Überwachen Sie das StorageGRID-System

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-118/monitor/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Überwachen Sie das StorageGRID-System . . . 1
- Überwachen eines StorageGRID-Systems: Übersicht . . . 1
- Das Dashboard anzeigen und verwalten . . . 1
  - Dashboard anzeigen . . . 2
  - Managen von Dashboards . . . 3
  - Dashboards konfigurieren . . . 4
- Zeigen Sie die Seite Knoten an . . . 4
  - Anzeigen der Seite Knoten: Übersicht . . . 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
  - Verwenden Sie die Registerkarte Aufgaben . . . 32
  - Zeigen Sie die Registerkarte Load Balancer an . . . 32
  - Zeigen Sie die Registerkarte Plattformdienste an . . . 34
  - Registerkarte Laufwerke managen anzeigen (nur SGF6112) . . . 35
  - Registerkarte „SANtricity System Manager“ anzeigen (nur E-Series) . . . 36
- Informationen, die regelmäßig überwacht werden müssen . . . 39
  - Was und wann zu überwachen . . . 39
  - Systemzustand überwachen . . . 39
  - Monitoring der Storage-Kapazität . . . 45
  - Überwachung des Information Lifecycle Management . . . 53
  - Überwachen Sie Netzwerk- und Systemressourcen . . . 54
  - Überwachen Sie die Mandantenaktivität . . . 58
  - Monitoring von S3- und Swift-Client-Operationen . . . 63
  - Monitoring von Lastverteilungsvorgängen . . . 64
  - Überwachen von Netzverbundverbindungen . . . 65
  - Überwachen Sie die Archivierungskapazität . . . 70
- Alarme und Alarme . . . 70
  - Alarme und Alarme verwalten: Übersicht . . . 70
  - Vergleichen von Warnungen und Alarmen . . . 71
  - Verwalten von Meldungen . . . 75
  - Alerts Referenz . . . 98
  - Häufig verwendete Prometheus-Kennzahlen . . . 110
  - Verwalten von Alarmen (Altsystem) . . . 116
  - Alarmreferenz (Altsystem) . . . 138
- Referenz für Protokolldateien . . . 168
  - Referenz für Protokolldateien: Übersicht . . . 168
  - StorageGRID-Softwareprotokolle . . . 170
  - Protokoll für Implementierung und Wartung . . . 177
  - Protokolle für Drittanbietersoftware . . . 177

Etwa bycast.log . . . 178
Konfigurieren Sie Überwachungsmeldungen und Protokollziele . . . 187
Überlegungen zur Verwendung eines externen Syslog-Servers . . . 187
Konfigurieren von Audit-Meldungen und externem Syslog-Server . . . 192
Verwenden Sie SNMP-Überwachung . . . 202
Verwenden Sie SNMP-Überwachung: Übersicht . . . 202
Konfigurieren Sie den SNMP-Agent . . . 203
Aktualisieren Sie den SNMP-Agent . . . 210
Zugriff auf MIB-Dateien . . . 212
Erfassung zusätzlicher StorageGRID-Daten . . . 214
Verwenden Sie Diagramme und Diagramme . . . 214
Verwenden Sie Textberichte . . . 225
PUT- und GET-Performance werden überwacht . . . 229
Überwachen von Objektverifizierungsvorgängen . . . 230
Monitoring von Ereignissen . . . 232
Audit-Meldungen prüfen . . . 236
Erfassen von Protokolldateien und Systemdaten . . . 237
Starten Sie manuell ein AutoSupport-Paket . . . 239
Sehen Sie sich den Baum der Grid Topology an . . . 240
Prüfen von Support-Kennzahlen . . . 241
Führen Sie eine Diagnose aus . . . 243
Erstellen benutzerdefinierter Überwachungsanwendungen . . . 247

Überwachen Sie das StorageGRID-System

Überwachen eines StorageGRID-Systems: Übersicht

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

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "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:

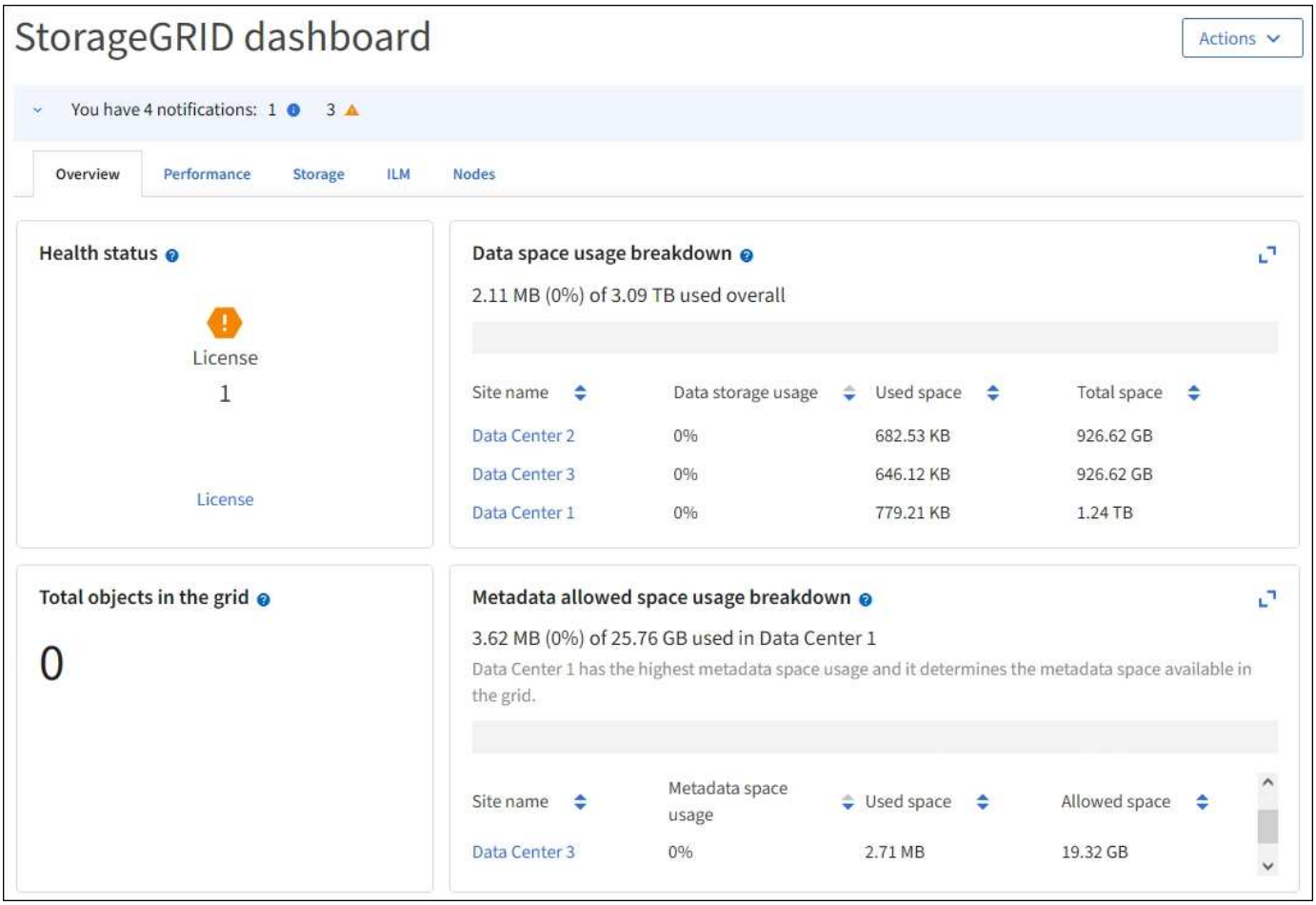
- "Das Dashboard anzeigen und verwalten"
- "Zeigen Sie die Seite Knoten an"
- "Überwachen Sie diese Aspekte des Systems regelmäßig:"
  - "Systemzustand"
  - "Storage-Kapazität"
  - "Informationslebenszyklus-Management"
  - "Netzwerk- und Systemressourcen"
  - "Mandantenaktivität"
  - "Lastverteilung"
  - "Netzverbundverbindungen"
  - "Archivierungskapazität"
- "Verwalten von Warnmeldungen und älteren Alarmen"
- "Anzeigen von Protokolldateien"
- "Konfigurieren von Überwachungsmeldungen und Protokollzielen"
- "Verwenden Sie einen externen Syslog-Server" Zur Erfassung von Audit-Informationen
- "Verwenden Sie SNMP für die Überwachung"
- "Zusätzliche StorageGRID-Daten abrufen", Einschließlich Kennzahlen und Diagnose

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
Leistung	Speichernutzung, im Zeitverlauf verwendeter Storage, S3- oder Swift-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- oder Swift-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 Sie **Schließen**.

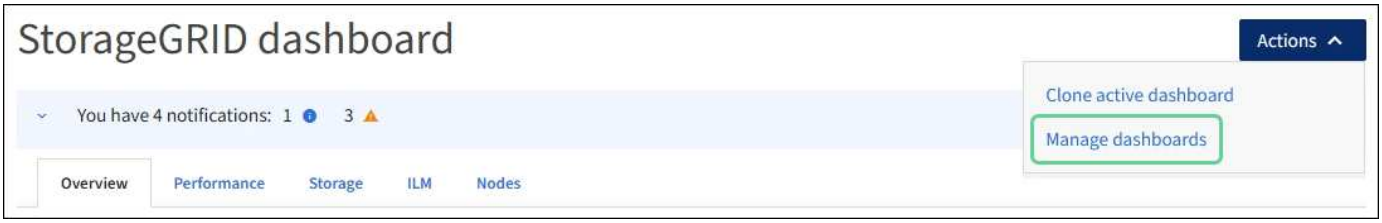
Managen von Dashboards

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

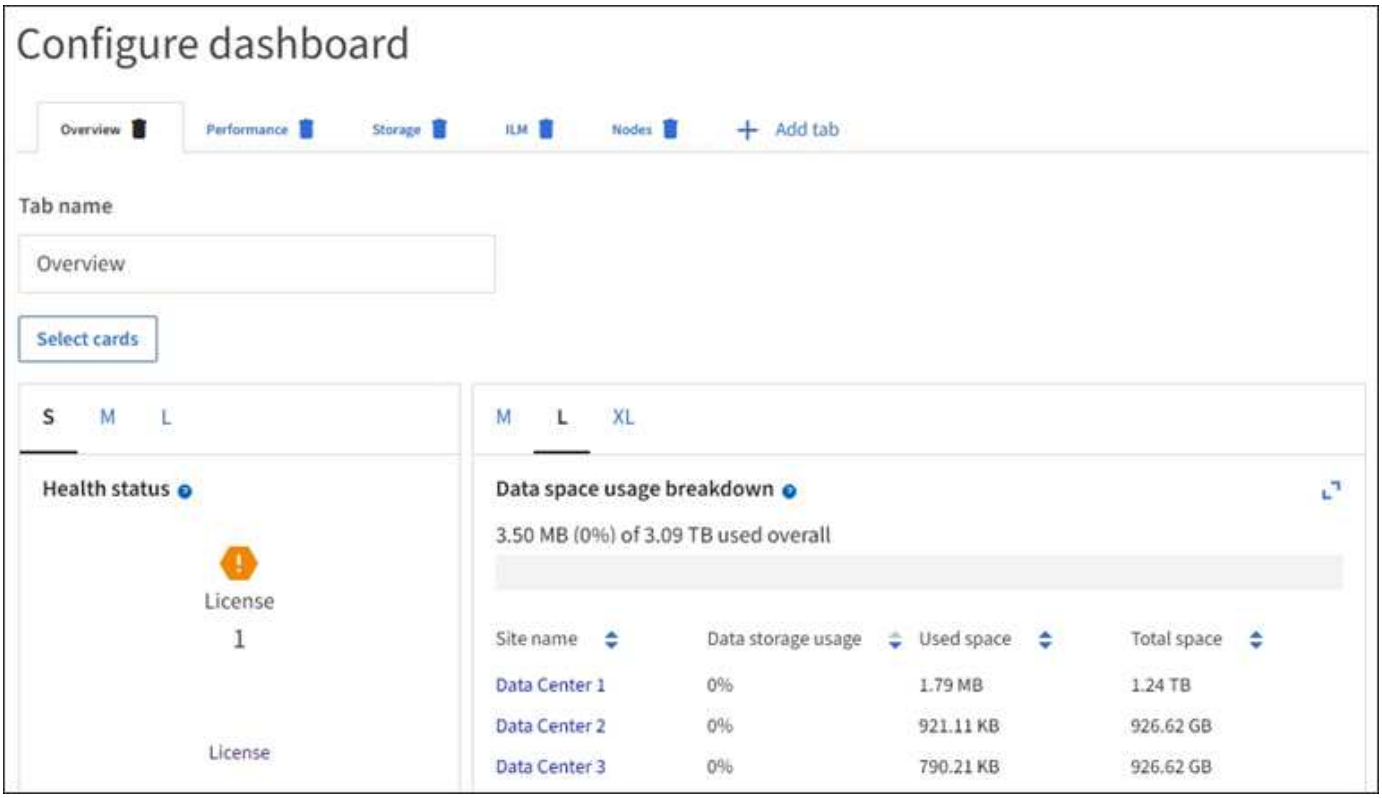
Um ein neues Dashboard durch Klonen des aktiven Dashboards zu erstellen, wählen Sie **actions** > **Clone Active Dashboard**.

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

Anzeigen der Seite Knoten: Übersicht

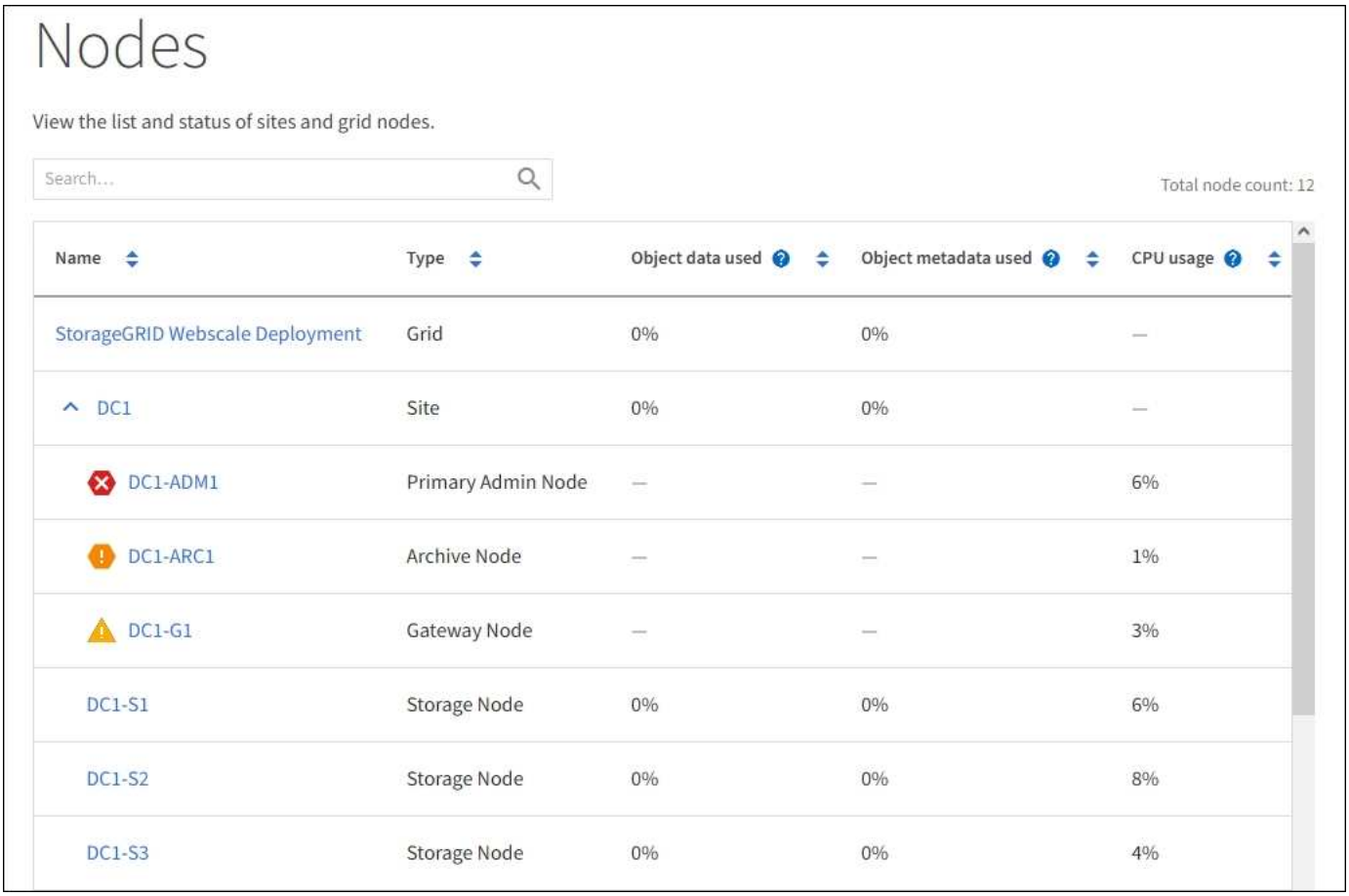
Wenn Sie detailliertere Informationen über das StorageGRID-System benötigen, als das Dashboard bietet, können Sie auf der Seite Nodes Metriken für das gesamte Grid, jeden Standort im Raster und jeden Node an einem Standort anzeigen.

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.



Symbole für Verbindungsstatus

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

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

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

Warnungssymbole

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

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

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

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

Zeigt Details zu einem System, Standort oder Node an

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

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

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

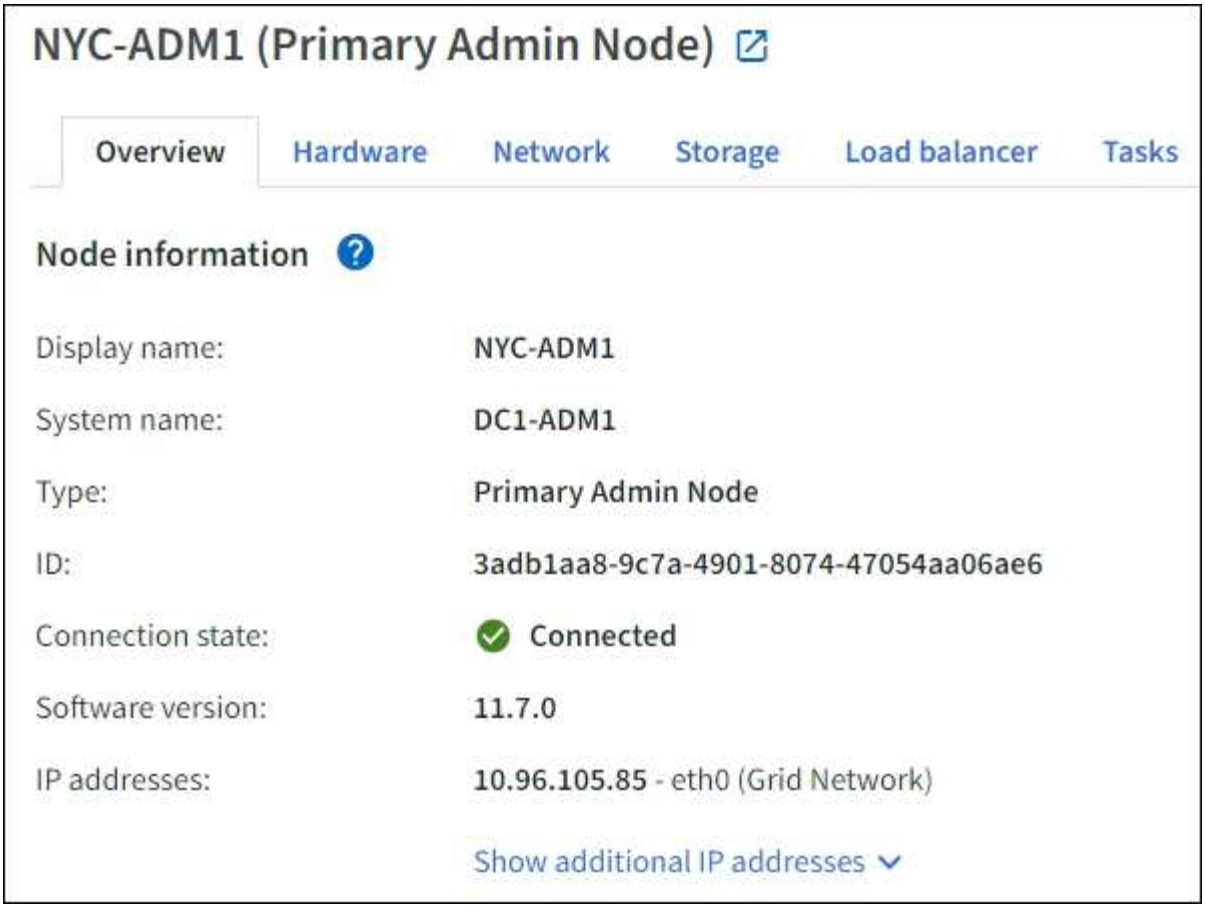
Zeigen Sie die Registerkarte Übersicht an

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

Die Registerkarte Übersicht wird für alle Knoten angezeigt.

Node-Informationen

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



Die Übersichtsinformationen für einen Knoten umfassen Folgendes:

- **Anzeigename** (wird nur angezeigt, wenn der Knoten umbenannt wurde): Der aktuelle Anzeigename für den Knoten. Verwenden Sie die "Benennen Sie Raster, Standorte und Nodes um" Vorgehensweise zum Aktualisieren dieses Werts.
- **Systemname**: Der Name, den Sie während der Installation für den Knoten eingegeben haben. Systemnamen werden für interne StorageGRID-Vorgänge verwendet und können nicht geändert werden.
- **Typ**: Node-Typ - Admin-Node, primärer Admin-Node, Storage-Node, Gateway-Node oder Archiv-Node.

> Die Unterstützung für Archivknoten ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten vom Archiv-Node auf ein externes Archiv-Storage-System über die S3-API wurde durch ILM Cloud Storage-Pools ersetzt, die mehr Funktionen bieten.

- **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 nach unten** : Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz 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.
- * Verbunden* : 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 „Warnmeldungen“ der Registerkarte „Übersicht“ sind alle aufgeführt "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.

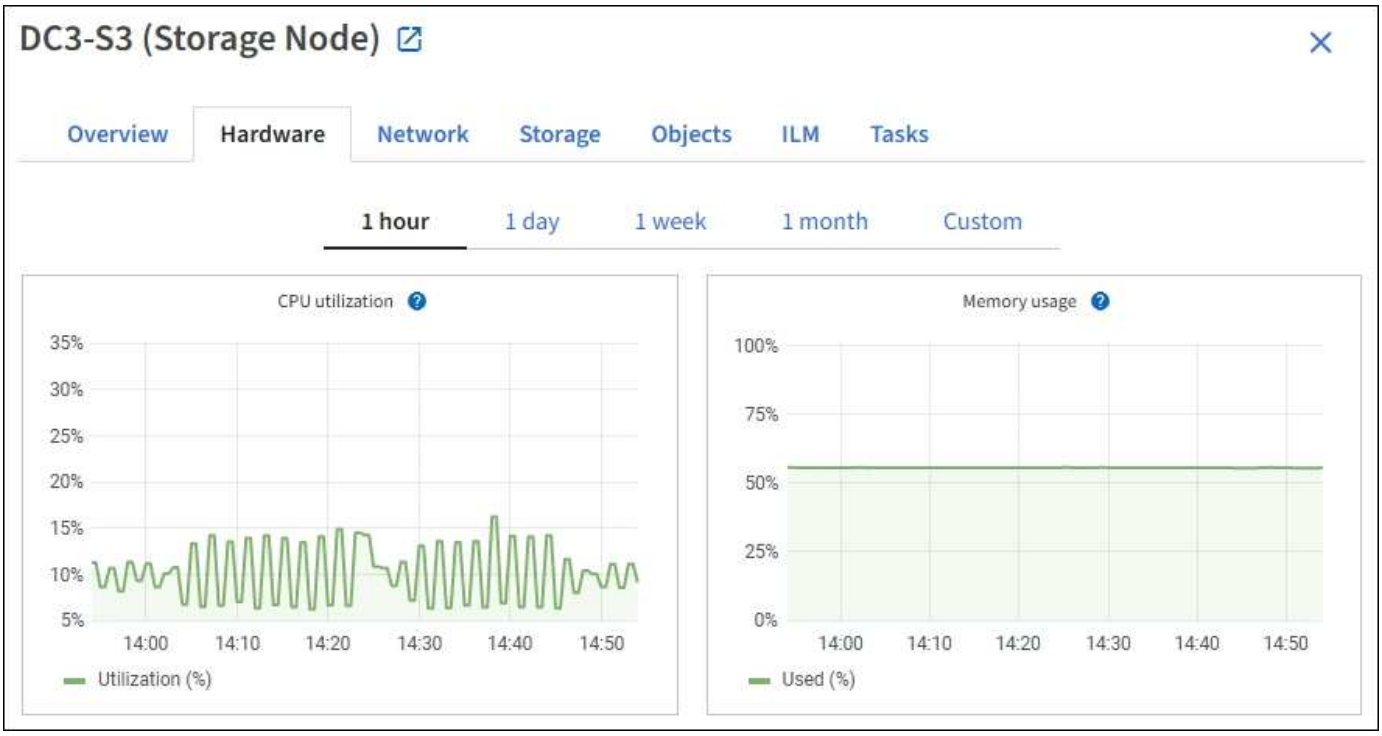
Warnmeldungen sind auch für enthalten "Status der Node-Verbindung".

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.

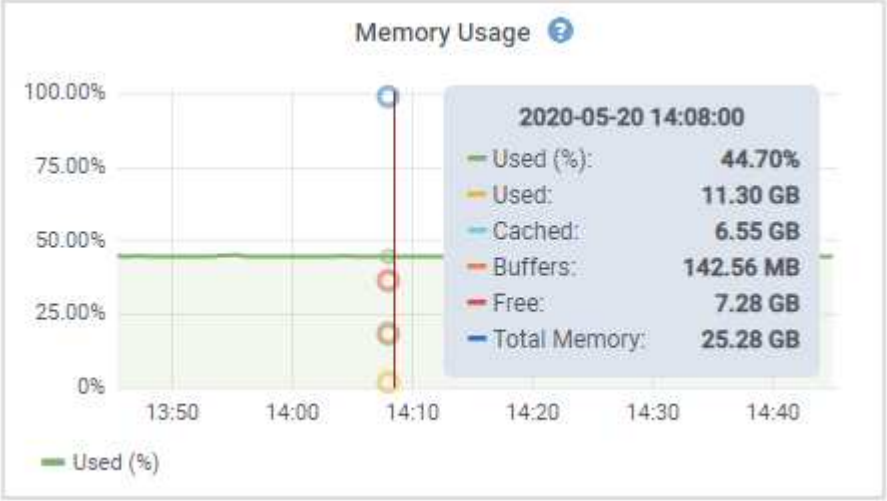
> Der Grid Manager wird mit jeder Version aktualisiert und stimmt möglicherweise nicht mit den Beispielbildern auf dieser Seite überein.

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

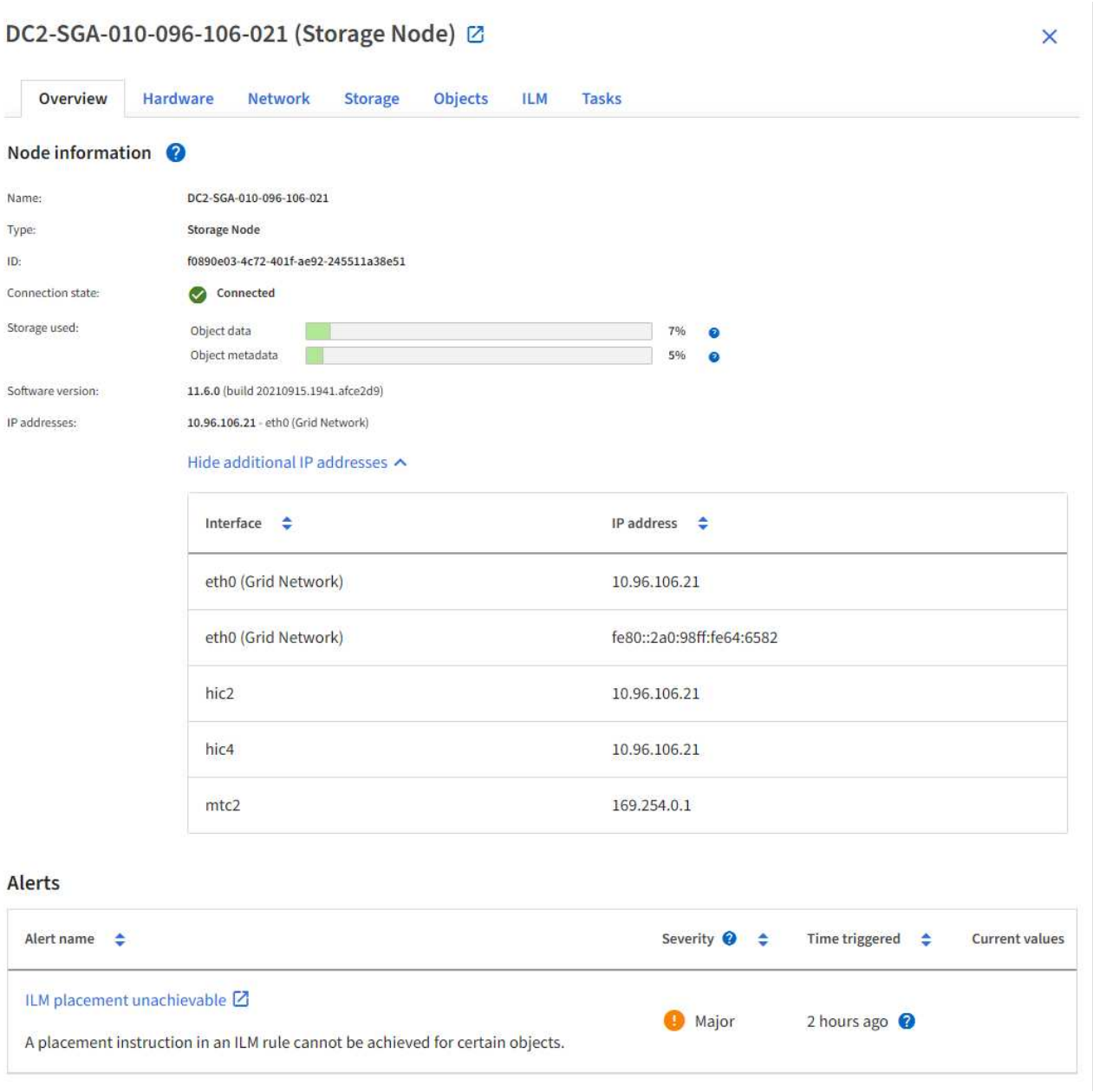
Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplattengeräte- und Netzwerkressourcen für jeden Appliance Storage Node aufgeführt. Außerdem können Sie den Arbeitsspeicher, die Storage-Hardware, die Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen,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

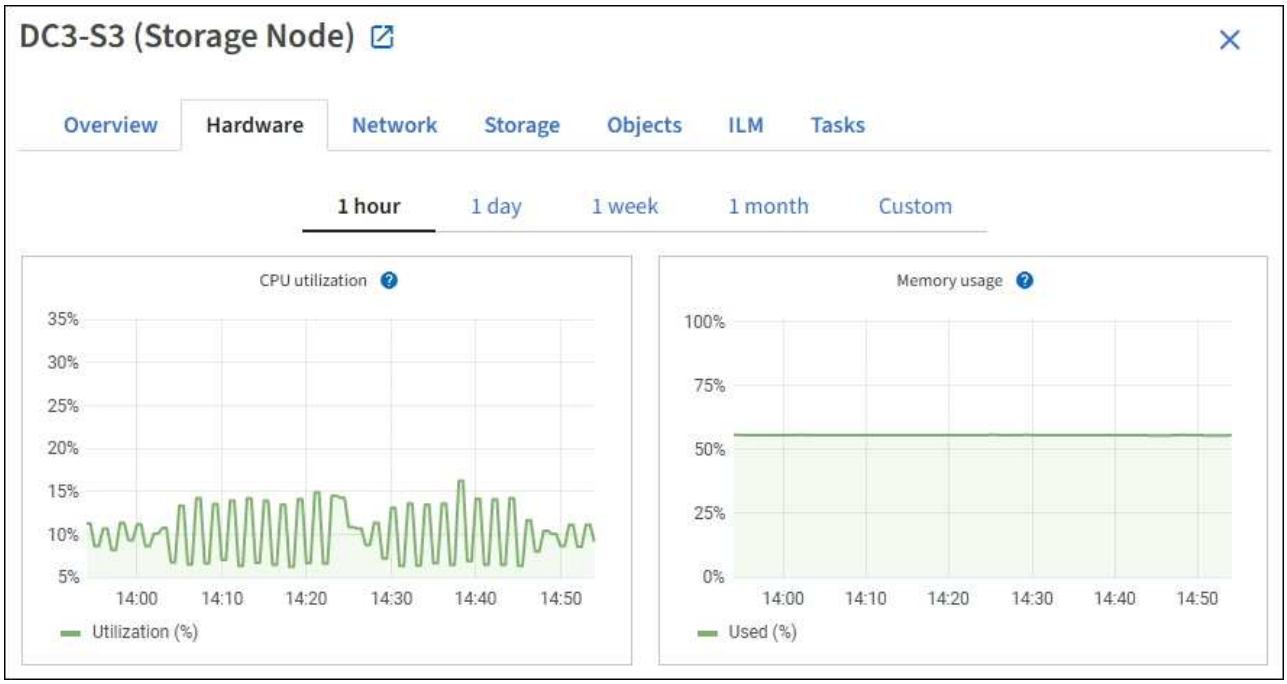
   - **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk.
   - **Hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID-Grid-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
   - **mtc**: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

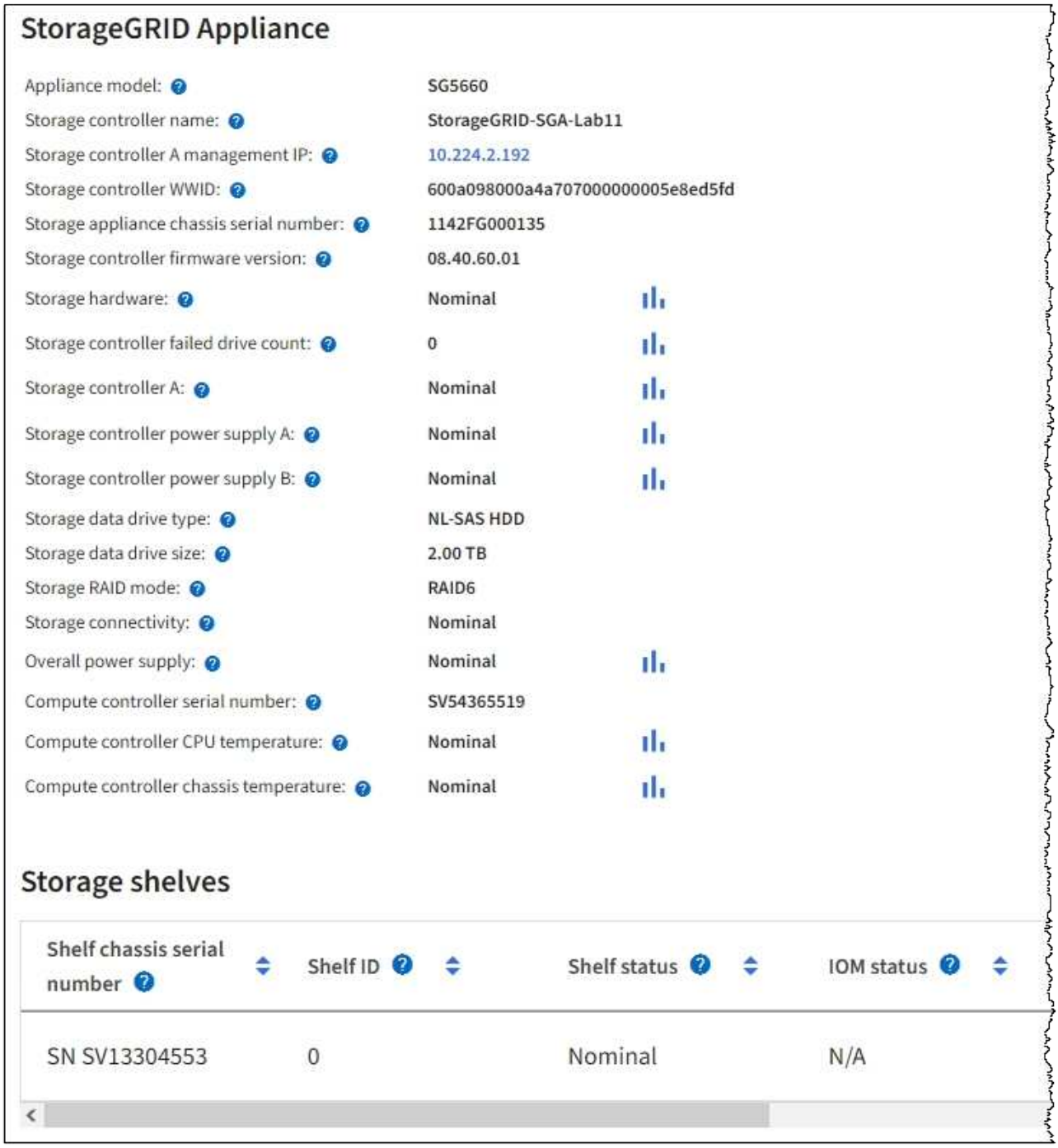
   a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren 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 Betriebssystem zuzugreifen, um Storage-Probleme zu beheben.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Controller B Management-IP	IP-Adresse für Management Port 1 auf Storage Controller B Sie verwenden diese IP, um auf das SANtricity Betriebssystem zuzugreifen, um Storage-Probleme zu beheben. Einige Appliance-Modelle besitzen keinen Storage Controller B.
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.
Storage-Hardware	Der Gesamtstatus der Hardware des Storage Controllers. Wenn SANtricity System Manager einen Status als Warnung für die Storage-Hardware meldet, meldet das StorageGRID System diesen Wert ebenfalls. Wenn der Status „erfordert Aufmerksamkeit“ lautet, überprüfen Sie zuerst den Storage Controller mit SANtricity OS. Stellen Sie dann sicher, dass keine weiteren Alarme vorhanden sind, die für den Rechencontroller gelten.
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 besitzen 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).
Größe der Speicherdatenlaufwerk	Die effektive Größe eines Datenlaufwerks. **Hinweis**: Für Knoten mit Erweiterungs-Shelfs, verwenden Sie das Datenlaufwerk-Größe für jedes Shelf Stattdessen. Die effektive Laufwerksgröße kann je nach Shelf abweichen.
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Konnektivität	Der Status der Storage-Konnektivität.
Gesamtnetzteil	Der Status aller Netzteile für das Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird nicht für Gerätelodelle angezeigt, die keinen BMC enthalten.
Seriennummer des Computing-Controllers	Die Seriennummer des Compute-Controllers.
Computing-Hardware	Der Status der Compute-Controller-Hardware Dieses Feld wird nicht für Appliance-Modelle angezeigt, die über keine separate Computing-Hardware und Speicher-Hardware verfügen.
CPU-Temperatur des Compute-Controllers	Der Temperaturstatus der CPU des Compute-Controllers.
Temperatur im Computing-Controller-Chassis	Der Temperaturstatus des Compute-Controllers.

+

Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Seriennummer des Shelf Chassis	Die Seriennummer für das Storage Shelf-Chassis.
Shelf-ID	Die numerische Kennung für das Storage-Shelf. • 99: Storage Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf **Hinweis:** Erweiterungseinschübe gelten nur für die SG6060 und SG6160.
Der Shelf-Status	Der Gesamtstatus des Storage Shelf.
EAM-Status	Der Status der ein-/Ausgangsmodule (IOMs) in beliebigen Erweiterungs-Shelfs. K. A., wenn es sich nicht um ein Erweiterungs-Shelf handelt

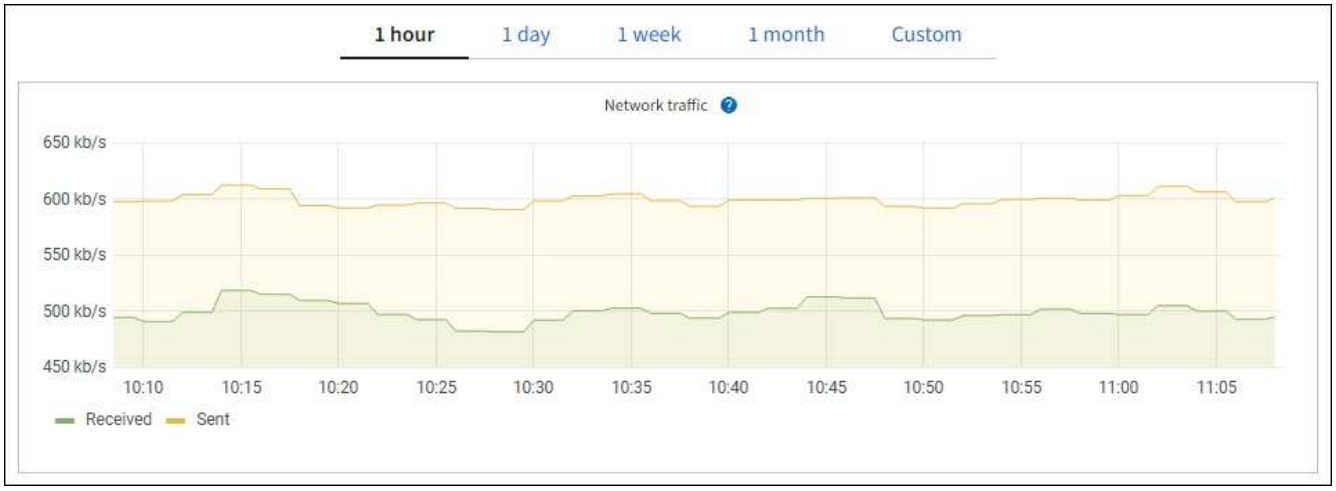
Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Netzteilstatus	Der Gesamtstatus der Netzteile für das Storage Shelf.
Status der Schublade	Der Zustand der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Lüfter im Storage Shelf.
Laufwerksschächte	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.

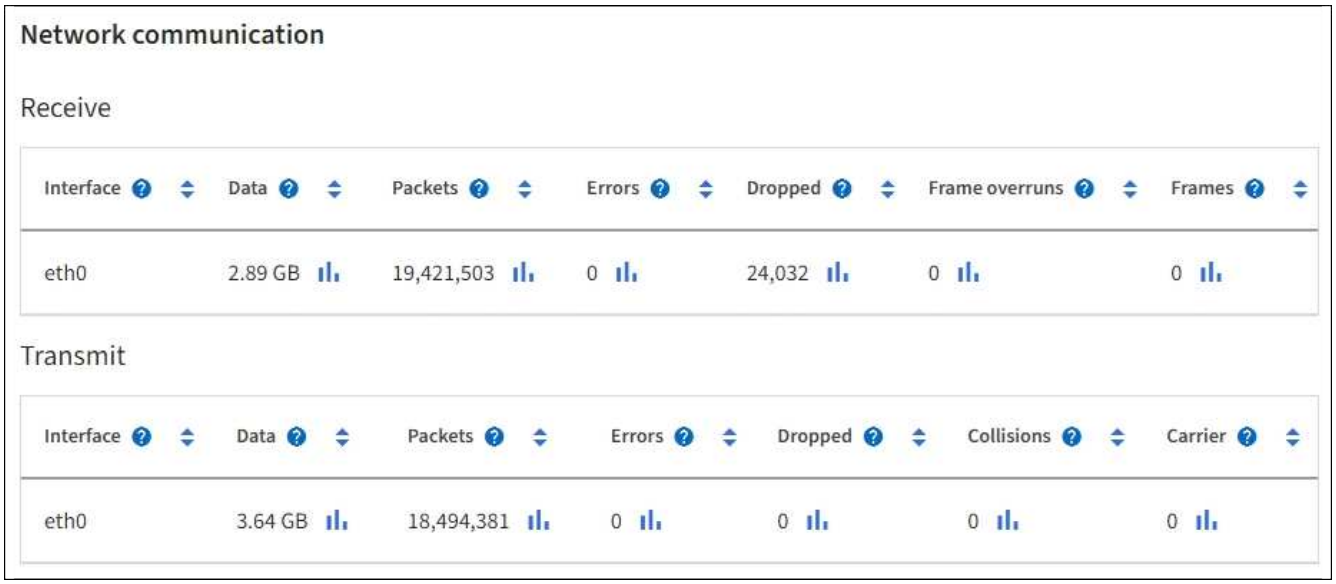
> Die in der Tabelle aufgeführten Werte gehen davon aus, dass alle vier Links verwendet werden.

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

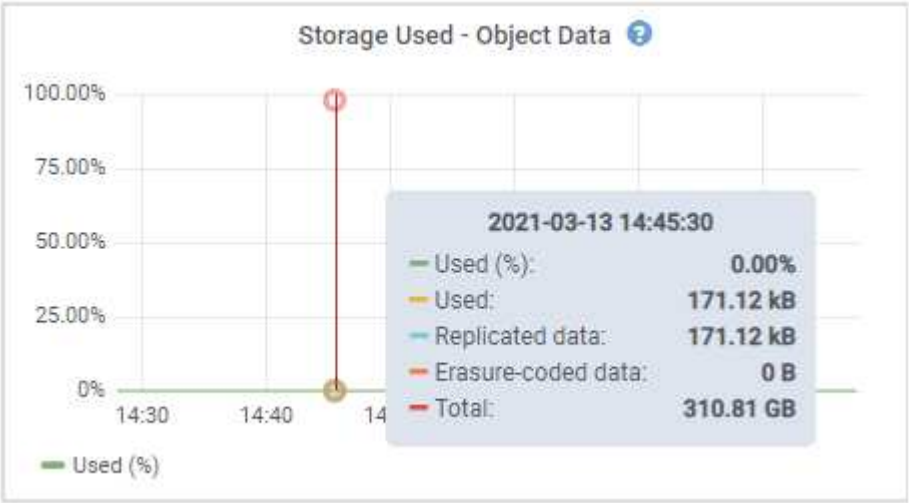
Siehe "Netzwerkverbindungen konfigurieren" Weitere Informationen zum Konfigurieren der 10/25-GbE-Ports.

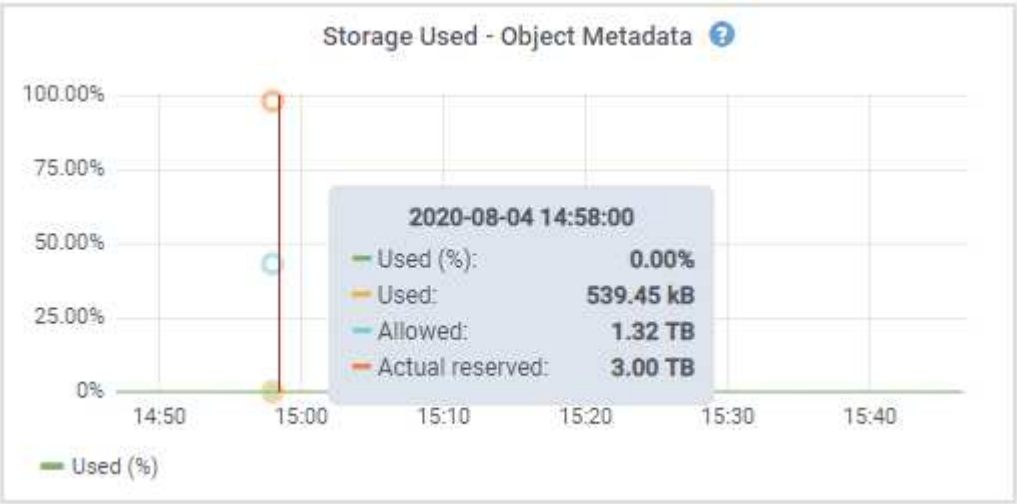
b. Lesen Sie den Abschnitt Netzwerkkommunikation.

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



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





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

Objektspeicher anzuzeigen.

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

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

Disk devices

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

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an

Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplatten- und

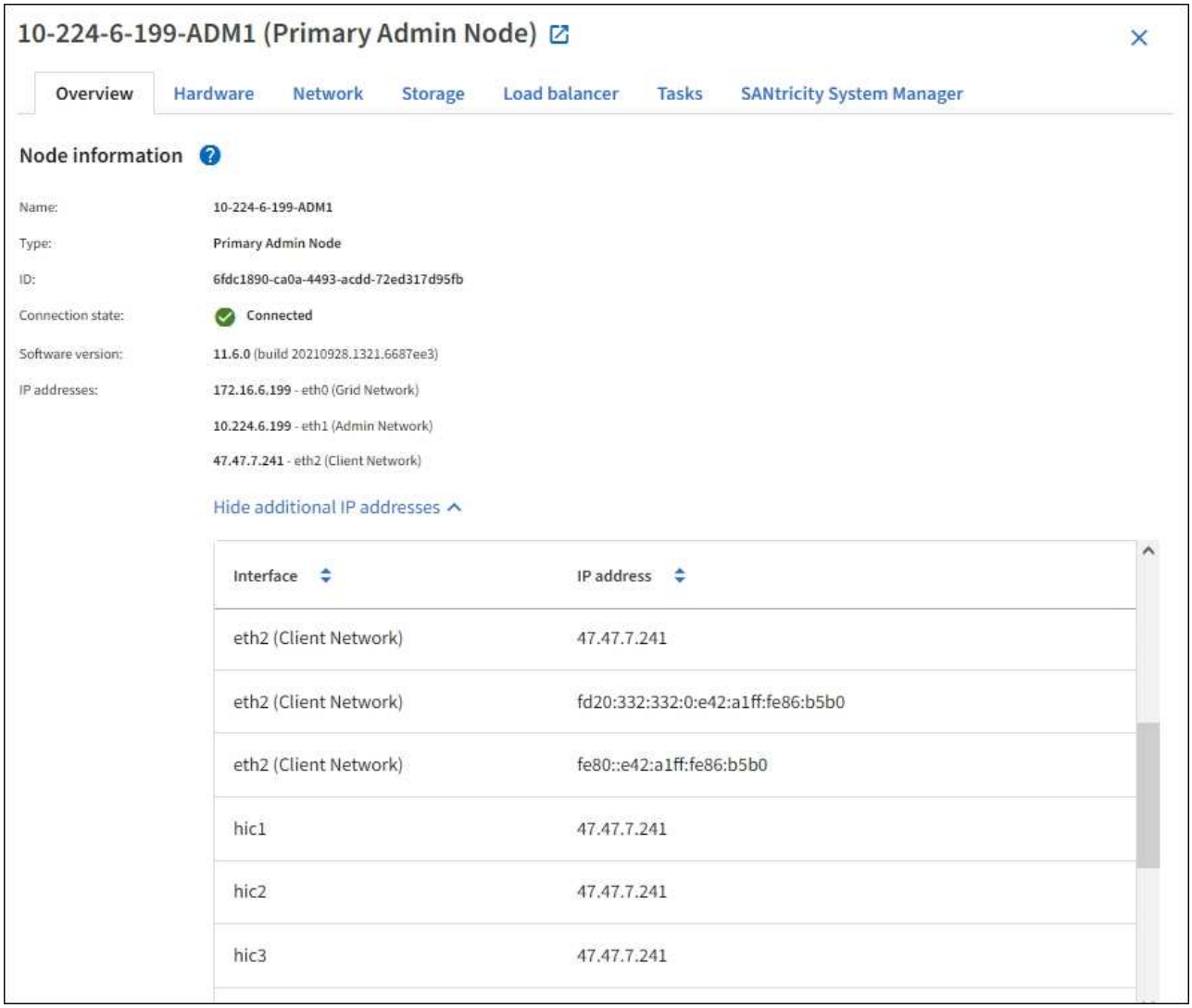
Netzwerkressourcen für jede Service-Appliance, die als Admin-Node oder Gateway-Node verwendet wird, aufgeführt. Außerdem können Sie Arbeitsspeicher, Storage-Hardware, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen, Daten empfangen und übertragen.

Schritte

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

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

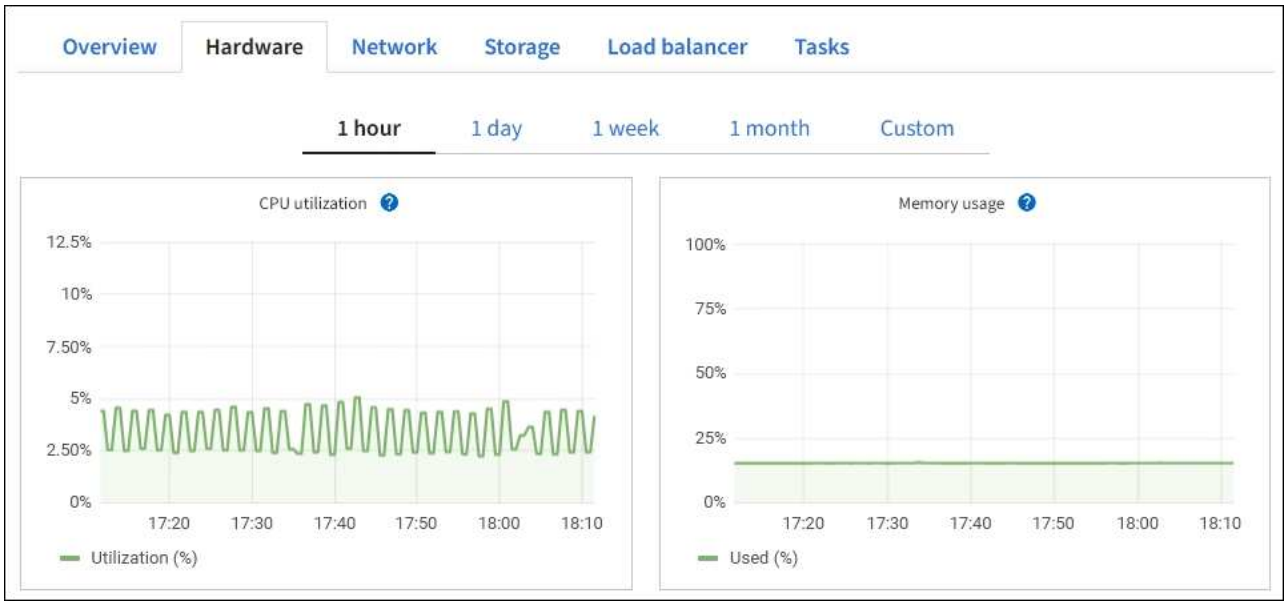
   - **Adlb** und **adlli**: Wird angezeigt, wenn Active/Backup Bonding für die Admin Network Interface verwendet wird
   - **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk.
   - **Hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander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



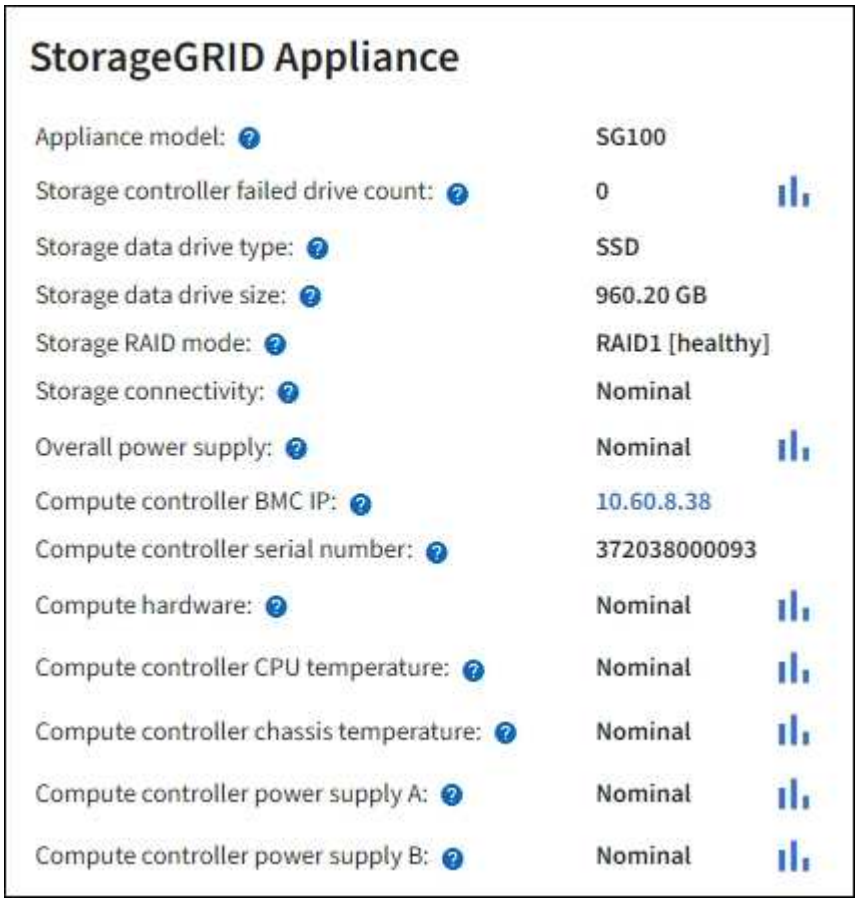
Im Abschnitt „Meldungen“ der Registerkarte „Übersicht“ werden alle aktiven Meldungen für den Node angezeigt.

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

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



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



Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance.

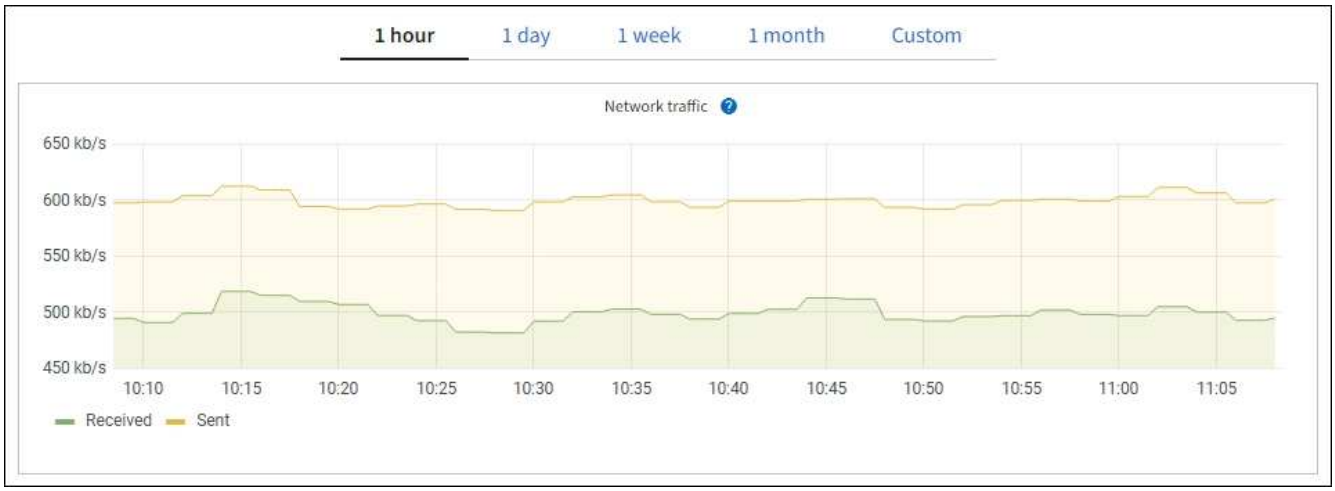
Feld in der Appliance-Tabelle	Beschreibung
Anzahl der Laufwerke bei Ausfall des Storage-Controllers	Die Anzahl der Laufwerke, die nicht optimal sind.
Typ des Speicherdatenspeichers	Der Laufwerkstyp in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe der Speicherdatenlaufwerk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

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

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

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

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



a. Lesen Sie den Abschnitt Netzwerkschnittstellen.

Network interfaces

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

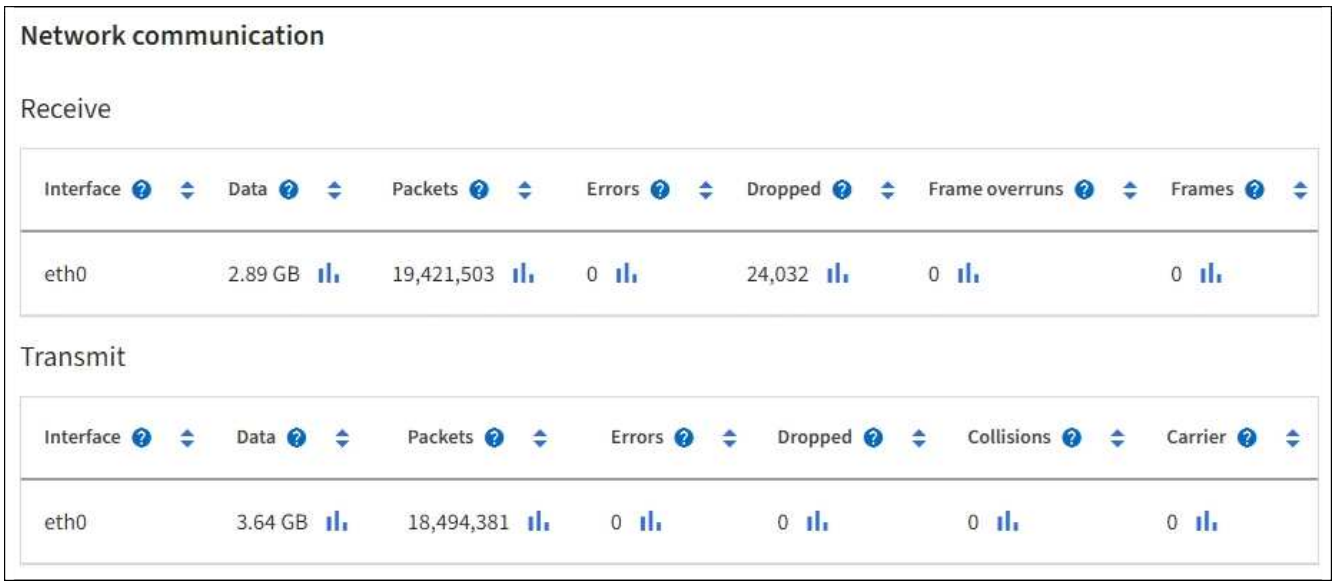
Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle Netzwerkschnittstellen, um festzustellen, ob die vier 40/100-GbE-Netzwerkanschlüsse auf der Appliance für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.

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

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

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

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



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

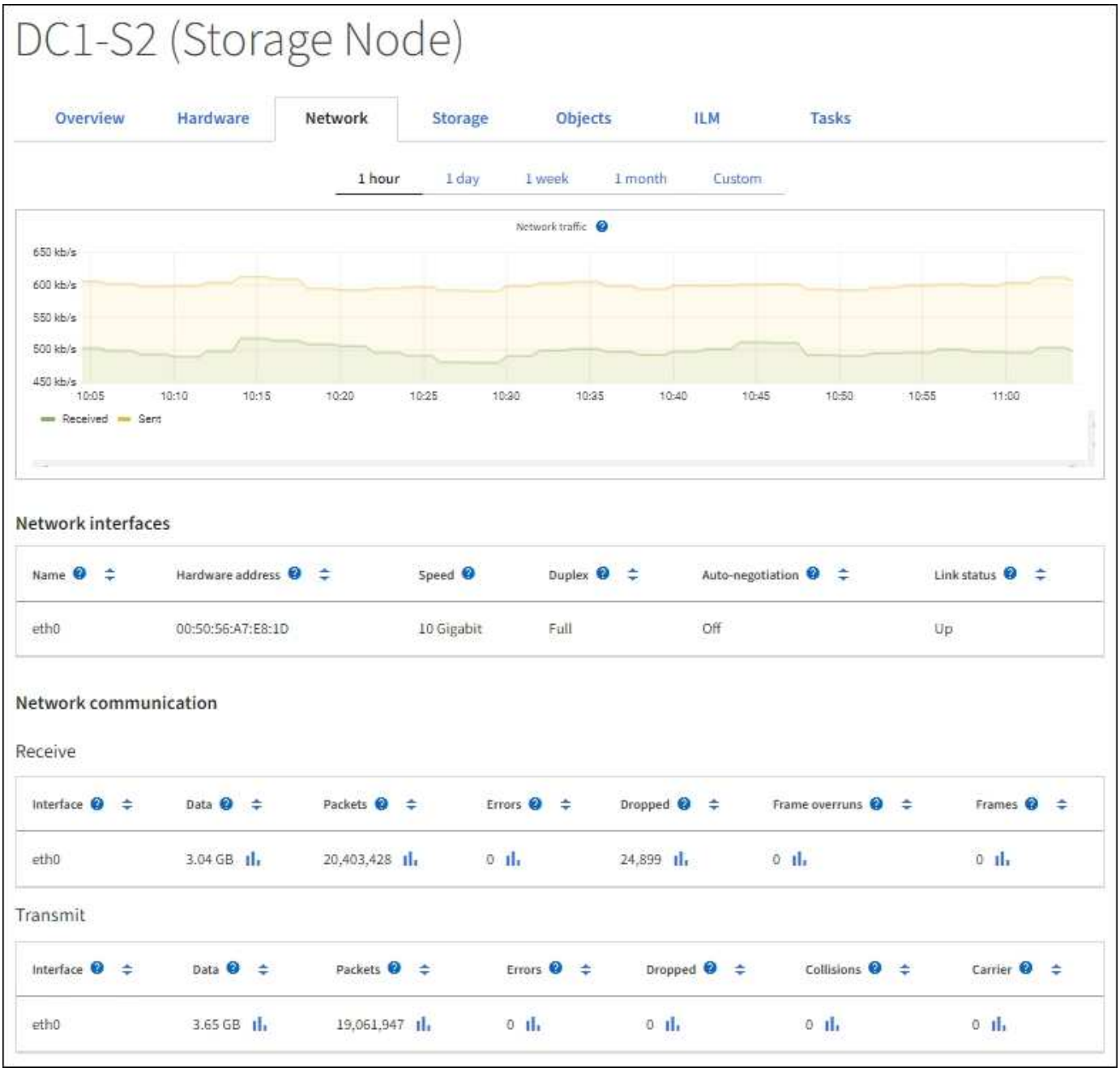
Zeigen Sie die Registerkarte Netzwerk an

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“

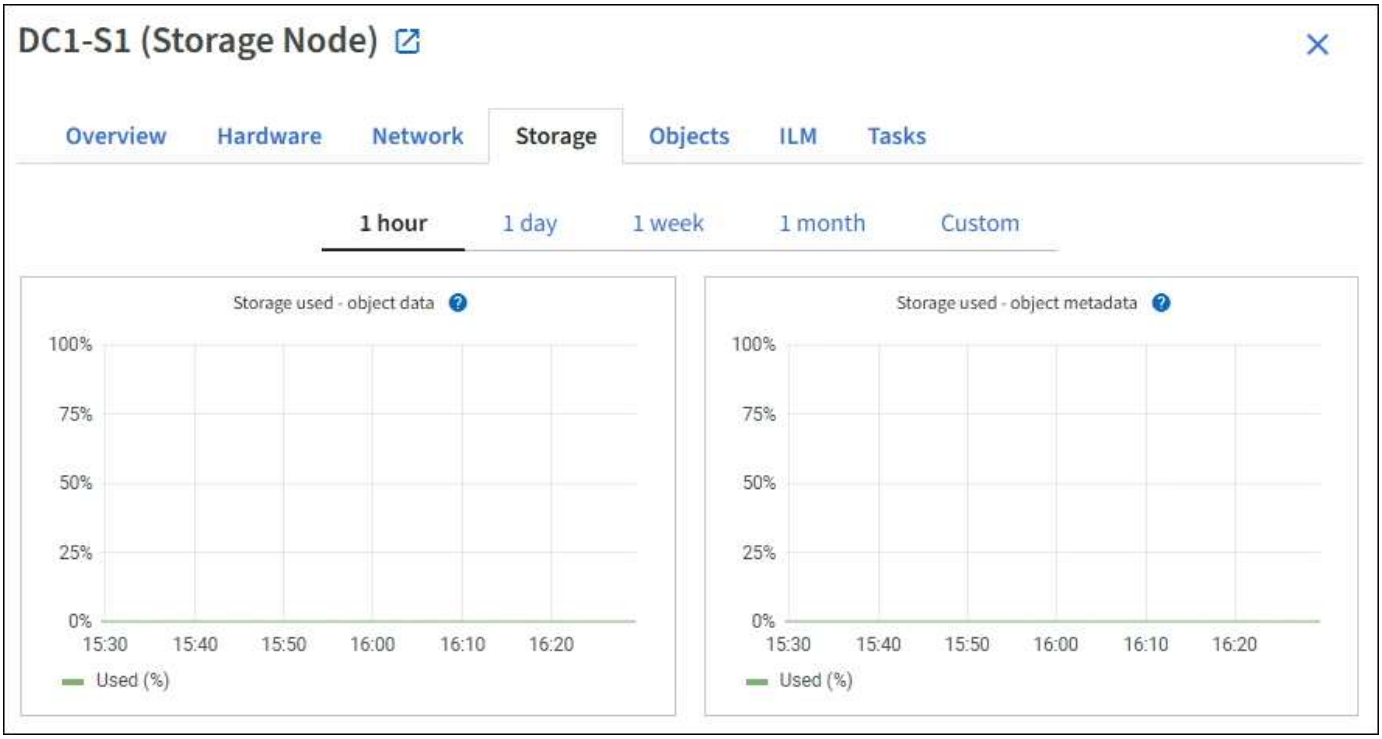
Die Registerkarte „Storage“ fasst Storage-Verfügbarkeit und andere Storage-Metriken zusammen.

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

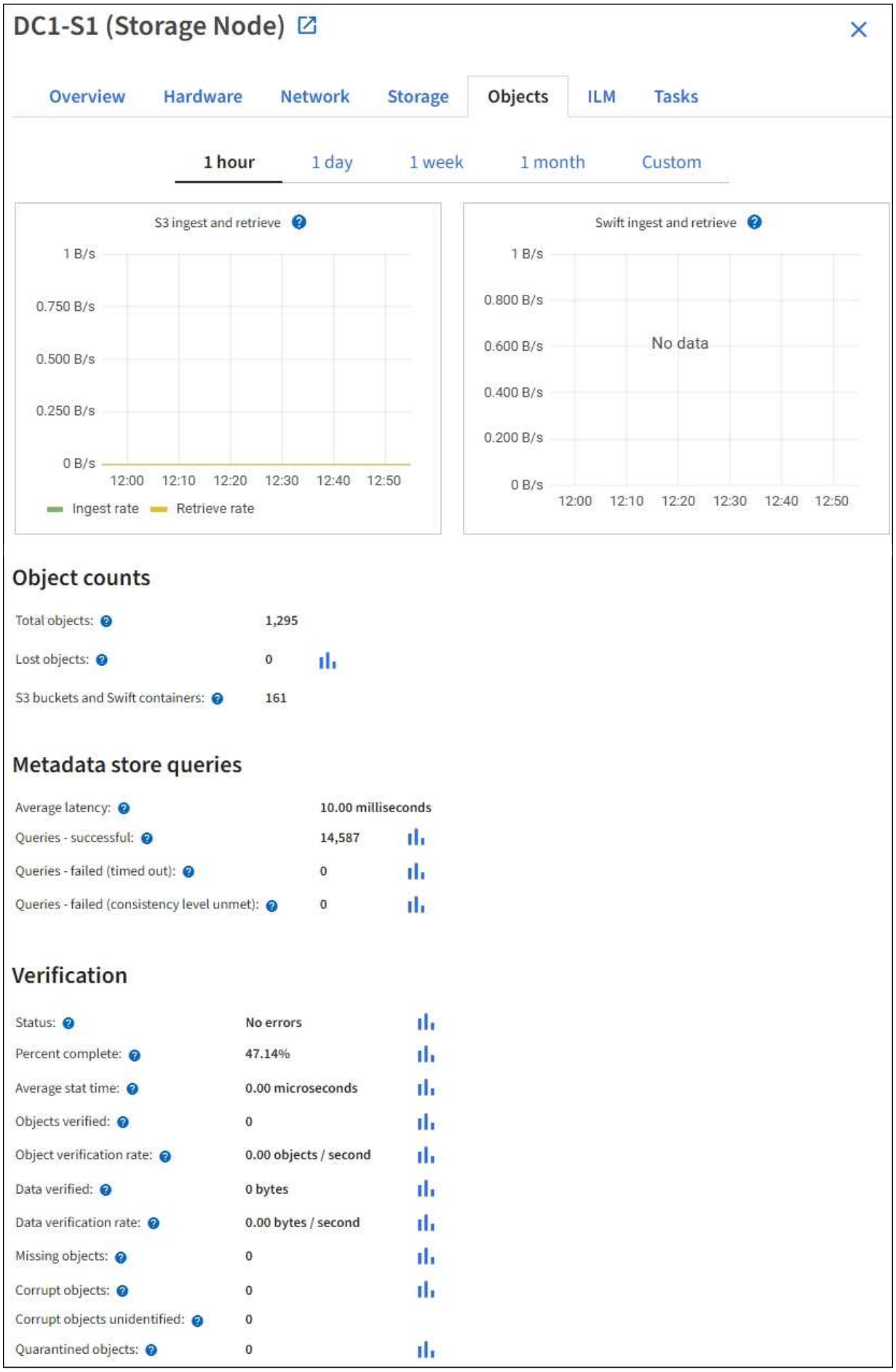
Verwandte Informationen

"Monitoring der Storage-Kapazität"

Zeigen Sie die Registerkarte Objekte an

Die Registerkarte Objekte enthält Informationen zu "S3" Und "Swift" Einspielraten und Abrufen.

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.

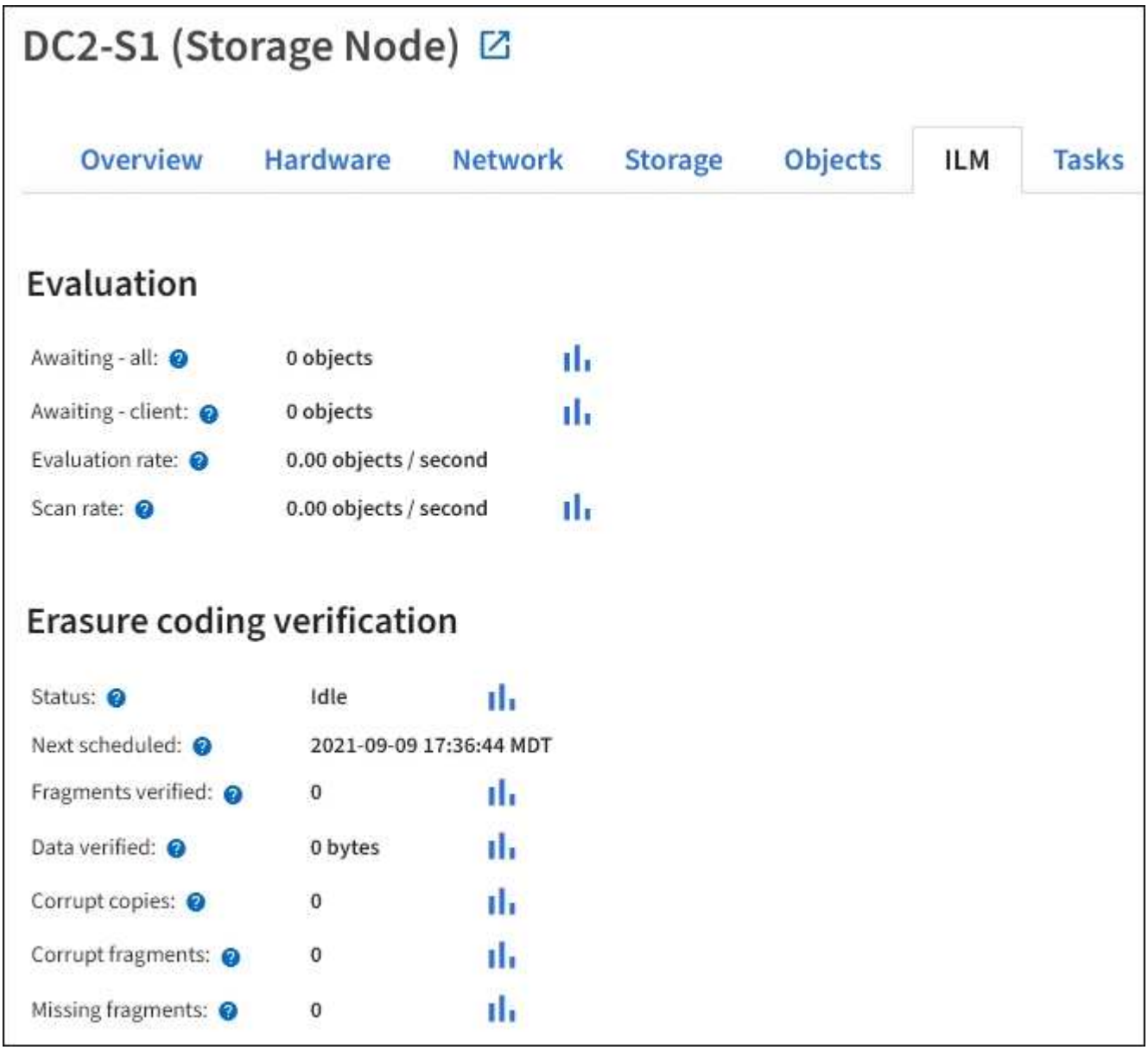

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

Verwenden Sie die Registerkarte Aufgaben

Die Registerkarte Aufgaben wird für alle Nodes angezeigt. Sie können auf dieser Registerkarte einen Node umbenennen oder neu booten oder einen Appliance-Node in den Wartungsmodus versetzen.

Die vollständigen Anforderungen und Anweisungen für die einzelnen Optionen auf dieser Registerkarte finden Sie im Folgenden:

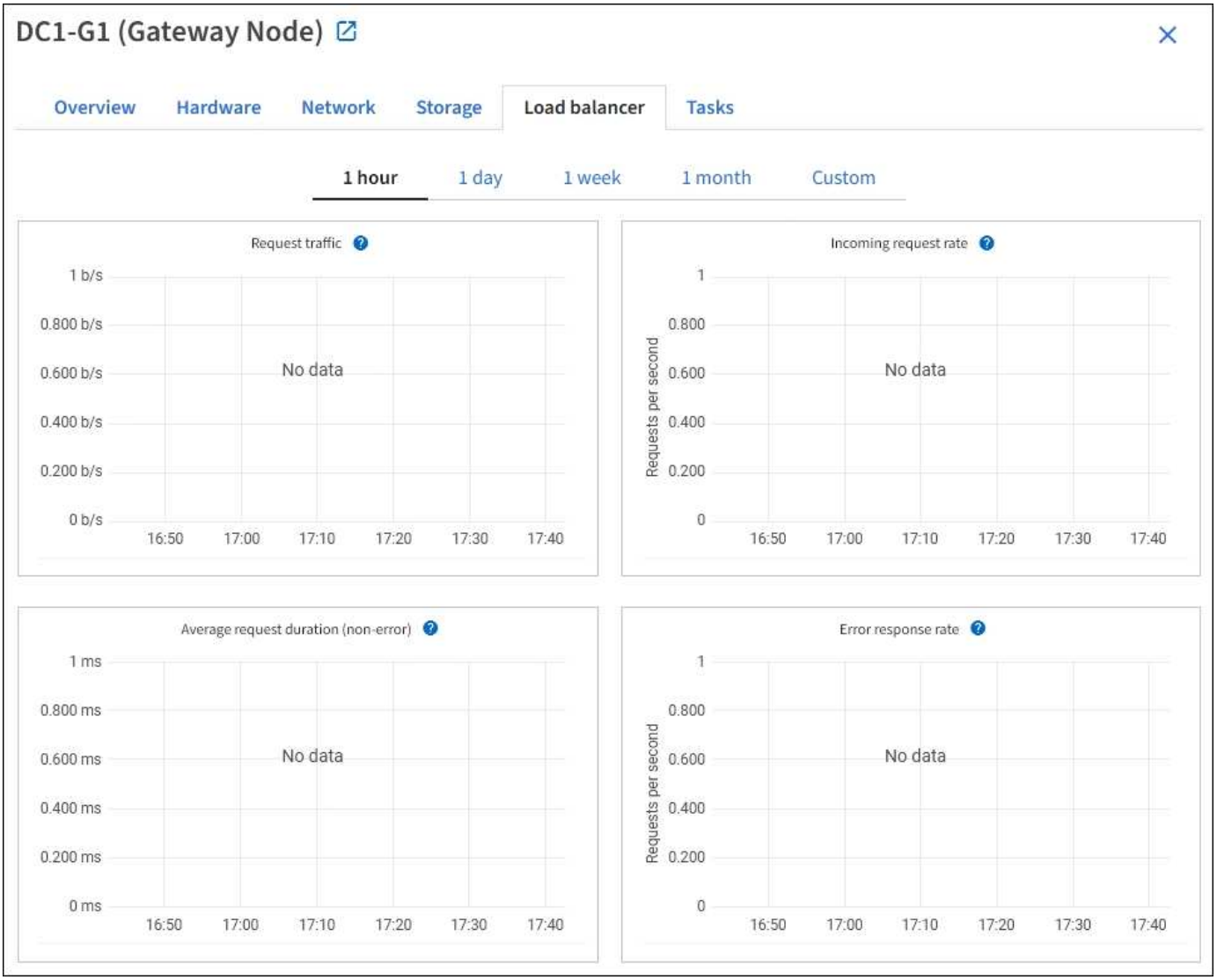
- "Benennen Sie Raster, Standorte und Nodes um"
- "Grid-Node neu booten"
- "Stellen Sie das Gerät in den Wartungsmodus"

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

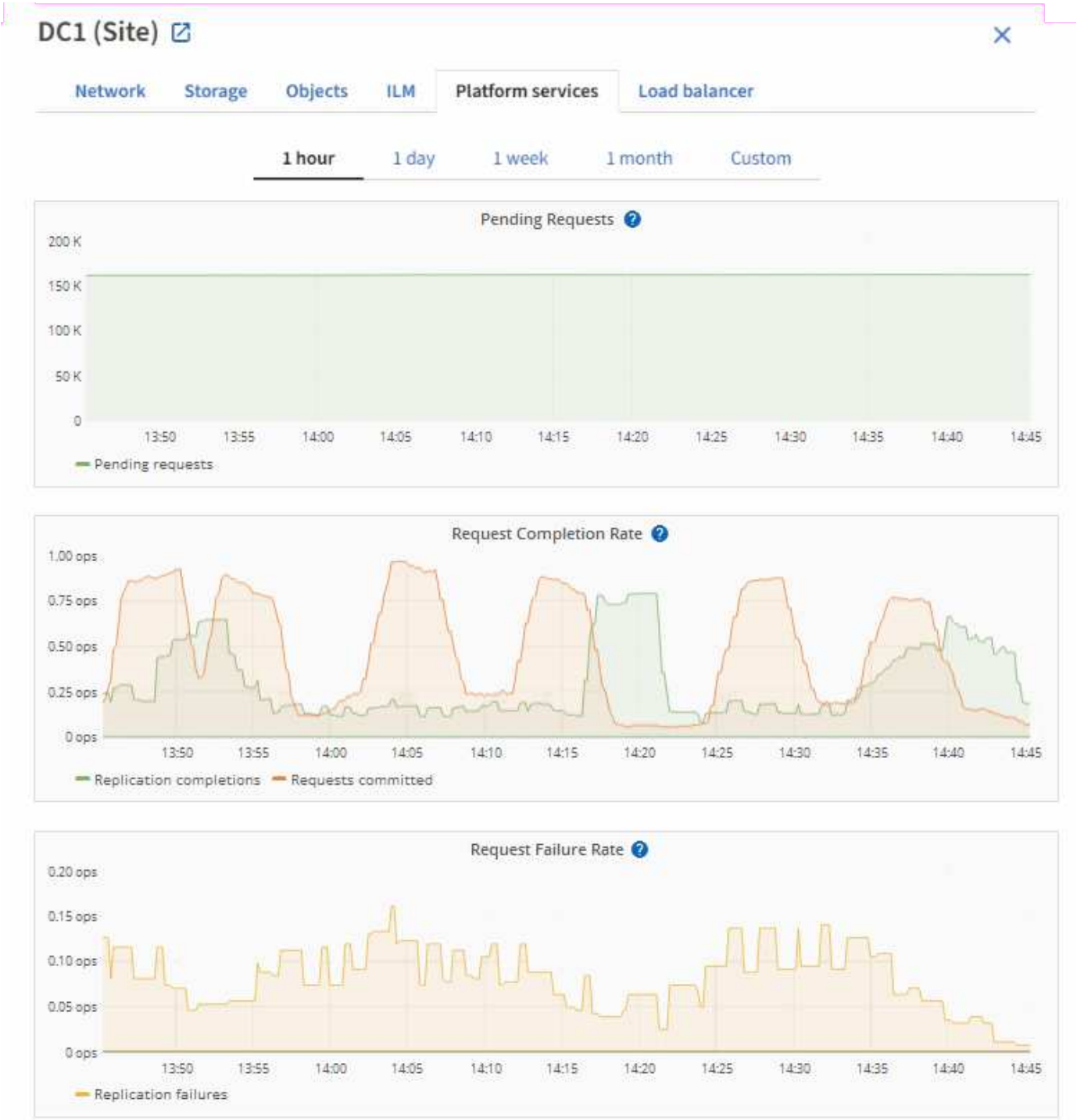
"Monitoring von Lastverteilungsvorgängen"

"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".

Registerkarte Laufwerke managen anzeigen (nur SGF6112)

Auf der Registerkarte Laufwerke managen können Sie auf Details zugreifen und Fehlerbehebungs- und Wartungsaufgaben an den Laufwerken in der SGF6112-Appliance durchführen.

> Die Registerkarte Laufwerke managen wird nur für SGF6112-Storage-Appliance-Nodes angezeigt.

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 das 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.

> 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

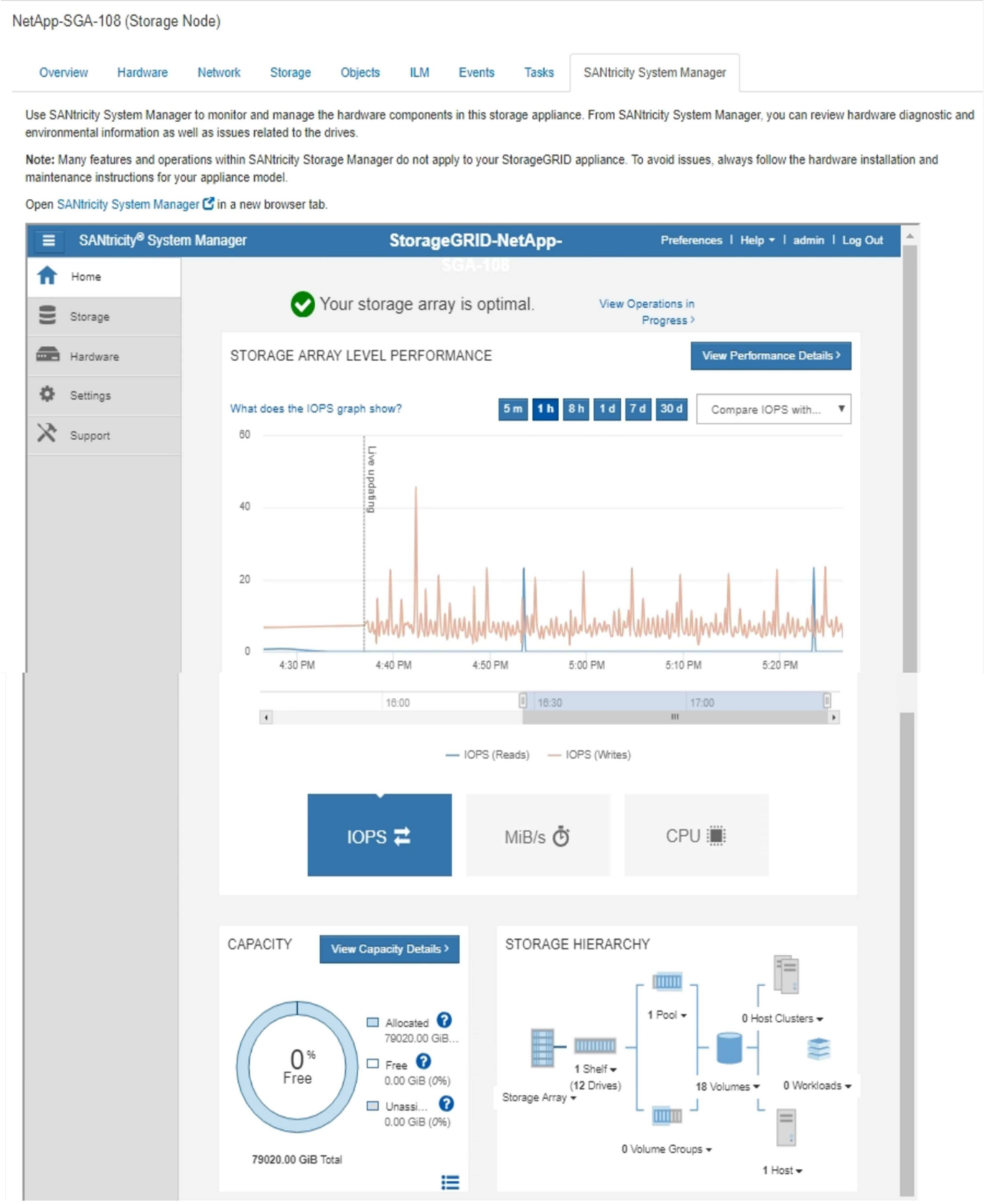
> Informationen zur Konfiguration eines Proxys für E-Series AutoSupport mit SANtricity System Manager finden Sie unter "Senden Sie E-Series AutoSupport-Pakete über StorageGRID".

Um über den Grid-Manager auf den SANtricity System Manager zugreifen zu können, müssen Sie über das 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.

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.

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 System Manager 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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "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
Tarif "Objekt- und Metadatenkapazität des Storage-Node" Wird verbraucht	Wöchentlich
"Information Lifecycle Management-Operationen"	Wöchentlich
"Netzwerk- und Systemressourcen"	Wöchentlich
"Mandantenaktivität"	Wöchentlich
"Client-Operationen für S3 und Swift"	Wöchentlich
"Lastverteilung"	Nach der Erstkonfiguration und nach Konfigurationsänderungen
"Netzverbundverbindungen"	Wöchentlich
"Kapazität des externen Archiv-Storage-Systems"	Wöchentlich

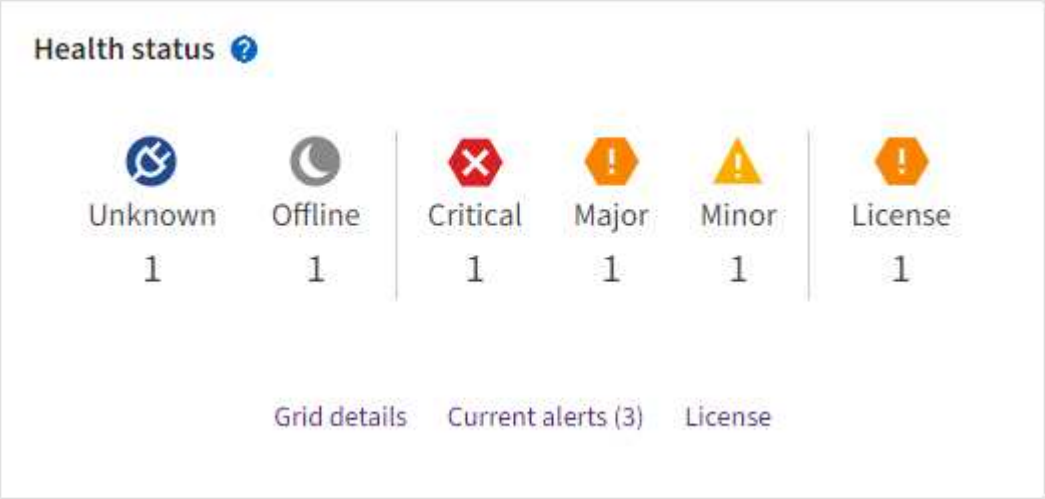
Systemzustand überwachen

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 Warnungen oder Alarme (Altsystem) angezeigt werden, sind nicht unbedingt Probleme mit dem Systembetrieb. Untersuchen Sie die auf der Statuskarte „Systemzustand“ des Grid Manager-Dashboards zusammengefassten Probleme.

Wenn Sie über Warnmeldungen benachrichtigt werden möchten, sobald diese ausgelöst werden, können Sie dies tun "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)	Warnmeldungen sind Derzeit aktiv.
Kürzlich behobene Warnmeldungen	In der letzten Woche ausgelöste Warnmeldungen Jetzt behoben.
Lizenz	Es liegt ein Problem mit der Softwarelizenz für dieses StorageGRID-System vor. Das können Sie "Aktualisieren Sie die Lizenzinformationen nach Bedarf".

Überwachen Sie die Status der Node-Verbindung

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

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

Anzeige aktueller und aufgelöster Warnmeldungen

Aktuelle Alarme: Wenn ein Alarm ausgelöst wird, wird ein Warnsymbol auf dem Dashboard angezeigt. Auf der Seite Knoten wird auch ein Warnungssymbol für den Knoten angezeigt. Wenn "Benachrichtigungen für Warnmeldungen sind konfiguriert", Eine E-Mail-Benachrichtigung wird ebenfalls 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 sich das Video angesehen: "Video: Übersicht über Warnmeldungen für StorageGRID 11.8"

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

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

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

Schritte

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

   Standardmäßig werden aktuelle Warnmeldungen wie folgt angezeigt:

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

     Die Seite Aktuelle Warnmeldungen wird alle zwei Minuten aktualisiert.

2. Um die Gruppen von Warnmeldungen zu erweitern, wählen Sie das Down-Menü aus ⌄. Um einzelne Warnmeldungen 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 aus ⇅ In jeder Spaltenüberschrift.
   - 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 die haben "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen" Um eine Warnregel 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 die haben "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen" So bearbeiten Sie eine Warnungsregel:

> 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.

Das können Sie "Informationen zur Storage-Kapazität anzeigen" Für das gesamte Grid, für jeden Standort und für jeden Storage-Node im 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.

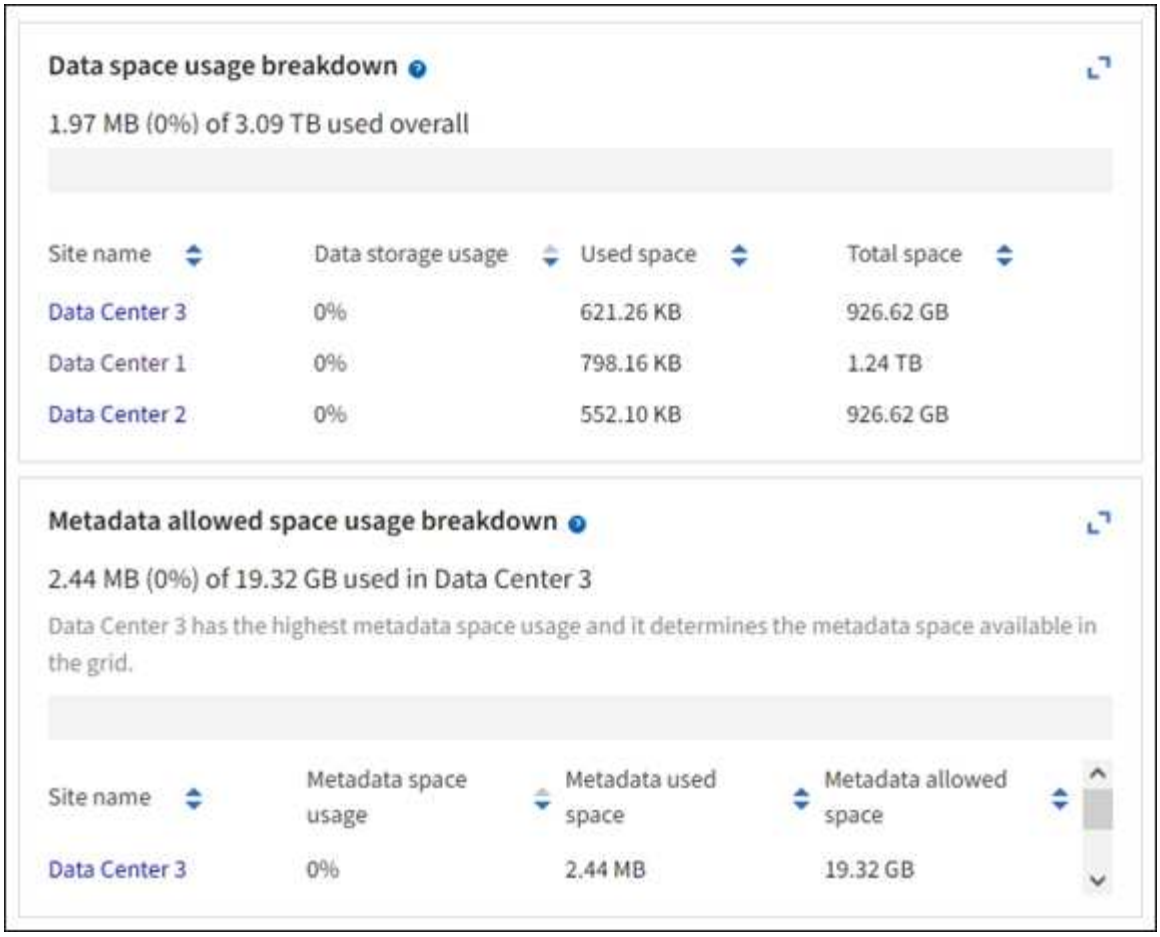
Schritte

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

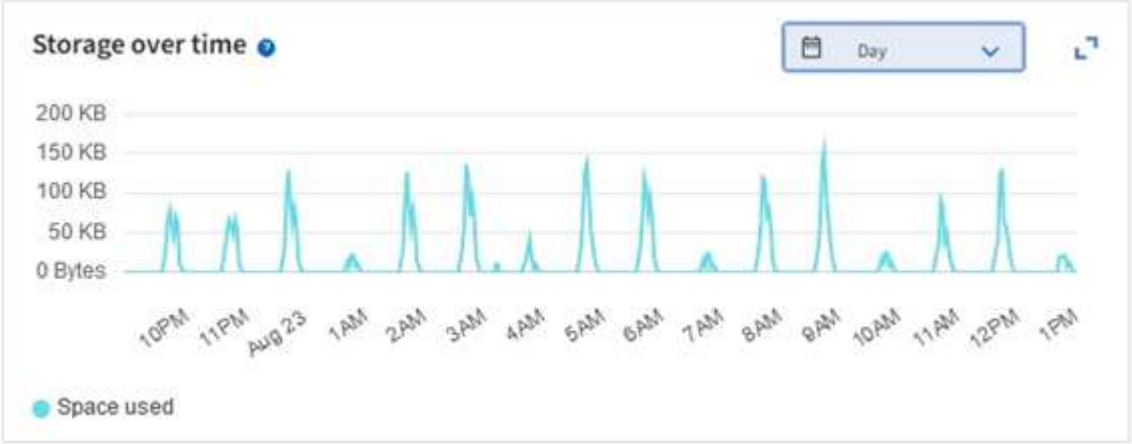
    a. Wählen Sie **Dashboard > Übersicht**.

    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.

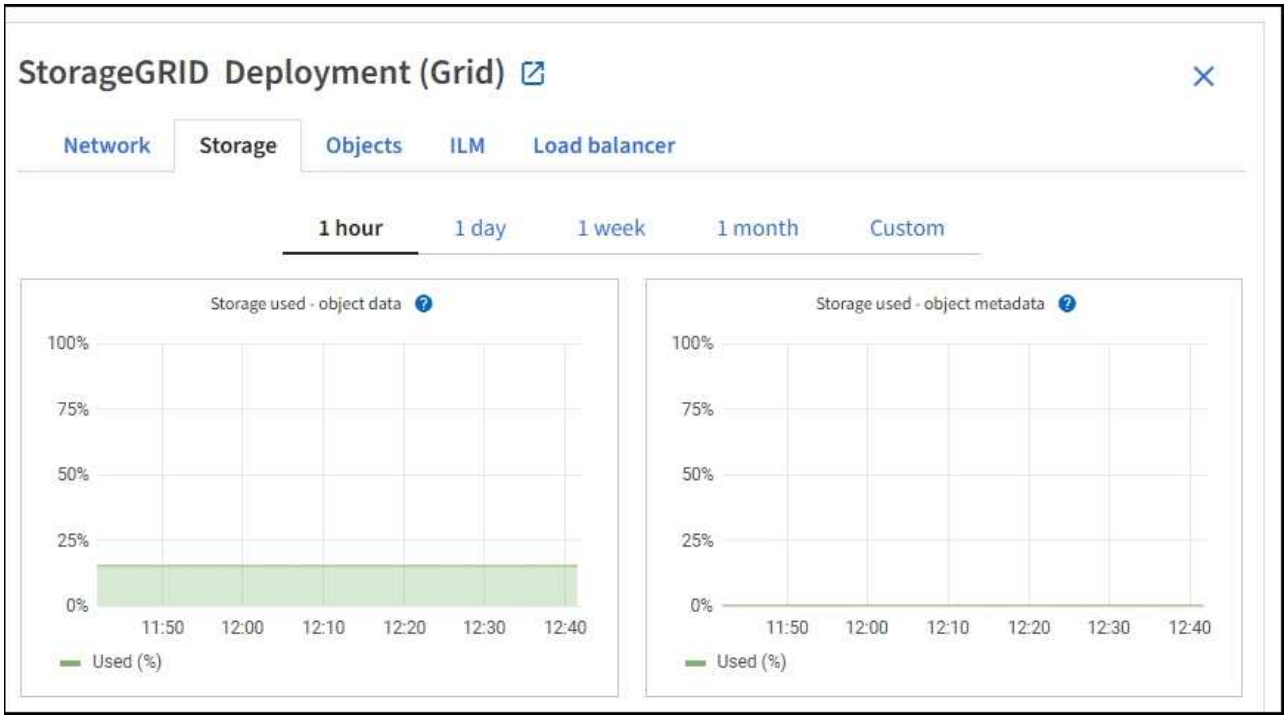
    > Die Zusammenfassung enthält keine Archivierungsmedien.



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**.
   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.

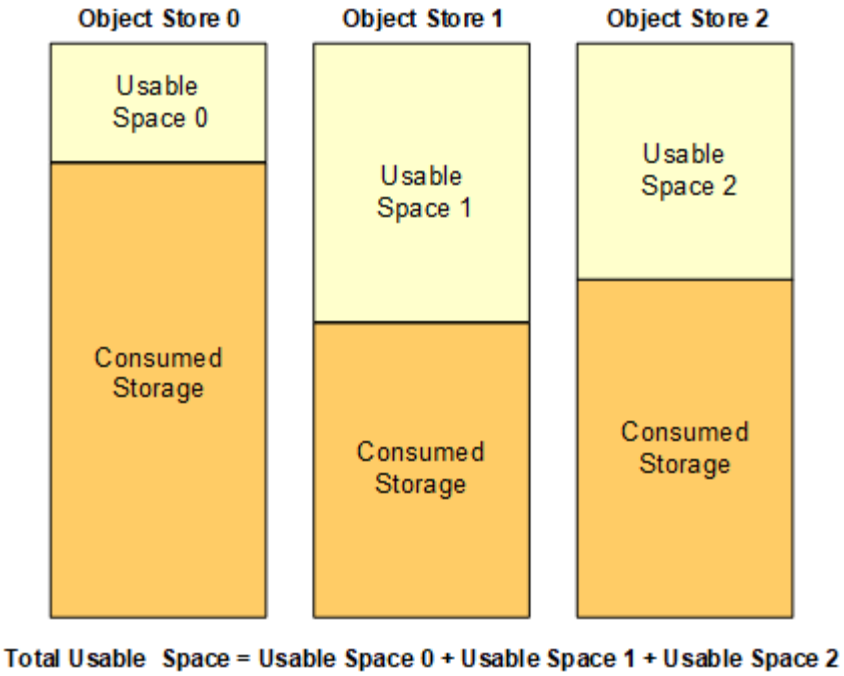
   Weitere Informationen zur Planung einer Speichererweiterung finden Sie im "Anweisungen zur Erweiterung von StorageGRID".

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

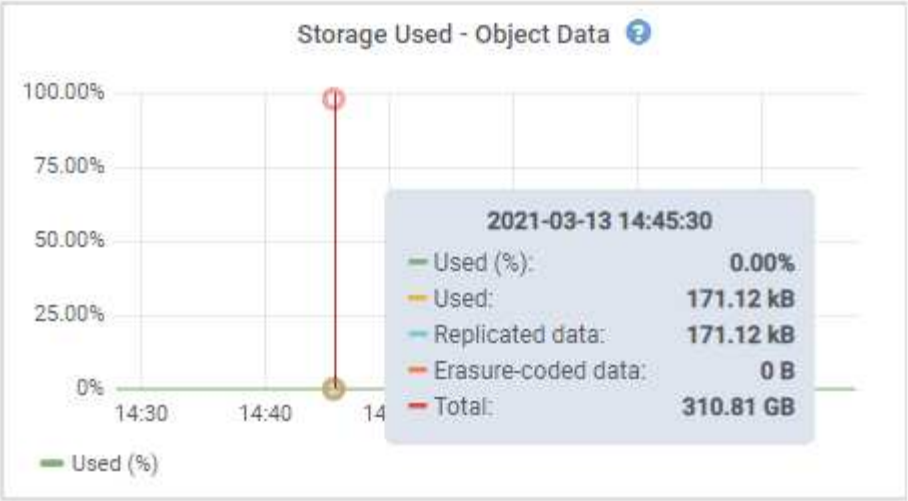
1. Wählen Sie **NODES** > ***Storage Node*** > **Storage** aus.

   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 der `storagegrid_storage_utilization_data_bytes` Metrisch.



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

> Klicken Sie auf die Diagrammsymbole, um Diagramme dieser Werte anzuzeigen In den Spalten verfügbar.

Disk devices

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

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Überwachen Sie die Werte im 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".

Der "Niedriger Objekt-Storage" Die Meldung wird ausgelöst, wenn nicht genügend Speicherplatz zum Speichern von Objektdaten auf einem Storage-Node verbleibt.

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

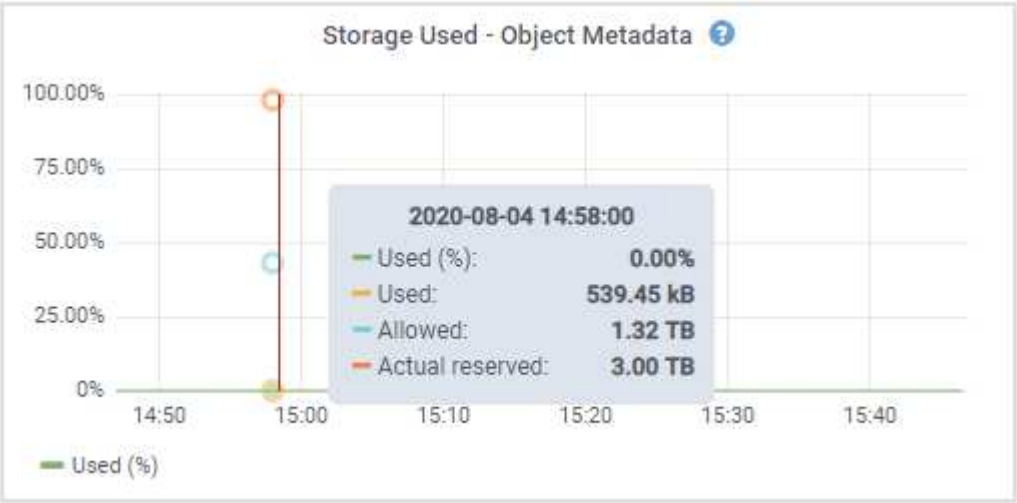
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage 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 **NODES** > ***Storage Node*** > **Storage** aus.
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. Informationen darüber, wie dieser Wert für jeden Storage-Node bestimmt wird, finden 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. Informationen dazu, wie dieser Wert für jeden Storage-Node berechnet wird, finden 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 Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten, um abzuschätzen, wann Sie dies benötigen "Erweitern Sie ein Raster".

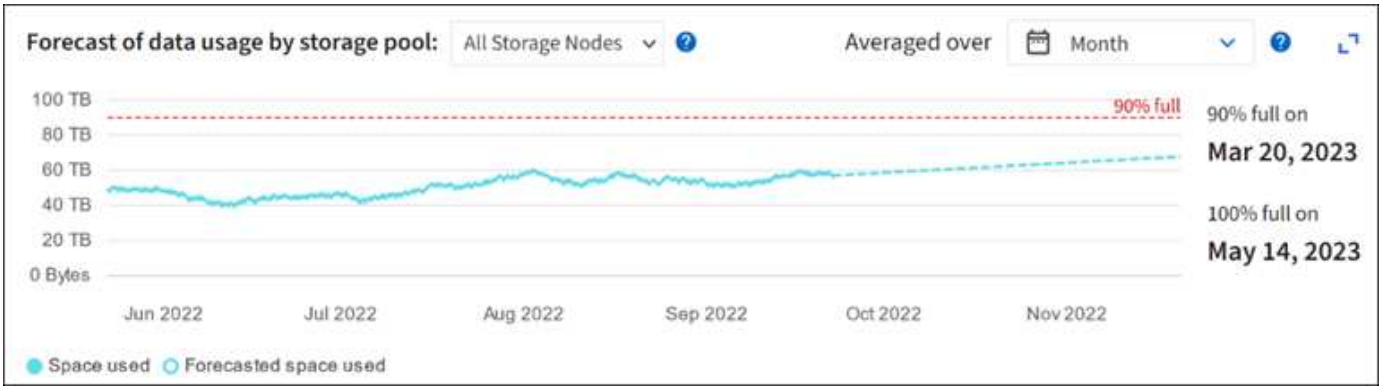
Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie einen kürzeren Bereich aus dem Pulldown-Menü **gemittelt über** aus, um nur die neuesten Aufnahmemuster wiederzugeben. Wenn Sie saisonale Muster bemerken, wählen Sie einen längeren Bereich aus.

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 Sie die Seite KNOTEN

Schritte

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

> Die Diagramme auf der Seite **NODES** werden in einem zukünftigen StorageGRID-Release durch die entsprechenden Dashboard-Karten ersetzt.

1. Wählen Sie **KNOTEN**.
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.
4. Sehen Sie sich im Abschnitt ILM-Warteschlange die folgenden Attribute an.

   > 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.

   - **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 Reparatur desselben Objekts erhöht sich möglicherweise erneut, wenn die Replikation nach der Reparatur fehlgeschlagen ist.

   Diese Attribute können nützlich sein, wenn Sie den Fortschritt der Wiederherstellung von Storage Node Volumes überwachen. Wenn die Anzahl der versuchten Reparaturen gestoppt wurde und ein vollständiger Scan abgeschlossen wurde, wurde die Reparatur wahrscheinlich abgeschlossen.

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.

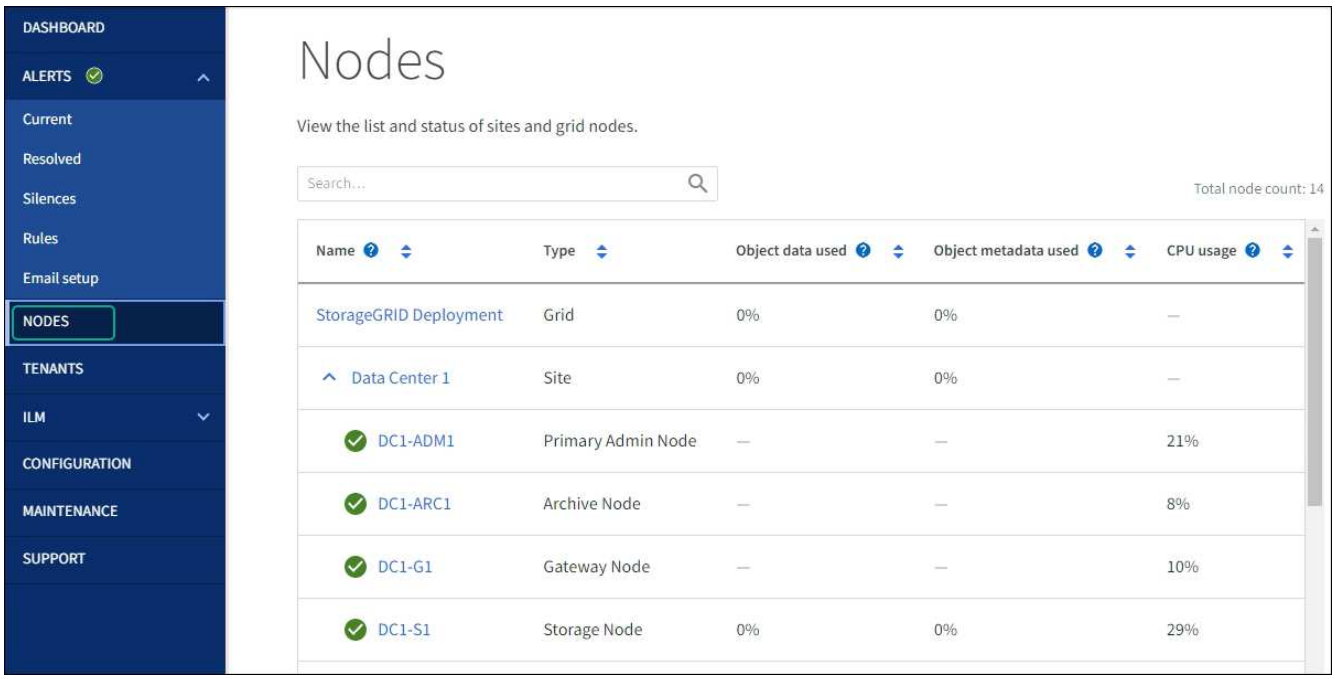
Überwachen Sie die Konnektivität und die Netzwerk-Performance mit dem Grid Manager, damit Sie bei Problemen umgehend auf Probleme reagieren können.

Darüber hinaus sollten Sie in Betracht ziehen "Erstellen von Klassifizierungsrichtlinien für den Netzwerkverkehr" So können Sie den Datenverkehr zu bestimmten Mandanten, Buckets, Subnetzen oder Endpunkten des Load Balancer überwachen. Sie können Richtlinien zur Begrenzung des Datenverkehrs nach Bedarf festlegen.

Schritte

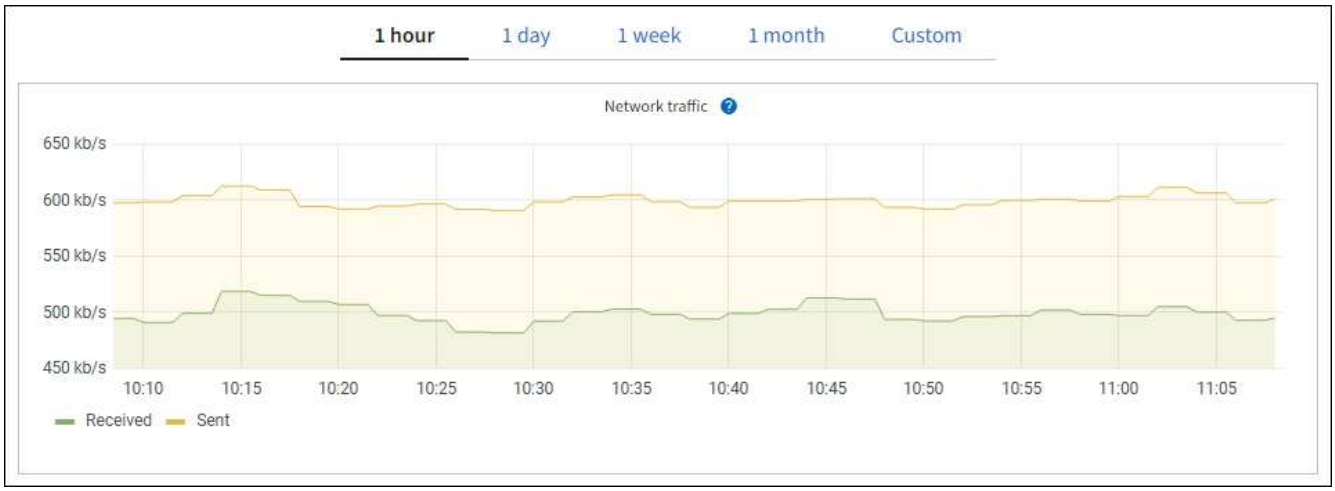
1. Wählen Sie **KNOTEN**.

   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

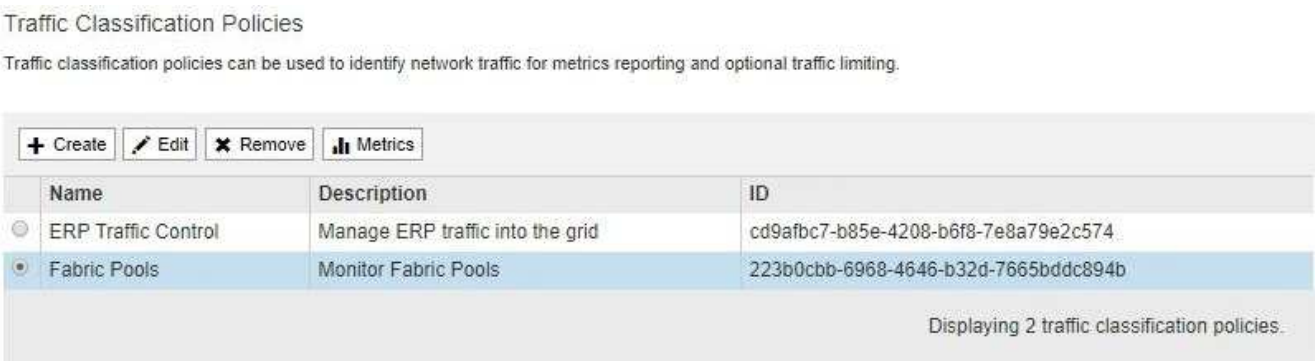
Transmit

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 **CONFIGURATION** > **Network** > **traffic classification**.

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"

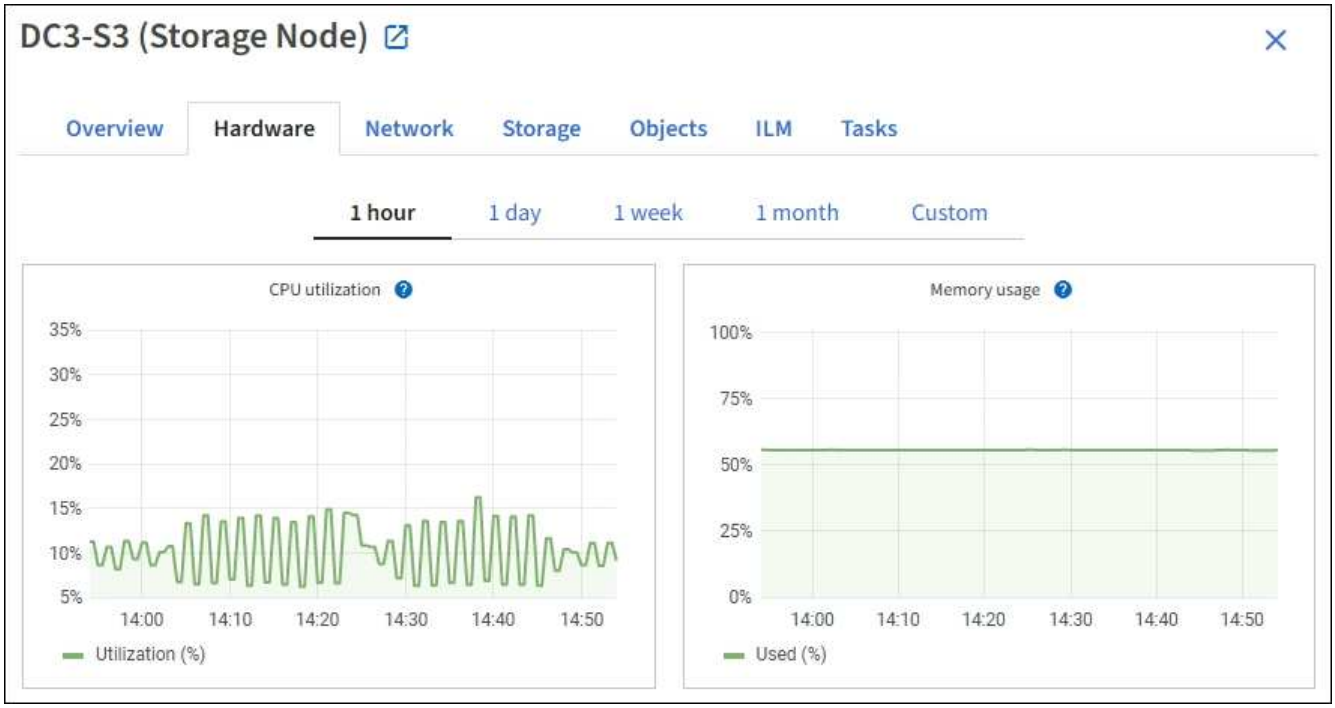
"Überwachen Sie die Status der Node-Verbindung"

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 **NODES** 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- und Swift-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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Root-Zugriff oder Mandantenkonten".

Alle Mandanten anzeigen

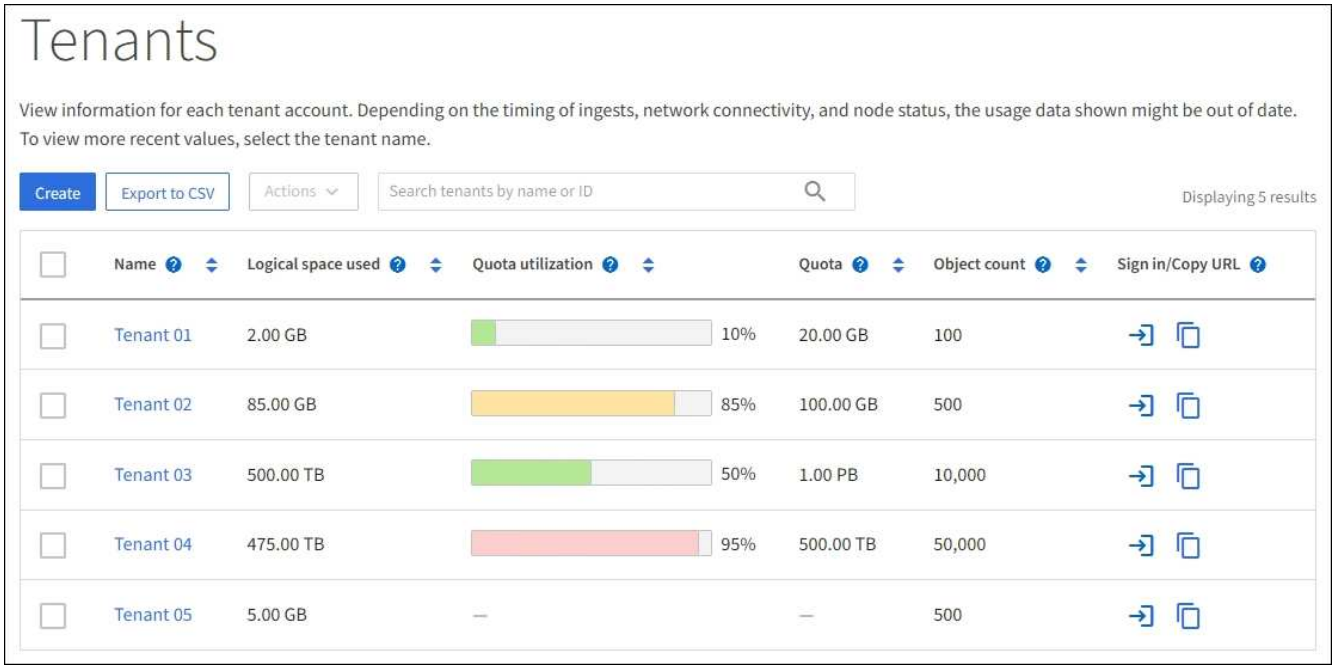
Auf der Seite Tenants werden grundlegende Informationen für alle aktuellen Mandantenkonten angezeigt.

Schritte

1. Wählen Sie **MIETER**.
2. Überprüfen Sie die auf den Mandanten-Seiten angezeigten Informationen.

   Für jeden Mandanten werden der verwendete logische Speicherplatz, die Kontingentnutzung, Kontingente und Objektanzahl aufgelistet. Wenn kein Kontingent für einen Mandanten festgelegt ist, enthalten die Felder Quotenauslastung und Quota einen Strich (—).

   > Die Werte für den genutzten Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.



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

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

   Der Inhalt des `.csv` Datei sieht wie das folgende Beispiel aus:

   Sie können das öffnen `.csv` Datei in einer Tabellenkalkulationsanwendung speichern oder in 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.

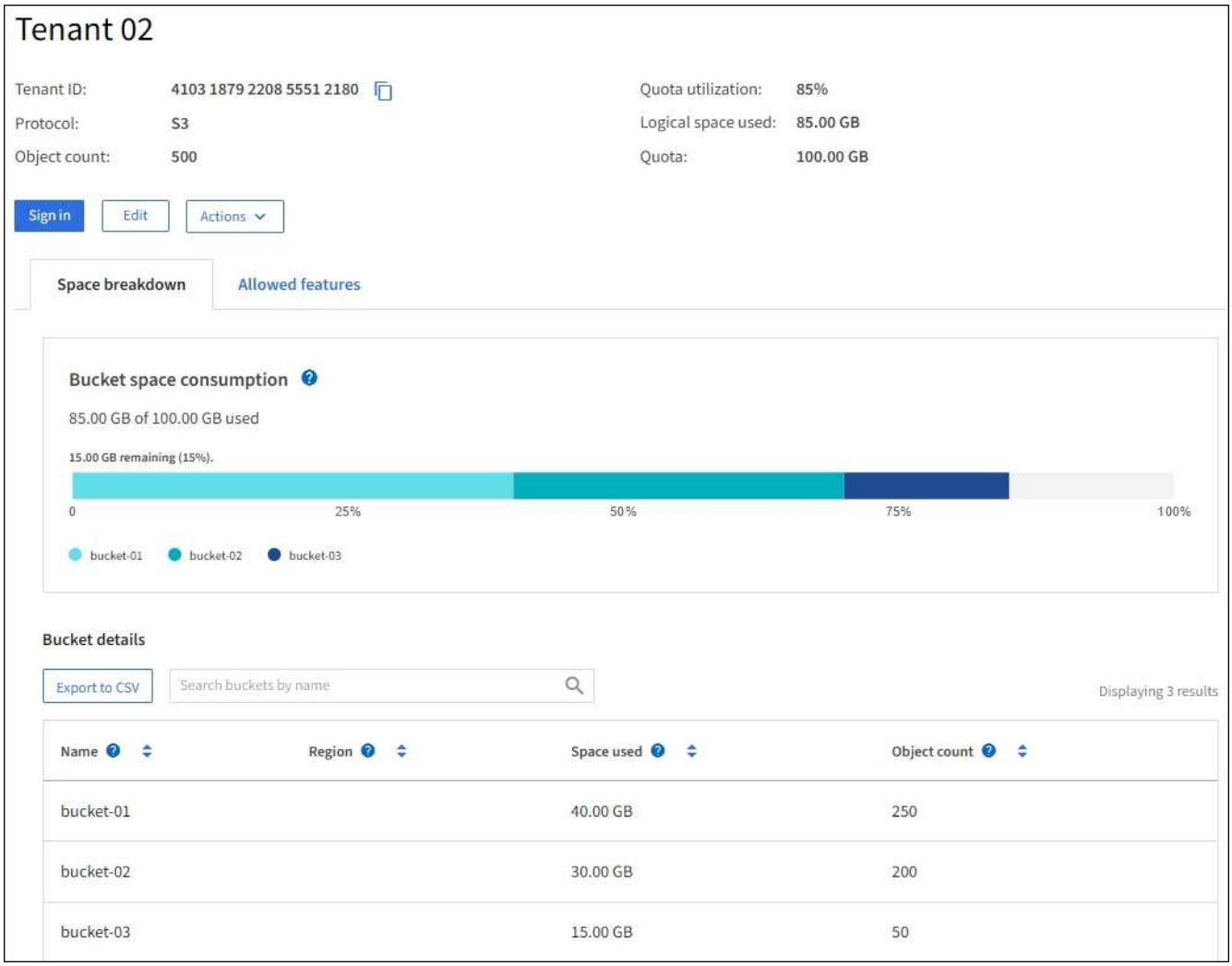
Zeigen Sie eine bestimmte Serviceeinheit an

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 bietet zusammenfassende Informationen für den Mandanten, einschließlich der Objektanzahl des Mandanten, der Kontingentauslastung, des verwendeten logischen Speicherplatzes und der Kontingenteinstellung.

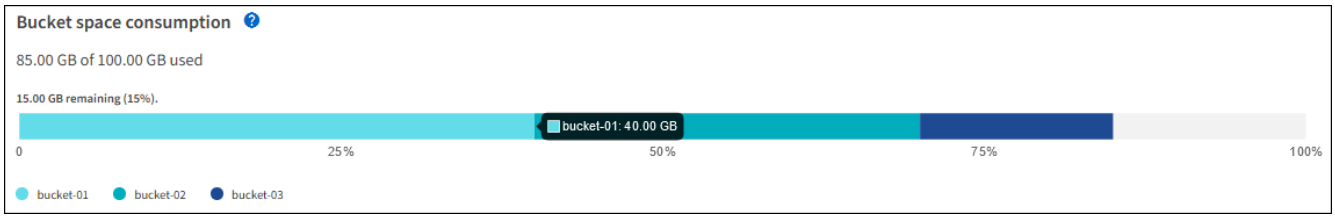
3. Sehen Sie sich auf der Registerkarte **Raumaufschlüsselung** das Diagramm **Speicherplatzverbrauch** an.

   In diesem Diagramm wird der gesamte Speicherplatzverbrauch aller S3-Buckets (oder Swift-Container) des Mandanten angezeigt.

   Wenn ein Kontingent für diesen Mandanten festgelegt wurde, wird die Menge der verwendeten und verbleibenden Kontingente im Text angezeigt (z. B. `85.00 GB of 100 GB used`). Wenn kein Kontingent festgelegt wurde, hat der Mieter eine unbegrenzte Quote, und der Text enthält nur die Menge des belegten Speicherplatzes (z. B. `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 Kontingentnutzung basiert auf internen Schätzungen und kann in einigen Fällen sogar 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 es vorübergehend verhindert werden, dass ein Mandant neue Objekte hochgeladen wird, bis die Kontingentnutzung neu berechnet wird. Berechnungen zur Kontingentnutzung können 10 Minuten oder länger dauern.

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

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 (oder Swift-Container) 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.

   Den Inhalt eines einzelnen S3-Mandanten `.csv` Datei sieht wie das folgende Beispiel aus:

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

   Sie können das öffnen `.csv` Datei in einer Tabellenkalkulationsanwendung speichern oder in 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. Siehe "Mandantenkonto bearbeiten" Wenn 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 **CONFIGURATION** > **Network** > **traffic classification**.

   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.

Siehe "Verwalten von Richtlinien zur Verkehrsklassifizierung" Finden Sie weitere Informationen.

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.

Siehe "Prüfung von Audit-Protokollen" Finden Sie weitere Informationen.

Verwenden Sie Prometheus-Kennzahlen

Optional können Sie mit den Prometheus-Kennzahlen Berichte über die Mandantenaktivität erstellen.

- Wählen Sie im Grid Manager die Option **SUPPORT** > **Tools** > **Metriken**. Kunden können vorhandene

Dashboards wie S3 Overview zur Überprüfung von Client-Aktivitäten nutzen.

> 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.

Siehe "Prüfen von Support-Kennzahlen" Finden Sie weitere Informationen.

Monitoring von S3- und Swift-Client-Operationen

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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

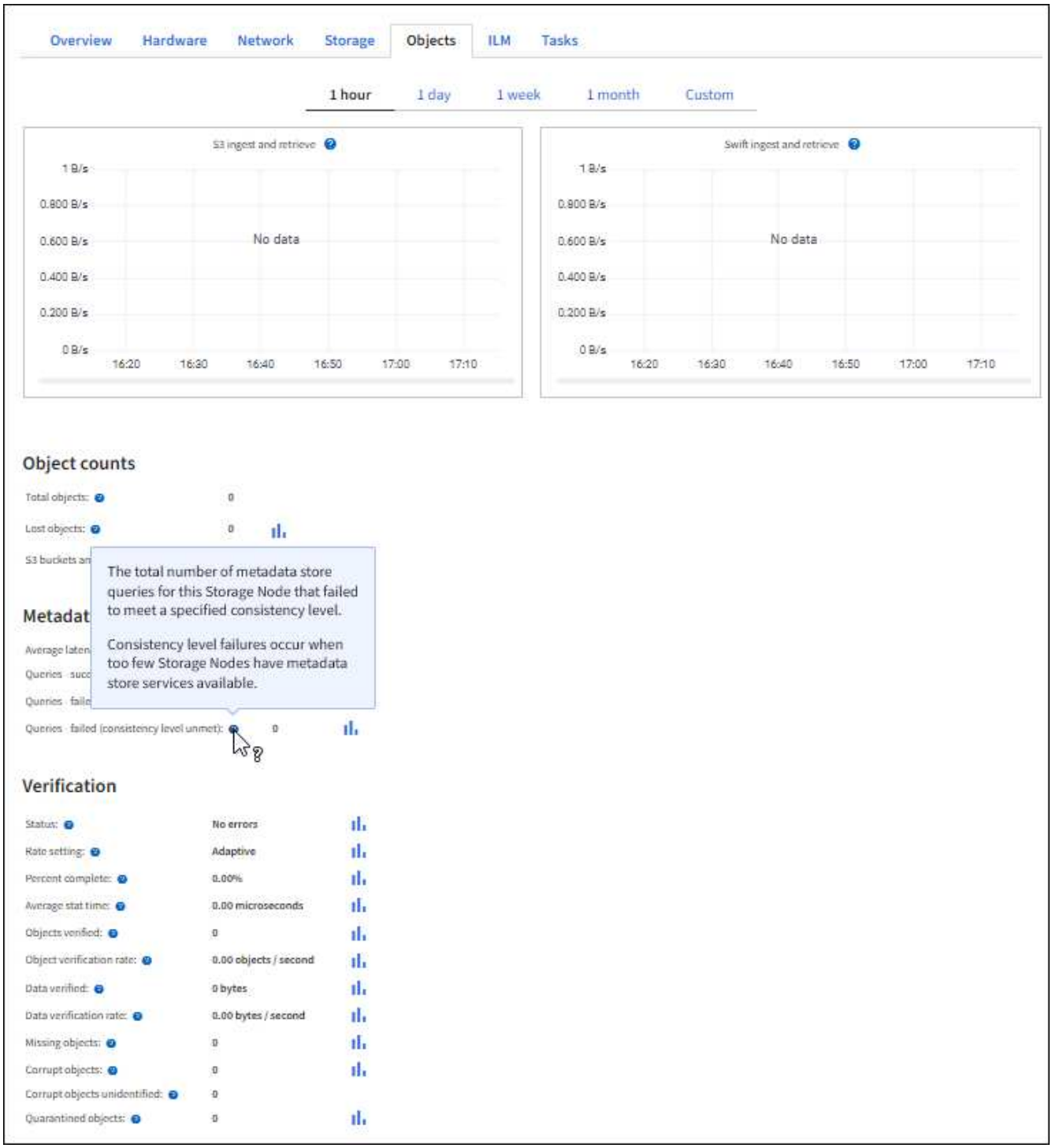
Schritte

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

   Das Diagramm zeigt die Aufnahme- und Abrufraten von S3 und Swift für das gesamte StorageGRID System 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 "Konfiguration von S3- und Swift-Client-Verbindungen".

Schritte

1. Wenn sich S3- oder Swift-Clients über den Load Balancer Service verbinden, überprüfen Sie, ob Admin-Nodes oder Gateway-Nodes den Datenverkehr aktiv verteilen, wie Sie erwarten:
   a. Wählen Sie **KNOTEN**.
   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 aus "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 zu allen überwachen "Netzverbundverbindungen", Detaillierte Informationen über eine bestimmte Verbindung, oder Prometheus Metriken über Grid-übergreifende Replikationsvorgänge. Sie können eine Verbindung von beiden Rastergitten aus überwachen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergitten mit einem beim Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung" Für das Raster sind Sie angemeldet.

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

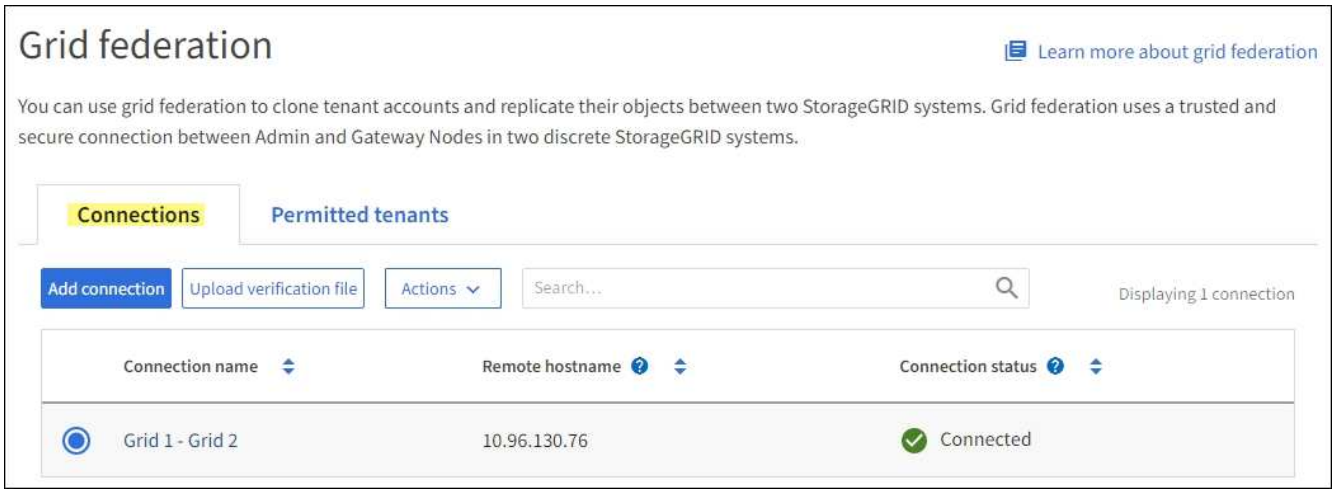
1. Wählen Sie **CONFIGURATION** > **System** > **Grid Federation**.

   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:

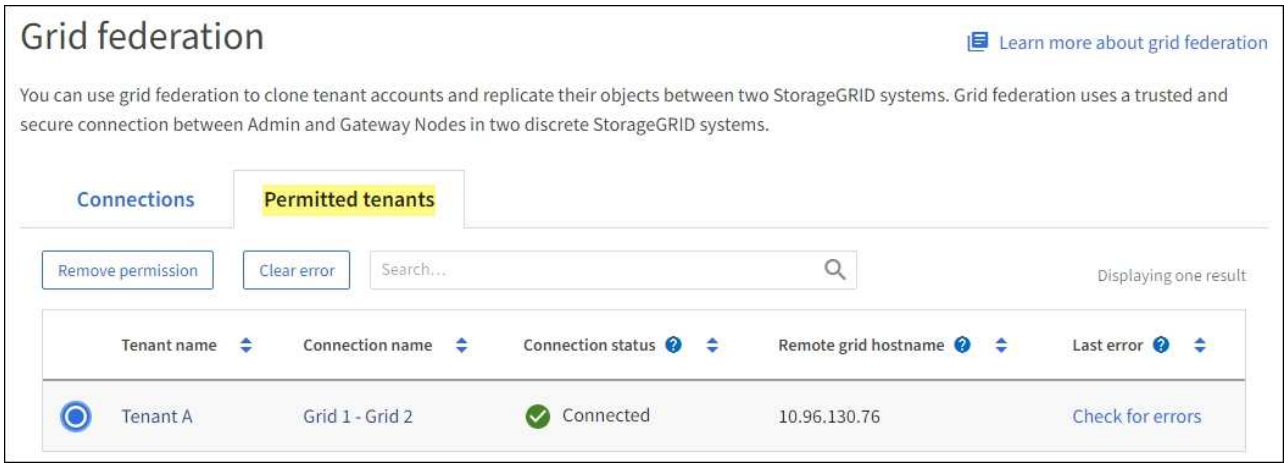
   - "Erstellen Sie eine neue Verbindung".
   - Wählen Sie eine vorhandene Verbindung zu aus "Bearbeiten oder testen".



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 eine zulässige Serviceeinheit und aus "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.

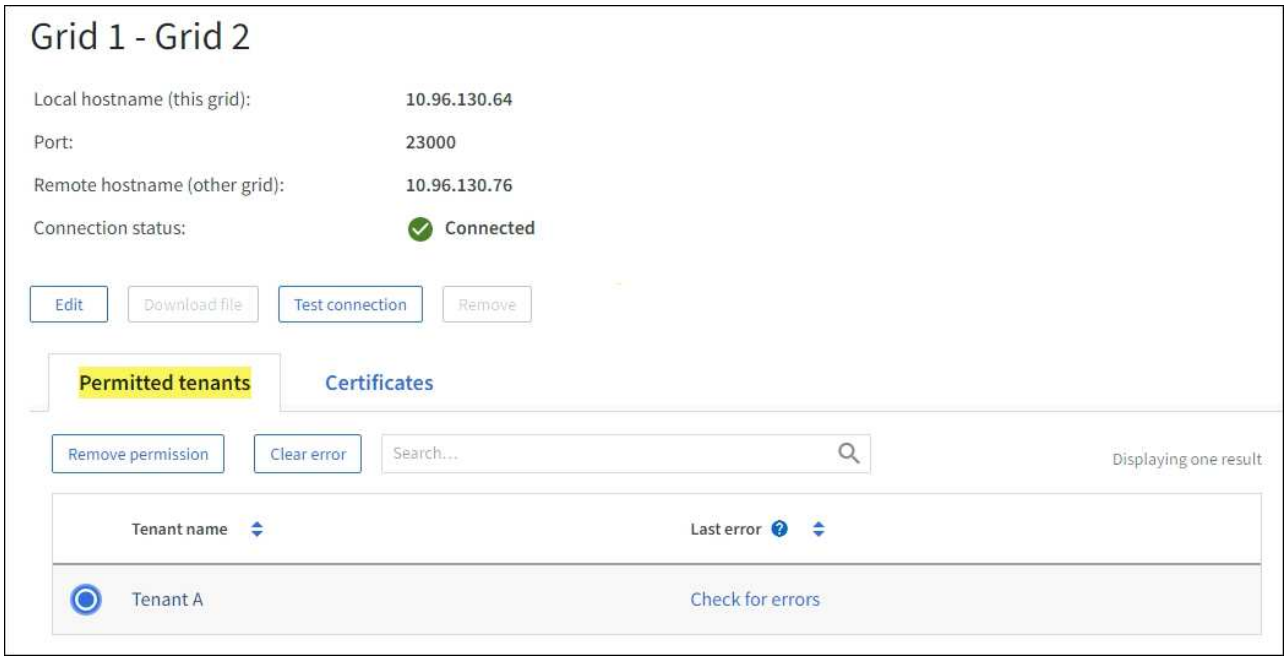
   Auf der Detailseite für die Verbindung können Sie:

   - Hier finden Sie grundlegende Statusinformationen zur Verbindung, einschließlich der lokalen und Remote-Hostnamen, des Ports und des Verbindungsstatus.
   - Wählen Sie eine Verbindung zu aus "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:

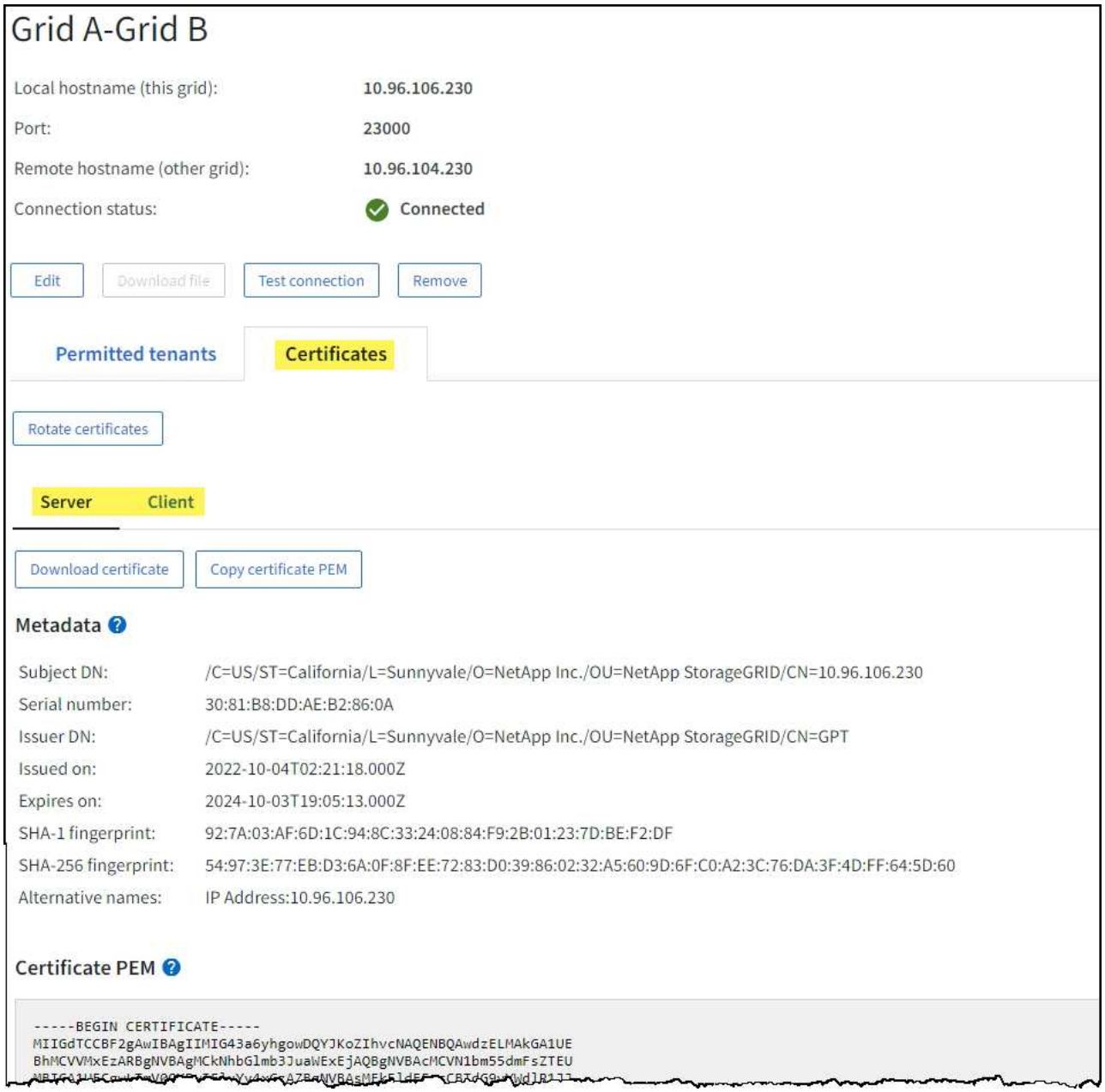
   - "Zeigen Sie die Detailseite für jeden zulässigen Mandanten an".
   - "Entfernen Sie die Berechtigung eines Mandanten" Um die Verbindung zu verwenden.
   - Überprüfen Sie auf Grid-übergreifende Replikationsfehler, und löschen Sie den letzten Fehler. Siehe "Fehler beim Grid-Verbund beheben".



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** > **Metrics**.

   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".

Überwachen Sie die Archivierungskapazität

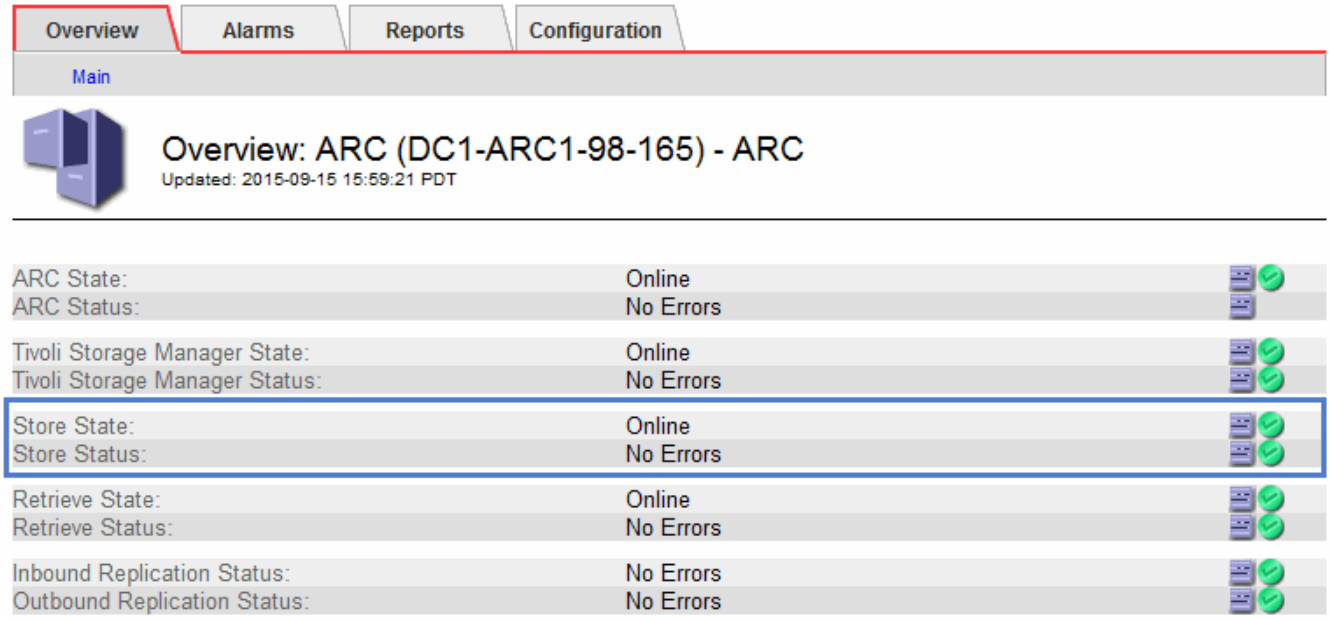
Sie können die Kapazität eines externen Archiv-Storage-Systems nicht direkt über das StorageGRID System überwachen. Sie können jedoch überwachen, ob der Archiv-Node dennoch Objektdaten an das Archivierungsziel senden kann. Dies kann darauf hindeuten, dass eine Erweiterung der Archivierungsmedien erforderlich ist.

Über diese Aufgabe

Sie können die Store-Komponente überwachen, um zu überprüfen, ob der Archiv-Node weiterhin Objektdaten an das Ziel-Archiv-Storage-System senden kann. Der ARVF-Alarm (Store Failures) zeigt möglicherweise auch an, dass das Zielspeichersystem die Kapazität erreicht hat und keine Objektdaten mehr annehmen kann.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC> Übersicht> Main**.
3. Überprüfen Sie die Attribute „Speicherstatus“ und „Speicherstatus“, um zu bestätigen, dass die Komponente „Speicher“ ohne Fehler online ist.



Eine Offline-Store-Komponente oder eine Komponente mit Fehlern weist möglicherweise darauf hin, dass das Ziel-Archivspeichersystem Objektdaten nicht mehr akzeptieren kann, da die Kapazität erreicht ist.

Alarme und Alarme

Alarme und Alarme verwalten: Übersicht

Das StorageGRID Alert System wurde entwickelt, um Sie über betriebliche Probleme zu informieren, die Ihre Aufmerksamkeit erfordern. Das alte Alarmsystem ist veraltet.

Meldungssystem

Das Alarmsystem wurde als Ihr vorrangiges Tool entwickelt, mit dem Sie alle eventuell auftretenden Probleme in Ihrem StorageGRID System überwachen können. Das Alarmsystem bietet eine benutzerfreundliche Oberfläche zum Erkennen, Bewerten und Beheben von Problemen.

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 Warnmeldung wird auf der Seite **NODES** Zusammenfassung und auf der Registerkarte **NODES** > ***Node*** > **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.

Altes Alarmsystem

Wie bei Warnungen werden auch Alarme mit bestimmten Schweregraden ausgelöst, wenn Attribute definierte Schwellenwerte erreichen. Im Gegensatz zu Warnmeldungen werden jedoch viele Alarme für Ereignisse ausgelöst, die Sie sicher ignorieren können, was zu einer übermäßigen Anzahl an E-Mail- oder SNMP-Benachrichtigungen führen kann.

> Das Alarmsystem ist veraltet und wird in einer zukünftigen Version entfernt. Wenn Sie weiterhin ältere Alarme verwenden, sollten Sie so schnell wie möglich auf das Alarmsystem umstellen.

Wenn ein Alarm ausgelöst wird, treten folgende Aktionen auf:

- Der Alarm wird auf der Seite **SUPPORT** > **Alarme (alt)** > **Aktuelle Alarme** angezeigt.
- Es wird eine E-Mail-Benachrichtigung gesendet, vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und eine oder mehrere Mailinglisten konfiguriert.
- Es kann eine SNMP-Benachrichtigung gesendet werden, vorausgesetzt, Sie haben den StorageGRID SNMP-Agent konfiguriert. (SNMP-Benachrichtigungen werden nicht für alle Alarme oder Alarmgrenzen gesendet.)

Vergleichen von Warnungen und Alarmen

Es gibt mehrere Ähnlichkeiten zwischen dem Alarmsystem und dem alten Alarmsystem, aber das Alarmsystem bietet erhebliche Vorteile und ist einfacher zu bedienen.

In der folgenden Tabelle erfahren Sie, wie Sie ähnliche Vorgänge ausführen.

	Meldungen	Alarme (Altsystem)
Wie sehe ich, welche Alarme oder Alarme aktiv sind?	• Wählen Sie den Link **Aktuelle Alarme** auf dem Dashboard aus. • Wählen Sie die Warnmeldung auf der Seite **NODES** > **Übersicht** aus. • Wählen Sie **ALERTS** > **Current**. "Anzeigen aktueller Warnmeldungen"	Wählen Sie **SUPPORT** > **Alarme (alt)** > **Aktueller Alarm** aus. "Verwalten von Alarmen (Altsystem)"
Was bewirkt, dass eine Warnung oder ein Alarm ausgelöst wird?	Alarme werden ausgelöst, wenn ein Prometheus-Ausdruck in einer Alarmregel für die spezifische Triggerbedingung und -Dauer als wahr bewertet wird. "Zeigen Sie Alarmregeln an"	Alarme werden ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht. "Verwalten von Alarmen (Altsystem)"
Wie kann ich das zugrunde liegende Problem lösen, wenn eine Meldung oder ein Alarm ausgelöst wird?	Die empfohlenen Aktionen für eine Warnmeldung sind in E-Mail-Benachrichtigungen enthalten und stehen auf den Alerts-Seiten im Grid Manager zur Verfügung. Falls erforderlich, werden weitere Informationen in der StorageGRID-Dokumentation bereitgestellt. "Alerts Referenz"	Sie können sich über einen Alarm informieren, indem Sie den Attributnamen auswählen oder in der StorageGRID-Dokumentation nach einem Alarmcode suchen. "Alarmreferenz (Altsystem)"
Wo kann ich eine Liste der Alarme oder Alarme sehen, die gelöst wurden?	Wählen Sie **ALARME** > **aufgelöst**. "Anzeige aktueller und aufgelöster Warnmeldungen"	Wählen Sie **SUPPORT** > **Alarme (alt)** > **Historische Alarme**. "Verwalten von Alarmen (Altsystem)"
Wo kann ich die Einstellungen verwalten?	Wählen Sie **ALERTS** > **Rules**. "Verwalten von Meldungen"	Wählen Sie **SUPPORT**. Verwenden Sie dann die Optionen im Abschnitt **Alarme (alt)** des Menüs. "Verwalten von Alarmen (Altsystem)"

	Meldungen	Alarme (Altsystem)
Welche Benutzergruppenberechtigungen brauche ich?	• Jeder, der sich beim Grid Manager anmelden kann, kann aktuelle und behobene Warnmeldungen anzeigen. • Sie müssen über die Berechtigung zum Verwalten von Warnmeldungen verfügen, um Stille, Warnmeldungen und Warnungsregeln zu verwalten. "StorageGRID verwalten"	• Jeder, der sich beim Grid Manager anmelden kann, kann ältere Alarme anzeigen. • Sie müssen über die Berechtigung zum Quittieren von Alarmen verfügen, um Alarme bestätigen zu können. • Sie müssen sowohl über die Konfiguration der Seite „Grid-Topologie“ als auch über andere Berechtigungen für die Rasterkonfiguration verfügen, um globale Alarme und E-Mail-Benachrichtigungen verwalten zu können. "StorageGRID verwalten"
Wie managt ich E-Mail-Benachrichtigungen?	Wählen Sie **ALERTS** > **Email Setup**. **Hinweis:** Da Alarme und Alarme unabhängige Systeme sind, wird das E-Mail-Setup für Alarm- und AutoSupport-Benachrichtigungen nicht für Benachrichtigungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden. "Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"	Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. "Verwalten von Alarmen (Altsystem)"
Wie verwalte ich SNMP Benachrichtigungen?	Wählen Sie **KONFIGURATION** > **Überwachung** > **SNMP-Agent**. "Verwenden Sie SNMP-Überwachung"	*Nicht unterstützt*

	Meldungen	Alarme (Altsystem)
Wie kontrolliere ich, wer Benachrichtigungen erhält?	1. Wählen Sie **ALERTS** > **Email Setup**. 2. Geben Sie im Abschnitt **Empfänger** eine E-Mail-Adresse für jede E-Mail-Liste oder Person ein, die eine E-Mail erhalten soll, wenn eine Benachrichtigung erfolgt. "Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"	1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. 2. Mailingliste wird erstellt. 3. Wählen Sie **Benachrichtigungen**. 4. Wählen Sie die Mailingliste aus. "Verwalten von Alarmen (Altsystem)"
Welche Admin Nodes senden Benachrichtigungen?	Ein einzelner Admin-Knoten (der bevorzugte Absender). "Was ist ein Admin-Node?"	Ein einzelner Admin-Knoten (der bevorzugte Absender). "Was ist ein Admin-Node?"
Wie kann ich einige Benachrichtigungen unterdrücken?	1. Wählen Sie **ALARME** > **Stille**. 2. Wählen Sie die Alarmregel aus, die stummschalten soll. 3. Geben Sie eine Dauer für die Stille an. 4. Wählen Sie den Schweregrad der Warnmeldung aus, den Sie stummschalten möchten. 5. Wählen Sie diese Option aus, um die Stille auf das gesamte Raster, einen einzelnen Standort oder einen einzelnen Knoten anzuwenden. **Hinweis**: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. "Benachrichtigung über Stille"	1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. 2. Wählen Sie **Benachrichtigungen**. 3. Wählen Sie eine Mailingliste aus, und wählen Sie **unterdrücken**. "Verwalten von Alarmen (Altsystem)"
Wie kann ich alle Benachrichtigungen unterdrücken?	Wählen Sie **ALARME** > **Stille** und dann **Alle Regeln**. **Hinweis**: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. "Benachrichtigung über Stille"	*Nicht unterstützt*

	Meldungen	Alarme (Altsystem)
Wie kann ich die Bedingungen und Trigger anpassen?	1. Wählen Sie **ALERTS** > **Rules**. 2. Wählen Sie eine Standardregel zum Bearbeiten aus, oder wählen Sie **benutzerdefinierte Regel erstellen**. "Bearbeiten von Meldungsregeln" "Erstellen benutzerdefinierter Warnungsregeln"	1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Globale Alarme**. 2. Erstellen Sie einen globalen benutzerdefinierten Alarm, um einen Standardalarm zu überschreiben oder ein Attribut zu überwachen, das keinen Standardalarm hat. "Verwalten von Alarmen (Altsystem)"
Wie deaktiviere ich eine einzelne Warnung oder einen einzelnen Alarm?	1. Wählen Sie **ALERTS** > **Rules**. 2. Wählen Sie die Regel aus, und wählen Sie **Regel bearbeiten**. 3. Deaktivieren Sie das Kontrollkästchen **aktiviert**. "Deaktivieren von Meldungsregeln"	1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Globale Alarme**. 2. Wählen Sie die Regel aus, und wählen Sie das Symbol Bearbeiten aus. 3. Deaktivieren Sie das Kontrollkästchen **aktiviert**. "Verwalten von Alarmen (Altsystem)"

Verwalten von Meldungen

Benachrichtigungen verwalten: Übersicht

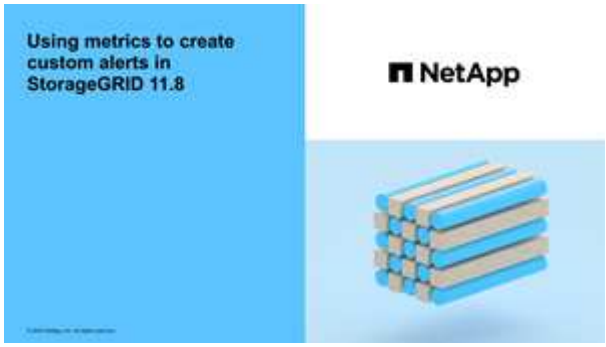
Das Warnsystem bietet eine benutzerfreundliche Oberfläche zum Erkennen, Bewerten und Beheben von Problemen, die während des StorageGRID-Betriebs auftreten können.

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

Weitere Informationen:

- Sehen Sie sich das Video an: "Video: Übersicht über Warnmeldungen für StorageGRID 11.8"

- Sehen Sie sich das Video an: "Video: Verwendung von Kennzahlen zum Erstellen von benutzerdefinierten Warnmeldungen in StorageGRID 11.8"



- Siehe "Alerts Referenz".

Zeigen Sie Alarmregeln an

Alarmregeln definieren die Bedingungen, die ausgelöst werden "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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".
- Optional haben Sie sich das Video angesehen: "Video: Übersicht über Warnmeldungen für StorageGRID 11.8"

Schritte

1. Wählen Sie **ALERTS** > **Rules**.

   Die Seite Alarmregeln wird angezeigt.

Alert Rules Learn more

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

+ Create custom rule Edit rule Remove custom rule

Name	Conditions	Type	Status
Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure{type="REC_EXPIRED_BATTERY"} *Major* > 0	Default	Enabled
Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure{type="REC_FAILED_BATTERY"} *Major* > 0	Default	Enabled
Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure{type="REC_BATTERY_WARN"} *Major* > 0	Default	Enabled
Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure{type="REC_BATTERY_NEAR_EXPIRATION"} *Major* > 0	Default	Enabled
Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure{type="REC_REMOVED_BATTERY"} *Major* > 0	Default	Enabled
Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure{type="REC_BATTERY_OVERTEMP"} *Major* > 0	Default	Enabled
Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_FAILED"} *Major* > 0	Default	Enabled
Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY"} *Major* > 0	Default	Enabled
Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED"} *Major* > 0	Default	Enabled
Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure{type="REC_CACHE_MEM_SIZE_MISMATCH"} *Major* > 0	Default	Enabled

Displaying 62 alert rules.

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

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

Spaltenüberschrift	Beschreibung
Bestimmten Bedingungen	Die Prometheus Ausdrücke, die bestimmen, wann diese Warnung ausgelöst wird. Eine Meldung kann auf einem oder mehreren der folgenden Schweregrade ausgelöst werden, jedoch ist für jeden Schweregrad ein Zustand nicht erforderlich. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge 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 besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst 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. • **Klein** : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die nicht von selbst geklärt werden, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
Typ	Der Typ der Warnregel: • **Standard**: Eine mit dem System bereitgestellte Warnregel. Sie können eine Standardwarnregel deaktivieren oder die Bedingungen und Dauer für eine Standardwarnregel bearbeiten. Eine Standard-Warnungsregel kann nicht entfernt werden. • **Standard***: Eine Standardwarnregel, die eine bearbeitete Bedingung oder Dauer enthält. Bei Bedarf können Sie eine geänderte Bedingung ganz einfach wieder auf die ursprüngliche Standardeinstellung zurücksetzen. • **Benutzerdefiniert**: Eine Alarmregel, die Sie erstellt haben. Sie können benutzerdefinierte Alarmregeln deaktivieren, bearbeiten und entfernen.
Status	Gibt an, ob diese Warnungsregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnungsregeln werden nicht ausgewertet, sodass keine Warnmeldungen ausgelöst werden.

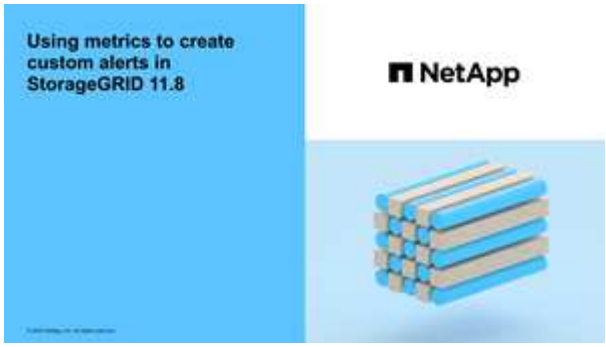
Erstellen benutzerdefinierter Warnungsregeln

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

Bevor Sie beginnen

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

- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".
- Sie kennen das "Häufig verwendete Prometheus-Kennzahlen".
- Sie verstehen den "Syntax der Prometheus-Abfragen".
- Optional haben Sie sich das Video angesehen: "Video: Verwendung von Kennzahlen zum Erstellen von benutzerdefinierten Warnmeldungen in StorageGRID 11.8".



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.

  Zum Beispiel zum Testen des Ausdrucks `node_memory_MemTotal_bytes < 24000000000`, Erste Ausführung `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.

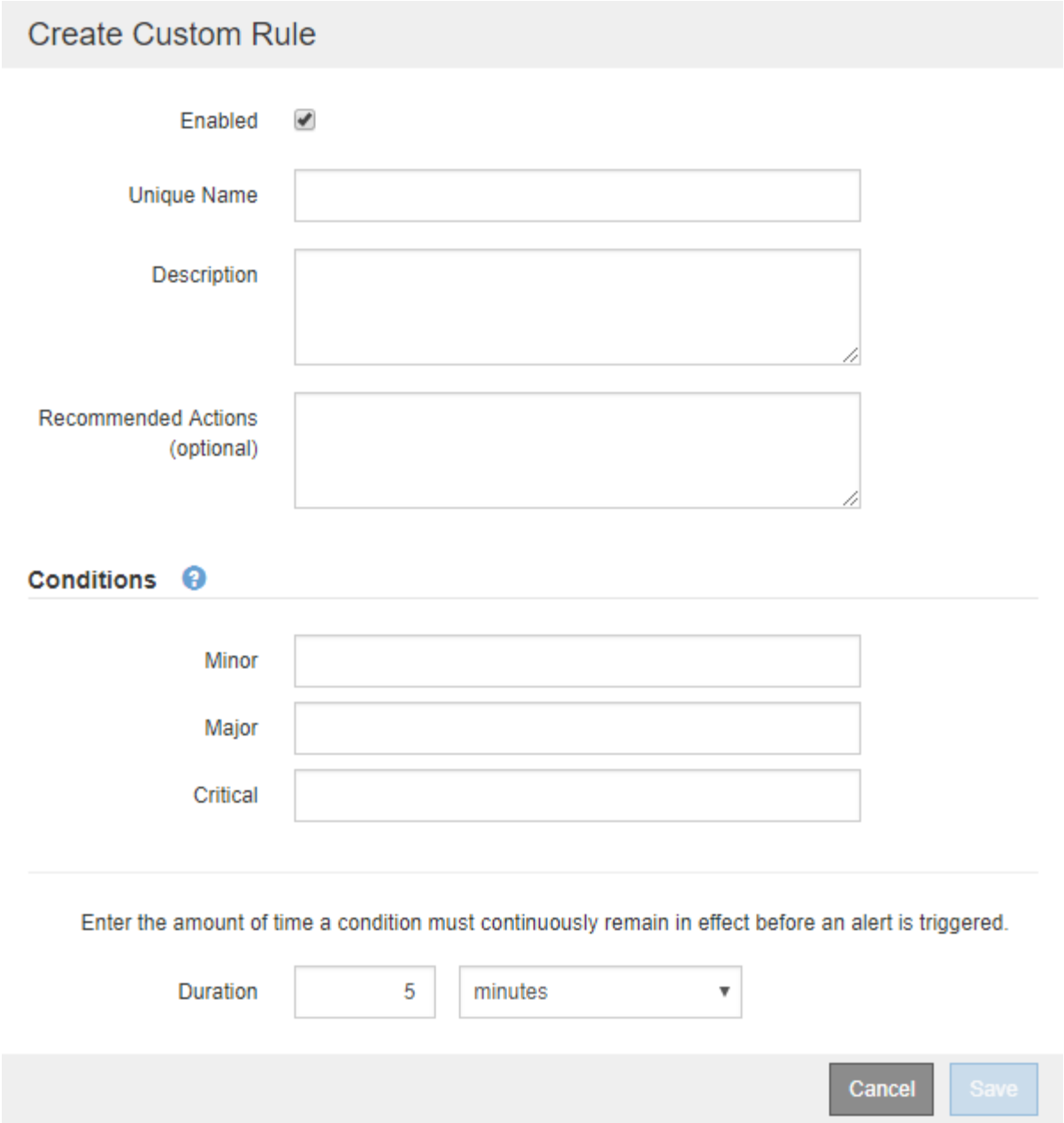
Schritte

1. Wählen Sie **ALERTS** > **Rules**.

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

6. Geben Sie im Feld **Dauer** 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 mit einem bei Grid Manager 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.

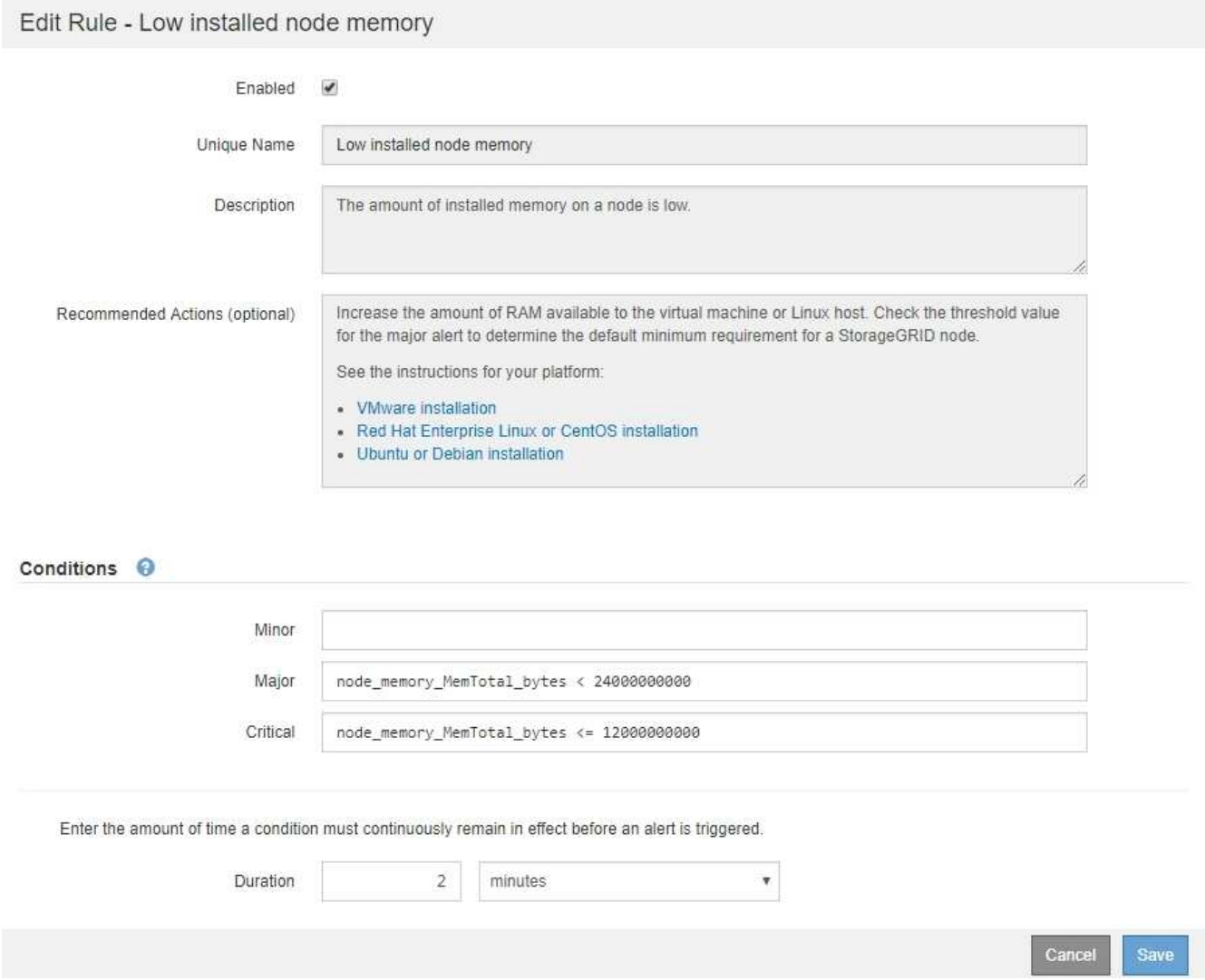
Schritte

1. Wählen Sie **ALERTS** > **Rules**.

   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.

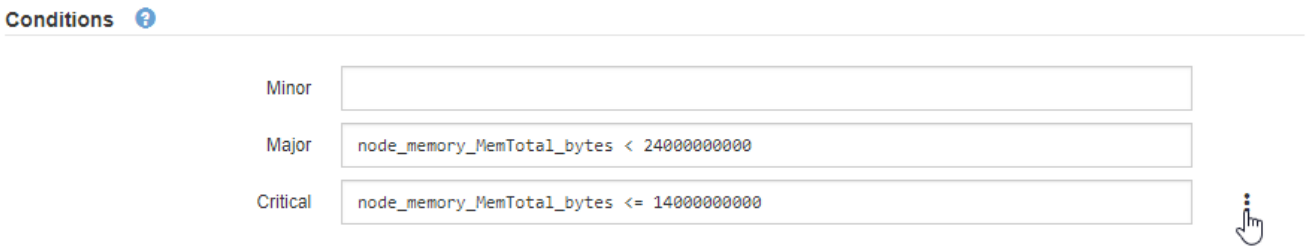
5. Aktualisieren Sie für benutzerdefinierte Warnungsregeln die folgenden Informationen, falls erforderlich.

   > 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 mit einem bei Grid Manager 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 **ALERTS** > **Rules**.

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

Schritte

1. Wählen Sie **ALERTS** > **Rules**.

   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 **CONFIGURATION** > **Monitoring** > **SNMP Agent** im Grid Manager oder die SNMP-Endpunkte für die Grid Management API verwenden, um den StorageGRID SNMP-Agent 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, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen. 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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Managen von Warnmeldungen oder Root-Zugriffsberechtigungen".

Über diese Aufgabe

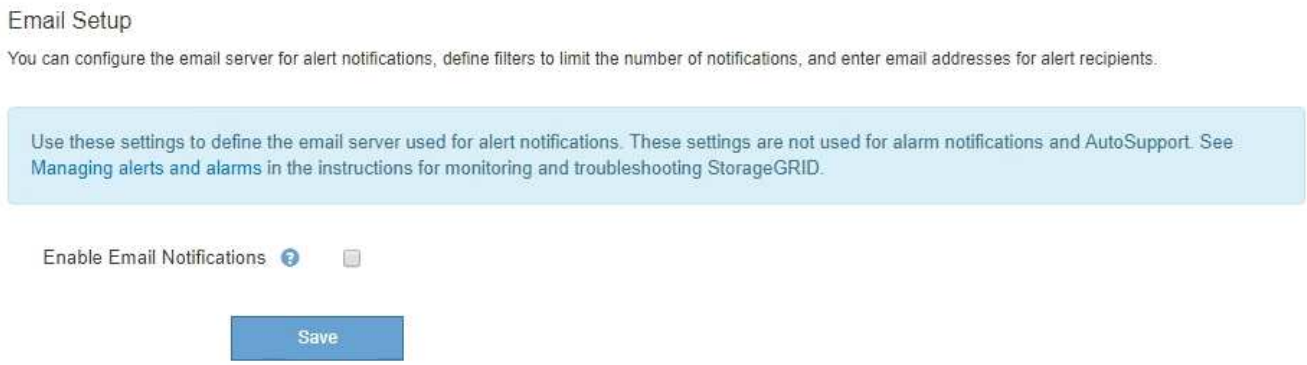
Da Alarme und Alarme unabhängige Systeme sind, wird die für Warnmeldungen verwendete E-Mail-Einrichtung nicht für Alarmmeldungen und AutoSupport-Pakete verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden.

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Pakete, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen. 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 **ALERTS** > **Email 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.
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, klicken Sie auf das Stift-Symbol, um dieses Feld zu aktualisieren.

Transport Layer Security (TLS)

Require TLS ☑

CA Certificate

```
-----BEGIN CERTIFICATE-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----END CERTIFICATE-----
```

Browse

Send Client Certificate ☑

Client Certificate

```
-----BEGIN CERTIFICATE-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----END CERTIFICATE-----
```

Browse

Private Key

```
-----BEGIN PRIVATE KEY-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----BEGIN PRIVATE KEY-----
```

Browse

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.

Schweregrad	Beschreibung
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 und älteren Alarmmeldungen, bei denen alle Admin-Knoten die Test-E-Mail senden.

8. Wählen Sie **Speichern**.

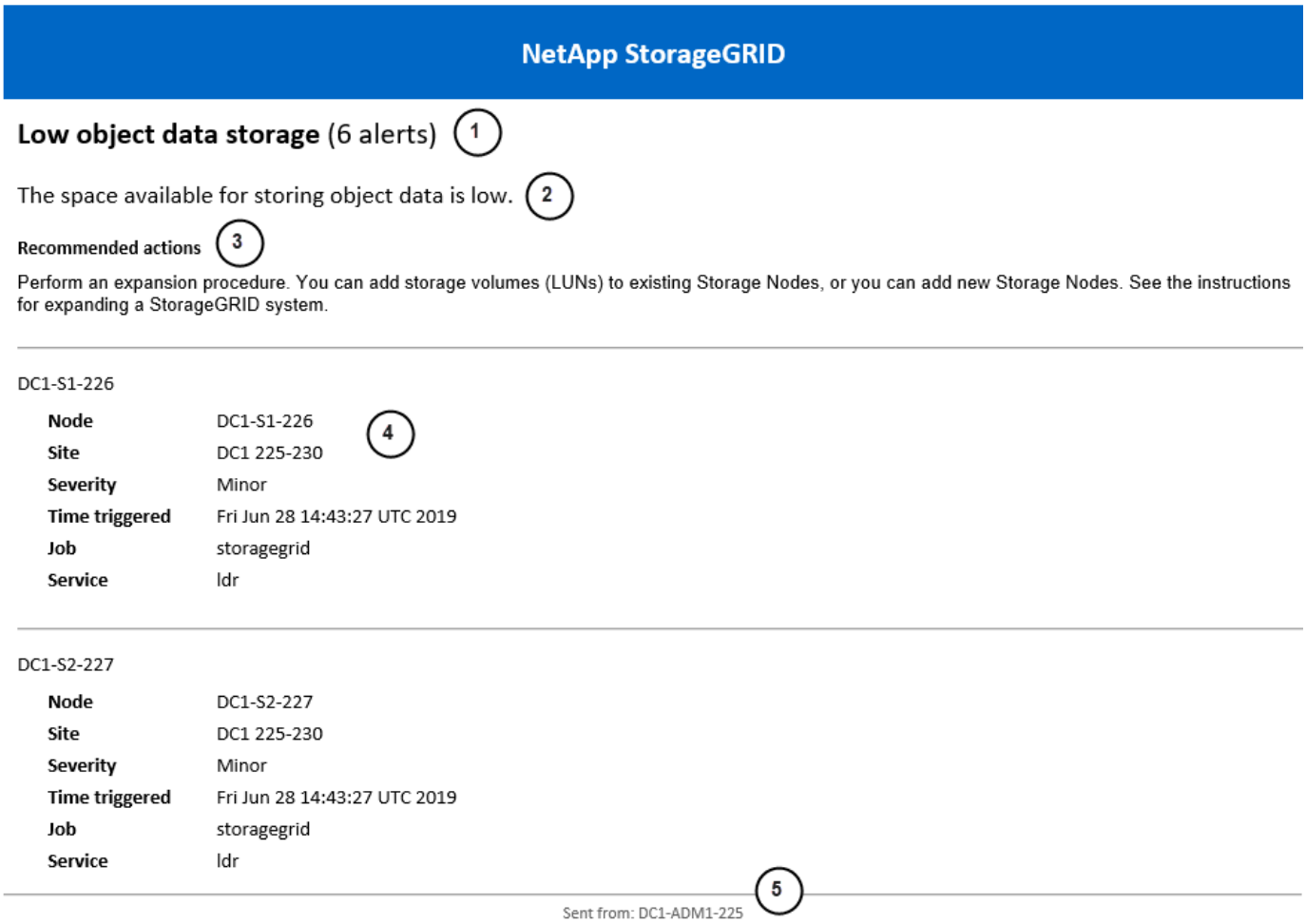
   Beim Senden einer Test-E-Mail werden Ihre Einstellungen nicht gespeichert. Sie müssen **Speichern** wählen.

   Die E-Mail-Einstellungen werden gespeichert.

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

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

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



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

Gruppierung von Warnungen

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

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

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

Verhalten	Beispiel
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnmeldung gelöst oder die Alarmregel stummgeschaltet wurde.	1. Am 8. März wird Alarm A für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Warnung A ist nicht gelöst oder stummgeschaltet. Weitere Benachrichtigungen erhalten Sie am 15. März, 22. März 29 usw.

Beheben Sie Warnmeldungen bei E-Mail-Benachrichtigungen

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

Bevor Sie beginnen

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

Schritte

1. Überprüfen Sie Ihre Einstellungen.
   a. Wählen Sie **ALERTS** > **Email 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 mit einem bei Grid Manager 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.

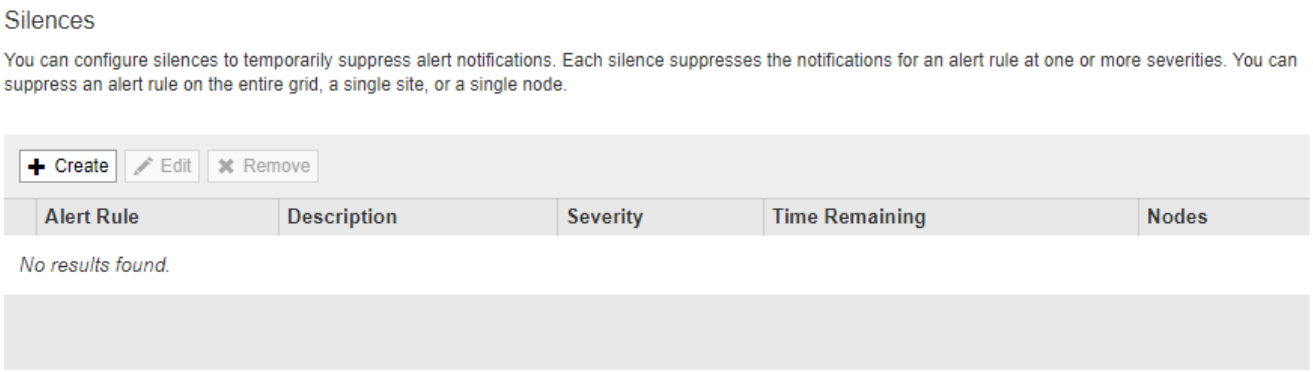
> Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn Sie eine Warnmeldung stummschalten, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

> Da Alarme und Alarme unabhängige Systeme sind, können Sie diese Funktion nicht zum Unterdrücken von Alarmmeldungen verwenden.

Schritte

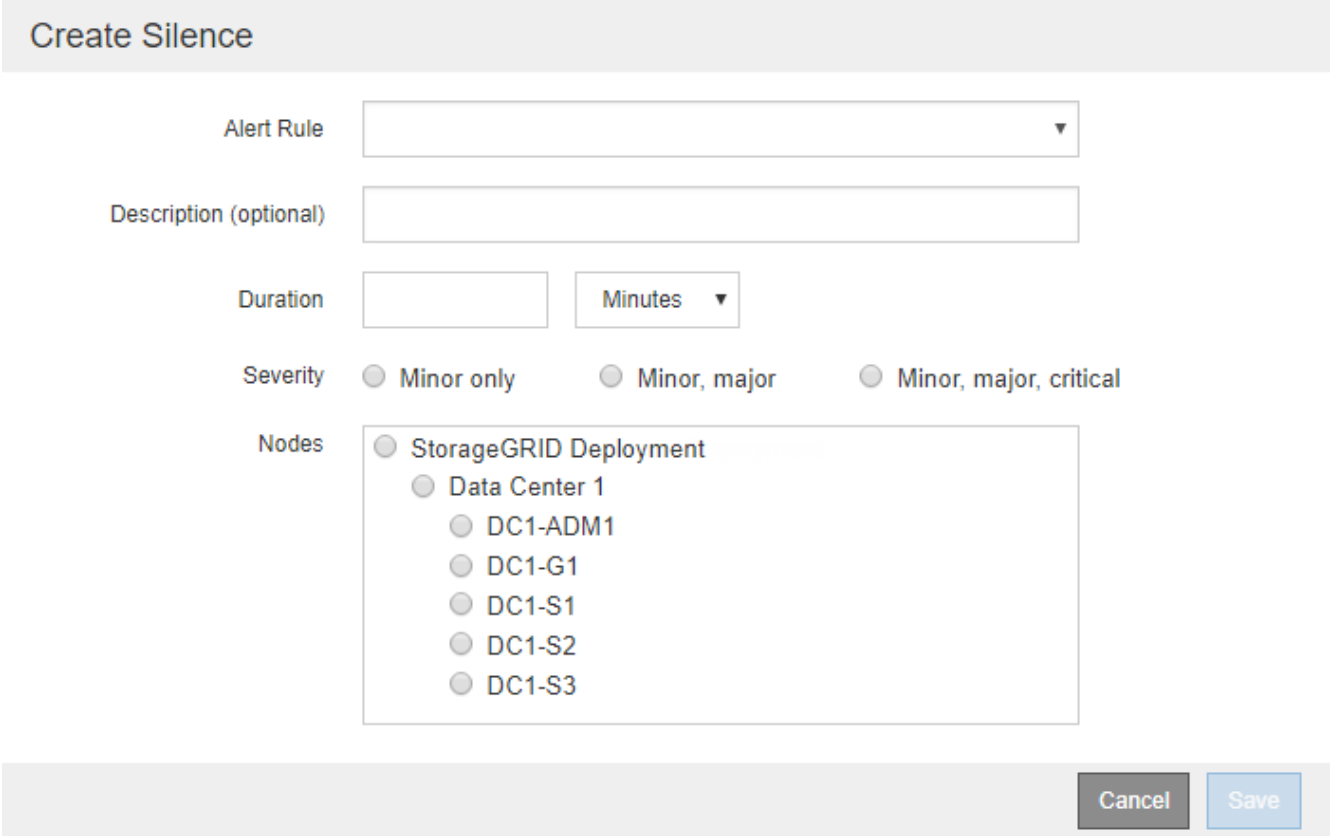
1. Wählen Sie **ALARME** > **Stille**.

   Die Seite „Stille“ wird angezeigt.

2. Wählen Sie **Erstellen**.

   Das Dialogfeld Stille erstellen wird angezeigt.



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

Feld	Beschreibung
Meldungsregel	Der Name der Alarmregel, die Sie stumm schalten möchten. Sie können eine beliebige Standard- oder benutzerdefinierte Warnungsregel auswählen, auch wenn die Alarmregel deaktiviert ist. **Hinweis:** Wählen Sie **Alle Regeln** aus, wenn Sie alle Alarmregeln mit den in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.
Beschreibung	Optional eine Beschreibung der Stille. Beschreiben Sie zum Beispiel den Zweck dieser Stille.
Dauer	Wie lange Sie möchten, dass diese Stille in Minuten, Stunden oder Tagen wirksam bleibt. Eine Stille kann von 5 Minuten bis 1,825 Tage (5 Jahre) in Kraft sein. **Hinweis:** eine Alarmregel sollte nicht für längere Zeit stummgemacht werden. Wenn eine Alarmregel stumm geschaltet ist, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang abgeschlossen wird. Möglicherweise müssen Sie jedoch eine erweiterte Stille verwenden, wenn eine Warnung durch eine bestimmte, vorsätzliche Konfiguration ausgelöst wird, wie z. B. bei den **Services Appliance Link Down**-Alarmen und den **Storage Appliance Link down**-Alarmen.

Feld	Beschreibung
Schweregrad	Welche Alarmschweregrade oder -Schweregrade stummgeschaltet werden sollten. Wenn die Warnung bei einem der ausgewählten Schweregrade ausgelöst wird, werden keine Benachrichtigungen gesendet.
Knoten	Auf welchen Knoten oder Knoten Sie diese Stille anwenden möchten. Sie können eine Meldungsregel oder alle Regeln im gesamten Grid, einer einzelnen Site oder einem einzelnen Node unterdrücken. Wenn Sie das gesamte Raster auswählen, gilt die Stille für alle Standorte und alle Knoten. Wenn Sie einen Standort auswählen, gilt die Stille nur für die Knoten an diesem Standort. **Hinweis:** Sie können nicht mehr als einen Knoten oder mehr als einen Standort für jede Stille auswählen. Sie müssen zusätzliche Stille erstellen, wenn Sie dieselbe Warnungsregel auf mehr als einem Node oder mehreren Standorten gleichzeitig unterdrücken möchten.

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

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

Verwandte Informationen

- "Konfigurieren Sie den SNMP-Agent"

Alerts Referenz

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

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

Einige der Standardwarnungen werden verwendet "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.
Fehler bei der BMC-Kommunikation des Geräts	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren.
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.
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.

Alarmname	Beschreibung
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.
Fehler des Appliance-das-Laufwerks erkannt	Bei einem Direct-Attached Storage (das)-Laufwerk in der Appliance wurde ein Problem festgestellt.
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.

Alarmname	Beschreibung
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.
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.
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.

Alarmname	Beschreibung
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 Datenträgerwarteschlange für Überwachungsmeldungen ist voll. Wenn diese Bedingung nicht erfüllt wird, können S3- oder Swift-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.

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.

Alarmname	Beschreibung
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.
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.

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.

Alarmname	Beschreibung
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.
E-Mail-Benachrichtigung fehlgeschlagen	Die E-Mail-Benachrichtigung für eine Warnmeldung konnte nicht gesendet werden.

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.

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.

Alarmname	Beschreibung
Ablauf des globalen Serverzertifikats für S3 und Swift	Das globale Serverzertifikat für S3 und Swift läuft demnächst 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.
Der ILM-Scan ist zu lang	Der Zeitaufwand für das Scannen, Bewerten und Anwenden von ILM auf Objekte ist zu lang.
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.
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.

Alarmname	Beschreibung
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.

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 Platz ist gering. Wenn diese Bedingung nicht erfüllt wird, können S3- oder Swift-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.
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	Der Speichervolumen Soft Read-Only-Wasserzeichen-Überschreiben ist kleiner als der für einen Speicherknoten optimierte Mindestwert.
Niedrige Root-Festplattenkapazität	Der auf der Stammfestplatte verfügbare Speicherplatz ist gering.

Alarmname	Beschreibung
Niedrige Datenkapazität des Systems	Der für /var/local verfügbare Speicherplatz ist gering. Wenn diese Bedingung nicht erfüllt wird, können S3- oder Swift-Vorgänge fehlschlagen.
Geringer Tmp-Telefonspeicherplatz	Der im Verzeichnis /tmp verfügbare Speicherplatz ist gering.

Warnmeldungen für das Node- oder Node-Netzwerk

Alarmname	Beschreibung
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.
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.

Alarmname	Beschreibung
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.
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.
Objekte verloren	Mindestens ein Objekt ist aus dem Raster verloren gegangen.
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.

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 ist länger als 5 Minuten offline, möglicherweise aufgrund des Neubootens des Node während der Formatierung des Volumes.
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 das NetApp Cryptographic Security Module ist aktiviert.
Neustart erforderlich zur Aktivierung von FIPS	Die Sicherheitsrichtlinie erfordert den FIPS-Modus, aber das NetApp Cryptographic Security Module ist deaktiviert.
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.

Das können Sie 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?

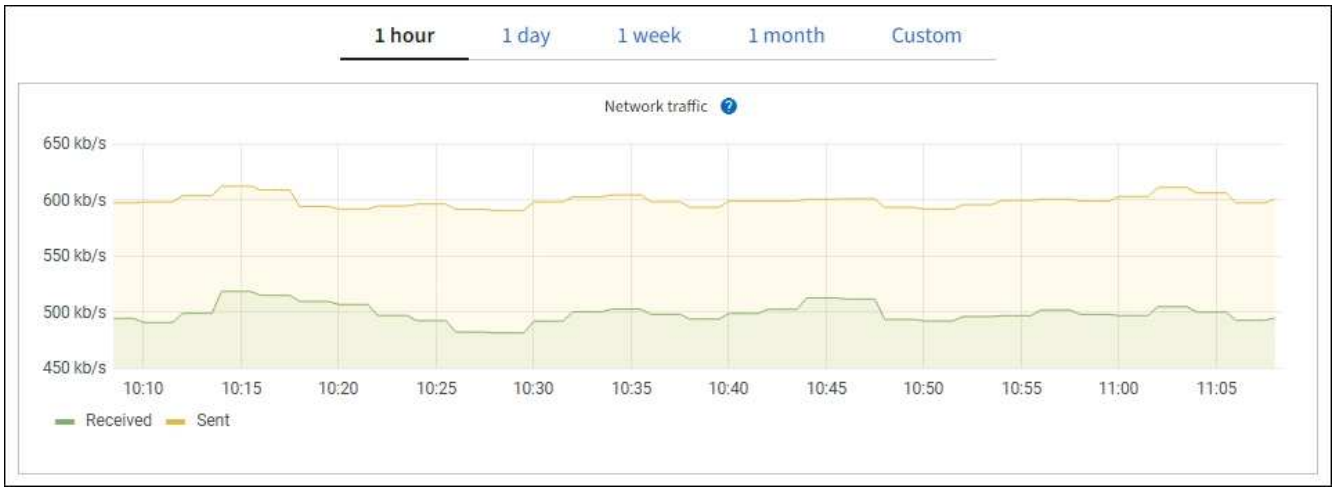
Prometheus Kennzahlen sind Zeitreihenmessungen. Der Prometheus-Service auf Admin-Nodes erfasst diese Kennzahlen von den Services auf allen Knoten. Metriken werden auf jedem Admin-Node gespeichert, bis der für Prometheus-Daten reservierte Speicherplatz voll ist. Wenn der `/var/local/mysql_ibdata/` Volume erreicht die Kapazität, zuerst werden 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**.) Obwohl mehr als tausend Kennzahlen verfügbar sind, ist nur eine relativ geringe Zahl zur Überwachung der wichtigsten 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** > **Diagnostics** und die Seite **SUPPORT** > **Tools** > **Metrics**: Diese Seiten, die in erster Linie für den technischen Support bestimmt sind, bieten verschiedene Tools und Diagramme, die die Werte von Prometheus Metrics 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 S3-Buckets und Swift-Container, die von diesem Storage-Node bekannt sind

storagegrid_Content_Objects

Die Gesamtzahl der von diesem Storage-Node bekannten S3 und Swift Datenobjekte. Die Anzahl ist nur für Datenobjekte gültig, die von Client-Applikationen erstellt werden, die über S3 oder Swift mit dem System interface.

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_Swift_Data_Transfers_Bytes_aufgenommen

Die Gesamtmenge der Daten, die Swift-Clients seit dem letzten Zurücksetzen des Attributs von diesem Storage-Node aufgenommen haben.

storagegrid_Swift_Data_Transfers_Bytes_abgerufen

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

storagegrid_Swift_Operations_fehlgeschlagen

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

storagegrid_Swift_Operations_erfolgreich

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

storagegrid_Swift_Operations_nicht autorisiert

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

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.

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

Verwalten von Alarmen (Altsystem)

Verwalten von Alarmen (Altsystem)

Das StorageGRID-Alarmsystem ist das ältere System, mit dem Störstellen identifiziert werden können, die manchmal während des normalen Betriebs auftreten.

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Alarmklassen (altes System)

Ein älterer Alarm kann zu einer von zwei sich gegenseitig ausschließenden Alarmklassen gehören.

- Standardalarme werden mit jedem StorageGRID-System geliefert und können nicht geändert werden. Sie können jedoch Standardalarme deaktivieren oder überschreiben, indem Sie globale benutzerdefinierte Alarme definieren.
- Globale benutzerdefinierte Alarme überwachen den Status aller Dienste eines bestimmten Typs im StorageGRID-System. Sie können einen globalen benutzerdefinierten Alarm erstellen, um einen Standardalarm zu überschreiben. Sie können auch einen neuen globalen benutzerdefinierten Alarm erstellen. Dies kann nützlich sein, um alle angepassten Bedingungen Ihres StorageGRID-Systems zu überwachen.

Alarmauslöselogik (Älteres System)

Ein alter Alarm wird ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht, der für eine Kombination aus Alarmklasse (Standard oder Global Custom) und Alarmschweregrade auf „true“ bewertet.

Symbol	Farbe	Alarmschweregrad	Bedeutung
	Gelb	Hinweis	Der Node ist mit dem Grid verbunden. Es ist jedoch eine ungewöhnliche Bedingung vorhanden, die den normalen Betrieb nicht beeinträchtigt.
	Hellorange	Gering	Der Node ist mit dem Raster verbunden, aber es existiert eine anormale Bedingung, die den Betrieb in Zukunft beeinträchtigen könnte. Sie sollten untersuchen, um eine Eskalation zu verhindern.
	Dunkelorange	Major	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die sich derzeit auf den Betrieb auswirkt. Um eine Eskalation zu vermeiden, ist eine sofortige Aufmerksamkeit erforderlich.
	Rot	Kritisch	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die normale Vorgänge angehalten hat. Sie sollten das Problem sofort beheben.

Für jedes numerische Attribut kann der Alarmschwerwert und der entsprechende Schwellwert eingestellt werden. Der NMS-Service auf jedem Admin-Node überwacht kontinuierlich die aktuellen Attributwerte im Vergleich zu konfigurierten Schwellenwerten. Wenn ein Alarm ausgelöst wird, wird eine Benachrichtigung an alle designierten Mitarbeiter gesendet.

Beachten Sie, dass ein Schweregrad „Normal“ keinen Alarm auslöst.

Attributwerte werden anhand der Liste der aktivierten Alarme bewertet, die für dieses Attribut definiert wurden. Die Liste der Alarme wird in der folgenden Reihenfolge überprüft, um die erste Alarmklasse mit einem definierten und aktivierten Alarm für das Attribut zu finden:

1. Globale benutzerdefinierte Alarme mit Alarmabtrennungen von kritisch bis zur Mitteilung.
2. Standardalarme mit Alarmtrennungen von kritisch bis Notice.

Nachdem in der höheren Alarmklasse ein aktivierter Alarm für ein Attribut gefunden wurde, wird der NMS-Dienst nur innerhalb dieser Klasse ausgewertet. Der NMS-Dienst wird nicht mit den anderen Klassen mit niedrigerer Priorität bewertet. Wenn also ein globaler benutzerdefinierter Alarm für ein Attribut aktiviert ist, wertet der NMS-Dienst den Attributwert nur gegen globale benutzerdefinierte Alarme aus. Standardalarme werden nicht ausgewertet. Somit kann ein aktivierter Standardalarm für ein Attribut die Kriterien erfüllen, die zum Auslösen eines Alarms erforderlich sind. Er wird jedoch nicht ausgelöst, da ein globaler benutzerdefinierter Alarm (der nicht den angegebenen Kriterien entspricht) für dasselbe Attribut aktiviert ist. Es wird kein Alarm ausgelöst und keine Benachrichtigung gesendet.

Beispiel für Alarmauslösung

Anhand dieses Beispiels können Sie verstehen, wie globale benutzerdefinierte Alarme und Standardalarme ausgelöst werden.

Im folgenden Beispiel ist ein Attribut mit einem globalen benutzerdefinierten Alarm und einem Standardalarm

definiert und aktiviert, wie in der folgenden Tabelle dargestellt.

	Globale benutzerdefinierte Alarmschwelle (aktiviert)	**Standard-Alarmschwellenwert (aktiviert)**
Hinweis	>= 1500	>= 1000
Gering	>= 15,000	>= 1000
Major	>=150,000	>= 250,000

Wird das Attribut bei einem Wert von 1000 ausgewertet, wird kein Alarm ausgelöst und keine Benachrichtigung gesendet.

Der globale benutzerdefinierte Alarm hat Vorrang vor dem Standardalarm. Ein Wert von 1000 erreicht für den globalen benutzerdefinierten Alarm keinen Schwellenwert eines Schweregrads. Daher wird der Alarmpegel als normal bewertet.

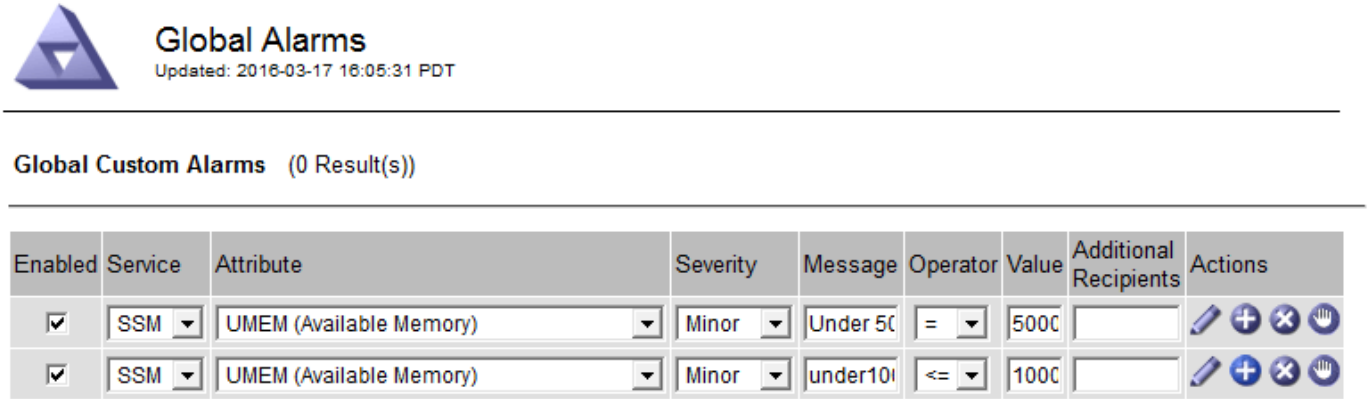
Wenn nach dem obigen Szenario der globale benutzerdefinierte Alarm deaktiviert ist, ändert sich nichts. Der Attributwert muss neu bewertet werden, bevor eine neue Alarmstufe ausgelöst wird.

Wenn der globale benutzerdefinierte Alarm deaktiviert ist und der Attributwert neu bewertet wird, wird der Attributwert anhand der Schwellenwerte für den Standardalarm ausgewertet. Die Alarmstufe löst einen Alarm für die Benachrichtigungsstufe aus, und eine E-Mail-Benachrichtigung wird an das entsprechende Personal gesendet.

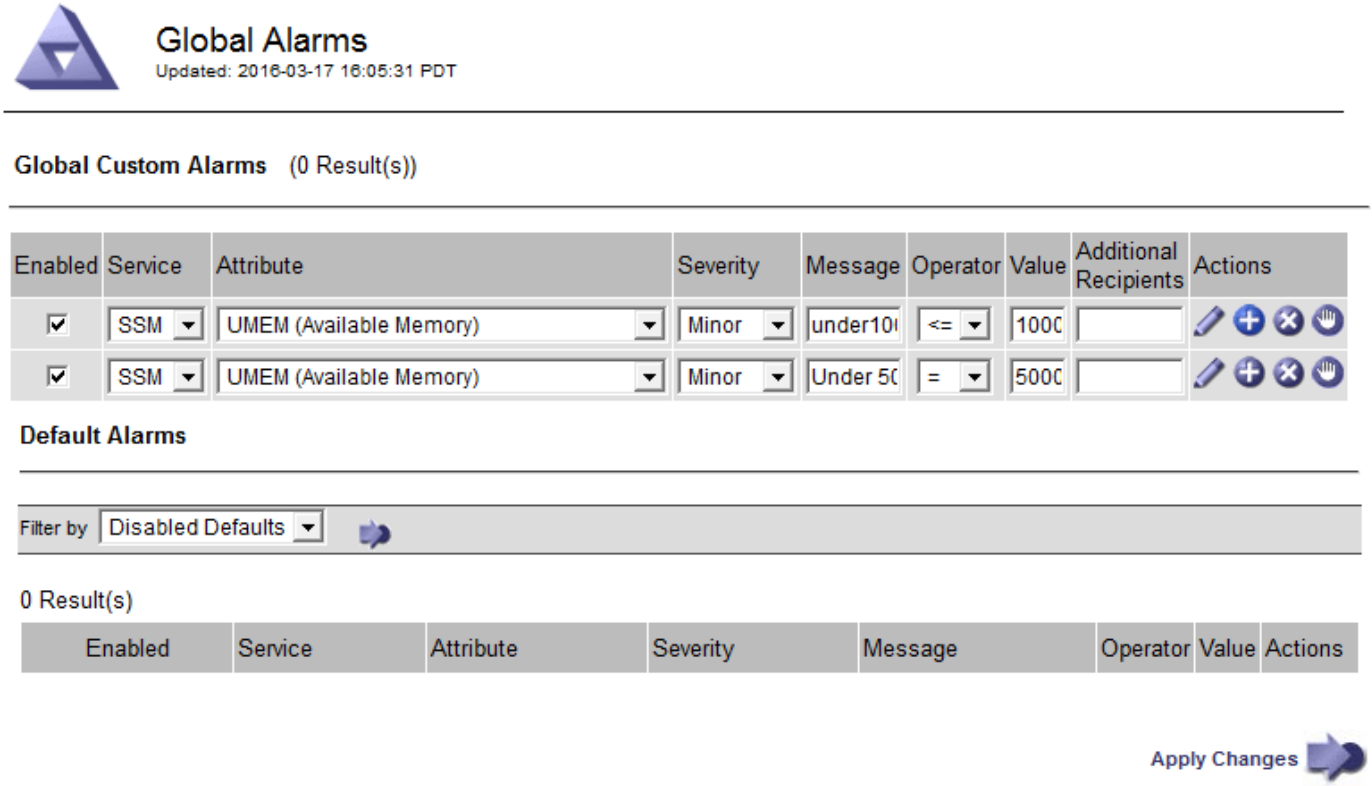
Alarme desselben Schweregrades

Wenn zwei globale benutzerdefinierte Alarme für dasselbe Attribut den gleichen Schweregrad aufweisen, werden die Alarme mit der Priorität „Top-Down“ ausgewertet.

Wenn UMEM beispielsweise auf 50 MB abfällt, wird der erste Alarm ausgelöst (= 50000000), nicht jedoch der untere Alarm (<=100000000).



Wird die Reihenfolge umgekehrt, wenn UMEM auf 100MB fällt, wird der erste Alarm (<=100000000) ausgelöst, nicht jedoch der darunter stehende Alarm (= 50000000).



Benachrichtigungen

Eine Benachrichtigung meldet das Auftreten eines Alarms oder die Änderung des Status eines Dienstes. Alarmbenachrichtigungen können per E-Mail oder über SNMP gesendet werden.

Um zu vermeiden, dass bei Erreichen eines Alarmschwellenwerts mehrere Alarme und Benachrichtigungen gesendet werden, wird der Schweregrad des Alarms anhand des aktuellen Alarmschwerfalls für das Attribut überprüft. Wenn es keine Änderung gibt, dann werden keine weiteren Maßnahmen ergriffen. Das bedeutet, dass der NMS-Dienst das System weiterhin überwacht, nur ein Alarm ausgelöst und Benachrichtigungen sendet, wenn er zum ersten Mal einen Alarmzustand für ein Attribut bemerkt. Wenn ein neuer Wertschwellenwert für das Attribut erreicht und erkannt wird, ändert sich der Schweregrad des Alarms und eine neue Benachrichtigung wird gesendet. Die Alarme werden gelöscht, wenn die Zustände wieder auf den normalen Stand zurückkehren.

Der in der Benachrichtigung über einen Alarmzustand angezeigte Triggerwert wird auf drei Dezimalstellen gerundet. Daher löst ein Attributwert von 1.9999 einen Alarm aus, dessen Schwellenwert unter (<) 2.0 liegt, obwohl die Alarmbenachrichtigung den Triggerwert als 2.0 anzeigt.

Neuer Services

Wenn neue Services durch Hinzufügen neuer Grid-Nodes oder -Standorte hinzugefügt werden, erben sie Standardalarme und globale benutzerdefinierte Alarme.

Alarme und Tabellen

In Tabellen angezeigte Alarmattribute können auf Systemebene deaktiviert werden. Alarme können für einzelne Zeilen in einer Tabelle nicht deaktiviert werden.

Die folgende Tabelle zeigt beispielsweise zwei kritische Einträge (VMFI)-Alarme. (Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***Storage-Node*** > **SSM** > **Ressourcen**.)

Sie können den VMFI-Alarm so deaktivieren, dass der VMFI-Alarm der kritischen Stufe nicht ausgelöst wird (beide derzeit kritischen Alarme werden in der Tabelle grün angezeigt); Sie können jedoch einen einzelnen Alarm in einer Tabellenzeile nicht deaktivieren, sodass ein VMFI-Alarm als kritischer Alarmwert angezeigt wird, während der andere grün bleibt.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Quittierung aktueller Alarme (Legacy-System)

Ältere Alarme werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Wenn Sie die Liste der alten Alarme verringern oder löschen möchten, können Sie die Alarme bestätigen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Sie müssen über die Berechtigung zum Quittieren von Alarmen verfügen.

Über diese Aufgabe

Da das alte Alarmsystem weiterhin unterstützt wird, wird die Liste der alten Alarme auf der Seite Aktuelle Alarme bei jedem neuen Alarm erhöht. Sie können die Alarme in der Regel ignorieren (da Alarme eine bessere Sicht auf das System bieten) oder die Alarme quittieren.

> Wenn Sie auf das Alarmsystem umgestellt haben, können Sie optional jeden älteren Alarm deaktivieren, um zu verhindern, dass er ausgelöst wird und der Anzahl der älteren Alarme hinzugefügt wird.

Wenn Sie einen Alarm quittieren, wird er nicht mehr auf der Seite „Aktuelle Alarme“ im Grid Manager aufgeführt, es sei denn, der Alarm wird auf der nächsten Schweregrade ausgelöst oder behoben und tritt erneut auf.

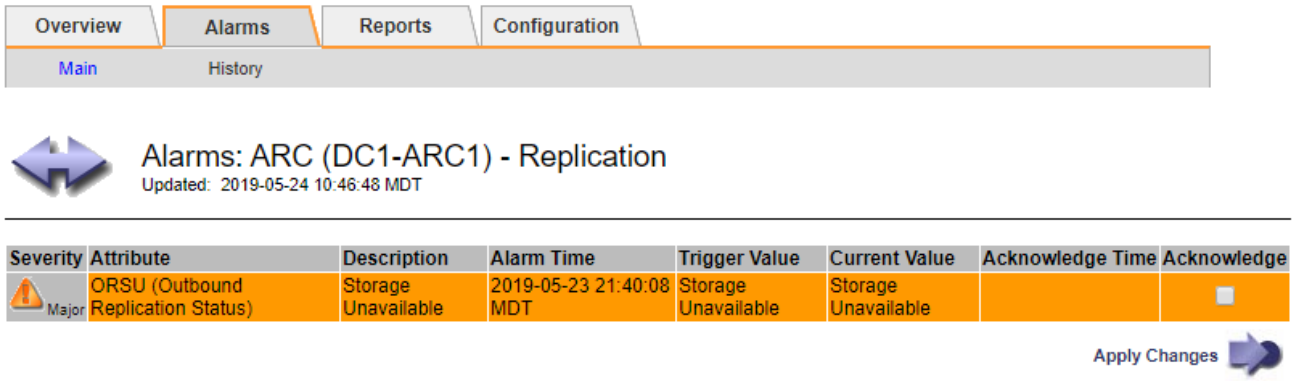
> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Aktueller Alarm** aus.

2. Wählen Sie in der Tabelle den Dienstnamen aus.

   Die Registerkarte Alarme für den ausgewählten Dienst wird angezeigt (**SUPPORT** > **Tools** > **Grid Topology** > ***Grid Node*** > ***Service*** > **Alarme**).



3. Aktivieren Sie das Kontrollkästchen **quittieren** für den Alarm, und klicken Sie auf **Änderungen übernehmen**.

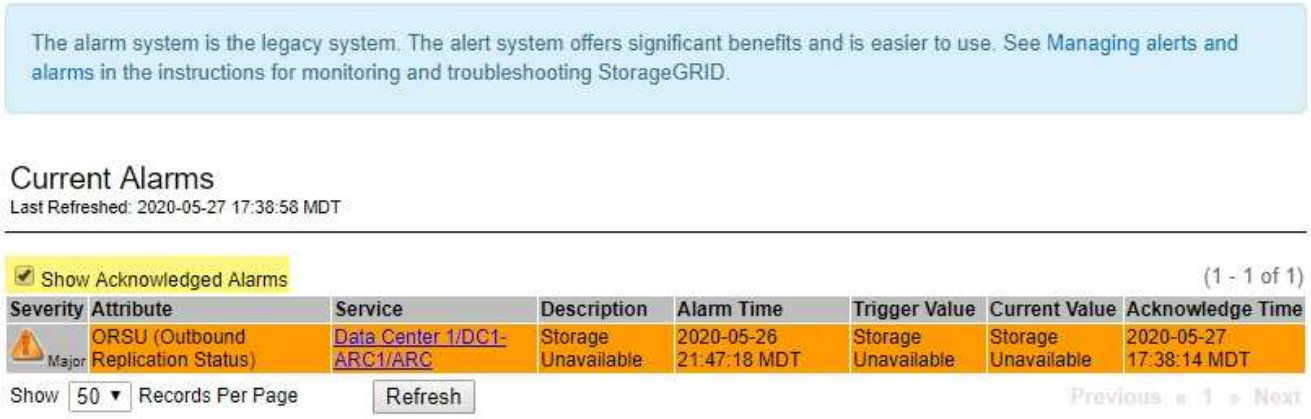
   Der Alarm wird nicht mehr auf dem Armaturenbrett oder der Seite Aktuelle Alarme angezeigt.

   > Wenn Sie einen Alarm bestätigen, wird die Quittierung nicht auf andere Admin-Knoten kopiert. Wenn Sie das Dashboard von einem anderen Admin-Knoten aus anzeigen, wird der aktive Alarm möglicherweise weiterhin angezeigt.

4. Zeigen Sie bei Bedarf bestätigte Alarme an.

   a. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Aktueller Alarm** aus.
   b. Wählen Sie **Bestätigte Alarme Anzeigen**.

      Alle quittierten Alarme werden angezeigt.



Standardalarme anzeigen (Altsystem)

Sie können die Liste aller älteren Standardalarme anzeigen.

Bevor Sie beginnen

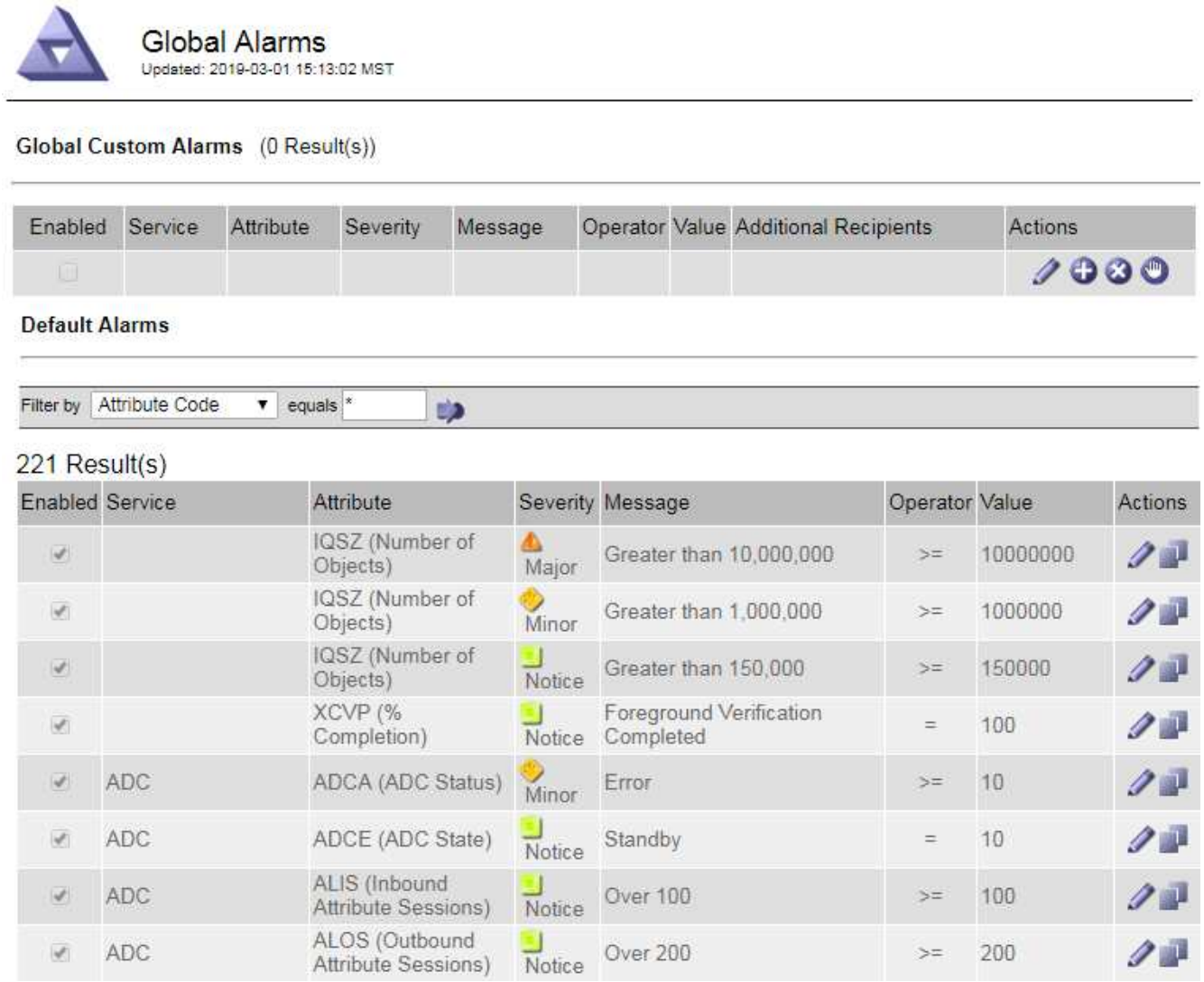
- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Globale Alarme**.
2. Wählen Sie für Filter by die Option **Attributcode** oder **Attributname** aus.
3. Geben Sie für gleich ein Sternchen ein: *
4. Klicken Sie auf den Pfeil Oder drücken Sie **Enter**.

   Alle Standardalarme werden aufgelistet.



Prüfen historischer Alarme und Alarmfrequenz (altes System)

Bei der Fehlerbehebung eines Problems können Sie überprüfen, wie oft in der Vergangenheit ein älterer Alarm ausgelöst wurde.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Führen Sie diese Schritte aus, um eine Liste aller Alarme zu erhalten, die über einen bestimmten Zeitraum ausgelöst wurden.
   a. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Historische Alarme**.
   b. Führen Sie einen der folgenden Schritte aus:
      - Klicken Sie auf einen der Zeiträume.

    - Geben Sie einen benutzerdefinierten Bereich ein, und klicken Sie auf **Benutzerdefinierte Abfrage**.

2. Befolgen Sie diese Schritte, um herauszufinden, wie oft Alarme für ein bestimmtes Attribut ausgelöst wurden.
    a. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
    b. Wählen Sie ***Grid Node*** > ***Service oder Component*** > **Alarme** > **Historie** aus.
    c. Wählen Sie das Attribut aus der Liste aus.
    d. Führen Sie einen der folgenden Schritte aus:
        - Klicken Sie auf einen der Zeiträume.
        - Geben Sie einen benutzerdefinierten Bereich ein, und klicken Sie auf **Benutzerdefinierte Abfrage**.

        Die Alarme werden in umgekehrter chronologischer Reihenfolge aufgeführt.

    e. Um zum Formular für die Anforderung des Alarmverlaufs zurückzukehren, klicken Sie auf **Historie**.

Globale benutzerdefinierte Alarme erstellen (altes System)

Sie haben möglicherweise globale benutzerdefinierte Alarme für das alte System verwendet, um bestimmte Überwachungsanforderungen zu erfüllen. Globale benutzerdefinierte Alarme können Alarmstufen haben, die Standardalarme überschreiben oder Attribute überwachen, die keinen Standardalarm haben.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

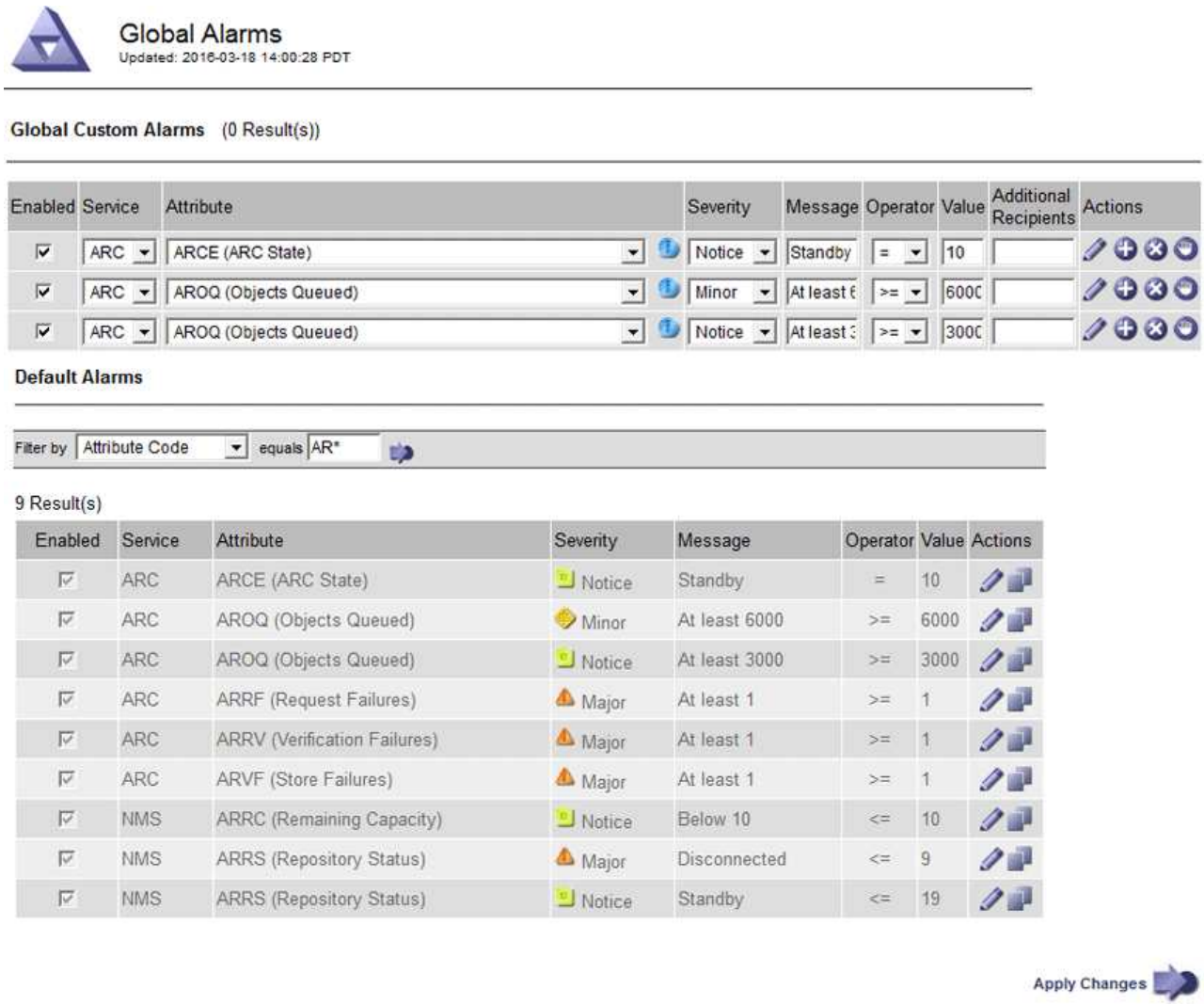
> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Globale benutzerdefinierte Alarme überschreiben Standardalarme. Sie sollten die Standardalarmwerte nur dann ändern, wenn dies unbedingt erforderlich ist. Durch Ändern der Standardalarme besteht die Gefahr, Probleme zu verbergen, die sonst einen Alarm auslösen könnten.

> Seien Sie vorsichtig, wenn Sie die Alarmeinstellungen ändern. Wenn Sie beispielsweise den Schwellenwert für einen Alarm erhöhen, können Sie ein zugrunde liegendes Problem möglicherweise nicht erkennen. Besprechen Sie Ihre vorgeschlagenen Änderungen mit dem technischen Support, bevor Sie eine Alarmeinstellung ändern.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Globale Alarme**.
2. Neue Zeile zur Tabelle „Globale benutzerdefinierte Alarme“ hinzufügen:
    - Um einen neuen Alarm hinzuzufügen, klicken Sie auf **Bearbeiten** (Wenn dies der erste Eintrag ist) oder **Einfügen**.



- Um einen Standardalarm zu ändern, suchen Sie nach dem Standardalarm.
  i. Wählen Sie unter Filter by entweder **Attributcode** oder **Attributname** aus.
  ii. Geben Sie einen Suchstring ein.

  Geben Sie vier Zeichen an oder verwenden Sie Platzhalter (z. B. A????). Oder ab*). Sternchen (*) stellen mehrere Zeichen dar und Fragezeichen (?) Stellt ein einzelnes Zeichen dar.

  iii. Klicken Sie auf den Pfeil Oder drücken Sie **Enter**.
  iv. Klicken Sie in der Ergebnisliste auf **Kopieren** Neben dem Alarm, den Sie ändern möchten.

  Der Standardalarm wird in die Tabelle „Globale benutzerdefinierte Alarme“ kopiert.

3. Nehmen Sie alle erforderlichen Änderungen an den Einstellungen für globale benutzerdefinierte Alarme vor:

Überschrift	Beschreibung
Aktiviert	Aktivieren oder deaktivieren Sie das Kontrollkästchen, um den Alarm zu aktivieren oder zu deaktivieren.

Überschrift	Beschreibung
Attribut	Wählen Sie den Namen und den Code des zu überwachenden Attributs aus der Liste aller Attribute aus, die für den ausgewählten Dienst oder die ausgewählte Komponente gelten. Um Informationen über das Attribut anzuzeigen, klicken Sie auf **Info** Neben dem Namen des Attributs.
Schweregrad	Das Symbol und der Text, der die Alarmstufe angibt.
Nachricht	Der Grund für den Alarm (Verbindung unterbrochen, Lagerraum unter 10 % usw.).
Operator	Operatoren für das Testen des aktuellen Attributwerts gegen den Wert-Schwellenwert: • = gleich • > größer als • < kleiner als • >= größer als oder gleich • <= kleiner als oder gleich • ≠ ist nicht gleich
Wert	Der Schwellwert des Alarms, der zum Testen mit dem tatsächlichen Wert des Attributs über den Operator verwendet wird. Die Eingabe kann eine einzelne Zahl, eine Reihe von Zahlen mit einem Doppelpunkt (1:3) oder eine kommagetrennte Liste von Zahlen und Bereichen sein.
Zusätzliche Empfänger	Eine zusätzliche Liste der E-Mail-Adressen, die bei Auslösung des Alarms benachrichtigt werden sollen. Dies ist zusätzlich zur Mailingliste, die auf der Seite **Alarme** > **E-Mail-Einrichtung** konfiguriert ist. Listen sind durch Komma abgegrenzt. **Hinweis:** Mailinglisten erfordern die Einrichtung des SMTP-Servers. Bestätigen Sie vor dem Hinzufügen von Mailinglisten, dass SMTP konfiguriert ist. Benachrichtigungen für benutzerdefinierte Alarme können Benachrichtigungen von globalen benutzerdefinierten oder Standardalarmen überschreiben.
Aktionen	Steuertasten zu: Bearbeiten Sie eine Zeile + Eine Zeile einfügen + Löschen Sie eine Zeile + Ziehen Sie eine Zeile nach oben oder unten + Kopieren Sie eine Zeile

4. Klicken Sie Auf **Änderungen Übernehmen**.

Deaktivieren von Alarmen (Legacy-System)

Die Alarme im alten Alarmsystem sind standardmäßig aktiviert, Sie können jedoch Alarme deaktivieren, die nicht erforderlich sind. Sie können auch die älteren Alarme deaktivieren, nachdem Sie vollständig auf das neue Alarmsystem umgestellt haben.

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Deaktivieren eines Standardalarms (Legacy-System)

Sie können einen der älteren Standardalarme für das gesamte System deaktivieren.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Durch Deaktivieren eines Alarms für ein Attribut, das derzeit über einen Alarm ausgelöst wird, wird der aktuelle Alarm nicht gelöscht. Der Alarm wird deaktiviert, wenn das Attribut das nächste Mal den Alarmschwellenwert überschreitet, oder Sie können den ausgelösten Alarm löschen.

> Deaktivieren Sie keine der älteren Alarme, bis Sie vollständig auf das neue Alarmsystem umgestellt haben. Andernfalls wird ein zugrunde liegendes Problem möglicherweise erst erkannt, wenn ein kritischer Vorgang nicht abgeschlossen wurde.

Schritte

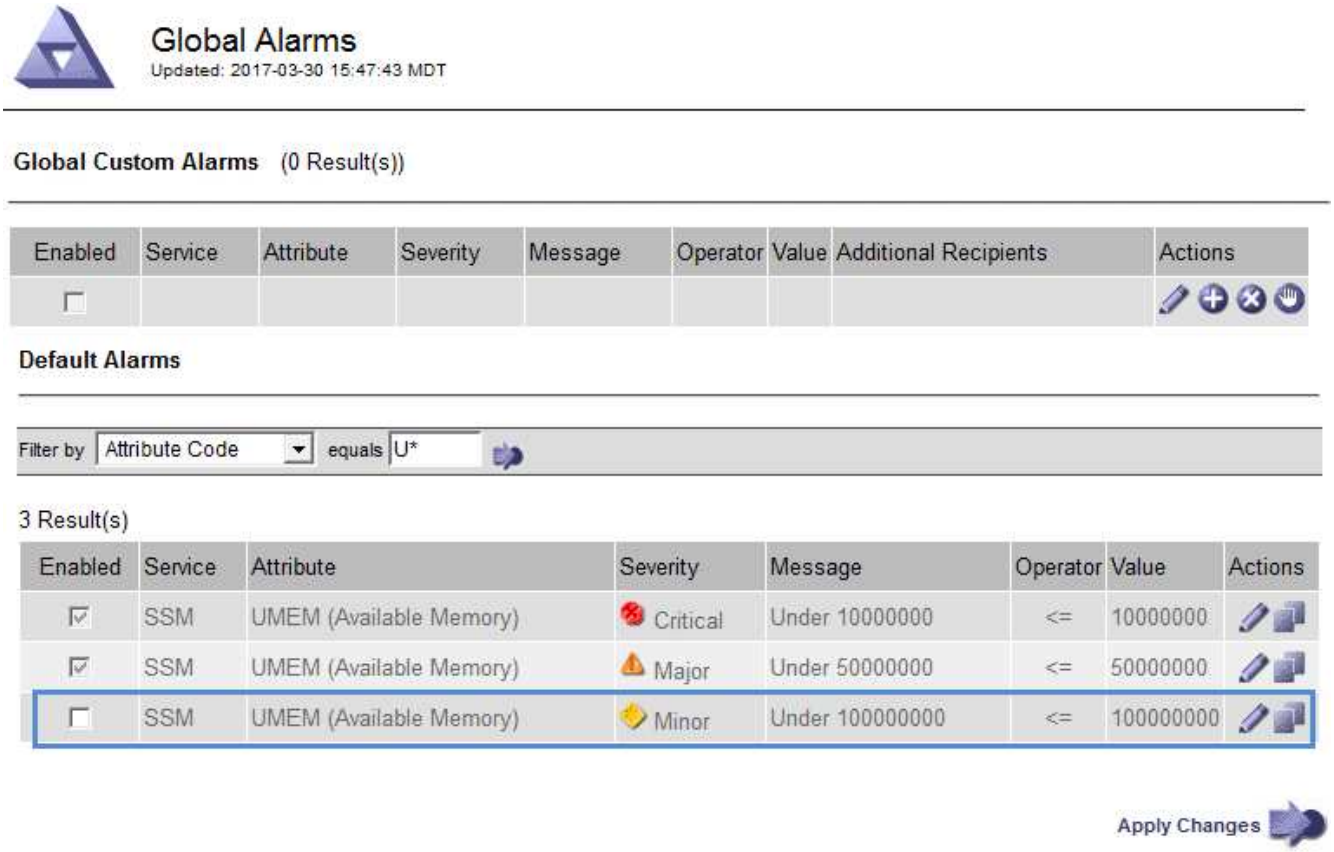
1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Globale Alarme**.
2. Suchen Sie nach dem Standardalarm, der deaktiviert werden soll.
   a. Wählen Sie im Abschnitt Standardalarme die Option **Filtern nach** > **Attributcode** oder **Attributname** aus.
   b. Geben Sie einen Suchstring ein.

      Geben Sie vier Zeichen an oder verwenden Sie Platzhalter (z. B. A????). Oder ab*). Sternchen (*) stellen mehrere Zeichen dar und Fragezeichen (?) Stellt ein einzelnes Zeichen dar.

   c. Klicken Sie auf den Pfeil Oder drücken Sie **Enter**.

      > Wenn Sie **deaktivierte Standardeinstellungen** auswählen, wird eine Liste aller derzeit deaktivierten Standardalarme angezeigt.

3. Klicken Sie in der Tabelle mit den Suchergebnissen auf das Symbol Bearbeiten Für den Alarm, den Sie deaktivieren möchten.



Das Kontrollkästchen **enabled** für den ausgewählten Alarm wird aktiviert.

4. Deaktivieren Sie das Kontrollkästchen **aktiviert**.
5. Klicken Sie Auf **Änderungen Übernehmen**.

   Der Standardalarm ist deaktiviert.

Globale benutzerdefinierte Alarme deaktivieren (Legacy-System)

Sie können einen veralteten globalen benutzerdefinierten Alarm für das gesamte System deaktivieren.

Bevor Sie beginnen

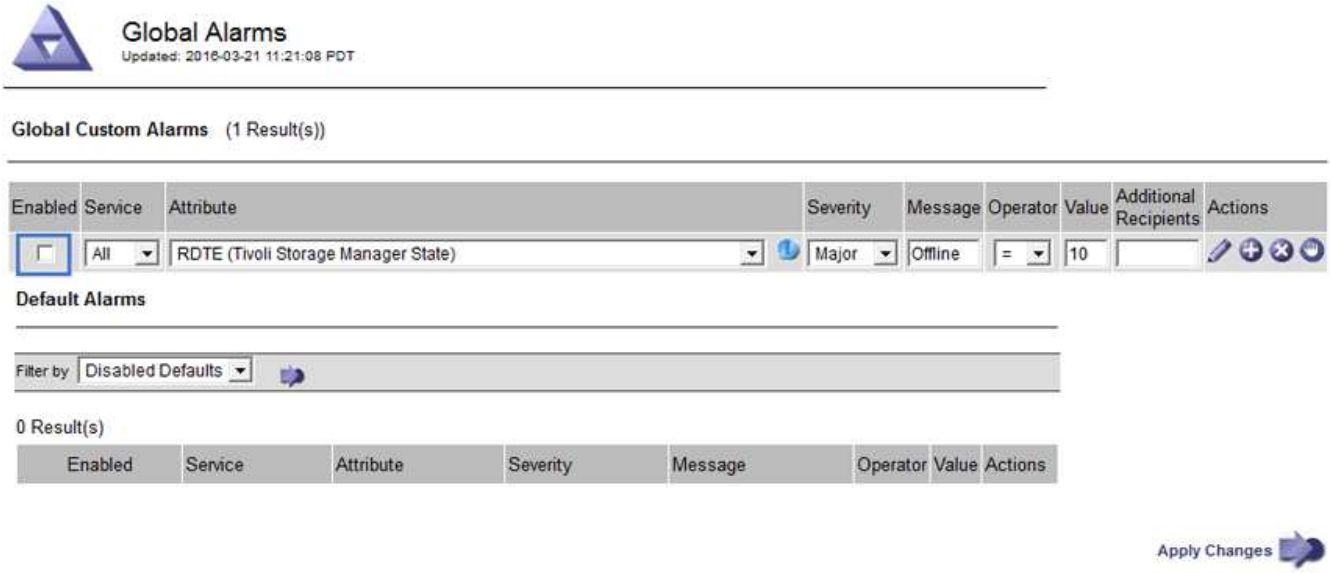
- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Durch Deaktivieren eines Alarms für ein Attribut, das derzeit über einen Alarm ausgelöst wird, wird der aktuelle Alarm nicht gelöscht. Der Alarm wird deaktiviert, wenn das Attribut das nächste Mal den Alarmschwellenwert überschreitet, oder Sie können den ausgelösten Alarm löschen.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Globale Alarme**.
2. Klicken Sie in der Tabelle Globale benutzerdefinierte Alarme auf **Bearbeiten** Neben dem Alarm, den Sie deaktivieren möchten.
3. Deaktivieren Sie das Kontrollkästchen **aktiviert**.



4. Klicken Sie Auf **Änderungen Übernehmen**.

   Der globale benutzerdefinierte Alarm ist deaktiviert.

Ausgelöste Alarme löschen (Legacy-System)

Wenn ein älterer Alarm ausgelöst wird, können Sie ihn löschen, anstatt ihn zu bestätigen.

Bevor Sie beginnen

- Sie müssen die haben `Passwords.txt` Datei:

Durch Deaktivieren eines Alarms für ein Attribut, das derzeit einen Alarm ausgelöst hat, wird der Alarm nicht gelöscht. Bei der nächsten Änderung des Attributs wird der Alarm deaktiviert. Sie können den Alarm bestätigen oder, wenn Sie den Alarm sofort löschen möchten, anstatt zu warten, bis sich der Attributwert ändert (was zu einer Änderung des Alarmstatus führt), können Sie den ausgelösten Alarm löschen. Dies ist hilfreich, wenn Sie einen Alarm sofort gegen ein Attribut löschen möchten, dessen Wert sich nicht oft ändert (z. B. Attribute für den Status).

1. Deaktivieren Sie den Alarm.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: *`ssh admin@primary_Admin_Node_IP`*
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
3. Starten Sie den NMS-Service neu: `service nms restart`
4. Melden Sie sich beim Admin-Knoten ab: `exit`

   Der Alarm wurde gelöscht.

Benachrichtigungen für Alarme konfigurieren (Altsystem)

StorageGRID System kann automatisch E-Mails und senden "SNMP-Benachrichtigungen" Wenn ein Alarm ausgelöst wird oder sich ein Servicenstatus ändert.

Standardmäßig werden keine Alarm-E-Mail-Benachrichtigungen gesendet. Für E-Mail-Benachrichtigungen müssen Sie den E-Mail-Server konfigurieren und die E-Mail-Empfänger angeben. Für SNMP-Benachrichtigungen müssen Sie den SNMP-Agent konfigurieren.

Arten von Alarmanmeldungen (Legacy-System)

Wenn ein älterer Alarm ausgelöst wird, sendet das StorageGRID System zwei Arten von Alarmmeldungen: Schweregrad und Service-Status.

Benachrichtigungen auf Schweregraden

Eine Alarm-E-Mail-Benachrichtigung wird gesendet, wenn ein älterer Alarm auf einer ausgewählten Schweregrade ausgelöst wird:

- Hinweis
- Gering
- Major
- Kritisch

Eine Mailingliste erhält alle Benachrichtigungen, die sich auf den Alarm für den ausgewählten Schweregrad beziehen. Eine Benachrichtigung wird auch gesendet, wenn der Alarm den Alarmpegel verlässt – entweder durch eine Lösung oder durch Eingabe eines anderen Schweregrads.

Service-Status-Benachrichtigungen

Eine Benachrichtigung über den Servicenstatus wird gesendet, wenn ein Dienst (z. B. der LDR-Dienst oder der NMS-Dienst) den ausgewählten Servicenstatus eingibt und den ausgewählten Servicenstatus verlässt. Dienststatus-Benachrichtigungen werden gesendet, wenn ein Dienst einen der folgenden Servicenstatus eingibt oder verlässt:

- Unbekannt
- Administrativ Nach Unten

Eine Mailingliste erhält alle Benachrichtigungen, die sich auf Änderungen im ausgewählten Status beziehen.

E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)

Wenn StorageGRID E-Mail-Benachrichtigungen senden soll, wenn ein älterer Alarm ausgelöst wird, müssen Sie die SMTP-Mail-Server-Einstellungen angeben. Das StorageGRID System sendet nur E-Mails, es kann keine E-Mails empfangen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Verwenden Sie diese Einstellungen, um den SMTP-Server zu definieren, der für ältere E-Mail-

Benachrichtigungen und AutoSupport-E-Mail-Nachrichten verwendet wird. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

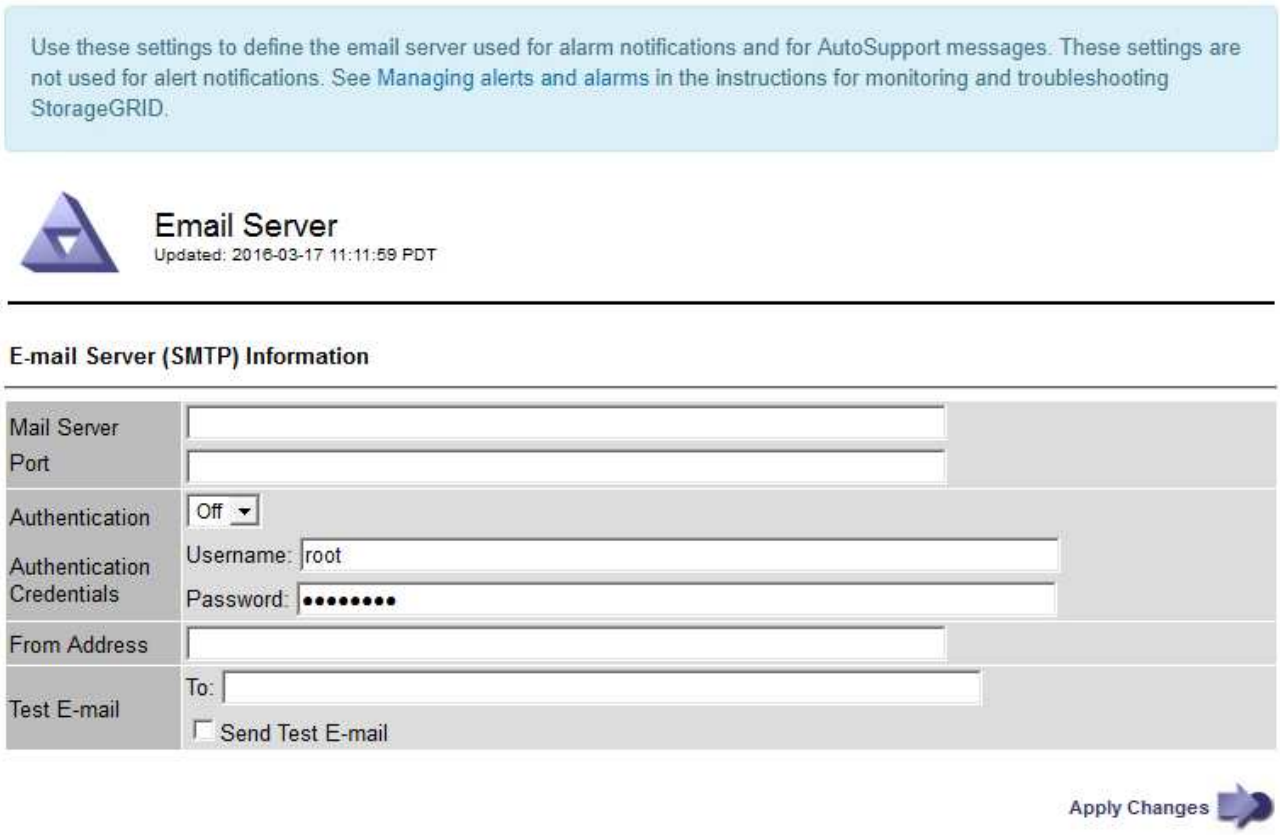
> Wenn Sie SMTP als Protokoll für AutoSupport-Pakete verwenden, haben Sie möglicherweise bereits einen SMTP-Mailserver konfiguriert. Derselbe SMTP-Server wird für Benachrichtigungen über Alarm-E-Mails verwendet, sodass Sie diesen Vorgang überspringen können. Siehe "Anweisungen für die Administration von StorageGRID".

SMTP ist das einzige Protokoll, das zum Senden von E-Mails unterstützt wird.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Server** aus.

   Die Seite E-Mail-Server wird angezeigt. Diese Seite wird auch verwendet, um den E-Mail-Server für AutoSupport-Pakete zu konfigurieren.



3. Fügen Sie die folgenden SMTP-Mail-Server-Einstellungen hinzu:

Element	Beschreibung
Mailserver	IP-Adresse des SMTP-Mail-Servers. Sie können anstelle einer IP-Adresse einen Hostnamen eingeben, wenn Sie zuvor DNS-Einstellungen auf dem Admin-Knoten konfiguriert haben.
Port	Portnummer für den Zugriff auf den SMTP-Mail-Server.

Element	Beschreibung
Authentifizierung	Ermöglicht die Authentifizierung des SMTP-Mail-Servers. Standardmäßig ist die Authentifizierung deaktiviert.
Authentifizierungsdaten	Benutzername und Passwort des SMTP-Mail-Servers. Wenn die Authentifizierung auf ein festgelegt ist, müssen ein Benutzername und ein Passwort für den Zugriff auf den SMTP-Mail-Server angegeben werden.

4. Geben Sie unter **von Address** eine gültige E-Mail-Adresse ein, die der SMTP-Server als sendende E-Mail-Adresse erkennt. Dies ist die offizielle E-Mail-Adresse, von der die E-Mail-Nachricht gesendet wird.
5. Senden Sie optional eine Test-E-Mail, um zu bestätigen, dass die SMTP-Mail-Servereinstellungen korrekt sind.
   a. Fügen Sie im Feld **E-Mail-Test** > **bis** eine oder mehrere Adressen hinzu, auf die Sie zugreifen können.

      Sie können eine einzelne E-Mail-Adresse oder eine kommagetrennte Liste von E-Mail-Adressen eingeben. Da der NMS-Dienst den Erfolg oder Fehler beim Senden einer Test-E-Mail nicht bestätigt, müssen Sie den Posteingang des Testempfängers überprüfen können.

   b. Wählen Sie **Test-E-Mail senden**.
6. Klicken Sie Auf **Änderungen Übernehmen**.

   Die SMTP-Mail-Server-Einstellungen werden gespeichert. Wenn Sie Informationen für eine Test-E-Mail eingegeben haben, wird diese E-Mail gesendet. Test-E-Mails werden sofort an den Mailserver gesendet und nicht über die Benachrichtigungswarteschlange gesendet. In einem System mit mehreren Admin-Nodes sendet jeder Admin-Node eine E-Mail. Der Empfang der Test-E-Mail bestätigt, dass Ihre SMTP-Mail-Server-Einstellungen korrekt sind und dass der NMS-Dienst erfolgreich eine Verbindung zum Mail-Server herstellt. Ein Verbindungsproblem zwischen dem NMS-Dienst und dem Mail-Server löst den Alarm für ältere MINUTEN (NMS Notification Status) auf der Stufe mit dem Schweregrad „Minor“ aus.

E-Mail-Vorlagen für Alarme erstellen (altes System)

Mithilfe von E-Mail-Vorlagen können Sie die Kopfzeile, Fußzeile und den Betreff einer früheren Alarm-E-Mail-Benachrichtigung anpassen. Sie können E-Mail-Vorlagen verwenden, um eindeutige Benachrichtigungen zu senden, die denselben Text an verschiedene Mailinglisten enthalten.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

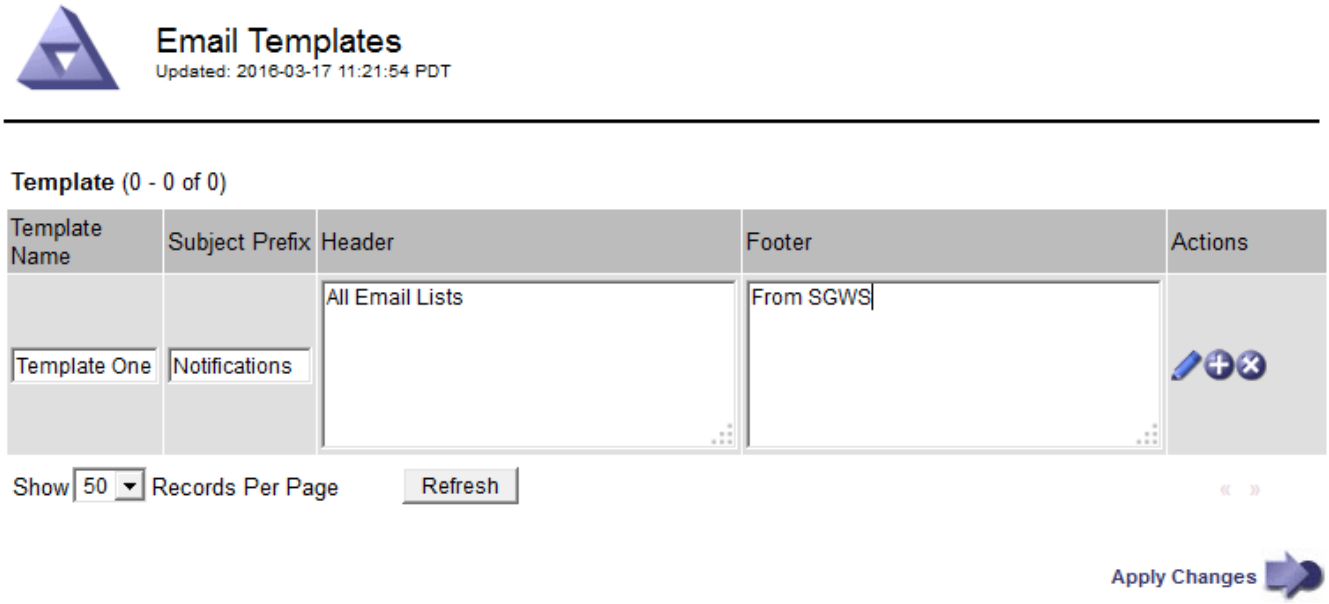
Mit diesen Einstellungen können Sie die E-Mail-Vorlagen festlegen, die für ältere Benachrichtigungen verwendet werden. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

Für unterschiedliche Mailinglisten sind möglicherweise andere Kontaktinformationen erforderlich. Vorlagen enthalten keinen Haupttext der E-Mail-Nachricht.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**.

2. Wählen Sie im Menü E-Mail die Option **Vorlagen**.
3. Klicken Sie Auf **Bearbeiten** (Oder **Einfügen** Falls dies nicht die erste Vorlage ist).



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

Element	Beschreibung
Vorlagenname	Eindeutiger Name zur Identifizierung der Vorlage. Vorlagennamen können nicht dupliziert werden.
Präfix Für Betreff	Optional Präfix, das am Anfang der Betreffzeile einer E-Mail angezeigt wird. Mit Präfixen können E-Mail-Filter einfach konfiguriert und Benachrichtigungen organisiert werden.
Kopfzeile	Optional Kopfzeilentext, der am Anfang des E-Mail-Nachrichtentextes erscheint. Der Kopfzeilentext kann verwendet werden, um den Inhalt der E-Mail-Nachricht mit Informationen wie Firmenname und Adresse zu versehen.
Fußzeile	Optional Fußzeilentext, der am Ende des E-Mail-Nachrichtentexts angezeigt wird. Über Fußzeile können Sie die eMail-Nachricht mit Erinnerungsdaten wie einer Telefonnummer oder einem Link zu einer Website schließen.

5. Klicken Sie Auf **Änderungen Übernehmen**.

   Es wird eine neue Vorlage für Benachrichtigungen hinzugefügt.

Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)

Mit Mailinglisten können Sie Empfänger benachrichtigen, wenn ein älterer Alarm ausgelöst wird oder wenn sich ein Servicenstatus ändert. Sie müssen mindestens eine Mailingliste erstellen, bevor Sie Alarm-E-Mail-Benachrichtigungen senden können. Um eine Benachrichtigung an einen einzelnen Empfänger zu senden,

erstellen Sie eine Mailingliste mit einer E-Mail-Adresse.

Bevor Sie beginnen

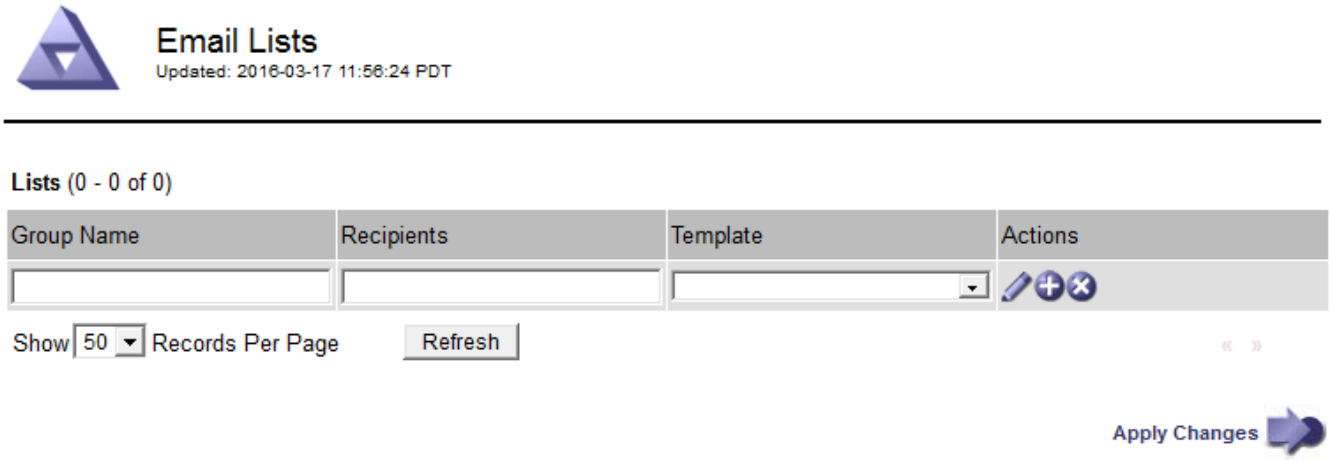
- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".
- Wenn Sie eine E-Mail-Vorlage für die Mailingliste (benutzerdefinierte Kopfzeile, Fußzeile und Betreffzeile) angeben möchten, müssen Sie die Vorlage bereits erstellt haben.

Über diese Aufgabe

Mit diesen Einstellungen können Sie die Mailinglisten definieren, die für Benachrichtigungen über ältere E-Mails verwendet werden. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Listen** aus.
3. Klicken Sie Auf **Bearbeiten** (Oder *Einfügen* Falls dies nicht die erste Mailingliste ist).



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

Element	Beschreibung
Gruppenname	Eindeutiger Name zur Identifizierung der Mailingliste. Mailinglistennamen können nicht dupliziert werden. **Hinweis:** Wenn Sie den Namen einer Mailingliste ändern, wird die Änderung nicht an die anderen Standorte weitergegeben, die den Namen der Mailingliste verwenden. Sie müssen alle konfigurierten Benachrichtigungen manuell aktualisieren, um den neuen Namen der Mailingliste zu verwenden.
Empfänger	Eine einzelne E-Mail-Adresse, eine zuvor konfigurierte Mailingliste oder eine kommagetrennte Liste von E-Mail-Adressen und Mailinglisten, an die Benachrichtigungen gesendet werden. **Hinweis:** Wenn eine E-Mail-Adresse zu mehreren Mailinglisten gehört, wird nur eine E-Mail-Benachrichtigung gesendet, wenn ein Benachrichtigungserlösungs-Ereignis auftritt.

Element	Beschreibung
Vorlage	Wählen Sie optional eine E-Mail-Vorlage aus, um eine eindeutige Kopfzeile, Fußzeile und Betreffzeile zu Benachrichtigungen hinzuzufügen, die an alle Empfänger dieser Mailingliste gesendet werden.

5. Klicken Sie Auf **Änderungen Übernehmen**.

   Es wird eine neue Mailingliste erstellt.

E-Mail-Benachrichtigungen für Alarme konfigurieren (Legacy-System)

Um E-Mail-Benachrichtigungen für das ältere Alarmsystem zu erhalten, müssen die Empfänger Mitglied einer Mailingliste sein und diese Liste zur Seite Benachrichtigungen hinzugefügt werden. Benachrichtigungen werden so konfiguriert, dass E-Mails nur dann an Empfänger gesendet werden, wenn ein Alarm mit einem bestimmten Schweregrad ausgelöst wird oder wenn sich ein Servicenstatus ändert. Empfänger erhalten somit nur die Benachrichtigungen, die sie erhalten müssen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".
- Sie müssen eine E-Mail-Liste konfiguriert haben.

Über diese Aufgabe

Mit diesen Einstellungen können Sie Benachrichtigungen für ältere Alarme konfigurieren. Diese Einstellungen werden nicht für Warnmeldungen verwendet.

Wenn eine E-Mail-Adresse (oder eine Liste) zu mehreren Mailinglisten gehört, wird nur eine E-Mail-Benachrichtigung gesendet, wenn ein Ereignis auftritt, bei dem eine Benachrichtigung ausgelöst wird. So kann beispielsweise eine Gruppe von Administratoren in Ihrem Unternehmen so konfiguriert werden, dass sie Benachrichtigungen für alle Alarme unabhängig vom Schweregrad erhalten. Eine andere Gruppe benötigt möglicherweise nur Benachrichtigungen für Alarme mit einem Schweregrad von „kritisch“. Sie können zu beiden Listen gehören. Wenn ein kritischer Alarm ausgelöst wird, erhalten Sie nur eine Benachrichtigung.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Benachrichtigungen** aus.
3. Klicken Sie Auf *Bearbeiten* (Oder *Einfügen* Wenn dies nicht die erste Benachrichtigung ist).
4. Wählen Sie unter E-Mail-Liste die Mailingliste aus.
5. Wählen Sie eine oder mehrere Alarmschweregrade und Servicestufen aus.
6. Klicken Sie Auf **Änderungen Übernehmen**.

   Benachrichtigungen werden an die Mailingliste gesendet, wenn Alarme mit dem ausgewählten Schweregrad „Alarm“ oder „Service“ ausgelöst oder geändert werden.

Alarmbenachrichtigungen für eine Mailingliste unterdrücken (Älteres System)

Sie können Alarmbenachrichtigungen für eine Mailingliste unterdrücken, wenn Sie nicht mehr möchten, dass die Mailingliste Benachrichtigungen über Alarme erhalten. Beispielsweise möchten Sie Benachrichtigungen über ältere Alarme unterdrücken, nachdem Sie zu Warnmeldungen gewechselt haben.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Verwenden Sie diese Einstellungen, um E-Mail-Benachrichtigungen für das ältere Alarmsystem zu unterdrücken. Diese Einstellungen gelten nicht für E-Mail-Benachrichtigungen.

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**.
2. Wählen Sie im Menü E-Mail die Option **Benachrichtigungen** aus.
3. Klicken Sie Auf **Bearbeiten** Neben der Mailingliste, für die Sie Benachrichtigungen unterdrücken möchten.
4. Aktivieren Sie unter unterdrücken das Kontrollkästchen neben der Mailingliste, die Sie unterdrücken möchten, oder wählen Sie **unterdrücken** oben in der Spalte, um alle Mailinglisten zu unterdrücken.
5. Klicken Sie Auf **Änderungen Übernehmen**.

   Ältere Alarmbenachrichtigungen werden für die ausgewählten Mailinglisten unterdrückt.

Anzeigen von älteren Alarmen

Alarme (Altsystem) werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Sie können die derzeit aktiven Alarme auf der Seite Aktuelle Alarme anzeigen.

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".

Schritte

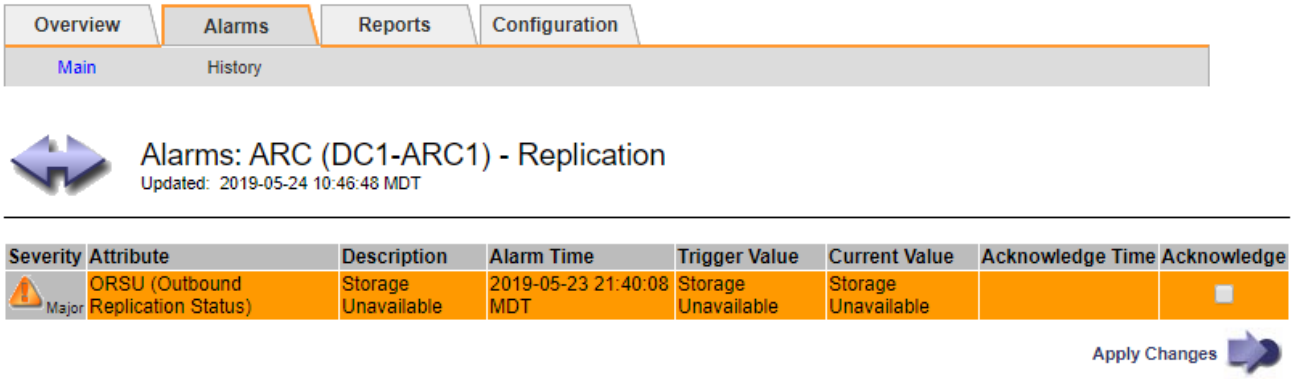
1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Aktueller Alarm** aus.

Das Alarmsymbol zeigt den Schweregrad jedes Alarms wie folgt an:

Symbol	Farbe	Alarmschwere grad	Bedeutung
	Gelb	Hinweis	Der Node ist mit dem Grid verbunden. Es ist jedoch eine ungewöhnliche Bedingung vorhanden, die den normalen Betrieb nicht beeinträchtigt.
	Hellorange	Gering	Der Node ist mit dem Raster verbunden, aber es existiert eine anormale Bedingung, die den Betrieb in Zukunft beeinträchtigen könnte. Sie sollten untersuchen, um eine Eskalation zu verhindern.
	Dunkelorange	Major	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die sich derzeit auf den Betrieb auswirkt. Um eine Eskalation zu vermeiden, ist eine sofortige Aufmerksamkeit erforderlich.
	Rot	Kritisch	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die normale Vorgänge angehalten hat. Sie sollten das Problem sofort beheben.

2. Um mehr über das Attribut zu erfahren, das den Alarm ausgelöst hat, klicken Sie mit der rechten Maustaste auf den Attributnamen in der Tabelle.
3. Um weitere Details zu einem Alarm anzuzeigen, klicken Sie in der Tabelle auf den Servicenamen.

   Die Registerkarte Alarme für den ausgewählten Dienst wird angezeigt (**SUPPORT** > **Tools** > **Grid Topology** > ***Grid Node*** > ***Service*** > **Alarme**).



4. Wenn Sie die Anzahl der aktuellen Alarme löschen möchten, können Sie optional Folgendes tun:
   - Bestätigen Sie den Alarm. Ein bestätigter Alarm wird nicht mehr in die Anzahl der älteren Alarme einbezogen, es sei denn, er wird auf der nächsten Stufe ausgelöst oder es wird behoben und tritt erneut auf.
   - Deaktivieren Sie einen bestimmten Standardalarm oder einen globalen benutzerdefinierten Alarm für das gesamte System, um eine erneute Auslösung zu verhindern.

Verwandte Informationen

"Alarmreferenz (Altsystem)"

"Quittierung aktueller Alarme (Legacy-System)"

"Deaktivieren von Alarmen (Legacy-System)"

Alarmreferenz (Altsystem)

In der folgenden Tabelle sind alle alten Standardalarme aufgeführt. Wenn ein Alarm ausgelöst wird, können Sie den Alarmcode in dieser Tabelle nach den empfohlenen Maßnahmen suchen.

> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Codieren	Name	Service	Empfohlene Maßnahmen
ABRL	Verfügbare Attributrelais	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Stellen Sie die Verbindung zu einem Dienst (einem ADC-Dienst) wieder her, der einen Attributrelais-Dienst so schnell wie möglich ausführt. Wenn keine verbundenen Attributrelais vorhanden sind, kann der Grid-Knoten keine Attributwerte an den NMS-Dienst melden. So kann der NMS-Dienst den Status des Dienstes nicht mehr überwachen oder Attribute für den Dienst aktualisieren. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ACMS	Verfügbare Metadaten	BARC, BLDR, BCMN	Ein Alarm wird ausgelöst, wenn ein LDR- oder ARC-Dienst die Verbindung zu einem DDS-Dienst verliert. In diesem Fall können die Aufnahme- und Abrufvorgänge nicht verarbeitet werden. Wenn die Nichtverfügbarkeit von DDS-Diensten nur ein kurzes vorübergehendes Problem ist, können Transaktionen verzögert werden. Überprüfen und Wiederherstellen der Verbindungen zu einem DDS-Dienst, um diesen Alarm zu löschen und den Service auf die volle Funktionalität zurückzugeben.
AKTE	Status Des Cloud Tiering Service	LICHTBOGEN	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Cloud Tiering - Simple Storage Service (S3). Wenn das ATTRIBUT ACTS für den Archiv-Node auf Read-Only aktiviert oder Read-Write deaktiviert ist, müssen Sie das Attribut auf Read-Write aktiviert setzen. Wenn ein Hauptalarm aufgrund eines Authentifizierungsfehlers ausgelöst wird, überprüfen Sie ggf. die mit dem Ziel-Bucket verknüpften Anmeldeinformationen und aktualisieren Sie Werte. Wenn aus irgendeinem anderen Grund ein Großalarm ausgelöst wird, wenden Sie sich an den technischen Support.
ADCA	ADC-Status	ADU	Wenn ein Alarm ausgelöst wird, wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***site*** > ***GRID Node*** > **ADC** > **Übersicht** > **Main** und **ADC** > **Alarme** > **Main**, um die Ursache des Alarms zu bestimmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
ADCE	ADC-Status	ADU	Wenn der Wert des ADC-Status Standby lautet, setzen Sie die Überwachung des Dienstes fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert des ADC-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AITE	Status Abrufen	BARC	Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert für „Abruffzustand“ auf „Ziel“ wartet, prüfen Sie den TSM Middleware-Server und stellen Sie sicher, dass er ordnungsgemäß funktioniert. Wenn der Archivknoten gerade zum StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass die Verbindung des Archiv-Knotens zum angestrebten externen Archiv-Speichersystem korrekt konfiguriert ist. Wenn der Wert des Status „Archivabrueve“ Offline lautet, versuchen Sie, den Status auf Online zu aktualisieren. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abruf** > **Konfiguration** > **Main**, wählen Sie **Archiv Status abrufen** > **Online** und klicken Sie auf **Änderungen anwenden**. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AITU	Status Abrufen	BARC	Wenn der Wert für „Status abrufen“ als Zielfehler gilt, prüfen Sie das ausgewählte externe Archivspeichersystem auf Fehler. Wenn der Wert des Status „Archivabrueve“ auf „Sitzung verloren“ lautet, prüfen Sie das ausgewählte externe Archivspeichersystem, um sicherzustellen, dass es online ist und ordnungsgemäß funktioniert. Überprüfen Sie die Netzwerkverbindung mit dem Ziel. Wenn der Wert des Status „Archiv abrufen“ Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.
ALIS	Eingehende Attributsitzungen	ADU	Wenn die Anzahl der eingehenden Attributsitzungen in einem Attributrelais zu groß wird, kann dies ein Hinweis sein, dass das StorageGRID-System unausgewogen geworden ist. Unter normalen Bedingungen sollten Attributsitzungen gleichmäßig auf ADC-Dienste verteilt werden. Ein Ungleichgewicht kann zu Performance-Problemen führen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ALOS	Ausgehende Attributsitzungen	ADU	Der ADC-Dienst verfügt über eine hohe Anzahl von Attributsitzungen und wird überlastet. Wenn dieser Alarm ausgelöst wird, wenden Sie sich an den technischen Support.
ALUR	Nicht Erreichbare Attributdatenbanken	ADU	Überprüfen Sie die Netzwerkverbindung mit dem NMS-Service, um sicherzustellen, dass der Dienst das Attribut-Repository kontaktieren kann. Wenn dieser Alarm ausgelöst wird und die Netzwerkverbindung gut ist, wenden Sie sich an den technischen Support.
AMQS	Audit-Nachrichten In Queued	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Meldungen nicht sofort an ein Audit-Relay oder Repository weitergeleitet werden können, werden die Meldungen in einer Datenträgerwarteschlange gespeichert. Wenn die Warteschlange voll wird, können Ausfälle auftreten. Um Ihnen die Möglichkeit zu geben, rechtzeitig zu reagieren, um einen Ausfall zu verhindern, werden AMQS-Alarme ausgelöst, wenn die Anzahl der Meldungen in der Datenträgerwarteschlange die folgenden Schwellenwerte erreicht: • Hinweis: Mehr als 100,000 Nachrichten • Minor: Mindestens 500,000 Nachrichten • Major: Mindestens 2,000,000 Nachrichten • Kritisch: Mindestens 5,000,000 Nachrichten Wenn ein AMQS-Alarm ausgelöst wird, überprüfen Sie die Belastung des Systems. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen. In diesem Fall können Sie den Alarm ignorieren. Wenn der Alarm weiterhin besteht und der Schweregrad erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. Verringern Sie die Betriebsrate des Clients oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie den Audit-Level auf Fehler oder aus ändern. Siehe "Konfigurieren von Überwachungsmeldungen und Protokollzielen".

Codieren	Name	Service	Empfohlene Maßnahmen
AOTE	Store State	BARC	Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Speicherstatus auf Ziel wartet, prüfen Sie das externe Archivspeichersystem und stellen Sie sicher, dass es ordnungsgemäß funktioniert. Wenn der Archivknoten gerade zum StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass die Verbindung des Archiv-Knotens zum angestrebten externen Archiv-Speichersystem korrekt konfiguriert ist. Wenn der Wert des Store State Offline lautet, prüfen Sie den Wert des Store Status. Beheben Sie alle Probleme, bevor Sie den Store-Status wieder auf Online verschieben.
AOTU	Speicherstatus	BARC	Wenn der Wert des Speicherstatus „Sitzung verloren“ lautet, prüfen Sie, ob das externe Archivspeichersystem verbunden und online ist. Wenn der Wert von Zielfehler ist, überprüfen Sie das externe Archivspeichersystem auf Fehler. Wenn der Wert des Speicherstatus Unbekannter Fehler lautet, wenden Sie sich an den technischen Support.
APMS	Storage Multipath-Konnektivität	SSM	Wenn der Multipath-Status-Alarm als „herabgesetzt“ angezeigt wird (wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**, und wählen Sie dann ***Site*** > ***Grid Node*** > **SSM** > **Events**), gehen Sie wie folgt vor: 1. Schließen Sie das Kabel an, das keine Kontrollleuchten anzeigt, oder ersetzen Sie es. 2. Warten Sie eine bis fünf Minuten. Ziehen Sie das andere Kabel erst nach mindestens fünf Minuten ab, nachdem Sie das erste Kabel angeschlossen haben. Das zu frühe Auflösen kann dazu führen, dass das Root-Volume schreibgeschützt ist, was erfordert, dass die Hardware neu gestartet wird. 3. Kehren Sie zur Seite **SSM** > **Resources** zurück, und überprüfen Sie, ob sich der Status „degraded“ Multipath im Abschnitt Speicherhardware in „nominal“ geändert hat.

Codieren	Name	Service	Empfohlene Maßnahmen
ARCE	BOGENZUSTAND	LICHTBOGEN	Der ARC-Dienst verfügt über einen Standby-Status, bis alle ARC-Komponenten (Replikation, Speicher, Abrufen, Ziel) gestartet wurden. Dann geht es zu Online. Wenn der Wert des ARC-Status nicht von Standby auf Online übergeht, überprüfen Sie den Status der ARC-Komponenten. Wenn der Wert für ARC-Status Offline lautet, starten Sie den Service neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AROQ	Objekte In Queued	LICHTBOGEN	Dieser Alarm kann ausgelöst werden, wenn das Wechselspeichergerät aufgrund von Problemen mit dem angestrebten externen Archivspeichersystem langsam läuft oder wenn mehrere Lesefehler auftreten. Überprüfen Sie das externe Archiv-Storage-System auf Fehler und stellen Sie sicher, dass es ordnungsgemäß funktioniert. In manchen Fällen kann dieser Fehler auf eine hohe Datenanforderung zurückzuführen sein. Überwachen Sie die Anzahl der Objekte, die sich in der Warteschlange befinden, bei abnehmender Systemaktivität.

Codieren	Name	Service	Empfohlene Maßnahmen
ARRF	Anfragefehler	LICHTBOGEN	Wenn ein Abruf aus dem Zielspeichersystem zur externen Archivierung fehlschlägt, versucht der Archivknoten den Abruf erneut, da der Ausfall durch ein vorübergehendes Problem verursacht werden kann. Wenn die Objektdaten jedoch beschädigt sind oder als dauerhaft nicht verfügbar markiert wurden, schlägt der Abruf nicht fehl. Stattdessen wird der Archivknoten kontinuierlich erneut versucht, den Abruf erneut zu versuchen, und der Wert für Anforderungsfehler steigt weiter. Dieser Alarm kann darauf hinweisen, dass die Speichermedien, auf denen die angeforderten Daten gespeichert sind, beschädigt sind. Überprüfen Sie das externe Archiv-Storage-System, um das Problem weiter zu diagnostizieren. Wenn Sie feststellen, dass die Objektdaten nicht mehr im Archiv sind, muss das Objekt aus dem StorageGRID System entfernt werden. Weitere Informationen erhalten Sie vom technischen Support. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abruf** > **Konfiguration** > **Main**, wählen Sie **Fehleranzahl der Anforderung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
ARRV	Verifizierungsfehler	LICHTBOGEN	Wenden Sie sich an den technischen Support, um das Problem zu diagnostizieren und zu beheben. Nachdem das Problem behoben wurde, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abrufen** > **Konfiguration** > **Main**, wählen Sie **Fehleranzahl der Überprüfung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
ARVF	Speicherfehler	LICHTBOGEN	Dieser Alarm kann aufgrund von Fehlern im externen Archivspeichersystem auftreten. Überprüfen Sie das externe Archiv-Storage-System auf Fehler und stellen Sie sicher, dass es ordnungsgemäß funktioniert. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abrufen** > **Konfiguration** > **Main**, wählen Sie **Anzahl der Fehler im Store zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
ASXP	Revisionsfreigaben	AMS	Ein Alarm wird ausgelöst, wenn der Wert der Revisionsfreigaben Unbekannt ist. Dieser Alarm kann auf ein Problem bei der Installation oder Konfiguration des Admin-Knotens hinweisen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUMA	AMS-Status	AMS	Wenn der Wert für AMS Status DB-Verbindungsfehler ist, starten Sie den Grid-Node neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUME	AMS-Staat	AMS	Wenn der Wert des AMS-Status Standby lautet, fahren Sie mit der Überwachung des StorageGRID-Systems fort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. Wenn der Wert von AMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUXS	Exportstatus Prüfen	AMS	Wenn ein Alarm ausgelöst wird, beheben Sie das zugrunde liegende Problem und starten Sie dann den AMS-Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
HINZUFÜGEN	Anzahl Ausgefallener Speicher-Controller-Laufwerke	SSM	Dieser Alarm wird ausgelöst, wenn ein oder mehrere Laufwerke in einem StorageGRID-Gerät ausgefallen sind oder nicht optimal sind. Ersetzen Sie die Laufwerke nach Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
BASF	Verfügbare Objektkennungen	CMN	Wenn ein StorageGRID System bereitgestellt wird, wird dem CMN-Service eine feste Anzahl von Objekt-IDs zugewiesen. Dieser Alarm wird ausgelöst, wenn das StorageGRID-System seine Versorgung mit Objektkennungen ausgibt. Wenden Sie sich an den technischen Support, um weitere Kennungen zuzuweisen.
BASS	Identifier Block Zuordnungsstatus	CMN	Standardmäßig wird ein Alarm ausgelöst, wenn Objektbezeichner nicht zugewiesen werden können, da das ADC-Quorum nicht erreicht werden kann. Die Zuweisung von Identifier-Blöcken im CMN-Dienst erfordert ein Quorum (50 % + 1) der ADC-Dienste, dass sie online und verbunden sind. Wenn das Quorum nicht verfügbar ist, kann der CMN-Dienst erst dann neue Identifizierungsblöcke zuweisen, wenn das ADC-Quorum wiederhergestellt ist. Bei Verlust des ADC-Quorums entstehen im Allgemeinen keine unmittelbaren Auswirkungen auf das StorageGRID-System (Kunden können weiterhin Inhalte aufnehmen und abrufen), da die Lieferung von Identifikatoren innerhalb eines Monats an anderer Stelle im Grid zwischengespeichert wird. Wenn der Zustand jedoch fortgesetzt wird, kann das StorageGRID-System nicht mehr neue Inhalte aufnehmen. Wenn ein Alarm ausgelöst wird, untersuchen Sie den Grund für den Verlust von ADC-Quorum (z. B. ein Netzwerk- oder Speicherknoten-Ausfall) und ergreifen Sie Korrekturmaßnahmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
BRDT	Temperatur Im Computing-Controller-Chassis	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur des Compute-Controllers in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Prüfen Sie die Hardware-Komponenten und Umweltprobleme auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Ein Alarm wird ausgelöst, wenn die Servicezeit (Sekunden) erheblich von der Betriebssystemzeit abweicht. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Servicezeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
BTSE	Uhrstatus	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Ein Alarm wird ausgelöst, wenn die Servicezeit nicht mit der vom Betriebssystem erfassten Zeit synchronisiert wird. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Zeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CAHP	Java Heap-Nutzung In Prozent	DDS	Ein Alarm wird ausgelöst, wenn Java die Garbage-Sammlung nicht mit einer Rate durchführen kann, die genügend Heap-Speicherplatz für eine ordnungsgemäße Funktion des Systems zulässt. Ein Alarm kann einen Benutzer-Workload anzeigen, der die im System verfügbaren Ressourcen für den DDS-Metadatenspeicher überschreitet. Überprüfen Sie die ILM-Aktivität im Dashboard, oder wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**, und wählen Sie dann ***site*** > ***Grid Node*** > **DDS** > **Ressourcen** > **Übersicht** > **Main** aus. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CASA	Data Store-Status	DDS	Wenn der Cassandra-Metadatenspeicher nicht mehr verfügbar ist, wird ein Alarm ausgelöst. Den Status von Cassandra überprüfen: 1. Melden Sie sich beim Storage-Node als admin und an `su` Um das Root-Kennwort zu verwenden, das in der Datei Passwords.txt angegeben ist. 2. Geben Sie Ein: `service cassandra status` 3. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: `service cassandra restart` Dieser Alarm kann auch zeigen, dass der Metadatenspeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert. Weitere Informationen zur Fehlerbehebung im Alarm Services: Status - Cassandra (SVST) in "Behebung von Metadatenproblemen". Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
FALL	Datenspeicherstatus	DDS	Dieser Alarm wird während der Installation oder Erweiterung ausgelöst, um anzuzeigen, dass ein neuer Datenspeicher in das Raster eingespeist wird.
CCNA	Computing-Hardware	SSM	Dieser Alarm wird ausgelöst, wenn der Status der Hardware des Computing-Controllers in einer StorageGRID-Appliance zu beachten ist.

Codieren	Name	Service	Empfohlene Maßnahmen
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	DDS	Dieser Alarm wird ausgelöst, wenn der effektive Metadatenraum (Metadaten Effective Space, CEMS) 70 % voll (kleiner Alarm), 90 % voll (Hauptalarm) und 100 % voll (kritischer Alarm) erreicht. Wenn dieser Alarm den Schwellenwert von 90 % erreicht, wird im Grid Manager eine Warnung auf dem Dashboard angezeigt. Sie müssen eine Erweiterung durchführen, um neue Speicherknoten so schnell wie möglich hinzuzufügen. Siehe "Erweitern Sie ein Raster". Wenn dieser Alarm den Schwellenwert von 100 % erreicht, müssen Sie die Aufnahme von Objekten beenden und Speicherknoten sofort hinzufügen. Cassandra erfordert eine bestimmte Menge an Speicherplatz zur Durchführung wichtiger Vorgänge wie Data-Compaction und Reparatur. Diese Vorgänge sind betroffen, wenn Objekt-Metadaten mehr als 100 % des zulässigen Speicherplatzes beanspruchen. Unerwünschte Ergebnisse können auftreten. **Hinweis**: Wenden Sie sich an den technischen Support, wenn Sie keine Speicherknoten hinzufügen können. Nachdem neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht. Siehe auch Informationen zur Fehlerbehebung für die Warnmeldung zu niedrigem Metadaten-Speicher in "Behebung von Metadatenproblemen". Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CMNA	CMN-Status	CMN	Wenn der Wert von CMN Status Fehler ist, wählen Sie **SUPPORT** > **Tools** > **Grid Topology** und dann ***site*** > ***Grid Node*** > **CMN** > **Übersicht** > **Main** und **CMN** > **Alarme** > **Main** aus, um die Fehlerursache zu ermitteln und das Problem zu beheben. Ein Alarm wird ausgelöst, und der Wert von CMN Status ist kein Online CMN während einer Hardwareaktualisierung des primären Admin-Knotens, wenn die CMNS geschaltet werden (der Wert des alten CMN-Status ist Standby und das neue ist Online). Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CPRC	Verbleibende Kapazität	NMS	Ein Alarm wird ausgelöst, wenn die verbleibende Kapazität (Anzahl der verfügbaren Verbindungen, die für die NMS-Datenbank geöffnet werden können) unter den konfigurierten Alarmschwerwert fällt. Wenn ein Alarm ausgelöst wird, wenden Sie sich an den technischen Support.
CPSA	Compute Controller Netzteil A	SSM	Wenn ein Problem mit der Stromversorgung A im Rechencontroller eines StorageGRID-Geräts auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.
CPSB	Compute Controller Netzteil B	SSM	Bei einem StorageGRID-Gerät wird ein Alarm ausgelöst, wenn ein Problem mit der Stromversorgung B im Compute-Controller auftritt. Ersetzen Sie die Komponente bei Bedarf.
KFUT	CPU-Temperatur für Compute Controller	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur der CPU im Compute-Controller in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Wenn es sich bei dem Speicherknoten um eine StorageGRID-Appliance handelt, gibt das StorageGRID-System an, dass eine Warnung für den Controller erforderlich ist. Prüfen Sie die Probleme mit den Hardwarekomponenten und der Umgebung auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
DNST	DNS-Status	SSM	Nach Abschluss der Installation wird im SSM-Service ein DNST-Alarm ausgelöst. Nachdem der DNS konfiguriert wurde und die neuen Serverinformationen alle Grid-Knoten erreichen, wird der Alarm abgebrochen.
ECCD	Beschädigte Fragmente Erkannt	LDR	Ein Alarm wird ausgelöst, wenn der Hintergrundverifizierungsprozess ein beschädigtes Fragment entdeckt, das nach der Löschung codiert wurde. Wenn ein beschädigtes Fragment erkannt wird, wird versucht, das Fragment neu zu erstellen. Setzen Sie die beschädigten Fragmente zurück, und kopieren Sie verlorene Attribute auf Null, und überwachen Sie sie, um zu sehen, ob die Zählung wieder hoch geht. Wenn die Anzahl steigt, kann es ein Problem mit dem zugrunde liegenden Speicher des Storage-Node geben. Eine Kopie von löschercodierten Objektdaten gilt erst dann als fehlend, wenn die Anzahl der verlorenen oder beschädigten Fragmente gegen die Fehlertoleranz des Löschcodes verstößt. Daher ist es möglich, ein beschädigtes Fragment zu haben und das Objekt trotzdem abrufen zu können. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
ACST	Verifizierungsstatus	LDR	Dieser Alarm zeigt den aktuellen Status des Hintergrundverifizierungsprozesses für mit der Löschung codierte Objektdaten auf diesem Storage Node an. Bei der Hintergrundüberprüfung wird ein Großalarm ausgelöst.
FOPN	Dateibeschreibung Öffnen	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Das FOPN kann während der Spitzenaktivität groß werden. Wenn der Support in Phasen mit langsamer Aktivität nicht geschmälert wird, wenden Sie sich an den technischen Support.
HSTE	HTTP-Status	BLDR	Siehe Empfohlene Maßnahmen für HSTU.

Codieren	Name	Service	Empfohlene Maßnahmen
HSTU	HTTP-Status	BLDR	HSTE und HSTU beziehen sich auf HTTP für allen LDR-Datenverkehr, einschließlich S3, Swift und anderem internen StorageGRID-Datenverkehr. Ein Alarm zeigt an, dass eine der folgenden Situationen aufgetreten ist: • HTTP wurde manuell in den Offline-Modus versetzt. • Das Attribut Auto-Start HTTP wurde deaktiviert. • Der LDR-Service wird heruntergefahren. Das Attribut Auto-Start HTTP ist standardmäßig aktiviert. Wenn diese Einstellung geändert wird, kann HTTP nach einem Neustart offline bleiben. Warten Sie gegebenenfalls, bis der LDR-Service neu gestartet wurde. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***Storage Node*** > **LDR** > **Konfiguration** aus. Wenn HTTP offline ist, stellen Sie es online. Vergewissern Sie sich, dass das Attribut Auto-Start HTTP aktiviert ist. Wenn HTTP offline bleibt, wenden Sie sich an den technischen Support.
HTAS	Automatisches Starten von HTTP	LDR	Gibt an, ob HTTP-Dienste beim Start automatisch gestartet werden sollen. Dies ist eine vom Benutzer angegebene Konfigurationsoption.
IRSU	Status Der Eingehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass die eingehende Replikation deaktiviert wurde. Konfigurationseinstellungen bestätigen: Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** > **Main** aus.

Codieren	Name	Service	Empfohlene Maßnahmen
LATA	Durchschnittliche Latenz	NMS	Überprüfen Sie auf Verbindungsprobleme. Überprüfen Sie die Systemaktivität, um zu bestätigen, dass die Systemaktivität erhöht wird. Eine Erhöhung der Systemaktivität führt zu einer Erhöhung der Attributdatenaktivität. Diese erhöhte Aktivität führt zu einer Verzögerung bei der Verarbeitung von Attributdaten. Dies kann normale Systemaktivität sein und wird unterseiten. Auf mehrere Alarme prüfen. Eine Erhöhung der durchschnittlichen Latenzzeit kann durch eine übermäßige Anzahl von ausgelösten Alarmen angezeigt werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
LDRE	LDR-Status	LDR	Wenn der Wert für LDR-Status Standby lautet, setzen Sie die Überwachung der Situation fort, und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für den LDR-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
VERLOREN	Verlorene Objekte	DDS, LDR	Wird ausgelöst, wenn das StorageGRID System eine Kopie des angeforderten Objekts von einer beliebigen Stelle im System nicht abrufen kann. Bevor ein Alarm VERLOREN GEGANGENE (verlorene Objekte) ausgelöst wird, versucht das System, ein fehlendes Objekt von einem anderen Ort im System abzurufen und zu ersetzen. Verloren gegangene Objekte stellen einen Datenverlust dar. Das Attribut Lost Objects wird erhöht, wenn die Anzahl der Speicherorte eines Objekts auf Null fällt, ohne dass der DDS-Service den Inhalt absichtlich löscht, um der ILM-Richtlinie gerecht zu werden. Untersuchen SIE VERLORENE (VERLORENE Objekte) Alarme sofort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. "Fehlerbehebung bei verlorenen und fehlenden Objektdaten"

Codieren	Name	Service	Empfohlene Maßnahmen
MCEP	Ablauf Des Managementschnittstelle-Zertifikats	CMN	Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf die Managementoberfläche verwendet wird, kurz vor Ablauf steht. 1. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Sicherheit** > **Zertifikate**. 2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus. 3. "Laden Sie ein neues Zertifikat für die Managementoberfläche hoch."
MINQ	E-Mail-Benachrichtigungen in Warteschlange	NMS	Überprüfen Sie die Netzwerkverbindungen der Server, auf denen der NMS-Dienst und der externe Mail-Server gehostet werden. Bestätigen Sie außerdem, dass die Konfiguration des E-Mail-Servers korrekt ist. "E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)"
MIN	E-Mail-Benachrichtigungsstatus	BNMS	Ein kleiner Alarm wird ausgelöst, wenn der NMS-Dienst keine Verbindung zum Mail-Server herstellen kann. Überprüfen Sie die Netzwerkverbindungen der Server, auf denen der NMS-Dienst und der externe Mail-Server gehostet werden. Bestätigen Sie außerdem, dass die Konfiguration des E-Mail-Servers korrekt ist. "E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)"
MISS	Status der NMS-Schnittstellen-Engine	BNMS	Ein Alarm wird ausgelöst, wenn die NMS-Schnittstellen-Engine auf dem Admin-Knoten, der Schnittstelleninhalte erfasst und generiert, vom System getrennt wird. Überprüfen Sie Server Manager, ob die Server-individuelle Anwendung ausgefallen ist.
NANG	Einstellung Für Automatische Netzwerkaushandlung	SSM	Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen. Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.

Codieren	Name	Service	Empfohlene Maßnahmen
NDUP	Einstellungen Für Den Netzwerkduplex	SSM	Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen. Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.
NLNK	Network Link Detect	SSM	Überprüfen Sie die Netzwerkverbindungen am Port und am Switch. Überprüfen Sie die Netzwerk-Router-, Switch- und Adapterkonfigurationen. Starten Sie den Server neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
RER	Fehler Beim Empfang	SSM	Die folgenden Ursachen können für NRER-Alarme sein: • Fehler bei der Vorwärtskorrektur (FEC) stimmen nicht überein • Switch-Port und MTU-NIC stimmen nicht überein • Hohe Link-Fehlerraten • NIC-Klingelpuffer überlaufen Weitere Informationen zur Fehlerbehebung im NRER-Alarm (Network Receive Error) in finden Sie unter "Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen".
NRLY	Verfügbare Audit-Relais	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Überwachungsrelais nicht mit ADC-Diensten verbunden sind, können keine Überwachungsereignisse gemeldet werden. Sie werden in eine Warteschlange eingereiht und stehen Benutzern nicht zur Verfügung, bis die Verbindung wiederhergestellt ist. Stellen Sie die Verbindung so schnell wie möglich zu einem ADC-Dienst wieder her. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NSCA	NMS-Status	NMS	Wenn der Wert des NMS-Status DB-Verbindungsfehler ist, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
NSCE	Bundesland des NMS	NMS	Wenn der Wert für den NMS-Status Standby lautet, setzen Sie die Überwachung fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für NMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NSPD	Schnell	SSM	Dies kann durch Probleme mit der Netzwerkverbindung oder der Treiberkompatibilität verursacht werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NTBR	Freie Tablespace	NMS	Wenn ein Alarm ausgelöst wird, überprüfen Sie, wie schnell sich die Datenbanknutzung geändert hat. Ein plötzlicher Abfall (im Gegensatz zu einer allmählichen Änderung im Laufe der Zeit) weist auf eine Fehlerbedingung hin. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. Durch das Anpassen des Alarmschwellenwerts können Sie proaktiv verwalten, wenn zusätzlicher Storage zugewiesen werden muss. Wenn der verfügbare Speicherplatz einen niedrigen Schwellenwert erreicht (siehe Alarmschwelle), wenden Sie sich an den technischen Support, um die Datenbankzuweisung zu ändern.
NTER	Übertragungsfehler	SSM	Diese Fehler können beseitigt werden, ohne manuell zurückgesetzt zu werden. Wenn sie nicht gelöscht werden, überprüfen Sie die Netzwerkhardware. Überprüfen Sie, ob die Adapterhardware und der Treiber korrekt installiert und konfiguriert sind, um mit Ihren Netzwerk-Routern und Switches zu arbeiten. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **SSM** > **Ressourcen** > **Konfiguration** > **Main**, wählen Sie **Zurücksetzen Fehleranzahl für Übertragung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
NTFQ	NTP-Frequenzverschiebung	SSM	Wenn der Frequenzversatz den konfigurierten Schwellenwert überschreitet, tritt wahrscheinlich ein Hardwareproblem mit der lokalen Uhr auf. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um einen Austausch zu vereinbaren.
NTLK	NTP Lock	SSM	Wenn der NTP-Daemon nicht an eine externe Zeitquelle gebunden ist, überprüfen Sie die Netzwerkverbindung zu den angegebenen externen Zeitquellen, deren Verfügbarkeit und deren Stabilität.
NTOF	NTP-Zeitverschiebung	SSM	Wenn der Zeitversatz den konfigurierten Schwellenwert überschreitet, liegt wahrscheinlich ein Hardwareproblem mit dem Oszillator der lokalen Uhr vor. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um einen Austausch zu vereinbaren.
NTSJ	Gewählte Zeitquelle Jitter	SSM	Dieser Wert gibt die Zuverlässigkeit und Stabilität der Zeitquelle an, die NTP auf dem lokalen Server als Referenz verwendet. Wenn ein Alarm ausgelöst wird, kann es ein Hinweis sein, dass der Oszillator der Zeitquelle defekt ist oder dass ein Problem mit der WAN-Verbindung zur Zeitquelle besteht.
NTSU	NTP-Status	SSM	Wenn der Wert von NTP Status nicht ausgeführt wird, wenden Sie sich an den technischen Support.
OPST	Gesamtstromstatus	SSM	Wenn die Stromversorgung eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Überprüfen Sie den Status von Netzteil A oder B, um festzustellen, welches Netzteil normal funktioniert. Falls erforderlich, ersetzen Sie das Netzteil.

Codieren	Name	Service	Empfohlene Maßnahmen
OQRT	Objekte Isoliert	LDR	Nachdem die Objekte automatisch vom StorageGRID-System wiederhergestellt wurden, können die isolierten Objekte aus dem Quarantäneverzeichnis entfernt werden. 1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. 2. Wählen Sie **Standort** > **Storage Node** > **LDR** > **Verifizierung** > **Konfiguration** > **Main**. 3. Wählen Sie **Gesperrte Objekte Löschen**. 4. Klicken Sie Auf **Änderungen Übernehmen**. Die isolierten Objekte werden entfernt und die Zählung wird auf Null zurückgesetzt.
ORSU	Status Der Ausgehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass eine ausgehende Replikation nicht möglich ist: Der Speicher befindet sich in einem Zustand, in dem Objekte nicht abgerufen werden können. Ein Alarm wird ausgelöst, wenn die ausgehende Replikation manuell deaktiviert wird. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** aus. Wenn der LDR-Dienst nicht zur Replikation verfügbar ist, wird ein Alarm ausgelöst. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** aus.
OSLF	Shelf-Status	SSM	Ein Alarm wird ausgelöst, wenn der Status einer der Komponenten im Speicher-Shelf einer Speichereinrichtung beeinträchtigt ist. Zu den Komponenten des Lagerregals gehören die IOMs, Lüfter, Netzteile und Laufwerksfächer.Wenn dieser Alarm ausgelöst wird, lesen Sie die Wartungsanleitung für Ihr Gerät.

Codieren	Name	Service	Empfohlene Maßnahmen
PMEM	Speicherauslastung Des Service (In Prozent)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Kann einen Wert von mehr als Y% RAM haben, wobei Y den Prozentsatz des Speichers repräsentiert, der vom Server verwendet wird. Zahlen unter 80 % sind normal. Über 90 % wird als Problem betrachtet. Wenn die Speicherauslastung für einen einzelnen Dienst hoch ist, überwachen Sie die Situation und untersuchen Sie sie. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
PSAS	Stromversorgung A-Status	SSM	Wenn die Stromversorgung A in einem StorageGRID-Gerät von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Ersetzen Sie bei Bedarf das Netzteil A.
PSBS	Netzteil B Status	SSM	Wenn die Stromversorgung B eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Falls erforderlich, ersetzen Sie das Netzteil B.
RDTE	Status Von Tivoli Storage Manager	BARC	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Status von Tivoli Storage Manager Offline lautet, überprüfen Sie den Status von Tivoli Storage Manager, und beheben Sie alle Probleme. Versetzen Sie die Komponente wieder in den Online-Modus. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Ziel** > **Konfiguration** > **Main**, wählen Sie **Tivoli Storage Manager State** > **Online** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
RDTU	Status Von Tivoli Storage Manager	BARC	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Tivoli Storage Manager Status auf Konfigurationsfehler gesetzt ist und der Archivknoten gerade dem StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass der TSM Middleware-Server richtig konfiguriert ist. Wenn der Wert des Tivoli Storage Manager-Status auf Verbindungsfehler oder Verbindungsfehler liegt, überprüfen Sie erneut die Netzwerkkonfiguration auf dem TSM Middleware-Server und die Netzwerkverbindung zwischen dem TSM Middleware-Server und dem StorageGRID-System. Wenn der Wert des Tivoli Storage Manager-Status Authentifizierungsfehler oder Authentifizierungsfehler beim erneuten Verbinden lautet, kann das StorageGRID-System eine Verbindung zum TSM-Middleware-Server herstellen, kann die Verbindung jedoch nicht authentifizieren. Überprüfen Sie, ob der TSM Middleware-Server mit dem richtigen Benutzer, Kennwort und Berechtigungen konfiguriert ist, und starten Sie den Service neu. Wenn der Wert des Tivoli Storage Manager Status als Sitzungsfehler lautet, ist eine etablierte Sitzung unerwartet verloren gegangen. Überprüfen Sie die Netzwerkverbindung zwischen dem TSM Middleware-Server und dem StorageGRID-System. Überprüfen Sie den Middleware-Server auf Fehler. Wenn der Wert von Tivoli Storage Manager Status Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
RIRF	Eingehende Replikationen — Fehlgeschlagen	BLDR, BARC	Eingehende Replikationen – fehlgeschlagener Alarm kann während Zeiten hoher Auslastung oder temporärer Netzwerkstörungen auftreten. Wenn die Systemaktivität verringert wird, sollte dieser Alarm gelöscht werden. Wenn die Anzahl der fehlgeschlagenen Replikationen weiter zunimmt, suchen Sie nach Netzwerkproblemen und überprüfen Sie, ob die LDR- und ARC-Quell- und Zieldienste online und verfügbar sind. Um die Zählung zurückzusetzen, wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** und dann ***site*** > ***Grid-Knoten*** > **LDR** > **Replikation** > **Konfiguration** > **Main**. Wählen Sie **Anzahl der fehlgeschlagene Inbound-Replikation zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
RIRQ	Eingehende Replikationen — In Warteschlange	BLDR, BARC	Alarme können in Zeiten hoher Auslastung oder temporärer Netzwerkstörungen auftreten. Wenn die Systemaktivität verringert wird, sollte dieser Alarm gelöscht werden. Wenn die Anzahl der Replikationen in der Warteschlange weiter steigt, suchen Sie nach Netzwerkproblemen und überprüfen Sie, ob die LDR- und ARC-Dienste von Quelle und Ziel online und verfügbar sind.
RORQ	Ausgehende Replikationen — In Warteschlange	BLDR, BARC	Die Warteschlange für ausgehende Replizierung enthält Objektdaten, die kopiert werden, um ILM-Regeln und von Clients angeforderte Objekte zu erfüllen. Ein Alarm kann aufgrund einer Systemüberlastung auftreten. Warten Sie, bis der Alarm gelöscht wird, wenn die Systemaktivität abnimmt. Wenn der Alarm erneut auftritt, fügen Sie die Kapazität durch Hinzufügen von Speicherknoten hinzu.
SAVP	Nutzbarer Speicherplatz (Prozent)	LDR	Wenn der nutzbare Speicherplatz einen niedrigen Schwellenwert erreicht, können Sie unter anderem das erweitern des StorageGRID-Systems oder das Verschieben von Objektdaten in die Archivierung über einen Archiv-Node einschließen.

Codieren	Name	Service	Empfohlene Maßnahmen
SCAS	Status	CMN	Wenn der Wert des Status für die aktive Grid-Aufgabe Fehler ist, suchen Sie die Grid-Task-Meldung. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **CMN** > **Grid Tasks** > **Übersicht** > **Main** aus. Die Grid-Task-Meldung zeigt Informationen über den Fehler an (z. B. „Check failed on Node 12130011“). Nachdem Sie das Problem untersucht und behoben haben, starten Sie die Grid-Aufgabe neu. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***Grid Node*** > **CMN** > **Grid Tasks** > **Konfiguration** > **Main** aus, und wählen Sie **Aktionen** > **Ausführen**. Wenn der Wert für Status für eine angespendete Grid-Aufgabe „Fehler“ lautet, versuchen Sie erneut, die Grid-Aufgabe zu beenden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SCEP	Ablaufdatum des Storage API-Service-Endpoints-Zertifikats	CMN	Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, kurz vor Ablauf steht. 1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**. 2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**. 3. "Laden Sie ein neues S3- und Swift-API-Zertifikat hoch."
SCHR	Status	CMN	Wenn der Wert von Status für die Aufgabe des historischen Rasters nicht belegt ist, untersuchen Sie den Grund und führen Sie die Aufgabe bei Bedarf erneut aus. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SCSA	Storage Controller A	SSM	Wenn in einer StorageGRID-Appliance ein Problem mit Storage Controller A auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
SCSB	Storage Controller B	SSM	Wenn ein Problem mit dem Storage Controller B in einer StorageGRID-Appliance auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf. Einige Appliance-Modelle besitzen keinen Storage Controller B.
SHLH.	Systemzustand	LDR	Wenn der Wert „Systemzustand“ für einen Objektspeicher „Fehler“ lautet, prüfen und korrigieren Sie Folgendes: • Probleme mit dem zu montiertem Volume • Fehler im Filesystem
SLSA	CPU-Auslastung durchschnittlich	SSM	Je höher der Wert des Busiers des Systems. Wenn der CPU-Lastdurchschnitt weiterhin mit einem hohen Wert besteht, sollte die Anzahl der Transaktionen im System untersucht werden, um zu ermitteln, ob dies zu diesem Zeitpunkt aufgrund einer hohen Last liegt. Ein Diagramm des CPU-Lastdurchschnitts anzeigen: Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***site*** > ***GRID Node*** > **SSM** > **Ressourcen** > **Berichte** > **Diagramme** aus. Wenn die Belastung des Systems nicht hoch ist und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SMST	Überwachungsstatus Protokollieren	SSM	Wenn der Wert des Protokollüberwachungsstatus für einen anhaltenden Zeitraum nicht verbunden ist, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SMTT	Ereignisse Insgesamt	SSM	Wenn der Wert von Total Events größer als Null ist, prüfen Sie, ob bekannte Ereignisse (z. B. Netzwerkfehler) die Ursache sein können. Wenn diese Fehler nicht gelöscht wurden (d. h., die Anzahl wurde auf 0 zurückgesetzt), können Alarme für Ereignisse insgesamt ausgelöst werden. Wenn ein Problem behoben ist, setzen Sie den Zähler zurück, um den Alarm zu löschen. Wählen Sie **NODES** > ***site*** > ***Grid Node*** > **Events** > **Ereignisanzahl zurücksetzen** aus. Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung zur Konfiguration der Grid-Topologie-Seite verfügen. Wenn der Wert für „Total Events“ null ist oder die Anzahl erhöht wird und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SNST	Status	CMN	Ein Alarm zeigt an, dass ein Problem beim Speichern der Grid-Task-Bundles vorliegt. Wenn der Wert von Status Checkpoint Error oder Quorum nicht erreicht ist, bestätigen Sie, dass ein Großteil der ADC-Dienste mit dem StorageGRID-System verbunden ist (50 Prozent plus einer) und warten Sie dann einige Minuten. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SOSS	Status Des Storage-Betriebssystems	SSM	Ein Alarm wird ausgelöst, wenn SANtricity OS darauf hinweist, dass ein Problem mit einer Komponente in einer StorageGRID-Appliance vorliegt. Wählen Sie **KNOTEN**. Wählen Sie dann **Appliance Storage Node** > **Hardware**. Blättern Sie nach unten, um den Status der einzelnen Komponenten anzuzeigen. Überprüfen Sie unter SANtricity OS die anderen Gerätekomponenten, um das Problem zu isolieren.

Codieren	Name	Service	Empfohlene Maßnahmen
SSMA	SSM-Status	SSM	Wenn der Wert des SSM Status Fehler ist, wählen Sie **SUPPORT** > **Tools** > **Grid Topology** und dann ***site*** > ***Grid Node*** > **SSM** > **Übersicht** > **Main** und **SSM** > **Übersicht** > **Alarme**, um die Ursache des Alarms zu bestimmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SSME	SSM-Status	SSM	Wenn der Wert des SSM-Status „Standby“ lautet, setzen Sie die Überwachung fort, und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert des SSM-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SSTS	Storage-Status	BLDR	Wenn der Wert des Speicherstatus nicht genügend verwendbarer Speicherplatz ist, ist auf dem Speicherknoten kein verfügbarer Speicherplatz mehr verfügbar. Die Datenausgabewerte werden auf andere verfügbare Speicherknoten umgeleitet. Abruf-Anfragen können weiterhin von diesem Grid-Node bereitgestellt werden. Zusätzlicher Speicher sollte hinzugefügt werden. Sie wirkt sich nicht auf die Funktionen des Endbenutzers aus, aber der Alarm bleibt bestehen, bis zusätzlicher Speicher hinzugefügt wird. Wenn der Wert für den Speicherstatus „Volume(s) nicht verfügbar“ ist, steht ein Teil des Speichers nicht zur Verfügung. Speicher und Abruf von diesen Volumes ist nicht möglich. Weitere Informationen erhalten Sie im Status des Volumes: Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** > **Übersicht** > **Main** aus. Die Gesundheit des Volumes ist unter Objektspeichern aufgeführt. Wenn der Wert des Speicherstatus Fehler ist, wenden Sie sich an den technischen Support. "Fehlersuche im SSTS-Alarm (Storage Status) durchführen"

Codieren	Name	Service	Empfohlene Maßnahmen
SVST	Status	SSM	Dieser Alarm wird gelöscht, wenn andere Alarme im Zusammenhang mit einem nicht laufenden Dienst gelöst werden. Verfolgen Sie die Alarme des Quelldienstes, um den Vorgang wiederherzustellen. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***GRID Node*** > **SSM** > **Services** > **Übersicht** > **Main** aus. Wenn der Status eines Dienstes als nicht ausgeführt angezeigt wird, ist sein Status „Administrativ ausgefallen“. Der Status des Dienstes kann aus folgenden Gründen als nicht ausgeführt angegeben werden: • Der Dienst wurde manuell beendet (`/etc/init.d/<service\> stop`). • Es liegt ein Problem mit der MySQL-Datenbank vor, und der Server Manager fährt den MI-Dienst herunter. • Ein Grid-Node wurde hinzugefügt, aber nicht gestartet. • Während der Installation ist ein Grid-Node noch nicht mit dem Admin-Node verbunden. Wenn ein Dienst als nicht ausgeführt aufgeführt ist, starten Sie den Dienst neu (`/etc/init.d/<service\> restart`). Dieser Alarm kann auch zeigen, dass der Metadatenspeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. "Fehlersuche im Alarm Services: Status - Cassandra (SVST) durchführen"
TMEM.	Installierter Speicher	SSM	Nodes, die mit weniger als 24 gib des installierten Speichers ausgeführt werden, können zu Performance-Problemen und Systeminstabilität führen. Die Menge des auf dem System installierten Arbeitsspeichers sollte auf mindestens 24 gib erhöht werden.

Codieren	Name	Service	Empfohlene Maßnahmen
POP	Ausstehende Vorgänge	ADU	Eine Meldungswarteschlange kann darauf hinweisen, dass der ADC-Dienst überlastet ist. Es können zu wenige ADC-Dienste an das StorageGRID-System angeschlossen werden. In einer großen Implementierung kann der ADC-Service Computing-Ressourcen hinzufügen oder das System benötigt zusätzliche ADC-Services.
UMEM	Verfügbarer Speicher	SSM	Wenn der verfügbare RAM knapp wird, prüfen Sie, ob es sich um ein Hardware- oder Softwareproblem handelt. Wenn es sich nicht um ein Hardwareproblem handelt oder wenn der verfügbare Speicher unter 50 MB liegt (der Standard-Alarmschwellenwert), wenden Sie sich an den technischen Support.
VMFI	Einträge Verfügbar	SSM	Dies deutet darauf hin, dass zusätzlicher Speicherplatz benötigt wird. Wenden Sie sich an den technischen Support.
VMFR	Speicherplatz Verfügbar	SSM	Wenn der Wert des verfügbaren Speicherplatzes zu niedrig wird (siehe Alarmschwellen), muss untersucht werden, ob sich die Log-Dateien aus dem Verhältnis heraus entwickeln oder Objekte, die zu viel Speicherplatz beanspruchen (siehe Alarmschwellen), die reduziert oder gelöscht werden müssen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
VMST	Status	SSM	Ein Alarm wird ausgelöst, wenn der Wert Status für das Bereitstellungsvolumen Unbekannt ist. Der Wert Unbekannt oder Offline kann darauf hinweisen, dass das Volume aufgrund eines Problems mit dem zugrunde liegenden Speichergerät nicht bereitgestellt oder darauf zugegriffen werden kann.
VPRI	Überprüfungspriorität	BLDR, BARC	Standardmäßig ist der Wert der Überprüfungspriorität adaptiv. Wenn die Überprüfungspriorität auf hoch eingestellt ist, wird ein Alarm ausgelöst, da die Speicherüberprüfung den normalen Betrieb des Dienstes verlangsamen kann.

Codieren	Name	Service	Empfohlene Maßnahmen
VSTU	Status Der Objektüberprüfung	BLDR	Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** > **Übersicht** > **Main** aus. Überprüfen Sie das Betriebssystem auf Anzeichen von Block- oder Dateisystemfehlern. Wenn der Wert des Objektverifizierungsstatus Unbekannter Fehler ist, weist er in der Regel auf ein niedriges Dateisystem- oder Hardwareproblem (I/O-Fehler) hin, das den Zugriff der Speicherverifizierung auf gespeicherte Inhalte verhindert. Wenden Sie sich an den technischen Support.
XAMS	Nicht Erreichbare Audit-Repositorys	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Überprüfen Sie die Netzwerkverbindung mit dem Server, der den Admin-Node hostet. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Referenz für Protokolldateien

Referenz für Protokolldateien: Übersicht

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"
- "Protokolle für Drittanbietersoftware"
- "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 Single-Log-Datei-Archiv. Wenn der primäre Admin-Node nicht verfügbar ist oder einen bestimmten Knoten nicht erreichen kann, können Sie für jeden Grid-Knoten wie folgt auf einzelne Protokolldateien zugreifen:

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

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)
cassandra	Cassandra Datenbankinformationen und Reaper Reparaturprotokolle.
eg	VCSs-Informationen über den aktuellen Knoten und EC-Gruppeninformationen nach Profil-ID.
Raster	Allgemeine Grid-Protokolle einschließlich Debug (`bycast.log`) Und `servermanager` Protokolle:
grid.xml	Die Grid-Konfigurationsdatei ist über alle Nodes hinweg freigegeben.
Hagroups	Hochverfügbarkeitsgruppen – Kennzahlen und Protokolle
Installieren	`Gdu-server` Und installieren Protokolle.
lumberjack.log	Debug-Meldungen im Zusammenhang mit Protokollerfassung.
Lambda-Schiedsrichter	Protokolle in Verbindung mit der S3 Select Proxy-Anforderung.
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.

Speicherort der Archivierung	Beschreibung
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.
Nginx-gw	Konfigurationsdateien und Protokolle für den Load Balancer und den Grid Federation
ntp	NTP-Konfigurationsdatei und -Protokolle
betriebssystem	Node- und Grid-Statusdatei, einschließlich Services `pid`.
Andere	Log-Dateien 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.
Floß	Protokolle aus dem in Plattformservices verwendeten Raft-Cluster.
ssh	Protokolle für SSH-Konfiguration und -Dienst.
snmp	SNMP-Agent-Konfiguration und Alarmzulassungs-/Deny-Listen, die für das Senden von SNMP-Benachrichtigungen verwendet werden.
Steckdosen-Daten	Sockendaten für Netzwerk-Debug.
system-commands.txt	Ausgabe von StorageGRID-Containerbefehlen. Enthält Systeminformationen wie z. B. Netzwerk- und Festplattenverwendung.

StorageGRID-Softwareprotokolle

Sie können StorageGRID-Protokolle verwenden, um Probleme zu beheben.

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

Allgemeine StorageGRID-Protokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/bycast.log	Die primäre StorageGRID-Fehlerbehebungsdatei. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes
/Var/local/log/bycast-err.log	Enthält eine Untergruppe von `bycast.log` (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes
/Var/local/Core/	Enthält alle Core Dump-Dateien, die erstellt wurden, wenn das Programm normal beendet wird. Mögliche Ursachen sind Assertion Failures, Verstöße oder Thread Timeouts. **Hinweis**: Die Datei `` `/var/local/core/kexec_cmd `` Ist normalerweise auf Appliance-Knoten vorhanden und weist keinen Fehler auf.	Alle Nodes

Verschlüsselungsbezogene Protokolle

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

Protokolle der Grid-Föderation

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

NMS-Protokolle

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

Server Manager-Protokolle

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

StorageGRID Serviceprotokolle

Dateiname	Hinweise	Gefunden am
/Var/local/log/acct.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/adc.errlog	Enthält den Standardfehlerstrom (Stderr) der entsprechenden Dienste. Pro Dienst gibt es eine Protokolldatei. Diese Dateien sind im Allgemeinen leer, es sei denn, es gibt Probleme mit dem Dienst.	Speicherknoten, auf denen der ADC-Service ausgeführt wird
/Var/local/log/ams.errlog		Admin-Nodes
/Var/local/log/Arc.errlog		Archiv-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

Dateiname	Hinweise	Gefunden am
/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/cts.errlog	Diese Protokolldatei wird nur erstellt, wenn der Zieltyp **Cloud Tiering - Simple Storage Service (S3) ist.**	Archiv-Nodes
/Var/local/log/dds.errlog		Storage-Nodes
/Var/local/log/dmv.errlog		Storage-Nodes
/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

Dateiname	Hinweise	Gefunden am
/Var/local/log/Lambda*	Enthält Protokolle für den S3 Select-Service.	Admin- und Gateway-Nodes Dieses Protokoll enthält nur bestimmte Admin- und Gateway-Knoten. Siehe "S3 Select Anforderungen und Einschränkungen für Admin und Gateway Nodes".
/Var/local/log/ldr.errlog		Storage-Nodes
/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.

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

Dateiname	Hinweise	Gefunden am
/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	Wurde während der Ausführung des erstellt `pa-move.sh` Skript:	Primärer Admin-Node
/Var/local/log/pa-move-new_pa.log	Wurde während der Ausführung des erstellt `pa-move.sh` Skript:	Primärer Admin-Node
/Var/local/log/pa-move-old_pa.log	Wurde während der Ausführung des erstellt `pa-move.sh` Skript:	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.	Primärer Admin-Node
/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

Protokolle für Drittanbietersoftware

Sie können die Softwareprotokolle von Drittanbietern verwenden, um Probleme zu beheben.

Kategorie	Dateiname	Hinweise	Gefunden am
Archivierung	/Var/local/log/dsierror.log	Fehlerinformationen für TSM Client APIs.	Archiv-Nodes
MySQL	/Var/local/log/mysql.err /Var/local/log/mysql-slow.log	Protokolldateien von MySQL erstellt. `mysql.err` Erfasst Datenbankfehler und Ereignisse wie Start-ups und Herunterfahren. `mysql-slow.log` (Das langsame Abfrageprotokoll) erfasst die SQL-Anweisungen, die mehr als 10 Sekunden in Anspruch genommen haben.	Admin-Nodes
Betriebssystem	/Var/local/log/messages	Dieses Verzeichnis enthält Protokolldateien für das Betriebssystem. Die in diesen Protokollen enthaltenen Fehler werden auch im Grid Manager angezeigt. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann **Topologie** > ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes
NTP	/Var/local/log/ntp.log /Var/lib/ntp/var/log/ntpstats/	`/var/local/log/ntp.log` Enthält die Protokolldatei für NTP-Fehlermeldungen. `/var/lib/ntp/var/log/ntpstats/` Verzeichnis enthält NTP-Zeitstatistiken. `loopstats` Statistikdaten für Datensätze-Loop-Filter. `peerstats` Zeichnet Informationen zu Peer-Statistiken auf.	Alle Nodes

Etwa bycast.log

Die Datei `/var/local/log/bycast.log` Ist die primäre Fehlerbehebungsdatei für die StorageGRID-Software. Es gibt ein `bycast.log` Datei für jeden Grid-Node. Die Datei enthält für diesen Grid-Node spezifische Meldungen.

Die Datei `/var/local/log/bycast-err.log` Ist eine Untergruppe von `bycast.log`. Er enthält Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“.

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. Siehe "Konfigurieren von Überwachungsmeldungen und Protokollzielen".

Dateirotation für bycast.log

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

Protokolldatei wird gestartet.

Die gespeicherte Datei wird umbenannt `bycast.log.1`, Und die neue Datei wird benannt `bycast.log`. Wenn das neue `bycast.log` Erreicht 1 GB, `bycast.log.1` Wird umbenannt und komprimiert zu werden `bycast.log.2.gz`, und `bycast.log` Wird umbenannt `bycast.log.1`.

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

Die Rotationsgrenze für `bycast-err.log` Sind 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 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. Siehe "Konfigurieren von Überwachungsmeldungen und Protokollzielen".

Verwandte Informationen

"Erfassen von Protokolldateien und Systemdaten"

Nachrichten in bycast.log

Nachrichten in `bycast.log` Geschrieben werden durch die ADE (Asynchronous Distributed Environment). 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
Knoten-ID	12455685
PROZESS-ID WIRD ADDIEREN	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHF
UTC-Systemzeit	2019-05-05T27T17:10:29.784677 (JJJJ-MM-DDTHH:MM:SS.UUUUUU)
Schweregrad	FEHLER

Nachrichtensegment	Wert im Beispiel
Interne Tracking-Nummer	0906
Nachricht	SVMR: Integritätsprüfung auf Volume 3 mit Grund 'AUSWEG' fehlgeschlagen

Nachrichten-Schweregrade in bycast.log

Die 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. Kritische Meldungen werden auch im Grid Manager angezeigt. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. Wählen Sie dann **Standort** > **Knoten** > **SSM** > **Events** aus.

Fehlercodes in `bycast.log`

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

In der folgenden Tabelle sind häufig nicht-numerische 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
ROVER	Version

Fehlercode	Bedeutung
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
015	ENOTBLK	Blockgerät erforderlich

Fehlernummer	Fehlercode	Bedeutung
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
037	ENOLCK	Keine Datensatzsperren verfügbar

Fehlernummer	Fehlercode	Bedeutung
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	Stufe 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		
059	EBFONT	Schlechtes Schriftdateiformat

Fehlernummer	Fehlercode	Bedeutung
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
080	ELIBBAD	Zugriff auf eine beschädigte, gemeinsam genutzte Bibliothek

Fehlernummer	Fehlercode	Bedeutung
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
100	ENETDOWN	Netzwerk ausgefallen

Fehlernummer	Fehlercode	Bedeutung
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
121	EREMOTEIO	Remote-I/O-Fehler

Fehlernummer	Fehlercode	Bedeutung
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 Überwachungsmeldungen und Protokollziele

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 eine vollständige Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers zu maximieren, werden bis zu 20 GB lokale Protokolle von Audit-Datensätzen verwendet (`localaudit.log`) Werden auf jedem Knoten gepflegt.

So konfigurieren Sie einen externen Syslog-Server

Informationen zum Konfigurieren eines externen Syslog-Servers finden Sie unter "Konfigurieren von Audit-Meldungen und externem 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. Die wichtigsten zusätzlichen Variablen sind für Audit-Protokolle der Prozentsatz der am häufigsten verwendeten S3-Vorgänge (im Vergleich zu RUFT) und die mittlere Größe der folgenden S3-Felder in Byte (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

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. Die wichtigsten zusätzlichen Variablen sind für Applikations-Protokolle die Datensicherungsstrategie (Replizierung vs Erasure Coding) – der Prozentsatz der S3-Operationen, die durchgeführt werden (im Vergleich zu Ruft/Other) und die durchschnittliche Größe der folgenden S3-Felder (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

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 von Audit-Meldungen und externem Syslog-Server

Sie können eine Reihe von Einstellungen für Überwachungsmeldungen konfigurieren. Sie können die Anzahl der aufgezeichneten Überwachungsmeldungen anpassen, HTTP-Anforderungsheader definieren, die Sie in die Audit-Nachrichten des Clients einbeziehen möchten, einen externen Syslog-Server konfigurieren und angeben, wo

Überwachungsprotokolle, Sicherheitsereignisprotokolle und StorageGRID-Softwareprotokolle gesendet werden.

Audit-Meldungen und -Protokolle zeichnen Systemaktivitäten und Sicherheitsereignisse auf und sind wichtige Tools für das Monitoring und die Fehlerbehebung. Alle StorageGRID Nodes generieren Audit-Meldungen und -Protokolle, um die Systemaktivität und -Ereignisse nachzuverfolgen.

Optional können Sie einen externen Syslog-Server konfigurieren, um Audit-Informationen Remote zu speichern. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Audit-Nachrichten auf die Performance minimiert, ohne dass die Vollständigkeit der Audit-Daten reduziert wird. 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. Siehe "Überlegungen für externen Syslog-Server" Entsprechende Details.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".
- Wenn Sie planen, einen externen Syslog-Server zu konfigurieren, haben Sie die geprüft "Überlegungen zur Verwendung eines externen Syslog-Servers" Und sichergestellt, dass der Server über genügend Kapazität verfügt, um die Protokolldateien zu empfangen und zu speichern.
- 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"

Diese Standardeinstellungen gelten, wenn Sie StorageGRID ursprünglich mit Version 10.3 oder höher installiert haben. Wenn Sie zunächst eine frühere Version von StorageGRID verwendet haben, wird der Standardwert für alle Kategorien auf Normal gesetzt.

Bei Upgrades sind Audit-Level-Konfigurationen nicht sofort wirksam.

Schritte

1. Wählen Sie **CONFIGURATION** > **Monitoring** > **Audit und Syslog-Server**.
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	Nur Fehlermeldungen sind protokollierte - Audit-Meldungen, für die der 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 für Ihre S3-Anwendungen keine detaillierte Aufzeichnung der Client-Leseoperationen benötigen, ändern Sie optional die Einstellung **Client-Lesevorgänge** auf **Fehler**, um die Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu verringern.

3. Wählen Sie **Speichern**.

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

Definieren Sie HTTP-Anforderungsheader

Sie können optional alle HTTP-Anforderungsheader definieren, die Sie in die Audit-Nachrichten des Clients aufnehmen möchten. Diese Protokoll-Header gelten nur für S3- und Swift-Anforderungen.

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.

> Header für Auditprotokoll-Anfragen werden nur protokolliert, wenn die Audit-Ebene für **Client** oder **Client-Schreibvorgänge** nicht **aus** ist.

3. Wählen Sie **Speichern**

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

Verwenden Sie einen externen syslog-Server

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 zu Wählen Sie Ziele für Audit-Informationen aus.

> Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können Sie zusätzliche Konfigurationsoptionen mithilfe des anwenden `audit-destinations` Endpunkte, die sich im Abschnitt „Private API“ der 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 Seite Audit- und Syslog-Server die Option **externen Syslog-Server konfigurieren** aus. Wenn Sie zuvor einen externen Syslog-Server konfiguriert haben, wählen Sie **externen Syslog-Server bearbeiten** aus.

   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
   - **Send Application logs**: Sendet Log-Dateien nützlich für die Fehlersuche einschließlich:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Nur Admin-Nodes)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter "StorageGRID-Softwareprotokolle".
2. Verwenden Sie die Dropdown-Menüs, um den Schweregrad und die Einrichtung (Meldungstyp) für jede zu sendende Kategorie von Audit-Informationen auszuwählen.

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

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

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

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

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

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

Anlage	Beschreibung

Passthrough	Jede Nachricht, die an das externe Syslog gesendet wird, hat denselben Einrichtungswert wie bei der lokalen Anmeldung am Knoten:
	• Für Audit-Protokolle lautet die an den externen Syslog-Server gesendete Einrichtung „local7“.
	• Bei Sicherheitsereignissen werden die Einrichtungswerte von der linux-Distribution auf den Knoten generiert.
	• Für Anwendungsprotokolle weisen die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Einrichtungswerte auf:
	  ◦ `bycast.log`: Benutzer oder Daemon
	  ◦ `bycast-err.log`: Benutzer, Daemon, local3 oder local4
	  ◦ `jaeger.log`: Local2
	  ◦ `nms.log`: Local3
	  ◦ `prometheus.log`: Local4
	  ◦ `raft.log`: Local5
	  ◦ `hagroups.log`: Local6

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)
11	FTP

Anlage	Beschreibung
12	NTP
13	Logaudit (Protokollaudit)
14	Logalert (Protokollwarnung)
15	Uhr (Uhrzeitdaemon)
16	Local0
17	gebietsschema 1
18	local2
19	Lokalisierung 3
20	local4
21	Lokalisierung 5
22	Lokalisierung 6
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**.

   Siehe "Fehlerbehebung für einen externen Syslog-Server" Um Ihnen bei der Behebung von Fehlern zu helfen.

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 Log-Collection-Infrastruktur. Das UDP-Protokoll ermöglicht keine so strenge Fehlererkennung wie das andere 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-Audit-Informationen werden erst dann an den externen Syslog-Server gesendet, wenn Sie ein Ziel auswählen, das den externen Syslog-Server enthält.

Wählen Sie Ziele für Audit-Informationen aus

Sie können festlegen, wo Audit-Protokolle, Sicherheitsereignisprotokolle und "StorageGRID-Softwareprotokolle" 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 auf der Seite Audit and syslog Server das Ziel für Audit-Informationen aus.

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

Option	Beschreibung
Nur lokale Knoten (Standard)	Überwachungsmeldungen, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden nicht an Admin-Nodes gesendet. Stattdessen werden sie nur auf den Knoten gespeichert, die sie generiert haben („der lokale Knoten“). Die auf jedem lokalen Knoten generierten Audit-Informationen werden in gespeichert `/var/local/log/localaudit.log`. **Hinweis**: StorageGRID entfernt periodisch 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 beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Auf jedem Node werden durchschnittlich etwa 20 GB an Protokolldaten gespeichert.
Admin-Nodes/lokale Nodes	Audit-Meldungen werden an das Überwachungsprotokoll auf Admin-Nodes gesendet, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden auf den Knoten gespeichert, die sie generiert haben. Die Audit-Informationen werden in folgenden Dateien gespeichert: • Admin-Nodes (primär und nicht primär): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Datei ist normalerweise leer oder fehlt. Sie kann sekundäre Informationen enthalten, z. B. eine zusätzliche Kopie einiger Nachrichten.
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf den lokalen Knoten gespeichert (`/var/local/log/localaudit.log`). Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Node 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 ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.

2. Wählen Sie **Speichern**.

   Es wird eine Warnmeldung angezeigt.

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

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

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

Verwenden Sie SNMP-Überwachung

Verwenden Sie SNMP-Überwachung: Übersicht

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 Alarme und Alarme. 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.

> Siehe "Zugriff auf MIB-Dateien" Wenn 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 den Alarm. Warnmeldungen werden vom 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 Warnmeldungen, mit denen diese Traps ausgelöst werden können, finden Sie im "Alerts Referenz".

- Sicher "Alarme (Altsystem)" Werden bei einem bestimmten oder höheren Schweregrad ausgelöst.

> SNMP-Benachrichtigungen werden nicht für jeden Alarm oder für jeden Schweregrad des Alarms gesendet.

Unterstützung von SNMP-Versionen

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

	SNMPv1	SNMPv2c	SNMPv3
Abfragen (GET und GETNEXT)	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen (TRAP und INFORM)	Nur Traps	Traps und informiert	Traps und informiert
Benachrichtigungsauthentifizierung	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	USM-Benutzer für jedes Trap-Ziel

Einschränkungen

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

Konfigurieren Sie den SNMP-Agent

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Alle Knoten im Grid verwenden dieselbe SNMP-Konfiguration.

Geben Sie die Grundkonfiguration an

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

Schritte

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

   Die Seite SNMP Agent wird angezeigt.

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

Feld	Beschreibung
Systemkontakt	Optional Der primäre Kontakt für das StorageGRID-System, der in SNMP-Nachrichten als sysContact zurückgegeben wird. Der Systemkontakt ist normalerweise eine E-Mail-Adresse. Dieser Wert gilt für alle Knoten im StorageGRID-System. **Systemkontakt** kann maximal 255 Zeichen lang sein.
Standort des Systems	Optional Der Speicherort des StorageGRID-Systems, der in SNMP-Nachrichten als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information sein, die hilfreich ist, um zu ermitteln, wo sich das StorageGRID System befindet. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Dieser Wert gilt für alle Knoten im StorageGRID-System. **Systemstandort** kann maximal 255 Zeichen lang sein.
Aktivieren Sie SNMP-Agentenbenachrichtigungen	• Wenn diese Option ausgewählt ist, sendet der StorageGRID-SNMP-Agent Trap- und Inform-Benachrichtigungen. • Wenn diese Option nicht ausgewählt ist, unterstützt der SNMP-Agent schreibgeschützten MIB-Zugriff, sendet jedoch keine SNMP-Benachrichtigungen.

Feld	Beschreibung
Aktivieren Sie Authentifizierungs-Traps	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er falsch authentifizierte Protokollmeldungen empfängt.

Geben Sie Community-Strings ein

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

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

Schritte

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

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

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

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

   Es sind bis zu fünf Zeichenfolgen zulässig.

Trap-Ziele erstellen

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

Schritte

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

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

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

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

SNMPv1

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

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

SNMPv2c

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

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

SNMPv3

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

Feld	Beschreibung
Typ	Gibt an, ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfangen des Traps.
Port	Verwenden Sie 162, den Standardport für SNMP-Traps, es sei denn, Sie müssen einen anderen Wert verwenden.
Protokoll	Verwenden Sie UDP, das das Standard-SNMP-Trap-Protokoll ist, es sei denn, Sie müssen TCP verwenden.
USM-Benutzer	Der USM-Benutzer, der für die Authentifizierung verwendet wird. • Wenn Sie **Trap** ausgewählt haben, werden nur USM-Benutzer ohne maßgebliche Engine-IDs angezeigt. • Wenn Sie **Inform** ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt. • Wenn keine Benutzer angezeigt werden: i. Erstellen und speichern Sie das Trap-Ziel. ii. Gehen Sie zu USM-Benutzer erstellen Und erstellen Sie den Benutzer. iii. Kehren Sie zur Registerkarte Trap-Ziele zurück, wählen Sie das gespeicherte Ziel aus der Tabelle aus und wählen Sie **Bearbeiten**. iv. Wählen Sie den Benutzer aus.

5. Wählen Sie **Erstellen**.

   Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

Erstellen Sie Agentenadressen

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

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

Schritte

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

Feld	Beschreibung
Internetprotokoll	Gibt an, ob diese Adresse IPv4 oder IPv6 verwendet. Standardmäßig verwendet SNMP IPv4.
Transportprotokoll	Ob diese Adresse UDP oder TCP verwendet. Standardmäßig verwendet SNMP UDP.
StorageGRID-Netzwerk	Welches StorageGRID-Netzwerk der Agent abhört. • Grid-, Admin- und Client-Netzwerke: Der SNMP-Agent hört auf Abfragen in allen drei Netzwerken. • Grid-Netzwerk • Admin-Netzwerk • Client-Netzwerk **Hinweis**: Wenn Sie das Client-Netzwerk für unsichere Daten verwenden und eine Agentenadresse für das Client-Netzwerk erstellen, beachten Sie, dass der SNMP-Datenverkehr ebenfalls unsicher ist.
Port	Optional die Portnummer, die der SNMP-Agent abhören soll. Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben. **Hinweis**: Wenn Sie den SNMP-Agent speichern, öffnet StorageGRID automatisch die Agentenadressen-Ports auf der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

3. Wählen Sie **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

Erstellen Sie USM-Benutzer

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

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

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

Schritte

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

Feld	Beschreibung
Benutzername	Ein eindeutiger Name für diesen USM-Benutzer. Benutzernamen dürfen maximal 32 Zeichen enthalten und dürfen keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht mehr geändert werden.
Schreibgeschützter MIB-Zugriff	Wenn diese Option ausgewählt ist, sollte dieser Benutzer Lesezugriff auf die MIB haben.
Maßgeblicher Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, ist die ID der autorisierenden Engine für diesen Benutzer. Geben Sie 10 bis 64 Hex-Zeichen (5 bis 32 Byte) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in Trap-Zielen für Informationen ausgewählt werden. Dieser Wert ist für USM-Benutzer, die in Trap-Zielen für Traps ausgewählt werden, nicht zulässig. **Hinweis**: Dieses Feld wird nicht angezeigt, wenn Sie **schreibgeschützter MIB-Zugriff** ausgewählt haben, da USM-Benutzer, die schreibgeschützten MIB-Zugriff haben, keine Engine-IDs haben können.
Sicherheitsstufe	Die Sicherheitsstufe für den USM-Benutzer: • **AuthPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort sowie ein Datenschutzprotokoll und ein Passwort angeben. • **AuthNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort angeben.
Authentifizierungsprotokoll	Stellen Sie immer SHA ein, welches das einzige unterstützte Protokoll ist (HMAC-SHA-96).
Passwort	Das Kennwort, das dieser Benutzer zur Authentifizierung verwendet.
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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

Siehe "Konfigurieren Sie den SNMP-Agent" Für Details zu den einzelnen Feldern 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).

Einzelheiten dazu, was Sie eingeben müssen, 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.

   Einzelheiten dazu, was Sie eingeben müssen, 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.

   Einzelheiten dazu, was Sie eingeben müssen, 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.

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

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)

   a. Grep für die StorageGRID-OID in der gesamten Struktur (mit `paste` Verbinden von Zeilen):

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

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

MIB-Dateiinhalte

Alle Objekte befinden sich unter der StorageGRID-OID.

Objektname	Objekt-ID (OID)	Beschreibung
iso.org.dod.internet. Private.Unternehmen. netapp.storagegrid		Das MIB-Modul für NetApp StorageGRID-Einheiten.

MIB-Objekte

Objektname	Objekt-ID (OID)	Beschreibung
ActiveAlertCount	**1.3.6.1.4.1.** 789.28669.1.3	Die Anzahl der aktiven Warnungen in der activeAlertTable.
ActiveAlertTable	**1.3.6.1.4.1.** 789.28669.1.4	Eine Tabelle mit aktiven Warnmeldungen in StorageGRID.
ActiveAlertId	**1.3.6.1.4.1.** 789.28669.1.4.1.1	Die ID der Warnmeldung. Nur im aktuellen Satz aktiver Warnungen eindeutig.
ActiveAlertName	**1.3.6.1.4.1.** 789.28669.1.4.1.2	Der Name der Warnmeldung.
ActiveAlertInstance	**1.3.6.1.4.1.** 789.28669.1.4.1.3	Der Name der Entität, die die Warnmeldung generiert hat, normalerweise der Knotenname.
ActiveAlertSchweregrad	**1.3.6.1.4.1.** 789.28669.1.4.1.4	Der Schweregrad der Meldung.
ActiveAlertStartTime	**1.3.6.1.4.1.** 789.28669.1.4.1.5	Das Datum und die Uhrzeit, zu der die Warnmeldung ausgelöst wurde.

Benachrichtigungstypen (Traps)

Alle Benachrichtigungen enthalten die folgenden Variablen als varbindes:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSchweregrad
- ActiveAlertStartTime

Benachrichtigungstyp	Objekt-ID (OID)	Beschreibung
ActiveMinorAlert	**1.3.6.1.4.1.** 789.28669.0.6	Ein Alarm mit geringem Schweregrad
ActiveMajorAlert	**1.3.6.1.4.1.** 789.28669.0.7	Ein Alarm mit dem Hauptschweregrad
ActiveCriticalAlert	**1.3.6.1.4.1.** 789.28669.0.8	Eine Meldung mit dem Schweregrad „kritisch“

Erfassung zusätzlicher StorageGRID-Daten

Verwenden Sie Diagramme und Diagramme

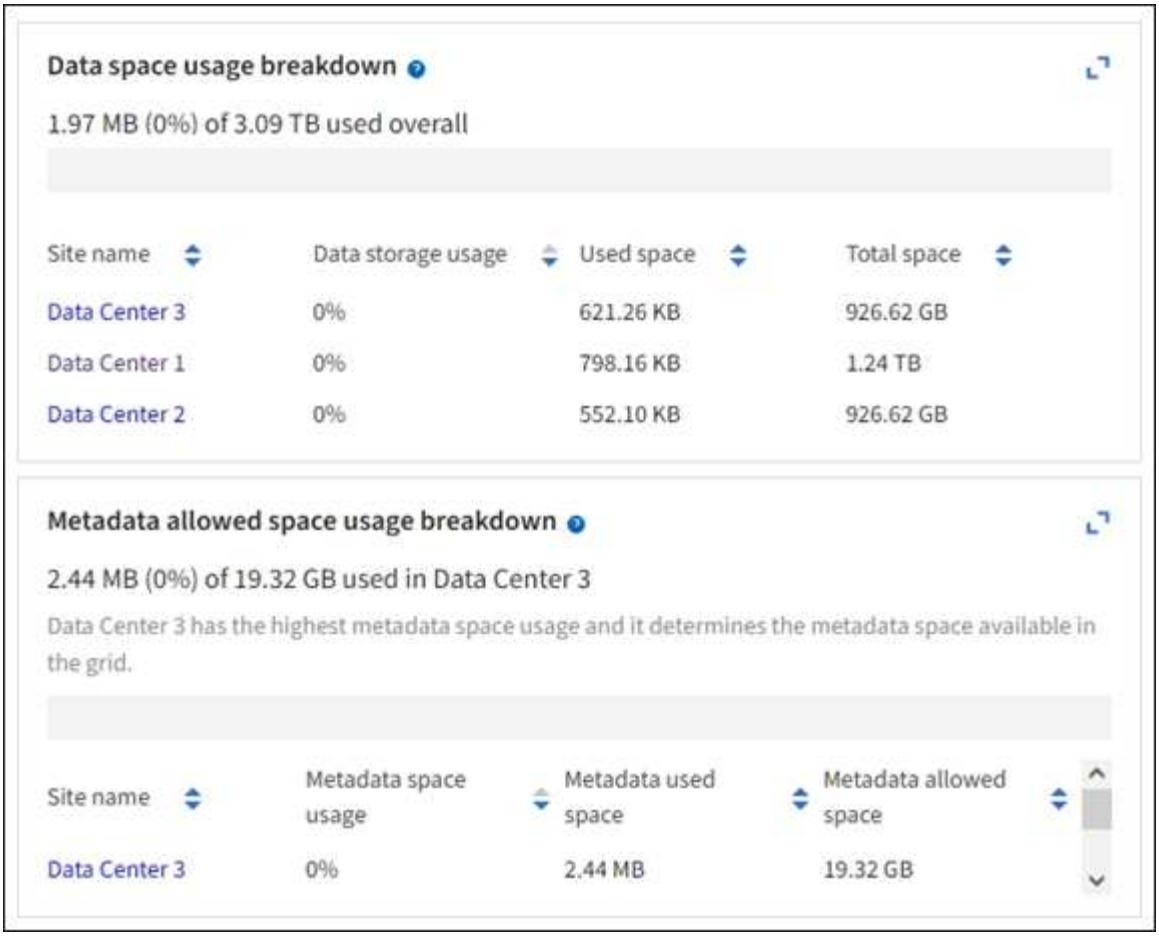
Mithilfe von Diagrammen und Berichten lässt sich der Zustand des StorageGRID Systems überwachen und Probleme beheben.

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

Diagrammtypen

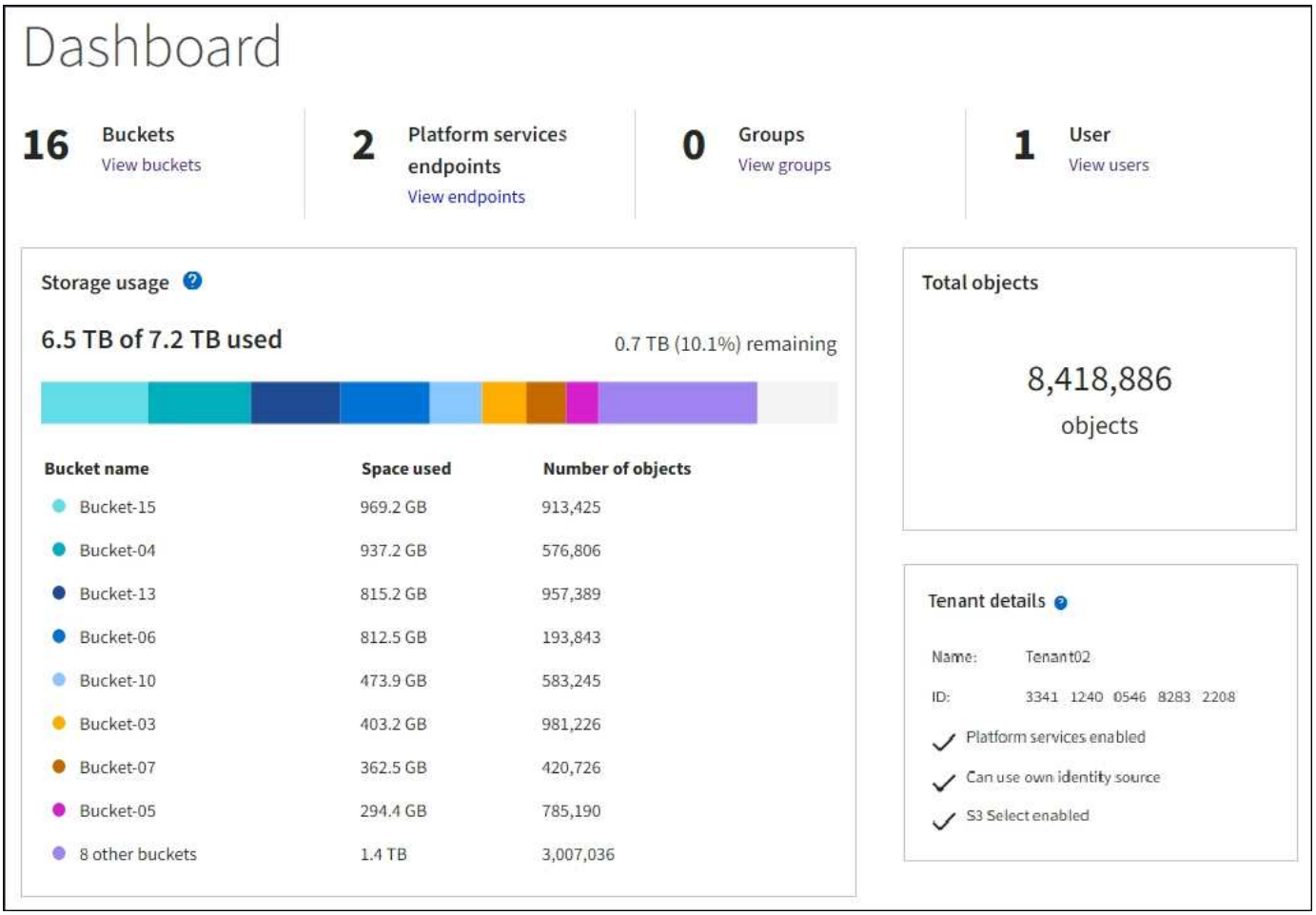
Diagramme und Diagramme fassen die Werte bestimmter StorageGRID-Metriken und -Attribute zusammen.

Das Grid Manager-Dashboard enthält Karten, die den verfügbaren Speicher für das Grid und jeden Standort zusammenfassen.



Im Fenster Storage Usage im Tenant Manager-Dashboard werden folgende Informationen angezeigt:

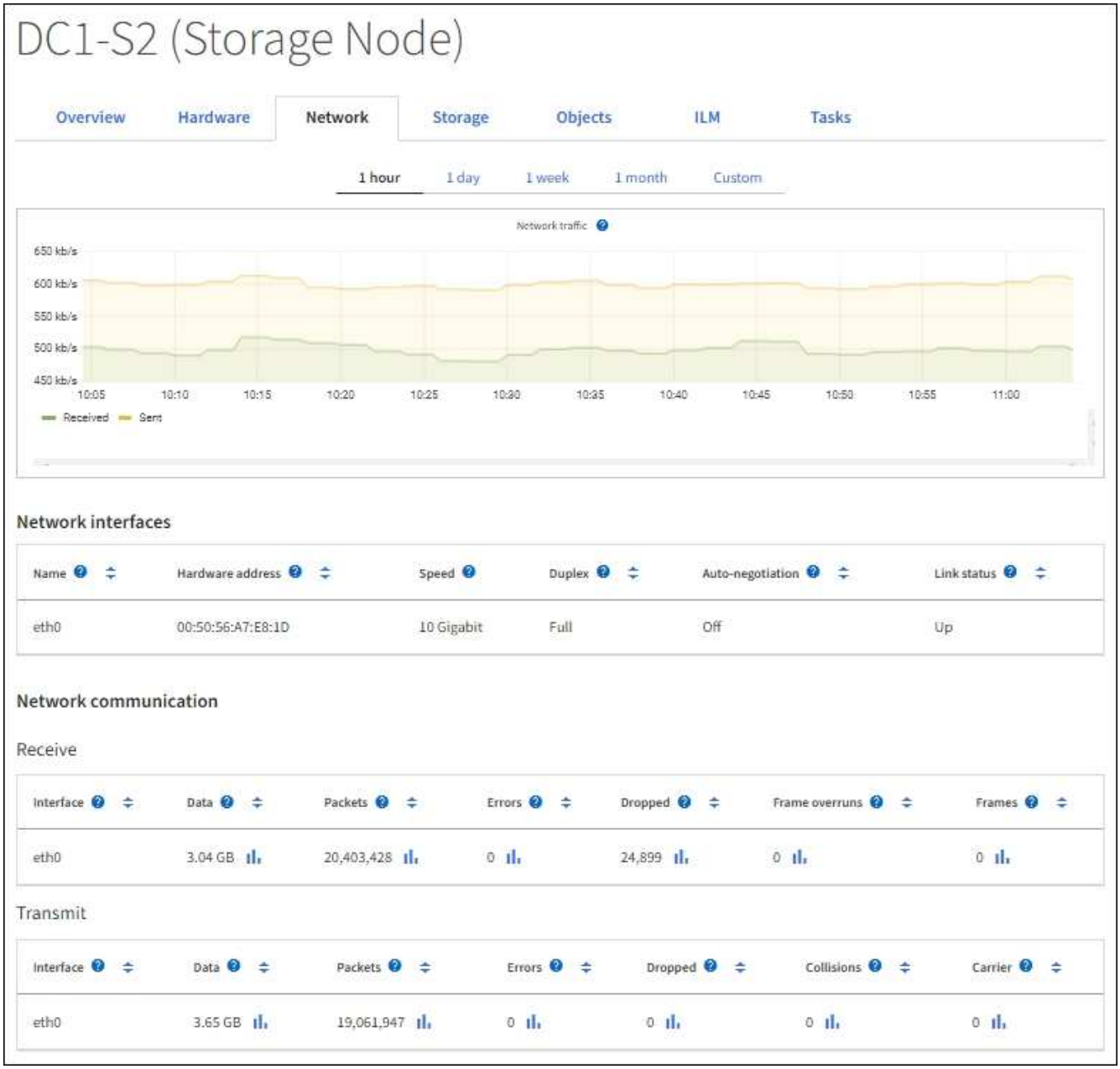
- Eine Liste der größten Buckets (S3) oder Container (Swift) für die Mandanten
- Ein Balkendiagramm, das die relative Größe der größten Buckets oder Container darstellt
- Der insgesamt verwendete Speicherplatz und, wenn ein Kontingent festgelegt ist, die Menge und der Prozentsatz des verbleibenden Speicherplatzes



Darüber hinaus stehen Diagramme zur Verfügung, die zeigen, wie sich StorageGRID-Metriken und -Attribute im Laufe der Zeit ändern, auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG** > **Tools** > **Grid-Topologie**.

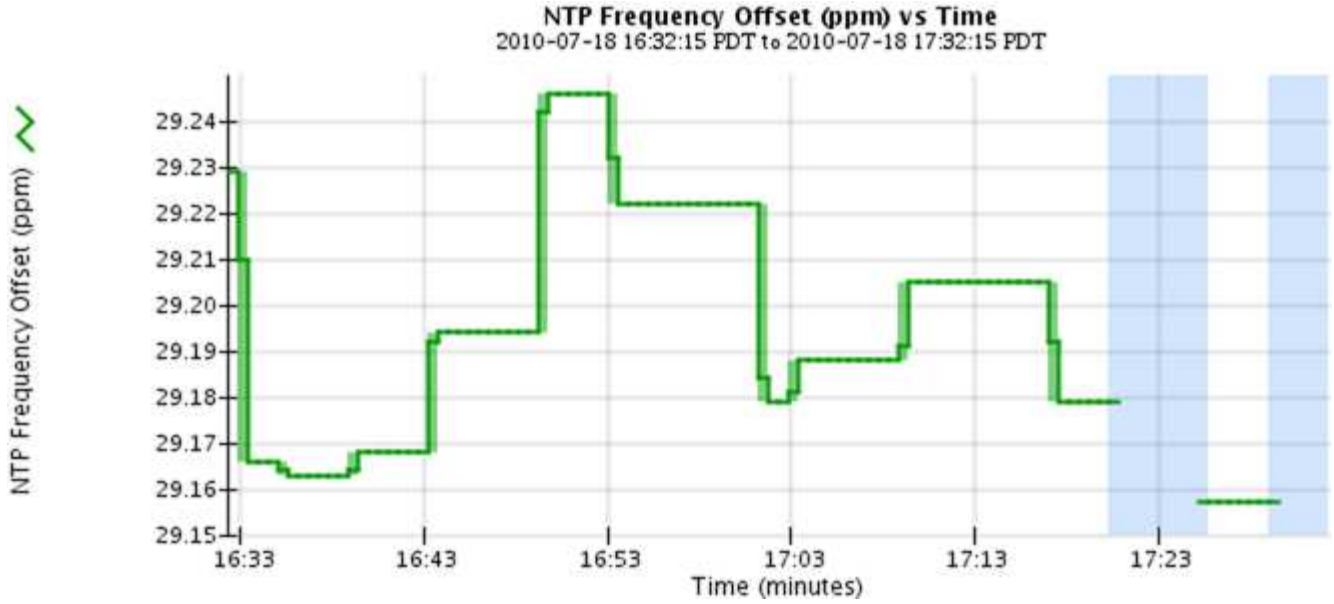
Es gibt vier Arten von Diagrammen:

- **Grafana-Diagramme**: Auf der Seite Knoten werden Grafana-Diagramme verwendet, um die Werte der Prometheus-Kennzahlen im Laufe der Zeit zu zeichnen. Die Registerkarte **NODES** > **Netzwerk** für einen Storage Node enthält beispielsweise ein Grafana-Diagramm für den Netzwerk-Traffic.

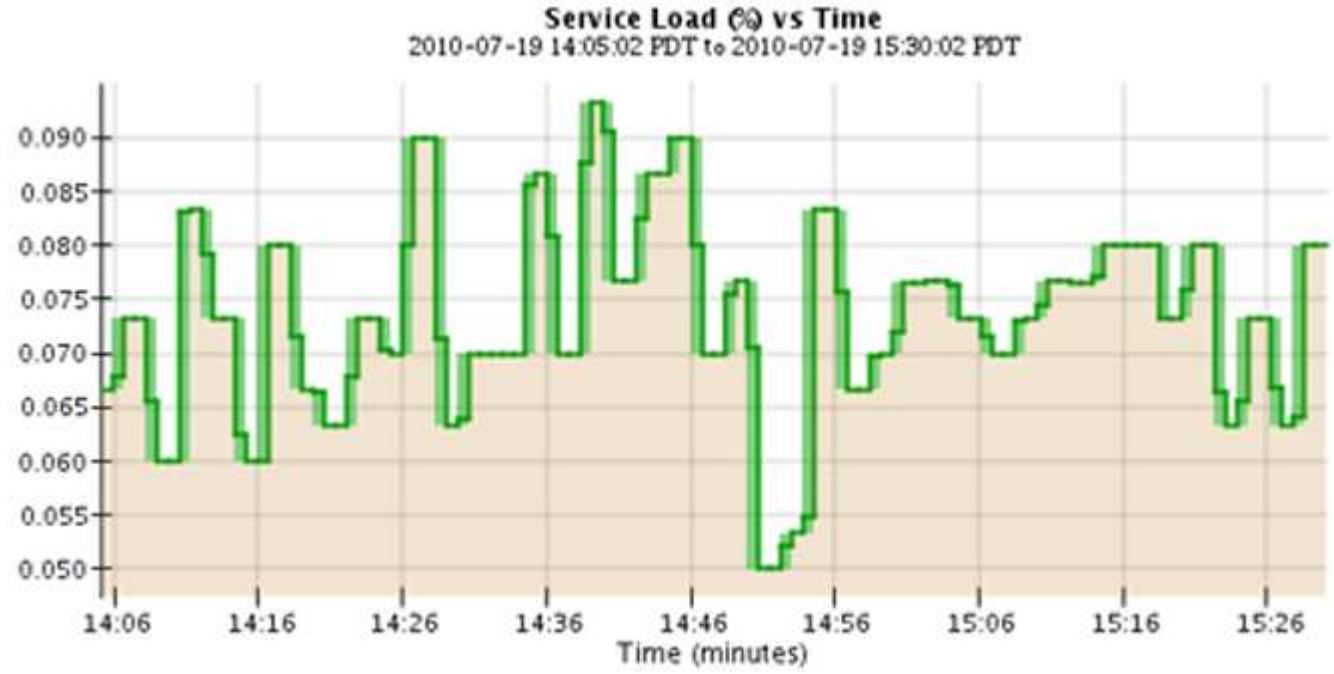


Grafana-Diagramme sind auch auf den vorkonfigurierten Dashboards enthalten, die auf der Seite **UNTERSTÜTZUNG** > **Tools** > **Metriken** verfügbar sind.

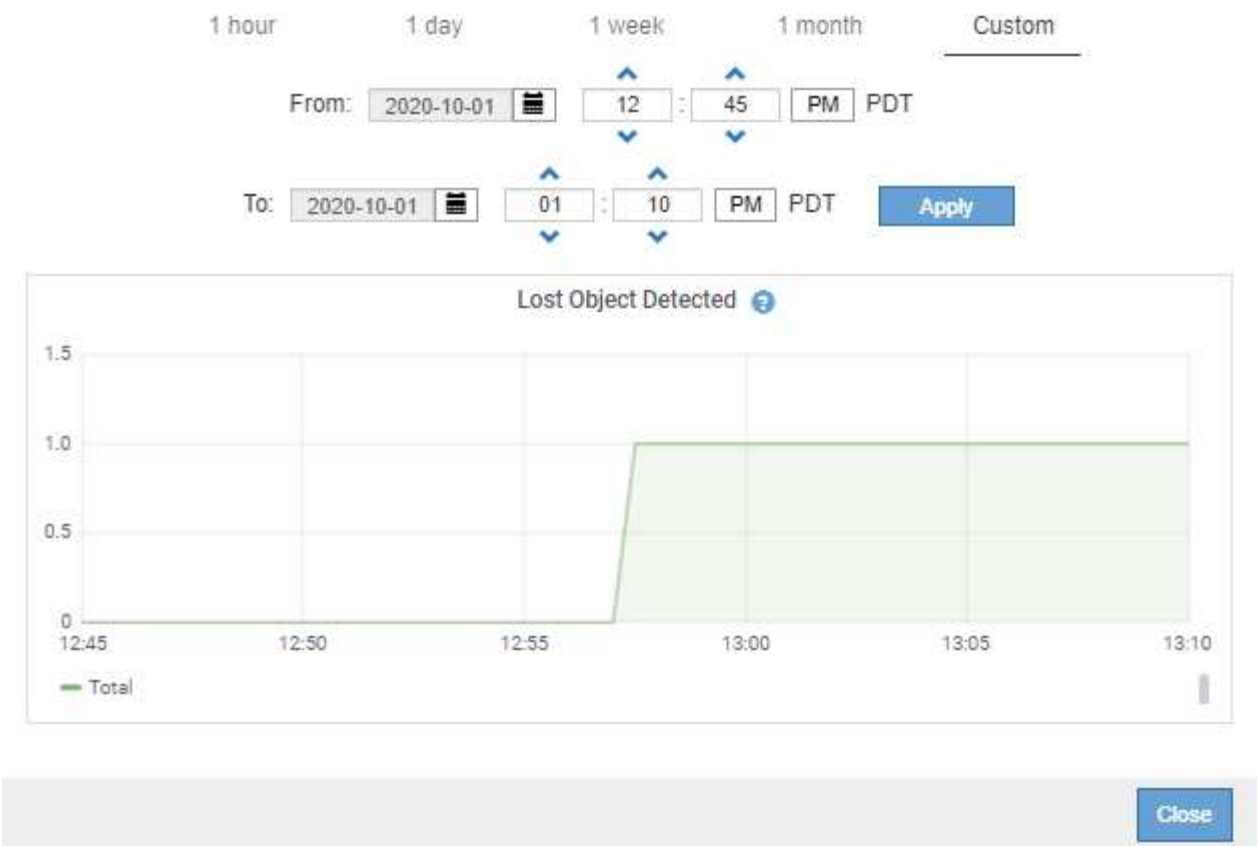
- **Liniendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG** > **Tools** > **Grid Topologie** (wählen Sie das Diagrammsymbol Nach einem Datenwert) werden Liniendiagramme verwendet, um die Werte von StorageGRID-Attributen zu zeichnen, die einen Einheitenwert haben (z. B. NTP-Frequenzversatz in ppm). Die Wertänderungen werden im Laufe der Zeit in regelmäßigen Datenintervallen (Bins) dargestellt.



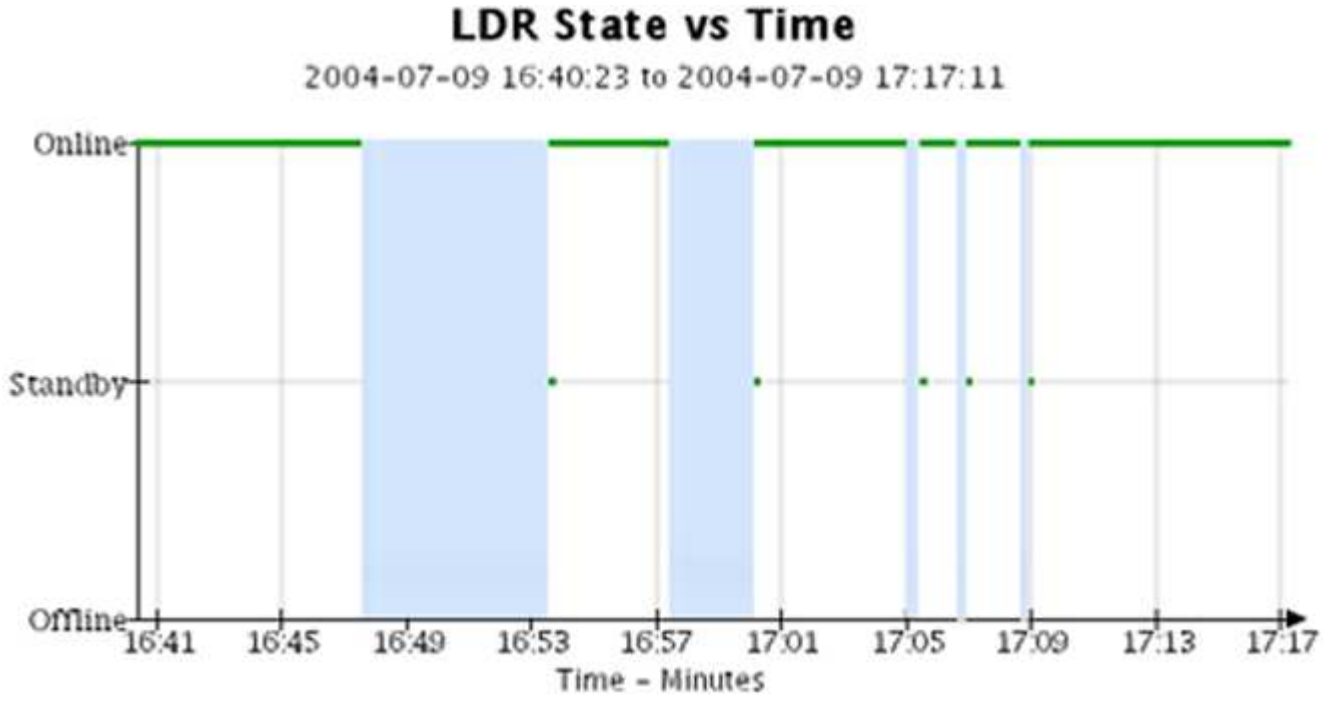
- **Flächendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG** > **Tools** > **Grid-Topologie** (wählen Sie das Diagrammsymbol Nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen zu zeichnen, z. B. Objektanzahl oder Dienstlastwerte. Die Flächendiagramme ähneln den Liniendiagrammen, enthalten jedoch eine hellbraune Schattierung unter der Linie. Die Wertänderungen werden im Laufe der Zeit in regelmäßigen Datenintervallen (Bins) dargestellt.



- Einige Diagramme sind mit einem anderen Diagrammsymbol gekennzeichnet Und haben ein anderes Format:



- **Zustandsdiagramm**: Verfügbar über die Seite **UNTERSTÜTZUNG** > **Tools** > **Grid-Topologie** (wählen Sie das Diagrammsymbol Nach einem Datenwert) werden Zustandsdiagramme verwendet, um Attributwerte zu zeichnen, die unterschiedliche Zustände darstellen, z. B. einen Servicestatus, der online, Standby oder offline sein kann. Statusdiagramme sind ähnlich wie Liniendiagramme, aber der Übergang ist ununterbrochen, d. h. der Wert springt von einem Statuswert zum anderen.



Verwandte Informationen

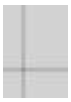
"Zeigen Sie die Seite Knoten an"

"Sehen Sie sich den Baum der Grid Topology an"

"Prüfen von Support-Kennzahlen"

Diagrammlegende

Die Linien und Farben, die zum Zeichnen von Diagrammen verwendet werden, haben eine besondere Bedeutung.

Beispiel	Bedeutung
	Gemeldete Attributwerte werden mit dunkelgrünen Linien dargestellt.
	Hellgrüne Schattierungen um dunkelgrüne Linien zeigen an, dass die tatsächlichen Werte in diesem Zeitbereich variieren und für eine schnellere Darstellung „binniert“ wurden. Die dunkle Linie stellt den gewichteten Durchschnitt dar. Der Bereich in hellgrün zeigt die maximalen und minimalen Werte innerhalb des Fachs an. Für Flächendiagramme wird ein hellbrauner Schattierung verwendet, um volumetrische Daten anzuzeigen.
	Leere Bereiche (keine Daten dargestellt) zeigen an, dass die Attributwerte nicht verfügbar waren. Der Hintergrund kann blau, grau oder eine Mischung aus grau und blau sein, je nach Status des Dienstes, der das Attribut meldet.
	Hellblaue Schattierung zeigt an, dass einige oder alle Attributwerte zu diesem Zeitpunkt unbestimmt waren; das Attribut war keine Meldung von Werten, da der Dienst sich in einem unbekannten Zustand befand.
	Graue Schattierung zeigt an, dass einige oder alle Attributwerte zu diesem Zeitpunkt nicht bekannt waren, da der Dienst, der die Attribute meldet, administrativ herabgesetzt war.
	Eine Mischung aus grauem und blauem Schatten zeigt an, dass einige der Attributwerte zu diesem Zeitpunkt unbestimmt waren (weil der Dienst sich in einem unbekannten Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldet, administrativ nach unten lag.

Zeigen Sie Diagramme und Diagramme an

Die Seite Nodes enthält die Diagramme und Diagramme, auf die Sie regelmäßig zugreifen sollten, um Attribute wie Speicherkapazität und Durchsatz zu überwachen. In einigen Fällen, vor allem bei der Arbeit mit technischem Support, können Sie die Seite **SUPPORT** > **Tools** > **Grid Topology** verwenden, um auf zusätzliche Diagramme zuzugreifen.

Bevor Sie beginnen

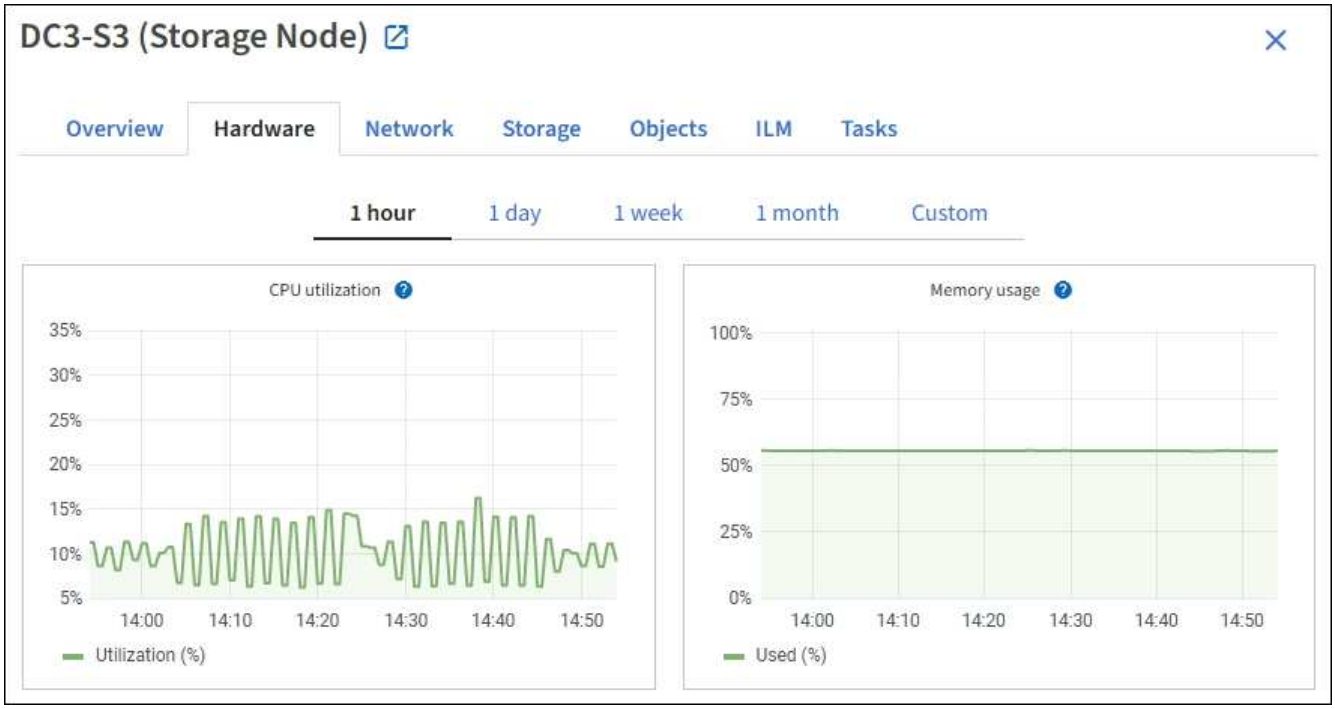
Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".

Schritte

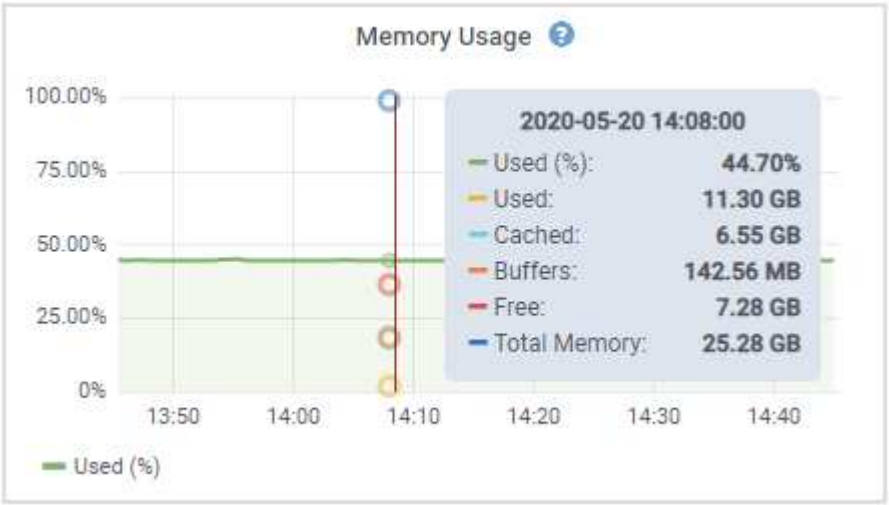
1. Wählen Sie **KNOTEN**. Wählen Sie dann einen Knoten, einen Standort oder das gesamte Raster aus.

2. Wählen Sie die Registerkarte aus, auf der Informationen angezeigt werden sollen.

   Einige Registerkarten enthalten eine oder mehrere Grafana-Diagramme, mit denen die Werte der Prometheus-Kennzahlen im Laufe der Zeit dargestellt werden. Die Registerkarte **NODES** > **Hardware** für einen Knoten enthält beispielsweise zwei Grafana-Diagramme.



3. Setzen Sie den Cursor optional auf das Diagramm, um detailliertere Werte für einen bestimmten Zeitpunkt anzuzeigen.



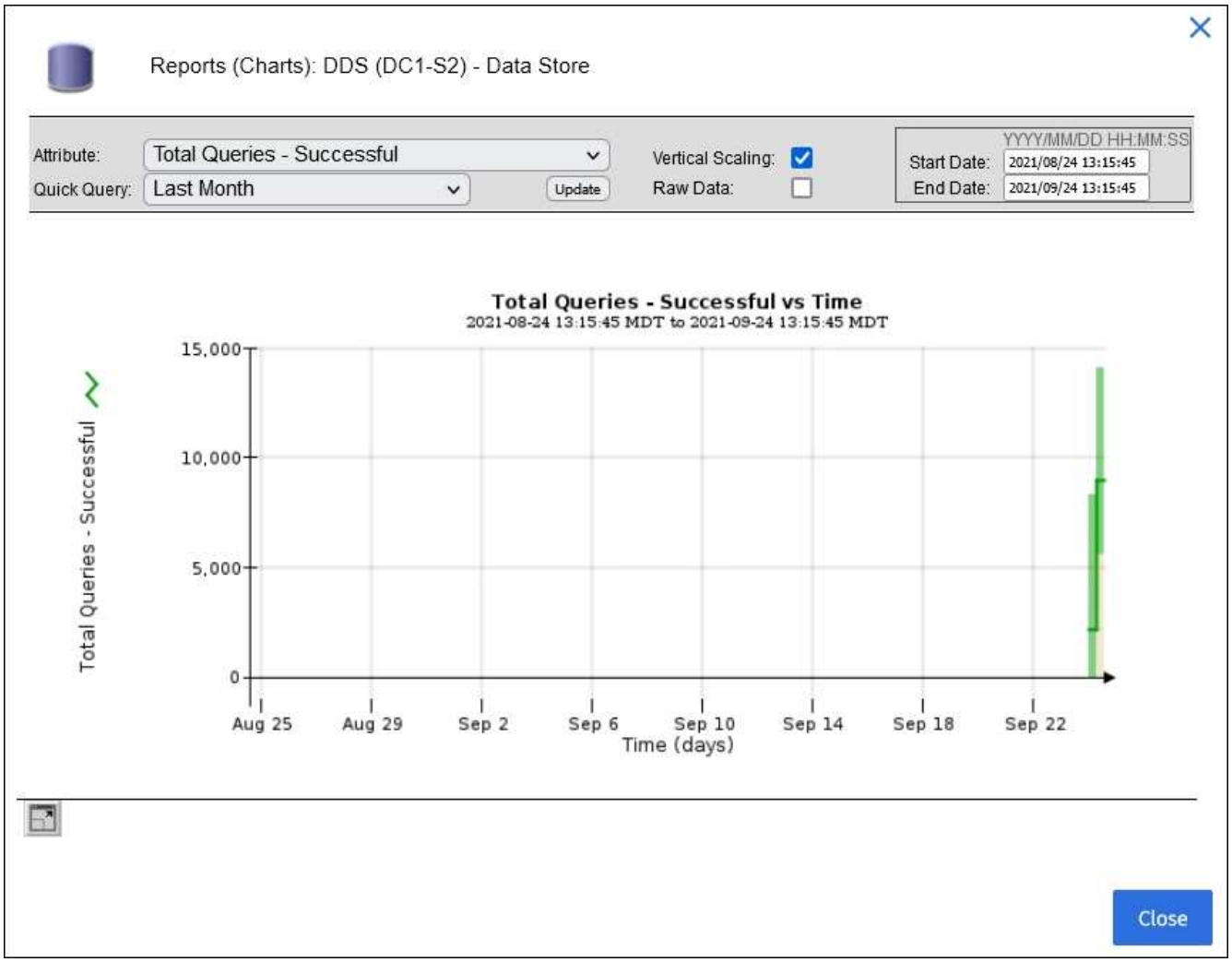
4. Bei Bedarf können Sie oft ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Wählen Sie in der Tabelle auf der Seite Knoten das Diagrammsymbol aus Rechts neben dem Attributnamen.

   Diagramme sind nicht für alle Metriken und Attribute verfügbar.

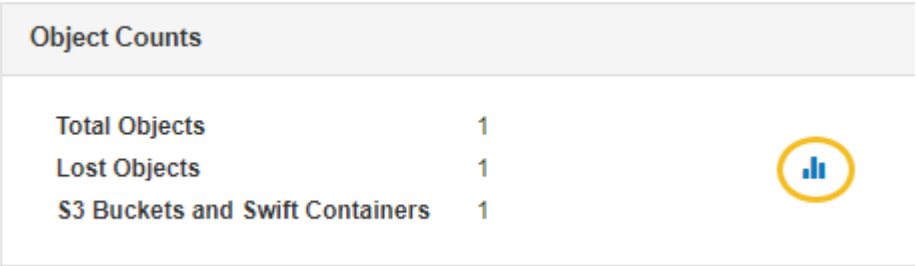
   Beispiel 1: Auf der Registerkarte Objekte für einen Speicherknoten können Sie das Diagrammsymbol auswählen Um die Gesamtzahl der erfolgreichen Metadaten-Speicherabfragen für den Speicherknoten

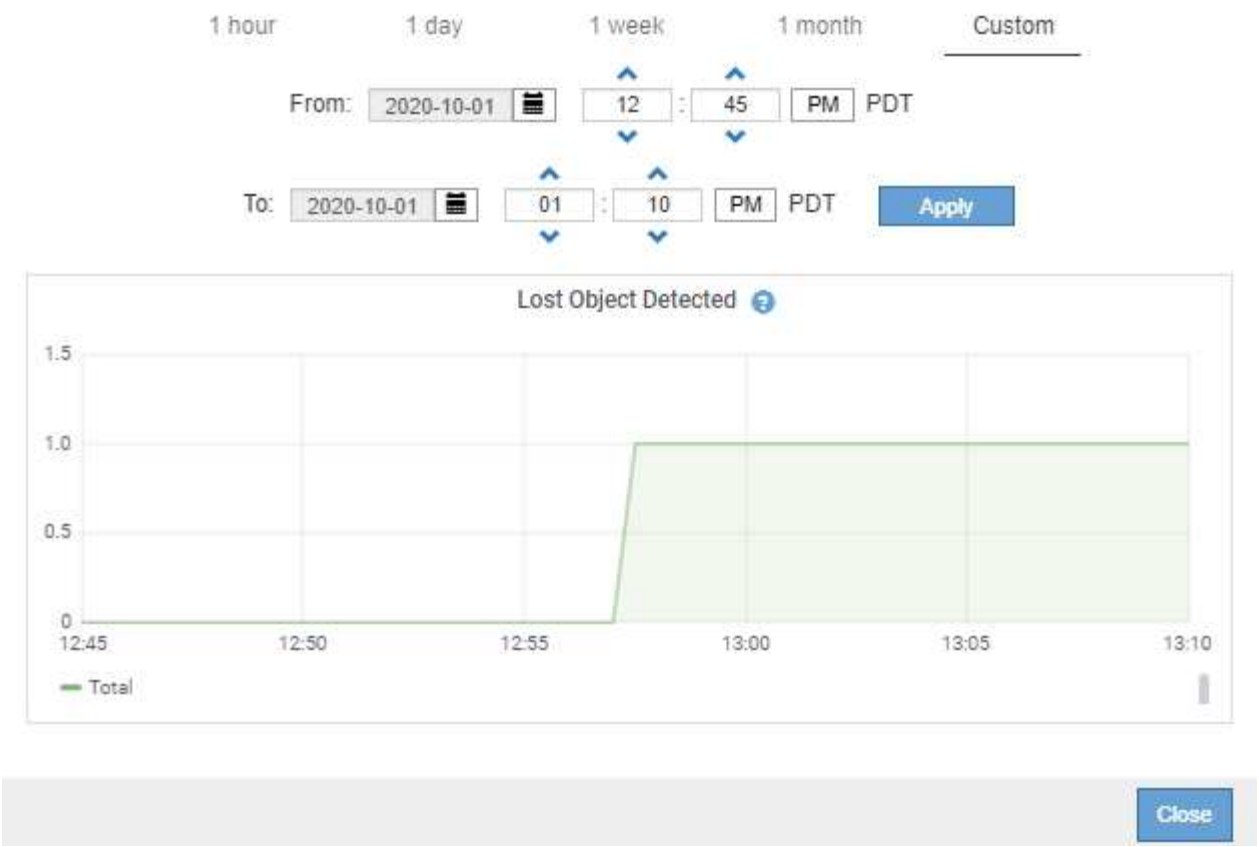
anzuzeigen.

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close



Beispiel 2: Auf der Registerkarte Objekte eines Storage Node können Sie das Diagramm-Symbol auswählen Zeigt die Grafana-Grafik der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte an.





5. Um Diagramme für Attribute anzuzeigen, die nicht auf der Seite Knoten angezeigt werden, wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**.
6. Wählen Sie ***Grid Node*** > ***Component oder Service*** > **Übersicht** > **Main** aus.
7. Wählen Sie das Diagrammsymbol aus Neben dem Attribut.

   Das Display wechselt automatisch zur Seite **Berichte** > **Diagramme**. Das Diagramm zeigt die Daten des Attributs über den letzten Tag an.

Diagramme generieren

Diagramme zeigen eine grafische Darstellung der Attributdatenwerte an. Die Berichte können an Datacenter-Standorten, Grid-Node, Komponenten oder Service erstellt werden.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Grid Node*** > ***Component oder Service*** > **Berichte** > **Diagramme** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Um den Start der Y-Achse bei Null zu erzwingen, deaktivieren Sie das Kontrollkästchen **Vertikale Skalierung**.

5. Um Werte mit voller Genauigkeit anzuzeigen, aktivieren Sie das Kontrollkästchen **Rohdaten** oder um Werte auf maximal drei Dezimalstellen zu runden (z. B. für als Prozentsätze gemeldete Attribute), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie den Zeitraum aus der Dropdown-Liste **Quick Query** aus, für den Sie einen Bericht erstellen möchten.

   Wählen Sie die Option Benutzerdefinierte Abfrage aus, um einen bestimmten Zeitbereich auszuwählen.

   Das Diagramm erscheint nach wenigen Augenblicken. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen.

7. Wenn Sie Benutzerdefinierte Abfrage ausgewählt haben, passen Sie den Zeitraum für das Diagramm an, indem Sie die Optionen **Startdatum** und **Enddatum** eingeben.

   Verwenden Sie das Format `YYYY/MM/DDHH:MM:SS` Ortszeit verwendet. Führende Nullen sind für das Format erforderlich. Beispiel: 2017/4/6 7:30:00 schlägt die Validierung fehl. Das richtige Format ist: 2017/04/06 07:30:00.

8. Wählen Sie **Aktualisieren**.

   Nach einigen Sekunden wird ein Diagramm erzeugt. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen. Abhängig von der für die Abfrage festgelegten Dauer wird entweder ein RAW-Textbericht oder ein aggregierter Textbericht angezeigt.

Verwenden Sie Textberichte

Textberichte zeigen eine textuelle Darstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Es gibt zwei Arten von Berichten, die je nach Zeitraum erstellt werden, für den Sie einen Bericht erstellen: RAW-Textberichte für Zeiträume unter einer Woche und Zusammenfassung von Textberichten für Zeiträume, die länger als eine Woche sind.

RAW-Textberichte

In einem RAW-Textbericht werden Details zum ausgewählten Attribut angezeigt:

- Empfangene Zeit: Lokales Datum und Uhrzeit, zu der ein Beispielwert der Daten eines Attributs vom NMS-Dienst verarbeitet wurde.
- Probenzeit: Lokales Datum und Uhrzeit, zu der ein Attributwert an der Quelle erfasst oder geändert wurde.
- Wert: Attributwert zur Probenzeit.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Zusammenfassen von Textberichten

Ein zusammengefasster Textbericht zeigt Daten über einen längeren Zeitraum (in der Regel eine Woche) an als einen reinen Textbericht. Jeder Eintrag ist das Ergebnis einer Zusammenfassung mehrerer Attributwerte (ein Aggregat von Attributwerten) durch den NMS-Dienst über einen Zeitraum in einem einzigen Eintrag mit durchschnittlichen, maximalen und minimalen Werten, die aus der Aggregation abgeleitet sind.

In jedem Eintrag werden die folgenden Informationen angezeigt:

- Aggregatzeit: Letztes lokales Datum und Zeitpunkt, zu dem der NMS-Dienst einen Satz von geänderten Attributwerten aggregiert (gesammelt) hat.
- Durchschnittswert: Der Mittelwert des Attributs über den aggregierten Zeitraum.
- Mindestwert: Der Mindestwert über den aggregierten Zeitraum.
- Maximalwert: Der Maximalwert über den aggregierten Zeitraum.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Erstellen von Textberichten

Textberichte zeigen eine textuelle Darstellung von Attributdatenwerten an, die vom NMS-Dienst verarbeitet wurden. Die Berichte können an Datacenter-Standorten, Grid-Node, Komponenten oder Service erstellt werden.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Für Attributdaten, die voraussichtlich kontinuierlich geändert werden, werden diese Attributdaten in regelmäßigen Abständen vom NMS-Dienst (an der Quelle) erfasst. Bei selten veränderlichen Attributdaten (z. B. Daten, die auf Ereignissen wie Statusänderungen basieren) wird ein Attributwert an den NMS-Dienst gesendet, wenn sich der Wert ändert.

Der angezeigte Berichtstyp hängt vom konfigurierten Zeitraum ab. Standardmäßig werden zusammengefasste Textberichte für Zeiträume generiert, die länger als eine Woche sind.

Der graue Text zeigt an, dass der Dienst während der Probenahme administrativ unten war. Blauer Text zeigt an, dass der Dienst in einem unbekannten Zustand war.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Grid Node*** > ***Component oder Service*** > **Berichte** > **Text** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Wählen Sie aus der Dropdown-Liste **Ergebnisse pro Seite** die Anzahl der Ergebnisse pro Seite aus.
5. Um Werte auf maximal drei Dezimalstellen zu runden (z. B. für als Prozentsätze gemeldete Attribute), deaktivieren Sie das Kontrollkästchen **Rohdaten**.
6. Wählen Sie den Zeitraum aus der Dropdown-Liste **Quick Query** aus, für den Sie einen Bericht erstellen möchten.

   Wählen Sie die Option Benutzerdefinierte Abfrage aus, um einen bestimmten Zeitbereich auszuwählen.

Der Bericht erscheint nach wenigen Augenblicken. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen.

7. Wenn Sie „Benutzerdefinierte Abfrage“ ausgewählt haben, müssen Sie den Zeitraum anpassen, an dem Sie einen Bericht erstellen möchten, indem Sie die Optionen **Startdatum** und **Enddatum** eingeben.

   Verwenden Sie das Format `YYYY/MM/DDHH:MM:SS` Ortszeit verwendet. Führende Nullen sind für das Format erforderlich. Beispiel: 2017/4/6 7:30:00 schlägt die Validierung fehl. Das richtige Format ist: 2017/04/06 07:30:00.

8. Klicken Sie Auf **Aktualisieren**.

   Nach wenigen Augenblicken wird ein Textbericht erstellt. Lassen Sie mehrere Minuten für die Tabulierung von langen Zeitbereichen. Abhängig von der für die Abfrage festgelegten Dauer wird entweder ein RAW-Textbericht oder ein aggregierter Textbericht angezeigt.

Exportieren von Textberichten

Exportierte Textberichte öffnen eine neue Browser-Registerkarte, auf der Sie die Daten auswählen und kopieren können.

Über diese Aufgabe

Die kopierten Daten können dann in einem neuen Dokument (z. B. in einer Tabelle) gespeichert und zur Analyse der Performance des StorageGRID-Systems verwendet werden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Erstellen Sie einen Textbericht.
3. Klicken Sie Auf *Exportieren*.

   Das Fenster Textbericht exportieren wird geöffnet, in dem der Bericht angezeigt wird.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Wählen Sie den Inhalt des Fensters „Textbericht exportieren“ aus, und kopieren Sie ihn.

   Diese Daten können jetzt in ein Dokument eines Drittanbieters wie z. B. in eine Tabelle eingefügt werden.

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

Um DIE PUT- und GET-Leistung zu überwachen, können Sie S3- und Swift-Befehle direkt von einer Workstation aus oder über die Open-Source S3tester-Anwendung ausführen. 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 in "Prüfprotokoll" Geben Sie die Gesamtzeit an, die für die Ausführung bestimmter Vorgänge erforderlich ist. 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 Vorgänge:

- **S3**: LÖSCHEN, HOLEN, KOPF, Metadaten aktualisiert, POST, PUT
- **SWIFT**: LÖSCHEN, HOLEN, KOPF, SETZEN

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.

- Das können Sie "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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".

Über diese Aufgabe

Zwei "Verifizierungsprozesse" Gewährleisten Sie gemeinsam die Datenintegrität:

- **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 auf Archiv-Nodes oder auf Objekten in einem Cloud-Speicherpool 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.

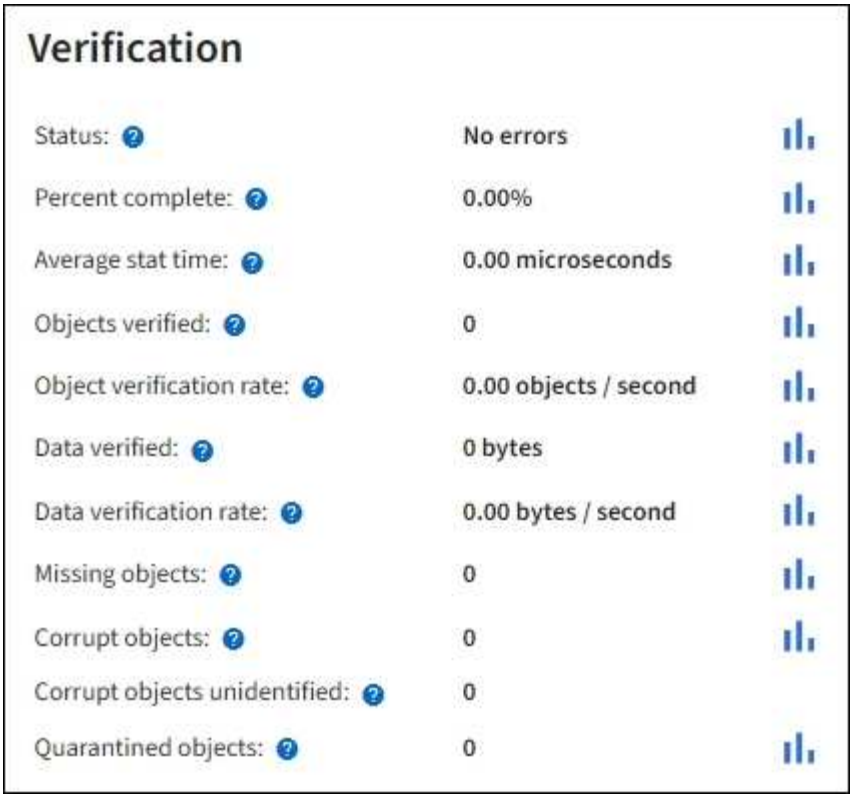
Schritte

1. Prüfen Sie die Ergebnisse aus Hintergrundverifizierungen:

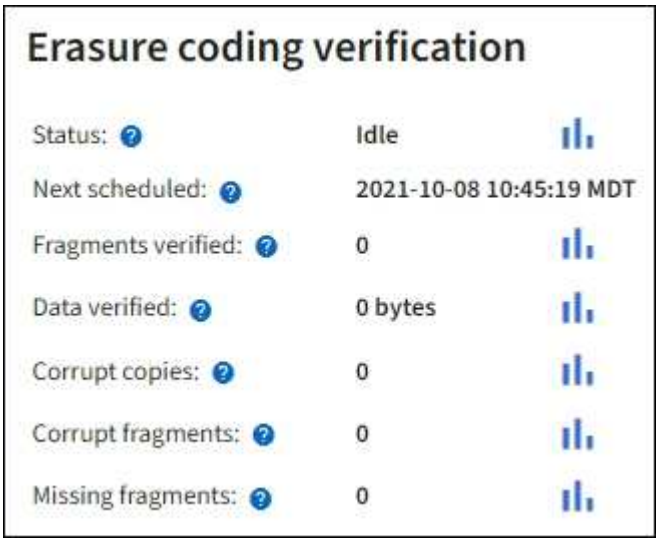
   a. Wählen Sie **NODES** > ***Storage Node*** > **Objekte** aus.

   b. Überprüfen Sie die Überprüfungsergebnisse:

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

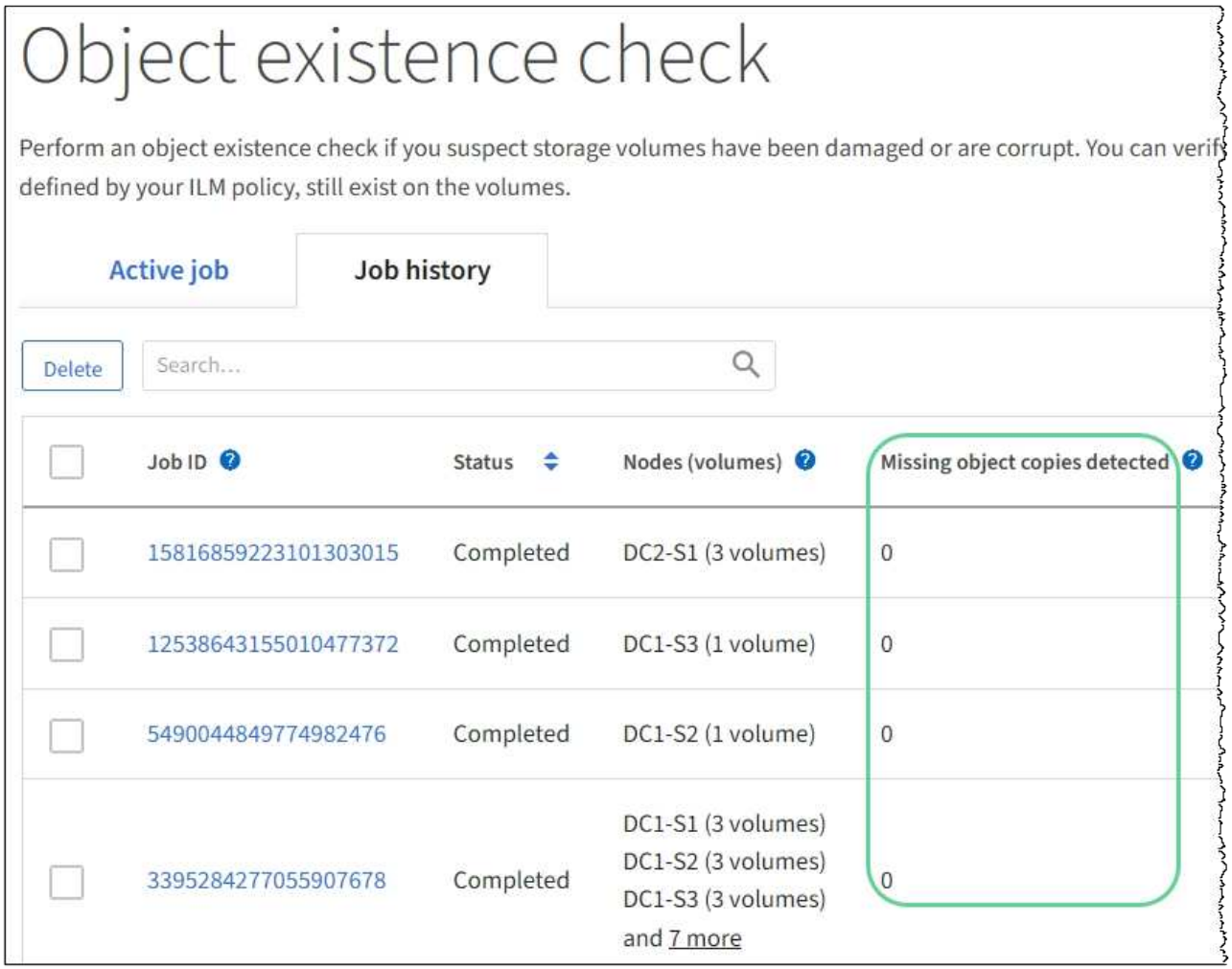


- Um die Überprüfung von Fragment mit Löschungscode zu überprüfen, wählen Sie ***Storage Node*** > **ILM** aus, und sehen Sie sich die Attribute im Abschnitt zur Verifizierung von Erasure-Coding an.



Wählen Sie das Fragezeichen aus ? Neben dem Namen eines Attributs wird Hilfetext angezeigt.

2. Überprüfen Sie die Ergebnisse von Objektprüfaufträgen:
   a. Wählen Sie **WARTUNG** > **Objekt Existenzprüfung** > **Jobverlauf**.
   b. Scannen Sie die Spalte „fehlende Objektkopien erkannt“. Wenn bei Jobs 100 oder mehr fehlende Objektkopien vorhanden waren und die Warnmeldung **Objects lost** ausgelöst wurde, wenden Sie sich an den technischen Support.



Monitoring von Ereignissen

Sie können Ereignisse überwachen, die von einem Grid-Node erkannt werden, einschließlich benutzerdefinierter Ereignisse, die Sie erstellt haben, um Ereignisse zu verfolgen, die auf dem Syslog-Server protokolliert werden. Die Meldung Letztes Ereignis, die im Grid Manager angezeigt wird, enthält weitere Informationen zum letzten Ereignis.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log` Protokolldatei. Siehe "Referenz für Protokolldateien".

Der SMTT-Alarm (Total Events) kann wiederholt durch Probleme wie Netzwerkprobleme, Stromausfälle oder Upgrades ausgelöst werden. Dieser Abschnitt enthält Informationen zur Untersuchung von Ereignissen, sodass Sie besser verstehen können, warum diese Alarme aufgetreten sind. Wenn ein Ereignis aufgrund eines bekannten Problems aufgetreten ist, können die Ereigniszähler sicher zurückgesetzt werden.

Schritte

1. Überprüfen Sie die Systemereignisse für jeden Grid-Node:
   a. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
   b. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Events** > **Übersicht** > **Main**.
2. Erstellen Sie eine Liste früherer Ereignismeldungen, um Probleme zu isolieren, die in der Vergangenheit aufgetreten sind:

a. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.

b. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Events** > **Berichte** aus.

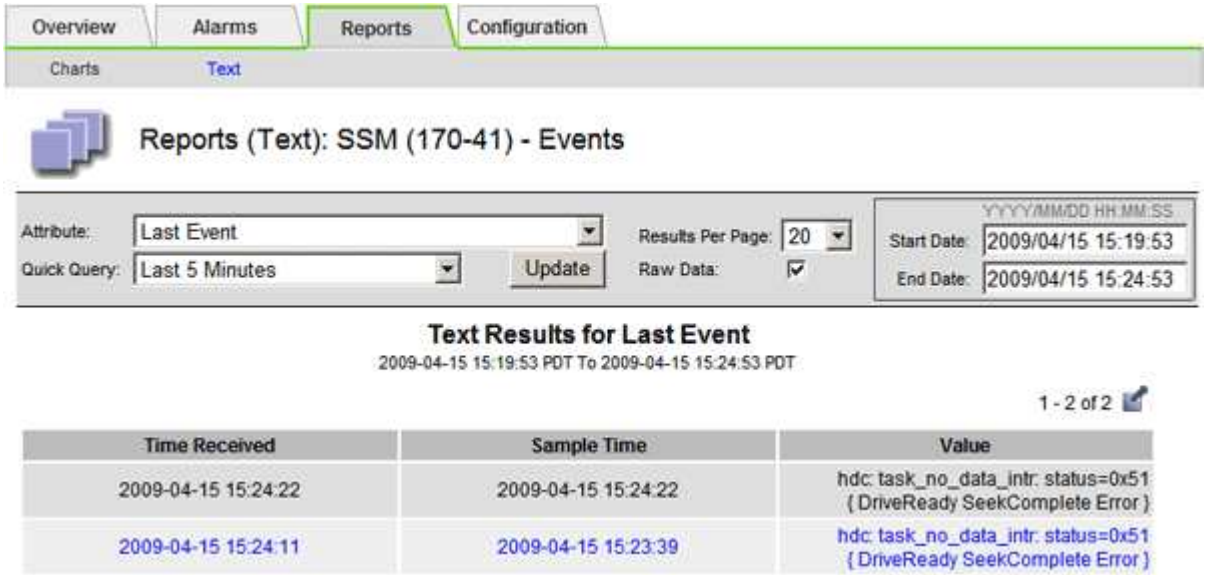
c. Wählen Sie **Text**.

Das Attribut **Letztes Ereignis** wird im nicht angezeigt "Diagrammansicht". So zeigen Sie es an:

d. Ändern Sie **Attribut** in **Letztes Ereignis**.

e. Wählen Sie optional einen Zeitraum für **Quick Query** aus.

f. Wählen Sie **Aktualisieren**.



Erstellen benutzerdefinierter Syslog-Ereignisse

Benutzerdefinierte Ereignisse ermöglichen die Verfolgung aller Kernel-, Daemon-, Fehler- und kritischen Benutzerereignisse auf der Ebene, die beim Syslog-Server protokolliert werden. Ein benutzerdefiniertes Ereignis kann nützlich sein, um das Auftreten von Systemprotokollmeldungen zu überwachen (und damit Netzwerksicherheitsereignisse und Hardwarefehler).

Über diese Aufgabe

Ziehen Sie in Betracht, benutzerdefinierte Ereignisse zu erstellen, um wiederkehrende Probleme zu überwachen. Die folgenden Überlegungen gelten für benutzerdefinierte Ereignisse.

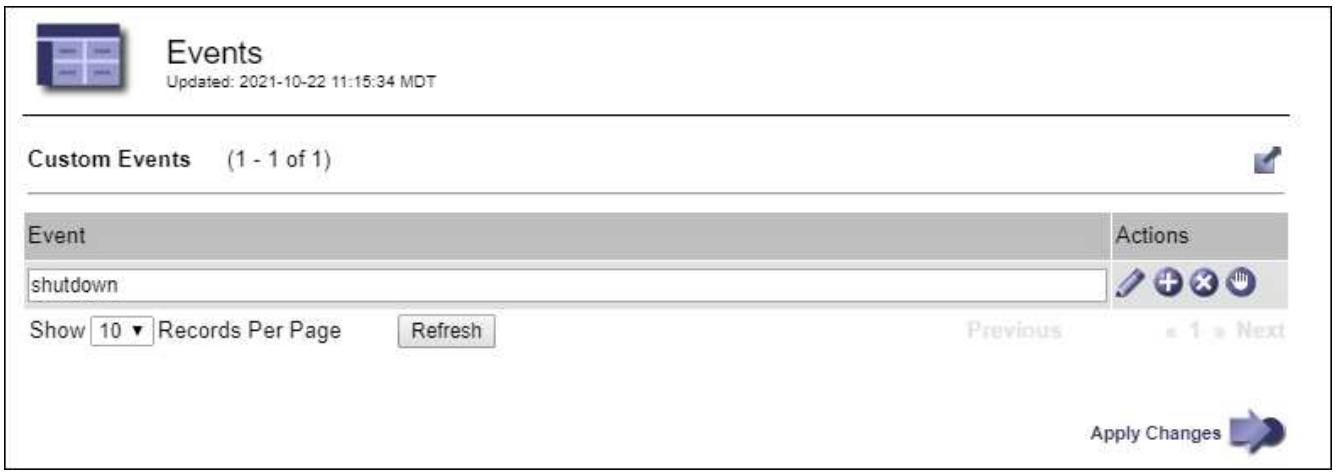
- Nach der Erstellung eines benutzerdefinierten Ereignisses wird jeder Vorgang überwacht.
- So erstellen Sie ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern im `/var/local/log/messages` Dateien, die Protokolle in diesen Dateien müssen:
  - Vom Kernel generiert
  - Wird vom Daemon oder vom Benutzerprogramm auf der Fehler- oder kritischen Ebene generiert

Hinweis: nicht alle Einträge im `/var/local/log/messages` Die Dateien werden abgeglichen, sofern sie nicht die oben genannten Anforderungen erfüllen.

Schritte

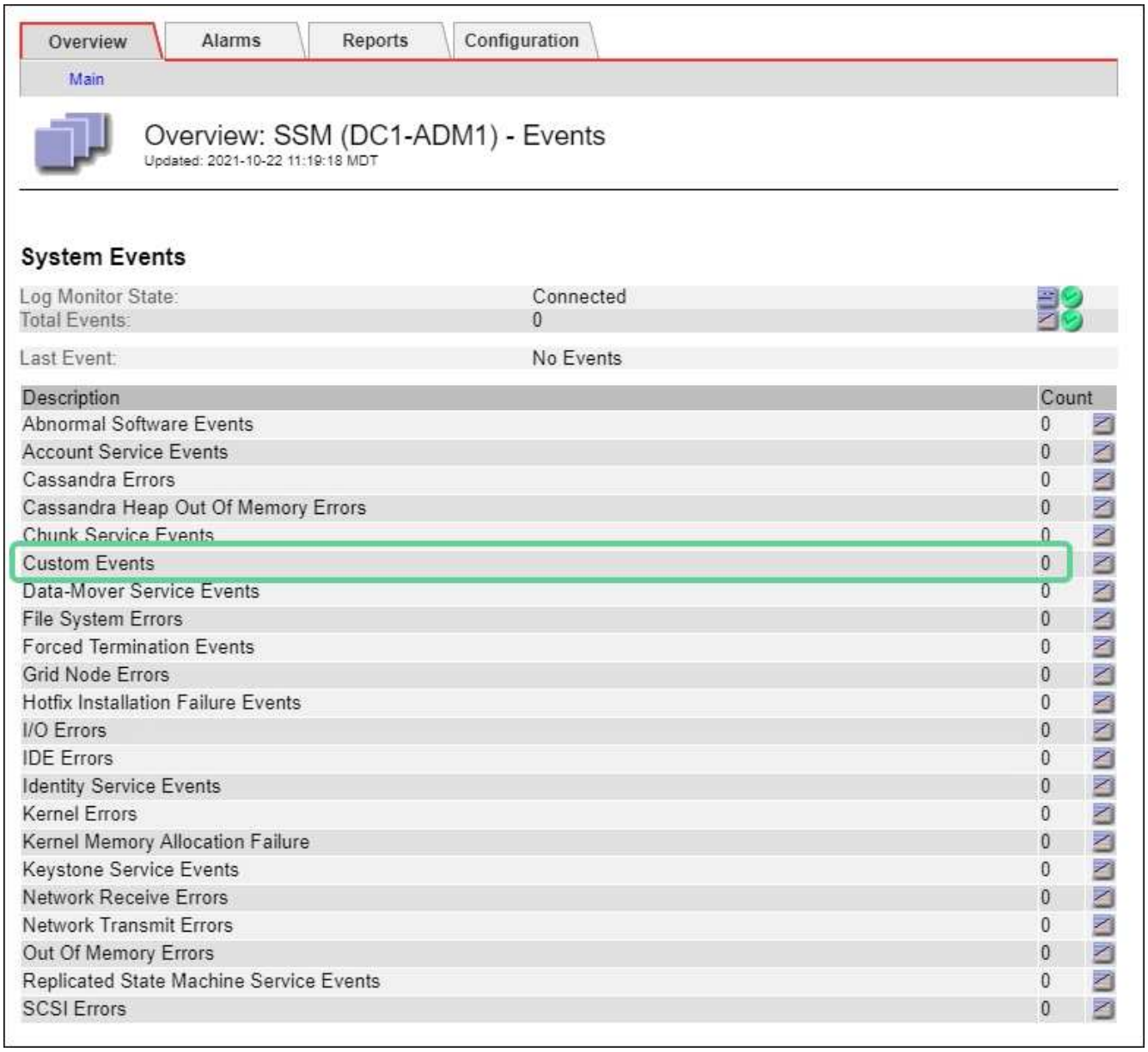
1. Wählen Sie **SUPPORT** > **Alarme (alt)** > **Benutzerdefinierte Ereignisse**.

2. Klicken Sie Auf **Bearbeiten** (Oder **Einfügen** Wenn dies nicht das erste Ereignis ist).
3. Geben Sie eine benutzerdefinierte Ereigniszeichenfolge ein, z. B. Herunterfahren



4. Wählen Sie **Änderungen Anwenden**.
5. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
6. Wählen Sie ***Grid Node*** > **SSM** > **Events** aus.
7. Suchen Sie den Eintrag für benutzerdefinierte Ereignisse in der Ereignistabelle, und überwachen Sie den Wert für **Zählung**.

   Wenn die Anzahl erhöht wird, wird ein benutzerdefiniertes Ereignis, das Sie überwachen, auf diesem Grid-Node ausgelöst.



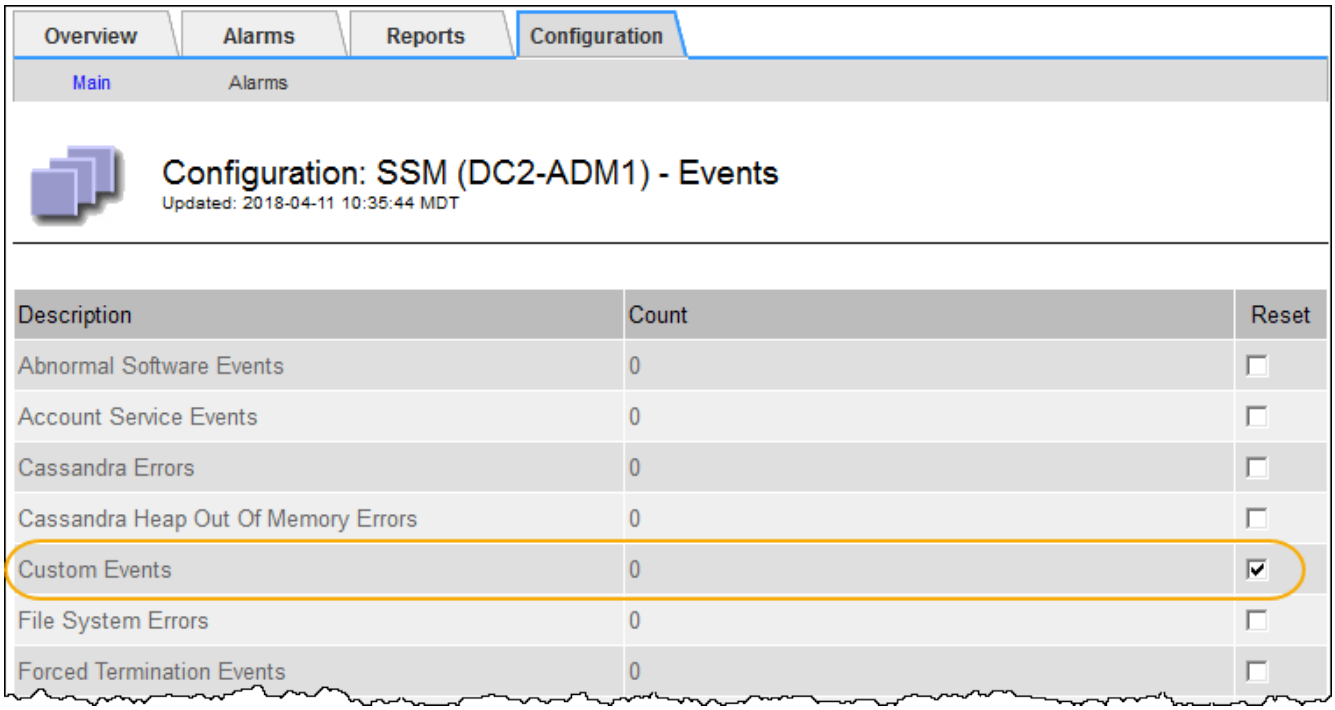
Setzen Sie die Anzahl der benutzerdefinierten Ereignisse auf Null zurück

Wenn Sie den Zähler nur für benutzerdefinierte Ereignisse zurücksetzen möchten, müssen Sie die Seite Grid Topology im Menü Support verwenden.

Beim Zurücksetzen eines Zählers wird der Alarm durch das nächste Ereignis ausgelöst. Wenn Sie einen Alarm quittieren, wird dieser Alarm dagegen nur erneut ausgelöst, wenn der nächste Schwellwert erreicht wird.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Grid Node*** > **SSM** > **Events** > **Konfiguration** > **Main** aus.
3. Aktivieren Sie das Kontrollkästchen **Zurücksetzen** für benutzerdefinierte Ereignisse.



4. Wählen Sie **Änderungen Anwenden**.

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.
- Lese- und Schreibvorgänge von Clients werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Erstellen, Ändern oder Abrufen eines Objekts vorgibt.
- 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.

Für den einfachen Zugriff auf Audit-Protokolle können Sie "Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS". Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien 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.
- "Erfahren Sie mehr über das Konfigurieren von Überwachungsmeldungen und Protokollzielen".

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

Erfassen von Protokolldateien und Systemdaten

Mit dem Grid Manager können Sie Protokolldateien und Systemdaten (einschließlich Konfigurationsdaten) für Ihr StorageGRID System abrufen.

Bevor Sie beginnen

- Sie müssen auf dem primären Admin-Knoten unter Verwendung eines beim Grid-Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

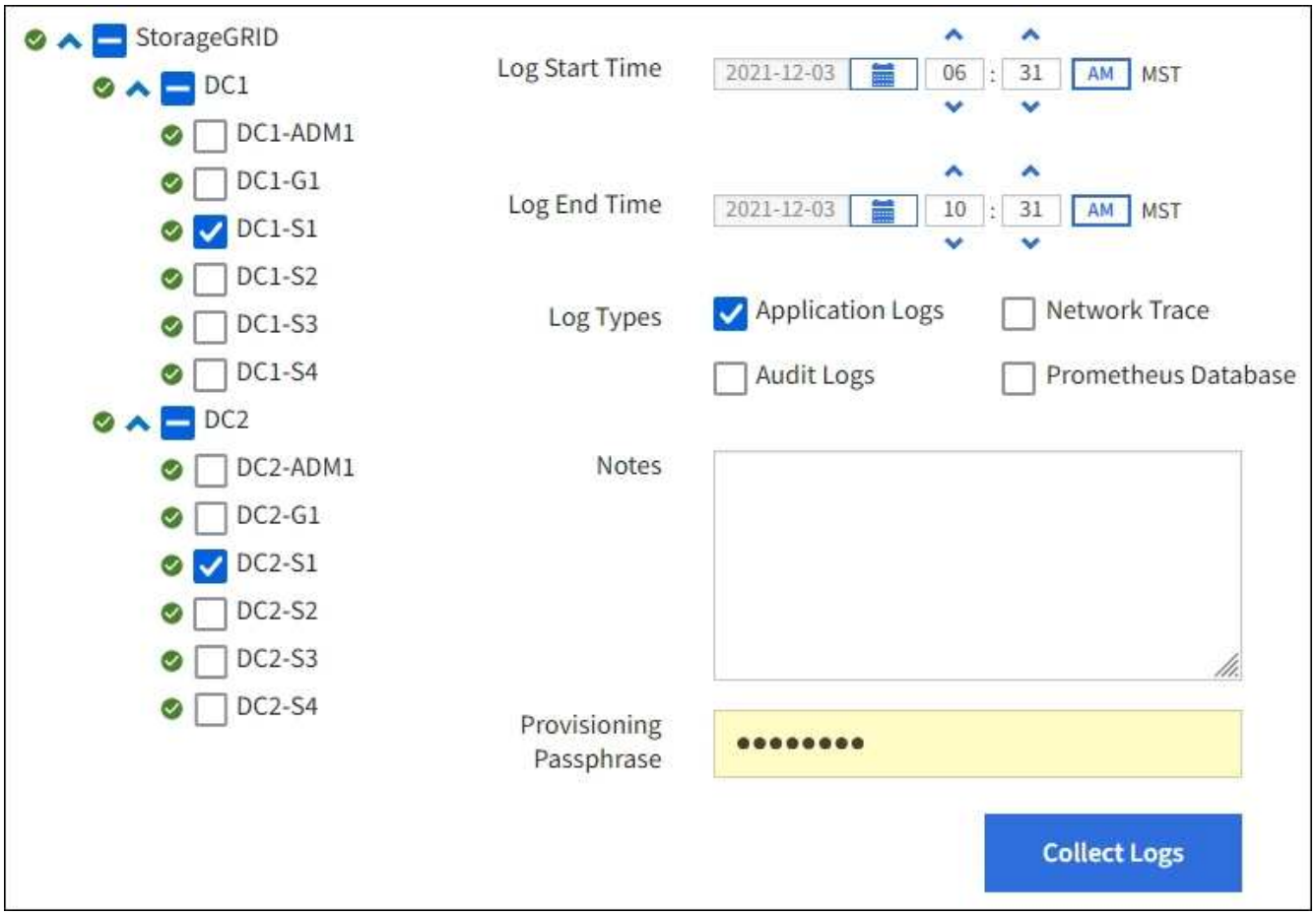
Über diese Aufgabe

Sie können den Grid Manager zum Sammeln verwenden "Log-Dateien", Systemdaten und Konfigurationsdaten von einem beliebigen Grid-Knoten für den von Ihnen ausgewählten Zeitraum. Die Daten werden in einer .tar.gz-Datei gesammelt und archiviert, die Sie dann auf Ihren lokalen Computer herunterladen können.

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. Siehe "Konfigurieren von Überwachungsmeldungen und Protokollzielen".

Schritte

1. Wählen Sie **SUPPORT** > **Extras** > **Protokolle**.



2. Wählen Sie die Grid-Knoten aus, für die Sie Protokolldateien sammeln möchten.

   Je nach Bedarf können Sie Log-Dateien für das gesamte Grid oder einen gesamten Datacenter-Standort sammeln.

3. Wählen Sie eine **Startzeit** und **Endzeit** aus, um den Zeitbereich der Daten festzulegen, die in die Protokolldateien aufgenommen werden sollen.

   Wenn Sie einen sehr langen Zeitraum auswählen oder Protokolle von allen Knoten in einem großen Raster sammeln, könnte das Protokollarchiv zu groß werden, um auf einem Knoten gespeichert zu werden, oder zu groß, um zum Download an den primären Admin-Knoten gesammelt zu werden. In diesem Fall müssen Sie die Protokollerfassung mit einem kleineren Datensatz neu starten.

4. Wählen Sie die Protokolltypen aus, die Sie sammeln möchten.
   - **Anwendungsprotokolle**: Anwendungsspezifische Protokolle, die der technische Support am häufigsten für die Fehlerbehebung verwendet. Die gesammelten Protokolle sind eine Teilmenge der verfügbaren Anwendungsprotokolle.
   - **Audit Logs**: Protokolle, die die während des normalen Systembetriebs erzeugten Audit-Meldungen enthalten.
   - **Network Trace**: Protokolle, die für das Debuggen von Netzwerken verwendet werden.
   - **Prometheus Datenbank**: Zeitreihenkennzahlen aus den Diensten auf allen Knoten.
5. Geben Sie optional Notizen zu den Protokolldateien ein, die Sie im Textfeld **Hinweise** sammeln.

   Mithilfe dieser Hinweise können Sie Informationen zum technischen Support über das Problem geben, das Sie zum Erfassen der Protokolldateien aufgefordert hat. Ihre Notizen werden einer Datei namens

hinzugefügt `info.txt`, Zusammen mit anderen Informationen über die Log-Datei-Sammlung. Der `info.txt` Die Datei wird im Archivpaket der Protokolldatei gespeichert.

6. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
7. Wählen Sie **Protokolle Sammeln**.

   Wenn Sie eine neue Anforderung senden, wird die vorherige Sammlung von Protokolldateien gelöscht.

   Auf der Seite „Protokolle“ können Sie den Fortschritt der Sammlung von Protokolldateien 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.

8. Wählen Sie **Download**, wenn die Sammlung der Protokolldatei abgeschlossen ist.

   Die Datei *.tar.gz* enthält alle Protokolldateien aller Grid-Knoten, in denen die Protokollsammlung erfolgreich war. In der kombinierten *.tar.gz*-Datei gibt es für jeden Grid-Knoten ein Log-File-Archiv.

Nachdem Sie fertig sind

Sie können das Archivpaket für die Protokolldatei später erneut herunterladen, wenn Sie es benötigen.

Optional können Sie **Löschen** wählen, um das Archiv-Paket der Protokolldatei zu entfernen und Speicherplatz freizugeben. Das aktuelle Archivpaket für die Protokolldatei wird beim nächsten Erfassen von Protokolldateien automatisch entfernt.

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 müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Sie müssen über die Berechtigung Root-Zugriff oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Wählen Sie auf der Registerkarte **Aktionen vom Benutzer ausgelöste AutoSupport** senden.

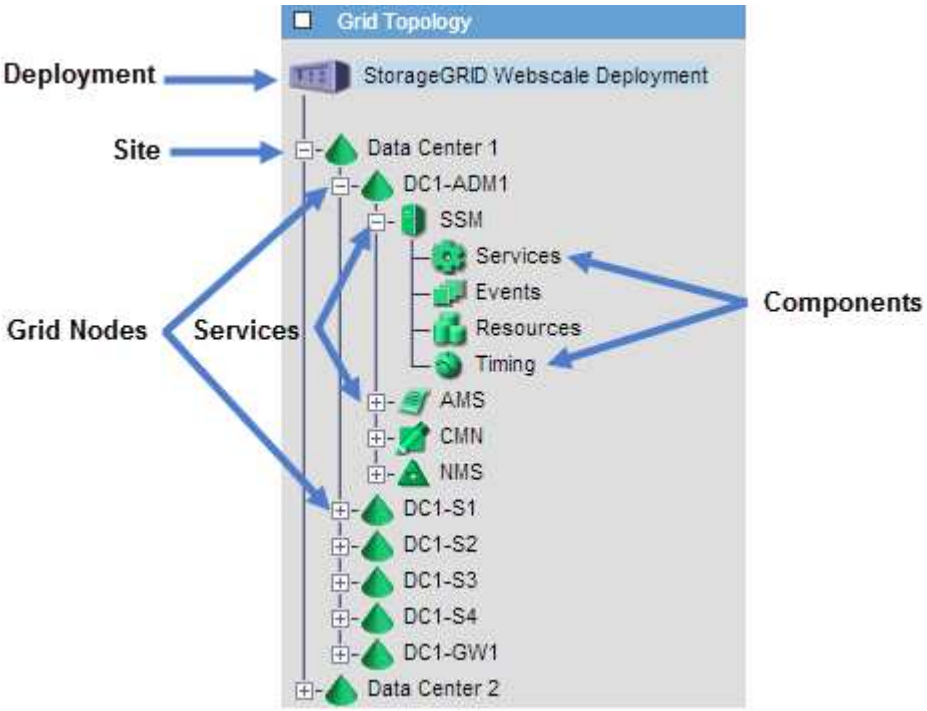
   StorageGRID versucht, ein AutoSupport-Paket an die NetApp-Support-Website zu senden. Wenn der Versuch erfolgreich ist, werden die **aktuellsten Ergebnisse** und **Letzte erfolgreiche Zeit** Werte auf der Registerkarte **Ergebnisse** aktualisiert. Wenn es ein Problem gibt, wird der Wert für das **Letzte Ergebnis** auf „fehlgeschlagen“ aktualisiert, und StorageGRID versucht nicht, das AutoSupport-Paket erneut zu senden.

   > Nachdem Sie ein vom Benutzer ausgelöstes AutoSupport-Paket gesendet haben, aktualisieren Sie die AutoSupport-Seite in Ihrem Browser nach 1 Minute, um auf die neuesten Ergebnisse zuzugreifen.

Sehen Sie sich den Baum der Grid Topology an

Die Grid Topology-Struktur bietet Zugriff auf detaillierte Informationen zu StorageGRID Systemelementen, einschließlich Standorten, Grid-Nodes, Services und Komponenten. In den meisten Fällen müssen Sie nur auf die Grid Topology-Struktur zugreifen, wenn Sie in der Dokumentation oder bei der Arbeit mit technischem Support angewiesen sind.

Um auf den Baum der Grid Topology zuzugreifen, wählen Sie **UNTERSTÜTZUNG** > **Tools** > **Grid-Topologie**.



Klicken Sie auf, um die Struktur der Grid Topology zu erweitern oder zu reduzieren ⊞ Oder ⊟ Am Standort, auf dem Node oder auf dem Service Level. Um alle Elemente der gesamten Site oder in jedem Knoten zu erweitern oder auszublenden, halten Sie die **<Strg>**-Taste gedrückt, und klicken Sie auf.

StorageGRID Attribute

Attribute berichten Werte und Status für viele Funktionen des StorageGRID-Systems. Für jeden Grid-Node, jeden Standort und das gesamte Raster sind Attributwerte verfügbar.

StorageGRID-Attribute werden an mehreren Stellen im Grid-Manager verwendet:

- **Knoten Seite**: Viele der auf der Seite Knoten angezeigten Werte sind StorageGRID-Attribute. (Auf den Seiten Nodes werden auch die Kennzahlen Prometheus angezeigt.)
- **Alarme**: Wenn Attribute definierte Schwellenwerte erreichen, werden StorageGRID-Alarme (Altsystem) auf bestimmten Schweregraden ausgelöst.
- **Grid Topology Tree**: Attributwerte werden im Grid Topology Tree (**UNTERSTÜTZUNG** > **Tools** > **Grid Topology**) angezeigt.
- **Ereignisse**: Systemereignisse treten auf, wenn bestimmte Attribute einen Fehler oder Fehlerzustand für einen Knoten aufzeichnen, einschließlich Fehler wie Netzwerkfehler.

Attributwerte

Die Attribute werden nach bestem Aufwand gemeldet und sind ungefähr richtig. Unter bestimmten Umständen können Attributaktualisierungen verloren gehen, beispielsweise der Absturz eines Service oder der Ausfall und die Wiederherstellung eines Grid-Node.

Darüber hinaus kann es zu Verzögerungen bei der Ausbreitung kommen, dass die Meldung von Attributen beeinträchtigt wird. Aktualisierte Werte für die meisten Attribute werden in festen Intervallen an das StorageGRID-System gesendet. Es kann mehrere Minuten dauern, bis ein Update im System sichtbar ist, und zwei Attribute, die sich mehr oder weniger gleichzeitig ändern, können zu leicht unterschiedlichen Zeiten gemeldet werden.

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 mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

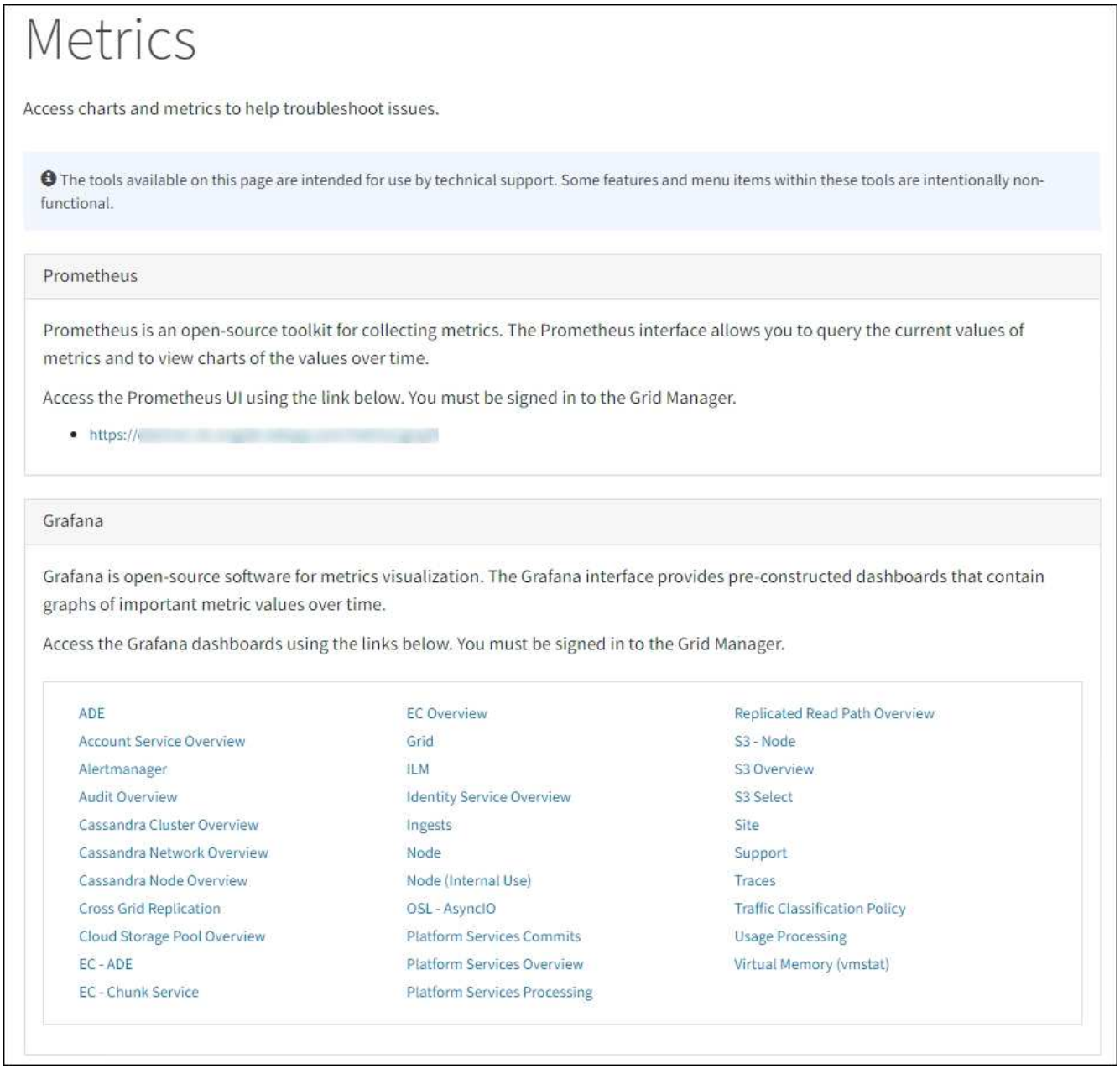
Auf der Seite Metriken können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist Open-Source-Software zum Sammeln von Kennzahlen. Grafana ist Open-Source-Software zur Visualisierung von Kennzahlen.

> 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 unter Anleitung des technischen Supports **SUPPORT** > **Tools** > **Metrics** aus.

   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.

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 mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "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 Werte liegen außerhalb des normalen Bereichs.
- **Achtung**: Ein oder mehrere der Werte liegen deutlich außerhalb des normalen Bereichs.

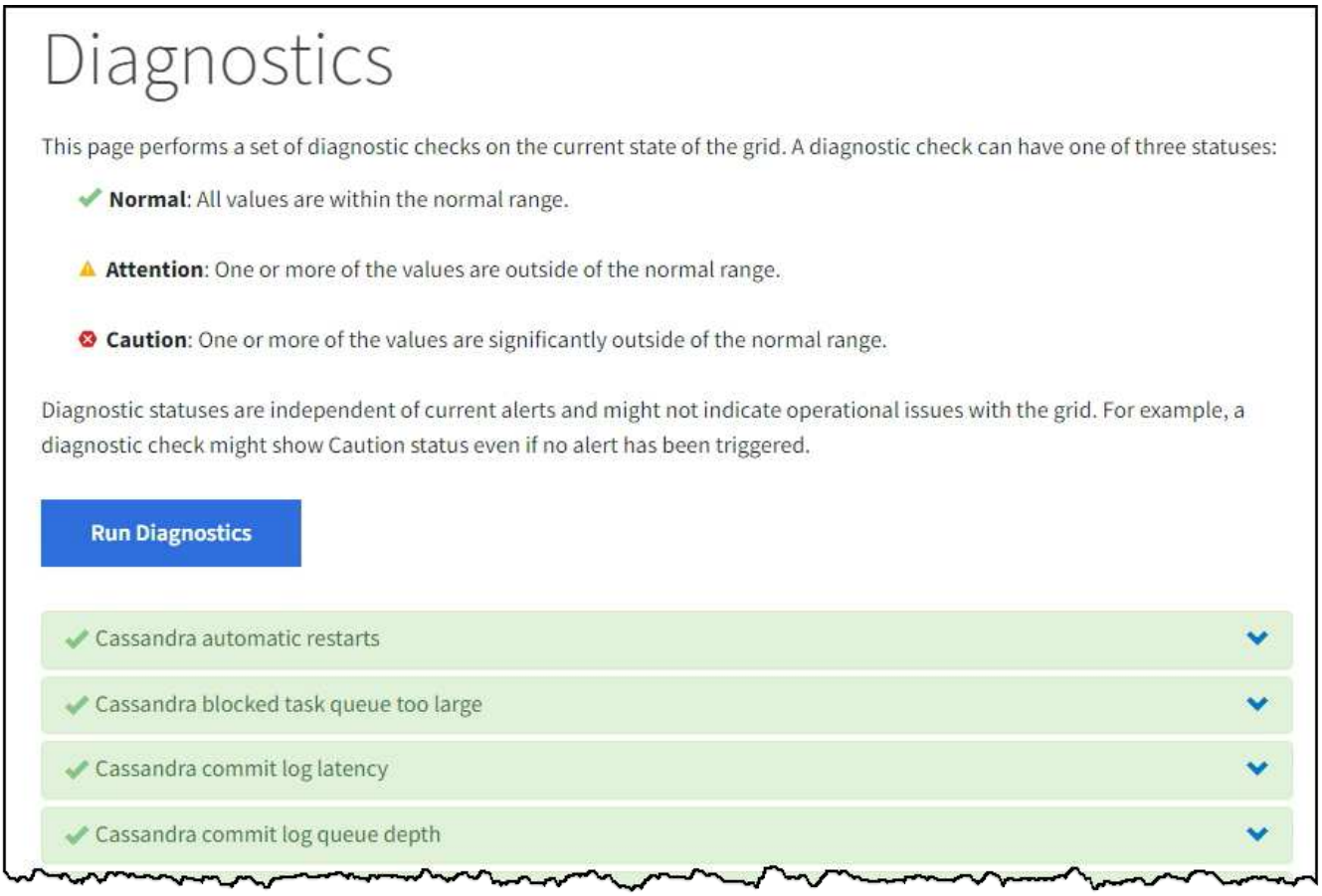
Diagnosestatus sind unabhängig von aktuellen Warnungen und zeigen möglicherweise keine betrieblichen Probleme mit dem Raster an. Beispielsweise wird bei einer Diagnose-Prüfung möglicherweise der Status „Achtung“ angezeigt, auch wenn keine Meldung ausgelöst wurde.

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 haben alle Diagnosen einen normalen Status.



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:

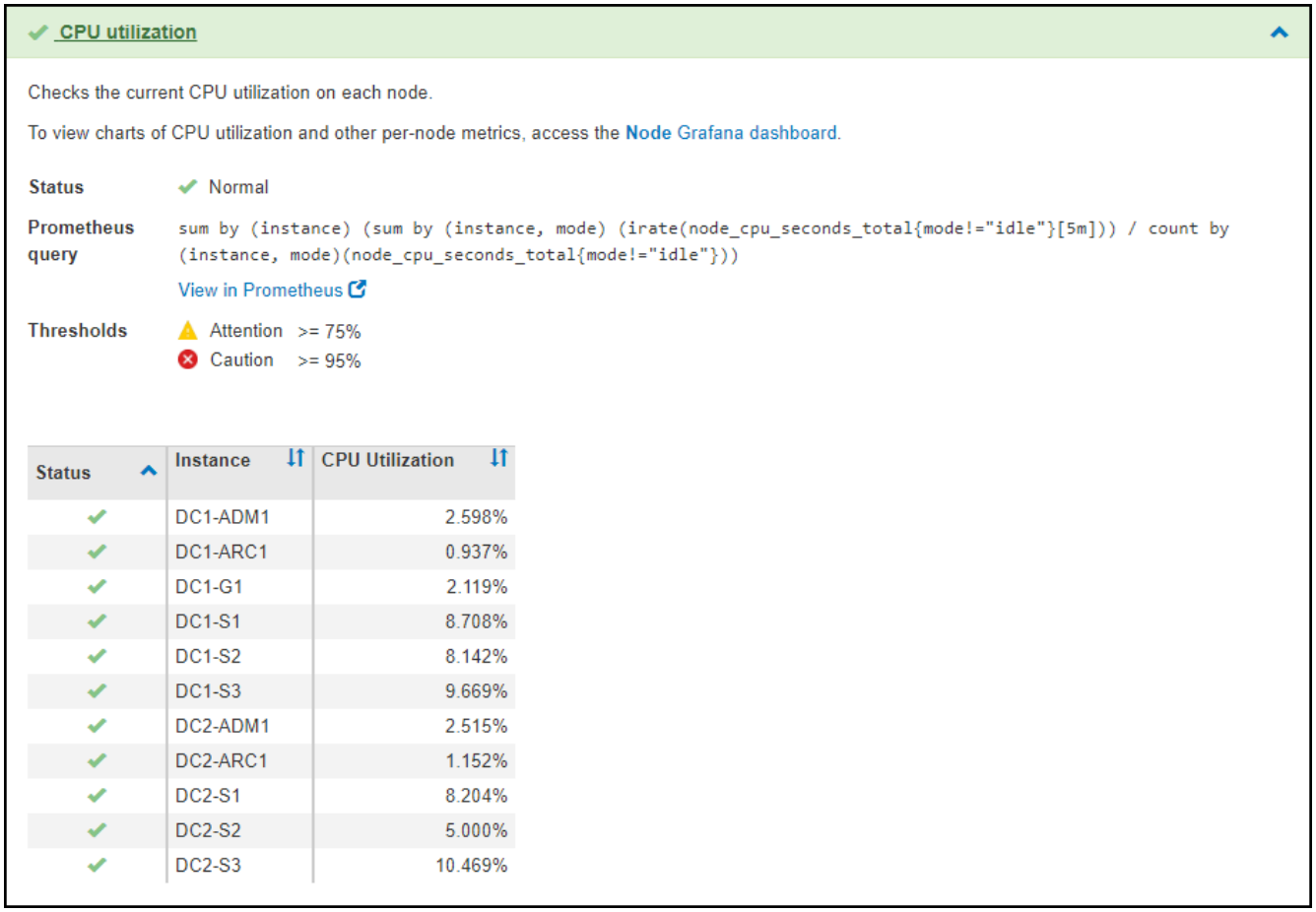
   - **Status**: Der aktuelle Status dieser Diagnose: Normal, Achtung oder Achtung.
   - **Prometheus query**: Bei Verwendung für die Diagnose, der Prometheus Ausdruck, der verwendet

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**: Eine Tabelle, die den Status und den Wert der Diagnose im gesamten StorageGRID-System anzeigt. In diesem Beispiel wird die aktuelle CPU-Auslastung für jeden Node in einem StorageGRID System angezeigt. Alle Node-Werte liegen unter den Warn- und Warnschwellenwerten, sodass der Gesamtstatus der Diagnose normal ist.



3. **Optional**: Um Grafana-Diagramme zu dieser Diagnose anzuzeigen, klicken Sie auf den Link **Grafana Dashboard**.

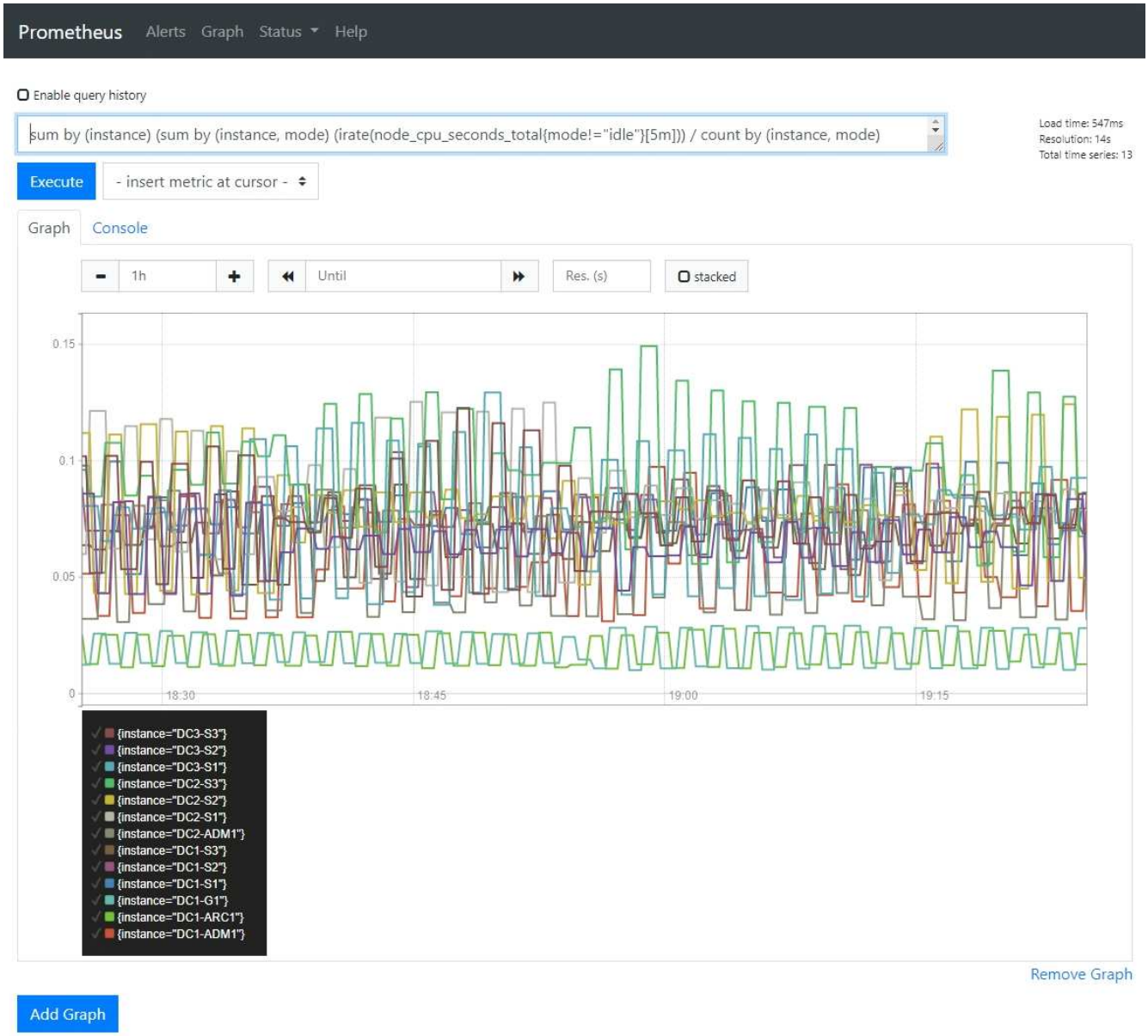
   Dieser Link wird nicht für alle Diagnosen angezeigt.

   Das zugehörige Grafana Dashboard wird angezeigt. In diesem Beispiel wird auf dem Node-Dashboard die CPU-Auslastung für diesen Node und andere Grafana-Diagramme für den Node angezeigt.

   > Sie können auch über den Abschnitt „Grafana“ auf der Seite * SUPPORT* > **Tools** > **Metriken** auf die vorkonfigurierten Dashboards von Grafana 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 © 2025 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.