# Überwachen Sie das StorageGRID-System

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


Überwachen Sie das StorageGRID-System . . . 1
- Überwachen Sie ein StorageGRID System . . . 1
- Das Dashboard anzeigen und verwalten . . . 1
  - Dashboard anzeigen . . . 2
  - Managen von Dashboards . . . 3
  - Dashboards konfigurieren . . . 4
- Zeigen Sie die Seite Knoten an . . . 4
  - Zeigen Sie die Seite Knoten an . . . 4
  - Zeigen Sie die Registerkarte Übersicht an . . . 7
  - Zeigen Sie die Registerkarte Hardware an . . . 9
  - Zeigen Sie die Registerkarte Netzwerk an . . . 26
  - Öffnen Sie die Registerkarte „Speicher“ . . . 27
  - Zeigen Sie die Registerkarte Objekte an . . . 29
  - Zeigen Sie die Registerkarte ILM an . . . 31
  - Zeigen Sie die Registerkarte Load Balancer an . . . 32
  - Zeigen Sie die Registerkarte Plattformdienste an . . . 33
  - Zeigen Sie die Registerkarte Laufwerke verwalten an . . . 34
  - Registerkarte „SANtricity System Manager“ anzeigen (nur E-Series) . . . 35
- Informationen, die regelmäßig überwacht werden müssen . . . 37
  - Was und wann zu überwachen . . . 37
  - Systemzustand überwachen . . . 37
  - Monitoring der Storage-Kapazität . . . 42
  - Überwachung des Information Lifecycle Management . . . 51
  - Überwachen Sie Netzwerk- und Systemressourcen . . . 52
  - Überwachen Sie die Mandantenaktivität . . . 56
  - Monitoring von S3-Client-Vorgängen . . . 61
  - Monitoring von Lastverteilungsvorgängen . . . 62
  - Überwachen von Netzverbundverbindungen . . . 63
- Verwalten von Meldungen . . . 68
  - Verwalten von Meldungen . . . 68
  - Zeigen Sie Alarmregeln an . . . 68
  - Erstellen benutzerdefinierter Warnungsregeln . . . 70
  - Bearbeiten von Meldungsregeln . . . 73
  - Deaktivieren von Meldungsregeln . . . 77
  - Entfernen Sie benutzerdefinierte Warnungsregeln . . . 78
  - Verwalten von Warnmeldungen . . . 78
  - Alerts Referenz . . . 87
  - Häufig verwendete Prometheus-Kennzahlen . . . 101
- Referenz für Protokolldateien . . . 106
  - Referenz für Protokolldateien . . . 106
  - StorageGRID-Softwareprotokolle . . . 110
  - Protokoll für Implementierung und Wartung . . . 117
  - Etwa bycast.log . . . 117

Konfigurieren Sie die Protokollverwaltung und den externen Syslog-Server . . . 126
Überlegungen zur Verwendung eines externen Syslog-Servers . . . 126
Konfigurieren der Protokollverwaltung . . . 131
Verwenden Sie SNMP-Überwachung . . . 141
Verwenden Sie SNMP-Überwachung . . . 142
Konfigurieren Sie den SNMP-Agent . . . 143
Aktualisieren Sie den SNMP-Agent . . . 150
Zugriff auf MIB-Dateien . . . 152
Erfassung zusätzlicher StorageGRID-Daten . . . 154
PUT- und GET-Performance werden überwacht . . . 154
Überwachen von Objektverifizierungsvorgängen . . . 154
Audit-Meldungen prüfen . . . 157
Erfassen von Protokolldateien und Systemdaten . . . 158
Starten Sie manuell ein AutoSupport-Paket . . . 160
Prüfen von Support-Kennzahlen . . . 160
E/A-Priorisierung ändern . . . 162
Führen Sie eine Diagnose aus . . . 163
Erstellen benutzerdefinierter Überwachungsanwendungen . . . 167

# 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:

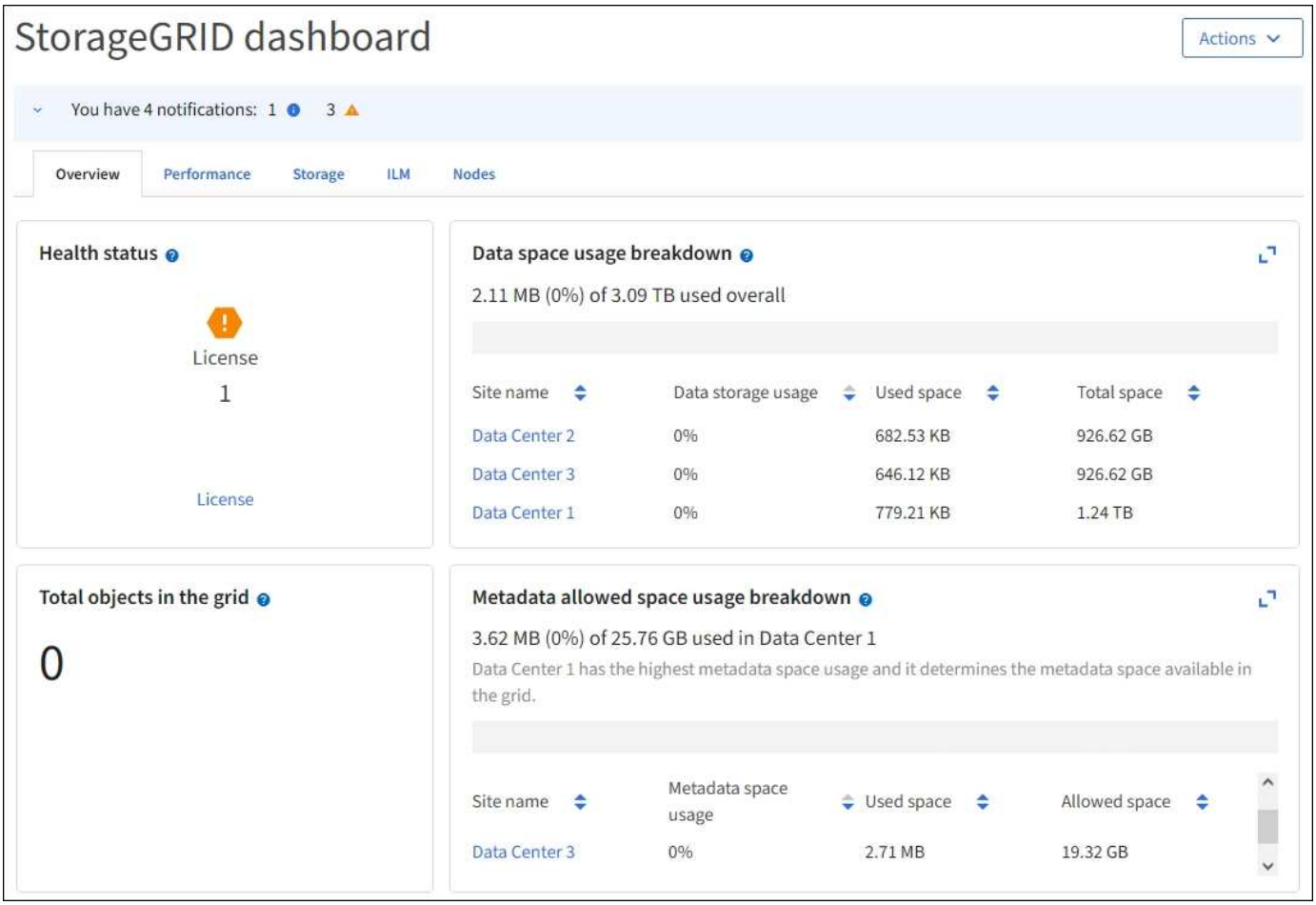
- "Das Dashboard anzeigen und verwalten"
- "Zeigen Sie die Seite Knoten an"
- "Überwachen Sie diese Aspekte des Systems regelmäßig:"
  - "Systemzustand"
  - "Storage-Kapazität"
  - "Informationslebenszyklus-Management"
  - "Netzwerk- und Systemressourcen"
  - "Mandantenaktivität"
  - "Lastverteilung"
  - "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. |

| Im vom System bereitgestellten Dashboard | Enthält |
|---|---|
| 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**.

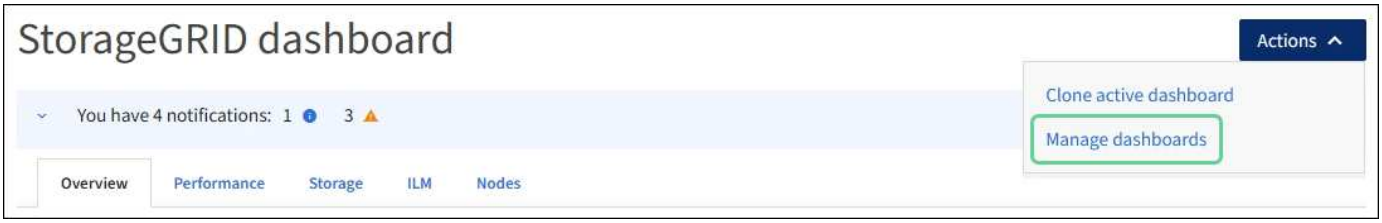
## Managen von Dashboards

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

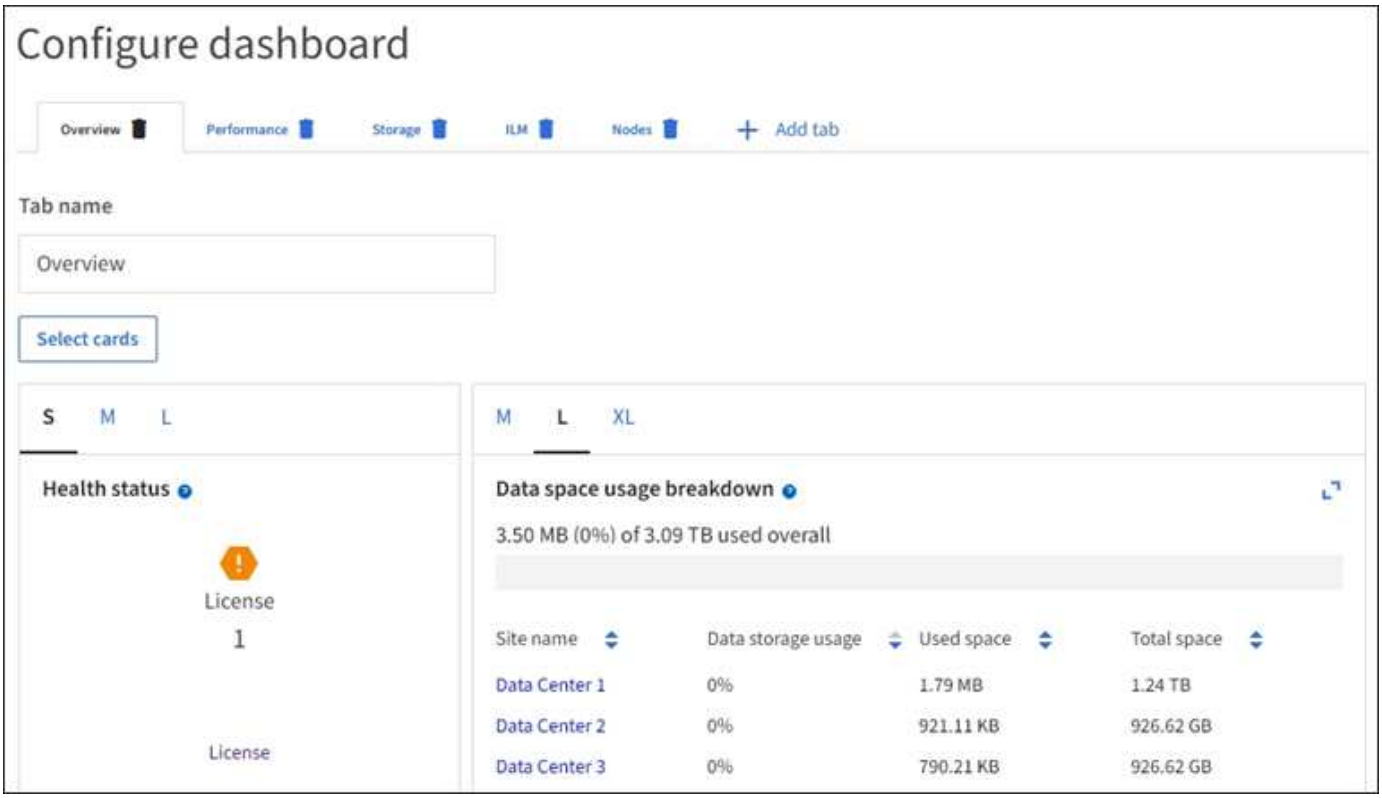
Um ein neues Dashboard durch Klonen des aktiven Dashboards zu erstellen, wählen Sie **actions** > **Clone Active Dashboard**.

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.

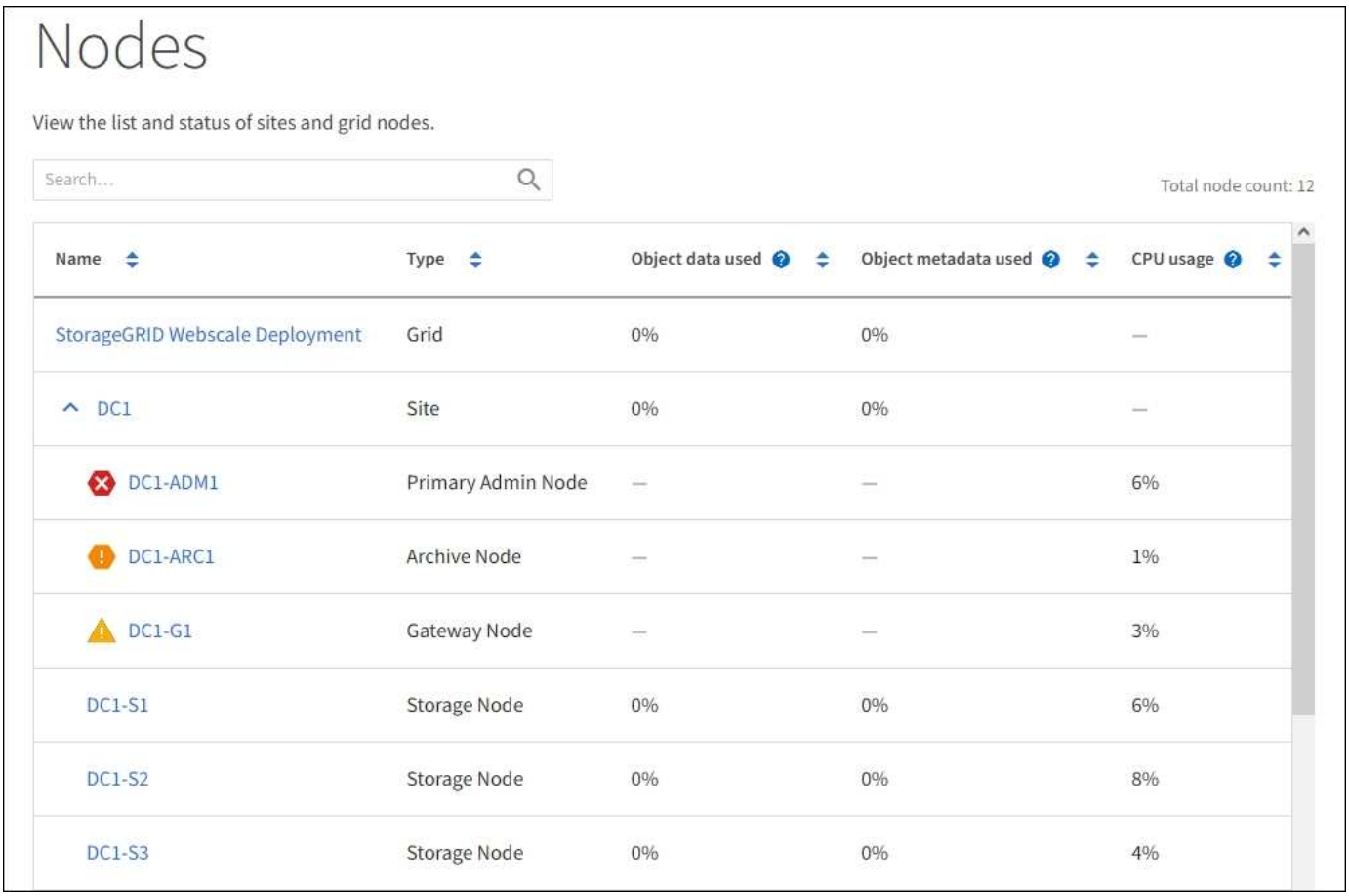
In der Tabelle Nodes werden Zusammenfassungsinformationen für das gesamte Raster, jeden Standort und jeden Node aufgeführt. Wenn ein Knoten getrennt ist oder eine aktive Warnmeldung hat, wird neben dem Knotennamen ein Symbol angezeigt. Wenn der Knoten verbunden ist und keine aktiven Warnmeldungen

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**<br><br>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.<br><br>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.<br><br>Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten.<br><br>**Hinweis**: Ein Knoten kann während des verwalteten Herunterfahrens als Unbekannt erscheinen. In diesen Fällen können Sie den Status Unbekannt ignorieren. |
| | **Nicht verbunden - Administrativ unten**<br><br>Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden.<br><br>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.<br><br>Aufgrund des zugrunde liegenden Problems sind diese Nodes oft ohne Eingriff wieder online. | Ermitteln Sie, ob Warnmeldungen Auswirkungen auf diesen Node haben.<br><br>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.

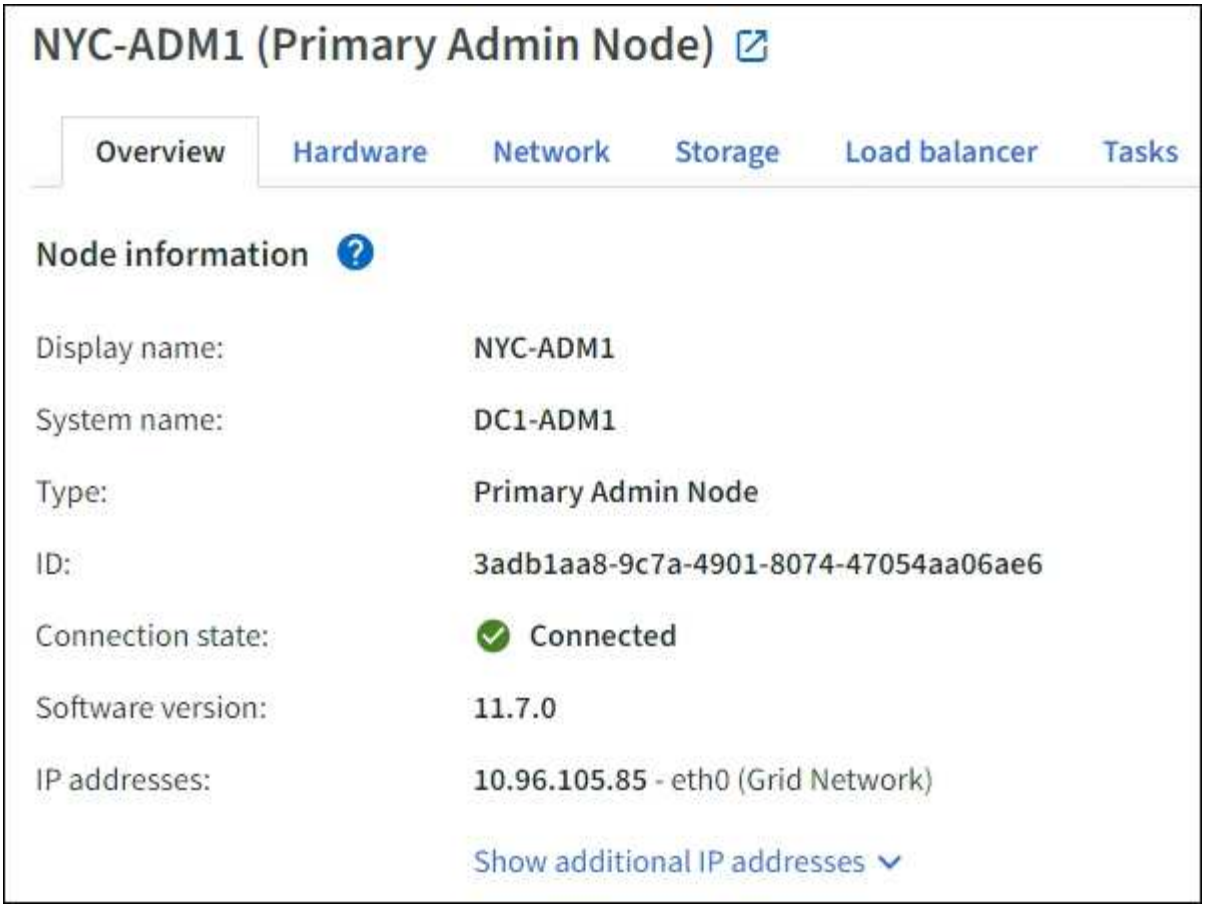
## Zeigen Sie die Registerkarte Übersicht an

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.

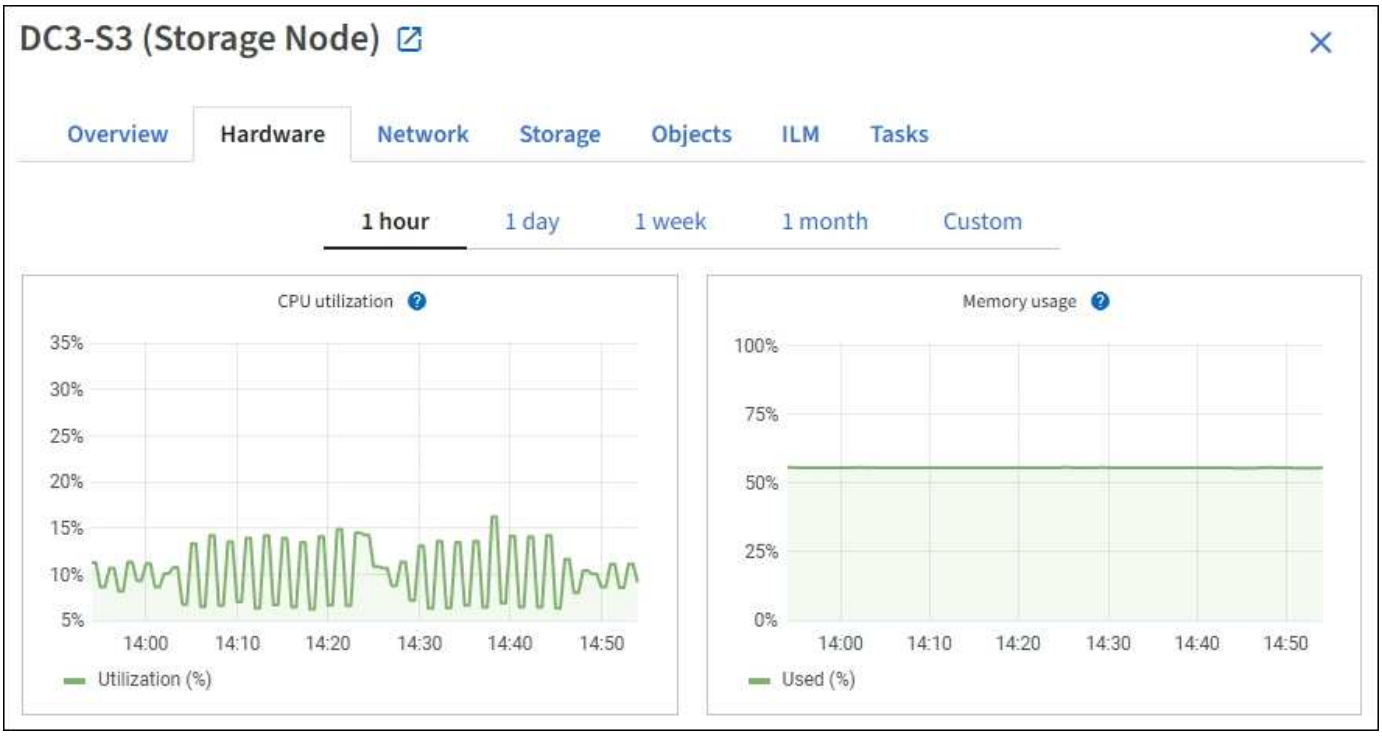
Warnungen sind auch für enthalten"Status der Node-Verbindung".

## 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.

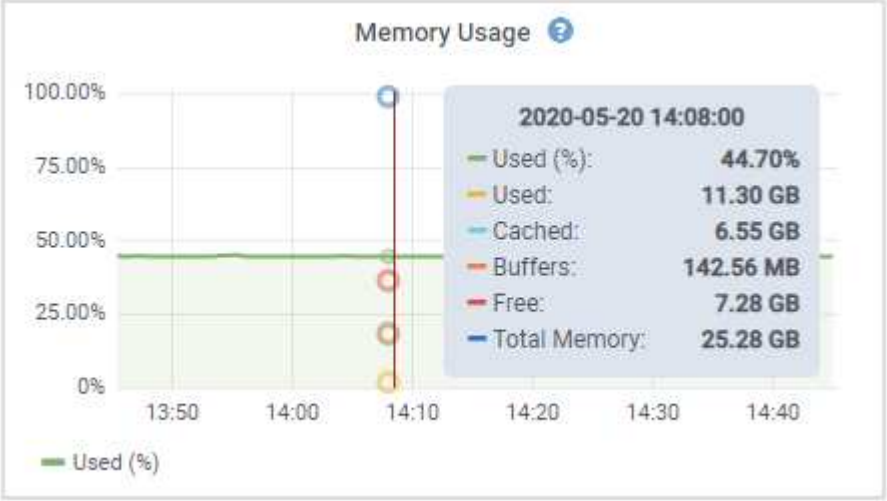
> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispielbildern auf dieser Seite überein.

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

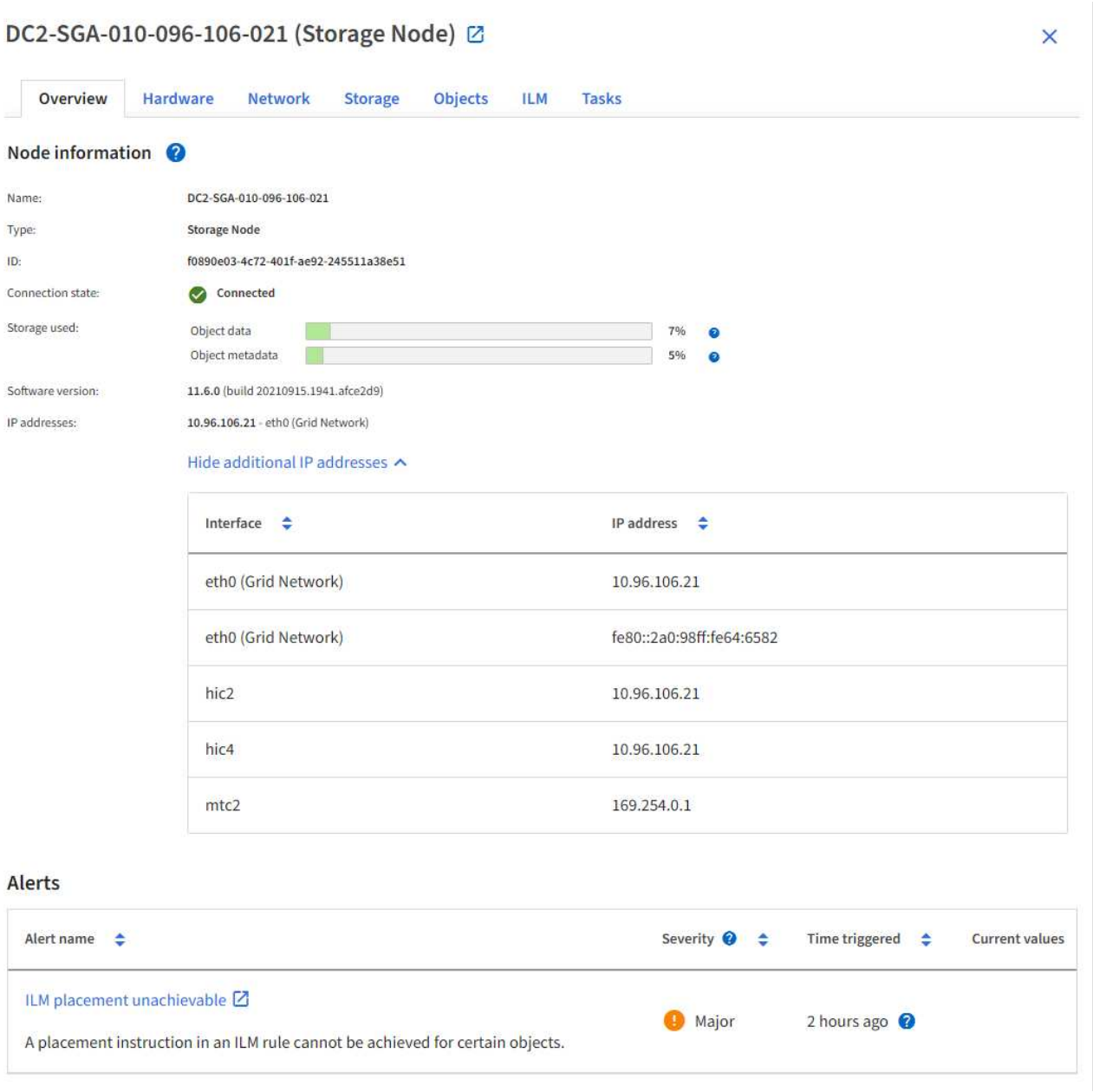
Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplattengeräte- und Netzwerkressourcen für jeden Appliance Storage Node aufgeführt. Außerdem können Sie den Arbeitsspeicher, die Storage-Hardware, die Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen,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

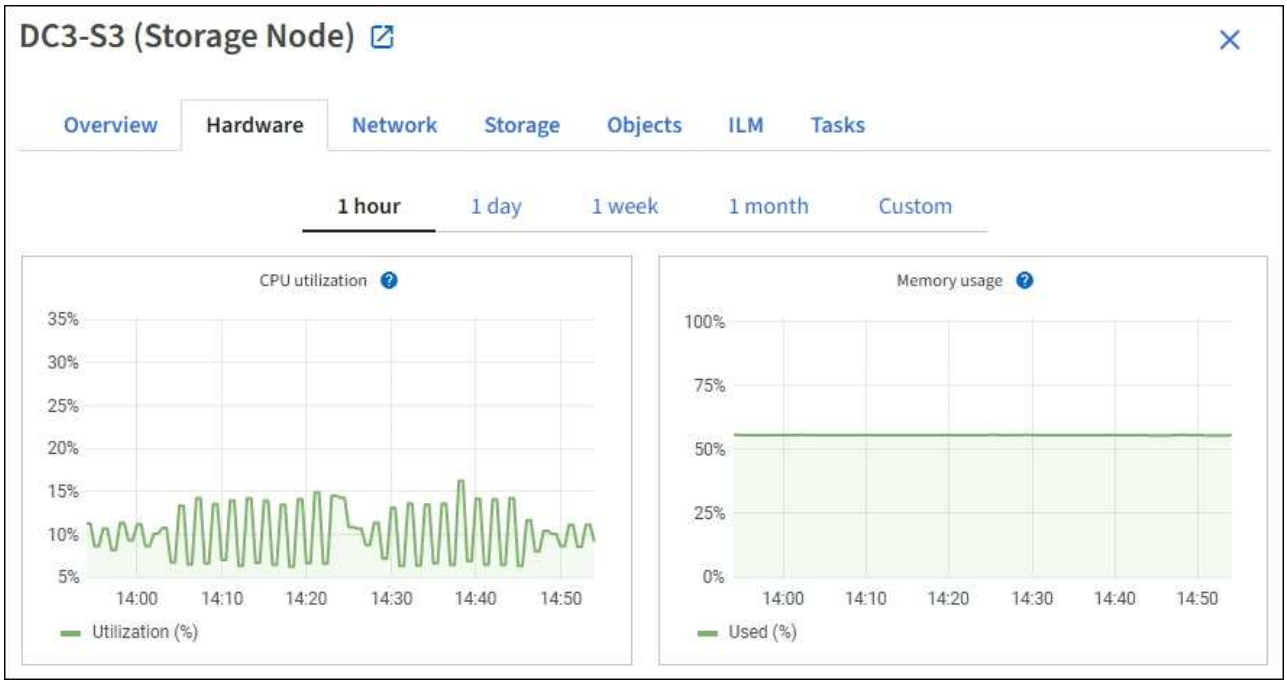
   - **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk.
   - **Hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID-Grid-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
   - **mtc**: 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.

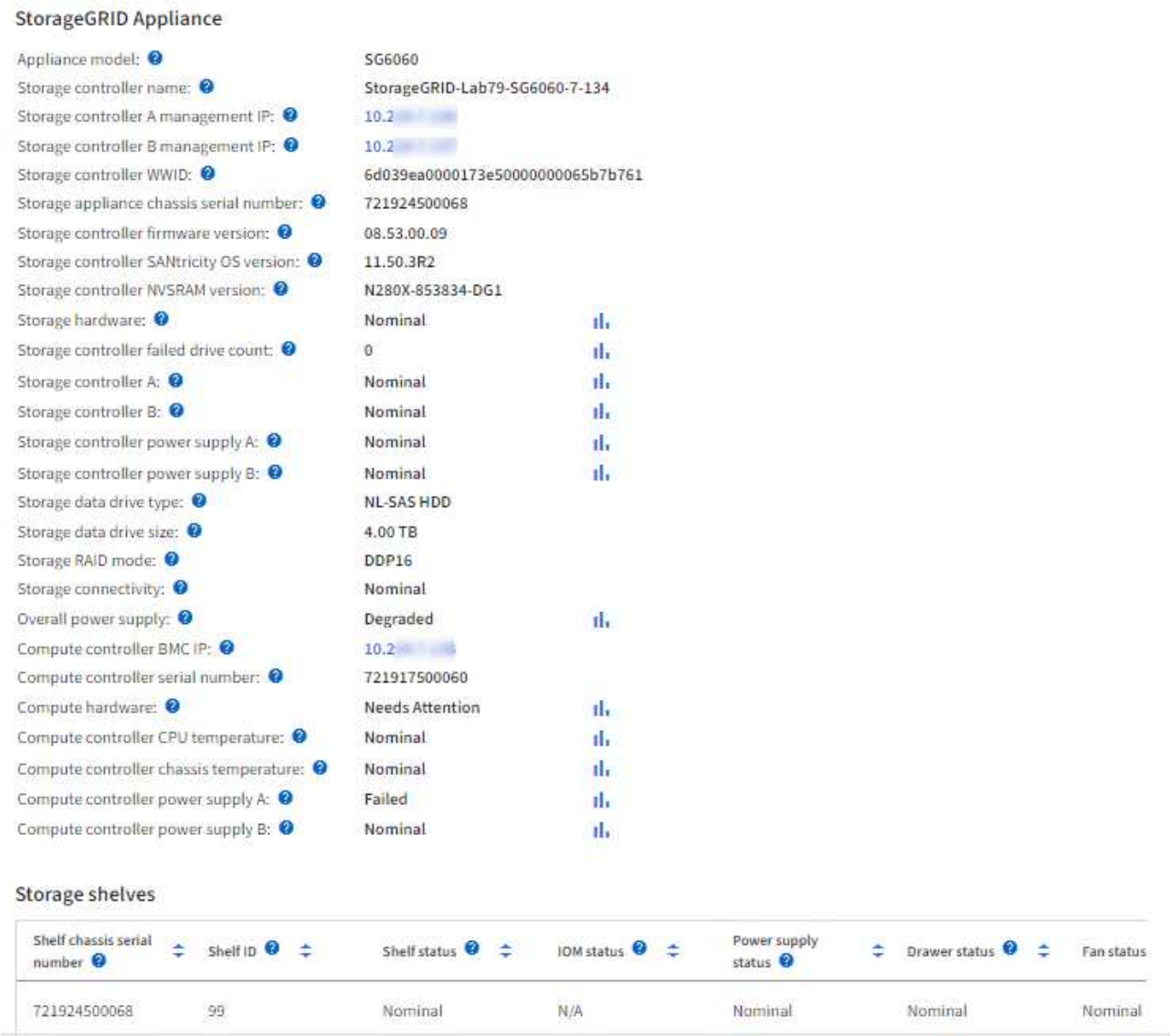
   a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren 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.<br><br>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.<br><br>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.<br><br>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.<br><br>Beim SG6160 wird auch die Größe des Cache-Laufwerks angezeigt.<br><br>**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.<br><br>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. |

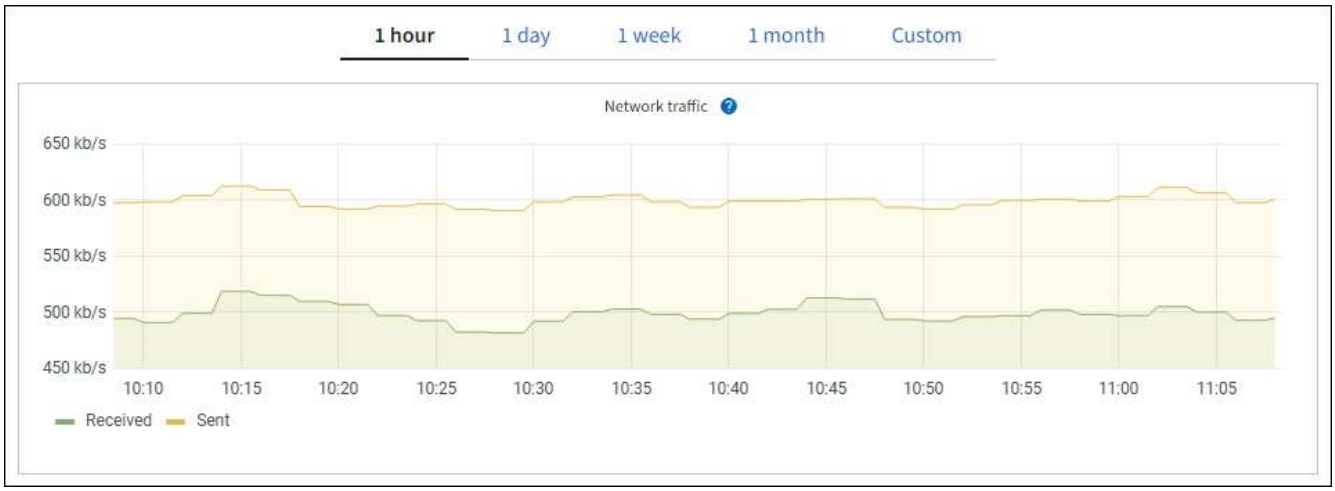
| Spalte in der Tabelle „Storage Shelfs“ | Beschreibung |
|---|---|
| Shelf-ID | Die numerische Kennung für das Storage-Shelf.<br>• 99: Storage Controller Shelf<br>• 0: Erstes Erweiterungs-Shelf<br>• 1: Zweites Erweiterungs-Shelf<br>**Hinweis:** Erweiterungseinschübe gelten nur für die SG6060 und SG6160. |
| 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.

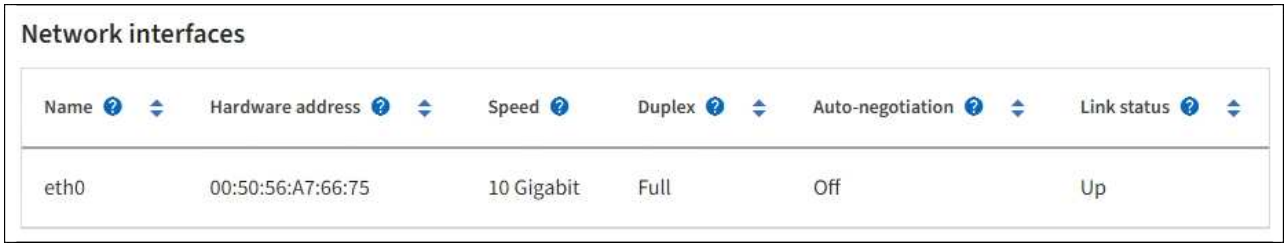
   Wenn ein Status nicht „nominal“ lautet, prüfen Sie alle aktuellen Warnmeldungen. Weitere Informationen zu einigen dieser Hardware-Werte finden Sie auch mit SANtricity System Manager. Informationen zur Installation und Wartung des Geräts finden Sie in den Anweisungen.

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.

**Network communication**

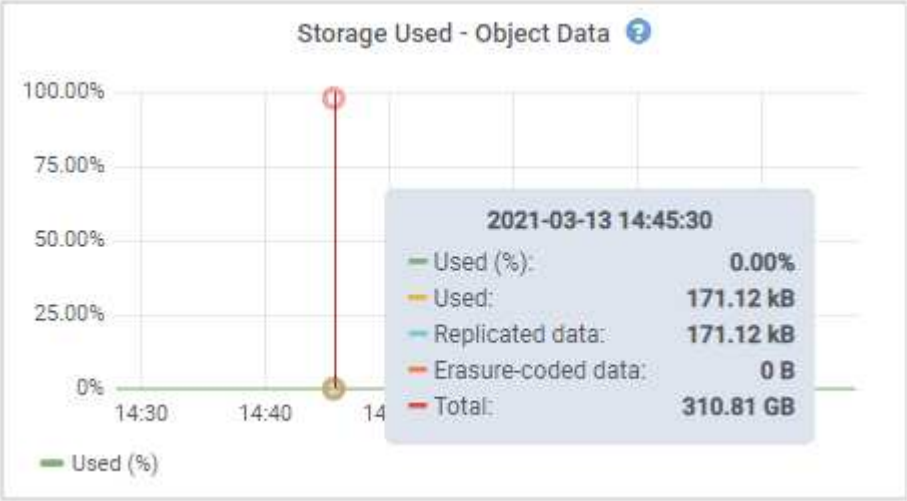
Receive

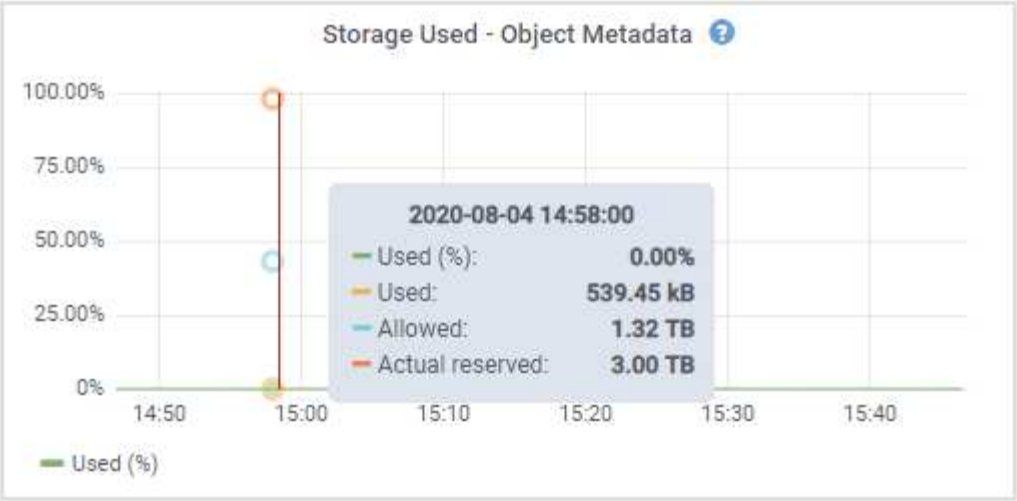
| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 |

Transmit

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

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.

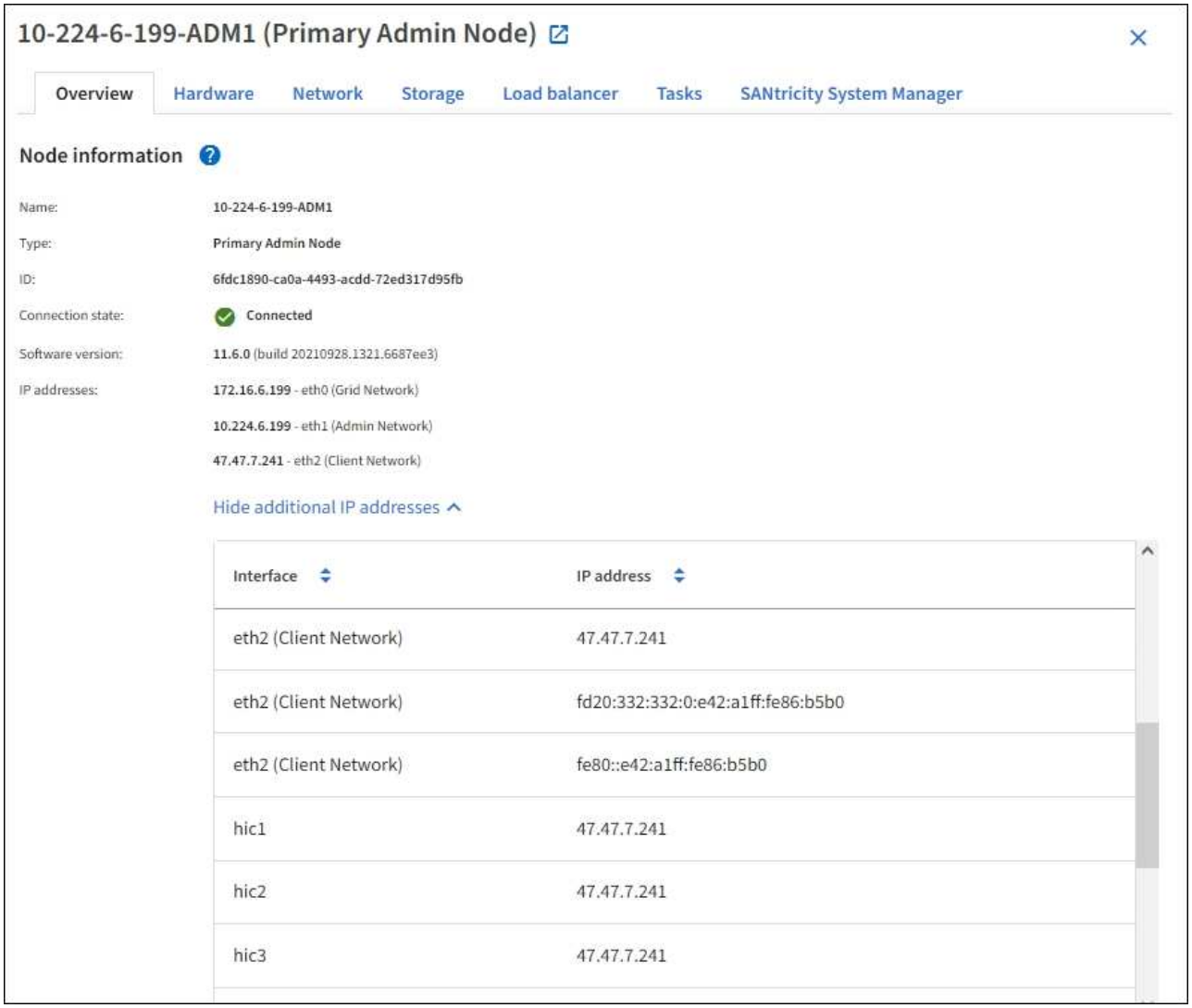
#### Schritte

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.

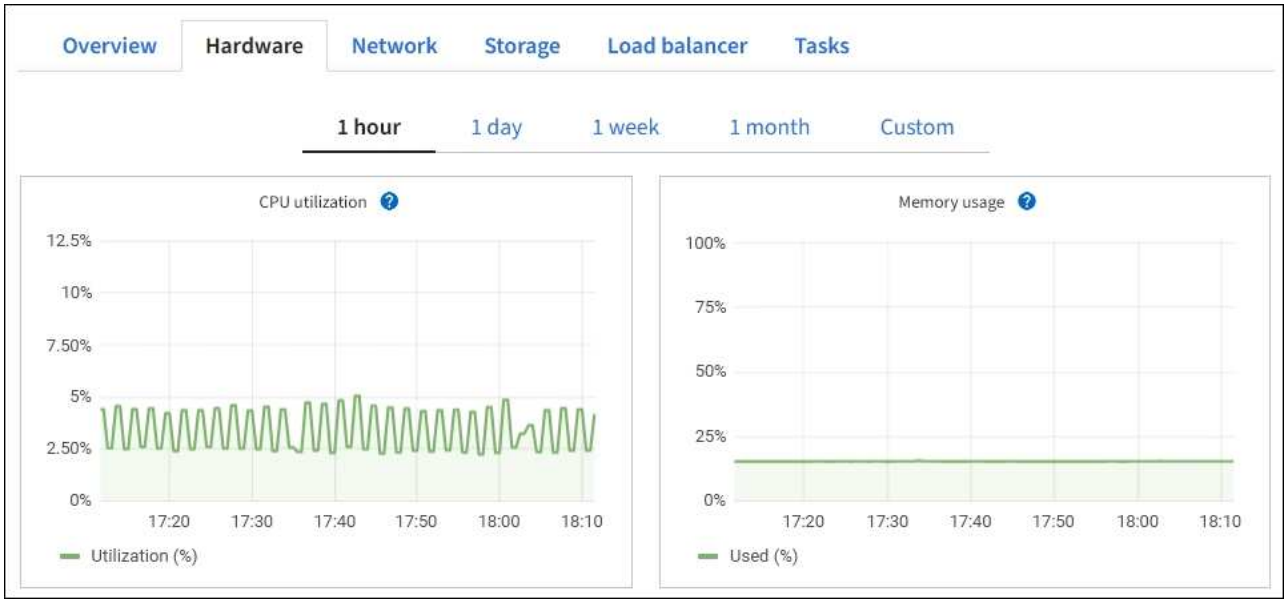



Im Abschnitt „Meldungen“ der Registerkarte „Übersicht“ werden alle aktiven Meldungen für den Node angezeigt.

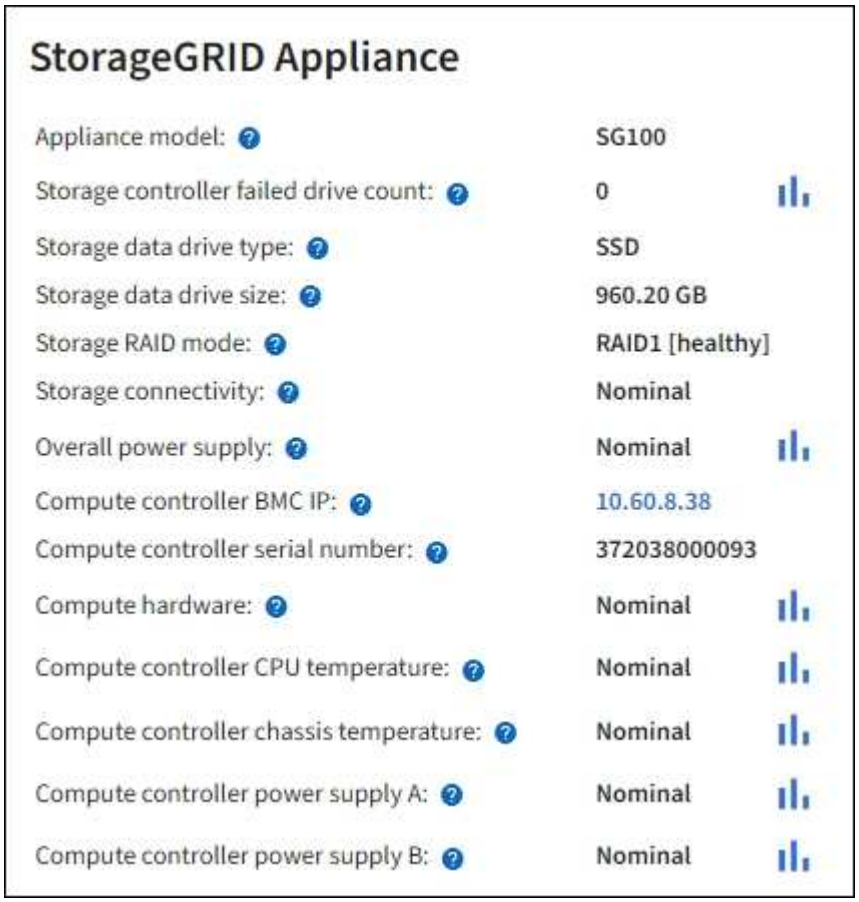
3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.

   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.



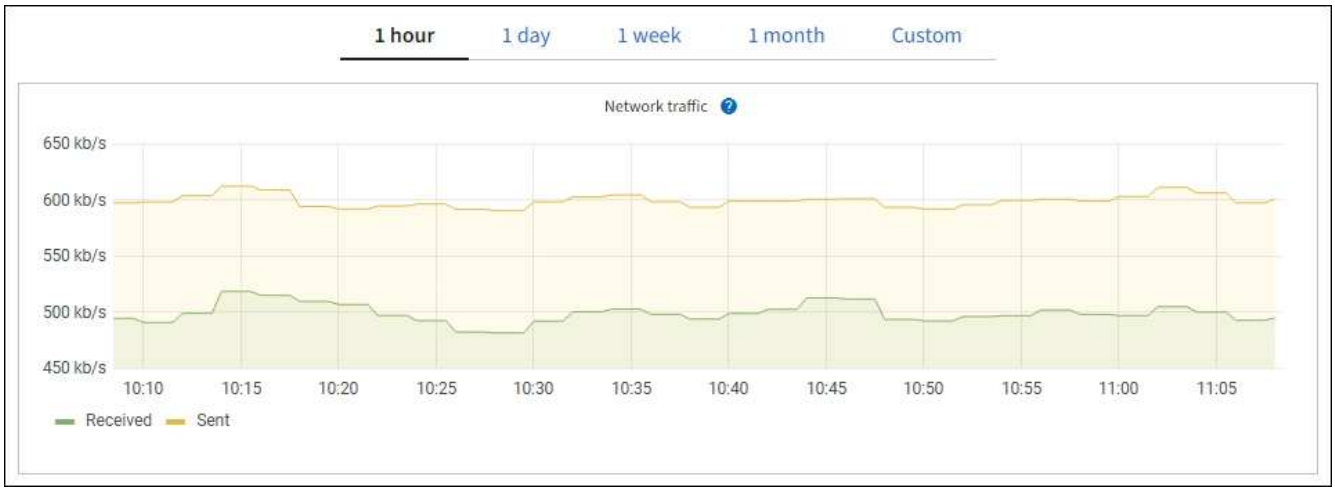
| Feld in der Appliance-Tabelle | Beschreibung |
| --- | --- |
| Appliance-Modell | Die Modellnummer für diese StorageGRID Appliance. |
| Anzahl der Laufwerke bei Ausfall des Storage-Controllers | Die Anzahl der Laufwerke, die nicht optimal sind. |
| Typ des Speicherdatenspeichers | Der Laufwerkstyp 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.<br><br>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 |

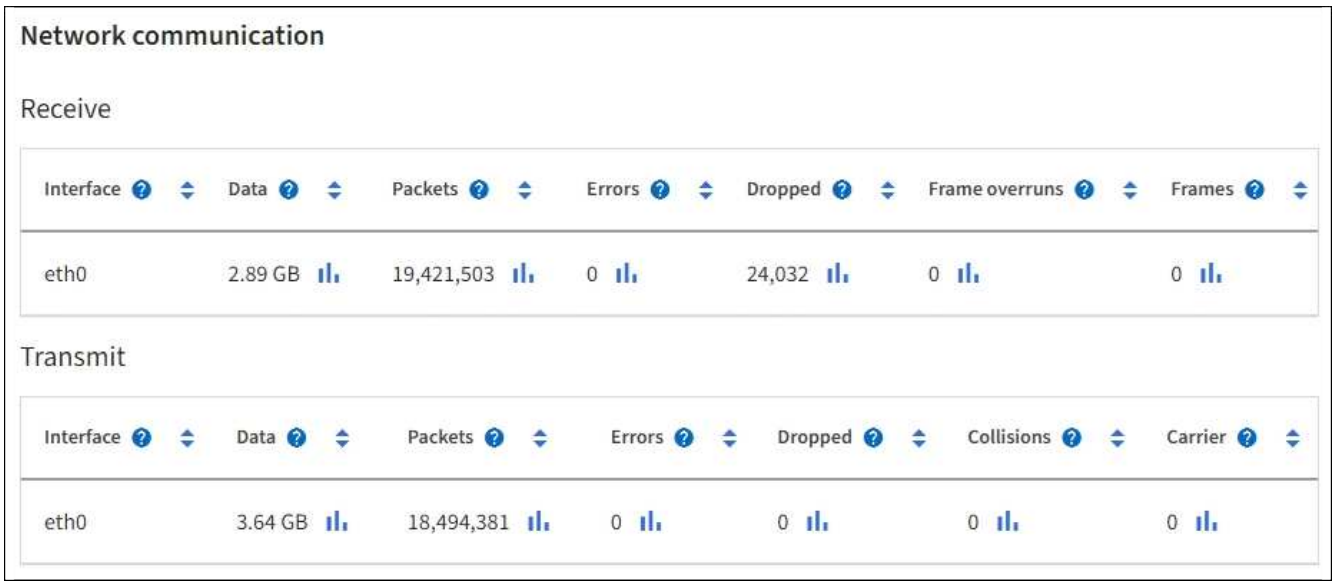
Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle Netzwerkschnittstellen, um festzustellen, ob die vier 40/100-GbE-Netzwerkanschlüsse auf der Appliance für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.

> 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.



**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 |

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

DO-REF-DC1-GW1 (Gateway Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks

**Disk devices**

| Name | World Wide Name | I/O load | Read rate | Write rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.02% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.03% | 0 bytes/s | 6 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 | 84.63 GB | Unknown |

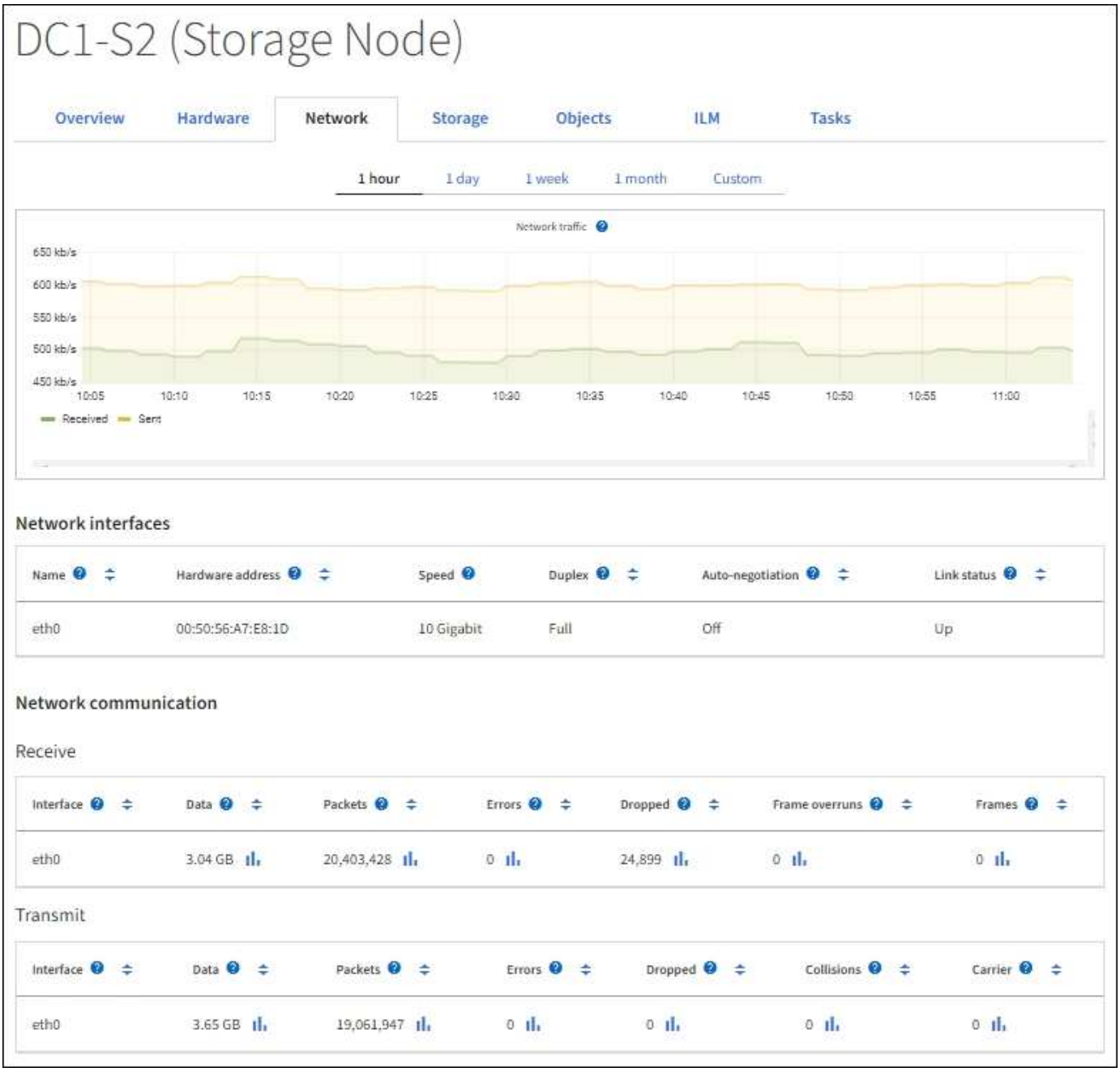
## Zeigen Sie die Registerkarte Netzwerk an

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“

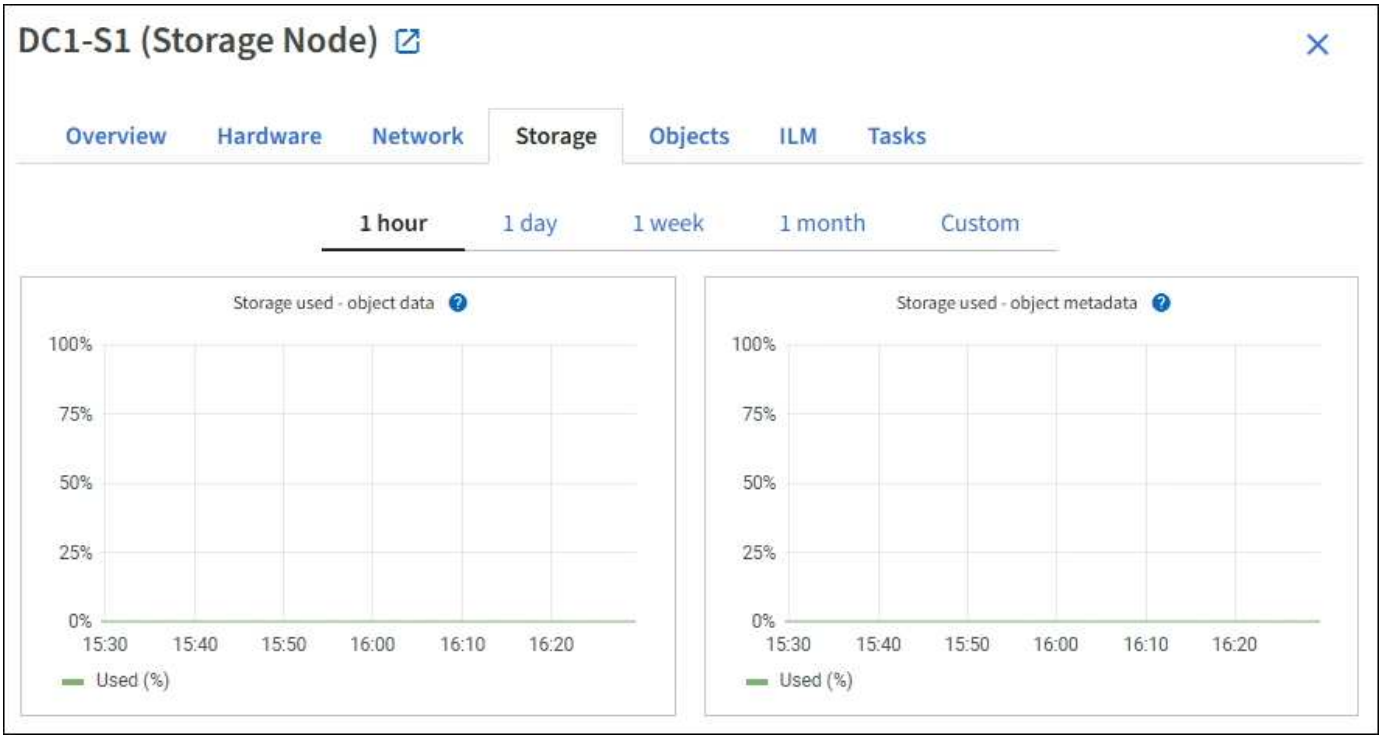
Die Registerkarte „Storage“ fasst Storage-Verfügbarkeit und andere Storage-Metriken zusammen.

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 |

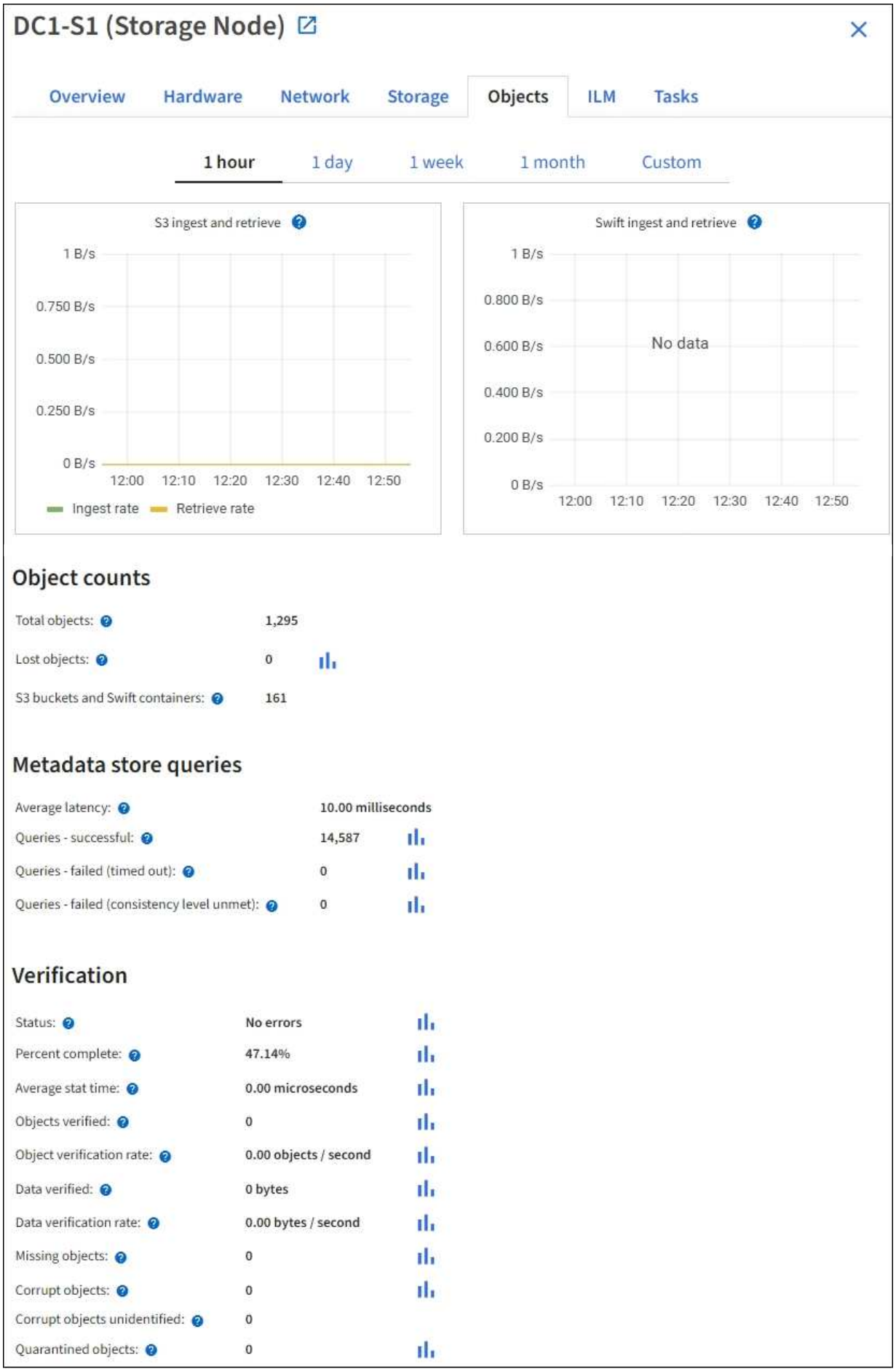
**Verwandte Informationen**

"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.

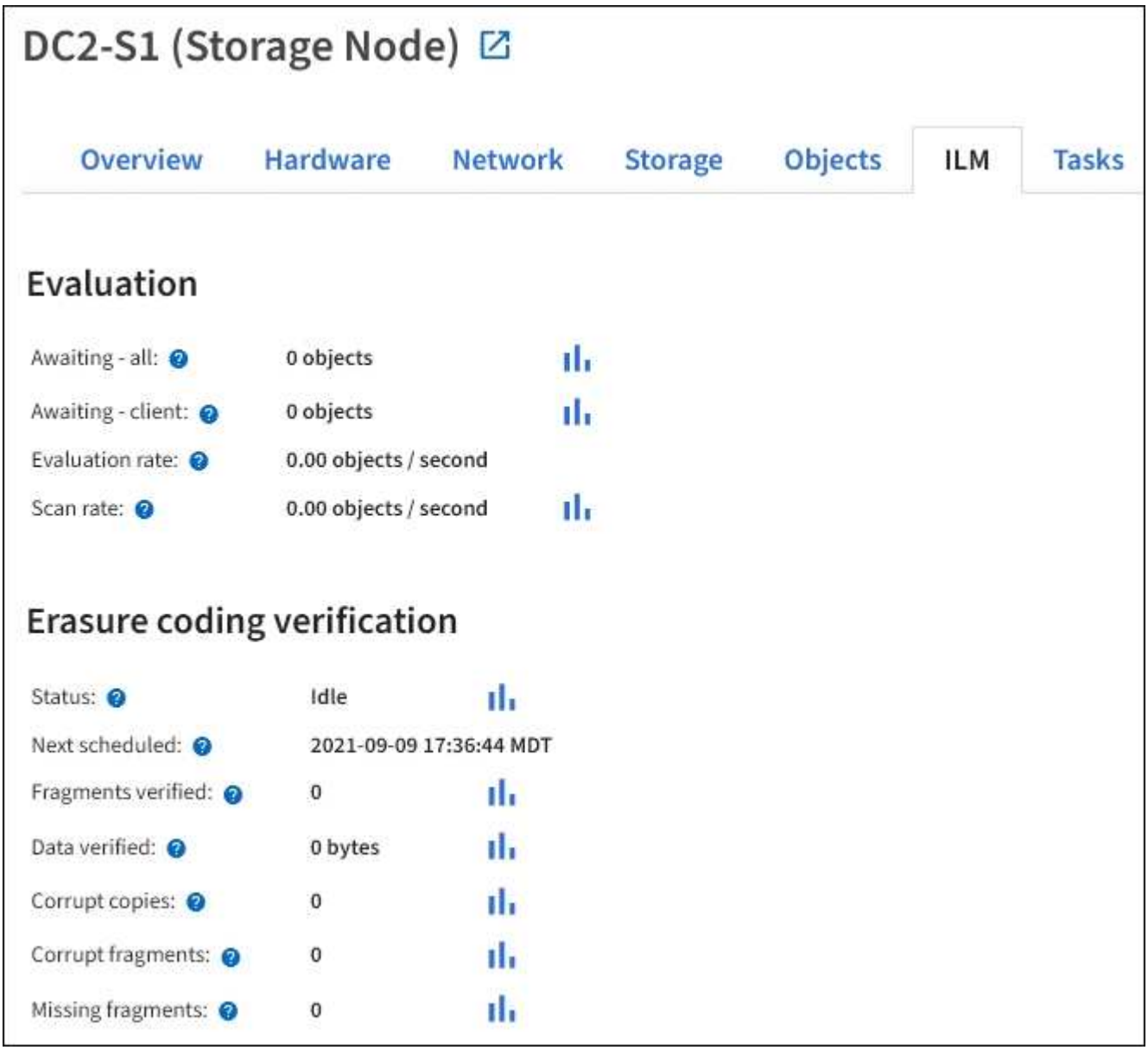

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

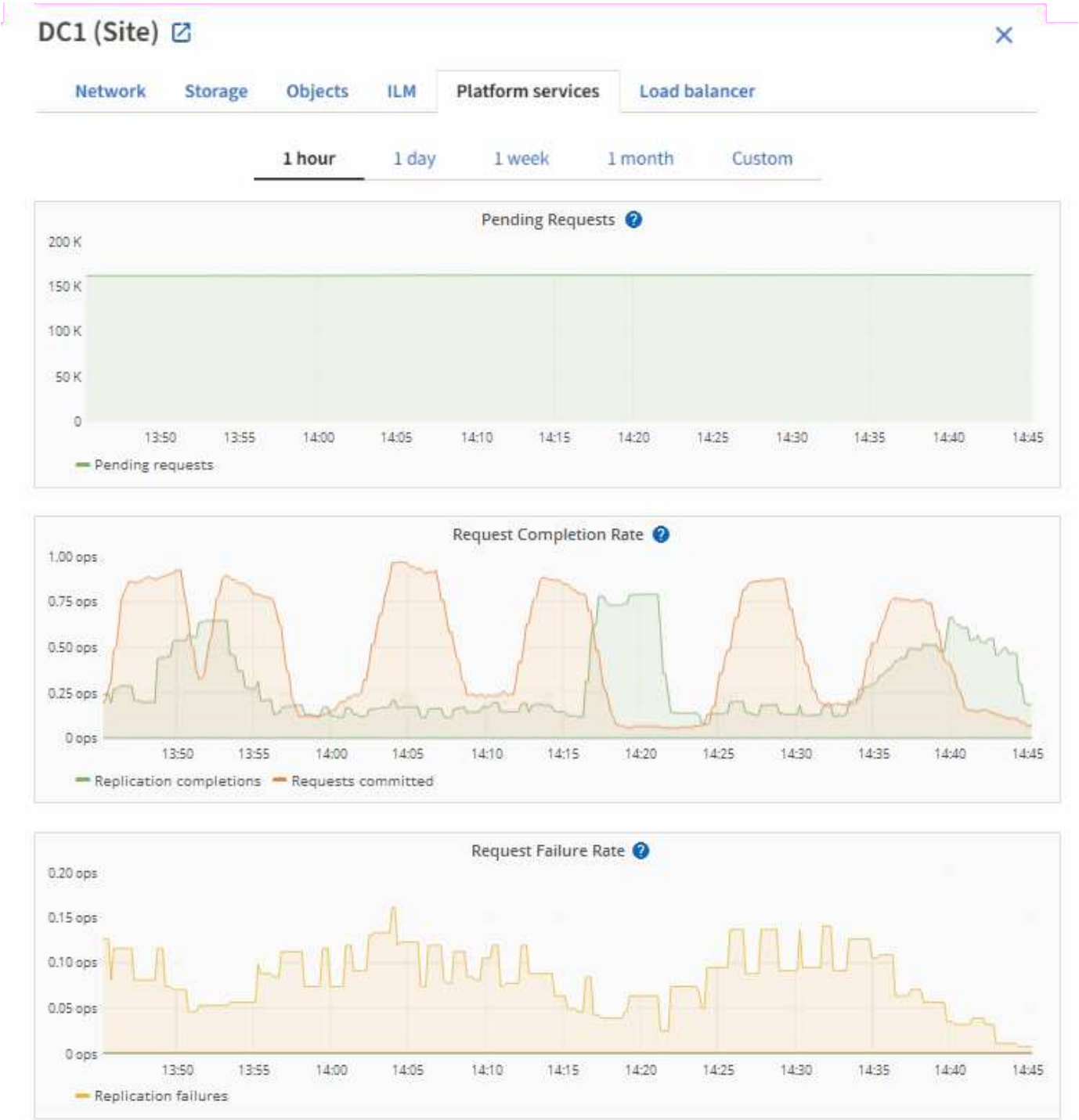
#### Verwandte Informationen

- "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:

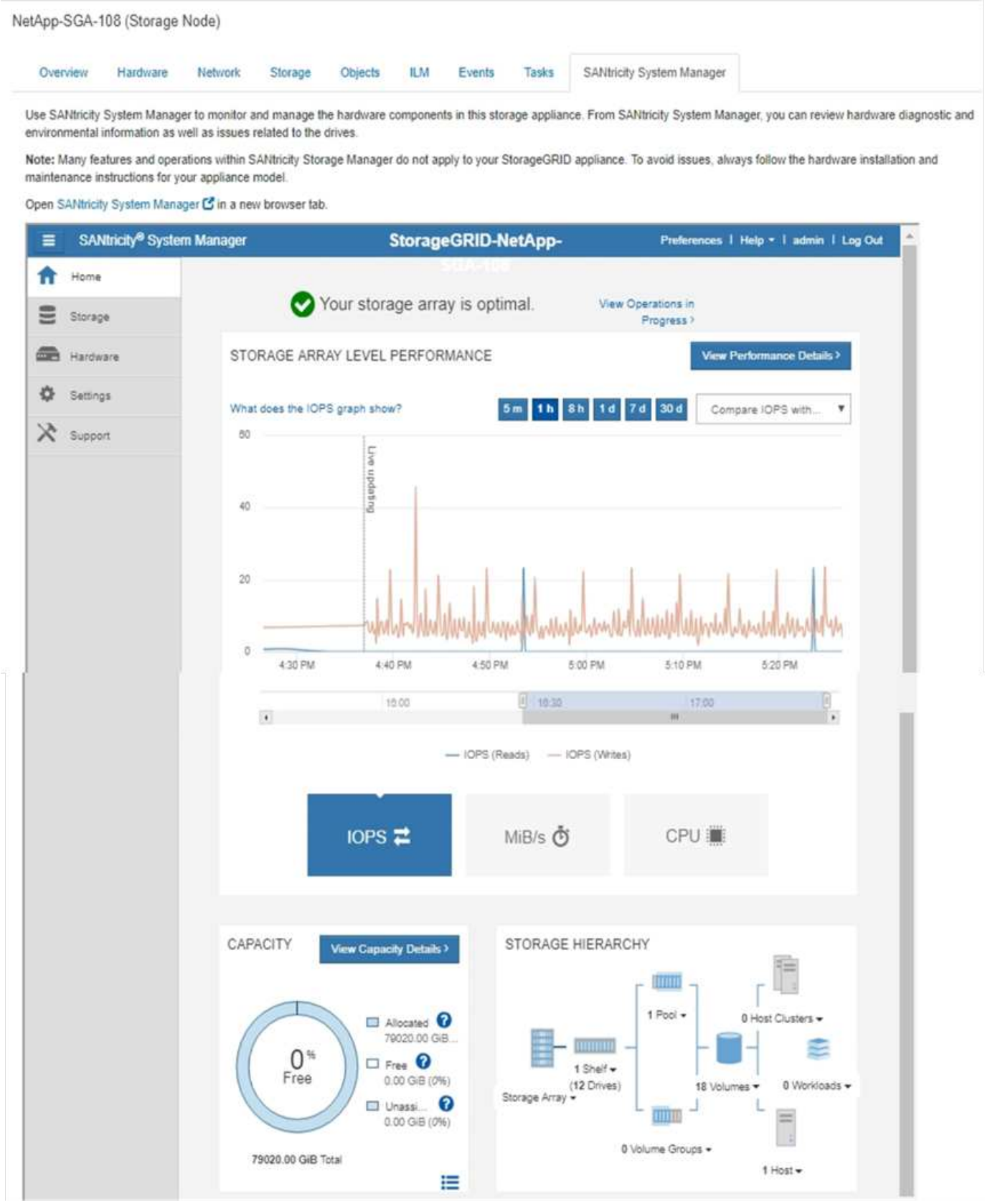
- Anzeige von Performance-Daten wie Performance auf Storage-Array-Ebene, I/O-Latenz, CPU-Auslastung des Storage-Controllers und Durchsatz
- Überprüfen Sie den Status der Hardwarekomponenten.
- Durchführung von Support-Funktionen, einschließlich Anzeige von Diagnosedaten und Konfiguration der E-Series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

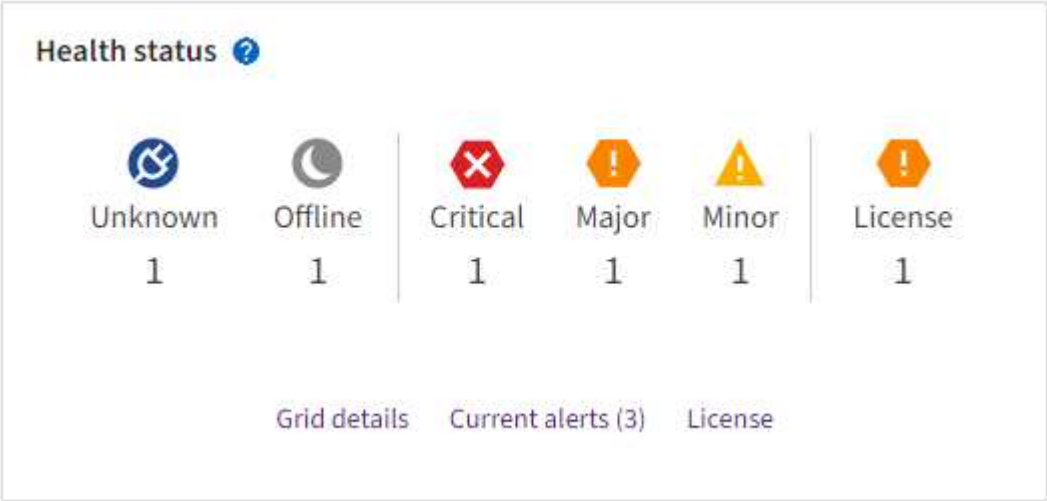
Überwachen Sie täglich den Gesamtzustand Ihres StorageGRID Systems.

### 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**<br><br>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.<br><br>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.<br><br>Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten.<br><br>**Hinweis**: Ein Knoten kann während des verwalteten Herunterfahrens als Unbekannt erscheinen. In diesen Fällen können Sie den Status Unbekannt ignorieren. |
| | **Nicht verbunden - Administrativ unten**<br><br>Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden.<br><br>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.<br><br>Aufgrund des zugrunde liegenden Problems sind diese Nodes oft ohne Eingriff wieder online. | Ermitteln Sie, ob Warnmeldungen Auswirkungen auf diesen Node haben.<br><br>Wenn eine oder mehrere Warnungen aktiv sind, Wählen Sie jede Warnmeldung aus und befolgen Sie die empfohlenen Maßnahmen. |
| | • Verbunden*<br><br>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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>**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.

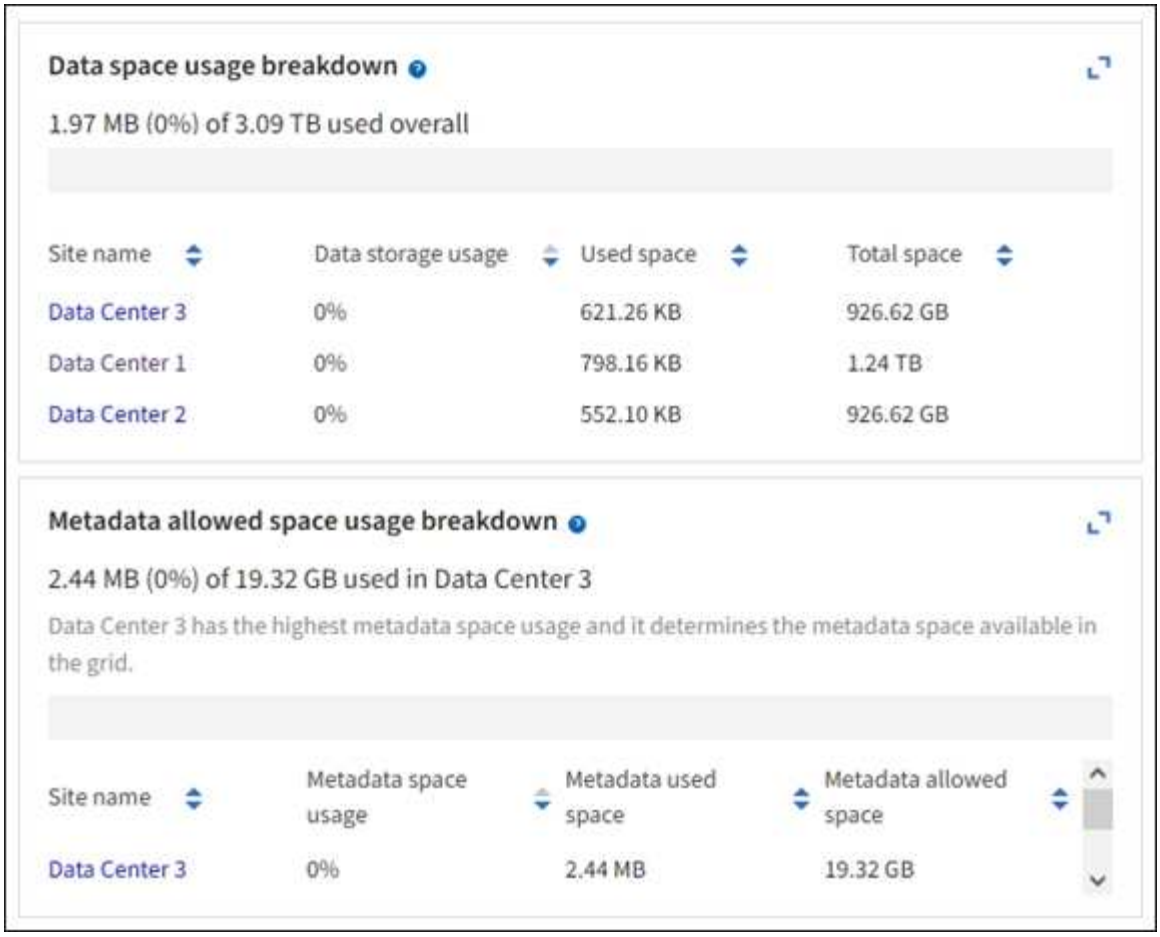
#### Schritte

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

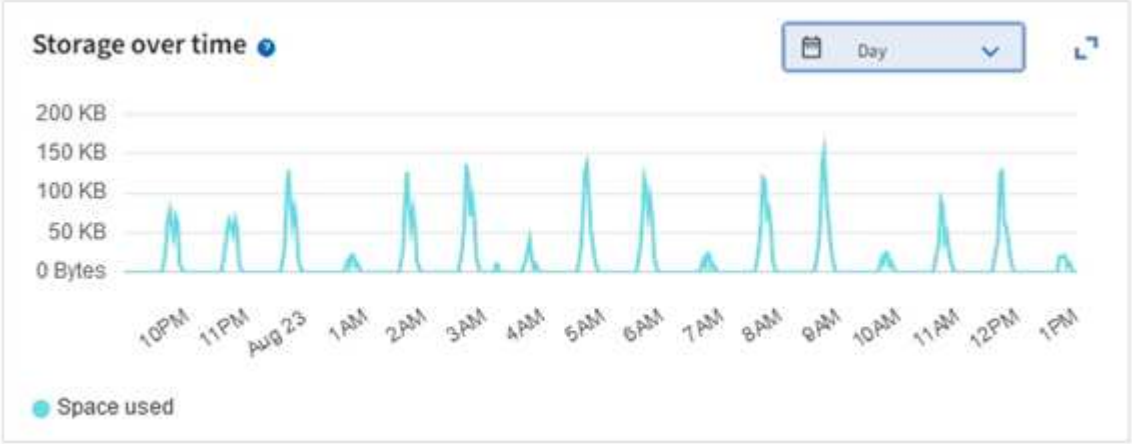
    a. Wählen Sie **Dashboard > Übersicht**.

    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.

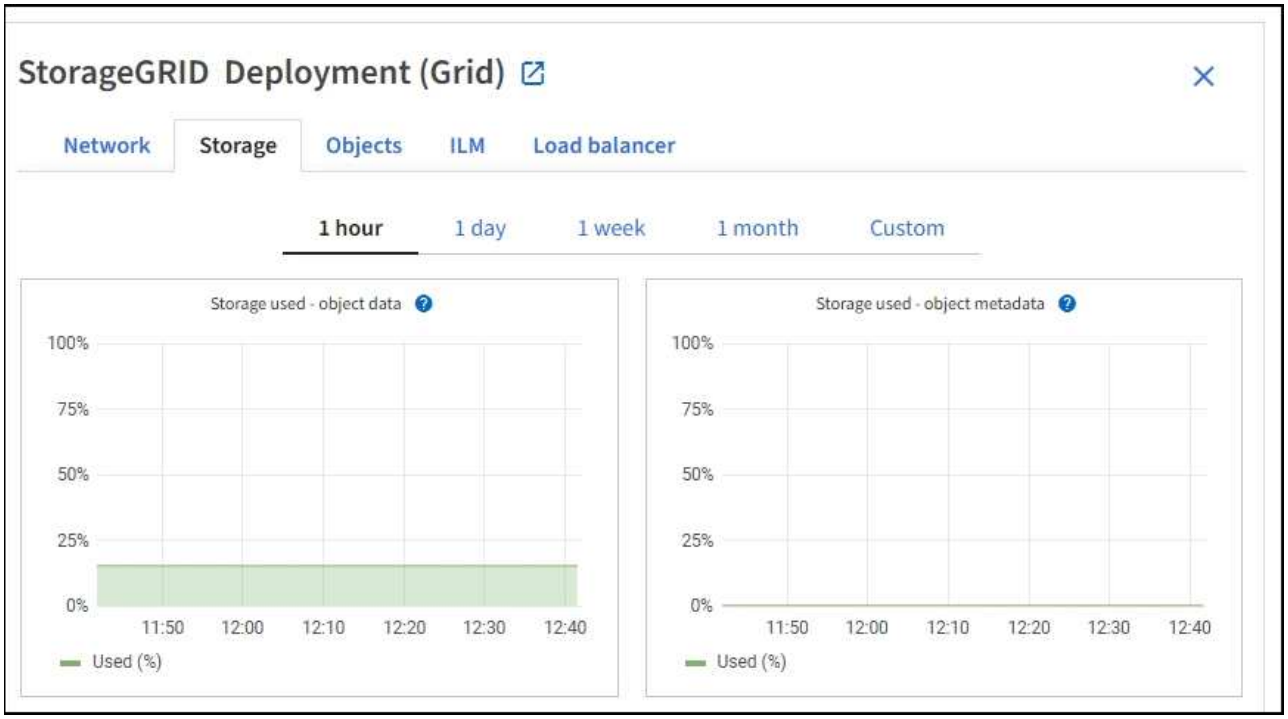
    > Die Zusammenfassung enthält keine Archivierungsmedien.




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.

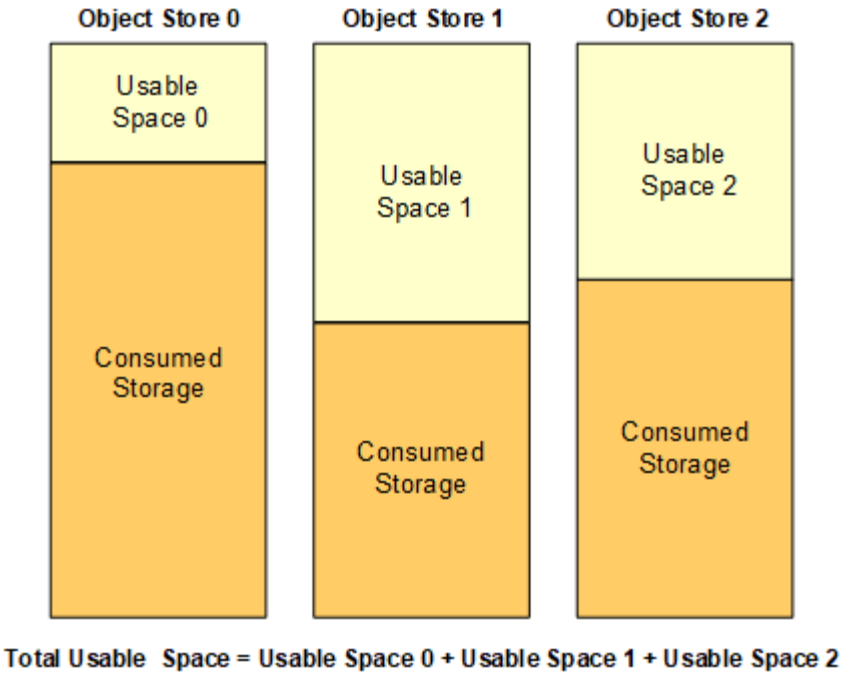
   Weitere Informationen zur Planung einer Speichererweiterung finden Sie im "Anweisungen zur Erweiterung von StorageGRID".

### 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**

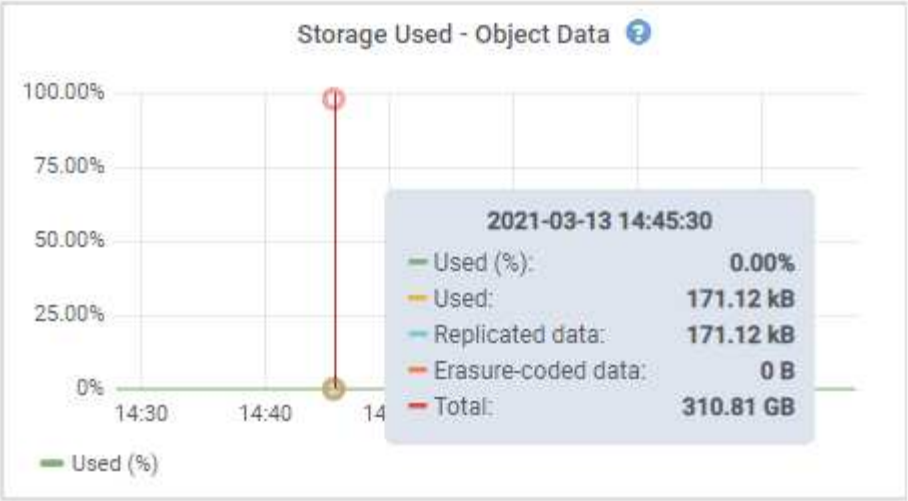
1. Wählen Sie **Knoten** > ***Speicherknoten*** > **Speicher**.

   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

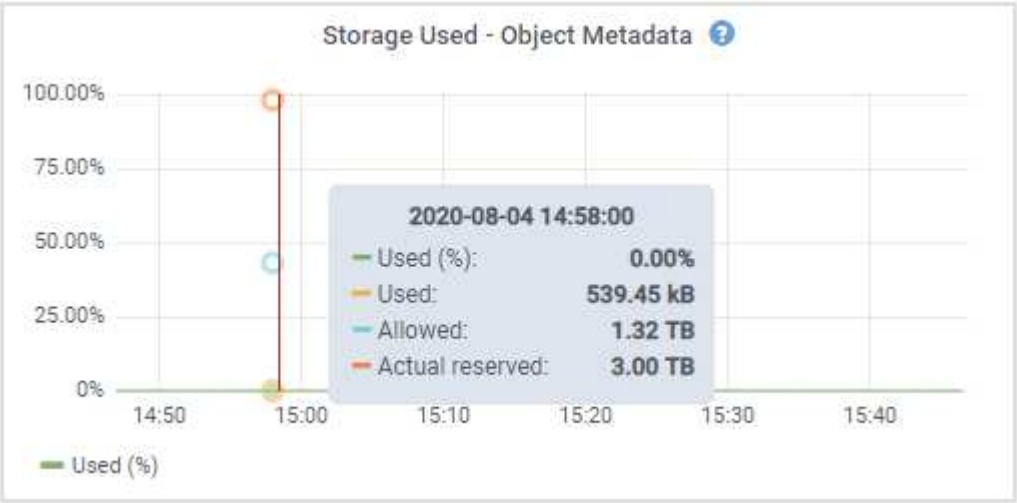
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage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

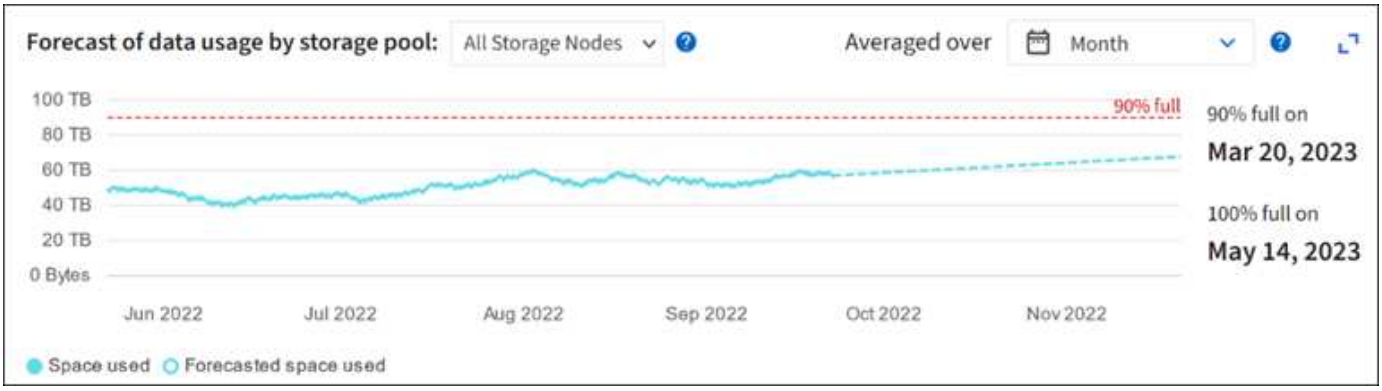
Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie einen kürzeren Bereich aus dem Pulldown-Menü **gemittelt über** aus, um nur die neuesten Aufnahmemuster wiederzugeben. Wenn Sie saisonale Muster bemerken, wählen Sie einen längeren Bereich aus.

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.

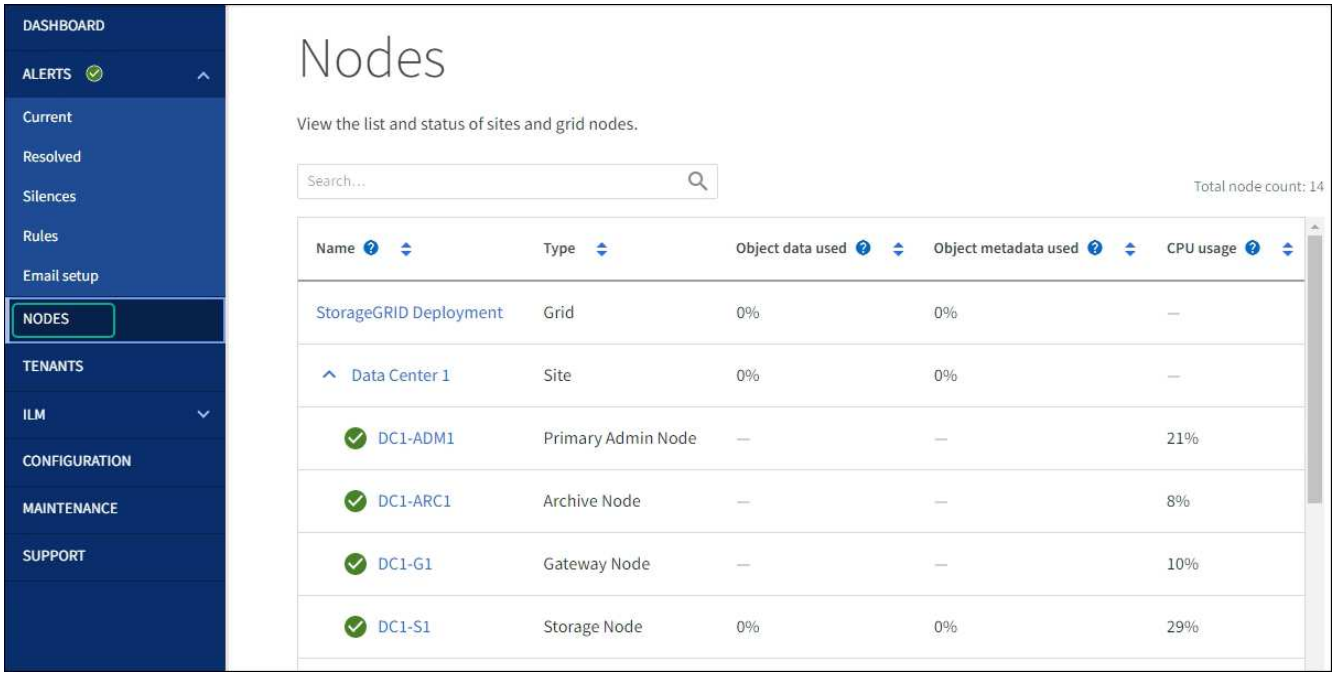
Überwachen Sie die Konnektivität und die Netzwerk-Performance mit dem Grid Manager, damit Sie bei Problemen umgehend auf Probleme reagieren können.

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**

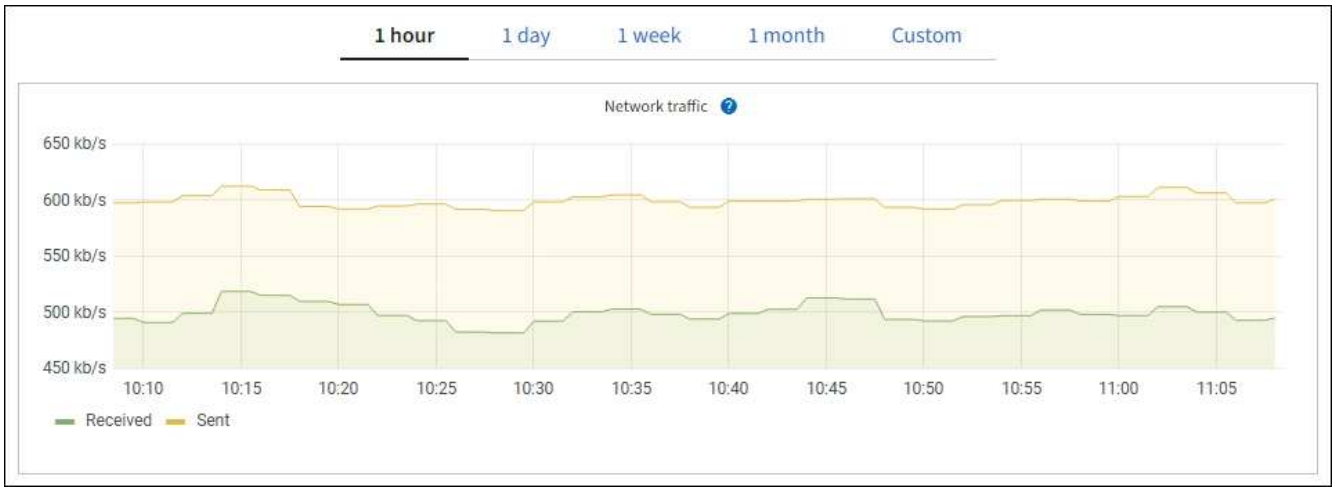
1. Wählen Sie **Knoten** aus.

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

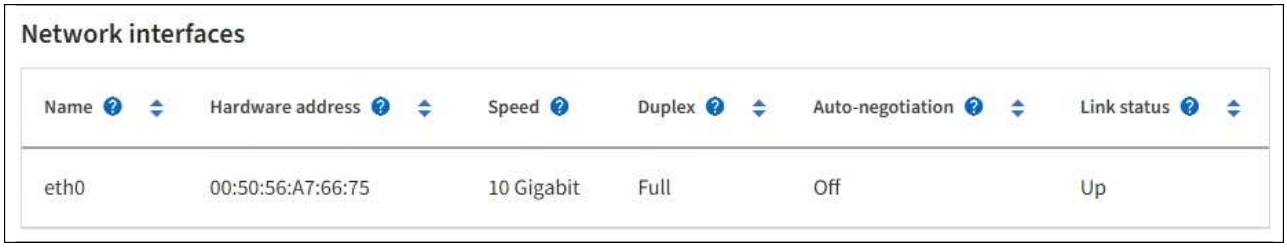



2. Wählen Sie den Grid-Namen, einen bestimmten Datacenter-Standort oder einen Grid-Node aus, und wählen Sie dann die Registerkarte **Netzwerk** aus.

   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.

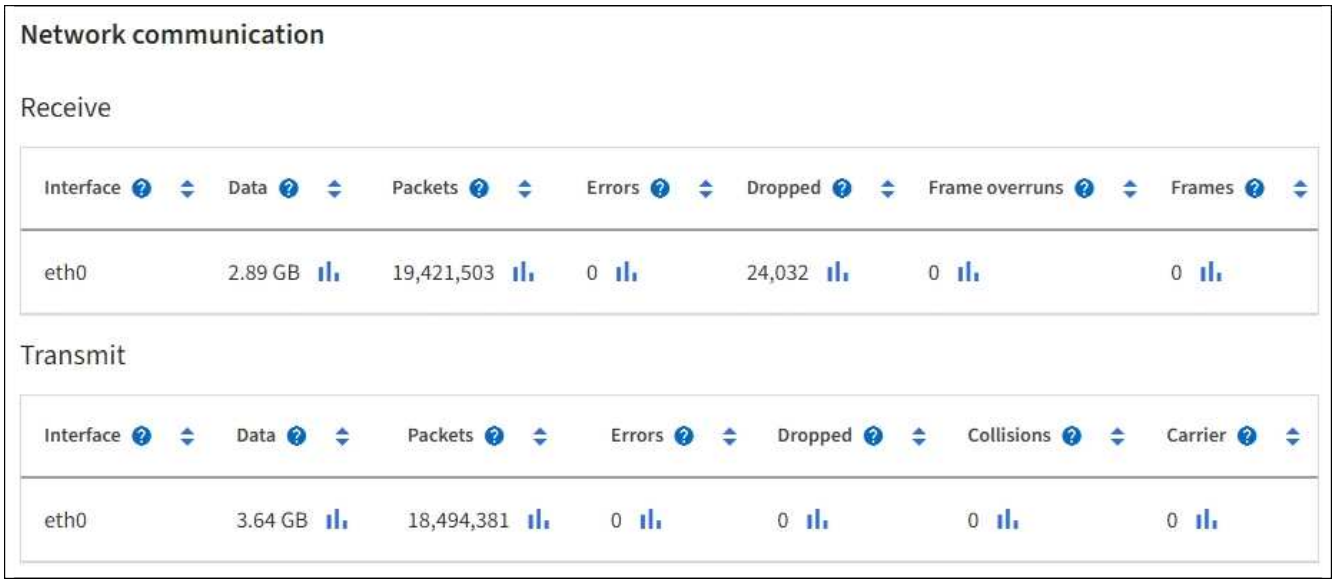


**Network interfaces**

| 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 |

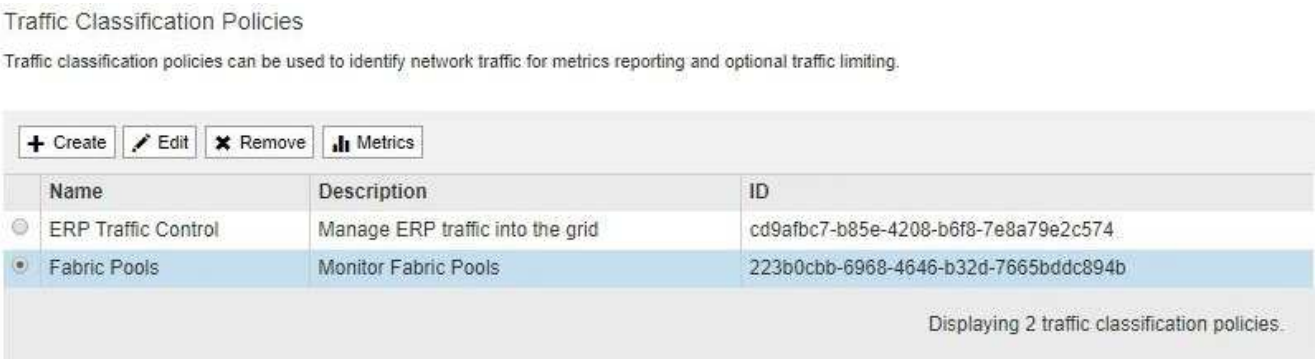
Transmit

| 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

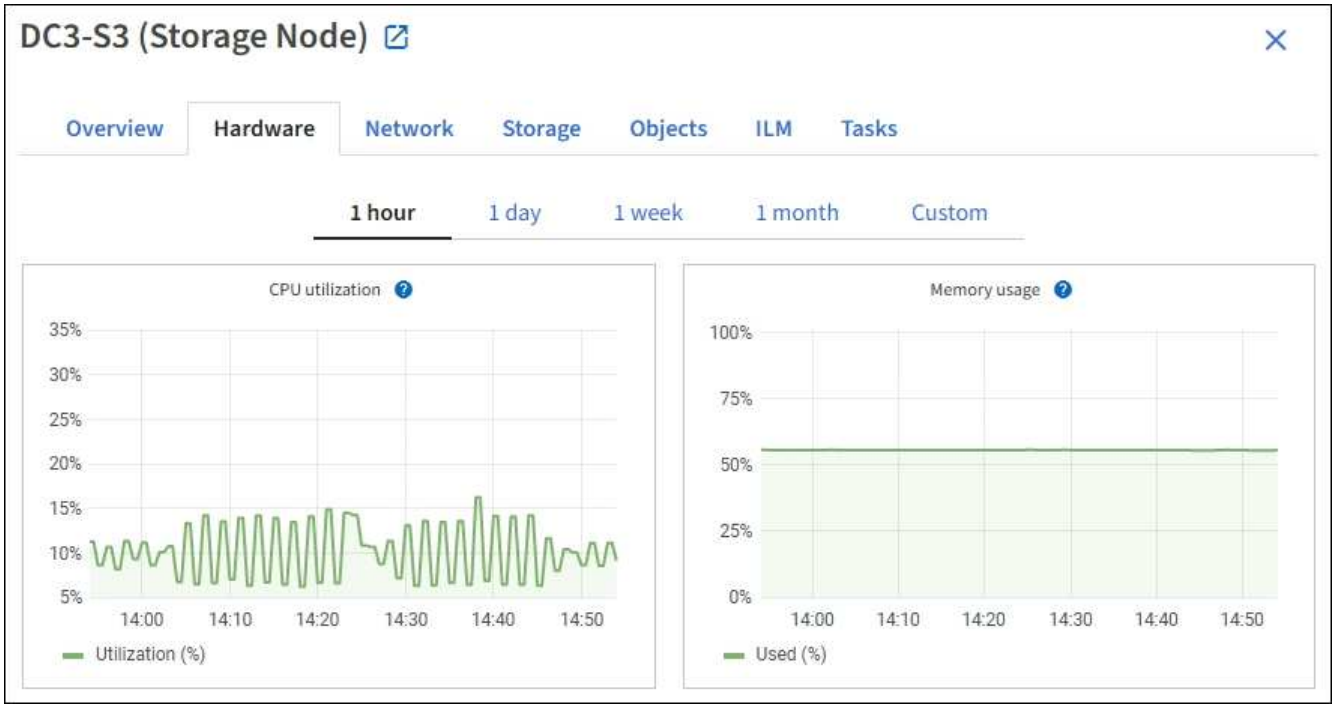
- "Zeigen Sie die Registerkarte Netzwerk an"
- "Überwachen Sie die Status der Node-Verbindung"

## 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

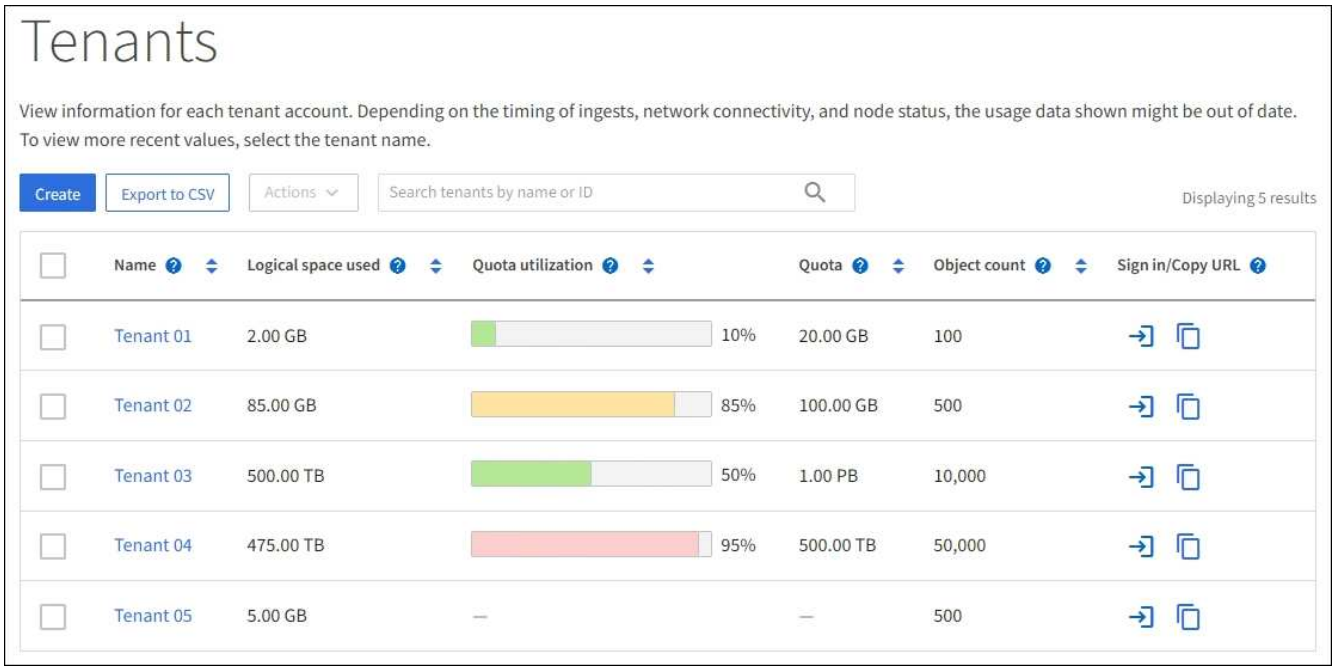
Auf der Seite Tenants werden grundlegende Informationen für alle aktuellen Mandantenkonten angezeigt.

**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.

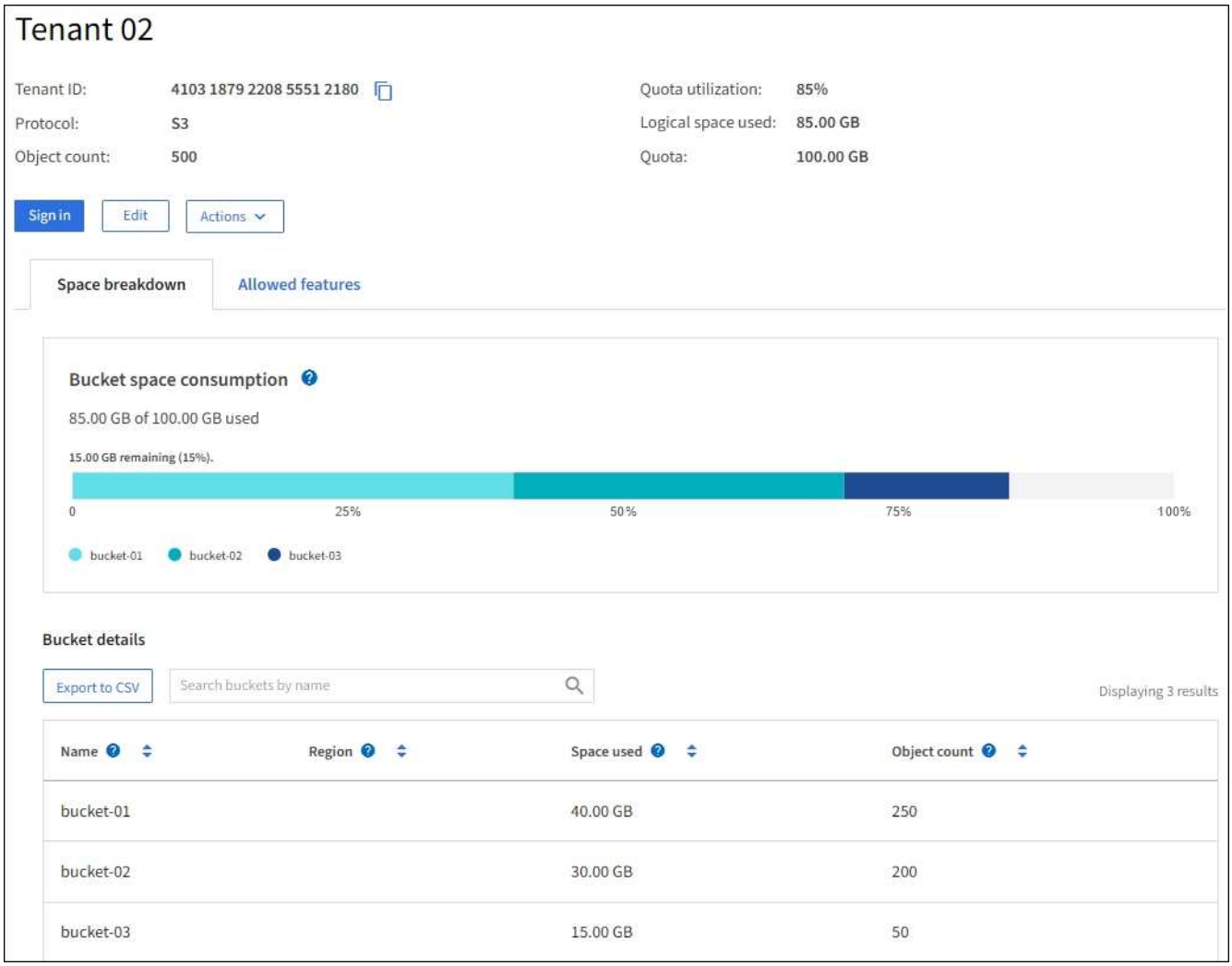
### Zeigen Sie eine bestimmte Serviceeinheit an

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.

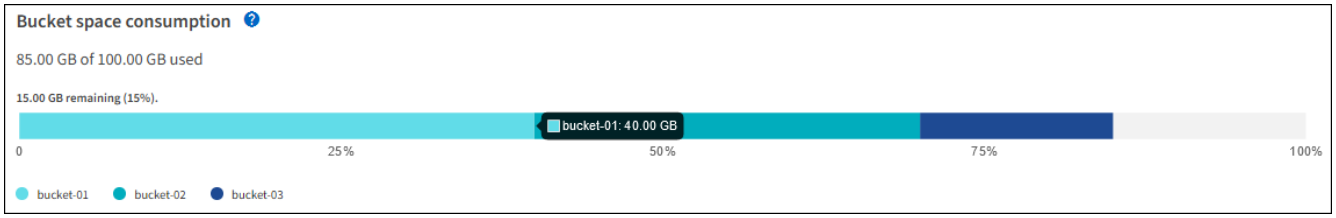
   > Die logische Größe aller Objekte, die zu diesem Mandanten gehören, umfasst unvollständige und laufende mehrteilige Uploads. Die Größe umfasst nicht den zusätzlichen physischen Speicherplatz, der für ILM-Richtlinien verwendet wird. Bei den Werten für den belegten Speicherplatz handelt es sich um Schätzungen.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

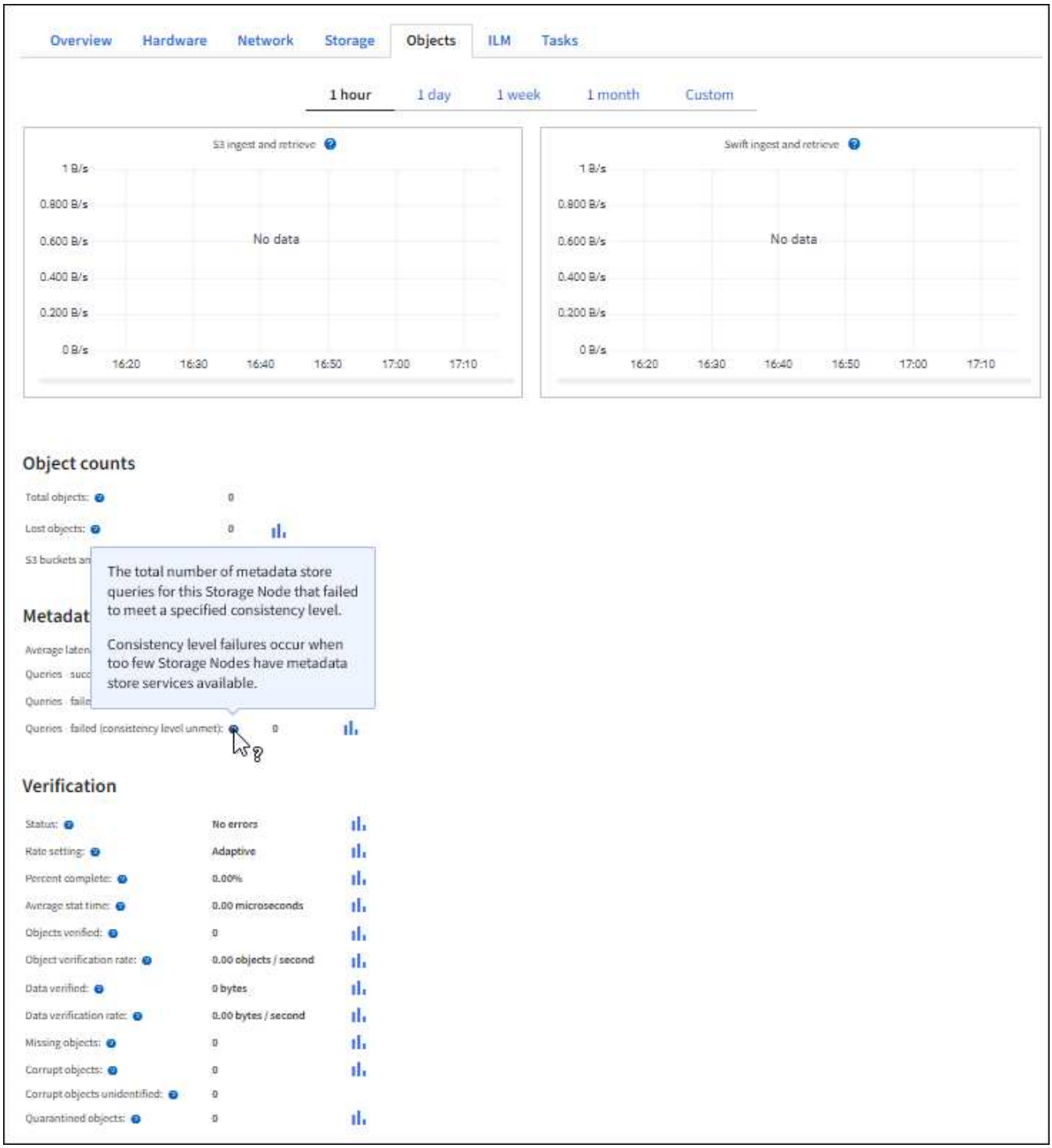
#### Schritte

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

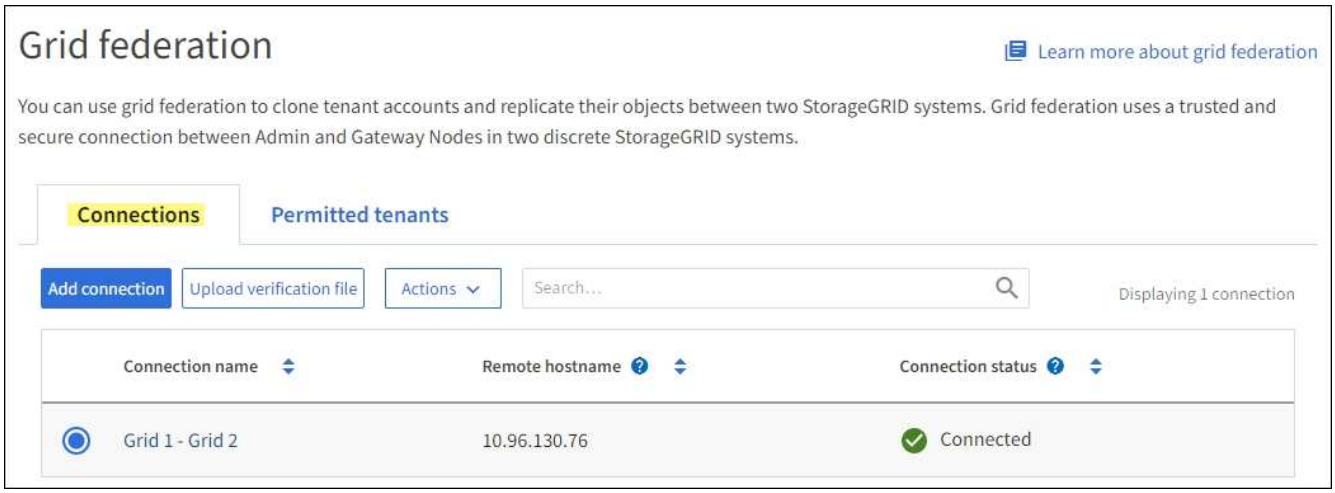
1. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.

   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:

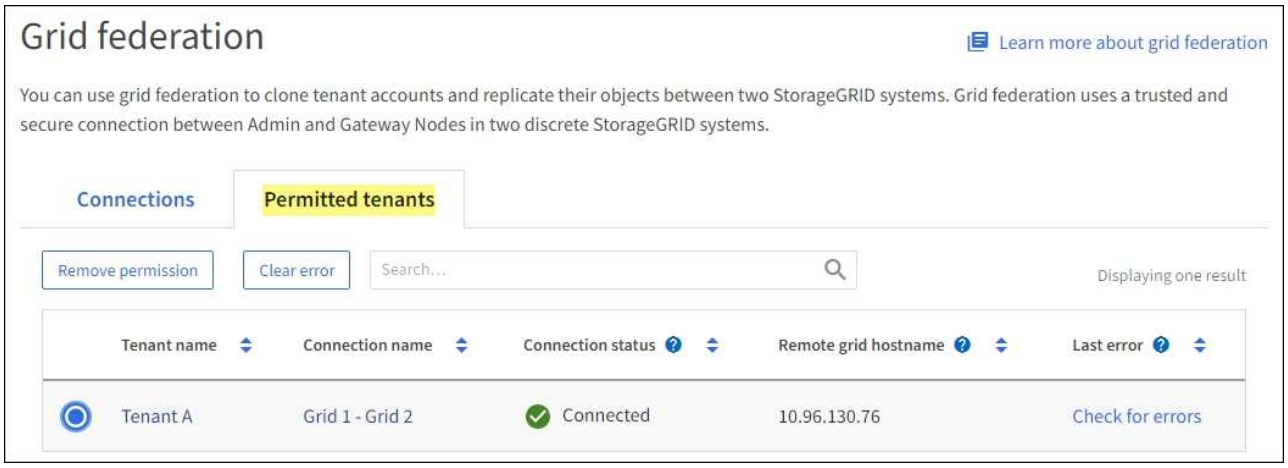
   - "Erstellen Sie eine neue Verbindung".
   - Wählen Sie eine vorhandene Verbindung zu "Bearbeiten oder testen".




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.

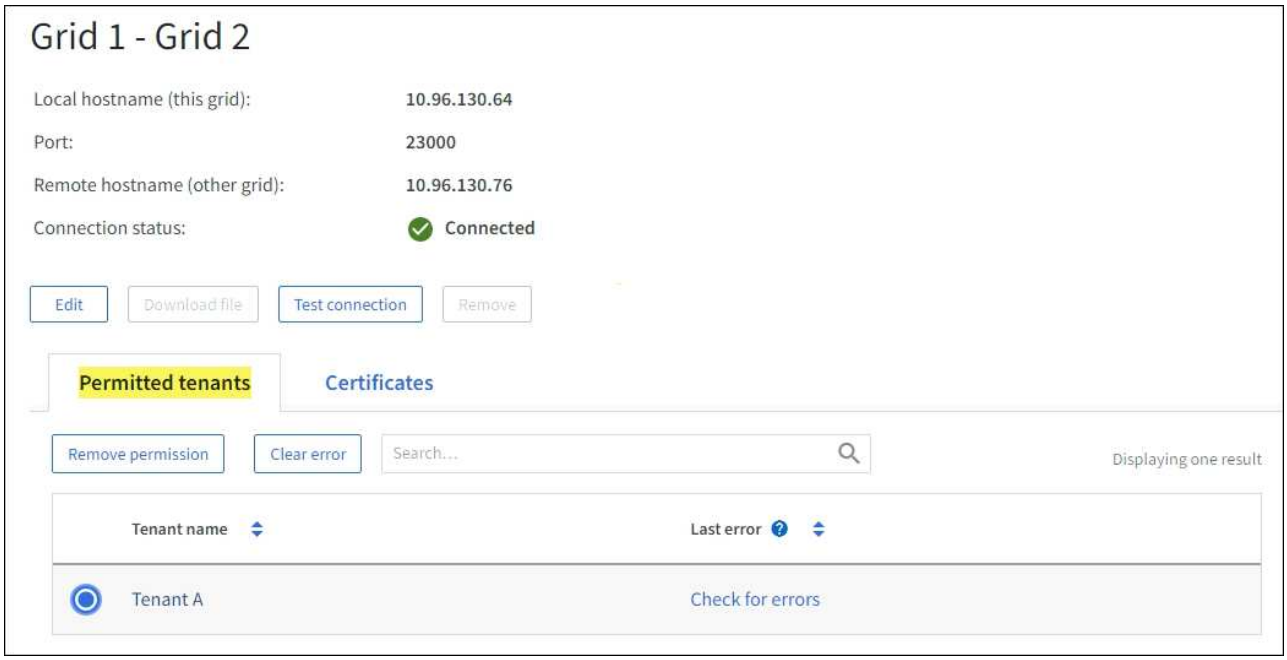
   Auf der Detailseite für die Verbindung können Sie:

   - 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:

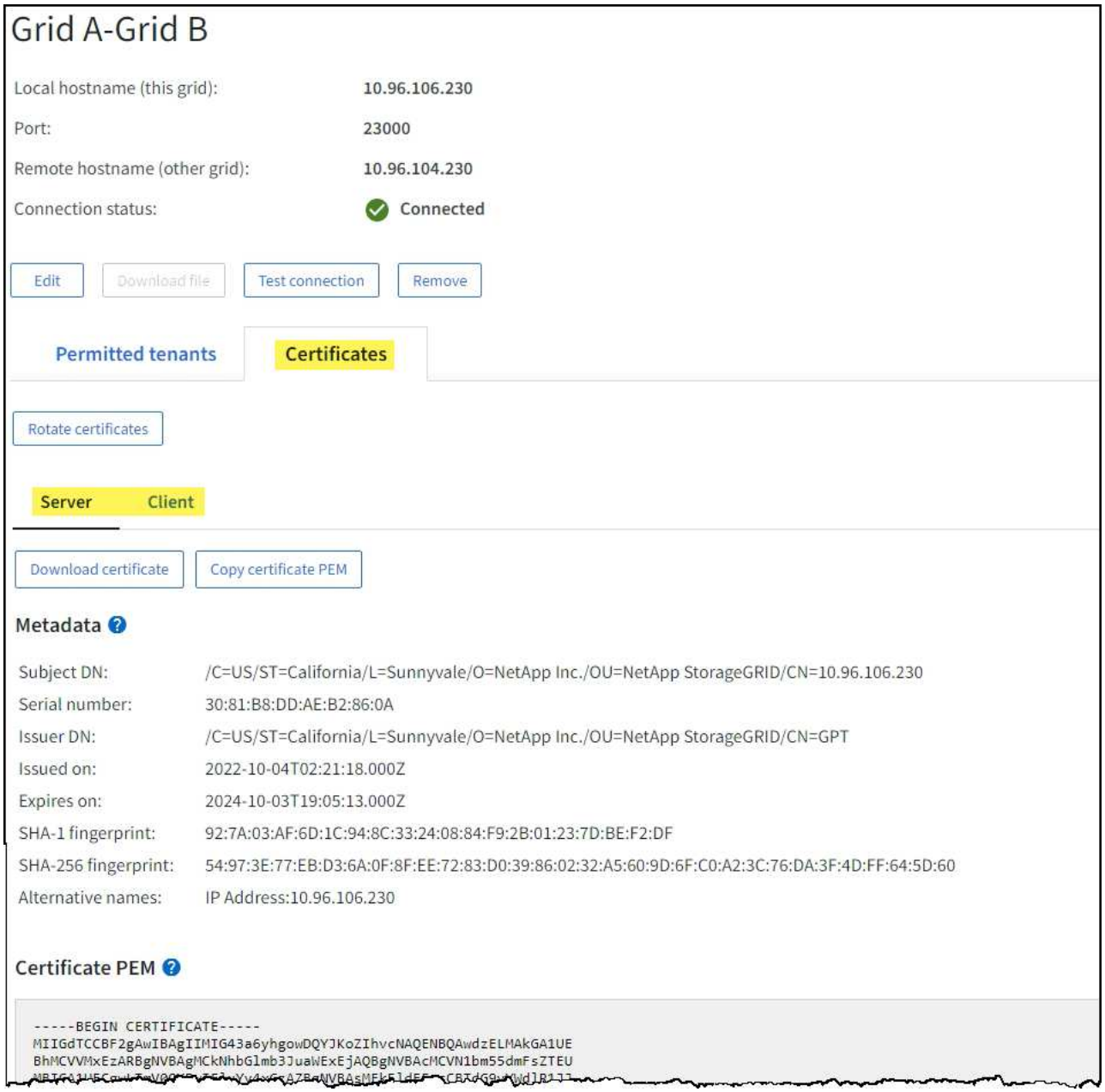
   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an".
   - "Entfernen Sie die Berechtigung eines Mandanten" Um die Verbindung zu verwenden.
   - Überprüfen Sie auf Grid-übergreifende Replikationsfehler, und löschen Sie den letzten Fehler. Siehe "Fehler beim Grid-Verbund beheben".




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**

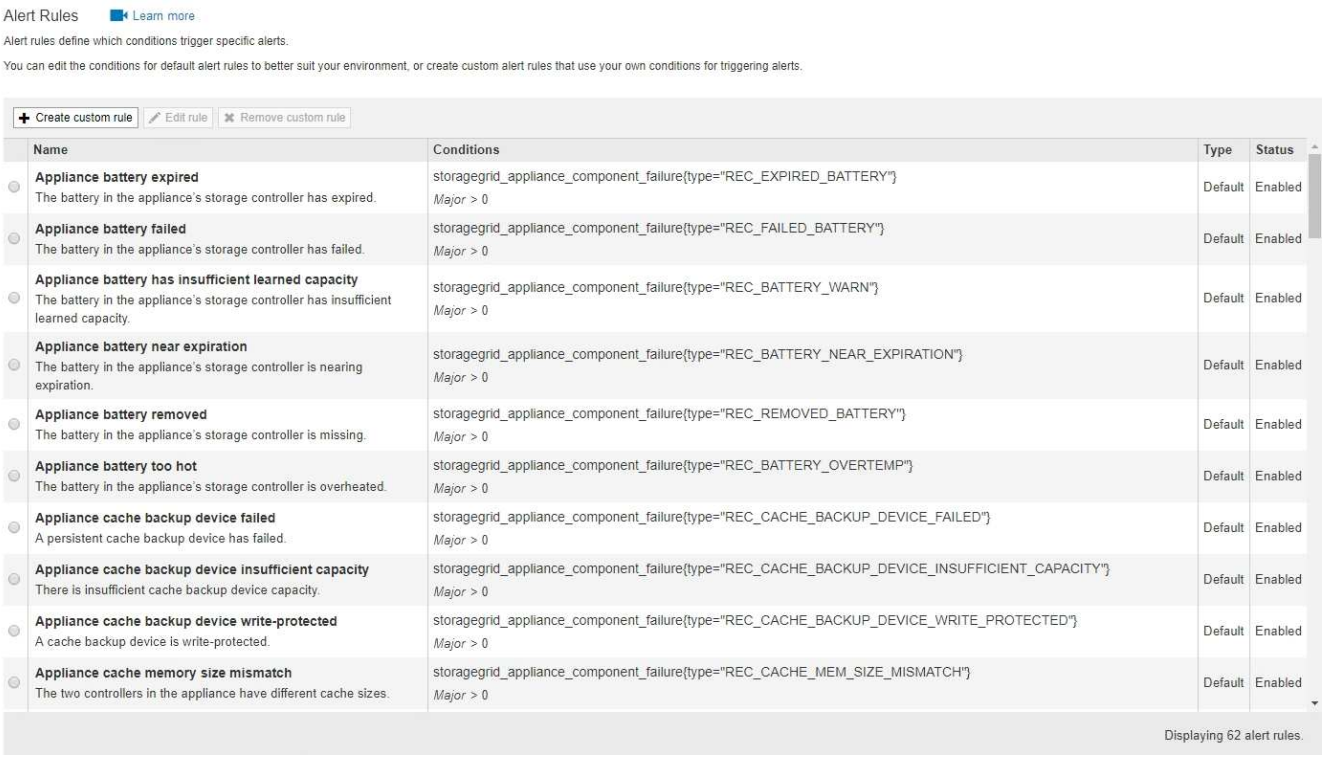
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".
- Optional haben Sie das Video angesehen:

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.<br>• **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.<br>• **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.<br>• **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:<br>• **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.<br>• **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.<br>• **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.

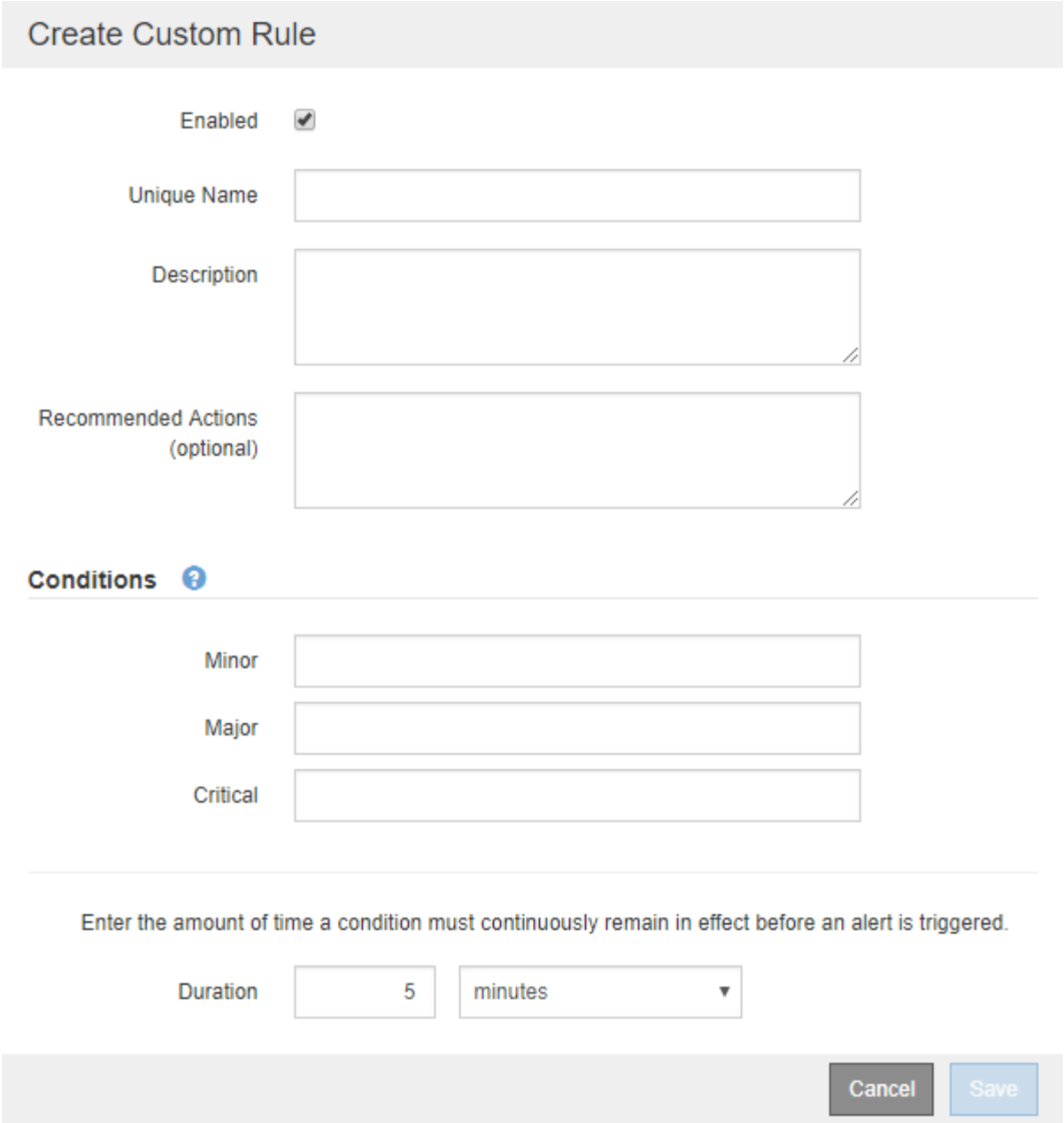
**Schritte**

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.

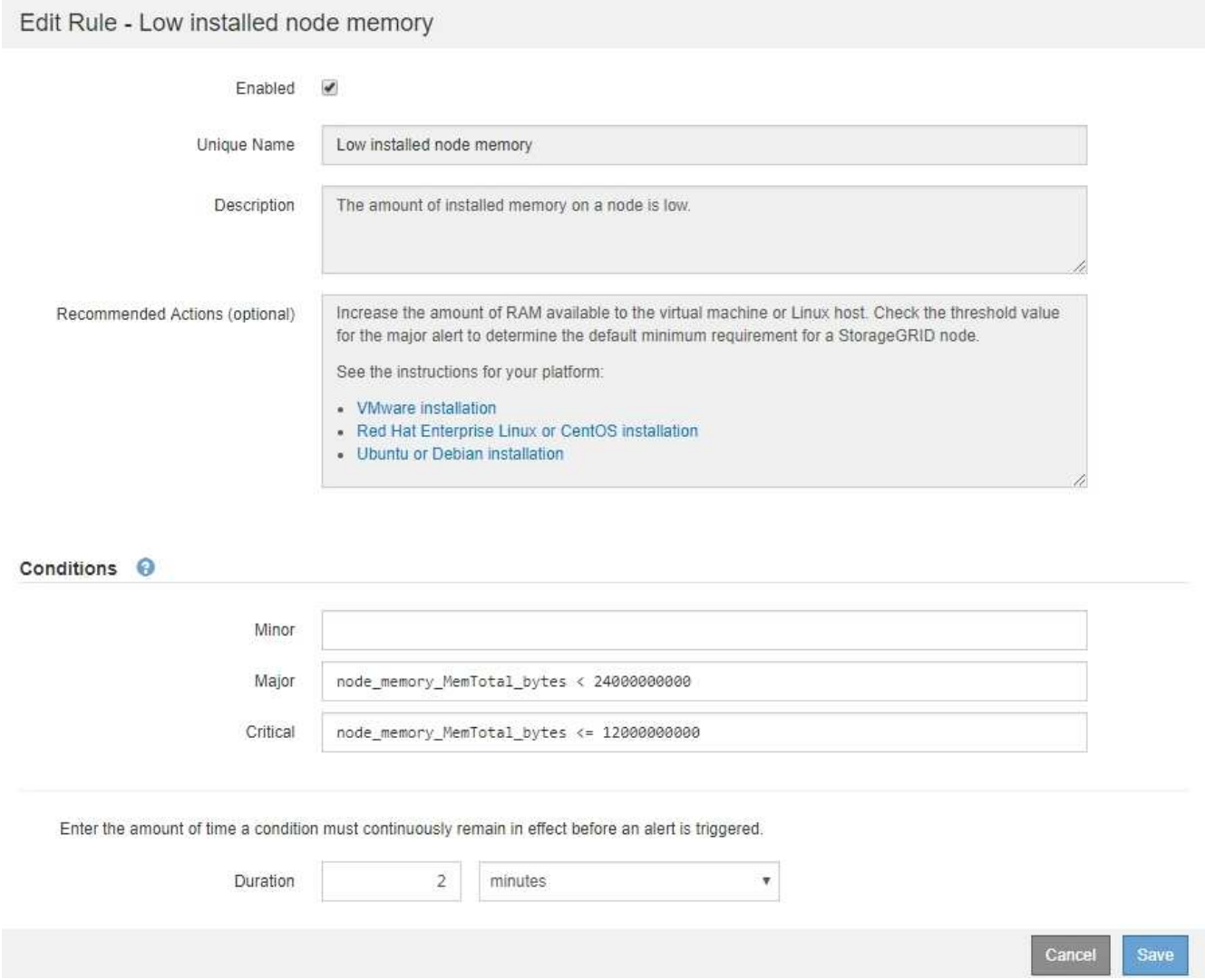
**Schritte**

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.

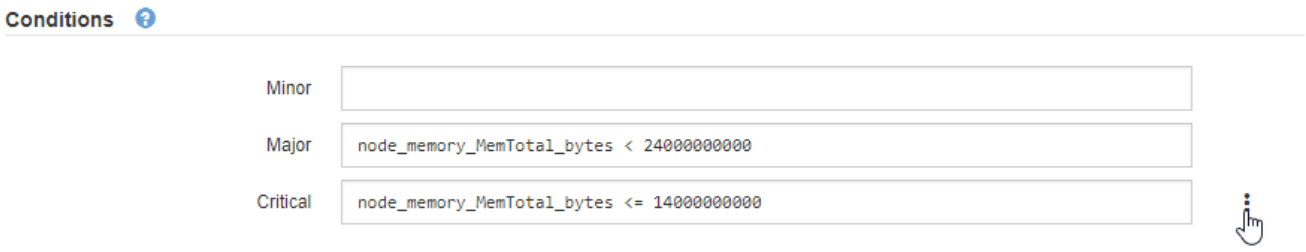
5. Aktualisieren Sie für benutzerdefinierte Warnungsregeln die folgenden Informationen, falls erforderlich.

   > 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**.

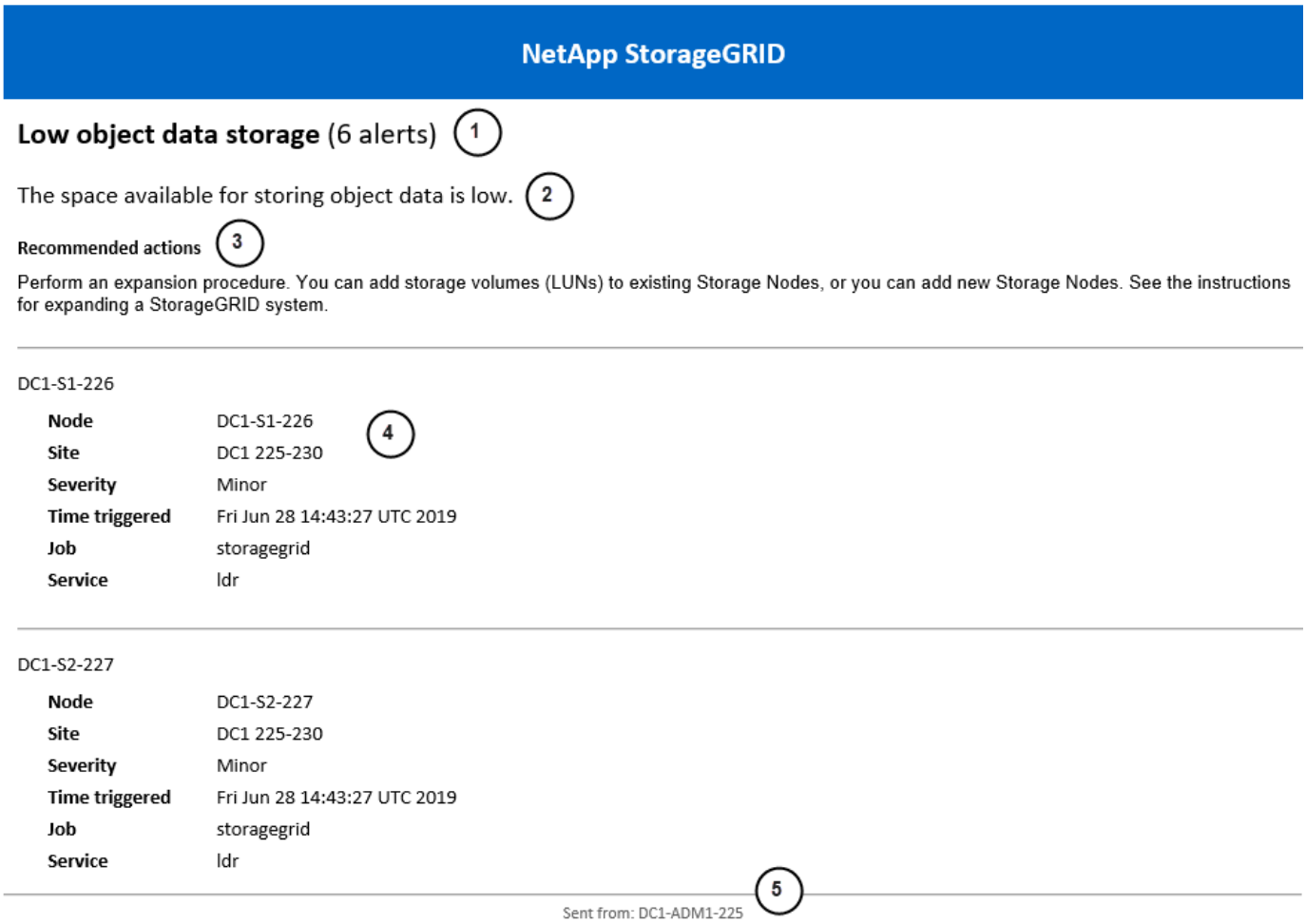
   Beim Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Sie müssen **Speichern** wählen.

   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.<br>• 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.<br>2. Alarm A wird auf Knoten 2 um 08:01 ausgelöst. Es wird keine Benachrichtigung gesendet.<br>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.<br>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.<br>2. Alarm A wird für Node 2 ausgelöst. Eine zweite Benachrichtigung wird gesendet.<br>3. Die Warnung A wird für Knoten 2 behoben, bleibt jedoch für Knoten 1 aktiv.<br>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.<br>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.

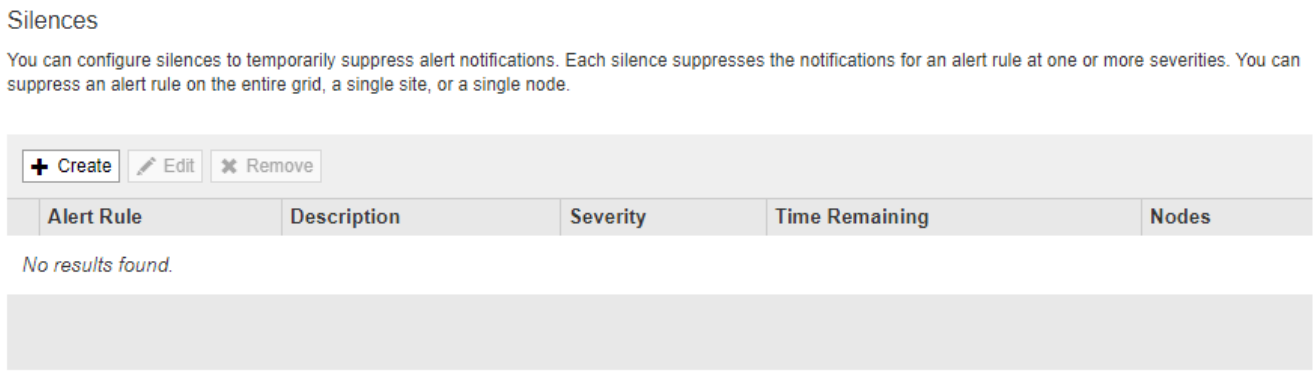
Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.

> 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**

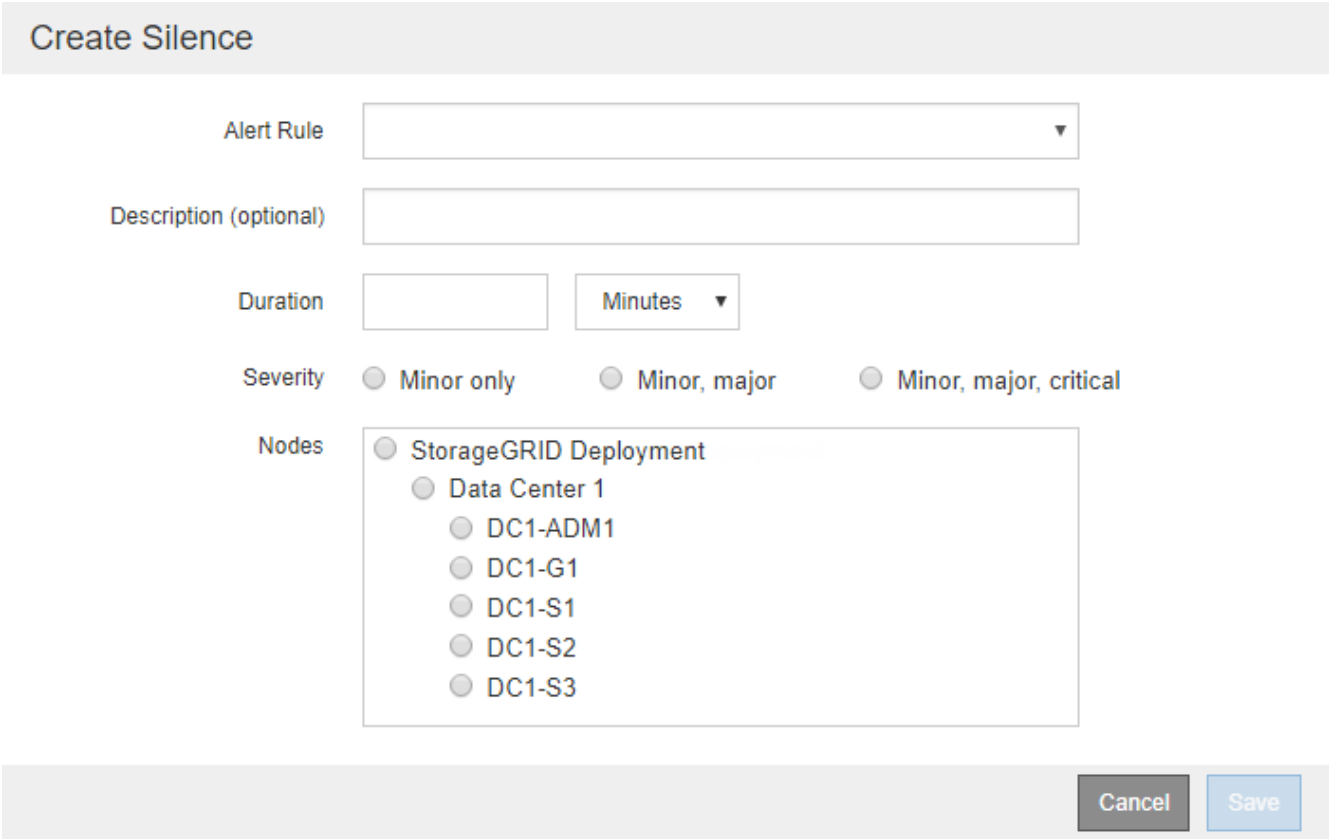
1. Wählen Sie **Warnungen** > **Stummschaltungen**.

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.<br><br>**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.<br><br>**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.<br><br>**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**.<br>b. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie bearbeiten möchten.<br>c. Wählen Sie **Bearbeiten**.<br>d. Ändern Sie die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten.<br>e. Wählen Sie **Speichern**. |

| Option | Beschreibung |
| --- | --- |
| Entfernen Sie eine Stille | a. Wählen Sie **Warnungen** > **Stummschaltungen**.<br>b. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie entfernen möchten.<br>c. Wählen Sie **Entfernen**.<br>d. Wählen Sie **OK**, um zu bestätigen, dass Sie diese Stille entfernen möchten.<br><br>**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".

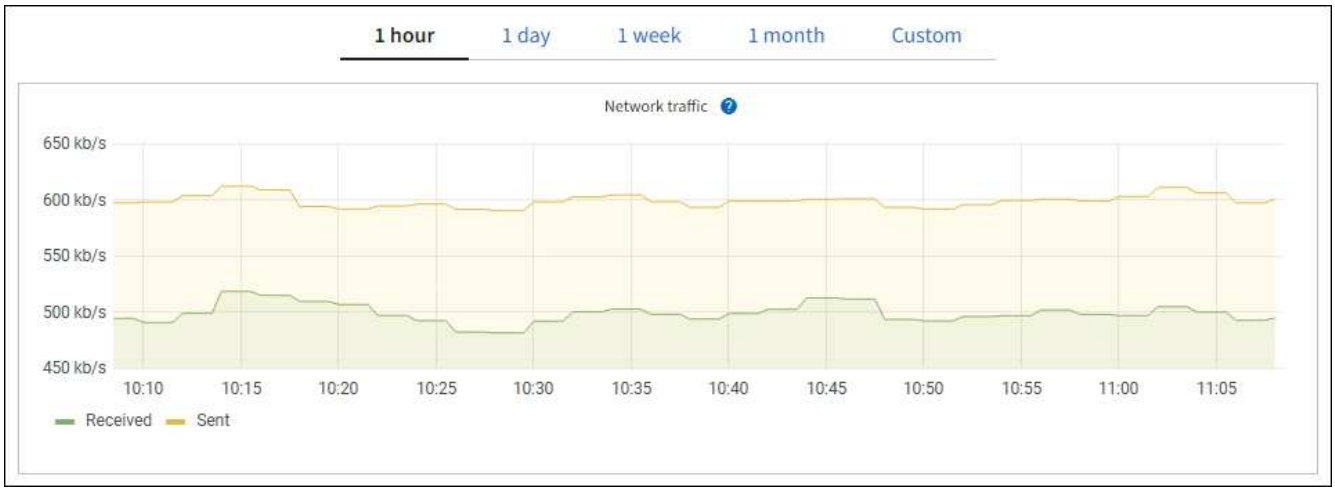
### Was sind Prometheus-Kennzahlen?

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.<br>◦ Diese Meldungen werden beim Exportieren mit syslog als Präfix festgelegt `mgmt:`.<br>◦ 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"`<br>• `cgr-access.log.gz`: Eingehende Grid-übergreifende Replikationsanforderungen.<br>◦ Diese Meldungen werden beim Exportieren mit syslog als Präfix festgelegt `cgr:`.<br>◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"`<br>• `endpoint-access.log.gz`: S3-Anfragen an Load Balancer-Endpunkte.<br>◦ Diese Meldungen werden beim Exportieren mit syslog als Präfix festgelegt `endpoint:`.<br>◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"`<br>• `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.<br><br>**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.<br>• Erfasst Ereignisse im Zusammenhang mit dem Betrieb des NMS-Dienstes. Beispielsweise E-Mail-Benachrichtigungen und Konfigurationsänderungen.<br>• Enthält XML-Paketaktualisierungen, die aus Konfigurationsänderungen im System resultieren.<br>• Enthält Fehlermeldungen zum Attribut Downsampling, das einmal täglich ausgeführt wird.<br>• 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.<br><br>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<br><br>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.<br><br>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:<br>• Für Prüfprotokolle lautet der Schweregrad „Info“.<br>• Bei Sicherheitsereignissen werden die Schweregrade von der Linux-Distribution auf den Knoten generiert.<br>• 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.<br>• 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:<br>• Für Audit-Protokolle lautet die an den externen Syslog-Server gesendete Einrichtung „local7“.<br>• Bei Sicherheitsereignissen werden die Einrichtungswerte von der linux-Distribution auf den Knoten generiert.<br>• Für Anwendungsprotokolle weisen die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Einrichtungswerte auf:<br>  ◦ `bycast.log`: Benutzer oder Daemon<br>  ◦ `bycast-err.log`: Benutzer, Daemon, local3 oder local4<br>  ◦ `jaeger.log`: Local2<br>  ◦ `nms.log`: Local3<br>  ◦ `prometheus.log`: Local4<br>  ◦ `raft.log`: Local5<br>  ◦ `hagroups.log`: Local6<br>• 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` .<br><br>**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:<br><br>• Admin-Knoten (primär und nicht primär): `/var/local/audit/export/audit.log`<br>• 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<br><br>(GET und GETNEXT) | Schreibgeschützte MIB-Abfragen | Schreibgeschützte MIB-Abfragen | Schreibgeschützte MIB-Abfragen |
| Abfrageauthentifizierung | Community-Zeichenfolge | Community-Zeichenfolge | Benutzer des benutzerbasierten Sicherheitsmodells (USM) |
| Benachrichtigungen<br><br>(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.<br><br>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.<br><br>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.<br>• 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.<br><br>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.<br><br>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.<br>• Wenn Sie **Trap** ausgewählt haben, werden nur USM-Benutzer ohne maßgebliche Engine-IDs angezeigt.<br>• Wenn Sie **Inform** ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt.<br>• Wenn keine Benutzer angezeigt werden:<br>i. Erstellen und speichern Sie das Trap-Ziel.<br>ii. Gehen Sie zuUSM-Benutzer erstellen, und erstellen Sie den Benutzer.<br>iii. Kehren Sie zur Registerkarte Trap-Ziele zurück, wählen Sie das gespeicherte Ziel aus der Tabelle aus und wählen Sie **Bearbeiten**.<br>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.<br><br>Standardmäßig verwendet SNMP IPv4. |
| Transportprotokoll | Ob diese Adresse UDP oder TCP verwendet.<br><br>Standardmäßig verwendet SNMP UDP. |
| StorageGRID-Netzwerk | Welches StorageGRID-Netzwerk der Agent abhört.<br><br>• Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent hört auf Abfragen in allen drei Netzwerken.<br>• Grid-Netzwerk<br>• Admin-Netzwerk<br>• Client-Netzwerk<br><br>**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.<br><br>Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben.<br><br>**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.<br><br>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.<br><br>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.<br><br>**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:<br><br>• **AuthPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort sowie ein Datenschutzprotokoll und ein Passwort angeben.<br>• **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.

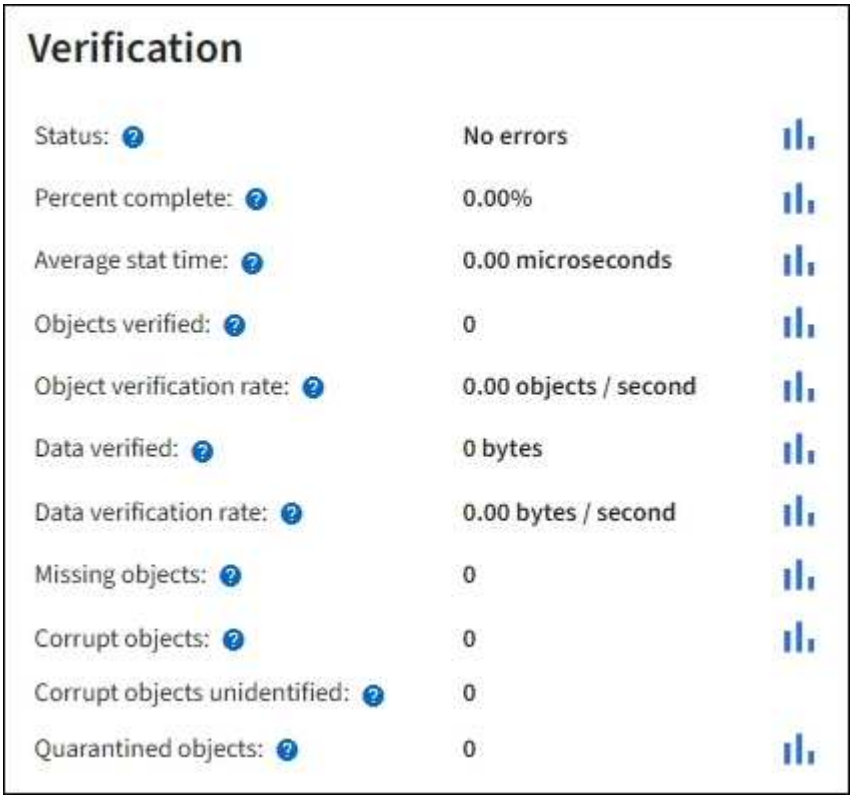
**Schritte**

1. Prüfen Sie die Ergebnisse aus Hintergrundverifizierungen:

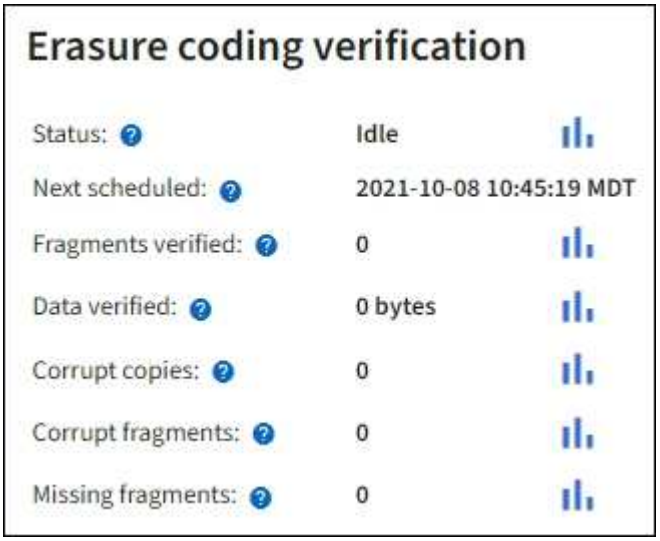
   a. Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte**.

   b. Überprüfen Sie die Überprüfungsergebnisse:

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

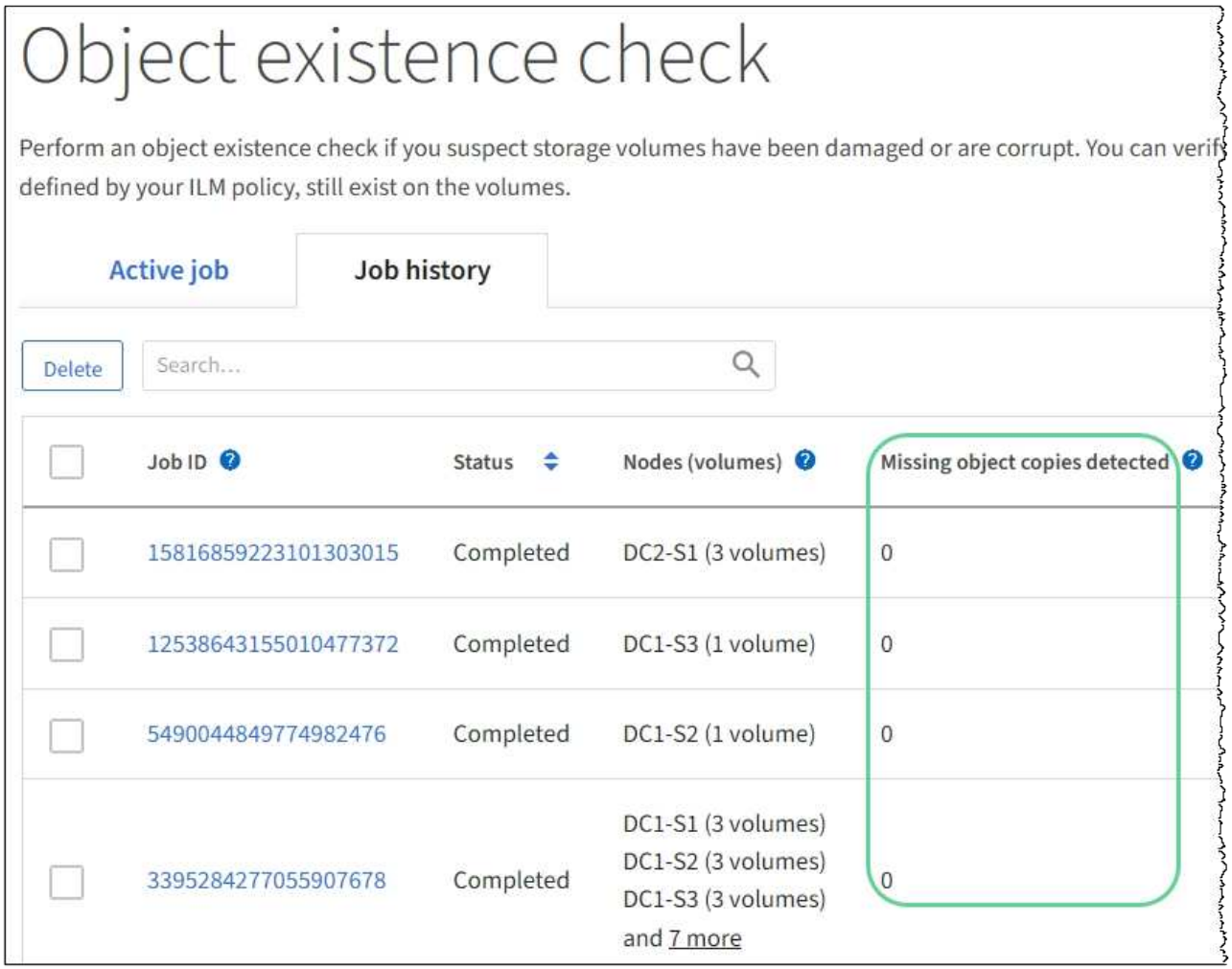


- Um die Überprüfung von Fragment mit Löschungscode zu überprüfen, wählen Sie ***Storage Node*** > **ILM** aus, und sehen Sie sich die Attribute im Abschnitt zur Verifizierung von Erasure-Coding an.




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

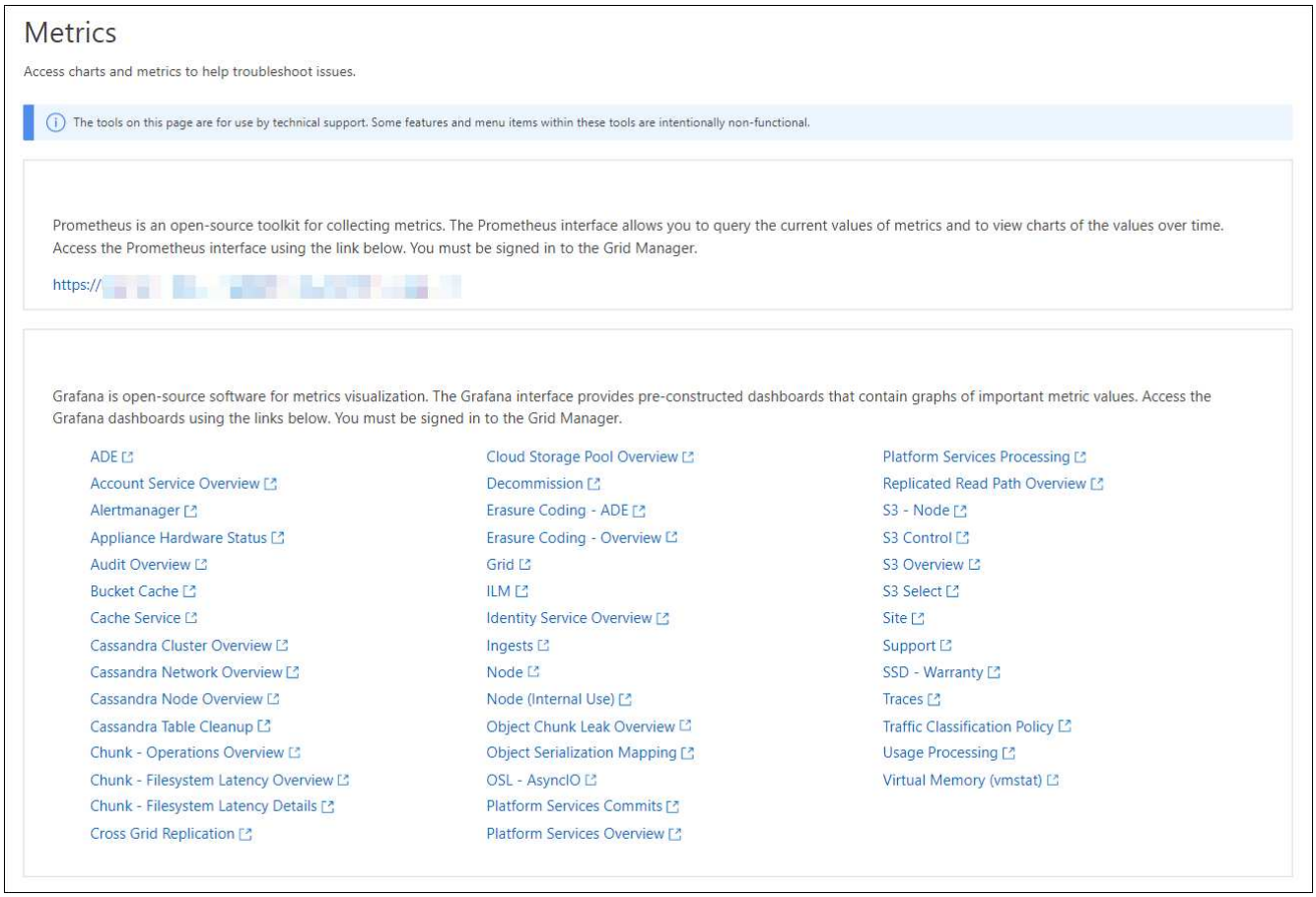
Auf der Seite Metriken können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist Open-Source-Software zum Sammeln von Kennzahlen. Grafana ist Open-Source-Software zur Visualisierung von Kennzahlen.

> 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.

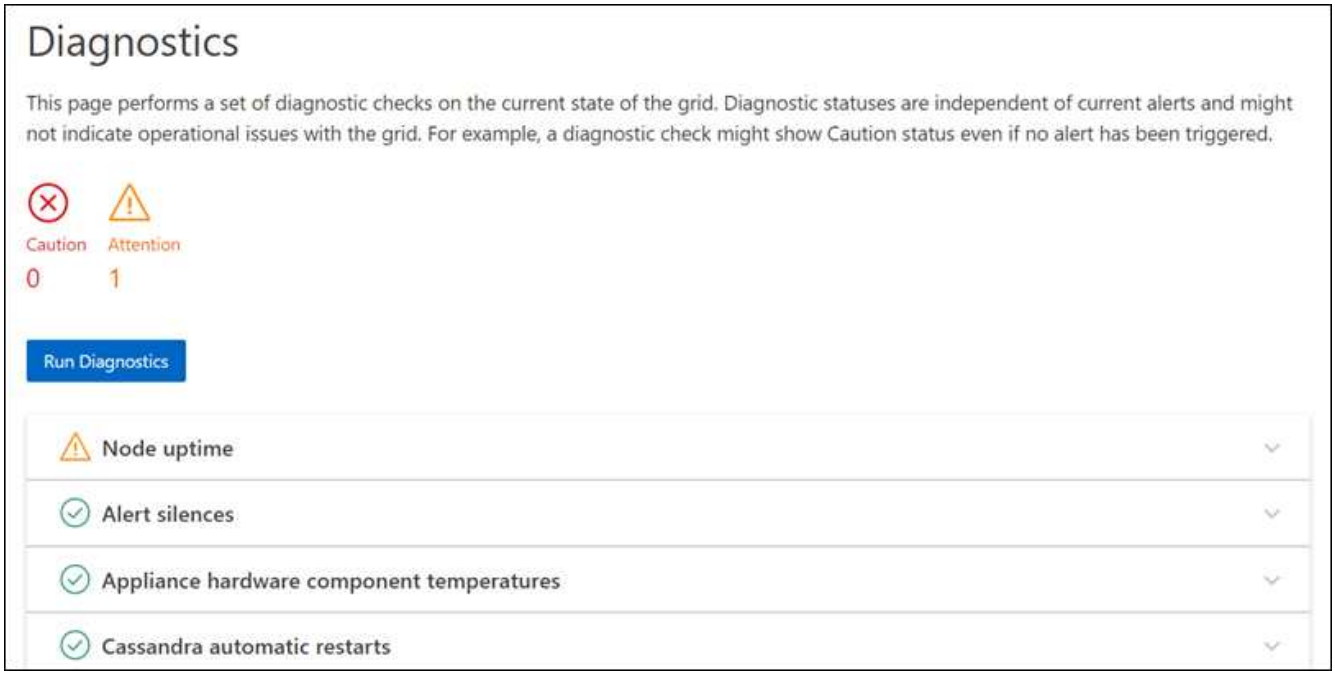
**Schritte**

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“.



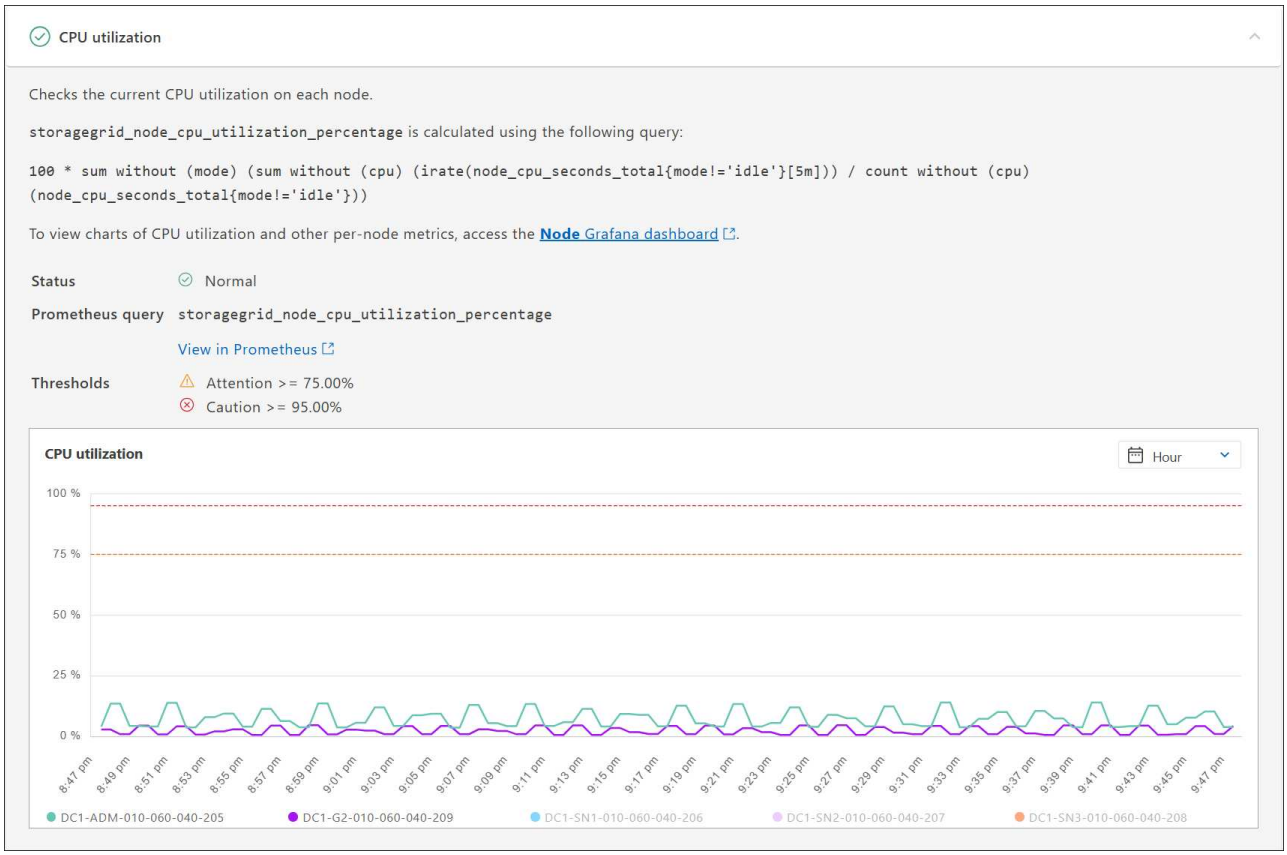

2. Wenn Sie mehr über eine bestimmte Diagnose erfahren möchten, klicken Sie auf eine beliebige Stelle in der Zeile.

   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**.

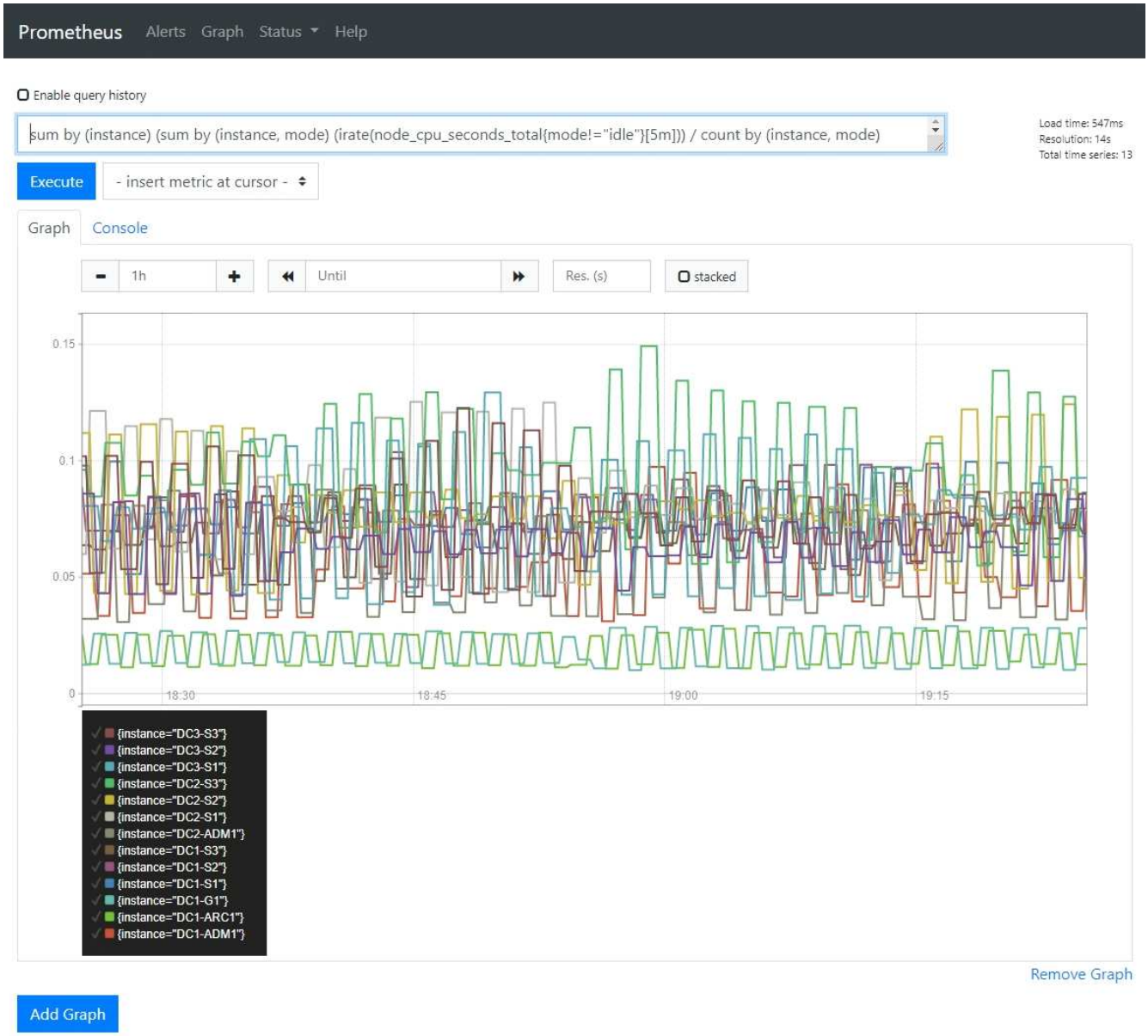
   Dieser Link wird nicht für alle Diagnosen angezeigt.

   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**.

**metrics** Operations on metrics

| | | |
|---|---|---|
| GET | `/grid/metric-labels/{label}/values` | Lists the values for a metric label |
| GET | `/grid/metric-names` | Lists all available metric names |
| GET | `/grid/metric-query` | Performs an instant metric query at a single point in time |
| GET | `/grid/metric-query-range` | Performs a metric query over a range of time |

Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung liegen über dem Umfang dieser Dokumentation hinaus.

**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.