werden die Profil-ID und die Gruppen-ID der Erasure Coding-Gruppe verwendet, die auf die Objektdaten angewendet wird. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3-Bucket/Key	Der S3-Bucket-Name und der S3-Schlüsselname.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	Das von Menschen lesbare Etikett, das der ILM-Regel gegeben wurde, die auf dieses Objekt angewendet wurde.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Container-CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur für segmentierte und mehrteilige Objekte verfügbar.
STAT	Status	Der Status des ILM-Betriebs. FERTIG: ILM-Vorgänge für das Objekt wurden abgeschlossen. DFER: Das Objekt wurde für zukünftige ILM-Neuevaluierungen markiert. PRGD: Das Objekt wurde aus dem StorageGRID-System gelöscht. NLOC: Die Objektdaten können nicht mehr im StorageGRID-System gefunden werden. Dieser Status kann darauf hinweisen, dass alle Kopien von Objektdaten fehlen oder beschädigt sind.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Versionsnummer eines neuen Objekts, das in einem versionierten Bucket erstellt wurde Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

Die ORLM-Überwachungsmeldung kann für ein einzelnes Objekt mehr als einmal ausgegeben werden. Sie wird beispielsweise immer dann ausgegeben, wenn eines der folgenden Ereignisse eintritt:

- ILM-Regeln für das Objekt sind dauerhaft erfüllt.
- ILM-Regeln für das Objekt werden für diese Epoche erfüllt.
- Das Objekt wurde durch ILM-Regeln gelöscht.
- Bei der Hintergrundüberprüfung wird erkannt, dass eine Kopie replizierter Objektdaten beschädigt ist. Das StorageGRID System führt eine ILM-Bewertung durch, um das beschädigte Objekt zu ersetzen.

Verwandte Informationen

- "Objektaufnahme von Transaktionen"
- "Löschen von Objekttransaktionen"

OVWR: Objektüberschreibung

Diese Meldung wird erzeugt, wenn ein externer (Client-angeforderter) Vorgang ein Objekt durch ein anderes Objekt überschrieben.

Codieren	Feld	Beschreibung
CBID	Kennung für Inhaltsblock (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des Objekts in Byte, das überschrieben wird.
OCBD	Kennung für Inhaltsblock (vorherige)	Die CBID für das vorherige Objekt.
UUID	Universally Unique ID (neu)	Die Kennung des neuen Objekts im StorageGRID System.
OUID	Universally Unique ID (vorherige)	Die Kennung für das vorherige Objekt innerhalb des StorageGRID-Systems.
PFAD	S3 Objektpfad	Der S3-Objektpfad, der sowohl für das vorherige als auch für das neue Objekt verwendet wird
RSLT	Ergebniscode	Ergebnis der Transaktion Objekt überschreiben. Das Ergebnis ist immer: ERFOLGREICH
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das überschreibende Objekt am angegebenen Standort gelöscht, was nicht der Standort ist, an dem das überschreibende Objekt aufgenommen wurde.

S3SL: S3 Select Request

Diese Meldung protokolliert einen Abschluss, nachdem eine S3 Select-Anforderung an den Client zurückgegeben wurde. Die S3SL-Meldung kann Fehlermeldungen und Fehlercodedetails enthalten. Die Anforderung war möglicherweise nicht erfolgreich.

Codieren	Feld	Beschreibung
BYSC	Gescannte Bytes	Anzahl der von Speicherknoten gescannten (empfangenen) Bytes. BYSC und BYPR unterscheiden sich wahrscheinlich, wenn das Objekt komprimiert wird. Wenn das Objekt komprimiert ist, hätte BYSC die komprimierte Byte-Anzahl und BYPR wären die Bytes nach der Dekomprimierung.
BYPR	Verarbeitetes Byte	Anzahl der verarbeiteten Bytes. Gibt an, wie viele Byte „gescannte Bytes“ tatsächlich von einem S3 Select-Job verarbeitet oder bearbeitet wurden.
BYRT	Bytes Zurückgegeben	Anzahl der Bytes, die ein S3 Select-Job an den Client zurückgegeben hat.
REPR	Datensätze Verarbeitet	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job von Storage-Nodes empfangen hat.
RERT	Datensätze Zurückgegeben	Anzahl der Datensätze oder Zeilen, die ein S3 Select-Job an den Client zurückgegeben hat.
JOFI	Job Abgeschlossen	Zeigt an, ob die Verarbeitung des S3 Select-Jobs abgeschlossen ist oder nicht. Wenn dies falsch ist, konnte der Job nicht abgeschlossen werden, und die Fehlerfelder enthalten wahrscheinlich Daten. Der Kunde hat möglicherweise Teilergebnisse oder gar keine Ergebnisse erhalten.
REID	Anforderungs-ID	Kennung für die S3-Select-Anforderung.
EXTM	Ausführungszeit	Die Zeit in Sekunden, die für den Abschluss des S3 Select Jobs benötigt wurde.
FEHLER	Fehlermeldung	Fehlermeldung, die der S3 Select-Job generiert hat.
ERY	Fehlertyp	Fehlertyp, den der S3 Select-Job generiert hat.
ERST	Fehler Bei Stacktrace	Fehler bei Stacktrace, den der S3 Select-Job generiert hat.
S3BK	S3 Bucket	Der S3-Bucket-Name

Codieren	Feld	Beschreibung
S3AK	S3 Access Key ID (Absender anfordern)	Die S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat.
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat.
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens.

SADD: Security Audit deaktiviert

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung der Überwachungsmeldungen deaktiviert hat; Audit-Meldungen werden nicht mehr erfasst oder geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, mit der das Audit deaktiviert wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Deaktivieren der Revisionsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Meldung besagt, dass die Protokollierung zuvor aktiviert, aber jetzt deaktiviert wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt (SADE) und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SADE: Sicherheits-Audit aktivieren

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung von Überwachungsmeldungen wiederhergestellt hat; Audit-Meldungen werden erneut erfasst und geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, die zum Aktivieren des Audits verwendet wird.

Codieren	Feld	Beschreibung
AEUN	Benutzername	Der Benutzername, der den Befehl zum Aktivieren der Audit-Protokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Nachricht bedeutet, dass die Protokollierung vorher deaktiviert (SADD) war, aber jetzt wiederhergestellt wurde. Dies wird in der Regel nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SCMT: Objekt Store Commit

Grid-Inhalte werden erst dann zur Verfügung gestellt oder als gespeichert erkannt, wenn sie bereitgestellt wurden (was bedeutet, dass sie dauerhaft gespeichert wurden). Dauerhaft gespeicherte Inhalte wurden vollständig auf Festplatte geschrieben und haben entsprechende Integritätsprüfungen bestanden. Diese Meldung wird ausgegeben, wenn ein Inhaltsblock auf den Speicher gesetzt wird.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der zu permanentem Speicher verpflichtet ist.
RSLT	Ergebniscode	Status zum Zeitpunkt, zu dem das Objekt auf Festplatte gespeichert wurde: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und überprüft wurde und nun angefordert werden kann. Er kann zur Nachverfolgung des Datenflusses im System eingesetzt werden.

SDEL: S3 LÖSCHEN

Wenn ein S3-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anforderung ausgeführt, das angegebene Objekt oder Bucket zu entfernen oder eine Bucket/Objekt-Unterressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.

Codieren	Feld	Beschreibung
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Vorgänge in Buckets enthalten dieses Feld nicht.
GFID	Verbindungs-ID der Grid-Verbindung	Die Verbindungs-ID der Grid-Verbundverbindung, die einer Grid-übergreifenden Löschanforderung für die Replikation zugeordnet ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation Source Account ID	Die Konto-ID des Mandanten im Quellraster für eine Grid-übergreifende Löschanforderung für die Replikation. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. `` `X-Forwarded-For` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Wert von der IP-Adresse des Absenders der Anfrage (SAIP-Überwachungsfeld) abweicht. `` `x-amz-bypass-governance-retention` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist.
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH

Codieren	Feld	Beschreibung
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

Codieren	Feld	Beschreibung
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUDM	Universell eindeutige Kennung für eine Löschmarkierung	Die Kennung einer Löschmarkierung. Meldungen des Überwachungsprotokolls geben entweder UUDM oder UUID an, wobei UUDM eine Löschmarkierung anzeigt, die als Ergebnis einer Anfrage zum Löschen von Objekten erstellt wurde, und UUID ein Objekt angibt.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SGET S3 ABRUFEN

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anforderung gestellt, ein Objekt abzurufen, die Objekte in einem Bucket aufzulisten oder eine Bucket/Objektunterressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. `X-Forwarded-For` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Wert von der IP-Adresse des Absenders der Anfrage (SAIP-Überwachungsfeld) abweicht.
LITY	ListObjekteV2	Eine *v2 Format* Antwort wurde angefordert. Weitere Informationen finden Sie unter "AWS ListObjectsV2". Nur für GET Bucket-Vorgänge.
NCHD	Anzahl der Kinder	Enthält Schlüssel und allgemeine Präfixe. Nur für GET Bucket-Vorgänge.
KLINGELTE	Bereichsleser	Nur für Bereichslesevorgänge. Gibt den Bereich der Bytes an, die von dieser Anforderung gelesen wurden. Der Wert nach dem Schrägstrich (/) zeigt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.

Codieren	Feld	Beschreibung
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
TRNC	Abgeschnitten oder nicht abgeschnitten	Setzen Sie auf false, wenn alle Ergebnisse zurückgegeben wurden. Setzen Sie auf wahr, wenn weitere Ergebnisse verfügbar sind, um zurückzukehren. Nur für GET Bucket-Vorgänge.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SHEA: S3 KOPF

Wenn ein S3-Client eine HEAD-Operation ausgibt, wird eine Anforderung gestellt, um die Existenz eines Objekts oder Buckets zu überprüfen und die Metadaten zu einem Objekt abzurufen. Diese Meldung wird vom Server ausgegeben, wenn der Vorgang erfolgreich war.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des überprüften Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. `` `X-Forwarded-For` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Wert von der IP-Adresse des Absenders der Anfrage (SAIP-Überwachungsfeld) abweicht. ``
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SPOS: S3-BEITRAG

Wenn ein S3-Client eine POST Object-Anforderung ausgibt, wird diese Meldung vom Server ausgegeben, wenn die Transaktion erfolgreich durchgeführt wurde.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. `` `X-Forwarded-For` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Wert von der IP-Adresse des Absenders der Anfrage (SAIP-Überwachungsfeld) abweicht. `` (Nicht erwartet für SPOS).
RSLT	Ergebniscode	Ergebnis der Anforderung „RestoreObject“. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend Für eine S3 Select Operation auf „Auswählen“ einstellen.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.

Codieren	Feld	Beschreibung
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Stellen Sie Informationen wieder her.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anforderung gestellt, ein neues Objekt oder einen Bucket zu erstellen oder eine Bucket/Objekt-Unterressource zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Konformitätseinstellungen, sofern diese in der Anforderung vorhanden sind (abgeschnitten auf die ersten 1024 Zeichen).
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
GFID	Verbindungs-ID der Grid-Verbindung	Die Verbindungs-ID der Grid-Verbundverbindung, die einer Grid-übergreifenden REPLIKATIONSANFORDERUNG ZUGEORDNET ist. Nur in Prüfprotokollen im Zielraster enthalten.
GFSA	Grid Federation Source Account ID	Die Konto-ID des Mandanten im Quellraster für eine Grid-übergreifende Replikations-PUT-Anforderung. Nur in Prüfprotokollen im Zielraster enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. `` `X-Forwarded-For` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Wert von der IP-Adresse des Absenders der Anfrage (SAIP-Überwachungsfeld) abweicht. `` `x-amz-bypass-governance-retention` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist.
LKEN	Objektsperre Aktiviert	Wert des Anforderungsheaders `x-amz-bucket-object-lock-enabled`, falls in der Anfrage vorhanden.
LKLH	Gesetzliche Sperren Für Objekte	Wert des Request Header `x-amz-object-lock-legal-hold`, falls vorhanden in der PutObject Anfrage.

Codieren	Feld	Beschreibung
LKMD	Aufbewahrungsmodus Für Objektsperre	Wert des Request Header `x-amz-object-lock-mode`, falls vorhanden in der PutObject Anfrage.
LKRU	Objektsperre Bis Datum Beibehalten	Wert des Request Header `x-amz-object-lock-retain-until-date`, falls vorhanden in der PutObject Anfrage. Die Werte sind auf einen Zeitraum von 100 Jahren nach Aufnahme des Objekts beschränkt.
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.

Codieren	Feld	Beschreibung
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Die neue Subressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
ULID	Upload-ID	Nur in SPUT-Meldungen für CompleteMultipartUpload-Vorgänge enthalten. Zeigt an, dass alle Teile hochgeladen und zusammengesetzt wurden.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Versionsnummer eines neuen Objekts, das in einem versionierten Bucket erstellt wurde Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.
VSST	Status Der Versionierung	Der neue Versionierungs-Status eines Buckets. Es werden zwei Zustände verwendet: "Aktiviert" oder "ausgesetzt". Operationen für Objekte enthalten dieses Feld nicht.

SREM: Objektspeicher Entfernen

Diese Meldung wird ausgegeben, wenn Inhalte aus einem persistenten Storage entfernt werden und nicht mehr über regelmäßige APIs zugänglich sind.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der aus dem permanenten Speicher gelöscht wurde.
RSLT	Ergebniscode	Gibt das Ergebnis der Aktionen zum Entfernen von Inhalten an. Der einzige definierte Wert ist: SUCS: Inhalt aus persistentem Storage entfernt

Diese Überwachungsmeldung bedeutet, dass ein bestimmter Inhaltsblock von einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Die Nachricht kann verwendet werden, um den Fluss gelöschter Inhalte innerhalb des Systems zu verfolgen.

SUPD: S3-Metadaten wurden 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 Metadatenaktualisierung erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Vorgänge in Buckets enthalten dieses Feld nicht.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert des HTTP-Anfrageheaders Consistency-Control, falls in der Anfrage 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 Byte. Vorgänge in Buckets enthalten dieses Feld nicht.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. `X-Forwarded-For` Wird automatisch einbezogen, wenn er in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Wert von der IP-Adresse des Absenders der Anfrage (SAIP-Überwachungsfeld) abweicht.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

Codieren	Feld	Beschreibung
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Versionsnummer der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Für Vorgänge in Buckets und Objekten mit nicht versionierten Buckets wird dieses Feld nicht berücksichtigt.

SVRF: Objektspeicherüberprüfung fehlgeschlagen

Diese Meldung wird ausgegeben, wenn ein Inhaltsblock den Verifizierungsprozess nicht erfolgreich durchführt. Jedes Mal, wenn replizierte Objektdaten von der Festplatte gelesen oder auf die Festplatte geschrieben werden, werden verschiedene Verifizierungsprüfungen durchgeführt, um sicherzustellen, dass die an den anfordernden Benutzer gesendeten Daten mit den ursprünglich im System aufgenommenen Daten identisch sind. Wenn eine dieser Prüfungen fehlschlägt, werden die beschädigten replizierten Objektdaten vom System automatisch gesperrt, um ein erneuten Abruf der Daten zu verhindern.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, bei der die Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Fehlertyp Verifikation: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Prüfung des Hashbasierten Nachrichtenauthentifizierungscodes (HMAC) fehlgeschlagen. EHSH: Unerwarteter verschlüsselter Content-Hash. PHSH: Unerwarteter Originalinhalt Hash. SEQC: Falsche Datensequenz auf der Festplatte. PERR: Ungültige Struktur der Festplattendatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.

Diese Meldung sollte genau überwacht werden. Fehler bei der Inhaltsüberprüfung können auf drohende Hardwareausfälle hinweisen.

Um zu bestimmen, welcher Vorgang die Meldung ausgelöst hat, lesen Sie den Wert des FELDS AMID (Modul-ID). Beispielsweise gibt ein SVFY-Wert an, dass die Meldung vom Storage Verifier-Modul generiert wurde, d. h. eine Hintergrundüberprüfung und STOR zeigt an, dass die Meldung durch den Abruf von Inhalten ausgelöst wurde.

SVRU: Objektspeicher überprüfen Unbekannt

Die Storage-Komponente des LDR-Service scannt kontinuierlich alle Kopien replizierter Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Codieren	Feld	Beschreibung
FPTH	Dateipfad	Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

Die Meldung SVRU: Object Store Verify Unknown Audit sollte genau überwacht werden. Es bedeutet, dass im Objektspeicher unerwartete Kopien von Objektdaten erkannt wurden. Diese Situation sollte sofort untersucht werden, um festzustellen, wie diese Kopien erstellt wurden, da sie auf drohende Hardwareausfälle hinweisen können.

SYSD: Knoten stoppen

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde. Normalerweise wird diese Meldung erst nach einem anschließenden Neustart gesendet, da die Warteschlange für Überwachungsmeldungen vor dem Herunterfahren nicht gelöscht wird. Suchen Sie nach der SYST-Meldung, die zu Beginn der Abschaltsequenz gesendet wird, wenn der Dienst nicht neu gestartet wurde.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Die RSLT eines SYSD kann nicht auf ein „schmutziges“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYST: Knoten wird angehalten

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde und dass der Dienst seine Abschaltsequenz initiiert hat. SYST kann verwendet werden, um festzustellen, ob das Herunterfahren angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das normalerweise nach dem Neustart des Dienstes gesendet wird).

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Der RSLT-Code einer SYST-Meldung kann nicht auf ein „schmutziges“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYSU: Knoten Start

Wenn ein Dienst neu gestartet wird, wird diese Meldung erzeugt, um anzugeben, ob die vorherige Abschaltung sauber (befahl) oder ungeordnet (unerwartet) war.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SUCS: Das System wurde sauber abgeschaltet. DSDN: Das System wurde nicht sauber heruntergefahren. VRGN: Das System wurde erstmals nach der Server-Installation (oder Neuinstallation) gestartet.

Die Meldung gibt nicht an, ob der Host-Server gestartet wurde, sondern nur der Reporting-Service. Diese Meldung kann verwendet werden, um:

- Diskontinuität im Prüfprotokoll erkennen.
- Ermitteln Sie, ob ein Service während des Betriebs ausfällt (da die verteilte Natur des StorageGRID Systems diese Fehler maskieren kann). Der Server Manager startet einen fehlgeschlagenen Dienst automatisch neu.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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