StorageGRID System überwachen

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-120/monitor/index.html on July 23, 2026. Always check docs.netapp.com for the latest.

Inhalt

StorageGRID System überwachen . . . 1
Ein StorageGRID System überwachen . . . 1
Anzeigen und Verwalten des Dashboards in StorageGRID . . . 1
Dashboard anzeigen . . . 2
Dashboards verwalten . . . 3
Dashboards konfigurieren . . . 4
Seite „Knoten“ . . . 5
Seite „StorageGRID-Knoten“ anzeigen . . . 5
Registerkarte „StorageGRID-Übersicht“ anzeigen . . . 8
Registerkarte „StorageGRID-Hardware“ anzeigen . . . 10
Registerkarte „StorageGRID-Netzwerk“ anzeigen . . . 27
Registerkarte „Storage“ in StorageGRID anzeigen . . . 28
Registerkarte „StorageGRID-Objekte“ anzeigen . . . 30
Die StorageGRID ILM-Registerkarte anzeigen . . . 32
Registerkarte „StorageGRID Load Balancer“ anzeigen . . . 33
Registerkarte „Dienste der StorageGRID-Plattform“ anzeigen . . . 34
Registerkarte „Laufwerke verwalten“ in StorageGRID anzeigen . . . 35
Die Registerkarte StorageGRID SANtricity System Manager anzeigen . . . 36
Informationen zur regelmäßigen Überwachung . . . 38
Was und wann in StorageGRID überwacht werden sollte . . . 38
Systemzustand in StorageGRID überwachen . . . 38
Überwachen Sie die Speicherkapazität in StorageGRID . . . 43
Überwachen Sie das Informationslebenszyklusmanagement in StorageGRID . . . 52
Überwachen Sie Netzwerk- und Systemressourcen in StorageGRID . . . 53
Überwachen Sie die Mieteraktivität in StorageGRID . . . 57
Überwachen Sie S3-Clientvorgänge in StorageGRID . . . 62
Überwachen Sie die Lastverteilungsvorgänge in StorageGRID . . . 63
Überwachen Sie StorageGRID Grid-Federation-Verbindungen . . . 65
Benachrichtigungen verwalten . . . 69
Warnmeldungen in StorageGRID verwalten . . . 69
StorageGRID-Alarmregeln anzeigen . . . 69
Erstellen Sie benutzerdefinierte Alarmregeln in StorageGRID . . . 71
Alarmregeln in StorageGRID bearbeiten . . . 74
Warnregeln in StorageGRID deaktivieren . . . 78
Benutzerdefinierte Alarmregeln in StorageGRID entfernen . . . 79
Benachrichtigungen verwalten . . . 79
Warnungen in StorageGRID . . . 88
Häufig verwendete Prometheus-Metriken in StorageGRID . . . 102
Referenz zu Protokolldateien . . . 108
StorageGRID-Protokolldateien . . . 108
StorageGRID Softwareprotokolle . . . 111
Bereitstellungs- und Wartungsprotokolle in StorageGRID . . . 118
Erfahren Sie mehr über die StorageGRID bycast.log . . . 119

Logverwaltung und externen Syslog-Server konfigurieren . . . 127
Externe Syslog-Server in StorageGRID . . . 127
Protokollverwaltung in StorageGRID konfigurieren . . . 133
SNMP Überwachung . . . 143
Verwenden Sie die SNMP-Überwachung in StorageGRID . . . 143
Konfigurieren Sie den SNMP-Agent in StorageGRID . . . 145
Aktualisieren Sie den StorageGRID SNMP-Agenten . . . 152
Auf StorageGRID MIB-Dateien zugreifen . . . 154
Zusätzliche StorageGRID Daten sammeln . . . 156
Überwachen Sie die PUT- und GET-Leistung in StorageGRID . . . 156
Überwachen Sie Objektverifizierungsoperationen in StorageGRID . . . 156
StorageGRID-Auditmeldungen prüfen . . . 159
Sammeln Sie StorageGRID-Protokolldateien und Systemdaten . . . 160
Ein StorageGRID AutoSupport Paket manuell auslösen . . . 162
Überprüfen Sie die StorageGRID-Support-Metriken . . . 162
Ändern Sie die E/A-Priorisierung in StorageGRID . . . 164
Führen Sie Diagnose in StorageGRID aus . . . 165
Erstellen Sie benutzerdefinierte Überwachungsanwendungen für StorageGRID . . . 169

StorageGRID System überwachen

Ein StorageGRID System überwachen

Das StorageGRID System sollte regelmäßig überwacht werden, damit die erwartete Leistung sichergestellt ist.

Bevor Sie beginnen

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

> Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, das Benutzer-Drop-down-Menü oben rechts im Grid Manager auswählen und anschließend **Benutzereinstellungen** wählen.

Über diese Aufgabe

Diese Anleitung beschreibt, wie Folgendes durchgeführt wird:

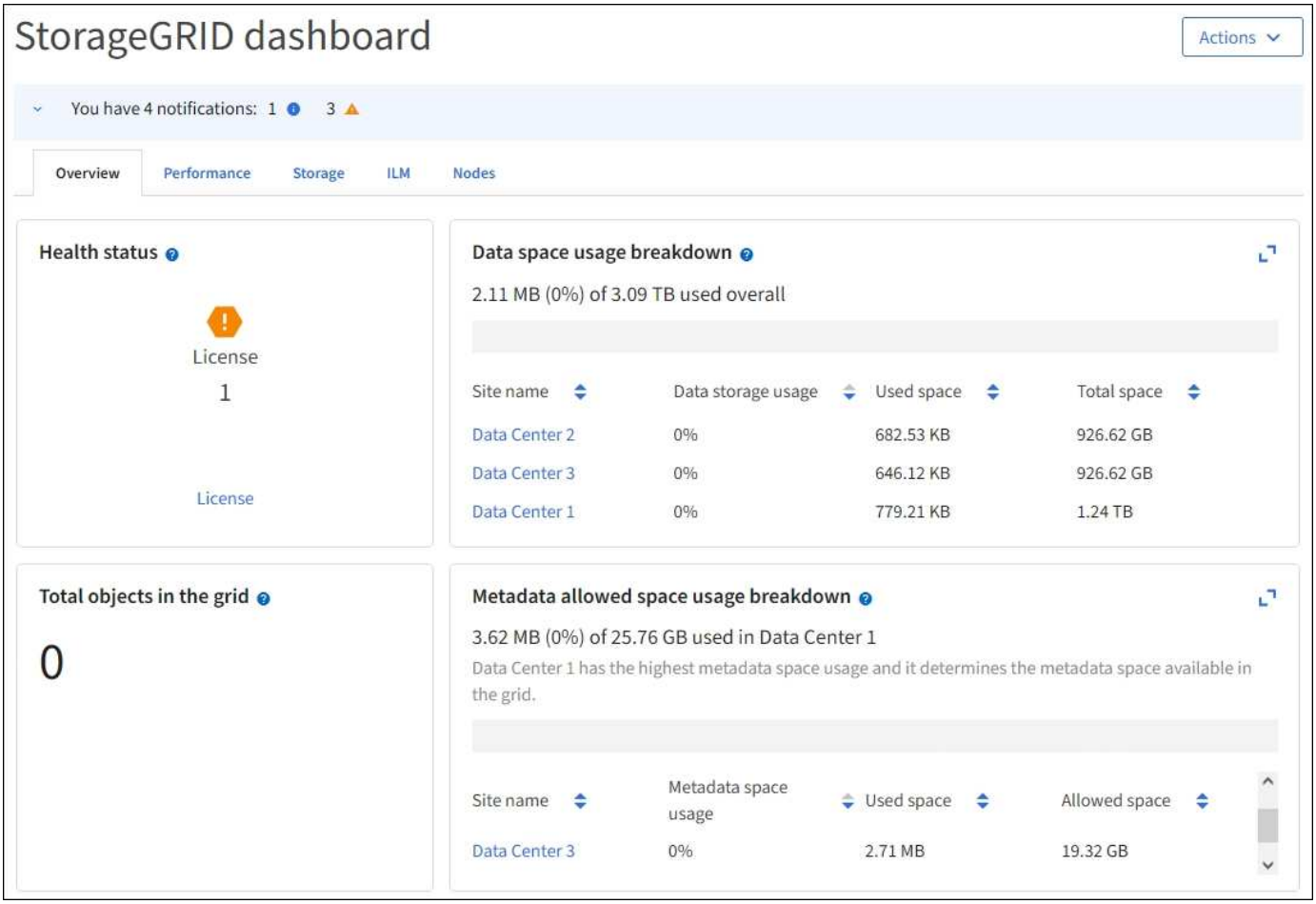
- "Dashboard anzeigen und verwalten"
- "Seite „Knoten“"
- "Diese Aspekte des Systems sollten regelmäßig überwacht werden:"
  - "Systemgesundheit"
  - "Speicherkapazität"
  - "Informationslebenszyklusmanagement"
  - "Netzwerk und Systemressourcen"
  - "Mandantenaktivität"
  - "Lastverteilungsoperationen"
  - "Grid Federation Verbindungen"
- "Benachrichtigungen verwalten"
- "Protokolldateien anzeigen"
- "Logverwaltung und externen Syslog-Server konfigurieren"
- "Einen externen Syslog Server verwenden" zum Sammeln von Prüfungsinformationen
- "SNMP für die Überwachung verwenden"
- "Änderung der I/O-Priorisierung"die relativen Prioritäten für E/A-Operationen zu ändern

Anzeigen und Verwalten des Dashboards in StorageGRID

Mithilfe des Dashboards können Sie Systemaktivitäten auf einen Blick überwachen. Es besteht die Möglichkeit, benutzerdefinierte Dashboards zu erstellen, um die eigene StorageGRID Implementierung zu überwachen.

Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, das Benutzer-Drop-down-Menü oben rechts im Grid Manager auswählen und anschließend **Benutzereinstellungen** wählen.

Ihr Dashboard kann je nach Systemkonfiguration unterschiedlich sein.



Dashboard anzeigen

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

Sie können das systemseitig bereitgestellte Dashboard unverändert verwenden. Zusätzlich ist es möglich, benutzerdefinierte Dashboards zu erstellen, die nur die Registerkarten und Karten enthalten, die für die Überwachung Ihrer StorageGRID Implementierung relevant sind.

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

Registerkarte auf dem vom System bereitgestellten Dashboard	Enthält
Überblick	Allgemeine Informationen über das Grid, wie aktive Warnmeldungen, Speichernutzung und die Gesamtzahl der Objekte im Grid.

Registerkarte auf dem vom System bereitgestellten Dashboard	Enthält
Performance	Speicherplatznutzung, Speicherverbrauch im Zeitverlauf, S3-Operationen, Anfragedauer, Fehlerrate.
Storage	Nutzung von Mandantenkontingenten und logischem Speicherplatz. Prognosen zur Speicherplatznutzung für Benutzerdaten und Metadaten.
ILM	Informationslebenszyklusmanagement Warteschlange und Auswertungsrate.
Nodes	CPU-, Daten- und Speichernutzung pro Knoten. S3-Operationen pro Knoten. Verteilung der Knoten auf die Standorte.

Einige Karten können zur besseren Ansicht maximiert werden. Das Maximieren-Symbol befindet sich in der oberen rechten Ecke der Karte. Zum Schließen einer maximierten Karte kann das Minimieren-Symbol oder **Schließen** ausgewählt werden.

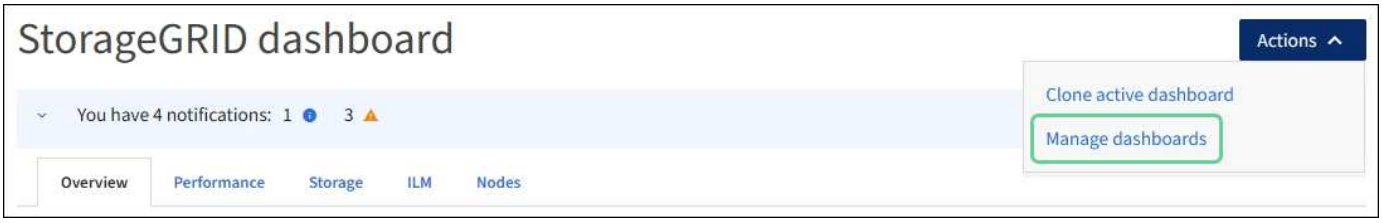
Dashboards verwalten

Wenn Sie über Root-Zugriff verfügen (siehe "Administratorgruppenberechtigungen"), stehen Ihnen die folgenden Verwaltungsaufgaben für Dashboards zur Verfügung:

- Ein benutzerdefiniertes Dashboard kann von Grund auf neu erstellt werden. Mit benutzerdefinierten Dashboards lässt sich steuern, welche StorageGRID Informationen angezeigt werden und wie diese Informationen organisiert sind.
- Ein Dashboard kann geklont werden, um benutzerdefinierte Dashboards zu erstellen.
- Ein aktives Dashboard für einen Benutzer festlegen. Das aktive Dashboard kann das vom System bereitgestellte Dashboard oder ein benutzerdefiniertes Dashboard sein.
- Ein Standard-Dashboard wird festgelegt, das allen Benutzern angezeigt wird, sofern sie nicht ihr eigenes Dashboard aktivieren.
- Einen Dashboard-Namen bearbeiten.
- Ein Dashboard kann bearbeitet werden, um Tabs und Karten hinzuzufügen oder zu entfernen. Es sind mindestens 1 und maximal 20 Tabs möglich.
- Ein Dashboard entfernen.

> Wenn Sie über eine andere Berechtigung als Root-Zugriff verfügen, kann nur ein aktives Dashboard festgelegt werden.

Zum Verwalten von Dashboards **Aktionen** > **Dashboards verwalten** auswählen.



Dashboards konfigurieren

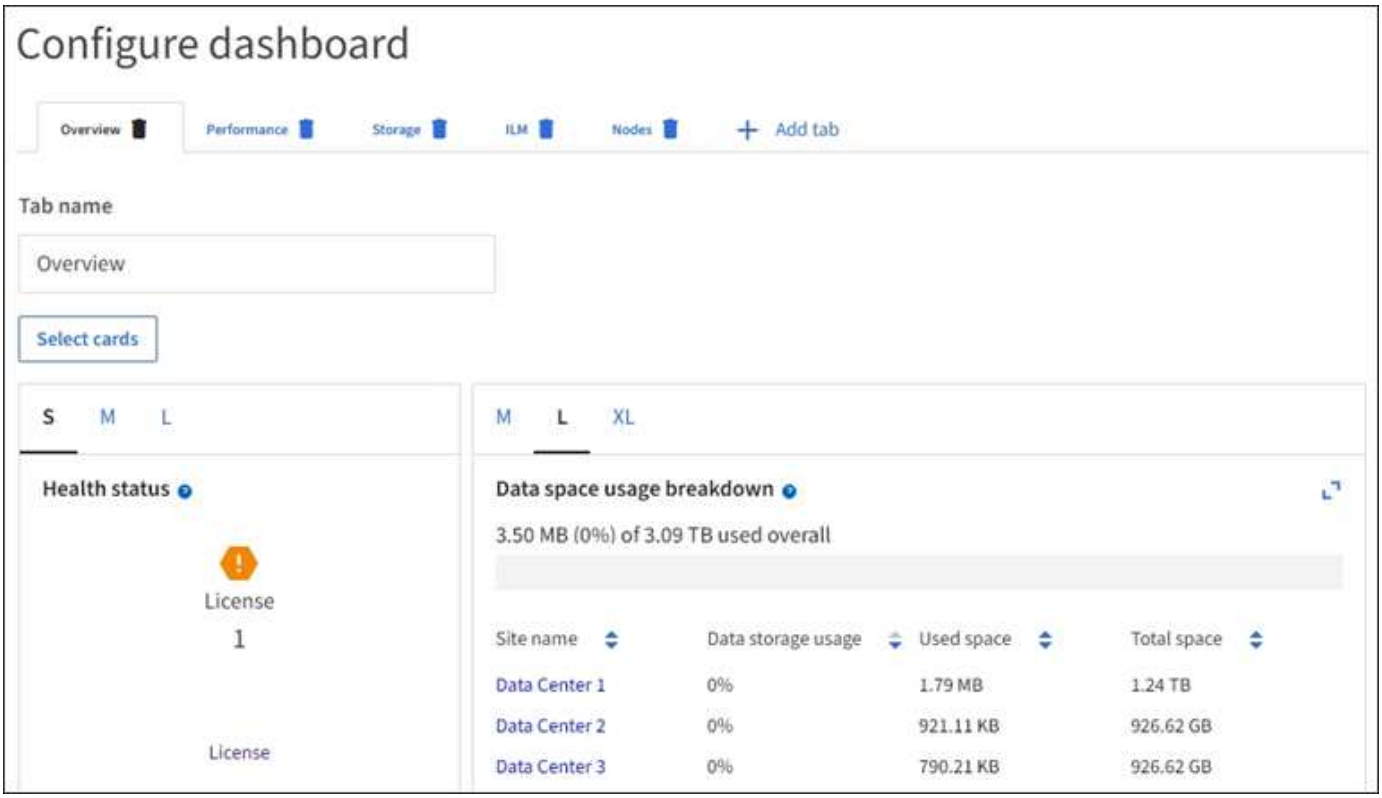
Ein neues Dashboard kann durch Klonen des aktiven Dashboards erstellt werden, indem **Aktionen** > **Aktives Dashboard klonen** ausgewählt wird.

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

Das vom System bereitgestellte Dashboard kann weder bearbeitet noch entfernt werden.

Bei der Konfiguration eines Dashboards können Sie:

- Tabs hinzufügen oder entfernen
- Tabs umbenennen und neuen Tabs eindeutige Namen zuweisen
- Karten für jede Registerkarte hinzufügen, entfernen oder neu anordnen (ziehen).
- Die Größe der einzelnen Karten kann oben auf der Karte durch Auswahl von **S**, **M**, **L** oder **XL** festgelegt werden.



Seite „Knoten“

Seite „StorageGRID-Knoten“ anzeigen

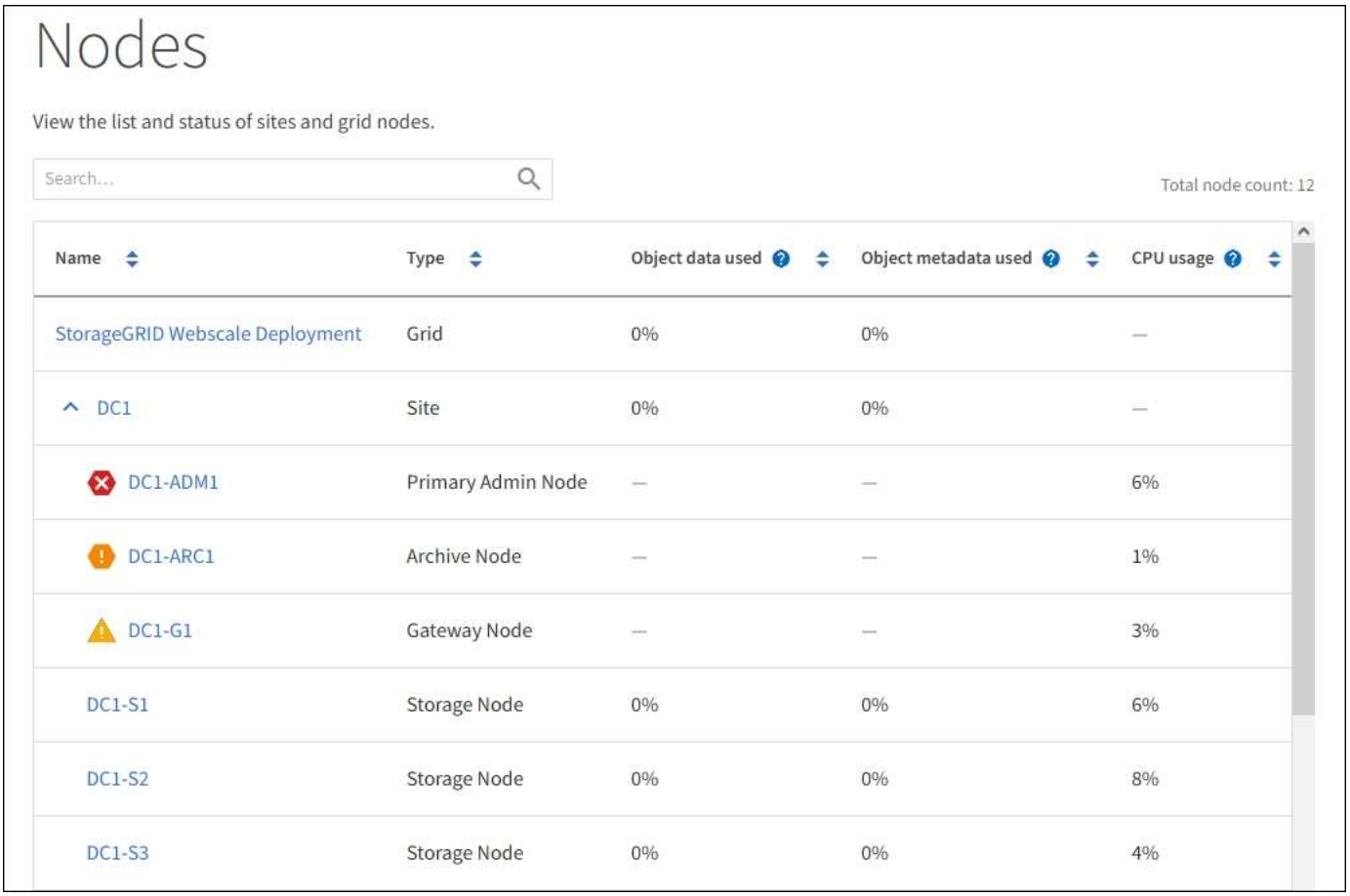
Wenn detailliertere Informationen über Ihr StorageGRID System benötigt werden, als das Dashboard bietet, kann auf der Seite „Nodes“ Metriken für das gesamte Grid, jeden Standort im Grid und jeden Node an einem Standort angezeigt werden.

Die Knotentabelle enthält zusammenfassende Informationen für das gesamte Grid, jeden Standort und jeden Knoten. Wenn ein Knoten nicht verbunden ist oder eine aktive Warnung vorliegt, erscheint ein Symbol neben dem Node-Name. Wenn der Knoten verbunden ist und keine aktiven Warnungen vorliegen, wird kein Symbol angezeigt.

> Wenn ein Knoten nicht mit dem Grid verbunden ist, beispielsweise während eines Upgrades oder im getrennten Zustand, sind bestimmte Messwerte möglicherweise nicht verfügbar oder werden in den Standort- und Grid-Gesamtwerten nicht berücksichtigt. Nach der Wiederherstellung der Verbindung eines Knotens mit dem Grid dauert es einige Minuten, bis sich die Werte stabilisieren.

> Um die Einheiten für die im Grid Manager angezeigten Speicherwerte zu ändern, das Benutzer-Drop-down-Menü oben rechts im Grid Manager auswählen und anschließend **Benutzereinstellungen** wählen.

> Die gezeigten Screenshots sind Beispiele. Ihre Ergebnisse können je nach StorageGRID Version abweichen.



Verbindungsstatussymbole

Wenn ein Node vom Grid getrennt ist, erscheint eines der folgenden Symbole neben dem Node-Name.

Symbol	Beschreibung	Aktion erforderlich
	Nicht verbunden - Unbekannt Aus unbekannten Gründen ist ein Knoten getrennt oder Dienste auf dem Knoten sind unerwartet ausgefallen. Beispielsweise könnte ein Dienst auf dem Knoten beendet worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Unterbrechung seine Netzwerkverbindung verloren haben. Die Warnung **Unable to communicate with node** kann ebenfalls ausgelöst werden. Andere Warnungen können ebenfalls aktiv sein.	Erfordert sofortige Aufmerksamkeit. "Jede Benachrichtigung auswählen" und den empfohlenen Maßnahmen folgen. Beispielsweise kann es erforderlich sein, einen Dienst neu zu starten, der angehalten wurde, oder den Host für den Knoten neu zu starten. **Hinweis**: Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. Der Status „Unbekannt“ kann in diesen Fällen ignoriert werden.

Symbol	Beschreibung	Aktion erforderlich
	Nicht verbunden - Administrativ deaktiviert Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden. Beispielsweise wurde der Knoten oder die darauf laufenden Dienste ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Eine oder mehrere Warnmeldungen könnten ebenfalls aktiv sein. Basierend auf dem zugrunde liegenden Problem gehen diese Nodes häufig ohne Eingreifen wieder online.	Es wird geprüft, ob Warnmeldungen diesen Knoten betreffen. Wenn eine oder mehrere Warnungen aktiv sind, "Jede Benachrichtigung auswählen" und die empfohlenen Maßnahmen befolgt werden.

Wenn ein Node vom Grid getrennt ist, kann eine zugrunde liegende Warnung vorliegen, aber es wird nur das Symbol „Nicht verbunden“ angezeigt. Die aktiven Warnungen für einen Node werden angezeigt, wenn der Node ausgewählt wird.

Warnsymbole

Wenn für einen Node-Name eine aktive Warnung vorliegt, wird eines der folgenden Symbole neben dem Node-Name angezeigt:

Kritisch: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder Dienstes gestoppt hat. Das zugrunde liegende Problem muss umgehend behoben werden. Kommt es zu keiner Lösung, können Dienstunterbrechungen und Datenverlust die Folge sein.

Schwerwiegend: Es liegt ein anormaler Zustand vor, der entweder den laufenden Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Es empfiehlt sich, schwerwiegende Warnungen zu untersuchen und zugrunde liegende Probleme zu beheben, damit der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder Dienstes nicht unterbricht.

Geringfügig: Das System funktioniert normal, es besteht jedoch eine Störung, die die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn sie anhält. Geringfügige Warnmeldungen, die nicht von selbst verschwinden, sollten überwacht und behoben werden, damit daraus kein schwerwiegenderes Problem entsteht.

Details zu einem System, Standort oder Node anzeigen

Um die in der Knotentabelle angezeigten Informationen zu filtern, eine Suchzeichenfolge im Feld **Suchen** eingeben. Eine Suche ist nach Systemnamen, Anzeigenamen oder Typ möglich (zum Beispiel **gat** eingeben, um schnell alle Gateway Nodes zu finden).

Informationen für das Grid, den Standort oder den Node anzeigen:

- Der Grid-Name zeigt eine zusammenfassende Übersicht der Statistiken für das gesamte StorageGRID System.

- Ein bestimmter Rechenzentrumsstandort kann ausgewählt werden, um eine zusammenfassende Übersicht der Statistiken für alle Nodes an diesem Standort zu sehen.
- Ein bestimmter Node kann ausgewählt werden, um detaillierte Informationen zu diesem Node anzuzeigen.

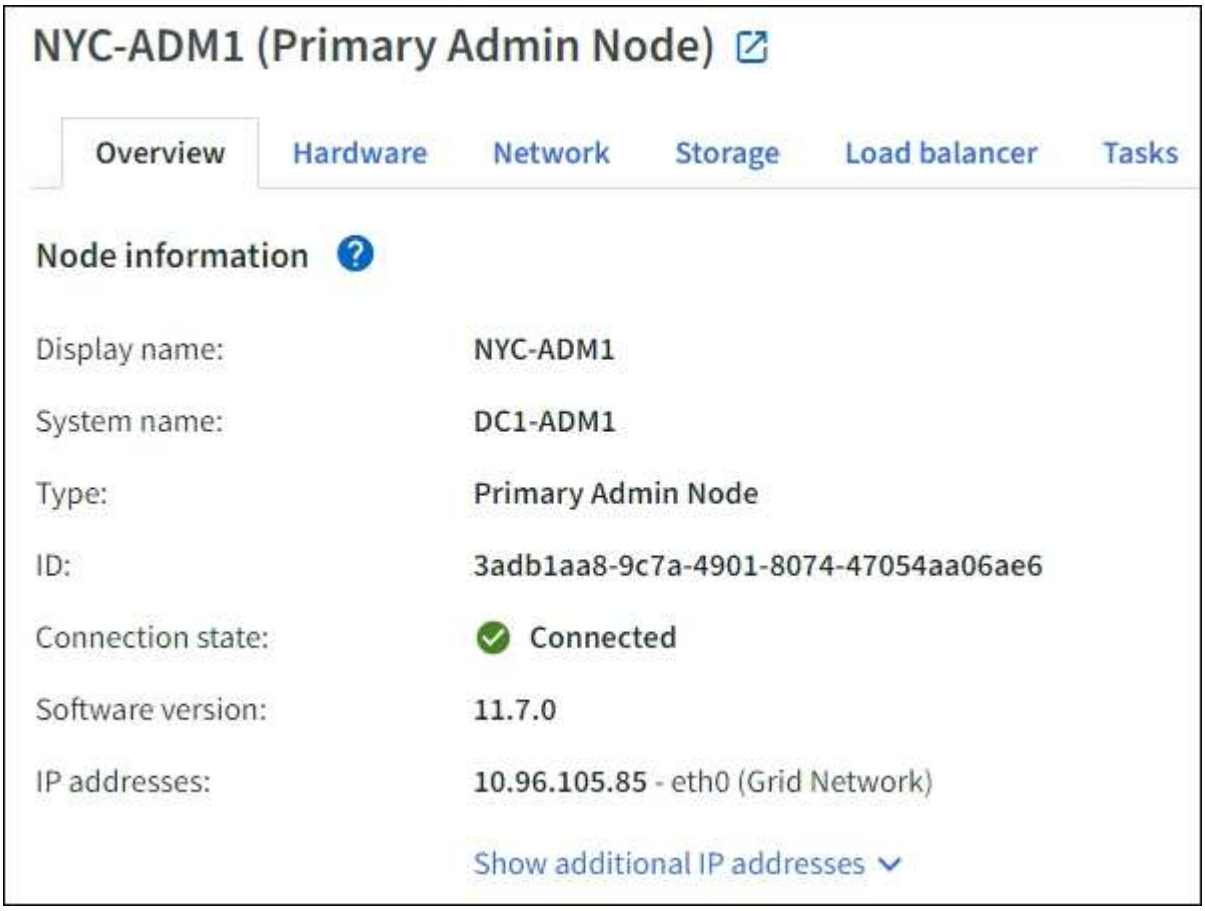
Registerkarte „StorageGRID-Übersicht“ anzeigen

Die Registerkarte „Übersicht“ bietet grundlegende Informationen zu jedem Node. Zudem werden dort alle aktuell den Node betreffenden Warnmeldungen angezeigt.

Die Registerkarte „Übersicht“ wird für alle Nodes angezeigt.

Knoteninformationen

Der Abschnitt „Knoteninformationen“ auf der Registerkarte „Übersicht“ enthält grundlegende Informationen über den Node.



Die Übersichtsinformationen für einen Node umfassen Folgendes:

- **Anzeigename** (wird nur angezeigt, wenn der Node-Name umbenannt wurde): Der aktuelle Anzeigename für den Node-Name. Die "Grid, Standorte und Knoten umbenennen"-Prozedur kann verwendet werden, um diesen Wert zu aktualisieren.
- **Systemname**: Der Name, den Sie während der Installation für den Node eingegeben haben. Systemnamen werden für interne StorageGRID Operationen verwendet und können nicht geändert werden.
- **Typ**: Der Knotentyp (Admin Node, primärer Admin Node, Storage Node oder Gateway Node).

- **ID**: Die eindeutige Kennung für den Node, die auch als UUID bezeichnet wird.
- **Verbindungsstatus**: Einer von drei Zuständen. Das Symbol für den schwerwiegendsten Zustand wird angezeigt.
  - **Unbekannt**: Aus unbekanntem Grund ist der Node nicht mit dem Grid verbunden oder ein oder mehrere Services sind unerwartet ausgefallen. Beispielsweise wurde die Netzwerkverbindung zwischen Nodes unterbrochen, die Stromversorgung ist ausgefallen oder ein Service ist ausgefallen. Die Warnung **Unable to communicate with node** kann ebenfalls ausgelöst werden. Weitere Warnungen können ebenfalls aktiv sein. In dieser Situation ist sofortige Aufmerksamkeit erforderlich.

    > Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. In diesen Fällen kann der Status „Unbekannt“ ignoriert werden.

  - **Administrativ nicht verfügbar**: Der Knoten ist aus einem erwarteten Grund nicht mit dem Grid verbunden. Beispielsweise wurde der Knoten oder die darauf laufenden Dienste ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Eine oder mehrere Warnmeldungen könnten ebenfalls aktiv sein.
  - **Verbunden**: Der Knoten ist mit dem Netz verbunden.
- **Verwendeter Speicher**: Nur für Storage Nodes.
  - **Objektdaten**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der auf dem Storage Node verwendet wurde.
  - **Objektmetadaten**: Der Prozentsatz des insgesamt für Objektmetadaten zulässigen Speicherplatzes, der auf dem Storage Node verwendet wurde.
- **Softwareversion**: Die Version von StorageGRID, die auf dem Node installiert ist.
- **HA groups**: Nur für Admin Node und Gateway Nodes. Wird angezeigt, wenn eine Netzwerkschnittstelle des Node in einer High Availability Group enthalten ist und ob diese Schnittstelle die Primary Schnittstelle ist.
- **IP-Adressen**: Die IP-Adressen des Knotens. **Weitere IP-Adressen anzeigen** zeigt die IPv4- und IPv6-Adressen sowie die Schnittstellenzuordnungen des Knotens an.

Warnmeldungen

Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle "Warnmeldungen, die diesen Node aktuell betreffen und noch nicht stummgeschaltet wurden" aufgelistet. Der Warnungsname kann ausgewählt werden, um weitere Details und empfohlene Maßnahmen anzuzeigen.

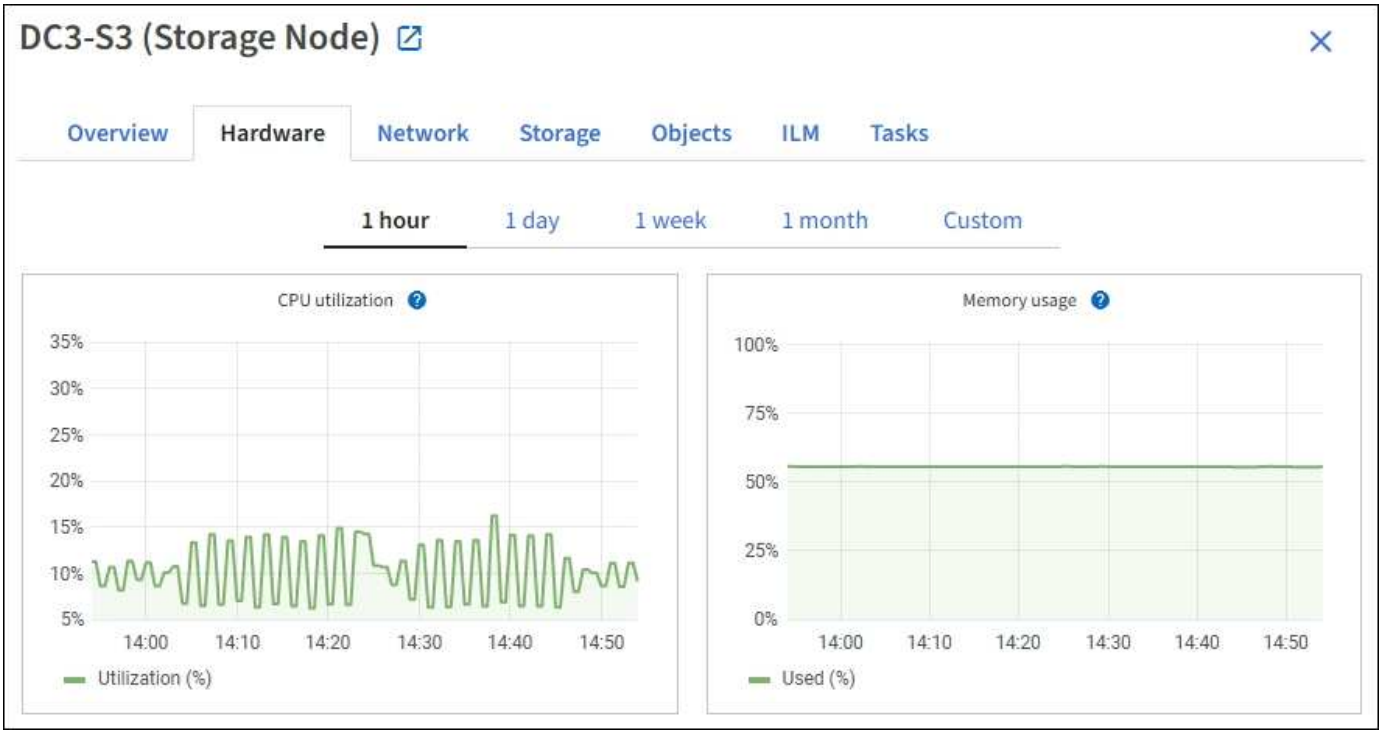
Warnmeldungen sind ebenfalls enthalten für "Knotenverbindungszustände".

Registerkarte „StorageGRID-Hardware“ anzeigen

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

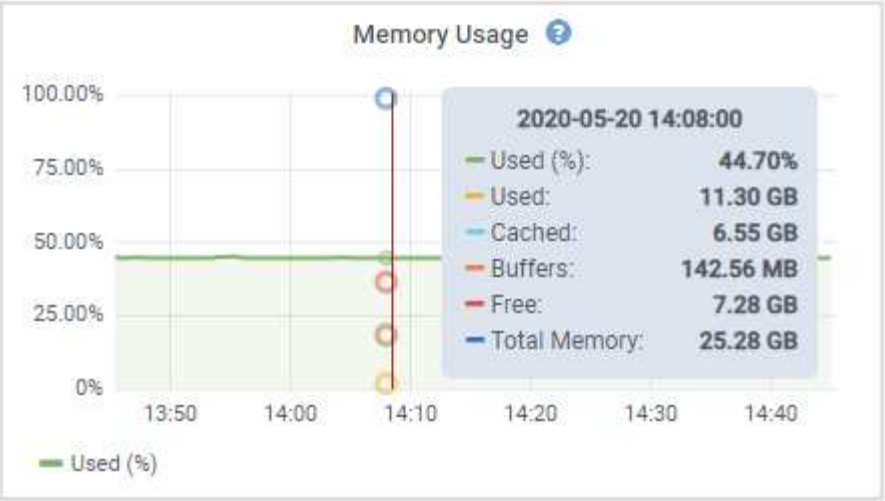
> Der Grid Manager wird mit jeder neuen Version aktualisiert und entspricht möglicherweise nicht den Beispiel-Screenshots auf dieser Seite.

Die Registerkarte „Hardware“ wird für alle Knoten angezeigt.



Um ein anderes Zeitintervall anzuzeigen, kann eines der Steuerelemente oberhalb des Diagramms oder der Grafik ausgewählt werden. Die verfügbaren Informationen können für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat angezeigt werden. Auch ein benutzerdefiniertes Intervall ist möglich, wodurch Datums- und Zeitbereiche angegeben werden können.

Details zur CPU-Auslastung und Speichernutzung werden angezeigt, wenn der Mauszeiger über die jeweiligen Diagramme positioniert wird.



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

Informationen zu Appliance Storage Nodes anzeigen

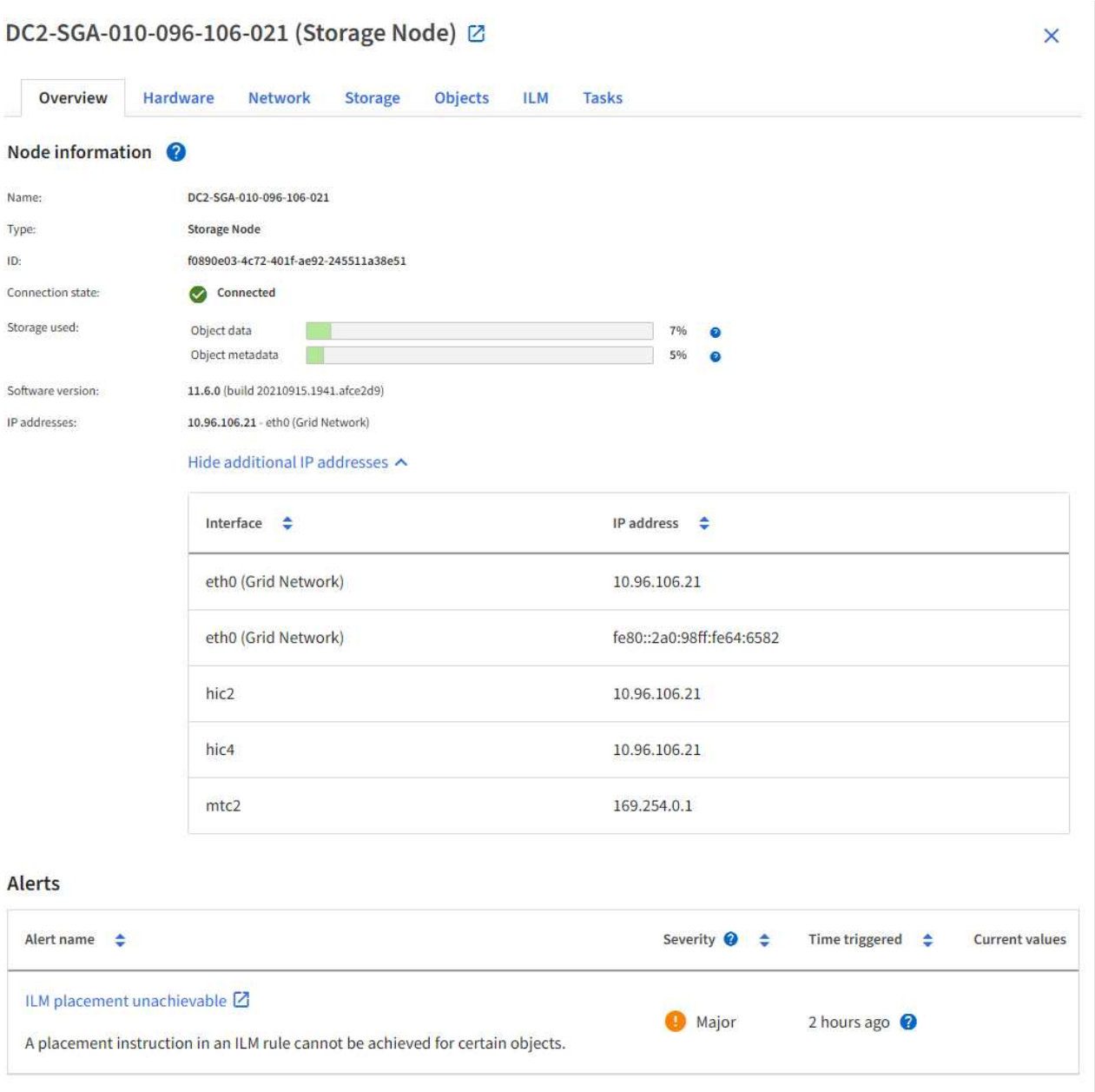
Die Seite „Knoten“ listet Informationen zum Dienststatus sowie zu allen Rechen-, Festplatten- und Netzwerkressourcen jedes Appliance Storage Node auf. Außerdem werden Arbeitsspeicher, Speicherhardware, Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen sowie empfangene und gesendete Daten angezeigt.

Schritte

1. Auf der Seite „Knoten“ einen Appliance-Speicherknoten auswählen.
2. **Übersicht** auswählen.

   Der Abschnitt „Knoteninformationen“ auf der Registerkarte „Übersicht“ zeigt zusammenfassende Informationen zum Knoten an, wie Name, Typ, ID und Verbindungsstatus. Die Liste der IP-Adressen enthält für jede Adresse den Namen der Schnittstelle, wie folgt:

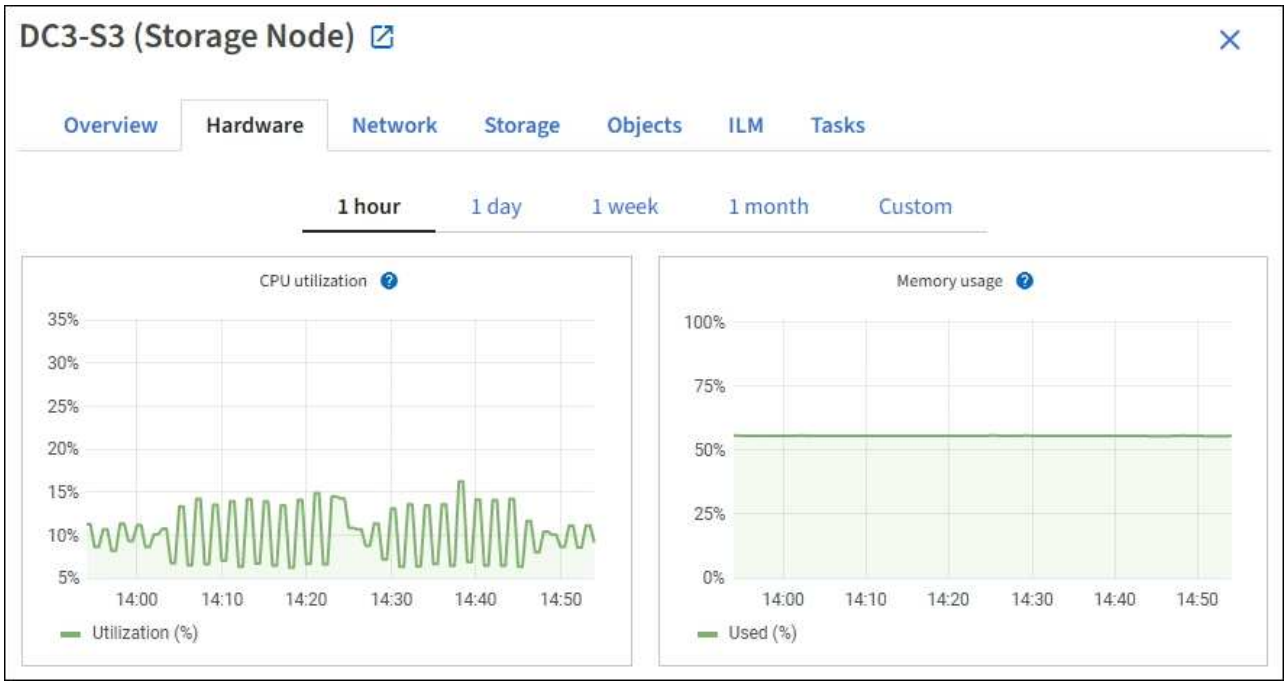
   - **eth**: Das Grid Network, Admin Network oder Client Network.
   - **hic**: Einer der physischen 10, 25 oder 100 GbE Ports des Geräts. Diese Ports können gebündelt und mit dem StorageGRID Grid Network (eth0) und dem Client Network (eth2) verbunden werden.
   - **mtc**: Einer der physischen 1 GbE Ports des Geräts. Eine oder mehrere mtc Schnittstellen werden gebündelt, um die StorageGRID Admin Network Schnittstelle (eth1) zu bilden. Weitere mtc Schnittstellen können für die temporäre lokale Verbindung eines Technikers im Rechenzentrum verfügbar bleiben.



Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ sind alle aktiven Warnungen für den Knoten aufgeführt.

3. **Hardware** auswählen, um weitere Informationen zum Gerät zu sehen.

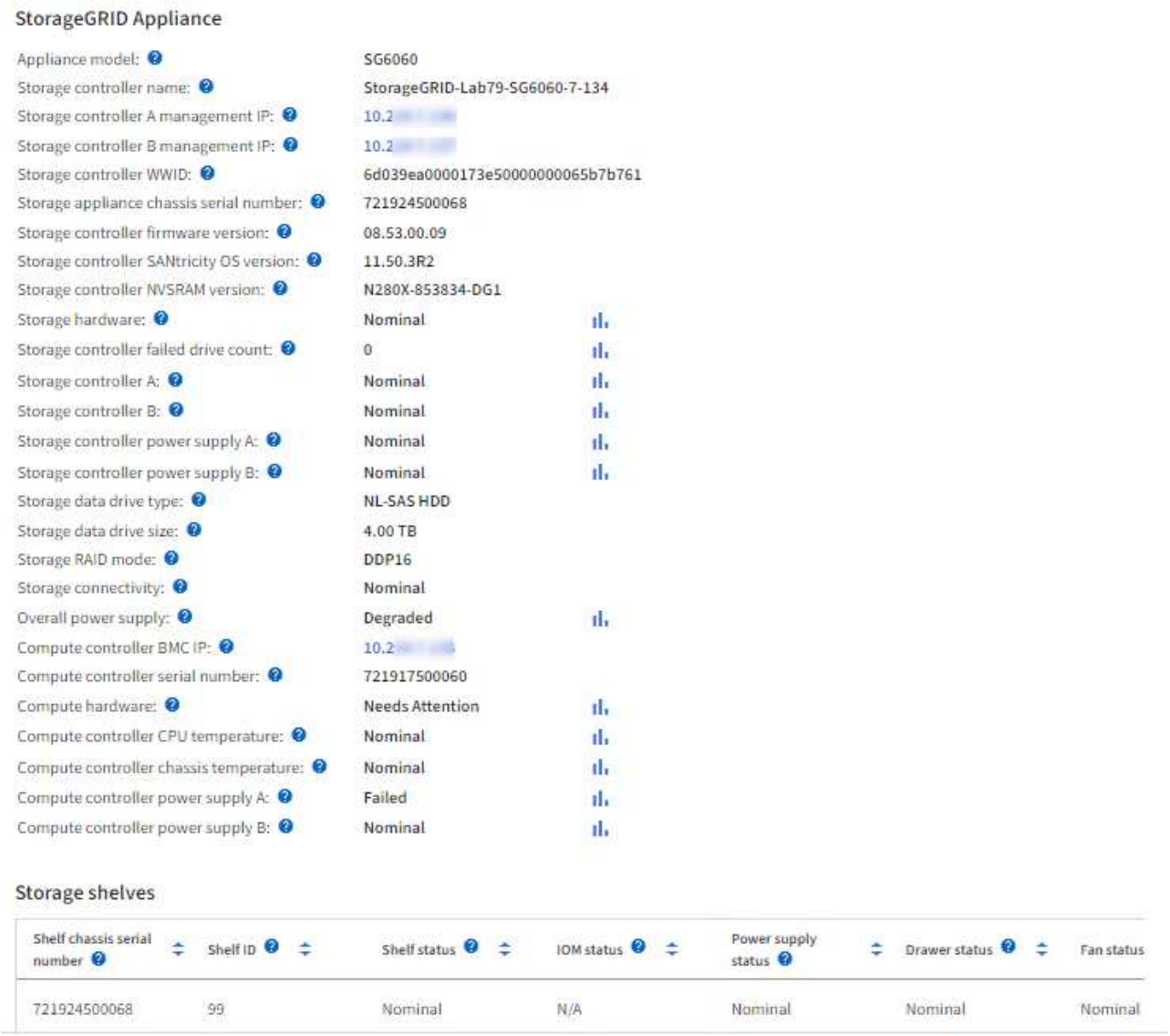
   a. Die Diagramme zur CPU-Auslastung und zum Speicher zeigen die prozentualen Werte der CPU- und Speichernutzung im Zeitverlauf. Zur Anzeige eines anderen Zeitintervalls steht eines der Steuerelemente oberhalb des Diagramms oder der Grafik zur Auswahl. Die verfügbaren Informationen können für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat angezeigt werden. Ein benutzerdefiniertes Intervall ermöglicht die Angabe von Datums- und Zeitbereichen.



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

> Einige Felder, wie Compute Controller BMC IP und Compute Hardware, erscheinen nur bei Appliances mit dieser Funktion.

Die Komponenten für die Storage Shelves und, falls sie Teil der Installation sind, die Expansion Shelves erscheinen in einer separaten Tabelle unterhalb der Appliance-Tabelle.



StorageGRID Appliance

Appliance model:	SG6060
Storage controller name:	StorageGRID-Lab79-SG6060-7-134
Storage controller A management IP:	10.2
Storage controller B management IP:	10.2
Storage controller WWID:	6d039ea0000173e50000000065b7b761
Storage appliance chassis serial number:	721924500068
Storage controller firmware version:	08.53.00.09
Storage controller SANtricity OS version:	11.50.3R2
Storage controller NVSRAM version:	N280X-853834-DG1
Storage hardware:	Nominal
Storage controller failed drive count:	0
Storage controller A:	Nominal
Storage controller B:	Nominal
Storage controller power supply A:	Nominal
Storage controller power supply B:	Nominal
Storage data drive type:	NL-SAS HDD
Storage data drive size:	4.00 TB
Storage RAID mode:	DDP16
Storage connectivity:	Nominal
Overall power supply:	Degraded
Compute controller BMC IP:	10.2
Compute controller serial number:	721917500060
Compute hardware:	Needs Attention
Compute controller CPU temperature:	Nominal
Compute controller chassis temperature:	Nominal
Compute controller power supply A:	Failed
Compute controller power supply B:	Nominal

Storage shelves

Shelf chassis serial number	Shelf ID	Shelf status	IOM status	Power supply status	Drawer status	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

Feld in der Appliance-Tabelle	Beschreibung
Gerätemodell	Die Modellnummer für dieses StorageGRID Gerät ist in SANtricity OS angegeben.
Name des Storage Controllers	Der Name für diese StorageGRID Appliance, wie er in SANtricity OS angezeigt wird.
Speichercontroller A Management-IP	IP-Adresse für Management-Port 1 auf dem Storage-Controller A. Diese IP-Adresse wird verwendet, um auf SANtricity OS zuzugreifen und Speicherprobleme zu beheben.
Management-IP-Adresse für Storage Controller B	IP-Adresse für Management-Port 1 auf dem Speicherkontroller B. Diese IP-Adresse wird verwendet, um auf SANtricity OS zuzugreifen und Speicherprobleme zu beheben. Einige Gerätemodelle verfügen nicht über einen Speichercontroller B.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Controller WWID	Die weltweite Kennung des Storage Controllers, die in SANtricity OS angezeigt wird.
Seriennummer des Gehäuses des Storage Appliance	Die Seriennummer des Chassis des Geräts.
Firmware-Version des Storage Controllers	Die Version der Firmware auf dem Speicherkontroller für dieses Gerät.
Speicherkontroller SANtricity OS Version	Die SANtricity OS Version des Speicherkontrollers A.
Speicherkontroller NVSRAM Version	NVSRAM Version des Speicherkontrollers, wie vom SANtricity System Manager gemeldet. Für die SG6060 und SG6160 wird bei einer NVSRAM-Versionsabweichung zwischen den beiden Controllern die Version von Controller A angezeigt. Wenn Controller A nicht installiert oder betriebsbereit ist, wird die Version von Controller B angezeigt.
Speicherhardware	Der Gesamtstatus der Storage Controller-Hardware. Wenn SANtricity System Manager für die Speicherhardware den Status „Achtung erforderlich“ meldet, meldet auch das StorageGRID System diesen Wert. Wenn der Status „Achtung erforderlich“ lautet, sollte zunächst der Speichercontroller mit SANtricity OS überprüft werden. Anschließend ist sicherzustellen, dass keine weiteren Warnmeldungen vorliegen, die den Compute Controller betreffen.
Anzahl der ausgefallenen Festplatten im Storage-Controller	Die Anzahl der Laufwerke, die nicht optimal sind.
Storage Controller A	Der Status des Speichercontrollers A.
Storage Controller B	Der Status des Speichercontrollers B. Einige Gerätemodelle verfügen nicht über einen Speichercontroller B.
Netzteil für Storage Controller A	Der Status der Stromversorgung A für den Speichercontroller.
Stromversorgung des Speichercontrollers B	Der Status der Stromversorgung B für den Speichercontroller.
Typ des Speicherdatenlaufwerks	Die Art der im Gerät verbauten Laufwerke, wie HDD (Festplatte) oder SSD (Solid State Drive).

Feld in der Appliance-Tabelle	Beschreibung
Speicherlaufwerksgröße	Die effektive Größe eines Datenlaufwerks. Für das SG6160 wird auch die Größe des Cache-Laufwerks angezeigt. **Hinweis**: Für Knoten mit Erweiterungs-Shelfs ist stattdessen Festplattengröße für jedes Shelf zu verwenden. Die effektive Festplattengröße kann je nach Shelf unterschiedlich sein.
Storage RAID-Modus	Der für das Gerät konfigurierte RAID Modus.
Speicherkonnektivität	Der Speicherverbindungsstatus.
Gesamtstromversorgung	Der Status aller Stromversorgungen des Geräts.
Compute Controller BMC IP	Die IP-Adresse des Baseboard Management Controller (BMC) Ports im Compute Controller. Diese IP-Adresse wird verwendet, um eine Verbindung zur BMC Schnittstelle herzustellen und die Hardware des Geräts zu überwachen und zu diagnostizieren. Dieses Feld wird bei Gerätemodellen, die keinen BMC enthalten, nicht angezeigt.
Seriennummer des Rechencontrollers	Die Seriennummer des Rechencontrollers.
Compute-Hardware	Der Status der Compute-Controller-Hardware. Dieses Feld wird bei Gerätemodellen ohne separate Compute-Hardware und Speicherhardware nicht angezeigt.
CPU-Temperatur des Compute Controllers	Der Temperaturstatus der CPU des Rechencontrollers.
Gehäusetemperatur des Compute Controllers	Der Temperaturstatus des Rechencontrollers.

+

Spalte in der Tabelle „Storage Shelves“	Beschreibung
Seriennummer des Regalchassis	Die Seriennummer des Storage-Shelf-Gehäuses.

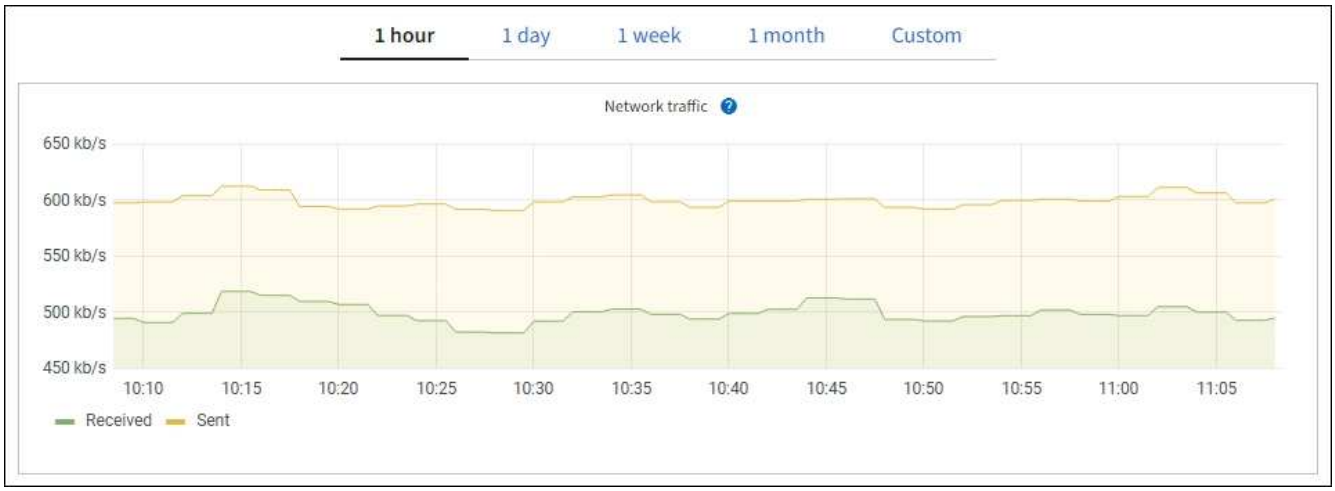
Spalte in der Tabelle „Storage Shelves“	Beschreibung
Shelf-ID	Die numerische Kennung für das Storage Shelf. • 99: Storage-Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf **Hinweis:** Erweiterungsregale gelten nur für SG6060 und SG6160.
Regalstatus	Der Gesamtstatus des Storage-Shelfs.
IOM Status	Der Status der Eingangs-/Ausgangsmodule (IOMs) in etwaigen Erweiterungs-Shelfs. Nicht zutreffend, falls es sich nicht um ein Erweiterungs-Shelf handelt.
Status der Stromversorgung	Der Gesamtstatus der Stromversorgungen für das Storage Shelf.
Schubladenstatus	Der Status der Schubladen im Storage Shelf. Nicht zutreffend, falls das Shelf keine Schubladen enthält.
Fanstatus	Der Gesamtzustand der Lüfter im Storage Shelf.
Laufwerksschächte	Die Gesamtzahl der Laufwerksschächte im Storage Shelf.
Datenlaufwerke	Die Anzahl der Laufwerke im Speichergehäuse, die zur Datenspeicherung verwendet werden.
Datenlaufwerkgröße	Die effektive Größe eines Datenlaufwerks im Speichergehäuse.
Cache-Laufwerke	Die Anzahl der Laufwerke im Speichergehäuse, die als Cache verwendet werden.
Cache-Laufwerksgröße	Die Größe des kleinsten Cache-Laufwerks im Speichergehäuse. Normalerweise haben alle Cache-Laufwerke die gleiche Größe.
Konfigurationsstatus	Der Konfigurationsstatus des Storage-Shelfs.

a. Bestätigt werden sollte, dass alle Statusangaben auf „Nominal“ stehen.

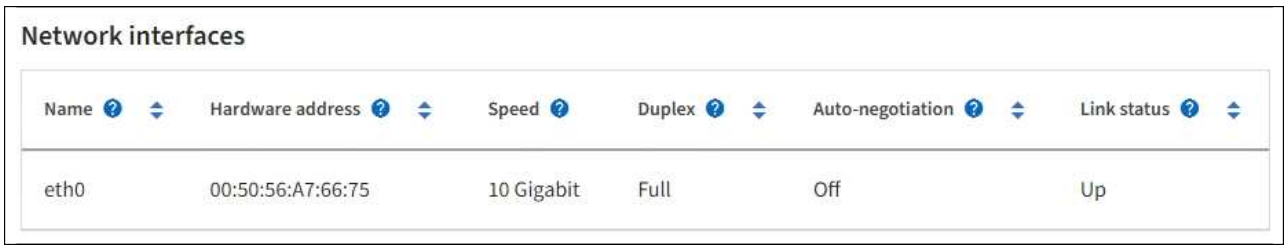
   Wenn der Status nicht „Nominal“ ist, sollten aktuelle Warnmeldungen überprüft werden. Mit SANtricity System Manager stehen weitere Informationen zu einigen dieser Hardwarewerte zur Verfügung. Die Anweisungen zur Installation und Wartung des Geräts sind zu beachten.

4. **Netzwerk** auswählen, um Informationen zu jedem Netzwerk anzuzeigen.

Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs.



a. Der Abschnitt Netzwerkschnittstellen kann überprüft werden.



Network interfaces

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

Anhand der folgenden Tabelle und der Werte in der Spalte **Speed** in der Tabelle „Netzwerkschnittstellen“ kann ermittelt werden, ob die 10/25-GbE Netzwerkports des Geräts für den Active/Backup-Modus oder den LACP-Modus konfiguriert wurden.

> Die in der Tabelle angegebenen Werte setzen voraus, dass alle vier Verbindungen genutzt werden.

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

Weitere Informationen zur Konfiguration der 10/25-GbE-Ports sind unter "Netzwerkverbindungen konfigurieren" verfügbar.

b. Der Abschnitt Netzwerkkommunikation enthält weitere Informationen.

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

Network communication

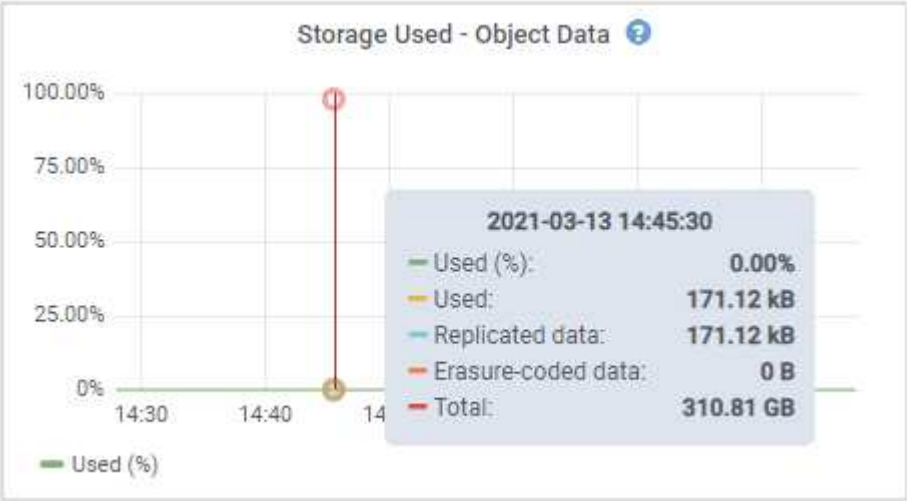
Receive

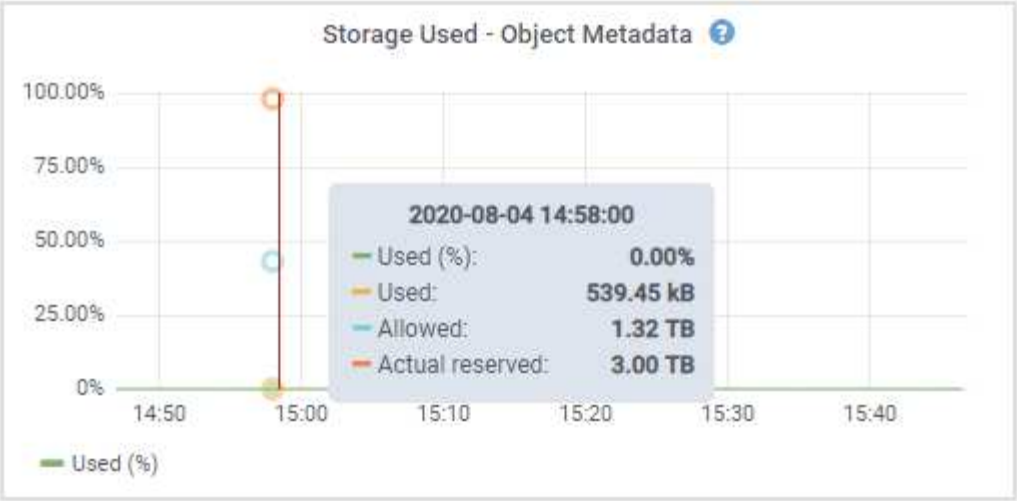
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

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

5. **Speicher** zeigt Diagramme, die die prozentuale Speichernutzung im Zeitverlauf für Objektdaten und Objektmetadaten sowie Informationen über Datenträger, Volumes und Objektspeicher anzeigen.





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

   Der Worldwide Name jeder Festplatte entspricht der Volume World-Wide Identifier (WWID), der angezeigt wird, wenn die Standard-Volume-Eigenschaften in SANtricity OS (der Management-Software, die mit dem Storage-Controller des Geräts verbunden ist) angezeigt werden.

   Zur Unterstützung bei der Interpretation der Lese- und Schreibstatistiken von Datenträgern in Bezug auf Volume-Mountpunkte entspricht der erste Teil des Namens, der in der Spalte **Name** der Tabelle „Disk Devices“ angezeigt wird (also *sdc*, *sdd*, *sde* usw.), dem Wert, der in der Spalte **Device** 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

Informationen zu Appliance Admin-Nodes und Gateway-Nodes

Die Seite „Knoten“ listet Informationen zum Dienststatus sowie zu allen Rechen-, Festplatten- und Netzwerkressourcen jeder Services Appliance auf, die als Admin Node oder Gateway Node verwendet wird. Es werden außerdem Arbeitsspeicher, Speicherhardware, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen sowie empfangene und gesendete Daten angezeigt.

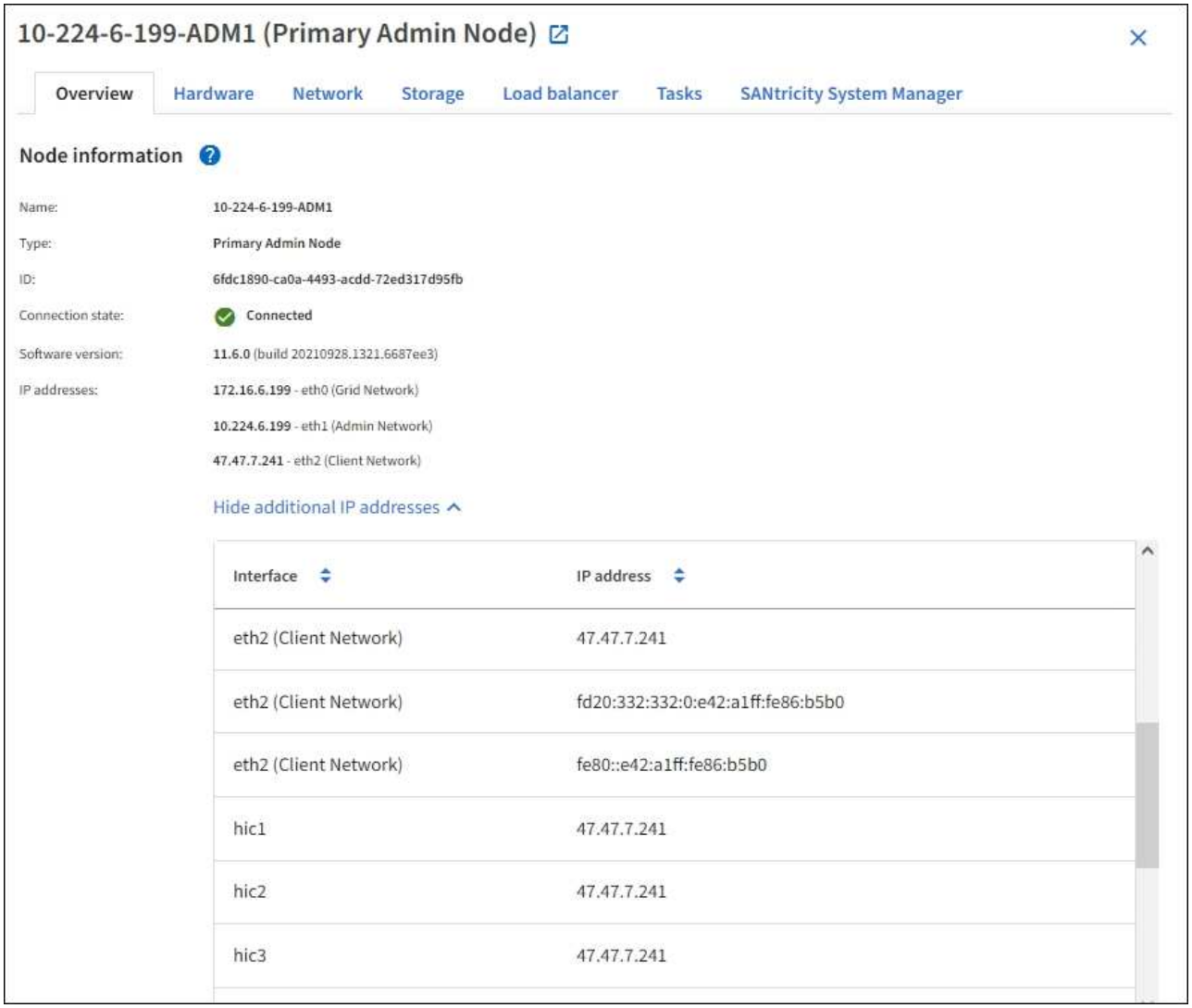
Schritte

1. Auf der Seite „Knoten“ einen Appliance Admin Node oder einen Appliance Gateway Node auswählen.
2. **Übersicht** auswählen.

   Der Abschnitt „Knoteninformationen“ auf der Registerkarte „Übersicht“ zeigt zusammenfassende

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

- **adllb** und **adlli**: Angezeigt, wenn für die Admin Network Schnittstelle aktives/Backup-Bonding verwendet wird
- **eth**: Das Grid Network, Admin Network oder Client Network.
- **hic**: Einer der physischen 10, 25 oder 100 GbE Ports des Geräts. Diese Ports können gebündelt und mit dem StorageGRID Grid Network (eth0) und dem Client Network (eth2) verbunden werden.
- **mtc**: Einer der physischen 1-GbE Ports des Geräts. Eine oder mehrere mtc Schnittstellen werden zu einer Admin Network Schnittstelle (eth1) zusammengefasst. Andere mtc Schnittstellen können für eine temporäre lokale Verbindung eines Technikers im Rechenzentrum verfügbar bleiben.

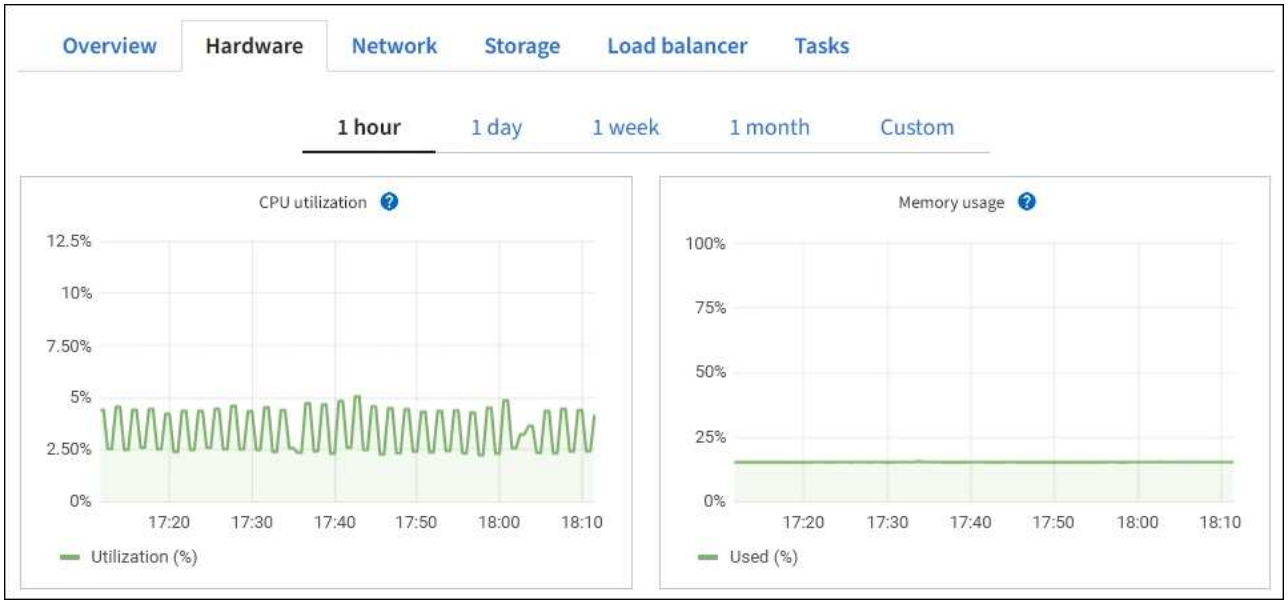


Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ sind alle aktiven Warnungen für den Knoten aufgeführt.

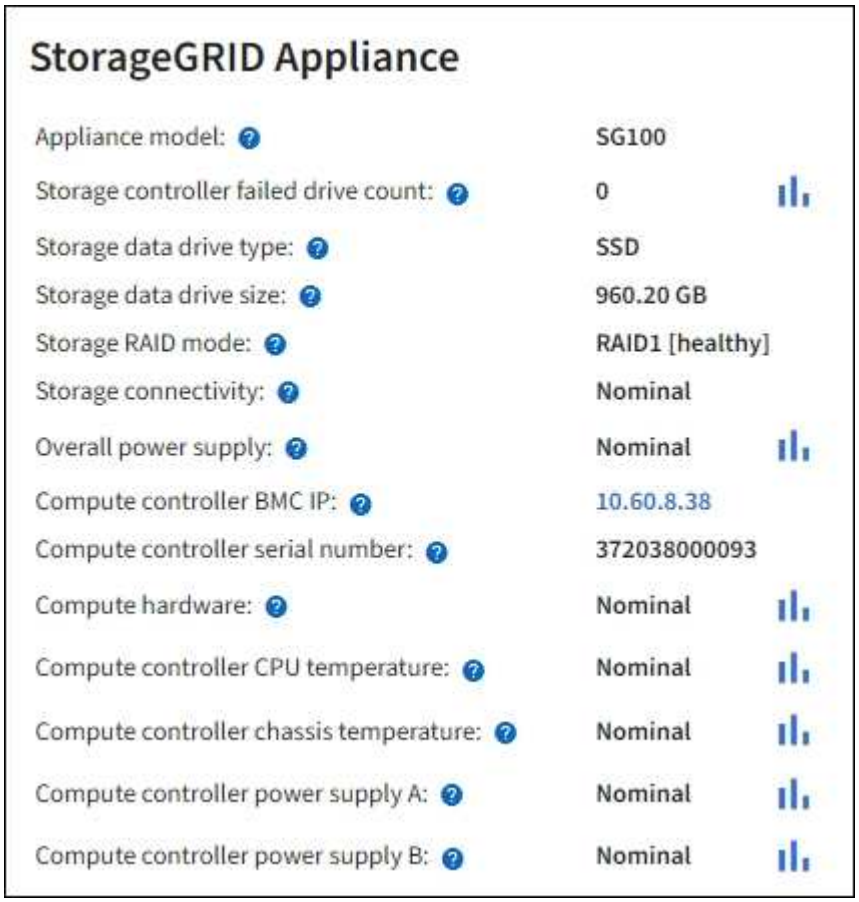
3. **Hardware** auswählen, um weitere Informationen zum Gerät zu sehen.

   a. Die Diagramme zur CPU-Auslastung und zum Speicher zeigen die prozentualen Werte der CPU- und Speichernutzung im Zeitverlauf. Zur Anzeige eines anderen Zeitintervalls steht eines der Steuerelemente oberhalb des Diagramms oder der Grafik zur Auswahl. Die verfügbaren Informationen können für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat angezeigt werden. Ein

benutzerdefiniertes Intervall ermöglicht die Angabe von Datums- und Zeitbereichen.



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



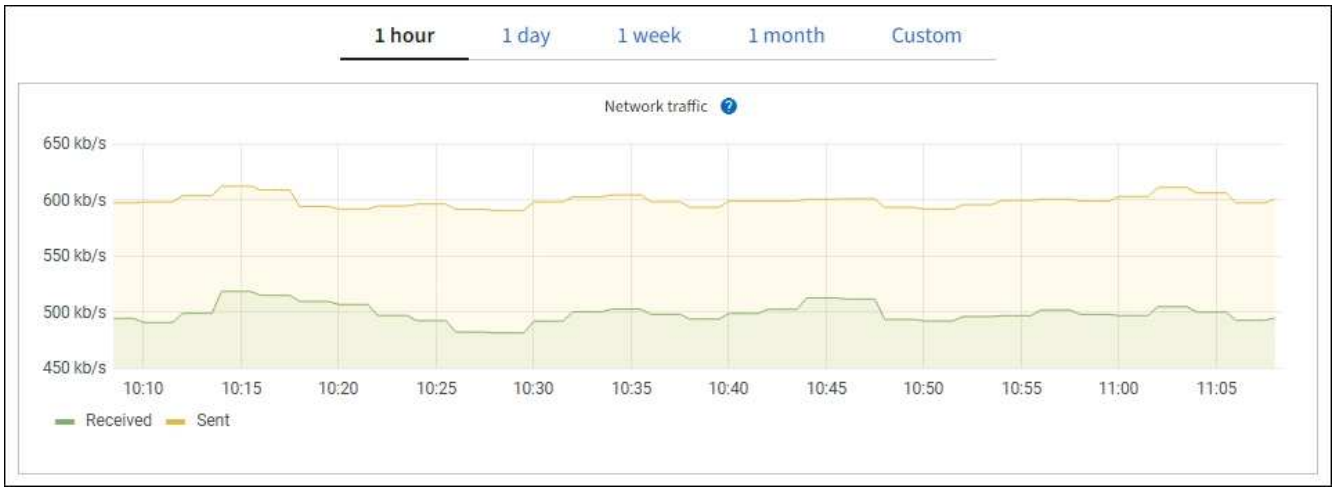
Feld in der Appliance-Tabelle	Beschreibung
Gerätemodell	Die Modellnummer für dieses StorageGRID Gerät.
Anzahl der ausgefallenen Festplatten im Storage-Controller	Die Anzahl der Laufwerke, die nicht optimal sind.
Typ des Speicherdatenlaufwerks	Die Art der im Gerät verbauten Laufwerke, wie HDD (Festplatte) oder SSD (Solid State Drive).
Speicherlaufwerksgröße	Die effektive Größe eines Datenlaufwerks.
Storage RAID-Modus	Der RAID-Modus für das Appliance.
Gesamtstromversorgung	Der Status aller Netzteile im Gerät.
Compute Controller BMC IP	Die IP-Adresse des Baseboard Management Controller (BMC) Ports im Compute Controller. Mit dieser IP-Adresse ist eine Verbindung zur BMC Schnittstelle möglich, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird bei Gerätemodellen, die keinen BMC enthalten, nicht angezeigt.
Seriennummer des Rechencontrollers	Die Seriennummer des Rechencontrollers.
Compute-Hardware	Der Status der Compute Controller Hardware.
CPU-Temperatur des Compute Controllers	Der Temperaturstatus der CPU des Rechencontrollers.
Gehäusetemperatur des Compute Controllers	Der Temperaturstatus des Rechencontrollers.

a. Bestätigt werden sollte, dass alle Statusangaben auf „Nominal“ stehen.

   Wenn der Status nicht „Normal“ ist, sollten aktuelle Warnmeldungen überprüft werden.

4. **Netzwerk** auswählen, um Informationen zu jedem Netzwerk anzuzeigen.

   Das Netzwerkverkehrsdiagramm bietet eine Zusammenfassung des gesamten Netzwerkverkehrs.



a. Der Abschnitt Netzwerkschnittstellen kann überprüft werden.

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

Anhand der folgenden Tabelle und der Werte in der Spalte **Speed** in der Tabelle „Network Interfaces“ lässt sich feststellen, ob die vier 40/100-GbE Netzwerkports des Geräts für den Active/Backup-Modus oder den LACP-Modus konfiguriert wurden.

> Die in der Tabelle angegebenen Werte setzen voraus, dass alle vier Verbindungen genutzt werden.

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

b. Der Abschnitt Netzwerkkommunikation enthält weitere Informationen.

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

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. **Speicher** zeigt Informationen über die Datenträger und Volumes auf der Services Appliance an.

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

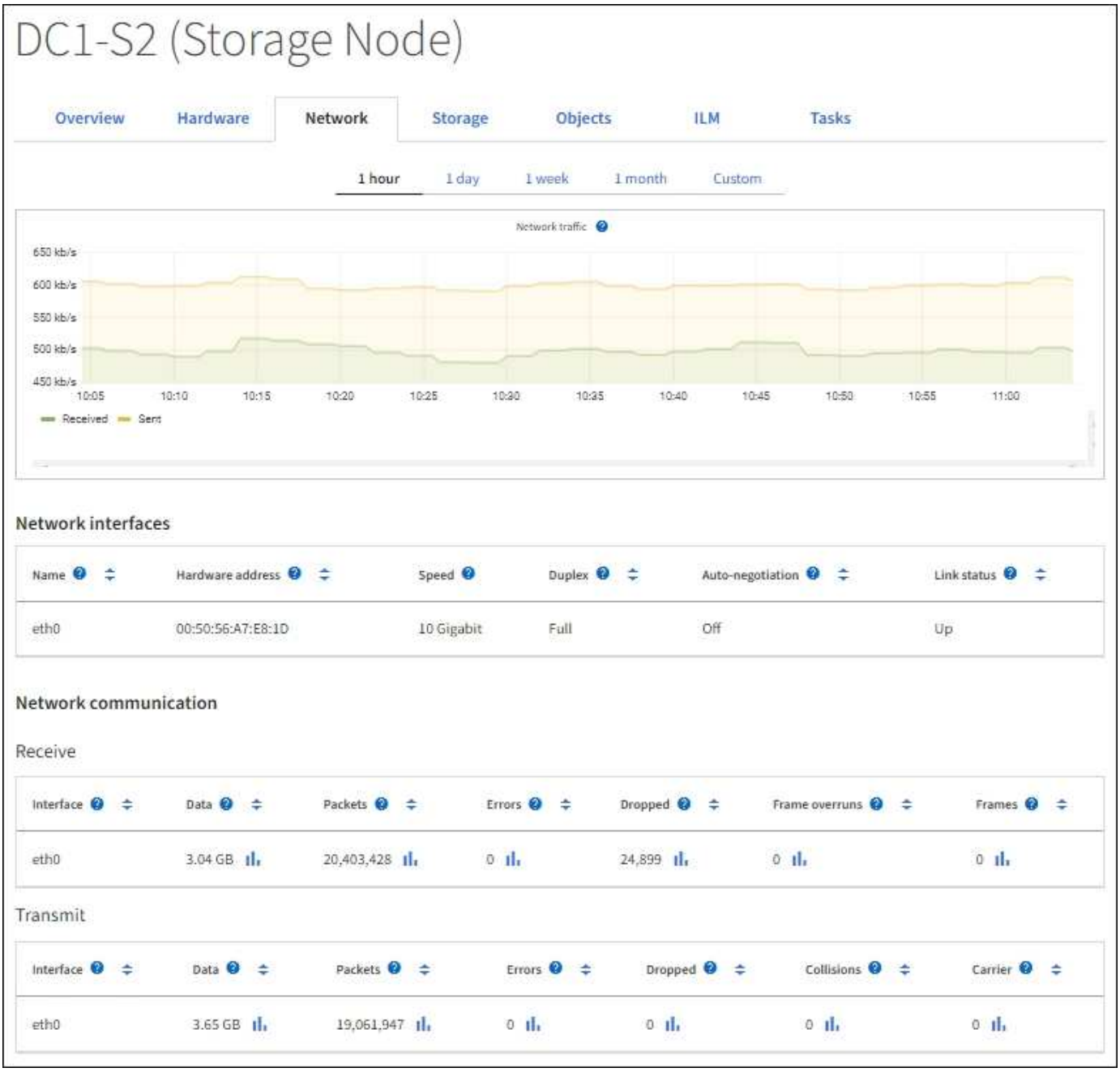
Registerkarte „StorageGRID-Netzwerk“ anzeigen

Auf der Registerkarte „Netzwerk“ wird ein Diagramm angezeigt, das den über alle Netzwerkschnittstellen des Node, Standorts oder Grids empfangenen und gesendeten Netzwerkverkehr darstellt.

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

Um ein anderes Zeitintervall anzuzeigen, kann eines der Steuerelemente oberhalb des Diagramms oder der Grafik ausgewählt werden. Die verfügbaren Informationen können für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat angezeigt werden. Auch ein benutzerdefiniertes Intervall ist möglich, wodurch Datums- und Zeitbereiche angegeben werden können.

Die Tabelle „Netzwerkschnittstellen“ liefert Informationen zu den physischen Netzwerkports jedes Knotens. Die Tabelle „Netzwerkkommunikation“ enthält Details zu den Empfangs- und Sendevorgängen jedes Knotens sowie zu etwaigen vom Treiber gemeldeten Fehlerzählern.



Verwandte Informationen

"Netzwerkverbindungen und Leistung überwachen"

Registerkarte „Storage“ in StorageGRID anzeigen

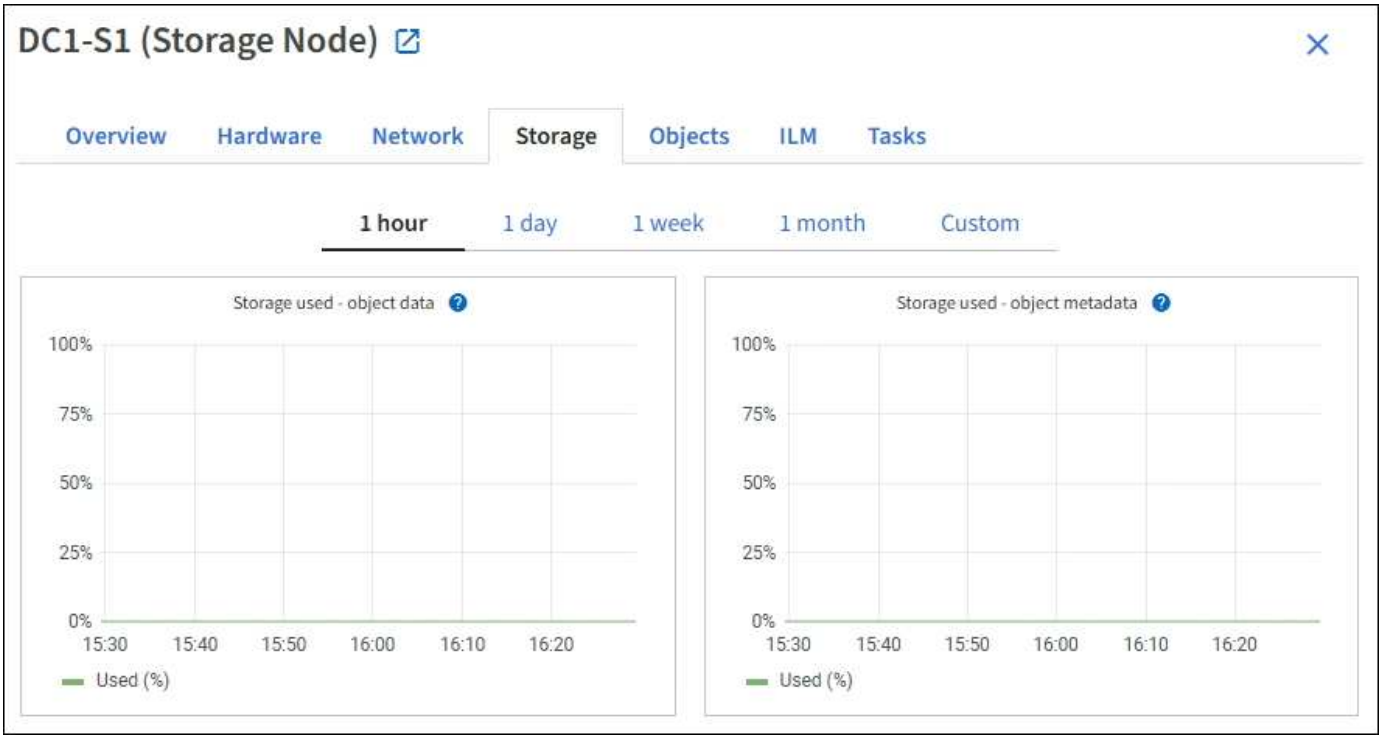
Die Registerkarte „Speicher“ fasst die Speicherverfügbarkeit und weitere Speicherkennzahlen zusammen.

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

Verwendete Speicherdiagramme

Für Storage Nodes, jeden Standort und das gesamte Grid enthält die Registerkarte „Speicher“ Diagramme, die zeigen, wie viel Speicherplatz im Laufe der Zeit von Objektdaten und Objektmetadaten genutzt wurde.

Wenn ein Knoten nicht mit dem Grid verbunden ist, beispielsweise während eines Upgrades oder im getrennten Zustand, sind bestimmte Messwerte möglicherweise nicht verfügbar oder werden in den Standort- und Grid-Gesamtwerten nicht berücksichtigt. Nach der Wiederherstellung der Verbindung eines Knotens mit dem Grid dauert es einige Minuten, bis sich die Werte stabilisieren.



Tabellen für Datenträgergeräte, Volumes und Objektspeicher

Für alle Knoten enthält die Registerkarte „Speicher“ Details zu den Datenträgern und Volumes des Knotens. Für Storage Nodes liefert die Tabelle „Object Stores“ Informationen zu jedem Speichervolume.

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

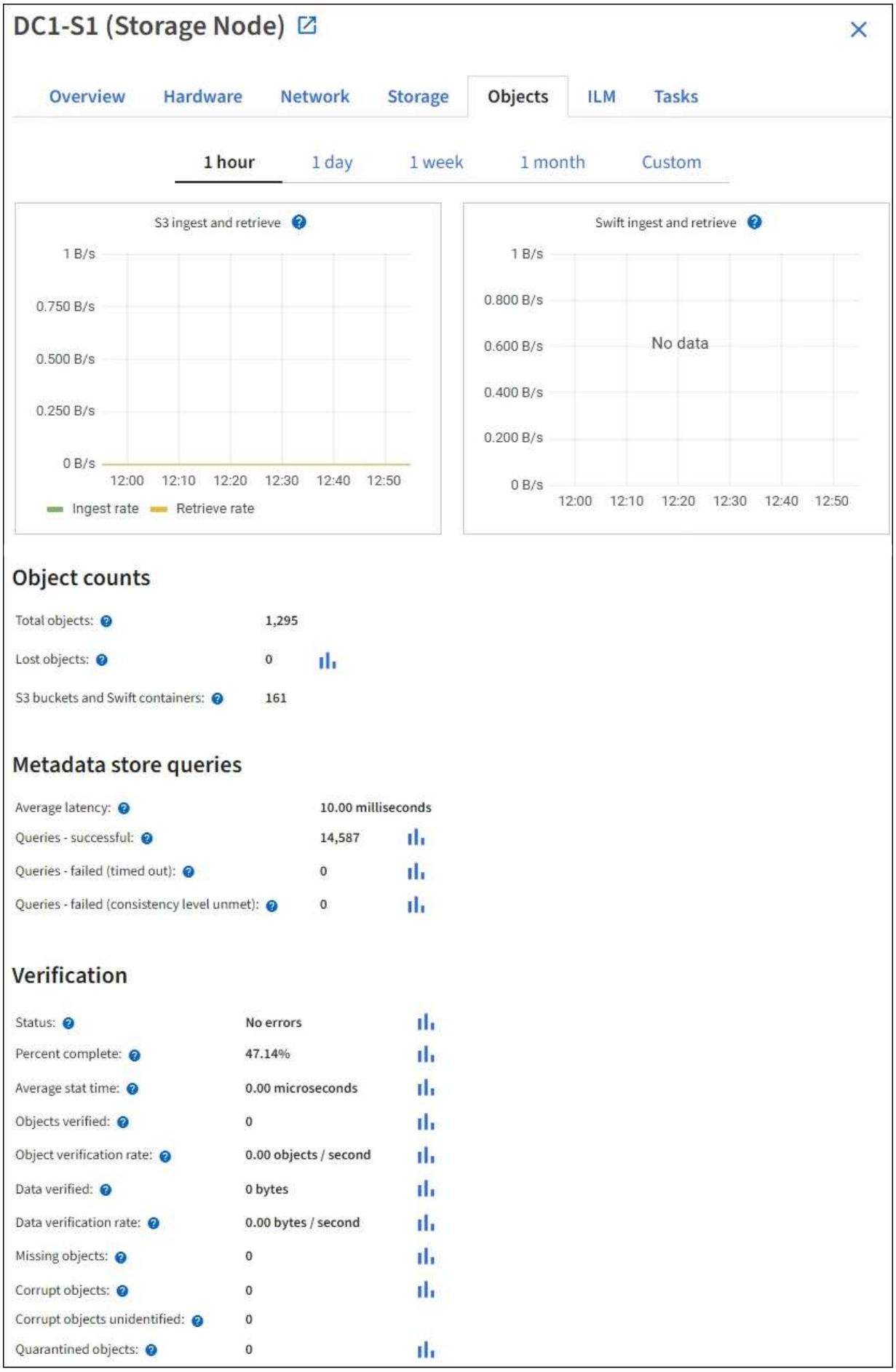
Verwandte Informationen

"Speicherkapazität überwachen"

Registerkarte „StorageGRID-Objekte“ anzeigen

Die Registerkarte „Objekte“ bietet Informationen über "S3-Ingest- und -Retrieve-Raten".

Die Registerkarte „Objekte“ wird für jeden Storage Node, jeden Standort und das gesamte Grid angezeigt. Für Storage Nodes liefert die Registerkarte „Objekte“ außerdem Objektanzahlen und Informationen zu Metadatenabfragen und Hintergrundüberprüfungen.

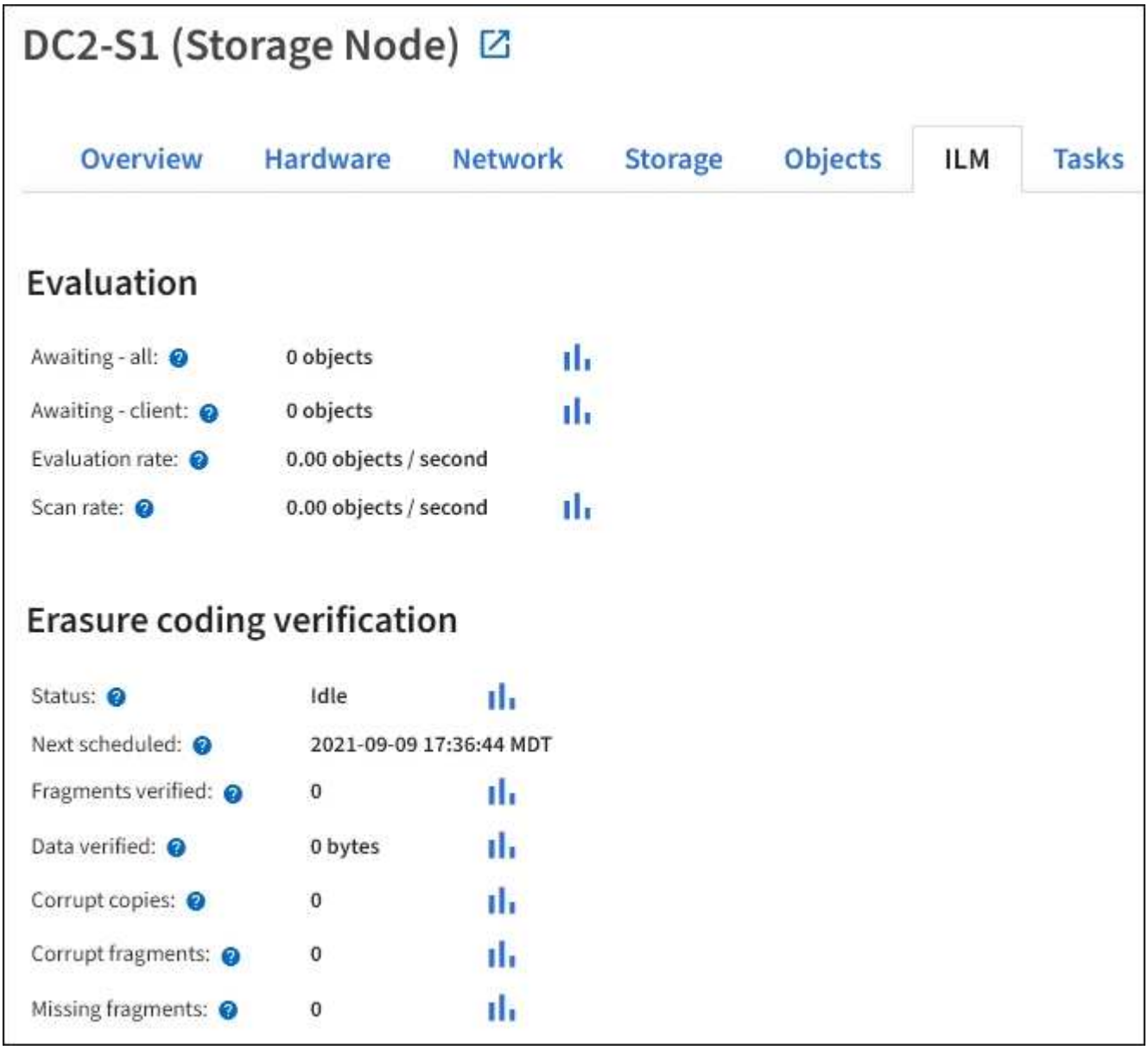

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

Die StorageGRID ILM-Registerkarte anzeigen

Die Registerkarte ILM bietet Informationen zu Vorgängen im Bereich Information Lifecycle Management (ILM).

Die Registerkarte „ILM“ wird für jeden Storage Node, jeden Standort und das gesamte Grid angezeigt. Für jeden Standort und das Grid zeigt die Registerkarte „ILM“ ein Diagramm der ILM-Warteschlange im Zeitverlauf. Für das Grid gibt diese Registerkarte außerdem die geschätzte Zeit an, die für einen vollständigen ILM-Scan aller Objekte benötigt wird.

Für Storage Nodes bietet die Registerkarte ILM Details zur ILM-Auswertung und Hintergrundprüfung für erasure-coded Objekte.



Verwandte Informationen

- "Information Lifecycle Management überwachen"
- "StorageGRID verwalten"

Registerkarte „StorageGRID Load Balancer“ anzeigen

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

Die Registerkarte „Load Balancer“ wird für Admin-Nodes und Gateway-Nodes, jeden Standort und das gesamte Grid angezeigt. Für jeden Standort bietet die Registerkarte „Load Balancer“ eine zusammenfassende Übersicht der Statistiken aller Nodes an diesem Standort. Für das gesamte Grid bietet die Registerkarte „Load Balancer“ eine zusammenfassende Übersicht der Statistiken aller Standorte.

Wenn keine E/A über den Load Balancer Service laufen oder kein Load Balancer konfiguriert ist, zeigen die Diagramme „Keine Daten“ an.

Anfrageverkehr

Dieses Diagramm zeigt einen gleitenden 3-Minuten-Durchschnitt des Datendurchsatzes zwischen den Load-Balancer-Endpunkten und den Clients, die die Anfragen stellen, in Bit pro Sekunde.

Dieser Wert wird nach Abschluss jeder Anfrage aktualisiert. Daher kann dieser Wert bei niedrigen Anfrageraten oder sehr lang andauernden Anfragen vom Echtzeit-Durchsatz abweichen. Im Tab „Netzwerk“ lässt sich eine realistischere Ansicht des aktuellen Netzwerkverhaltens anzeigen.

Eingehende Anfragerate

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

Durchschnittliche Anfragedauer (ohne Fehler)

Dieses Diagramm zeigt den gleitenden 3-Minuten-Durchschnitt der Anfragedauern, aufgeschlüsselt nach Anfragetyp (GET, PUT, HEAD und DELETE). Die Dauer jeder Anfrage beginnt, wenn ein Anfrageheader vom Load Balancer Service geparst wird, und endet, wenn der vollständige Antworttext an den Client zurückgegeben wird.

Fehlerreaktionsrate

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

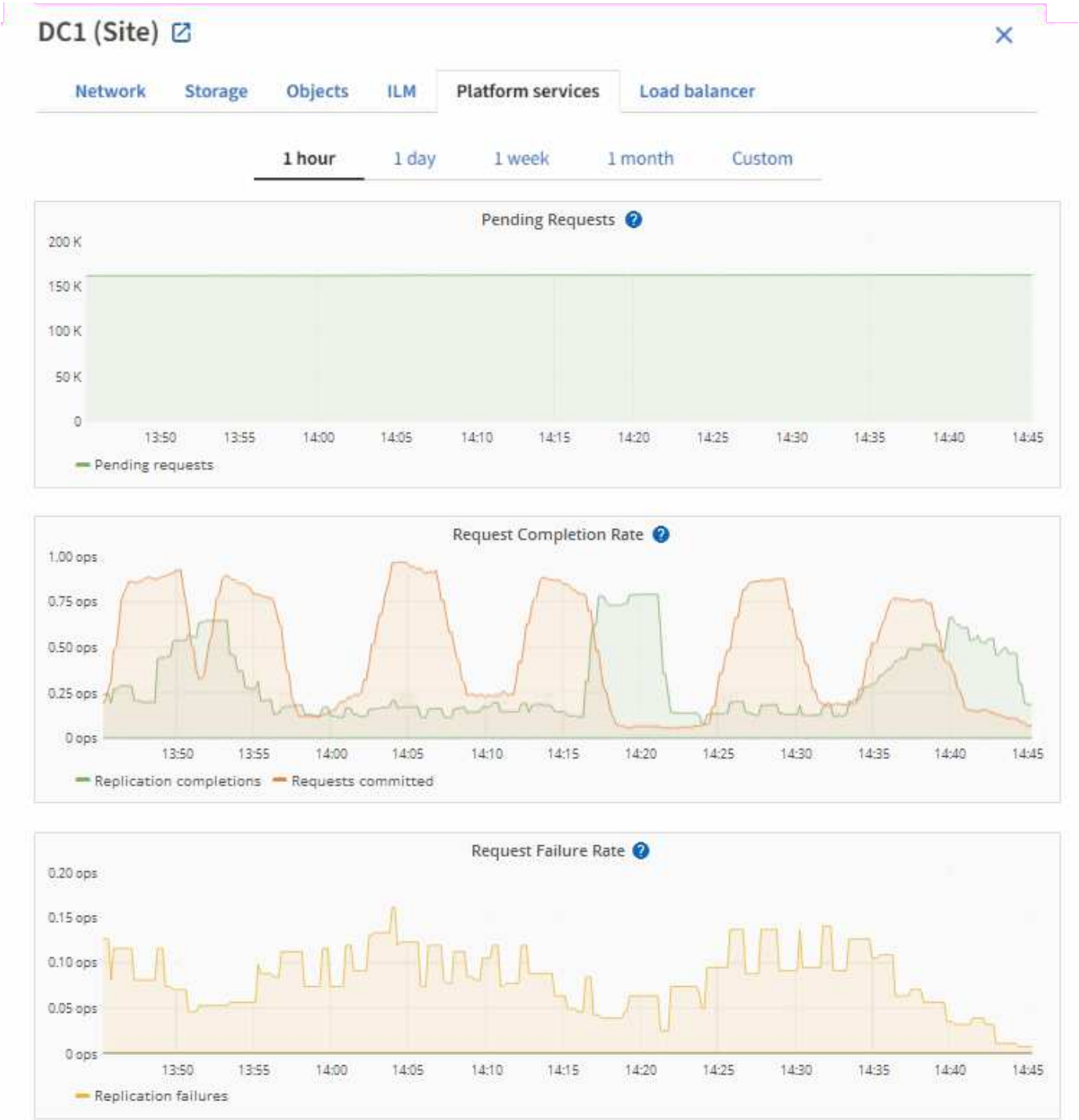
Verwandte Informationen

- "Lastverteilungsvorgänge überwachen"
- "StorageGRID verwalten"

Registerkarte „Dienste der StorageGRID-Plattform“ anzeigen

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

Für jede Site wird die Registerkarte „Plattformdienste“ angezeigt. Diese Registerkarte bietet Informationen zu S3-Plattformdiensten wie CloudMirror Replikation und den Suchintegrationsdienst. Diagramme auf dieser Registerkarte zeigen Kennzahlen wie die Anzahl ausstehender Anfragen, die Abschlussrate von Anfragen und die Fehlerrate von Anfragen.



Weitere Informationen zu den S3-Plattformdiensten, einschließlich Details zur Fehlerbehebung, sind unter "Anleitungen zur Administration von StorageGRID" zu finden.

Registerkarte „Laufwerke verwalten“ in StorageGRID anzeigen

Die Registerkarte „Laufwerke verwalten“ ermöglicht den Zugriff auf Details sowie die Durchführung von Fehlerbehebungs- und Wartungsaufgaben an Laufwerken in den Appliances, die diese Funktion unterstützen.

Über die Registerkarte „Laufwerke verwalten“ sind folgende Aktionen möglich:

- Eine Übersicht der Datenspeicherlaufwerke im Gerät anzeigen.
- Eine Tabelle zeigt jeden Laufwerksstandort, Typ, Status, Firmware-Version und die Seriennummer auf.
- Fehlerbehebungs- und Wartungsfunktionen an jedem Laufwerk ausführen

Um auf die Registerkarte „Laufwerke verwalten“ zugreifen zu können, muss die "Administrator- oder Root-Zugriffsberechtigung für Storage Appliance" vorhanden sein.

Informationen zur Verwendung der Registerkarte „Laufwerke verwalten“ finden sich unter "Die Registerkarte „Laufwerke verwalten“ verwenden".

Die Registerkarte StorageGRID SANtricity System Manager anzeigen

Die Registerkarte SANtricity System Manager ermöglicht den Zugriff auf SANtricity System Manager, ohne dass der Management-Port des Storage-Appliance konfiguriert oder angeschlossen werden muss. Mit dieser Registerkarte lassen sich Hardware-Diagnose- und Umgebungsinformationen sowie laufwerksbezogene Probleme anzeigen.

> Der Zugriff auf SANtricity System Manager über den Grid Manager ist im Allgemeinen nur zur Überwachung der Appliance-Hardware und zur Konfiguration der E-Series AutoSupport vorgesehen. Viele Funktionen und Vorgänge im SANtricity System Manager, wie beispielsweise das Aktualisieren der Firmware, gelten nicht für die Überwachung Ihrer StorageGRID Appliance. Zur Vermeidung von Problemen sind stets die Hardware-Wartungsanweisungen für Ihre Appliance zu beachten. Zur Aktualisierung der SANtricity Firmware siehe die "Wartungskonfigurationsverfahren" für Ihre Storage Appliance.

> Die Registerkarte SANtricity System Manager wird nur für Speicher-Appliance-Nodes angezeigt, die E-Series Hardware verwenden.

Mit dem SANtricity System Manager sind folgende Aktionen möglich:

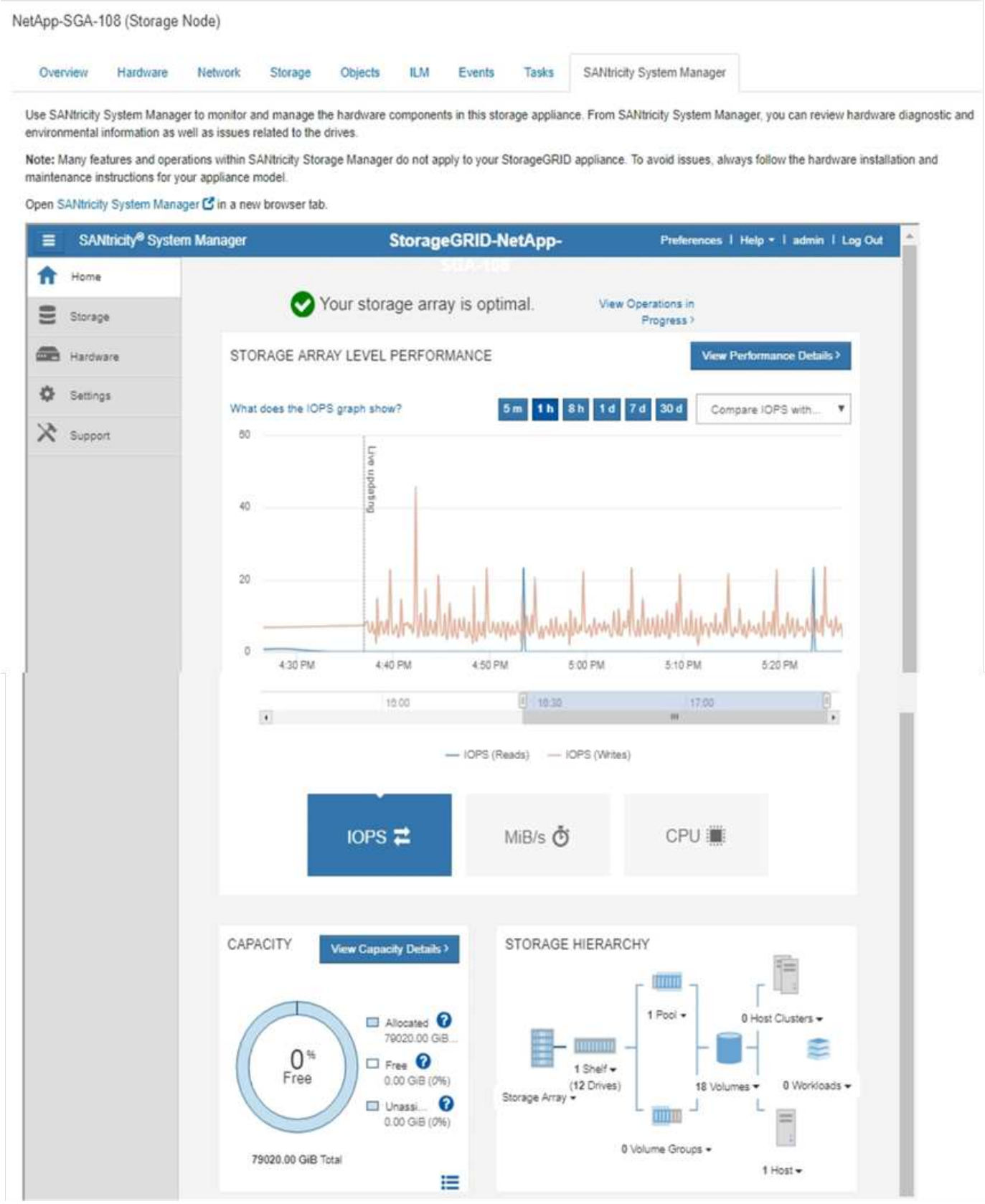
- Leistungsdaten wie die Leistung des Speicherarrays, die E/A-Latenz, die CPU-Auslastung des Speichercontrollers und den Durchsatz aufrufen, darunter Leistungsdaten auf Speicherarray-Ebene.
- Status der Hardwarekomponenten prüfen.
- Unterstützungsfunktionen einschließlich der Anzeige von Diagnosedaten und der Konfiguration von E-Series AutoSupport ausführen.

> Um den SANtricity System Manager zur Konfiguration eines Proxys für E-Series AutoSupport zu verwenden, siehe "E-Series AutoSupport-Pakete über StorageGRID senden".

Um über Grid Manager auf SANtricity System Manager zugreifen zu können, muss die "Administrator- oder Root-Zugriffsberechtigung für Storage Appliance" vorhanden sein.

> Für den Zugriff auf SANtricity System Manager mit dem Grid Manager ist SANtricity Firmware 8.70 oder höher erforderlich.

Die Registerkarte zeigt die Startseite des SANtricity System Manager an.



Der Link „SANtricity System Manager“ kann verwendet werden, um den SANtricity System Manager in einem neuen Browserfenster zur besseren Ansicht zu öffnen.

Details zur Leistung und Kapazitätsauslastung auf Speicherarray-Ebene werden angezeigt, wenn der

Mauszeiger über die einzelnen Diagramme positioniert wird.

Weitere Details zum Anzeigen der über die Registerkarte SANtricity System Manager zugänglichen Informationen finden sich unter "NetApp E-Series und SANtricity Dokumentation".

Informationen zur regelmäßigen Überwachung

Was und wann in StorageGRID überwacht werden sollte

Auch wenn das StorageGRID System bei Fehlern oder dem Ausfall von Teilen des Grids weiterhin funktionieren kann, sollten potenzielle Probleme überwacht und behoben werden, bevor sie die Effizienz oder Verfügbarkeit des Grids beeinträchtigen.

Bevor Sie beginnen

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

Über Überwachungsaufgaben

Ein stark ausgelastetes System erzeugt große Datenmengen. Die folgende Liste enthält Hinweise zu den wichtigsten Informationen, die fortlaufend überwacht werden sollten.

Was überwacht werden sollte	Frequenz
"Systemgesundheitsstatus"	Täglich
Rate, mit der "Speicherknotenobjekt und Metadatenkapazität" verbraucht wird	Wöchentlich
"Information Lifecycle Management-Operationen"	Wöchentlich
"Netzwerk und Systemressourcen"	Wöchentlich
"Mandantenaktivität"	Wöchentlich
"S3 Client-Operationen"	Wöchentlich
"Lastverteilungsoperationen"	Nach der Erstkonfiguration und nach Konfigurationsänderungen
"Grid Federation Verbindungen"	Wöchentlich

Systemzustand in StorageGRID überwachen

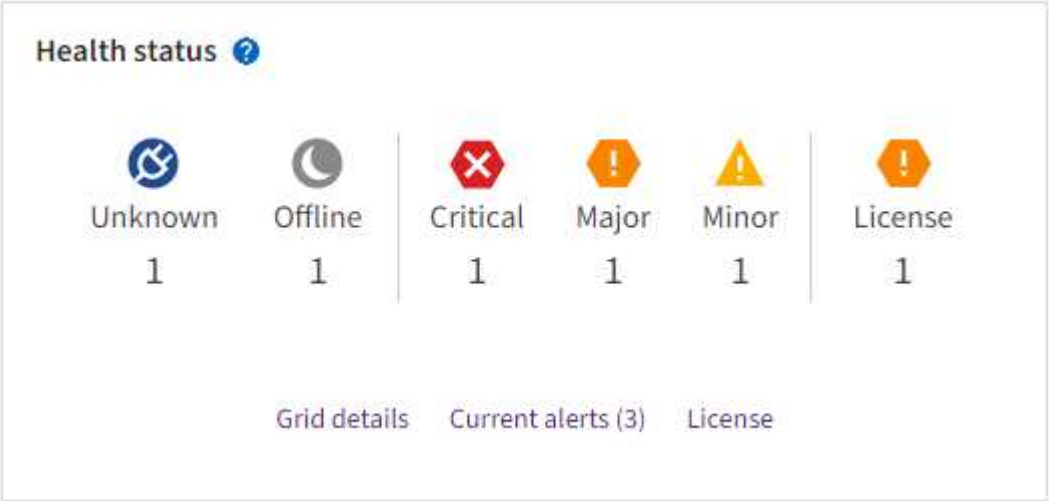
Der allgemeine Zustand Ihres StorageGRID-Systems kann täglich überwacht werden.

Über diese Aufgabe

Das StorageGRID System kann auch dann weiterarbeiten, wenn Teile des Grids nicht verfügbar sind. Potenzielle Probleme, die durch Warnmeldungen angezeigt werden, sind nicht zwangsläufig Probleme mit dem

Systembetrieb. Probleme, die auf der Statuskarte „Systemzustand“ des Grid Manager Dashboards zusammengefasst sind, sollten untersucht werden.

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



Wenn Probleme auftreten, erscheinen Links, die das Anzeigen weiterer Details ermöglichen:

Link	Erscheint, wenn…
Grid-Details	Alle Knoten sind getrennt (Verbindungsstatus Unknown oder Administratively Down).
Aktuelle Warnmeldungen (Kritisch, Schwerwiegend, Geringfügig)	Warnmeldungen sind derzeit aktiv.
Kürzlich behobene Warnmeldungen	In der vergangenen Woche ausgelöste Warnmeldungen sind nun gelöst.
Lizenz	Es gibt ein Problem mit der Softwarelizenz für dieses StorageGRID System. Sie können "Lizenzinformationen bei Bedarf aktualisieren".

Verbindungszustände der Überwachungsknoten

Wenn ein oder mehrere Knoten vom Grid getrennt sind, könnten kritische StorageGRID Vorgänge beeinträchtigt werden. Die Verbindungszustände der Knoten sollten überwacht und etwaige Probleme zeitnah behoben werden.

Symbol	Beschreibung	Aktion erforderlich
	Nicht verbunden - Unbekannt Aus unbekannten Gründen ist ein Knoten getrennt oder Dienste auf dem Knoten sind unerwartet ausgefallen. Beispielsweise könnte ein Dienst auf dem Knoten beendet worden sein oder der Knoten könnte aufgrund eines Stromausfalls oder einer unerwarteten Unterbrechung seine Netzwerkverbindung verloren haben. Die Warnung **Unable to communicate with node** kann ebenfalls ausgelöst werden. Andere Warnungen können ebenfalls aktiv sein.	Erfordert sofortige Aufmerksamkeit. Jede Benachrichtigung auswählen und die empfohlenen Maßnahmen befolgen. Beispielsweise kann es erforderlich sein, einen Dienst neu zu starten, der angehalten wurde, oder den Host für den Knoten neu zu starten. **Hinweis**: Während verwalteter Herunterfahrvorgänge kann ein Knoten als „Unbekannt“ angezeigt werden. Der Status „Unbekannt“ kann in diesen Fällen ignoriert werden.
	Nicht verbunden - Administrativ deaktiviert Aus einem erwarteten Grund ist der Node nicht mit dem Grid verbunden. Beispielsweise wurde der Knoten oder die darauf laufenden Dienste ordnungsgemäß heruntergefahren, der Knoten wird neu gestartet oder die Software wird aktualisiert. Eine oder mehrere Warnmeldungen könnten ebenfalls aktiv sein. Basierend auf dem zugrunde liegenden Problem gehen diese Nodes häufig ohne Eingreifen wieder online.	Es wird geprüft, ob Warnmeldungen diesen Knoten betreffen. Wenn eine oder mehrere Warnungen aktiv sind, Jede Benachrichtigung auswählen befolgen Sie die empfohlenen Maßnahmen.
	Verbunden Der Knoten ist mit dem Grid verbunden.	Keine Maßnahmen erforderlich.

Aktuelle und behobene Warnmeldungen

Aktuelle Warnmeldungen: Wenn eine Warnmeldung ausgelöst wird, wird ein Warnsymbol im Dashboard angezeigt. Ein Warnsymbol wird auch für den Knoten auf der Seite „Knoten“ angezeigt. Wenn "E-Mail-Benachrichtigungen für Warnmeldungen sind konfiguriert", wird zusätzlich eine E-Mail-Benachrichtigung gesendet, sofern die Warnmeldung nicht stummgeschaltet wurde.

Behobene Warnmeldungen: Es besteht die Möglichkeit, nach behobenen Warnmeldungen zu suchen und deren Historie anzuzeigen.

Optional haben Sie sich das Video angesehen:

Benachrichtigungsübersicht

Die folgende Tabelle beschreibt die im Grid Manager angezeigten Informationen zu aktuellen und behobenen

Warnmeldungen.

Spaltenüberschrift	Beschreibung
Name oder Titel	Der Name der Warnung und ihre Beschreibung.
Schwere	Der Schweregrad der Warnung. Bei aktuellen Warnungen zeigt die Titelzeile an, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten. **Kritisch**: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Knotens oder Dienstes gestoppt hat. Das zugrunde liegende Problem muss umgehend behoben werden. Kommt es zu keiner Lösung, können Dienstunterbrechungen und Datenverlust die Folge sein. **Schwerwiegend**: Es liegt ein anormaler Zustand vor, der entweder den laufenden Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Es empfiehlt sich, schwerwiegende Warnungen zu untersuchen und zugrunde liegende Probleme zu beheben, damit der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder Dienstes nicht unterbricht. **Geringfügig**: Das System funktioniert normal, es besteht jedoch eine Störung, die die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn sie anhält. Geringfügige Warnmeldungen, die nicht von selbst verschwinden, sollten überwacht und behoben werden, damit daraus kein schwerwiegenderes Problem entsteht.
Zeitausgelöst	**Aktuelle Warnmeldungen**: Datum und Uhrzeit der Auslösung der Warnmeldung in Ihrer Ortszeit und in UTC. Wenn mehrere Warnmeldungen gruppiert sind, zeigt die Titelzeile die Zeiten für die aktuellste Instanz der Warnmeldung (*newest*) und die älteste Instanz der Warnmeldung (*oldest*) an. **Behobene Warnmeldungen**: Wie lange es her ist, dass die Warnmeldung ausgelöst wurde.
Standort/Knoten	Name des Standorts und des Knotens, an dem die Warnung auftritt oder aufgetreten ist.
Status	Ob die Warnung aktiv, stummgeschaltet oder behoben ist. Wenn mehrere Warnungen gruppiert sind und im Dropdown-Menü **Alle Warnungen** ausgewählt ist, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung aktiv sind und wie viele Instanzen stummgeschaltet wurden.
Zeitpunkt der Behebung (nur behobene Warnmeldungen)	Wie lange es her ist, dass die Warnung behoben wurde.

Spaltenüberschrift	Beschreibung
Aktuelle Werte oder *Datenwerte*	Der Wert der Metrik, die die Warnung ausgelöst hat. Für einige Warnungen werden zusätzliche Werte angezeigt, die das Verständnis und die Untersuchung der Warnung unterstützen. Beispielsweise umfassen die bei einer **Low object data storage** Warnung angezeigten Werte den Prozentsatz des belegten Speicherplatzes, die Gesamtmenge des Speicherplatzes und die Menge des belegten Speicherplatzes. **Hinweis:** Wenn mehrere aktuelle Warnungen gruppiert sind, werden die aktuellen Werte nicht in der Titelzeile angezeigt.
Ausgelöste Werte (nur behobene Warnmeldungen)	Der Wert der Metrik, die die Warnung ausgelöst hat. Für einige Warnungen werden zusätzliche Werte angezeigt, die das Verständnis und die Untersuchung der Warnung unterstützen. Beispielsweise umfassen die bei einer **Low object data storage** Warnung angezeigten Werte den Prozentsatz des belegten Speicherplatzes, die Gesamtmenge des Speicherplatzes und die Menge des belegten Speicherplatzes.

Schritte

1. Wählen Sie den Link **Aktuelle Warnungen** oder **Behobene Warnungen**, um eine Liste der Warnungen in diesen Kategorien anzuzeigen. Die Details einer Warnung sind auch über **Knoten** > ***node*** > **Übersicht** und anschließend durch Auswahl der Warnung in der Warnungstabelle einsehbar.

   Standardmäßig werden aktuelle Warnmeldungen wie folgt angezeigt:

   - Die zuletzt ausgelösten Warnmeldungen werden zuerst angezeigt.
   - Mehrere Warnmeldungen desselben Typs werden als Gruppe angezeigt.
   - Stummgeschaltete Warnmeldungen werden nicht angezeigt.
   - Bei einer bestimmten Warnung auf einem bestimmten Knoten wird, wenn die Schwellenwerte für mehr als einen Schweregrad erreicht werden, nur die Warnung mit dem höchsten Schweregrad angezeigt. Das heißt, wenn die Schwellenwerte für die Schweregrade gering, schwer und kritisch erreicht werden, wird nur die Warnung mit dem Schweregrad kritisch angezeigt.

     Die Seite mit den aktuellen Benachrichtigungen wird alle zwei Minuten aktualisiert.

2. Um Gruppen von Benachrichtigungen zu erweitern, wählen Sie den Pfeil nach unten ⌄. Um einzelne Benachrichtigungen in einer Gruppe zu reduzieren, wählen Sie den Pfeil nach oben ⌃ oder den Namen der Gruppe.
3. Um einzelne Warnmeldungen anstelle von Gruppen von Warnmeldungen anzuzeigen, das Kontrollkästchen **Gruppenwarnmeldungen** deaktivieren.
4. Um aktuelle Benachrichtigungen oder Benachrichtigungsgruppen zu sortieren, die Auf-/Abwärtspfeile ⇅ in den jeweiligen Spaltenüberschriften auswählen.
   - Wenn **Gruppenbenachrichtigungen** ausgewählt ist, werden sowohl die Benachrichtigungsgruppen als auch die einzelnen Benachrichtigungen innerhalb jeder Gruppe sortiert. Beispielsweise kann es sinnvoll sein, die Benachrichtigungen in einer Gruppe nach **Auslösezeitpunkt** zu sortieren, um das aktuellste Vorkommen einer bestimmten Benachrichtigung zu finden.
   - Wenn **Gruppenwarnungen** gelöscht werden, wird die gesamte Liste der Warnungen sortiert. Zum Beispiel kann eine Sortierung aller Warnungen nach **Knoten/Standort** dabei helfen, alle Warnungen zu sehen, die einen bestimmten Knoten betreffen.

5. Aktuelle Benachrichtigungen können nach Status (**Alle Benachrichtigungen**, **Aktiv** oder **Stummgeschaltet**) mit dem Dropdown-Menü oben in der Tabelle gefiltert werden.

   Siehe "Alarmbenachrichtigungen stummschalten".

6. Behobene Warnmeldungen sortieren:
   - Wählen Sie einen Zeitraum aus dem Dropdown-Menü **Bei Auslösung** aus.
   - Im Dropdown-Menü **Schweregrad** können ein oder mehrere Schweregrade ausgewählt werden.
   - Eine oder mehrere Standard- oder benutzerdefinierte Warnregeln können im Dropdown-Menü **Warnregel** ausgewählt werden, um nach behobenen Warnmeldungen zu filtern, die sich auf eine bestimmte Warnregel beziehen.
   - Im Dropdown-Menü **Knoten** kann ein oder mehrere Knoten ausgewählt werden, um nach behobenen Warnmeldungen zu filtern, die sich auf einen bestimmten Knoten beziehen.
7. Details zu einer bestimmten Warnung werden angezeigt, wenn die entsprechende Warnung ausgewählt wird. Ein Dialogfeld bietet Details und empfohlene Maßnahmen für die ausgewählte Warnung.
8. (Optional) Für eine bestimmte Warnung kann „Diese Warnung stummschalten“ ausgewählt werden, um die Warnungsregel stummzuschalten, die diese Warnung ausgelöst hat.

   Sie müssen über die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten" verfügen, um eine Alarmregel stummzuschalten.

   > Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Warnregel stummzuschalten. Wenn eine Warnregel stummgeschaltet ist, könnte ein zugrundeliegendes Problem erst erkannt werden, wenn es die Ausführung eines kritischen Vorgangs verhindert.

9. Die aktuellen Bedingungen für die Alarmregel können wie folgt angezeigt werden:
   a. In den Alarmdetails die Option **Bedingungen anzeigen** auswählen.

      Ein Popup wird angezeigt, das den Prometheus-Ausdruck für jeden definierten Schweregrad auflistet.

   b. Um das Pop-up zu schließen, außerhalb des Pop-ups klicken.
10. Optional kann **Regel bearbeiten** ausgewählt werden, um die Alarmregel zu bearbeiten, die diesen Alarm ausgelöst hat.

    Sie benötigen die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten" Berechtigung, um eine Alarmregel zu bearbeiten.

    > Seien Sie vorsichtig beim Bearbeiten einer Alarmregel. Wenn Sie Auslösewerte ändern, wird ein zugrundeliegendes Problem möglicherweise erst erkannt, wenn es die Ausführung eines kritischen Vorgangs verhindert.

11. Zum Schließen der Benachrichtigungsdetails **Schließen** auswählen.

Überwachen Sie die Speicherkapazität in StorageGRID

Der insgesamt verfügbare Speicherplatz sollte überwacht werden, damit dem StorageGRID System weder für Objekte noch für Objektmetadaten der Speicherplatz ausgeht.

StorageGRID speichert Objektdaten und Objektmetadaten getrennt und reserviert einen bestimmten Speicherplatz für eine verteilte Cassandra Datenbank, die Objektmetadaten enthält. Der gesamte Speicherplatzverbrauch für Objekte und für Objektmetadaten sowie die Entwicklung des jeweiligen Verbrauchs sollte überwacht werden. Dadurch wird eine vorausschauende Planung für die Hinzufügung von Knoten und die Vermeidung von Serviceausfällen ermöglicht.

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

Die Speicherkapazität des gesamten Grids überwachen

Die Gesamtspeicherkapazität Ihres Grids sollte überwacht werden, damit ausreichend freier Speicherplatz für Objektdaten und Objektmetadaten verbleibt. Ein Verständnis dafür, wie sich die Speicherkapazität im Laufe der Zeit verändert, unterstützt die Planung zur Erweiterung um Storage Nodes oder Speichervolumes, bevor die nutzbare Speicherkapazität des Grids ausgeschöpft ist.

Das Grid Manager Dashboard ermöglicht eine schnelle Einschätzung, wie viel Speicherplatz für das gesamte Grid und für jedes einzelne Rechenzentrum verfügbar ist. Die Seite „Knoten“ bietet detailliertere Werte für Objektdaten und Objektmetadaten.

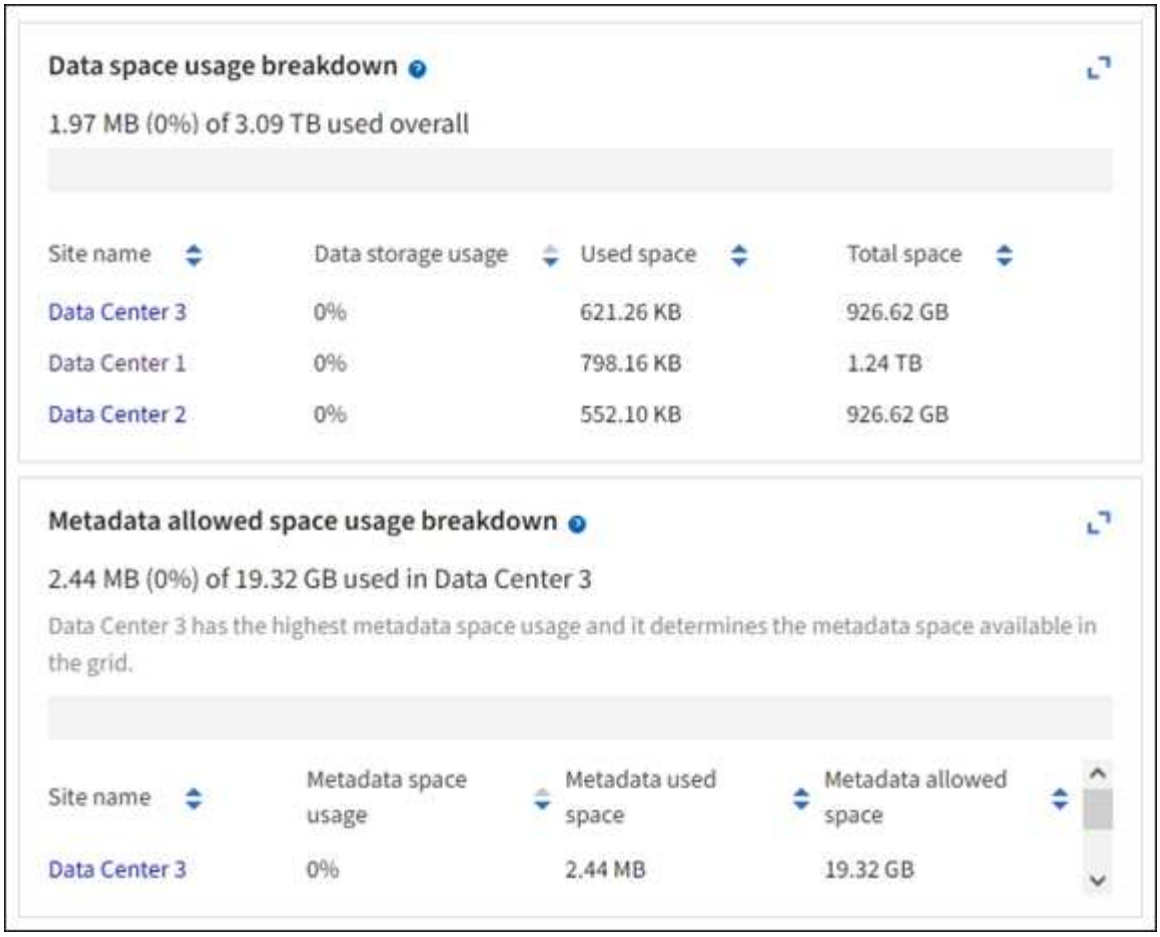
Schritte

1. Es kann ermittelt werden, wie viel Speicherplatz für das gesamte Grid und für jedes einzelne Rechenzentrum zur Verfügung steht.

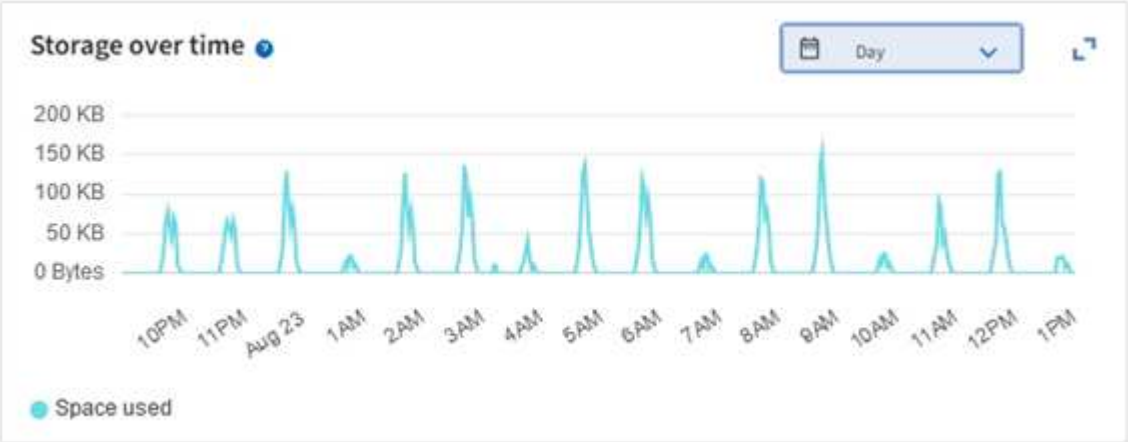
    a. **Dashboard > Übersicht** auswählen.

    b. Beachten Sie die Werte auf den Karten „Aufschlüsselung der Datenspeichernutzung“ und „Aufschlüsselung der zulässigen Metadatenspeichernutzung“. Jede Karte zeigt den prozentualen Anteil der Speichernutzung, die Kapazität des belegten Speicherplatzes und den insgesamt verfügbaren bzw. zulässigen Speicherplatz pro Standort.

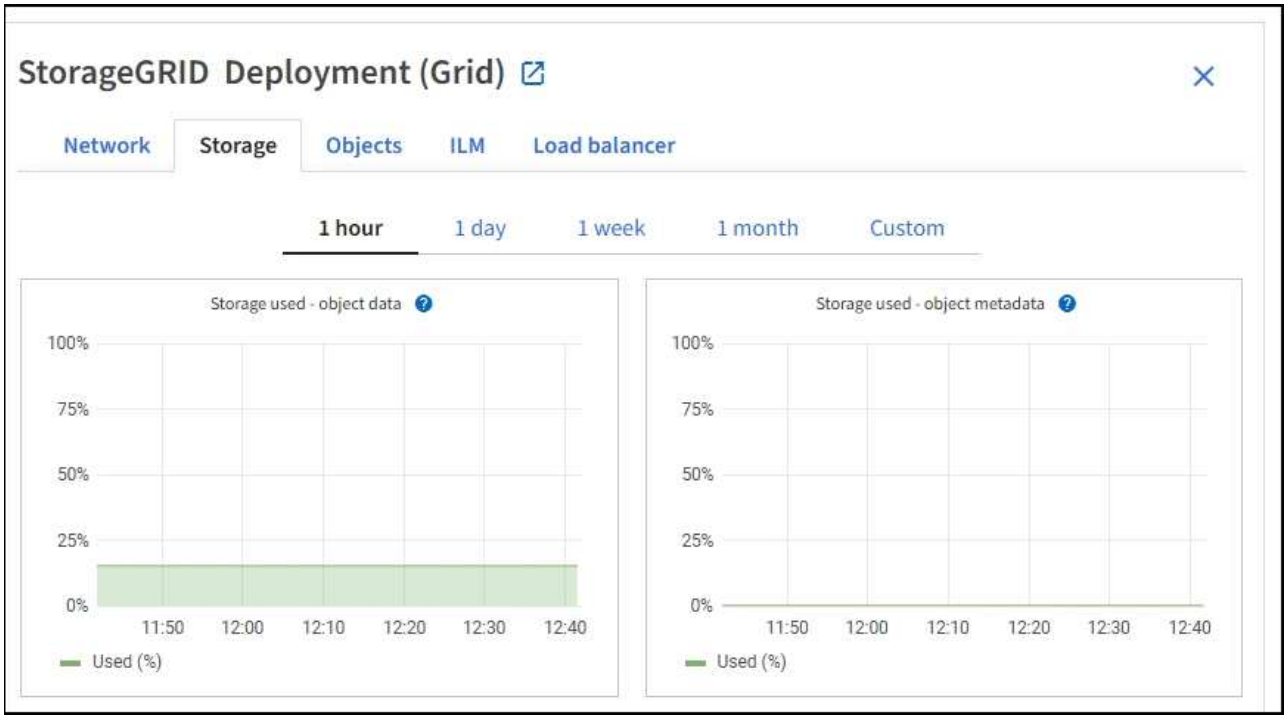
    > Die Zusammenfassung umfasst keine Archivmedien.



a. Beachten Sie das Diagramm auf der Karte „Storage over time“. Das Dropdown-Menü für den Zeitraum unterstützt dabei, zu erkennen, wie schnell Speicherplatz verbraucht wird.



2. Auf der Seite „Knoten“ sind zusätzliche Details darüber verfügbar, wie viel Speicherplatz bereits genutzt wurde und wie viel Speicherplatz im Grid noch für Objektdaten und Objektmetadaten zur Verfügung steht.
   a. Wählen Sie **Knoten**.
   b. ***grid*** > **Speicher** auswählen.



c. Positionieren Sie den Cursor über die Diagramme **Storage used - object data** und **Storage used - object metadata**, um zu sehen, wie viel Objektspeicher und Objektmetadatenspeicher für das gesamte Grid verfügbar sind und wie viel im Laufe der Zeit genutzt wurde.

> Die Gesamtwerte für einen Standort oder das Grid beinhalten keine Knoten, die seit mindestens fünf Minuten keine Metriken gemeldet haben, wie zum Beispiel Offline-Knoten.

3. Es sollte eine Erweiterung zur Hinzufügung von Storage Nodes oder Speichervolumes vorgesehen werden, bevor die nutzbare Speicherkapazität des Grids aufgebraucht ist.

   Bei der Planung des Zeitpunkts einer Erweiterung ist zu berücksichtigen, wie lange die Beschaffung und Installation zusätzlicher Storage dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, kann es bevorzugt werden, die Erweiterung vorzunehmen, wenn die vorhandenen Speicherknoten etwa zu 70 % belegt sind, um die Anzahl der hinzuzufügenden Knoten zu reduzieren.

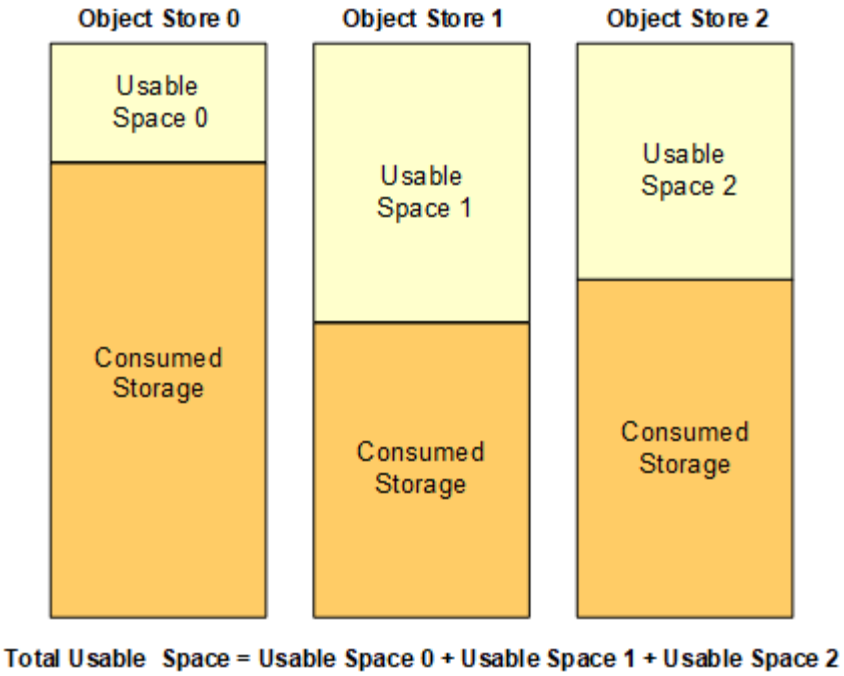
   Weitere Informationen zur Planung einer Speichererweiterung sind im "Anleitung zum Erweitern von StorageGRID" zu finden.

Speicherkapazität für jeden Storage Node überwachen

Der gesamte nutzbare Speicherplatz jedes Storage Node sollte überwacht werden, um sicherzustellen, dass der Node über ausreichend Speicherplatz für neue Objektdaten verfügt.

Über diese Aufgabe

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



Schritte

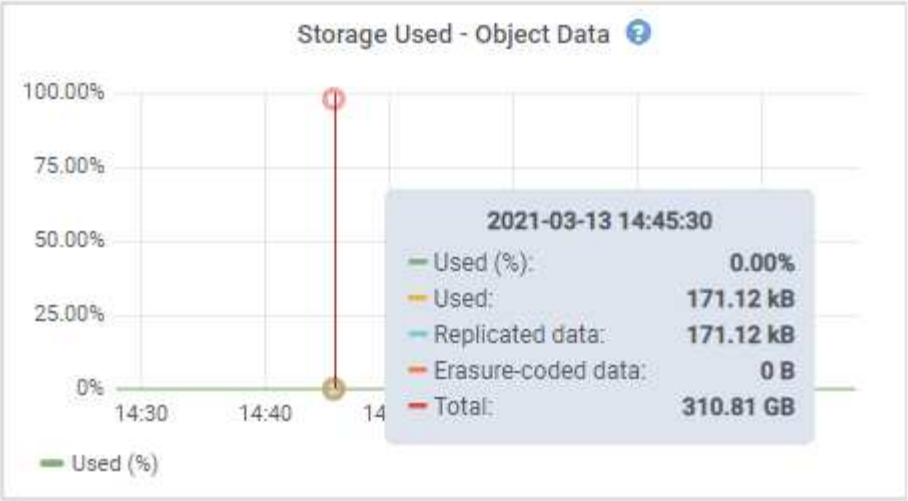
1. Wählen Sie **Nodes** > ***Storage Node*** > **Storage**.

   Die Diagramme und Tabellen für den Knoten werden angezeigt.

2. Positionieren Sie Ihren Cursor über das Diagramm „Storage used - object data“.

   Folgende Werte werden angezeigt:

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



3. Die verfügbaren Werte in den Tabellen „Volumes“ und „Object Stores“ unterhalb der Diagramme sind ersichtlich.

> Zum Anzeigen von Diagrammen dieser Werte auf die Diagrammsymbole in den verfügbaren Spalten klicken.

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. Die Werte sollten im Zeitverlauf überwacht werden, um die Geschwindigkeit abzuschätzen, mit der nutzbarer Speicherplatz verbraucht wird.
5. Um den normalen Systembetrieb aufrechtzuerhalten, Storage Nodes oder Speichervolumes hinzufügen oder Objektdaten archivieren, bevor der nutzbare Speicherplatz aufgebraucht ist.

   Bei der Planung des Zeitpunkts einer Erweiterung ist zu berücksichtigen, wie lange die Beschaffung und Installation zusätzlicher Storage dauern wird.

   > Wenn Ihre ILM-Richtlinie Erasure Coding verwendet, kann es bevorzugt werden, die Erweiterung vorzunehmen, wenn die vorhandenen Speicherknoten etwa zu 70 % belegt sind, um die Anzahl der hinzuzufügenden Knoten zu reduzieren.

Weitere Informationen zur Planung einer Speichererweiterung sind im "Anleitung zum Erweitern von

StorageGRID" zu finden.

Die "Niedriger Objektdatenspeicher" Warnung wird ausgelöst, wenn auf einem Storage Node nicht mehr genügend Speicherplatz für Objektdaten vorhanden ist.

Metadatenkapazität der Objekte für jeden Storage Node überwachen

Die Metadatennutzung jedes Storage Node sollte überwacht werden, damit ausreichend Speicherplatz für essentielle Datenbankoperationen verfügbar bleibt. Neue Storage Nodes müssen an jedem Standort hinzugefügt werden, bevor die Objektmetadaten 100 % des erlaubten Metadatenspeicherplatzes überschreiten.

Über diese Aufgabe

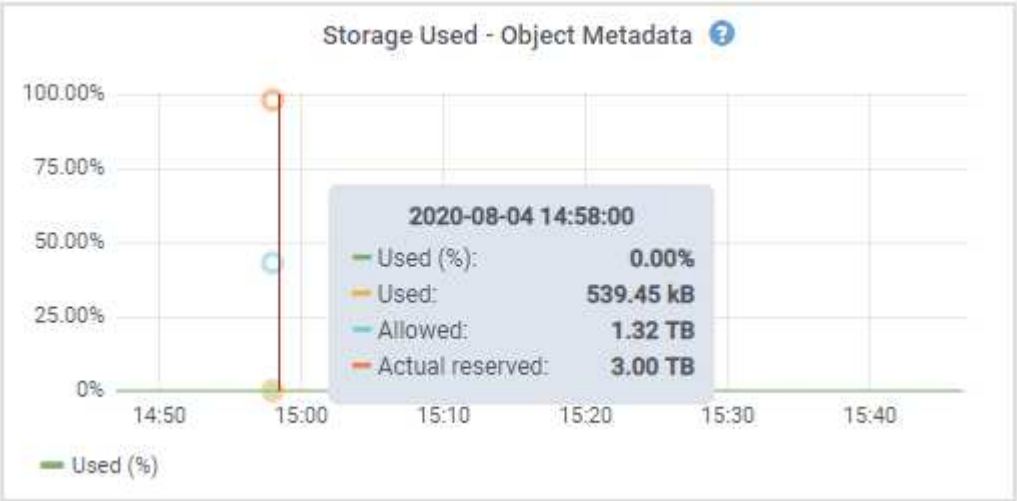
StorageGRID speichert an jedem Standort drei Kopien der Objektmetadaten, um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig auf alle Storage Nodes jedes Standorts verteilt und nutzen dabei den für Metadaten reservierten Speicherplatz auf Storage Volume 0 jedes Storage Node.

In manchen Fällen kann die Metadatenkapazität des Grids schneller erschöpft sein als seine Objektspeicherkapazität. Beispielsweise kann es erforderlich sein, Storage Nodes hinzuzufügen, um die Metadatenkapazität zu erhöhen, wenn typischerweise große Mengen kleiner Objekte aufgenommen werden, auch wenn noch ausreichend Objektspeicherkapazität vorhanden ist.

Zu den Faktoren, die die Nutzung von Metadaten erhöhen können, gehören die Größe und Menge der Benutzermetadaten und Tags, die Gesamtzahl der Teile bei einem Multipart-Upload und die Häufigkeit von Änderungen an den ILM-Speicherorten.

Schritte

1. Wählen Sie **Nodes** > ***Storage Node*** > **Storage**.
2. Positionieren Sie den Mauszeiger über das Diagramm „Storage used - object metadata“, um die Werte für einen bestimmten Zeitpunkt anzuzeigen.



Verwendet (%)

Der Prozentsatz des zulässigen Metadatenbereichs, der auf diesem Storage Node verwendet wurde.

Prometheus Metriken: `storagegrid_storage_utilization_metadata_bytes` und `storagegrid_storage_utilization_metadata_allowed_bytes`

Gebraucht

Die Bytes des zulässigen Metadatenbereichs, die auf diesem Storage Node verwendet wurden.

Prometheus Metrik: `storagegrid_storage_utilization_metadata_bytes`

Erlaubt

Der für Objektmetadaten auf diesem Storage Node vorgesehene Speicherplatz. Wie dieser Wert für jeden Storage Node bestimmt wird, ist im "vollständige Beschreibung des zulässigen Metadatenbereichs" beschrieben.

Prometheus Metrik: `storagegrid_storage_utilization_metadata_allowed_bytes`

Tatsächlich reserviert

Der tatsächlich für Metadaten auf diesem Storage Node reservierte Speicherplatz. Umfasst den zulässigen Speicherplatz und den für essentielle Metadatenoperationen erforderlichen Speicherplatz. Wie dieser Wert für jeden Storage Node berechnet wird, ist im "vollständige Beschreibung des tatsächlich reservierten Speicherplatzes für Metadaten" beschrieben.

Die Prometheus-Metrik wird in einer zukünftigen Version hinzugefügt.

> Die Gesamtwerte für einen Standort oder das Grid beinhalten keine Knoten, die seit mindestens fünf Minuten keine Metriken gemeldet haben, wie zum Beispiel Offline-Knoten.

3. Wenn der Wert **Auslastung (%)** 70 % oder höher ist, sollte das StorageGRID System durch das Hinzufügen von Storage Nodes zu jedem Standort erweitert werden.

> Die Warnung „Geringer Metadatenspeicher“ wird ausgelöst, wenn der Wert für „Belegt (%)“ bestimmte Schwellenwerte erreicht. Unerwünschte Ergebnisse können auftreten, wenn Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes belegen.

Beim Hinzufügen neuer Knoten gleicht das System die Objektmetadaten automatisch auf alle Storage Nodes innerhalb des Standorts aus. Siehe "Anleitung zur Erweiterung eines StorageGRID Systems".

Raumnutzungsprognosen überwachen

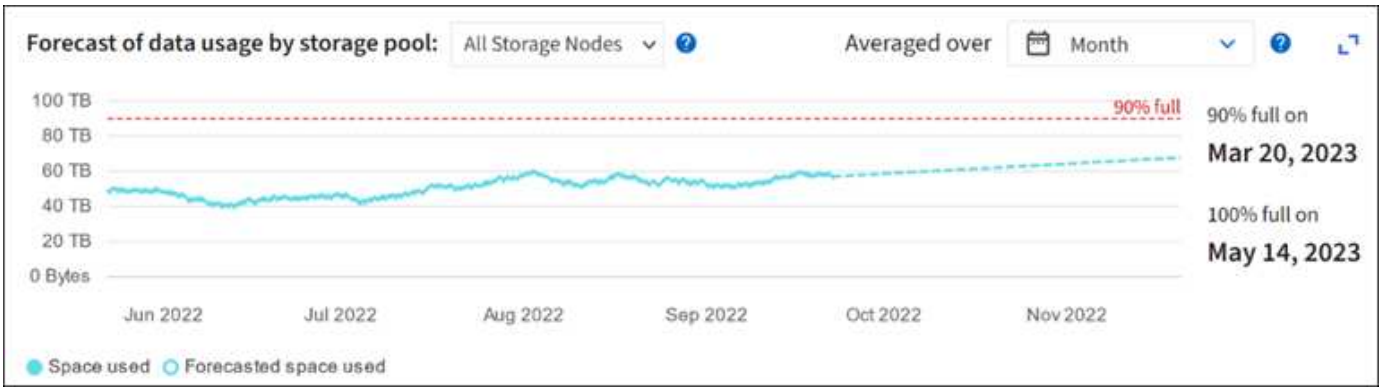
Prognosen zur Speichernutzung von Benutzerdaten und Metadaten überwachen, um abzuschätzen, wann "ein Grid erweitern" erforderlich sein wird.

Wenn Sie feststellen, dass sich die Verbrauchsrate im Laufe der Zeit ändert, wählen Sie im Dropdown-Menü **Durchschnitt über** einen kürzeren Zeitraum, um nur die aktuellsten Ingest-Muster abzubilden. Wenn saisonale Muster erkennbar sind, empfiehlt sich die Auswahl eines längeren Zeitraums.

Bei einer neuen StorageGRID Installation empfiehlt es sich, zunächst genügend Daten und Metadaten ansammeln zu lassen, bevor die Prognosen zur Speicherplatznutzung ausgewertet werden.

Schritte

1. Im Dashboard die Option **Speicher** auswählen.
2. Die Dashboard-Karten Prognose der Datennutzung nach Speicherpool und Prognose der Metadatennutzung nach Standort werden angezeigt.
3. Anhand dieser Werte lässt sich abschätzen, wann neue Storage Nodes für die Daten- und Metadatenspeicherung hinzugefügt werden müssen.



Überwachen Sie das Informationslebenszyklusmanagement in StorageGRID

Das Informationslebenszyklusmanagement-System (ILM) bietet Datenmanagement für alle im Grid gespeicherten Objekte. Es ist erforderlich, die ILM-Operationen zu überwachen, um zu verstehen, ob das Grid die aktuelle Last bewältigen kann oder ob zusätzliche Ressourcen benötigt werden.

Über diese Aufgabe

Das StorageGRID System verwaltet Objekte durch Anwendung der aktiven ILM-Richtlinien. Die ILM-Richtlinien und zugehörigen ILM-Regeln legen fest, 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, mit der StorageGRID ILM auswerten kann, übersteigen, wodurch das System Objekte, deren ILM-Platzierungsanweisungen nicht nahezu in Echtzeit erfüllt werden können, in eine Warteschlange stellt. Es sollte überwacht werden, ob StorageGRID mit den Clientaktionen Schritt hält.

Die Registerkarte „Grid Manager Dashboard“ verwenden

Schritte

Die Registerkarte „ILM“ auf dem Grid Manager Dashboard bietet eine Übersicht zur Überwachung von ILM-Vorgängen:

1. Melden Sie sich beim Grid Manager an.
2. Im Dashboard die Registerkarte ILM auswählen und die Werte auf der ILM-Warteschlangenkarte (Objekte) und der ILM-Bewertungsratenkarte notieren.

   Vorübergehende Spitzenwerte in der ILM-Warteschlange (Objekte) auf dem Dashboard sind zu erwarten. Wenn die Warteschlange jedoch kontinuierlich ansteigt und nicht abnimmt, benötigt das Grid mehr Ressourcen für einen effizienten Betrieb: entweder mehr Storage Nodes oder, falls die ILM-Richtlinie Objekte an entfernten Standorten platziert, mehr Bandbreite.

Die Seite „Knoten“ verwenden

Schritte

Zusätzlich können die ILM-Warteschlangen über die Seite **Knoten** untersucht werden:

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

1. Wählen Sie **Knoten**.
2. ***grid name*** > **ILM** auswählen.
3. Positionieren Sie den Cursor über den ILM-Warteschlangengraphen, um den Wert der folgenden Attribute zu einem bestimmten Zeitpunkt zu sehen:
   - **Objekte in der Warteschlange (aus Clientoperationen)**: Die Gesamtzahl der Objekte, die aufgrund von Clientoperationen (zum Beispiel Ingest) auf die ILM-Auswertung warten.
   - **Objekte in der Warteschlange (aus allen Operationen)**: Die Gesamtzahl der Objekte, die auf die ILM-Auswertung warten.
   - **Scanrate (Objekte/Sek.)**: Die Rate, mit der Objekte im Grid gescannt und für ILM in die Warteschlange gestellt werden.
   - **Auswertungsrate (Objekte/Sek.)**: Die aktuelle Rate, mit der Objekte im Grid anhand der ILM-Richtlinie ausgewertet werden.

     Der Abschnitt „ILM-Warteschlange“ ist nur für das Grid enthalten. Diese Informationen werden auf der Registerkarte „ILM“ für einen Standort oder Storage Node nicht angezeigt.
4. Im Abschnitt ILM-Warteschlange werden die folgenden Attribute angezeigt.
   - **Scandauer - geschätzt**: Die geschätzte Zeit für einen vollständigen ILM-Scan aller Objekte.

     Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde.
   - **Reparaturversuche**: Die Gesamtzahl der Objektreparaturvorgänge für replizierte Daten, die versucht wurden. Dieser Zähler wird jedes Mal erhöht, wenn ein Storage Node versucht, ein Objekt mit hohem Risiko zu reparieren. ILM-Reparaturen mit hohem Risiko erhalten Priorität, wenn das Grid ausgelastet ist.

     Die Reparatur desselben Objekts kann erneut inkrementiert werden, wenn die Replikation nach der Reparatur fehlgeschlagen ist. + Diese Attribute können nützlich sein, wenn der Fortschritt der Storage Node Volume-Wiederherstellung überwacht wird. Wenn die Anzahl der durchgeführten Reparaturen nicht mehr ansteigt und ein vollständiger Scan abgeschlossen wurde, ist die Reparatur wahrscheinlich abgeschlossen.
5. Alternativ lässt sich eine Prometheus-Abfrage für `storagegrid_ilm_scan_period_estimated_minutes` und `storagegrid_ilm_repairs_attempted` einreichen.

Überwachen Sie Netzwerk- und Systemressourcen in StorageGRID

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

Netzwerkverbindungen und Leistung überwachen

Netzwerkverbindung und Bandbreite sind besonders wichtig, wenn Ihre Richtlinie für das Informationslebenszyklusmanagement (ILM) replizierte Objekte zwischen Standorten kopiert oder Objekte mit Löschcodierung mithilfe eines Schemas speichert, das Schutz vor Standortverlust bietet. Ist das Netzwerk zwischen den Standorten nicht verfügbar, die Netzwerklatenz zu hoch oder die Bandbreite unzureichend, können einige ILM-Regeln Objekte möglicherweise nicht am erwarteten Ort platzieren. Dies kann zu Fehlern

bei der Aufnahme (wenn die Option „Strenge Aufnahme“ für ILM-Regeln ausgewählt ist) oder zu einer schlechten Aufnahmeleistung und ILM-Rückständen führen.

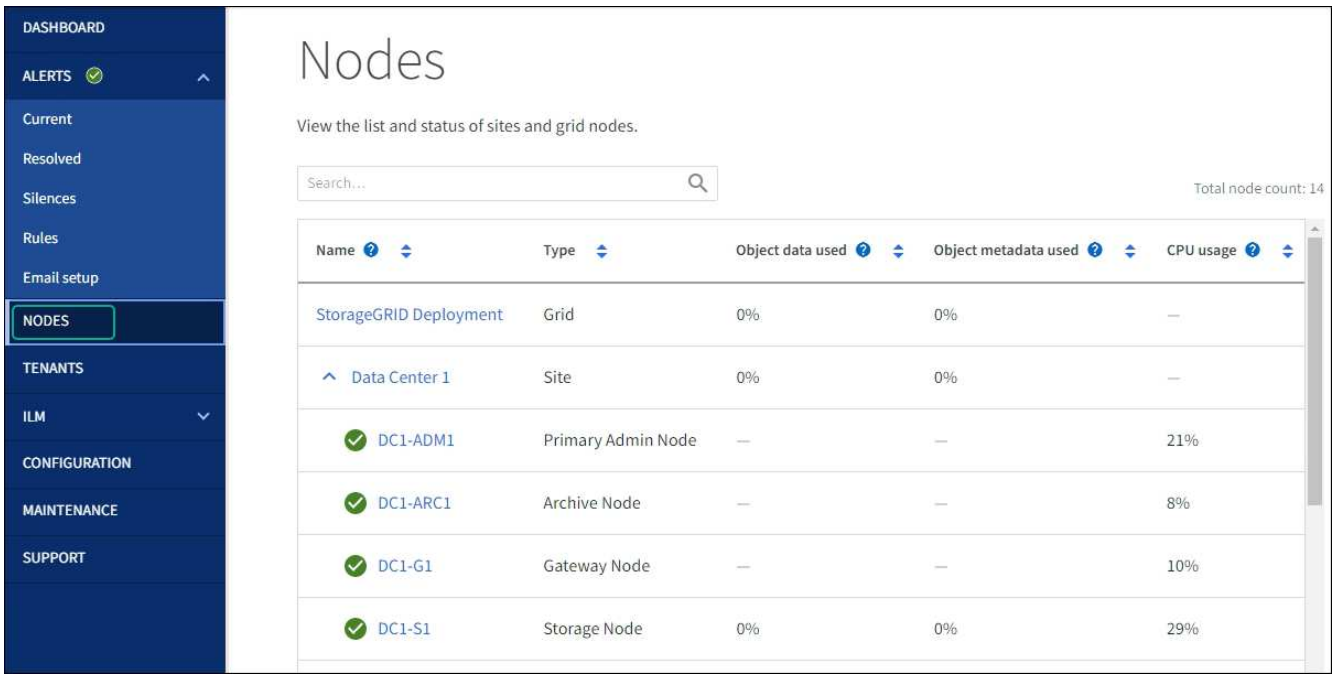
Mit dem Grid Manager lassen sich Konnektivität und Netzwerkleistung überwachen, sodass etwaige Probleme umgehend behoben werden können.

Zusätzlich sollte "Erstellung von Richtlinien zur Klassifizierung des Netzwerkverkehrs" in Betracht gezogen werden, um den Datenverkehr bestimmter Mandanten, Buckets, Subnetze oder Load-Balancer-Endpunkte überwachen zu können. Richtlinien zur Begrenzung des Datenverkehrs können nach Bedarf festgelegt werden.

Schritte

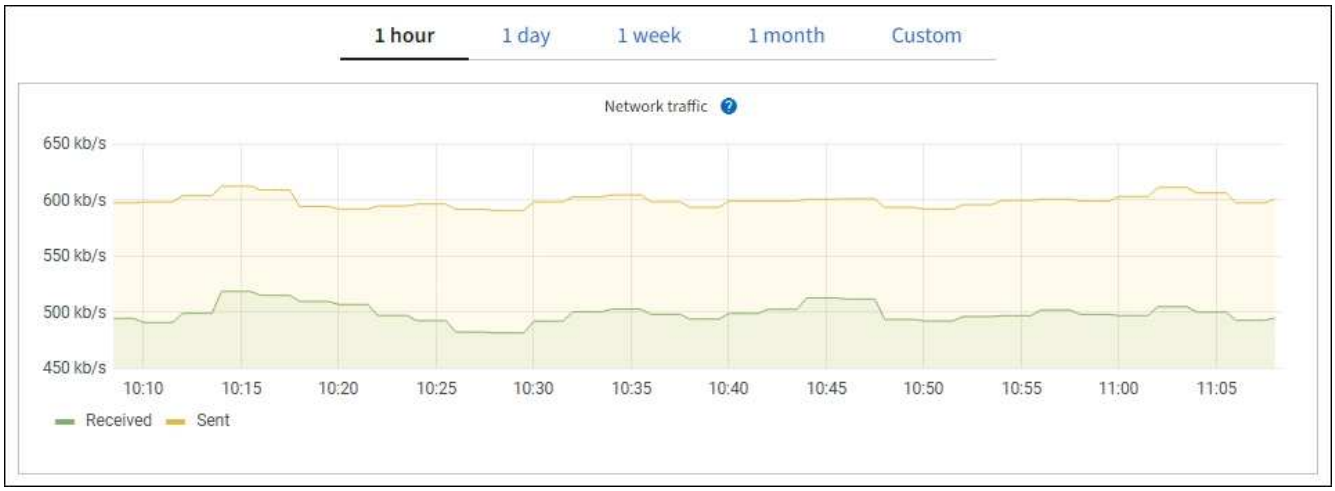
1. Wählen Sie **Knoten**.

   Die Seite „Knoten“ wird angezeigt. Jeder Knoten im Grid wird tabellarisch aufgelistet.



2. Den Grid-Namen, einen bestimmten Rechenzentrumsstandort oder einen Grid-Knoten auswählen und anschließend die Registerkarte **Netzwerk** auswählen.

   Das Netzwerkverkehrsdiagramm bietet eine Übersicht über den gesamten Netzwerkverkehr für das Grid als Ganzes, den Rechenzentrumsstandort oder den Knoten.



a. Wenn ein Grid-Knoten ausgewählt wurde, kann der Abschnitt **Netzwerkschnittstellen** der Seite weiter unten eingesehen werden.

Network interfaces

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

b. Für Grid-Knoten nach unten scrollen, um den Abschnitt **Netzwerkkommunikation** auf der Seite zu überprüfen.

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

Network communication

Receive

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

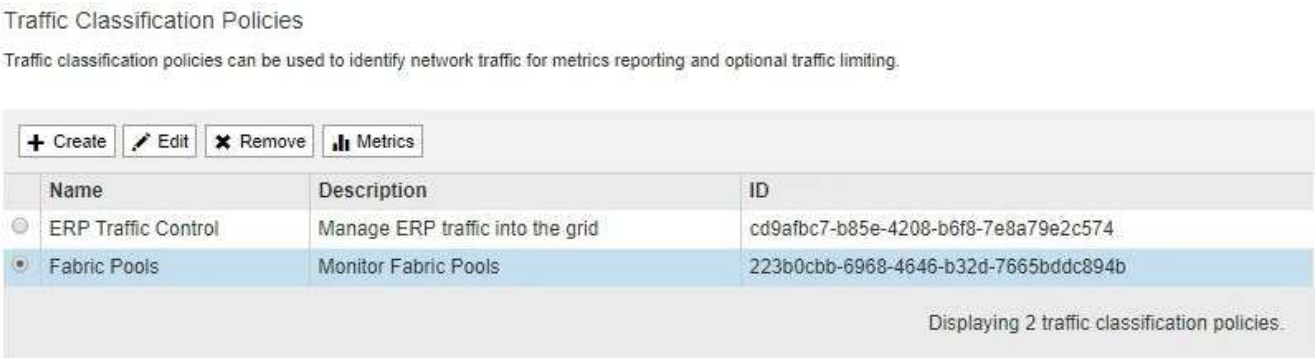
Transmit

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

3. Die mit den Richtlinien zur Verkehrsklassifizierung verknüpften Metriken ermöglichen die Überwachung des Netzwerkverkehrs.

a. **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung** auswählen.

Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt und die bestehenden Richtlinien sind in der Tabelle aufgeführt.



a. Zur Anzeige von Diagrammen, die die mit einer Richtlinie verknüpften Netzwerkmetriken darstellen, das Optionsfeld links neben der Richtlinie auswählen und anschließend auf **Metriken** klicken.

b. Anhand der Diagramme lässt sich der mit der Richtlinie verbundene Netzwerkverkehr nachvollziehen.

   Wenn eine Richtlinie zur Verkehrsklassifizierung darauf ausgelegt ist, den Netzwerkverkehr zu begrenzen, sollte analysiert werden, wie häufig der Verkehr begrenzt wird, und ob die Richtlinie weiterhin den Anforderungen entspricht. Von Zeit zu Zeit "Jede Richtlinie zur Verkehrsklassifizierung kann bei Bedarf angepasst werden.".

Verwandte Informationen

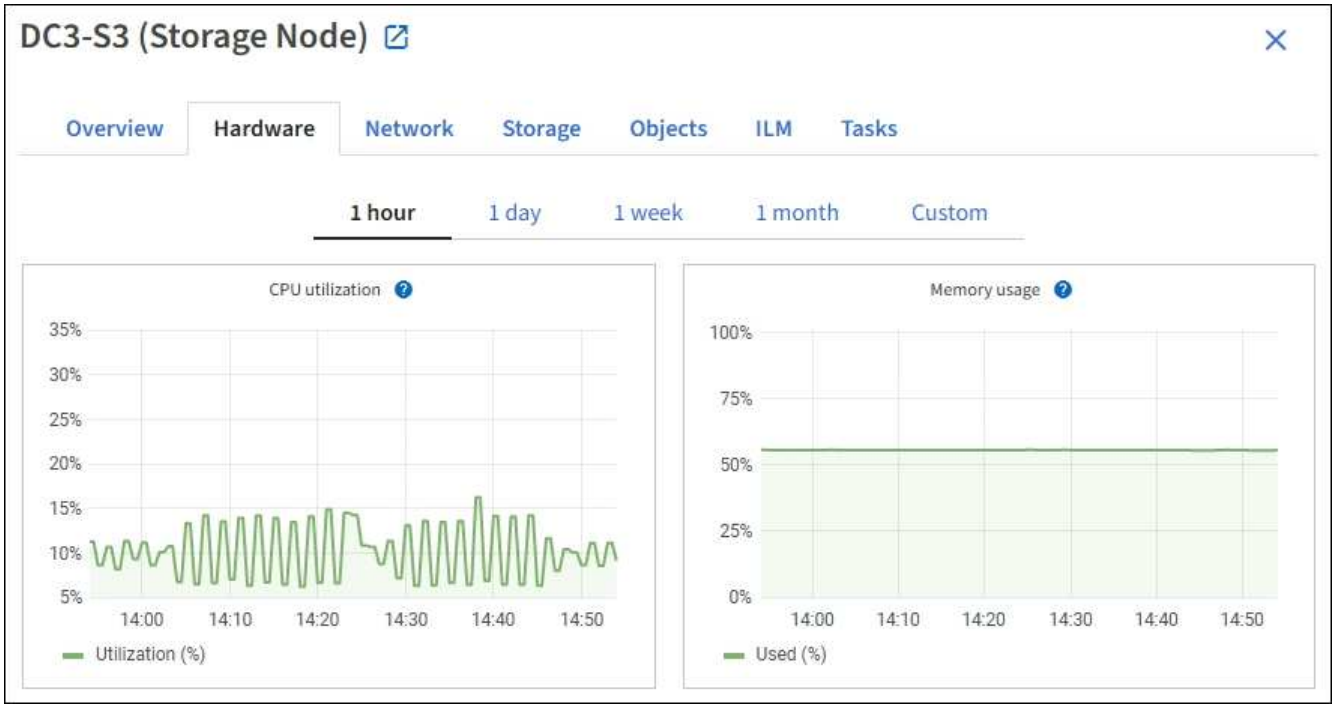
- "Netzwerk-Registerkarte anzeigen"
- "Verbindungszustände der Überwachungsknoten"

Ressourcen auf Knotenebene überwachen

Die einzelnen Grid-Knoten werden überwacht, um deren Ressourcenauslastung zu prüfen. Wenn Knoten dauerhaft überlastet sind, könnten für einen effizienten Betrieb weitere Knoten erforderlich sein.

Schritte

1. Auf der Seite **Knoten** den Knoten auswählen.
2. Die Registerkarte **Hardware** zeigt Diagramme zur CPU-Auslastung und Speichernutzung an.



3. Um ein anderes Zeitintervall anzuzeigen, kann eines der Steuerelemente oberhalb des Diagramms oder der Grafik ausgewählt werden. Die verfügbaren Informationen können für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat angezeigt werden. Auch ein benutzerdefiniertes Intervall ist möglich, wodurch Datums- und Zeitbereiche angegeben werden können.
4. Wenn der Knoten auf einem Storage Appliance oder Services Appliance gehostet wird, nach unten scrollen, um die Tabellen der Komponenten anzuzeigen. Der Status aller Komponenten sollte „Nominal“ sein. Komponenten mit einem anderen Status sollten überprüft werden.

Verwandte Informationen

- "Informationen zu Appliance Storage Nodes anzeigen"
- "Informationen zu Appliance Admin-Nodes und Gateway-Nodes"

Überwachen Sie die Mieteraktivität in StorageGRID

Sämtliche S3-Clientaktivitäten sind StorageGRID Mandantenkonten zugeordnet. Mit dem Grid Manager ist eine Überwachung der Speichernutzung oder des Netzwerkverkehrs für alle Mandanten oder einen bestimmten Mandanten möglich. Das Revisionsprotokoll oder die Grafana Dashboards liefern detailliertere Informationen darüber, wie Mandanten StorageGRID nutzen.

Bevor Sie beginnen

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

Alle Mandanten anzeigen

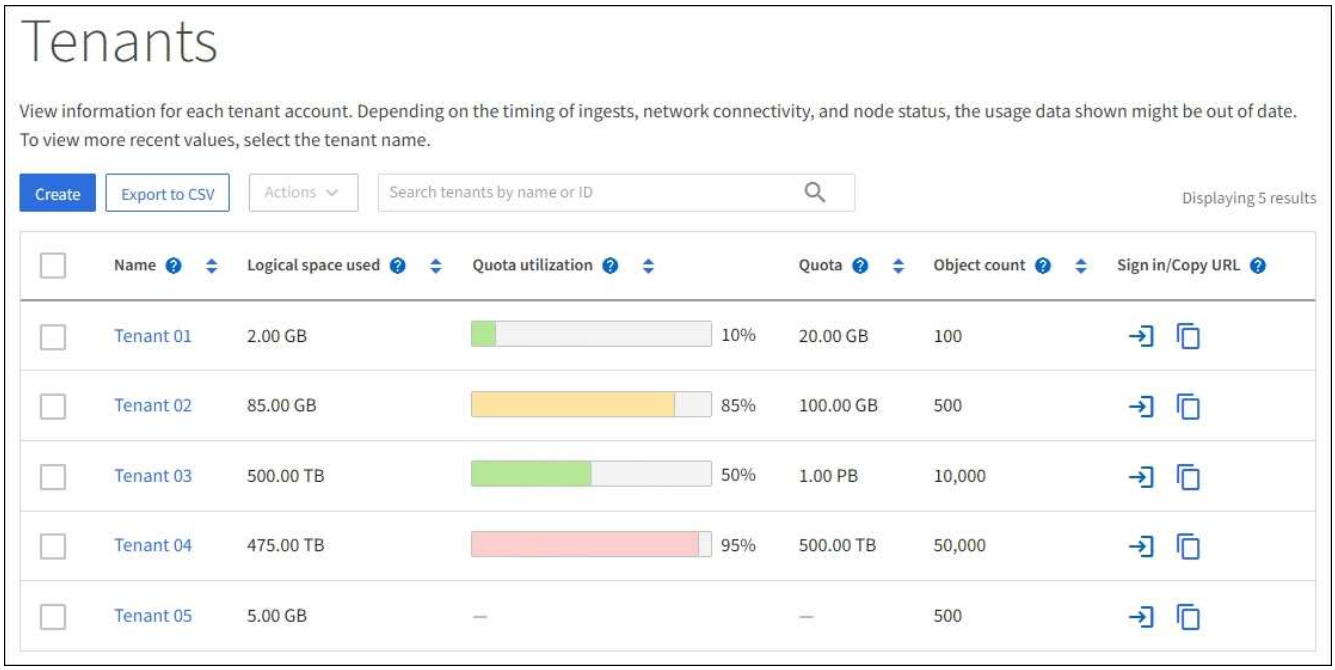
Die Seite „Mieter“ zeigt grundlegende Informationen zu allen aktuellen Mieterkonten.

Schritte

1. **Tenants** auswählen.
2. Die auf den Mieterseiten angezeigten Informationen werden angezeigt.

   Für jeden Mandanten werden der belegte logische Speicherplatz, die Kontingentnutzung, das Kontingent und die Anzahl der Objekte aufgeführt. Wenn für einen Mandanten kein Kontingent festgelegt ist, enthalten die Felder Kontingentnutzung und Kontingent einen Bindestrich (—).

   > Die logische Größe aller Objekte dieses Mandanten umfasst unvollständige und laufende Multipart-Uploads. Die Größe enthält keinen zusätzlichen physischen Speicherplatz, der für ILM-Richtlinien verwendet wird. Die Werte für den verwendeten Speicherplatz sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Datenaufnahme, die Netzwerkverbindung und den Knotenstatus beeinflusst.



3. Optional ist eine Anmeldung bei einem Mandantenkonto möglich, indem der Anmeldelink in der Spalte **Anmelden/URL kopieren** ausgewählt wird.
4. Optional kann die URL der Anmeldeseite eines Mandanten kopiert werden, indem der Link „URL kopieren“ in der Spalte „Anmelden/URL kopieren“ ausgewählt wird.
5. Optional kann **Exportieren nach CSV** ausgewählt werden, um eine `.csv` Datei mit den Nutzungswerten für alle Mandanten anzuzeigen und zu exportieren.

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

   Der Inhalt der `.csv` Datei sieht beispielsweise so aus:

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

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

verwenden.

6. Falls keine Objekte aufgelistet sind, kann optional **Aktionen** > **Löschen** ausgewählt werden, um einen oder mehrere Mandanten zu entfernen. Siehe "Mandantenkonto löschen".

   Ein Mandantenkonto kann nicht entfernt werden, wenn das Konto Buckets oder Container enthält.

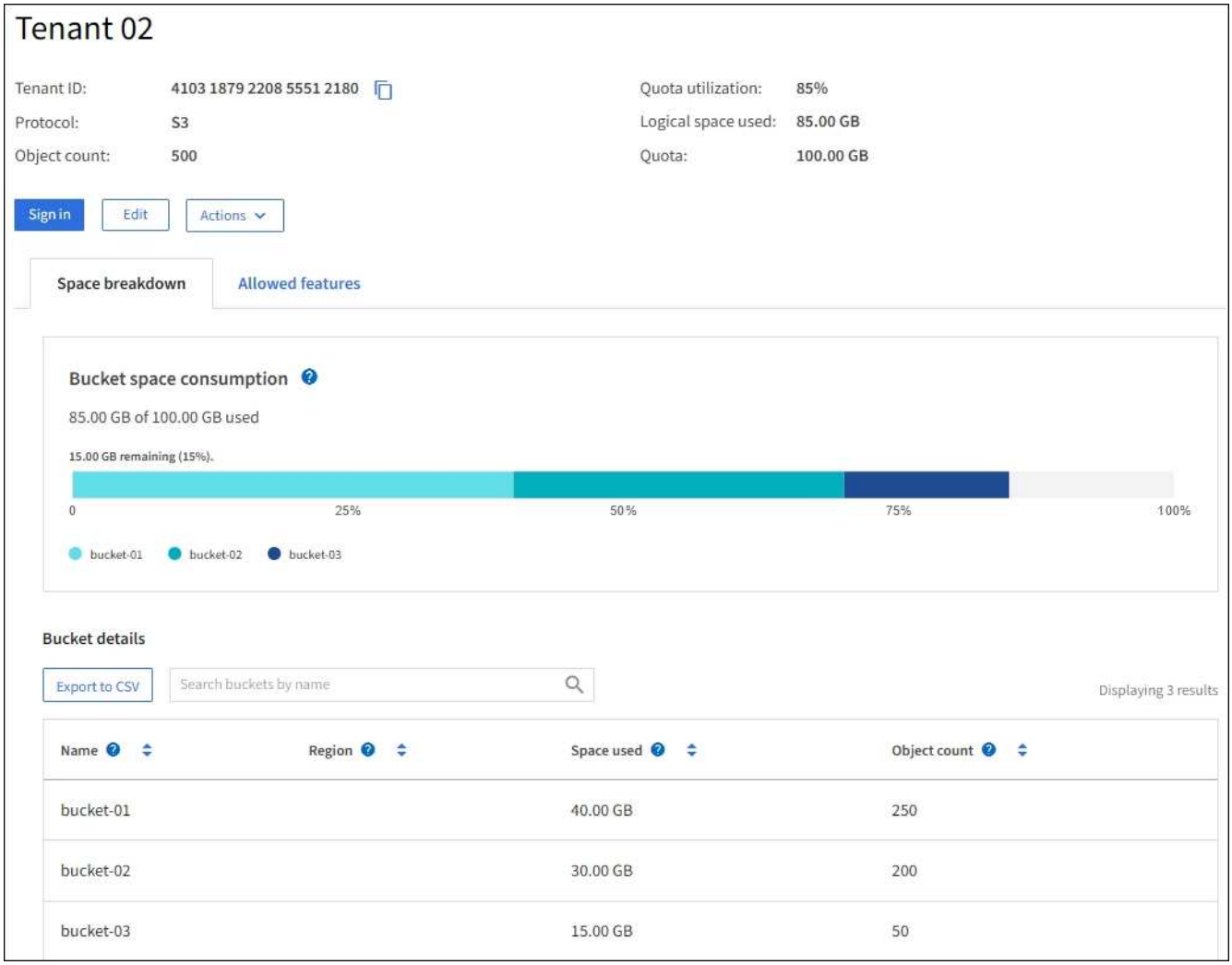
Einen bestimmten Mandanten anzeigen

Sie können Details zu einem bestimmten Mandanten einsehen.

Schritte

1. Der Name des Mieters wird auf der Seite „Mieter“ ausgewählt.

   Die Mieterdetailseite wird angezeigt.



2. Die Mieterübersicht befindet sich oben auf der Seite.

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

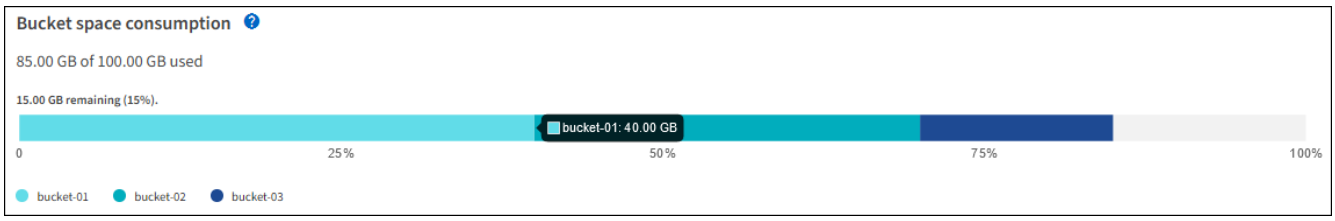
Die logische Größe aller Objekte dieses Mandanten umfasst unvollständige und laufende Multipart-Uploads. Die Größe enthält keinen zusätzlichen physischen Speicherplatz, der für ILM-Richtlinien verwendet wird. Die Werte für den verwendeten Speicherplatz sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Datenaufnahme, die Netzwerkverbindung und den Knotenstatus beeinflusst.

3. Auf der Registerkarte **Platzaufteilung** befindet sich das Diagramm **Platzverbrauch** zur Überprüfung.

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

   Wurde für diesen Mandanten ein Kontingent festgelegt, wird die genutzte und verbleibende Kontingentmenge als Text angezeigt (zum Beispiel, `85.00 GB of 100 GB used`). Wurde kein Kontingent festgelegt, verfügt der Mandant über ein unbegrenztes Kontingent, und der Text enthält nur die belegte Speichermenge (zum Beispiel, `85.00 GB used`). Das Balkendiagramm zeigt den Prozentsatz des Kontingents in jedem Bucket oder Container. Wenn der Mandant das Speicherkontingent um mehr als 1 % und mindestens 1 GB überschritten hat, zeigt das Diagramm das Gesamtkontingent und den Überschuss an.

   Sie können den Mauszeiger über das Balkendiagramm bewegen, um den von jedem Bucket oder Container belegten Speicherplatz zu sehen. Sie können den Mauszeiger über das Segment für freien Speicherplatz bewegen, um die verbleibende Speicherkontingentmenge zu sehen.



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

Die Kontingentnutzung eines Mandanten gibt die Gesamtmenge der Objektdaten an, die der Mandant in StorageGRID hochgeladen hat (logische Größe). Die Kontingentnutzung entspricht nicht dem Speicherplatz, der für die Speicherung von Kopien dieser Objekte und ihrer Metadaten verwendet wird (physische Größe).

Die Warnregel **Tenant quota usage high** kann aktiviert werden, um festzustellen, ob Mandanten ihre Kontingente verbrauchen. Wenn aktiviert, wird diese Warnung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Anweisungen finden Sie unter "Benachrichtigungsregeln bearbeiten".

4. Auf der Registerkarte **Space breakdown** werden die **Bucket details** angezeigt.

   Diese Tabelle listet die S3-Buckets des Mandanten auf. Der belegte Speicherplatz entspricht der Gesamtmenge der Objektdaten im Bucket oder Container. Dieser Wert entspricht nicht dem Speicherplatz,

der für ILM-Kopien und Objektmetadaten erforderlich ist.

5. Optional kann **Exportieren nach CSV** ausgewählt werden, um eine .csv-Datei mit den Nutzungswerten für jeden Bucket oder Container anzuzeigen und zu exportieren.

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

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

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

6. Optional kann die Registerkarte **Zugelassene Funktionen** ausgewählt werden, um eine Liste der für den Mandanten aktivierten Berechtigungen und Funktionen anzuzeigen. Siehe "Mandantenkonto bearbeiten", falls eine Änderung dieser Einstellungen erforderlich ist.
7. Verfügt der Mandant über die Berechtigung **Use grid federation connection**, kann optional die Registerkarte **Grid federation** ausgewählt werden, um mehr über die Verbindung zu erfahren.

   Siehe "Was ist Grid Federation?" und "Verwaltung der zulässigen Mandanten für die Grid Federation".

Netzwerkverkehr anzeigen

Wenn für einen Mandanten Richtlinien zur Verkehrsklassifizierung eingerichtet sind, sollte der Netzwerkverkehr für diesen Mandanten überprüft werden.

Schritte

1. **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung** auswählen.

   Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt und die bestehenden Richtlinien sind in der Tabelle aufgeführt.

2. Die Liste der Richtlinien kann überprüft werden, um diejenigen zu identifizieren, die für einen bestimmten Mieter gelten.
3. Die mit einer Richtlinie verknüpften Metriken werden angezeigt, indem das Optionsfeld links neben der Richtlinie ausgewählt und **Metriken** ausgewählt wird.
4. Die Diagramme geben Aufschluss darüber, wie häufig die Richtlinie den Datenverkehr einschränkt und ob eine Anpassung der Richtlinie erforderlich ist.

Siehe "Verkehrsklassifizierungsrichtlinien verwalten" für weitere Informationen.

Das Revisionsprotokoll verwenden

Optional ist die Nutzung des Revisionsprotokolls für eine detailliertere Überwachung der Aktivitäten eines Mandanten möglich.

Beispielsweise können Sie die folgenden Arten von Informationen überwachen:

- Spezifische Client-Operationen, wie PUT, GET oder DELETE

- Objektgrößen
- Die ILM-Regel, die auf Objekte angewendet wird
- Die Quell-IP-Adresse der Clientanfragen

Revisionsprotokolle werden in Textdateien geschrieben, die mit einem Log-Analyse-Tool Ihrer Wahl ausgewertet werden können. Dadurch entsteht ein besseres Verständnis der Client-Aktivitäten oder es lassen sich ausgefeilte Kostenverrechnungs- und Abrechnungsmodelle umsetzen.

Siehe "Audit-Protokolle prüfen" für weitere Informationen.

Prometheus Metriken nutzen

Optional lassen sich Prometheus-Metriken zur Berichterstattung über die Aktivitäten der Mandanten verwenden.

- Im Grid Manager unter **Support** > **Tools** > **Metriken** auswählen. Vorhandene Dashboards wie S3 Overview können zur Überprüfung von Clientaktivitäten genutzt werden.

> Die auf der Seite „Metriken“ verfügbaren Tools sind primär für den Einsatz durch den technischen Support vorgesehen. Einige Funktionen und Menüpunkte innerhalb dieser Tools sind absichtlich nicht funktionsfähig.

- Oben im Grid Manager das Hilfesymbol auswählen und anschließend **API documentation** wählen. Die Metriken im Abschnitt Metrics der Grid Management API ermöglichen das Erstellen benutzerdefinierter Alarmregeln und Dashboards für die Mandantenaktivität.

Siehe "Support-Metriken überprüfen" für weitere Informationen.

Überwachen Sie S3-Clientvorgänge in StorageGRID

Sie können die Geschwindigkeit der Objektaufnahme und -abfrage sowie Metriken für Objektanzahl, Abfragen und Verifizierung überwachen. Sie können die Anzahl erfolgreicher und fehlgeschlagener Versuche von Clientanwendungen zum Lesen, Schreiben und Ändern von Objekten im StorageGRID System einsehen.

Bevor Sie beginnen

Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

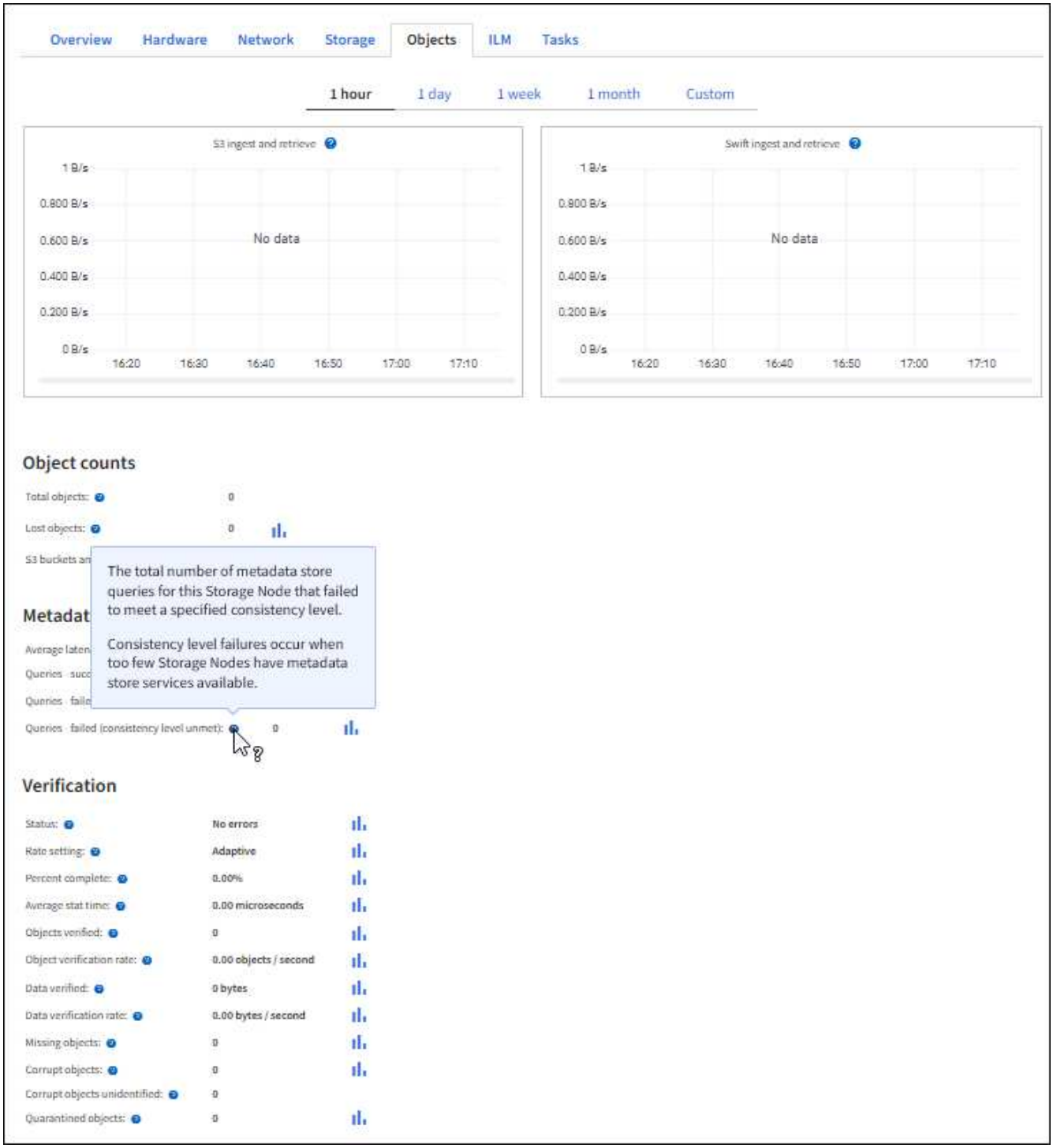
Schritte

1. Im Dashboard die Registerkarte **Leistung** auswählen.
2. Siehe die S3-Diagramme, die die Anzahl der von den Storage Nodes durchgeführten Client-Operationen und die Anzahl der von den Storage Nodes empfangenen API-Anfragen im ausgewählten Zeitraum zusammenfassen.
3. **Knoten** auswählen, um auf die Seite „Knoten“ zuzugreifen.
4. Auf der Startseite von Nodes (Grid-Ebene) die Registerkarte **Objekte** auswählen.

   Das Diagramm zeigt die S3-Aufnahme- und -Abrufraten für Ihr gesamtes StorageGRID System in Byte pro Sekunde sowie die aufgenommene oder abgerufene Datenmenge. Es besteht die Möglichkeit, ein Zeitintervall auszuwählen oder ein benutzerdefiniertes Intervall anzuwenden.

5. Informationen zu einem bestimmten Storage Node werden angezeigt, wenn der Node in der Liste auf der linken Seite ausgewählt und die Registerkarte **Objekte** ausgewählt wird.

   Das Diagramm zeigt die Aufnahme- und Abrufraten für den Knoten. Die Registerkarte enthält außerdem Metriken für Objektanzahlen, Metadatenabfragen und Verifizierungsvorgänge.



Überwachen Sie die Lastverteilungsvorgänge in StorageGRID

Wenn Sie einen Load Balancer zur Verwaltung von Clientverbindungen zu StorageGRID verwenden, empfiehlt es sich, die Load-Balancing-Vorgänge nach der anfänglichen

Konfiguration des Systems sowie nach Konfigurationsänderungen oder einer Erweiterung zu überwachen.

Über diese Aufgabe

Sie können den Load Balancer Service auf Admin Nodes oder Gateway Nodes oder einen externen Load Balancer eines Drittanbieters verwenden, um Client-Anfragen auf mehrere Storage Nodes zu verteilen.

Nach der Konfiguration des Lastausgleichs sollte bestätigt werden, dass die Objekterfassungs- und -abrufvorgänge gleichmäßig auf die Storage Nodes verteilt werden. Eine gleichmäßige Verteilung der Anfragen stellt sicher, dass StorageGRID auch unter Last auf Clientanfragen reagiert und kann dazu beitragen, die Clientleistung aufrechtzuerhalten.

Wenn Sie eine Hochverfügbarkeitsgruppe (HA) von Gateway Nodes oder Admin Nodes im Aktiv-Backup-Modus konfiguriert haben, verteilt nur ein Node in der Gruppe aktiv Client-Anfragen.

Weitere Informationen finden sich unter "Konfiguration von S3 Clientverbindungen".

Schritte

1. Wenn S3-Clients über den Load Balancer Service eine Verbindung herstellen, sollte geprüft werden, ob die Admin Nodes oder Gateway Nodes den Datenverkehr wie erwartet aktiv verteilen:
   a. Wählen Sie **Knoten**.
   b. Es wird ein Gateway-Knoten oder ein Admin-Node ausgewählt.
   c. Auf der Registerkarte **Übersicht** lässt sich prüfen, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle „Primär“ hat.

      Knoten mit der Rolle „Primary“ und Knoten, die keiner HA-Gruppe angehören, sollten Anfragen aktiv an Clients verteilen.

   d. Für jeden Knoten, der aktiv Client-Anfragen verteilen soll, die "Registerkarte Load Balancer" auswählen.
   e. Das Diagramm des Load Balancer Request Traffic der letzten Woche gibt Aufschluss darüber, ob der Node aktiv Anforderungen verteilt hat.

      Knoten in einer Active-Backup HA-Gruppe können zeitweise die Backup-Rolle übernehmen. Während dieser Zeit verteilen die Knoten keine Client-Anfragen.

   f. Das Diagramm der eingehenden Anforderungsrate des Load Balancers für die letzte Woche bietet einen Überblick über den Objektdurchsatz des Knotens.
   g. Diese Schritte sind für jeden Admin Node oder Gateway Node im StorageGRID System zu wiederholen.
   h. Optional können Verkehrsklassifizierungsrichtlinien verwendet werden, um eine detailliertere Analyse des vom Load Balancer Service bedienten Datenverkehrs anzuzeigen.
2. Es sollte sichergestellt sein, dass diese Anfragen gleichmäßig auf die Storage Nodes verteilt werden.
   a. ***Storage Node*** > **LDR** > **HTTP** auswählen.
   b. Die Anzahl der **derzeit eingerichteten eingehenden Sitzungen** kann überprüft werden.
   c. Für jeden Storage Node im Grid wiederholen.

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

Überwachen Sie StorageGRID Grid-Federation-Verbindungen

Sie können grundlegende Informationen zu allen "${post_edited_translations.segment}"Verbindungen, detaillierte Informationen zu einer bestimmten Verbindung oder Prometheus-Metriken zu netzübergreifenden Replikationsvorgängen überwachen. Eine Verbindung kann von jedem Grid aus überwacht werden.

Bevor Sie beginnen

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

Alle Verbindungen anzeigen

Die Seite Grid federation zeigt grundlegende Informationen über alle Grid federation-Verbindungen und über alle Mandantenkonten, die zur Nutzung von Grid federation-Verbindungen berechtigt sind.

Schritte

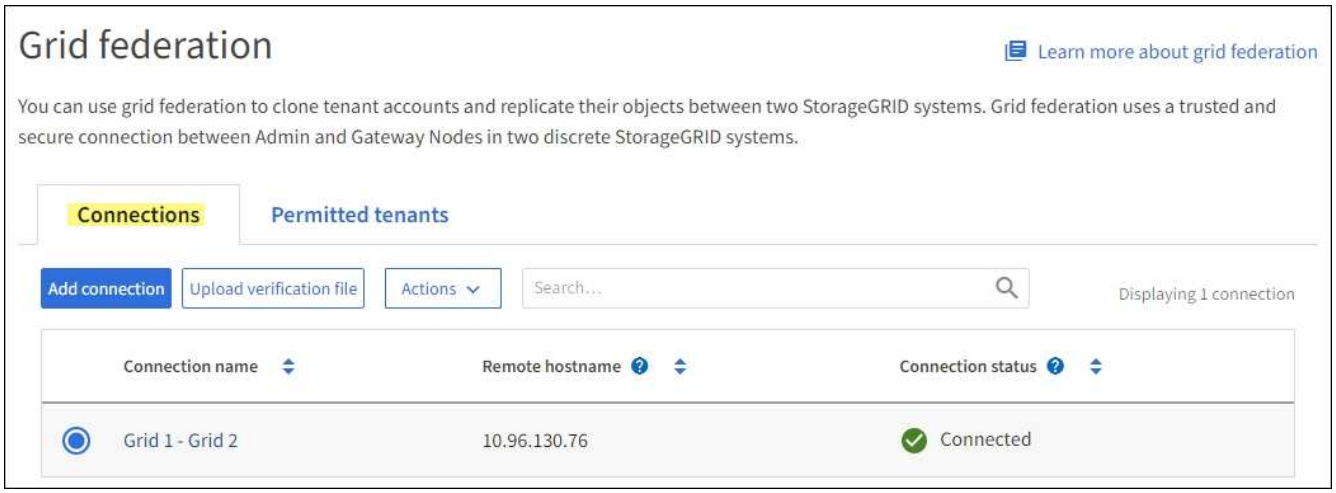
1. Wählen Sie **Konfiguration** > **System** > **Grid federation**.

   Die Grid federation Seite wird angezeigt.

2. Grundlegende Informationen zu allen Verbindungen in diesem Grid sind auf der Registerkarte **Verbindungen** zu finden.

   Über diese Registerkarte sind folgende Aktionen möglich:

   - "Neue Verbindung erstellen".
   - Wählen Sie eine bestehende Verbindung zu "bearbeiten oder testen".

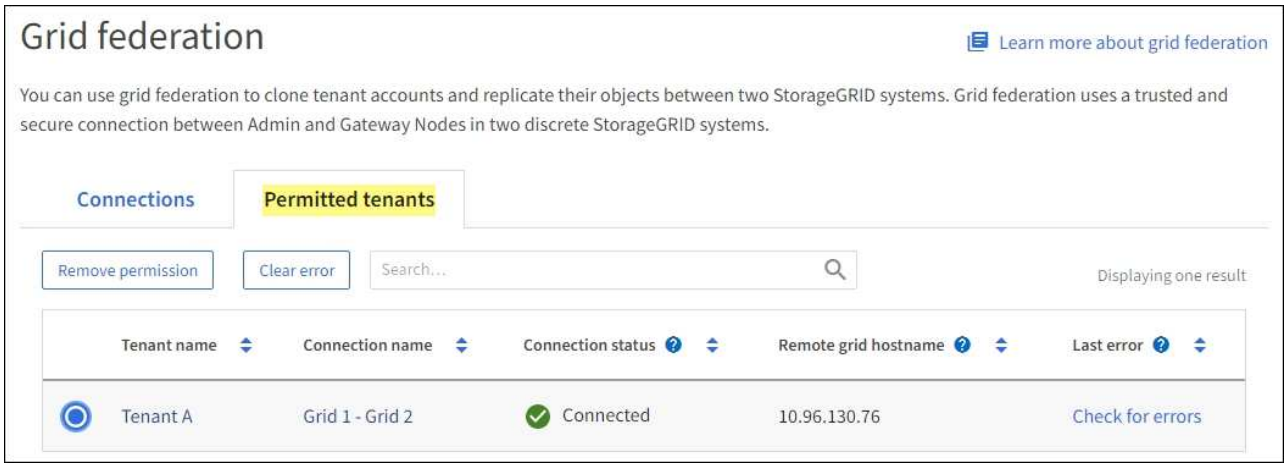


3. Grundlegende Informationen zu allen Mandantenkonten in diesem Grid, die über die Berechtigung **Grid-Federationsverbindung verwenden** verfügen, sind auf der Registerkarte **Zulässige Mandanten** zu finden.

   Über diese Registerkarte sind folgende Aktionen möglich:

   - "Die Detailseite für jeden zugelassenen Mandanten anzeigen".

- Die Detailseite für jede Verbindung kann angezeigt werden. Siehe Eine bestimmte Verbindung anzeigen.
- Wählen Sie einen zulässigen Mandanten aus und "die Berechtigung entfernen".
- Auf Fehler bei der gridübergreifenden Replikation prüfen und den letzten Fehler gegebenenfalls beheben. Siehe "Fehler in der Grid-Federation beheben".



Eine bestimmte Verbindung anzeigen

Details zu einer bestimmten Grid Federation Verbindung können angezeigt werden.

Schritte

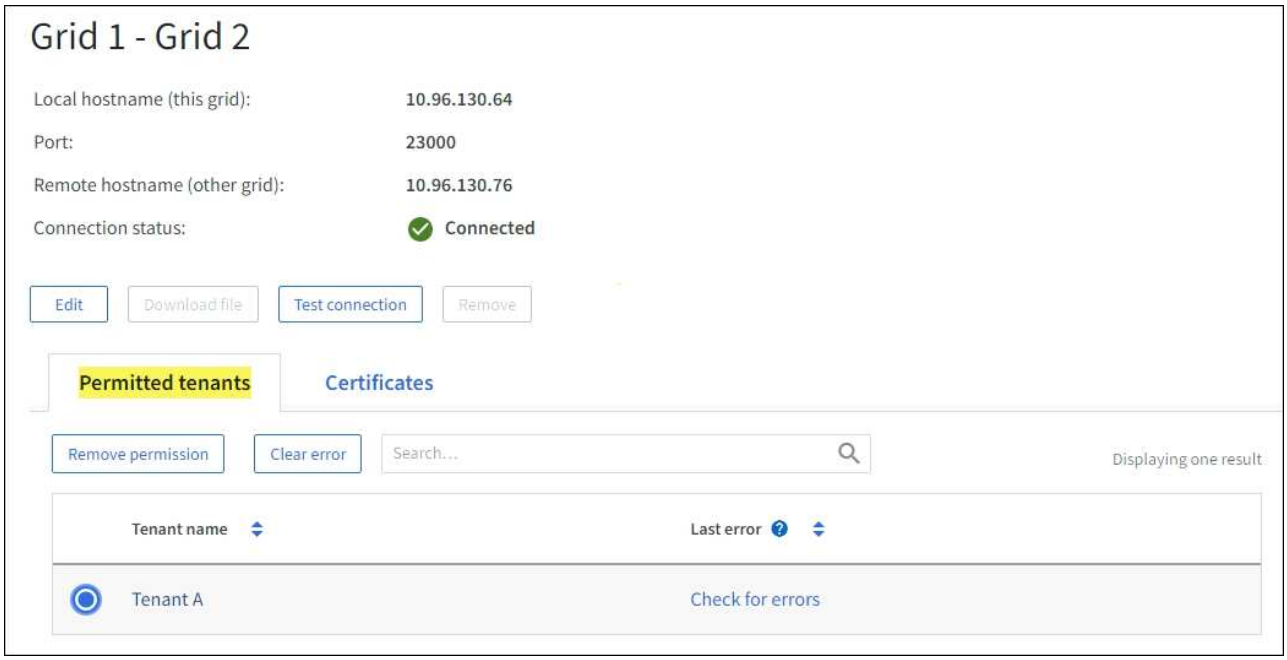
1. Wählen Sie auf der Seite Grid federation entweder einen der beiden Tabs aus und dann den Verbindungsnamen aus der Tabelle.

   Auf der Detailseite der Verbindung sind folgende Aktionen möglich:

   - Grundlegende Statusinformationen zur Verbindung, einschließlich der lokalen und entfernten Hostnamen, des Ports und des Verbindungsstatus, sind ersichtlich.
   - Wählen Sie eine Verbindung zu "bearbeiten, testen oder entfernen".
2. Beim Anzeigen einer bestimmten Verbindung zeigt die Registerkarte **Zulässige Mandanten** Details zu den für die Verbindung zulässigen Mandanten an.

   Über diese Registerkarte sind folgende Aktionen möglich:

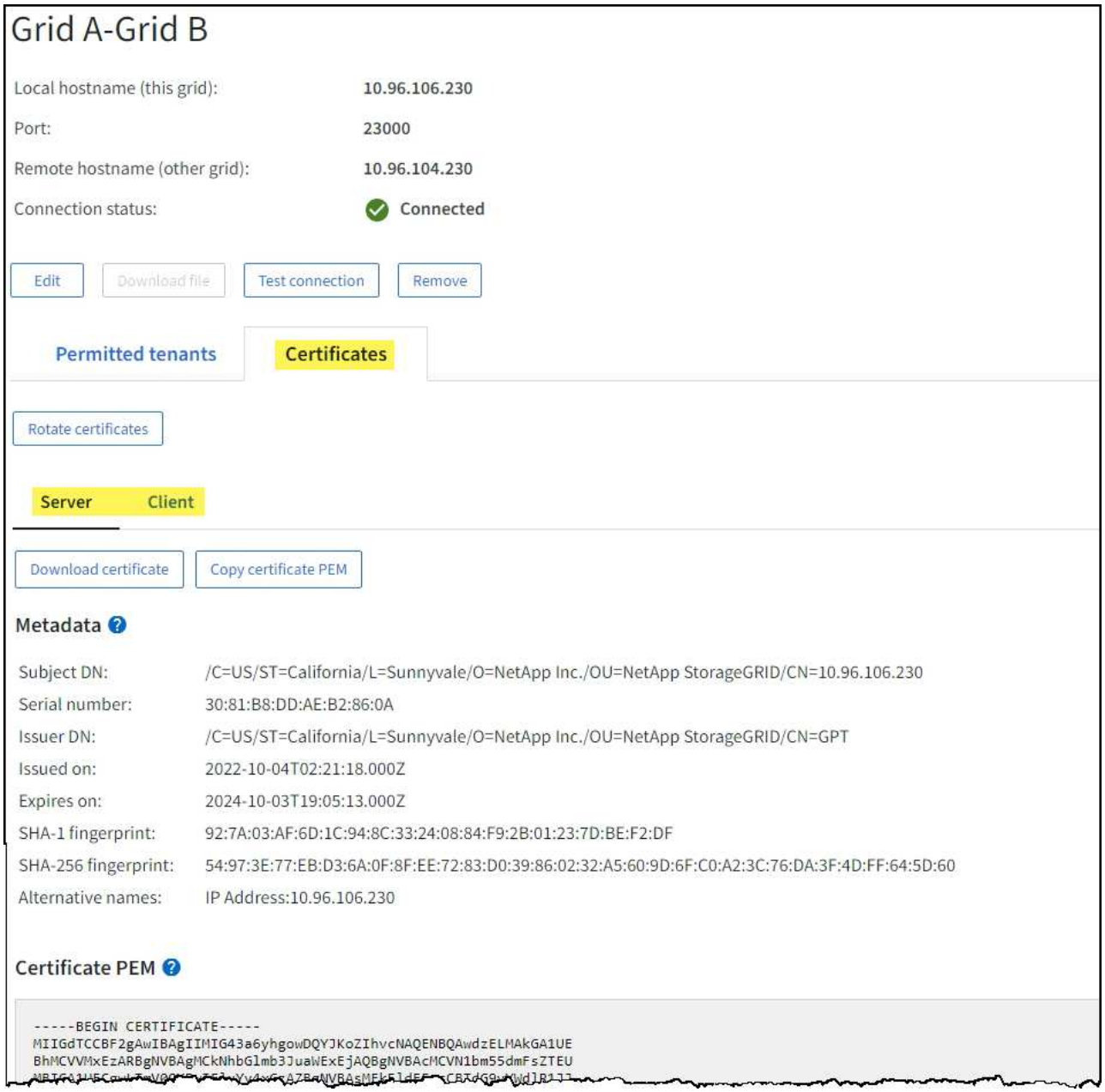
   - "Die Detailseite für jeden zugelassenen Mandanten anzeigen".
   - "Die Berechtigung eines Mandanten entfernen" die Verbindung zu nutzen.
   - Auf Replikationsfehler zwischen den Grids prüfen und den letzten Fehler beheben. Siehe "Fehler in der Grid-Federation beheben".



3. Beim Anzeigen einer bestimmten Verbindung kann auf der Registerkarte **Zertifikate** die vom System generierten Server- und Clientzertifikate für diese Verbindung angezeigt werden.

   Über diese Registerkarte sind folgende Aktionen möglich:

   - "Verbindungszertifikate austauschen".
   - **Server** oder **Client** auswählen, um das zugehörige Zertifikat anzuzeigen oder herunterzuladen oder die Zertifikat-PEM zu kopieren.



Kennzahlen zur netzübergreifenden Replikation überprüfen

Im Cross-Grid Replication Dashboard in Grafana stehen Prometheus-Metriken zu Cross-Grid-Replikationsvorgängen in Ihrem Grid zur Ansicht bereit.

Schritte

1. Im Grid Manager **Support** > **Tools** > **Metrics** auswählen.

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

2. Im Grafana Bereich der Seite **Cross Grid Replication** auswählen.

   Ausführliche Anweisungen finden Sie unter "Support-Metriken überprüfen".

3. Um die Replikation von Objekten, deren Replikation fehlgeschlagen ist, erneut zu versuchen, siehe "Fehlgeschlagene Replikationsvorgänge identifizieren und erneut versuchen".

Benachrichtigungen verwalten

Warnmeldungen in StorageGRID verwalten

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

Warnmeldungen werden bei bestimmten Schweregraden ausgelöst, wenn die Bedingungen der Warnregel als erfüllt gelten. Wenn eine Warnmeldung ausgelöst wird, erfolgen die folgenden Aktionen:

- Ein Symbol für den Schweregrad der Warnung wird im Grid Manager auf dem Dashboard angezeigt, und die Anzahl der aktuellen Warnungen wird erhöht.
- Die Warnung wird auf der **Knoten** Übersichtsseite und auf der Registerkarte **Knoten** > ***node*** > **Übersicht** angezeigt.
- Eine E-Mail-Benachrichtigung wird versendet, sofern ein SMTP-Server konfiguriert und E-Mail-Adressen für die Empfänger angegeben wurden.
- Eine Simple Network Management Protocol (SNMP)-Benachrichtigung wird gesendet, vorausgesetzt, Sie haben den StorageGRID SNMP-Agent konfiguriert.

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

Weitere Informationen:

- Videos im Überblick:

  Benachrichtigungsübersicht

  Benutzerdefinierte Benachrichtigungen

- Siehe "Benachrichtigungsreferenz".

StorageGRID-Alarmregeln anzeigen

Alarmregeln definieren die Bedingungen, die "spezifische Warnmeldungen" auslösen. StorageGRID enthält eine Reihe von Standard-Alarmregeln, die unverändert verwendet oder angepasst werden können, oder es können benutzerdefinierte Alarmregeln erstellt werden.

Die Liste aller Standard- und benutzerdefinierten Alarmregeln zeigt, welche Bedingungen die einzelnen Alarme auslösen und ob Alarme deaktiviert sind.

Bevor Sie beginnen

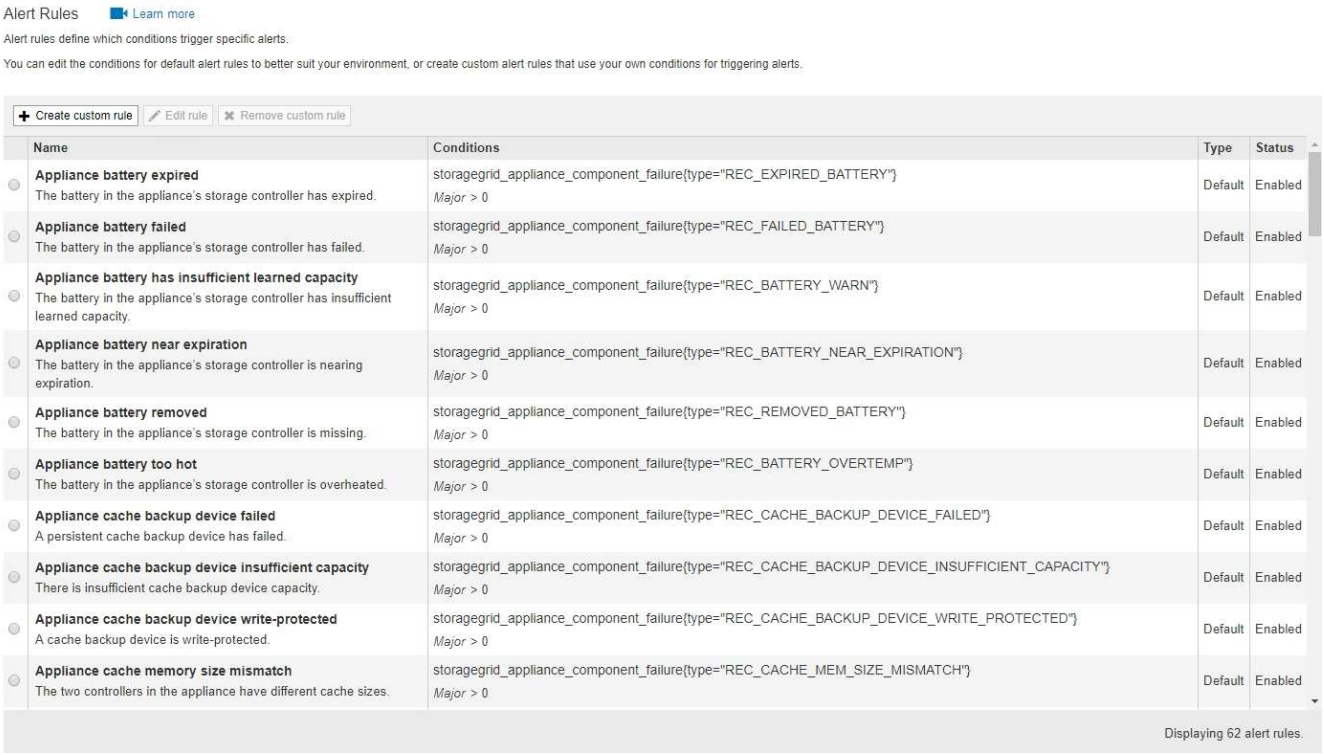
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".
- Optional haben Sie sich das Video angesehen:

Benachrichtigungsübersicht

Schritte

1. **Benachrichtigungen** > **Regeln** auswählen.

   Die Seite „Alarmregeln“ wird angezeigt.



2. In der Tabelle der Alarmregeln sind die Informationen aufgeführt:

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

Spaltenüberschrift	Beschreibung
Bedingungen	Die Prometheus-Ausdrücke, die festlegen, wann diese Warnung ausgelöst wird. Eine Warnung kann bei einem oder mehreren der folgenden Schweregrade ausgelöst werden, jedoch ist keine Bedingung für jeden Schweregrad erforderlich. • **Kritisch**: Es liegt ein anormaler Zustand vor, der den normalen Betrieb eines StorageGRID Node oder Service gestoppt hat. Das zugrunde liegende Problem muss umgehend behoben werden. Kommt es zu keiner Lösung, können Dienstunterbrechungen und Datenverlust die Folge sein. • **Schwerwiegend**: Es liegt ein anormaler Zustand vor, der entweder den laufenden Betrieb beeinträchtigt oder sich dem Schwellenwert für eine kritische Warnung nähert. Es empfiehlt sich, schwerwiegende Warnungen zu untersuchen und zugrunde liegende Probleme zu beheben, damit der anormale Zustand den normalen Betrieb eines StorageGRID Knotens oder Dienstes nicht unterbricht. • **Geringfügig**: Das System arbeitet normal, es besteht jedoch eine Störung, die die Funktionsfähigkeit des Systems beeinträchtigen könnte, wenn sie anhält. Geringfügige Warnmeldungen, die nicht von selbst verschwinden, sollten überwacht und behoben werden, damit daraus kein schwerwiegenderes Problem entsteht.
Typ	Die Art der Alarmregel: • **Standard**: Eine mit dem System bereitgestellte Alarmregel. Sie können eine Standardalarmregel deaktivieren oder die Bedingungen und die Dauer für eine Standardalarmregel bearbeiten. Sie können eine Standardalarmregel nicht entfernen. • **Standard***: Eine Standard-Alarmregel, die eine bearbeitete Bedingung oder Dauer enthält. Bei Bedarf lässt sich eine geänderte Bedingung einfach auf den ursprünglichen Standardwert zurücksetzen. • **Benutzerdefiniert**: Eine von Ihnen erstellte Alarmregel. Sie können benutzerdefinierte Alarmregeln deaktivieren, bearbeiten und entfernen.
Status	Ob diese Alarmregel aktuell aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Alarmregeln werden nicht ausgewertet, daher werden keine Alarme ausgelöst.

Erstellen Sie benutzerdefinierte Alarmregeln in StorageGRID

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

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

- Sie sind mit dem "häufig verwendete Prometheus Metriken" vertraut.
- Sie verstehen das "Syntax von Prometheus Abfragen".
- Optional haben Sie sich das Video angesehen:

  Benutzerdefinierte Benachrichtigungen

Über diese Aufgabe

StorageGRID validiert keine benutzerdefinierten Warnmeldungen. Bei der Erstellung benutzerdefinierter Warnregeln gelten die folgenden allgemeinen Richtlinien:

- Sehen Sie sich die Bedingungen für die Standard-Alarmregeln an und nutzen Sie diese als Beispiele für Ihre benutzerdefinierten Alarmregeln.
- Wenn Sie für eine Alarmregel mehrere Bedingungen definieren, sollte für alle Bedingungen derselbe Ausdruck verwendet werden. Anschließend kann der Schwellenwert für jede Bedingung geändert werden.
- Jede Bedingung sollte sorgfältig auf Tippfehler und Logikfehler überprüft werden.
- Verwenden Sie ausschließlich die in der Grid Management API aufgeführten Metriken.
- Beim Testen eines Ausdrucks mit der Grid Management API ist zu beachten, dass eine „erfolgreiche“ Antwort ein leerer Antworttext sein kann (keine Warnung ausgelöst). Um festzustellen, ob die Warnung tatsächlich ausgelöst wird, kann vorübergehend ein Schwellenwert auf einen Wert gesetzt werden, der aktuell als zutreffend erwartet wird.

  Beispielsweise kann zum Testen des Ausdrucks `node_memory_MemTotal_bytes < 24000000000` zunächst `node_memory_MemTotal_bytes >= 0` ausgeführt werden, um sicherzustellen, dass die erwarteten Ergebnisse zurückgegeben werden (alle Knoten liefern einen Wert). Anschließend werden der Operator und der Schwellenwert wieder auf die vorgesehenen Werte geändert und erneut ausgeführt. Keine Ergebnisse weisen darauf hin, dass für diesen Ausdruck derzeit keine Warnungen vorliegen.

- Es sollte nicht davon ausgegangen werden, dass eine benutzerdefinierte Warnung funktioniert, solange nicht validiert wurde, dass die Warnung wie erwartet ausgelöst wird.

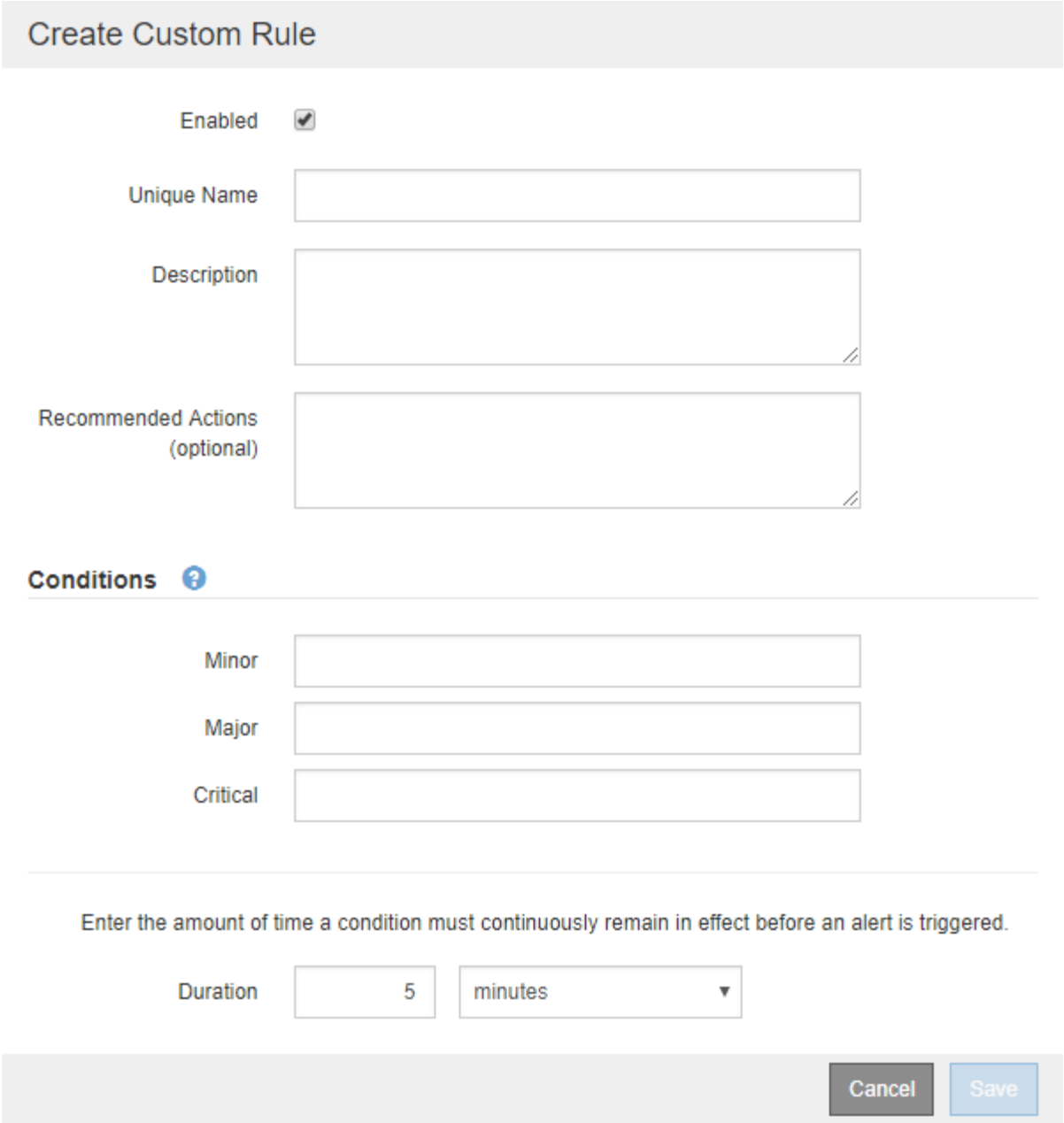
Schritte

1. **Benachrichtigungen** > **Regeln** auswählen.

   Die Seite „Alarmregeln“ wird angezeigt.

2. **Benutzerdefinierte Regel erstellen** auswählen.

   Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.



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

   Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und keine Alarme 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 „Alarme“ angezeigt und ist auch der Betreff für E-Mail-Benachrichtigungen. Namen für Alarmregeln können zwischen 1 und 64 Zeichen lang sein.

Feld	Beschreibung
Beschreibung	Eine Beschreibung des aufgetretenen Problems. Die Beschreibung ist die Warnmeldung, die auf der Seite „Warnungen“ und in E-Mail-Benachrichtigungen angezeigt wird. Beschreibungen für Warnregeln können zwischen 1 und 128 Zeichen umfassen.
Empfohlene Maßnahmen	Optional die empfohlenen Aktionen, die beim Auslösen dieser Warnung durchgeführt werden sollten. Empfohlene Aktionen als Klartext (ohne Formatierungscodes) eingeben. Empfohlene Aktionen für Warnungsregeln können zwischen 0 und 1.024 Zeichen umfassen.

5. Im Abschnitt „Bedingungen“ einen Prometheus-Ausdruck für einen oder mehrere der Alarm-Schweregrade eingeben.

   Ein einfacher Ausdruck hat üblicherweise die Form:

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

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

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

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

6. Im Feld **Dauer** die Zeitspanne eingeben, die eine Bedingung ununterbrochen wirksam bleiben muss, bevor die Warnung ausgelöst wird, und eine Zeiteinheit auswählen.

   Um eine Warnung sofort auszulösen, wenn eine Bedingung erfüllt ist, **0** eingeben. Diesen Wert erhöhen, um zu verhindern, dass temporäre Bedingungen Warnungen auslösen.

   Die Standardeinstellung beträgt 5 Minuten.

7. **Speichern** auswählen.

   Das Dialogfeld schließt sich, und die neue benutzerdefinierte Alarmregel erscheint in der Tabelle „Alarmregeln“.

Alarmregeln in StorageGRID bearbeiten

Sie können eine Alarmregel bearbeiten, um die Auslösebedingungen zu ändern. Bei einer benutzerdefinierten Alarmregel können außerdem der Regelnamen, die Beschreibung und die empfohlenen Aktionen aktualisiert werden.

Bevor Sie beginnen

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

- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

Über diese Aufgabe

Beim Bearbeiten einer Standard-Warnregel können die Bedingungen für geringfügige, schwerwiegende und kritische Warnungen sowie die Dauer geändert werden. Beim Bearbeiten einer benutzerdefinierten Warnregel können außerdem der Name, die Beschreibung und die empfohlenen Aktionen der Regel bearbeitet werden.

> Seien Sie vorsichtig beim Bearbeiten einer Alarmregel. Wenn Sie Auslösewerte ändern, wird ein zugrundeliegendes Problem möglicherweise erst erkannt, wenn es die Ausführung eines kritischen Vorgangs verhindert.

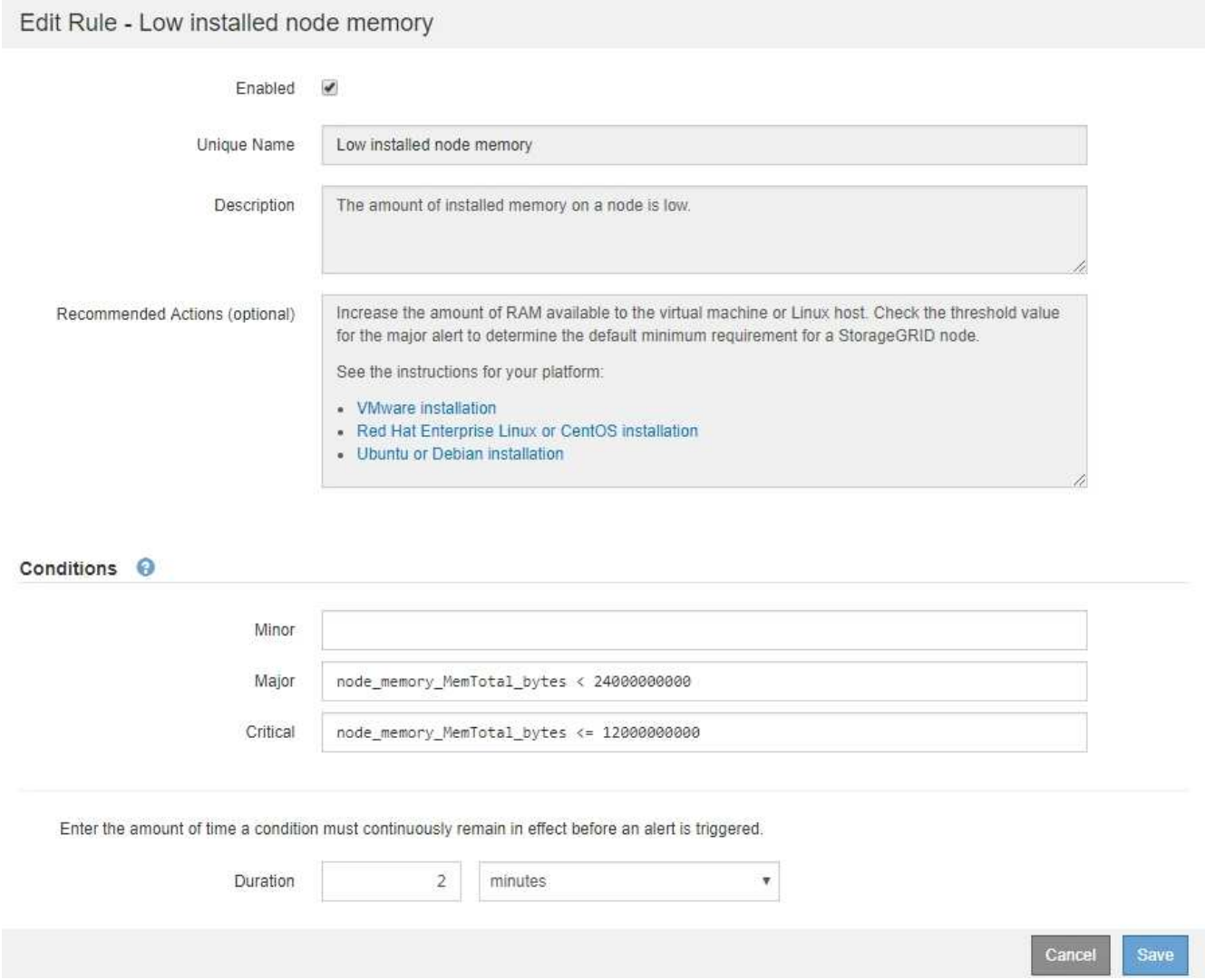
Schritte

1. **Benachrichtigungen** > **Regeln** auswählen.

   Die Seite „Alarmregeln“ wird angezeigt.

2. Wählen Sie das Optionsfeld für die Alarmregel aus, die bearbeitet werden soll.
3. **Regel bearbeiten** auswählen.

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



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

   Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und keine Alarme ausgelöst.

   Wenn Sie die Alarmregel für einen aktuellen Alarm deaktivieren, müssen Sie einige Minuten warten, bis der Alarm nicht mehr als aktiver Alarm angezeigt wird.

   Generell wird davon abgeraten, eine Standard-Warnregel zu deaktivieren. Wenn eine Warnregel deaktiviert ist, wird ein zugrundeliegendes Problem möglicherweise erst erkannt, wenn es die Ausführung eines kritischen Vorgangs verhindert.

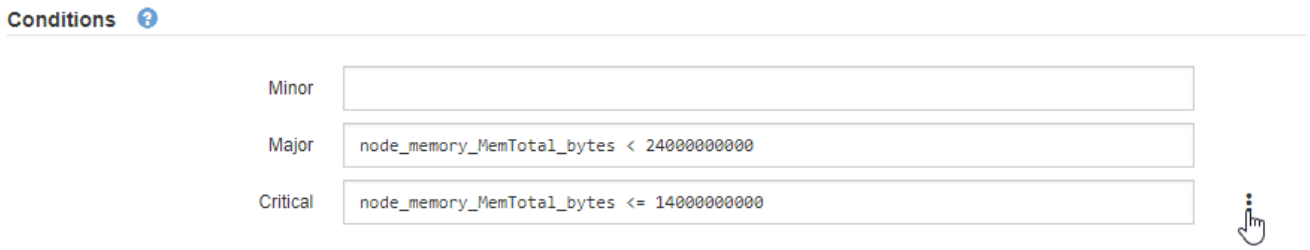
5. Für benutzerdefinierte Alarmregeln sind die folgenden Informationen nach Bedarf zu aktualisieren.

   Diese Informationen können für Standard-Alarmregeln nicht bearbeitet werden.

Feld	Beschreibung
Eindeutiger Name	Ein eindeutiger Name für diese Regel. Der Name der Alarmregel wird auf der Seite „Alarme“ angezeigt und ist auch der Betreff für E-Mail-Benachrichtigungen. Namen für Alarmregeln können zwischen 1 und 64 Zeichen lang sein.
Beschreibung	Eine Beschreibung des aufgetretenen Problems. Die Beschreibung ist die Warnmeldung, die auf der Seite „Warnungen“ und in E-Mail-Benachrichtigungen angezeigt wird. Beschreibungen für Warnregeln können zwischen 1 und 128 Zeichen umfassen.
Empfohlene Maßnahmen	Optional die empfohlenen Aktionen, die beim Auslösen dieser Warnung auszuführen sind. Empfohlene Aktionen sind als Klartext (ohne Formatierungscodes) einzugeben. Empfohlene Aktionen für Warnungsregeln können zwischen 0 und 1.024 Zeichen umfassen.

6. Im Abschnitt „Bedingungen“ den Prometheus-Ausdruck für einen oder mehrere der Alarm-Schweregrade eingeben oder aktualisieren.

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



> Wenn Sie die Bedingungen für eine bestehende Warnung aktualisieren, werden Ihre Änderungen möglicherweise erst umgesetzt, wenn die vorherige Bedingung behoben ist. Das nächste Mal, wenn eine der Bedingungen für die Regel erfüllt ist, werden die aktualisierten Werte in der Warnung angezeigt.

Ein einfacher Ausdruck hat üblicherweise die Form:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

7. Im Feld **Dauer** die Zeitspanne eingeben, die eine Bedingung ununterbrochen wirksam bleiben muss, bevor die Warnung ausgelöst wird, und die Zeiteinheit auswählen.

Um eine Warnung sofort auszulösen, wenn eine Bedingung erfüllt ist, **0** eingeben. Diesen Wert erhöhen, um zu verhindern, dass temporäre Bedingungen Warnungen auslösen.

Die Standardeinstellung beträgt 5 Minuten.

8. **Speichern** auswählen.

   Wenn eine Standard-Alarmregel bearbeitet wurde, erscheint in der Spalte **Typ Default**. Wenn eine Standard- oder benutzerdefinierte Alarmregel deaktiviert wurde, erscheint in der Spalte **Status Disabled**.

Warnregeln in StorageGRID deaktivieren

Sie können den Aktivierungs-/Deaktivierungsstatus für eine Standard- oder benutzerdefinierte Alarmregel ändern.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

Über diese Aufgabe

Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und keine Alarme ausgelöst.

> Generell wird davon abgeraten, eine Standard-Warnregel zu deaktivieren. Wenn eine Warnregel deaktiviert ist, wird ein zugrundeliegendes Problem möglicherweise erst erkannt, wenn es die Ausführung eines kritischen Vorgangs verhindert.

Schritte

1. **Benachrichtigungen** > **Regeln** auswählen.

   Die Seite „Alarmregeln“ wird angezeigt.

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

   Das Dialogfeld „Regel bearbeiten“ wird angezeigt.

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

   Wenn eine Alarmregel deaktiviert ist, werden ihre Ausdrücke nicht ausgewertet und keine Alarme ausgelöst.

   > Wenn die Alarmregel für einen aktuellen Alarm deaktiviert wird, kann es einige Minuten dauern, bis der Alarm nicht mehr als aktiver Alarm angezeigt wird.

5. **Speichern** auswählen.

   Deaktiviert erscheint in der Spalte **Status**.

Benutzerdefinierte Alarmregeln in StorageGRID entfernen

Eine benutzerdefinierte Alarmregel kann entfernt werden, falls sie nicht mehr verwendet werden soll.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

Schritte

1. **Benachrichtigungen** > **Regeln** auswählen.

   Die Seite „Alarmregeln“ wird angezeigt.

2. Das Optionsfeld für die benutzerdefinierte Alarmregel auswählen, die entfernt werden soll.

   Eine Standard-Warnregel kann nicht entfernt werden.

3. **Benutzerdefinierte Regel entfernen** auswählen.

   Es erscheint ein Bestätigungsdialogfeld.

4. **OK** auswählen, um die Warnregel zu entfernen.

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

Benachrichtigungen verwalten

SNMP-Benachrichtigungen für StorageGRID-Warnungen einrichten

Wenn StorageGRID SNMP-Benachrichtigungen senden soll, wenn Warnmeldungen auftreten, muss der StorageGRID SNMP-Agent aktiviert und mindestens ein Trap-Ziel konfiguriert werden.

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

Weitere Informationen zur Konfiguration des SNMP-Agenten finden sich unter "SNMP Überwachung".

Nach der Konfiguration des StorageGRID SNMP-Agenten 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 darüber zu informieren, dass innerhalb von StorageGRID etwas passiert ist, wie zum Beispiel das Auslösen einer Warnung. Traps werden in allen drei Versionen von SNMP unterstützt.
- Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Erhält der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung, sendet er die Inform so lange erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist. Informs werden in SNMPv2c und SNMPv3 unterstützt.

Trap- und Inform-Benachrichtigungen werden gesendet, wenn eine Standard- oder benutzerdefinierte Warnung bei jedem Schweregrad ausgelöst wird. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, ist eine Stummschaltung für die Warnung zu konfigurieren. Siehe "Alarmbenachrichtigungen stummschalten".

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

E-Mail-Benachrichtigungen für StorageGRID-Warnungen einrichten

Wenn E-Mail-Benachrichtigungen bei Warnmeldungen gesendet werden sollen, müssen Informationen zu Ihrem SMTP-Server angegeben werden. Es müssen außerdem die E-Mail-Adressen der Empfänger der Warnmeldungen eingegeben werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

Über diese Aufgabe

Die für Benachrichtigungen verwendete E-Mail-Konfiguration wird nicht für AutoSupport-Pakete verwendet. Es kann jedoch derselbe E-Mail-Server für alle Benachrichtigungen verwendet werden.

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

Schritte

1. **Benachrichtigungen** > **E-Mail-Einrichtung** auswählen.

   Die Seite „E-Mail-Einrichtung“ erscheint.

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**, um anzugeben, dass Benachrichtigungs-E-Mails gesendet werden, wenn Warnmeldungen die konfigurierten Schwellenwerte erreichen.

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

3. Im Abschnitt „E-Mail (SMTP) Server“ werden die Informationen eingegeben, die StorageGRID für den Zugriff auf Ihren SMTP-Server benötigt.

   Falls Ihr SMTP-Server eine Authentifizierung erfordert, müssen sowohl ein Benutzername als auch ein Passwort angegeben werden.

Feld	Eingeben
Mail-Server	Der vollqualifizierte Domainname (FQDN) oder die IP-Adresse des SMTP-Servers.

Feld	Eingeben
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 für die Authentifizierung ein.
Passwort (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie das Passwort zur Authentifizierung ein.

4. Im Abschnitt „E-Mail-Adressen“ die E-Mail-Adressen des Absenders und jedes Empfängers eingeben.
   a. Für die **Absender-E-Mail-Adresse** ist eine gültige E-Mail-Adresse anzugeben, die als Absenderadresse für Benachrichtigungen verwendet wird.

      Zum Beispiel: `storagegrid-alerts@example.com`

   b. Im Abschnitt „Empfänger“ eine E-Mail-Adresse für jede E-Mail-Liste oder Person eingeben, die im Falle einer Benachrichtigung eine E-Mail erhalten soll.

      Das Plus-Symbol ➕ auswählen, um Empfänger hinzuzufügen.

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

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

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

   b. Das Kontrollkästchen **Clientzertifikat senden** ist zu aktivieren, wenn Ihr SMTP-E-Mail-Server von den Absendern verlangt, Clientzertifikate zur Authentifizierung bereitzustellen.
   c. Im Feld **Client Certificate** ist das PEM-codierte Clientzertifikat anzugeben, das an den SMTP-Server gesendet wird.

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

   d. Im Feld **Privater Schlüssel** ist der private Schlüssel für das Clientzertifikat in unverschlüsselter PEM-Kodierung einzugeben.

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

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

6. Im Abschnitt „Filter“ wird ausgewählt, welche Alarm-Schweregrade zu E-Mail-Benachrichtigungen führen sollen, es sei denn, die Regel für einen bestimmten Alarm wurde stummgeschaltet.

Schwere	Beschreibung
Geringfügig, schwerwiegend, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die geringfügige, schwerwiegende oder kritische Bedingung für eine Alarmregel erfüllt ist.
Wichtig, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die schwerwiegende oder kritische Bedingung für eine Alarmregel erfüllt ist. Für geringfügige Alarme werden keine Benachrichtigungen gesendet.
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur versendet, wenn die kritische Bedingung für eine Alarmregel erfüllt ist. Benachrichtigungen werden nicht für geringfügige oder schwerwiegende Alarme versendet.

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

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

   b. Die Postfächer aller E-Mail-Empfänger sollten überprüft und bestätigt werden, dass eine Test-E-Mail eingegangen ist.

      > Wenn die E-Mail nicht innerhalb weniger Minuten empfangen wird oder die Warnmeldung **E-Mail-Benachrichtigung fehlgeschlagen** ausgelöst wird, sollten die Einstellungen überprüft und der Vorgang erneut versucht werden.

   c. Bei beliebigen anderen Admin-Knoten anmelden und eine Test-E-Mail senden, um die Konnektivität von allen Standorten zu überprüfen.

      > Beim Testen von Benachrichtigungen müssen Sie sich auf jedem Admin Node anmelden, um die Verbindung zu überprüfen. Dies unterscheidet sich vom Testen von AutoSupport-Paketen, bei dem alle Admin Nodes die Test-E-Mail versenden.

8. **Speichern** auswählen.

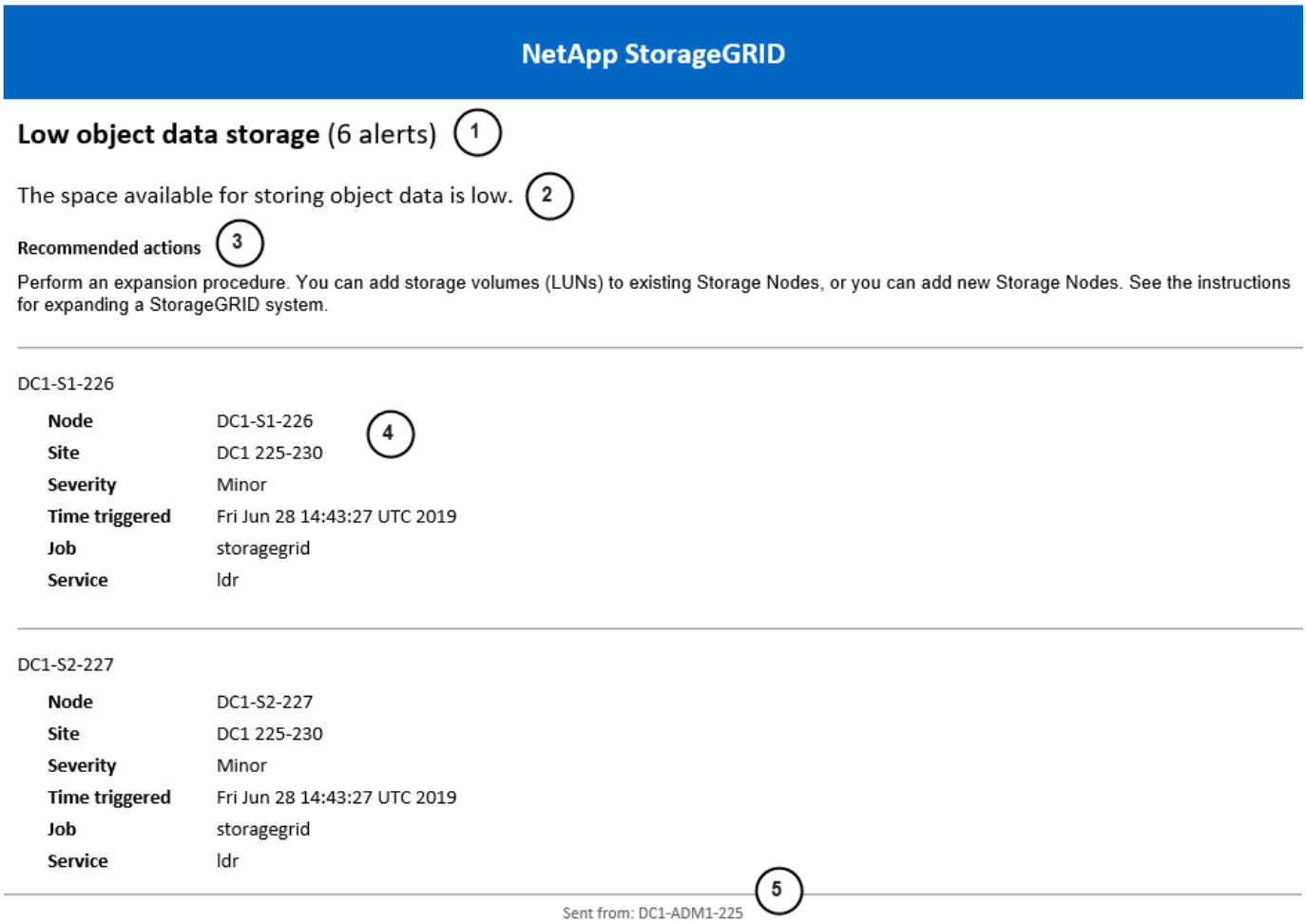
   Das Senden einer Test-E-Mail speichert Ihre Einstellungen nicht. **Speichern** muss ausgewählt werden.

   Die E-Mail-Einstellungen sind gespeichert.

Informationen in E-Mail-Benachrichtigungen zu Warnmeldungen

Nach der Konfiguration des SMTP-E-Mail-Servers werden E-Mail-Benachrichtigungen an die festgelegten Empfänger gesendet, wenn eine Warnung ausgelöst wird, es sei denn, die Warnungsregel ist durch eine Stummschaltung unterdrückt. Siehe "Alarmbenachrichtigungen stummschalten".

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



Callout	Beschreibung
1	Der Name der Warnung, gefolgt von der Anzahl der aktiven Instanzen dieser Warnung.
2	Die Beschreibung der Warnung.
3	Empfohlene Maßnahmen für die Warnmeldung.
4	Details zu jeder aktiven Instanz der Warnung, einschließlich des betroffenen Knotens und Standorts, des Schweregrads, der UTC-Zeit, zu der die Warnungsregel ausgelöst wurde, sowie des Namens des betroffenen Jobs und Dienstes.
5	Der Hostname des Admin Node, der die Benachrichtigung gesendet hat.

Wie Warnmeldungen gruppiert werden

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

Die folgende Tabelle enthält Beispiele dafür, wie StorageGRID mehrere Warnmeldungen in E-Mail-Benachrichtigungen gruppiert.

Verhalten	Beispiel
Jede Alarmbenachrichtigung gilt nur für Alarme mit demselben Namen. Wenn zwei Alarme mit unterschiedlichen Namen gleichzeitig ausgelöst werden, werden zwei E-Mail-Benachrichtigungen gesendet.	• Alarm A wird gleichzeitig auf zwei Knoten ausgelöst. Es wird nur eine Benachrichtigung gesendet. • Alarm A wird auf Knoten 1 ausgelöst, und Alarm B wird gleichzeitig auf Knoten 2 ausgelöst. Zwei Benachrichtigungen werden gesendet, jeweils eine für jeden Alarm.
Bei einer bestimmten Warnung auf einem bestimmten Knoten wird, wenn die Schwellenwerte für mehr als einen Schweregrad erreicht werden, nur für die schwerwiegendste Warnung eine Benachrichtigung gesendet.	• Alarm A wird ausgelöst und die Schwellenwerte für geringfügige, schwerwiegende und kritische Alarme werden erreicht. Eine Benachrichtigung wird für den kritischen Alarm gesendet.
Beim ersten Auftreten einer Warnung wartet StorageGRID 2 Minuten, bevor eine Benachrichtigung gesendet wird. Wenn in diesem Zeitraum weitere Warnungen mit demselben Namen ausgelöst werden, fasst StorageGRID alle Warnungen in der ersten Benachrichtigung zusammen.	1. Alarm A wird auf Knoten 1 um 08:00 Uhr 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 über beide Instanzen der Warnmeldung zu berichten.
Wird eine weitere Warnung mit demselben Namen ausgelöst, wartet StorageGRID 10 Minuten, bevor eine neue Benachrichtigung gesendet wird. Die neue Benachrichtigung enthält alle aktiven Warnungen (aktuelle Warnungen, die nicht stummgeschaltet wurden), auch wenn sie bereits zuvor gemeldet wurden.	1. Alarm A wird um 08:00 Uhr auf Knoten 1 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 (10 Minuten später) gesendet. Beide Knoten werden gemeldet.
Wenn mehrere aktuelle Warnungen mit demselben Namen vorhanden sind und eine dieser Warnungen behoben wurde, wird keine neue Benachrichtigung gesendet, wenn die Warnung auf dem Knoten, für den die Warnung behoben wurde, erneut auftritt.	1. Für Knoten 1 wird Alarm A ausgelöst. Eine Benachrichtigung wird versendet. 2. Alarm A wird für Knoten 2 ausgelöst. Eine zweite Benachrichtigung wird gesendet. 3. Warnung A wurde für Knoten 2 behoben, bleibt aber für Knoten 1 weiterhin aktiv. 4. Alarm A wird für Knoten 2 erneut ausgelöst. Es wird keine neue Benachrichtigung gesendet, da der Alarm für Knoten 1 noch aktiv ist.

Verhalten	Beispiel
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnung behoben sind oder die Warnungsregel stummgeschaltet wird.	1. Am 8. März wird für Knoten 1 die Warnung A ausgelöst. Eine Benachrichtigung wird gesendet. 2. Warnung A wurde weder behoben noch stummgeschaltet. Weitere Benachrichtigungen werden am 15. März, 22. März, 29. März und so weiter gesendet.

Fehlerbehebung bei E-Mail-Benachrichtigungen für Warnmeldungen

Falls die Warnung **E-Mail-Benachrichtigungsfehler** ausgelöst wird oder Sie die Testbenachrichtigung per E-Mail nicht erhalten, können diese Schritte zur Behebung des Problems durchgeführt werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

Schritte

1. Einstellungen überprüfen.
   a. **Benachrichtigungen** > **E-Mail-Einrichtung** auswählen.
   b. Es sollte überprüft werden, ob die Einstellungen des E-Mail-Servers (SMTP) korrekt sind.
   c. Es sollte überprüft werden, ob gültige E-Mail-Adressen für die Empfänger angegeben wurden.
2. Überprüfen Sie Ihren Spamfilter und stellen Sie sicher, dass die E-Mail nicht in einen Junk-Ordner gesendet wurde.
3. Lassen Sie von Ihrem E-Mail-Administrator bestätigen, dass E-Mails von der Absenderadresse nicht blockiert werden.
4. Eine Protokolldatei für den Admin-Knoten sammeln und anschließend den technischen Support kontaktieren.

   Der technische Support kann die Informationen in den Protokollen nutzen, um zu ermitteln, was schiefgelaufen ist. Beispielsweise könnte die Datei prometheus.log einen Fehler beim Verbindungsaufbau zum von Ihnen angegebenen Server anzeigen.

   Siehe "Protokolldateien und Systemdaten sammeln".

Warnmeldungen in StorageGRID stummschalten

Optional lassen sich Stummschaltungen konfigurieren, um Warnmeldungen vorübergehend zu unterdrücken.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Benachrichtigungen oder Root-Zugriffsberechtigungen verwalten".

Über diese Aufgabe

Sie können Alarmregeln für das gesamte Grid, einen einzelnen Standort oder einen einzelnen Knoten und für einen oder mehrere Schweregrade stummschalten. Jede Stummschaltung unterdrückt alle

Benachrichtigungen für eine einzelne Alarmregel oder für alle Alarmregeln.

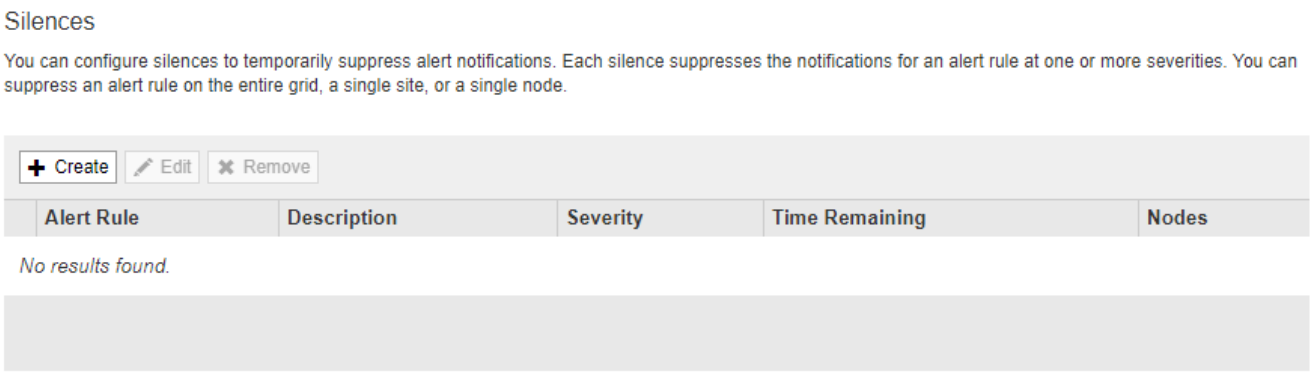
Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stummschaltungen auch SNMP-Traps und Informs.

> Seien Sie vorsichtig, wenn Sie eine Warnregel unterdrücken. Wenn Sie eine Warnregel unterdrücken, wird ein zugrundeliegendes Problem möglicherweise erst erkannt, wenn es die Ausführung eines kritischen Vorgangs verhindert.

Schritte

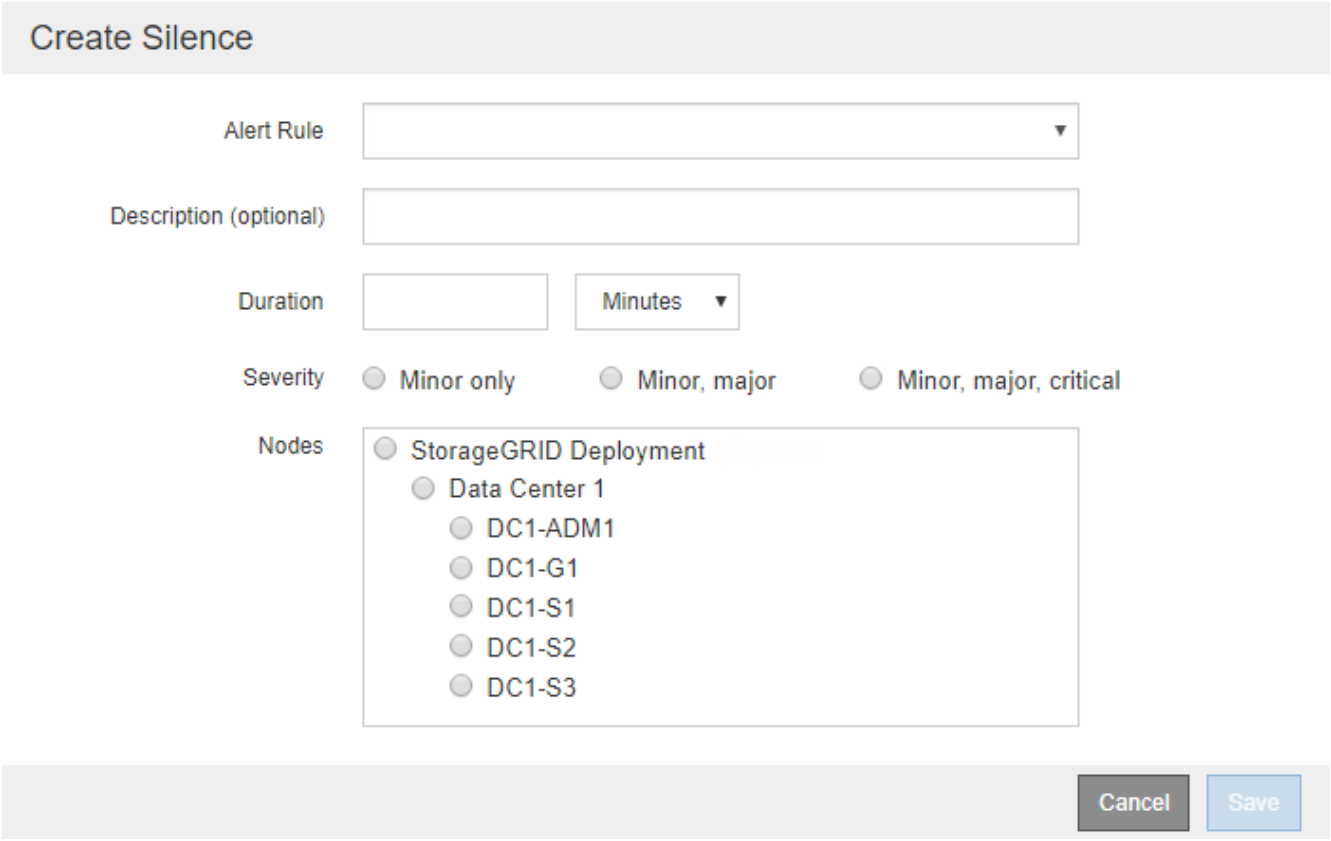
1. **Benachrichtigungen** > **Stummschaltungen** auswählen.

   Die Seite „Stille“ wird angezeigt.



2. Wählen Sie **Create**.

   Das Dialogfeld „Stille erstellen“ wird angezeigt.



3. Folgende Informationen auswählen oder eingeben:

Feld	Beschreibung
Alarmregel	Der Name der Benachrichtigungsregel, die Sie stummschalten möchten. Es kann jede Standard- oder benutzerdefinierte Benachrichtigungsregel ausgewählt werden, auch wenn die Benachrichtigungsregel deaktiviert ist. **Hinweis: Alle Regeln** kann ausgewählt werden, um alle Alarmregeln mit den in diesem Dialogfeld angegebenen Kriterien stummzuschalten.
Beschreibung	Optional kann eine Beschreibung der Stille angegeben werden. Zum Beispiel kann der Zweck dieser Stille beschrieben werden.
Dauer	Wie lange diese Stille in Minuten, Stunden oder Tagen wirksam bleiben soll. Eine Stille kann zwischen 5 Minuten und 1.825 Tagen (5 Jahren) wirksam sein. **Hinweis:** Sie sollten eine Alarmregel nicht über einen längeren Zeitraum stummschalten. Wenn eine Alarmregel stummgeschaltet ist, wird ein zugrundeliegendes Problem möglicherweise erst erkannt, wenn es die Ausführung eines kritischen Vorgangs verhindert. Eine längere Stummschaltung kann jedoch erforderlich sein, wenn ein Alarm durch eine bestimmte, beabsichtigte Konfiguration ausgelöst wird, wie es beispielsweise bei den **Services appliance link down**-Alarmen und den **Storage appliance link down**-Alarmen der Fall sein kann.
Schwere	Welche Schweregrade sollen unterdrückt werden. Wenn die Warnung bei einem der ausgewählten Schweregrade ausgelöst wird, werden keine Benachrichtigungen gesendet.
Nodes	Auf welche Knoten oder welchen Knoten diese Stummschaltung angewendet werden soll. Eine Alarmregel oder alle Regeln können im gesamten Grid, an einem einzelnen Standort oder auf einem einzelnen Knoten unterdrückt werden. Wenn das gesamte Grid ausgewählt wird, gilt die Stummschaltung für alle Standorte und alle Knoten. Wenn ein Standort ausgewählt wird, gilt die Stummschaltung nur für die Knoten an diesem Standort. **Hinweis:** Für jede Stummschaltung kann nicht mehr als ein Knoten oder mehr als ein Standort ausgewählt werden. Zusätzliche Stummschaltungen sind erforderlich, wenn dieselbe Alarmregel gleichzeitig auf mehr als einem Knoten oder mehr als einem Standort unterdrückt werden soll.

4. **Speichern** auswählen.
5. Wenn eine Stille vor deren Ablauf geändert oder beendet werden soll, kann sie bearbeitet oder entfernt werden.

Option	Beschreibung
Eine Stille bearbeiten	a. **Benachrichtigungen** > **Stummschaltungen** auswählen. b. In der Tabelle das Optionsfeld für die Stille auswählen, die bearbeitet werden soll. c. **Bearbeiten** auswählen. d. Die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten ändern. e. **Speichern** auswählen.
Eine Stille entfernen	a. **Benachrichtigungen** > **Stummschaltungen** auswählen. b. In der Tabelle das Optionsfeld für die Stille auswählen, die entfernt werden soll. c. Wählen Sie **Remove**. d. **OK** auswählen, um zu bestätigen, dass diese Stille entfernt werden soll. **Hinweis**: Benachrichtigungen werden nun versendet, sobald diese Warnung ausgelöst wird (sofern sie nicht durch eine andere Stummschaltung unterdrückt werden). Wenn diese Warnung aktuell ausgelöst ist, kann es einige Minuten dauern, bis E-Mail- oder SNMP-Benachrichtigungen versendet werden und die Seite „Warnungen“ aktualisiert wird.

Verwandte Informationen

"Den SNMP-Agenten konfigurieren"

Warnungen in StorageGRID

Diese Referenz listet die Standardwarnungen auf, die im Grid Manager angezeigt werden. Empfohlene Maßnahmen sind in der Warnmeldung enthalten, die Sie erhalten.

Bei Bedarf lassen sich benutzerdefinierte Alarmregeln erstellen, die zu Ihrem Systemmanagement-Ansatz passen.

Einige der Standardwarnungen verwenden "Prometheus-Metriken".

Gerätewarnungen

Alarmname	Beschreibung
Gerätebatterie abgelaufen	Die Batterie im Storage-Controller des Geräts ist abgelaufen.
Gerätebatterie ausgefallen	Die Batterie im Storage-Controller des Geräts ist ausgefallen.
Die Batterie des Geräts hat eine unzureichend erlernte Kapazität	Die Batterie im Speichercontroller des Geräts hat eine unzureichend erlernte Kapazität.

Alarmname	Beschreibung
Gerätebatterie nahe am Ablaufdatum	Die Batterie im Storage-Controller des Geräts nähert sich dem Ende ihrer Lebensdauer.
Gerätebatterie entfernt	Die Batterie im Storage-Controller des Geräts fehlt.
Gerätebatterie zu heiß	Die Batterie im Storage-Controller des Geräts ist überhitzt.
BMC-Kommunikationsfehler der Appliance	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren.
Fehler am Appliance-Boot-Gerät erkannt	Es wurde ein Problem mit dem Boot-Gerät in der Appliance festgestellt.
Das Sicherungsgerät für den Appliance Cache ist ausgefallen.	Ein Gerät zur Sicherung des persistenten Caches ist ausgefallen.
Unzureichende Kapazität des Appliance Cache-Backup-Geräts	Die Kapazität des Cache-Backup-Geräts reicht nicht aus.
Appliance Cache Backup-Gerät schreibgeschützt	Ein Cache Backup-Gerät ist schreibgeschützt.
Größenkonflikt im Cache-Speicher der Appliance	Die beiden Controller im Gerät haben unterschiedliche Cache-Größen.
CMOS-Batterie-Fehler der Appliance	Es wurde ein Problem mit der CMOS-Batterie des Geräts festgestellt.
Die Gehäusetemperatur des Appliance Compute Controllers ist zu hoch	Die Temperatur des Rechencontrollers in einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.
Die CPU-Temperatur des Appliance Compute Controllers ist zu hoch.	Die Temperatur der CPU im Compute Controller eines StorageGRID Geräts hat einen nominalen Schwellenwert überschritten.
Der Appliance Compute Controller benötigt Aufmerksamkeit.	Im Compute-Controller einer StorageGRID Appliance wurde ein Hardwarefehler festgestellt.
Das Netzteil des Appliance Compute Controllers A hat ein Problem.	Das Netzteil A im Rechencontroller hat ein Problem.
Das Netzteil B des Appliance Compute Controllers weist ein Problem auf.	Das Netzteil B im Rechencontroller hat ein Problem.

Alarmname	Beschreibung
Der Dienst zur Überwachung der Appliance Compute-Hardware ist ausgefallen.	Der Dienst zur Überwachung des Speicherhardware-Status ist ausgefallen.
Das DAS-Laufwerk der Appliance überschreitet das Limit für die pro Tag geschriebene Datenmenge.	Täglich wird eine übermäßige Datenmenge auf ein Laufwerk geschrieben, was zum Verlust der Garantie führen kann.
Fehler im DAS-Laufwerk des Appliance erkannt	Es wurde ein Problem mit einem direkt angeschlossenen Speicherlaufwerk (DAS) im Appliance festgestellt.
Das Appliance DAS-Laufwerk befindet sich im falschen Steckplatz oder Node.	Ein direkt angeschlossenes Speicherlaufwerk (DAS) befindet sich im falschen Steckplatz oder Node.
Die DAS Laufwerkspositionsanzeigeleuchte des Geräts leuchtet	Die Laufwerkslokalisierungsanzeige für ein oder mehrere direkt angeschlossene Storage-Laufwerke (DAS) in einem Storage Node einer Appliance ist eingeschaltet.
Wiederherstellung des DAS-Laufwerks einer Appliance	Ein direkt angeschlossenes Speicherlaufwerk (DAS) wird neu aufgebaut. Dies ist zu erwarten, wenn es kürzlich ausgetauscht oder entfernt und wieder eingesetzt wurde.
Fehler beim Appliance-Lüfter erkannt	Es wurde ein Problem mit einer Lüftereinheit im Gerät festgestellt.
Fibre Channel-Fehler des Geräts erkannt	Es wurde ein Problem mit der Fibre Channel Verbindung zwischen dem Storage Controller des Geräts und dem Compute Controller festgestellt.
Ausfall des Fibre Channel HBA-Ports des Geräts	Ein Fibre Channel HBA Port ist defekt oder ausgefallen.
Appliance Flash Cache-Laufwerke nicht optimal	Die für den SSD Cache verwendeten Laufwerke sind nicht optimal.
Appliance-Verbindung/Batteriegehäuse entfernt	Der Verbindungs-/Batteriebehälter fehlt.
Fehlender LACP-Port der Appliance	Ein Port an einem StorageGRID Gerät nimmt nicht an der LACP-Bond teil.
Netzwerkkartenfehler des Geräts erkannt	Es wurde ein Problem mit der Netzwerkkarte (NIC) des Geräts festgestellt.

Alarmname	Beschreibung
Gesamtstromversorgung der Appliance beeinträchtigt	Die Leistung eines StorageGRID Geräts ist von der empfohlenen Betriebsspannung abgewichen.
SANtricity OS Software-Update für Appliance erforderlich	SANtricity Softwareversion ist niedriger als die empfohlene Mindestversion für diese Version von StorageGRID.
Kritische SSD-Gerätewarnung	Ein Appliance-SSD meldet eine kritische Warnung.
Ausfall des Appliance Storage Controllers A	Der Speichercontroller A in einer StorageGRID Appliance ist ausgefallen.
Ausfall des Appliance Storage Controllers B	Der Storage-Controller B in einer StorageGRID Appliance ist ausgefallen.
Ausfall des Appliance-Speichercontrollers	In einem StorageGRID Appliance ist ein oder mehrere Laufwerke ausgefallen oder sind nicht optimal.
Hardwareproblem mit dem Appliance Storage-Controller	SANtricity Software meldet für eine Komponente in einem StorageGRID Gerät den Status „Aktionsbedarf“.
Ausfall der Stromversorgung des Appliance Storage Controllers	Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abgewichen.
Ausfall der Stromversorgung B des Appliance Storage Controllers	Die Stromversorgung B in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abgewichen.
Der Service zur Überwachung der Appliance Storage-Hardware ist ausgefallen	Der Dienst zur Überwachung des Speicherhardware-Status ist ausgefallen.
Appliance Storage Shelves beeinträchtigt	Der Status einer der Komponenten im Storage Shelf eines Storage Appliance ist beeinträchtigt.
Gerätetemperatur überschritten	Die Nenn- oder Maximaltemperatur für den Storage-Controller des Geräts wurde überschritten.
Temperatursensor der Appliance entfernt	Ein Temperatursensor wurde entfernt.
UEFI Secure-Boot-Fehler der Appliance	Ein Gerät wurde nicht sicher hochgefahren.
Die Festplatten-I/O ist sehr langsam	Sehr langsame Festplatten-E/A könnte die Grid-Performance beeinträchtigen.

Alarmname	Beschreibung
Lüfterfehler des Storage Appliance erkannt	Ein Problem mit einer Lüftereinheit im Speichercontroller eines Geräts wurde erkannt.
Storage-Appliance-Speicheranbindung beeinträchtigt	Es besteht ein Problem mit einer oder mehreren Verbindungen zwischen dem Compute Controller und dem Storage Controller.
Speichermedium nicht zugänglich	Auf ein Speichermedium kann nicht zugegriffen werden.

Audit- und Syslog-Warnmeldungen

Alarmname	Beschreibung
Audit-Logs werden der In-Memory-Warteschlange hinzugefügt	Der Knoten kann keine Protokolle an den lokalen Syslog Server senden und die In-Memory-Warteschlange füllt sich.
Fehler bei der Weiterleitung des externen Syslog-Servers	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten.
Lange Prüfwarteschlange	Die Warteschlange für Prüfmeldungen ist voll. Wenn dieses Problem nicht behoben wird, können S3-Operationen fehlschlagen.
Protokolle werden der Warteschlange auf der Festplatte hinzugefügt	Der Knoten kann keine Protokolle an den externen Syslog-Server weiterleiten und die Warteschlange auf der Festplatte füllt sich.

Bucket-Benachrichtigungen

Alarmname	Beschreibung
FabricPool Bucket hat eine nicht unterstützte Bucket-Konsistenzeinstellung.	Ein FabricPool Bucket verwendet die Konsistenzstufe „Available“ oder „Strong-site“, die nicht unterstützt wird.
FabricPool Bucket verfügt über eine nicht unterstützte Versionierungseinstellung.	Ein FabricPool Bucket verfügt über aktivierte Versionierung oder S3 Object Lock, was nicht unterstützt wird.

Cassandra Warnungen

Alarmname	Beschreibung
Cassandra Auto-Compactor-Fehler	Beim Cassandra Auto-Compactor ist ein Fehler aufgetreten.
Cassandra Auto-Compactor-Metriken veraltet	Die Metriken, die den Cassandra Auto-Compactor beschreiben, sind veraltet.

Alarmname	Beschreibung
Cassandra-Kommunikationsfehler	Die Knoten, auf denen der Cassandra-Dienst läuft, haben Schwierigkeiten bei der Kommunikation untereinander.
Cassandra Compactions überlastet	Der Cassandra Compaction-Prozess ist überlastet.
Cassandra-Fehler beim Schreiben zu großer Datenmengen	Ein interner StorageGRID-Prozess hat eine zu große Schreibanforderung an Cassandra gesendet.
Cassandra Reparaturmetriken veraltet	Die Kennzahlen, die Cassandra-Reparaturaufträge beschreiben, sind veraltet.
Der Reparaturfortschritt von Cassandra ist langsam	Der Fortschritt der Cassandra Datenbankreparaturen ist langsam.
Cassandra Repair Service nicht verfügbar	Der Cassandra Reparaturservice ist nicht verfügbar.
Cassandra-Tabellenbeschädigung	Cassandra hat eine Tabellenbeschädigung festgestellt. Cassandra startet automatisch neu, wenn eine Tabellenbeschädigung festgestellt wird.

Cloud Storage Pool-Benachrichtigungen

Alarmname	Beschreibung
Fehler bei der Verbindung zum Cloud Storage Pool	Bei der Integritätsprüfung der Cloud Storage Pools wurden ein oder mehrere neue Fehler festgestellt.
Ablauf der IAM Roles Anywhere End-Entity-Zertifizierung	Das IAM Roles Anywhere Endbenutzerzertifikat läuft demnächst ab.

Warnungen zur gridübergreifenden Replikation

Alarmname	Beschreibung
Permanenter Ausfall der netzübergreifenden Replikation	Es ist ein Fehler bei der gridübergreifenden Replikation aufgetreten, der ein Eingreifen des Benutzers zur Behebung erfordert.
Ressourcen für die netzübergreifende Replikation nicht verfügbar	Cross-Grid-Replikationsanforderungen sind ausstehend, da eine Ressource nicht verfügbar ist.

DHCP-Warnmeldungen

Alarmname	Beschreibung
DHCP Lease abgelaufen	Die DHCP-Lease für eine Netzwerkschnittstelle ist abgelaufen.
DHCP Lease läuft bald ab	Das DHCP-Lease einer Netzwerkschnittstelle läuft in Kürze ab.
DHCP-Server nicht verfügbar	Der DHCP Server ist nicht verfügbar.

Debug- und Trace-Warnmeldungen

Alarmname	Beschreibung
Auswirkungen des Debuggens auf die Leistung	Wenn der Debug-Modus aktiviert ist, kann die Systemleistung negativ beeinflusst werden.
Trace-Konfiguration aktiviert	Wenn die Trace-Konfiguration aktiviert ist, kann sich dies negativ auf die Systemleistung auswirken.

E-Mail- und AutoSupport-Benachrichtigungen

Alarmname	Beschreibung
AutoSupport-Nachricht konnte nicht gesendet werden	Die letzte AutoSupport-Nachricht konnte nicht gesendet werden.
Fehler bei der Domainnamenauflösung	Der StorageGRID Knoten war nicht in der Lage, Domänennamen aufzulösen.
E-Mail-Benachrichtigungsfehler	Die E-Mail-Benachrichtigung für eine Warnung konnte nicht gesendet werden.
Archivierungsziel-Bucket für Protokolle nicht gefunden	Der Ziel-Bucket für die Protokollarchivierung fehlt, was verhindert, dass Protokolle im Ziel-Bucket archiviert werden.
SNMP Inform-Fehler	Fehler beim Senden von SNMP Inform-Benachrichtigungen an ein Trap-Ziel.
Externer SSH-Zugriff aktiviert	Der externe SSH-Zugriff ist seit mehr als 24 Stunden aktiviert.
SSH- oder Konsolenanmeldung erkannt	In den letzten 24 Stunden hat sich ein Benutzer mit Web Console oder SSH angemeldet.

Erasure-Coding (EC)-Warnungen

Alarmname	Beschreibung
Fehler bei der EC Neuausrichtung	Das EC-Neugewichtsverfahren ist fehlgeschlagen oder wurde abgebrochen.
EC-Reparaturfehler	Ein Reparaturjob für EC-Daten ist fehlgeschlagen oder wurde gestoppt.
EC-Reparatur ins Stocken geraten	Die Reparaturarbeiten an den EC-Daten sind ins Stocken geraten.
Fehler bei der Überprüfung des Erasure-Coded-Fragments	Mit Löschcodierung versehene Fragmente können nicht mehr verifiziert werden. Beschädigte Fragmente werden möglicherweise nicht repariert.

Benachrichtigungen zum Ablauf von Zertifikaten

Alarmname	Beschreibung
Ablauf des Admin Proxy CA-Zertifikats	Mindestens ein Zertifikat im CA-Bundle des Admin-Proxyservers läuft demnächst ab.
Ablauf des Client-Zertifikats	Mindestens ein Client-Zertifikat läuft demnächst ab.
Ablauf des globalen Serverzertifikats für S3	Das globale Serverzertifikat für S3 läuft demnächst ab.
Ablauf des Load Balancer Endpunktzertifikats	Mindestens ein Load Balancer Endpunktzertifikat läuft demnächst ab.
Ablauf des Serverzertifikats für die Managementoberfläche	Das für die Managementoberfläche verwendete Serverzertifikat läuft demnächst ab.
Ablauf des externen Syslog-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zur Signierung des externen Syslog-Serverzertifikats verwendet wurde, läuft demnächst ab.
Ablauf des externen Syslog-Client-Zertifikats	Das Clientzertifikat für einen externen Syslog-Server läuft demnächst ab.
Ablauf des externen Syslog-Server-Zertifikats	Das vom externen Syslog-Server präsentierte Serverzertifikat läuft demnächst ab.

Grid Network-Warnmeldungen

Alarmname	Beschreibung
MTU-Fehlanpassung im Grid Network	Die MTU-Einstellung für die Grid Network Schnittstelle (eth0) unterscheidet sich erheblich zwischen den Knoten im Grid.

Warnungen zur Grid-Föderation

Alarmname	Beschreibung
Ablauf des Grid Federation-Zertifikats	Mindestens ein Zertifikat der Grid Federation läuft demnächst ab.
Verbindungsfehler in der Grid-Föderation	Die Grid Federation Verbindung zwischen dem lokalen und dem entfernten Grid funktioniert nicht.

Warnmeldungen bei hoher Auslastung oder hoher Latenz

Alarmname	Beschreibung
Hohe Java Heap-Nutzung	Ein hoher Prozentsatz des Java-Heap-Speichers wird verwendet.
Hohe Latenz bei Metadatenabfragen	Die durchschnittliche Abfragezeit für Cassandra-Metadaten ist zu lang.

Warnungen zur Identitätsföderation

Alarmname	Beschreibung
Synchronisierungsfehler der Identitätsföderation	Die Synchronisierung von föderierten Gruppen und Benutzern aus der Identitätsquelle ist nicht möglich.
Fehler bei der Synchronisierung der Identitätsföderation für einen Mandanten	Die Synchronisierung von Verbundgruppen und Benutzern aus der vom Mandanten konfigurierten Identitätsquelle ist nicht möglich.

Warnmeldungen zum Information Lifecycle Management (ILM)

Alarmname	Beschreibung
ILM Platzierung nicht erreichbar	Eine Platzierungsanweisung in einer ILM-Regel kann für bestimmte Objekte nicht umgesetzt werden.
Niedrige ILM Scanrate	Die ILM Abtastrate ist auf weniger als 100 Objekte/Sekunde eingestellt.

Warnmeldungen des Key Management Servers (KMS)

Alarmname	Beschreibung
Ablauf des KMS CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), mit dem das Zertifikat des Schlüsselverwaltungsservers (KMS) signiert wurde, läuft demnächst ab.
Ablauf des KMS Clientzertifikats	Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft demnächst ab

Alarmname	Beschreibung
Die KMS Konfiguration konnte nicht geladen werden.	Die Konfiguration für den Schlüsselverwaltungsserver ist vorhanden, konnte jedoch nicht geladen werden.
KMS-Verbindungsfehler	Ein Appliance-Knoten konnte keine Verbindung zum Key Management Server für seinen Standort herstellen.
KMS-Verschlüsselungsschlüsselname nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt.
KMS-Verschlüsselungsschlüsselrotation fehlgeschlagen	Alle Appliance Volumes wurden erfolgreich entschlüsselt, aber bei einem oder mehreren Volumes konnte nicht auf den neuesten Schlüssel rotiert werden.
KMS ist nicht konfiguriert	Für diese Website existiert kein Schlüsselverwaltungsserver.
Der KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln.	Auf einem Gerät mit aktivierter Knotenverschlüsselung konnten ein oder mehrere Volumes mit dem aktuellen KMS-Schlüssel nicht entschlüsselt werden.
Ablauf des KMS-Serverzertifikats	Das vom Key Management Server (KMS) verwendete Serverzertifikat läuft demnächst ab.
Verbindungsfehler des KMS-Servers	Ein Appliance-Knoten konnte keine Verbindung zu einem oder mehreren Servern im Schlüsselverwaltungsserver-Cluster für seinen Standort herstellen.

Load Balancer-Warnmeldungen

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

Warnungen zur lokalen Zeitabweichung

Alarmname	Beschreibung
Großer Zeitversatz der Ortsuhr	Die Abweichung zwischen der lokalen Uhrzeit und der Network Time Protocol (NTP) Zeit ist zu groß.

Warnungen bei geringem Arbeitsspeicher oder geringem Speicherplatz

Alarmname	Beschreibung
Geringe Revisionsprotokoll-Speicherkapazität	Der verfügbare Speicherplatz für Revisionsprotokolle ist gering. Wenn dieses Problem nicht behoben wird, können S3-Operationen fehlschlagen.
Geringer verfügbarer Knotenspeicher	Die auf einem Knoten verfügbare RAM-Menge ist gering.
Geringer freier Speicherplatz für Storage-Pool	Der im Storage Node verfügbare Speicherplatz für Objektdaten ist gering.
Geringer installierter Knotenspeicher	Die installierte Speicherkapazität des Knotens ist gering.
Geringer Metadatenspeicher	Der verfügbare Speicherplatz für Objektmetadaten ist gering.
Niedrige Metrik Festplattenkapazität	Der verfügbare Speicherplatz für die Metrikdatenbank ist gering.
Niedriger Objektdatenspeicher	Der verfügbare Speicherplatz für Objektdaten ist gering.
Überschreiben des niedrigen schreibgeschützten Wasserzeichens	Der Wert für die Überschreibung des Soft-Read-Only-Watermarks des Speichervolumens ist niedriger als das minimale optimierte Watermark für einen Storage Node.
Geringe Root-Disk-Kapazität	Der verfügbare Speicherplatz auf der Root-Festplatte ist gering.
Geringe Systemdatenkapazität	Der verfügbare Speicherplatz für /var/local ist knapp. Wenn dieses Problem nicht behoben wird, können S3-Operationen fehlschlagen.
Geringer freier Speicherplatz im temporären Verzeichnis	Der verfügbare Speicherplatz im Verzeichnis /tmp ist knapp.

Knoten- oder Knotennetzwerk-Warnmeldungen

Alarmname	Beschreibung
ADC-Quorum nicht erreicht	Der Speicherknoten mit ADC-Dienst ist offline. Erweiterungs- und Außerbetriebnahmevorgänge sind blockiert, bis das ADC-Quorum wiederhergestellt ist.
Admin Network Empfangsnutzung	Die Auslastung des Admin Network ist hoch.
Admin Network Übertragungsnutzung	Die Auslastung des Admin Network ist hoch.

Alarmname	Beschreibung
Firewall-Konfigurationsfehler	Die Firewall-Konfiguration konnte nicht angewendet werden.
Managementoberflächen-Endpunkte im Fallback-Modus	Alle Managementoberfläche-Endpunkte greifen schon viel zu lange auf die Standardports zurück.
Fehler bei der Netzwerkverbindung des Node	Beim Übertragen von Daten zwischen den Knoten sind Fehler aufgetreten.
Empfangsfehler im Knotennetzwerk	Ein hoher Prozentsatz der von einem Knoten empfangenen Netzwerk-Frames wies Fehler auf.
Knoten nicht mit NTP-Server synchronisiert	Der Knoten ist nicht mit dem Network Time Protocol (NTP)-Server synchronisiert.
Knoten nicht mit NTP-Server gesperrt	Der Knoten ist nicht an einen Network Time Protocol (NTP)-Server gebunden.
Netzwerk des Non-appliance-Knotens ausgefallen	Mindestens ein Netzwerkgerät ist ausgefallen oder nicht verbunden.
Verbindung der Servicegeräte im Admin-Netzwerk unterbrochen	Die Schnittstelle des Geräts zum Admin Network (eth1) ist ausgefallen oder getrennt.
Die Verbindung des Services Appliance zum Admin-Netzwerkport 1 ist unterbrochen.	Der Admin Network Port 1 des Geräts ist ausgefallen oder nicht angeschlossen.
Verbindung des Servicegeräts im Client Network unterbrochen	Die Schnittstelle des Geräts zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung der Services Appliance an Netzwerkport 1 unterbrochen	Netzwerkport 1 am Gerät ist ausgefallen oder getrennt.
Servicegerät-Verbindung an Netzwerkport 2 unterbrochen	Netzwerkport 2 des Geräts ist ausgefallen oder getrennt.
Servicegerät-Link an Netzwerkport 3 ausgefallen	Netzwerkport 3 des Geräts ist ausgefallen oder getrennt.
Verbindung des Services Appliance zu Netzwerkport 4 unterbrochen	Netzwerkport 4 am Gerät ist ausgefallen oder getrennt.
Verbindung des Storage Appliance im Admin-Netzwerk unterbrochen	Die Schnittstelle des Geräts zum Admin Network (eth1) ist ausgefallen oder getrennt.

Alarmname	Beschreibung
Verbindung des Storage Appliance zu Admin Network Port 1 unterbrochen	Der Admin Network Port 1 des Geräts ist ausgefallen oder nicht angeschlossen.
Verbindung zum Storage Appliance im Clientnetzwerk unterbrochen	Die Schnittstelle des Geräts zum Client-Netzwerk (eth2) ist ausgefallen oder getrennt.
Verbindung des Storage Appliance an Netzwerkport 1 unterbrochen	Netzwerkport 1 am Gerät ist ausgefallen oder getrennt.
Verbindung des Storage Appliance an Netzwerkport 2 unterbrochen	Netzwerkport 2 des Geräts ist ausgefallen oder getrennt.
Verbindung des Storage Appliance an Netzwerkport 3 unterbrochen	Netzwerkport 3 des Geräts ist ausgefallen oder getrennt.
Verbindung des Storage Appliance an Netzwerkport 4 unterbrochen	Netzwerkport 4 am Gerät ist ausgefallen oder getrennt.
Speicherknoten befindet sich nicht im gewünschten Speicherzustand	Der LDR-Dienst auf einem Storage Node kann aufgrund eines internen Fehlers oder eines volumenbezogenen Problems nicht in den gewünschten Zustand wechseln.
TCP-Verbindungsnutzung	Die Anzahl der TCP-Verbindungen auf diesem Knoten nähert sich der maximal nachverfolgbaren Anzahl.
Kommunikation mit dem Knoten nicht möglich	Ein oder mehrere Dienste reagieren nicht oder der Knoten ist nicht erreichbar.
Unerwarteter Neustart des Knotens	Ein Knoten wurde innerhalb der letzten 24 Stunden unerwartet neu gestartet.

Objektwarnungen

Alarmname	Beschreibung
Objektexistenzprüfung fehlgeschlagen	Der Auftrag zur Überprüfung der Objektexistenz ist fehlgeschlagen.
Objektexistenzprüfung angehalten	Der Job zur Überprüfung der Objektexistenz ist hängen geblieben.
Objekte, die möglicherweise verloren gegangen sind	Ein oder mehrere Objekte sind möglicherweise aus dem Grid verloren gegangen.
Verwaiste Objekte erkannt	Es wurden verwaiste Objekte entdeckt.

Alarmname	Beschreibung
S3 PUT Objektgröße zu groß	Ein Client versucht eine PUT Object-Operation, die die Größenbeschränkungen von S3 überschreitet.
Nicht identifiziertes beschädigtes Objekt erkannt	Im replizierten Objektspeicher wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte.

Objektbeschädigungswarnungen

Alarmname	Beschreibung
Objektgrößenkonflikt	Während der Überprüfung der Objektexistenz wurde eine unerwartete Objektgröße festgestellt.

Benachrichtigungen von Plattformdiensten

Alarmname	Beschreibung
Die Kapazität der Plattformdienste für ausstehende Anfragen ist gering.	Die Anzahl der ausstehenden Anfragen an die Plattformdienste nähert sich der Kapazitätsgrenze.
Plattformdienste nicht verfügbar	An einem Standort sind zu wenige Speicherknoten mit dem RSM-Dienst aktiv oder verfügbar.

Warnungen zum Storage-Volumen

Alarmname	Beschreibung
Speichervolumen erfordert Aufmerksamkeit	Ein Speichervolumen ist offline und benötigt Aufmerksamkeit.
Das Speichervolumen muss wiederhergestellt werden	Ein Speichervolumen wurde wiederhergestellt und muss zurückgespielt werden.
Speichervolumen offline	Ein Speichervolumen ist seit mehr als 5 Minuten offline.
Versuch, das Speichervolume erneut einzubinden	Ein Speichervolume war offline und hat eine automatische Wiedereinbindung ausgelöst. Dies könnte auf ein Laufwerksproblem oder Dateisystemfehler hinweisen.
Die Wiederherstellung des Volumes konnte die Reparatur der replizierten Daten nicht starten.	Die Reparatur replizierter Daten für ein repariertes Volume konnte nicht automatisch gestartet werden.

StorageGRID Services-Warnungen

Alarmname	Beschreibung
nginx Service mit Backup-Konfiguration	Die Konfiguration des nginx Service ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.
nginx-gw Service mit Backup-Konfiguration	Die Konfiguration des nginx-gw Dienstes ist ungültig. Die vorherige Konfiguration wird jetzt verwendet.
Neustart erforderlich, um FIPS zu deaktivieren	Die Sicherheitsrichtlinie erfordert keinen FIPS-Modus, aber FIPS-Module sind in Verwendung.
Neustart erforderlich, um FIPS zu aktivieren	Die Sicherheitsrichtlinie erfordert den FIPS-Modus, aber FIPS-Module sind nicht in Verwendung.
SSH-Dienst mit Backup-Konfiguration	Die Konfiguration des SSH-Dienstes ist ungültig. Die vorherige Konfiguration wird nun verwendet.

Mandantenwarnungen

Alarmname	Beschreibung
Hohe Mandantenquotenauslastung	Ein hoher Prozentsatz des Quota-Speicherplatzes wird verwendet. Diese Regel ist standardmäßig deaktiviert, da sie zu viele Benachrichtigungen verursachen könnte.

Häufig verwendete Prometheus-Metriken in StorageGRID

Diese Liste häufig verwendeter Prometheus-Metriken bietet einen besseren Überblick über die Bedingungen in den Standard-Alarmregeln oder dient als Grundlage für die Erstellung von Bedingungen für benutzerdefinierte Alarmregeln.

Sie können auch Eine vollständige Liste aller Kennzahlen erhalten.

Weitere Informationen zur Syntax von Prometheus-Abfragen finden Sie unter "Prometheus-Abfragen".

Was sind Prometheus Metriken?

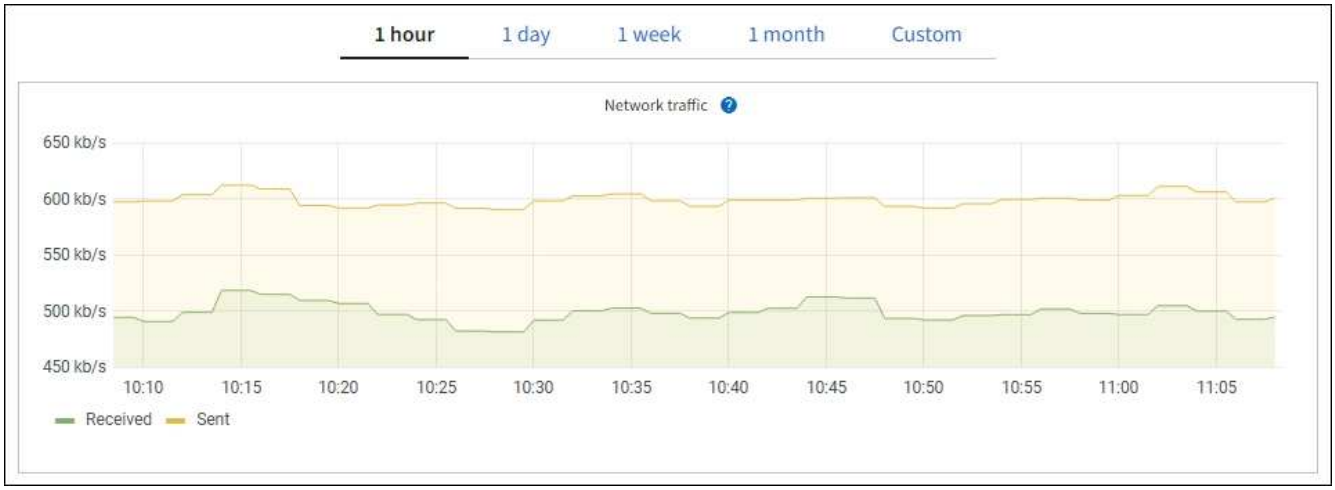
Prometheus-Metriken sind Zeitreihenmessungen. Der Prometheus-Dienst auf den Admin-Nodes sammelt diese Metriken von den Diensten auf allen Nodes. Die Metriken werden auf jedem Admin-Node gespeichert, bis der für Prometheus-Daten reservierte Speicherplatz voll ist. Wenn das `/var/local/mysql_ibdata/` Volume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

Wo werden Prometheus Metriken verwendet?

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

- **Knotenseite**: Die auf der Knotenseite verfügbaren Diagramme und Grafiken nutzen das Visualisierungstool Grafana, um die von Prometheus erfassten Zeitreihenmetriken anzuzeigen. Grafana

stellt Zeitreihendaten in Diagramm- und Grafikform dar, während Prometheus als Backend-Datenquelle dient.



- **Warnungen**: Warnungen werden bei bestimmten Schweregraden ausgelöst, wenn die Bedingungen der Warnungsregeln, die Prometheus-Metriken verwenden, als wahr ausgewertet werden.
- **Grid Management API**: Prometheus-Metriken können in benutzerdefinierten Alarmregeln oder mit externen Automatisierungstools verwendet werden, um das StorageGRID-System zu überwachen. Eine vollständige Liste der Prometheus-Metriken ist über die Grid Management API verfügbar. (Im oberen Bereich des Grid Manager das Hilfesymbol auswählen und dann **API documentation** > **metrics** wählen.) Obwohl mehr als tausend Metriken verfügbar sind, ist nur eine relativ geringe Anzahl erforderlich, um die wichtigsten StorageGRID Operationen zu überwachen.

  Metriken, die *private* in ihrem Namen enthalten, sind nur für den internen Gebrauch bestimmt und können sich zwischen StorageGRID Versionen ohne Vorankündigung ändern.

- Die Seiten **Support** > **Tools** > **Diagnostics** und **Support** > **Tools** > **Metrics**: Diese Seiten, die in erster Linie für den technischen Support gedacht sind, bieten verschiedene Tools und Diagramme, die die Werte der Prometheus-Metriken verwenden.

  Einige Funktionen und Menüpunkte auf der Seite „Metriken“ sind absichtlich nicht funktionsfähig und unterliegen Änderungen.

Liste der gebräuchlichsten Kennzahlen

Die folgende Liste enthält die am häufigsten verwendeten Prometheus Metriken.

Metriken, die *private* in ihrem Namen enthalten, sind nur für den internen Gebrauch bestimmt und können sich zwischen StorageGRID Releases ohne vorherige Ankündigung ändern.

alertmanager_notifications_failed_total

Die Gesamtzahl der fehlgeschlagenen Warnbenachrichtigungen.

node_filesystem_avail_bytes

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

node_memory_MemAvailable_bytes

Speicherinformationsfeld MemAvailable_bytes.

Knoten Netzwerkträger

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

node_network_receive_errs_total

Netzwerkgerätstatistik `receive_errs`.

node_network_transmit_errs_total

Netzwerkgerätstatistik `transmit_errs`.

storagegrid_administratively_down

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

StorageGRID Appliance Compute Controller Hardwarestatus

Der Status der Compute Controller Hardware in einem Appliance.

storagegrid_appliance_failed_disks

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

StorageGRID Appliance Storage-Controller-Hardwarestatus

Der Gesamtstatus der Storage-Controller-Hardware in einem Appliance.

StorageGRID Inhalts-Buckets und -Container

Die Gesamtzahl der von diesem Storage Node erkannten S3-Buckets.

StorageGRID Inhaltsobjekte

Die Gesamtzahl der von diesem Storage Node erkannten S3-Datenobjekte. Die Zählung ist nur für Datenobjekte gültig, die von Clientanwendungen erstellt wurden, die über S3 mit dem System interagieren.

storagegrid_content_objects_lost

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

"Fehlerbehebung bei verlorenen und fehlenden Objektdaten"

storagegrid_http_sessions_incoming_attempted

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

storagegrid_http_sessions_incoming_currently_established

Die Anzahl der aktuell aktiven (offenen) HTTP-Sitzungen auf dem Storage Node.

storagegrid_http_sessions_incoming_failed

Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen wurden, entweder aufgrund einer fehlerhaften HTTP-Anfrage oder 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 Knoten, die nach dem Scan auf die ILM-Auswertung warten.

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

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

storagegrid_ilm_awaiting_client_objects

Die Gesamtzahl der Objekte auf diesem Knoten, die auf die ILM-Auswertung aus Clientoperationen (zum Beispiel Ingest) warten.

storagegrid_ilm_awaiting_total_objects

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

storagegrid_ilm_scan_objects_per_second

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

storagegrid_ilm_scan_period_estimated_minutes

Die geschätzte Zeit für einen vollständigen ILM-Scan auf diesem Node.

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

storagegrid_load_balancer_endpoint_cert_expiry_time

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

Durchschnittliche Latenz von StorageGRID-Metadatenabfragen in Millisekunden

Die durchschnittliche Zeit, die für die Ausführung einer Abfrage gegen den Metadatenspeicher über diesen Dienst erforderlich ist.

storagegrid_network_received_bytes

Die Gesamtmenge der seit der Installation empfangenen Daten.

storagegrid_network_transmitted_bytes

Die Gesamtmenge der seit der Installation gesendeten Daten.

StorageGRID Node-CPU-Auslastung in Prozent

Der Prozentsatz der verfügbaren CPU-Zeit, der aktuell von diesem Dienst genutzt wird. Zeigt, wie stark der Dienst ausgelastet ist. Die verfügbare CPU-Zeit hängt von der Anzahl der CPUs des Servers ab.

storagegrid_ntp_chosen_time_source_offset_milliseconds

Systematische Zeitverschiebung, die durch eine gewählte Zeitquelle verursacht wird. Eine Verschiebung entsteht, wenn die Verzögerung bis zum Erreichen einer Zeitquelle nicht der Zeit entspricht, die die Zeitquelle benötigt, um den NTP Client zu erreichen.

storagegrid_ntp_locked

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

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

Die Gesamtmenge der Daten, die von S3-Clients von diesem Storage Node seit dem letzten Zurücksetzen des Attributs abgerufen wurden.

storagegrid_s3_operations_failed

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

storagegrid_s3_operations_successful

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

storagegrid_s3_operations_unauthorized

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

storagegrid_servercertificate_management_interface_cert_expiry_days

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

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

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

storagegrid_service_cpu_seconds

Die kumulierte Zeit, während der die CPU von diesem Dienst seit der Installation genutzt wurde.

storagegrid Dienst Speichernutzungsbytes

Die Menge an Arbeitsspeicher (RAM), die dieser Dienst aktuell verwendet. Dieser Wert ist identisch mit dem von der Linux-Top-Dienstprogramm als RES angezeigten Wert.

storagegrid_service_network_received_bytes

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

storagegrid_service_network_transmitted_bytes

Die Gesamtmenge der von diesem Dienst gesendeten Daten.

storagegrid_service_restarts

Die Gesamtzahl der Neustarts des Dienstes.

storagegrid_service_runtime_seconds

Die Gesamtzeit, die der Dienst seit der Installation in Betrieb ist.

storagegrid_service_uptime_seconds

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

storagegrid_storage_state_current

Der aktuelle Status der Speicherdienste. Die Attributwerte sind:

- 10 = Offline

- 15 = Wartung
- 20 = Nur-Lesezugriff
- 30 = Online

StorageGRID Speicherstatus

Der aktuelle Status der Speicherdienste. Die Attributwerte sind:

- 0 = Keine Fehler
- 10 = Im Übergang
- 20 = Unzureichender freier Speicherplatz
- 30 = Volume(s) nicht verfügbar
- 40 = Fehler

storagegrid_storage_utilization_data_bytes

Eine Schätzung der Gesamtgröße der replizierten und mit Erasure-Codierung versehenen Objektdaten auf dem Storage Node.

storagegrid_storage_utilization_metadata_allowed_bytes

Der gesamte Speicherplatz auf Volume 0 jedes Storage Node, der für Objektmetadaten erlaubt ist. Dieser Wert ist stets geringer als der tatsächlich für Metadaten reservierte Speicherplatz auf einem Node, da ein Teil des reservierten Speicherplatzes für essentielle Datenbankoperationen (wie Komprimierung und Reparatur) sowie zukünftige Hardware- und Software-Upgrades benötigt wird. Der erlaubte Speicherplatz für Objektmetadaten steuert die Gesamtkapazität der Objekte.

storagegrid_storage_utilization_metadata_bytes

Die Menge der Objektmetadaten auf Speichervolume 0, in Bytes.

storagegrid_Speicherauslastung_Gesamtspeicherplatz_Bytes

Die Gesamtmenge des allen Objektspeichern zugewiesenen Speicherplatzes.

StorageGRID_Speicherauslastung_verwendbarer_Speicherplatz_Bytes

Die insgesamt verbleibende Menge an Objektspeicherplatz. Berechnet durch Addition des verfügbaren Speicherplatzes aller Objektspeicher auf dem Storage Node.

storagegrid_tenant_usage_data_bytes

Die logische Größe aller Objekte für den Mandanten.

storagegrid_tenant_usage_object_count

Die Anzahl der Objekte für den Mandanten.

storagegrid_tenant_usage_quota_bytes

Die maximal verfügbare Menge an logischem Speicherplatz für die Objekte des Mandanten. Wenn keine Kontingentmetrik angegeben ist, steht unbegrenzt viel Speicherplatz zur Verfügung.

Eine Liste aller Kennzahlen abrufen

Die vollständige Liste der Metriken ist über die Grid Management API verfügbar.

Schritte

1. Oben im Grid Manager das Hilfesymbol auswählen und anschließend **API documentation** wählen.

2. Die **Metrik**-Operationen befinden sich an folgender Stelle.
3. Die `GET /grid/metric-names`Operation ausführen.
4. Die Ergebnisse herunterladen.

Referenz zu Protokolldateien

StorageGRID-Protokolldateien

StorageGRID stellt Protokolle bereit, die Ereignisse, Diagnosemeldungen und Fehlerzustände erfassen. Es kann vorkommen, dass Protokolldateien gesammelt und an den technischen Support weitergeleitet werden müssen, um die Fehlerbehebung zu unterstützen.

Die Protokolle werden wie folgt kategorisiert:

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

> Die Angaben zu den einzelnen Protokolltypen dienen lediglich als Referenz. Die Protokolle sind für die erweiterte Fehlerbehebung durch den technischen Support vorgesehen. Fortgeschrittene Techniken, die die Rekonstruktion des Problemverlaufs anhand der Audit-Protokolle und der Anwendungsprotokolldateien beinhalten, fallen nicht in den Rahmen dieser Anleitung.

Auf die Protokolle zugreifen

Um auf die Protokolle zuzugreifen, können Sie "Protokolldateien und Systemdaten sammeln" von einem oder mehreren Knoten als einzelnes Protokolldateiarchiv abrufen. Alternativ ist der Zugriff auf einzelne Protokolldateien für jeden Grid-Knoten wie folgt möglich:

Schritte

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

Protokolle an den Syslog Server exportieren

Der Export der Protokolle an den Syslog-Server bietet folgende Funktionen:

- Eine Liste aller Grid Manager und Tenant Manager Anfragen sowie der S3 Anfragen wird bereitgestellt.
- Bessere Transparenz bei S3-Anfragen, die Fehler zurückgeben, ohne die Leistungseinbußen, die durch Audit-Protokollierungsmethoden verursacht werden.
- Zugriff auf HTTP-Layer-Anfragen und Fehlercodes, die leicht zu parsen sind.
- Bessere Transparenz hinsichtlich der Anfragen, die von den Verkehrsklassifikatoren am Load Balancer blockiert wurden.

Zum Exportieren der Protokolle siehe "Logverwaltung und externen Syslog-Server konfigurieren".

Protokolldateikategorien

Das StorageGRID-Protokolldateiarchiv enthält die für jede Kategorie beschriebenen Protokolle sowie zusätzliche Dateien, die Metriken und Debug-Befehlsausgaben enthalten.

Archivierungsort	Beschreibung
Prüfung	Während des normalen Systembetriebs generierte Audit-Meldungen.
Base-OS-Protokolle	Informationen zum Basisbetriebssystem, einschließlich StorageGRID Image Versionen.
Pakete	Globale Konfigurationsinformationen (Bundles).
cache-svc	Cache-Service-Protokolle (nur auf Gateway-Knoten).
cassandra	Cassandra Datenbankinformationen und Reaper-Reparaturprotokolle.
ec	VCS-Informationen über den aktuellen Knoten und EC-Gruppeninformationen nach Profil-ID.
Grid	Allgemeine Grid-Protokolle einschließlich Debug (`bycast.log`) und `servermanager` Protokolle.
grid.json	Die Grid Konfigurationsdatei wird von allen Knoten gemeinsam genutzt. Zusätzlich ist `node.json` spezifisch für den aktuellen Knoten.
hagroups	Metriken und Protokolle von Hochverfügbarkeitsgruppen.
installieren	`Gdu-server` und Installationsprotokolle.
Lambda-Arbitrator	Protokolle im Zusammenhang mit der S3 Select Proxy-Anfrage.
durchgesickert	Protokolle des leakd-Dienstes.
lumberjack.log	Debug-Meldungen im Zusammenhang mit der Protokollerfassung.
Kennzahlen	Serviceprotokolle für Grafana, Jaeger, node exporter und Prometheus.
miscd	Miscd Zugriffs- und Fehlerprotokolle.
mysql	Die MariaDB Datenbankkonfiguration und zugehörige Protokolle.
net	Von netzwerkbezogenen Skripten und dem Dynip-Dienst generierte Protokolle.

Archivierungsort	Beschreibung
nginx	Konfigurationsdateien und Protokolle für Load Balancer und Grid Federation. Enthält außerdem die Traffic-Protokolle von Grid Manager und Tenant Manager.
nginx-gw	• `access.log`: Protokollmeldungen zu Anfragen von Grid Manager und Tenant Manager. ◦ Diese Meldungen sind mit `mgmt:` versehen, wenn sie mit syslog exportiert werden. ◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: Eingehende Cross-Grid-Replikationsanforderungen. ◦ Diese Meldungen sind mit `cgr:` versehen, wenn sie mit syslog exportiert werden. ◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: S3-Anfragen an Load Balancer-Endpunkte. ◦ Diese Meldungen sind mit `endpoint:` versehen, wenn sie mit syslog exportiert werden. ◦ Das Format dieser Protokollmeldungen ist `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: Bezieht sich auf die neue DNS-Prüfwarnung.
ntp	NTP Konfigurationsdatei und Protokolle.
Verwaiste Objekte	Protokolle zu verwaisten Objekten.
Betriebssystem	Knoten- und Grid-Statusdatei, einschließlich Dienste `pid`.
andere	Protokolldateien unter `/var/local/log`, die nicht in anderen Ordnern gesammelt werden.
perf	Leistungsinformationen für CPU, Netzwerk und Festplatten-E/A.
prometheus-data	Aktuelle Prometheus-Metriken, sofern die Protokollsammlung Prometheus-Daten enthält.
Bereitstellung	Protokolle im Zusammenhang mit dem Grid-Bereitstellungsprozess.

Archivierungsort	Beschreibung
Raft	Protokolle des Raft-Clusters, die in Plattformdiensten verwendet werden.
ssh	Protokolle im Zusammenhang mit der SSH-Konfiguration und dem Service.
SNMP	SNMP-Agentenkonfiguration, die für das Senden von SNMP-Benachrichtigungen verwendet wird.
Sockets-Daten	Socket-Daten für Netzwerk-Debug.
system-commands.txt	Ausgabe der StorageGRID Containerbefehle. Enthält Systeminformationen, wie Netzwerk- und Festplattennutzung.
Synchronize-Recovery-Package	Im Zusammenhang mit der Aufrechterhaltung der Konsistenz des neuesten Wiederherstellungspakets auf allen Admin Nodes und Storage Nodes, die den ADC-Service hosten.

StorageGRID Softwareprotokolle

Mit StorageGRID Protokollen lassen sich Probleme beheben.

> Wenn Sie Ihre Protokolle an einen externen Syslog-Server senden oder das Ziel von Audit-Informationen wie dem `bycast.log` und `nms.log` ändern möchten, siehe "Protokollverwaltung konfigurieren".

Allgemeine StorageGRID Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/bycast.log	Die primäre StorageGRID Fehlerbehebungsdatei.	Alle Knoten
/var/local/log/bycast-err.log	Enthält eine Teilmenge von `bycast.log` (Meldungen mit Schweregrad ERROR und CRITICAL). CRITICAL-Meldungen werden ebenfalls im System angezeigt.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/core/	Enthält alle Core-Dump-Dateien, die bei einem abnormalen Programmabbruch erstellt wurden. Mögliche Ursachen sind Assertionsfehler, Verstöße oder Thread-Timeouts. **Hinweis**: Die Datei `/var/local/core/kexec_cmd` ist normalerweise auf den Appliance-Knoten vorhanden und stellt keinen Fehler dar.	Alle Knoten

Protokolle im Zusammenhang mit Verschlüsselung

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

Protokolle der Grid Federation

Dateiname	Hinweise	Gefunden auf
/var/local/log/update_grid_federation_config.log	Enthält Protokolle im Zusammenhang mit der Generierung von nginx- und nginx-gw-Konfigurationen für Grid Federation-Verbindungen.	Alle Knoten

NMS-Protokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/nms.log	• Erfasst Benachrichtigungen vom Grid Manager und vom Tenant Manager. • Erfasst Ereignisse im Zusammenhang mit dem Betrieb des NMS-Dienstes. Beispielsweise E-Mail-Benachrichtigungen und Konfigurationsänderungen. • Enthält XML-Bundle-Aktualisierungen, die sich aus im System vorgenommenen Konfigurationsänderungen ergeben. • Enthält Fehlermeldungen im Zusammenhang mit dem einmal täglich durchgeführten Downsampling von Attributen. • Enthält Fehlermeldungen des Java-Webservers, beispielsweise Fehler bei der Seitengenerierung und HTTP-Status-500-Fehler. • Enthält Protokolle im Zusammenhang mit AutoSupport.	Admin-Nodes
/var/local/log/nms.errlog	Enthält Fehlermeldungen im Zusammenhang mit MySQL Datenbank-Upgrades. Enthält den Standardfehlerstrom (stderr) der entsprechenden Dienste. Pro Dienst existiert eine Protokolldatei. Diese Dateien sind in der Regel leer, es sei denn, es treten Probleme mit dem Dienst auf.	Admin-Nodes
/var/local/log/nms.requestlog	Enthält Informationen über ausgehende Verbindungen von der Management-API zu internen StorageGRID Services.	Admin-Nodes

Server-Manager-Protokolle

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

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

StorageGRID Dienstprotokolle

Dateiname	Hinweise	Gefunden auf
/var/local/log/acct.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/adc.errlog	Enthält den Standardfehlerstrom (stderr) der entsprechenden Dienste. Pro Dienst existiert eine Protokolldatei. Diese Dateien sind in der Regel leer, es sei denn, es treten Probleme mit dem Dienst auf.	Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/ams.errlog		Admin-Nodes
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	Cache-Service-Protokolle.	Gateway-Nodes
/var/local/log/cassandra/system.log	Informationen für den Metadatenspeicher (Cassandra Datenbank), die verwendet werden können, wenn beim Hinzufügen neuer Storage Nodes Probleme auftreten oder wenn die nodetool repair Aufgabe hängen bleibt.	Speicherknoten
/var/local/log/cassandra-reaper.log	Informationen zum Cassandra Reaper Dienst, der Reparaturen an den Daten in der Cassandra Datenbank durchführt.	Speicherknoten
/var/local/log/cassandra-reaper.errlog	Fehlerinformationen für den Cassandra Reaper Dienst.	Speicherknoten
/var/local/log/chunk.errlog		Speicherknoten
/var/local/log/cmn.errlog		Admin-Nodes

Dateiname	Hinweise	Gefunden auf
/var/local/log/cms.errlog	Diese Protokolldatei kann auf Systemen vorhanden sein, die von einer älteren Version von StorageGRID aktualisiert wurden. Sie enthält veraltete Informationen.	Speicherknoten
/var/local/log/dds.errlog		Speicherknoten
/var/local/log/dmv.errlog		Speicherknoten
/var/local/log/dynip*	Enthält Protokolle im Zusammenhang mit dem dynip Service, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Knoten
/var/local/log/grafana.log	Das Protokoll, das mit dem Grafana Service verknüpft ist und zur Visualisierung von Metriken 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 Zustandsänderungen, wie den Übergang von BACKUP zu MASTER oder FAULT.	Admin Nodes und Gateway Nodes
/var/local/log/idnt.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird
/var/local/log/jaeger.log	Das Protokoll, das mit dem jaeger Service verknüpft ist und für die Trace-Erfassung verwendet wird.	Alle Knoten
/var/local/log/kstn.errlog		Speicherknoten, auf denen der ADC-Dienst ausgeführt wird

Dateiname	Hinweise	Gefunden auf
/var/local/log/lambda*	Enthält Protokolle für den S3 Select Service.	Admin- und Gateway-Knoten Nur bestimmte Admin- und Gateway-Knoten enthalten dieses Protokoll. Siehe "S3 Select Anforderungen und Beschränkungen für Admin- und Gateway-Knoten".
/var/local/log/ldr.errlog		Speicherknoten
/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 Knoten bietet, wie zum Beispiel das Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Knoten
/var/local/log/nginx/*.log	Enthält Protokolle für den nginx-Dienst, der als Authentifizierung und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und Dynip) fungiert, damit Dienste auf anderen Knoten über HTTPS-APIs angesprochen werden können.	Alle Knoten
/var/local/log/nginx-gw/*.log	Enthält allgemeine Protokolle im Zusammenhang mit dem nginx-gw Service, einschließlich Fehlerprotokollen und Protokollen für die eingeschränkten Admin-Ports auf den Admin-Nodes.	Admin Nodes und Gateway Nodes
/var/local/log/nginx-gw/cgr-access.log.gz	Enthält Zugriffsprotokolle im Zusammenhang mit dem gridübergreifenden Replikationsverkehr.	Administratorknoten, Gateway-Knoten oder beides, abhängig von der Grid-Federation-Konfiguration. Nur im Ziel-Grid für die gridübergreifende Replikation vorhanden.

Dateiname	Hinweise	Gefunden auf
/var/local/log/nginx-gw/endpoint-access.log.gz	Enthält Zugriffsprotokolle für den Load Balancer Service, der den Lastausgleich des S3-Datenverkehrs von Clients zu Storage Nodes bereitstellt.	Admin Nodes und Gateway Nodes
/var/local/log/persistence*	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Stammfestplatte verwaltet, die auch nach einem Neustart erhalten bleiben müssen.	Alle Knoten
/var/local/log/prometheus.log	Für alle Knoten sind das Node Exporter Service-Log und das ade-exporter Metrics Service-Log enthalten. Für Admin-Knoten sind außerdem Protokolle für die Dienste Prometheus und Alert Manager enthalten.	Alle Knoten
/var/local/log/raft.log	Enthält die Ausgabe der Bibliothek, die vom RSM-Dienst für das Raft-Protokoll verwendet wird.	Speicherknoten mit RSM Dienst
/var/local/log/rms.errlog	Enthält Protokolle für den Replicated State Machine Service (RSM) Dienst, der für S3 Plattformdienste verwendet wird.	Speicherknoten mit RSM Dienst
/var/local/log/ssm.errlog		Alle Knoten
/var/local/log/update-s3vs-domains.log	Enthält Protokolle im Zusammenhang mit der Verarbeitung von Aktualisierungen für die S3 virtual hosted domain names Konfiguration. In den Anweisungen zur Implementierung von S3 Client-Anwendungen finden sich weitere Informationen.	Admin- und Gateway-Knoten
/var/local/log/update-snmp-firewall.*	Enthält Protokolle zu den Firewall-Ports, die für SNMP verwaltet werden.	Alle Knoten
/var/local/log/update-sysl.log	Enthält Protokolle im Zusammenhang mit Änderungen an der System-Syslog-Konfiguration.	Alle Knoten

Dateiname	Hinweise	Gefunden auf
/var/local/log/update-traffic-classes.log	Enthält Protokolle im Zusammenhang mit Änderungen an der Konfiguration der Verkehrsklassifikatoren.	Admin- und Gateway-Knoten
/var/local/log/update-utcn.log	Enthält Protokolle im Zusammenhang mit dem Modus „Untrusted Client Network“ auf diesem Knoten.	Alle Knoten

Verwandte Informationen

- "Über die bycast.log"
- "S3 REST-API verwenden"

Bereitstellungs- und Wartungsprotokolle in StorageGRID

Die Bereitstellungs- und Wartungsprotokolle bieten Unterstützung bei der Fehlerbehebung.

Dateiname	Hinweise	Gefunden auf
/var/local/log/install.log	Erstellt während der Softwareinstallation. Enthält ein Protokoll der Installationsereignisse.	Alle Knoten
/var/local/log/expansion-progress.log	Erstellt im Rahmen der Erweiterungsmaßnahmen. Enthält eine Aufzeichnung der Erweiterungsereignisse.	Speicherknoten
/var/local/log/pa-move.log	Erstellt während der Ausführung des `pa-move.sh` Skripts.	Primärer Admin-Knoten
/var/local/log/pa-move-new_pa.log	Erstellt während der Ausführung des `pa-move.sh` Skripts.	Primärer Admin-Knoten
/var/local/log/pa-move-old_pa.log	Erstellt während der Ausführung des `pa-move.sh` Skripts.	Primärer Admin-Knoten
/var/local/log/gdu-server.log	Erstellt vom GDU Service. Enthält Ereignisse im Zusammenhang mit Bereitstellungs- und Wartungsverfahren, die vom primären Admin-Node verwaltet werden.	Admin-Nodes
/var/local/log/send_admin_hw.log	Wurde während der Installation erstellt. Enthält Debugging-Informationen zur Kommunikation eines Knotens mit dem primären Admin Node.	Alle Knoten
/var/local/log/upgrade.log	Erstellt während eines Software-Upgrades. Enthält eine Aufzeichnung der Software-Update-Ereignisse.	Alle Knoten

Erfahren Sie mehr über die StorageGRID bycast.log

Die Datei `/var/local/log/bycast.log` ist die primäre Datei zur Fehlerbehebung für die StorageGRID-Software. Für jeden Grid-Knoten gibt es eine `bycast.log` Datei. Die Datei enthält Meldungen, die spezifisch für diesen Grid-Knoten sind.

Die Datei `/var/local/log/bycast-err.log` ist eine Teilmenge von `bycast.log`. Sie enthält Meldungen mit dem Schweregrad ERROR und CRITICAL.

Optional kann das Ziel der Audit-Logs geändert und Audit-Informationen an einen externen Syslog-Server gesendet werden. Lokale Protokolle der Audit-Einträge werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe "Logverwaltung und externen Syslog-Server konfigurieren".

Dateirotation für bycast.log

Wenn die `bycast.log` Datei 1 GB groß ist, wird die bestehende Datei gespeichert und eine neue Protokolldatei erstellt.

Die gespeicherte Datei wird umbenannt `bycast.log.1`, und die neue Datei erhält den Namen `bycast.log`. Wenn die neue `bycast.log` 1 GB erreicht, `bycast.log.1` wird sie umbenannt und komprimiert, um `bycast.log.2.gz` zu werden, und `bycast.log` wird umbenannt `bycast.log.1`.

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

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

> Wenn eine Protokolldatei komprimiert wurde, darf sie nicht am selben Speicherort dekomprimiert werden, an dem sie geschrieben wurde. Das Dekomprimieren der Datei am selben Speicherort kann die Protokollrotationsskripte beeinträchtigen.

Optional kann das Ziel der Audit-Logs geändert und Audit-Informationen an einen externen Syslog-Server gesendet werden. Lokale Protokolle der Audit-Einträge werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe "Logverwaltung und externen Syslog-Server konfigurieren".

Verwandte Informationen

"Protokolldateien und Systemdaten sammeln"

Meldungen in bycast.log

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

Beispiel einer ADE-Nachricht:

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

ADE-Meldungen enthalten die folgenden Informationen:

Nachrichtensegment	Wert im Beispiel
Knoten-ID	12455685
ADE-Prozess-ID	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHR
UTC Systemzeit	2019-05-05T27T17:10:29.784677 (YYYY-MM-DDTHH:MM:SS.uuuuuu)
Schweregrad	FEHLER
Interne Nachverfolgungsnummer	0906
Nachricht	SVMR: Die Integritätsprüfung für Volume 3 ist mit dem Grund 'TOUT' fehlgeschlagen.

Schweregrade von Meldungen in bycast.log

Die Meldungen in `bycast.log` sind Schweregraden zugeordnet.

Beispiel:

- **HINWEIS** – Es ist ein Ereignis eingetreten, das protokolliert werden sollte. Die meisten Protokollmeldungen befinden sich auf dieser Ebene.
- **WARNUNG** — Es ist ein unerwarteter Zustand aufgetreten.
- **FEHLER** — Ein schwerwiegender Fehler ist aufgetreten, der die Abläufe beeinträchtigen wird.
- **KRITISCH** – Es ist ein anormaler Zustand eingetreten, der den normalen Betrieb gestoppt hat. Die zugrunde liegende Ursache sollte umgehend behoben werden.

Fehlercodes in `bycast.log`

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

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

Fehlercode	Bedeutung
SUCS	Kein Fehler
GERR	Unbekannt
ABGESAGT	Abgesagt

Fehlercode	Bedeutung
ABRT	Abgebrochen
TOUT	Zeitüberschreitung
INVL	Ungültig
NFND	Nicht gefunden
VERS	Version
CONF	Konfiguration
FEHLER	Fehlgeschlagen
ICPL	Unvollständig
ERLEDIGT	Erledigt
SUNV	Dienst nicht verfügbar

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

Fehlernummer	Fehlercode	Bedeutung
001	EPERM	Betrieb nicht gestattet
002	ENOENT	Keine solche Datei oder Verzeichnis
003	ESRCH	Kein solcher Prozess
004	EINTR	Unterbrochener Systemaufruf
005	EIO	E/A Fehler
006	ENXIO	Kein solches Gerät oder keine solche Adresse
007	E2BIG	Argumentliste zu lang
008	ENOEXEC	Exec-Formatfehler
009	EBADF	Ungültige Dateinummer
010	ECHILD	Keine Kindprozesse

Fehlernummer	Fehlercode	Bedeutung
011	EAGAIN	Erneut versuchen
012	ENOMEM	Speicher erschöpft
013	EACCES	Zugriff verweigert
014	FEHLER	Falsche Adresse
015	ENOTBLK	Blockgerät erforderlich
016	EBUSY	Gerät oder Ressource belegt
017	EEXIST	Datei existiert
018	EXDEV	Geräteübergreifende Verbindung
019	ENODEV	Kein solches Gerät
020	ENOTDIR	Kein Verzeichnis
021	EISDIR	Ist ein Verzeichnis
022	EINVAL	Ungültiges Argument
023	ENFILE	Dateitabellenüberlauf
024	EMFILE	Zu viele geöffnete Dateien
025	ENOTTY	Keine Schreibmaschine
026	ETXTBSY	Textdatei belegt
027	EFBIG	Datei zu groß
028	ENOSPC	Kein Speicherplatz mehr auf dem Gerät
029	ESPIPE	Ungültiger Suchvorgang
030	EROFS	Schreibgeschütztes Dateisystem
031	EMLINK	Zu viele Links
032	EPIPE	Verbindung unterbrochen

Fehlernummer	Fehlercode	Bedeutung
033	EDOM	Mathematisches Argument außerhalb des Definitionsbereichs der Funktion
034	ERANGE	Mathematisches Ergebnis nicht darstellbar
035	EDEADLK	Ein Ressourcen-Deadlock würde auftreten.
036	ENAMETOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperren verfügbar
038	ENOSYS	Funktion nicht implementiert
039	ENOTEMPTY	Verzeichnis nicht leer
040	ELOOP	Zu viele symbolische Verknüpfungen gefunden
041		
042	ENOMSG	Keine Meldung des gewünschten Typs
043	EIDRM	Kennung entfernt
044	ECHRNG	Kanalnummer außerhalb des gültigen Bereichs
045	EL2NSYNC	Level 2 nicht synchronisiert
046	EL3HLT	Stufe 3 gestoppt
047	EL3RST	Level 3 zurücksetzen
048	ELNRNG	Verbindungsnummer außerhalb des zulässigen Bereichs
049	EUNATCH	Protokolltreiber nicht angehängt
050	ENOCSI	Keine CSI Struktur verfügbar
051	EL2HLT	Stufe 2 gestoppt
052	EBADE	Ungültiger Austausch
053	EBADR	Ungültiger Anforderungsdeskriptor

Fehlernummer	Fehlercode	Bedeutung
054	EXFULL	Exchange vollständig
055	ENOANO	Keine Anode
056	EBADRQC	Ungültiger Anforderungscode
057	EBADSLT	Ungültiger Slot
058		
059	EBFONT	Ungültiges Schriftartdateiformat
060	ENOSTR	Gerät ist kein Stream
061	ENODATA	Keine Daten verfügbar
062	ETIME	Zeitüberschreitung
063	ENOSR	Keine Stream-Ressourcen mehr verfügbar
064	ENONET	Die Maschine ist nicht im Netzwerk.
065	ENOPKG	Paket nicht installiert
066	EREMOTE	Objekt ist remote
067	ENOLINK	Die Verbindung wurde getrennt.
068	EADV	Werbefehler
069	ESRMNT	Srmount Fehler
070	ECOMM	Kommunikationsfehler beim Senden
071	EPROTO	Protokollfehler
072	EMULTIHOP	Multihop-Versuch
073	EDOTDOT	RFS spezifischer Fehler
074	EBADMSG	Keine Datenmeldung
075	ÜBERLAUF	Wert zu groß für den definierten Datentyp

Fehlernummer	Fehlercode	Bedeutung
076	ENOTUNIQ	Name nicht eindeutig im Netzwerk
077	EBADFD	Dateideskriptor in fehlerhaftem Zustand
078	EREMCHG	Remote-Adresse geändert
079	ELIBACC	Auf eine benötigte gemeinsam genutzte Bibliothek kann nicht zugegriffen werden
080	ELIBBAD	Zugriff auf eine beschädigte gemeinsam genutzte Bibliothek
081	ELIBSCN	
082	ELIBMAX	Versuch, zu viele gemeinsam genutzte Bibliotheken einzubinden
083	ELIBEXEC	Eine gemeinsam genutzte Bibliothek kann nicht direkt ausgeführt werden.
084	EILSEQ	Ungültige Bytefolge
085	ERESTART	Der unterbrochene Systemaufruf sollte neu gestartet werden
086	ESTRPIPE	Streams Pipe-Fehler
087	EUSERS	Zu viele Nutzer
088	ENOTSOCK	Socket-Operation an Nicht-Socket
089	EDESTADDRREQ	Zieladresse erforderlich
090	EMSGSIZE	Nachricht zu lang
091	EPROTOTYPE	Falscher Protokolltyp für Socket
092	ENOPROTOOPT	Protokoll nicht verfügbar
093	EPROTONOSUPPORT	Protokoll nicht unterstützt
094	ESOCKTNOSUPPORT	Sockeltyp wird nicht unterstützt

Fehlernummer	Fehlercode	Bedeutung
095	EOPNOTSUPP	Vorgang wird auf dem Transportendpunkt nicht unterstützt
096	EPFNOSUPPORT	Protokollfamilie nicht unterstützt
097	EAFNOSUPPORT	Adressfamilie wird vom Protokoll nicht unterstützt
098	EADDRINUSE	Adresse wird bereits verwendet
099	EADDRNOTAVAIL	Angeforderte Adresse kann nicht zugewiesen werden
100	ENETDOWN	Netzwerk ist ausgefallen
101	ENETUNREACH	Netzwerk nicht erreichbar
102	ENETRESET	Netzwerkverbindung aufgrund eines Resets getrennt
103	ECONNABORTED	Die Software hat die Verbindung beendet
104	ECONNRESET	Verbindung vom Gegenüber zurückgesetzt
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Senden nach Abschaltung des Transportendpunkts nicht möglich
109	ETOOMANYREFS	Zu viele Referenzen: kann nicht zusammengefügt werden
110	Zeitüberschreitung	Zeitüberschreitung bei der Verbindung
111	ECONNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHOSTUNREACH	Keine Route zum Host
114	EALREADY	Operation läuft bereits

Fehlernummer	Fehlercode	Bedeutung
115	EINPROGRESS	Vorgang läuft
116		
117	EUCLEAN	Die Struktur muss bereinigt werden.
118	ENOTNAM	Keine XENIX-Datei mit dem Namenstyp
119	ENAVAIL	Keine XENIX Semaphore verfügbar
120	EISNAM	Ist eine benannte Datei
121	EREMOTEIO	Remote I/O-Fehler
122	EDQUOT	Quota überschritten
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ABGESAGT	Vorgang abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEYEXPIRED	Schlüssel ist abgelaufen
128	EKEYREVOKED	Der Schlüssel wurde widerrufen
129	EKEYREJECTED	Der Schlüssel wurde vom Dienst abgelehnt
130	EOWNERDEAD	Für robuste Mutexe: Besitzer ist verstorben
131	ENOTRECOVERABLE	Für robuste Mutexe: Zustand nicht wiederherstellbar

Logverwaltung und externen Syslog-Server konfigurieren

Externe Syslog-Server in StorageGRID

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID, der zur zentralen Erfassung von Revisionsprotokollinformationen verwendet werden kann. Die Nutzung eines externen Syslog-Servers ermöglicht eine Reduzierung des Netzwerkverkehrs auf den Admin-Knoten und eine effizientere Verwaltung der Informationen. Für StorageGRID entspricht das ausgehende Syslog-Nachrichtenpaketformat RFC 3164.

Zu den Arten von Revisionsprotokollinformationen, die an den externen Syslog-Server gesendet werden können, gehören:

- Revisionsprotokolle, die die während des normalen Systembetriebs generierten Audit-Meldungen enthalten
- Sicherheitsrelevante Ereignisse wie Anmeldungen und Eskalationen auf Root
- Anwendungsprotokolle, die möglicherweise angefordert werden, falls es erforderlich ist, einen Support-Fall zu eröffnen, um ein aufgetretenes Problem zu untersuchen

Wann ein externer Syslog Server verwendet wird

Ein externer Syslog-Server ist besonders nützlich, wenn Sie ein großes Grid betreiben, mehrere Arten von S3-Anwendungen verwenden oder alle Revisionsprotokoll-Daten speichern möchten. Das Senden von Revisionsprotokoll-Informationen an einen externen Syslog-Server ermöglicht Folgendes:

- Auditinformationen wie Auditmeldungen, Anwendungsprotokolle und Sicherheitsereignisse effizienter erfassen und verwalten.
- Der Netzwerkverkehr auf den Admin-Knoten wird reduziert, da die Revisionsprotokoll-Informationen direkt von den verschiedenen Storage Nodes an den externen Syslog-Server übertragen werden, ohne einen Admin-Knoten passieren zu müssen.

> Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle, die größer als 8.192 Bytes sind, am Ende der Nachricht abgeschnitten, um den üblichen Beschränkungen in Implementierungen externer Syslog-Server zu entsprechen.

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

Konfiguration eines externen Syslog-Servers

Informationen zur Konfiguration eines externen Syslog-Servers sind unter "Logverwaltung und externen Syslog-Server konfigurieren" zu finden.

Wenn die Konfiguration des TLS- oder RELP/TLS-Protokolls vorgesehen ist, müssen die folgenden Zertifikate vorhanden sein:

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

> 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. Es ergibt sich kein wesentlicher Sicherheitsvorteil durch die Verwendung eines verschlüsselten privaten Schlüssels, da sowohl der Schlüssel als auch die Passphrase gespeichert werden müssen; zur Vereinfachung wird empfohlen, einen unverschlüsselten privaten Schlüssel zu verwenden, sofern verfügbar.

So lässt sich die Größe des externen Syslog-Servers abschätzen

Normalerweise wird Ihr Grid so dimensioniert, dass ein bestimmter Durchsatz erreicht wird, der in S3-Operationen pro Sekunde oder Bytes pro Sekunde angegeben wird. Beispielsweise könnte die Anforderung bestehen, dass Ihr Grid 1.000 S3-Operationen pro Sekunde oder 2.000 MB pro Sekunde an Objekt-Ingestionen und Abrufen verarbeiten kann. Die Dimensionierung Ihres externen Syslog-Servers sollte den Datenanforderungen Ihres Grids entsprechen.

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

S3-Operationen pro Sekunde in Schätzformeln verwenden

Wenn Ihr Grid für einen Durchsatz in Byte pro Sekunde dimensioniert wurde, muss diese Dimensionierung in S3-Operationen pro Sekunde umgerechnet werden, um die Schätzformeln anwenden zu können. Um den Grid-Durchsatz umzurechnen, ist zunächst die durchschnittliche Objektgröße zu bestimmen, was mithilfe der Informationen in vorhandenen Revisionsprotokollen und Metriken (sofern vorhanden) oder auf Grundlage Ihres Wissens über die Anwendungen, die StorageGRID verwenden, erfolgen kann. Beispielsweise: Wenn Ihr Grid für einen Durchsatz von 2.000 MB/Sekunde dimensioniert wurde und die durchschnittliche Objektgröße 2 MB beträgt, wurde Ihr Grid so ausgelegt, dass es 1.000 S3-Operationen pro Sekunde (2.000 MB / 2 MB) verarbeiten kann.

> Die Formeln zur Dimensionierung externer Syslog-Server in den folgenden Abschnitten liefern Schätzwerte für den Normalfall (statt für den Worst-Case). Abhängig von Ihrer Konfiguration und Arbeitslast kann die Anzahl der Syslog-Meldungen oder das Volumen der Syslog-Daten höher oder niedriger ausfallen als von den Formeln vorhergesagt. Die Formeln sind ausschließlich als Richtlinien zu verwenden.

Schätzformeln für Revisionsprotokolle

Wenn Sie keine anderen Informationen über Ihre S3-Workload haben als die Anzahl der S3-Operationen pro Sekunde, die Ihr Grid voraussichtlich unterstützen wird, lässt sich das Volumen der Revisionsprotokolle, die Ihr externer Syslog-Server verarbeiten muss, anhand der folgenden Formeln schätzen, unter der Annahme, dass die Audit Levels auf die Standardwerte belassen werden (alle Kategorien auf Normal eingestellt, außer Storage, das auf Error eingestellt ist):

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

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

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Für Revisionsprotokolle sind die wichtigsten zusätzlichen Variablen der Prozentsatz der S3-Operationen, die PUTs (im Vergleich zu GETS) sind, und die durchschnittliche Größe der folgenden S3-Felder in Byte (die in der Tabelle verwendeten 4-stelligen Abkürzungen sind die Feldnamen des Revisionsprotokolls):

Code	Feld	Beschreibung
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
S3BK	S3 Bucket	Der Name des S3 Buckets.
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.

P steht für den Prozentsatz der S3-Operationen, die PUTs sind, wobei 0 ≤ P ≤ 1 gilt (bei einer 100%igen PUT-Last ist P = 1, bei einer 100%igen GET-Last ist P = 0).

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

Wenn Sie die Werte für P und K bestimmen können, lässt sich mithilfe der folgenden Formeln das Volumen der Revisionsprotokolle abschätzen, die Ihr externer Syslog-Server verarbeiten muss, vorausgesetzt, die Audit Levels bleiben auf den Standardeinstellungen (alle Kategorien auf Normal eingestellt, außer Storage, das auf Error eingestellt ist):

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

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

Schätzformeln für nicht standardmäßige Revisionsprotokollstufen

Die bereitgestellten Formeln für Revisionsprotokolle gehen von den Standard-Einstellungen für die Überwachungsstufe aus (alle Kategorien auf „Normal“ gesetzt, außer Storage, das auf „Fehler“ gesetzt ist). Detaillierte Formeln zur Schätzung der Rate und der durchschnittlichen Größe von Revisionsprotokoll-Meldungen bei nicht standardmäßigen Einstellungen der Überwachungsstufe sind nicht verfügbar. Die folgende Tabelle kann jedoch zur groben Schätzung der Rate verwendet werden; die bereitgestellte Formel für die durchschnittliche Größe von Revisionsprotokollen kann genutzt werden, wobei zu beachten ist, dass dies

wahrscheinlich zu einer Überschätzung führt, da die „zusätzlichen“ Revisionsprotokoll-Meldungen im Durchschnitt kleiner sind als die Standardmeldungen.

Zustand	Formel
Replikation: Alle Revisionsprotokollstufen sind auf Debug oder Normal eingestellt	Revisionsprotokollrate = 8 x S3-Operationsrate
Erasure Coding: Alle Revisionsprotokoll-Stufen sind auf Debug oder Normal eingestellt.	Dieselbe Formel wie für die Standardeinstellungen verwenden

Schätzformeln für Sicherheitsereignisse

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

Schätzformeln für Anwendungsprotokolle

Wenn Sie keine anderen Informationen über Ihre S3-Arbeitslast haben als die Anzahl der S3-Operationen pro Sekunde, die Ihr Grid voraussichtlich unterstützen wird, lässt sich das Volumen der Anwendungsprotokolle, die Ihr externer Syslog-Server verarbeiten muss, mithilfe der folgenden Formeln abschätzen:

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

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

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Für Anwendungsprotokolle sind die wichtigsten zusätzlichen Variablen die Datensicherungsstrategie (Replikation vs. Erasure Coding), der Anteil der S3-Operationen, die PUTs sind (im Vergleich zu GETs/anderen), und die durchschnittliche Größe in Byte der folgenden S3-Felder (die in der Tabelle verwendeten 4-stelligen Abkürzungen sind die Feldnamen des Revisionsprotokolls):

Code	Feld	Beschreibung
SACC	Name des S3-Tenant-Kontos (Absender der Anfrage)	Der Name des Mandantenkontos des Benutzers, der die Anfrage gesendet hat. Bei anonymen Anfragen leer.
SBAC	Name des S3-Tenant-Kontos (Bucket-Inhaber)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von kontoübergreifendem oder anonymem Zugriff verwendet.
S3BK	S3 Bucket	Der Name des S3 Buckets.

Code	Feld	Beschreibung
S3KY	S3 Schlüssel	Der S3-Schlüsselname, ohne den Bucket-Namen. Operationen auf Buckets berücksichtigen dieses Feld nicht.

Beispielhafte Größenabschätzungen

In diesem Abschnitt werden Beispielanwendungen der Schätzformeln für Grids mit den folgenden Methoden des Datenschutzes erläutert:

- Replication
- Erasure Coding

Wenn Sie Replikation zum Datenschutz verwenden

Sei P der Prozentsatz der S3-Operationen, die PUTs sind, wobei 0 ≤ P ≤ 1 (bei einer PUT-Auslastung von 100 % gilt P = 1 und bei einer GET-Auslastung von 100 % gilt P = 0).

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

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

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

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

Wenn Sie Erasure Coding zum Datenschutz verwenden

Sei P der Prozentsatz der S3-Operationen, die PUTs sind, wobei 0 ≤ P ≤ 1 (bei einer PUT-Auslastung von 100 % gilt P = 1 und bei einer GET-Auslastung von 100 % gilt P = 0).

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

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

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

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

Protokollverwaltung in StorageGRID konfigurieren

Bei Bedarf können Revisionsstufen, Protokollheader sowie der Speicherort von Revisionsmeldungen und Revisionsprotokollen konfiguriert werden.

Alle StorageGRID-Knoten generieren Revisionsprotokoll-Meldungen und Protokolle, um Systemaktivitäten und Ereignisse zu verfolgen. Revisionsprotokoll-Meldungen und Protokolle sind unerlässliche Werkzeuge für die Überwachung und Fehlerbehebung.

Optional kann "Konfiguration eines externen Syslog-Servers" verwendet werden, um Revisionsinformationen extern zu speichern. Die Nutzung eines externen Servers minimiert die Auswirkungen der Protokollierung von Revisionsmeldungen, ohne die Vollständigkeit der Revisionsdaten zu verringern. Ein externer Syslog Server ist besonders nützlich bei einem großen Grid, bei der Nutzung mehrerer S3 Anwendungen oder wenn alle Revisionsdaten aufbewahrt werden sollen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "${post_edited_translations.segment}".
- Wenn Sie planen, einen externen Syslog-Server zu konfigurieren, wurden die "Überlegungen zur Verwendung eines externen Syslog Servers" überprüft und befolgt.
- Wenn die Konfiguration eines externen Syslog-Servers mit dem TLS- oder RELP/TLS-Protokoll vorgesehen ist, sind die erforderlichen Server-CA- und Client-Zertifikate sowie der private Client-Schlüssel vorhanden.

Ebenen der Revisionsprotokollmeldungen ändern

Für jede der folgenden Kategorien von Meldungen im Revisionsprotokoll kann ein unterschiedliches Prüfprotokollierungsniveau festgelegt werden:

Prüfkategorie	Standardeinstellung	Weitere Informationen
System	Normal	"System-Revisionsmeldungen"
Storage	Fehler	"Objektspeicher Revisionsprotokollmeldungen"
Management	Normal	"Management-Revisionsprotokollmeldung"

Prüfkategorie	Standardeinstellung	Weitere Informationen
Client-Lesevorgänge	Normal	"Client-Lese-Revisionsprotokollmeldungen"
Client schreibt	Normal	"Client schreibt Revisionsprotokollmeldungen"
ILM	Normal	"ILM-Revisionsprotokollmeldungen"
Gridübergreifende Replikation	Fehler	"${post_edited_translations.segment}"

Während Aktualisierungen werden Revisionsprotokoll-Konfigurationen nicht sofort wirksam.

Schritte

1. **Konfiguration** > **Überwachung** > **Protokollverwaltung** auswählen.
2. Für jede Kategorie von Prüfmeldungen wird eine Prüfstufe aus der Dropdown-Liste ausgewählt:

Audit-Ebene	Beschreibung
Aus	Es werden keine Revisionsprotokollmeldungen aus dieser Kategorie protokolliert.
Fehler	Es werden nur Fehlermeldungen protokolliert, also Revisionsprotokoll-Meldungen, deren Ergebniscode nicht „erfolgreich“ (SUCS) war.
Normal	Standardmäßige Transaktionsmeldungen werden protokolliert, also die in dieser Anleitung für die jeweilige Kategorie aufgeführten Meldungen.
Debug	Veraltet. Diese Stufe verhält sich genauso wie die normale Revisionsprotokoll-Stufe.

Die für eine bestimmte Stufe enthaltenen Meldungen umfassen auch diejenigen, die auf höheren Stufen protokolliert würden. Zum Beispiel enthält die Stufe Normal alle Fehlermeldungen.

Wenn keine detaillierte Aufzeichnung der Client-Lesevorgänge für Ihre S3-Anwendungen erforderlich ist, kann die Einstellung **Client Reads** optional auf **Error** geändert werden, um die Anzahl der im Revisionsprotokoll erfassten Audit-Meldungen zu verringern.

3. **Speichern** auswählen.

HTTP-Anfrageheader festlegen

Optional können Sie beliebige HTTP-Anforderungsheader definieren, die in Audit-Meldungen für Lese- und Schreibvorgänge des Clients aufgenommen werden.

Schritte

1. Im Abschnitt **Revisionsprotokoll-Header** werden die HTTP-Anforderungsheader definiert, die in die Lese- und Schreib-Revisionsprotokollmeldungen des Clients aufgenommen werden sollen.

   Ein Sternchen (*) dient als Platzhalter, um null oder mehr Zeichen abzugleichen. Die Escape-Sequenz (*) dient dazu, ein tatsächliches Sternchen abzugleichen.

2. **Weitere Überschrift hinzufügen** kann ausgewählt werden, um bei Bedarf zusätzliche Überschriften zu erstellen.

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

   > Die Header der Revisionsprotokoll-Anforderungen werden nur protokolliert, wenn die Audit-Stufe für **Client Reads** oder **Client Writes** nicht auf **Aus** steht.

3. **Speichern** auswählen

Protokollspeicherort konfigurieren

Standardmäßig werden Revisionsprotokoll-Meldungen und Protokolle auf den Knoten gespeichert, auf denen sie generiert werden. Sie werden regelmäßig rotiert und schließlich gelöscht, um zu verhindern, dass sie übermäßigen Speicherplatz belegen. Wenn Revisionsprotokoll-Meldungen und eine Teilmenge der Protokolle extern gespeichert werden sollen, einen externen Syslog Server verwenden.

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

Einen externen Syslog-Server verwenden

Optional kann ein externer Syslog-Server konfiguriert werden, um Revisionsprotokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Ort außerhalb Ihres Grids zu speichern.

> Wenn kein externer Syslog-Server verwendet werden soll, diesen Schritt überspringen und zu Protokollspeicherort auswählen gehen.

> Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können zusätzliche Konfigurationsoptionen mithilfe der `audit-destinations` Endpunkte angewendet werden, die sich im privaten API-Bereich der "Grid Management API" befinden. Beispielsweise kann die API verwendet werden, wenn für verschiedene Knotengruppen unterschiedliche Syslog-Server genutzt werden sollen.

Syslog-Informationen eingeben

Im Assistenten „Externen Syslog-Server konfigurieren“ werden die Informationen bereitgestellt, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. Auf der Registerkarte „Lokaler Knoten und externer Server“ die Option **Externen Syslog-Server konfigurieren** auswählen. Oder, falls zuvor bereits ein externer Syslog-Server konfiguriert wurde, die Option **Externen Syslog-Server bearbeiten** auswählen.

   Der Assistent zum Konfigurieren des externen Syslog-Servers wird angezeigt.

2. Für den Schritt **Syslog-Informationen eingeben** des Assistenten ist im Feld **Host** eine gültige vollqualifizierte Domain oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server einzugeben.
3. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine ganze Zahl zwischen 1 und 65535 sein). Der Standardport ist 514.
4. Das Protokoll, das zum Senden von Revisionsprotokollinformationen an den externen Syslog-Server verwendet wird, auswählen.

   Die Verwendung von **TLS** oder **RELP/TLS** wird empfohlen. Zum Verwenden einer dieser Optionen muss ein Serverzertifikat hochgeladen werden. Die Verwendung von Zertifikaten trägt zur Absicherung der Verbindungen zwischen Ihrem Grid und dem externen Syslog-Server bei. Weitere Informationen finden sich unter "Sicherheitszertifikate verwalten".

   Alle Protokolloptionen erfordern die Unterstützung und Konfiguration durch den externen Syslog-Server. Es ist eine Option auszuwählen, die mit dem externen Syslog-Server kompatibel ist.

   > Das Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls und gewährleistet die zuverlässige Zustellung von Ereignismeldungen. Durch den Einsatz von RELP kann der Verlust von Revisionsprotokollinformationen verhindert werden, falls Ihr externer Syslog-Server neu gestartet werden muss.

5. Wählen Sie **Weiter**.
6. Wenn **TLS** oder **RELP/TLS** ausgewählt wurde, sind die Server-CA-Zertifikate, das Client-Zertifikat und der private Client-Schlüssel hochzuladen.
   a. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel aus, den Sie verwenden möchten.
   b. Wählen Sie die Zertifikats- oder Schlüsseldatei aus.
   c. **Öffnen** auswählen, um die Datei hochzuladen.

      Neben dem Namen der Zertifikats- oder Schlüsseldatei erscheint ein grünes Häkchen, das anzeigt, dass die Datei erfolgreich hochgeladen wurde.
7. Wählen Sie **Weiter**.

Syslog-Inhalte verwalten

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

Schritte

1. Für den Schritt **Syslog-Inhalte verwalten** des Assistenten wird jede Art von Revisionsinformationen ausgewählt, die an den externen Syslog-Server gesendet werden soll.
   - **Revisionsprotokolle senden**: Sendet StorageGRID Ereignisse und Systemaktivitäten
   - **Sicherheitsereignisse senden**: Sendet Sicherheitsereignisse, wie wenn ein nicht autorisierter Benutzer versucht, sich anzumelden, oder ein Benutzer sich als Root anmeldet
   - **Anwendungsprotokolle senden**: Sendet "Protokolldateien der StorageGRID Software" nützliche Informationen zur Fehlerbehebung, einschließlich:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`

    - `nms.log` (nur für Administratorknoten)
    - `prometheus.log`
    - `raft.log`
    - `hagroups.log`
  - **Zugriffsprotokolle senden**: Sendet HTTP-Zugriffsprotokolle für externe Anfragen an Grid Manager, Tenant Manager, konfigurierte Load Balancer-Endpunkte und Grid Federation-Anfragen von Remote-Systemen.
2. Mit den Dropdown-Menüs lassen sich der Schweregrad und die Einrichtung (Nachrichtentyp) für jede Kategorie von Revisionsprotokoll-Informationen auswählen, die Sie senden möchten.

   Die Festlegung von Schweregrad- und Anlagenwerten kann dabei helfen, die Protokolle auf anpassbare Weise zu aggregieren und so die Analyse zu erleichtern.

   a. Für **Schweregrad** entweder **Durchleitung** auswählen oder einen Schweregradwert zwischen 0 und 7 festlegen.

      Wenn Sie einen Wert auswählen, wird dieser auf alle Nachrichten dieses Typs angewendet. Informationen zu unterschiedlichen Schweregraden gehen verloren, wenn Sie Schweregrad durch einen festen Wert überschreiben.

Schwere	Beschreibung
Durchleitung	Jede an das externe Syslog gesendete Nachricht weist denselben Schweregrad auf wie bei der lokalen Protokollierung auf dem Knoten: • Für Revisionsprotokolle ist der Schweregrad "info". • Für Sicherheitsereignisse werden die Schweregrade von der Linux-Distribution auf den Knoten generiert. • Für Anwendungsprotokolle variieren die Schweregrade je nach Problem zwischen „info“ und „notice“. Beispielsweise ergibt das Hinzufügen eines NTP-Servers und das Konfigurieren einer HA-Gruppe den Wert „info“, während das absichtliche Stoppen des SSM- oder RSM-Dienstes den Wert „notice“ ergibt. • Für Zugriffsprotokolle ist der Schweregrad "info".
0	Notfall: System ist nicht verwendbar
1	Warnung: Sofortiges Handeln erforderlich
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber bedeutsamer Zustand

Schwere	Beschreibung
6	Informational: Informationsmeldungen
7	Debug: Meldungen auf Debug-Ebene

b. Für **Anlage** ist entweder **Durchleitung** auszuwählen oder ein Anlagenwert zwischen 0 und 23.

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

Einrichtung	Beschreibung

Durchleitung	Jede an das externe Syslog gesendete Nachricht hat denselben Facility-Wert wie bei der lokalen Protokollierung auf dem Knoten:
	• Für Revisionsprotokolle wird die Facility "local7" an den externen Syslog-Server gesendet.
	• Für Sicherheitsereignisse werden die Facility-Werte von der Linux-Distribution auf den Knoten generiert.
	• Für Anwendungsprotokolle haben die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Facility-Werte:
	  ◦ `bycast.log`: Benutzer oder Daemon
	  ◦ `bycast-err.log`: Benutzer, Daemon, local3 oder local4
	  ◦ `jaeger.log`: local2
	  ◦ `nms.log`: local3
	  ◦ `prometheus.log`: local4
	  ◦ `raft.log`: local5
	  ◦ `hagroups.log`: local6
	• Für Zugriffsprotokolle wird die Facility "local0" an den externen Syslog-Server gesendet.

0	kern (Kernelmeldungen)
1	Benutzer (Meldungen auf Benutzerebene)
2	E-Mail
3	Daemon (Systemdaemons)
4	auth (Sicherheits-/Autorisierungsmeldungen)
5	syslog (Meldungen, die intern von syslogd generiert werden)

Einrichtung	Beschreibung
6	lpr (Zeilendrucker Subsystem)
7	Nachrichten (Netzwerknachrichten Subsystem)
8	UUCP
9	cron (Uhr-Daemon)
10	Sicherheit (Sicherheits-/Autorisierungsmeldungen)
11	FTP
12	NTP
13	logaudit (Revisionsprotokoll)
14	logalert (Protokollwarnung)
15	Uhr (Uhr-Daemon)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Wählen Sie **Weiter**.

Testnachrichten senden

Bevor Sie einen externen Syslog-Server verwenden, sollte veranlasst werden, dass alle Knoten in Ihrem Grid Testnachrichten an den externen Syslog-Server senden. Diese Testnachrichten dienen dazu, die gesamte Infrastruktur zur Protokollerfassung zu validieren, bevor die Übertragung von Daten an den externen Syslog-Server erfolgt.

> Die Konfiguration des externen Syslog Servers sollte erst verwendet werden, nachdem bestätigt wurde, dass der externe Syslog Server von jedem Knoten in Ihrem Grid eine Testnachricht erhalten hat und dass die Nachricht wie erwartet verarbeitet wurde.

Schritte

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

   Ein grünes Banner signalisiert, dass die Konfiguration gespeichert wurde.

2. Andernfalls **Testnachrichten senden** auswählen (empfohlen).

   Testergebnisse werden fortlaufend auf der Seite angezeigt, bis der Test beendet wird. Während der Test läuft, werden Ihre Revisionsprotokollmeldungen weiterhin an die zuvor konfigurierten Ziele gesendet.

3. Wenn während der Konfiguration des Syslog-Servers oder zur Laufzeit Fehler auftreten, sollten diese behoben werden und **Testnachrichten senden** erneut ausgewählt werden.

   Siehe "Fehlerbehebung bei einem externen Syslog Server" zur Unterstützung bei der Behebung etwaiger Fehler.

4. Warten Sie, bis ein grünes Banner angezeigt wird, das bestätigt, dass alle Knoten die Tests bestanden haben.
5. Prüfen Sie auf Ihrem Syslog-Server, ob Testnachrichten wie erwartet empfangen und verarbeitet werden.

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

6. **Stoppen und beenden** auswählen.

   Sie werden zurück zur Seite **Audit und syslog server** geleitet. Ein grünes Banner zeigt an, dass die syslog server-Konfiguration gespeichert wurde.

   > StorageGRID Revisionsprotokollinformationen werden erst an den externen Syslog-Server gesendet, wenn ein Ziel ausgewählt wird, das den externen Syslog-Server enthält.

Protokollspeicherort auswählen

Sie können festlegen, wohin Revisionsprotokolle, Sicherheitsereignisprotokolle, "StorageGRID Anwendungsprotokolle" und Zugriffsprotokolle gesendet werden.

StorageGRID verwendet standardmäßig lokale Knoten als Revisionsprotokollziele und speichert die Revisionsprotokollinformationen in `/var/local/log/localaudit.log`.

Bei Verwendung von `/var/local/log/localaudit.log`Grid Manager und Tenant Manager Revisionsprotokoll werden die Revisionsprotokoll-Einträge möglicherweise an einen Storage Node gesendet. Es lässt sich mit dem `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`Befehl feststellen, welcher Node die aktuellsten Einträge enthält.

Einige Ziele sind nur verfügbar, wenn ein externer Syslog-Server konfiguriert wurde.

Schritte

1. Wählen Sie **Protokollspeicherort** > **Lokaler Knoten und externer Server**.
2. Zum Ändern des Speicherorts für die Protokolltypen kann eine andere Option ausgewählt werden.

Nur lokale Knoten und **Externer Syslog-Server** bieten in der Regel bessere Leistung.

Option	Beschreibung
Nur lokale Knoten (Standard)	Audit-Meldungen, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden nicht an Admin-Nodes gesendet. Stattdessen werden sie nur auf den Knoten gespeichert, die sie generiert haben („dem lokalen Knoten“). Die auf jedem lokalen Knoten generierten Audit-Informationen werden in `/var/local/log/localaudit.log` gespeichert. **Hinweis**: StorageGRID entfernt lokale Protokolle regelmäßig in einer Rotation, um Speicherplatz freizugeben. Wenn die Protokolldatei eines Knotens 1 GB erreicht, wird die bestehende Datei gespeichert und eine neue Protokolldatei gestartet. Das Rotationslimit für das Protokoll beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Im Durchschnitt werden auf jedem Knoten etwa 20 GB Protokolldaten gespeichert. Um Protokolle über einen längeren Zeitraum zu speichern, Ein Mandant und ein Bucket für die Protokollspeicherung verwenden.
Admin Nodes/lokale Knoten	Audit-Meldungen werden an das Revisionsprotokoll auf den Admin Nodes gesendet, und Sicherheitsereignisprotokolle sowie Anwendungsprotokolle werden auf den Nodes gespeichert, die sie generiert haben. Die Audit-Informationen werden in den folgenden Dateien gespeichert: • Admin Nodes (primäre und nicht-primäre): `/var/local/audit/export/audit.log` • Alle Knoten: Die `/var/local/log/localaudit.log` Datei ist in der Regel leer oder fehlt. Sie kann sekundäre Informationen enthalten, wie eine zusätzliche Kopie einiger Nachrichten.

Option	Beschreibung
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 der externe Syslog-Server konfiguriert wurde. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog Server konfiguriert.
Admin Nodes und externer Syslog-Server	Audit-Meldungen werden an das Revisionsprotokoll (`/var/local/audit/export/audit.log`) auf den Admin-Knoten gesendet, 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 der externe Syslog-Server konfiguriert wurde. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog Server konfiguriert haben.

3. **Speichern** auswählen.

   Es erscheint eine Warnmeldung.

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

   Neue Protokolldateien werden an die von Ihnen ausgewählten Ziele gesendet. Vorhandene Protokolldateien bleiben an ihrem aktuellen Speicherort.

Einen Bucket verwenden

Protokolldateien werden regelmäßig rotiert. Ein S3-Bucket im selben Grid dient zur Speicherung von Protokolldateien über einen längeren Zeitraum.

1. Wählen Sie **Protokollspeicherort** > **Bucket verwenden**.
2. Das Kontrollkästchen **Archivprotokolle aktivieren** auswählen.
3. Falls der angezeigte Mandant und Bucket nicht die gewünschten sind, **Mandant und Bucket ändern** auswählen und anschließend entweder **Mandant und Bucket erstellen** oder **Mandant und Bucket auswählen** wählen.

Mandant und Bucket erstellen

a. Einen neuen Mieternamen eingeben.
b. Ein Passwort für den neuen Mandanten eingeben und bestätigen.
c. Geben Sie einen neuen Bucket Namen ein.
d. **Erstellen und aktivieren** auswählen.

Mandant und Bucket auswählen

a. Einen Mandantennamen aus der Auswahlliste auswählen.
b. Einen Bucket aus dem Dropdown-Menü auswählen.
c. **Auswählen und aktivieren** auswählen.

4. **Speichern** auswählen.

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

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

   Beispiel:

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

SNMP Überwachung

Verwenden Sie die SNMP-Überwachung in StorageGRID

Wenn StorageGRID mithilfe des Simple Network Management Protocol (SNMP) überwacht werden soll, ist die Konfiguration des mit StorageGRID enthaltenen SNMP-Agenten erforderlich.

- "Den SNMP-Agenten konfigurieren"
- "Den SNMP-Agent aktualisieren"

Fähigkeiten

Jeder StorageGRID Knoten führt einen SNMP-Agenten (Daemon) aus, der eine MIB bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Warnmeldungen. Die MIB enthält außerdem Systembeschreibungsinformationen wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID Knoten unterstützt zudem eine Teilmenge der MIB-II-Objekte.

> Siehe "Zugriff auf MIB-Dateien", falls Sie die MIB-Dateien auf Ihren Grid-Knoten herunterladen möchten.

SNMP ist anfänglich auf allen Knoten deaktiviert. Bei der Konfiguration des SNMP-Agenten erhalten alle StorageGRID-Knoten dieselbe Konfiguration.

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP Protokolls. Es steht schreibgeschützter MIB Zugriff für Abfragen zur Verfügung, und es können zwei Arten von ereignisgesteuerten Benachrichtigungen an ein Managementsystem gesendet werden:

Fallen

Traps sind Benachrichtigungen, die vom SNMP-Agenten gesendet werden und keine Bestätigung durch das Managementsystem erfordern. Traps dienen dazu, das Managementsystem darüber zu informieren, dass innerhalb von StorageGRID etwas passiert ist, wie zum Beispiel das Auslösen einer Warnmeldung.

Traps werden in allen drei Versionen von SNMP unterstützt.

Informiert

Informs ähneln Traps, erfordern jedoch eine Bestätigung durch das Managementsystem. Erhält der SNMP-Agent innerhalb einer bestimmten Zeit keine Bestätigung, sendet er die Inform so lange erneut, bis eine Bestätigung eingeht oder der maximale Wiederholungswert erreicht ist.

Informs werden in SNMPv2c und SNMPv3 unterstützt.

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

- Eine Standard- oder benutzerdefinierte Warnung wird bei jedem Schweregrad ausgelöst. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, muss "eine Stille konfigurieren" für die Warnung vorgenommen werden. Warnungsbenachrichtigungen werden vom "bevorzugter Absender Admin Node" gesendet.

  Jede Warnung wird basierend auf dem Schweregrad einer von drei Trap-Typen zugeordnet: activeMinorAlert, activeMajorAlert und activeCriticalAlert. Eine Liste der Warnungen, die diese Traps auslösen können, ist unter "Benachrichtigungsreferenz" zu finden.

SNMP-Version Unterstützung

Die Tabelle bietet eine Übersicht auf hoher Ebene darüber, was für jede SNMP-Version unterstützt wird.

	SNMPv1	**SNMPv2c**	**SNMPv3**
Anfragen (GET und GETNEXT)	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-String	Community-String	Benutzerbasiertes Sicherheitsmodell (USM) Benutzer
Benachrichtigungen (TRAP und INFORM)	Nur Traps	Traps und informiert	Traps und informiert

	SNMPv1	SNMPv2c	SNMPv3
Benachrichtigungs-Authentifizierung	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 den schreibgeschützten Zugriff auf MIBs. Schreibzugriff wird nicht unterstützt.
- Alle Knoten im Grid erhalten die gleiche Konfiguration.
- SNMPv3: StorageGRID unterstützt den Transport Support Mode (TSM) nicht.
- SNMPv3: Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).
- SNMPv3: Das einzige unterstützte Datenschutzprotokoll ist AES.

Konfigurieren Sie den SNMP-Agent in StorageGRID

Sie können den StorageGRID SNMP-Agenten so konfigurieren, dass ein SNMP-Managementsystem eines Drittanbieters für den Lesezugriff auf MIBs und Benachrichtigungen verwendet wird.

Bevor Sie beginnen

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

Über diese Aufgabe

Der StorageGRID SNMP-Agent unterstützt SNMPv1, SNMPv2c und SNMPv3. Der Agent kann für eine oder mehrere Versionen konfiguriert werden. Für SNMPv3 wird ausschließlich die User Security Model (USM) Authentifizierung unterstützt.

Alle Knoten im Grid verwenden die gleiche SNMP Konfiguration.

Grundlegende Konfiguration angeben

Im ersten Schritt wird der StorageGRID SMNP-Agent aktiviert und grundlegende Informationen bereitgestellt.

Schritte

1. **Konfiguration** > **Überwachung** > **SNMP agent** auswählen.

   Die SNMP-Agentenseite wird angezeigt.

2. Um den SNMP-Agenten auf allen Grid-Knoten zu aktivieren, das Kontrollkästchen **SNMP aktivieren** auswählen.
3. Folgende Informationen sind im Abschnitt „Grundkonfiguration“ anzugeben.

Feld	Beschreibung
Systemkontakt	Optional. Der primäre Ansprechpartner für das StorageGRID System, der in SNMP-Meldungen als sysContact zurückgegeben wird. Der Systemkontakt ist üblicherweise eine E-Mail-Adresse. Dieser Wert gilt für alle Knoten im StorageGRID System. **Systemkontakt** darf maximal 255 Zeichen lang sein.
Systemstandort	Optional. Der Standort des StorageGRID Systems, der in SNMP-Meldungen als sysLocation zurückgegeben wird. Der Systemstandort kann jede Information enthalten, die zur Identifizierung des Standorts Ihres StorageGRID Systems geeignet ist. Beispielsweise kann die Straßenadresse einer Einrichtung verwendet werden. Dieser Wert gilt für alle Knoten im StorageGRID System. **Systemstandort** darf maximal 255 Zeichen umfassen.
SNMP Agent-Benachrichtigungen aktivieren	• Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Trap- und Inform-Benachrichtigungen. • Wird diese Option nicht ausgewählt, unterstützt der SNMP-Agent den Lesezugriff auf die MIB, sendet aber keine SNMP-Benachrichtigungen.
Authentifizierungsfallen aktivieren	Wenn diese Option ausgewählt ist, sendet der StorageGRID SNMP-Agent Authentifizierungs-Traps, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.

Community-Strings eingeben

Wenn Sie SNMPv1 oder SNMPv2c verwenden, ist der Abschnitt „Community-Zeichenfolgen“ auszufüllen.

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

Schritte

1. Für **schreibgeschützte Community** kann optional eine Community-Zeichenfolge eingegeben werden, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agentadressen zu erlauben.

   > Um die Sicherheit Ihres StorageGRID Systems zu gewährleisten, sollte „public“ nicht als Community-Zeichenfolge verwendet werden. Wenn dieses Feld leer bleibt, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID Systems als Community-Zeichenfolge.

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

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

   Bis zu fünf Zeichenfolgen sind zulässig.

Fallenziele erstellen

Im Abschnitt „Weitere Konfigurationen“ auf der Registerkarte „Trap-Ziele“ lassen sich ein oder mehrere Ziele für StorageGRID Trap- oder Inform-Benachrichtigungen definieren. Nach Aktivierung des SNMP-Agenten und Auswahl von **Speichern** sendet StorageGRID bei ausgelösten Warnmeldungen Benachrichtigungen an jedes definierte Ziel. Standardbenachrichtigungen werden ebenfalls für die unterstützten MIB-II-Entitäten (zum Beispiel ifDown und coldStart) gesendet.

Schritte

1. Im Feld **Standard-Trap-Community** kann optional die Standard-Community-Zeichenfolge eingegeben werden, die für SNMPv1- oder SNMPv2-Trap-Ziele verwendet werden soll.

   Bei Bedarf kann beim Definieren eines bestimmten Trap-Ziels eine andere ("benutzerdefinierte") Community-Zeichenfolge angegeben werden.

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

2. Zum Hinzufügen eines Trap-Ziels **Erstellen** auswählen.
3. Wählen Sie aus, welche SNMP-Version für dieses Trap-Ziel verwendet wird.
4. Das Formular „Trap-Ziel erstellen“ für die ausgewählte Version ausfüllen.

SNMPv1

Wenn SNMPv1 als Version ausgewählt wurde, sind diese Felder auszufüllen.

Feld	Beschreibung
Typ	Muss ein Trap für SNMPv1 sein.
Host	Eine IPv4- oder IPv6-Adresse oder ein vollqualifizierter Domänenname (FQDN) zum Empfangen der Trap.
Port	Port 162, der Standardport für SNMP-Traps, wird verwendet, sofern nicht ein anderer Wert erforderlich ist.
Protokoll	UDP ist das Standard-SNMP-Trap-Protokoll, sofern nicht TCP verwendet werden muss.
Community-String	Die standardmäßige Trap-Community kann verwendet werden, falls eine angegeben wurde, oder eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel kann eingegeben werden. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

SNMPv2c

Wenn SNMPv2c als Version ausgewählt wurde, sind diese Felder auszufüllen.

Feld	Beschreibung
Typ	Ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfang der Trap.
Port	Port 162 ist der Standardport für SNMP-Traps, sofern nicht ein anderer Wert erforderlich ist.
Protokoll	UDP ist das Standard-SNMP-Trap-Protokoll, sofern nicht TCP verwendet werden muss.
Community-String	Die standardmäßige Trap-Community kann verwendet werden, falls eine angegeben wurde, oder eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel kann eingegeben werden. Die benutzerdefinierte Community-Zeichenfolge darf maximal 32 Zeichen lang sein und keine Leerzeichen enthalten.

SNMPv3

Wenn SNMPv3 als Version ausgewählt wurde, sind diese Felder auszufüllen.

Feld	Beschreibung
Typ	Ob das Ziel für Traps oder Informs verwendet wird.
Host	Eine IPv4- oder IPv6-Adresse oder ein FQDN zum Empfang der Trap.
Port	Port 162 ist der Standardport für SNMP-Traps, sofern nicht ein anderer Wert erforderlich ist.
Protokoll	UDP ist das Standard-SNMP-Trap-Protokoll, sofern nicht TCP verwendet werden muss.
USM-Benutzer	Der USM-Benutzer, der für die Authentifizierung verwendet wird. • Wenn **Trap** ausgewählt wurde, werden nur USM-Benutzer ohne autoritative Engine-IDs angezeigt. • Wenn **Inform** ausgewählt wurde, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt. • Wenn keine Benutzer angezeigt werden: i. Das Fallenziel wird erstellt und gespeichert. ii. Wechseln Sie zu USM-Benutzer anlegen und erstellen Sie den Benutzer. iii. Zurück zur Registerkarte „Fallenziele“, das gespeicherte Ziel in der Tabelle auswählen und **Bearbeiten** wählen. iv. Den Benutzer auswählen.

5. Wählen Sie **Create**.

   Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

Agentenadressen erstellen

Optional kann auf der Registerkarte „Agentadressen“ im Abschnitt „Weitere Konfigurationen“ eine oder mehrere „Listening-Adressen“ angegeben werden. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Abfragen empfangen kann.

Wenn keine Agentenadresse konfiguriert wird, ist die Standard-Listening-Adresse UDP-Port 161 auf allen StorageGRID Netzwerken.

Schritte

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

Feld	Beschreibung
Internetprotokoll	Ob diese Adresse IPv4 oder IPv6 verwendet. Standardmäßig verwendet SNMP IPv4.
Transportprotokoll	Ob diese Adresse UDP oder TCP verwendet. Standardmäßig verwendet SNMP UDP.
StorageGRID Netzwerk	Auf welchem StorageGRID Netzwerk der Agent lauschen wird. • Grid, Admin und Client Netzwerke: Der SNMP-Agent nimmt Anfragen auf allen drei Netzwerken entgegen. • Grid-Netzwerk • ${post_edited_translations.segment} • Client-Netzwerk **Hinweis**: Wenn das Client-Netzwerk für unsichere Daten verwendet wird und eine Agentenadresse für das Client-Netzwerk erstellt wird, ist zu beachten, dass auch der SNMP-Datenverkehr unsicher ist.
Port	Optional kann die Portnummer angegeben werden, auf der der SNMP-Agent lauschen soll. Der Standard-UDP-Port für einen SNMP-Agent ist 161, aber es kann jede ungenutzte Portnummer eingegeben werden. **Hinweis**: Beim Speichern des SNMP-Agenten öffnet StorageGRID automatisch die Agentenadressen-Ports in der internen Firewall. Es ist sicherzustellen, dass externe Firewalls den Zugriff auf diese Ports zulassen.

3. Wählen Sie **Create**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

USM-Benutzer erstellen

Wenn Sie SNMPv3 verwenden, kann auf der Registerkarte „USM-Benutzer“ im Abschnitt „Weitere Konfigurationen“ festgelegt werden, welche USM-Benutzer berechtigt sind, die MIB abzufragen oder Traps und Informs zu empfangen.

> Für SNMPv3-*Trap*-Ziele wird empfohlen, für jeden Admin Node einen USM-Benutzer zu erstellen. Wenn nicht jeder Admin Node über einen USM-Benutzer verfügt, empfängt Ihr Managementsystem unter Umständen keine Benachrichtigungen mehr, wenn der primäre Admin Node ausfällt.

SNMPv3 *inform* Ziele müssen Benutzer mit Engine-IDs haben. SNMPv3 *trap* Ziele dürfen keine Benutzer mit Engine-IDs haben.

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

Schritte

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

Feld	Beschreibung
Benutzername	Ein einzigartiger Name für diesen USM Benutzer. Benutzernamen dürfen maximal 32 Zeichen lang sein und keine Leerzeichen enthalten. Der Benutzername kann nach der Erstellung des Benutzers nicht mehr geändert werden.
MIB-Zugriff mit Leseberechtigung	Wenn diese Option ausgewählt ist, sollte dieser Benutzer nur Lesezugriff auf die MIB haben.
Autoritative Engine-ID	Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, die autoritative Engine-ID für diesen Benutzer. Geben Sie 10 bis 64 Hexadezimalzeichen (5 bis 32 Byte) ohne Leerzeichen ein. Dieser Wert ist für USM-Benutzer erforderlich, die in den Trap-Zielen für Informs ausgewählt werden. Dieser Wert ist für USM-Benutzer, die in den Trap-Zielen für Traps ausgewählt werden, nicht zulässig. **Hinweis**: Dieses Feld wird nicht angezeigt, wenn Sie **Nur-Lesezugriff auf die MIB** ausgewählt haben, da USM-Benutzer mit Nur-Lesezugriff auf die MIB keine Engine-IDs haben können.
Sicherheitsstufe	Das Sicherheitsniveau für den USM-Benutzer: • **authPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Es muss ein Authentifizierungsprotokoll und ein Passwort sowie ein Datenschutzprotokoll und ein Passwort angegeben werden. • **authNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Es ist erforderlich, ein Authentifizierungsprotokoll und ein Passwort anzugeben.
Authentifizierungsprotokoll	Immer auf SHA eingestellt, da dies das einzige unterstützte Protokoll ist (HMAC-SHA-96).
Passwort	Das Passwort, das dieser Benutzer für die Authentifizierung verwendet.

Feld	Beschreibung
Datenschutzprotokoll	Wird nur angezeigt, wenn **authPriv** ausgewählt wurde und immer auf AES gesetzt ist, da dies das einzige unterstützte Datenschutzprotokoll ist.
Passwort	Wird nur angezeigt, wenn **authPriv** ausgewählt wurde. Das Passwort, das dieser Benutzer für die Privatsphäre verwendet.

3. Wählen Sie **Create**.

   Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

4. Nach Abschluss der SNMP-Agentenkonfiguration **Speichern** auswählen.

   Die neue SNMP-Agentenkonfiguration wird aktiv.

Aktualisieren Sie den StorageGRID SNMP-Agenten

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

Bevor Sie beginnen

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

Über diese Aufgabe

Details zu den einzelnen Feldern auf der SNMP-Agenten-Seite sind unter "Den SNMP-Agenten konfigurieren" zu finden. **Speichern** am unteren Rand der Seite muss ausgewählt werden, damit Änderungen auf den einzelnen Registerkarten übernommen werden.

Schritte

1. **Konfiguration** > **Überwachung** > **SNMP agent** auswählen.

   Die SNMP-Agentenseite wird angezeigt.

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

   Wenn der SNMP-Agent erneut aktiviert wird, bleiben alle vorherigen SNMP-Konfigurationseinstellungen erhalten.

3. Optional lassen sich die Informationen im Abschnitt „Grundkonfiguration“ aktualisieren:
   a. Bei Bedarf können der **Systemkontakt** und der **Systemstandort** aktualisiert werden.
   b. Optional kann das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren** ausgewählt oder deaktiviert werden, um zu steuern, ob der StorageGRID SNMP-Agent Trap- und Inform-Benachrichtigungen sendet.

      Wenn dieses Kontrollkästchen deaktiviert ist, unterstützt der SNMP-Agent den Lesezugriff auf die MIB,

sendet aber keine SNMP-Benachrichtigungen.

c. Optional kann das Kontrollkästchen **Authentifizierungs-Traps aktivieren** ausgewählt oder deaktiviert werden, um zu steuern, ob der StorageGRID SNMP-Agent Authentifizierungs-Traps sendet, wenn er nicht ordnungsgemäß authentifizierte Protokollnachrichten empfängt.

4. Wenn SNMPv1 oder SNMPv2c verwendet wird, kann optional eine **Read-only community** im Abschnitt Community-Strings aktualisiert oder hinzugefügt werden.
5. Zum Aktualisieren der Trap-Ziele die Registerkarte Trap-Ziele im Abschnitt Weitere Konfigurationen auswählen.

   Über diese Registerkarte können ein oder mehrere Ziele für StorageGRID Trap- oder Inform-Benachrichtigungen definiert werden. Wenn der SNMP-Agent aktiviert und **Speichern** ausgewählt wird, sendet StorageGRID Benachrichtigungen an jedes definierte Ziel, sobald Warnmeldungen ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten (z. B. ifDown und coldStart) gesendet.

   Weitere Informationen zu den einzugebenden Angaben finden Sie unter "Trap-Ziele erstellen".

   - Optional kann die Standard-Trap-Community aktualisiert oder entfernt werden.

     Wenn Sie die Standard-Trap-Community entfernen, muss zuerst sichergestellt werden, dass alle vorhandenen Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

   - Zum Hinzufügen eines Trap-Ziels **Erstellen** auswählen.
   - Um ein Trap-Ziel zu bearbeiten, das Optionsfeld auswählen und **Bearbeiten** wählen.
   - Um ein Trap-Ziel zu entfernen, das Optionsfeld auswählen und **Entfernen** wählen.
   - Um Änderungen zu übernehmen, unten auf der Seite **Speichern** auswählen.
6. Zum Aktualisieren der Agentenadressen die Registerkarte Agentenadressen im Abschnitt Weitere Konfigurationen auswählen.

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

   Weitere Informationen zu den einzugebenden Angaben finden Sie unter "Agentenadressen erstellen".

   - Zum Hinzufügen einer Agentenadresse **Erstellen** auswählen.
   - Um eine Agentenadresse zu bearbeiten, das Optionsfeld auswählen und **Bearbeiten** wählen.
   - Zum Entfernen einer Agentenadresse das Optionsfeld auswählen und **Entfernen** wählen.
   - Um Änderungen zu übernehmen, unten auf der Seite **Speichern** auswählen.
7. Zum Aktualisieren der USM Benutzer die Registerkarte USM Benutzer im Abschnitt Andere Konfigurationen auswählen.

   Mit dieser Registerkarte werden die USM-Benutzer festgelegt, die berechtigt sind, die MIB abzufragen oder Traps und Informs zu empfangen.

   Weitere Informationen zu den einzugebenden Angaben finden Sie unter "USM-Benutzer anlegen".

   - Zum Hinzufügen eines USM-Benutzers **Erstellen** auswählen.
   - Zum Bearbeiten eines USM-Benutzers das Optionsfeld auswählen und **Bearbeiten** wählen.

Der Benutzername eines bestehenden USM-Benutzers kann nicht geändert werden. Um einen Benutzernamen zu ändern, ist es erforderlich, den Benutzer zu entfernen und einen neuen zu erstellen.

> Wenn Sie die autoritative Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer aktuell für ein Ziel ausgewählt ist, muss das Ziel bearbeitet oder entfernt werden. Andernfalls tritt beim Speichern der SNMP Agent-Konfiguration ein Validierungsfehler auf.

- Zum Entfernen eines USM-Benutzers das Optionsfeld auswählen und **Entfernen** wählen.

  > Wenn der entfernte Benutzer aktuell als Trap-Ziel ausgewählt ist, muss das Ziel bearbeitet oder entfernt werden. Andernfalls tritt beim Speichern der SNMP Agent Konfiguration ein Validierungsfehler auf.

- Um Änderungen zu übernehmen, unten auf der Seite **Speichern** auswählen.

8. Nach der Aktualisierung der SNMP-Agentenkonfiguration **Speichern** auswählen.

Auf StorageGRID MIB-Dateien zugreifen

MIB-Dateien enthalten Definitionen und Informationen zu den Eigenschaften verwalteter Ressourcen und Dienste für die Knoten in Ihrem Grid. Es besteht Zugriff auf MIB-Dateien, die die Objekte und Benachrichtigungen für StorageGRID definieren. Diese Dateien können für die Überwachung Ihres Grids nützlich sein.

Weitere Informationen zu SNMP und MIB-Dateien sind unter "SNMP Überwachung" verfügbar.

Zugriff auf MIB-Dateien

Führen Sie die folgenden Schritte aus, um auf die MIB-Dateien zuzugreifen.

Schritte

1. **Konfiguration** > **Überwachung** > **SNMP agent** auswählen.
2. Wählen Sie auf der SNMP-Agent-Seite die Datei aus, die Sie herunterladen möchten:
   - **NETAPP-STORAGEGRID-MIB.txt**: Definiert die Alarmtabelle und die Benachrichtigungen (Traps), die auf allen Admin-Nodes zugänglich sind.
   - **ES-NETAPP-06-MIB.mib**: Definiert Objekte und Benachrichtigungen für E-Series-basierte Appliances.
   - **MIB_1_10.zip**: Definiert Objekte und Benachrichtigungen für Appliances mit einer BMC Schnittstelle.

   > Sie können auch an folgendem Speicherort auf jedem StorageGRID Node auf MIB-Dateien zugreifen: `/usr/share/snmp/mibs`

3. Zum Extrahieren der StorageGRID OIDs aus der MIB-Datei:

   a. Die OID des Stamms der StorageGRID MIB erhalten:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Ergebnis: `.1.3.6.1.4.1.789.28669` (`28669` ist immer die OID für StorageGRID)

   b. Im gesamten Baum nach der StorageGRID-OID mit `grep` suchen (unter Verwendung von `paste` zum

Verbinden der Zeilen):

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

Der `snmptranslate`Befehl bietet zahlreiche Optionen, die für die Untersuchung der MIB nützlich sind. Dieser Befehl ist auf jedem StorageGRID Node verfügbar.

MIB-Dateiinhalt

Alle Objekte befinden sich unter der StorageGRID OID.

Objektname	Objekt-ID (OID)	Beschreibung
		Das MIB-Modul für NetApp StorageGRID Entitäten.

MIB Objekte

Objektname	Objekt-ID (OID)	Typ	Zugang	MIB Modul	Beschreibung
activeAlertCount		Integer32	Nur lesbar	NETAPP-STORAGEGRID-MIB	Die Anzahl der aktiven Warnmeldungen in der activeAlertTable.
activeAlertTable		Abfolge von ActiveAlertEntry	Nicht zugänglich	NETAPP-STORAGEGRID-MIB	Eine Tabelle der aktiven Warnmeldungen in StorageGRID.
activeAlertEntry		Sequenz	Nicht zugänglich	NETAPP-STORAGEGRID-MIB	Eine einzelne StorageGRID Warnung, indiziert nach Warn-ID.
activeAlertId		Oktettzeichenkette	Nur lesbar	NETAPP-STORAGEGRID-MIB	Die ID der Warnung. Nur innerhalb der aktuell aktiven Warnungen eindeutig.
activeAlertName		Oktettzeichenkette	Nur lesbar	NETAPP-STORAGEGRID-MIB	Der Name der Warnung.
activeAlertInstance		Oktettzeichenkette	Nur lesbar	NETAPP-STORAGEGRID-MIB	Der Name der Entität, die die Warnung ausgelöst hat, typischerweise der Node-Name.
activeAlertSeverity		Oktettzeichenkette	Nur lesbar	NETAPP-STORAGEGRID-MIB	Der Schweregrad der Warnung.

Objektname	Objekt-ID (OID)	Typ	Zugang	MIB Modul	Beschreibung
activeAlertStartTime		Datum und Uhrzeit	Nur lesbar	NETAPP-STORAGEGRID-MIB	Der Zeitpunkt, zu dem die Warnmeldung ausgelöst wurde.

Zusätzliche StorageGRID Daten sammeln

Überwachen Sie die PUT- und GET-Leistung in StorageGRID

Die Leistung bestimmter Operationen, wie Objektspeicher und Abrufen von Objekten, kann überwacht werden, um Änderungen zu erkennen, die möglicherweise weitere Untersuchungen erfordern.

Über diese Aufgabe

Um die Leistung von PUT- und GET-Anfragen zu überwachen, können S3-Befehle direkt von einer Workstation ausgeführt oder die Open-Source-Anwendung S3tester verwendet werden. Mit diesen Methoden lässt sich die Leistung unabhängig von Faktoren bewerten, die außerhalb von StorageGRID liegen, wie etwa Problemen mit einer Client-Anwendung oder mit einem externen Netzwerk.

Bei Tests von PUT- und GET-Operationen gelten die folgenden Richtlinien:

- Verwenden Sie Objektgrößen, die mit den Objekten vergleichbar sind, die Sie üblicherweise in Ihr Grid einfügen.
- Operationen können sowohl an lokalen als auch an entfernten Standorten durchgeführt werden.

Meldungen im "Revisionsprotokoll" geben die Gesamtzeit an, die für bestimmte Operationen erforderlich ist. Beispielsweise lässt sich die gesamte Verarbeitungszeit einer S3 GET-Anfrage anhand des Werts des Attributs TIME in der SGET Audit-Nachricht nachvollziehen. Das Attribut TIME ist auch in den Audit-Nachrichten für die folgenden S3-Operationen zu finden: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Beim Analysieren der Ergebnisse sollte sowohl die durchschnittliche Zeit zur Bearbeitung einer Anfrage als auch der insgesamt erreichbare Durchsatz betrachtet werden. Die gleichen Tests sollten regelmäßig wiederholt und die Ergebnisse aufgezeichnet werden, sodass sich Trends erkennen lassen, die möglicherweise einer weiteren Untersuchung bedürfen.

- Sie können "S3tester von GitHub herunterladen".

Überwachen Sie Objektverifizierungsoperationen in StorageGRID

Das StorageGRID System kann die Integrität der Objektdaten auf Storage Nodes überprüfen und dabei sowohl beschädigte als auch fehlende Objekte erkennen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "${post_edited_translations.segment}".

Über diese Aufgabe

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

- Die **Hintergrundprüfung** läuft automatisch und überprüft kontinuierlich die Korrektheit der Objektdaten.

  Die Hintergrundprüfung überprüft automatisch und kontinuierlich alle Storage Nodes, um festzustellen, ob beschädigte Kopien replizierter und mit Erasure-Coding versehener Objektdaten vorhanden sind. Wenn Probleme festgestellt werden, versucht das StorageGRID System automatisch, die beschädigten Objektdaten durch Kopien zu ersetzen, die an anderer Stelle im System gespeichert sind. Die Hintergrundprüfung wird nicht für Objekte in einem Cloud Storage Pool durchgeführt.

  > Die Warnung **Unbekanntes beschädigtes Objekt erkannt** wird ausgelöst, wenn das System ein beschädigtes Objekt erkennt, das nicht automatisch korrigiert werden kann.

- Die **Objektexistenzprüfung** kann von einem Benutzer ausgelöst werden, um schneller das Vorhandensein (wenn auch nicht die Korrektheit) von Objektdaten zu überprüfen.

  Die Objektexistenzprüfung verifiziert, ob alle erwarteten replizierten Kopien von Objekten und Erasure-Coding-Fragmenten auf einem Storage Node vorhanden sind. Die Objektexistenzprüfung bietet eine Möglichkeit zur Überprüfung der Integrität von Speichermedien, insbesondere wenn ein kürzlich aufgetretenes Hardwareproblem die Datenintegrität beeinträchtigt haben könnte.

Die Ergebnisse der Hintergrundüberprüfungen und Objekt-Existenzprüfungen sollten regelmäßig geprüft werden. Alle Fälle von beschädigten oder fehlenden Objektdaten sind umgehend zu untersuchen, um die Ursache zu ermitteln.

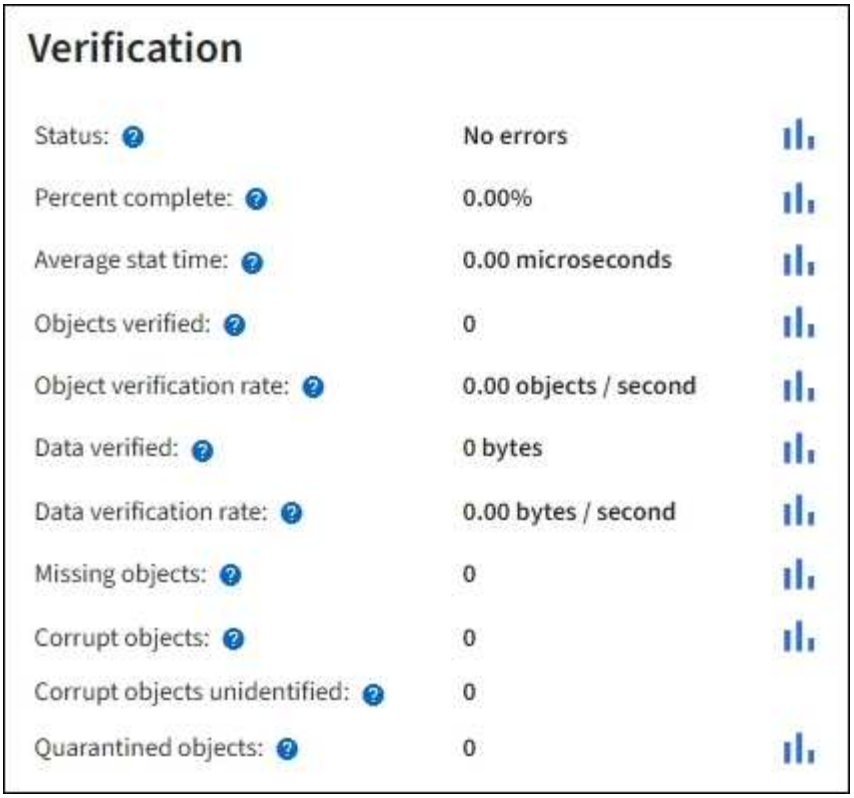
Schritte

1. Ergebnisse der Hintergrundüberprüfungen:

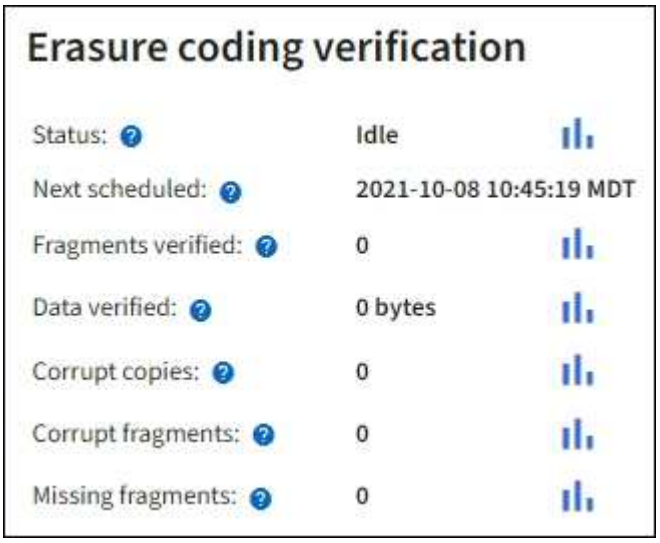
   a. Wählen Sie **Knoten** > **Speicherknoten** > **Objekte**.

   b. Verifizierungsergebnisse prüfen:

      - Zur Überprüfung der verifizierten replizierten Objektdaten können die Attribute im Abschnitt „Verifizierung“ betrachtet werden.

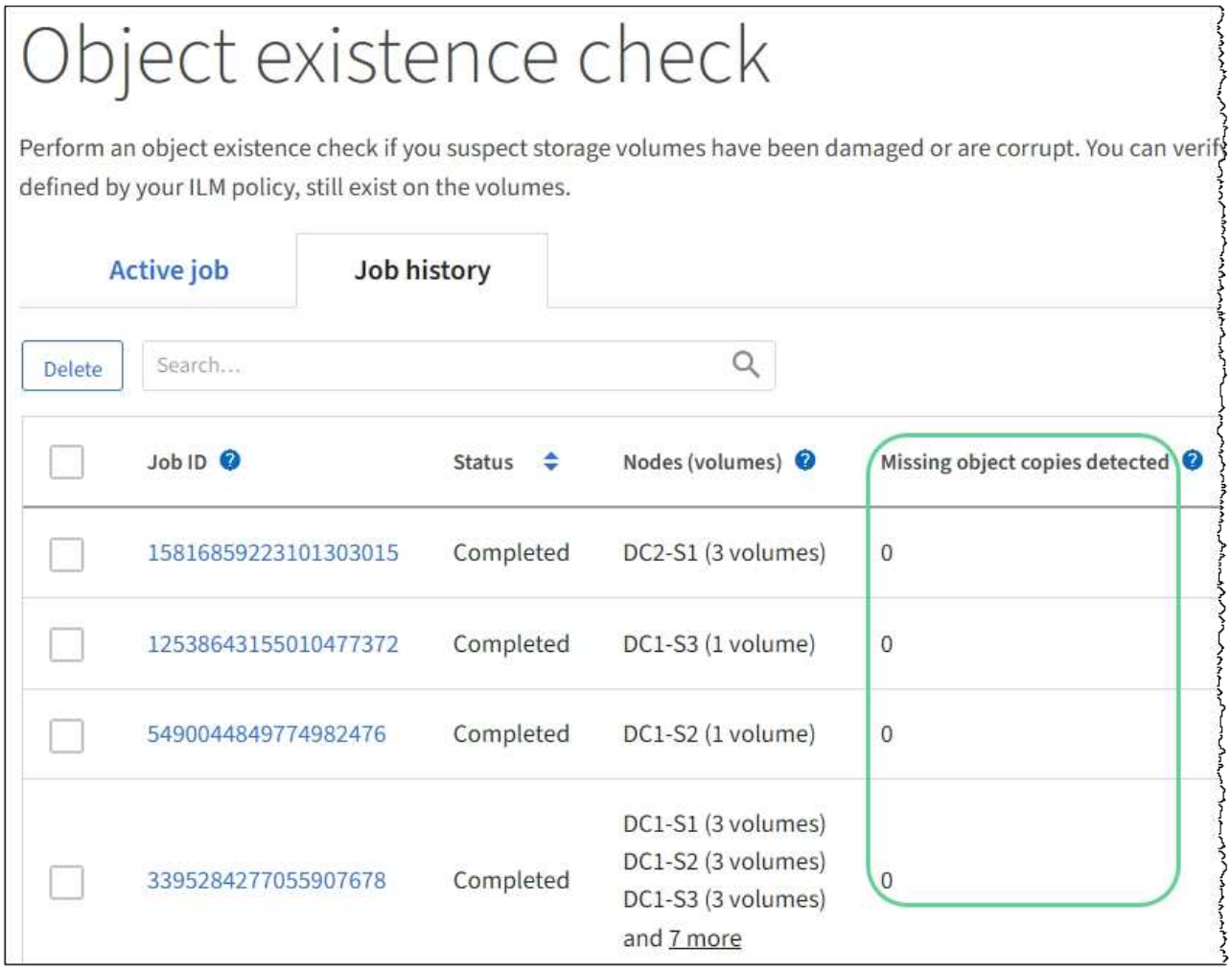


- Zur Überprüfung der Erasure-Coding-Fragmentverifizierung wird ***Storage Node*** > **ILM** ausgewählt und die Attribute im Abschnitt Erasure-Coding-Verifizierung betrachtet.



Das Fragezeichen ? neben dem Namen eines Attributs zeigt einen Hilfetext an.

2. Ergebnisse der Objektexistenzprüfungsjobs anzeigen:
   a. Wählen Sie **Wartung** > **Objektexistenzprüfung** > **Auftragsverlauf**.
   b. Die Spalte „Fehlende Objektkopien erkannt“ prüfen. Wenn bei einem Auftrag 100 oder mehr Objektkopien fehlen und die Warnung „Objekte möglicherweise verloren“ ausgelöst wurde, sollte der technische Support kontaktiert werden.



StorageGRID-Auditmeldungen prüfen

Audit-Meldungen können dabei helfen, die detaillierten Abläufe Ihres StorageGRID Systems besser zu verstehen. Revisionsprotokolle lassen sich zur Fehlerbehebung und zur Bewertung der Performance nutzen.

Während des normalen Systembetriebs generieren alle StorageGRID Dienste Revisionsprotokollmeldungen wie folgt:

- System-Audit-Meldungen beziehen sich auf das Auditsystem selbst, Grid-Knotenzustände, systemweite Aufgabenaktivitäten und Service-Backup-Operationen.
- Die Revisionsprotokoll-Meldungen für Objektspeicher beziehen sich auf die Speicherung und Verwaltung von Objekten innerhalb von StorageGRID, einschließlich Objektspeicherung und -abrufen, Grid-Node-zu-Grid-Node-Übertragungen und Verifizierungen.
- Lese- und Schreib-Revisionsprotokollmeldungen werden protokolliert, wenn eine S3-Clientanwendung eine Anfrage zum Erstellen, Ändern oder Abrufen eines Objekts stellt.
- Management Revisionsprotokoll-Meldungen protokollieren Benutzeranfragen an die Management-API.

Jeder Admin-Knoten speichert Revisionsprotokoll-Meldungen in Textdateien. Die Revisionsprotokoll-Freigabe enthält die aktive Datei (audit.log) sowie komprimierte Revisionsprotokolle der Vortage. Jeder Knoten im Grid speichert außerdem eine Kopie der auf dem Knoten generierten Revisionsprotokoll-Informationen.

Auf die Revisionsprotokolldateien kann direkt über die Befehlszeile des Admin-Knotens zugegriffen werden.

StorageGRID sendet standardmäßig Revisionsprotokoll-Informationen, oder das Ziel kann geändert werden:

- StorageGRID verwendet standardmäßig lokale Knoten als Revisionsprotokoll-Ziele.
- Revisionsprotokoll-Einträge von Grid Manager und Tenant Manager können an einen Storage Node gesendet werden.
- Optional kann das Ziel der Revisionsprotokolle geändert und Audit-Informationen an einen externen Syslog-Server gesendet werden. Lokale Revisionsprotokolle werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist.
- "Informationen zur Konfiguration der Protokollverwaltung".

Details zur Revisionsprotokoll Logdatei, zum Format der Audit-Meldungen, zu den Arten von Audit-Meldungen und zu den zur Analyse von Audit-Meldungen verfügbaren Tools finden sich unter "Audit-Protokolle prüfen".

Sammeln Sie StorageGRID-Protokolldateien und Systemdaten

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

Bevor Sie beginnen

- Sie sind im Grid Manager auf einem beliebigen Admin-Node mit einem "unterstützte Webbrowser" angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie besitzen die Bereitstellungspassphrase.

Über diese Aufgabe

Mit dem Grid Manager lassen sich "Protokolldateien", Systemdaten und Konfigurationsdaten von beliebigen Grid-Knoten für den gewählten Zeitraum erfassen. Die Daten werden gesammelt und in einer `.tar.gz` Datei archiviert, die anschließend auf den lokalen Computer heruntergeladen oder an den technischen Support gesendet werden kann.

Optional kann das Ziel der Audit-Logs geändert und Audit-Informationen an einen externen Syslog-Server gesendet werden. Lokale Protokolle der Audit-Einträge werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe "Logverwaltung und externen Syslog-Server konfigurieren".

Schritte

1. Wählen Sie **Support** > **Tools** > **Protokollsammlung**. Eine Tabelle mit Knoten wird angezeigt.
2. Wählen Sie die Grid-Knoten aus, für die Protokolldateien gesammelt werden sollen.

   Sie können nach Node-Name, Standort und Knotentyp sortieren. Die Spalten Standort und Knotentyp enthalten Filter zur Auswahl einzelner Standorte und Knotentypen.

3. Wählen Sie **Weiter**.
4. Wählen Sie den Datums- und Zeitbereich der Daten aus, die in die Protokolldateien aufgenommen werden.

   Wenn ein sehr langer Zeitraum ausgewählt wird oder Protokolle von allen Nodes in einem großen Grid erfasst werden, kann das Protokollarchiv zu groß werden, um auf einem Node gespeichert zu werden oder von einem Admin Node für den Download gesammelt zu werden. Tritt einer dieser Fälle ein, sollte die Protokollerfassung mit einer kleineren Datenmenge erneut gestartet werden.

5. Wählen Sie die Arten von Protokollen aus, die erfasst werden sollen.
   - **Anwendungsprotokolle**: Anwendungsspezifische Protokolle, die der technische Support am häufigsten zur Fehlerbehebung verwendet. Die erfassten Protokolle stellen eine Teilmenge der verfügbaren Anwendungsprotokolle dar.
   - **Audit-Protokolle**: Protokolle, die die während des normalen Systembetriebs generierten Audit-Meldungen enthalten.
   - **Network Trace**: Protokolle, die für das Netzwerk-Debugging verwendet werden.
   - **Prometheus Datenbank**: Zeitreihenmetriken der Dienste auf allen Nodes.
6. Optional kann das Textfeld **Notizen** verwendet werden, um Anmerkungen zu den gesammelten Protokolldateien einzugeben.

   Diese Notizen können verwendet werden, um dem technischen Support Informationen zu dem Problem bereitzustellen, das zur Sammlung der Protokolldateien geführt hat. Ihre Notizen werden zusammen mit anderen Informationen zur Protokolldateisammlung in einer Datei namens `info.txt` gespeichert. Die `info.txt` Datei wird im Protokolldateiarchivpaket gespeichert.

7. Im Textfeld **Bereitstellungspassphrase** die Bereitstellungspassphrase für Ihr StorageGRID System eingeben.
8. **Protokolle sammeln** auswählen.

   Auf der Seite „Protokollsammlung“ lässt sich der Fortschritt der Protokolldateisammlung für jeden Grid-Knoten überwachen.

   Falls eine Fehlermeldung bezüglich der Protokollgröße angezeigt wird, kann das Sammeln von Protokollen für einen kürzeren Zeitraum oder für weniger Knoten Abhilfe schaffen.

9. Falls die Protokollerfassung fehlschlägt:
   - Wenn die Meldung „Protokollsammlung fehlgeschlagen“ erscheint, kann die Protokollsammlung wiederholt oder die Sitzung ohne erneuten Versuch beendet werden.
   - Wenn die Meldung "Protokollsammlung teilweise fehlgeschlagen" erscheint, können Sie die Protokollsammlung wiederholen, die Sitzung beenden, die unvollständige Protokolldatei herunterladen oder die unvollständige Protokolldatei an AutoSupport senden.
10. Wenn die Protokolldateierfassung abgeschlossen ist:
    - **Herunterladen** auswählen, um die `.tar.gz` Datei herunterzuladen.
    - **Senden an AutoSupport** auswählen, um die `.tar.gz` Datei an den technischen Support zu senden.

      Die `.tar.gz` Datei enthält alle Protokolldateien aller Grid-Knoten, bei denen die Protokollerfassung erfolgreich war. Die kombinierte `.tar.gz` Datei enthält für jeden Grid-Knoten ein Protokolldateiarchiv.

    Der Gegenstand des AutoSupport Pakets ist `USER_TRIGGERED_SUPPORT_BUNDLE`.

11. Wählen Sie **Fertigstellen**.

    Die `.tar.gz` Datei wird gelöscht, wenn **Fertigstellen** ausgewählt wird. Vor dem Löschen sollte die Datei heruntergeladen oder versendet werden.

Ein StorageGRID AutoSupport Paket manuell auslösen

Um den technischen Support bei der Fehlerbehebung Ihres StorageGRID Systems zu unterstützen, kann ein AutoSupport-Paket manuell zum Senden ausgelöst werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie verfügen über die Root-Zugriffsberechtigung oder die Berechtigung zur Konfiguration anderer Grids.

Schritte

1. **Support** > **Tools** > **AutoSupport** auswählen.
2. Auf der Registerkarte **Aktionen Benutzerausgelöste AutoSupport senden** auswählen.

   StorageGRID versucht, ein AutoSupport-Paket an die NetApp Support Site zu senden. Bei Erfolg werden die Werte für **Letztes Ergebnis** und **Letzter erfolgreicher Zeitpunkt** auf der Registerkarte **Ergebnisse** aktualisiert. Tritt ein Problem auf, wird der Wert für **Letztes Ergebnis** auf „Fehlgeschlagen“ gesetzt, und StorageGRID versucht nicht, das AutoSupport-Paket erneut zu senden.

3. Nach einer Minute die AutoSupport-Seite im Browser aktualisieren, um auf die neuesten Ergebnisse zuzugreifen.

> Außerdem können Sie "umfangreichere Protokolldateien und Systemdaten erfassen" und sie an die NetApp Support Site senden.

Überprüfen Sie die StorageGRID-Support-Metriken

Bei der Fehlersuche besteht die Möglichkeit, gemeinsam mit dem technischen Support detaillierte Metriken und Diagramme für Ihr StorageGRID System zu überprüfen.

Bevor Sie beginnen

- Sie müssen mit einem "unterstützte Webbrowser" im Grid Manager angemeldet sein.
- Du hast "spezifische Zugriffsberechtigungen".

Über diese Aufgabe

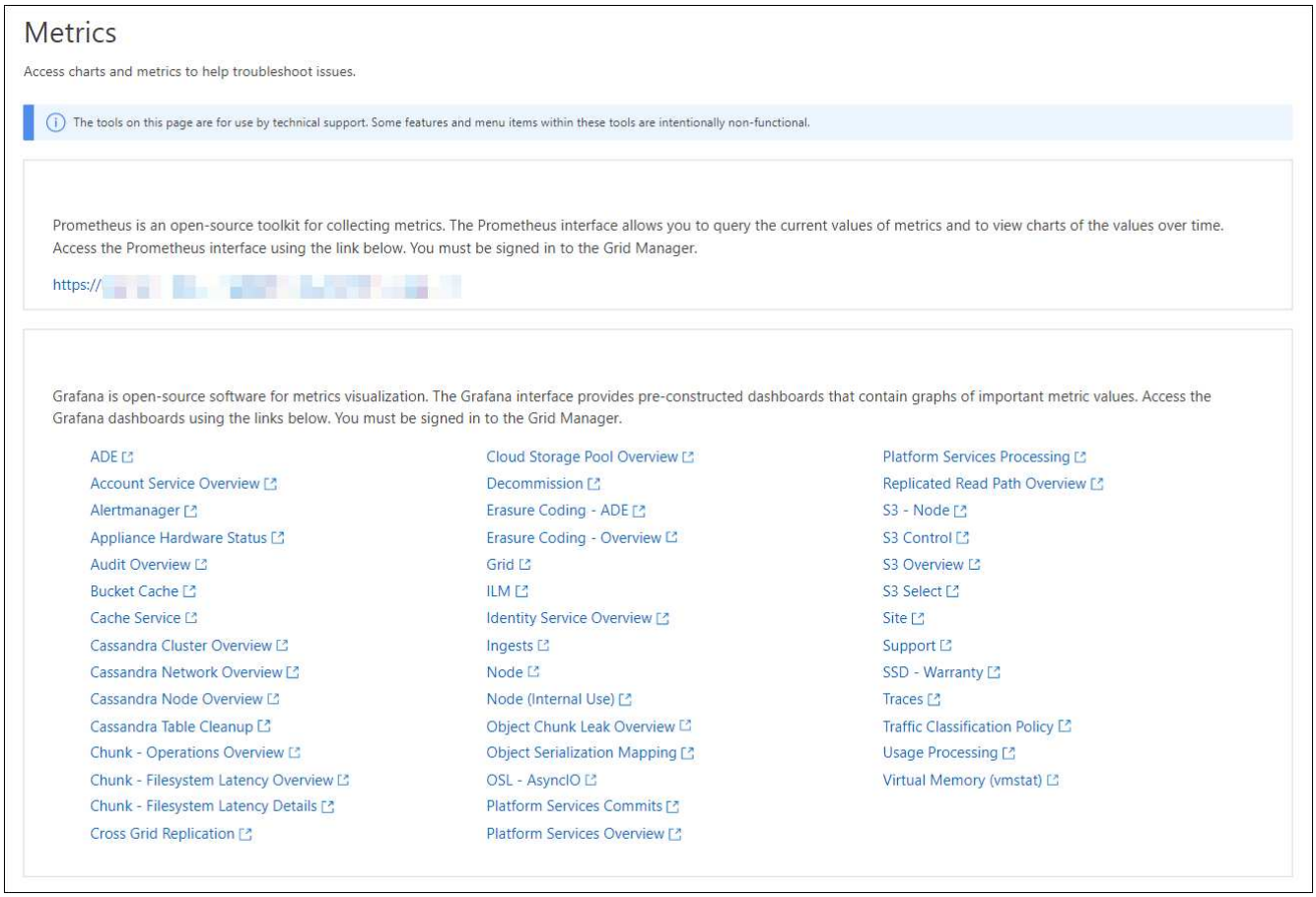
Die Seite „Metriken“ ermöglicht den Zugriff auf die Benutzeroberflächen von Prometheus und Grafana. Prometheus ist Open-Source-Software zur Erfassung von Metriken. Grafana ist Open-Source-Software zur Visualisierung von Metriken.

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

Schritte

1. Wie vom technischen Support vorgegeben, **Support** > **Tools** > **Metrics** auswählen.

   Ein Beispiel für die Seite „Metriken“ ist hier dargestellt:



2. Zum Abfragen der aktuellen Werte der StorageGRID-Metriken und zum Anzeigen von Diagrammen der Werte im Zeitverlauf auf den Link im Abschnitt Prometheus klicken.

   Die Prometheus-Oberfläche wird angezeigt. Mit dieser Oberfläche lassen sich Abfragen zu den verfügbaren StorageGRID-Metriken ausführen und StorageGRID-Metriken im Zeitverlauf grafisch darstellen.

   > Metriken, die *private* in ihrem Namen enthalten, sind nur für den internen Gebrauch bestimmt und können sich zwischen StorageGRID Versionen ohne Vorankündigung ändern.

3. Zum Zugriff auf vorgefertigte Dashboards mit Diagrammen der StorageGRID-Metriken im Zeitverlauf stehen die Links im Abschnitt Grafana zur Verfügung.

   Die Grafana Oberfläche für den ausgewählten Link erscheint.

Ändern Sie die E/A-Priorisierung in StorageGRID

Die Priorisierung von Ein-/Ausgabe (E/A) ermöglicht eine Änderung der relativen Prioritäten für E/A-Operationen im Grid.

Standardmäßig hat der PUT- und GET-E/A-Verkehr von Clients höchste Priorität gegenüber Hintergrundaktivitäten wie dem Löschen von erasure-coded (EC) Daten und der EC-Reparatur. Durch eine Erhöhung der Priorität von Aktivitäten wie dem Löschen von erasure-coded (EC) Daten und der EC-Reparatur können diese Aufgaben möglicherweise schneller abgeschlossen werden. Die Wirksamkeit von Änderungen bei der E/A-Priorisierung wird durch die Rate der Clientanfragen, Schwankungen im Netzwerkverkehr und andere laufende Netzwerkaufgaben beeinflusst.

Bevor Sie beginnen

- Die Seite zur I/O-Priorisierung bietet einen Überblick darüber, welche Optionen Auswirkungen auf Ihr Grid haben könnten.
- Es sollte bewertet werden, ob der laufende Clientverkehr längere Wartezeiten oder Client-Timeouts problemlos verkraften kann.

- Es empfiehlt sich, die Auswirkungen der Priorisierungsänderung zu überwachen und bei Bedarf anzupassen. Diese Änderungen werden schnell umgesetzt, ihre Wirkung kann jedoch erst nach Stunden sichtbar werden.

Schritte

1. **Support** > **E/A-Priorisierung** auswählen.
2. (Optional) Die Priorität für die EC-Bereinigung und Reparatur kann für Hintergrundvorgänge, die EC-Daten bereinigen, von den Standardwerten geändert werden.

   Die standardmäßige niedrige EC-Bereinigungs- und Reparaturpriorität wird für Grids mit RAID-basierten Knoten verwendet.

3. **Speichern** auswählen.
4. Die "Metriken" sollte überwacht werden, um die Auswirkungen von Priorisierungsänderungen zu beurteilen.

Führen Sie Diagnose in StorageGRID aus

Bei der Fehlersuche besteht die Möglichkeit, gemeinsam mit dem technischen Support Diagnose auf Ihrem StorageGRID System durchzuführen und die Ergebnisse zu überprüfen.

- "Support-Metriken überprüfen"
- "Häufig verwendete Prometheus Metriken"

Bevor Sie beginnen

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

Über diese Aufgabe

Die Diagnoseseite führt eine Reihe von Diagnoseprüfungen des aktuellen Zustands des Grids durch. Jede Diagnoseprüfung kann einen von drei Statuswerten annehmen:

- **Normal**: Alle Werte liegen im Normalbereich.
- **Achtung**: Mindestens ein Wert liegt außerhalb des normalen Bereichs.
- **Vorsicht**: Einer oder mehrere der Werte liegen deutlich außerhalb des Normbereichs.

Die Diagnosestatus sind unabhängig von aktuellen Warnmeldungen und weisen möglicherweise nicht auf betriebliche Probleme mit dem Grid hin. Beispielsweise kann eine Diagnoseprüfung den Status „Warnung“ anzeigen, selbst wenn keine Warnmeldung ausgelöst wurde.

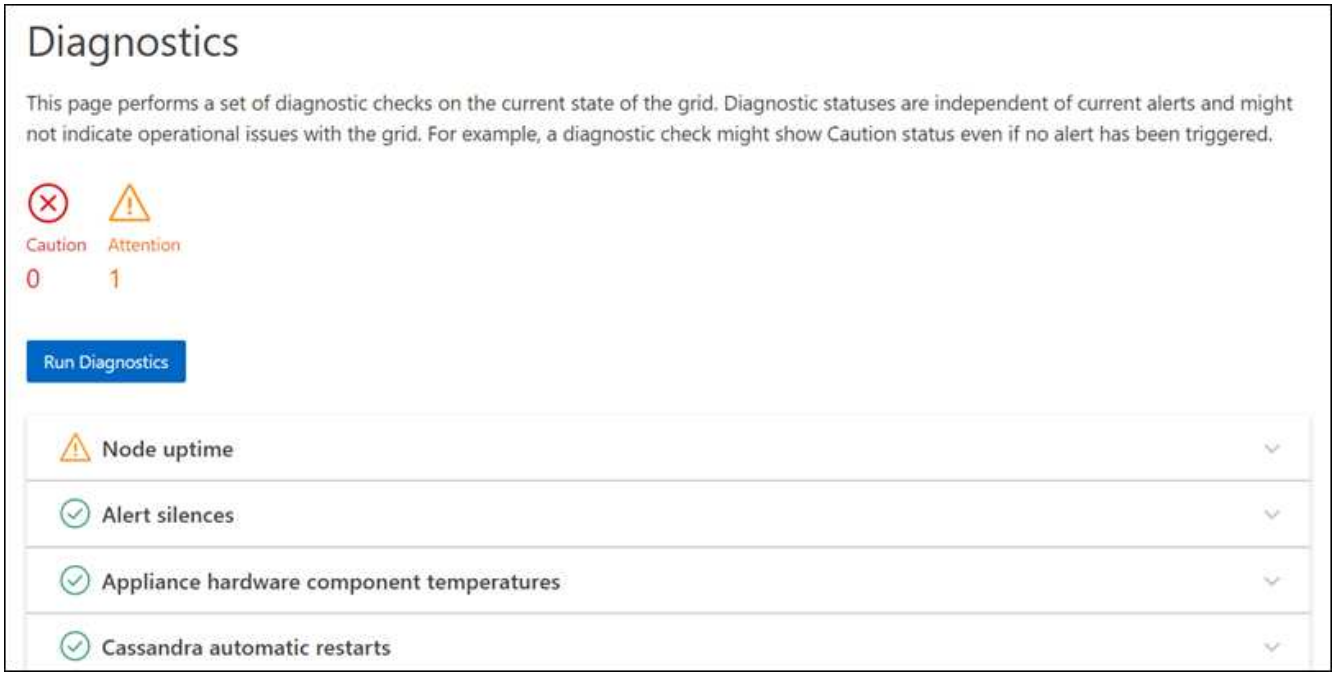
Schritte

1. **Support** > **Tools** > **Diagnose** auswählen.

   Die Seite „Diagnose“ wird angezeigt und listet die Ergebnisse jeder Diagnoseprüfung auf. Die Ergebnisse sind nach Schweregrad (Vorsicht, Aufmerksamkeit und dann Normal) sortiert. Innerhalb jedes Schweregrads sind die Ergebnisse alphabetisch sortiert.

   In diesem Beispiel hat eine Diagnose den Status „Aufmerksamkeit“ und drei Diagnosen haben den Status

„Normal“.



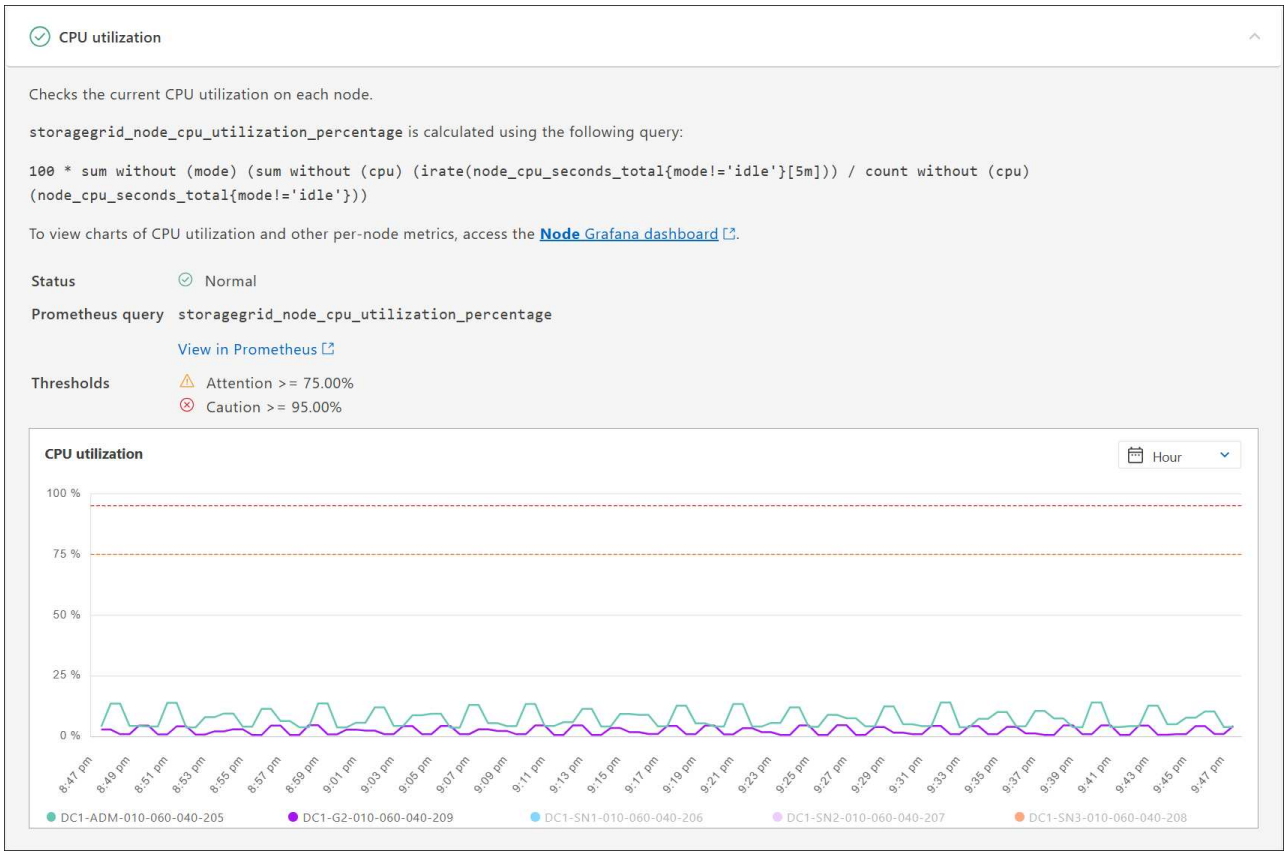
2. Weitere Informationen zu einer bestimmten Diagnose erhalten Sie, wenn Sie irgendwo in die Zeile klicken.

   Details zur Diagnose und deren aktuellen Ergebnissen werden angezeigt. Folgende Details sind aufgeführt:

   - **Status**: Der aktuelle Status dieser Diagnose: Normal, Aufmerksamkeit oder Vorsicht.
   - **Prometheus-Abfrage**: Falls für die Diagnose verwendet, der Prometheus-Ausdruck, der zur Generierung der Statuswerte verwendet wurde. (Ein Prometheus-Ausdruck wird nicht für alle Diagnosen verwendet.)
   - **Schwellenwerte**: Sofern für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden abnormalen Diagnosestatus. (Schwellenwerte werden nicht für alle Diagnosen verwendet.)

     Diese Schwellenwerte können nicht geändert werden.

   - **Statuswerte**: Ein Diagramm und eine Tabelle (Tabelle nicht im Screenshot dargestellt) zeigen den Status und den Wert der Diagnose im gesamten StorageGRID System. In diesem Beispiel wird die aktuelle CPU-Auslastung für jeden Knoten in einem StorageGRID System angezeigt. Alle Knotenwerte liegen unterhalb der Schwellenwerte für Attention und Caution, daher ist der Gesamtstatus der Diagnose Normal.



3. **Optional**: Um Grafana-Diagramme zu dieser Diagnose anzuzeigen, **Grafana dashboard** auswählen.

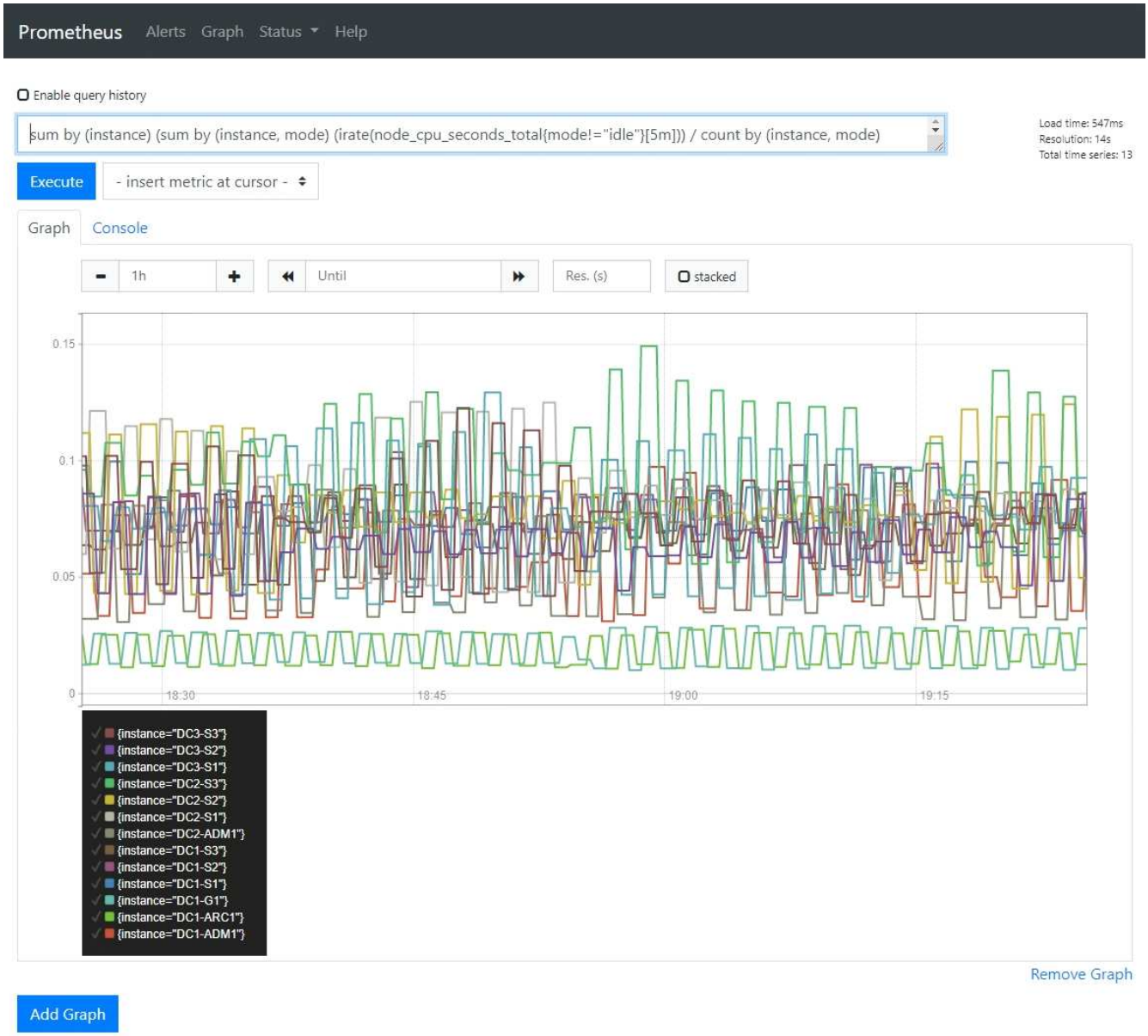
   Dieser Link wird nicht für alle Diagnose angezeigt.

   Das zugehörige Grafana Dashboard wird angezeigt. In diesem Beispiel wird das Node Dashboard angezeigt, das die CPU-Auslastung dieses Knotens im Zeitverlauf sowie weitere Grafana-Diagramme für den Knoten darstellt.

   > Auch über den Grafana-Bereich der Seite **Support** > **Tools** > **Metrics** besteht Zugriff auf die vorkonfigurierten Grafana Dashboards.

4. **Optional**: Ein Diagramm des Prometheus-Ausdrucks im Zeitverlauf ist über **In Prometheus anzeigen** einsehbar.

   Ein Prometheus-Graph des im Diagnoseverfahren verwendeten Ausdrucks wird angezeigt.



Erstellen Sie benutzerdefinierte Überwachungsanwendungen für StorageGRID

Mit den über die Grid Management API verfügbaren StorageGRID Metriken lassen sich benutzerdefinierte Überwachungsanwendungen und Dashboards erstellen.

Wenn Sie Metriken überwachen möchten, die nicht auf einer bestehenden Seite des Grid Managers angezeigt werden, oder wenn Sie benutzerdefinierte Dashboards für StorageGRID erstellen möchten, kann die Grid Management API verwendet werden, um StorageGRID-Metriken abzufragen.

Sie können auch direkt mit einem externen Überwachungstool wie Grafana auf Prometheus-Metriken zugreifen. Die Verwendung eines externen Tools erfordert das Hochladen oder Generieren eines administrativen Clientzertifikats, damit StorageGRID das Tool zur Authentifizierung aus Sicherheitsgründen zulassen kann. Siehe "Anleitungen zur Administration von StorageGRID".

Um die API-Operationen für Metriken, einschließlich der vollständigen Liste der verfügbaren Metriken, anzuzeigen, zum Grid Manager wechseln. Oben auf der Seite das Hilfesymbol auswählen und dann **API documentation** > **metrics** wählen.

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 Details zur Implementierung einer benutzerdefinierten Überwachungsanwendung gehen über den Rahmen dieser Dokumentation hinaus.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

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

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

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

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

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

Markeninformationen

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