Monitoring und Fehlerbehebung

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Monitoring und Fehlerbehebung

Überwachen Sie ein StorageGRID System

Erfahren Sie, wie Sie ein StorageGRID System überwachen und eventuelle Probleme bewerten. Listet alle Systemmeldungen auf.

- "Verwenden des Grid Managers zur Überwachung"
- "Informationen, die Sie regelmäßig überwachen sollten"
- "Verwalten von Meldungen und Alarmen"
- "Verwendung von SNMP-Überwachung"
- "Erfassung weiterer StorageGRID-Daten"
- "Fehlerbehebung für ein StorageGRID System"
- "Alerts Referenz"
- "Alarmreferenz (Altsystem)"
- "Referenz für Protokolldateien"

Verwenden des Grid Managers zur Überwachung

Der Grid Manager ist das wichtigste Tool für das Monitoring Ihres StorageGRID Systems. In diesem Abschnitt wird das Grid Manager Dashboard vorgestellt sowie ausführliche Informationen zu den Seiten Nodes bereitgestellt.

- "Anforderungen an einen Webbrowser"
- "Anzeigen des Dashboards"
- "Anzeigen der Seite Knoten"

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

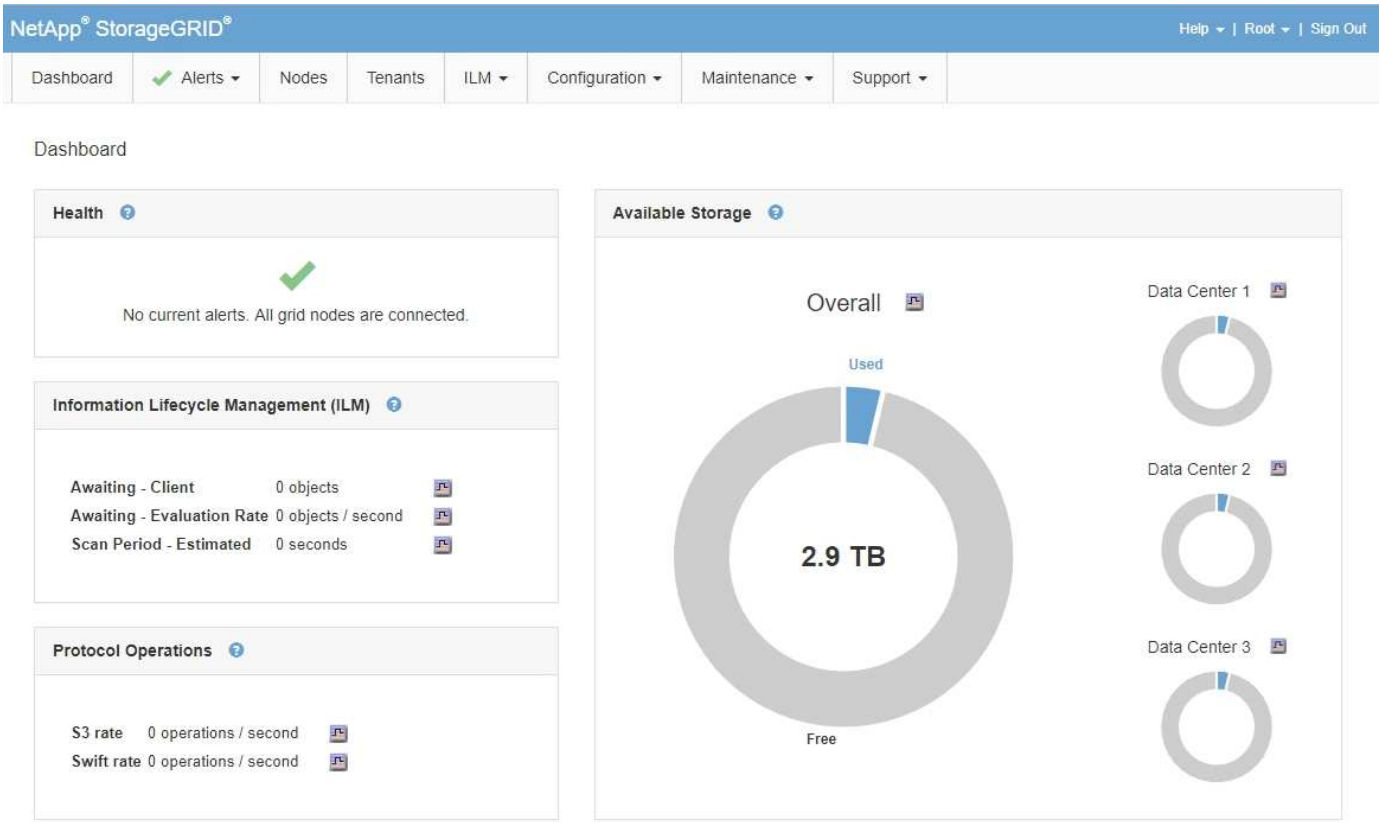
Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024

Browserbreite	Pixel
Optimal	1280

Anzeigen des Dashboards

Wenn Sie sich zum ersten Mal beim Grid Manager anmelden, können Sie über das Dashboard Systemaktivitäten auf einen Blick überwachen. Das Dashboard enthält Informationen zum Systemzustand, über Auslastungsmetriken sowie über Betriebstrends und -Diagramme.



Systemzustand

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Fasst den Systemzustand zusammen. Ein grünes Häkchen bedeutet, dass keine aktuellen Warnmeldungen vorhanden sind und alle Grid-Nodes verbunden sind. Jedes andere Symbol bedeutet, dass mindestens eine aktuelle Warnung oder ein nicht getrennter Knoten vorhanden ist.	Möglicherweise werden mindestens ein der folgenden Links angezeigt: • **Grid Details**: Wird angezeigt, wenn Knoten getrennt sind (Verbindungsstatus unbekannt oder Administrativ ausgefallen). Klicken Sie auf den Link oder klicken Sie auf das blaue oder graue Symbol, um zu ermitteln, welche Nodes betroffen sind. • **Aktuelle Meldungen**: Wird angezeigt, wenn derzeit Alarme aktiv sind. Klicken Sie auf den Link oder klicken Sie auf **kritisch**, **Major** oder **Minor**, um die Details auf der Seite **Alarme** > **Aktuell** anzuzeigen. • **Kürzlich behobene Alarme**: Wird angezeigt, wenn alle in der letzten Woche ausgelösten Benachrichtigungen jetzt behoben sind. Klicken Sie auf den Link, um die Details auf der Seite **Alerts** > **aufgelöst** anzuzeigen. • **Legacy-Alarme**: Wird angezeigt, wenn derzeit Alarme (Legacy-System) aktiv sind. Klicken Sie auf den Link, um die Details auf der Seite **Support** > **Alarme (alt)** > **Aktuelle Alarme** anzuzeigen. • **Lizenz**: Wird angezeigt, wenn ein Problem mit der Softwarelizenz für dieses StorageGRID-System vorliegt. Klicken Sie auf den Link, um die Details auf der Seite **Wartung** > **System** > **Lizenz** anzuzeigen.	• "Monitoring der Verbindungsstatus der Nodes" • "Anzeigen aktueller Meldungen" • "Anzeigen gelöster Warnmeldungen" • "Anzeigen von Legacy-Alarmen" • "StorageGRID verwalten"

Bereich „Verfügbare Lagerung“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die verfügbare und genutzte Speicherkapazität im gesamten Grid an, nicht einschließlich Archivmedien. Das Gesamtdiagramm stellt die Gesamtgesamtwerte für das gesamte Grid dar. Ist dies ein Grid mit mehreren Standorten, werden für jeden Datacenter-Standort zusätzliche Diagramme angezeigt. Anhand dieser Informationen können Sie den verwendeten Speicher mit dem verfügbaren Speicher vergleichen. Wenn Sie ein Grid mit mehreren Standorten verwenden, können Sie feststellen, welcher Standort mehr Storage verbraucht.	• Um die Kapazität anzuzeigen, platzieren Sie den Cursor über die verfügbaren und genutzten Kapazitätsbereiche des Diagramms. • Um Kapazitätstrends über einen Datumsbereich anzuzeigen, klicken Sie auf das Diagrammsymbol Für das Gesamtraster oder einen Standort im Datacenter. • Um Details anzuzeigen, wählen Sie **Knoten**. Anschließend können Sie die Registerkarte „Storage“ für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen.	• "Anzeigen der Registerkarte „Speicher“" • "Monitoring der Storage-Kapazität"

Bereich „Information Lifecycle Management“ (ILM)

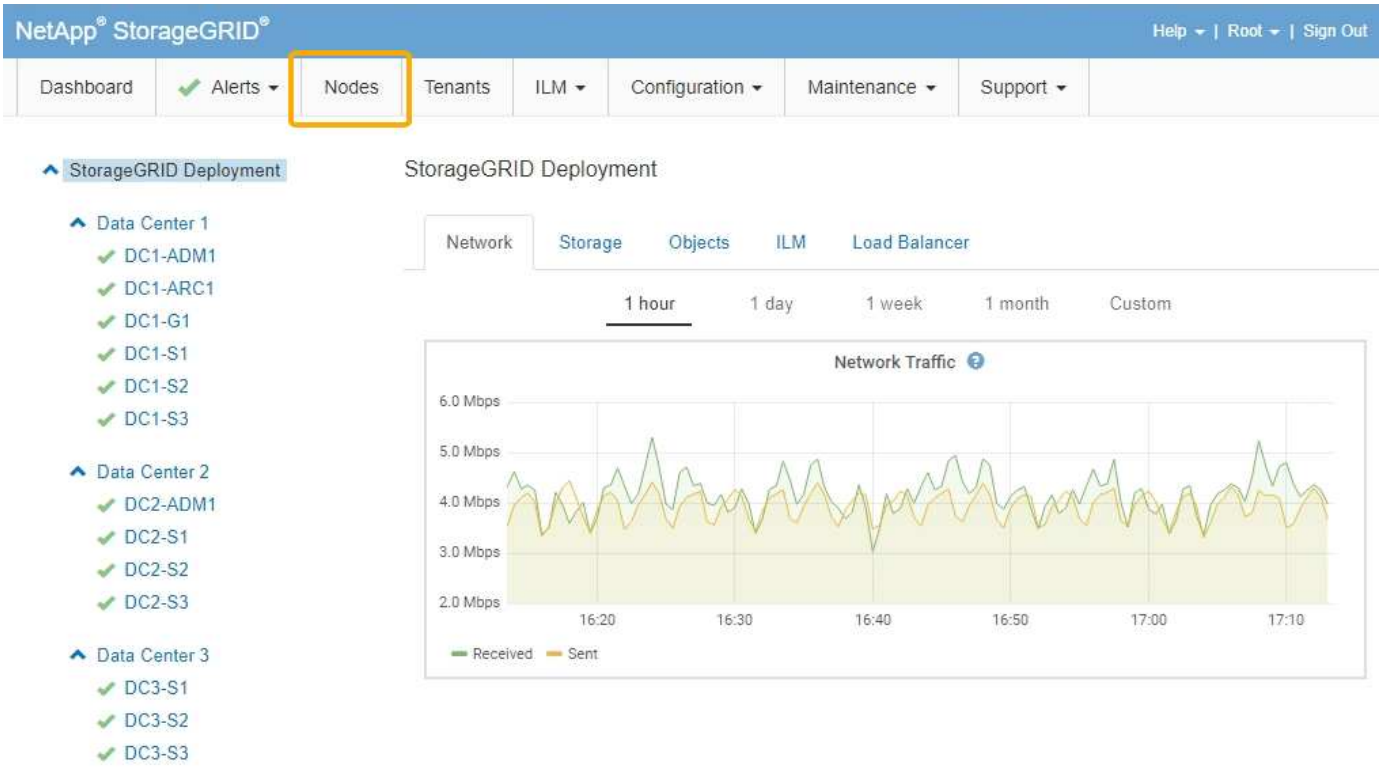
Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die aktuellen ILM-Vorgänge und ILM-Warteschlangen für das System an. Sie können diese Informationen für das Monitoring der Arbeitsbelastung Ihres Systems verwenden. • **Ausstehend - Client**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aus Client-Operationen warten (zum Beispiel Aufnahme). • **Ausstehend - Evaluation Rate**: Die aktuelle Rate, mit der Objekte ausgewertet werden, entspricht der ILM-Richtlinie im Grid. • **Scan Period - Estimated**: Die geschätzte Zeit, um einen vollständigen ILM-Scan aller Objekte abzuschließen. **Hinweis:** Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde.	• Um Details anzuzeigen, wählen Sie **Knoten**. Anschließend können Sie die ILM-Registerkarte für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen. • Um die vorhandenen ILM-Regeln anzuzeigen, wählen Sie **ILM** > **Regeln**. • Um die vorhandenen ILM-Richtlinien anzuzeigen, wählen Sie **ILM** > **Richtlinien**.	• "Anzeigen der Registerkarte ILM" • "StorageGRID verwalten".

Bereich „Protokollbetrieb“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die Anzahl der protokollspezifischen Vorgänge (S3 und Swift) an, die vom System durchgeführt werden. Sie können diese Informationen nutzen, um die Workloads und die Effizienz Ihres Systems zu überwachen. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.	• Um Details anzuzeigen, wählen Sie **Knoten**. Anschließend können Sie die Registerkarte Objekte für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen. • Um Trends über einen Datumsbereich anzuzeigen, klicken Sie auf das Diagrammsymbol Rechts neben der S3- oder Swift-Protokollrate.	• "Anzeigen der Registerkarte Objekte" • "S3 verwenden" • "Verwenden Sie Swift"

Anzeigen der Seite Knoten

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



In der Baumansicht links sehen Sie alle Standorte und alle Knoten in Ihrem StorageGRID-System. Das Symbol für jeden Knoten gibt an, ob der Knoten verbunden ist oder ob aktive Warnmeldungen vorliegen.

Symbole für Verbindungsstatus

Wenn ein Knoten von der Tabelle getrennt wird, zeigt die Strukturansicht ein blaues oder graues Verbindungssymbol an, nicht das Symbol für die zugrunde liegenden Warnungen.

- **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.

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

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

Warnungssymbole

Wenn ein Knoten mit dem Raster verbunden ist, wird in der Strukturansicht eines der folgenden Symbole angezeigt, je nachdem, ob aktuelle Warnmeldungen für den Knoten vorhanden sind.

- * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen.
- **Major** : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet.
- **Klein** : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
- **Normal** : Es sind keine Alarme aktiv, und der Knoten ist mit dem Raster verbunden.

Anzeigen von Details zu einem System, Standort oder Node

Um die verfügbaren Informationen anzuzeigen, klicken Sie auf die entsprechenden Links auf der linken Seite, wie folgt:

- Wählen Sie den Grid-Namen aus, um eine Zusammenfassung der Statistiken für Ihr gesamtes StorageGRID System anzuzeigen. (Der Screenshot zeigt ein System mit dem Namen „StorageGRID Deployment“.)
- Wählen Sie einen bestimmten Datacenter-Standort aus, um eine aggregierte Zusammenfassung der Statistiken für alle Nodes an diesem Standort anzuzeigen.
- Wählen Sie einen bestimmten Node aus, um detaillierte Informationen zu diesem Node anzuzeigen.

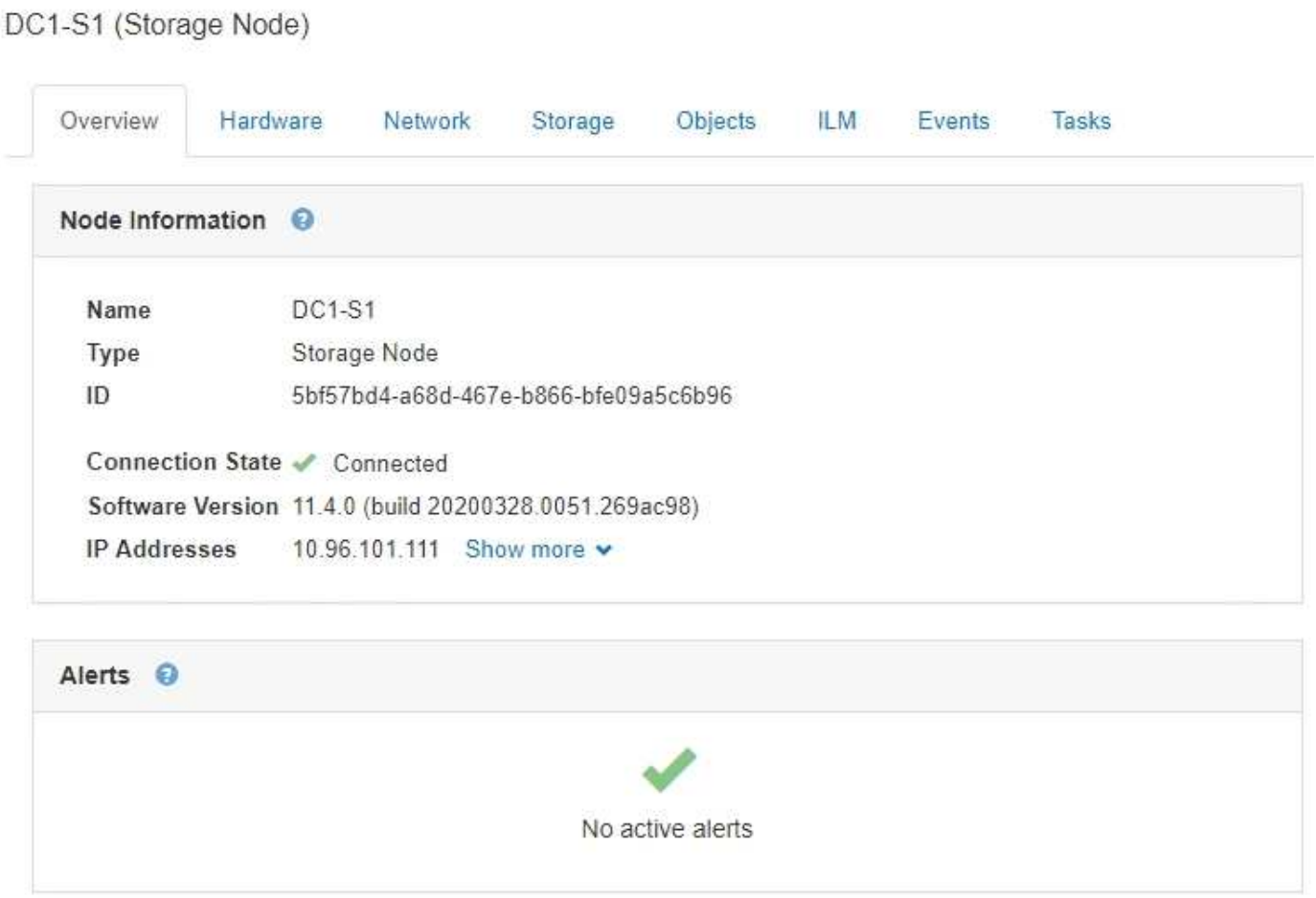
Anzeigen der Registerkarte Übersicht

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

Die Registerkarte Übersicht wird für alle Knoten angezeigt.

Node-Informationen

Im Abschnitt Knoteninformationen auf der Registerkarte Übersicht werden grundlegende Informationen zum Grid-Knoten angezeigt.



Die Übersichtsinformationen für einen Knoten umfassen Folgendes:

- **Name**: Der Hostname, der dem Knoten zugewiesen und im Grid Manager angezeigt wird.
- **Typ**: Der Node-Typ - Admin-Node, Storage Node, Gateway-Node oder Archiv-Node.
- **ID**: Die eindeutige Kennung für den Knoten, die auch als UUID bezeichnet wird.
- **Verbindungsstatus**: Einer von drei Zuständen. Das Symbol für den schwersten Zustand wird angezeigt.
  - **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.

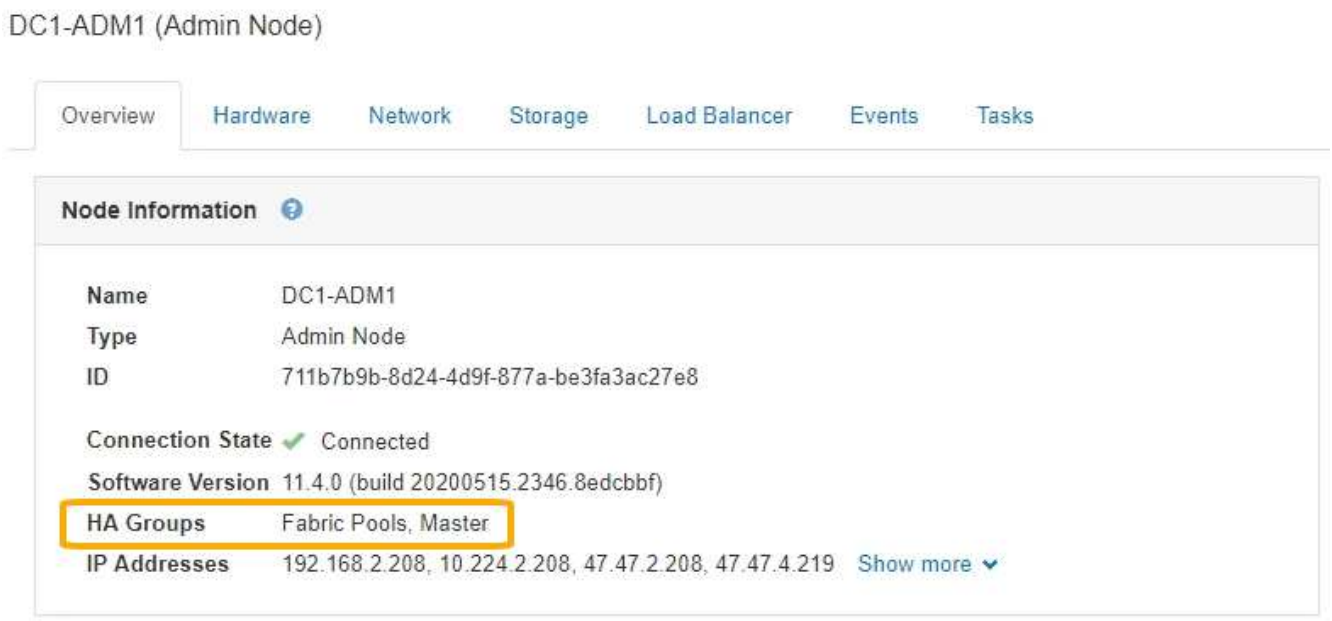
    Ein Node wird möglicherweise während des verwalteten Herunterfahrens als „Unbekannt“ angezeigt. In diesen Fällen können Sie den Status Unbekannt ignorieren.

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

möglicherweise auch aktiv.

- * Verbunden* ✔: Der Knoten ist mit dem Raster verbunden.

- **Software-Version**: Die Version von StorageGRID, die auf dem Knoten installiert ist.
- **HA-Gruppen**: Nur für Admin-Node und Gateway-Knoten. Wird angezeigt, ob eine Netzwerkschnittstelle auf dem Knoten in einer Hochverfügbarkeitsgruppe enthalten ist und ob diese Schnittstelle der Master oder der Backup ist.



- **IP-Adressen**: Die IP-Adressen des Knotens. Klicken Sie auf **Mehr anzeigen**, um die IPv4- und IPv6-Adressen und Schnittstellenzuordnungen des Knotens anzuzeigen:
  - Eth0: Grid Network
  - Eth1: Admin Network
  - Eth2: Client-Netzwerk

Meldungen

Im Abschnitt „Warnungen“ der Registerkarte „Übersicht“ werden alle Warnmeldungen aufgeführt, die derzeit diesen Knoten betreffen, die nicht stummgeschaltet wurden. Klicken Sie auf den Namen der Warnmeldung, um weitere Details und empfohlene Aktionen anzuzeigen.

Verwandte Informationen

"Monitoring der Verbindungsstatus der Nodes"

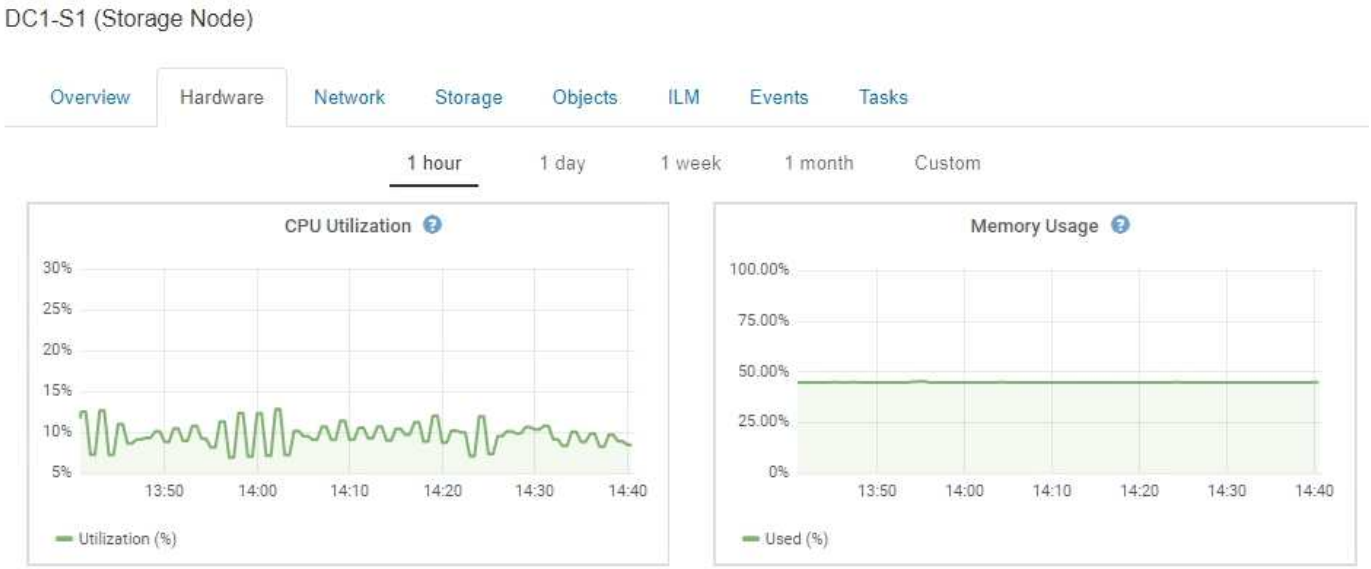
"Anzeigen aktueller Meldungen"

"Anzeigen einer bestimmten Meldung"

Anzeigen der Registerkarte Hardware

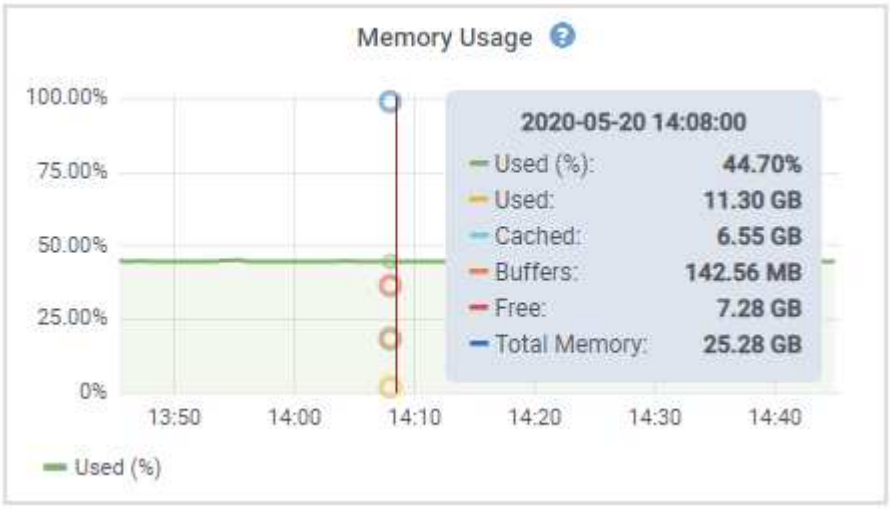
Auf der Registerkarte Hardware werden für jeden Node CPU-Auslastung und Arbeitsspeicherauslastung sowie zusätzliche Hardware-Informationen über Appliances angezeigt.

Die Registerkarte Hardware wird für alle Nodes angezeigt.



Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, mit dem Sie Datum und Zeitbereiche festlegen können.

Wenn Sie Details zur CPU-Auslastung und Arbeitsspeicherauslastung anzeigen möchten, bewegen Sie den Mauszeiger über jedes Diagramm.



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

Verwandte Informationen

"Anzeigen von Informationen zu Appliance-Speicherknoten"

"Anzeigen von Informationen zu Appliance Admin Nodes und Gateway Nodes"

Registerkarte Netzwerk anzeigen

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

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

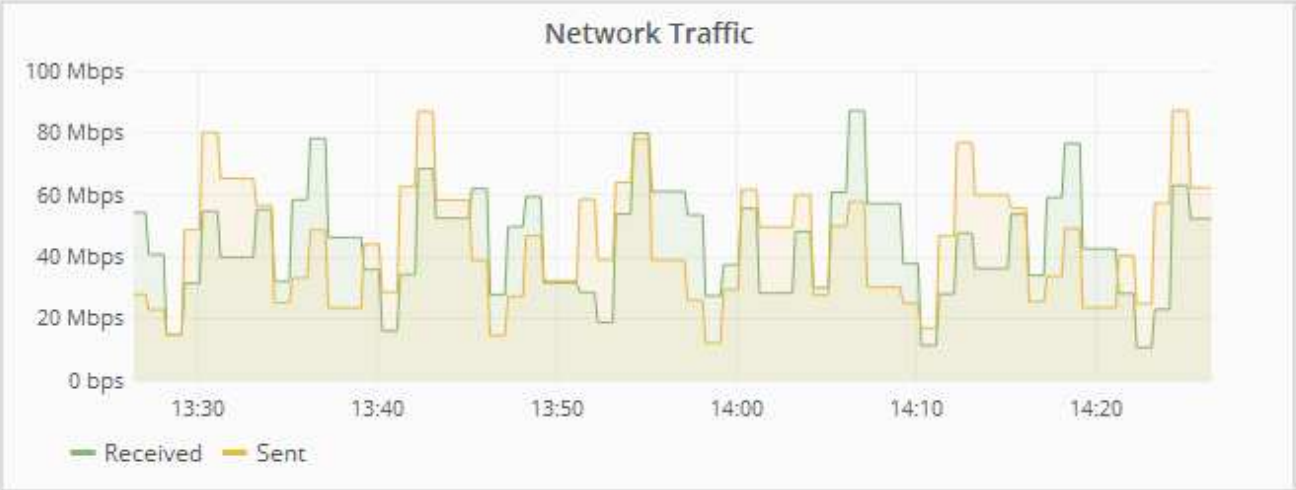
Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, mit dem Sie Datum und Zeitbereiche festlegen können.

Für Knoten bietet die Tabelle Netzwerkschnittstellen Informationen zu den physischen Netzwerkports jedes Node. Die Tabelle Netzwerkkommunikation enthält Details zu den Empfangs- und Übertragungsvorgängen jedes Knotens sowie zu den vom Treiber gemeldeten Fehlerzählern.

DC1-S1-226 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events

1 hour | 1 day | 1 week | 1 month | 1 year | Custom



Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	00:50:56:A8:2A:75	10 Gigabit	Full	Off	Up

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	738.858 GB	904,587,345	0	14,340	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	677.555 GB	465,715,998	0	0	0	0

Verwandte Informationen

"Monitoring von Netzwerkverbindungen und Performance"

Anzeigen der Registerkarte „Speicher“

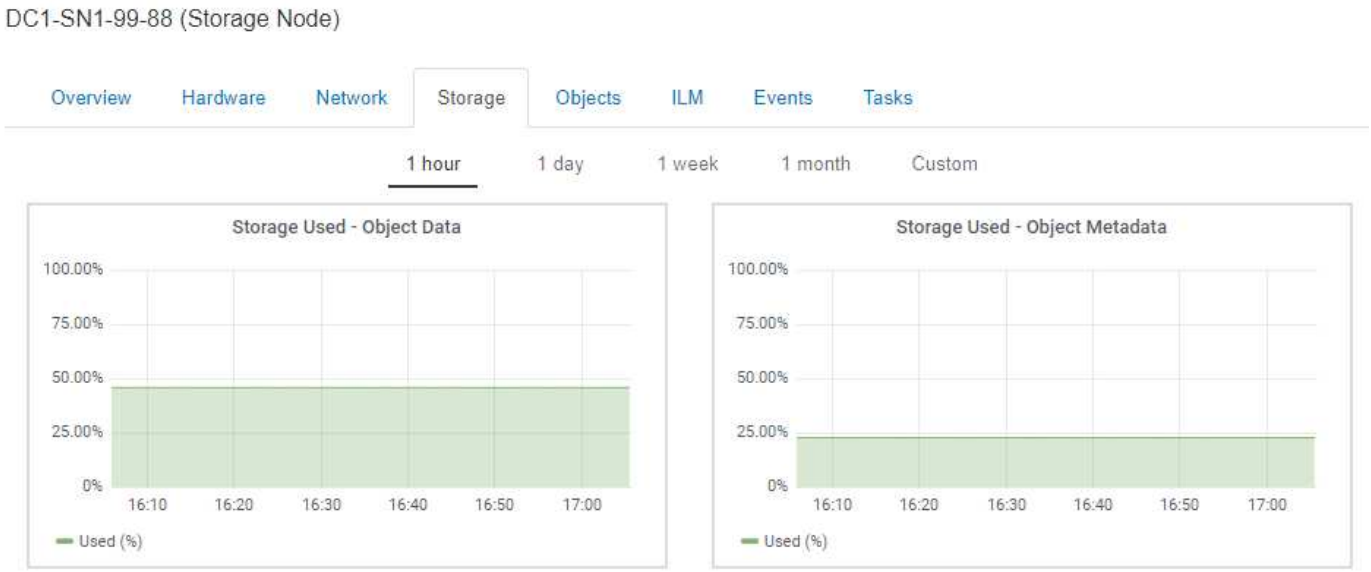
Die Registerkarte „Storage“ fasst Storage-Verfügbarkeit und andere Storage-Metriken zusammen.

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

Verwendete Diagramme im Storage

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

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



Festplattengeräte, Volumes und Objektspeichertabellen

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

Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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

"Überwachung der Storage-Kapazität für das gesamte Grid"

"Monitoring der Storage-Kapazität für jeden Storage-Node"

"Monitoring der Objekt-Metadaten-Kapazität für jeden Storage Node"

Anzeigen der Registerkarte Ereignisse

Auf der Registerkarte Ereignisse wird die Anzahl der Systemfehler oder Fehlerereignisse für einen Node angezeigt, einschließlich der Fehler, z. B. Netzwerkfehler.

Die Registerkarte Ereignisse wird für alle Nodes angezeigt.

Wenn Probleme mit einem bestimmten Knoten auftreten, erfahren Sie auf der Registerkarte Ereignisse mehr über das Problem. Der technische Support kann auch die Informationen auf der Registerkarte Ereignisse verwenden, um Ihnen bei der Fehlerbehebung zu helfen.

Sie können diese Aufgaben über die Registerkarte Ereignisse ausführen:

- Verwenden Sie die Informationen aus dem Feld **Letztes Ereignis** oben in der Tabelle, um festzustellen, welches Ereignis zuletzt aufgetreten ist.
- Klicken Sie auf das Diagrammsymbol Für ein bestimmtes Ereignis, um zu sehen, wann dieses Ereignis im Laufe der Zeit aufgetreten ist.

- Zurücksetzen der Ereignisanzahl auf Null nach Behebung von Problemen.

Verwandte Informationen

"Monitoring von Ereignissen"

"Anzeigen von Diagrammen und Diagrammen"

"Ereignisanzahl wird zurückgesetzt"

Verwenden der Registerkarte Task zum Neustart eines Grid-Knotens

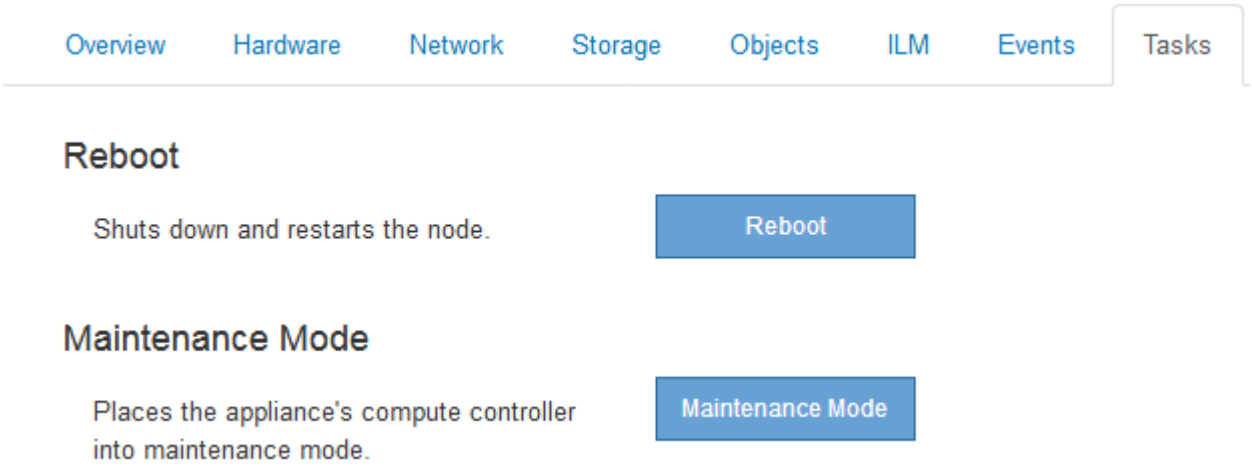
Auf der Registerkarte Task können Sie den ausgewählten Knoten neu starten. Die Registerkarte Task wird für alle Knoten angezeigt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Über diese Aufgabe

Auf der Registerkarte Task können Sie einen Knoten neu starten. Für Geräteknoten können Sie die Registerkarte Aufgabe auch verwenden, um das Gerät in den Wartungsmodus zu versetzen.



- Beim Neubooten eines Grid-Node auf der Registerkarte Task wird der Befehl zum Neubooten auf dem Ziel-Node ausgegeben. Beim Neubooten eines Node wird der Node heruntergefahren und neu gestartet. Alle Dienste werden automatisch neu gestartet.

  Wenn Sie einen Storage-Node neu booten möchten, beachten Sie Folgendes:

  - Wenn eine ILM-Regel ein Aufnahmeverhalten von Dual-Commit angibt oder die Regel einen Ausgleich angibt und nicht sofort alle erforderlichen Kopien erstellen kann, werden neu aufgenommenen Objekte sofort von StorageGRID auf zwei Storage-Nodes am selben Standort übertragen und ILM wird später ausgewertet. Wenn Sie zwei oder mehr Storage-Nodes an einem bestimmten Standort neu starten möchten, können Sie während des Neustarts möglicherweise nicht auf diese Objekte zugreifen.
  - Um sicherzustellen, dass Sie während des Neubootens eines Storage-Node auf alle Objekte zugreifen können, beenden Sie die Verarbeitung von Objekten an einem Standort etwa eine Stunde lang, bevor

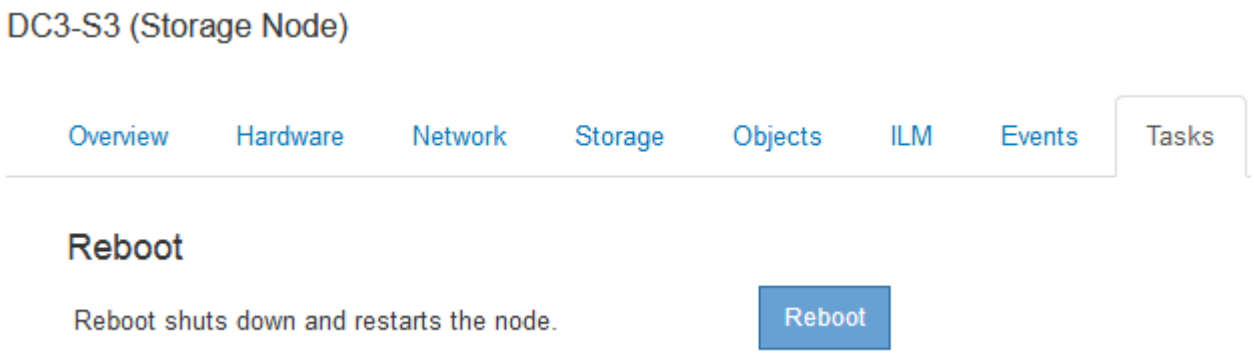
Sie den Node neu booten.

- Möglicherweise müssen Sie eine StorageGRID Appliance in den Wartungsmodus versetzen, um bestimmte Verfahren durchzuführen, z. B. das Ändern der Link-Konfiguration oder den Austausch eines Storage Controllers. Anweisungen hierzu finden Sie in der Installations- und Wartungsanleitung für das Gerät.

> Wenn Sie eine Appliance in den Wartungsmodus versetzen, ist das Gerät möglicherweise für den Remote-Zugriff nicht verfügbar.

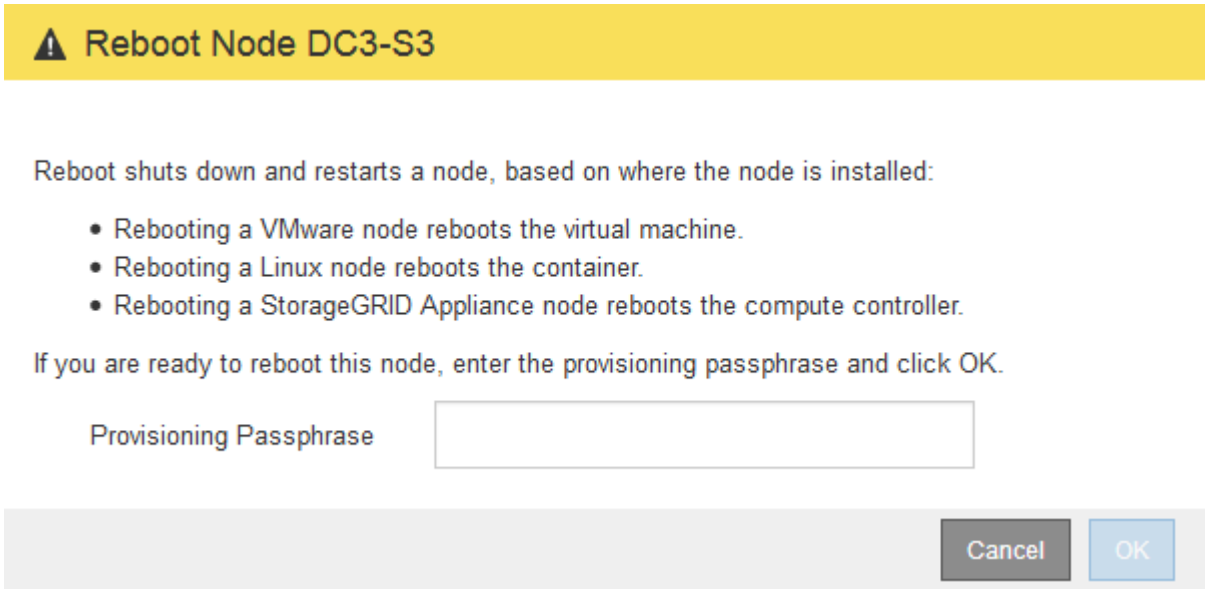
Schritte

1. Wählen Sie **Knoten**.
2. Wählen Sie den Grid-Node aus, den Sie neu booten möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.



4. Klicken Sie Auf **Neustart**.

Ein Bestätigungsdialogfeld wird angezeigt.



> Wenn Sie den primären Admin-Knoten neu starten, wird im Bestätigungsdialogfeld darauf hingewiesen, dass die Verbindung Ihres Browsers zum Grid Manager vorübergehend verloren geht, wenn Dienste beendet werden.

5. Geben Sie die Provisionierungs-Passphrase ein, und klicken Sie auf **OK**.
6. Warten Sie, bis der Node neu gebootet wird.

   Es kann einige Zeit dauern, bis Dienste heruntergefahren werden.

   Wenn der Knoten neu gestartet wird, wird das graue Symbol (Administrativ Down) auf der linken Seite der Seite Knoten angezeigt. Wenn alle Dienste wieder gestartet wurden, ändert sich das Symbol wieder in seine ursprüngliche Farbe.

Verwandte Informationen

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

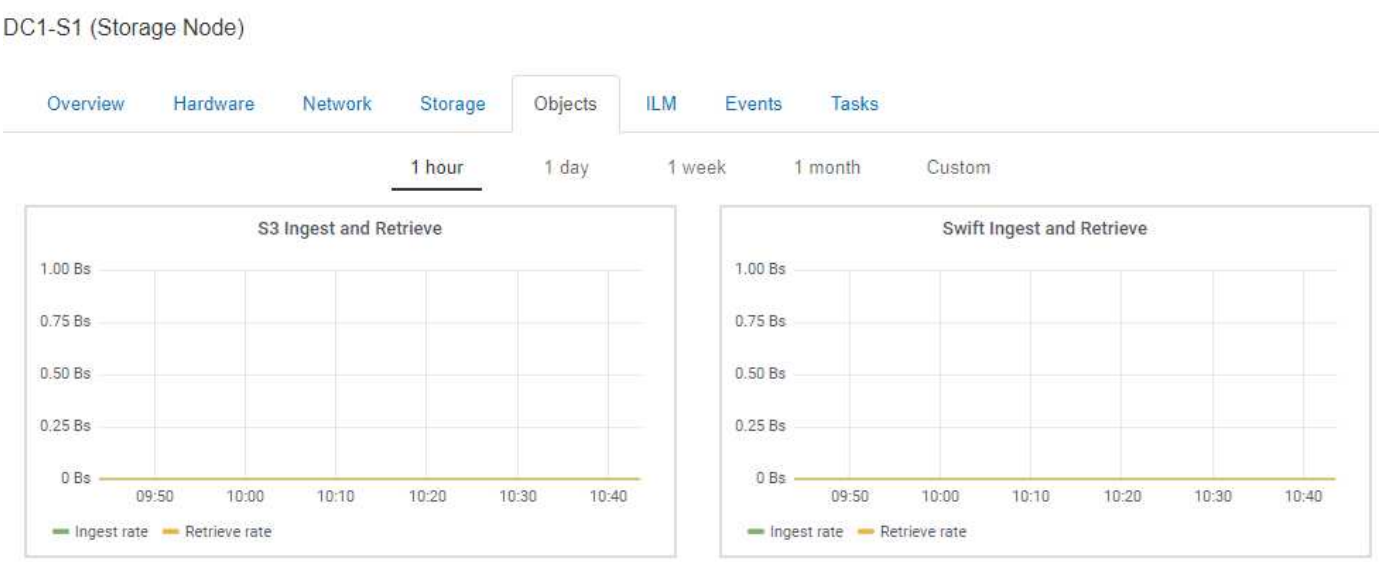
"SG5600 Storage Appliances"

"SG100 SG1000 Services-Appliances"

Anzeigen der Registerkarte Objekte

Die Registerkarte „Objekte“ bietet Informationen zur Aufnahme- und Abrufrate von S3 und Swift.

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



Object Counts

Total Objects	0
Lost Objects	0
S3 Buckets and Swift Containers	0

Queries

Average Latency	5.74 milliseconds
Queries - Successful	12,403
Queries - Failed (timed-out)	0
Queries - Failed (consistency level unmet)	0

Verification

Status	No Errors
Rate Setting	Adaptive
Percent Complete	0.00%
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

Verwandte Informationen

"S3 verwenden"

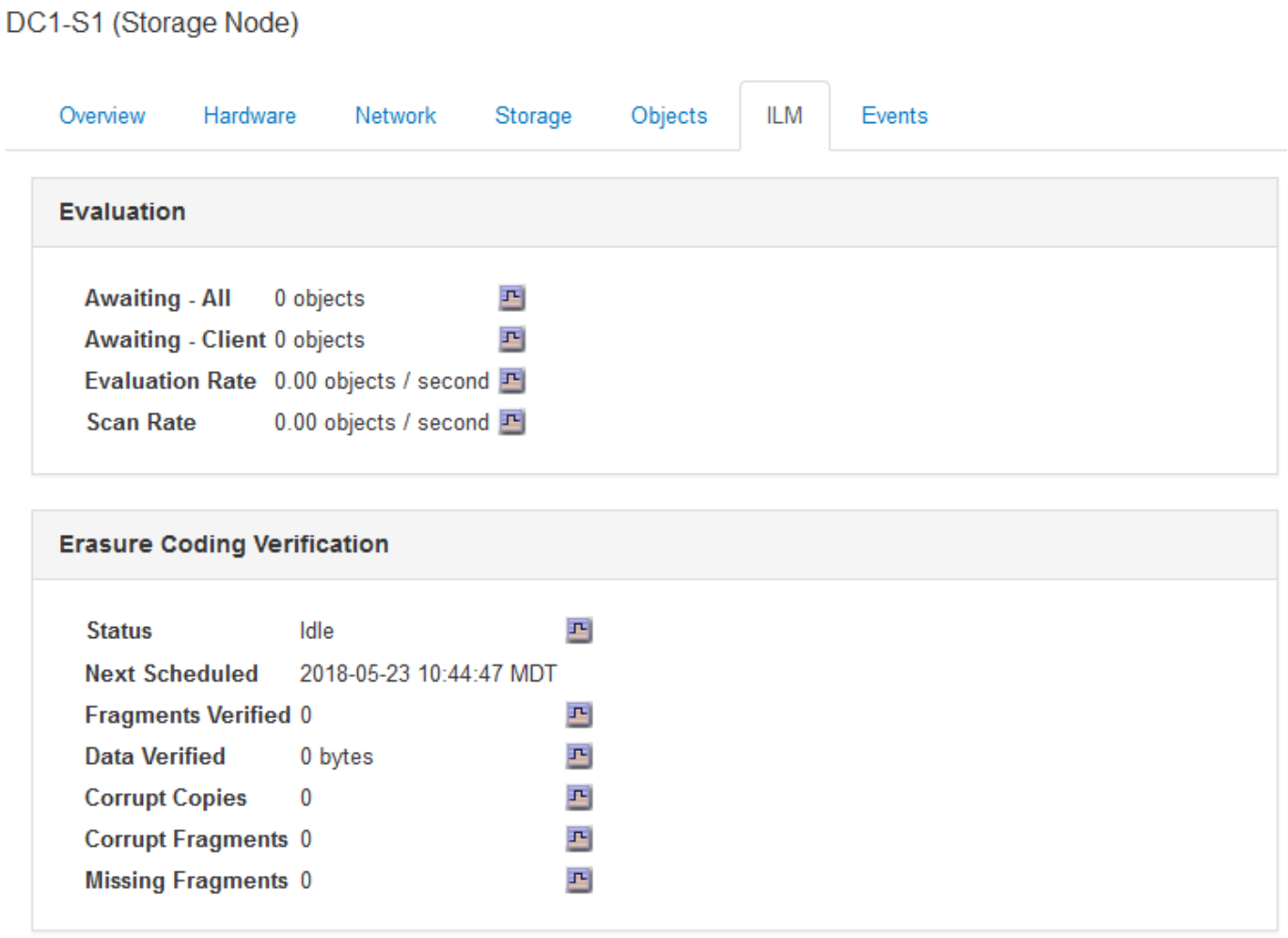
"Verwenden Sie Swift"

Anzeigen der Registerkarte ILM

Die Registerkarte ILM enthält Informationen zu ILM-Vorgängen (Information Lifecycle Management).

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

Für Storage-Nodes bietet die Registerkarte ILM Details zur ILM-Bewertung und zur Hintergrundüberprüfung codierten Objekten.



Verwandte Informationen

"Überwachung des Information Lifecycle Management"

"StorageGRID verwalten"

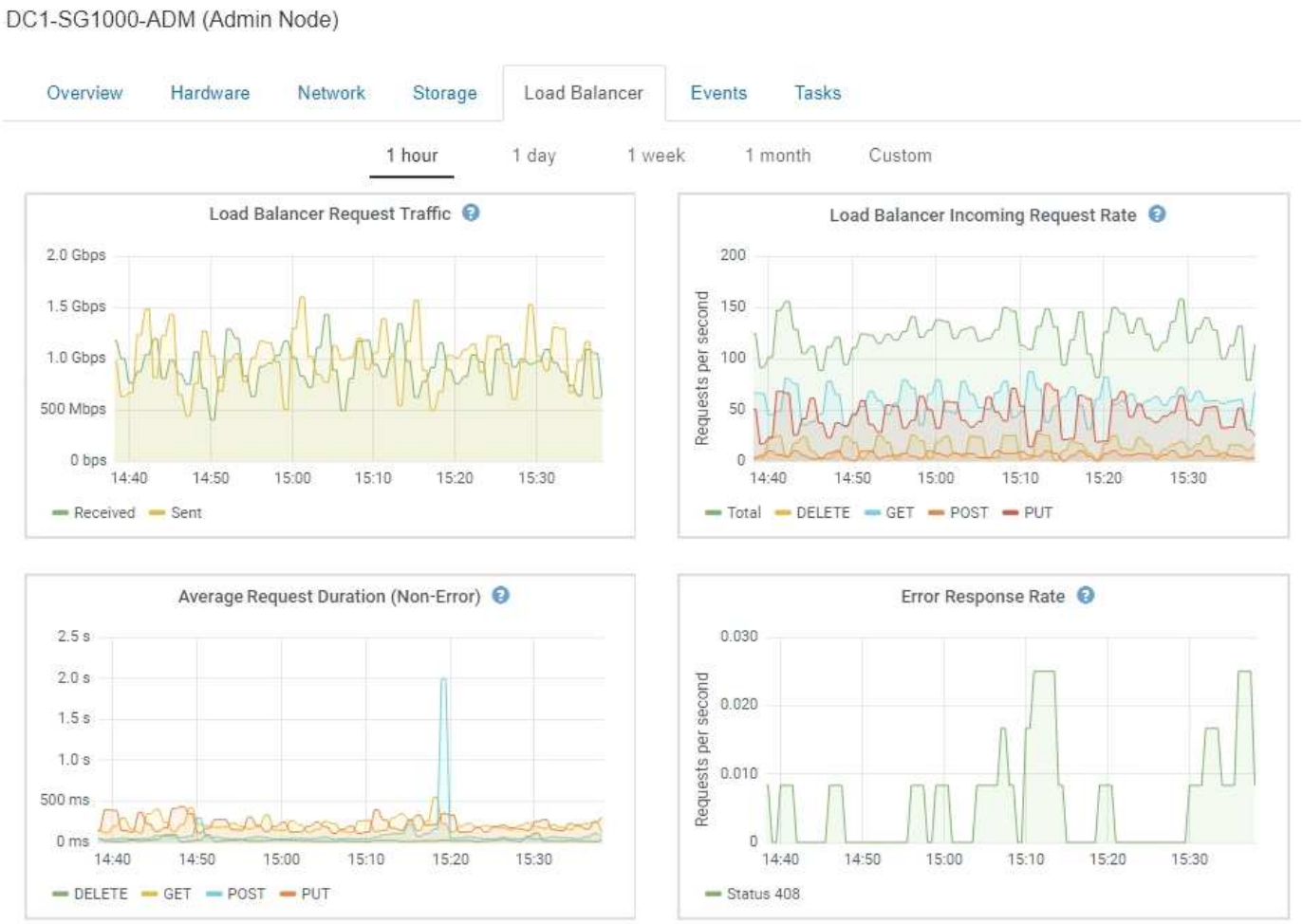
Anzeigen der Registerkarte Load Balancer

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

Die Registerkarte Load Balancer wird für Admin-Nodes und Gateway-Nodes, jeden Standort und das gesamte

Raster angezeigt. Die Registerkarte Load Balancer bietet für jeden Standort eine zusammengefasste Zusammenfassung der Statistiken für alle Nodes an diesem Standort. Die Registerkarte Load Balancer bietet für das gesamte Raster eine zusammengefasste Zusammenfassung der Statistiken für alle Standorte.

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



Traffic Für Lastausgleichsanfragen

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

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

Eingehende Anfragerate Für Den Lastausgleich Des Balancer

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

Durchschnittliche Anfragendauer (Ohne Fehler)

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

Fehlerreaktionsrate

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

Verwandte Informationen

"Monitoring von Lastverteilungsvorgängen"

"StorageGRID verwalten"

Registerkarte Plattformdienste anzeigen

Die Registerkarte Platform Services enthält Informationen zu allen S3-Plattform-Servicevorgängen an einem Standort.

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

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

Verwandte Informationen

"StorageGRID verwalten"

Anzeigen von Informationen zu Appliance-Speicherknoten

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

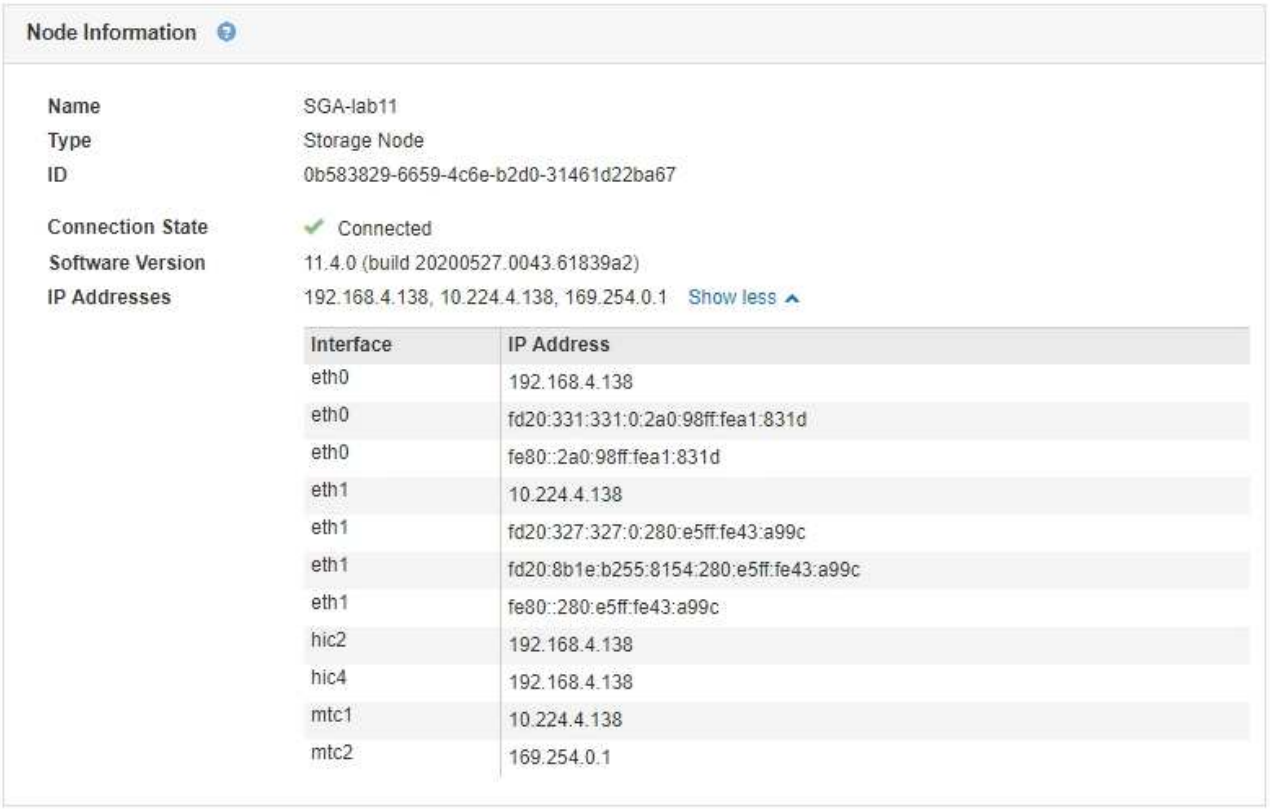
Controller-Firmware-Version, Netzwerkressourcen, Netzwerkschnittstellen, Netzwerkadressen und empfangen und übertragen Daten.

Schritte

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

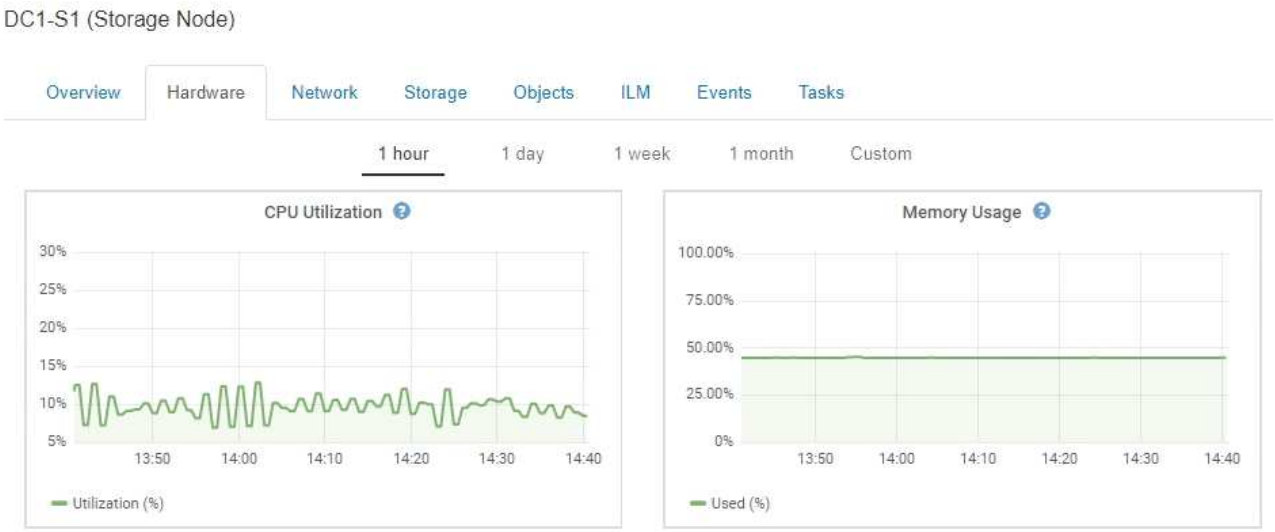
   In der Tabelle Node Information auf der Registerkarte Übersicht werden die ID und der Name des Node, der Node-Typ, die installierte Softwareversion und die dem Node zugeordneten IP-Adressen angezeigt. Die Spalte Interface enthält den Namen der Schnittstelle wie folgt:

   - **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk.
   - **Hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID-Grid-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
   - **mtc**: Einer der physischen 1-GbE-Ports auf der Appliance, die mit dem StorageGRID Admin Network (eth1) verbunden oder kalibriert und verbunden werden können.



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

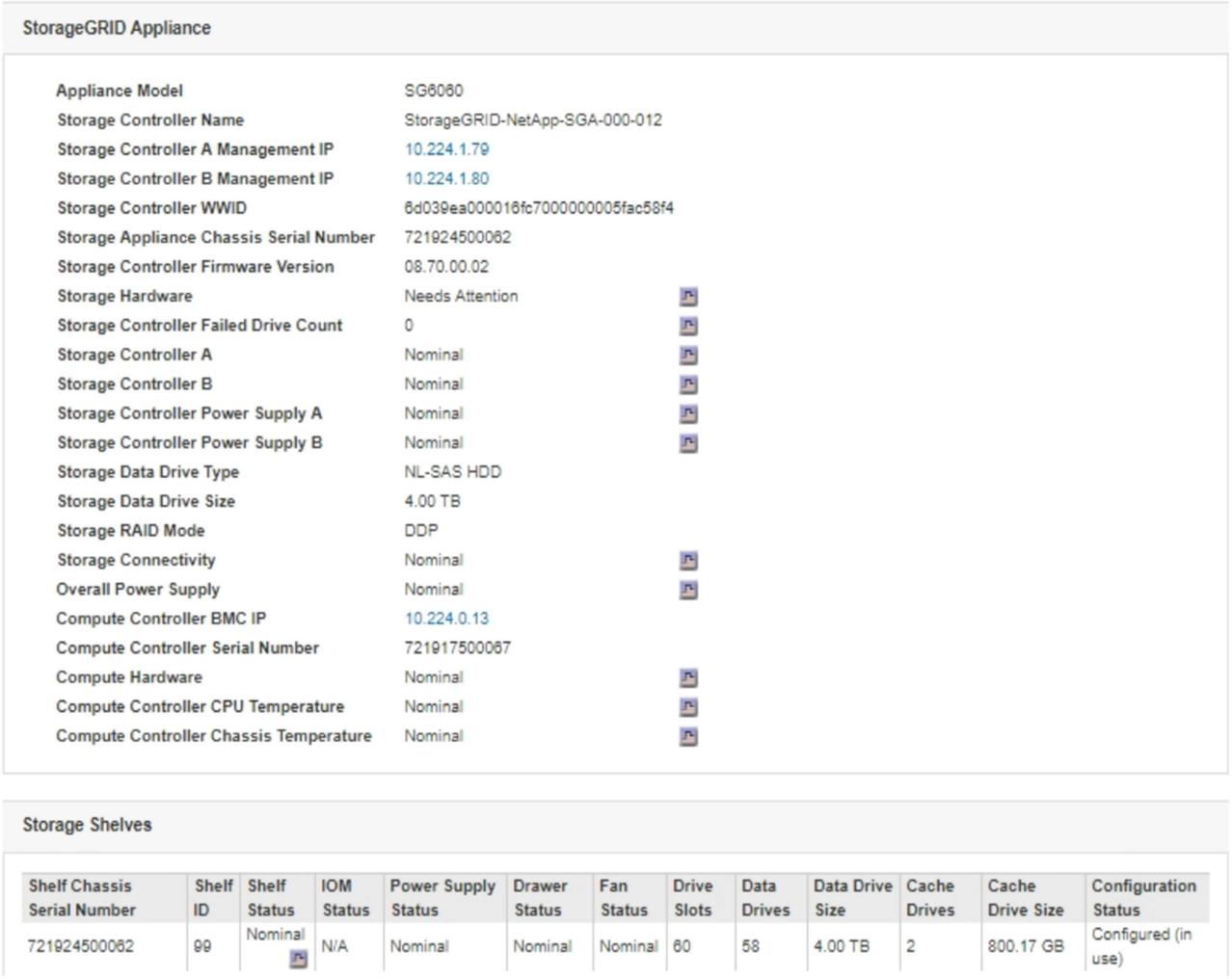
   a. Sehen Sie sich die CPU-Auslastung und die Speicherdiagramme an, um den Prozentsatz der CPU- und Arbeitsspeicherauslastung im Laufe der Zeit zu ermitteln. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren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



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

> Einige Felder, wie BMC IP und Compute Hardware, werden nur für Geräte mit dieser Funktion angezeigt.

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



Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer dieser StorageGRID Appliance, dargestellt in der SANtricity Software.
Storage Controller-Name	Der Name dieser in der SANtricity Software angezeigten StorageGRID Appliance.
Storage Controller A Management-IP	IP-Adresse für Management Port 1 auf Storage Controller A Sie verwenden diese IP für den Zugriff auf die SANtricity Software zur Fehlerbehebung bei Speicherproblemen.
Storage Controller B Management-IP	IP-Adresse für Management Port 1 auf Storage Controller B Sie verwenden diese IP für den Zugriff auf die SANtricity Software zur Fehlerbehebung bei Speicherproblemen. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B

Feld in der Appliance-Tabelle	Beschreibung
WWID des Storage Controller	Die weltweite Kennung des Storage-Controllers in der SANtricity Software.
Seriennummer Des Storage Appliance Chassis	Die Seriennummer des Gehäuses des Geräts.
Firmware-Version Des Speicher-Controllers	Die Version der Firmware auf dem Storage Controller für dieses Gerät.
Storage-Hardware	Der Gesamtstatus der Hardware des Storage Controllers. Wenn SANtricity System Manager einen Status als Warnung für die Storage-Hardware meldet, meldet das StorageGRID System diesen Wert ebenfalls. Wenn der Status „`Anforderungen einer Warnung erfüllt,`“ zunächst den Storage Controller mithilfe der SANtricity Software prüfen. Stellen Sie dann sicher, dass keine weiteren Alarme vorhanden sind, die für den Rechencontroller gelten.
Anzahl Ausgefallener Speicher-Controller-Laufwerke	Anzahl an Laufwerken, die nicht optimal sind.
Storage Controller A	Der Status von Speicher-Controller A.
Storage Controller B	Der Status von Storage Controller B. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B
Netzteil A für Speichercontroller	Der Status von Netzteil A für den Storage Controller.
Speicher-Controller-Netzteil B	Der Status von Netzteil B für den Speicher-Controller.
Typ Des Storage-Datenlaufwerks	Die Art der Laufwerke in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe Der Speicherdatenlaufwerke	Gesamtkapazität einschließlich aller Datenlaufwerke in der Appliance.
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.
Storage-Konnektivität	Der Status der Storage-Konnektivität.

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

+

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

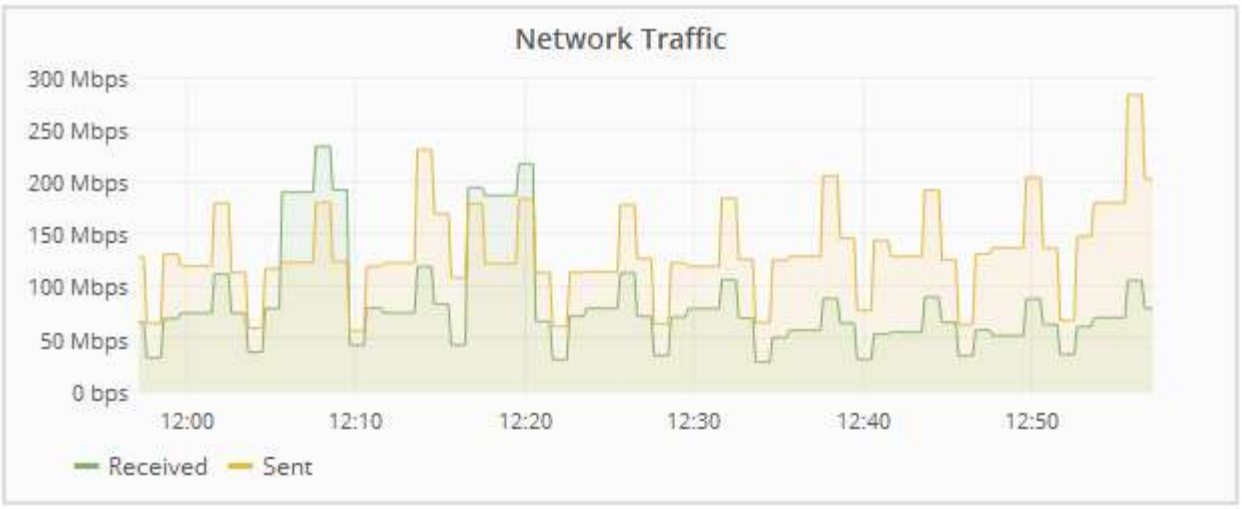
Spalte in der Tabelle „Storage Shelfs“	Beschreibung
Netzteilstatus	Der Gesamtstatus der Netzteile für das Storage Shelf.
Status Der Schublade	Der Zustand der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Lüfter im Storage Shelf.
Laufwerksteckplätze	Die Gesamtzahl der Laufwerksschächte im Storage-Shelf.
Datenlaufwerke	Die Anzahl der Laufwerke im Storage Shelf, die für den Datenspeicher verwendet werden.
Größe Des Datenlaufwerks	Die effektive Größe eines Datenlaufwerks im Storage Shelf.
Cache-Laufwerke	Die Anzahl der Laufwerke im Storage Shelf, die als Cache verwendet werden.
Größe Des Cache-Laufwerks	Die Größe des kleinsten Cache-Laufwerks im Storage-Shelf. Normalerweise haben Cache-Laufwerke dieselbe Größe.
Konfigurationsstatus	Der Konfigurationsstatus des Storage Shelf.

4. Bestätigen Sie, dass alle Status „`Nominal`“ sind.

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

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

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



a. Lesen Sie den Abschnitt Netzwerkschnittstellen.

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

Verwenden Sie die folgende Tabelle mit den Werten in der Spalte **Geschwindigkeit** in der Tabelle Netzwerkschnittstellen, um festzustellen, ob die 10/25-GbE-Netzwerkanschlüsse auf dem Gerät für den aktiven/Backup-Modus oder den LACP-Modus konfiguriert wurden.

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

Verbindungsmodus	Bond-Modus	Einzelne HIC-Verbindungsgeschwindigkeit (Schluck1, 2, Schluck3, Schluck4)	Erwartete Grid-/Client-Netzwerkgeschwindigkeit (eth0,eth2)
Aggregat	LACP	25	100

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

Weitere Informationen zur Konfiguration der 10/25-GbE-Ports finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

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

Network Communication

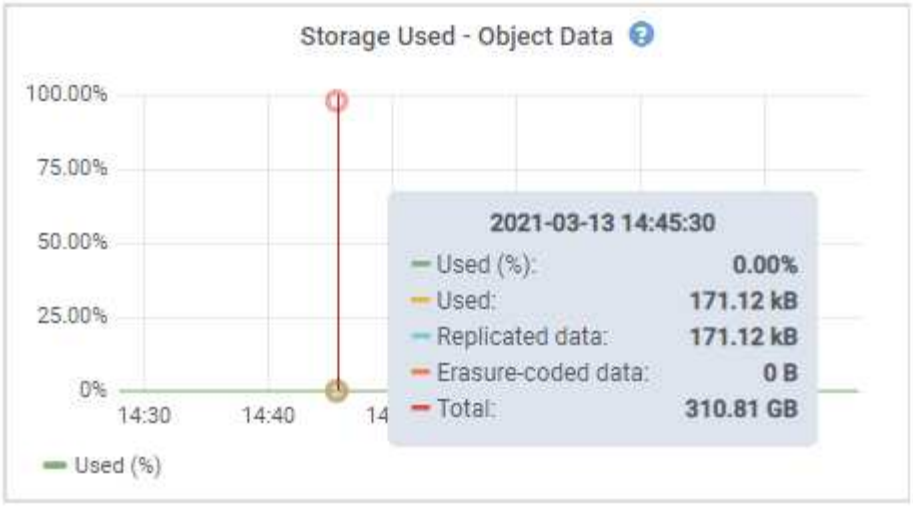
Receive

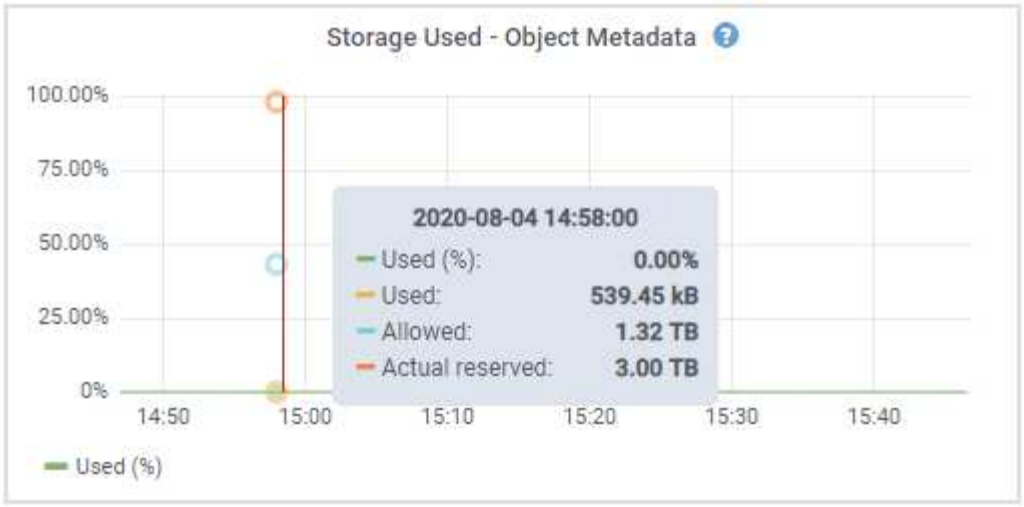
Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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

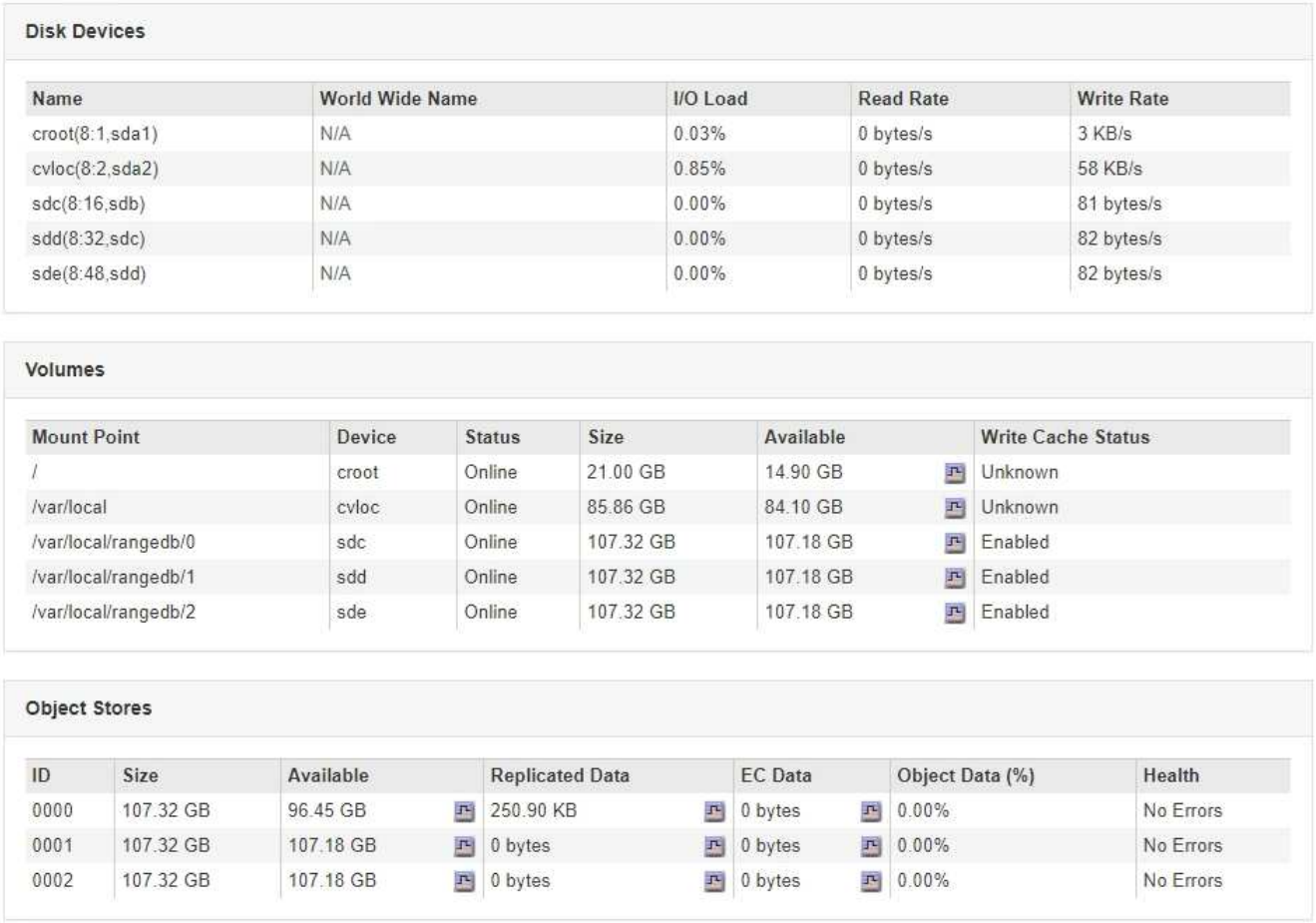




a. Blättern Sie nach unten, um die verfügbaren Speichermengen für jedes Volume und jeden Objektspeicher anzuzeigen.

   Der weltweite Name jeder Festplatte entspricht der World-Wide Identifier (WWID) des Volumes, die angezeigt wird, wenn Sie die standardmäßigen Volume-Eigenschaften in der SANtricity Software anzeigen (die Management-Software, die mit dem Storage Controller der Appliance verbunden ist).

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



Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 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

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Anzeigen der Registerkarte SANtricity System Manager

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

Die Registerkarte SANtricity System Manager wird für Storage-Appliance-Nodes angezeigt.

Mit SANtricity System Manager sind folgende Vorgänge möglich:

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

So konfigurieren Sie mit SANtricity System Manager einen Proxy für E-Series AutoSupport: Lesen Sie die Anweisungen in Administration StorageGRID.

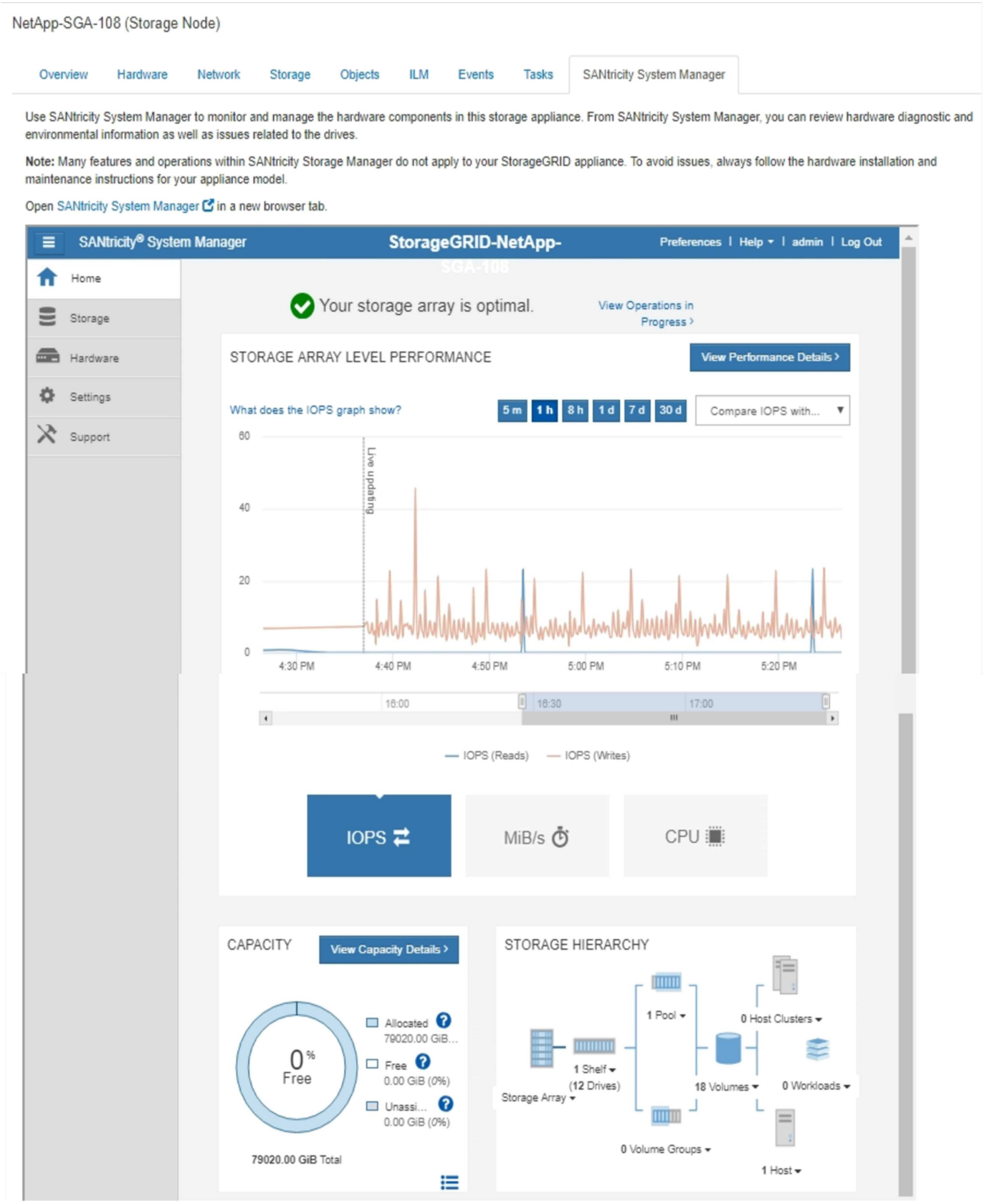
"StorageGRID verwalten"

Um über den Grid Manager auf SANtricity System Manager zuzugreifen, müssen Sie über die Administratorberechtigung für die Speicheranwendung oder über die Berechtigung für den Root-Zugriff verfügen.

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

Der Zugriff auf den SANtricity System Manager über den Grid Manager erlaubt in der Regel nur die Überwachung der Appliance-Hardware und die Konfiguration der E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring Ihrer StorageGRID Appliance. Um Probleme zu vermeiden, befolgen Sie immer die Hardware-Installations- und Wartungsanweisungen für Ihr Gerät.

Die Registerkarte zeigt die Startseite von SANtricity System Manager an



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

Wenn Sie Details zur Performance und Kapazitätsauslastung des Storage Array anzeigen möchten, halten Sie

den Mauszeiger über jedes Diagramm.

Weitere Informationen zum Anzeigen der Informationen, auf die über die Registerkarte SANtricity System Manager zugegriffen werden kann, finden Sie in den Informationen in "NetApp E-Series Systems Documentation Center"

Anzeigen von Informationen zu Appliance Admin Nodes und Gateway Nodes

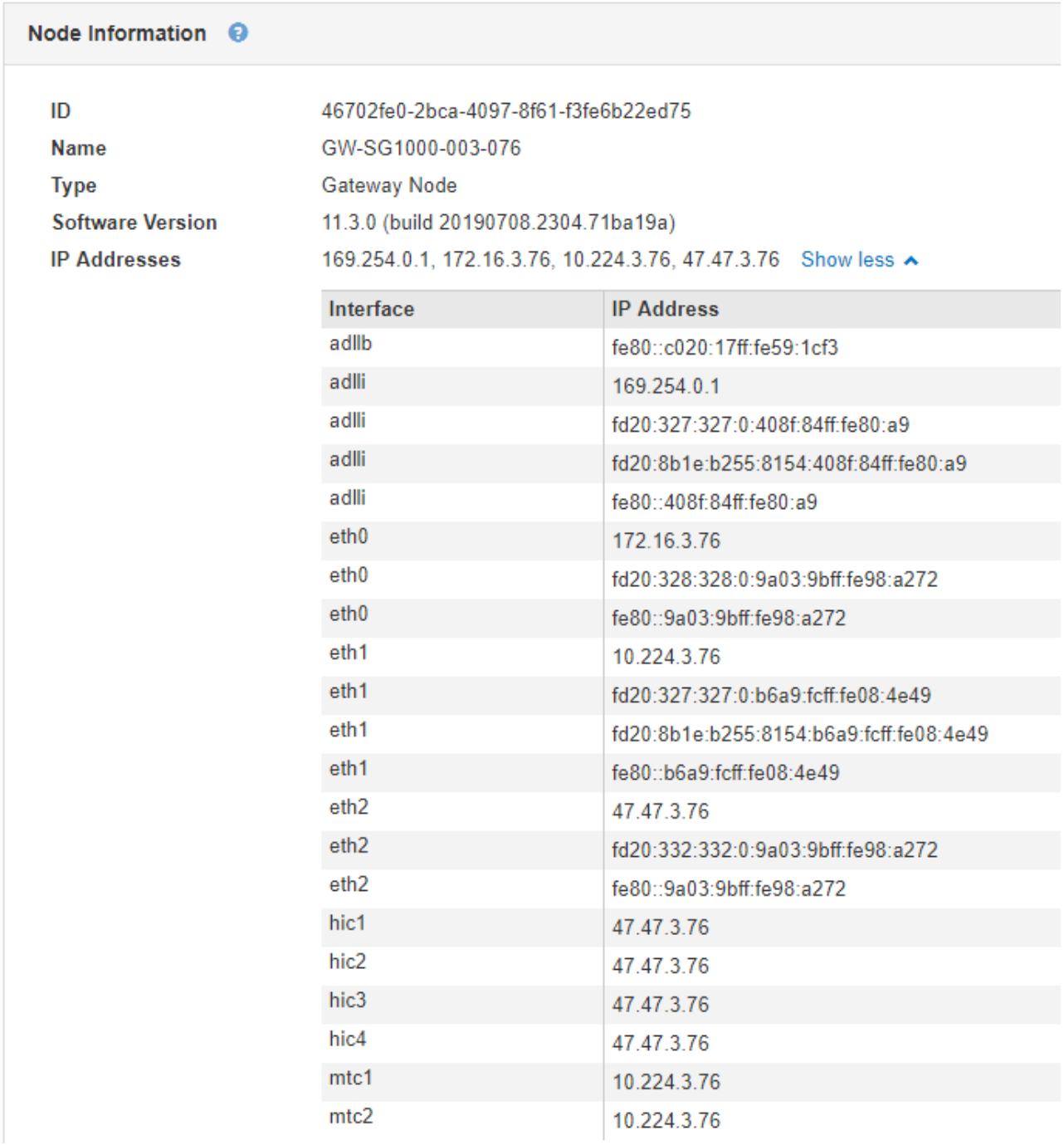
Auf der Seite Nodes werden Informationen zum Serviczustand sowie alle Computing-, Festplatten- und Netzwerkressourcen für jede Service-Appliance, die für einen Admin-Node oder einen Gateway-Node verwendet wird, aufgeführt. Außerdem können Sie Arbeitsspeicher, Storage-Hardware, Netzwerkressourcen, Netzwerkschnittstellen,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

Schritte

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

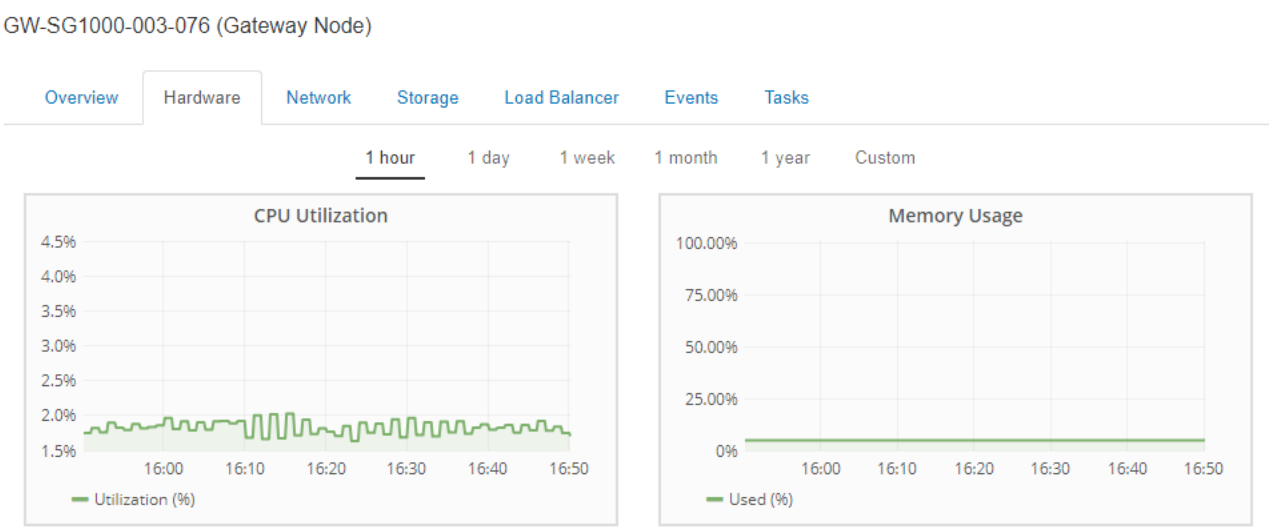
   In der Tabelle Node Information auf der Registerkarte Übersicht werden die ID und der Name des Node, der Node-Typ, die installierte Softwareversion und die dem Node zugeordneten IP-Adressen angezeigt. Die Spalte Interface enthält den Namen der Schnittstelle wie folgt:

   - **Adlb** und **adlli**: Wird angezeigt, wenn Active/Backup Bonding für die Admin Network Interface verwendet wird
   - **eth**: Das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk.
   - **Hic**: Einer der physischen 10-, 25- oder 100-GbE-Ports auf dem Gerät. Diese Ports können miteinander verbunden und mit dem StorageGRID-Grid-Netzwerk (eth0) und dem Client-Netzwerk (eth2) verbunden werden.
   - **mtc**: Einer der physischen 1-GbE-Ports auf der Appliance, die mit dem StorageGRID Admin Network (eth1) verbunden oder kalibriert und verbunden werden können.

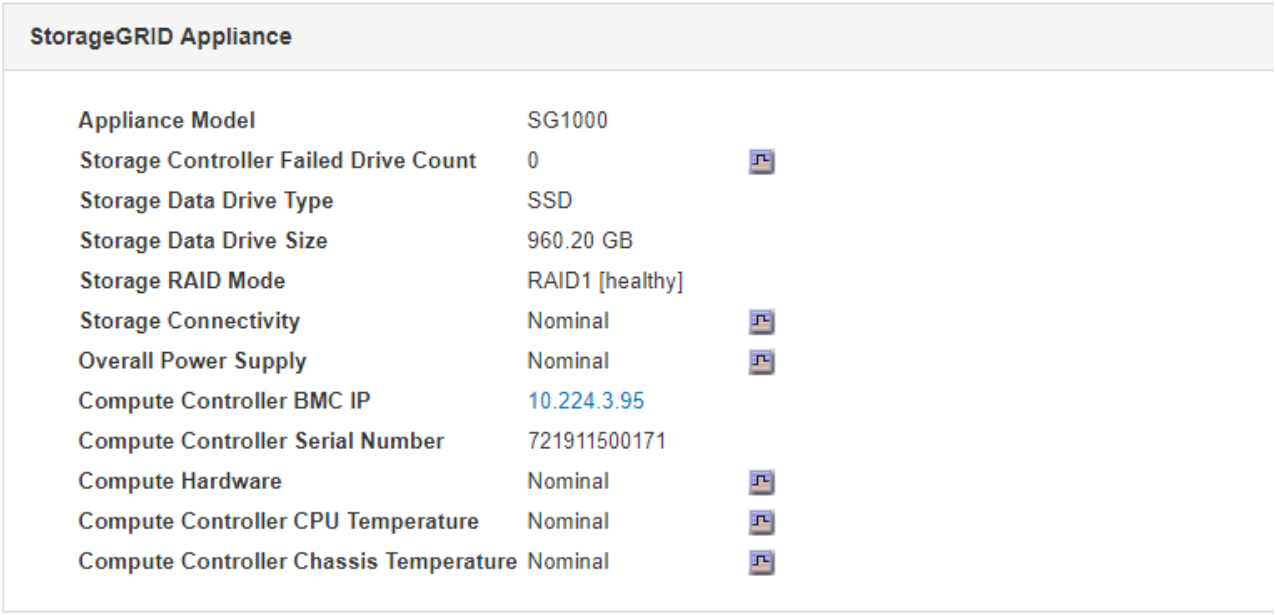


3. Wählen Sie **Hardware**, um weitere Informationen über das Gerät anzuzeigen.

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



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



Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer für diese StorageGRID Appliance.
Anzahl Ausgefallener Speicher-Controller-Laufwerke	Anzahl an Laufwerken, die nicht optimal sind.
Typ Des Storage-Datenlaufwerks	Die Art der Laufwerke in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe Der Speicherdatenlaufwerke	Gesamtkapazität einschließlich aller Datenlaufwerke in der Appliance.

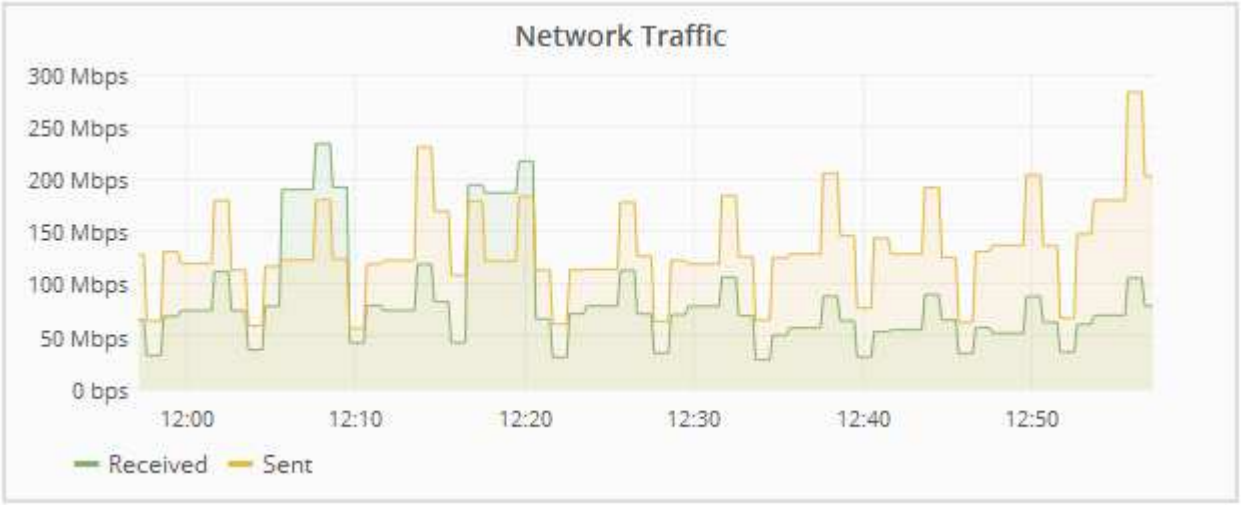
Feld in der Appliance-Tabelle	Beschreibung
Storage RAID-Modus	Der RAID-Modus für die Appliance.
Gesamtnetzteil	Der Status aller Netzteile im Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie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

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

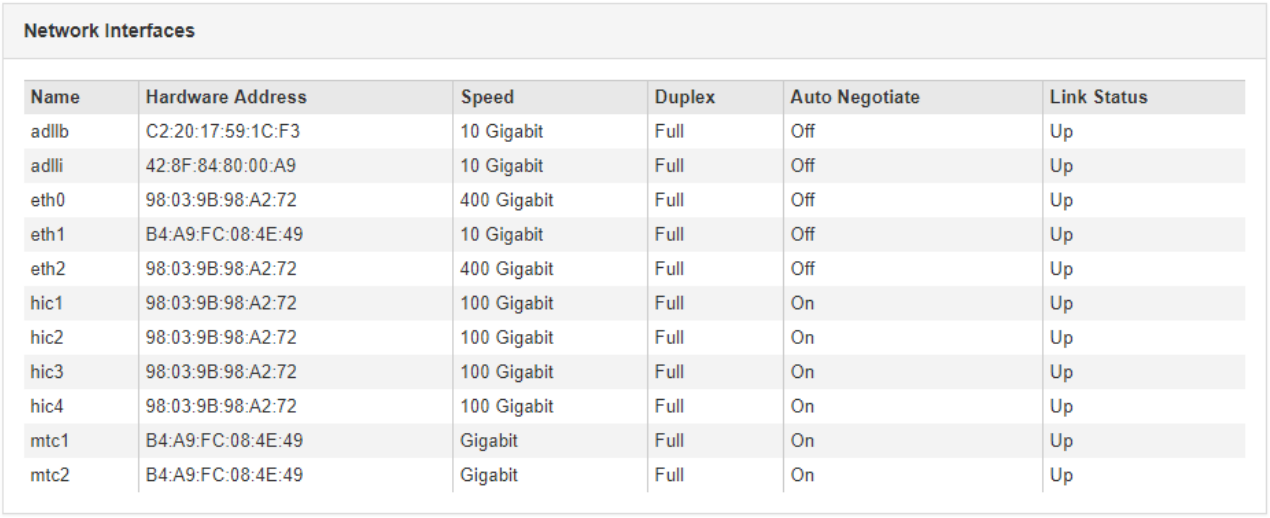
   Wenn der Status nicht „`Nominal`“ lautet, überprüfen Sie alle aktuellen Warnmeldungen.

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

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



a. Lesen Sie den Abschnitt Netzwerkschnittstellen.



Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
adllb	C2:20:17:59:1C:F3	10 Gigabit	Full	Off	Up
adlli	42:8F:84:80:00:A9	10 Gigabit	Full	Off	Up
eth0	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
eth1	B4:A9:FC:08:4E:49	10 Gigabit	Full	Off	Up
eth2	98:03:9B:98:A2:72	400 Gigabit	Full	Off	Up
hic1	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic2	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic3	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
hic4	98:03:9B:98:A2:72	100 Gigabit	Full	On	Up
mtc1	B4:A9:FC:08:4E:49	Gigabit	Full	On	Up
mtc2	B4:A9:FC:08:4E:49	Gigabit	Full	On	Up

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

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

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

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

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

Network Communication

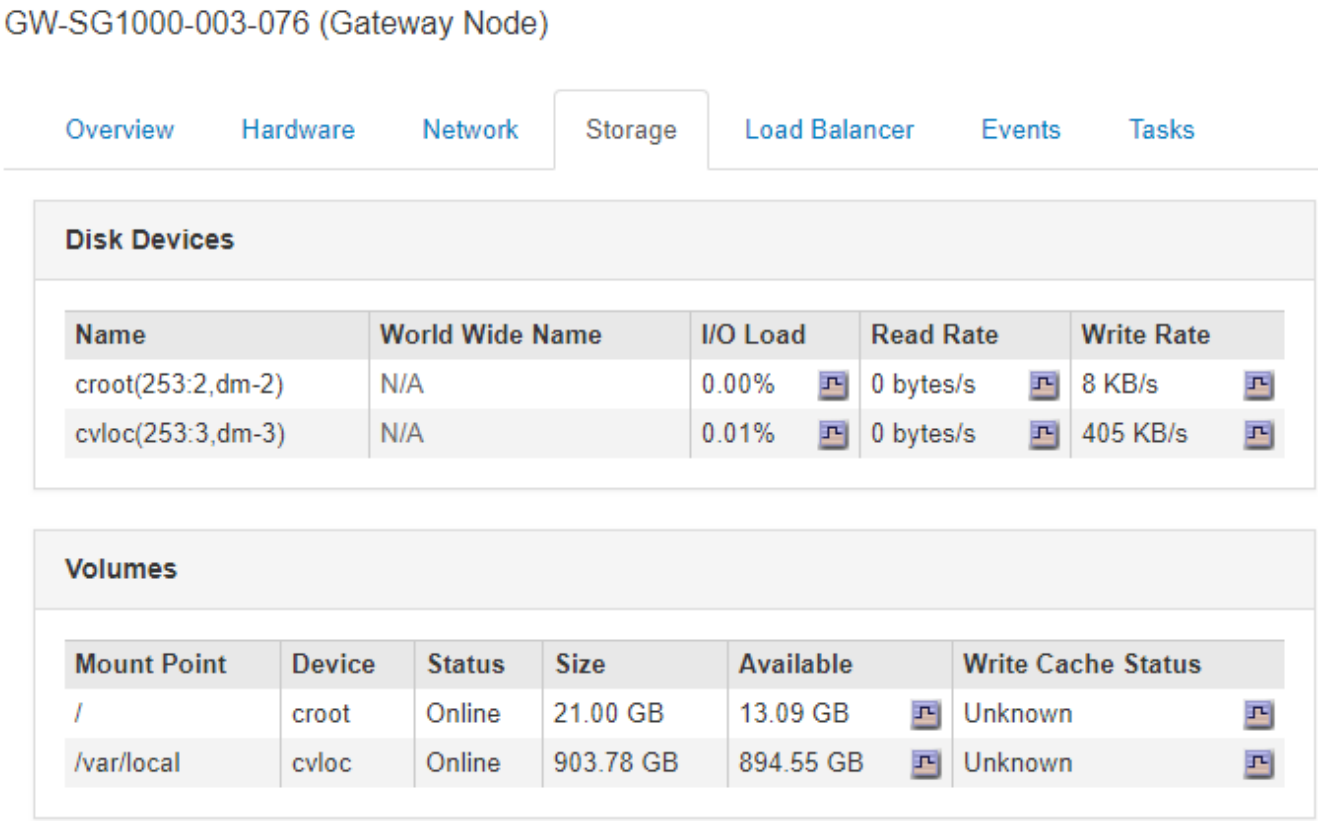
Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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



Verwandte Informationen

"SG100 SG1000 Services-Appliances"

Informationen, die Sie regelmäßig überwachen sollten

StorageGRID ist ein fehlertolerantes, verteiltes Storage-System, das den Betrieb selbst bei Fehlern oder Nichtverfügbarkeit von Nodes oder Standorten unterstützt. Sie müssen den Systemzustand, die Workloads und die Nutzungsstatistiken proaktiv überwachen, damit Sie Maßnahmen ergreifen können, um potenzielle Probleme zu beheben, bevor sie die Effizienz oder Verfügbarkeit des Grid beeinträchtigen.

Ein überlastetes System generiert große Datenmengen. Dieser Abschnitt enthält eine Anleitung zu den wichtigsten Informationen, die fortlaufend überwacht werden sollen. Dieser Abschnitt enthält die folgenden Unterabschnitte:

- "Monitoring des Systemzustands"
- "Monitoring der Storage-Kapazität"
- "Überwachung des Information Lifecycle Management"
- "Monitoring der Performance-, Netzwerk- und Systemressourcen"
- "Monitoring der Mandantenaktivitäten"
- "Monitoring der Archivierungskapazität"
- "Monitoring von Lastverteilungsvorgängen"
- "Anwenden von Hotfixes oder Aktualisieren der Software, falls erforderlich"

Was überwacht werden soll	Frequenz
Die Systemintegritätsdaten, die im Grid Manager DashboardHinweis angezeigt werden, wenn sich etwas vom vorherigen Tag geändert hat.	Täglich
Rate, mit welcher Objekt- und Metadatenkapazität des Storage-Node genutzt wird	Wöchentlich
Information Lifecycle Management-Operationen	Wöchentlich
Performance-, Netzwerk- und Systemressourcen: • Abfragelatenz • Konnektivität und Networking • Ressourcen auf Node-Ebene	Wöchentlich
Mandantenaktivität	Wöchentlich
Kapazität des externen Archiv-Storage-Systems	Wöchentlich
Lastverteilung	Nach der Erstkonfiguration und nach Konfigurationsänderungen
Verfügbarkeit von Software-Hotfixes und Software-Upgrades	Monatlich

Monitoring des Systemzustands

Sie sollten täglich den allgemeinen Zustand Ihres StorageGRID Systems überwachen.

Das StorageGRID System ist fehlertolerant und funktioniert weiterhin, wenn Teile des Grids nicht verfügbar sind. Das erste Anzeichen eines potenziellen Problems mit Ihrem StorageGRID System ist wahrscheinlich eine Warnmeldung oder ein Alarm (Legacy-System) und nicht unbedingt ein Problem beim Systembetrieb. Wenn Sie die Systemintegrität beachten, können Sie kleinere Probleme erkennen, bevor sie den Betrieb oder die Netzeffizienz beeinträchtigen.

Das Teilfenster „Systemzustand“ im Grid Manager Dashboard bietet eine Zusammenfassung von Problemen, die Ihr System möglicherweise beeinträchtigen. Sie sollten alle auf dem Dashboard angezeigten Probleme untersuchen.

> Damit Sie über Warnungen benachrichtigt werden können, sobald sie ausgelöst werden, können Sie E-Mail-Benachrichtigungen für Warnungen einrichten oder SNMP-Traps konfigurieren.

1. Melden Sie sich beim Grid Manager an, um das Dashboard anzuzeigen.
2. Überprüfen Sie die Informationen im Bedienfeld „Systemzustand“.

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

Verlinken	Zeigt An
Grid-Details	Wird angezeigt, wenn Knoten getrennt sind (Verbindungsstatus unbekannt oder Administrativ ausgefallen). Klicken Sie auf den Link oder klicken Sie auf das blaue oder graue Symbol, um zu ermitteln, welche Nodes betroffen sind.
Aktuelle Meldungen	Wird angezeigt, wenn derzeit Meldungen aktiv sind. Klicken Sie auf den Link oder klicken Sie auf **kritisch**, **Major** oder **Minor**, um die Details auf der Seite **Alarme** > **Aktuell** anzuzeigen.
Kürzlich behobene Warnmeldungen	Wird angezeigt, wenn in der letzten Woche ausgelöste Benachrichtigungen jetzt behoben sind. Klicken Sie auf den Link, um die Details auf der Seite **Alerts** > **aufgelöst** anzuzeigen.
Ältere Alarme	Wird angezeigt, wenn derzeit Alarme (Legacy-System) aktiv sind. Klicken Sie auf den Link, um die Details auf der Seite **Support** > **Alarme (alt)** > **Aktuelle Alarme** anzuzeigen. **Hinweis:** während das alte Alarmsystem weiterhin unterstützt wird, bietet das Alarmsystem erhebliche Vorteile und ist einfacher zu bedienen.
Lizenz	Wird angezeigt, wenn es ein Problem mit der Softwarelizenz für dieses StorageGRID-System gibt. Klicken Sie auf den Link, um die Details auf der Seite **Wartung** > **System** > **Lizenz** anzuzeigen.

Verwandte Informationen

"StorageGRID verwalten"

"Einrichten von E-Mail-Benachrichtigungen für Meldungen"

"Verwendung von SNMP-Überwachung"

Monitoring der Verbindungsstatus der Nodes

Wenn ein oder mehrere Nodes vom Grid getrennt werden, können kritische StorageGRID-Vorgänge beeinträchtigt werden. Sie müssen den Status der Node-Verbindung überwachen und Probleme unverzüglich beheben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Nodes können einen von drei Verbindungszuständen haben:

- **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.

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

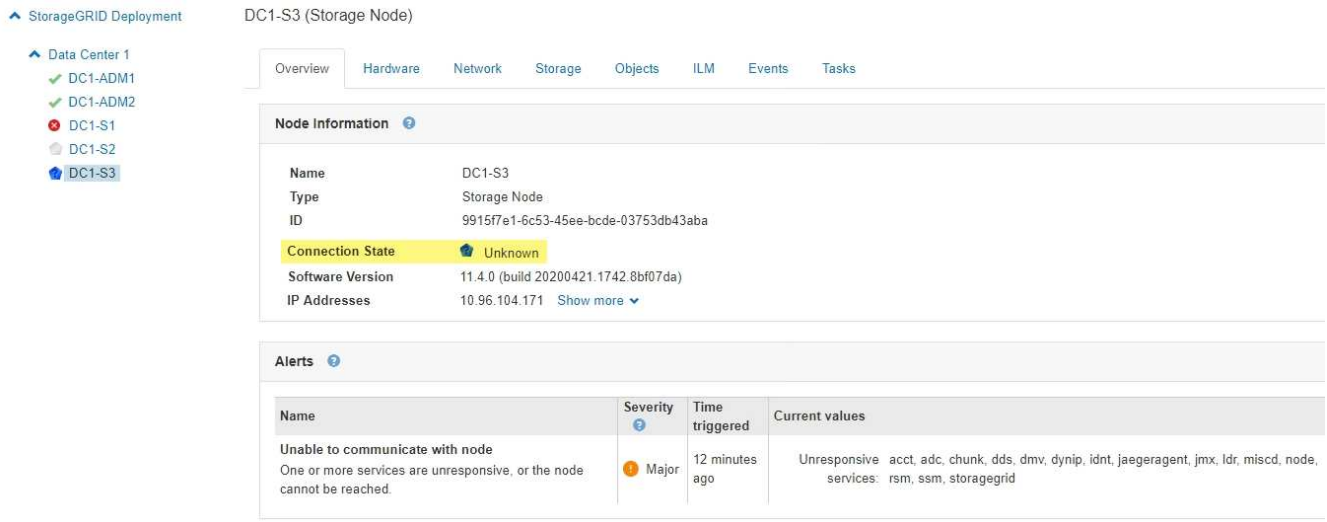
- **Nicht verbunden - Administrativ unten** : Der Knoten ist aus einem erwarteten Grund nicht mit dem Netz verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert. Mindestens ein Alarm ist möglicherweise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

Schritte

1. Wenn im Bedienfeld „Systemzustand“ des Dashboards ein blaues oder graues Symbol angezeigt wird, klicken Sie auf das Symbol oder klicken Sie auf **Rasterdetails**. (Die blauen oder grauen Symbole und der Link **Grid Details** werden nur angezeigt, wenn mindestens ein Knoten vom Raster getrennt ist.)

   Die Übersichtsseite des ersten blauen Knotens in der Knotenstruktur wird angezeigt. Wenn keine blauen Knoten vorhanden sind, wird die Übersichtsseite für den ersten grauen Knoten in der Struktur angezeigt.

   Im Beispiel hat der Speicherknoten DC1-S3 ein blaues Symbol. Der **Verbindungsstatus** im Fenster Knoteninformationen lautet **Unbekannt**, und die Warnung **mit Knoten** kann nicht kommunizieren* ist aktiv. Die Meldung gibt an, dass ein oder mehrere Services nicht mehr reagiert oder der Node nicht erreicht werden kann.



2. Wenn ein Knoten über ein blaues Symbol verfügt, führen Sie die folgenden Schritte aus:
   a. Wählen Sie jede Warnung in der Tabelle aus, und befolgen Sie die empfohlenen Aktionen.

      Beispielsweise müssen Sie einen Dienst neu starten, der angehalten wurde, oder den Host für den Node neu starten.

   b. Wenn der Node nicht wieder in den Online-Modus versetzt werden kann, wenden Sie sich an den technischen Support.
3. Wenn ein Knoten über ein graues Symbol verfügt, führen Sie die folgenden Schritte aus:

   Graue Nodes werden während der Wartungsvorgänge erwartet und sind möglicherweise mit einem oder mehreren Warnmeldungen verbunden. Basierend auf dem zugrunde liegenden Problem werden diese „`administrativ unterliegenden`“ Nodes oft ohne Eingreifen wieder online geschaltet.

   a. Überprüfen Sie den Abschnitt „Meldungen“ und bestimmen Sie, ob Warnmeldungen diesen Node beeinträchtigen.
   b. Wenn eine oder mehrere Warnmeldungen aktiv sind, wählen Sie jede Warnung in der Tabelle aus, und befolgen Sie die empfohlenen Aktionen.
   c. Wenn der Node nicht wieder in den Online-Modus versetzt werden kann, wenden Sie sich an den technischen Support.

Verwandte Informationen

"Alerts Referenz"

"Verwalten Sie erholen"

Anzeigen aktueller Meldungen

Wenn eine Meldung ausgelöst wird, wird auf dem Dashboard ein Meldungssymbol angezeigt. Auf der Seite Knoten wird auch ein Warnungssymbol für den Knoten angezeigt. Es kann auch eine E-Mail-Benachrichtigung gesendet werden, es sei denn, die Warnung wurde stummgeschaltet.

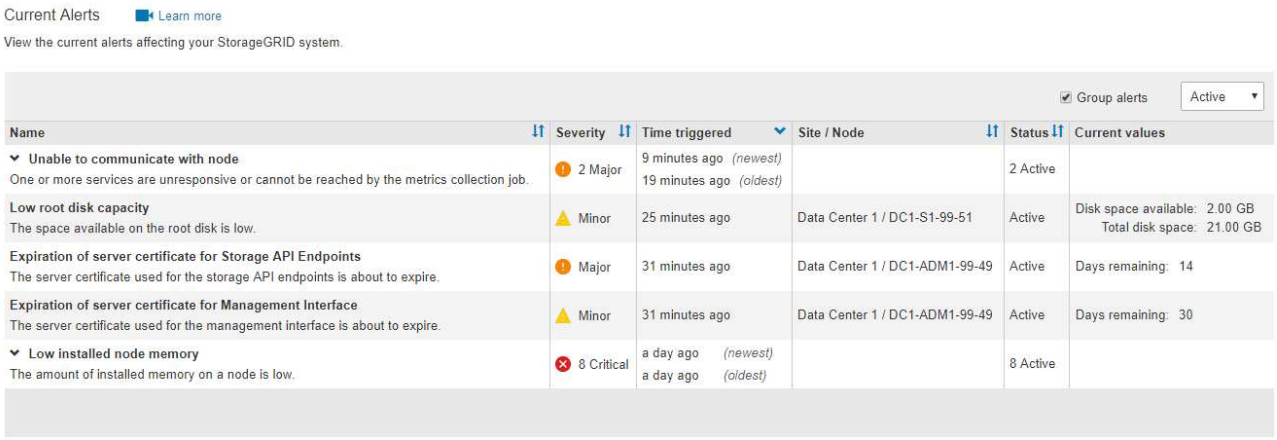
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wenn eine oder mehrere Warnmeldungen aktiv sind, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Fenster Systemzustand des Dashboards auf das Warnsymbol oder klicken Sie auf **Aktuelle Meldungen**. (Ein Warnsymbol und der Link **Current Alerts** werden nur angezeigt, wenn mindestens eine Warnung aktuell aktiv ist.)
   - Wählen Sie **Alarme** > **Aktuell**.

     Die Seite Aktuelle Meldungen wird angezeigt. Er listet alle Warnmeldungen auf, die derzeit Ihr StorageGRID System beeinträchtigen.



     Standardmäßig werden Alarme wie folgt angezeigt:

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

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

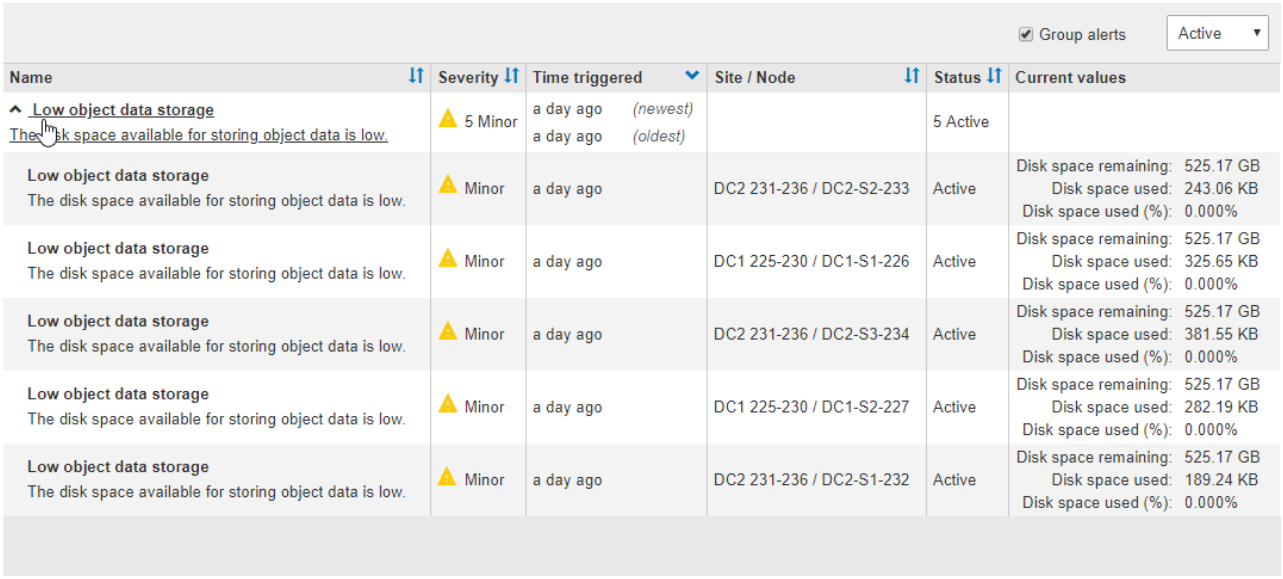
2. Überprüfen Sie die Informationen in der Tabelle.

Spaltenüberschrift	Beschreibung
Name	Der Name der Warnmeldung und deren Beschreibung.

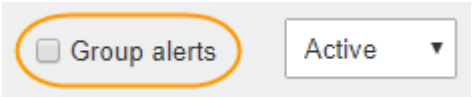
Spaltenüberschrift	Beschreibung
Schweregrad	Der Schweregrad der Meldung. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • **Major** : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • **Klein** : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.
Auslösezeit	Wie lange vor der Warnmeldung ausgelöst wurde. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile Zeiten für die letzte Instanz der Warnmeldung (*neueste*) und die älteste Instanz der Warnmeldung (*älteste*) an.
Standort/Knoten	Der Name des Standorts und des Nodes, an dem die Meldung ausgeführt wird. Wenn mehrere Warnmeldungen gruppiert sind, werden die Standort- und Node-Namen in der Titelzeile nicht angezeigt.

Spaltenüberschrift	Beschreibung
Status	Gibt an, ob die Warnung aktiv ist oder stummgeschaltet wurde. Wenn mehrere Warnungen gruppiert sind und **Alle Alarme** in der Dropdown-Liste ausgewählt ist, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung aktiv sind und wie viele Instanzen zum Schweigen gebracht wurden.
Aktuelle Werte	Der aktuelle Wert der Metrik, der die Meldung ausgelöst hat. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Meldung mit * Objekt-Datenspeicher* enthalten beispielsweise den Prozentsatz des verwendeten Festplattenspeichers, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Festplattenspeichers. **Hinweis:** Wenn mehrere Warnungen gruppiert sind, werden die aktuellen Werte in der Titelzeile nicht angezeigt.

3. So erweitern und reduzieren Sie Alarmgruppen:
   - Um die einzelnen Alarme in einer Gruppe anzuzeigen, klicken Sie auf das nach-unten-Symbol ⌄ In der Überschrift, oder klicken Sie auf den Namen der Gruppe.
   - Um die einzelnen Alarme in einer Gruppe auszublenden, klicken Sie auf das nach-oben-Symbol ⌃ In der Überschrift, oder klicken Sie auf den Namen der Gruppe.



4. Um einzelne Warnungen anstelle von Meldegruppen anzuzeigen, deaktivieren Sie das Kontrollkästchen **Gruppenwarnungen** oben in der Tabelle.



5. Zum Sortieren von Warnungen oder Warnungsgruppen klicken Sie auf die nach-oben/unten-Pfeile ⇅ In jeder Spaltenüberschrift.
   - Wenn **Group Alerts** ausgewählt ist, werden sowohl die Warnungsgruppen als auch die einzelnen Alarme innerhalb jeder Gruppe sortiert. Sie können beispielsweise die Warnungen in einer Gruppe nach **Zeit ausgelöst** sortieren, um die aktuellste Instanz eines bestimmten Alarms zu finden.
   - Wenn **Group Alerts** nicht ausgewählt ist, wird die gesamte Liste der Warnungen sortiert. Beispielsweise können Sie alle Warnungen nach **Node/Site** sortieren, um alle Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.
6. Um die Warnungen nach Status zu filtern, verwenden Sie das Dropdown-Menü oben in der Tabelle.

   - Wählen Sie * Alle Alarme*, um alle aktuellen Warnungen anzuzeigen (sowohl aktive als auch stummgeschaltet).
   - Wählen Sie **aktiv** aus, um nur die aktuellen Alarme anzuzeigen, die aktiv sind.
   - Wählen Sie **stummgeschaltet** aus, um nur die aktuellen Meldungen anzuzeigen, die zum Schweigen gebracht wurden.
7. Um Details zu einer bestimmten Warnmeldung anzuzeigen, wählen Sie die Warnmeldung aus der Tabelle aus.

   Ein Dialogfeld für die Meldung wird angezeigt. Siehe Anweisungen zum Anzeigen einer bestimmten Warnmeldung.

Verwandte Informationen

"Anzeigen einer bestimmten Meldung"

"Stummschalten von Warnmeldungen"

Anzeigen gelöster Warnmeldungen

Sie können den Verlauf der behobenen Warnungen suchen und anzeigen.

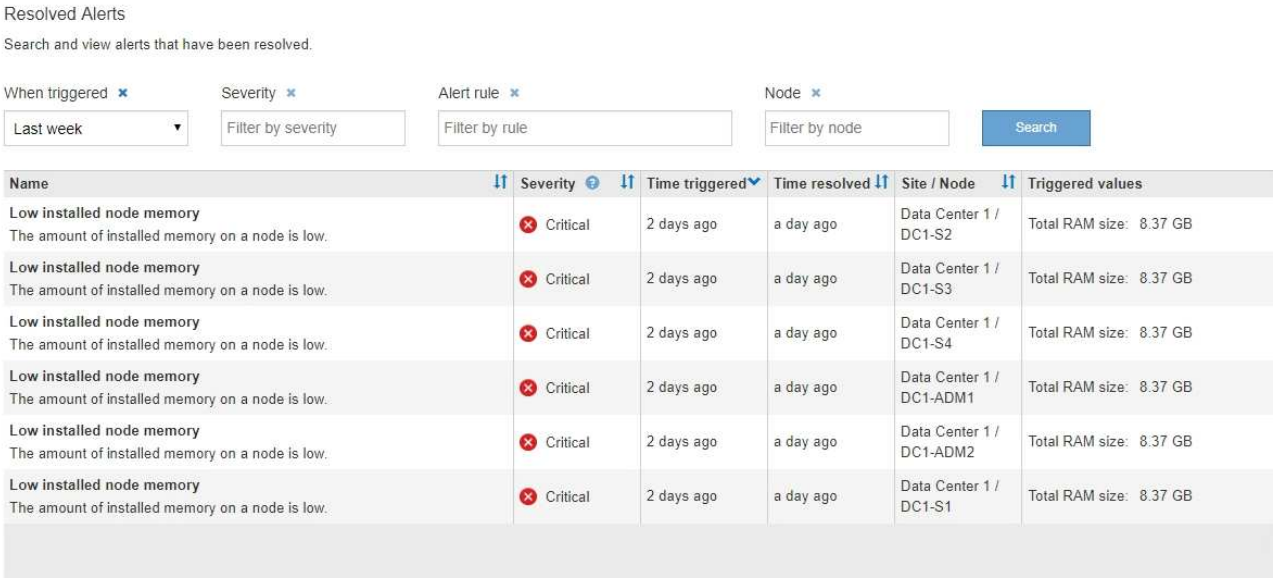
Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Führen Sie einen der folgenden Schritte aus, um aufgelöste Warnmeldungen anzuzeigen:
   - Klicken Sie im Bedienfeld „Systemzustand“ auf **Zuletzt behobene Alarme**.

     Der Link **Kürzlich behobene Alarme** wird nur angezeigt, wenn in der letzten Woche eine oder mehrere Warnungen ausgelöst wurden und nun behoben wurden.
   - Wählen Sie **Alarme** > **Aufgelöst**. Die Seite „behobene Warnmeldungen“ wird angezeigt. Standardmäßig werden behobene Benachrichtigungen, die in der letzten Woche ausgelöst wurden, angezeigt, wobei zuerst die zuletzt ausgelösten Meldungen angezeigt werden. Die Warnmeldungen auf dieser Seite wurden zuvor auf der Seite „Aktuelle Meldungen“ oder in einer E-Mail-Benachrichtigung angezeigt.



2. Überprüfen Sie die Informationen in der Tabelle.

Spaltenüberschrift	Beschreibung
Name	Der Name der Warnmeldung und deren Beschreibung.
Schweregrad	Der Schweregrad der Meldung. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • **Major** : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • **Klein** : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.

Spaltenüberschrift	Beschreibung
Auslösezeit	Wie lange vor der Warnmeldung ausgelöst wurde.
Zeit für eine Lösung	Wie lange zuvor wurde die Warnung behoben.
Standort/Knoten	Der Name des Standorts und des Node, auf dem die Meldung aufgetreten ist.
Ausgelöste Werte	Der Wert der Metrik, der den Auslöser der Meldung verursacht hat. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Meldung mit * Objekt-Datenspeicher* enthalten beispielsweise den Prozentsatz des verwendeten Festplattenspeichers, die Gesamtmenge des Speicherplatzes und die Menge des verwendeten Festplattenspeichers.

3. Um die gesamte Liste der aufgelösten Warnmeldungen zu sortieren, klicken Sie auf die Pfeile nach oben/unten ⇅ In jeder Spaltenüberschrift.

   Sie können beispielsweise aufgelöste Warnmeldungen nach **Site/Node** sortieren, um die Warnungen anzuzeigen, die einen bestimmten Knoten betreffen.

4. Optional können Sie die Liste der aufgelösten Warnmeldungen mithilfe der Dropdown-Menüs oben in der Tabelle filtern.
   a. Wählen Sie im Dropdown-Menü **When Triggered** einen Zeitraum aus, um aufgelöste Warnmeldungen anzuzeigen, basierend darauf, wie lange sie ausgelöst wurden.

      Sie können nach Benachrichtigungen suchen, die innerhalb der folgenden Zeiträume ausgelöst wurden:

      - Letzte Stunde
      - Letzter Tag
      - Letzte Woche (Standardansicht)
      - Letzten Monat
      - Zu jedem Zeitpunkt
      - Benutzerdefiniert (ermöglicht das Festlegen des Anfangsdatums und des Enddatum für den Zeitraum)

   b. Wählen Sie im Dropdown-Menü **Severity** einen oder mehrere Schweregrade aus, um nach gelösten Warnmeldungen eines bestimmten Schweregrads zu filtern.
   c. Wählen Sie im Dropdown-Menü **Warnregel** eine oder mehrere Standard- oder benutzerdefinierte Warnungsregeln aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einer bestimmten Alarmregel zusammenhängen.
   d. Wählen Sie im Dropdown-Menü **Node** einen oder mehrere Knoten aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einem bestimmten Knoten verbunden sind.
   e. Klicken Sie Auf **Suchen**.

5. Um Details zu einer bestimmten aufgelösten Warnmeldung anzuzeigen, wählen Sie die Warnmeldung aus der Tabelle aus.

   Ein Dialogfeld für die Meldung wird angezeigt. Siehe Anweisungen zum Anzeigen einer bestimmten Warnmeldung.

Verwandte Informationen

"Anzeigen einer bestimmten Meldung"

Anzeigen einer bestimmten Meldung

Sie können detaillierte Informationen zu einer Meldung anzeigen, die derzeit Ihr StorageGRID System beeinträchtigt, oder eine Meldung, die behoben wurde. Zu den Details gehören empfohlene Korrekturmaßnahmen, der Zeitpunkt, zu dem die Meldung ausgelöst wurde, und der aktuelle Wert der Metriken in Bezug auf diese Meldung. Optional können Sie eine aktuelle Warnung stummschalten oder die Alarmregel aktualisieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

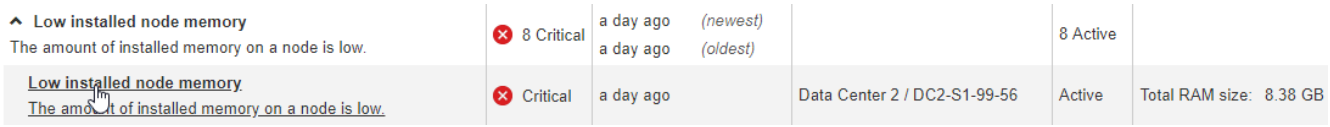
1. Führen Sie einen der folgenden Schritte aus, je nachdem, ob Sie eine aktuelle oder behobene Warnmeldung anzeigen möchten:

Spaltenüberschrift	Beschreibung
Aktueller Alarm	• Klicken Sie im Fenster Systemzustand des Dashboards auf den Link **Aktuelle Meldungen**. Dieser Link wird nur angezeigt, wenn mindestens eine Warnung aktuell aktiv ist. Dieser Link ist ausgeblendet, wenn keine aktuellen Warnmeldungen vorhanden sind oder alle aktuellen Warnmeldungen stummgeschaltet wurden. • Wählen Sie **Alarme** > **Aktuell**. • Wählen Sie auf der Seite **Nodes** die Registerkarte **Übersicht** für einen Knoten mit einem Warnsymbol. Klicken Sie dann im Abschnitt Meldungen auf den Namen der Warnmeldung.

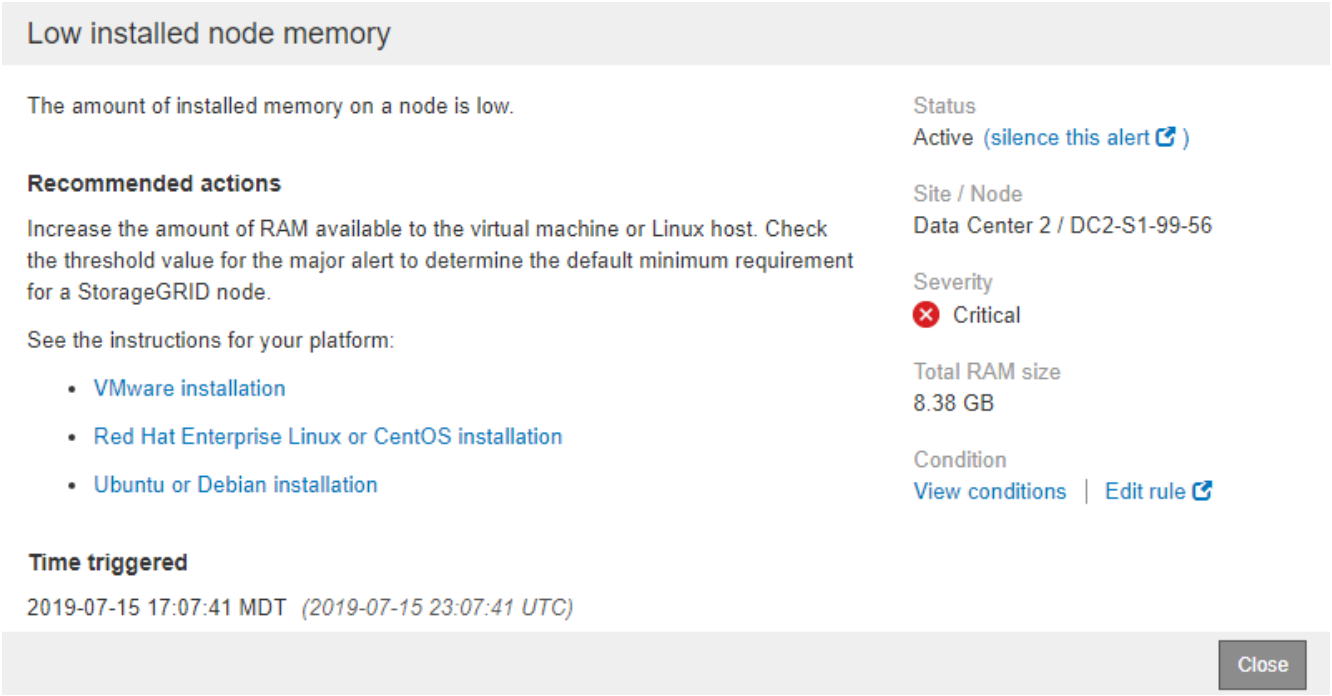
Spaltenüberschrift	Beschreibung
Alarm wurde behoben	• Klicken Sie im Fenster Systemzustand des Dashboards auf den Link **Zuletzt behobene Alarme**. (Dieser Link wird nur angezeigt, wenn in der vergangenen Woche eine oder mehrere Warnmeldungen ausgelöst wurden und jetzt behoben werden. Dieser Link ist ausgeblendet, wenn in der letzten Woche keine Warnmeldungen ausgelöst und behoben wurden.) • Wählen Sie **Alarme** > **Aufgelöst**.

2. Erweitern Sie je nach Bedarf eine Gruppe von Warnungen, und wählen Sie dann die Warnmeldung aus, die Sie anzeigen möchten.

Wählen Sie die Meldung und nicht die Überschrift einer Gruppe von Warnungen aus.



Ein Dialogfeld wird angezeigt und enthält Details für die ausgewählte Warnmeldung.



3. Prüfen Sie die Warnmeldungsdetails.

Informationsdaten	Beschreibung
Titel	Der Name der Warnmeldung.

Informationsdaten	Beschreibung
Erster Absatz	Die Beschreibung der Warnmeldung.
Empfohlene Maßnahmen	Die empfohlenen Aktionen für diese Warnmeldung.
Auslösezeit	Datum und Uhrzeit der Auslösung der Warnmeldung zu Ihrer lokalen Zeit und zu UTC.
Zeit für eine Lösung	Nur bei gelösten Warnmeldungen wurde das Datum und die Uhrzeit der Behebung der Warnmeldung in Ihrer lokalen Zeit und in UTC angegeben.
Status	Der Status der Warnmeldung: Aktiv, stummgeschaltet oder gelöst.
Standort/Knoten	Der Name des von der Meldung betroffenen Standorts und Nodes.
Schweregrad	Der Schweregrad der Meldung. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • **Major** : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • **Klein** : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenderen Problem führen.

Informationsdaten	Beschreibung
Datenwerte	Der aktuelle Wert der Metrik für diese Meldung. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Warnung für **Low-Metadaten-Speicher** enthalten beispielsweise den Prozentsatz des belegten Speicherplatzes, den gesamten Speicherplatz und die Menge des verwendeten Festplattenspeichers.

4. Klicken Sie optional auf **stummschalten Sie diese Warnung**, um die Alarmregel, die diese Warnung ausgelöst hat, stillzuschalten.

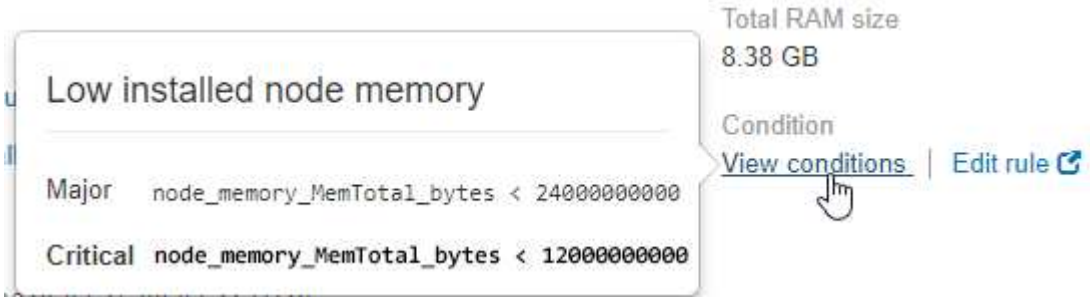
   Sie müssen über die Berechtigung Warnungen verwalten oder Root-Zugriff verfügen, um eine Alarmregel stillzuschalten.

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

5. So zeigen Sie die aktuellen Bedingungen für die Meldungsregel an:

   a. Klicken Sie in den Alarmdetails auf **Bedingungen anzeigen**.

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



   a. Um das Popup-Fenster zu schließen, klicken Sie außerhalb des Popup-Dialogfenster auf eine beliebige Stelle.

6. Klicken Sie optional auf **Regel bearbeiten**, um die Warnregel zu bearbeiten, die die Warnung ausgelöst hat:

   Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen, um eine Alarmregel zu bearbeiten.

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

7. Klicken Sie zum Schließen der Warnungsdetails auf **Schließen**.

Verwandte Informationen

"Stummschalten von Warnmeldungen"

"Bearbeiten einer Meldungsregel"

Anzeigen von Legacy-Alarmen

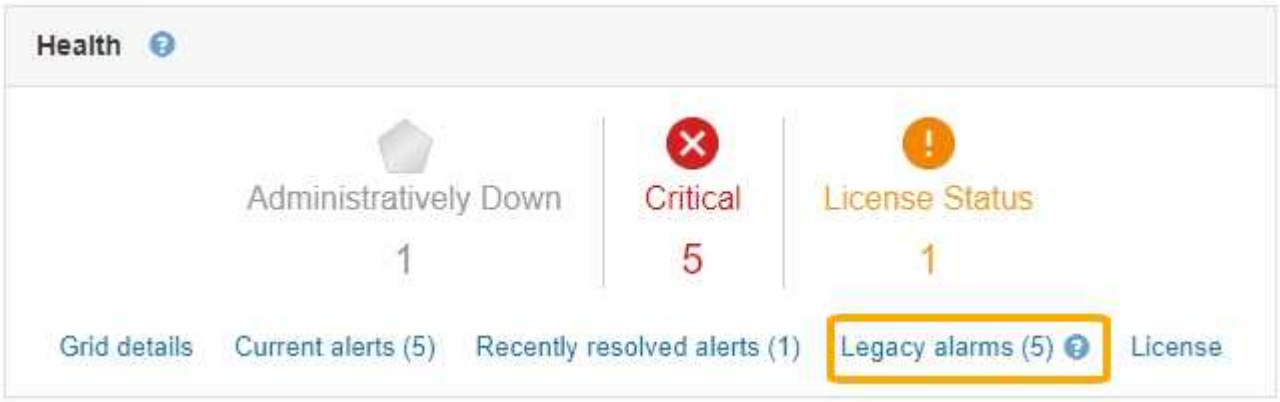
Alarme (Altsystem) werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Sie können die derzeit aktiven Alarme über das Dashboard oder die Seite Aktuelle Alarme anzeigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn einer oder mehrere der älteren Alarme derzeit aktiv sind, enthält das Bedienfeld „Systemzustand“ auf dem Dashboard einen Link „Legacy-Alarme*“. Die Zahl in Klammern gibt an, wie viele Alarme derzeit aktiv sind.



Die Zählung der **Legacy-Alarme** auf dem Dashboard wird immer dann erhöht, wenn ein älterer Alarm ausgelöst wird. Diese Zählung wird sogar erhöht, wenn Sie Alarm-E-Mail-Benachrichtigungen deaktiviert haben. Sie können diese Zahl in der Regel ignorieren (da Warnmeldungen eine bessere Übersicht über das System bieten) oder die derzeit aktiven Alarme anzeigen.

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

Schritte

1. Führen Sie einen der folgenden Schritte aus, um die vorhandenen Alarme anzuzeigen:
   - Klicken Sie im Bedienfeld „Systemzustand“ auf **Legacy-Alarme**. Dieser Link wird nur angezeigt, wenn derzeit mindestens ein Alarm aktiv ist.
   - Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**. Die Seite Aktuelle Alarme wird angezeigt.

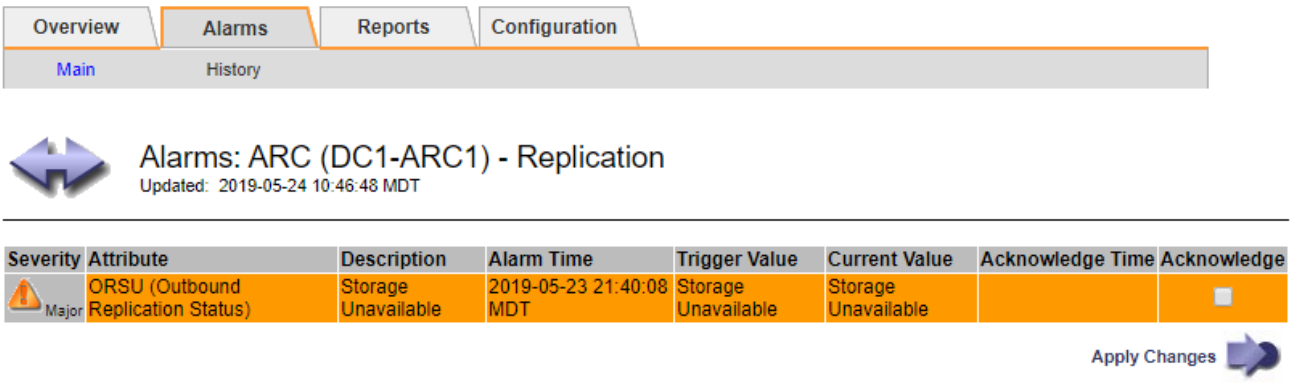
Das Alarmsymbol zeigt den Schweregrad jedes Alarms wie folgt an:

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

Symbol	Farbe	Alarmschweregrad	Bedeutung
	Rot	Kritisch	Der Node ist mit dem Grid verbunden. Es ist jedoch eine anormale Bedingung vorhanden, die normale Vorgänge angehalten hat. Sie sollten das Problem sofort beheben.

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

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



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

Verwandte Informationen

"Alarmreferenz (Altsystem)"

"Bestätigen aktueller Alarme (Altsystem)"

"Deaktivieren von Alarmen (Altsystem)"

Monitoring der Storage-Kapazität

Sie müssen den insgesamt nutzbaren Speicherplatz auf Storage-Nodes überwachen, um sicherzustellen, dass dem StorageGRID System nicht der Speicherplatz für Objekte oder Objekt-Metadaten zur Verfügung steht.

StorageGRID speichert Objektdaten und Objektmetadaten separat und behält eine bestimmte Menge an Speicherplatz für eine verteilte Cassandra-Datenbank mit Objekt-Metadaten bei. Überwachen Sie den

Gesamtspeicherplatz für Objekte und Objekt-Metadaten sowie Trends für den Speicherplatz, der für jeden verbraucht wird. So können Sie das Hinzufügen von Nodes vorausschauender planen und Serviceausfälle vermeiden.

Sie können Storage-Kapazitätsinformationen für das gesamte Grid, für jeden Standort und für jeden Storage-Node in Ihrem StorageGRID-System anzeigen.

Verwandte Informationen

"Anzeigen der Registerkarte „Speicher“"

Überwachung der Storage-Kapazität für das gesamte Grid

Die Storage-Gesamtkapazität für das Grid muss überwacht werden, um zu gewährleisten, dass ausreichend freier Speicherplatz für Objekt- und Objekt-Metadaten verbleibt. Wenn Sie verstehen, wie sich die Storage-Kapazität im Laufe der Zeit verändert, können Sie Storage-Nodes oder Storage-Volumes planen, bevor die nutzbare Storage-Kapazität des Grid verbraucht wird.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

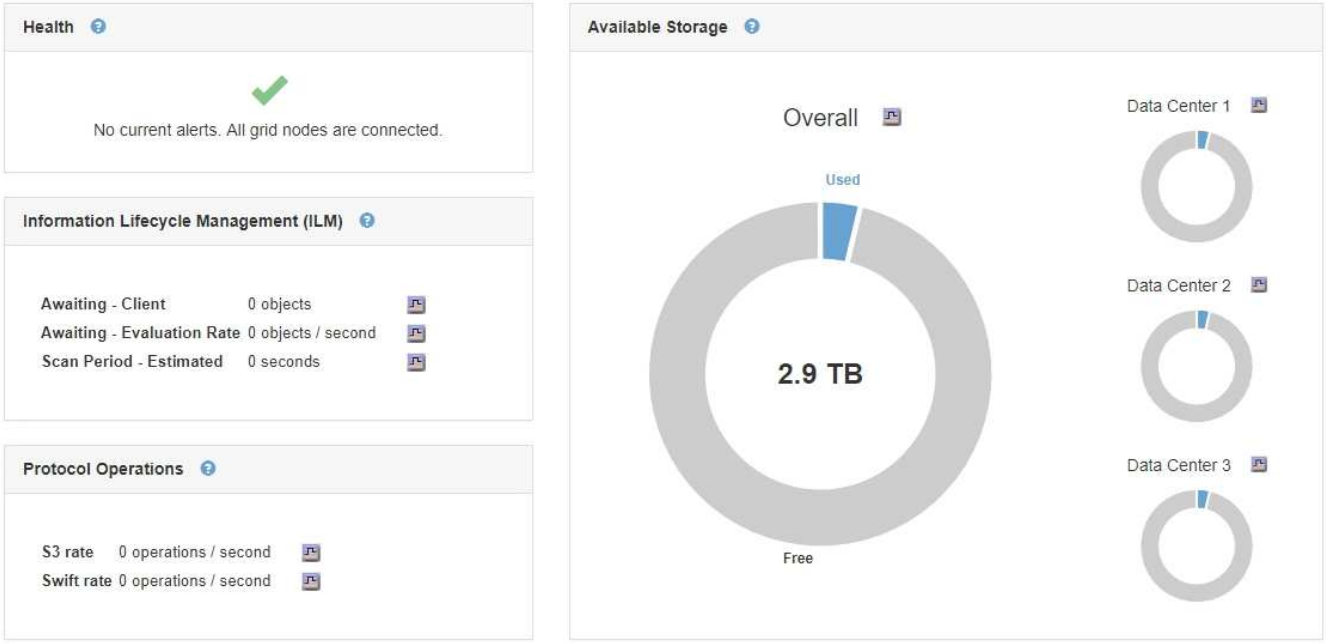
Über diese Aufgabe

Über das Dashboard im Grid Manager können Sie schnell ermitteln, wie viel Storage für das gesamte Grid und für jedes Datacenter zur Verfügung steht. Die Seite Knoten enthält detailliertere Werte für Objektdaten und Objektmetadaten.

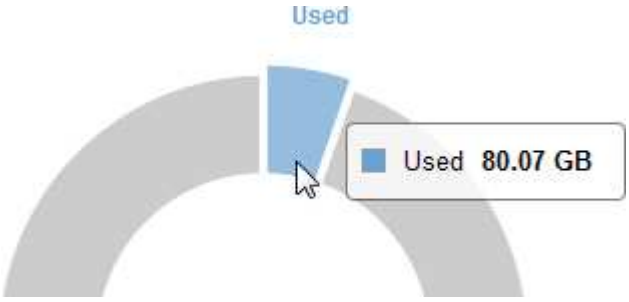
Schritte

1. Beurteilen Sie, wie viel Storage für das gesamte Grid und das jeweilige Datacenter verfügbar ist.
   a. Wählen Sie **Dashboard**.
   b. Notieren Sie sich im Fenster Verfügbare Speicherkapazität die Zusammenfassung der freien und genutzten Speicherkapazität.

      Die Zusammenfassung enthält keine Archivierungsmedien.



a. Platzieren Sie den Cursor über die freien bzw. genutzten Kapazitätsbereiche des Diagramms, um genau zu sehen, wie viel Speicherplatz frei oder verwendet wird.



b. Sehen Sie sich das Diagramm für die einzelnen Datacenter an, um Grids für mehrere Standorte zu verwenden.

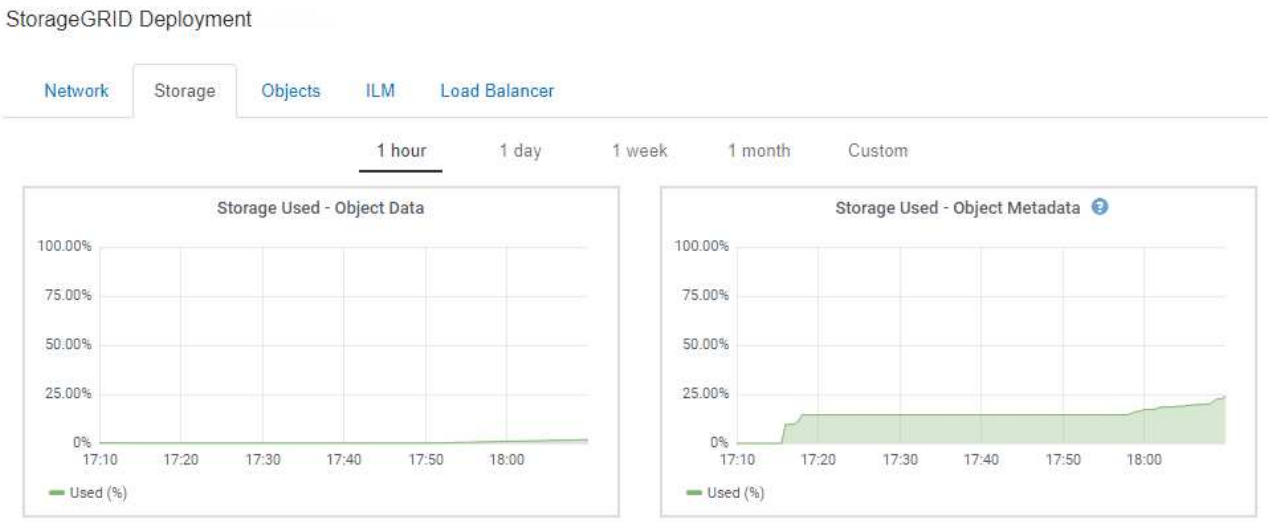
c. Klicken Sie auf das Diagrammsymbol Für das Gesamtdiagramm oder für ein einzelnes Datacenter, um ein Diagramm anzuzeigen, in dem die Kapazitätsauslastung im Laufe der Zeit dargestellt wird.

   Eine Grafik zeigt den prozentualen Anteil an der genutzten Storage-Kapazität (%) gegenüber Die Uhrzeit wird angezeigt.

2. Ermitteln Sie, wie viel Storage genutzt wurde und wie viel Storage für Objekt- und Objekt-Metadaten verfügbar ist.

   a. Wählen Sie **Knoten**.

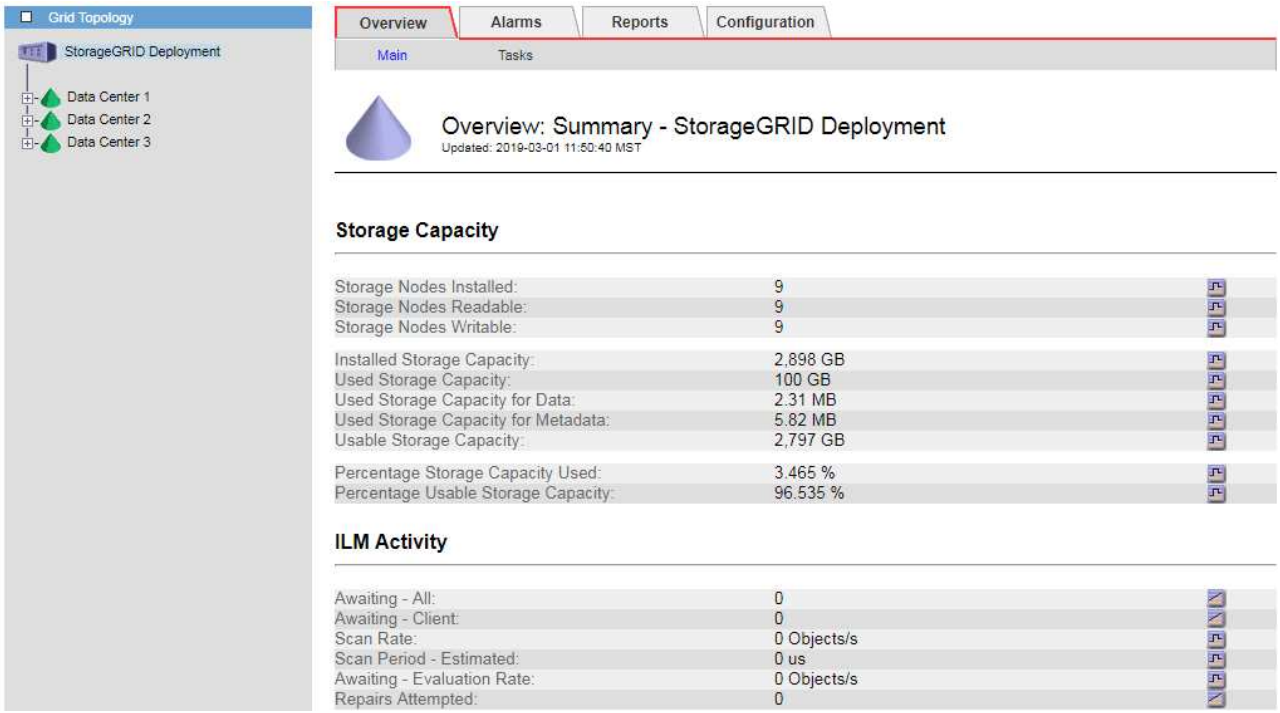
   b. Wählen Sie ***Grid*** > **Storage** aus.



c. Bewegen Sie den Mauszeiger über den Speicher verwendet - Objektdaten und den verwendeten Speicher - Objektmetadaten-Diagramme, um zu ermitteln, wie viel Objekt-Storage und Objekt-Metadaten im gesamten Grid zur Verfügung stehen und wieviel Storage über die Zeit verwendet wurde.

> ⓘ Die Gesamtwerte für einen Standort oder das Grid enthalten keine Nodes, die mindestens fünf Minuten lang keine Kennzahlen enthalten, z. B. Offline-Nodes.

3. Sehen Sie sich gemäß dem technischen Support weitere Details zur Speicherkapazität Ihres Grids an.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***Grid*** > **Übersicht** > **Main**.



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

   Berücksichtigen Sie bei der Planung des Zeitplans für eine Erweiterung, wie lange die Beschaffung und

Installation von zusätzlichem Storage dauern wird.

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

Weitere Informationen zur Planung einer Speichererweiterung finden Sie in den Anweisungen zur Erweiterung von StorageGRID.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

Monitoring der Storage-Kapazität für jeden Storage-Node

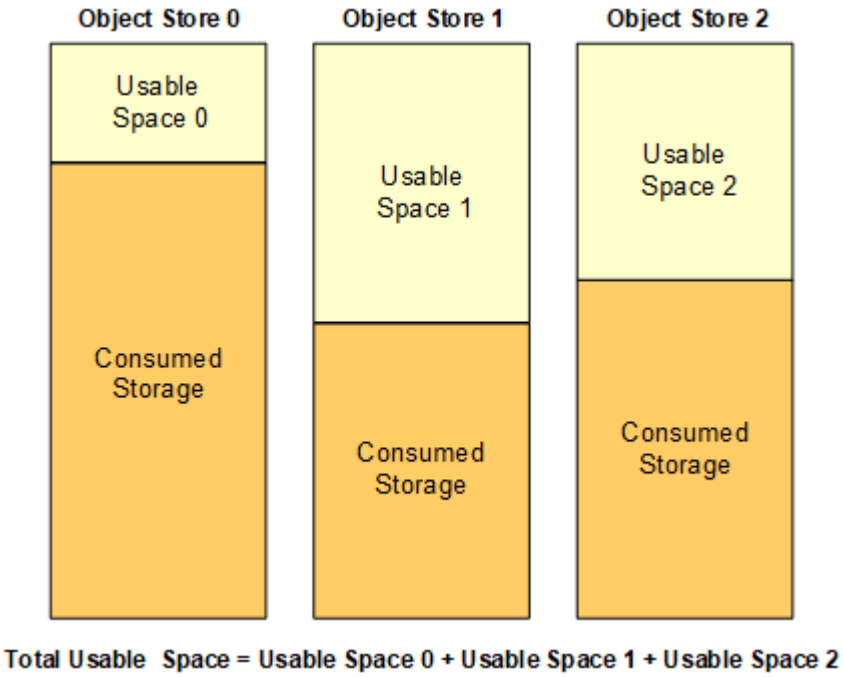
Sie müssen den gesamten nutzbaren Speicherplatz für jeden Storage-Node überwachen, um sicherzustellen, dass der Node über genügend Speicherplatz für neue Objektdaten verfügt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

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



Schritte

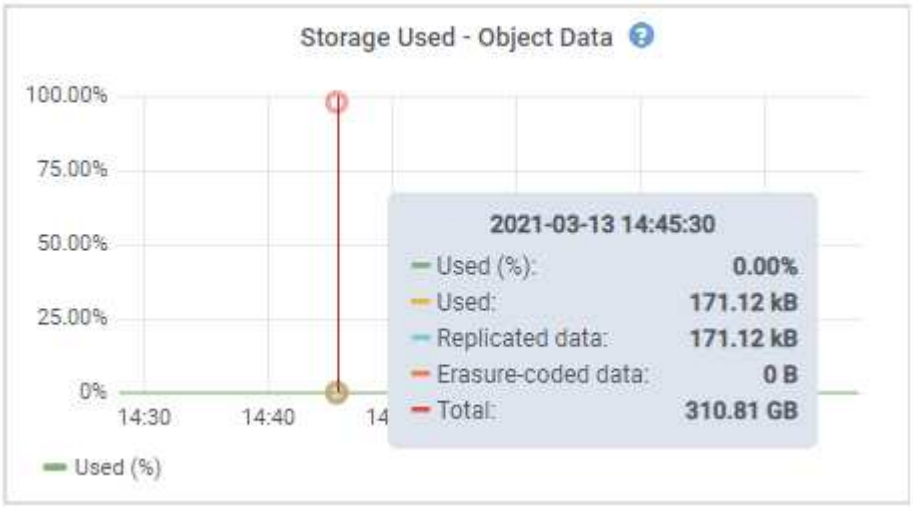
1. Wählen Sie **Nodes** > ***Storage Node*** > **Storage** Aus.

   Die Diagramme und Tabellen für den Node werden angezeigt.

2. Bewegen Sie den Mauszeiger über das Diagramm „verwendete Daten – Objektdaten“.

   Die folgenden Werte werden angezeigt:

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



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

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

Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	0.03%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.85%	0 bytes/s	58 KB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	81 bytes/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	14.90 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.10 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 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	96.45 GB	250.90 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

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

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

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

   Weitere Informationen zur Planung einer Speichererweiterung finden Sie in den Anweisungen zur Erweiterung von StorageGRID.

   Der Alarm * Low Object Data Storage* und der Legacy Storage Status (SSTS) werden ausgelöst, wenn nicht genügend Speicherplatz zum Speichern von Objektdaten auf einem Storage Node vorhanden ist.

Verwandte Informationen

"StorageGRID verwalten"

"Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“"

"Erweitern Sie Ihr Raster"

Monitoring der Objekt-Metadaten-Kapazität für jeden Storage Node

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

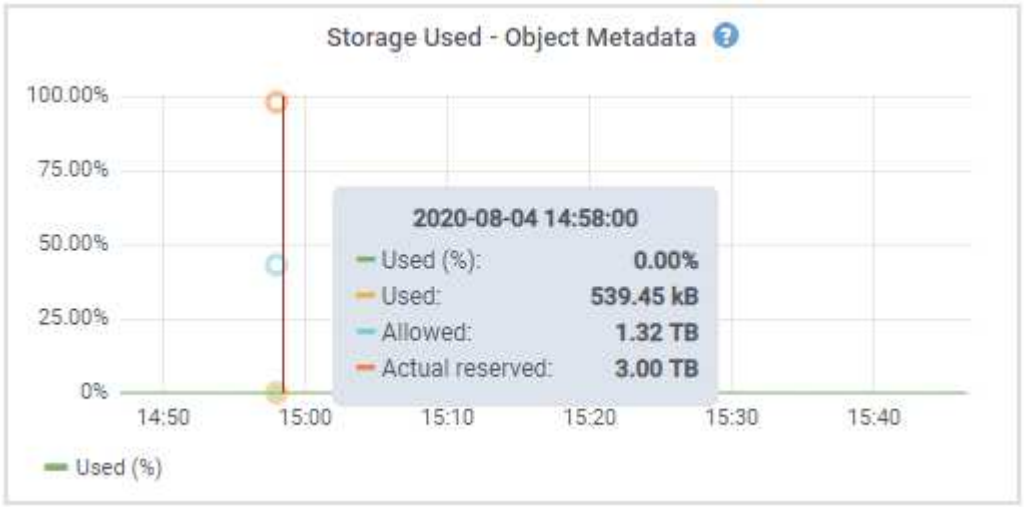
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage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

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

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

Schritte

1. Wählen Sie **Nodes** > ***Storage Node*** > **Storage** Aus.
2. Bewegen Sie den Mauszeiger über das Diagramm „verwendete Objekte – Metadaten“, um die Werte für eine bestimmte Zeit anzuzeigen.



Wert	Beschreibung	Prometheus metrisch
Nutzung (%)	Der Prozentsatz des zulässigen Metadaten-Speicherplatzes, der auf diesem Storage-Node verwendet wurde.	`storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes`
Verwendet	Die Bytes des zulässigen Metadaten-Speicherplatzes, der auf diesem Speicherknoten verwendet wurde.	`storagegrid_storage_utilization_metadata_bytes`
Zulässig	Der zulässige Speicherplatz für Objektmetadaten auf diesem Storage-Node. Erfahren Sie, wie dieser Wert für die einzelnen Speicherknoten bestimmt ist, und lesen Sie die Anweisungen zur Verwaltung von StorageGRID.	`storagegrid_storage_utilization_metadata_allowed_bytes`
Ist reserviert	Der tatsächliche Speicherplatz, der für Metadaten auf diesem Speicherknoten reserviert ist. Beinhaltet den zulässigen Speicherplatz und den erforderlichen Speicherplatz für wichtige Metadaten-Vorgänge. Informationen dazu, wie dieser Wert für die einzelnen Storage-Nodes berechnet wird, finden Sie in den Anweisungen für die Administration von StorageGRID.	`storagegrid_storage_utilization_metadata_reserved_bytes`

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

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

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

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

Verwandte Informationen

"Fehlerbehebung für Storage-Warnmeldungen bei niedrigen Metadaten"

"StorageGRID verwalten"

"Erweitern Sie Ihr Raster"

Überwachung des Information Lifecycle Management

Das Information Lifecycle Management-System (ILM) ermöglicht Datenmanagement für alle im Grid gespeicherten Objekte. Sie müssen die ILM-Vorgänge überwachen, um nachzuvollziehen, ob das Grid die aktuelle Auslastung handhaben kann oder ob weitere Ressourcen erforderlich sind.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

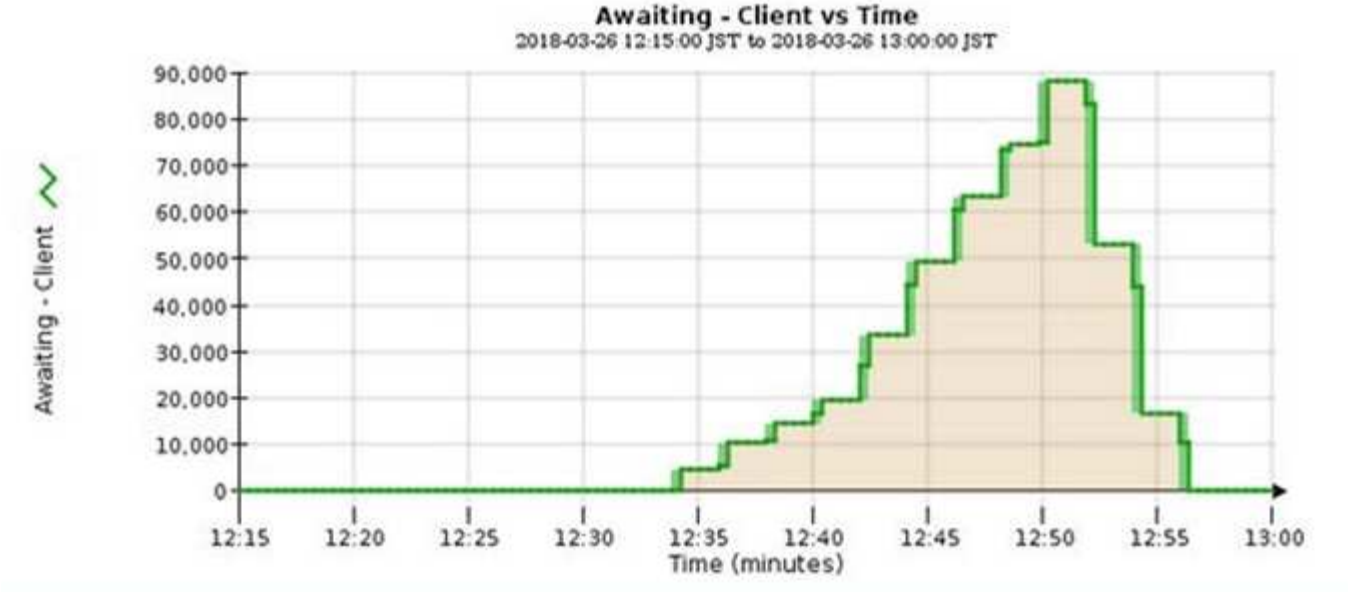
Das StorageGRID System managt Objekte mithilfe der aktiven ILM-Richtlinie. Die ILM-Richtlinie und die zugehörigen ILM-Regeln bestimmen die Anzahl der Kopien, die Art der erstellten Kopien, das Erstellen von Kopien und die Dauer der Aufbewahrung jeder Kopie.

Bei der Objektaufnahme und anderen objektbezogenen Aktivitäten kann die Rate überschritten werden, mit der StorageGRID ILM bewerten kann. Das System muss dann Objekte in eine Warteschlange stellen, deren ILM-Platzierung nicht nahezu in Echtzeit erfüllt werden kann. Sie können überwachen, ob StorageGRID mit den Client-Aktionen Schritt hält, indem Sie das Attribut „Warten – Client“ schreiben.

So setzen Sie dieses Attribut auf:

1. Melden Sie sich beim Grid Manager an.
2. Suchen Sie über das Dashboard im Bereich Information Lifecycle Management (ILM) den Eintrag **wartet auf - Client**.
3. Klicken Sie auf das Diagrammsymbol .

Das Beispieldiagramm zeigt eine Situation, in der die Anzahl der Objekte, die auf eine ILM-Bewertung warten, vorübergehend nicht aufrechtzuerhalten ist, dann aber gesunken ist. Ein solcher Trend zeigt, dass ILM vorübergehend nicht in Echtzeit erfüllt wurde.



Temporäre Spitzen in der Tabelle von wartet - Client sind zu erwarten. Wenn der in der Grafik angezeigte Wert jedoch weiter steigt und nie sinkt, erfordert das Grid mehr Ressourcen für einen effizienten Betrieb: Entweder mehr Storage-Nodes oder, wenn die ILM-Richtlinie Objekte an Remote-Standorten platziert, erhöht sich die Netzwerkbandbreite.

Sie können ILM-Warteschlangen mithilfe der Seite **Nodes** genauer untersuchen.

Schritte

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

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

   - **Scan Period - Estimated**: Die geschätzte Zeit, um einen vollständigen ILM-Scan aller Objekte abzuschließen.

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

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

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

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

Monitoring der Performance-, Netzwerk- und Systemressourcen

Sie sollten die Performance-, Netzwerk- und Systemressourcen überwachen, um zu ermitteln, ob StorageGRID die aktuelle Last bewältigen kann und ob die Client-Performance im Laufe der Zeit nicht abnimmt.

Monitoring der Abfragelatenz

Client-Aktionen wie Speichern, Abrufen oder Löschen von Objekten erstellen Abfragen für die verteilte Datenbank der Objektmetadaten des Grid. Sie sollten Trends bei der Abfragelatenz überwachen, um sicherzustellen, dass die Grid-Ressourcen für die aktuelle Auslastung ausreichend sind.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

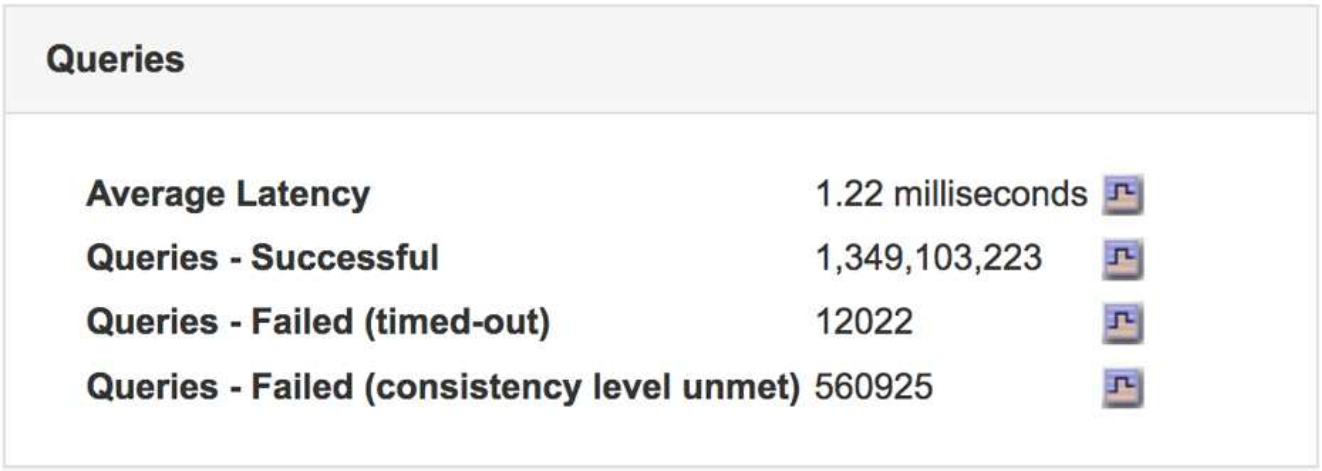
Temporäre Steigerungen der Abfragelatenz sind normal und können durch eine plötzliche Zunahme der Aufnahmeraten verursacht werden. Ausgefallene Abfragen sind ebenfalls normal und können aus vorübergehenden Netzwerkproblemen oder Knoten resultieren, die vorübergehend nicht verfügbar sind. Wenn jedoch die durchschnittliche Zeit für eine Abfrage steigt, sinkt die Gesamtleistung des Grids.

Wenn Sie feststellen, dass die Abfragelatenz im Laufe der Zeit zunimmt, sollten Sie in Erwägung ziehen, weitere Storage-Nodes in einem Erweiterungsverfahren hinzuzufügen, um zukünftige Workloads zu erfüllen.

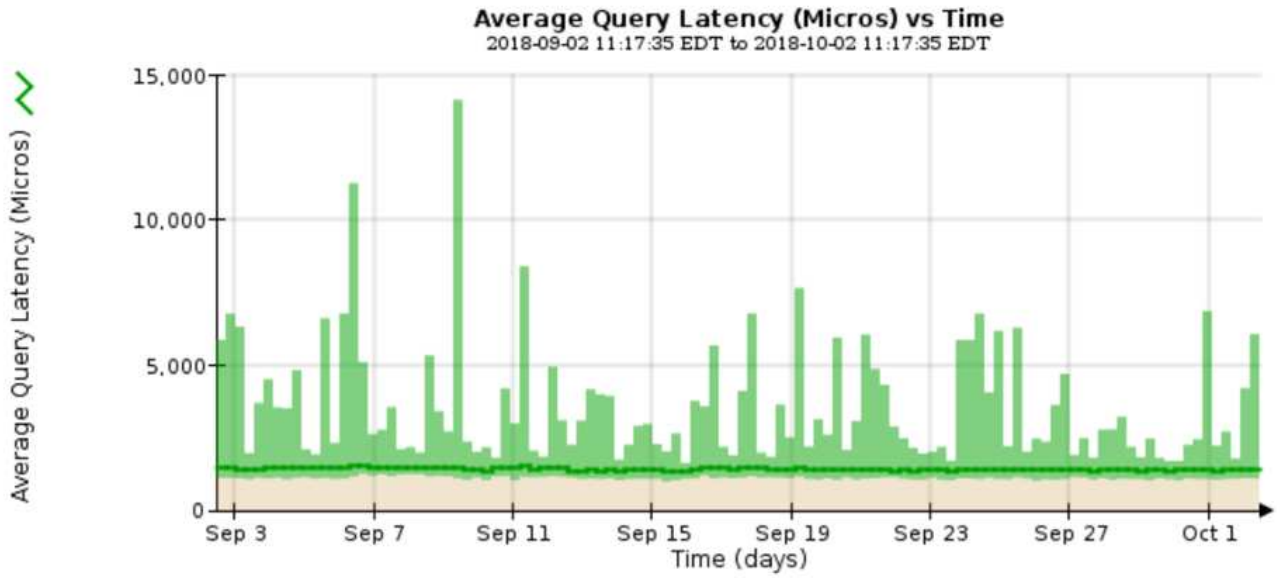
Die Warnung **hohe Latenz für Metadatenabfragen** wird ausgelöst, wenn die durchschnittliche Zeit für Abfragen zu lang ist.

Schritte

1. Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte** Aus.
2. Blättern Sie nach unten zur Tabelle Abfragen, und zeigen Sie den Wert für die durchschnittliche Latenz an.



3. Klicken Sie auf das Diagrammsymbol Um den Wert im Zeitverlauf zu erstellen.



Das Beispieldiagramm zeigt Spitzen in der Abfragelatenz während des normalen Grid-Betriebs.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

Monitoring von Netzwerkverbindungen und Performance

Die Grid-Nodes müssen miteinander kommunizieren können, damit das Grid betrieben werden kann. Die Integrität des Netzwerks zwischen Knoten und Standorten und die Netzwerkbandbreite zwischen Standorten sind für einen effizienten Betrieb entscheidend.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Netzwerkkonnektivität und Bandbreite sind besonders wichtig, wenn Ihre Richtlinien für Information Lifecycle Management (ILM) replizierte Objekte zwischen Standorten kopieren oder Erasure Coding-codierte Objekte

mit einem Schema speichern, das Site-Loss-Schutz bietet. Wenn das Netzwerk zwischen Standorten nicht verfügbar ist, die Netzwerklatenz zu hoch ist oder die Netzwerkbandbreite nicht ausreicht, können einige ILM-Regeln Objekte möglicherweise nicht an den erwarteten Stellen platzieren. Dies kann zu Aufnahmeausfällen führen (wenn die strikte Aufnahme-Option für ILM-Regeln ausgewählt ist) oder zu unzureichenden Aufnahme-Performance und ILM-Backlogs.

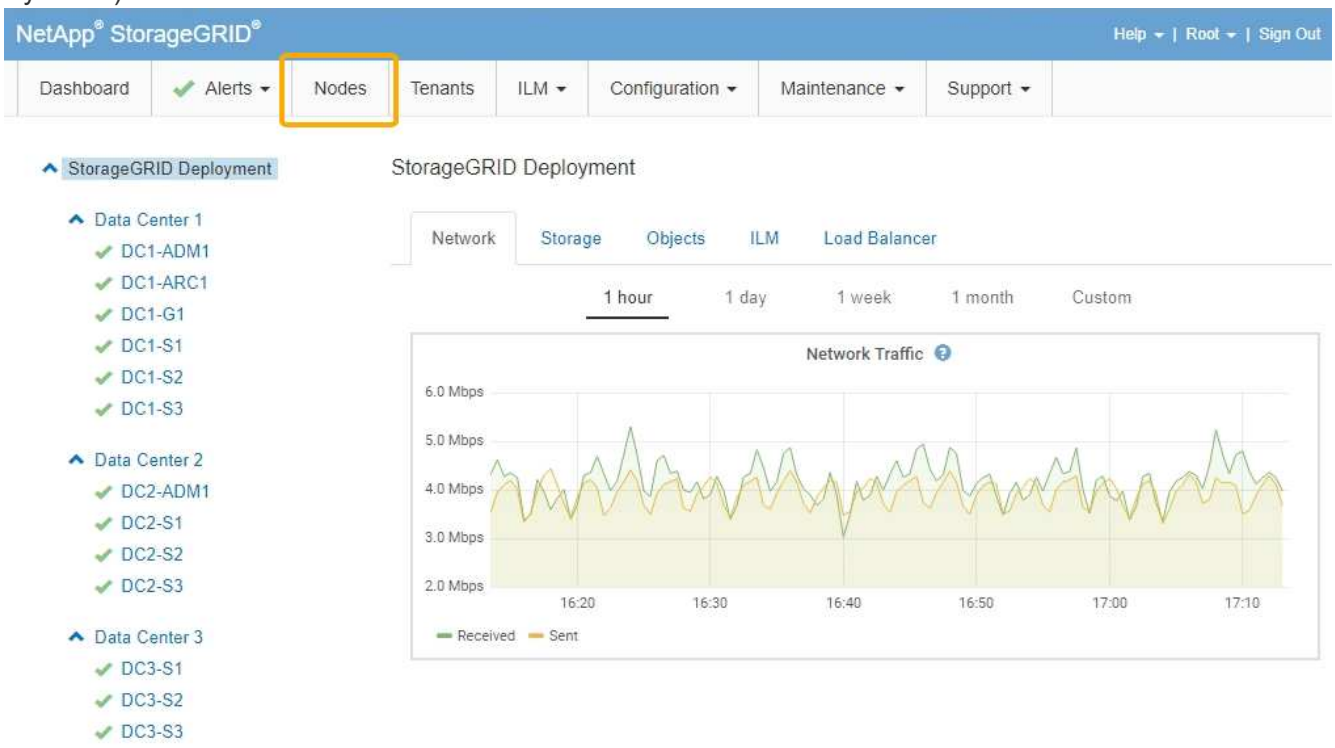
Mit dem Grid Manager können Sie die Konnektivität und die Netzwerk-Performance überwachen, damit Sie Probleme umgehend beheben können.

Darüber hinaus sollten Richtlinien für die Klassifizierung des Netzwerkverkehrs erstellt werden, um den Datenverkehr im Zusammenhang mit bestimmten Mandanten, Buckets, Subnetzen oder Load Balancer-Endpunkten zu überwachen und einzuschränken. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Schritte

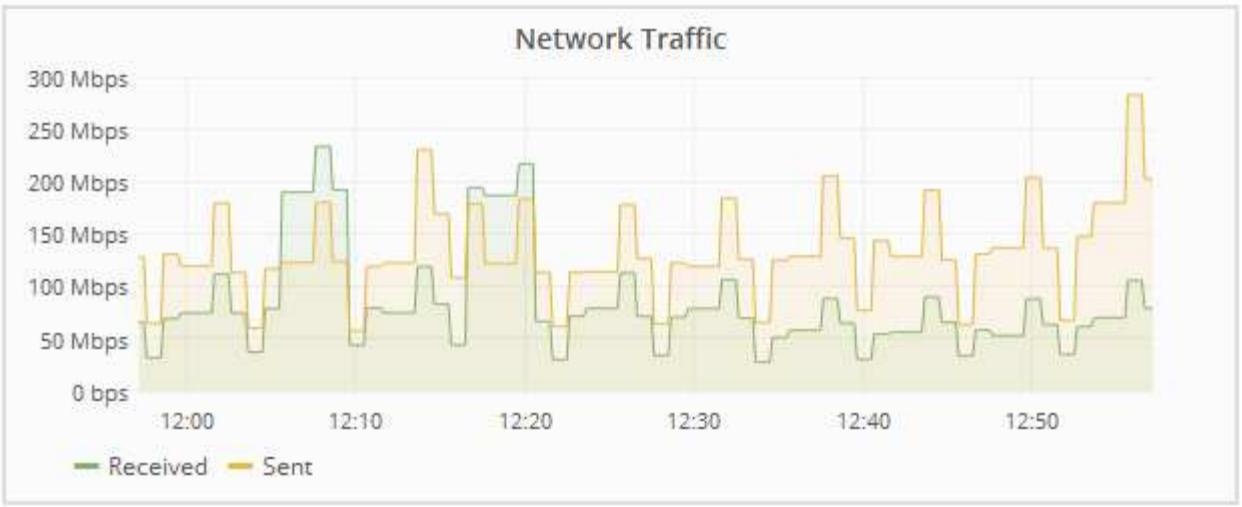
1. Wählen Sie **Knoten**.

   Die Seite Knoten wird angezeigt. Die Knotensymbole zeigen auf einen Blick an, welche Knoten verbunden sind (grünes Häkchen-Symbol) und welche Knoten getrennt sind (blaue oder graue Symbole).



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

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



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

Network Interfaces

Name	Hardware Address	Speed	Duplex	Auto Negotiate	Link Status
eth0	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
eth1	D8:C4:97:2A:E4:9E	Gigabit	Full	Off	Up
eth2	50:6B:4B:42:D7:11	100 Gigabit	Full	Off	Up
hic1	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic2	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic3	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
hic4	50:6B:4B:42:D7:11	25 Gigabit	Full	Off	Up
mtc1	D8:C4:97:2A:E4:9E	Gigabit	Full	On	Up
mtc2	D8:C4:97:2A:E4:9F	Gigabit	Full	On	Up

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

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

Network Communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame Overruns	Frames
eth0	3.250 TB	5,610,578,144	0	8,327	0	0
eth1	1.205 GB	9,828,095	0	32,049	0	0
eth2	849.829 GB	186,349,407	0	10,269	0	0
hic1	114.864 GB	303,443,393	0	0	0	0
hic2	2.315 TB	5,351,180,956	0	305	0	0
hic3	1.690 TB	1,793,580,230	0	0	0	0
hic4	194.283 GB	331,640,075	0	0	0	0
mtc1	1.205 GB	9,828,096	0	0	0	0
mtc2	1.168 GB	9,564,173	0	32,050	0	0

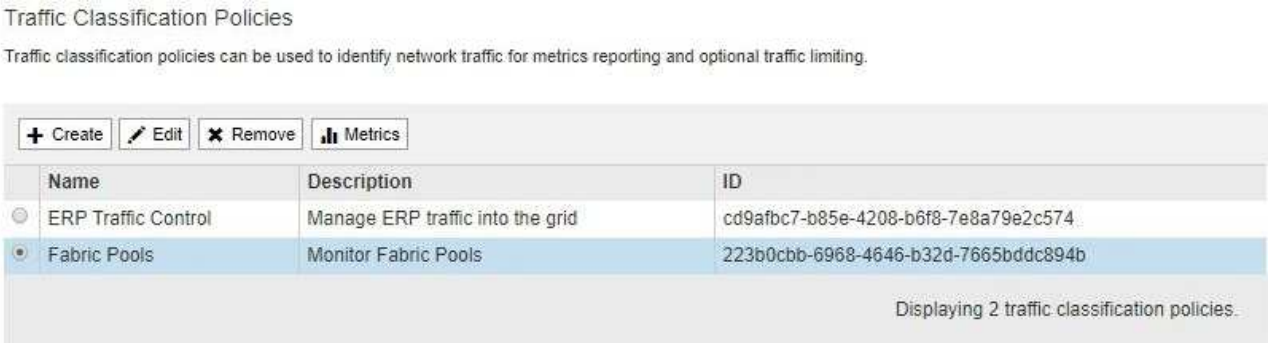
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	5.759 TB	5,789,638,626	0	0	0	0
eth1	4.563 MB	41,520	0	0	0	0
eth2	855.404 GB	139,975,194	0	0	0	0
hic1	289.248 GB	326,321,151	5	0	0	5
hic2	1.636 TB	2,640,416,419	18	0	0	18
hic3	3.219 TB	4,571,516,003	33	0	0	33
hic4	1.687 TB	1,658,180,262	22	0	0	22
mtc1	4.563 MB	41,520	0	0	0	0
mtc2	49.678 KB	609	0	0	0	0

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

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

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



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

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

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

Informationen zum Erstellen, Bearbeiten oder Löschen von Richtlinien für die Verkehrsklassifizierung finden Sie in den Anweisungen für die Verwaltung von StorageGRID.

Verwandte Informationen

"Registerkarte Netzwerk anzeigen"

"Monitoring der Verbindungsstatus der Nodes"

"StorageGRID verwalten"

Monitoring der Ressourcen auf Node-Ebene

Sie sollten einzelne Grid-Nodes überwachen, um die Ressourcenauslastung zu überprüfen.

Was Sie benötigen

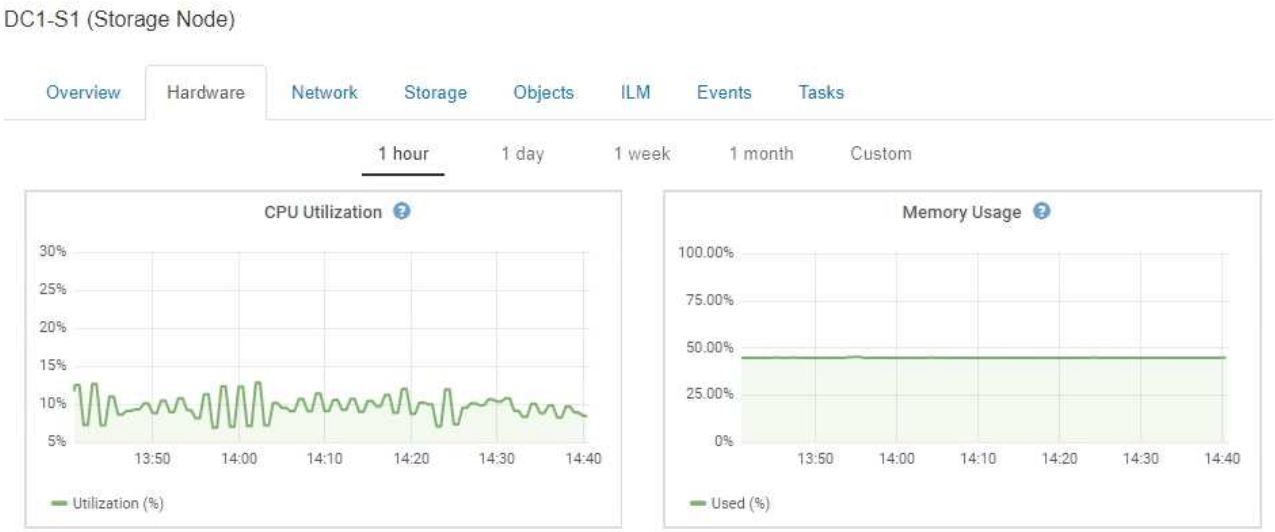
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Sind Nodes konsistent überlastet, sind möglicherweise mehr Nodes erforderlich, um einen effizienten Betrieb zu gewährleisten.

Schritte

1. So zeigen Sie Informationen zur Hardwareauslastung eines Grid-Node an:
   a. Wählen Sie auf der Seite **Nodes** den Knoten aus.
   b. Wählen Sie die Registerkarte **Hardware** aus, um Grafiken der CPU-Auslastung und der Speicherauslastung anzuzeigen.



c. Um ein anderes Zeitintervall anzuzeigen, wählen Sie eines der Steuerelemente oberhalb des Diagramms oder Diagramms aus. Sie können die verfügbaren Informationen für Intervalle von 1 Stunde, 1 Tag, 1 Woche oder 1 Monat anzeigen. Sie können auch ein benutzerdefiniertes Intervall festlegen, mit dem Sie Datum und Zeitbereiche festlegen können.

d. Wenn der Node auf einer Storage Appliance oder einer Services Appliance gehostet wird, scrollen Sie nach unten, um die Komponententabellen anzuzeigen. Der Status aller Komponenten sollte „`Nominal`“ sein. Untersuchen Sie Komponenten, die einen anderen Status haben.

Verwandte Informationen

"Anzeigen von Informationen zu Appliance-Speicherknoten"

"Anzeigen von Informationen zu Appliance Admin Nodes und Gateway Nodes"

Monitoring der Mandantenaktivitäten

Alle Client-Aktivitäten sind mit einem Mandantenkonto verknüpft. Mit dem Grid Manager lässt sich die Storage-Nutzung oder der Netzwerk-Traffic eines Mandanten überwachen. Alternativ können mit dem Audit-Protokoll oder Grafana Dashboards ausführlichere Informationen zur Verwendung von StorageGRID durch Mandanten erstellt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über Root Access oder Administrator-Berechtigung verfügen.

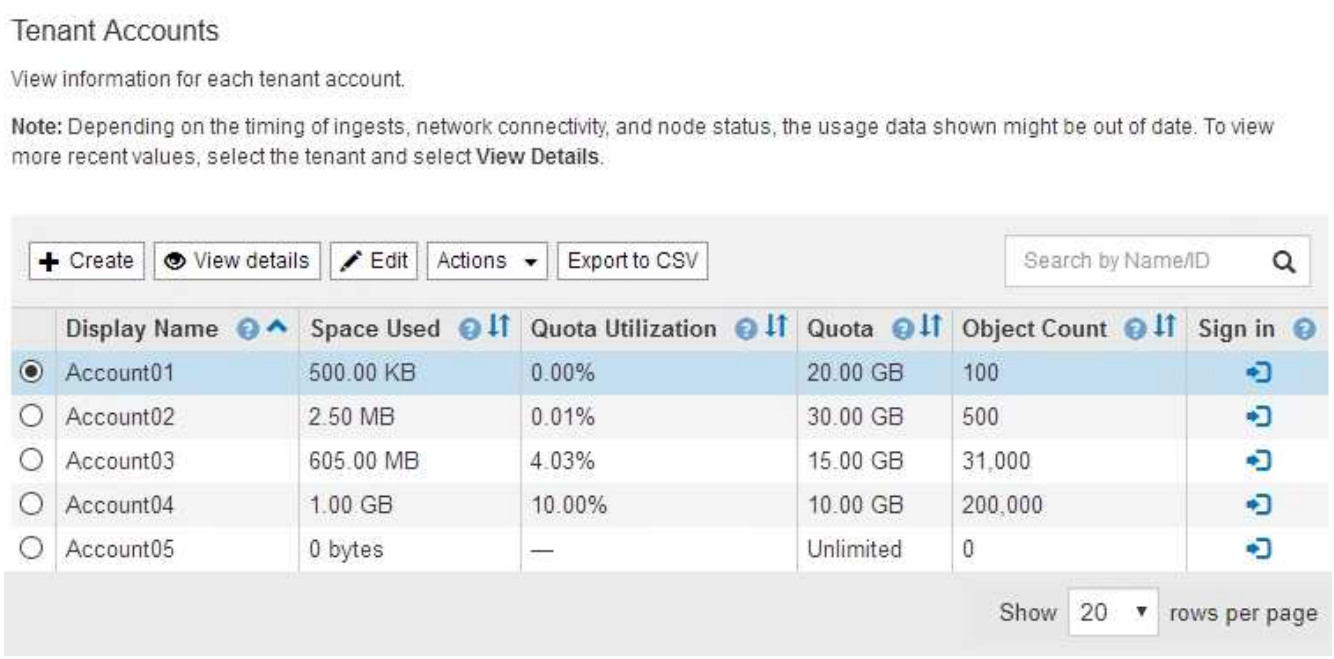
Über diese Aufgabe

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

Schritte

1. Wählen Sie **Mieter** aus, um den von allen Mietern genutzten Speicherplatz zu überprüfen.

   Für jeden Mandanten werden der genutzte Speicherplatz, die Kontingentnutzung, die Kontingente und die Objektanzahl aufgelistet. Wenn kein Kontingent für einen Mandanten festgelegt ist, enthält das Feld Quotenauslastung einen Strich (-) und das Quota-Feld gibt „`Unlimited`“ an.



Wenn Ihr System mehr als 20 Elemente enthält, können Sie festlegen, wie viele Zeilen auf jeder Seite gleichzeitig angezeigt werden. Verwenden Sie das Suchfeld, um nach einem Mandantenkonto zu suchen, indem Sie den Namen oder die Mandanten-ID anzeigen.

Sie können sich bei einem Mandantenkonto anmelden, indem Sie den Link in der Spalte **Anmelden** der Tabelle auswählen.

2. Wählen Sie optional **in CSV exportieren** aus, um eine .csv-Datei anzuzeigen und zu exportieren, die die Nutzungswerte für alle Mandanten enthält.

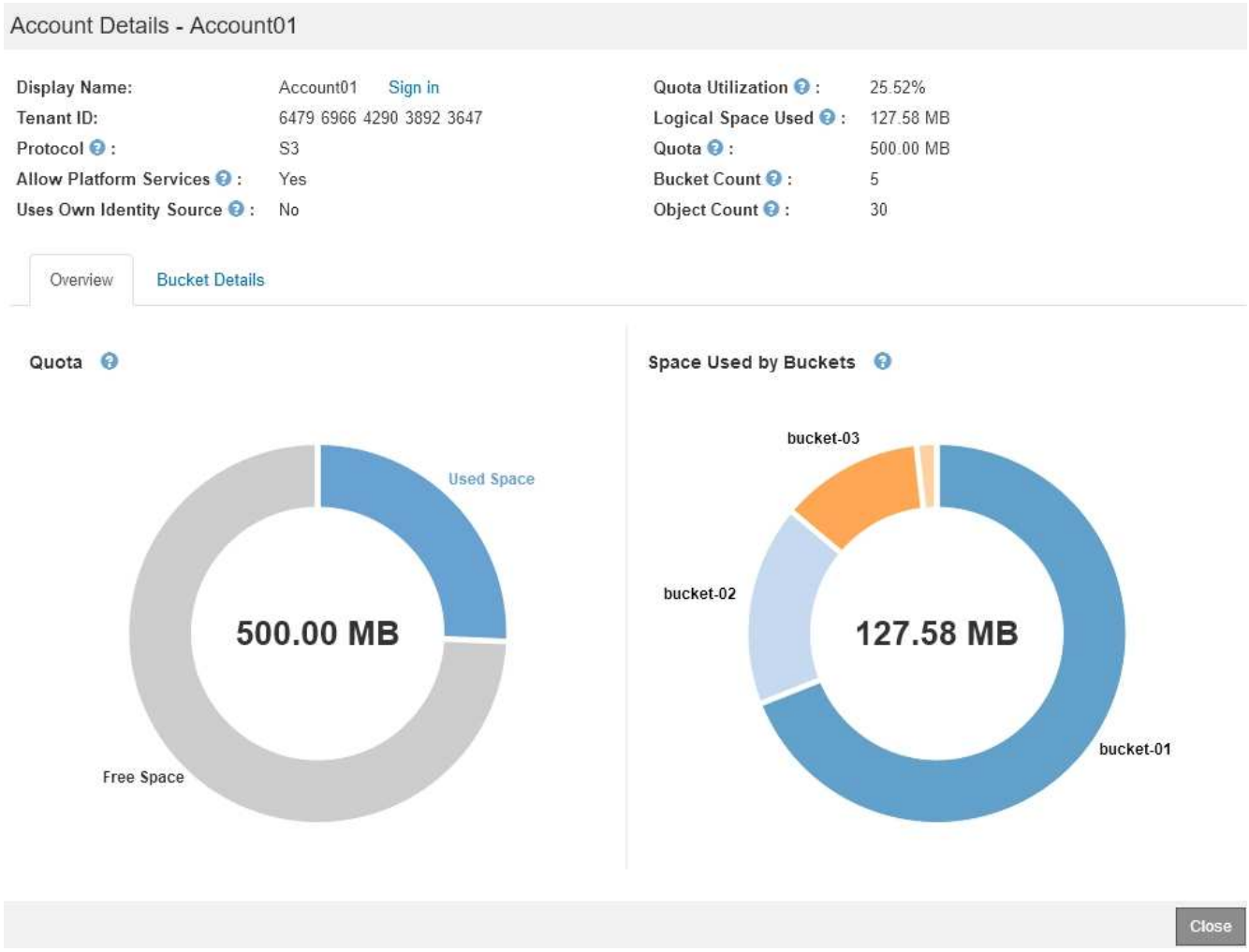
   Sie werden aufgefordert, das zu öffnen oder zu speichern `.csv` Datei:

   Der Inhalt einer .csv-Datei sieht wie das folgende Beispiel aus:

   Sie können die .csv-Datei in einer Tabellenkalkulationsanwendung öffnen oder sie automatisiert verwenden.

3. Um Details für einen bestimmten Mieter einschließlich der Nutzungsdiagramme anzuzeigen, wählen Sie auf der Seite Mandantenkonten das Mandantenkonto aus und wählen dann **Details anzeigen**.

   Die Seite Kontodetails wird angezeigt und enthält zusammenfassende Informationen, ein Diagramm, das die Anzahl der verwendeten und verbleibenden Kontingente darstellt, sowie ein Diagramm, das die Menge der Objektdaten in Buckets (S3) oder Containern (Swift) darstellt.



- **Quote**

  Wenn für diesen Mieter eine Quote festgelegt wurde, zeigt das Diagramm **quota** an, wie viel von dieser Quote dieser Mieter verwendet hat und wie viel noch verfügbar ist. Wenn kein Kontingent festgelegt wurde, hat der Mieter eine unbegrenzte Quote und eine Informationsmeldung wird angezeigt. Wenn der Mieter das Speicherkontingent um mehr als 1 % und mindestens 1 GB überschritten hat, zeigt das Diagramm das Gesamtkontingent und den Überschuss an.

  Sie können den Cursor über das Segment „verwendeter Speicherplatz“ platzieren, um die Anzahl der gespeicherten Objekte und die insgesamt verwendeten Bytes anzuzeigen. Sie können den Cursor über das Segment Freier Speicherplatz platzieren, um zu sehen, wie viele Bytes Speicherplatz verfügbar sind.

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

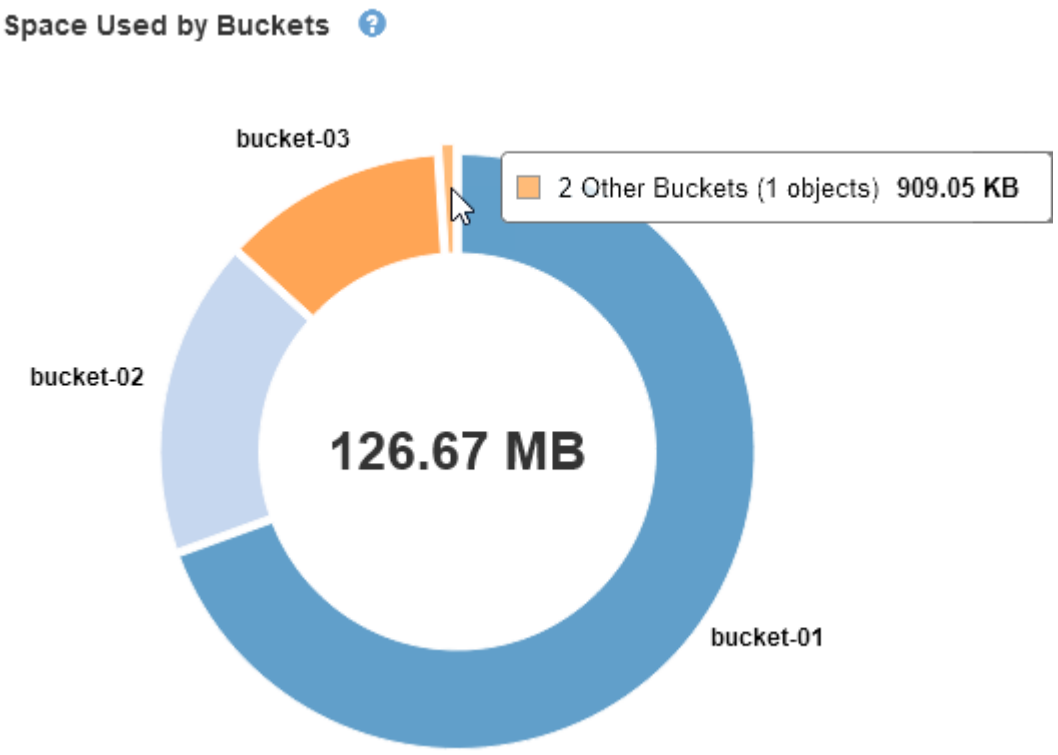
Die Kontingentnutzung eines Mandanten gibt die Gesamtanzahl der Objektdaten an, die der Mandant auf StorageGRID (logische Größe) hochgeladen hat. Die Kontingentnutzung stellt nicht den Speicherplatz dar, der zur Speicherung von Kopien dieser Objekte und ihrer Metadaten verwendet wird (physische Größe).

Sie können die Warnung * Tenant Quotenverbrauch hoch* aktivieren, um festzustellen, ob Mieter ihre Quoten verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Weitere Informationen finden Sie in der Referenz zu Warnmeldungen.

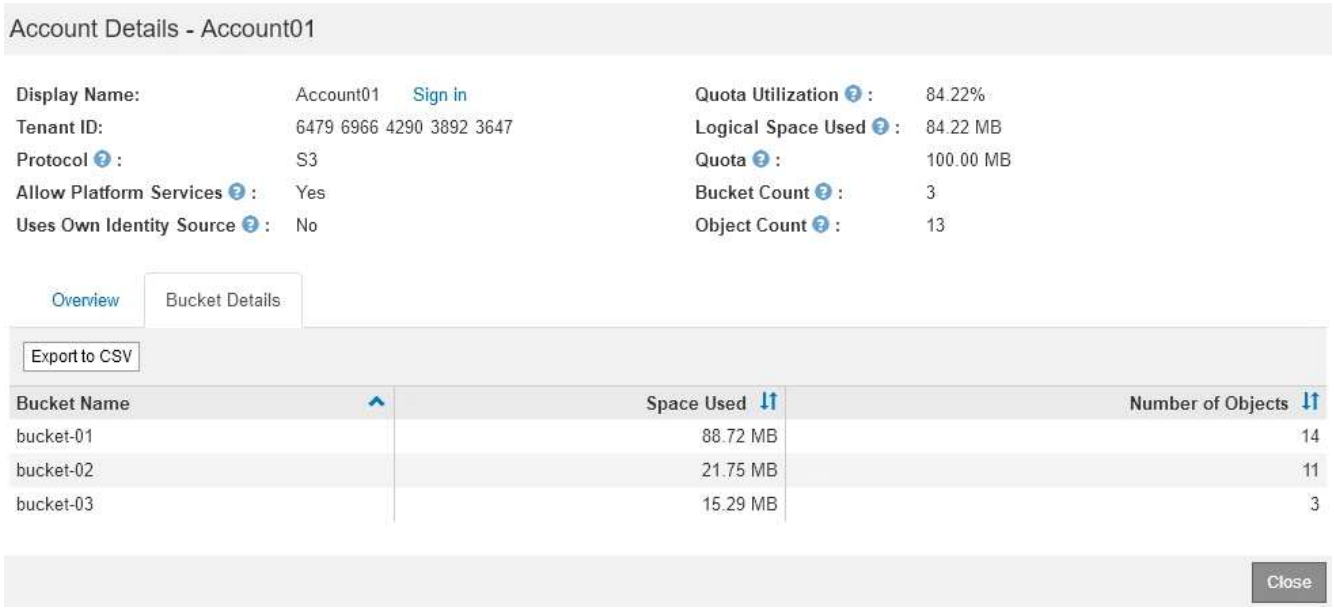
- **Verwendeter Platz**

  Das Diagramm **Space used by Buckets** (S3) or **Space used by Containers** (Swift) zeigt die größten Eimer für den Mieter. Der verwendete Speicherplatz ist die Gesamtgröße der Objektdaten im Bucket. Dieser Wert stellt nicht den Storage-Platzbedarf für ILM-Kopien und Objekt-Metadaten dar.

  Wenn der Mandant mehr als neun Buckets oder Container enthält, werden sie in einem Segment zusammengefasst, das als „Sonstige“ bezeichnet wird. Einige Diagrammsegmente sind möglicherweise zu klein, um ein Etikett aufzunehmen. Sie können den Cursor auf ein beliebiges Segment setzen, um die Beschriftung zu sehen und weitere Informationen zu erhalten, darunter die Anzahl der gespeicherten Objekte und die Gesamtzahl der Bytes für jeden Bucket oder Container.



4. Wählen Sie **Bucket Details** (S3) oder **Container Details** (Swift) aus, um eine Liste der verwendeten Abstände und die Anzahl der Objekte für die einzelnen Buckets oder Container des Mandanten anzuzeigen.



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

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

   Der Inhalt der .csv-Datei eines einzelnen S3-Mandanten sieht wie folgt aus:

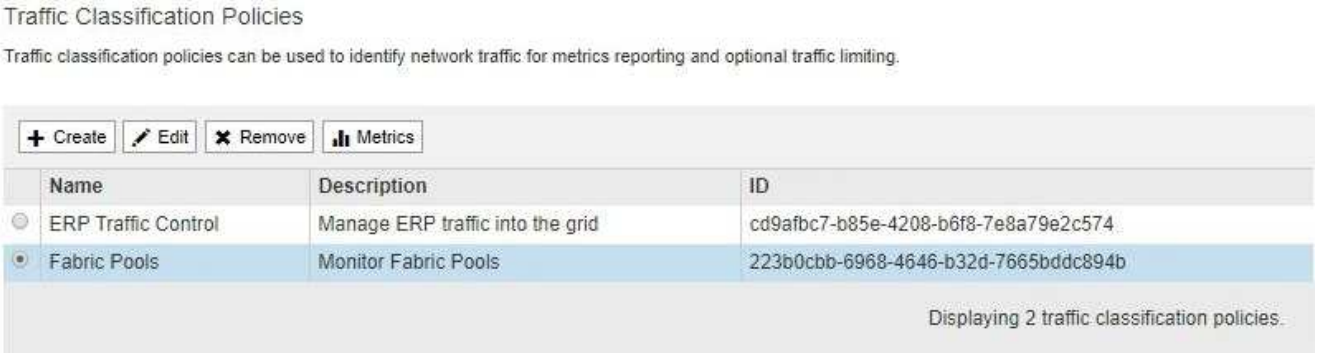
Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   Sie können die .csv-Datei in einer Tabellenkalkulationsanwendung öffnen oder sie automatisiert verwenden.

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

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

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



   a. Anhand der Liste der Richtlinien können Sie diejenigen ermitteln, die für einen bestimmten Mandanten

gelten.

b. Um Metriken anzuzeigen, die mit einer Richtlinie verknüpft sind, wählen Sie das Optionsfeld links neben der Richtlinie aus, und klicken Sie dann auf **Metriken**.

c. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

   Informationen zum Erstellen, Bearbeiten oder Löschen von Richtlinien für die Verkehrsklassifizierung finden Sie in den Anweisungen für die Verwaltung von StorageGRID.

7. Optional können Sie das Audit-Protokoll verwenden, um eine granularere Überwachung der Aktivitäten eines Mandanten zu ermöglichen.

   Sie können beispielsweise folgende Informationstypen überwachen:

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

   Audit-Protokolle werden in Textdateien geschrieben, die Sie mit einem Tool Ihrer Wahl analysieren können. Dadurch können Sie Kundenaktivitäten besser verstehen oder ausgereifte Chargeback- und Abrechnungsmodelle implementieren. Weitere Informationen finden Sie in den Anweisungen zum Verständnis von Überwachungsmeldungen.

8. Optional können Sie mit den Prometheus Kennzahlen die Mandantenaktivität erfassen:

   - Wählen Sie im Grid Manager die Option **Support** > **Tools** > **Metriken** aus. Kunden können vorhandene Dashboards wie S3 Overview zur Überprüfung von Client-Aktivitäten nutzen.

     > Die auf der Seite Metriken verfügbaren Tools sind in erster Linie für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig.

   - Wählen Sie **Hilfe** > **API-Dokumentation**. Sie können die Kennzahlen im Abschnitt „Kennzahlen“ der Grid Management API verwenden, um benutzerdefinierte Alarmregeln und Dashboards für Mandantenaktivitäten zu erstellen.

Verwandte Informationen

"Alerts Referenz"

"Prüfung von Audit-Protokollen"

"StorageGRID verwalten"

"Überprüfen von Support-Metriken"

Monitoring der Archivierungskapazität

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

Was Sie benötigen

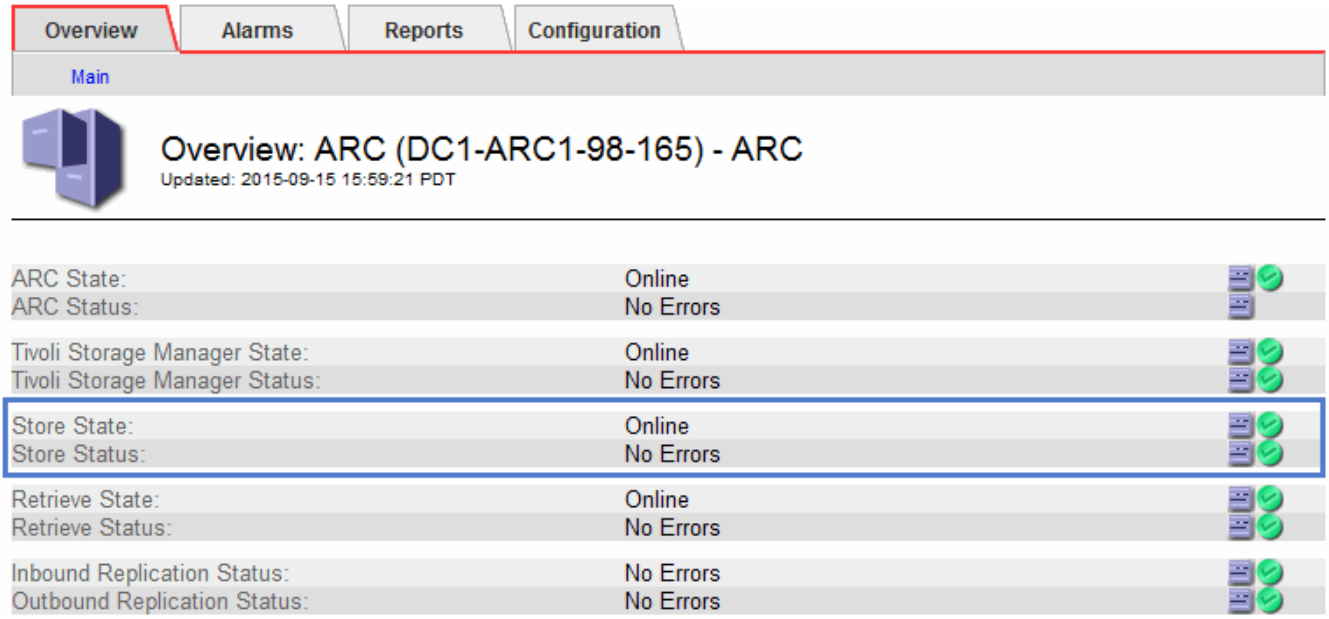
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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

Schritte

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



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

Verwandte Informationen

"StorageGRID verwalten"

Monitoring von Lastverteilungsvorgängen

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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

Der CLB-Service ist veraltet.

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

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

Lesen Sie den Abschnitt zum Konfigurieren von Client-Verbindungen in den Anweisungen zur Administration von StorageGRID.

Schritte

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

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

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

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

   f. Prüfen Sie das Diagramm der eingehenden Lastbalancer-Anfragerate für die letzte Woche, um den Objektdurchsatz des Nodes zu überprüfen.
   g. Wiederholen Sie diese Schritte für jeden Admin-Node oder Gateway-Node im StorageGRID-System.
   h. Optional können Sie anhand von Traffic-Klassifizierungsrichtlinien eine detailliertere Aufschlüsselung des vom Load Balancer Service servierten Datenverkehrs anzeigen.
2. Wenn S3- oder Swift-Clients eine Verbindung über den CLB-Service (veraltet) herstellen, führen Sie die folgenden Prüfungen durch:
   a. Wählen Sie **Knoten**.
   b. Wählen Sie einen Gateway-Node aus.
   c. Überprüfen Sie auf der Registerkarte **Übersicht**, ob sich eine Knotenschnittstelle in einer HA-Gruppe befindet und ob die Knotenschnittstelle die Rolle des Master hat.

      Nodes mit der Rolle „Master“ und Nodes, die sich nicht in einer HA-Gruppe befinden, sollten Anfragen

aktiv an die Clients verteilen.

d. Wählen Sie für jeden Gateway Node, der Clientanforderungen aktiv verteilen soll, **Support** > **Tools** > **Grid Topology** aus.

e. Wählen Sie ***Gateway Node*** > **CLB** > **HTTP** > **Übersicht** > **Main** aus.

f. Überprüfen Sie die Anzahl der **eingehenden Sitzungen - eingerichtet**, um zu überprüfen, ob der Gateway-Node aktiv Anforderungen bearbeitet hat.

3. Stellen Sie sicher, dass diese Anfragen gleichmäßig auf Speicherknoten verteilt werden.

a. Wählen Sie ***Storage Node*** > **LDR** > **HTTP** aus.

b. Überprüfen Sie die Anzahl der **derzeit festgelegten eingehenden Sitzungen**.

c. Wiederholen Sie diesen Vorgang für jeden Speicherknoten im Raster.

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

Verwandte Informationen

"StorageGRID verwalten"

"Anzeigen der Registerkarte Load Balancer"

Anwenden von Hotfixes oder Aktualisieren der Software, falls erforderlich

Wenn ein Hotfix oder eine neue Version der StorageGRID-Software verfügbar ist, sollten Sie prüfen, ob das Update für Ihr System geeignet ist, und installieren Sie es, falls erforderlich.

Über diese Aufgabe

StorageGRID Hotfixes enthalten Software-Änderungen, die außerhalb einer Feature- oder Patch-Freigabe verfügbar gemacht werden. Die gleichen Änderungen sind in einer zukünftigen Version enthalten.

Schritte

1. StorageGRID finden Sie auf der Seite zu NetApp Downloads.

"NetApp Downloads: StorageGRID"

2. Wählen Sie den Abwärtspfeil für das Feld **Typ/Version auswählen** aus, um eine Liste der zum Herunterladen verfügbaren Aktualisierungen anzuzeigen:

- **StorageGRID Software-Versionen**: 11.*x.y*
- **StorageGRID Hotfixes**: 11.*x. y.y.z*

3. Überprüfen Sie die Änderungen, die im Update enthalten sind:

a. Wählen Sie die Version aus dem Pulldown-Menü aus und klicken Sie auf **Go**.

b. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.

c. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Akzeptieren und fortfahren**.

Die Download-Seite für die ausgewählte Version wird angezeigt.

4. Erfahren Sie mehr über die Änderungen in der Softwareversion oder Hotfix.

- Informationen zu einer neuen Softwareversion finden Sie im Thema „`Was ist neu`“ in den Anweisungen zum Aktualisieren von StorageGRID.
- Für einen Hotfix laden Sie die README-Datei herunter, um eine Zusammenfassung der Änderungen im Hotfix zu erhalten.

5. Wenn Sie entscheiden, dass ein Softwareupdate erforderlich ist, suchen Sie die Anweisungen, bevor Sie fortfahren.
   - Folgen Sie bei einer neuen Softwareversion sorgfältig den Anweisungen für das Upgrade von StorageGRID.
   - Suchen Sie bei einem Hotfix in der Recovery- und Wartungsanleitung nach dem Hotfix-Verfahren

Verwandte Informationen

"Software-Upgrade"

"Verwalten Sie erholen"

Verwalten von Meldungen und Alarmen

Das StorageGRID Alert System wurde entwickelt, um Sie über betriebliche Probleme zu informieren, die Ihre Aufmerksamkeit erfordern. Bei Bedarf können Sie auch das alte Alarmsystem zur Überwachung Ihres Systems verwenden. Dieser Abschnitt enthält die folgenden Unterabschnitte:

- "Vergleichen von Meldungen und Alarmen"
- "Verwalten von Meldungen"
- "Verwalten von Alarmen (Altsystem)"

StorageGRID beinhaltet zwei Systeme, mit denen Sie über Probleme informiert werden.

Meldungssystem

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

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

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

Altes Alarmsystem

Das Alarmsystem wird unterstützt, gilt jedoch als ein altes System. Wie bei Warnungen werden auch Alarme

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

Wenn ein Alarm ausgelöst wird, treten folgende Aktionen auf:

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

Vergleichen von Meldungen und Alarmen

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

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

	Meldungen	**Alarme (Altsystem)**
Wie sehe ich, welche Alarme oder Alarme aktiv sind?	• Klicken Sie im Dashboard auf den Link **Aktuelle Alarme**. • Klicken Sie auf der Seite **Nodes** > **Übersicht** auf den Hinweis. • Wählen Sie **Alarme** > **Aktuell**. "Anzeigen aktueller Meldungen"	• Klicken Sie im Dashboard auf den Link **Legacy-Alarme**. • Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**. "Anzeigen von Legacy-Alarmen"
Was bewirkt, dass eine Meldung oder eine Warnung ausgelöst wird?	Alarme werden ausgelöst, wenn ein Prometheus-Ausdruck in einer Alarmregel für die spezifische Triggerbedingung und -Dauer als wahr bewertet wird. "Anzeigen von Meldungsregeln"	Alarme werden ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht. "Alarmauslöselogik (Älteres System)"

	Meldungen	Alarme (Altsystem)
Wie kann ich das zugrunde liegende Problem lösen, wenn eine Meldung oder ein Alarm ausgelöst wird?	Die empfohlenen Aktionen für eine Warnmeldung sind in E-Mail-Benachrichtigungen enthalten und stehen auf den Alerts-Seiten im Grid Manager zur Verfügung. Falls erforderlich, werden weitere Informationen in der StorageGRID-Dokumentation bereitgestellt. "Alerts Referenz"	Sie können sich über einen Alarm informieren, indem Sie auf den Attributnamen klicken. Alternativ können Sie in der StorageGRID-Dokumentation nach einem Alarmcode suchen. "Alarmreferenz (Altsystem)"
Wo kann eine Liste der Warnungen oder Alarme gelöst werden?	• Klicken Sie auf dem Dashboard auf den Link * Kürzlich aufgelöste Warnmeldungen*. • Wählen Sie **Alarme** > **Aufgelöst**. "Anzeigen gelöster Warnmeldungen"	Wählen Sie **Support** > **Alarme (alt)** > **Historische Alarme**. "Überprüfung historischer Alarme und Alarmfrequenz (Altsystem)"
Wo kann ich die Einstellungen verwalten?	Wählen Sie **Alarme**. Verwenden Sie anschließend die Optionen im Menü Meldungen. "Verwalten von Meldungen"	Wählen Sie **Support**. Verwenden Sie dann die Optionen im Abschnitt **Alarme (alt)** des Menüs. "Verwalten von Alarmen (Altsystem)"
Welche Benutzergruppenberechtigungen brauche ich?	• Jeder, der sich beim Grid Manager anmelden kann, kann aktuelle und behobene Warnmeldungen anzeigen. • Sie müssen über die Berechtigung zum Verwalten von Warnungen verfügen, um Stille, Warnmeldungen und Alarmregeln zu verwalten. "StorageGRID verwalten"	• Jeder, der sich beim Grid Manager anmelden kann, kann ältere Alarme anzeigen. • Sie müssen über die Berechtigung Alarme quittieren verfügen, um Alarme zu quittieren. • Zur Verwaltung globaler Alarme und E-Mail-Benachrichtigungen müssen Sie sowohl über die Seitenkonfiguration der Grid-Topologie als auch über andere Grid-Konfigurationen verfügen. "StorageGRID verwalten"

	Meldungen	Alarme (Altsystem)
Wie managt ich E-Mail-Benachrichtigungen?	Wählen Sie **Alarme** > **E-Mail-Einrichtung**. **Hinweis:** Da Alarme und Alarme unabhängige Systeme sind, wird das E-Mail-Setup für Alarm- und AutoSupport-Benachrichtigungen nicht für Benachrichtigungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden. "Verwalten von Warnmeldungen"	Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. "Konfigurieren von Benachrichtigungen für Alarme (Legacy-System)"
Wie verwalte ich SNMP Benachrichtigungen?	Wählen Sie **Konfiguration** > **Überwachung** > **SNMP-Agent**. "Verwendung von SNMP-Überwachung"	Wählen Sie **Konfiguration** > **Überwachung** > **SNMP-Agent**. "Verwendung von SNMP-Überwachung" **Hinweis**: SNMP-Benachrichtigungen werden nicht für jeden Alarm oder Alarm Schweregrad gesendet. "Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"
Wie kontrolliere ich, wer Benachrichtigungen erhält?	1. Wählen Sie **Alarme** > **E-Mail-Einrichtung**. 2. Geben Sie im Abschnitt **Empfänger** eine E-Mail-Adresse für jede E-Mail-Liste oder Person ein, die eine E-Mail erhalten soll, wenn eine Benachrichtigung erfolgt. "Einrichten von E-Mail-Benachrichtigungen für Meldungen"	1. Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. 2. Mailingliste wird erstellt. 3. Wählen Sie **Benachrichtigungen**. 4. Wählen Sie die Mailingliste aus. "Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)" "Konfigurieren von E-Mail-Benachrichtigungen für Alarme (Altsystem)"
Welche Admin Nodes senden Benachrichtigungen?	Ein einziger Admin-Node (der „`bevorzugte Absender`“). "StorageGRID verwalten"	Ein einziger Admin-Node (der „`bevorzugte Absender`“). "StorageGRID verwalten"

	Meldungen	Alarme (Altsystem)
Wie kann ich einige Benachrichtigungen unterdrücken?	1. Wählen Sie **Alarme** > **Stille**. 2. Wählen Sie die Alarmregel aus, die stummschalten soll. 3. Geben Sie eine Dauer für die Stille an. 4. Wählen Sie den Schweregrad der Warnmeldung aus, den Sie stummschalten möchten. 5. Wählen Sie diese Option aus, um die Stille auf das gesamte Raster, einen einzelnen Standort oder einen einzelnen Knoten anzuwenden. **Hinweis**: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. "Stummschalten von Warnmeldungen"	1. Wählen Sie **Support** > **Alarme (alt)** > **Legacy E-Mail-Einrichtung**. 2. Wählen Sie **Benachrichtigungen**. 3. Wählen Sie eine Mailingliste aus, und wählen Sie **unterdrücken**. "Unterdrückung von Alarmmeldungen für eine Mailingliste (Legacy-System)"
Wie kann ich alle Benachrichtigungen unterdrücken?	Wählen Sie **Alarme** > **Stille** und dann **Alle Regeln**. **Hinweis**: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. "Stummschalten von Warnmeldungen"	1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**. 2. Aktivieren Sie das Kontrollkästchen **Benachrichtigung Alle unterdrücken**. **Hinweis**: Das Unterdrückung von E-Mail-Benachrichtigungen systemweit unterdrückt auch ereignisgesteuerte AutoSupport-E-Mails. "Systemweite Unterdrückung von E-Mail-Benachrichtigungen"

	Meldungen	Alarme (Altsystem)
Wie kann ich die Bedingungen und Trigger anpassen?	1. Wählen Sie **Alarme** > **Warnregeln**. 2. Wählen Sie eine Standardregel zum Bearbeiten aus, oder wählen Sie **benutzerdefinierte Regel erstellen**. "Bearbeiten einer Meldungsregel" "Erstellen benutzerdefinierter Warnungsregeln"	1. Wählen Sie **Support** > **Alarme (alt)** > **Globale Alarme**. 2. Erstellen Sie einen globalen benutzerdefinierten Alarm, um einen Standardalarm zu überschreiben oder ein Attribut zu überwachen, das keinen Standardalarm hat. "Erstellen von globalen benutzerdefinierten Alarmen (Legacy-System)"
Wie deaktiviere ich eine einzelne Warnung oder einen einzelnen Alarm?	1. Wählen Sie **Alarme** > **Warnregeln**. 2. Wählen Sie die Regel aus, und klicken Sie auf **Regel bearbeiten**. 3. Deaktivieren Sie das Kontrollkästchen **aktiviert**. "Deaktivieren einer Meldungsregel"	1. Wählen Sie **Support** > **Alarme (alt)** > **Globale Alarme**. 2. Wählen Sie die Regel aus, und klicken Sie auf das Symbol Bearbeiten. 3. Deaktivieren Sie das Kontrollkästchen **aktiviert**. "Deaktivieren eines Standardalarms (älteres System)" "Deaktivieren von globalen benutzerdefinierten Alarmen (Legacy-System)"

Verwalten von Meldungen

Mithilfe von Meldungen können Sie verschiedene Ereignisse und Bedingungen innerhalb des StorageGRID Systems überwachen. Sie können Benachrichtigungen verwalten, indem Sie benutzerdefinierte Warnmeldungen erstellen, Standardwarnungen bearbeiten oder deaktivieren, E-Mail-Benachrichtigungen für Warnungen einrichten und Benachrichtigungen deaktivieren.

Verwandte Informationen

"Anzeigen aktueller Meldungen"

"Anzeigen gelöster Warnmeldungen"

"Anzeigen einer bestimmten Meldung"

"Alerts Referenz"

Um welche Warnmeldungen geht es

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

- Das Warnsystem konzentriert sich auf umsetzbare Probleme im System. Anders als bei einigen Alarmen im Legacy-System werden bei Ereignissen, die eine sofortige Aufmerksamkeit erfordern, Warnmeldungen ausgelöst und nicht bei Ereignissen, die sicher ignoriert werden können.
- Die Seite „Aktuelle Meldungen“ bietet eine benutzerfreundliche Oberfläche zum Anzeigen aktueller Probleme. Sie können die Liste nach einzelnen Warnungen und Alarmgruppen sortieren. Beispielsweise können Sie alle Meldungen nach Node/Standort sortieren, um zu sehen, welche Meldungen sich auf einen bestimmten Node auswirken. Oder Sie möchten die Meldungen in einer Gruppe nach der Zeit sortieren, die ausgelöst wird, um die letzte Instanz einer bestimmten Warnmeldung zu finden.
- Die Seite „gelöste Warnmeldungen“ enthält ähnliche Informationen wie auf der Seite „Aktuelle Meldungen“. Sie können jedoch einen Verlauf der behobenen Warnmeldungen suchen und anzeigen, einschließlich des Auslöseverlaufs und der Behebung des Alarms.
- Mehrere Warnmeldungen desselben Typs werden in einer E-Mail gruppiert, um die Anzahl der Benachrichtigungen zu reduzieren. Darüber hinaus werden auf der Seite „Meldungen“ mehrere Warnmeldungen desselben Typs als Gruppe angezeigt. Sie können Warnungsgruppen erweitern oder ausblenden, um die einzelnen Warnmeldungen ein- oder auszublenden. Wenn z. B. mehrere Knoten die Meldung **nicht in der Lage, mit Knoten** zu kommunizieren ungefähr zur gleichen Zeit melden, wird nur eine E-Mail gesendet und die Warnung wird als Gruppe auf der Seite Warnungen angezeigt.
- Warnmeldungen verwenden intuitive Namen und Beschreibungen, um das Problem schnell zu verstehen. Meldungsbenachrichtigungen umfassen Details zum betroffenen Node und Standort, den Schweregrad der Warnmeldung, den Zeitpunkt, zu dem die Meldungsregel ausgelöst wurde, und den aktuellen Wert der Metriken in Bezug auf die Meldung.
- Warnmeldungen per E-Mail und die auf den Seiten „Aktuelle Warnmeldungen und gelöste Warnmeldungen“ angezeigten Warnmeldungen enthalten empfohlene Aktionen zur Behebung von Warnmeldungen. Dazu gehören häufig direkte Links zum StorageGRID Dokumentationszentrum, damit detailliertere Fehlerbehebungsmaßnahmen leichter gefunden und zugänglich sind.
- Wenn Sie die Benachrichtigungen für eine Warnung vorübergehend auf einem oder mehreren Schweregraden unterdrücken müssen, können Sie ganz einfach eine bestimmte Alarmregel für eine bestimmte Dauer und für das gesamte Grid, eine einzelne Site oder einen einzelnen Node stummschalten. Sie können auch während einer geplanten Wartung, z. B. einer Software-Aktualisierung, alle Alarmregeln stummschalten.
- Sie können die standardmäßigen Alarmregeln nach Bedarf bearbeiten. Sie können eine Meldungsregel vollständig deaktivieren oder deren Triggerbedingungen und -Dauer ändern.
- Sie können benutzerdefinierte Alarmregeln erstellen, um auf die für Ihre Situation relevanten spezifischen Bedingungen abzielen und eigene Empfehlungen auszuarbeiten. Um die Bedingungen für eine benutzerdefinierte Warnung zu definieren, erstellen Sie Ausdrücke mithilfe der Prometheus-Metriken, die im Abschnitt Kennzahlen der Grid Management API verfügbar sind.

Verwalten von Meldungsregeln

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

Anzeigen von Meldungsregeln

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

Was Sie benötigen

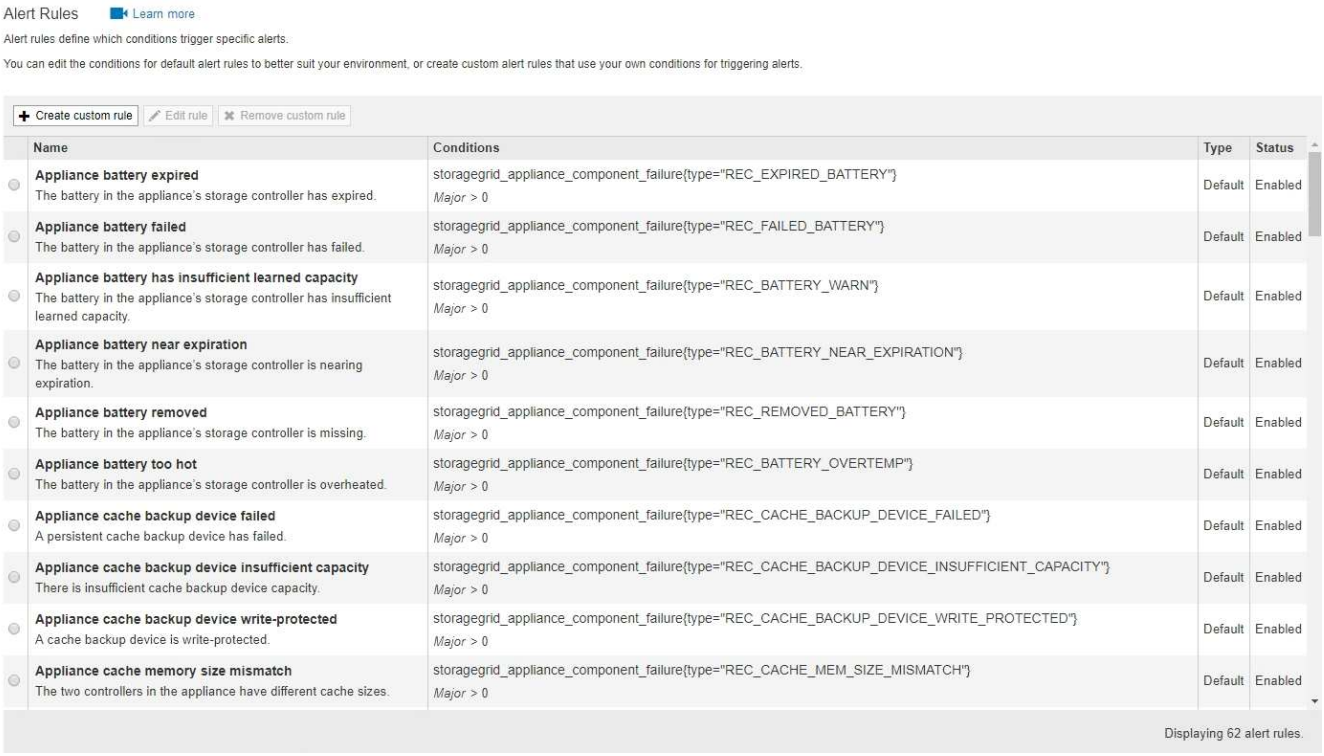
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.



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

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

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

Spaltenüberschrift	Beschreibung
Status	Gibt an, ob diese Warnungsregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnregeln werden nicht ausgewertet, sodass keine Warnmeldungen ausgelöst werden.

Verwandte Informationen

"Alerts Referenz"

Erstellen benutzerdefinierter Warnungsregeln

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Über diese Aufgabe

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

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

  Zum Beispiel zum Testen des Ausdrucks `node_memory_MemTotal_bytes < 24000000000`, Erste Ausführung `node_memory_MemTotal_bytes >= 0` Und stellen Sie sicher, dass Sie die erwarteten Ergebnisse erhalten (alle Knoten geben einen Wert zurück). Ändern Sie dann den Operator und den Schwellenwert wieder auf die gewünschten Werte und führen Sie die Ausführung erneut aus. Keine Ergebnisse zeigen an, dass für diesen Ausdruck keine aktuellen Warnmeldungen vorhanden sind.

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

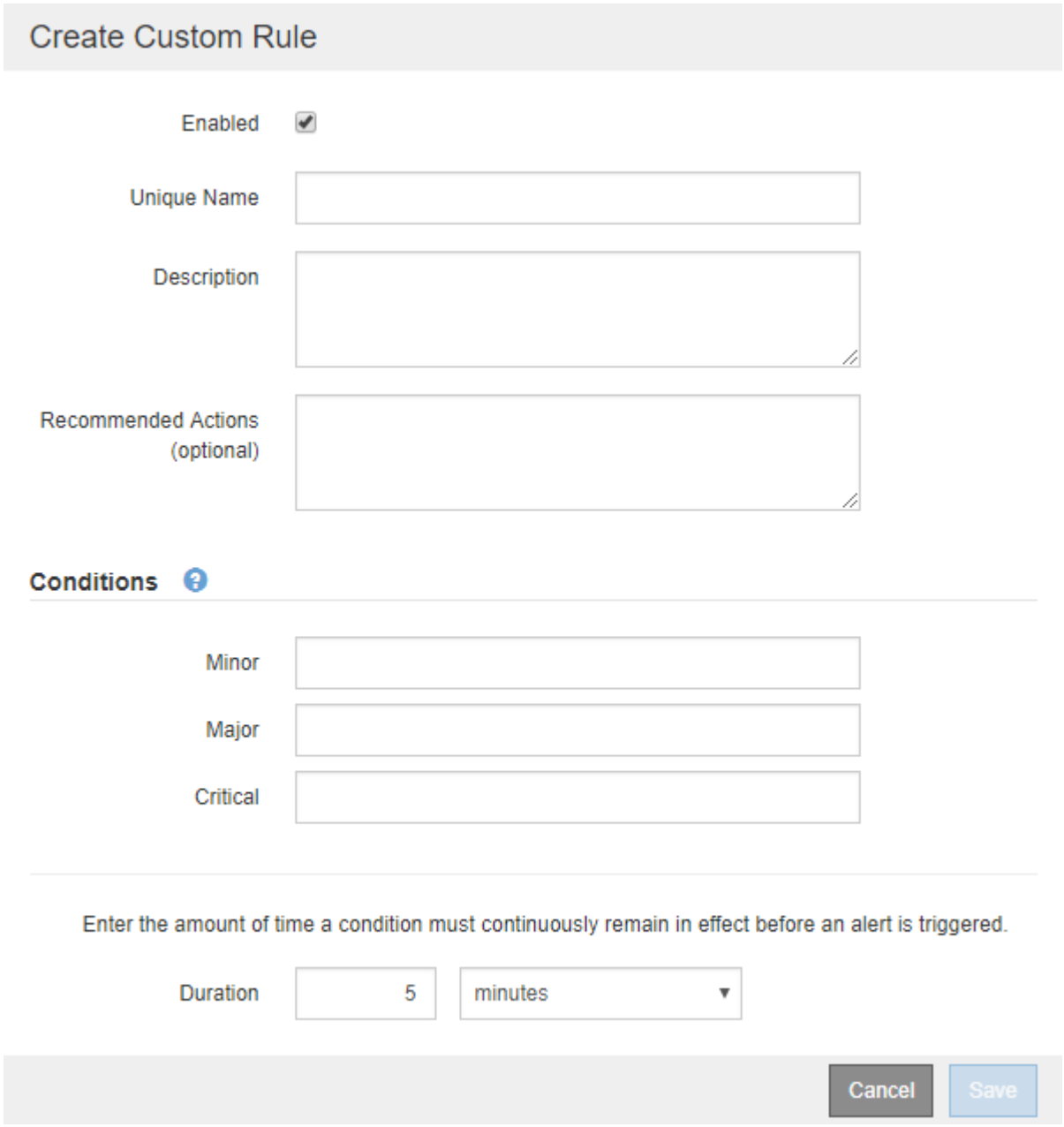
Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.

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

Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.



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

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

4. Geben Sie die folgenden Informationen ein:

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

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

   Ein Grundausdruck ist in der Regel die Form:

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

   Ausdrücke können eine beliebige Länge haben, aber in einer einzigen Zeile in der Benutzeroberfläche angezeigt werden. Mindestens ein Ausdruck ist erforderlich.

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

   Informationen über die Verwendung der Grid-Management-API finden Sie in den Anweisungen für die Administration von StorageGRID. Einzelheiten zur Syntax der Prometheus-Abfragen finden Sie in der Dokumentation für Prometheus.

   Dieser Ausdruck bewirkt, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Knoten weniger als 24,000,000,000 Byte (24 GB) beträgt.

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

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

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

Der Standardwert ist 5 Minuten.

7. Klicken Sie Auf **Speichern**.

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

Verwandte Informationen

"StorageGRID verwalten"

"Häufig verwendete Prometheus-Kennzahlen"

"Prometheus: Grundlagen der Abfrage"

Bearbeiten einer Meldungsregel

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Über diese Aufgabe

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

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

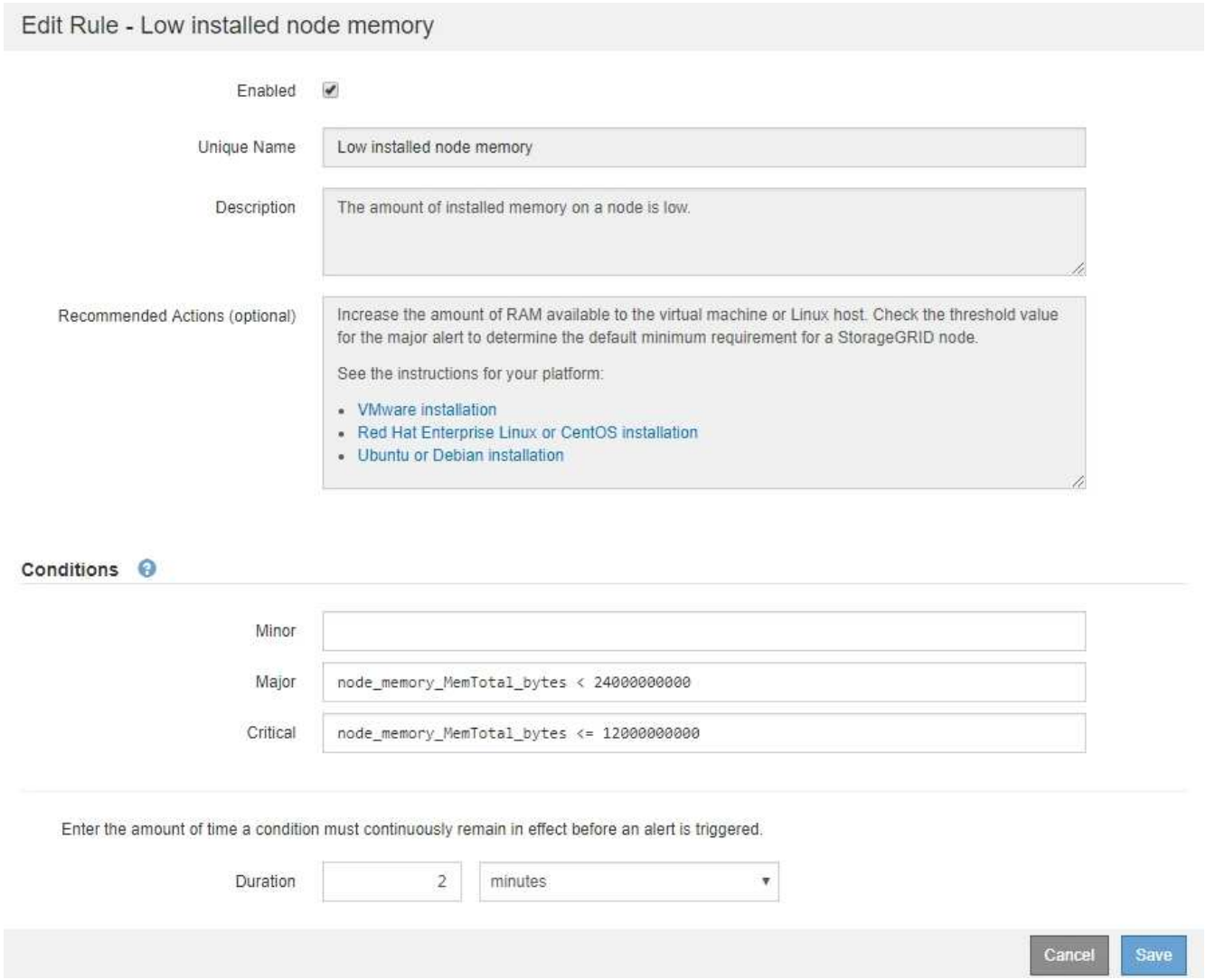
Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.

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

   Das Dialogfeld Regel bearbeiten wird angezeigt. In diesem Beispiel wird eine Standardwarnregel angezeigt: 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 Alarmregel derzeit aktiviert ist.

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

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

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

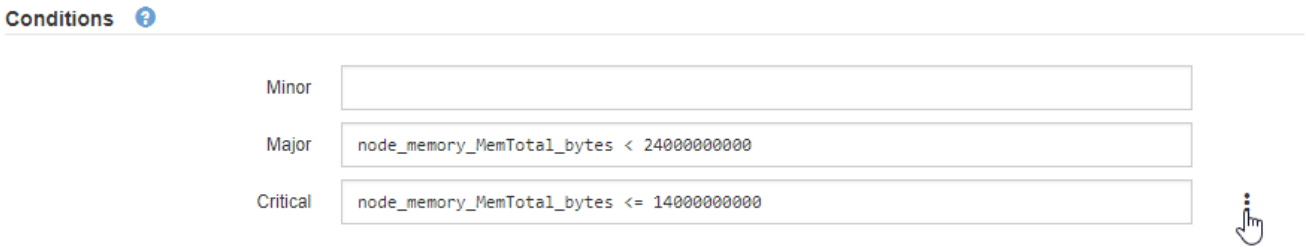
5. Aktualisieren Sie für benutzerdefinierte Warnungsregeln die folgenden Informationen, falls erforderlich.

   Diese Informationen können nicht für Standardwarnregeln bearbeitet werden.

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

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

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



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

Ein Grundausdruck ist in der Regel die Form:

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

Ausdrücke können eine beliebige Länge haben, aber in einer einzigen Zeile in der Benutzeroberfläche angezeigt werden. Mindestens ein Ausdruck ist erforderlich.

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

Informationen über die Verwendung der Grid-Management-API finden Sie in den Anweisungen für die Administration von StorageGRID. Einzelheiten zur Syntax der Prometheus-Abfragen finden Sie in der Dokumentation für Prometheus.

Dieser Ausdruck bewirkt, dass eine Warnung ausgelöst wird, wenn die Menge des installierten RAM für einen Knoten weniger als 24,000,000,000 Byte (24 GB) beträgt.

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

   Der Standardwert ist 5 Minuten.

8. Klicken Sie Auf **Speichern**.

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

Verwandte Informationen

"StorageGRID verwalten"

"Häufig verwendete Prometheus-Kennzahlen"

"Prometheus: Grundlagen der Abfrage"

Deaktivieren einer Meldungsregel

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Über diese Aufgabe

Wenn eine Meldungsregel deaktiviert ist, werden seine Ausdrücke nicht ausgewertet und es werden keine Warnmeldungen ausgelöst.

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

Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.

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

   Das Dialogfeld Regel bearbeiten wird angezeigt.

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

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

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

5. Klicken Sie Auf **Speichern**.

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

Entfernen einer benutzerdefinierten Warnungsregel

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Schritte

1. Wählen Sie **Alarme** > **Warnregeln**.

   Die Seite Alarmregeln wird angezeigt.

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

   Sie können keine Standardwarnregel entfernen.

3. Klicken Sie auf **Benutzerdefinierte Regel entfernen**.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf **OK**, um die Warnregel zu entfernen.

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

Verwalten von Warnmeldungen

Wenn eine Warnmeldung ausgelöst wird, kann StorageGRID E-Mail-Benachrichtigungen und SNMP-Benachrichtigungen (Simple Network Management Protocol) senden.

Einrichten von SNMP-Benachrichtigungen für Alarme

Wenn StorageGRID SNMP-Benachrichtigungen senden soll, wenn Warnmeldungen auftreten, müssen Sie den StorageGRID SNMP-Agent aktivieren und ein oder mehrere Trap-Ziele konfigurieren.

Über diese Aufgabe

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

Informationen zum Konfigurieren des SNMP-Agenten finden Sie im Abschnitt zur Verwendung der SNMP-Überwachung.

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

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

Trap- und Informieren-Benachrichtigungen werden gesendet, wenn eine Standard- oder benutzerdefinierte Warnung auf einem Schweregrad ausgelöst wird. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie eine Stille für die Warnung konfigurieren. Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde. Standardmäßig ist der primäre Admin-Node ausgewählt. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

> Trap- und Informieren-Benachrichtigungen werden auch dann gesendet, wenn bestimmte Alarme (Legacy-System) mit einem bestimmten Schweregrad oder höher ausgelöst werden. SNMP-Benachrichtigungen werden jedoch nicht für jeden Alarm oder jeden Schweregrad gesendet.

Verwandte Informationen

"Verwendung von SNMP-Überwachung"

"Stummschalten von Warnmeldungen"

"StorageGRID verwalten"

"Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"

Einrichten von E-Mail-Benachrichtigungen für Meldungen

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Was Sie benötigen

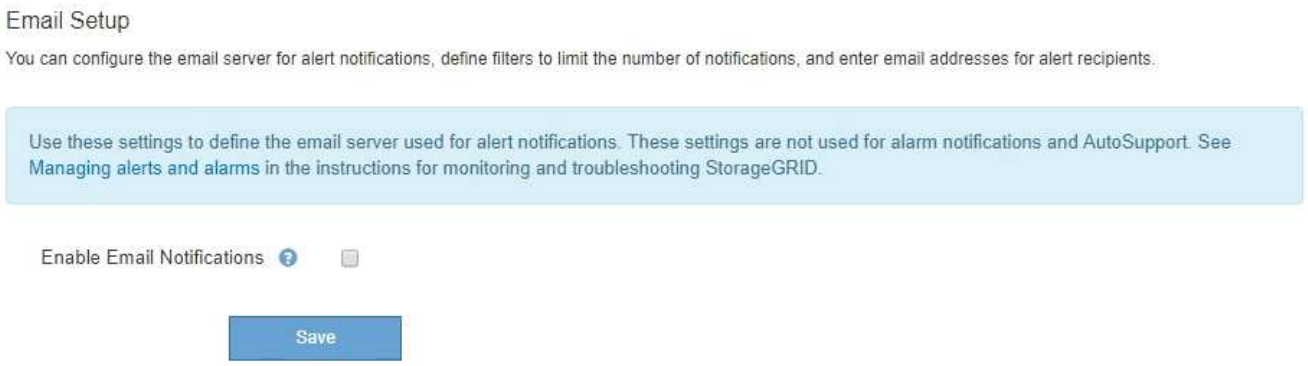
Da es sich bei den Alarmen um unabhängige Systeme handelt, wird das E-Mail-Setup, das für Alarmbenachrichtigungen verwendet wird, nicht für Alarmbenachrichtigungen und AutoSupport-Meldungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden.

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten enthält, können Sie auswählen, welcher Admin-Knoten der bevorzugte Absender von Warnmeldungen sein soll. Der gleiche „`bevorzugte Absender`“ wird auch für Benachrichtigungen zu Alarmen und AutoSupport-Nachrichten verwendet. Standardmäßig ist der primäre Admin-Node ausgewählt. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Schritte

1. Wählen Sie **Alarme** > **E-Mail-Einrichtung**.

   Die Seite E-Mail-Einrichtung wird angezeigt.



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

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

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

   Wenn Ihr SMTP-Server eine Authentifizierung erfordert, müssen Sie sowohl einen Benutzernamen als auch ein Kennwort angeben. Außerdem müssen Sie TLS benötigen und ein CA-Zertifikat vorlegen.

Feld	Eingabe
Mailserver	Der vollständig qualifizierte Domänenname (FQDN) oder die IP-Adresse des SMTP-Servers.
Port	Der Port, der für den Zugriff auf den SMTP-Server verwendet wird. Muss zwischen 1 und 65535 liegen.

Feld	Eingabe
Benutzername (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen ein, mit dem Sie sich authentifizieren möchten.
Kennwort (optional)	Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie das Kennwort für die Authentifizierung ein.

4. Geben Sie im Abschnitt E-Mail-Adressen die E-Mail-Adressen für den Absender und für jeden Empfänger ein.

   a. Geben Sie für die **Absender E-Mail-Adresse** eine gültige E-Mail-Adresse an, die als Absenderadresse für Benachrichtigungen verwendet werden soll.

      Beispiel: `storagegrid-alerts@example.com`

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

      Klicken Sie auf das Plus-Symbol ➕ Um Empfänger hinzuzufügen.

5. Aktivieren Sie im Abschnitt Transport Layer Security (TLS) das Kontrollkästchen **TLS erforderlich**, wenn für die Kommunikation mit dem SMTP-Server Transportschichtsicherheit (TLS) erforderlich ist.

   a. Geben Sie im Feld **CA-Zertifikat** das CA-Zertifikat ein, das zur Überprüfung der Identifizierung des SMTP-Servers verwendet wird.

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

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

b. Aktivieren Sie das Kontrollkästchen **Client-Zertifikat senden**, wenn Ihr SMTP-E-Mail-Server E-Mail-Absender benötigt, um Clientzertifikate zur Authentifizierung bereitzustellen.

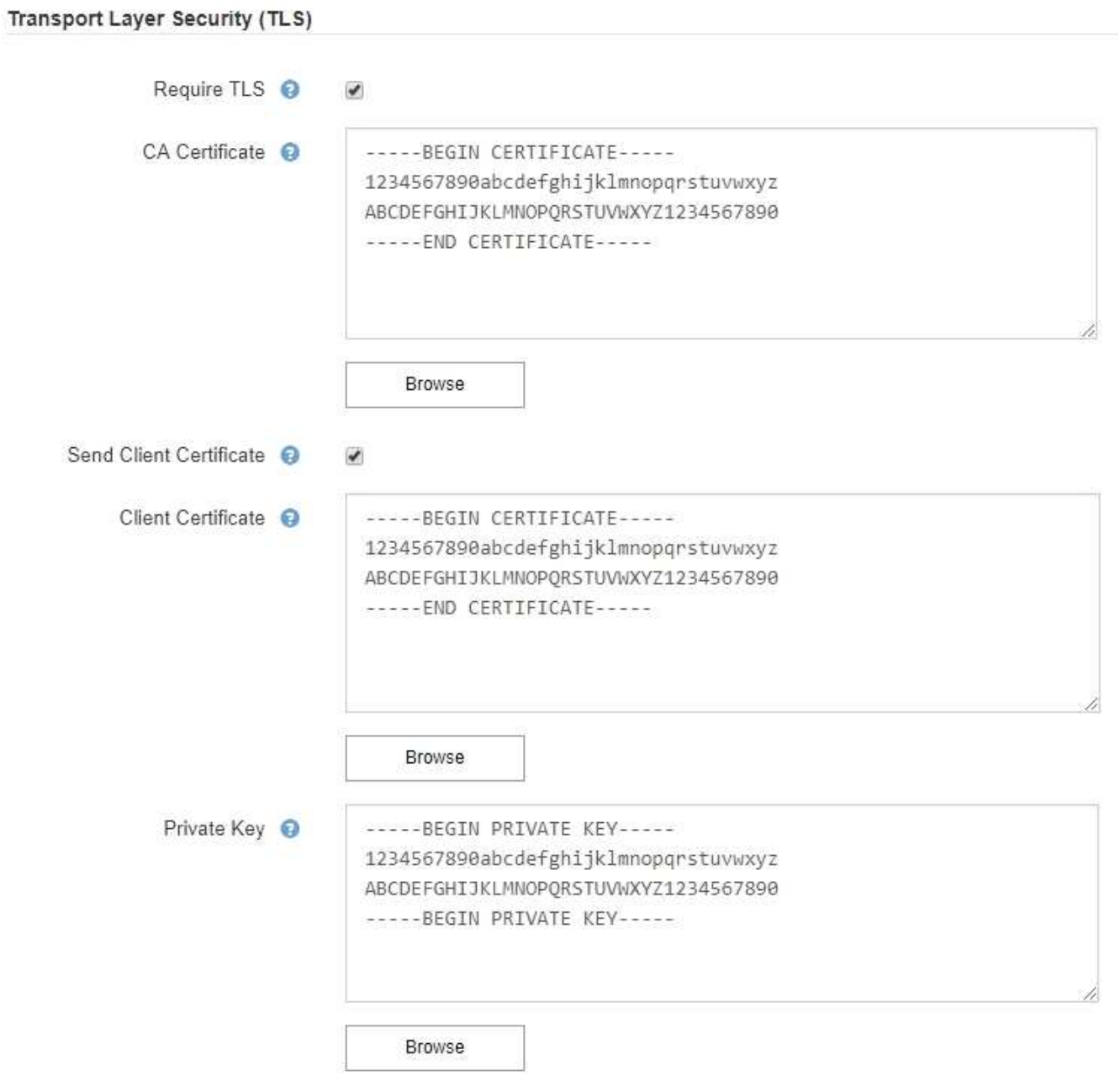
c. Geben Sie im Feld **Client Certificate** das PEM-codierte Clientzertifikat an, das an den SMTP-Server gesendet werden kann.

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

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

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

   Wenn Sie das E-Mail-Setup bearbeiten müssen, klicken Sie auf das Stift-Symbol, um dieses Feld zu aktualisieren.



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

Schweregrad	Beschreibung
Klein, groß, kritisch	Eine E-Mail-Benachrichtigung wird gesendet, wenn die kleine, größere oder kritische Bedingung für eine Alarmregel erfüllt wird.
Kritisch	Wenn die Hauptbedingung für eine Warnmeldung erfüllt ist, wird eine E-Mail-Benachrichtigung gesendet. Es werden keine Benachrichtigungen für kleinere Warnmeldungen gesendet.

Schweregrad	Beschreibung
Nur kritisch	Eine E-Mail-Benachrichtigung wird nur gesendet, wenn die kritische Bedingung für eine Alarmregel erfüllt ist. Es werden keine Benachrichtigungen für kleinere oder größere Warnmeldungen gesendet.

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

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

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

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

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

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

8. Klicken Sie Auf **Speichern**.

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

   Die E-Mail-Einstellungen werden gespeichert.

Verwandte Informationen

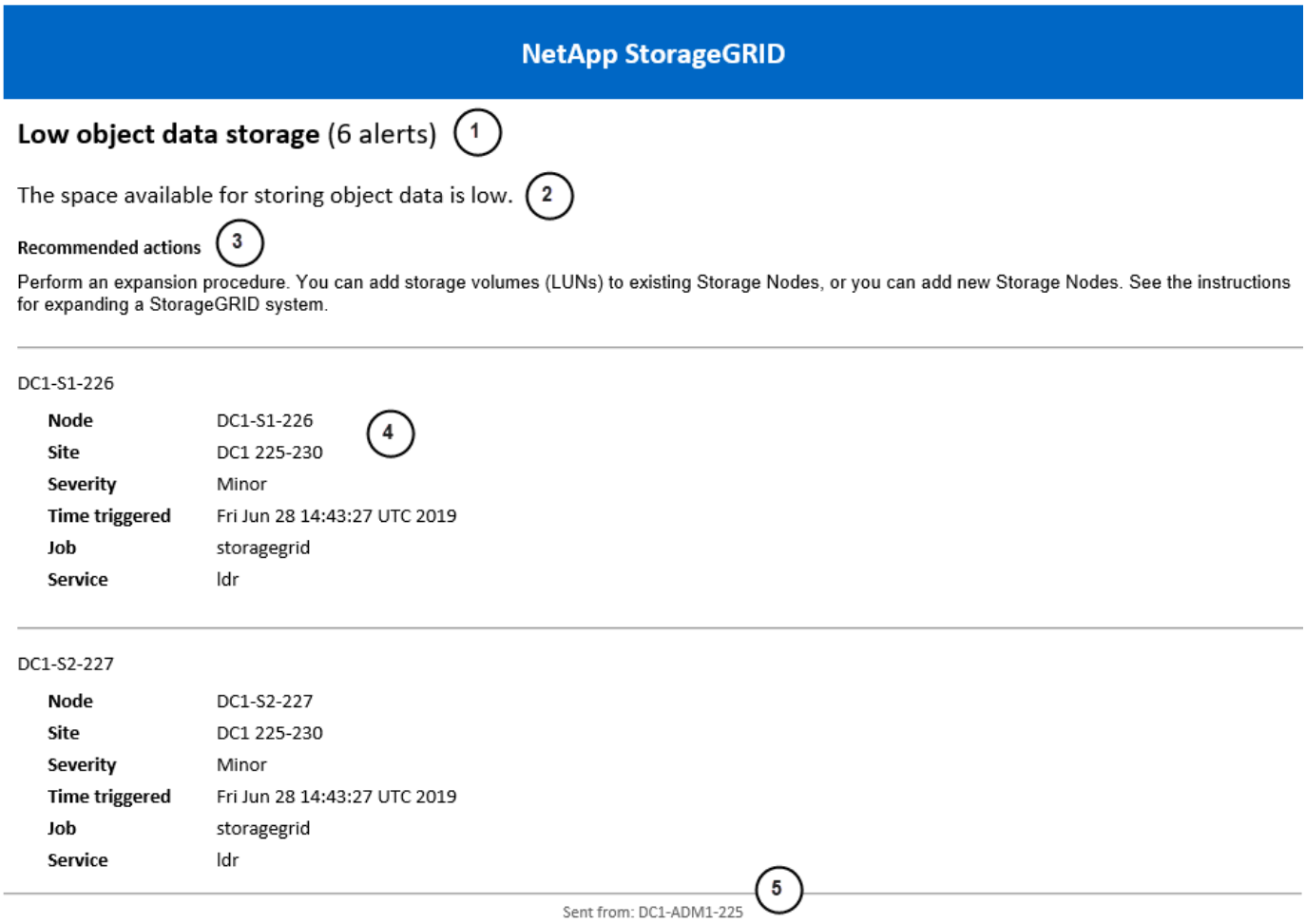
"Fehlerbehebung bei Warnmeldungen per E-Mail"

"Verwalten Sie erholen"

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

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

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:



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

Verwandte Informationen

"Stummschalten von Warnmeldungen"

Wie StorageGRID Alarme in E-Mail-Benachrichtigungen gruppiert

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

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

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

Verhalten	Beispiel
Wenn mehrere aktuelle Warnmeldungen mit demselben Namen vorliegen und eine dieser Meldungen gelöst wird, wird eine neue Benachrichtigung nicht gesendet, wenn die Meldung auf dem Node, für den die Meldung behoben wurde, erneut auftritt.	1. Für Knoten 1 wird eine Warnmeldung A ausgelöst. Eine Benachrichtigung wird gesendet. 2. Für Knoten 2 wird eine Warnmeldung A ausgelöst. Eine zweite Benachrichtigung wird gesendet. 3. Die Warnung A wird für Knoten 2 behoben, bleibt jedoch für Knoten 1 aktiv. 4. Für Node 2 wird erneut eine Warnmeldung A ausgelöst. Es wird keine neue Benachrichtigung gesendet, da die Meldung für Node 1 noch aktiv ist.
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnmeldung gelöst oder die Alarmregel stummgeschaltet wurde.	1. Am 8. März wird Alarm A für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Warnung A ist nicht gelöst oder stummgeschaltet. Weitere Benachrichtigungen erhalten Sie am 15. März, 22. März 29 usw.

Fehlerbehebung bei Warnmeldungen per E-Mail

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Schritte

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

   Der technische Support kann anhand der in den Protokollen enthaltenen Informationen ermitteln, was schief gelaufen ist. Beispielsweise kann die Datei prometheus.log einen Fehler anzeigen, wenn Sie eine Verbindung zu dem von Ihnen angegebenen Server herstellen.

Verwandte Informationen

"Protokolldateien und Systemdaten werden erfasst"

Stummschalten von Warnmeldungen

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff verfügen.

Über diese Aufgabe

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

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

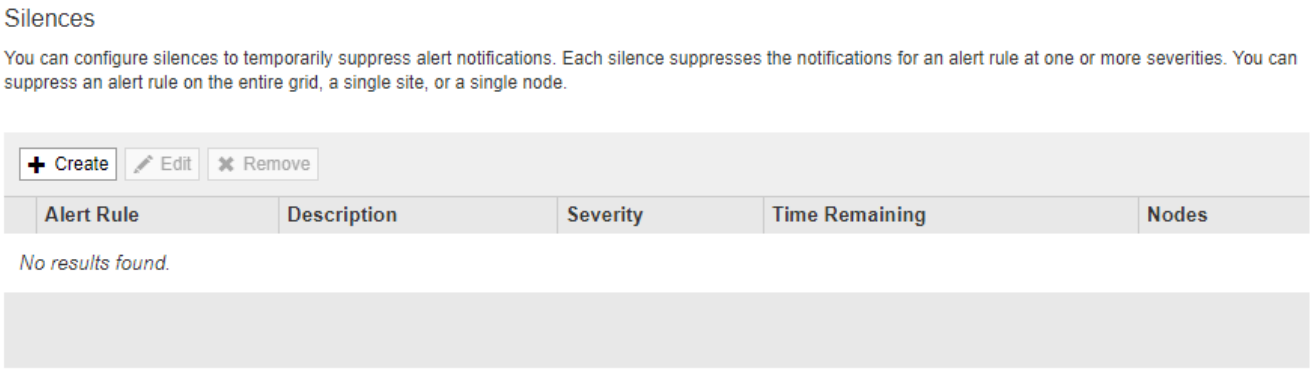
Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummzuschalten. Wenn Sie eine Warnmeldung stummschalten, können Sie ein zugrunde liegendes Problem möglicherweise erst erkennen, wenn ein kritischer Vorgang nicht abgeschlossen werden kann.

Da es sich bei Alarmmeldungen und Warnmeldungen um unabhängige Systeme handelt, können Sie diese Funktion nicht verwenden, um Alarmbenachrichtigungen zu unterdrücken.

Schritte

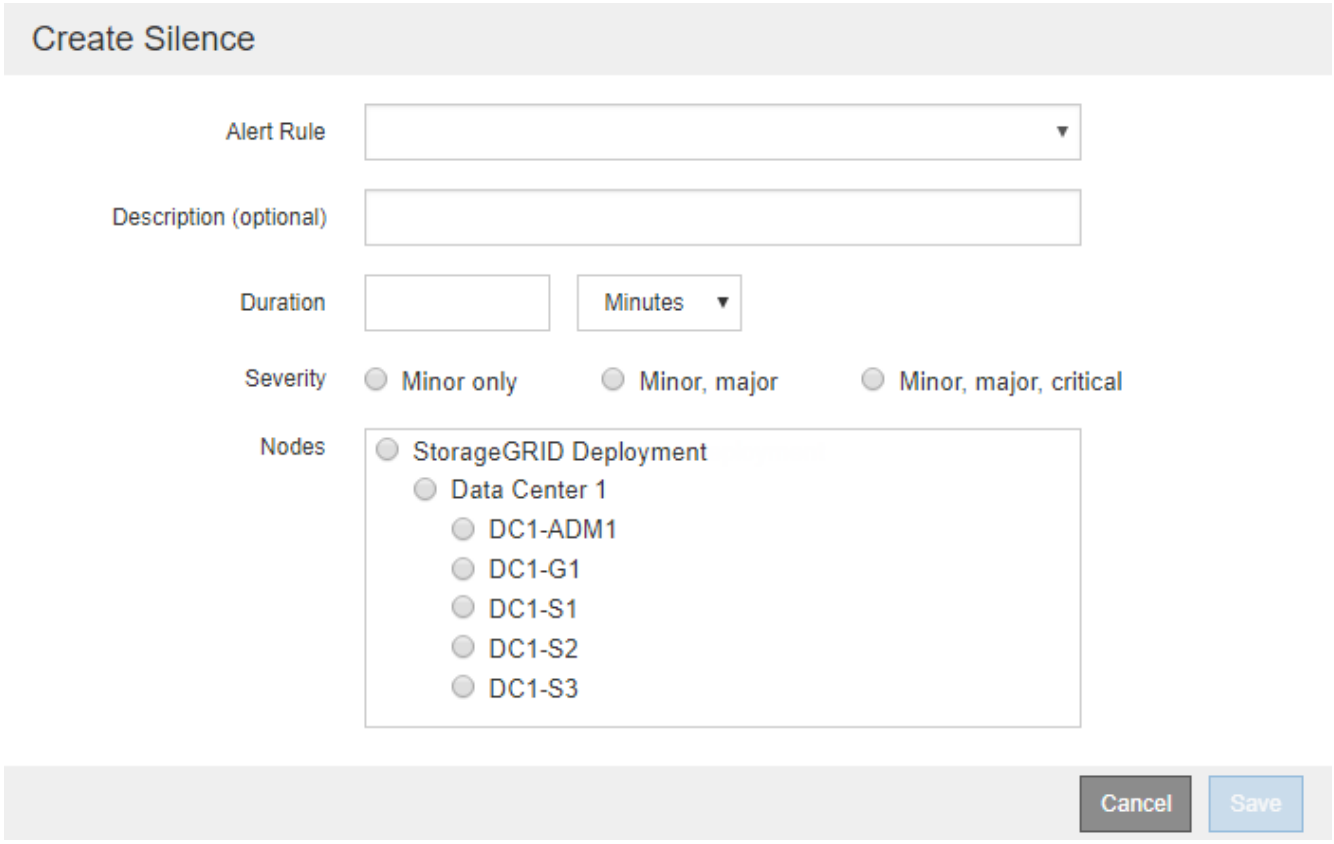
1. Wählen Sie **Alarme** > **Stille**.

   Die Seite „Stille“ wird angezeigt.



2. Wählen Sie **Erstellen**.

   Das Dialogfeld Stille erstellen wird angezeigt.



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

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

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

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

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

Verwandte Informationen

"Konfigurieren des SNMP-Agenten"

Verwalten von Alarmen (Altsystem)

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

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

Verwandte Informationen

"Alarmreferenz (Altsystem)"

"Anzeigen von Legacy-Alarmen"

"StorageGRID verwalten"

Alarmklassen (altes System)

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

Standardalarme

Jedes StorageGRID System verfügt über Standardalarme und kann nicht geändert werden. Sie können jedoch Standardalarme deaktivieren oder überschreiben, indem Sie globale benutzerdefinierte Alarme definieren.

Globale benutzerdefinierte Alarme

Globale benutzerdefinierte Alarme überwachen den Status aller Dienste eines bestimmten Typs im StorageGRID-System. Sie können einen globalen benutzerdefinierten Alarm erstellen, um einen Standardalarm zu überschreiben. Sie können auch einen neuen globalen benutzerdefinierten Alarm erstellen. Dies kann nützlich sein, um alle angepassten Bedingungen Ihres StorageGRID-Systems zu überwachen.

Verwandte Informationen

"Anzeigen von Standardalarmen (Legacy-System)"

"Deaktivieren eines Standardalarms (älteres System)"

"Erstellen von globalen benutzerdefinierten Alarmen (Legacy-System)"

"Deaktivieren von globalen benutzerdefinierten Alarmen (Legacy-System)"

Alarmauslöselogik (Älteres System)

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

Symbol	Farbe	Alarmschweregrad	Bedeutung
	Gelb	Hinweis	Der Node ist mit dem Grid verbunden. Es ist jedoch eine ungewöhnliche Bedingung vorhanden, die den normalen Betrieb nicht beeinträchtigt.

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

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

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

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

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

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

wird kein Alarm ausgelöst und keine Benachrichtigung gesendet.

Beispiel für Alarmauslösung

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

Im folgenden Beispiel ist ein Attribut mit einem globalen benutzerdefinierten Alarm und einem Standardalarm definiert und aktiviert, wie in der folgenden Tabelle dargestellt.

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

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

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

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

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

Alarme desselben Schweregrades

Wenn zwei globale benutzerdefinierte Alarme für dasselbe Attribut den gleichen Schweregrad haben, werden die Alarme mit der Priorität „`top down`“ bewertet.

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

Global Alarms

Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
☑	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		

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

Global Alarms

Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions

Apply Changes

Benachrichtigungen

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

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

Der in der Benachrichtigung über einen Alarmzustand angezeigte Triggerwert wird auf drei Dezimalstellen

gerundet. Daher löst ein Attributwert von 1.9999 einen Alarm aus, dessen Schwellenwert unter (<) 2.0 liegt, obwohl die Alarmbenachrichtigung den Triggerwert als 2.0 anzeigt.

Neuer Services

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

Alarme und Tabellen

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

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

Sie können den VMFI-Alarm so deaktivieren, dass der VMFI-Alarm auf kritischer Ebene nicht ausgelöst wird (beide derzeit kritischen Alarme erscheinen in der Tabelle als grün); Es ist jedoch nicht möglich, einen einzelnen Alarm in einer Tabellenzeile zu deaktivieren, so dass ein VMFI-Alarm als kritischer Füllstandalarm angezeigt wird, während der andere grün bleibt.

Volumes

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

Bestätigen aktueller Alarme (Altsystem)

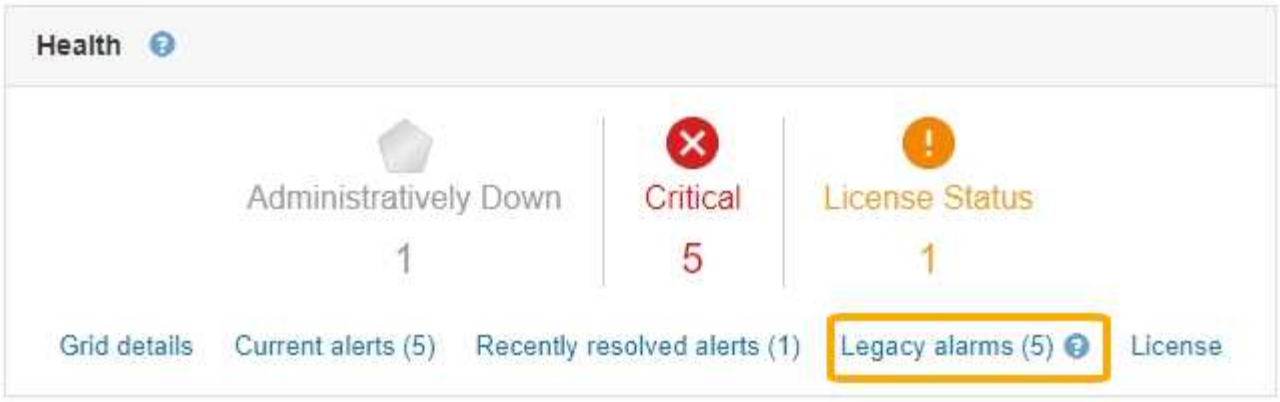
Ältere Alarme werden ausgelöst, wenn Systemattribute die Alarmschwellenwerte erreichen. Wenn Sie die Anzahl der alten Alarme auf dem Dashboard verringern oder löschen möchten, können Sie die Alarme bestätigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Alarme quittieren verfügen.

Über diese Aufgabe

Wenn derzeit ein Alarm aus dem alten System aktiv ist, enthält das Bedienfeld „Systemzustand“ auf dem Dashboard einen Link „Legacy-Alarme*“. Die Zahl in Klammern gibt an, wie viele ältere Alarme derzeit aktiv sind.



Da das veraltete Alarmsystem weiterhin unterstützt wird, wird die Anzahl der auf dem Dashboard angezeigten älteren Alarme erhöht, sobald ein neuer Alarm auftritt. Diese Anzahl wird erhöht, auch wenn E-Mail-Benachrichtigungen nicht mehr für Alarme gesendet werden. Sie können diese Zahl in der Regel einfach ignorieren (da Warnmeldungen eine bessere Übersicht über das System bieten) oder die Alarme quittieren.

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

Wenn Sie einen Alarm quittieren, wird er nicht mehr in die Anzahl der älteren Alarme einbezogen, es sei denn, der Alarm wird auf der nächsten Stufe ausgelöst oder er wird behoben und tritt erneut auf.

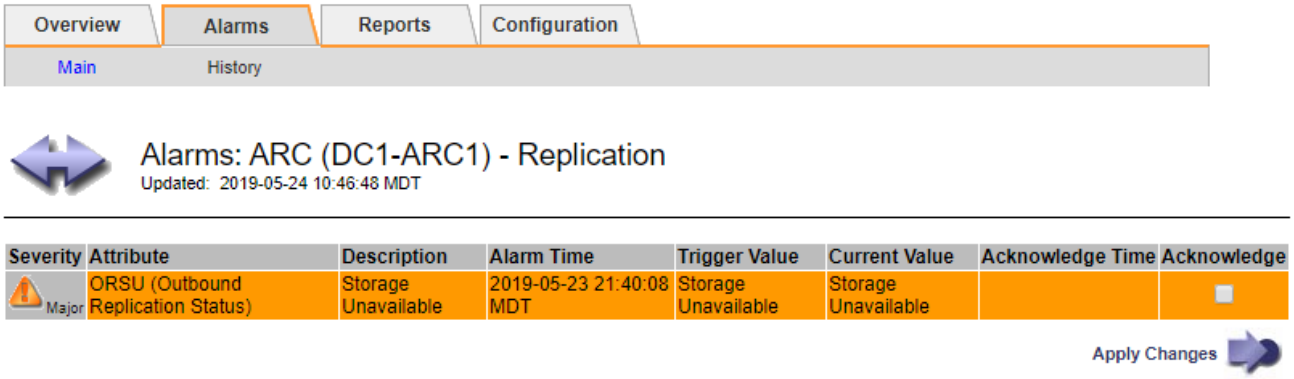
Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

Schritte

1. Um den Alarm anzuzeigen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Bedienfeld „Systemzustand“ auf **Legacy-Alarme**. Dieser Link wird nur angezeigt, wenn derzeit mindestens ein Alarm aktiv ist.
   - Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**. Die Seite Aktuelle Alarme wird angezeigt.

2. Klicken Sie in der Tabelle auf den Dienstnamen.

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



3. Aktivieren Sie das Kontrollkästchen * Quittieren* für den Alarm, und klicken Sie auf **Änderungen anwenden**.

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

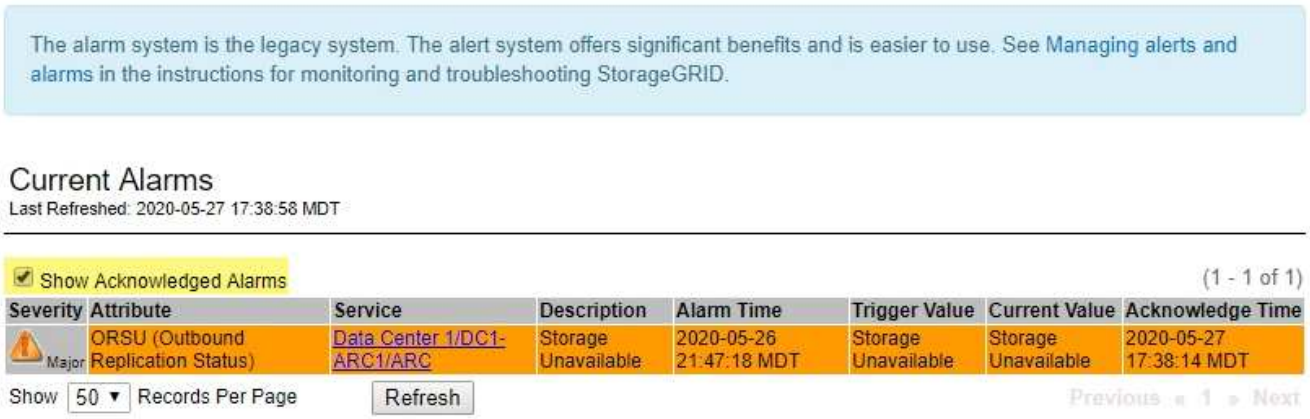
   Wenn Sie einen Alarm bestätigen, wird die Quittierung nicht auf andere Admin-Knoten kopiert. Wenn Sie das Dashboard aus einem anderen Administratorknoten anzeigen, wird möglicherweise weiterhin der aktive Alarm angezeigt.

4. Zeigen Sie bei Bedarf bestätigte Alarme an.

   a. Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**.

   b. Wählen Sie **Bestätigte Alarme Anzeigen**.

      Alle quittierten Alarme werden angezeigt.



Verwandte Informationen

"Alarmreferenz (Altsystem)"

Anzeigen von Standardalarmen (Legacy-System)

Sie können die Liste aller älteren Standardalarme anzeigen.

Was Sie benötigen

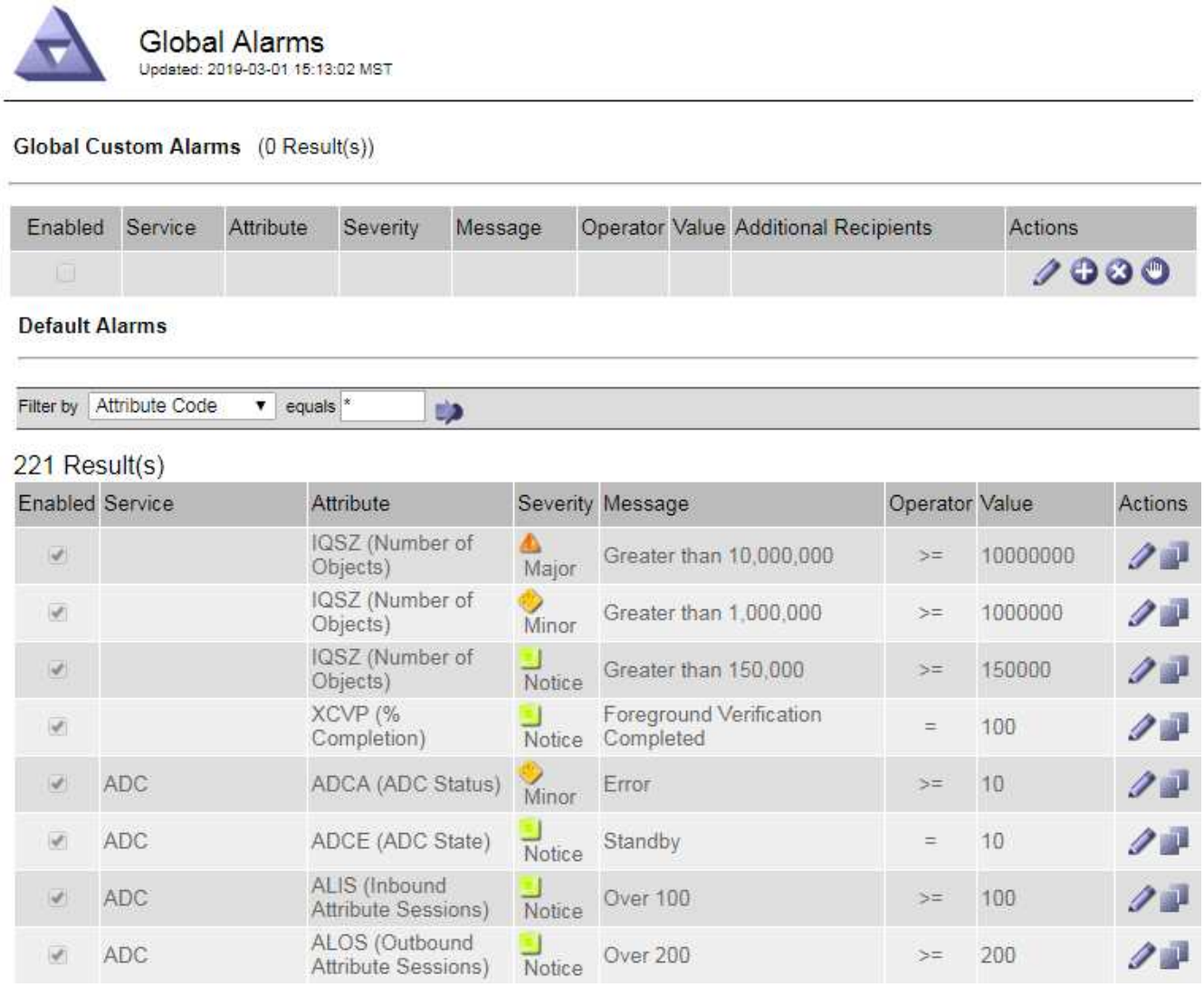
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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

Schritte

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

   Alle Standardalarme werden aufgelistet.



Überprüfung historischer Alarme und Alarmfrequenz (Altsystem)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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

Schritte

1. Führen Sie diese Schritte aus, um eine Liste aller Alarme zu erhalten, die über einen bestimmten Zeitraum ausgelöst wurden.
   a. Wählen Sie **Support** > **Alarme (alt)** > **Historische Alarme**.
   b. Führen Sie einen der folgenden Schritte aus:
      - Klicken Sie auf einen der Zeiträume.
      - Geben Sie einen benutzerdefinierten Bereich ein, und klicken Sie auf **Benutzerdefinierte Abfrage**.
2. Befolgen Sie diese Schritte, um herauszufinden, wie oft Alarme für ein bestimmtes Attribut ausgelöst wurden.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***Grid Node*** > ***Service oder Component*** > **Alarme** > **Historie** aus.
   c. Wählen Sie das Attribut aus der Liste aus.
   d. Führen Sie einen der folgenden Schritte aus:
      - Klicken Sie auf einen der Zeiträume.
      - Geben Sie einen benutzerdefinierten Bereich ein, und klicken Sie auf **Benutzerdefinierte Abfrage**.

      Die Alarme werden in umgekehrter chronologischer Reihenfolge aufgeführt.
   e. Um zum Formular für die Anforderung des Alarmverlaufs zurückzukehren, klicken Sie auf **Historie**.

Verwandte Informationen

"Alarmreferenz (Altsystem)"

Erstellen von globalen benutzerdefinierten Alarmen (Legacy-System)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

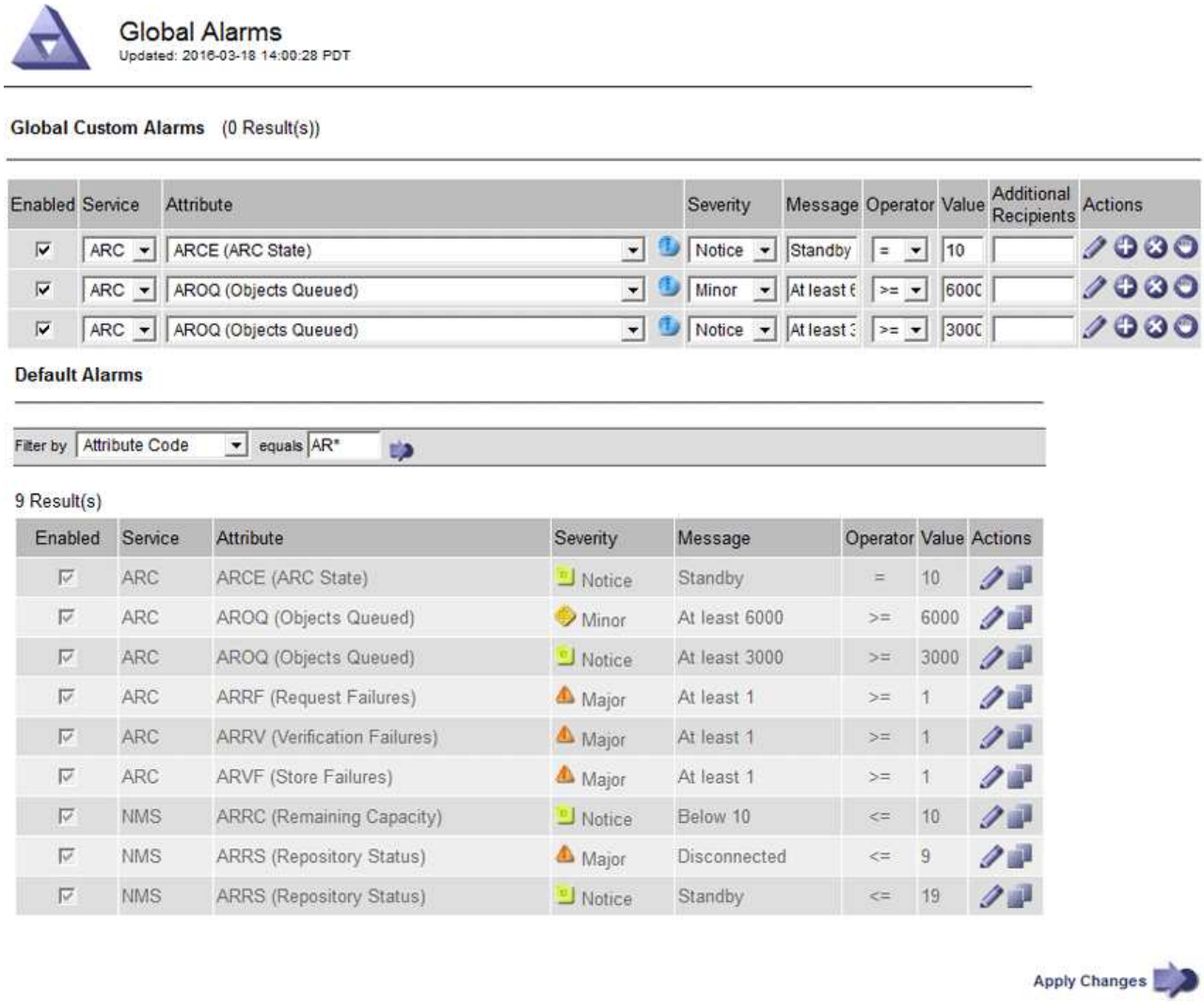
> Das alte Alarmsystem wird zwar weiterhin unterstützt, bietet jedoch deutliche Vorteile und ist einfacher zu bedienen.

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

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

Schritte

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



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

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

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

iv. Klicken Sie in der Ergebnisliste auf **Kopieren** Neben dem Alarm, den Sie ändern möchten.

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

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

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

Überschrift	Beschreibung
Aktionen	Steuertasten zu:  Bearbeiten Sie eine Zeile  Eine Zeile einfügen  Löschen Sie eine Zeile  Ziehen Sie eine Zeile nach oben oder unten  Kopieren Sie eine Zeile

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

Verwandte Informationen

"Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"

Deaktivieren von Alarmen (Altsystem)

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

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

Deaktivieren eines Standardalarms (älteres System)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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

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

Schritte

1. Wählen Sie **Support** > **Alarme (alt)** > **Globale Alarme**.
2. Suchen Sie nach dem Standardalarm, der deaktiviert werden soll.

   a. Wählen Sie im Abschnitt Standardalarme die Option **Filtern nach** > **Attributcode** oder **Attributname** aus.

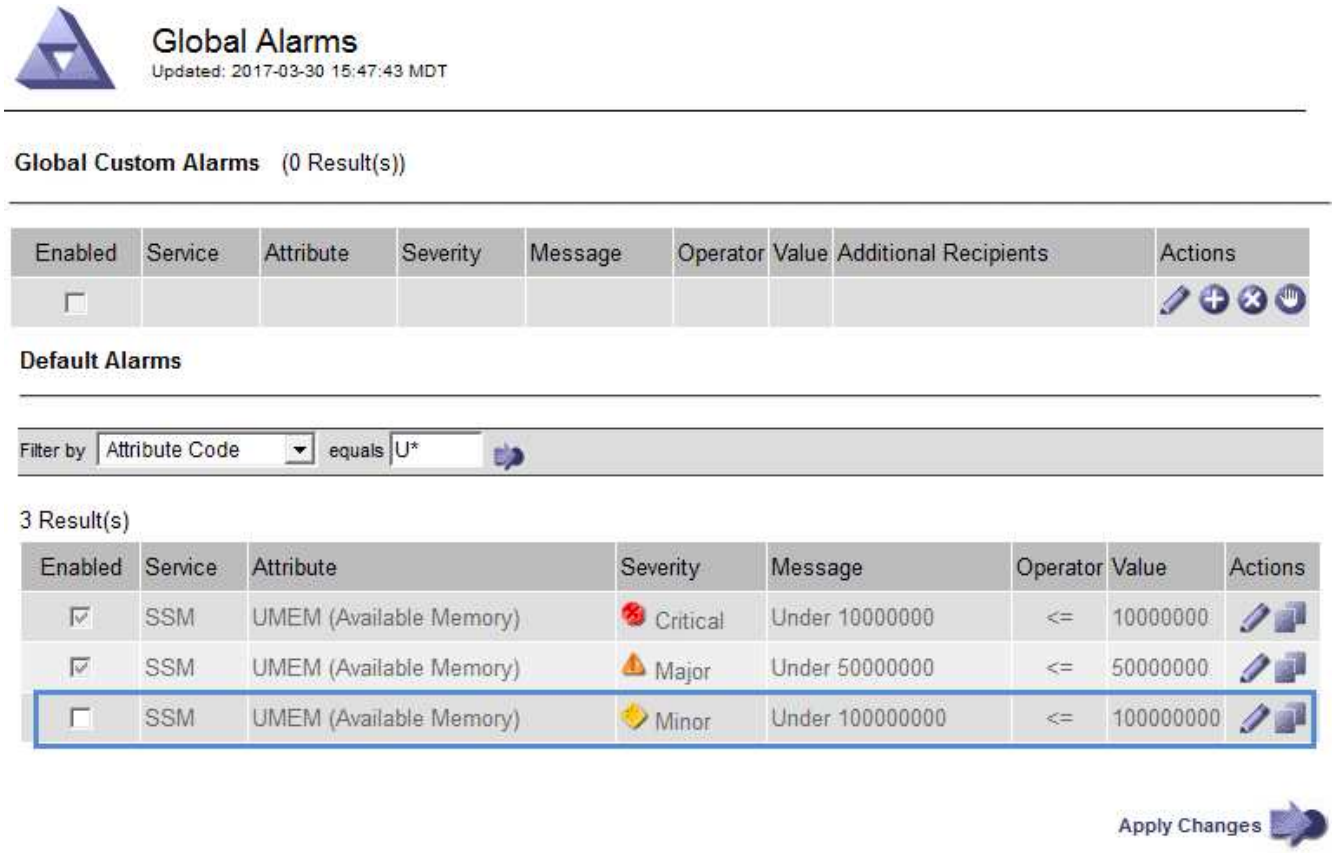
b. Geben Sie einen Suchstring ein.

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

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

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

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



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

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

   Der Standardalarm ist deaktiviert.

Deaktivieren von globalen benutzerdefinierten Alarmen (Legacy-System)

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

Was Sie benötigen

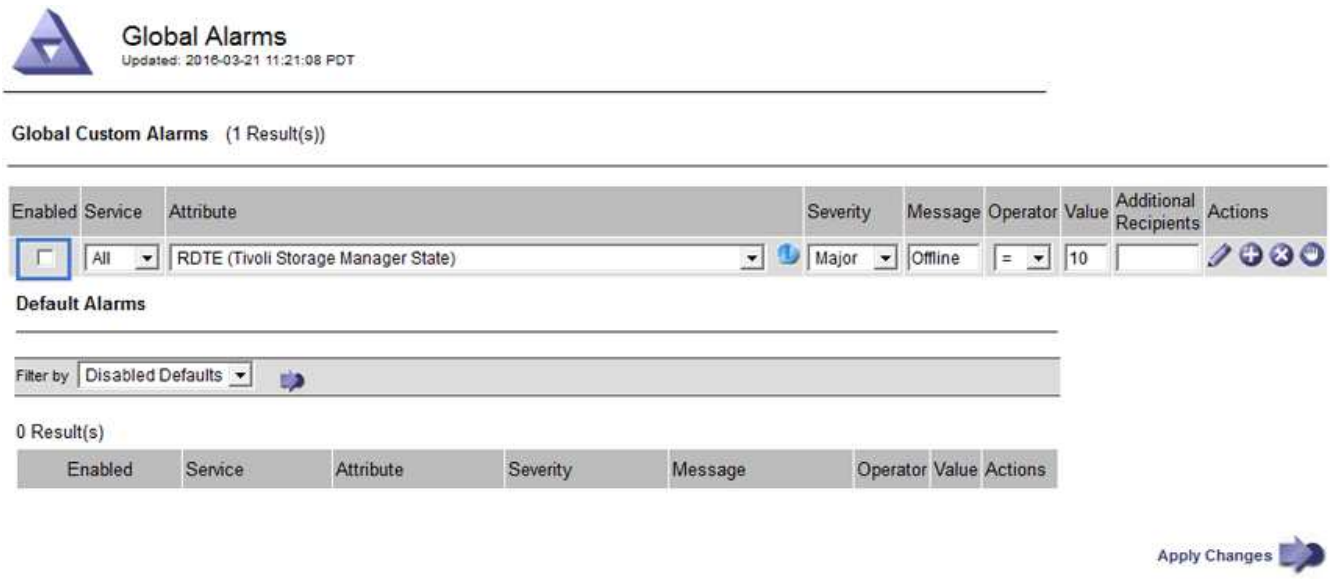
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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

Schritte

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



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

   Der globale benutzerdefinierte Alarm ist deaktiviert.

Ausgelöste Alarme löschen (Legacy-System)

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

Was Sie benötigen

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

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

1. Deaktivieren Sie den Alarm.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: *`ssh admin@primary_Admin_Node_IP`*
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

   Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Starten Sie den NMS-Service neu: `service nms restart`
4. Melden Sie sich beim Admin-Knoten ab: `exit`

   Der Alarm wurde gelöscht.

Verwandte Informationen

"Deaktivieren von Alarmen (Altsystem)"

Konfigurieren von Benachrichtigungen für Alarme (Legacy-System)

Das StorageGRID System kann automatisch E-Mail- und SNMP-Benachrichtigungen senden, wenn ein Alarm ausgelöst wird oder sich ein Servicestatus ändert.

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

Verwandte Informationen

"Verwendung von SNMP-Überwachung"

Arten von Alarmanmeldungen (Legacy-System)

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

Benachrichtigungen auf Schweregraden

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

- Hinweis
- Gering
- Major
- Kritisch

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

Service-Status-Benachrichtigungen

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

- Unbekannt
- Administrativ Nach Unten

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

Verwandte Informationen

"Konfigurieren von E-Mail-Benachrichtigungen für Alarme (Altsystem)"

Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Verwenden Sie diese Einstellungen, um den SMTP-Server zu definieren, der für ältere E-Mail-Benachrichtigungen und AutoSupport-E-Mail-Nachrichten verwendet wird. Diese Einstellungen werden nicht für Benachrichtigungen verwendet.

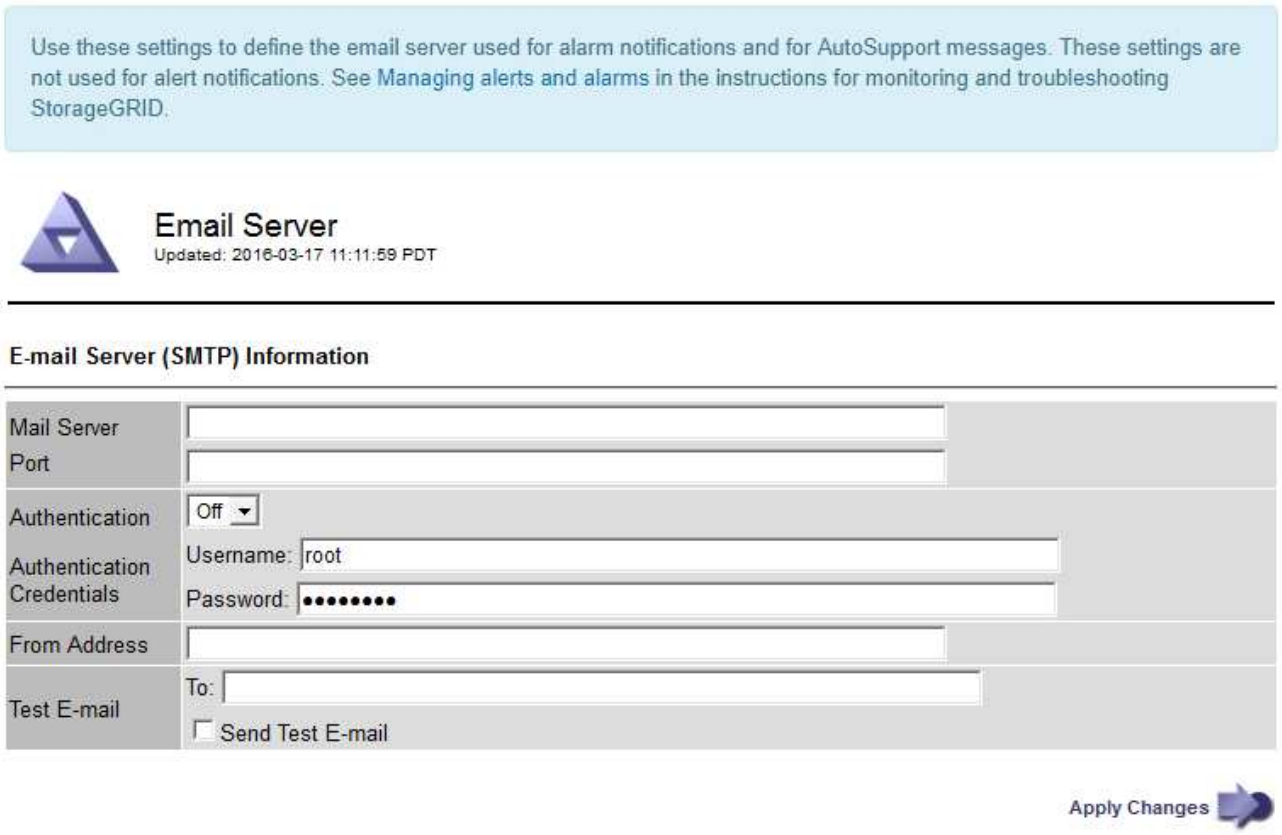
> Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, haben Sie möglicherweise bereits einen SMTP-Mail-Server konfiguriert. Derselbe SMTP-Server wird für Benachrichtigungen über Alarm-E-Mails verwendet, sodass Sie diesen Vorgang überspringen können. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

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

Schritte

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

   Die Seite E-Mail-Server wird angezeigt. Auf dieser Seite wird auch der E-Mail-Server für AutoSupport-Meldungen konfiguriert.



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

Element	Beschreibung
Mailserver	IP-Adresse des SMTP-Mail-Servers. Sie können anstelle einer IP-Adresse einen Hostnamen eingeben, wenn Sie zuvor DNS-Einstellungen auf dem Admin-Knoten konfiguriert haben.
Port	Portnummer für den Zugriff auf den SMTP-Mail-Server.
Authentifizierung	Ermöglicht die Authentifizierung des SMTP-Mail-Servers. Standardmäßig ist die Authentifizierung deaktiviert.
Authentifizierungsdaten	Benutzername und Passwort des SMTP-Mail-Servers. Wenn die Authentifizierung auf ein festgelegt ist, müssen ein Benutzername und ein Passwort für den Zugriff auf den SMTP-Mail-Server angegeben werden.

4. Geben Sie unter **von Address** eine gültige E-Mail-Adresse ein, die der SMTP-Server als sendende E-Mail-Adresse erkennt. Dies ist die offizielle E-Mail-Adresse, von der die E-Mail-Nachricht gesendet wird.
5. Senden Sie optional eine Test-E-Mail, um zu bestätigen, dass die SMTP-Mail-Servereinstellungen korrekt sind.

a. Fügen Sie im Feld **E-Mail-Test** > **bis** eine oder mehrere Adressen hinzu, auf die Sie zugreifen können.

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

b. Wählen Sie **Test-E-Mail senden**.

6. Klicken Sie Auf **Änderungen Übernehmen**.

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

Verwandte Informationen

"StorageGRID verwalten"

Erstellen von E-Mail-Vorlagen für Alarme (altes System)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

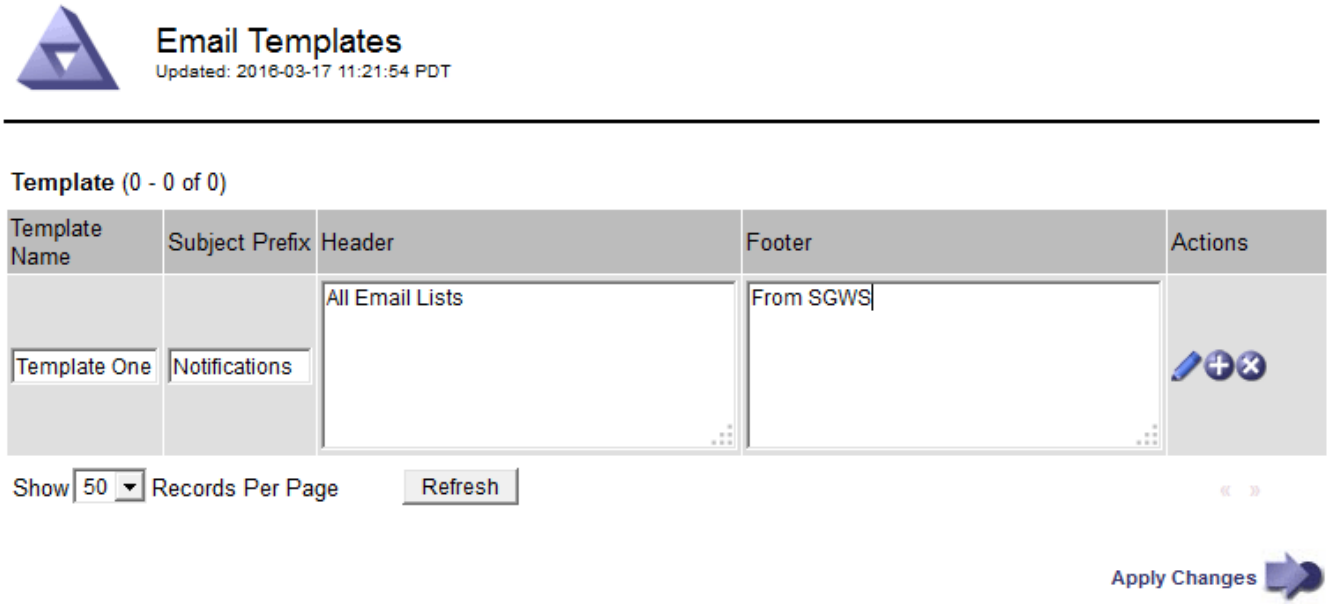
Über diese Aufgabe

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

Für unterschiedliche Mailinglisten sind möglicherweise andere Kontaktinformationen erforderlich. Vorlagen enthalten nicht den Textkörper der E-Mail-Nachricht.

Schritte

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



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

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

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

   Es wird eine neue Vorlage für Benachrichtigungen hinzugefügt.

Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)

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

Was Sie benötigen

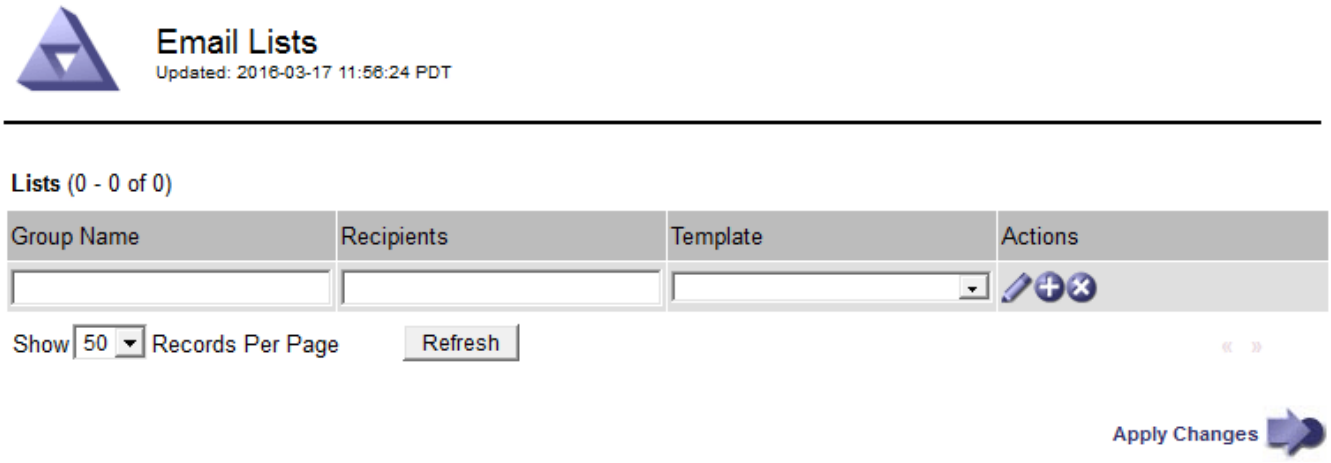
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie eine E-Mail-Vorlage für die Mailingliste (benutzerdefinierte Kopfzeile, Fußzeile und Betreffzeile) angeben möchten, müssen Sie die Vorlage bereits erstellt haben.

Über diese Aufgabe

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

Schritte

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



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

Element	Beschreibung
Gruppenname	Eindeutiger Name zur Identifizierung der Mailingliste. Mailinglistennamen können nicht dupliziert werden. **Hinweis:** Wenn Sie den Namen einer Mailingliste ändern, wird die Änderung nicht an die anderen Standorte weitergegeben, die den Namen der Mailingliste verwenden. Sie müssen alle konfigurierten Benachrichtigungen manuell aktualisieren, um den neuen Namen der Mailingliste zu verwenden.

Element	Beschreibung
Empfänger	Eine einzelne E-Mail-Adresse, eine zuvor konfigurierte Mailingliste oder eine kommagetrennte Liste von E-Mail-Adressen und Mailinglisten, an die Benachrichtigungen gesendet werden. **Hinweis:** Wenn eine E-Mail-Adresse zu mehreren Mailinglisten gehört, wird nur eine E-Mail-Benachrichtigung gesendet, wenn ein Benachrichtigungserlösungs-Ereignis auftritt.
Vorlage	Wählen Sie optional eine E-Mail-Vorlage aus, um eine eindeutige Kopfzeile, Fußzeile und Betreffzeile zu Benachrichtigungen hinzuzufügen, die an alle Empfänger dieser Mailingliste gesendet werden.

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

   Es wird eine neue Mailingliste erstellt.

Verwandte Informationen

"Erstellen von E-Mail-Vorlagen für Alarme (altes System)"

Konfigurieren von E-Mail-Benachrichtigungen für Alarme (Altsystem)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen eine E-Mail-Liste konfiguriert haben.

Über diese Aufgabe

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

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

Schritte

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

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

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

Verwandte Informationen

"Erstellen von Mailinglisten für Alarmbenachrichtigungen (Altsystem)"

"Arten von Alarmanmeldungen (Legacy-System)"

Unterdrückung von Alarmmeldungen für eine Mailingliste (Legacy-System)

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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

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

Schritte

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

   Ältere Alarmbenachrichtigungen werden für die ausgewählten Mailinglisten unterdrückt.

Systemweite Unterdrückung von E-Mail-Benachrichtigungen

Sie können die Fähigkeit des StorageGRID Systems blockieren, E-Mail-Benachrichtigungen für ältere Alarme und AutoSupport-Meldungen mit Ereignisauslösung zu senden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

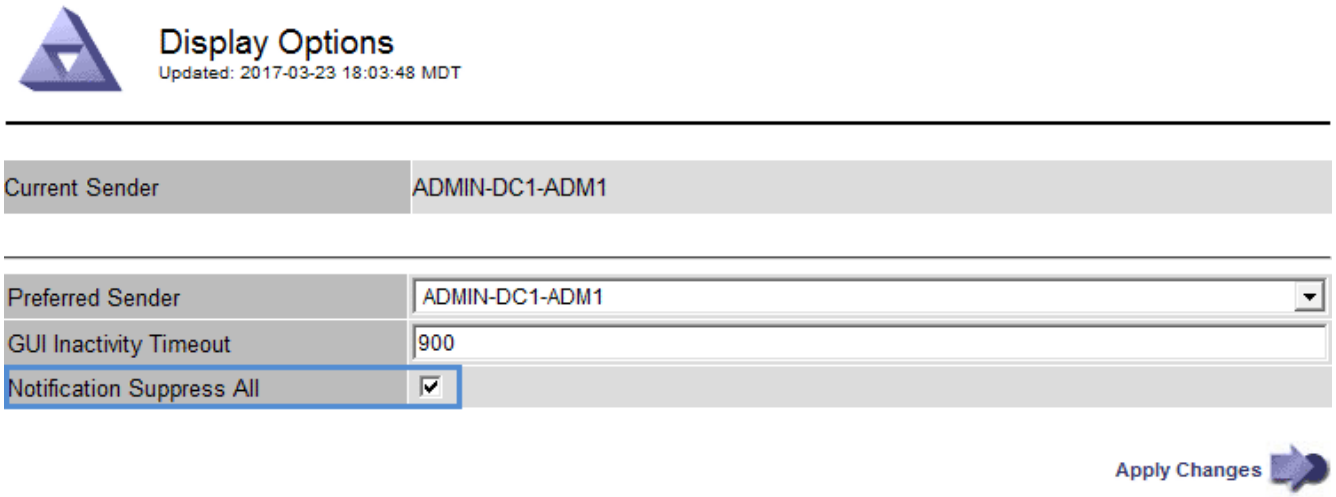
Über diese Aufgabe

Verwenden Sie diese Option, um E-Mail-Benachrichtigungen für ältere Alarme und AutoSupport-Meldungen, bei denen Ereignisse ausgelöst werden, zu unterdrücken.

Diese Option unterdrückt Benachrichtigungen per E-Mail nicht. Zudem werden wöchentliche oder benutzergesteuerte AutoSupport-Meldungen nicht unterdrückt.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Wählen Sie im Menü Anzeigeoptionen die Option **Optionen**.
3. Wählen Sie **Benachrichtigung Alle Unterdrücken**.



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

   Auf der Seite Benachrichtigungen (**Konfiguration** > **Benachrichtigungen**) wird die folgende Meldung angezeigt:

Verwandte Informationen

"StorageGRID verwalten"

Verwendung von SNMP-Überwachung

Wenn Sie StorageGRID mit dem Simple Network Management Protocol (SNMP) überwachen möchten, müssen Sie den SNMP-Agent konfigurieren, der in StorageGRID enthalten ist.

- "Konfigurieren des SNMP-Agenten"
- "SNMP-Agent wird aktualisiert"

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine Management

Information Base (MIB) bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Alarme und Alarme. Die MIB enthält auch Informationen zur Systembeschreibung wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID-Knoten unterstützt auch eine Untergruppe von MIB-II-Objekten.

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

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

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

  Traps werden in allen drei Versionen von SNMP unterstützt.

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

  Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

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

- Eine Standardwarnung oder eine benutzerdefinierte Meldung wird für jeden Schweregrad ausgelöst. Um SNMP-Benachrichtigungen für eine Warnung zu unterdrücken, müssen Sie eine Stille für die Warnung konfigurieren. Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde.
- Bestimmte Alarme (Altsystem) werden mit einem bestimmten Schweregrad oder höher ausgelöst.

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

Unterstützung von SNMP-Versionen

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

	SNMPv1	SNMPv2c	SNMPv3
Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen	Schreibgeschützte MIB-Abfragen
Abfrageauthentifizierung	Community-Zeichenfolge	Community-Zeichenfolge	Benutzer des benutzerbasierten Sicherheitsmodells (USM)
Benachrichtigungen	Nur Traps	Traps und informiert	Traps und informiert

	SNMPv1	SNMPv2c	SNMPv3
Benachrichtigungsauthentifizierung	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	Standard-Trap-Community oder eine benutzerdefinierte Community-Zeichenfolge für jedes Trap-Ziel	USM-Benutzer für jedes Trap-Ziel

Einschränkungen

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

Zugriff auf die MIB

Sie können auf die MIB-Definitionsdatei an der folgenden Stelle auf einem beliebigen StorageGRID-Knoten zugreifen:

/Usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt

Verwandte Informationen

"Alerts Referenz"

"Alarmreferenz (Altsystem)"

"Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)"

"Stummschalten von Warnmeldungen"

Konfigurieren des SNMP-Agenten

Sie können den StorageGRID SNMP-Agent konfigurieren, wenn Sie ein Drittanbieter-SNMP-Verwaltungssystem für schreibgeschützten MIB-Zugriff und Benachrichtigungen verwenden möchten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Der StorageGRID SNMP Agent unterstützt alle drei Versionen des SNMP-Protokolls. Sie können den Agent für eine oder mehrere Versionen konfigurieren.

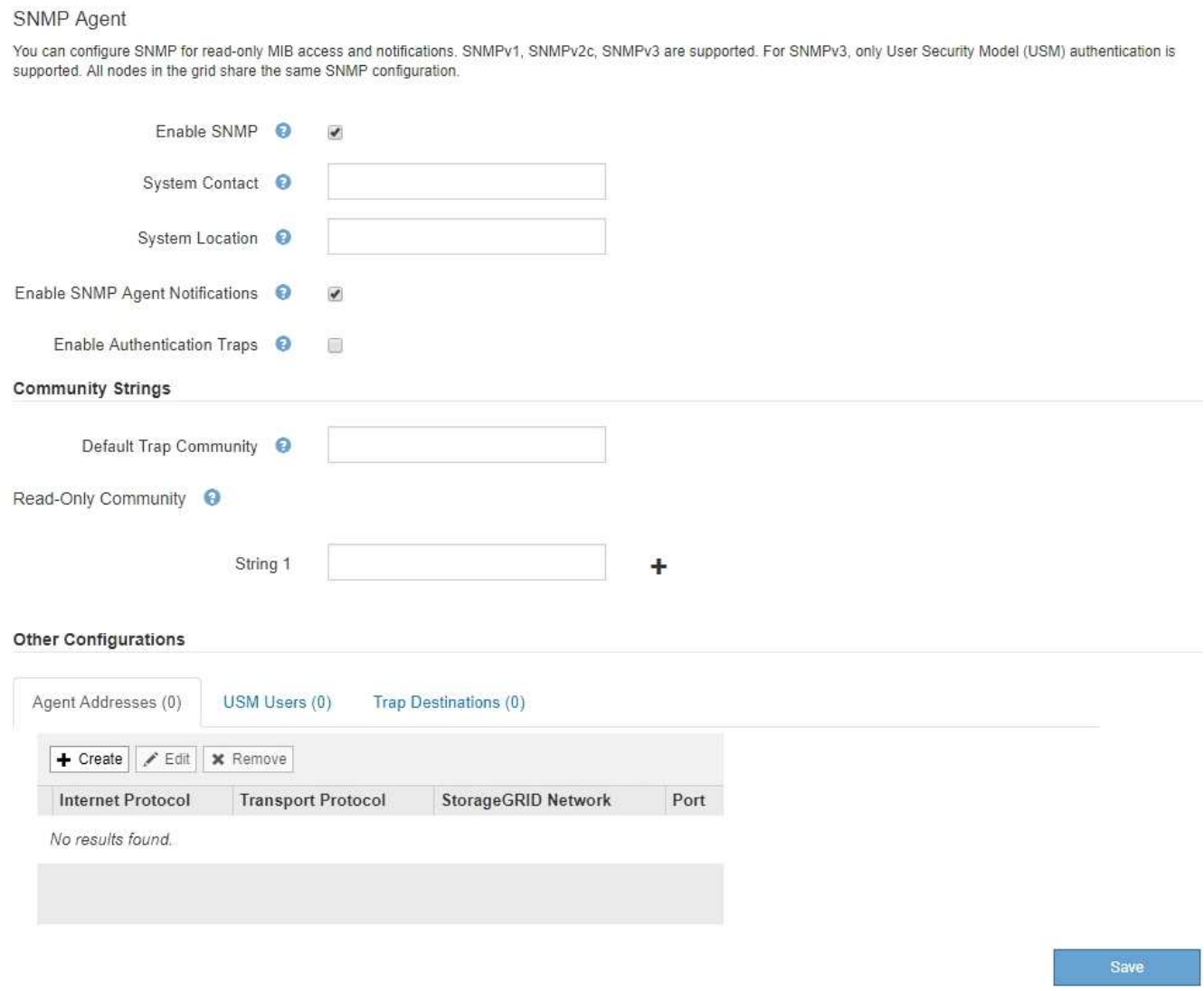
Schritte

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

   Die Seite SNMP-Agent wird angezeigt.

2. Um den SNMP-Agent auf allen Grid-Knoten zu aktivieren, aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.

   Die Felder zum Konfigurieren eines SNMP-Agenten werden angezeigt.



3. Geben Sie im Feld **Systemkontakt** den Wert ein, den StorageGRID in SNMP-Nachrichten für sysContact bereitstellen soll.

   Der Systemkontakt ist in der Regel eine E-Mail-Adresse. Der von Ihnen ausliefern Wert gilt für alle Nodes im StorageGRID System. **Systemkontakt** kann maximal 255 Zeichen lang sein.

4. Geben Sie im Feld **Systemstandort** den Wert ein, den StorageGRID in SNMP-Nachrichten für sysLocation bereitstellen soll.

Der Systemstandort kann alle Informationen sein, die für die Identifizierung des Standortes Ihres StorageGRID-Systems nützlich sind. Sie können beispielsweise die Straßenadresse einer Einrichtung verwenden. Der von Ihnen ausliefern Wert gilt für alle Nodes im StorageGRID System. **Systemposition** kann maximal 255 Zeichen enthalten.

5. Aktivieren Sie das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, wenn der StorageGRID-SNMP-Agent Trap senden und Benachrichtigungen informieren soll.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, unterstützt der SNMP-Agent den schreibgeschützten MIB-Zugriff, aber es sendet keine SNMP-Benachrichtigungen.

6. Aktivieren Sie das Kontrollkästchen **Authentifizierungsfallen aktivieren**, wenn der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap senden soll, wenn er eine nicht ordnungsgemäß authentifizierte Protokollnachricht empfängt.
7. Wenn Sie SNMPv1 oder SNMPv2c verwenden, füllen Sie den Abschnitt „Gemeinschaftsfolgen“ aus.

   Die Felder in diesem Abschnitt werden für die Community-basierte Authentifizierung in SNMPv1 oder SNMPv2c verwendet. Diese Felder gelten nicht für SNMPv3.

   a. Geben Sie im Feld **Default Trap Community** optional die Standard-Community-Zeichenfolge ein, die Sie für Trap-Ziele verwenden möchten.

      Bei Bedarf können Sie eine andere („`Custom`")-Community-Zeichenfolge angeben Definieren Sie ein bestimmtes Trap-Ziel.

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

   b. Geben Sie für **Read-Only Community** eine oder mehrere Community-Strings ein, um schreibgeschützten MIB-Zugriff auf IPv4- und IPv6-Agent-Adressen zu ermöglichen. Klicken Sie auf das Pluszeichen ➕ Um mehrere Zeichenfolgen hinzuzufügen.

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

      Jede Community-Zeichenfolge kann maximal 32 Zeichen enthalten und darf keine Leerzeichen enthalten. Es sind bis zu fünf Zeichenfolgen zulässig.

      ⓘ Verwenden Sie nicht „`public`“ als Community-String, um die Sicherheit Ihres StorageGRID-Systems zu gewährleisten. Wenn Sie keine Community-Zeichenfolge eingeben, verwendet der SNMP-Agent die Grid-ID Ihres StorageGRID-Systems als Community-String.

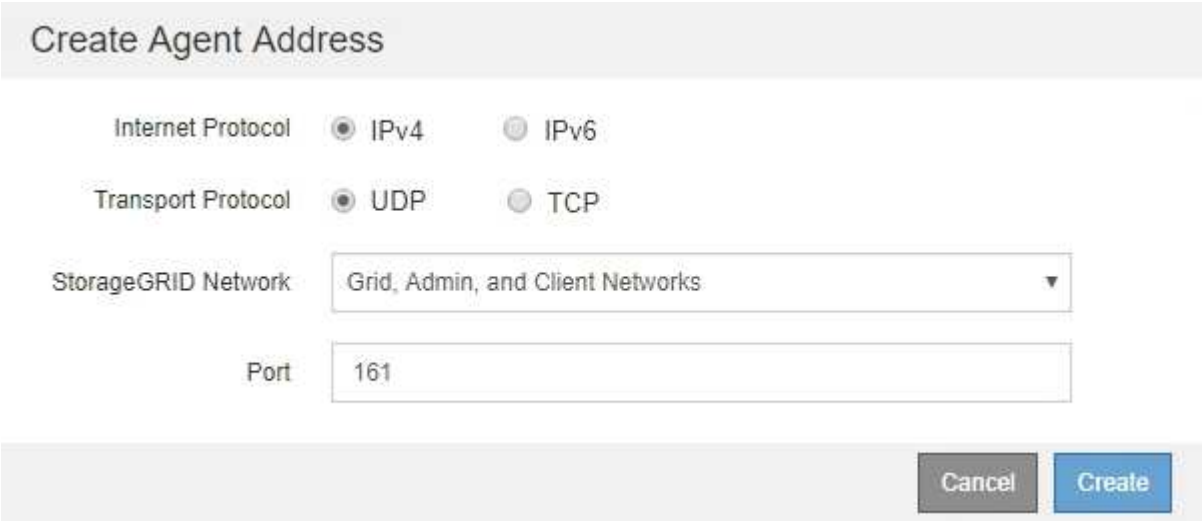
8. Wählen Sie optional im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

   Verwenden Sie diese Registerkarte, um eine oder mehrere „`Listening-Adressen`“ anzugeben. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Anfragen erhalten kann. Jede Agentenadresse umfasst ein Internetprotokoll, ein Transportprotokoll, ein StorageGRID-Netzwerk und optional einen Port.

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

   a. Klicken Sie Auf **Erstellen**.

Das Dialogfeld Agentenadresse erstellen wird angezeigt.



b. Wählen Sie für **Internet Protocol** aus, ob diese Adresse IPv4 oder IPv6 verwendet.

   Standardmäßig verwendet SNMP IPv4.

c. Wählen Sie für **Transport Protocol** aus, ob diese Adresse UDP oder TCP verwenden soll.

   Standardmäßig verwendet SNMP UDP.

d. Wählen Sie im Feld **StorageGRID-Netzwerk** das StorageGRID-Netzwerk aus, auf dem die Abfrage empfangen wird.
   - Grid-, Admin- und Client-Netzwerke: StorageGRID sollte SNMP-Abfragen in allen drei Netzwerken abhören.
   - Grid-Netzwerk
   - Admin-Netzwerk
   - Client-Netzwerk

   > Um sicherzustellen, dass die Clientkommunikation mit StorageGRID sicher bleibt, sollten Sie keine Agentenadresse für das Clientnetzwerk erstellen.

e. Geben Sie im Feld **Port** optional die Portnummer ein, die der SNMP-Agent anhören soll.

   Der Standard-UDP-Port für einen SNMP-Agenten ist 161, Sie können jedoch alle nicht verwendeten Portnummern eingeben.

   > Wenn Sie den SNMP-Agent speichern, öffnet StorageGRID automatisch die Agent-Adressen-Ports in der internen Firewall. Sie müssen sicherstellen, dass alle externen Firewalls den Zugriff auf diese Ports zulassen.

f. Klicken Sie Auf **Erstellen**.

   Die Agentenadresse wird erstellt und der Tabelle hinzugefügt.

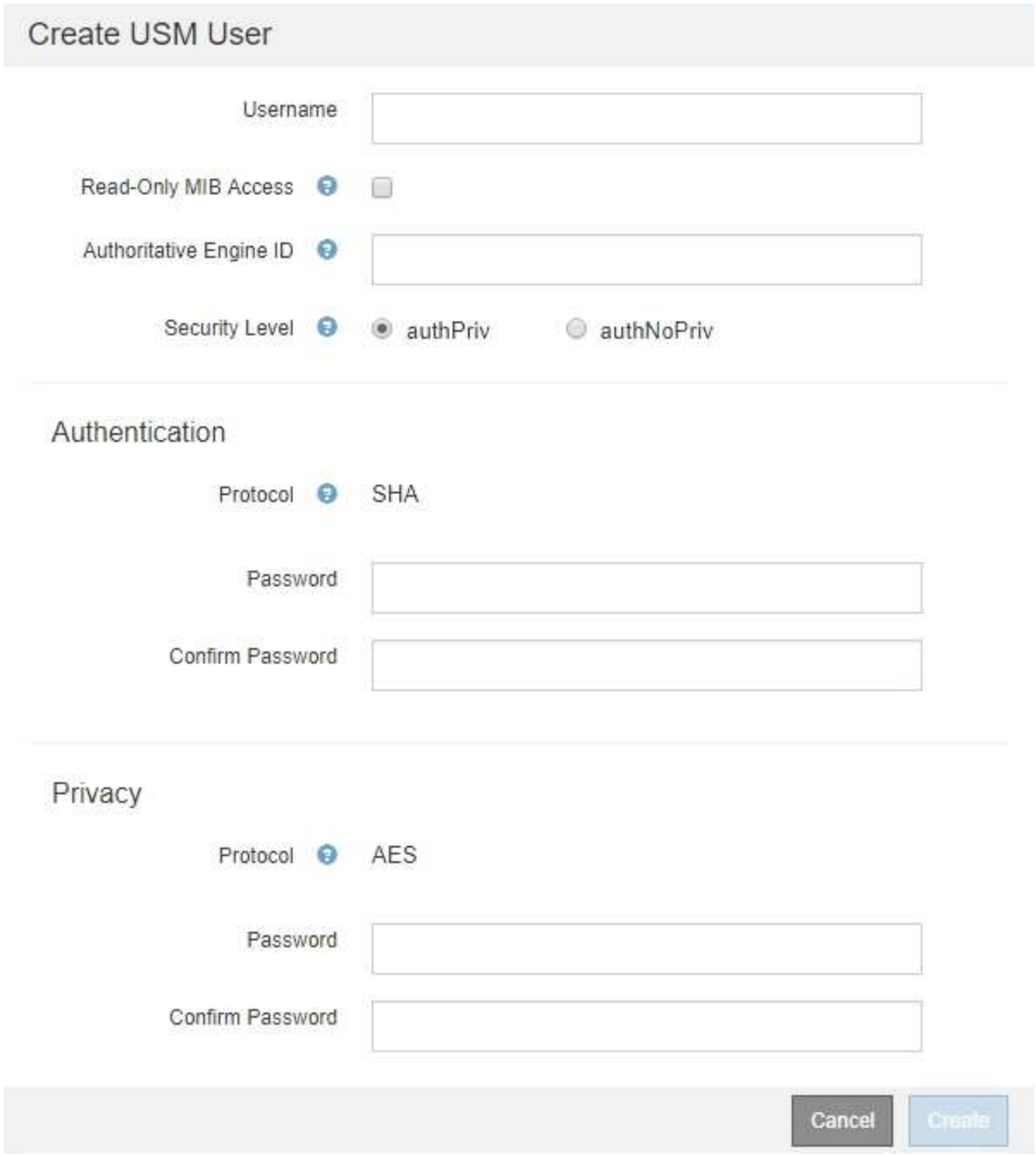
9. Wenn Sie SNMPv3 verwenden, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.

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

   Dieser Schritt gilt nicht, wenn Sie nur SNMPv1 oder SNMPv2c verwenden.

   a. Klicken Sie Auf **Erstellen**.

      Das Dialogfeld USM-Benutzer erstellen wird angezeigt.



b. Geben Sie einen eindeutigen **Benutzername** für diesen USM-Benutzer ein.

   Benutzernamen haben maximal 32 Zeichen und können keine Leerzeichen enthalten. Der Benutzername kann nach dem Erstellen des Benutzers nicht geändert werden.

c. Aktivieren Sie das Kontrollkästchen **schreibgeschütztes MIB Access**, wenn dieser Benutzer nur Lesezugriff auf die MIB haben soll.

   Wenn Sie **schreibgeschütztes MIB Access** auswählen, ist das Feld **autoritative Engine ID** deaktiviert.

   USM-Benutzer mit schreibgeschütztem MIB-Zugriff können keine Engine-IDs haben.

d. Wenn dieser Benutzer in einem Inform-Ziel verwendet wird, geben Sie die **autoritative Engine-ID** für

diesen Benutzer ein.

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

Die autoritative Engine-ID kann zwischen 5 und 32 Byte hexadezimal sein.

e. Wählen Sie eine Sicherheitsstufe für den USM-Benutzer aus.
   - **AuthPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und Datenschutz (Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort sowie ein Datenschutzprotokoll und ein Passwort angeben.
   - **AuthNoPriv**: Dieser Benutzer kommuniziert mit Authentifizierung und ohne Datenschutz (keine Verschlüsselung). Sie müssen ein Authentifizierungsprotokoll und ein Passwort angeben.

f. Geben Sie das Passwort ein, das dieser Benutzer zur Authentifizierung verwenden soll, und bestätigen Sie es.

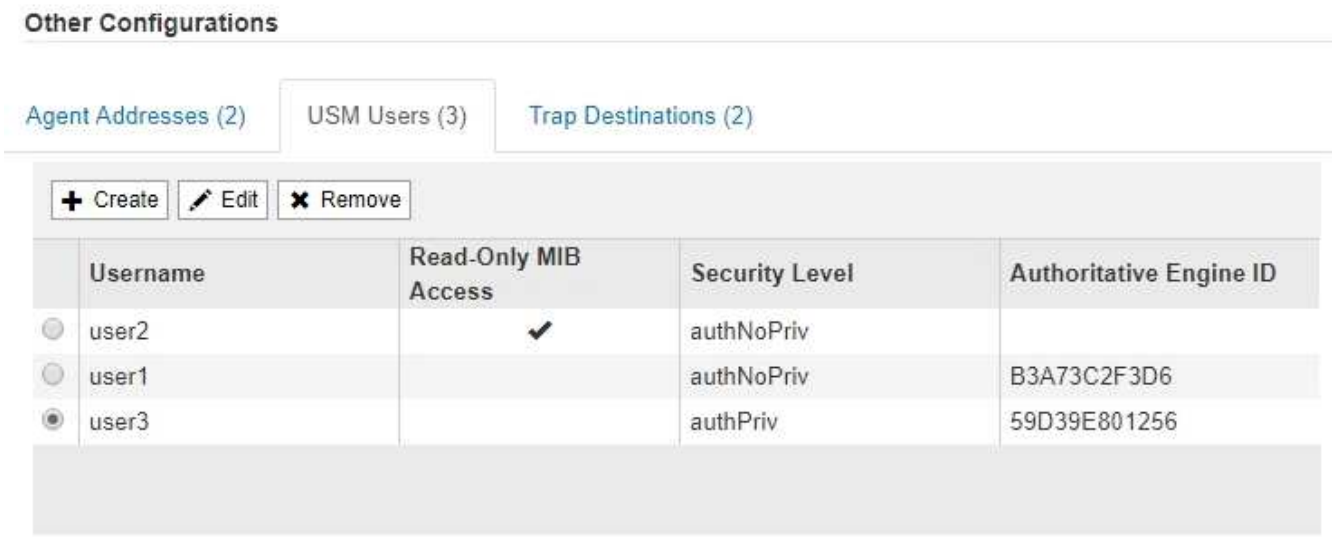
> Das einzige unterstützte Authentifizierungsprotokoll ist SHA (HMAC-SHA-96).

g. Wenn Sie **authPriv** ausgewählt haben, geben Sie das Passwort ein und bestätigen Sie es.

> Das einzige unterstützte Datenschutzprotokoll ist AES.

h. Klicken Sie Auf **Erstellen**.

Der USM-Benutzer wird erstellt und der Tabelle hinzugefügt.

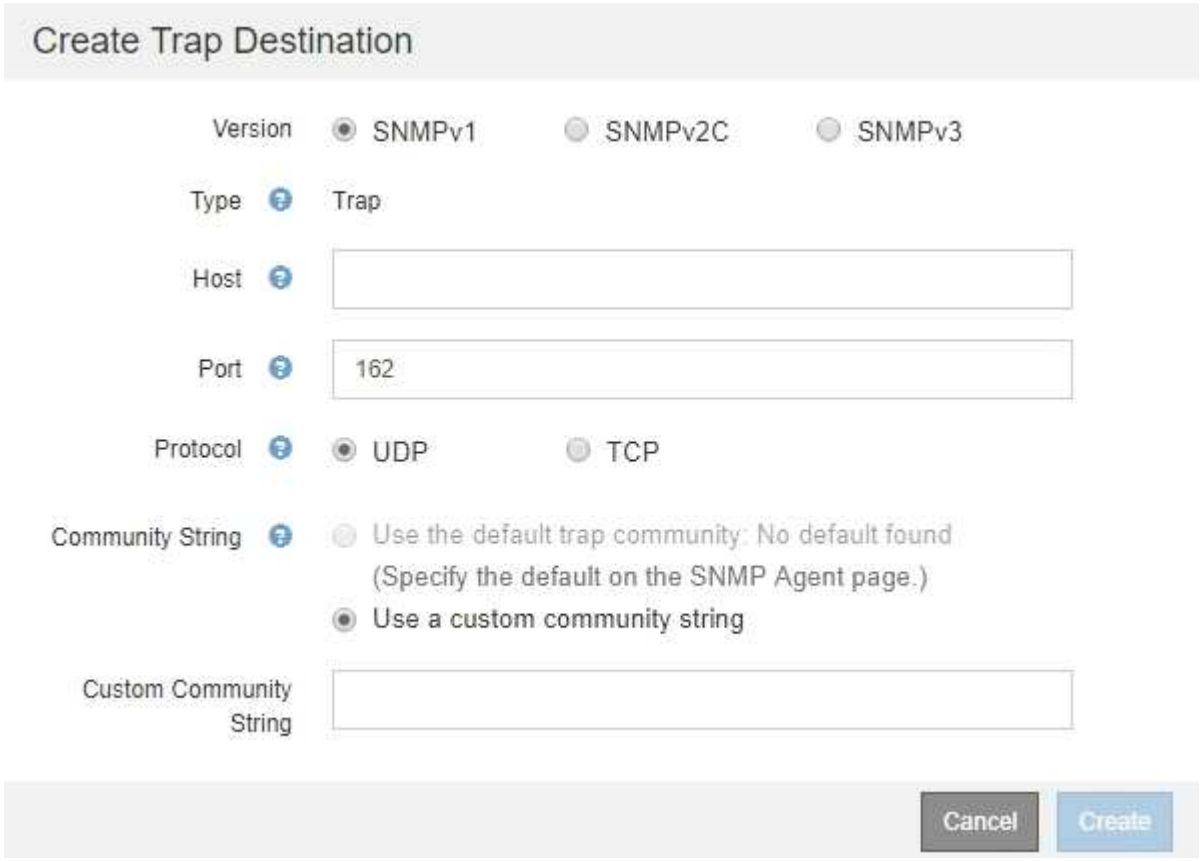


10. Wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Trap-Ziele aus.

Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agent aktivieren und auf **Speichern** klicken, beginnt StorageGRID mit dem Senden von Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen und Alarme ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

a. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld Trap-Ziel erstellen wird angezeigt.



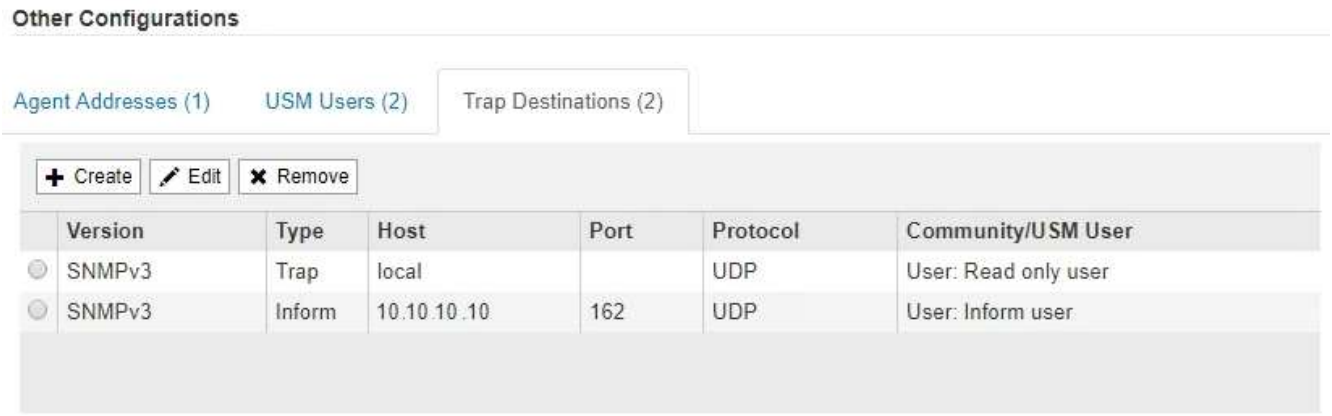
b. Wählen Sie im Feld **Version** die SNMP-Version für diese Benachrichtigung aus.
c. Füllen Sie das Formular aus, basierend auf der ausgewählten Version

Version	Geben Sie diese Informationen an
SNMPv1	**Hinweis:** für SNMPv1 kann der SNMP-Agent nur Traps senden. Informationen werden nicht unterstützt. i. Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. ii. Verwenden Sie für **Port** den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iii. Verwenden Sie für **Protokoll** den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) iv. Verwenden Sie die Standard-Trap-Community, wenn eine auf der Seite SNMP Agent angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.
SNMPv2c	i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird. ii. Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. iii. Verwenden Sie für **Port** den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iv. Verwenden Sie für **Protokoll** den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) v. Verwenden Sie die Standard-Trap-Community, wenn eine auf der Seite SNMP Agent angegeben wurde, oder geben Sie eine benutzerdefinierte Community-Zeichenfolge für dieses Trap-Ziel ein. Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.

Version	Geben Sie diese Informationen an
SNMPv3	i. Wählen Sie aus, ob das Ziel für Traps oder Informationsflüsse verwendet wird. ii. Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse (oder FQDN) ein, um den Trap zu empfangen. iii. Verwenden Sie für **Port** den Standardwert (162), es sei denn, Sie müssen einen anderen Wert verwenden. (162 ist der Standard-Port für SNMP-Traps.) iv. Verwenden Sie für **Protokoll** den Standard (UDP). TCP wird ebenfalls unterstützt. (UDP ist das Standard-SNMP-Trap-Protokoll.) v. Wählen Sie den USM-Benutzer aus, der zur Authentifizierung verwendet werden soll. ◦ Wenn Sie **Trap** ausgewählt haben, werden nur USM-Benutzer ohne maßgebliche Engine-IDs angezeigt. ◦ Wenn Sie **Inform** ausgewählt haben, werden nur USM-Benutzer mit autoritativen Engine-IDs angezeigt.

d. Klicken Sie Auf **Erstellen**.

Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.



11. Wenn Sie die SNMP-Agent-Konfiguration abgeschlossen haben, klicken Sie auf **Speichern**

Die neue SNMP-Agent-Konfiguration wird aktiv.

Verwandte Informationen

"Stummschalten von Warnmeldungen"

SNMP-Agent wird aktualisiert

Sie können SNMP-Benachrichtigungen deaktivieren, Community-Strings aktualisieren

oder Agent-Adressen, USM-Benutzer und Trap-Ziele hinzufügen oder entfernen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Immer wenn Sie die SNMP-Agent-Konfiguration aktualisieren, müssen Sie auf der Seite SNMP-Agent auf **Speichern** klicken, um alle Änderungen zu speichern, die Sie auf jeder Registerkarte vorgenommen haben.

Schritte

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

   Die Seite SNMP-Agent wird angezeigt.

2. Wenn Sie den SNMP-Agent auf allen Grid-Knoten deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **SNMP aktivieren** und klicken Sie auf **Speichern**.

   Der SNMP-Agent ist für alle Grid-Knoten deaktiviert. Wenn Sie den Agent später wieder aktivieren, werden alle vorherigen SNMP-Konfigurationseinstellungen beibehalten.

3. Aktualisieren Sie optional die Werte, die Sie für **Systemkontakt** und **Systemstandort** eingegeben haben.
4. Deaktivieren Sie optional das Kontrollkästchen **SNMP-Agent-Benachrichtigungen aktivieren**, wenn der StorageGRID-SNMP-Agent nicht mehr Trap senden und Benachrichtigungen informieren soll.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, unterstützt der SNMP-Agent den schreibgeschützten MIB-Zugriff, aber es sendet keine SNMP-Benachrichtigungen.

5. Deaktivieren Sie optional das Kontrollkästchen **Authentifizierungsfallen aktivieren**, wenn Sie nicht mehr möchten, dass der StorageGRID-SNMP-Agent einen Authentifizierungs-Trap sendet, wenn er eine nicht ordnungsgemäß authentifizierte Protokollnachricht empfängt.
6. Wenn Sie SNMPv1 oder SNMPv2c verwenden, aktualisieren Sie optional den Abschnitt Community Strings.

   Die Felder in diesem Abschnitt werden für die Community-basierte Authentifizierung in SNMPv1 oder SNMPv2c verwendet. Diese Felder gelten nicht für SNMPv3.

   > Wenn Sie den Standard-Community-String entfernen möchten, müssen Sie zunächst sicherstellen, dass alle Trap-Ziele eine benutzerdefinierte Community-Zeichenfolge verwenden.

7. Wenn Sie Agentenadressen aktualisieren möchten, wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Agentenadressen aus.

Verwenden Sie diese Registerkarte, um eine oder mehrere „`Listening-Adressen`“ anzugeben. Dies sind die StorageGRID-Adressen, auf denen der SNMP-Agent Anfragen erhalten kann. Jede Agentenadresse umfasst ein Internetprotokoll, ein Transportprotokoll, ein StorageGRID-Netzwerk und einen Port.

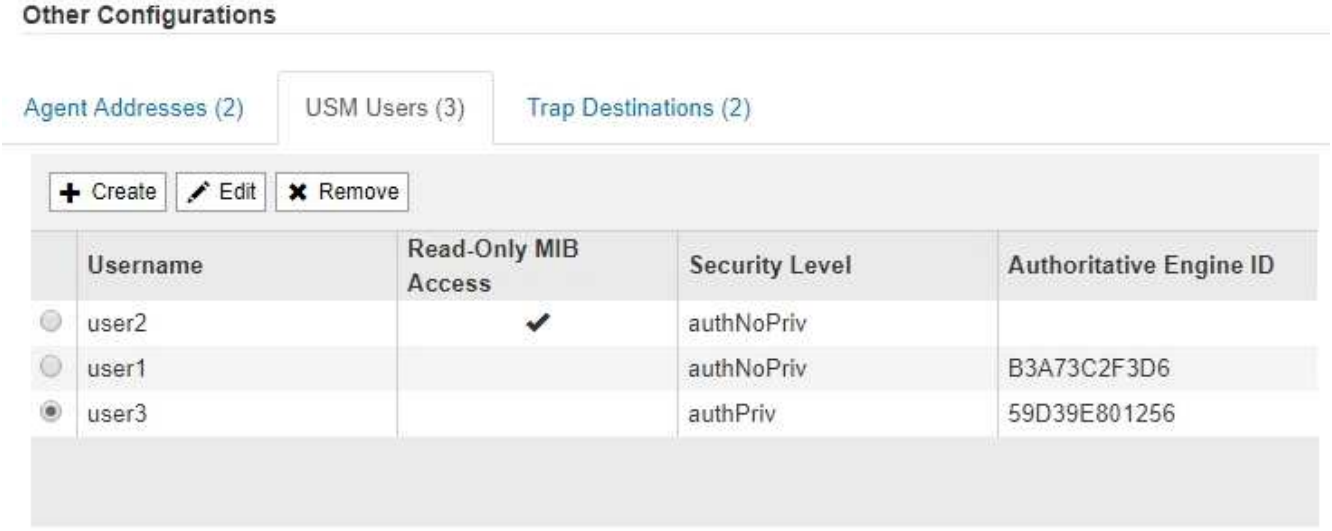
a. Um eine Agentenadresse hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.

b. Um eine Agentenadresse zu bearbeiten, aktivieren Sie das Optionsfeld für die Adresse und klicken auf **Bearbeiten**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.

c. Um eine Agentenadresse zu entfernen, wählen Sie das Optionsfeld für die Adresse aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie diese Adresse entfernen möchten.

d. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

8. Wenn Sie USM-Benutzer aktualisieren möchten, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte USM-Benutzer aus.



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

a. Um einen USM-Benutzer hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für USM-

Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

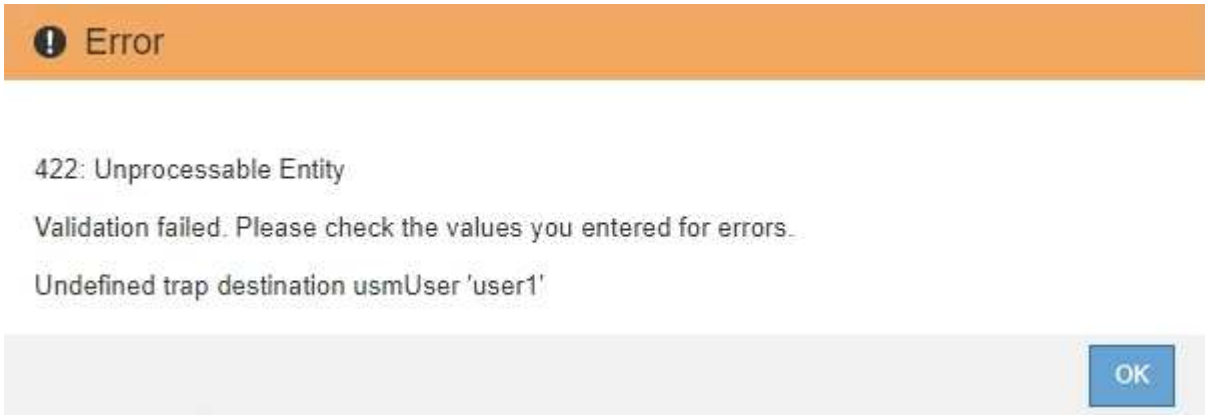
b. Um einen USM-Benutzer zu bearbeiten, wählen Sie das Optionsfeld für den Benutzer aus, und klicken Sie auf **Bearbeiten**. Lesen Sie dann den Schritt für USM-Benutzer in den Anweisungen zur Konfiguration des SNMP-Agenten.

   Der Benutzername für einen bestehenden USM-Benutzer kann nicht geändert werden. Wenn Sie einen Benutzernamen ändern müssen, müssen Sie den Benutzer entfernen und einen neuen erstellen.

   Wenn Sie die autorisierende Engine-ID eines Benutzers hinzufügen oder entfernen und dieser Benutzer derzeit für ein Ziel ausgewählt ist, müssen Sie das Ziel bearbeiten oder entfernen, wie in Schritt beschrieben SNMP-Trap-Ziel. Andernfalls tritt ein Validierungsfehler auf, wenn Sie die SNMP-Agent-Konfiguration speichern.

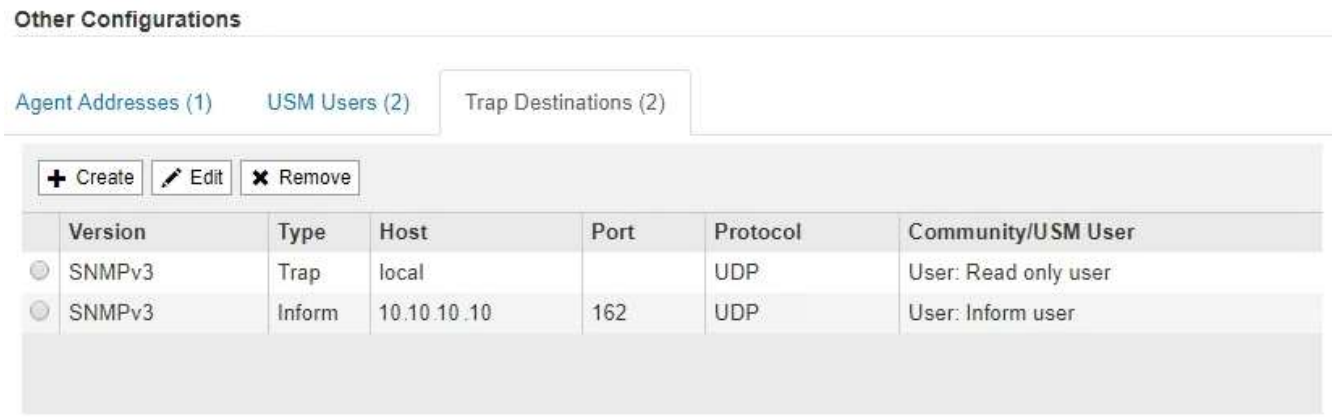
c. Um einen USM-Benutzer zu entfernen, wählen Sie das Optionsfeld für den Benutzer aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie diesen Benutzer entfernen möchten.

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



a. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

1. Wenn Sie Trap-Ziele aktualisieren möchten, wählen Sie im Abschnitt Weitere Konfigurationen die Registerkarte Trap-Ziele aus.



Auf der Registerkarte Trap-Ziele können Sie ein oder mehrere Ziele für StorageGRID-Trap definieren oder Benachrichtigungen informieren. Wenn Sie den SNMP-Agent aktivieren und auf **Speichern** klicken, beginnt StorageGRID mit dem Senden von Benachrichtigungen an jedes definierte Ziel. Benachrichtigungen werden gesendet, wenn Warnungen und Alarme ausgelöst werden. Standardbenachrichtigungen werden auch für die unterstützten MIB-II-Entitäten gesendet (z. B. ifdown und coldstart).

a. Um ein Trap-Ziel hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
b. Um ein Trap-Ziel zu bearbeiten, wählen Sie das Optionsfeld für den Benutzer aus und klicken auf **Bearbeiten**. Lesen Sie dann den Schritt für Trap-Ziele in den Anweisungen zur Konfiguration des SNMP-Agenten.
c. Um ein Trap-Ziel zu entfernen, wählen Sie das Optionsfeld für das Ziel aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie dieses Ziel entfernen möchten.
d. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

2. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, klicken Sie auf **Speichern**.

Verwandte Informationen

"Konfigurieren des SNMP-Agenten"

Erfassung weiterer StorageGRID-Daten

Es gibt verschiedene zusätzliche Möglichkeiten, Daten zu erfassen und zu analysieren, die bei der Untersuchung des Zustands Ihres StorageGRID Systems oder bei der Arbeit mit dem technischen Support zur Behebung von Problemen hilfreich sein können.

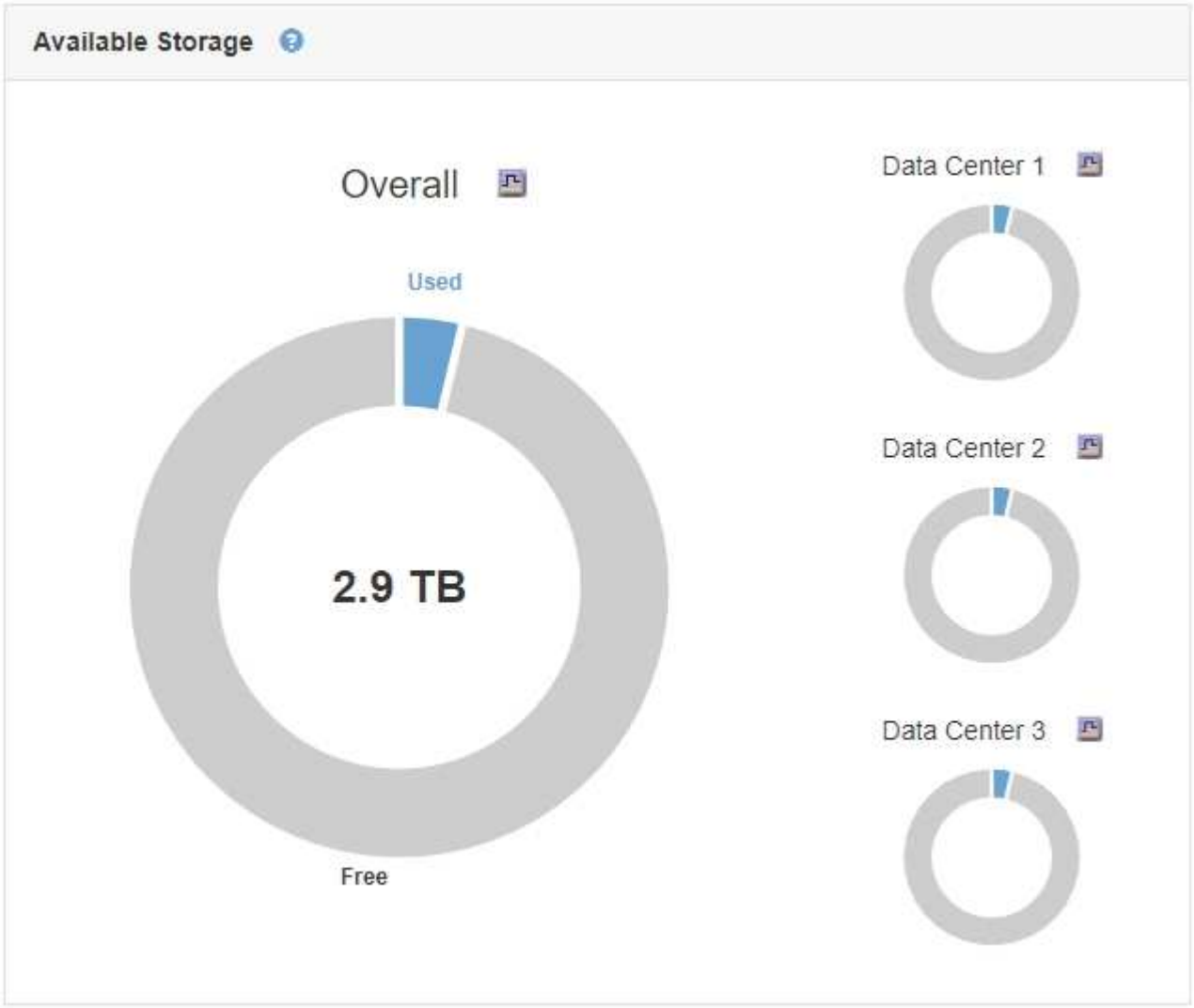
- "Verwenden von Diagrammen und Berichten"
- "Monitoring PUT und GET Performance"
- "Monitoring von Objektverifizierungsvorgängen"
- "Monitoring von Ereignissen"
- "Überprüfen von Audit-Meldungen"
- "Protokolldateien und Systemdaten werden erfasst"
- "Manuelles Auslösen einer AutoSupport-Meldung"
- "Anzeigen der Struktur der Grid Topology"
- "Überprüfen von Support-Metriken"
- "Diagnose wird ausgeführt"
- "Erstellen benutzerdefinierter Überwachungsanwendungen"

Verwenden von Diagrammen und Berichten

Mithilfe von Diagrammen und Berichten lässt sich der Zustand des StorageGRID Systems überwachen und Probleme beheben. Die im Grid Manager verfügbaren Diagrammtypen und Berichte umfassen Tortendiagramme (nur auf dem Dashboard), Diagramme und Textberichte.

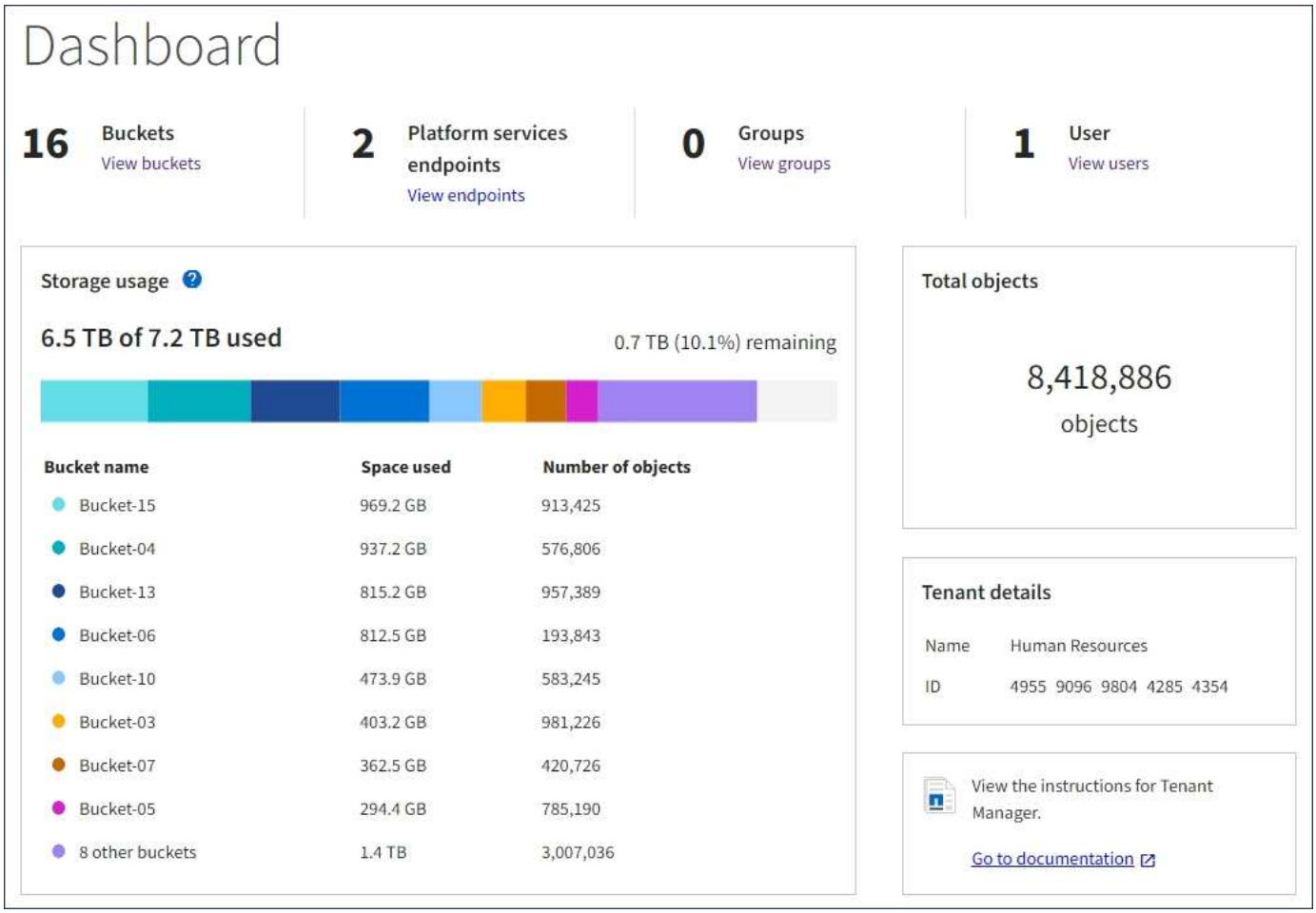
Diagramme und Diagramme fassen die Werte bestimmter StorageGRID-Metriken und -Attribute zusammen.

Das Grid Manager Dashboard enthält PIE-Diagramme (Donut), um den verfügbaren Speicher für das Grid und jeden Standort zusammenzufassen.



Im Bereich Speichernutzung auf dem Tenant Manager Dashboard werden folgende Informationen angezeigt:

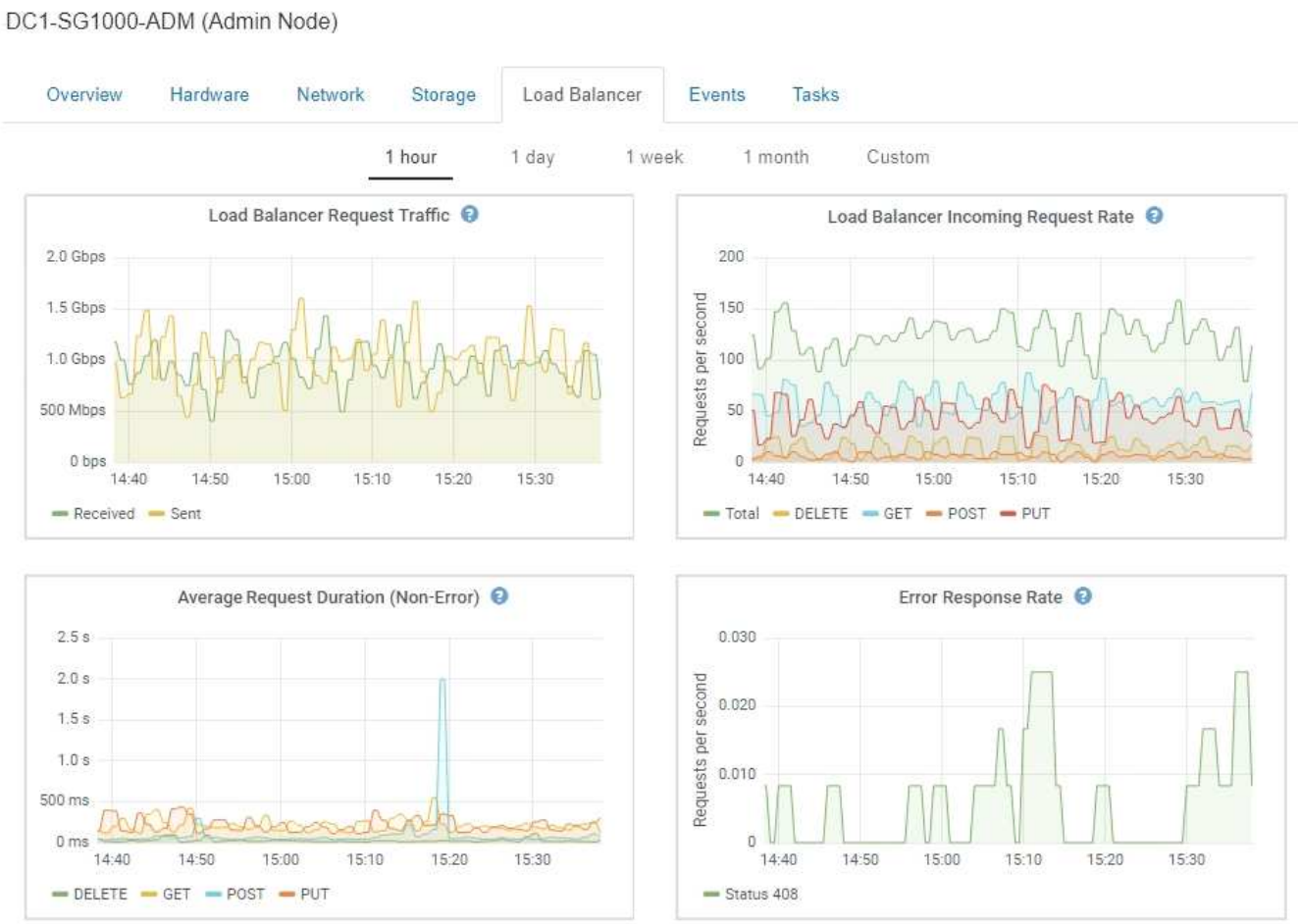
- Eine Liste der größten Buckets (S3) oder Container (Swift) für die Mandanten
- Ein Balkendiagramm, das die relative Größe der größten Buckets oder Container darstellt
- Der insgesamt verwendete Speicherplatz und, wenn ein Kontingent festgelegt ist, die Menge und der Prozentsatz des verbleibenden Speicherplatzes



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

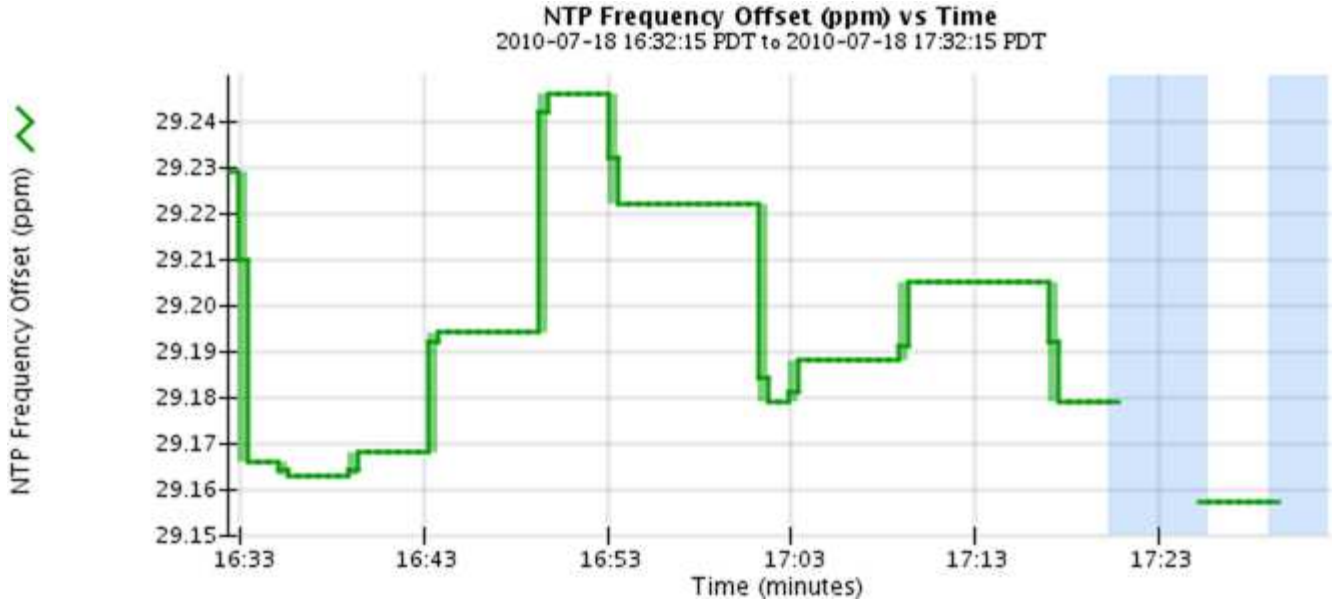
Es gibt vier Arten von Diagrammen:

- **Grafana-Diagramme**: Auf der Seite Knoten werden Grafana-Diagramme verwendet, um die Werte der Prometheus-Kennzahlen im Laufe der Zeit zu zeichnen. Die Registerkarte **Nodes** > **Load Balancer** für einen Admin-Node enthält beispielsweise vier Grafana-Diagramme.

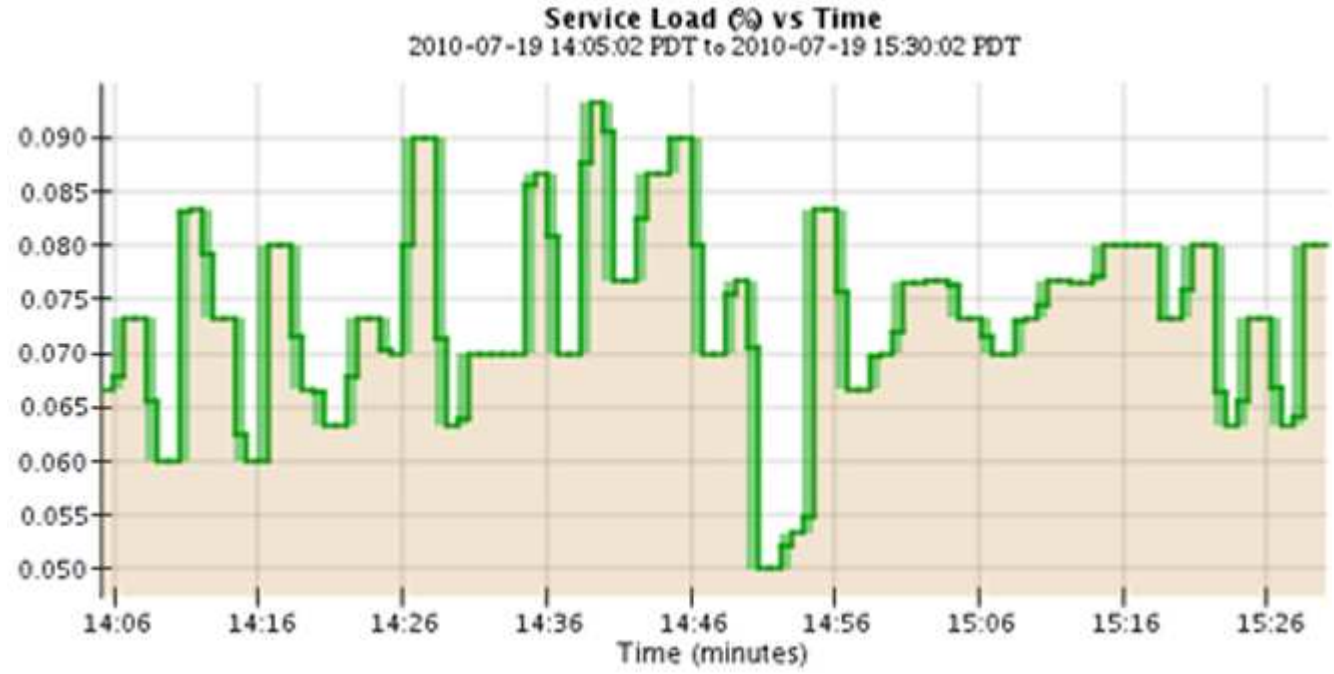


Grafana-Diagramme sind auch auf den vorkonfigurierten Dashboards enthalten, die auf der Seite **Support** > **Tools** > **Metrics** verfügbar sind.

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

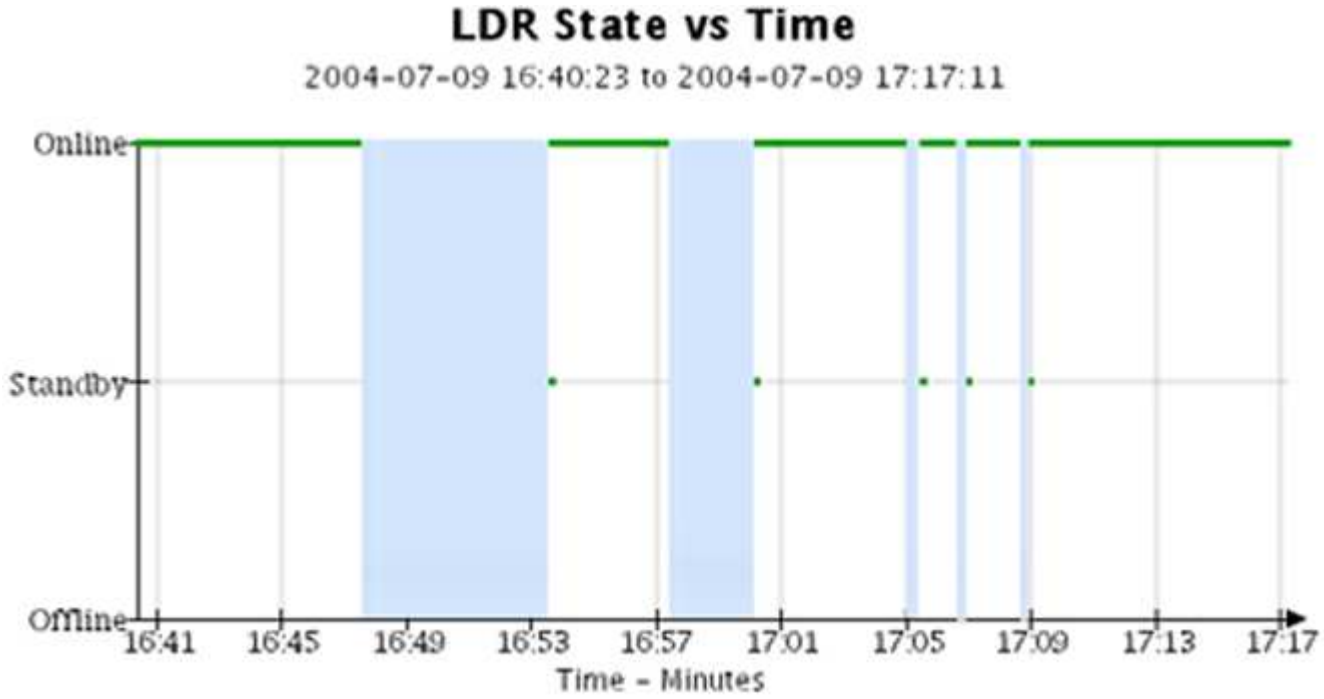


- **Flächendiagramme**: Verfügbar auf der Seite Knoten und auf der Seite **Support** > **Tools** > **Grid Topology** (Klicken Sie auf das Diagrammsymbol Nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen zu zeichnen, z. B. Objektanzahl oder Dienstlastwerte. Die Flächendiagramme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



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

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



Verwandte Informationen

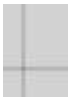
"Anzeigen der Seite Knoten"

"Anzeigen der Struktur der Grid Topology"

"Überprüfen von Support-Metriken"

Diagrammlegende

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

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

Anzeigen von Diagrammen und Diagrammen

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

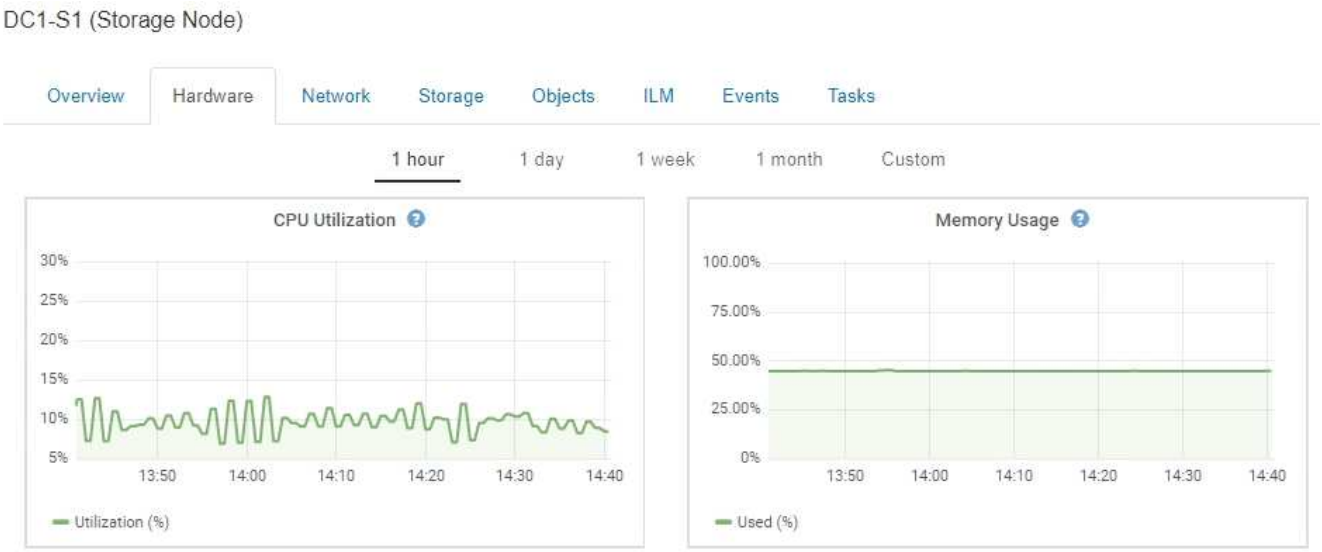
Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

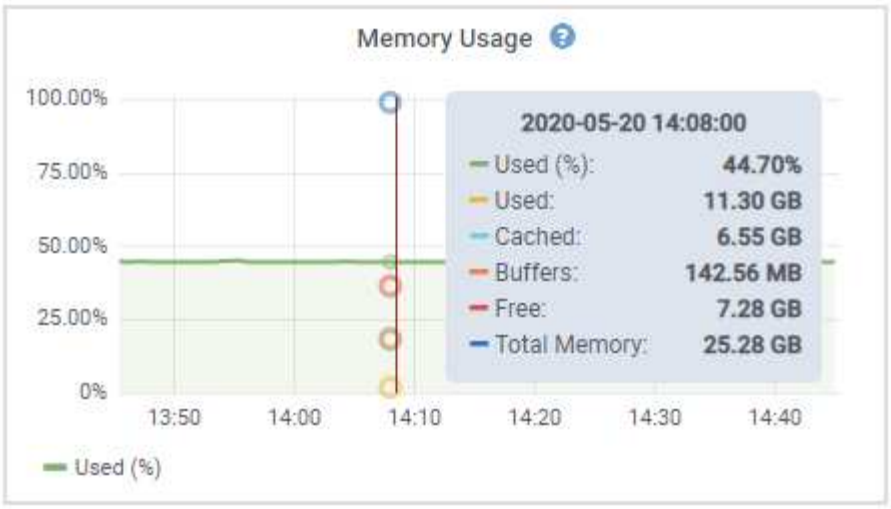
Schritte

1. Wählen Sie **Knoten**. Wählen Sie dann einen Knoten, einen Standort oder das gesamte Raster aus.
2. Wählen Sie die Registerkarte aus, auf der Informationen angezeigt werden sollen.

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



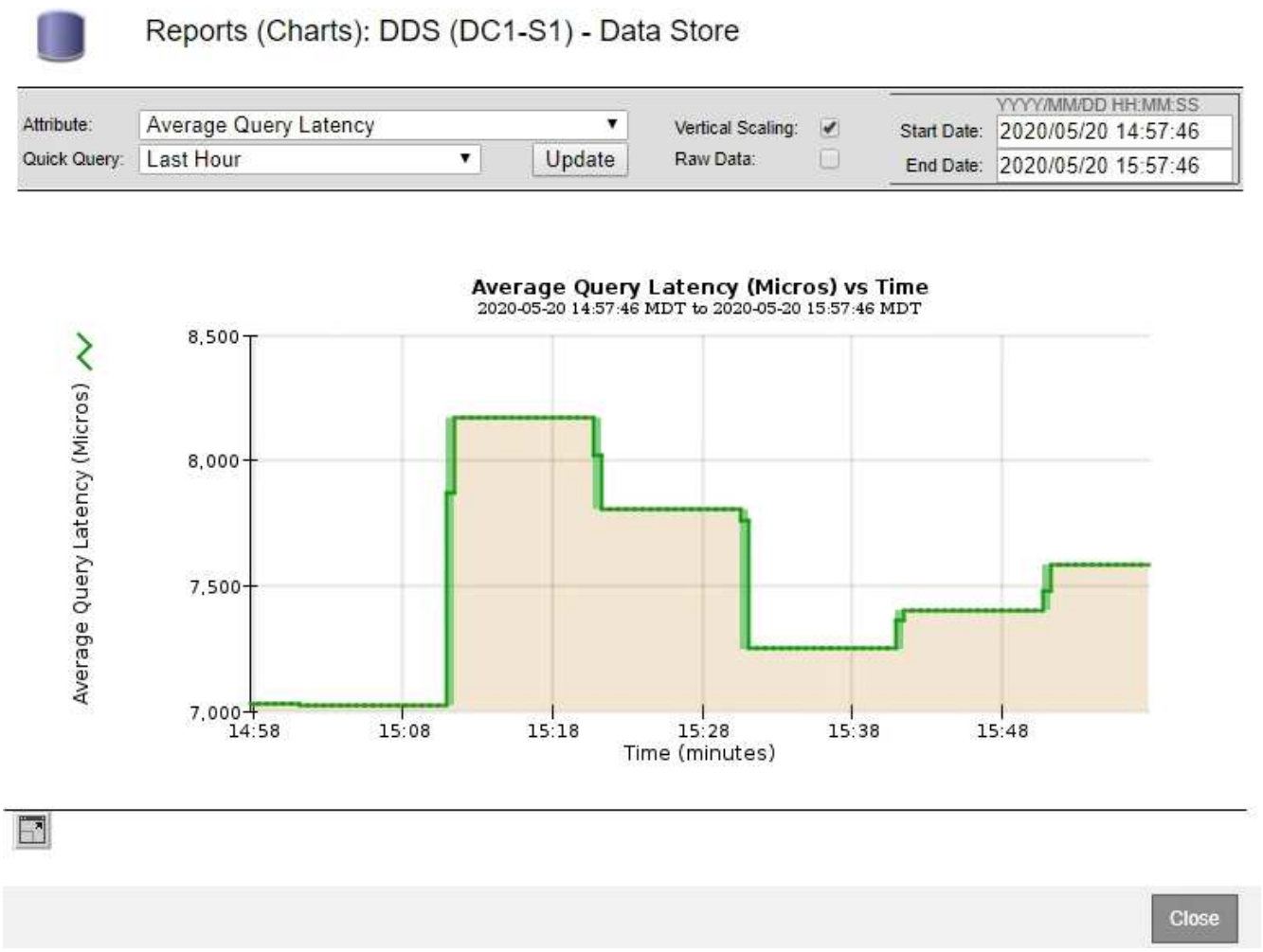
3. Bewegen Sie den Cursor optional über das Diagramm, um detailliertere Werte für einen bestimmten Zeitpunkt anzuzeigen.



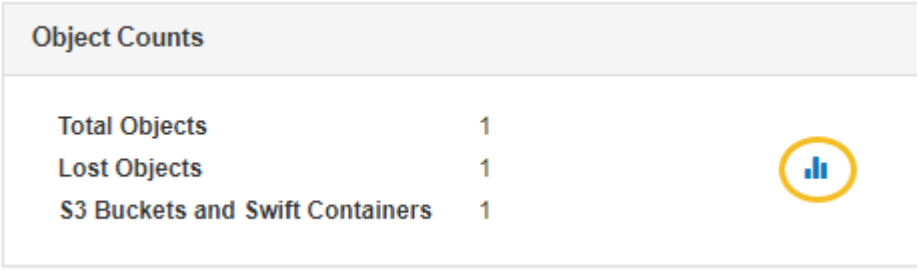
4. Bei Bedarf können Sie oft ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Klicken Sie in der Tabelle auf der Seite Knoten auf das Diagrammsymbol Oder Rechts neben dem Attributnamen.

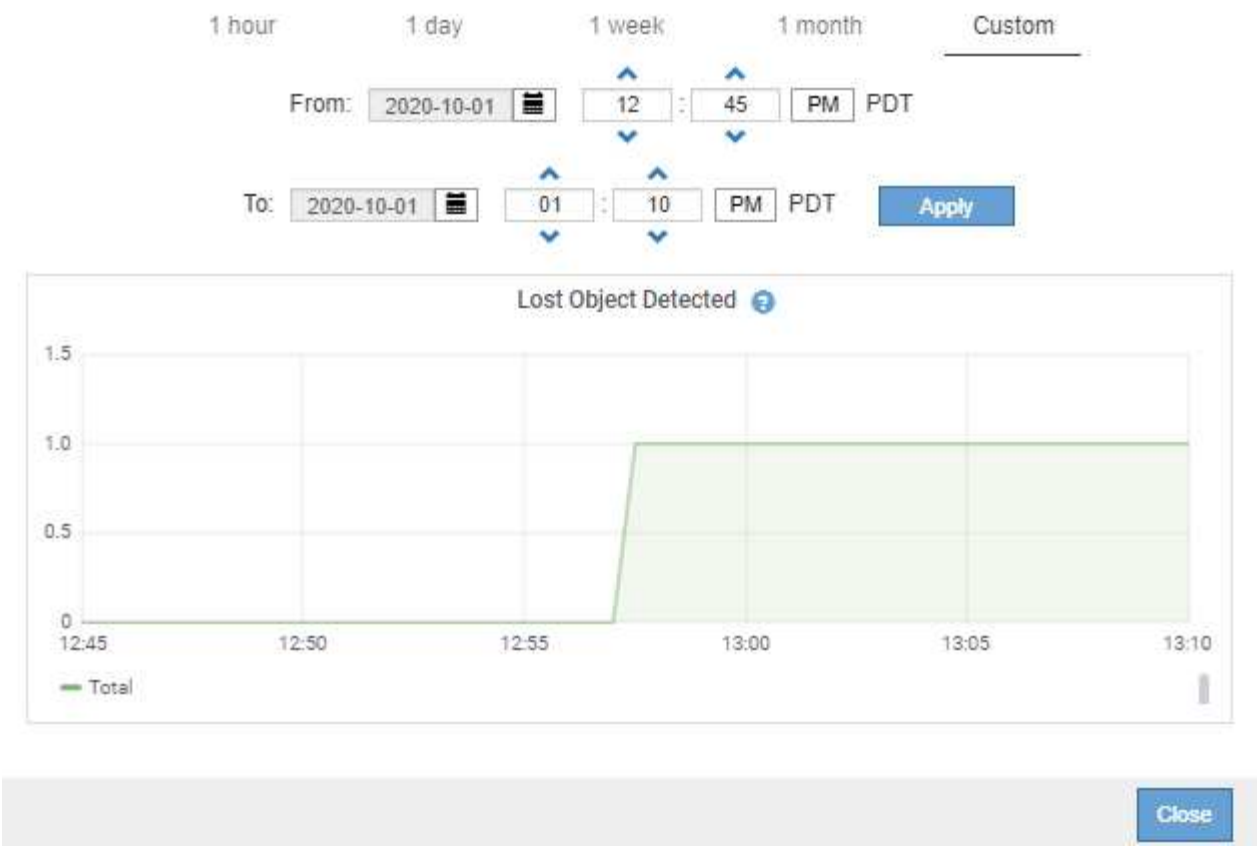
   Diagramme sind nicht für alle Metriken und Attribute verfügbar.

   Beispiel 1: Auf der Registerkarte Objekte für einen Speicherknoten können Sie auf das Diagrammsymbol klicken Um die durchschnittliche Latenz einer Metadatenabfrage im Laufe der Zeit anzuzeigen.



Beispiel 2: Auf der Registerkarte Objekte für einen Speicherknoten können Sie auf das Diagrammsymbol klicken Zeigt die Grafana-Grafik der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte an.





5. Um Diagramme für Attribute anzuzeigen, die nicht auf der Knotenseite angezeigt werden, wählen Sie **Support** > **Tools** > **Grid Topology**.
6. Wählen Sie ***Grid Node*** > ***Component oder Service*** > **Übersicht** > **Main** aus.
7. Klicken Sie auf das Diagrammsymbol Neben dem Attribut.

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

Diagramme werden erstellt

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Grid Node*** > ***Component oder Service*** > **Berichte** > **Diagramme** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Um die Y-Achse auf Null zu starten, deaktivieren Sie das Kontrollkästchen **Vertikale Skalierung**.

5. Um Werte mit voller Präzision anzuzeigen, aktivieren Sie das Kontrollkästchen **Raw Data** oder um Werte auf maximal drei Dezimalstellen zu runden (z. B. bei Attributen, die als Prozentsätze angegeben werden), deaktivieren Sie das Kontrollkästchen **Raw Data**.
6. Wählen Sie den Zeitraum aus der Dropdown-Liste **Quick Query** aus, für den Sie einen Bericht erstellen möchten.

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

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

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

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

8. Klicken Sie Auf **Aktualisieren**.

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

9. Wenn Sie das Diagramm drucken möchten, klicken Sie mit der rechten Maustaste, und wählen Sie **Drucken**, und ändern Sie die erforderlichen Druckereinstellungen und klicken Sie auf **Drucken**.

Arten von Textberichten

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

RAW-Textberichte

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

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

Text Results for Services: Load - System Logging

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

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

Zusammenfassen von Textberichten

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

In jedem Eintrag werden die folgenden Informationen angezeigt:

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

Text Results for Attribute Send to Relay Rate

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

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

Textberichte werden erstellt

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

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

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

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

Schritte

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

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

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

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

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

8. Klicken Sie Auf **Aktualisieren**.

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

9. Wenn Sie den Bericht drucken möchten, klicken Sie mit der rechten Maustaste, und wählen Sie **Drucken**, und ändern Sie die erforderlichen Druckereinstellungen und klicken Sie auf **Drucken**.

Exportieren von Textberichten

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

Über diese Aufgabe

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

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Erstellen Sie einen Textbericht.
3. Klicken Sie Auf *Exportieren*.

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

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

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

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

Monitoring PUT und GET Performance

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

Über diese Aufgabe

Um DIE PUT- und GET-Leistung zu überwachen, können Sie S3- und Swift-Befehle direkt von einer Workstation aus oder über die Open-Source S3tester-Anwendung ausführen. Mit diesen Methoden können Sie die Leistung unabhängig von Faktoren bewerten, die außerhalb von StorageGRID liegen, z. B. Probleme mit einer Client-Applikation oder Probleme mit einem externen Netzwerk.

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

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

Meldungen im Prüfprotokoll geben die Gesamtzeit an, die für die Ausführung bestimmter Vorgänge erforderlich ist. Um z. B. die Gesamtverarbeitungszeit für eine S3-GET-Anforderung zu bestimmen, können Sie den Wert des ZEITATTRIBUTS in der SGET-Audit-Nachricht prüfen. Das ZEITATTRIBUT finden Sie auch in den Audit-Meldungen für die folgenden Vorgänge:

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

Bei der Analyse von Ergebnissen sollten Sie die durchschnittliche Zeit zur Erfüllung einer Anfrage sowie den Gesamtdurchsatz betrachten, den Sie erreichen können. Wiederholen Sie die gleichen Tests regelmäßig, und

notieren Sie die Ergebnisse, damit Sie Trends erkennen können, die möglicherweise untersucht werden müssen.

- Sie können S3tester von github:https://github.com/s3tester herunterladen

Verwandte Informationen

"Prüfung von Audit-Protokollen"

Monitoring von Objektverifizierungsvorgängen

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

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Es gibt zwei Überprüfungsprozesse, die zusammenarbeiten, um die Datenintegrität zu gewährleisten:

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

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

  > Die Warnung **nicht identifiziertes korruptes Objekt erkannt** wird ausgelöst, wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann.

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

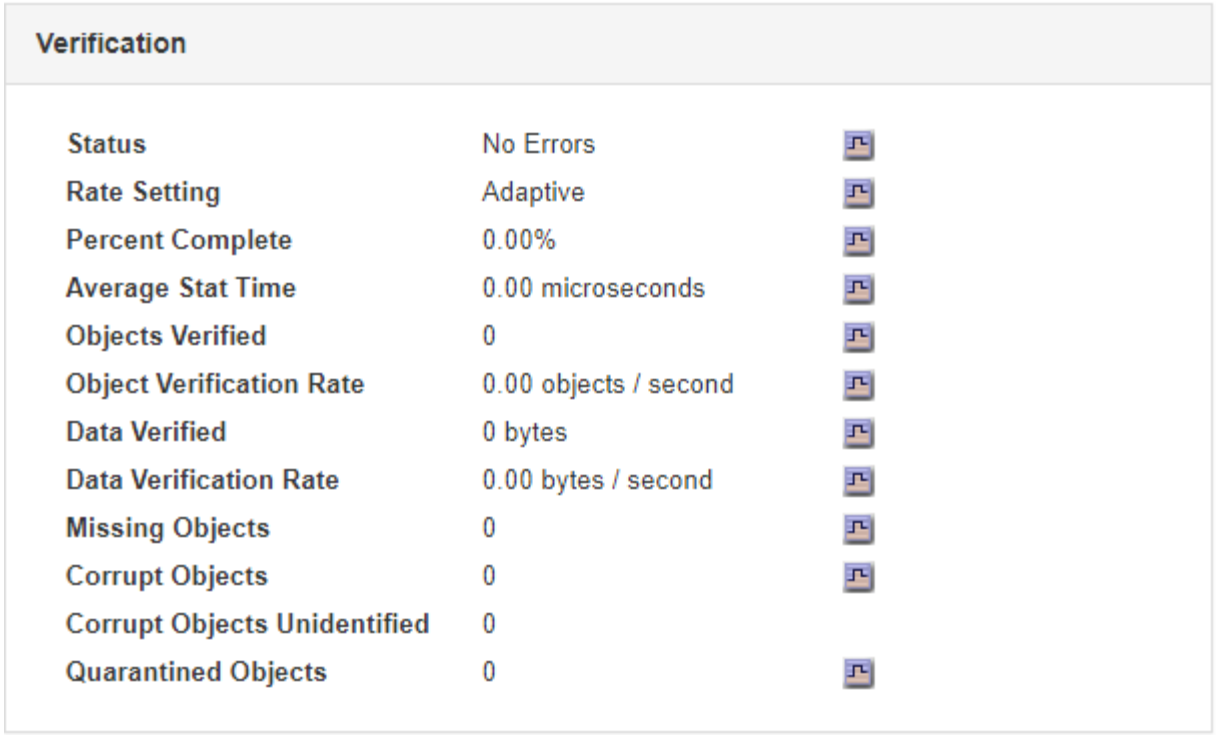
  Bei der Vordergrundüberprüfung können Sie die Existenz replizierter und Erasure-codierter Objektdaten auf einem bestimmten Storage-Node überprüfen und überprüfen, ob alle Objekte vorhanden sein sollen. Sie können die Vordergrundüberprüfung auf allen oder einigen Objektspeichern eines Storage Node ausführen, um festzustellen, ob es bei einem Speichergerät Integritätsprobleme gibt. Eine große Anzahl von fehlenden Objekten kann darauf hindeuten, dass es ein Problem mit der Speicherung gibt.

Um Ergebnisse aus Hintergrund- und Vordergrundverifizierungen, wie z. B. beschädigte oder fehlende Objekte, zu prüfen, können Sie auf der Seite Knoten einen Speicherknoten sehen. Sie sollten alle Instanzen von beschädigten oder fehlenden Objektdaten sofort untersuchen, um die Ursache zu ermitteln.

Schritte

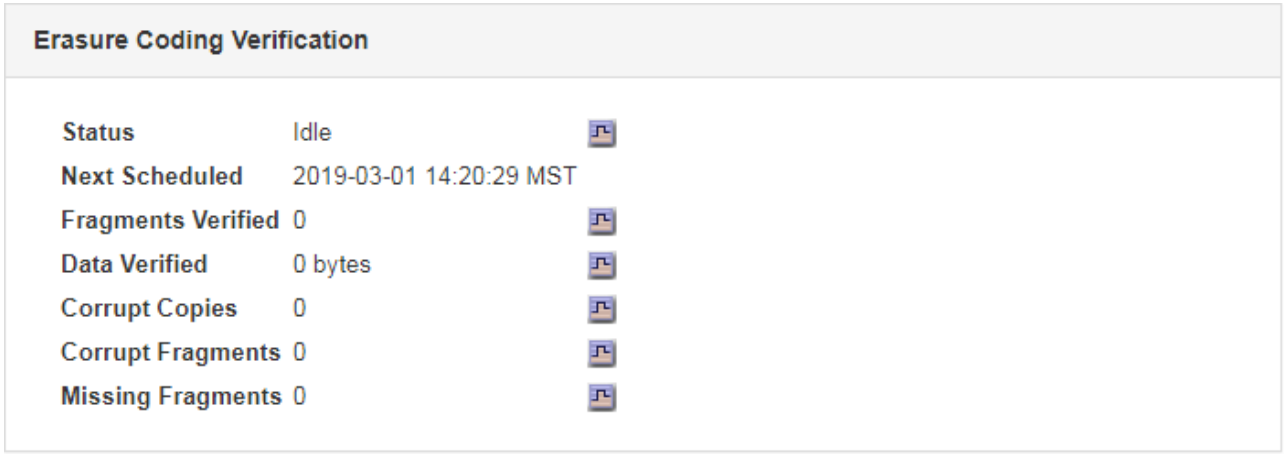
1. Wählen Sie **Knoten**.
2. Wählen Sie ***Speicherknoten*** > **Objekte** Aus.
3. So prüfen Sie die Überprüfungsergebnisse:

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



Klicken Sie in der Tabelle auf den Namen eines Attributs, um den Hilfetext anzuzeigen.

- Um die Überprüfung von Fragment mit Löschungscode zu überprüfen, wählen Sie ***Storage Node*** > **ILM** aus, und sehen Sie sich die Attribute in der Tabelle „Erasure Coding Verification“ an.



Klicken Sie in der Tabelle auf den Namen eines Attributs, um den Hilfetext anzuzeigen.

Verwandte Informationen

"Überprüfen der Objektintegrität"

Monitoring von Ereignissen

Sie können Ereignisse überwachen, die von einem Grid-Node erkannt werden, einschließlich benutzerdefinierter Ereignisse, die Sie erstellt haben, um Ereignisse zu verfolgen, die auf dem Syslog-Server protokolliert werden. Die Meldung Letztes Ereignis,

die im Grid Manager angezeigt wird, enthält weitere Informationen zum letzten Ereignis.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log` Protokolldatei.

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

Überprüfen von Ereignissen auf der Seite Knoten

Auf der Seite Nodes werden die Systemereignisse für jeden Grid-Node aufgeführt.

1. Wählen Sie **Knoten**.
2. Wählen Sie ***Grid Node*** > **Events** aus.
3. Stellen Sie oben auf der Seite fest, ob ein Ereignis für **Letztes Ereignis** angezeigt wird, das das letzte Ereignis beschreibt, das vom Grid-Knoten erkannt wurde.

   Das Ereignis wird wortgetreu vom Grid-Node übermittelt und enthält alle Protokollmeldungen mit dem Schweregrad „FEHLER“ oder „KRITISCH“.
4. Überprüfen Sie in der Tabelle, ob die Anzahl für ein Ereignis oder einen Fehler nicht Null ist.
5. Klicken Sie nach dem Beheben von Problemen auf **Ereignisanzahl zurücksetzen**, um die Zählung auf Null zurückzusetzen.

Überprüfen von Ereignissen auf der Seite Grid Topology

Auf der Seite Grid Topology werden außerdem die Systemereignisse für jeden Grid-Node aufgeführt.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Events** > **Übersicht** > **Main**.

Verwandte Informationen

"Ereignisanzahl wird zurückgesetzt"

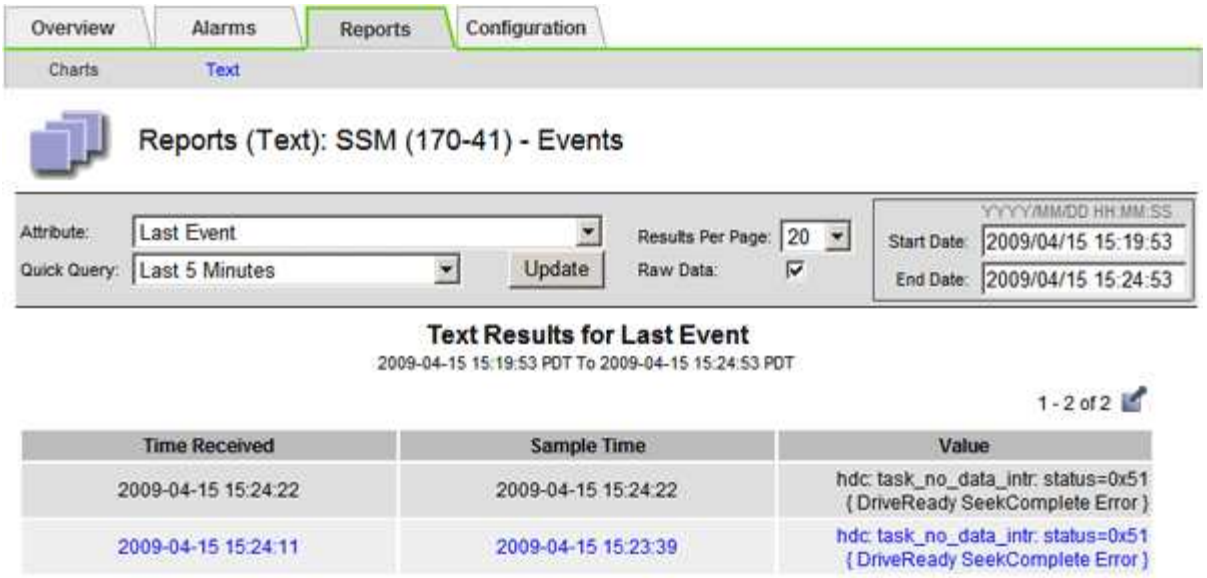
"Referenz für Protokolldateien"

Vorherige Ereignisse überprüfen

Sie können eine Liste vorheriger Ereignismeldungen generieren, um Probleme zu isolieren, die in der Vergangenheit aufgetreten sind.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Events** > **Berichte** aus.
3. Wählen Sie **Text**.

   Das Attribut **Letztes Ereignis** wird in der Ansicht Diagramme nicht angezeigt.
4. Ändern Sie **Attribut** in **Letztes Ereignis**.
5. Wählen Sie optional einen Zeitraum für **Quick Query** aus.
6. Klicken Sie Auf **Aktualisieren**.



Verwandte Informationen

"Verwenden von Diagrammen und Berichten"

Ereignisanzahl wird zurückgesetzt

Nach dem Beheben von Systemereignissen können Sie die Ereignisanzahl auf Null zurücksetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung für die Konfiguration der Seite für die Grid-Topologie verfügen.

Schritte

1. Wählen Sie **Nodes** > ***Grid Node*** > **Events** Aus.
2. Stellen Sie sicher, dass jedes Ereignis mit einer Zählung von mehr als 0 gelöst wurde.
3. Klicken Sie auf **Ereignisanzahl zurücksetzen**.

Events

Last Event No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Heap Out Of Memory Errors	0
Cassandra unhandled exceptions	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Node Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0
Stat Service Events	0
Storage Hardware Events	0
System Time Events	0

Reset event counts

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

Über diese Aufgabe

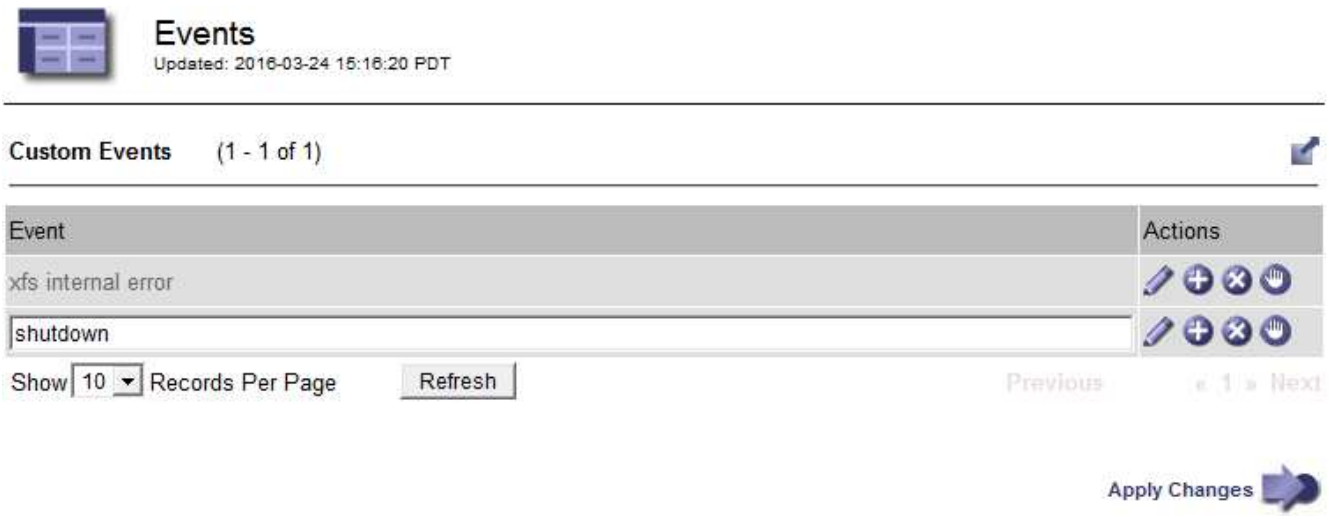
Ziehen Sie in Betracht, benutzerdefinierte Ereignisse zu erstellen, um wiederkehrende Probleme zu überwachen. Die folgenden Überlegungen gelten für benutzerdefinierte Ereignisse.

- Nach der Erstellung eines benutzerdefinierten Ereignisses wird jeder Vorgang überwacht. Auf der Seite **Nodes** > ***GRID Node*** > **Events** können Sie einen kumulativen Zählwert für alle benutzerdefinierten Ereignisse anzeigen.
- So erstellen Sie ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern im `/var/log/messages` Oder `/var/log/syslog` Dateien, die Protokolle in diesen Dateien müssen:
  - Vom Kernel generiert
  - Wird vom Daemon oder vom Benutzerprogramm auf der Fehler- oder kritischen Ebene generiert

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

Schritte

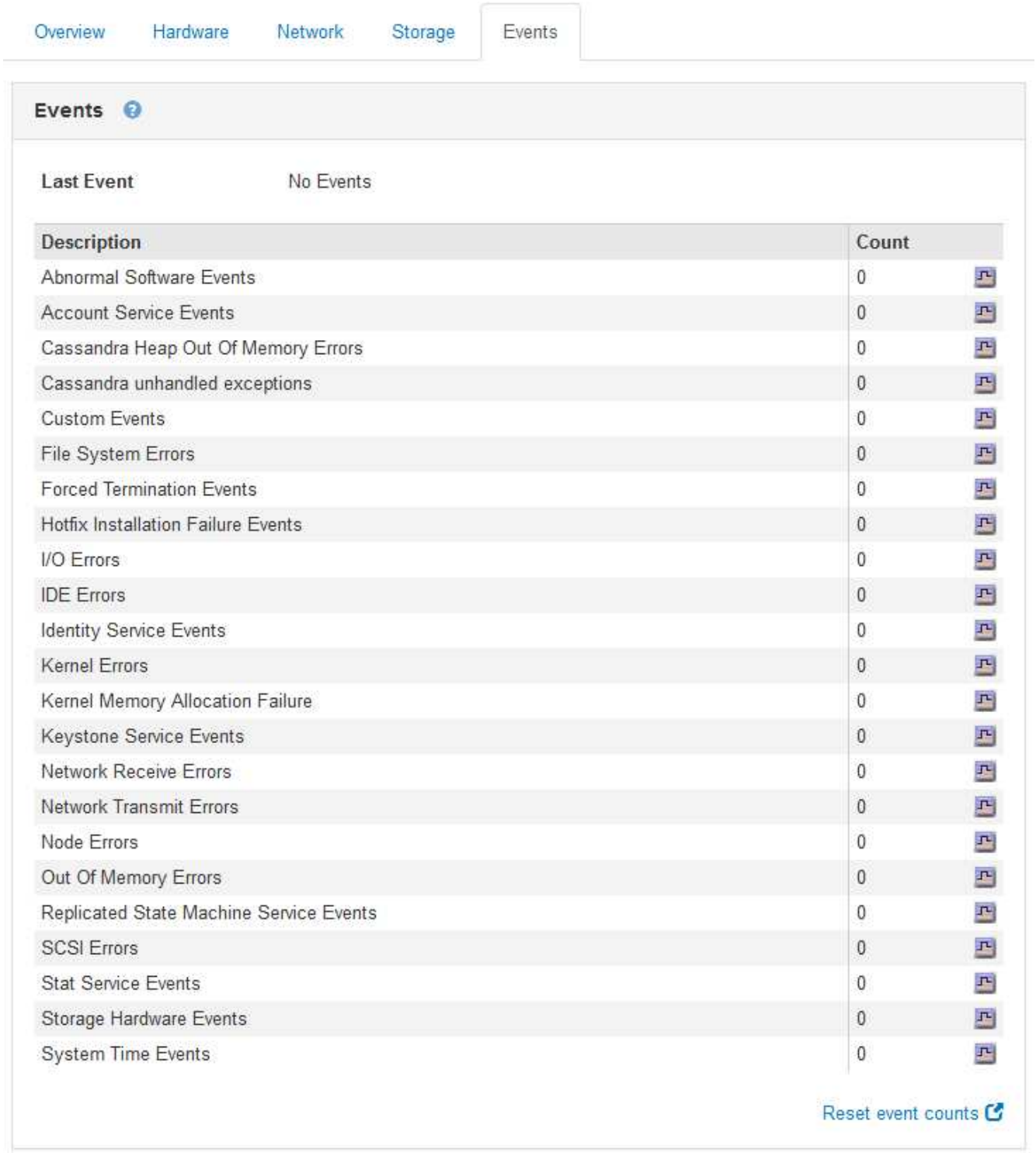
1. Wählen Sie **Konfiguration** > **Überwachung** > **Ereignisse**.
2. Klicken Sie Auf **Bearbeiten** (Oder **Einfügen** Wenn dies nicht das erste Ereignis ist).
3. Geben Sie eine benutzerdefinierte Ereigniszeichenfolge ein, z. B. Herunterfahren



4. Klicken Sie Auf **Änderungen Übernehmen**.
5. Wählen Sie **Knoten**. Wählen Sie dann ***GRID Node*** > **Events** aus.
6. Suchen Sie den Eintrag für benutzerdefinierte Ereignisse in der Ereignistabelle, und überwachen Sie den Wert für **Zählung**.

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

Node ausgelöst.



Zurücksetzen der Anzahl benutzerdefinierter Ereignisse auf Null

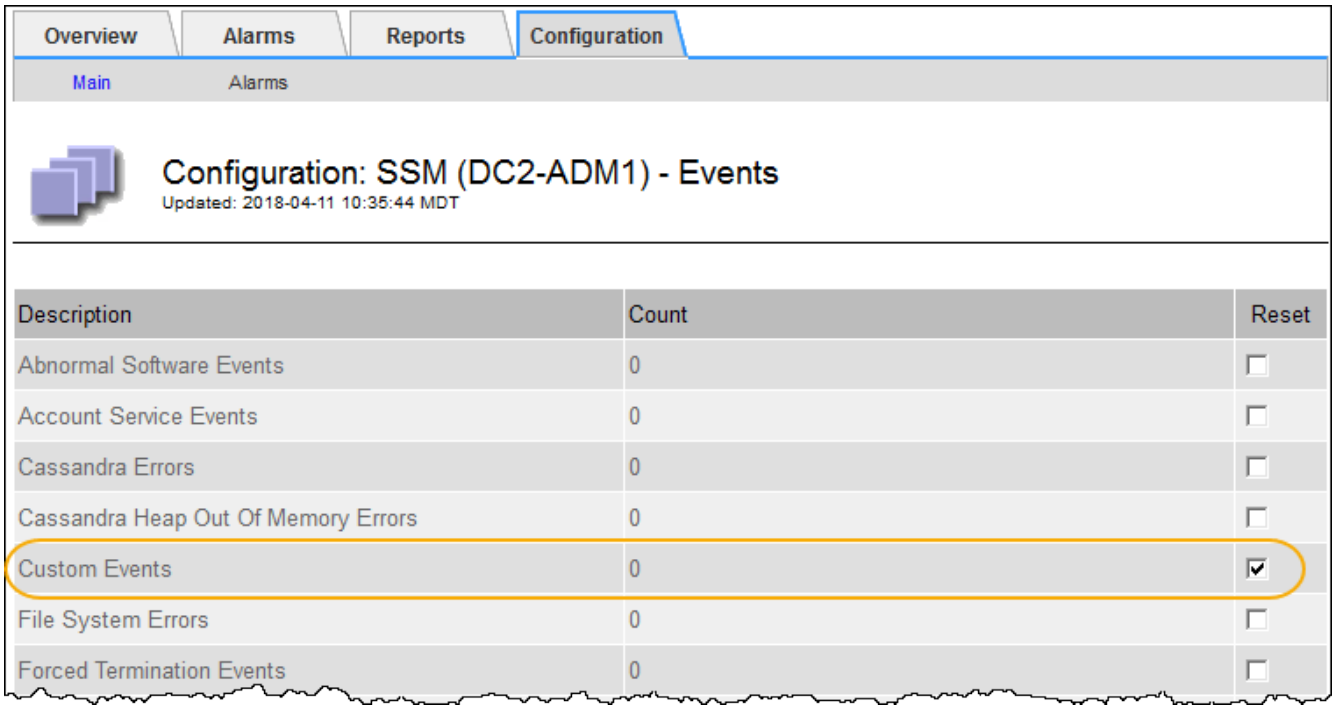
Wenn Sie den Zähler nur für benutzerdefinierte Ereignisse zurücksetzen möchten, müssen Sie die Seite Grid Topology im Menü Support verwenden.

Über diese Aufgabe

Beim Zurücksetzen eines Zählers wird der Alarm durch das nächste Ereignis ausgelöst. Wenn Sie einen Alarm

quittieren, wird dieser Alarm dagegen nur erneut ausgelöst, wenn der nächste Schwellwert erreicht wird.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Grid Node*** > **SSM** > **Events** > **Konfiguration** > **Main** aus.
3. Aktivieren Sie das Kontrollkästchen **Zurücksetzen** für benutzerdefinierte Ereignisse.



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

Überprüfen von Audit-Meldungen

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

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

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

Jeder Admin-Knoten speichert Audit-Meldungen in Textdateien. Die Revisionsfreigabe enthält die aktive Datei (Audit.log) sowie komprimierte Audit-Protokolle aus früheren Tagen.

Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf die Audit-Share sowohl für NFS als auch für CIFS (veraltet) konfigurieren. Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Details zur Audit-Protokolldatei, zum Format von Audit-Meldungen, zu den Typen von Audit-Meldungen und zu den verfügbaren Tools zur Analyse von Audit-Meldungen finden Sie in den Anweisungen für Audit-Meldungen. Weitere Informationen zum Konfigurieren des Zugriffs auf Audit-Clients finden Sie in den Anweisungen für die Administration von StorageGRID.

Verwandte Informationen

"Prüfung von Audit-Protokollen"

"StorageGRID verwalten"

Protokolldateien und Systemdaten werden erfasst

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

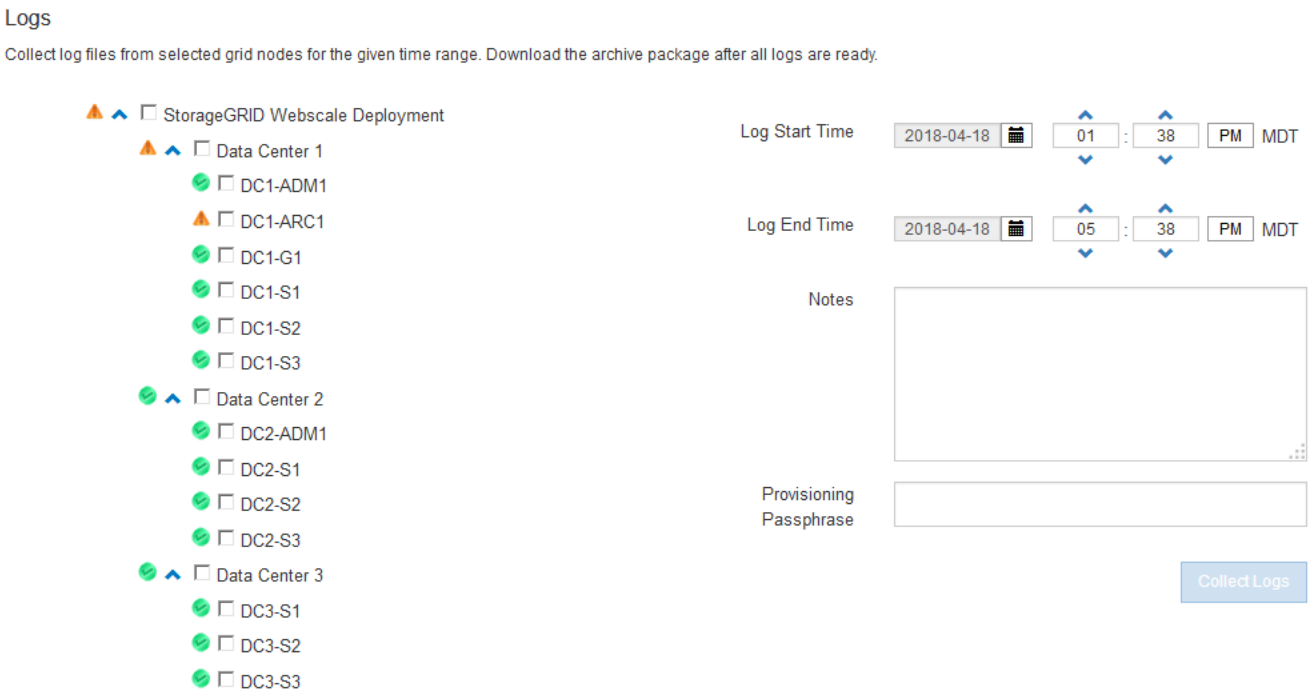
Über diesen Taak

Mit dem Grid Manager können Sie Protokolldateien, Systemdaten und Konfigurationsdaten für den von Ihnen ausgewählten Zeitraum von einem beliebigen Grid-Node aus erfassen. Die Daten werden in einer .tar.gz-Datei gesammelt und archiviert, die Sie dann auf Ihren lokalen Computer herunterladen können.

Da Anwendungsprotokolle sehr groß sein können, muss das Zielverzeichnis, in dem Sie die archivierten Protokolldateien herunterladen, mindestens 1 GB freien Speicherplatz haben.

Schritte

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



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

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

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

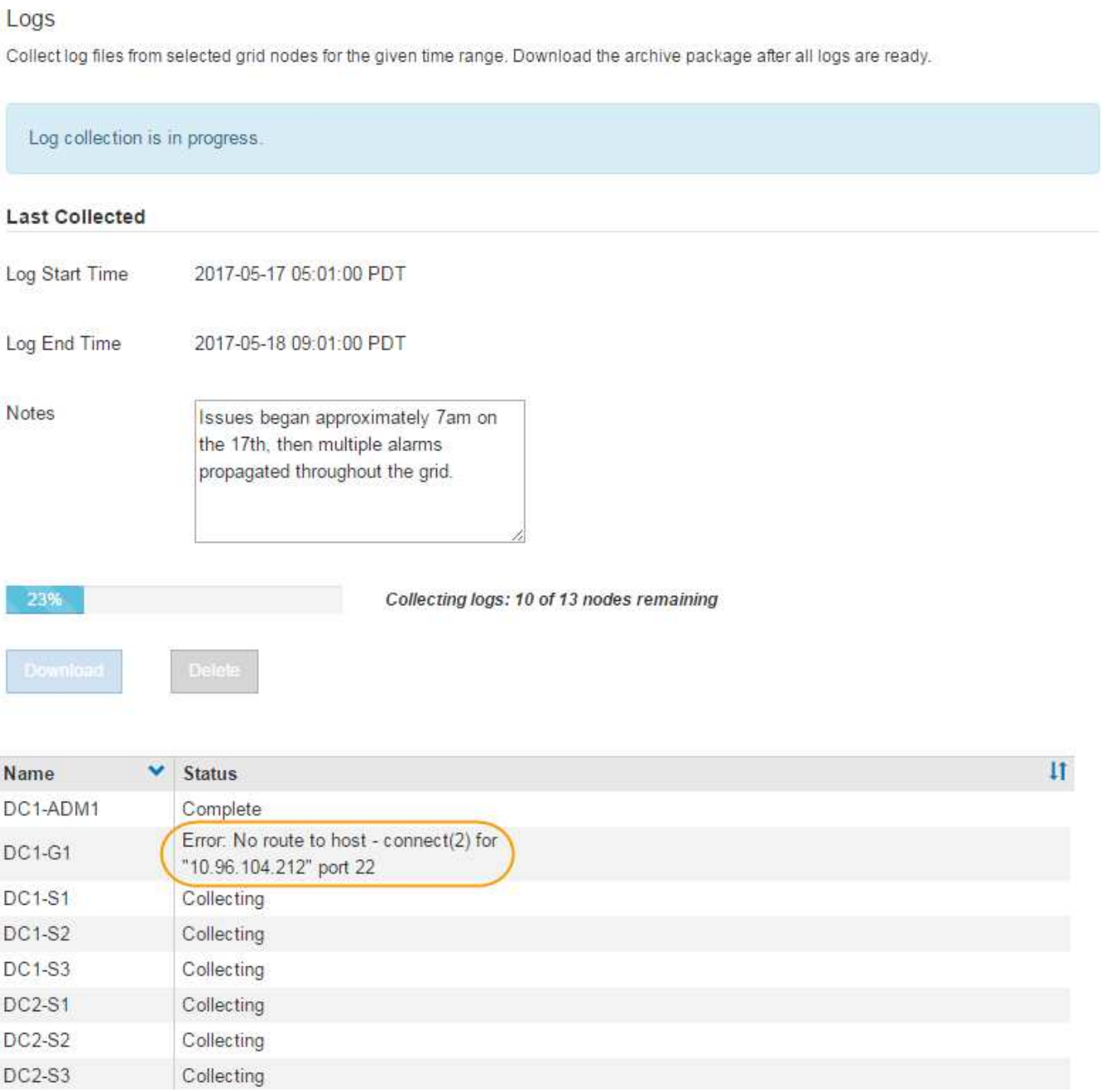
   Wenn Sie einen sehr langen Zeitraum auswählen oder Protokolle von allen Knoten in einem großen Raster sammeln, könnte das Protokollarchiv zu groß werden, um auf einem Knoten gespeichert zu werden, oder zu groß, um zum Download an den primären Admin-Knoten gesammelt zu werden. In diesem Fall müssen Sie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

4. Geben Sie optional Hinweise zu den Protokolldateien ein, die Sie im Textfeld **Hinweise** sammeln.

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

5. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
6. Klicken Sie Auf **Protokolle Sammeln**.

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



Auf der Seite „Protokolle“ können Sie den Fortschritt der Sammlung von Protokolldateien für jeden Grid-Knoten überwachen.

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

7. Klicken Sie auf **Download**, wenn die Sammlung der Protokolldatei abgeschlossen ist.

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

Nachdem Sie fertig sind

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

Optional können Sie auf **Löschen** klicken, um das Archiv-Paket der Protokolldatei zu entfernen und

Speicherplatz freizugeben. Das aktuelle Archivpaket für die Protokolldatei wird beim nächsten Erfassen von Protokolldateien automatisch entfernt.

Verwandte Informationen

"Referenz für Protokolldateien"

Manuelles Auslösen einer AutoSupport-Meldung

Um den technischen Support bei der Fehlerbehebung bei Problemen mit Ihrem StorageGRID System zu unterstützen, können Sie manuell eine AutoSupport Meldung auslösen, die gesendet werden soll.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **Support** > **Extras** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Wählen Sie **vom Benutzer ausgelöste AutoSupport senden** aus.

   StorageGRID versucht, eine AutoSupport Nachricht an den technischen Support zu senden. Wenn der Versuch erfolgreich ist, werden die **aktuellsten Ergebnisse** und **Letzte erfolgreiche Zeit** Werte auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, werden die **neuesten Ergebnisse**-Werte auf „Fehlgeschlagen“ aktualisiert, und StorageGRID versucht nicht, die AutoSupport-Nachricht erneut zu senden.

   > Nachdem Sie eine vom Benutzer ausgelöste AutoSupport-Nachricht gesendet haben, aktualisieren Sie die AutoSupport-Seite im Browser nach 1 Minute, um auf die neuesten Ergebnisse zuzugreifen.

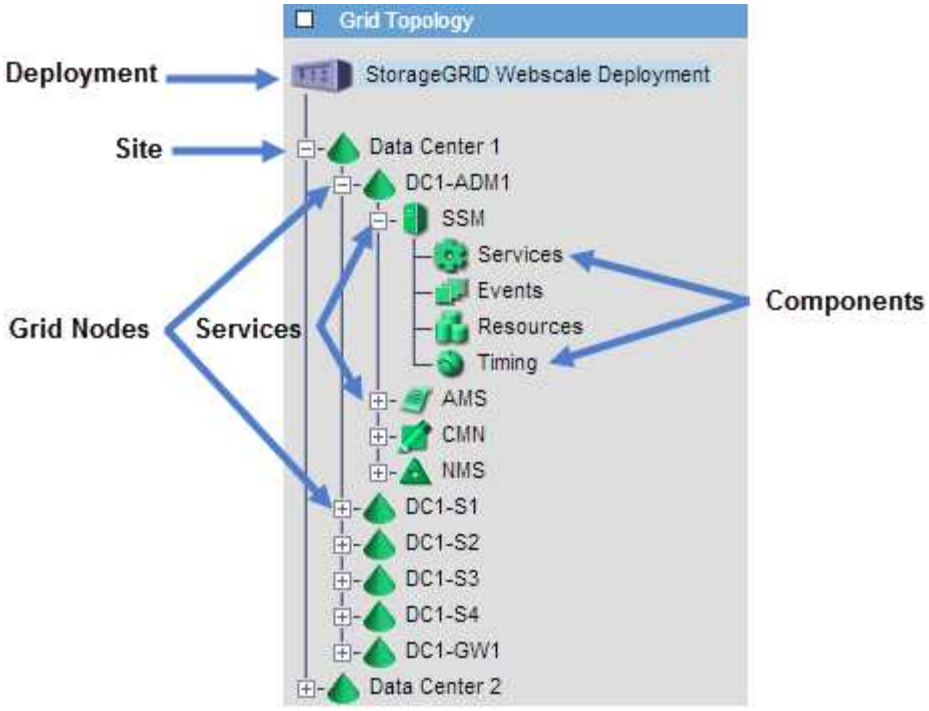
Verwandte Informationen

"Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"

Anzeigen der Struktur der Grid Topology

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

Um auf den Baum der Grid Topology zuzugreifen, wählen Sie **Support** > **Tools** > **Grid Topology**.



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

Überprüfen von Support-Metriken

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte Metriken und Diagramme für Ihr StorageGRID System prüfen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

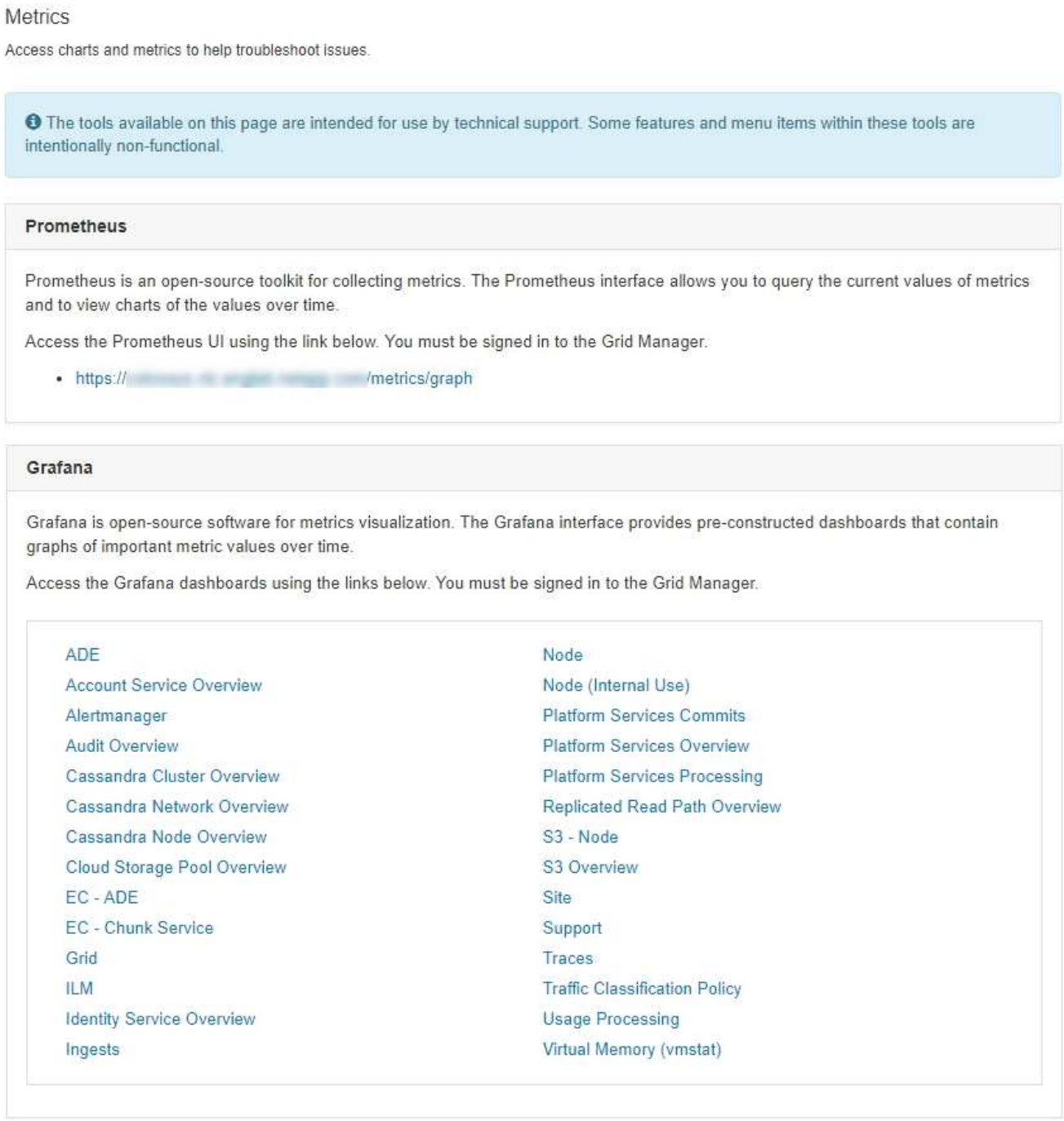
Auf der Seite Metriken können Sie auf die Benutzeroberflächen von Prometheus und Grafana zugreifen. Prometheus ist Open-Source-Software zum Sammeln von Kennzahlen. Grafana ist Open-Source-Software zur Visualisierung von Kennzahlen.

> ⓘ Die auf der Seite Metriken verfügbaren Tools sind für den technischen Support bestimmt. Einige Funktionen und Menüelemente in diesen Tools sind absichtlich nicht funktionsfähig und können sich ändern.

Schritte

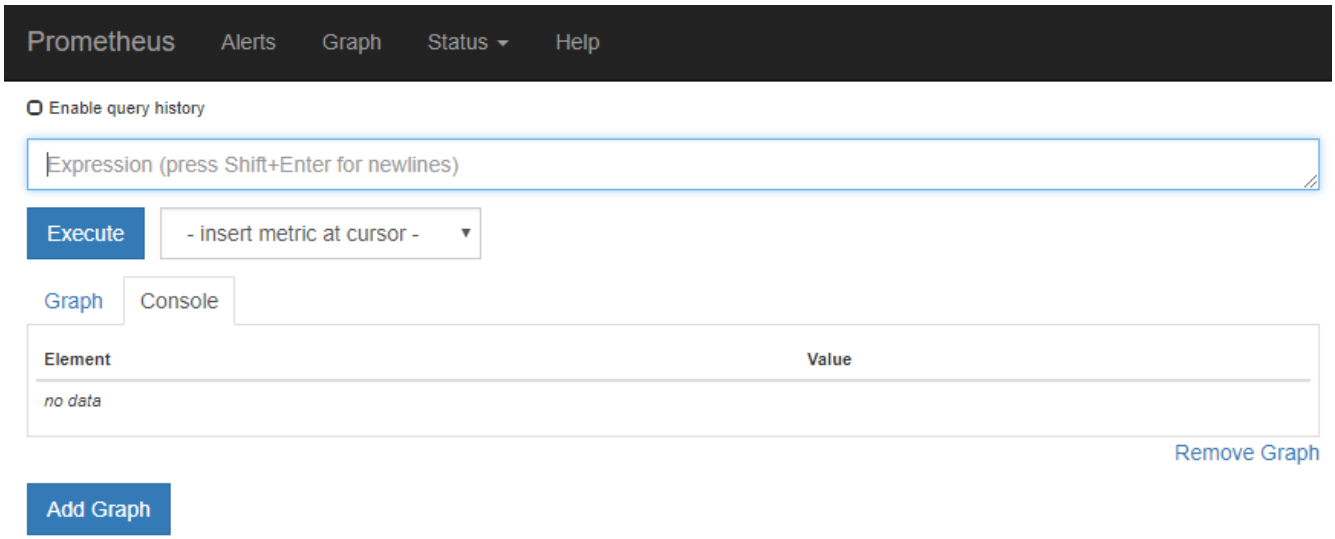
1. Wählen Sie nach Anweisung des technischen Supports **Support** > **Tools** > **Metriken**.

   Die Seite Metriken wird angezeigt.



2. Um die aktuellen Werte der StorageGRID-Metriken abzufragen und Diagramme der Werte im Zeitverlauf anzuzeigen, klicken Sie im Abschnitt Prometheus auf den Link.

   Das Prometheus-Interface wird angezeigt. Sie können über diese Schnittstelle Abfragen für die verfügbaren StorageGRID-Metriken ausführen und StorageGRID-Metriken im Laufe der Zeit grafisch darstellen.



Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

3. Um über einen längeren Zeitraum auf vorkonfigurierte Dashboards mit Diagrammen zu StorageGRID-Kennzahlen zuzugreifen, klicken Sie im Abschnitt „Grafana“ auf die Links.

   Die Grafana-Schnittstelle für den ausgewählten Link wird angezeigt.

Verwandte Informationen

"Häufig verwendete Prometheus-Kennzahlen"

Diagnose wird ausgeführt

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support eine Diagnose auf Ihrem StorageGRID-System durchführen und die Ergebnisse überprüfen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die Seite Diagnose führt eine Reihe von diagnostischen Prüfungen zum aktuellen Status des Rasters durch. Jede diagnostische Prüfung kann einen von drei Zuständen haben:

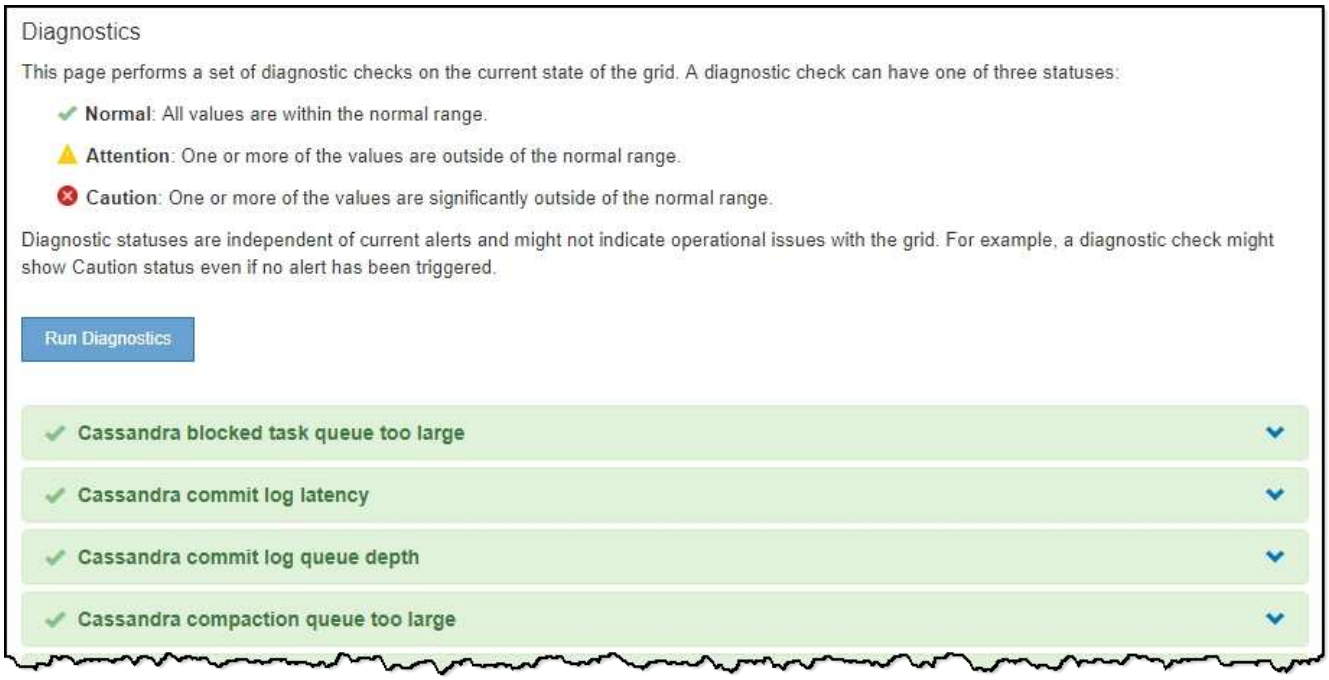
- **Normal**: Alle Werte liegen im Normalbereich.
- **Achtung**: Ein oder mehrere Werte liegen außerhalb des normalen Bereichs.
- **Achtung**: Ein oder mehrere der Werte liegen deutlich außerhalb des normalen Bereichs.

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

Schritte

1. Wählen Sie **Support** > **Tools** > **Diagnose**.

   Die Seite Diagnose wird angezeigt und zeigt die Ergebnisse für jede Diagnosetest an. Im Beispiel haben alle Diagnosen einen normalen Status.



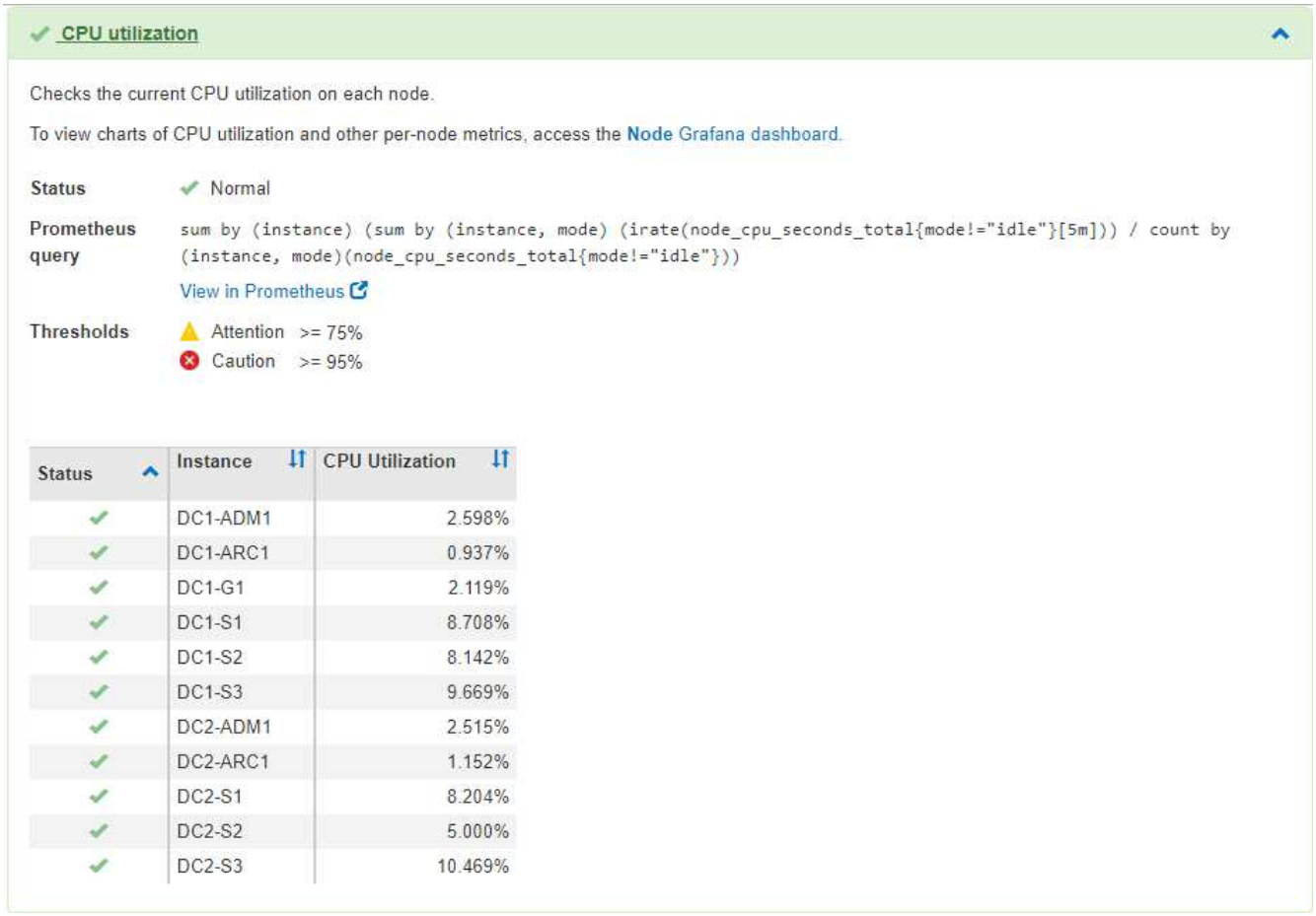
2. Wenn Sie mehr über eine bestimmte Diagnose erfahren möchten, klicken Sie auf eine beliebige Stelle in der Zeile.

   Details zur Diagnose und ihren aktuellen Ergebnissen werden angezeigt. Folgende Details sind aufgelistet:

   - **Status**: Der aktuelle Status dieser Diagnose: Normal, Achtung oder Achtung.
   - **Prometheus query**: Bei Verwendung für die Diagnose, der Prometheus Ausdruck, der verwendet wurde, um die Statuswerte zu generieren. (Ein Prometheus-Ausdruck wird nicht für alle Diagnosen verwendet.)
   - **Schwellenwerte**: Wenn für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden anormalen Diagnosestatus. (Schwellwerte werden nicht für alle Diagnosen verwendet.)

     Sie können diese Schwellenwerte nicht ändern.

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



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

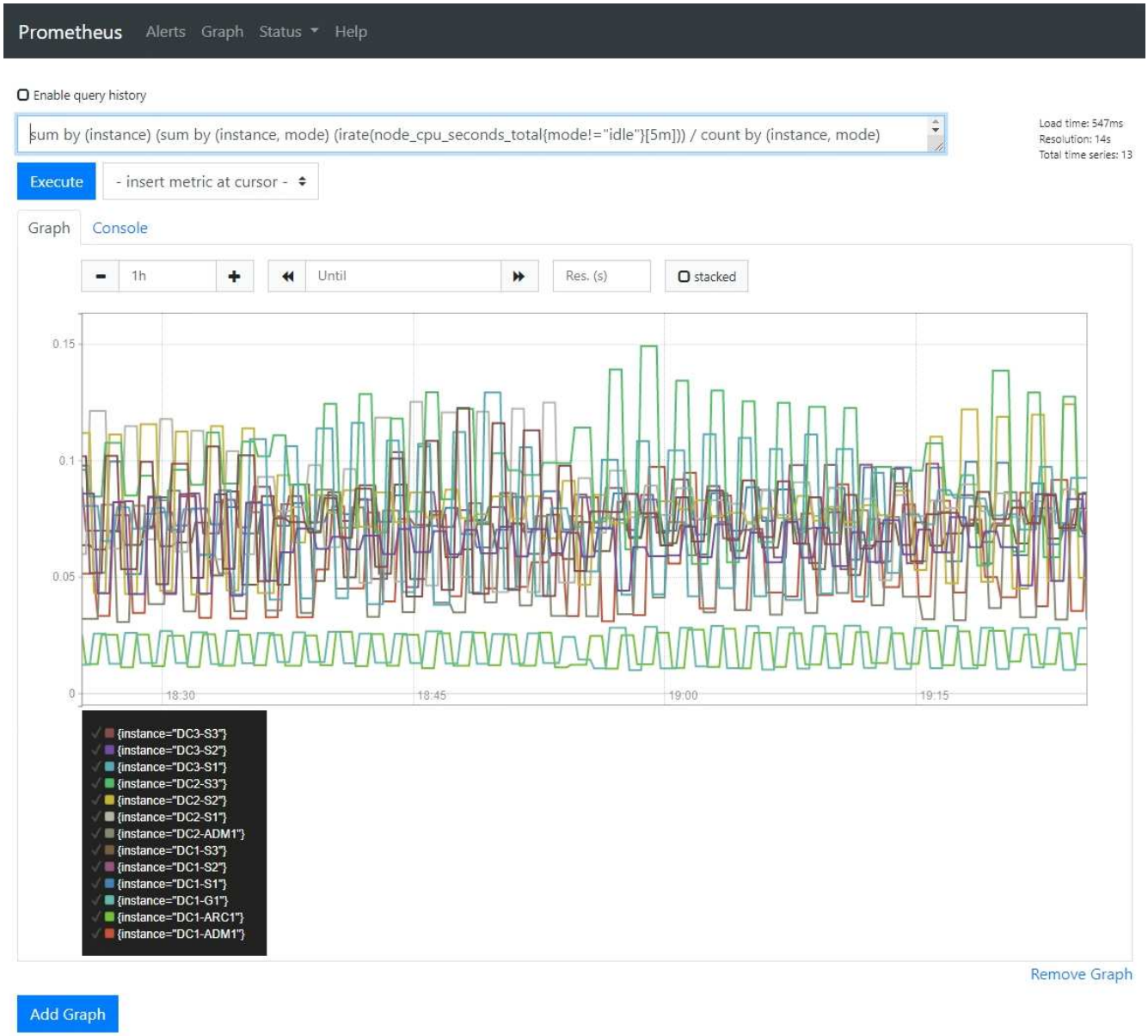
   Dieser Link wird nicht für alle Diagnosen angezeigt.

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

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

4. **Optional**: Um ein Diagramm des Prometheus-Ausdrucks über die Zeit zu sehen, klicken Sie auf **Anzeigen in Prometheus**.

   Es wird ein Prometheus-Diagramm des in der Diagnose verwendeten Ausdrucks angezeigt.



Verwandte Informationen

"Überprüfen von Support-Metriken"

"Häufig verwendete Prometheus-Kennzahlen"

Erstellen benutzerdefinierter Überwachungsanwendungen

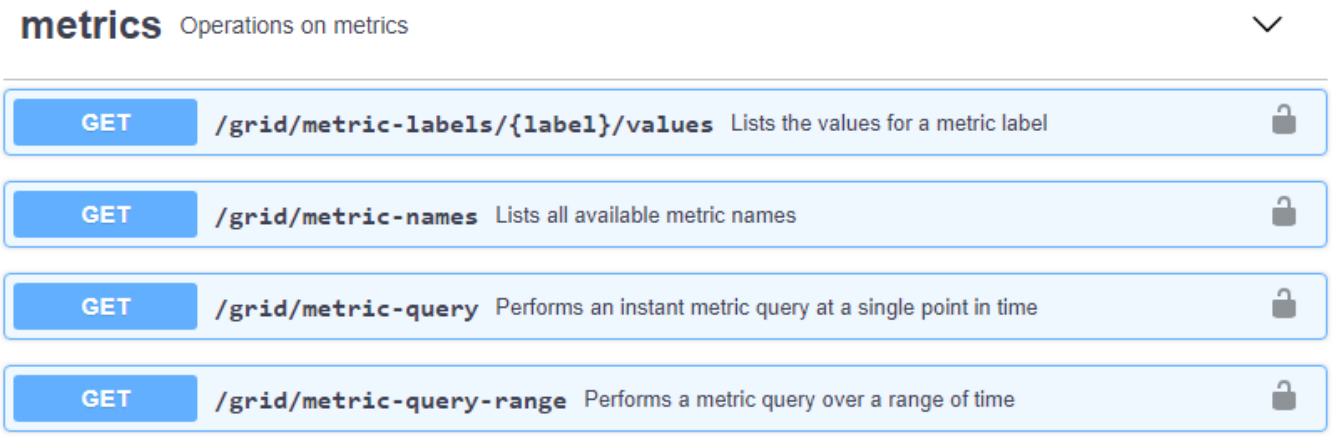
Mithilfe der StorageGRID-Kennzahlen der Grid-Management-API können Sie benutzerdefinierte Monitoring-Applikationen und Dashboards erstellen.

Wenn Sie Kennzahlen überwachen möchten, die nicht auf einer vorhandenen Seite des Grid Managers angezeigt werden, oder wenn Sie benutzerdefinierte Dashboards für StorageGRID erstellen möchten, können Sie mithilfe der Grid Management API die StorageGRID-Kennzahlen abfragen.

Über ein externes Monitoring-Tool wie Grafana können Sie auch direkt auf die Prometheus Metriken zugreifen. Zur Verwendung eines externen Tools müssen Sie ein Administrator-Clientzertifikat hochladen oder erstellen, damit StorageGRID das Tool für die Sicherheit authentifizieren kann. Lesen Sie die Anweisungen zum

Verwalten von StorageGRID.

Um die Vorgänge der Kennzahlen-API einschließlich der vollständigen Liste der verfügbaren Metriken anzuzeigen, gehen Sie zum Grid Manager und wählen Sie **Hilfe** > **API-Dokumentation** > **Metriken**.



Die Einzelheiten zur Implementierung einer benutzerdefinierten Überwachungsanwendung liegen über dem Umfang dieses Leitfadens hinaus.

Verwandte Informationen

"StorageGRID verwalten"

Alerts Referenz

In der folgenden Tabelle sind alle standardmäßigen StorageGRID-Warnmeldungen aufgeführt. Bei Bedarf können Sie benutzerdefinierte Alarmregeln erstellen, die Ihrem Systemmanagement entsprechen.

Hier finden Sie Informationen zu den häufig verwendeten Prometheus-Kennzahlen, um sich über die Metriken zu informieren, die in einigen dieser Warnmeldungen verwendet werden.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts abgelaufen	Der Akku im Speicher-Controller des Geräts ist abgelaufen. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts fehlgeschlagen	Der Akku im Speicher-Controller des Geräts ist ausgefallen. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Akku des Geräts weist nicht genügend Kapazität auf	Der Akku im Speicher-Controller des Geräts weist nicht genügend Kapazität auf. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Akku des Geräts befindet sich nahe dem Ablauf	Der Akku im Speicher-Controller des Geräts läuft langsam ab. 1. Setzen Sie die Batterie bald wieder ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts entfernt	Der Akku im Speicher-Controller des Geräts fehlt. 1. Setzen Sie eine Batterie ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Akku des Geräts ist zu heiß	Die Batterie im Speicher-Controller des Geräts ist überhitzt. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Mögliche Gründe für die Temperaturerhöhung wie Lüfter- oder HLK-Ausfall untersuchen. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Fehler bei der BMC-Kommunikation des Geräts	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren. 1. Vergewissern Sie sich, dass der BMC ordnungsgemäß funktioniert. Wählen Sie **Nodes**, und wählen Sie dann die Registerkarte **Hardware** für den Geräteknoten aus. Suchen Sie das BMC IP-Feld für den Compute Controller, und navigieren Sie zu dieser IP-Adresse. 2. Versuchen Sie, BMC-Kommunikation wiederherzustellen, indem Sie den Knoten in den Wartungsmodus versetzen und dann das Gerät aus- und wieder einschalten. Siehe Installations- und Wartungsanleitung für Ihr Gerät. ◦ "SG6000 Storage-Appliances" ◦ "SG100 SG1000 Services-Appliances" 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Fehler beim Sichern des Appliance-Cache	Ein persistentes Cache-Sicherungsgerät ist fehlgeschlagen. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.
Gerät-Cache-Backup-Gerät unzureichende Kapazität	Die Kapazität des Cache-Sicherungsgeräts ist nicht ausreichend. Wenden Sie sich an den technischen Support.
Appliance Cache Backup-Gerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt. Wenden Sie sich an den technischen Support.
Die Größe des Appliance-Cache-Speichers stimmt nicht überein	Die beiden Controller in der Appliance haben unterschiedliche Cache-Größen. Wenden Sie sich an den technischen Support.
Die Temperatur des Computing-Controller-Chassis des Geräts ist zu hoch	Die Temperatur des Computing-Controllers in einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten. 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Die CPU-Temperatur des Appliance-Compute-Controllers ist zu hoch	Die Temperatur der CPU im Computing-Controller einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten. 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"
Aufmerksamkeit für Compute-Controller ist erforderlich	Im Compute-Controller einer StorageGRID-Appliance wurde ein Hardwarefehler erkannt. 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Ein Problem besteht in der Stromversorgung Des Computercontrollers A des Geräts	Stromversorgung A im Compute-Controller weist ein Problem auf.Diese Warnmeldung weist möglicherweise darauf hin, dass das Netzteil ausgefallen ist oder dass es ein Problem bei der Stromversorgung hat. 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"
Das Netzteil B des Compute-Controllers ist ein Problem	Netzteil B im Compute-Controller weist ein Problem auf.Diese Warnmeldung weist möglicherweise darauf hin, dass das Netzteil ausgefallen ist oder dass es ein Problem bei der Stromversorgung hat. 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Der Service zur Überwachung der Computing-Hardware des Appliances ist ausgesetzt	Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt. 1. Überprüfen Sie den Status des eos-Systemstatusdienstes in der Basis-os. 2. Wenn sich der Dienst im Status „angehalten“ oder „Fehler“ befindet, starten Sie den Dienst neu. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Fibre-Channel-Fehler des Geräts erkannt	Es liegt ein Problem mit der Fibre Channel-Verbindung zwischen den Storage-Controllern und den Computing-Controllern in der Appliance vor. 1. Prüfen Sie die Hardwarekomponenten auf Fehler (**Nodes** > ***Appliance Node*** > **Hardware**). Wenn der Status einer der Komponenten nicht „`Nominal`“ lautet, führen Sie folgende Schritte aus: a. Stellen Sie sicher, dass die Fibre Channel-Kabel zwischen den Controllern vollständig verbunden sind. b. Stellen Sie sicher, dass die Fibre-Channel-Kabel frei von übermäßigen Kurven sind. c. Vergewissern Sie sich, dass die SFP+-Module richtig eingesetzt sind. **Hinweis:** Wenn dieses Problem weiterhin besteht, kann das StorageGRID-System die problematische Verbindung automatisch offline schalten. 1. Bei Bedarf die Komponenten austauschen. Siehe Installations- und Wartungsanleitung für Ihr Gerät.
Fehler des Fibre-Channel-HBA-Ports des Geräts	Ein Fibre Channel-HBA-Port ist ausgefallen oder ist ausgefallen.Kontaktieren Sie den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Appliance Flash Cache Laufwerke sind nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal. 1. Ersetzen Sie die SSD-Cache-Laufwerke. Siehe Installations- und Wartungsanleitung für das Gerät. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Geräteverbindung/Batteriebehälter entfernt	Der Verbindungs-/Batteriebehälter fehlt. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in der Anleitung zum Austauschen eines Speichercontrollers in der Installations- und Wartungsanleitung des Geräts enthalten. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Geräte-LACP-Port fehlt	Ein Port auf einer StorageGRID-Appliance beteiligt sich nicht an der LACP-Verbindung. 1. Überprüfen Sie die Konfiguration für den Switch. Stellen Sie sicher, dass die Schnittstelle in der richtigen Link-Aggregationsgruppe konfiguriert ist. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Das gesamte Netzteil des Geräts ist heruntergestuft	Die Leistung eines StorageGRID-Geräts ist von der empfohlenen Betriebsspannung abweichen. 1. Überprüfen Sie den Status von Netzteil A und B, um festzustellen, welches Netzteil ungewöhnlich funktioniert, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "SG100 SG1000 Services-Appliances"
Ausfall des Appliance Storage Controller A	Der Speicher-Controller A in einer StorageGRID-Appliance ist ausgefallen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Fehler beim Speicher-Controller B des Geräts	Bei Speicher-Controller B in einer StorageGRID-Appliance ist ein Fehler aufgetreten. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Laufwerksausfall des Appliance-Storage-Controllers	Mindestens ein Laufwerk in einer StorageGRID-Appliance ist ausgefallen oder nicht optimal. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Hardwareproblem des Appliance Storage Controllers	SANtricity meldet, dass für eine Komponente einer StorageGRID Appliance ein Hinweis erforderlich ist. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Ausfall der Stromversorgung des Speicher-Controllers	Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abweichen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Fehler bei Netzteil B des Speicher-Controllers	Stromversorgung B bei einem StorageGRID-Gerät hat von der empfohlenen Betriebsspannung abweichen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Monitordienst der Appliance-Storage-Hardware ist ausgesetzt	Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt. 1. Überprüfen Sie den Status des eos-Systemstatusdienstes in der Basis-os. 2. Wenn sich der Dienst im Status „angehalten“ oder „Fehler“ befindet, starten Sie den Dienst neu. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Appliance Storage-Shelfs ist beeinträchtigt	Der Status einer der Komponenten im Storage Shelf für eine Storage Appliance ist beeinträchtigt. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware entnehmen Sie bitte den folgenden Hinweisen: ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"
Gerätetemperatur überschritten	Die nominale oder maximale Temperatur für den Lagercontroller des Geräts wurde überschritten. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Mögliche Gründe für die Temperaturerhöhung wie Lüfter- oder HLK-Ausfall untersuchen. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Temperatursensor des Geräts entfernt	Ein Temperatursensor wurde entfernt. Wenden Sie sich an den technischen Support.
Cassandra Auto-Kompaktor-Fehler	Der Cassandra-Autocompfaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank für Überschreibungen und das Löschen schwerer Workloads. Diese Bedingung bleibt bestehen, aber bei bestimmten Workloads kommt es zu einem unerwartet hohen Metadatenverbrauch. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Auto-Kompaktor-Kennzahlen veraltet	Die Kennzahlen, die den Cassandra Auto-Kompaktor beschreiben, sind veraltet. Der Cassandra Auto-Kompaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank bei Überschreibungen und Löten schwerer Workloads. Während diese Warnung weiterhin angezeigt wird, kommt es bei bestimmten Workloads zu einem unerwartet hohen Metadatenverbrauch. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.
Cassandra Kommunikationsfehler	Die Knoten, auf denen der Cassandra-Service ausgeführt wird, haben Probleme bei der Kommunikation miteinander.Diese Warnung zeigt an, dass etwas die Kommunikation zwischen Knoten beeinträchtigt. Möglicherweise gibt es ein Netzwerkproblem, oder der Cassandra-Service ist auf einem oder mehreren Storage-Nodes nicht verfügbar. 1. Bestimmen Sie, ob ein anderer Alarm einen oder mehrere Speicherknoten betrifft. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Prüfen Sie, ob ein Netzwerkproblem einen oder mehrere Speicherknoten betreffen könnte. 3. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 4. Wählen Sie für jeden Speicherknoten in Ihrem System **SSM** > **Services** aus. Stellen Sie sicher, dass der Status des Cassandra-Service“` läuft.`“ 5. Wenn Cassandra nicht ausgeführt wird, befolgen Sie die Schritte zum Starten oder Neustarten eines Dienstes in den Recovery- und Wartungsanweisungen. 6. Wenn jetzt alle Instanzen des Cassandra-Service ausgeführt werden und die Warnmeldung nicht behoben wurde, wenden Sie sich an den technischen Support. "Verwalten Sie erholen"

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra-Kompensation überlastet	Der Cassandra-Verdichtungsvorgang ist überlastet.Wenn der Verdichtungsvorgang überlastet ist, kann die Lese-Performance beeinträchtigt und der RAM-Speicher möglicherweise aufgebraucht werden. Auch der Cassandra-Service reagiert möglicherweise nicht oder stürzt ab. 1. Starten Sie den Cassandra-Service neu, indem Sie die Schritte zum Neustart eines Service in den Recovery- und Wartungsanweisungen befolgen. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. "Verwalten Sie erholen"
Veraltete Reparaturkennzahlen für Cassandra	Die Kennzahlen, die Cassandra-Reparaturaufträge beschreiben, sind veraltet. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Booten Sie den Node neu. Gehen Sie im Grid Manager zu **Nodes**, wählen Sie den Knoten und wählen Sie die Registerkarte Aufgaben aus. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Cassandra Reparaturfortschritt langsam	Der Fortschritt der Cassandra-Reparaturen ist langsam.bei langsamen Datenbankreparaturen wird die Datenkonsistenz von Cassandra behindert. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Vergewissern Sie sich, dass alle Speicherknoten online sind und keine netzwerkbezogenen Warnmeldungen vorliegen. 2. Überwachen Sie diese Warnung bis zu zwei Tage lang, um zu prüfen, ob das Problem selbst behoben wird. 3. Wenn die Reparatur der Datenbank langsam fortgesetzt wird, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Reparaturservice nicht verfügbar	Der Cassandra-Reparaturservice ist nicht verfügbar.der Cassandra-Reparaturservice ist auf allen Speicherknoten vorhanden und bietet wichtige Reparaturfunktionen für die Cassandra-Datenbank. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 2. Wählen Sie für jeden Speicherknoten in Ihrem System **SSM** > **Services** aus. Stellen Sie sicher, dass der Status des Cassandra Reaper Service „läuft“. 3. Wenn Cassandra Reaper nicht ausgeführt wird, befolgen Sie die Schritte zum Starten oder Neustarten eines Dienstes in den Anweisungen zur Wiederherstellung und Wartung. 4. Wenn jetzt alle Instanzen des Cassandra Reaper Service ausgeführt werden und die Warnmeldung nicht behoben ist, wenden Sie sich an den technischen Support. "Verwalten Sie erholen"
Verbindungsfehler beim Cloud-Storage-Pool	Bei der Zustandsprüfung für Cloud-Storage-Pools wurde ein oder mehrere neue Fehler erkannt. 1. Wechseln Sie auf der Seite „Speicherpools“ zum Abschnitt „Cloud-Speicherpools“. 2. Sehen Sie sich die Spalte Letzter Fehler an, um zu ermitteln, welcher Cloud Storage Pool einen Fehler hat. 3. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management. "Objektmanagement mit ILM"

Alarmname	Beschreibung und empfohlene Aktionen
DHCP-Leasing abgelaufen	Das DHCP-Leasing auf einer Netzwerkschnittstelle ist abgelaufen.Falls das DHCP-Leasing abgelaufen ist, befolgen Sie die empfohlenen Aktionen: 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. "Verwalten Sie erholen"
DHCP-Leasing läuft bald ab	Der DHCP-Lease auf einer Netzwerkschnittstelle läuft bald ab.um zu verhindern, dass der DHCP-Leasing abläuft, befolgen Sie die empfohlenen Maßnahmen: 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. "Verwalten Sie erholen"

Alarmname	Beschreibung und empfohlene Aktionen
DHCP-Server nicht verfügbar	Der DHCP-Server ist nicht verfügbar.der StorageGRID-Node kann den DHCP-Server nicht kontaktieren. Das DHCP-Leasing für die IP-Adresse des Node kann nicht validiert werden. 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. "Verwalten Sie erholen"

Alarmname	Beschreibung und empfohlene Aktionen
Die Festplatten-I/O ist sehr langsam	Sehr langsamer Festplatten-I/O könnte sich auf die StorageGRID-Performance auswirken. 1. Wenn das Problem mit einem Storage Appliance-Node zusammenhängt, überprüfen Sie mithilfe von SANtricity System Manager auf fehlerhafte Laufwerke, Laufwerke mit prognostizierte Fehler oder laufende Festplattenreparaturen. Überprüfen Sie auch den Status der Fibre Channel- oder SAS-Links zwischen den Computing-Ressourcen und den Storage Controllern der Appliance, um zu überprüfen, ob Links ausgefallen sind oder übermäßige Fehlerraten angezeigt werden. 2. Überprüfen Sie das Storage-System, das die Volumes dieses Nodes hostet, um die Ursache des langsamen I/O zu ermitteln und zu korrigieren 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. Betroffene Nodes können Services deaktivieren und sich neu starten, um keine Auswirkungen auf die allgemeine Grid-Performance zu haben. Wenn der zugrunde liegende Zustand beseitigt ist und diese Nodes eine normale I/O-Performance erkennen, wird der gesamte Service automatisch wiederhergestellt.

Alarmname	Beschreibung und empfohlene Aktionen
E-Mail-Benachrichtigung fehlgeschlagen	Die E-Mail-Benachrichtigung für einen Alarm konnte nicht gesendet werden.dieser Alarm wird ausgelöst, wenn eine Benachrichtigung per E-Mail fehlschlägt oder eine Test-E-Mail (gesendet von der Seite **Alerts** > **Email Setup**) nicht zugestellt werden kann. 1. Melden Sie sich über den Admin-Node in der Spalte **Standort/Node** der Warnmeldung bei Grid Manager an. 2. Rufen Sie die Seite **Alerts** > **E-Mail-Setup** auf, überprüfen Sie die Einstellungen und ändern Sie diese, falls erforderlich. 3. Klicken Sie auf **Test-E-Mail senden** und prüfen Sie den Posteingang eines Testempfängers für die E-Mail. Eine neue Instanz dieser Warnmeldung kann ausgelöst werden, wenn die Test-E-Mail nicht gesendet werden kann. 4. Wenn die Test-E-Mail nicht gesendet werden konnte, bestätigen Sie, dass Ihr E-Mail-Server online ist. 5. Wenn der Server funktioniert, wählen Sie **Support** > **Tools** > **Protokolle** aus, und sammeln Sie das Protokoll für den Admin-Knoten. Geben Sie einen Zeitraum an, der 15 Minuten vor und nach der Zeit der Warnmeldung liegt. 6. Extrahieren Sie das heruntergeladene Archiv und überprüfen Sie den Inhalt von `prometheus.log (_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log)`. 7. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.
Ablauf der auf der Seite Client Certificates konfigurierten Zertifikate	Ein oder mehrere Zertifikate, die auf der Seite Clientzertifikate konfiguriert sind, laufen bald ab. 1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Client-Zertifikate**. 2. Wählen Sie ein Zertifikat aus, das bald abläuft. 3. Wählen Sie **Bearbeiten** aus, um ein neues Zertifikat hochzuladen oder zu erstellen. 4. Wiederholen Sie diese Schritte für jedes Zertifikat, das bald abläuft. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
Ablauf des Endpunktzertifikats des Load Balancer	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen kurz vor dem Ablauf. 1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Balancer-Endpunkte Laden**. 2. Wählen Sie einen Endpunkt mit einem Zertifikat aus, das bald abläuft. 3. Wählen Sie **Endpunkt bearbeiten** aus, um ein neues Zertifikat hochzuladen oder zu erstellen. 4. Wiederholen Sie diese Schritte für jeden Endpunkt mit einem abgelaufenen Zertifikat oder einem Endpunkt, der bald ausläuft. Weitere Informationen zum Verwalten von Endpunkten für den Load Balancer finden Sie in den Anweisungen zum Verwalten von StorageGRID. "StorageGRID verwalten"
Ablauf des Serverzertifikats für die Managementoberfläche	Das für die Managementoberfläche verwendete Serverzertifikat läuft bald ab. 1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**. 2. Laden Sie im Abschnitt Management Interface Server Certificate ein neues Zertifikat hoch. "StorageGRID verwalten"
Ablauf des Serverzertifikats für Storage-API-Endpunkte	Das Serverzertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, läuft bald ab. 1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**. 2. Laden Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte ein neues Zertifikat hoch. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
MTU-Diskrepanz bei dem Grid-Netzwerk	Die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) unterscheidet sich deutlich von den Knoten im Grid.die Unterschiede in den MTU-Einstellungen könnten darauf hindeuten, dass einige, aber nicht alle, eth0-Netzwerke für Jumbo-Frames konfiguriert sind. Eine MTU-Größe von mehr als 1000 kann zu Problemen mit der Netzwerkleistung führen. "Fehlerbehebung bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU"
Hohe Java-Heap-Nutzung	Ein hoher Prozentsatz von Java Heap-Speicherplatz wird verwendet.Wenn der Java-Heap voll wird, können Metadaten-Dienste nicht mehr verfügbar sein und Clientanforderungen können fehlschlagen. 1. Überprüfen Sie die ILM-Aktivitäten auf dem Dashboard. Diese Warnmeldung kann sich selbst beheben, wenn der ILM-Workload abnimmt. 2. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Hohe Latenz bei Metadatenanfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.ein Anstieg der Abfragelatenz kann durch eine Hardwareänderung, wie den Austausch einer Festplatte oder eine Workload-Änderung, wie eine plötzliche Zunahme der Ingests, verursacht werden. 1. Ermitteln, ob sich Hardware- oder Workload-Änderungen während der Erhöhung der Abfragelatenz ergeben. 2. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Synchronisierungsfehler bei der Identitätsföderation	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren. 1. Vergewissern Sie sich, dass der konfigurierte LDAP-Server online und verfügbar ist. 2. Überprüfen Sie die Einstellungen auf der Seite Identity Federation. Vergewissern Sie sich, dass alle Werte aktuell sind. Siehe „`Konfigurieren einer föderierten Identitätsquelle`“ in den Anweisungen zur Verwaltung von StorageGRID. 3. Klicken Sie auf **Verbindung testen**, um die Einstellungen für den LDAP-Server zu validieren. 4. Wenden Sie sich an den technischen Support, wenn das Problem nicht gelöst werden kann. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
ILM-Platzierung nicht erreichbar	Eine Platzierungsanweisung in einer ILM-Regel kann für bestimmte Objekte nicht erreicht werden.Diese Warnung zeigt an, dass ein von einer Platzierungsanweisung erforderlicher Node nicht verfügbar ist oder dass eine ILM-Regel falsch konfiguriert ist. Eine Regel kann beispielsweise mehr replizierte Kopien angeben, als Storage Nodes vorhanden sind. 1. Stellen Sie sicher, dass alle Nodes online sind. 2. Wenn alle Nodes online sind, lesen Sie die Anweisungen zur Platzierung in allen ILM-Regeln, die die aktive ILM-Richtlinie verwenden. Vergewissern Sie sich, dass für alle Objekte gültige Anweisungen vorliegen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management. 3. Aktualisieren Sie bei Bedarf die Regeleinstellungen und aktivieren Sie eine neue Richtlinie. ⓘ Es kann bis zu 1 Tag dauern, bis die Warnung gelöscht wird. 4. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. ⓘ Diese Warnmeldung wird möglicherweise während eines Upgrades angezeigt und kann einen Tag nach Abschluss des Upgrades bestehen. Wenn diese Warnung durch ein Upgrade ausgelöst wird, wird sie von selbst gelöscht. "Objektmanagement mit ILM"

Alarmname	Beschreibung und empfohlene Aktionen
Der ILM-Scan ist zu lang	Die Zeit zum Scannen, Bewerten von Objekten und Anwenden von ILM ist zu lang.Wenn die geschätzte Zeit für die Durchführung eines kompletten ILM-Scans aller Objekte zu lang ist (siehe **Scan Period - Estimated** auf dem Dashboard), wird die aktive ILM-Richtlinie möglicherweise nicht auf neu aufgenommene Objekte angewendet. Änderungen der ILM-Richtlinie werden möglicherweise nicht auf vorhandene Objekte angewendet. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Vergewissern Sie sich, dass alle Speicherknoten online sind. 3. Verringern Sie vorübergehend den Client-Traffic. Wählen Sie beispielsweise im Grid Manager die Option **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung** aus, und erstellen Sie eine Richtlinie, die die Bandbreite oder die Anzahl der Anforderungen begrenzt. 4. Wenn Festplatten-I/O oder -CPU überlastet sind, versuchen Sie, die Last zu reduzieren oder die Ressource zu erhöhen. 5. Aktualisieren Sie ggf. ILM-Regeln für die Verwendung der synchronen Platzierung (Standard für Regeln, die nach StorageGRID 11.3 erstellt wurden). 6. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
ILM-Scan-Rate niedrig	Die ILM-Scan-Rate ist auf weniger als 100 Objekte/Sekunde eingestellt.Diese Warnmeldung gibt an, dass jemand die ILM-Scan-Rate für Ihr System auf weniger als 100 Objekte/Sekunde geändert hat (Standard: 400 Objekte/Sekunde). Die aktive ILM-Richtlinie wird möglicherweise nicht auf neu aufgenommene Objekte angewendet. Nachfolgende Änderungen der ILM-Richtlinie werden nicht auf vorhandene Objekte angewendet. 1. Ermitteln, ob im Rahmen einer laufenden Support-Untersuchung eine temporäre Änderung der ILM-Scanrate vorgenommen wurde. 2. Wenden Sie sich an den technischen Support. Ändern Sie nie die ILM-Scanrate, ohne den technischen Support zu kontaktieren.
ABLAUF DES KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des KMS-Zertifikats (Key Management Server) verwendet wird, läuft bald ab. 1. Aktualisieren Sie mithilfe der KMS-Software das CA-Zertifikat für den Schlüsselverwaltungsserver. 2. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 3. Wählen Sie den KMS aus, der über eine Warnung für den Zertifikatsstatus verfügt. 4. Wählen Sie **Bearbeiten**. 5. Wählen Sie **Weiter** aus, um zu Schritt 2 zu wechseln (Serverzertifikat hochladen). 6. Wählen Sie **Durchsuchen**, um das neue Zertifikat hochzuladen. 7. Wählen Sie **Speichern**. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
ABLAUF DES KMS-Clientzertifikats	Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft bald ab. 1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 2. Wählen Sie den KMS aus, der über eine Warnung für den Zertifikatsstatus verfügt. 3. Wählen Sie **Bearbeiten**. 4. Wählen Sie **Weiter** aus, um zu Schritt 3 zu wechseln (Client-Zertifikate hochladen). 5. Wählen Sie **Durchsuchen**, um das neue Zertifikat hochzuladen. 6. Wählen Sie **Durchsuchen**, um den neuen privaten Schlüssel hochzuladen. 7. Wählen Sie **Speichern**. "StorageGRID verwalten"
KMS-Konfiguration konnte nicht geladen werden	Es ist die Konfiguration für den Verschlüsselungsmanagement-Server vorhanden, konnte aber nicht geladen werden. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
KMS-Verbindungsfehler	Ein Appliance-Node konnte keine Verbindung zum Schlüsselmanagementserver für seinen Standort herstellen. 1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 2. Vergewissern Sie sich, dass die Port- und Hostnamen-Einträge korrekt sind. 3. Vergewissern Sie sich, dass das Serverzertifikat, das Clientzertifikat und der private Schlüssel des Clientzertifikats korrekt und nicht abgelaufen sind. 4. Stellen Sie sicher, dass Firewall-Einstellungen es dem Appliance-Knoten ermöglichen, mit dem angegebenen KMS zu kommunizieren. 5. Beheben Sie alle Netzwerk- oder DNS-Probleme. 6. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt. 1. Vergewissern Sie sich, dass der dem Standort zugewiesene KMS den korrekten Namen für den Verschlüsselungsschlüssel und alle vorherigen Versionen verwendet. 2. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen	Alle Appliance-Volumes wurden entschlüsselt, aber ein oder mehrere Volumes konnten nicht auf den neuesten Schlüssel rotieren.Kontaktieren Sie den technischen Support.
KM ist nicht konfiguriert	Für diesen Standort ist kein Schlüsselverwaltungsserver vorhanden. 1. Wählen Sie im Grid Manager die Option **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** aus. 2. Fügen Sie für diese Site einen KMS hinzu oder fügen Sie einen Standard-KMS hinzu. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	Ein oder mehrere Volumes auf einer Appliance mit aktivierter Node-Verschlüsselung konnten nicht mit dem aktuellen KMS-Schlüssel entschlüsselt werden. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Stellen Sie sicher, dass auf dem Verschlüsselungsmanagement-Server (KMS) der konfigurierte Verschlüsselungsschlüssel und alle vorherigen Schlüsselversionen vorhanden sind. 3. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
Ablauf DES KMS-Serverzertifikats	Das vom KMS (Key Management Server) verwendete Serverzertifikat läuft in Kürze ab. 1. Aktualisieren Sie mithilfe der KMS-Software das Serverzertifikat für den Schlüsselverwaltungsserver. 2. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
Große Audit-Warteschlange	Die Datenträgerwarteschlange für Überwachungsmeldungen ist voll. 1. Prüfen Sie die Last auf dem System. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen und Sie können die Warnung ignorieren. 2. Wenn die Meldung weiterhin angezeigt wird und der Schweregrad erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. 3. Verringern Sie die Betriebsrate des Clients oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie das Audit-Level für Client-Schreibvorgänge ändern und der Client auf Fehler oder aus liest (**Konfiguration** > **Überwachung** > **Audit**). "Prüfung von Audit-Protokollen"
Geringe Kapazität der Auditprotokoll-Festplatte	Der für Audit-Protokolle verfügbare Platz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedriger verfügbarer Node-Speicher	Die RAM-Menge, die auf einem Knoten verfügbar ist, ist gering.der niedrige verfügbare RAM kann auf eine Änderung der Arbeitslast oder eine Speicherlecks bei einem oder mehreren Knoten hinweisen. 1. Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. 2. Wenn der verfügbare Speicher unter den Hauptwarnschwellenwert fällt, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Wenig freier Speicherplatz für den Speicherpool	Der Speicherplatz, der zur Speicherung von Objektdaten in einem Speicherpool verfügbar ist, ist gering. 1. Wählen Sie **ILM** > **Storage Pools** aus. 2. Wählen Sie den Speicherpool aus, der in der Warnmeldung aufgeführt ist, und wählen Sie **Details anzeigen**. 3. Ermitteln, wo zusätzliche Storage-Kapazität erforderlich ist Sie können entweder jedem Standort im Speicherpool Storage-Nodes hinzufügen oder einem oder mehreren vorhandenen Storage-Nodes Storage-Volumes (LUNs) hinzufügen. 4. Führen Sie ein Erweiterungsverfahren durch, um die Speicherkapazität zu erhöhen. "Erweitern Sie Ihr Raster"
Wenig installierter Node-Speicher	Der installierte Speicher auf einem Knoten ist gering.Erhöhen Sie die RAM-Menge, die für die virtuelle Maschine oder den Linux-Host verfügbar ist. Überprüfen Sie den Schwellenwert für die Hauptwarnung, um die standardmäßige Mindestanforderung für einen StorageGRID-Node zu bestimmen. Die Installationsanweisungen für Ihre Plattform finden Sie unter: • "Installieren Sie Red hat Enterprise Linux oder CentOS" • "Installieren Sie Ubuntu oder Debian" • "VMware installieren"

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger Metadaten-Storage	Der für die Speicherung von Objektmetadaten verfügbare Platz ist niedrig.**kritischer Alarm** 1. Die Aufnahme von Objekten beenden. 2. Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. **Großalarm** Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. • Kleine Warnung* 1. Überwachen Sie die Rate, mit der Objekt-Metadatenspeicherplatz verwendet wird. Wählen Sie **Nodes** > ***Storage Node*** > **Storage** aus, und zeigen Sie das Diagramm verwendete Speicherdaten - Objektmetadaten an. 2. Fügen Sie Speicherknoten in einem Erweiterungsverfahren So bald wie möglich hinzu. Sobald neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht. "Fehlerbehebung für Storage-Warnmeldungen bei niedrigen Metadaten" "Erweitern Sie Ihr Raster"
Niedrige Kenngrößen für die Festplattenkapazität	Der für die Kennzahlendatenbank verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger Objekt-Storage	Der zur Speicherung von Objektdaten verfügbare Speicherplatz ist gering.Durchführung einer Erweiterung. Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen. "Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“" "Erweitern Sie Ihr Raster"
Niedrige Root-Festplattenkapazität	Der für die Root-Festplatte verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedrige Datenkapazität des Systems	Der verfügbare Speicherplatz für StorageGRID-Systemdaten im /var/local-Dateisystem ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Fehler bei der Node-Netzwerkverbindung	Beim Übertragen der Daten zwischen nodes.Network Verbindungsfehlern sind Fehler aufgetreten, die sich ohne manuelles Eingreifen beheben lassen. Wenden Sie sich an den technischen Support, wenn die Fehler nicht behoben sind. "Fehlerbehebung bei dem NRER-Alarm (Network Receive Error)"

Alarmname	Beschreibung und empfohlene Aktionen
Node-Netzwerkannahme-Frame-Fehler	Bei einem hohen Prozentsatz der von einem Node empfangenen Netzwerkframes sind Fehler aufgetreten.Diese Warnmeldung weist möglicherweise auf ein Hardwareproblem hin, z. B. ein schlechtes Kabel oder ein ausgefallener Transceiver an beiden Enden der Ethernet-Verbindung. 1. Wenn Sie eine Appliance verwenden, versuchen Sie, jeden SFP+ oder SFP28 Transceiver und jedes Kabel nacheinander auszutauschen, um zu prüfen, ob die Warnmeldung gelöscht wird. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Node ist nicht mit dem NTP-Server synchronisiert	Die Zeit des Node ist nicht mit dem NTP-Server (Network Time Protocol) synchronisiert. 1. Vergewissern Sie sich, dass Sie mindestens vier externe NTP-Server angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern. 2. Überprüfen Sie, ob alle NTP-Server normal funktionieren. 3. Überprüfen Sie die Verbindungen zu den NTP-Servern. Stellen Sie sicher, dass sie nicht durch eine Firewall blockiert sind.
Der Node ist nicht mit dem NTP-Server gesperrt	Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt. 1. Vergewissern Sie sich, dass Sie mindestens vier externe NTP-Server angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern. 2. Überprüfen Sie, ob alle NTP-Server normal funktionieren. 3. Überprüfen Sie die Verbindungen zu den NTP-Servern. Stellen Sie sicher, dass sie nicht durch eine Firewall blockiert sind.
Netzwerk außerhalb des Appliance-Node ist ausgefallen	Mindestens ein Netzwerkgerät ist ausgefallen oder nicht verbunden. Diese Warnung zeigt an, dass eine Netzwerkschnittstelle (eth) für einen Knoten, der auf einer virtuellen Maschine oder einem Linux-Host installiert ist, nicht zugänglich ist. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Objekte verloren	Ein oder mehrere Objekte sind aus dem Raster verloren gegangen.Diese Warnung kann darauf hindeuten, dass die Daten dauerhaft verloren gegangen sind und nicht wieder abgerufen werden können. 1. Untersuchen Sie diesen Alarm sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. Sie können auch ein verlorenes Objekt wiederherstellen, wenn Sie eine prompte Aktion ausführen. "Fehlerbehebung verloren gegangene und fehlende Objektdaten" 2. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück: a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. b. Wählen Sie ***site*** > ***Grid Node*** > **LDR** > **Data Store** > **Konfiguration** > **Main** für den Speicherknoten, der die Warnung erhöht hat. c. Wählen Sie **Anzahl der verlorenen Objekte zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
Plattform-Services nicht verfügbar	Zu wenige Speicherknoten mit dem RSM-Dienst laufen oder sind an einem Standort verfügbar.Stellen Sie sicher, dass die meisten Speicherknoten, die den RSM-Dienst am betroffenen Standort haben, ausgeführt werden und in einem nicht fehlerfreien Zustand sind. Siehe „`Fehlerbehebung bei Plattformdiensten`“ in den Anweisungen für die Administration von StorageGRID. "StorageGRID verwalten"

Alarmname	Beschreibung und empfohlene Aktionen
Services-Appliance-Verbindung am Admin-Netzwerkanschluss 1 getrennt	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie das Kabel und die physische Verbindung zum Admin-Netzwerkanschluss 1. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG100 SG1000 Services-Appliances" ◦ "Deaktivieren einer Meldungsregel"
Services-Appliance-Link im Admin-Netzwerk (oder Client-Netzwerk) herunter	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG100 SG1000 Services-Appliances" ◦ "Deaktivieren einer Meldungsregel"

Alarmname	Beschreibung und empfohlene Aktionen
Services-Appliance-Verbindung an Netzwerkport 1, 2, 3 oder 4 getrennt	Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG100 SG1000 Services-Appliances" ◦ "Deaktivieren einer Meldungsregel"
Die Speicherkonnektivität der Services-Appliance ist herabgesetzt	Einer der beiden SSDs in einer Services-Appliance ist ausgefallen oder die Synchronisierung mit der anderen Appliance-Funktion ist nicht beeinträchtigt. Sie sollten das Problem jedoch sofort beheben. Wenn beide Laufwerke ausfallen, funktioniert die Appliance nicht mehr. 1. Wählen Sie im Grid Manager die Option **Nodes** > ***Services Appliance*, und wählen Sie dann die Registerkarte Hardware** aus. 2. Überprüfen Sie die Meldung im Feld * Storage RAID Mode*. 3. Wenn die Meldung den Status eines Neusynchronisierung anzeigt, warten Sie, bis der Vorgang abgeschlossen ist, und bestätigen Sie dann, dass die Warnmeldung behoben wurde. Eine Neusynchronisierung bedeutet, dass SSD kürzlich ersetzt oder aus einem anderen Grund erneut synchronisiert wird. 4. Wenn die Meldung angibt, dass eine der SSDs ausgefallen ist, ersetzen Sie das ausgefallene Laufwerk so bald wie möglich. Anweisungen zum Austauschen eines Laufwerks in einer Services Appliance finden Sie im Installations- und Wartungshandbuch für SG100- und SG1000-Geräte. "SG100 SG1000 Services-Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Verknüpfung der Speicher-Appliance auf Admin-Netzwerk-Port 1 ausgefallen	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie das Kabel und die physische Verbindung zum Admin-Netzwerkanschluss 1. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "Deaktivieren einer Meldungsregel"
Link der Storage Appliance ist im Admin-Netzwerk (oder Client-Netzwerk) inaktiv.	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "Deaktivieren einer Meldungsregel"

Alarmname	Beschreibung und empfohlene Aktionen
Verbindung der Storage Appliance über Netzwerkport 1, 2, 3 oder 4 getrennt	Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager die Option **Alarme** > **Warnregeln** aus, wählen Sie die Regel aus und klicken Sie auf **Regel bearbeiten**. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances" ◦ "Deaktivieren einer Meldungsregel"
Die Storage-Konnektivität der Storage-Appliance ist herabgesetzt	Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller. 1. Gehen Sie zum Gerät, um die Port-Kontrollleuchten zu überprüfen. 2. Wenn die LEDs eines Ports nicht leuchten, überprüfen Sie, ob das Kabel ordnungsgemäß angeschlossen ist. Ersetzen Sie bei Bedarf das Kabel. 3. Warten Sie bis zu fünf Minuten. Wenn ein zweites Kabel ausgetauscht werden muss, ziehen Sie den Stecker mindestens 5 Minuten lang nicht ab. Andernfalls kann das Root-Volume schreibgeschützt sein und die Hardware neu starten. 4. Wählen Sie im Grid Manager die Option **Nodes** aus. Wählen Sie dann die Registerkarte Hardware des Node aus, auf dem das Problem aufgetreten ist. Vergewissern Sie sich, dass die Alarmbedingung behoben ist.

Alarmname	Beschreibung und empfohlene Aktionen
Speichergerät nicht zugänglich	Auf ein Speichergerät kann nicht zugegriffen werden.Diese Warnung zeigt an, dass ein Volume nicht gemountet oder auf ein Problem mit einem zugrunde liegenden Speichergerät zugegriffen werden kann. 1. Überprüfen Sie den Status aller für den Knoten verwendeten Speichergeräte: ◦ Wenn der Knoten auf einer virtuellen Maschine oder einem Linux-Host installiert ist, befolgen Sie die Anweisungen für Ihr Betriebssystem, um die Hardware-Diagnose auszuführen oder eine Dateisystemprüfung durchzuführen. ▪ "Installieren Sie Red hat Enterprise Linux oder CentOS" ▪ "Installieren Sie Ubuntu oder Debian" ▪ "VMware installieren" ◦ Wenn der Node auf einer SG100-, SG1000- oder SG6000-Appliance installiert ist, verwenden Sie den BMC. ◦ Wenn der Node auf einer SG5600 oder SG5700 Appliance installiert ist, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. ◦ "SG6000 Storage-Appliances" ◦ "SG5700 Storage-Appliances" ◦ "SG5600 Storage Appliances"

Alarmname	Beschreibung und empfohlene Aktionen
Hohe Kontingentnutzung für Mandanten	Ein hoher Prozentsatz des Kontingentspeichers wird verwendet. Wenn ein Mieter seine Quote überschreitet, werden Neuanlässe abgelehnt. Diese Warnungsregel ist standardmäßig deaktiviert, da sie eine Vielzahl von Benachrichtigungen erzeugen kann. 1. Wählen Sie im Grid Manager die Option **Miters** aus. 2. Sortieren Sie die Tabelle nach **Quotenausnutzung**. 3. Wählen Sie einen Mandanten aus, dessen Quotenauslastung fast 100 % beträgt. 4. Führen Sie einen oder beide der folgenden Schritte aus: ◦ Wählen Sie **Bearbeiten**, um das Speicherkontingent für den Mieter zu erhöhen. ◦ Benachrichtigen Sie den Mandanten, dass seine Kontingentauslastung hoch ist.

Alarmname	Beschreibung und empfohlene Aktionen
Kommunikation mit Knoten nicht möglich	Ein oder mehrere Dienste reagieren nicht, oder der Node kann nicht erreicht werden.Diese Warnmeldung gibt an, dass ein Node aus einem unbekannten Grund getrennt ist. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren. Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. Wenn das Problem weiterhin besteht: 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Vergewissern Sie sich, dass alle Dienste auf diesem Knoten ausgeführt werden. Wenn ein Dienst angehalten wird, versuchen Sie, ihn zu starten. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung. 3. Stellen Sie sicher, dass der Host für den Node eingeschaltet ist. Falls nicht, starten Sie den Host. Wenn mehr als ein Host ausgeschaltet ist, lesen Sie die Recovery- und Wartungsanweisungen. 4. Bestimmen Sie, ob zwischen diesem Knoten und dem Admin-Node ein Problem mit der Netzwerkverbindung besteht. 5. Wenn Sie die Meldung nicht beheben können, wenden Sie sich an den technischen Support. "Verwalten Sie erholen"
Unerwarteter Node-Neustart	Ein Node wurde in den letzten 24 Stunden unerwartet neu gebootet. 1. Überwachen Sie diesen Alarm. Der Alarm wird nach 24 Stunden gelöscht. Wenn der Node jedoch unerwartet neu gebootet wird, wird die Warnmeldung erneut ausgelöst. 2. Wenn Sie die Meldung nicht beheben können, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Nicht identifizierte beschädigte Objekte erkannt	Im replizierten Objekt-Storage wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte. 1. Ermitteln Sie, ob Probleme mit dem zugrunde liegenden Speicher auf einem Speicherknoten auftreten. Führen Sie beispielsweise die Hardwarediagnose aus oder führen Sie eine Dateisystemprüfung durch. 2. Führen Sie nach der Behebung von Storage-Problemen die Vordergrundüberprüfung aus, um festzustellen, ob Objekte fehlen und wenn möglich ersetzt werden. 3. Überwachen Sie diesen Alarm. Die Warnmeldung wird nach 24 Stunden gelöscht, wird jedoch erneut ausgelöst, wenn das Problem noch nicht behoben wurde. 4. Wenn Sie die Meldung nicht beheben können, wenden Sie sich an den technischen Support. "Vordergrundüberprüfung wird ausgeführt"

Verwandte Informationen

"Häufig verwendete Prometheus-Kennzahlen"

Häufig verwendete Prometheus-Kennzahlen

Der Prometheus-Service auf Admin-Knoten sammelt Zeitreihungskennzahlen aus den Diensten auf allen Knoten. Während Prometheus mehr als tausend Kennzahlen erfasst, sind zur Überwachung der wichtigsten StorageGRID Vorgänge eine relativ kleine Zahl erforderlich.

In der folgenden Tabelle sind die am häufigsten verwendeten Prometheus-Kennzahlen aufgeführt und eine Zuordnung jeder Metrik zu dem entsprechenden Attribut (im Alarmsystem verwendet).

Sie können diese Liste nutzen, um die Bedingungen in den Standardwarnregeln besser zu verstehen oder die Bedingungen für benutzerdefinierte Alarmregeln zu erstellen. Für eine vollständige Liste der Metriken wählen Sie **Hilfe** > **API-Dokumentation**.

Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

Die Prometheus Kennzahlen werden 31 Tage lang aufbewahrt.

Prometheus metrisch	Beschreibung
Alertmanager_notifications_failed_total	Die Gesamtzahl der fehlgeschlagenen Warnmeldungen.
Node_Filesystem_verfügbare_Byte	Die Menge an Dateisystemspeicherplatz, die nicht-Root-Benutzern in Bytes zur Verfügung steht.
Node_Memory_MemAvailable_Bytes	Feld Speicherinformationen MemAvailable_Bytes.
Node_Network_Carrier	Transportwert von /sys/class/net/<iface>.
Node_Network_receive_errs_total	Statistik für Netzwerkgeräte receive_errs.
Node_Network_transmit_errs_total	Statistik für Netzwerkgeräte transmit_errs.
storagegrid_administrativ_down	Der Node ist aus einem erwarteten Grund nicht mit dem Grid verbunden. Beispielsweise wurde der Node oder die Services für den Node ordnungsgemäß heruntergefahren, der Node neu gebootet oder die Software wird aktualisiert.
storagegrid_Appliance_Compute_Controller_Hardware_Status	Der Status der Computing-Controller-Hardware in einer Appliance.
storagegrid_Appliance_failed_Disks	Für den Storage-Controller in einer Appliance die Anzahl der Laufwerke, die nicht optimal sind.
storagegrid_Appliance_Storage_Controller_Hardware_Status	Der Gesamtstatus der Hardware eines Storage Controllers in einer Appliance.
storagegrid_Content_Buckets_und_Containern	Die Gesamtzahl der S3-Buckets und Swift-Container, die von diesem Storage-Node bekannt sind
storagegrid_Content_Objects	Die Gesamtzahl der von diesem Storage-Node bekannten S3 und Swift Datenobjekte. Die Anzahl ist nur für Datenobjekte gültig, die von Client-Applikationen erstellt werden, die über S3 oder Swift mit dem System interface.
storagegrid_Content_Objects_Lost	Gesamtzahl der vom StorageGRID System erkannten Objekte, die von diesem Service als fehlend erkannt werden. Es sollten Maßnahmen ergriffen werden, um die Ursache des Schadens zu ermitteln und ob eine Erholung möglich ist. "Fehlerbehebung verloren gegangene und fehlende Objektdaten"

Prometheus metrisch	Beschreibung
storagegrid_http_Sessions_Incoming_versuchte	Die Gesamtzahl der HTTP-Sitzungen, die zu einem Speicherknoten versucht wurden.
storagegrid_http_Sessions_Incoming_derzeit_etablier tes	Die Anzahl der derzeit aktiven HTTP-Sitzungen (offen) auf dem Speicherknoten.
storagegrid_http_Sessions_INCOMING_FAILED	Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen wurden, entweder aufgrund einer fehlerhaften HTTP-Anfrage oder aufgrund eines Fehlers bei der Verarbeitung eines Vorgangs.
storagegrid_http_Sessions_Incoming_successful	Die Gesamtzahl der erfolgreich abgeschlossenen HTTP-Sitzungen.
storagegrid_ilm_awaiting_background_Objects	Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus dem Scan warten
storagegrid_ilm_awaiting_Client_Evaluation_Objects_ per_Second	Die aktuelle Rate, mit der Objekte im Vergleich zur ILM-Richtlinie auf diesem Node bewertet werden.
storagegrid_ilm_awaiting_Client_Objects	Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus den Client-Vorgängen (z. B. Aufnahme) warten
storagegrid_ilm_awaiting_total_Objects	Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten
storagegrid_ilm_Scan_Objects_per_Second	Die Geschwindigkeit, mit der Objekte des Node gescannt und für ILM in der Warteschlange gestellt werden.
storagegrid_ilm_Scan_Period_Geschätzter_Minuten	Die geschätzte Zeit zum Abschließen eines vollständigen ILM-Scans auf diesem Node. **Hinweis:** Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die sich im Besitz dieses Knotens befinden.
storagegrid_Load_Balancer_Endpoint_cert_expiry_ti me	Die Ablaufzeit des Endpunktzertifikats des Load Balancer in Sekunden seit der Epoche.
storagegrid_Metadatenabfragen_average_Latency_M illisekunden	Die durchschnittliche Zeit, die zum Ausführen einer Abfrage des Metadatenspeichers über diesen Service benötigt wird.

Prometheus metrisch	Beschreibung
storagegrid_Network_received_Byte	Die Gesamtmenge der seit der Installation empfangenen Daten.
storagegrid_Network_transmited_Byte	Die Gesamtmenge der seit der Installation gesendeten Daten.
storagegrid_ntp_Chooed_time_source_Offset_Millisekunden	Systematischer Zeitversatz, der von einer ausgewählten Zeitquelle bereitgestellt wird. Offset wird eingeführt, wenn die Verzögerung zum Erreichen einer Zeitquelle nicht der Zeit entspricht, die für das Erreichen des NTP-Clients benötigt wird.
storagegrid_ntp_gesperrt	Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt.
storagegrid_s3_Data_Transfers_Bytes_aufgenommen	Die Gesamtmenge an Daten, die seit dem letzten Zurücksetzen des Attributs von S3-Clients auf diesen Storage-Node aufgenommen wurden.
storagegrid_s3_Data_Transfers_Bytes_abgerufen	Die Gesamtanzahl der Daten, die von S3-Clients von diesem Speicherknoten seit dem letzten Zurücksetzen des Attributs abgerufen wurden.
storagegrid_s3_Operations_fehlgeschlagen	Die Gesamtzahl der fehlgeschlagenen S3-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen solche, die durch S3-Autorisierungsfehler verursacht wurden.
storagegrid_s3_Operations_erfolgreich	Die Gesamtzahl der erfolgreichen S3-Vorgänge (HTTP-Statuscode 2xx).
storagegrid_s3_Operations_nicht autorisiert	Die Gesamtzahl der fehlerhaften S3-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind.
storagegrid_Servercertifikat_Management_Interface_cert_expiry_days	Die Anzahl der Tage vor Ablauf des Managementschnittstelle-Zertifikats.
storagegrid_Serverzertifikat_Storage_API_endpunkte s_cert_expiry_days	Die Anzahl der Tage, bevor das Objekt-Speicher-API-Zertifikat abläuft.
storagegrid_Service_cpu_Sekunden	Der kumulierte Zeitaufwand, die die CPU seit der Installation bei diesem Service verwendet hat.
storagegrid_Service_Load	Der Prozentsatz der verfügbaren CPU-Zeit, die derzeit von diesem Service genutzt wird. Gibt an, wie beschäftigt der Dienst ist. Die verfügbare CPU-Zeit hängt von der Anzahl der CPUs für den Server ab.

Prometheus metrisch	Beschreibung
storagegrid_Service_Memory_Usage_Byte	Die Speichermenge (RAM), die derzeit von diesem Dienst verwendet wird. Dieser Wert ist identisch mit dem, der vom Linux-Top-Dienstprogramm als RES angezeigt wird.
storagegrid_Service_Network_received_Byte	Die Gesamtanzahl der Daten, die seit der Installation von diesem Service eingehen.
storagegrid_Service_Network_transmited_Byte	Die Gesamtanzahl der von diesem Service gesendeten Daten.
storagegrid_Service_startet neu	Die Gesamtanzahl der Neustarts des Dienstes.
storagegrid_Service_Runtime_seconds	Die Gesamtzeit, die der Service seit der Installation ausgeführt hat.
storagegrid_Service_Uptime_Sekunden	Die Gesamtzeit, die der Dienst seit dem letzten Neustart ausgeführt hat.
storagegrid_Storage_State_current	Der aktuelle Status der Storage-Services. Attributwerte sind: • 10 = Offline • 15 = Wartung • 20 = schreibgeschützt • 30 = Online
storagegrid_Storage_Status	Der aktuelle Status der Storage-Services. Attributwerte sind: • 0 = Keine Fehler • 10 = In Transition • 20 = Nicht Genügend Freier Speicherplatz • 30 = Volume(s) nicht verfügbar • 40 = Fehler
storagegrid_Storage_Utifficiendatiy_Metadata_Bytes	Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten auf dem Storage-Node

Prometheus metrisch	Beschreibung
storagegrid_Storage_Utiffici“_Metadata_allowed_Bytes	Der gesamte Speicherplatz auf Volume 0 jedes Storage-Node, der für Objekt-Metadaten zulässig ist. Dieser Wert ist immer kleiner als der tatsächlich für Metadaten auf einem Node reservierte Speicherplatz, da für grundlegende Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades ein Teil des reservierten Speicherplatzes benötigt wird. Der zulässige Speicherplatz für Objektmetadaten steuert die allgemeine Objektkapazität.
storagegrid_Storage_Utifficiendatiy_Metadata_Bytes	Die Menge der Objekt-Metadaten auf dem Storage-Volume 0 in Bytes.
storagegrid_Storage_Utisation_Metadata_reservierte_Bytes	Der gesamte Speicherplatz auf Volume 0 jedes Storage-Node, der tatsächlich für Objekt-Metadaten reserviert ist. Für jeden angegebenen Storage-Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Node und der Einstellung des systemweiten reservierten Speicherplatzes ab.
storagegrid_Storage_Utifficienfficienals_total_space_Bytes	Der gesamte Speicherplatz, der allen Objektspeichern zugewiesen ist.
storagegrid_Storage_Utiable_space_Bytes	Die verbleibende Menge an Objekt-Storage. Berechnet durch Hinzufügen der verfügbaren Menge an Speicherplatz für alle Objektspeichern auf dem Storage-Node.
storagegrid_Swift_Data_Transfers_Bytes_aufgenommen	Die Gesamtmenge der Daten, die Swift-Clients seit dem letzten Zurücksetzen des Attributs von diesem Storage-Node aufgenommen haben.
storagegrid_Swift_Data_Transfers_Bytes_abgerufen	Die Gesamtanzahl der Daten, die Swift-Clients von diesem Speicherknoten seit dem letzten Zurücksetzen des Attributs abgerufen haben.
storagegrid_Swift_Operations_fehlgeschlagen	Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen solche, die durch Swift-Autorisierungsfehler verursacht wurden.
storagegrid_Swift_Operations_erfolgreich	Die Gesamtzahl der erfolgreichen Swift-Vorgänge (HTTP-Statuscode 2xx).

Prometheus metrisch	Beschreibung
storagegrid_Swift_Operations_nicht autorisiert	Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind (HTTP-Statuscodes 401, 403, 405).
storagegrid_Tenant_Usage_Data_Byte	Die logische Größe aller Objekte für den Mandanten.
storagegrid_Tenant_Usage_object_count	Die Anzahl der Objekte für den Mandanten.
storagegrid_Tenant_Usage_quota_bytes	Die maximale Menge an logischem Speicherplatz, die für die Objekte des Mandanten verfügbar ist Wenn keine Quota-Metrik angegeben wird, steht eine unbegrenzte Menge an Speicherplatz zur Verfügung.

Alarmreferenz (Altsystem)

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

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

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

Codieren	Name	Service	Empfohlene Maßnahmen
ACMS	Verfügbare Metadaten	BARC, BLDR, BCMN	Ein Alarm wird ausgelöst, wenn ein LDR- oder ARC-Dienst die Verbindung zu einem DDS-Dienst verliert. In diesem Fall können Transaktionen nicht verarbeitet werden. Wenn die Nichtverfügbarkeit von DDS-Diensten nur ein kurzes vorübergehendes Problem ist, können Transaktionen verzögert werden. Überprüfen und Wiederherstellen der Verbindungen zu einem DDS-Dienst, um diesen Alarm zu löschen und den Service auf die volle Funktionalität zurückzugeben.

Codieren	Name	Service	Empfohlene Maßnahmen
AKTE	Status Des Cloud Tiering Service	LICHTBOGEN	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Cloud Tiering - Simple Storage Service (S3). Wenn das ATTRIBUT ACTS für den Archiv-Node auf Read-Only aktiviert oder Read-Write deaktiviert ist, müssen Sie das Attribut auf Read-Write aktiviert setzen. Wenn ein Hauptalarm aufgrund eines Authentifizierungsfehlers ausgelöst wird, überprüfen Sie ggf. die mit dem Ziel-Bucket verknüpften Anmeldeinformationen und aktualisieren Sie Werte. Wenn aus irgendeinem anderen Grund ein Großalarm ausgelöst wird, wenden Sie sich an den technischen Support.
ADCA	ADC-Status	ADU	Wenn ein Alarm ausgelöst wird, wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***GRID Node*** > **ADC** > **Übersicht** > **Main** und **ADC** > **Alarme** > **Main**, um die Ursache des Alarms zu bestimmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ADCE	ADC-Status	ADU	Wenn der Wert des ADC-Status Standby lautet, setzen Sie die Überwachung des Dienstes fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert des ADC-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AITE	Status Abrufen	BARC	Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert für „Abruffzustand“ auf „Ziel“ wartet, prüfen Sie den TSM Middleware-Server und stellen Sie sicher, dass er ordnungsgemäß funktioniert. Wenn der Archivknoten gerade zum StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass die Verbindung des Archiv-Knotens zum angestrebten externen Archiv-Speichersystem korrekt konfiguriert ist. Wenn der Wert des Status „Archivabrueve“ Offline lautet, versuchen Sie, den Status auf Online zu aktualisieren. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abruf** > **Konfiguration** > **Main**, wählen Sie **Archiv Status abrufen** > **Online** und klicken Sie auf **Änderungen anwenden**. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AITU	Status Abrufen	BARC	Wenn der Wert für „Status abrufen“ als Zielfehler gilt, prüfen Sie das ausgewählte externe Archivspeichersystem auf Fehler. Wenn der Wert des Status „Archivabrueve“ auf „Sitzung verloren“ lautet, prüfen Sie das ausgewählte externe Archivspeichersystem, um sicherzustellen, dass es online ist und ordnungsgemäß funktioniert. Überprüfen Sie die Netzwerkverbindung mit dem Ziel. Wenn der Wert des Status „Archiv abrufen“ Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.
ALIS	Eingehende Attributsitzungen	ADU	Wenn die Anzahl der eingehenden Attributsitzungen in einem Attributrelais zu groß wird, kann dies ein Hinweis sein, dass das StorageGRID-System unausgewogen geworden ist. Unter normalen Bedingungen sollten Attributsitzungen gleichmäßig auf ADC-Dienste verteilt werden. Ein Ungleichgewicht kann zu Performance-Problemen führen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ALOS	Ausgehende Attributsitzungen	ADU	Der ADC-Dienst verfügt über eine hohe Anzahl von Attributsitzungen und wird überlastet. Wenn dieser Alarm ausgelöst wird, wenden Sie sich an den technischen Support.
ALUR	Nicht Erreichbare Attributdatenbanken	ADU	Überprüfen Sie die Netzwerkverbindung mit dem NMS-Service, um sicherzustellen, dass der Dienst das Attribut-Repository kontaktieren kann. Wenn dieser Alarm ausgelöst wird und die Netzwerkverbindung gut ist, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AMQS	Audit-Nachrichten In Queued	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Meldungen nicht sofort an ein Audit-Relais oder ein Repository weitergeleitet werden können, werden die Meldungen in einer Disk-Warteschlange gespeichert. Wenn die Warteschlange voll wird, können Ausfälle auftreten. Um Ihnen die Möglichkeit zu geben, rechtzeitig zu reagieren, um einen Ausfall zu verhindern, werden AMQS-Alarme ausgelöst, wenn die Anzahl der Meldungen in der Datenträgerwarteschlange die folgenden Schwellenwerte erreicht: • Hinweis: Mehr als 100,000 Nachrichten • Minor: Mindestens 500,000 Nachrichten • Major: Mindestens 2,000,000 Nachrichten • Kritisch: Mindestens 5,000,000 Nachrichten Wenn ein AMQS-Alarm ausgelöst wird, überprüfen Sie die Belastung des Systems. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen. In diesem Fall können Sie den Alarm ignorieren. Wenn der Alarm weiterhin besteht und der Schweregrad erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-

Codieren	Name	Service	Empfohlene Maßnahmen
AOTE	Store State	BARC	Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Speicherstatus auf Ziel wartet, prüfen Sie das externe Archivspeichersystem und stellen Sie sicher, dass es ordnungsgemäß funktioniert. Wenn der Archivknoten gerade zum StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass die Verbindung des Archiv-Knotens zum angestrebten externen Archiv-Speichersystem korrekt konfiguriert ist. Wenn der Wert des Store State Offline lautet, prüfen Sie den Wert des Store Status. Beheben Sie alle Probleme, bevor Sie den Store-Status wieder auf Online verschieben.
AOTU	Speicherstatus	BARC	Wenn der Wert des Speicherstatus „Sitzung verloren“ lautet, prüfen Sie, ob das externe Archivspeichersystem verbunden und online ist. Wenn der Wert von Zielfehler ist, überprüfen Sie das externe Archivspeichersystem auf Fehler. Wenn der Wert des Speicherstatus Unbekannter Fehler lautet, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
APMS	Storage Multipath-Konnektivität	SSM	Wenn der Alarm für den Multipath-Status als „`Dabgestuft`“ angezeigt wird (wählen Sie **Unterstützung** > **Tools** > **Grid-Topologie**, und wählen Sie dann ***site*** > ***Grid-Knoten*** > **SSM** > **Ereignisse**), gehen Sie folgendermaßen vor: 1. Schließen Sie das Kabel an, das keine Kontrollleuchten anzeigt, oder ersetzen Sie es. 2. Warten Sie eine bis fünf Minuten. Ziehen Sie das andere Kabel erst fünf Minuten nach dem Anschließen des ersten Kabels ab. Das zu frühe Auflösen kann dazu führen, dass das Root-Volume schreibgeschützt ist, was erfordert, dass die Hardware neu gestartet wird. 3. Kehren Sie zur Seite **SSM** > **Ressourcen** zurück, und überprüfen Sie, ob der Multipath-Status im Abschnitt Speicherhardware in „ `DNominal`` “ geändert wurde.

Codieren	Name	Service	Empfohlene Maßnahmen
ARCE	BOGENZUSTAND	LICHTBOGEN	Der ARC-Dienst verfügt über einen Standby-Status, bis alle ARC-Komponenten (Replikation, Speicher, Abrufen, Ziel) gestartet wurden. Dann geht es zu Online. Wenn der Wert des ARC-Status nicht von Standby auf Online übergeht, überprüfen Sie den Status der ARC-Komponenten. Wenn der Wert für ARC-Status Offline lautet, starten Sie den Service neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AROQ	Objekte In Queued	LICHTBOGEN	Dieser Alarm kann ausgelöst werden, wenn das Wechselspeichergerät aufgrund von Problemen mit dem angestrebten externen Archivspeichersystem langsam läuft oder wenn mehrere Lesefehler auftreten. Überprüfen Sie das externe Archiv-Storage-System auf Fehler und stellen Sie sicher, dass es ordnungsgemäß funktioniert. In manchen Fällen kann dieser Fehler auf eine hohe Datenanforderung zurückzuführen sein. Überwachen Sie die Anzahl der Objekte, die sich in der Warteschlange befinden, bei abnehmender Systemaktivität.

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

Codieren	Name	Service	Empfohlene Maßnahmen
ARRV	Verifizierungsfehler	LICHTBOGEN	Wenden Sie sich an den technischen Support, um das Problem zu diagnostizieren und zu beheben. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abrufen** > **Konfiguration** > **Main**, wählen Sie **Fehleranzahl der Überprüfung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
ARVF	Speicherfehler	LICHTBOGEN	Dieser Alarm kann aufgrund von Fehlern im externen Archivspeichersystem auftreten. Überprüfen Sie das externe Archiv-Storage-System auf Fehler und stellen Sie sicher, dass es ordnungsgemäß funktioniert. Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Abrufen** > **Konfiguration** > **Main**, wählen Sie **Anzahl der Fehler im Store zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
ASXP	Revisionsfreigaben	AMS	Ein Alarm wird ausgelöst, wenn der Wert der Revisionsfreigaben Unbekannt ist. Dieser Alarm kann auf ein Problem bei der Installation oder Konfiguration des Admin-Knotens hinweisen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUMA	AMS-Status	AMS	Wenn der Wert für AMS Status DB-Verbindungsfehler ist, starten Sie den Grid-Node neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
AUME	AMS-Status	AMS	Wenn der Wert des AMS-Status Standby lautet, fahren Sie mit der Überwachung des StorageGRID-Systems fort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. Wenn der Wert von AMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
AUXS	Exportstatus Prüfen	AMS	Wenn ein Alarm ausgelöst wird, beheben Sie das zugrunde liegende Problem und starten Sie dann den AMS-Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
HINZUFÜGEN	Anzahl Ausgefallener Speicher-Controller-Laufwerke	SSM	Dieser Alarm wird ausgelöst, wenn ein oder mehrere Laufwerke in einem StorageGRID-Gerät ausgefallen sind oder nicht optimal sind. Ersetzen Sie die Laufwerke nach Bedarf.
BASF	Verfügbare Objektkennungen	CMN	Wenn ein StorageGRID System bereitgestellt wird, wird dem CMN-Service eine feste Anzahl von Objekt-IDs zugewiesen. Dieser Alarm wird ausgelöst, wenn das StorageGRID-System seine Versorgung mit Objektkennungen ausgibt. Wenden Sie sich an den technischen Support, um weitere Kennungen zuzuweisen.

Codieren	Name	Service	Empfohlene Maßnahmen
BASS	Identifier Block Zuordnungsstatus	CMN	Standardmäßig wird ein Alarm ausgelöst, wenn Objektkennungen nicht zugewiesen werden können, da ADC Quorum nicht erreicht werden kann. Die Zuweisung von Identifier-Blöcken im CMN-Dienst erfordert ein Quorum (50 % + 1) der ADC-Dienste, dass sie online und verbunden sind. Wenn Quorum nicht verfügbar ist, kann der CMN-Dienst keine neuen Identifikationsblöcke zuweisen, bis das ADC-Quorum wieder hergestellt wird. Bei Verlust des ADC-Quorums entstehen im Allgemeinen keine unmittelbaren Auswirkungen auf das StorageGRID-System (Kunden können weiterhin Inhalte aufnehmen und abrufen), da die Lieferung von Identifikatoren innerhalb eines Monats an anderer Stelle im Grid zwischengespeichert wird. Wenn der Zustand jedoch fortgesetzt wird, kann das StorageGRID-System nicht mehr neue Inhalte aufnehmen. Wenn ein Alarm ausgelöst wird, untersuchen Sie den Grund für den Verlust von ADC-Quorum (z. B. ein Netzwerk- oder Speicherknoten-Ausfall) und ergreifen Sie Korrekturmaßnahmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
BRDT	Temperatur Im Computing-Controller-Chassis	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur des Compute-Controllers in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Prüfen Sie die Hardware-Komponenten und Umweltprobleme auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Ein Alarm wird ausgelöst, wenn die Servicezeit (Sekunden) erheblich von der Betriebssystemzeit abweicht. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Servicezeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
BTSE	Uhrstatus	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Ein Alarm wird ausgelöst, wenn die Servicezeit nicht mit der vom Betriebssystem erfassten Zeit synchronisiert wird. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Zeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CAHP	Java Heap-Nutzung In Prozent	DDS	Ein Alarm wird ausgelöst, wenn Java die Garbage-Sammlung nicht mit einer Rate durchführen kann, die genügend Heap-Speicherplatz für eine ordnungsgemäße Funktion des Systems zulässt. Ein Alarm kann einen Benutzer-Workload anzeigen, der die im System verfügbaren Ressourcen für den DDS-Metadatenspeicher überschreitet. Überprüfen Sie die ILM-Aktivität im Dashboard, oder wählen Sie **Support** > **Tools** > **Grid Topology** und dann ***site*** > ***Grid Node*** > **DDS** > **Ressourcen** > **Übersicht** > **Main**. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CAIH	Anzahl Der Verfügbaren Aufnahmeziele	CLB	Dieser Alarm ist veraltet.
CAQH	Anzahl Der Verfügbaren Ziele	CLB	Dieser Alarm wird gelöscht, wenn die zugrunde liegenden Probleme der verfügbaren LDR-Dienste behoben werden. Stellen Sie sicher, dass die HTTP-Komponente der LDR-Dienste online ist und ordnungsgemäß ausgeführt wird. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CASA	Data Store-Status	DDS	Wenn der Cassandra-Metadatenspeicher nicht mehr verfügbar ist, wird ein Alarm ausgelöst. Den Status von Cassandra überprüfen: 1. Melden Sie sich beim Storage-Node als admin und an `su` Um das Root-Kennwort zu verwenden, das in der Datei Passwords.txt angegeben ist. 2. Geben Sie Ein: `service cassandra status` 3. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: `service cassandra restart` Dieser Alarm kann auch zeigen, dass der Metadatenspeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert. "Fehlerbehebung im Alarm Services: Status - Cassandra (SVST)" Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
FALL	Datenspeicherstatus	DDS	Dieser Alarm wird während der Installation oder Erweiterung ausgelöst, um anzuzeigen, dass ein neuer Datenspeicher in das Raster eingespeist wird.
CES	Eingehende Sitzungen – Eingerichtet	CLB	Dieser Alarm wird ausgelöst, wenn auf dem Gateway Node 20,000 oder mehr HTTP-Sitzungen aktiv (offen) sind. Wenn ein Client zu viele Verbindungen hat, können Verbindungsfehler auftreten. Sie sollten den Workload reduzieren.
CCNA	Computing-Hardware	SSM	Dieser Alarm wird ausgelöst, wenn der Status der Hardware des Computing-Controllers in einer StorageGRID-Appliance zu beachten ist.

Codieren	Name	Service	Empfohlene Maßnahmen
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	DDS	Dieser Alarm wird ausgelöst, wenn der effektive Metadatenraum (Metadaten Effective Space, CEMS) 70 % voll (kleiner Alarm), 90 % voll (Hauptalarm) und 100 % voll (kritischer Alarm) erreicht. Wenn dieser Alarm den Schwellenwert von 90 % erreicht, wird im Dashboard im Grid Manager eine Warnung angezeigt. Sie müssen eine Erweiterung durchführen, um neue Speicherknoten so schnell wie möglich hinzuzufügen. Anweisungen zum erweitern eines StorageGRID-Grids finden Sie in der Anleitung. Wenn dieser Alarm den Schwellenwert von 100 % erreicht, müssen Sie die Aufnahme von Objekten beenden und Speicherknoten sofort hinzufügen. Cassandra erfordert eine bestimmte Menge an Speicherplatz zur Durchführung wichtiger Vorgänge wie Data-Compaction und Reparatur. Diese Vorgänge sind betroffen, wenn Objekt-Metadaten mehr als 100 % des zulässigen Speicherplatzes beanspruchen. Unerwünschte Ergebnisse können auftreten. **Hinweis**: Wenden Sie sich an den technischen Support, wenn Sie keine Speicherknoten hinzufügen können. Sobald neue
256			

Codieren	Name	Service	Empfohlene Maßnahmen
CLBA	CLB-Status	CLB	Wenn ein Alarm ausgelöst wird, wählen Sie **Support** > **Tools** > **Grid Topologie** und wählen Sie dann ***site*** > ***Grid Node*** > **CLB** > **Übersicht** > **Main** und **CLB** > **Alarme** > **Main**, um die Ursache des Alarms zu ermitteln und das Problem zu beheben. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CLBE	Der Status des CLB	CLB	Wenn der Wert des CLB-Status Standby lautet, setzen Sie die Überwachung der Situation fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Status Offline lautet und keine bekannten Probleme mit der Serverhardware (z. B. nicht angeschlossen) oder eine geplante Ausfallzeit auftreten, starten Sie den Service neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CMNA	CMN-Status	CMN	Wenn der Wert von CMN Status Fehler ist, wählen Sie **Support** > **Tools** > **Grid Topology** und dann ***site*** > ***Grid Node*** > **CMN** > **Übersicht** > **Main** und **CMN** > **Alarme** > **Main** aus, um die Fehlerursache zu ermitteln und das Problem zu beheben. Ein Alarm wird ausgelöst, und der Wert von CMN Status ist kein Online CMN während einer Hardwareaktualisierung des primären Admin-Knotens, wenn die CMNS geschaltet werden (der Wert des alten CMN-Status ist Standby und das neue ist Online). Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CPRC	Verbleibende Kapazität	NMS	Ein Alarm wird ausgelöst, wenn die verbleibende Kapazität (Anzahl der verfügbaren Verbindungen, die für die NMS-Datenbank geöffnet werden können) unter den konfigurierten Alarmschwerwert fällt. Wenn ein Alarm ausgelöst wird, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CPSA	Compute Controller Netzteil A	SSM	Wenn ein Problem mit der Stromversorgung A im Rechencontroller eines StorageGRID-Geräts auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.
CPSB	Compute Controller Netzteil B	SSM	Bei einem StorageGRID-Gerät wird ein Alarm ausgelöst, wenn ein Problem mit der Stromversorgung B im Compute-Controller auftritt. Ersetzen Sie die Komponente bei Bedarf.
KFUT	CPU-Temperatur für Compute Controller	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur der CPU im Compute-Controller in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Wenn es sich bei dem Speicherknoten um eine StorageGRID-Appliance handelt, gibt das StorageGRID-System an, dass eine Warnung für den Controller erforderlich ist. Prüfen Sie die Probleme mit den Hardwarekomponenten und der Umgebung auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
DNST	DNS-Status	SSM	Nach Abschluss der Installation wird im SSM-Service ein DNST-Alarm ausgelöst. Nachdem der DNS konfiguriert wurde und die neuen Serverinformationen alle Grid-Knoten erreichen, wird der Alarm abgebrochen.

Codieren	Name	Service	Empfohlene Maßnahmen
ECCD	Beschädigte Fragmente Erkannt	LDR	Ein Alarm wird ausgelöst, wenn die Hintergrundüberprüfung ein korruptes Fragment mit Löschungscode erkennt. Wenn ein beschädigtes Fragment erkannt wird, wird versucht, das Fragment neu zu erstellen. Setzen Sie die beschädigten Fragmente zurück, und kopieren Sie verlorene Attribute auf Null, und überwachen Sie sie, um zu sehen, ob die Zählung wieder hoch geht. Wenn die Anzahl höher ist, kann es zu einem Problem mit dem zugrunde liegenden Speicher des Storage-Nodes kommen. Eine Kopie von Objektdaten mit Löschungscode wird erst dann als fehlend betrachtet, wenn die Anzahl der verlorenen oder korrupten Fragmente die Fehlertoleranz des Löschcodes verletzt. Daher ist es möglich, ein korruptes Fragment zu haben und das Objekt trotzdem abrufen zu können. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
ACST	Verifizierungsstatus	LDR	Dieser Alarm zeigt den aktuellen Status des Hintergrundverifizierungsverfahrens für das Löschen codierter Objektdaten auf diesem Speicherknoten an. Bei der Hintergrundüberprüfung wird ein Großalarm ausgelöst.
FOPN	Dateibeschreibung Öffnen	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Das FOPN kann während der Spitzenaktivität groß werden. Wenn der Support in Phasen mit langsamer Aktivität nicht geschmälert wird, wenden Sie sich an den technischen Support.
HSTE	HTTP-Status	BLDR	Siehe Empfohlene Maßnahmen für HSTU.

Codieren	Name	Service	Empfohlene Maßnahmen
HSTU	HTTP-Status	BLDR	HSTE und HSTU beziehen sich auf das HTTP-Protokoll für den gesamten LDR-Datenverkehr, einschließlich S3, Swift und anderen internen StorageGRID-Datenverkehr. Ein Alarm zeigt an, dass eine der folgenden Situationen aufgetreten ist: • Das HTTP-Protokoll wurde manuell in den Offline-Modus versetzt. • Das Attribut Auto-Start HTTP wurde deaktiviert. • Der LDR-Service wird heruntergefahren. Das Attribut Auto-Start HTTP ist standardmäßig aktiviert. Wenn diese Einstellung geändert wird, kann HTTP nach einem Neustart offline bleiben. Warten Sie gegebenenfalls, bis der LDR-Service neu gestartet wurde. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Storage Node*** > **LDR** > **Konfiguration** aus. Wenn das HTTP-Protokoll offline ist, versetzen Sie es in den Online-Modus. Vergewissern Sie sich, dass das Attribut Auto-Start HTTP aktiviert ist. Wenden Sie sich an den technischen Support, wenn das HTTP-Protokoll offline bleibt.

Codieren	Name	Service	Empfohlene Maßnahmen
HTAS	Automatisches Starten von HTTP	LDR	Gibt an, ob HTTP-Dienste beim Start automatisch gestartet werden sollen. Dies ist eine vom Benutzer angegebene Konfigurationsoption.
IRSU	Status Der Eingehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass die eingehende Replikation deaktiviert wurde. Konfigurationseinstellungen bestätigen: Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** > **Main** aus.

Codieren	Name	Service	Empfohlene Maßnahmen
LATA	Durchschnittliche Latenz	NMS	Überprüfen Sie auf Verbindungsprobleme. Überprüfen Sie die Systemaktivität, um zu bestätigen, dass die Systemaktivität erhöht wird. Eine Erhöhung der Systemaktivität führt zu einer Erhöhung der Attributdatenaktivität. Diese erhöhte Aktivität führt zu einer Verzögerung bei der Verarbeitung von Attributdaten. Dies kann normale Systemaktivität sein und wird unterseiten. Auf mehrere Alarme prüfen. Eine Erhöhung der durchschnittlichen Latenzzeit kann durch eine übermäßige Anzahl von ausgelösten Alarmen angezeigt werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
LDRE	LDR-Status	LDR	Wenn der Wert des LDR-Status Standby lautet, setzen Sie die Überwachung der Situation fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für den LDR-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
VERLOREN	Verlorene Objekte	DDS, LDR	Wird ausgelöst, wenn das StorageGRID System eine Kopie des angeforderten Objekts von einer beliebigen Stelle im System nicht abrufen kann. Bevor ein Alarm VERLOREN GEGANGENE (verlorene Objekte) ausgelöst wird, versucht das System, ein fehlendes Objekt von einem anderen Ort im System abzurufen und zu ersetzen. Verloren gegangene Objekte stellen einen Datenverlust dar. Das Attribut Lost Objects wird erhöht, wenn die Anzahl der Speicherorte eines Objekts auf Null fällt, ohne dass der DDS-Service den Inhalt absichtlich löscht, um der ILM-Richtlinie gerecht zu werden. Untersuchen SIE VERLORENE (VERLORENE Objekte) Alarme sofort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. "Fehlerbehebung verloren gegangene und fehlende Objektdaten"

Codieren	Name	Service	Empfohlene Maßnahmen
MCEP	Ablauf Des Managementschnittstelle-Zertifikats	CMN	Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf die Managementoberfläche verwendet wird, kurz vor Ablauf steht. 1. Gehen Sie zu **Konfiguration** > **Serverzertifikate**. 2. Laden Sie im Abschnitt Management Interface Server Certificate ein neues Zertifikat hoch. "StorageGRID verwalten"
MINQ	E-Mail-Benachrichtigungen in Warteschlange	NMS	Überprüfen Sie die Netzwerkverbindungen der Server, auf denen der NMS-Dienst und der externe Mail-Server gehostet werden. Bestätigen Sie außerdem, dass die Konfiguration des E-Mail-Servers korrekt ist. "Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"

Codieren	Name	Service	Empfohlene Maßnahmen
MIN	E-Mail-Benachrichtigungsstatus	BNMS	Ein kleiner Alarm wird ausgelöst, wenn der NMS-Dienst keine Verbindung zum Mail-Server herstellen kann. Überprüfen Sie die Netzwerkverbindungen der Server, auf denen der NMS-Dienst und der externe Mail-Server gehostet werden. Bestätigen Sie außerdem, dass die Konfiguration des E-Mail-Servers korrekt ist. "Konfigurieren von E-Mail-Servereinstellungen für Alarme (Legacy-System)"
MISS	Status der NMS-Schnittstellen-Engine	BNMS	Ein Alarm wird ausgelöst, wenn die NMS-Schnittstellen-Engine auf dem Admin-Knoten, der Schnittstelleninhalte erfasst und generiert, vom System getrennt wird. Überprüfen Sie Server Manager, ob die Server-individuelle Anwendung ausgefallen ist.
NANG	Einstellung Für Automatische Netzwerkaushandlung	SSM	Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen. Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.

Codieren	Name	Service	Empfohlene Maßnahmen
NDUP	Einstellungen Für Den Netzwerkduplex	SSM	Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen. Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.
NLNK	Network Link Detect	SSM	Überprüfen Sie die Netzwerkverbindungen am Port und am Switch. Überprüfen Sie die Netzwerk-Router-, Switch- und Adapterkonfigurationen. Starten Sie den Server neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
RER	Fehler Beim Empfang	SSM	Die folgenden Ursachen können für NRER-Alarme sein: • Fehler bei der Vorwärtskorrektur (FEC) stimmen nicht überein • Switch-Port und MTU-NIC stimmen nicht überein • Hohe Link-Fehlerraten • NIC-Klingelpuffer überlaufen "Fehlerbehebung bei dem NRER-Alarm (Network Receive Error)"

Codieren	Name	Service	Empfohlene Maßnahmen
NRLY	Verfügbare Audit-Relais	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Relais nicht an ADC-Dienste angeschlossen sind, können Audit-Ereignisse nicht gemeldet werden. Sie werden in eine Warteschlange eingereiht und stehen Benutzern nicht zur Verfügung, bis die Verbindung wiederhergestellt ist. Stellen Sie die Verbindung so schnell wie möglich zu einem ADC-Dienst wieder her. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NSCA	NMS-Status	NMS	Wenn der Wert des NMS-Status DB-Verbindungsfehler ist, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NSCE	Bundesland des NMS	NMS	Wenn der Wert für den NMS-Status Standby lautet, setzen Sie die Überwachung fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für NMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
NSPD	Schnell	SSM	Dies kann durch Probleme mit der Netzwerkverbindung oder der Treiberkompatibilität verursacht werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NTBR	Freie Tablespace	NMS	Wenn ein Alarm ausgelöst wird, überprüfen Sie, wie schnell sich die Datenbanknutzung geändert hat. Ein plötzlicher Abfall (im Gegensatz zu einer allmählichen Änderung im Laufe der Zeit) weist auf eine Fehlerbedingung hin. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. Durch das Anpassen des Alarmschwellenwerts können Sie proaktiv verwalten, wenn zusätzlicher Storage zugewiesen werden muss. Wenn der verfügbare Speicherplatz einen niedrigen Schwellenwert erreicht (siehe Alarmschwelle), wenden Sie sich an den technischen Support, um die Datenbankzuweisung zu ändern.

Codieren	Name	Service	Empfohlene Maßnahmen
NTER	Übertragungsfehler	SSM	Diese Fehler können beseitigt werden, ohne manuell zurückgesetzt zu werden. Wenn sie nicht klar sind, überprüfen Sie die Netzwerk-Hardware. Überprüfen Sie, ob die Adapterhardware und der Treiber korrekt installiert und konfiguriert sind, um mit Ihren Netzwerk-Routern und Switches zu arbeiten. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **SSM** > **Ressourcen** > **Konfiguration** > **Main**, wählen Sie **Zurücksetzen Fehleranzahl für Übertragung zurücksetzen** und klicken Sie auf **Änderungen anwenden**.
NTFQ	NTP-Frequenzverschiebung	SSM	Wenn der Frequenzversatz den konfigurierten Schwellenwert überschreitet, tritt wahrscheinlich ein Hardwareproblem mit der lokalen Uhr auf. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um einen Austausch zu vereinbaren.

Codieren	Name	Service	Empfohlene Maßnahmen
NTLK	NTP Lock	SSM	Wenn der NTP-Daemon nicht an eine externe Zeitquelle gebunden ist, überprüfen Sie die Netzwerkverbindung zu den angegebenen externen Zeitquellen, deren Verfügbarkeit und deren Stabilität.
NTOF	NTP-Zeitverschiebung	SSM	Wenn der Zeitversatz den konfigurierten Schwellenwert überschreitet, liegt wahrscheinlich ein Hardwareproblem mit dem Oszillator der lokalen Uhr vor. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um einen Austausch zu vereinbaren.
NTSJ	Gewählte Zeitquelle Jitter	SSM	Dieser Wert gibt die Zuverlässigkeit und Stabilität der Zeitquelle an, die NTP auf dem lokalen Server als Referenz verwendet. Wenn ein Alarm ausgelöst wird, kann es ein Hinweis sein, dass der Oszillator der Zeitquelle defekt ist oder dass ein Problem mit der WAN-Verbindung zur Zeitquelle besteht.
NTSU	NTP-Status	SSM	Wenn der Wert von NTP Status nicht ausgeführt wird, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
OPST	Gesamtstromstatus	SSM	Wenn die Stromversorgung eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Überprüfen Sie den Status von Netzteil A oder B, um festzustellen, welches Netzteil normal funktioniert. Falls erforderlich, ersetzen Sie das Netzteil.
OQRT	Objekte Isoliert	LDR	Nachdem die Objekte automatisch vom StorageGRID-System wiederhergestellt wurden, können die isolierten Objekte aus dem Quarantäneverzeichnis entfernt werden. 1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. 2. Wählen Sie **Standort** > **Storage Node** > **LDR** > **Verifizierung** > **Konfiguration** > **Main**. 3. Wählen Sie **Gesperrte Objekte Löschen**. 4. Klicken Sie Auf **Änderungen Übernehmen**. Die isolierten Objekte werden entfernt und die Zählung wird auf Null zurückgesetzt.

Codieren	Name	Service	Empfohlene Maßnahmen
ORSU	Status Der Ausgehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass die ausgehende Replikation nicht möglich ist: Der Speicher befindet sich in einem Zustand, in dem Objekte nicht abgerufen werden können. Ein Alarm wird ausgelöst, wenn die ausgehende Replikation manuell deaktiviert wird. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** aus. Wenn der LDR-Dienst nicht zur Replikation verfügbar ist, wird ein Alarm ausgelöst. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** aus.
OSLF	Shelf-Status	SSM	Ein Alarm wird ausgelöst, wenn der Status einer der Komponenten im Speicher-Shelf einer Speichereinrichtung beeinträchtigt ist. Zu den Komponenten des Lagerregals gehören die IOMs, Lüfter, Netzteile und Laufwerksfächer.Wenn dieser Alarm ausgelöst wird, lesen Sie die Wartungsanleitung für Ihr Gerät.

Codieren	Name	Service	Empfohlene Maßnahmen
PMEM	Speicherauslastung Des Service (In Prozent)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Kann einen Wert von mehr als Y% RAM haben, wobei Y den Prozentsatz des Speichers repräsentiert, der vom Server verwendet wird. Zahlen unter 80 % sind normal. Über 90 % wird als Problem betrachtet. Wenn die Speicherauslastung für einen einzelnen Dienst hoch ist, überwachen Sie die Situation und untersuchen Sie sie. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
PSAS	Stromversorgung A-Status	SSM	Wenn die Stromversorgung A in einem StorageGRID-Gerät von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Ersetzen Sie bei Bedarf das Netzteil A.
PSBS	Netzteil B Status	SSM	Wenn die Stromversorgung B eines StorageGRID-Geräts von der empfohlenen Betriebsspannung abweicht, wird ein Alarm ausgelöst. Falls erforderlich, ersetzen Sie das Netzteil B.

Codieren	Name	Service	Empfohlene Maßnahmen
RDTE	Status Von Tivoli Storage Manager	BARC	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Status von Tivoli Storage Manager Offline lautet, überprüfen Sie den Status von Tivoli Storage Manager, und beheben Sie alle Probleme. Versetzen Sie die Komponente wieder in den Online-Modus. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **ARC** > **Ziel** > **Konfiguration** > **Main**, wählen Sie **Tivoli Storage Manager State** > **Online** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
RDTU	Status Von Tivoli Storage Manager	BARC	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM). Wenn der Wert des Tivoli Storage Manager Status auf Konfigurationsfehler gesetzt ist und der Archivknoten gerade dem StorageGRID-System hinzugefügt wurde, stellen Sie sicher, dass der TSM Middleware-Server richtig konfiguriert ist. Wenn der Wert des Tivoli Storage Manager-Status auf Verbindungsfehler oder Verbindungsfehler liegt, überprüfen Sie erneut die Netzwerkkonfiguration auf dem TSM Middleware-Server und die Netzwerkverbindung zwischen dem TSM Middleware-Server und dem StorageGRID-System. Wenn der Wert für Tivoli Storage Manager Status Authentifizierungsfehler oder Authentifizierungsfehler ist, kann eine erneute Verbindung hergestellt werden. Das StorageGRID-System kann eine Verbindung zum TSM Middleware-Server herstellen, die Verbindung kann jedoch nicht authentifiziert werden. Überprüfen Sie, ob der TSM Middleware-Server mit dem richtigen Benutzer, Kennwort und Berechtigungen konfiguriert ist, und starten Sie den Service neu.
278			Wenn der Wert des Tivoli Storage Manager Status

Codieren	Name	Service	Empfohlene Maßnahmen
RIRF	Eingehende Replikationen — Fehlgeschlagen	BLDR, BARC	Eingehende Replikationen – fehlgeschlagener Alarm kann während Zeiten hoher Auslastung oder temporärer Netzwerkstörungen auftreten. Wenn die Systemaktivität verringert wird, sollte dieser Alarm gelöscht werden. Wenn die Anzahl der fehlgeschlagenen Replikationen weiter zunimmt, suchen Sie nach Netzwerkproblemen und überprüfen Sie, ob die LDR- und ARC-Quell- und Zieldienste online und verfügbar sind. Um die Zählung zurückzusetzen, wählen Sie **Support** > **Tools** > **Grid Topologie** und dann ***site*** > ***Grid Node*** > **LDR** > **Replikation** > **Konfiguration** > **Main**. Wählen Sie **Anzahl der fehlgeschlagene Inbound-Replikation zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Codieren	Name	Service	Empfohlene Maßnahmen
RIRQ	Eingehende Replikationen — In Warteschlange	BLDR, BARC	Alarme können in Zeiten hoher Auslastung oder temporärer Netzwerkstörungen auftreten. Wenn die Systemaktivität verringert wird, sollte dieser Alarm gelöscht werden. Wenn die Anzahl der Replikationen in der Warteschlange weiter steigt, suchen Sie nach Netzwerkproblemen und überprüfen Sie, ob die LDR- und ARC-Dienste von Quelle und Ziel online und verfügbar sind.
RORQ	Ausgehende Replikationen — In Warteschlange	BLDR, BARC	Die Warteschlange für ausgehende Replizierung enthält Objektdaten, die kopiert werden, um ILM-Regeln und von Clients angeforderte Objekte zu erfüllen. Ein Alarm kann aufgrund einer Systemüberlastung auftreten. Warten Sie, bis der Alarm gelöscht wird, wenn die Systemaktivität abnimmt. Wenn der Alarm erneut auftritt, fügen Sie die Kapazität durch Hinzufügen von Speicherknoten hinzu.
SAVP	Nutzbarer Speicherplatz (Prozent)	LDR	Wenn der nutzbare Speicherplatz einen niedrigen Schwellenwert erreicht, können Sie unter anderem das erweitern des StorageGRID-Systems oder das Verschieben von Objektdaten in die Archivierung über einen Archiv-Node einschließen.

Codieren	Name	Service	Empfohlene Maßnahmen
SCAS	Status	CMN	Wenn der Wert des Status für die aktive Grid-Aufgabe Fehler ist, suchen Sie die Grid-Task-Meldung. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **CMN** > **Grid Tasks** > **Übersicht** > **Main** aus. Die Grid-Aufgabenmeldung zeigt Informationen zum Fehler an (z. B. „`Check failed on Node 12130011`“). Nachdem Sie das Problem untersucht und behoben haben, starten Sie die Grid-Aufgabe neu. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Grid Node*** > **CMN** > **Grid Tasks** > **Konfiguration** > **Main** aus, und wählen Sie **Aktionen** > **Ausführen**. Wenn der Wert des Status für einen abgebrochenen Grid-Task Fehler ist, versuchen Sie, den Grid-Task zu abbrechen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SCEP	Ablaufdatum des Storage API-Service-Endpoints-Zertifikats	CMN	Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, kurz vor Ablauf steht. 1. Gehen Sie zu **Konfiguration** > **Serverzertifikate**. 2. Laden Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte ein neues Zertifikat hoch. "StorageGRID verwalten"
SCHR	Status	CMN	Wenn der Wert von Status für die Aufgabe des historischen Rasters nicht belegt ist, untersuchen Sie den Grund und führen Sie die Aufgabe bei Bedarf erneut aus. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SCSA	Storage Controller A	SSM	Wenn in einer StorageGRID-Appliance ein Problem mit Storage Controller A auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
SCSB	Storage Controller B	SSM	Wenn ein Problem mit dem Storage Controller B in einer StorageGRID-Appliance auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B
SHLH.	Systemzustand	LDR	Wenn der Wert „Systemzustand“ für einen Objektspeicher „Fehler“ lautet, prüfen und korrigieren Sie Folgendes: • Probleme mit dem zu montiertem Volume • Fehler im Filesystem

Codieren	Name	Service	Empfohlene Maßnahmen
SLSA	CPU-Auslastung durchschnittlich	SSM	Je höher der Wert des Busiers des Systems. Wenn der CPU-Lastdurchschnitt weiterhin mit einem hohen Wert besteht, sollte die Anzahl der Transaktionen im System untersucht werden, um zu ermitteln, ob dies zu diesem Zeitpunkt aufgrund einer hohen Last liegt. Ein Diagramm des CPU-Lastdurchschnitts anzeigen: Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***GRID Node*** > **SSM** > **Ressourcen** > **Berichte** > **Diagramme** aus. Wenn die Belastung des Systems nicht hoch ist und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SMST	Überwachungsstatus Protokollieren	SSM	Wenn der Wert des Protokollüberwachungsstatus für einen anhaltenden Zeitraum nicht verbunden ist, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SMTT	Ereignisse Insgesamt	SSM	Wenn der Wert von Total Events größer als Null ist, prüfen Sie, ob bekannte Ereignisse (z. B. Netzwerkfehler) die Ursache sein können. Wenn diese Fehler nicht gelöscht wurden (d. h., die Anzahl wurde auf 0 zurückgesetzt), können Alarme für Ereignisse insgesamt ausgelöst werden. Wenn ein Problem behoben ist, setzen Sie den Zähler zurück, um den Alarm zu löschen. Wählen Sie **Nodes** > ***site*** > ***Grid Node*** > **Events** > **Ereignisanzahl zurücksetzen** aus. Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen. Wenn der Wert für „Total Events“ null ist oder die Anzahl erhöht wird und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SNST	Status	CMN	Ein Alarm zeigt an, dass ein Problem beim Speichern der Grid-Task-Bundles vorliegt. Wenn der Wert von Status Checkpoint Error oder Quorum nicht erreicht ist, bestätigen Sie, dass ein Großteil der ADC-Dienste mit dem StorageGRID-System verbunden ist (50 Prozent plus einer) und warten Sie dann einige Minuten. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SOSS	Status Des Storage-Betriebssystems	SSM	Ein Alarm wird ausgelöst, wenn die SANtricity-Software angibt, dass bei einer Komponente in einer StorageGRID-Appliance ein „`muss beachtet werden`“-Problem vorliegt. Wählen Sie **Knoten**. Wählen Sie dann **Appliance Storage Node** > **Hardware**. Blättern Sie nach unten, um den Status der einzelnen Komponenten anzuzeigen. Prüfen Sie in der SANtricity-Software die Komponenten anderer Appliances, um das Problem zu isolieren.

Codieren	Name	Service	Empfohlene Maßnahmen
SSMA	SSM-Status	SSM	Wenn der Wert des SSM Status Fehler ist, wählen Sie **Support** > **Tools** > **Grid Topology** und dann ***site*** > ***Grid Node*** > **SSM** > **Übersicht** > **Main** und **SSM** > **Übersicht** > **Alarme**, um die Ursache des Alarms zu bestimmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SSME	SSM-Status	SSM	Wenn der Wert des SSM-Status „Standby“ lautet, setzen Sie die Überwachung fort, und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für SSM-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
SSTS	Storage-Status	BLDR	Wenn der Wert des Speicherstatus nicht genügend verwendbarer Speicherplatz ist, ist auf dem Speicherknoten kein verfügbarer Speicherplatz mehr verfügbar. Die Datenausgabewerte werden auf andere verfügbare Speicherknoten umgeleitet. Abruf-Anfragen können weiterhin von diesem Grid-Node bereitgestellt werden. Zusätzlicher Speicher sollte hinzugefügt werden. Sie wirkt sich nicht auf die Funktionen des Endbenutzers aus, aber der Alarm bleibt bestehen, bis zusätzlicher Speicher hinzugefügt wird. Wenn der Wert für den Speicherstatus „Volume(s) nicht verfügbar“ ist, steht ein Teil des Speichers nicht zur Verfügung. Speicher und Abruf von diesen Volumes ist nicht möglich. Weitere Informationen erhalten Sie in der Ausgabe des Health: Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***site*** > ***GRID Node*** > **LDR** > **Storage** > **Übersicht** > **Main** aus. Die Gesundheit des Volumes ist unter Objektspeichern aufgeführt. Wenn der Wert des Speicherstatus Fehler ist, wenden Sie sich an den technischen Support. "Fehlerbehebung beim SSTS-Alarm (Storage Status)"

Codieren	Name	Service	Empfohlene Maßnahmen
SVST	Status	SSM	Dieser Alarm wird gelöscht, wenn andere Alarme im Zusammenhang mit einem nicht laufenden Dienst gelöst werden. Verfolgen Sie die Alarme des Quelldienstes, um den Vorgang wiederherzustellen. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***GRID Node*** > **SSM** > **Services** > **Übersicht** > **Main** aus. Wenn der Status eines Dienstes als nicht ausgeführt angezeigt wird, ist sein Status „Administrativ ausgefallen“. Der Status des Dienstes kann aus folgenden Gründen als nicht ausgeführt angegeben werden: • Der Dienst wurde manuell beendet (`/etc/init.d/<service\> stop`). • Es liegt ein Problem mit der MySQL-Datenbank vor, und der Server Manager fährt den MI-Dienst herunter. • Ein Grid-Node wurde hinzugefügt, aber nicht gestartet. • Während der Installation ist ein Grid-Node noch nicht mit dem Admin-Node verbunden. Wenn ein Dienst als nicht ausgeführt aufgeführt ist, starten Sie den Dienst neu (`/etc/init.d/<service\> restart`).
			Dieser Alarm kann auch

Codieren	Name	Service	Empfohlene Maßnahmen
TMEM.	Installierter Speicher	SSM	Nodes, die mit weniger als 24 gib des installierten Speichers ausgeführt werden, können zu Performance-Problemen und Systeminstabilität führen. Die Menge des auf dem System installierten Arbeitsspeichers sollte auf mindestens 24 gib erhöht werden.
POP	Ausstehende Vorgänge	ADU	Eine Meldungswarteschlange kann darauf hinweisen, dass der ADC-Dienst überlastet ist. Es können zu wenige ADC-Dienste an das StorageGRID-System angeschlossen werden. In einer großen Implementierung kann der ADC-Service Computing-Ressourcen hinzufügen oder das System benötigt zusätzliche ADC-Services.
UMEM	Verfügbarer Speicher	SSM	Wenn der verfügbare RAM knapp wird, prüfen Sie, ob es sich um ein Hardware- oder Softwareproblem handelt. Wenn es sich nicht um ein Hardwareproblem handelt oder wenn der verfügbare Speicher unter 50 MB liegt (der Standard-Alarmschwellenwert), wenden Sie sich an den technischen Support.
VMFI	Einträge Verfügbar	SSM	Dies deutet darauf hin, dass zusätzlicher Speicherplatz benötigt wird. Wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
VMFR	Speicherplatz Verfügbar	SSM	Wenn der Wert des verfügbaren Speicherplatzes zu niedrig wird (siehe Alarmschwellen), muss untersucht werden, ob sich die Log-Dateien aus dem Verhältnis heraus entwickeln oder Objekte, die zu viel Speicherplatz beanspruchen (siehe Alarmschwellen), die reduziert oder gelöscht werden müssen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
VMST	Status	SSM	Ein Alarm wird ausgelöst, wenn der Wert Status für das Bereitstellungsvolumen Unbekannt ist. Ein Wert von Unbekannt oder Offline kann darauf hindeuten, dass das Volume aufgrund eines Problems mit dem zugrunde liegenden Speichergerät nicht gemountet oder darauf zugegriffen werden kann.
VPRI	Überprüfungspriorität	BLDR, BARC	Standardmäßig ist der Wert der Überprüfungspriorität adaptiv. Wenn die Überprüfungspriorität auf hoch eingestellt ist, wird ein Alarm ausgelöst, da die Speicherüberprüfung den normalen Betrieb des Dienstes verlangsamen kann.

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

Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)

In der folgenden Tabelle sind die älteren Alarme aufgeführt, die SNMP-Benachrichtigungen generieren. Im Gegensatz zu Warnmeldungen generieren nicht alle Alarme SNMP-Benachrichtigungen. Nur die aufgeführten Alarme erzeugen SNMP-Benachrichtigungen und nur bei dem angegebenen Schweregrad oder höher.

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

Codieren	Name	Schweregrad
ACMS	Verfügbare Metadaten	Kritisch
AITE	Status Abrufen	Gering
AITU	Status Abrufen	Major
AMQS	Audit-Nachrichten In Queued	Hinweis
AOTE	Store State	Gering
AOTU	Speicherstatus	Major
AROQ	Objekte In Queued	Gering
ARRF	Anfragefehler	Major
ARRV	Verifizierungsfehler	Major
ARVF	Speicherfehler	Major
ASXP	Revisionsfreigaben	Gering
AUMA	AMS-Status	Gering
AUXS	Exportstatus Prüfen	Gering
BTOF	Offset	Hinweis
CAHP	Java Heap-Nutzung In Prozent	Major
CAQH	Anzahl Der Verfügbaren Ziele	Hinweis
CASA	Data Store-Status	Major
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	Major
CLBE	Der Status des CLB	Kritisch
DNST	DNS-Status	Kritisch
ACST	Verifizierungsstatus	Major

Codieren	Name	Schweregrad
HSTE	HTTP-Status	Major
HTAS	Automatisches Starten von HTTP	Hinweis
VERLOREN	Verlorene Objekte	Major
MINQ	E-Mail-Benachrichtigungen in Warteschlange	Hinweis
MIN	E-Mail-Benachrichtigungsstatus	Gering
NANG	Einstellung Für Automatische Netzwerkaushandlung	Hinweis
NDUP	Einstellungen Für Den Netzwerkduplex	Gering
NLNK	Network Link Detect	Gering
RER	Fehler Beim Empfang	Hinweis
NSPD	Schnell	Hinweis
NTER	Übertragungsfehler	Hinweis
NTFQ	NTP-Frequenzverschiebung	Gering
NTLK	NTP Lock	Gering
NTOF	NTP-Zeitverschiebung	Gering
NTSJ	Gewählte Zeitquelle Jitter	Gering
NTSU	NTP-Status	Major
OPST	Gesamtstromstatus	Major
ORSU	Status Der Ausgehenden Replikation	Hinweis
PSAS	Stromversorgung A-Status	Major
PSBS	Netzteil B Status	Major

Codieren	Name	Schweregrad
RDTE	Status Von Tivoli Storage Manager	Hinweis
RDTU	Status Von Tivoli Storage Manager	Major
SAVP	Nutzbarer Speicherplatz (Prozent)	Hinweis
SHLH.	Systemzustand	Hinweis
SLSA	CPU-Auslastung durchschnittlich	Hinweis
SMTT	Ereignisse Insgesamt	Hinweis
SNST	Status	
SOSS	Status Des Storage-Betriebssystems	Hinweis
SSTS	Storage-Status	Hinweis
SVST	Status	Hinweis
TMEM.	Installierter Speicher	Gering
UMEM	Verfügbarer Speicher	Gering
VMST	Status	Gering
VPRI	Überprüfungspriorität	Hinweis
VSTU	Status Der Objektüberprüfung	Hinweis

Referenz für Protokolldateien

In den folgenden Abschnitten werden die Protokolle zum Erfassen von Ereignissen, Diagnosemeldungen und Fehlerbedingungen aufgeführt. Möglicherweise werden Sie gebeten, Protokolldateien zu sammeln und an den technischen Support zu leiten, um bei der Fehlerbehebung zu helfen.

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

Die Tabellen in diesem Abschnitt dienen nur als Referenz. Die Protokolle sind für erweiterte Fehlerbehebung durch den technischen Support bestimmt. Fortschrittliche Techniken, die die Wiederherstellung des Problemverlaufs mit Hilfe der Audit-Protokolle und der Anwendung Log-Dateien beinhalten, liegen außerhalb des Geltungsbereichs dieses Handbuchs.

Um auf diese Protokolle zuzugreifen, können Sie Log-Dateien und Systemdaten (**Support** > **Tools** > **Logs**) sammeln. Wenn der primäre Admin-Node nicht verfügbar ist oder keinen bestimmten Node erreichen kann, können Sie wie folgt auf die Protokolle für jeden Grid-Node zugreifen:

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

Verwandte Informationen

"Protokolldateien und Systemdaten werden erfasst"

StorageGRID-Softwareprotokolle

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

Allgemeine StorageGRID-Protokolle

Dateiname	Hinweise	Gefunden am
`/var/local/log/bycast.log`	Die Datei `bycast.log` Ist die primäre StorageGRID-Fehlerbehebungsdatei. Die Datei `bycast-err.log` Enthält eine Untergruppe von `bycast.log` (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes
`/var/local/log/bycast-err.log`	Die Datei `bycast.log` Ist die primäre StorageGRID-Fehlerbehebungsdatei. Die Datei `bycast-err.log` Enthält eine Untergruppe von `bycast.log` (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes

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

Server Manager-Protokolle

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

Protokolle für StorageGRID-Services

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

Dateiname	Hinweise	Gefunden am
`/var/local/log/cassandra/system.log`	Informationen für den Metadatenspeicher (Cassandra-Datenbank), die verwendet werden können, wenn Probleme beim Hinzufügen neuer Storage-Nodes auftreten oder wenn der nodetool-Reparaturauftrag abgestellt wird.	Storage-Nodes
`/var/local/log/cassandra-reaper.log`	Informationen zum Cassandra Reaper Service, der Reparaturen der Daten in der Cassandra-Datenbank durchführt.	Storage-Nodes
`/var/local/log/cassandra-reaper.errlog`	Fehlerinformationen für den Cassandra Reaper Service.	Storage-Nodes
`/var/local/log/chunk.errlog`		Storage-Nodes
`/var/local/log/clb.errlog`	Fehlerinformationen für den CLB-Dienst. **Hinweis:** der CLB-Service ist veraltet.	Gateway-Nodes
`/var/local/log/cmn.errlog`		Admin-Nodes
`/var/local/log/cms.errlog`	Diese Protokolldatei ist möglicherweise auf Systemen vorhanden, die von einer älteren StorageGRID-Version aktualisiert wurden. Er enthält Informationen zu Altsystemen.	Storage-Nodes
`/var/local/log/cts.errlog`	Diese Protokolldatei wird nur erstellt, wenn der Zieltyp **Cloud Tiering - Simple Storage Service (S3) ist.**	Archiv-Nodes
`/var/local/log/dds.errlog`		Storage-Nodes
`/var/local/log/dmv.errlog`		Storage-Nodes

Dateiname	Hinweise	Gefunden am
`/var/local/log/dynip*`	Enthält Protokolle zum Dynap-Dienst, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Nodes
`/var/local/log/grafana.log`	Das mit dem Grafana-Service verknüpfte Protokoll, das für die Visualisierung von Kennzahlen im Grid Manager verwendet wird.	Admin-Nodes
`/var/local/log/hagroups.log`	Das Protokoll, das mit Hochverfügbarkeitsgruppen verknüpft ist.	Admin-Nodes und Gateway-Nodes
`/var/local/log/hagroups_events.log`	Verfolgt Statusänderungen, beispielsweise den Übergang von BACKUP zu MASTER oder FEHLER.	Admin-Nodes und Gateway-Nodes
`/var/local/log/idnt.errlog`		Speicherknoten, auf denen der ADC-Service ausgeführt wird
`/var/local/log/jaeger.log`	Das Protokoll, das mit dem jaeger-Dienst verknüpft ist, das für die Trace-Erfassung verwendet wird.	Alle Nodes
`/var/local/log/kstn.errlog`		Speicherknoten, auf denen der ADC-Service ausgeführt wird
`/var/local/log/ldr.errlog`		Storage-Nodes
`/var/local/log/miscd/*.log`	Enthält Protokolle für den MISCd-Dienst (Information Service Control Daemon), der eine Schnittstelle zum Abfragen und Verwalten von Diensten auf anderen Knoten sowie zum Verwalten von Umgebungskonfigurationen auf dem Node bereitstellt, z. B. zum Abfragen des Status von Diensten, die auf anderen Knoten ausgeführt werden.	Alle Nodes

Dateiname	Hinweise	Gefunden am
`/var/local/log/nginx/*.log`	Enthält Protokolle für den nginx-Dienst, der als Authentifizierung und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und dynIP) fungiert, um über HTTPS-APIs mit Diensten auf anderen Knoten kommunizieren zu können.	Alle Nodes
`/var/local/log/nginx-gw/*.log`	Enthält Protokolle für die eingeschränkten Admin-Ports an Admin-Nodes und für den Load Balancer Service, der den Lastenausgleich von S3- und Swift-Datenverkehr von Clients zu Storage-Nodes ermöglicht.	Admin-Nodes und Gateway-Nodes
`/var/local/log/persistence*`	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Root-Festplatte verwaltet, die bei einem Neustart erhalten bleiben müssen.	Alle Nodes
`/var/local/log/prometheus.log`	Enthält für alle Knoten das Service-Protokoll für den Knoten-Exporter und das Kennzahlungsprotokoll der ade-Exporter. Für Admin-Knoten enthält auch Protokolle für die Prometheus- und Alert Manager-Dienste.	Alle Nodes
`/var/local/log/raft.log`	Enthält die Ausgabe der Bibliothek, die vom RSM-Dienst für das Raft-Protokoll verwendet wird.	Storage-Nodes mit RSM-Service
`/var/local/log/rms.errlog`	Enthält Protokolle für den RSM-Service (Replicated State Machine Service), der für S3-Plattformservices verwendet wird.	Storage-Nodes mit RSM-Service
`/var/local/log/ssm.errlog`		Alle Nodes

Dateiname	Hinweise	Gefunden am
`/var/local/log/update-s3vs-domains.log`	Enthält Protokolle zur Verarbeitung von Updates für die Konfiguration virtueller gehosteter S3-Domänennamen.Siehe Anweisungen für die Implementierung von S3-Client-Applikationen.	Admin- und Gateway-Nodes
`/var/local/log/update-snmp-firewall.*`	Enthalten Protokolle im Zusammenhang mit den Firewall-Ports, die für SNMP verwaltet werden.	Alle Nodes
`/var/local/log/update-sysl.log`	Enthält Protokolle in Bezug auf Änderungen an der Syslog-Konfiguration des Systems.	Alle Nodes
`/var/local/log/update-traffic-classes.log`	Enthält Protokolle, die sich auf Änderungen an der Konfiguration von Traffic-Klassifikatoren beziehen.	Admin- und Gateway-Nodes
`/var/local/log/update-utcn.log`	Enthält Protokolle, die sich auf diesem Knoten im Netzwerk des nicht vertrauenswürdigen Clients beziehen.	Alle Nodes

NMS-Protokolle

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

Verwandte Informationen

"Etwa bycast.log"

"S3 verwenden"

Protokoll für Implementierung und Wartung

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

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

Protokolle für Drittanbietersoftware

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

Kategorie	Dateiname	Hinweise	Gefunden am

Apache2-Protokolle	`/var/local/log/apache2/access.log`
	`/var/local/log/apache2/error.log`
	
	`/var/local/log/apache2/other_vhosts_access.log`
		Protokolldateien für apache2.	Admin-Nodes

Archivierung	`/var/local/log/dsierror.log`	Fehlerinformationen für TSM Client APIs.	Archiv-Nodes

Kategorie	Dateiname	Hinweise	Gefunden am
MySQL	/Var/local/log/mysql.err`  `/var/local/log/mysql.err` `/var/local/log/mysql-slow.log`	Protokolldateien von MySQL erstellt. Die Datei mysql.err erfasst Datenbankfehler und Ereignisse wie Start-ups und Herunterfahren. Die Datei mysql-slow.log (das langsame Abfrageprotokoll) erfasst die SQL-Anweisungen, die mehr als 10 Sekunden in Anspruch genommen haben.	Admin-Nodes
Betriebssystem	`/var/local/log/messages`	Dieses Verzeichnis enthält Protokolldateien für das Betriebssystem. Die in diesen Protokollen enthaltenen Fehler werden auch im Grid Manager angezeigt. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann **Topologie** > ***Site*** > ***Node*** > **SSM** > **Events** aus.	Alle Nodes

NTP	`/var/local/log/ntp.log`
	
	`/var/lib/ntp/var/log/ntpstats/`
		Der `/var/local/log/ntp.log` Enthält die Protokolldatei für NTP-Fehlermeldungen.
		
		Der `/var/lib/ntp/var/log/ntpstats/` Verzeichnis enthält NTP-Zeitstatistiken.
		
		`loopstats` Statistikdaten für Datensätze-Loop-Filter.
		
		`peerstats` Zeichnet Informationen zu Peer-Statistiken auf.
			Alle Nodes

Kategorie	Dateiname	Hinweise	Gefunden am
Samba	`/var/local/log/samba/`	Das Samba-Protokollverzeichnis enthält eine Protokolldatei für jeden Samba-Prozess (smb, nmb und winbind) und jeden Client-Hostnamen/jede IP.	Admin-Node für den Export der Revisionsfreigabe über CIFS konfiguriert

Etwa bycast.log

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

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

Dateirotation für bycast.log

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

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

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

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

> Wenn eine Protokolldatei komprimiert wurde, dürfen Sie sie nicht auf den gleichen Speicherort dekomprimieren, an dem sie geschrieben wurde. Die Dekomprimierung der Datei an demselben Speicherort kann die Drehskripte des Protokolls beeinträchtigen.

Verwandte Informationen

"Protokolldateien und Systemdaten werden erfasst"

Nachrichten in bycast.log

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

Dies ist ein Beispiel für eine 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
Node-ID	12455685
PROZESS-ID WIRD ADDIEREN	0357819531
Modulname	SVMR
Nachrichtenkennung	EVHF
UTC-Systemzeit	2019-05-05T27T17:10:29.784677 (JJJJ-MM-DDTHH:MM:SS.UUUUUU)
Schweregrad	FEHLER
Interne Tracking-Nummer	0906
Nachricht	SVMR: Integritätsprüfung auf Volume 3 mit Grund 'AUSWEG' fehlgeschlagen

Nachrichten-Schweregrade in bycast.log

Die Meldungen in `bycast.log` Werden Schweregrade zugewiesen.

Beispiel:

- **HINWEIS** — ein Ereignis, das aufgezeichnet werden soll, ist aufgetreten. Die meisten Protokollmeldungen befinden sich auf dieser Ebene.
- **WARNUNG** — ein unerwarteter Zustand ist aufgetreten.
- **ERROR** — ein großer Fehler ist aufgetreten, der sich auf den Betrieb auswirkt.
- **KRITISCH** — Es ist ein anormaler Zustand aufgetreten, der den normalen Betrieb gestoppt hat. Sie sollten umgehend mit dem zugrunde liegenden Zustand beginnen. Kritische Meldungen werden auch im Grid Manager angezeigt. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann **Standort** > **Knoten** > **SSM** > **Events** aus.

Fehlercodes in bycast.log

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

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

Fehlercode	Bedeutung
SUKZ	Kein Fehler
GERR	Unbekannt
STORNO	Storniert
ABRT	Abgebrochen
TOUT	Zeitüberschreitung
INVL	Ungültig
NFND	Nicht gefunden
ROVER	Version
CONF	Konfiguration
FEHLER	Fehlgeschlagen
ICPL	Unvollständig
FERTIG	Fertig
SUNV	Service nicht verfügbar

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

Fehlernummer	Fehlercode	Bedeutung
001	EPERM	Vorgang nicht zulässig
002	ENOENT	Keine solche Datei oder Verzeichnis
003	ESRCH	Kein solcher Prozess
004	EINTR	Unterbrochener Systemanruf
005	EIO	I/O-Fehler
006	ENXIO	Dieses Gerät oder diese Adresse ist nicht vorhanden

Fehlernummer	Fehlercode	Bedeutung
007	E2BIG	Argumentliste zu lang
008	ENOEXEC	Fehler im Executive-Format
009	EBADF	Ungültige Dateinummer
010	ECHILD	Keine Kinderprozesse
011	EAGAIN	Versuchen Sie es erneut
012	ENOMEM	Nicht genügend Arbeitsspeicher
013	EACCES	Berechtigung verweigert
014	FAULT	Ungültige Adresse
015	ENOTBLK	Blockgerät erforderlich
016	EBUSY	Gerät oder Ressource beschäftigt
017	EEXIST	Datei vorhanden
018	EXDEV	Geräteübergreifende Verbindung
019	ENODEV	Kein solches Gerät
020	ENOTDIR	Kein Verzeichnis
021	EISDIR	Ist ein Verzeichnis
022	EINVAL	Ungültiges Argument
023	DATEI	Dateitabelle-Überlauf
024	EMFILE	Zu viele geöffnete Dateien
025	ENOTTY	Keine Schreibmaschine
026	ETXTBSY	Textdatei belegt
027	EFBIG	Datei zu groß
028	ENOSPC	Kein Platz mehr auf dem Gerät

Fehlernummer	Fehlercode	Bedeutung
029	ESPIPE	Illegale Suche
030	EROFS	Schreibgeschütztes Dateisystem
031	EMLINK	Zu viele Links
032	E-ROHR	Gebrochenes Rohr
033	EDOM	Math Argument aus Domäne der Funktion
034	ERANGE	Math Ergebnis nicht darstellbar
035	EDEADLK	Ressourcen-Deadlock würde eintreten
036	ENAMETOOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperren verfügbar
038	ENOSYS	Funktion nicht implementiert
039	ENOTEMPTY	Verzeichnis nicht leer
040	ELOOP	Es wurden zu viele symbolische Links gefunden
041		
042	ENOMSG	Keine Nachricht vom gewünschten Typ
043	EIDRM	Kennung entfernt
044	ECHRNG	Kanalnummer außerhalb des Bereichs
045	EL2NSYNC	Ebene 2 nicht synchronisiert
046	EL3HLT	Stufe 3 angehalten
047	EL3RST	Stufe 3 zurücksetzen

Fehlernummer	Fehlercode	Bedeutung
048	ELNRNG	Verbindungsnummer außerhalb des Bereichs
049	EUNATCH	Protokolltreiber nicht angeschlossen
050	ENOCSI	Keine CSI-Struktur verfügbar
051	EL2HLT	Stufe 2 angehalten
052	EBADE	Ungültiger Austausch
053	EBADR	Ungültiger Anforderungsdeskriptor
054	EXFULL	Exchange voll
055	ENOANO	Keine Anode
056	EBADRQC	Ungültiger Anforderungscode
057	EBADSLT	Ungültiger Steckplatz
058		
059	EBFONT	Schlechtes Schriftdateiformat
060	ENOSTR	Gerät kein Strom
061	ENODATA	Keine Daten verfügbar
062	ETIME	Timer abgelaufen
063	ENOSR	Aus Datenströmen: Ressourcen
064	ENONET	Die Maschine befindet sich nicht im Netzwerk
065	ENOPKG	Paket nicht installiert
066	EREMOTE	Das Objekt ist Remote
067	ENOLINK	Verbindung wurde getrennt

Fehlernummer	Fehlercode	Bedeutung
068	ADV	Fehler anzeigen
069	ESRMNT	SrMount-Fehler
070	ECOMM	Kommunikationsfehler beim Senden
071	EPROTO	Protokollfehler
072	EMULTIHOP	MultiHop versucht
073	EDOTDOT	RFS-spezifischer Fehler
074	EBADMSG	Keine Datennachricht
075	EOVERFLOW	Wert zu groß für definierten Datentyp
076	ENOTUNIQ	Name nicht eindeutig im Netzwerk
077	EBADFD	Dateideskriptor im schlechten Zustand
078	EREMCHG	Remote-Adresse geändert
079	ELIBACC	Der Zugriff auf eine erforderliche gemeinsam genutzte Bibliothek ist nicht möglich
080	ELIBBAD	Zugriff auf eine beschädigte, gemeinsam genutzte Bibliothek
081	ELIBSCN	
082	ELIBMAX	Es wird versucht, zu viele gemeinsam genutzte Bibliotheken zu verbinden
083	ELIBEXEC	Kann eine gemeinsam genutzte Bibliothek nicht direkt ausführen
084	EILSEQ	Ungültige Byte-Sequenz
085	ERESTART	Unterbrochener Systemanruf sollte neu gestartet werden

Fehlernummer	Fehlercode	Bedeutung
086	ESTRPIPE	Leitungsfehler
087	EUSERS	Zu viele Benutzer
088	ENOTSOCK	Buchsenbetrieb an nicht-Socket
089	EDESTADDRREQ	Zieladresse erforderlich
090	EMSGSIZE	Nachricht zu lang
091	EPROTOTYPE	Protokoll falscher Typ für Socket
092	ENOPROTOOPT	Protokoll nicht verfügbar
093	EPROTONOSUPPORT	Protokoll nicht unterstützt
094	ESOCKTNOSUPPORT	Socket-Typ nicht unterstützt
095	EOPNOTSUPP	Der Vorgang wird auf dem Transportendpunkt nicht unterstützt
096	EPFNOSUPPORT	Protokollfamilie wird nicht unterstützt
097	EAFNOSUPPORT	Adressfamilie wird nicht durch Protokoll unterstützt
098	EADDRINUSE	Die Adresse wird bereits verwendet
099	EADDRNOTAVAIL	Angeforderte Adresse kann nicht zugewiesen werden
100	ENETDOWN	Netzwerk ausgefallen
101	ENETUNREACH	Netzwerk nicht erreichbar
102	ENETRESET	Die Verbindung wurde aufgrund von Reset unterbrochen
103	ECONNABORTED	Software verursacht Verbindungsabbruch
104	ECONNNRESET	Verbindungsrücksetzung durch Peer

Fehlernummer	Fehlercode	Bedeutung
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Senden nach dem Herunterfahren des Transportendpunkts nicht möglich
109	ETOMANYREFS	Zu viele Referenzen: Keine Spleißung möglich
110	ETIMEDOUT	Zeitüberschreitung bei Verbindung
111	ECONNNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHEOSTUNREACH	Keine Route zum Host
114	EALREADY	Der Vorgang wird bereits ausgeführt
115	EINPROGRESS	Vorgang wird jetzt ausgeführt
116		
117	EUCLEAN	Struktur muss gereinigt werden
118	ENOTNAM	Keine XENIX-Datei mit dem Namen
119	ENAVAIL	Keine XENIX-Semaphore verfügbar
120	EISNAM	Ist eine Datei mit dem Namen
121	EREMOTEIO	Remote-I/O-Fehler
122	EDQUOT	Kontingent überschritten

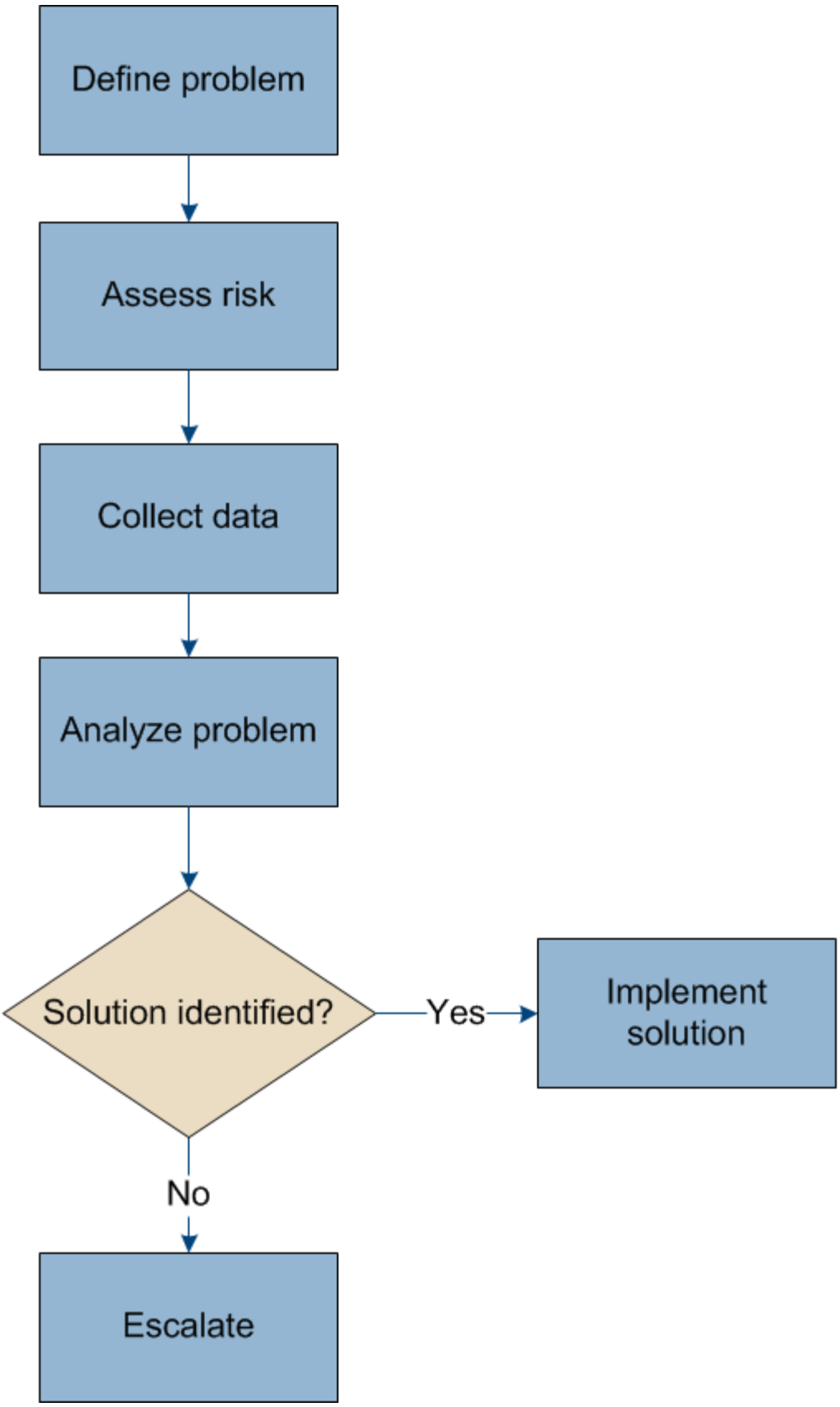
Fehlernummer	Fehlercode	Bedeutung
123	ENOMEDIUM	Kein Medium gefunden
124	EMEDIUMTYPE	Falscher Medientyp
125	ECANCELED	Vorgang Abgebrochen
126	ENOKEY	Erforderlicher Schlüssel nicht verfügbar
127	EKEYEXPIRED	Schlüssel abgelaufen
128	EKEYREVOKED	Schlüssel wurde widerrufen
129	EKEYREJECTED	Schlüssel wurde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

Fehler in einem StorageGRID System beheben

Wenn bei der Verwendung eines StorageGRID-Systems ein Problem auftritt, finden Sie in den Tipps und Richtlinien dieses Abschnitts Hilfe zum ermitteln und Beheben des Problems.

Überblick über die Problembestimmung

Wenn bei der Administration eines StorageGRID-Systems ein Problem auftritt, können Sie das Problem mithilfe des in dieser Abbildung beschriebenen Prozesses identifizieren und analysieren. In vielen Fällen können Sie Probleme selbstständig lösen. In diesem Fall müssen Sie jedoch einige Probleme an den technischen Support eskalieren.



Definition des Problems

Der erste Schritt zur Lösung eines Problems besteht darin, das Problem klar zu definieren.

Diese Tabelle enthält Beispiele für die Arten von Informationen, die Sie erfassen können, um ein Problem zu definieren:

Frage	Beispielantwort
Was macht das StorageGRID-System? Was sind die Symptome?	Client-Applikationen melden, dass Objekte nicht in StorageGRID aufgenommen werden können.
Wann hat das Problem begonnen?	Die Objektaufnahme wurde am 8. Januar 2020 um 14:50 Uhr verweigert.
Wie haben Sie das Problem zum ersten Mal bemerkt?	Durch Client-Anwendung benachrichtigt. Auch Benachrichtigung per E-Mail erhalten.
Tritt das Problem konsequent oder nur in manchen Fällen auf?	Das Problem ist noch nicht behoben.
Wenn das Problem regelmäßig auftritt, welche Schritte dazu führen, dass es auftritt	Das Problem tritt jedes Mal auf, wenn ein Client versucht, ein Objekt aufzunehmen.
Wenn das Problem zeitweise auftritt, wann tritt es auf? Notieren Sie die Zeiten der einzelnen Vorfälle, die Sie kennen.	Das Problem ist nicht intermittierend.
Haben Sie dieses Problem schon einmal gesehen? Wie oft hatten Sie dieses Problem in der Vergangenheit?	Dies ist das erste Mal, dass ich dieses Thema gesehen habe.

Bewertung von Risiken und Auswirkungen auf das System

Bewerten Sie nach Definition des Problems sein Risiko und die Auswirkungen auf das StorageGRID System. Beispielsweise bedeutet das Vorhandensein kritischer Warnmeldungen nicht zwangsläufig, dass das System keine Kernservices liefert.

In dieser Tabelle sind die Auswirkungen eines Beispielproblems auf Systemvorgänge zusammengefasst:

Frage	Beispielantwort
Kann das StorageGRID System Inhalte aufnehmen?	Nein
Können Client-Anwendungen Inhalte abrufen?	Einige Objekte können abgerufen werden, andere können nicht.
Sind Daten gefährdet?	Nein
Ist die Fähigkeit, Geschäfte zu führen, stark beeinträchtigt?	Ja, da Client-Applikationen keine Objekte auf dem StorageGRID System speichern und Daten nicht konsistent abgerufen werden können.

Erfassen von Daten

Nach dem Definition des Problems und der Bewertung der Risiken und Auswirkungen können Sie Daten zur Analyse sammeln. Die Art der Daten, die am nützlichsten zu erfassen sind, hängt von der Art des Problems ab.

Art der zu erfassenden Daten	Warum diese Daten sammeln	Anweisungen
Zeitplan der neuesten Änderungen erstellen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	• Erstellen einer Chronik der neuesten Änderungen
Prüfen von Warnungen und Alarmen	Mithilfe von Warnfunktionen und Alarmen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme geben. Überprüfen Sie die Liste der aktuellen Warnungen und Alarme, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat. Prüfen Sie die in der Vergangenheit ausgelösten Warnmeldungen und Alarme, um zusätzliche Einblicke zu erhalten.	• "Anzeigen aktueller Meldungen" • "Anzeigen von Legacy-Alarmen" • "Anzeigen gelöster Warnmeldungen" • "Überprüfung historischer Alarme und Alarmfrequenz (Altsystem)"
Monitoring von Ereignissen	Ereignisse umfassen Systemfehler oder Fehlerereignisse für einen Node, einschließlich Fehler wie Netzwerkfehler. Überwachen Sie Ereignisse, um weitere Informationen zu Problemen zu erhalten oder um Hilfe bei der Fehlerbehebung zu erhalten.	• "Anzeigen der Registerkarte Ereignisse" • "Monitoring von Ereignissen"
Trends anhand von Diagramm- und Textberichten identifizieren	Trends liefern wertvolle Hinweise darauf, wann Probleme zuerst auftraten, und können Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	• "Verwenden von Diagrammen und Berichten"
Basispläne erstellen	Sammeln von Informationen über die normalen Stufen verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Grundlinien können wertvolle Hinweise liefern.	• Basisvorgänge werden erstellt
Durchführen von Einspeisung und Abruf von Tests	Zur Fehlerbehebung von Performance-Problemen bei Aufnahme und Abruf können Objekte auf einer Workstation gespeichert und abgerufen werden. Vergleichen Sie die Ergebnisse mit denen, die bei der Verwendung der Client-Anwendung angezeigt werden.	• "Monitoring PUT und GET Performance"

Art der zu erfassenden Daten	Warum diese Daten sammeln	Anweisungen
Audit-Meldungen prüfen	Überprüfen Sie Audit-Meldungen, um StorageGRID Vorgänge im Detail zu befolgen. Die Details in Audit-Meldungen können bei der Behebung vieler Arten von Problemen, einschließlich von Performance-Problemen, nützlich sein.	• "Überprüfen von Audit-Meldungen"
Überprüfen Sie Objektstandorte und Storage-Integrität	Wenn Sie Speicherprobleme haben, stellen Sie sicher, dass Objekte an der gewünschten Stelle platziert werden. Überprüfen Sie die Integrität von Objektdaten auf einem Storage-Node.	"Monitoring von Objektverifizierungsvorgängen".
Datenerfassung für technischen Support	Vom technischen Support werden Sie möglicherweise aufgefordert, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um Probleme zu beheben.	• "Protokolldateien und Systemdaten werden erfasst" • "Manuelles Auslösen einer AutoSupport-Meldung" • "Überprüfen von Support-Metriken"

Erstellen einer Chronik der neuesten Änderungen

Wenn ein Problem auftritt, sollten Sie berücksichtigen, was sich kürzlich geändert hat und wann diese Änderungen aufgetreten sind.

- Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.
- Durch eine Zeitleiste von Änderungen können Sie feststellen, welche Änderungen für ein Problem verantwortlich sein könnten und wie jede Änderung ihre Entwicklung beeinflusst haben könnte.

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann jede Änderung stattgefunden hat und welche relevanten Details über die Änderung angezeigt werden, und Informationen darüber, was während der Änderung noch passiert ist:

Zeit der Änderung	Art der Änderung	Details
Beispiel: • Wann haben Sie die Node-Wiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Prozess unterbrochen?	Was ist los? Was haben Sie gemacht?	Dokumentieren Sie alle relevanten Details zu der Änderung. Beispiel: • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Änderungen bei Client-Workloads Achten Sie darauf, zu beachten, ob mehrere Änderungen gleichzeitig durchgeführt wurden. Wurde diese Änderung beispielsweise vorgenommen, während ein Upgrade durchgeführt wurde?

Beispiele für signifikante aktuelle Änderungen

Hier einige Beispiele für potenziell signifikante Änderungen:

- Wurde das StorageGRID System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde kürzlich ein Upgrade des Systems durchgeführt? Wurde ein Hotfix angewendet?
- Wurde irgendeine Hardware in letzter Zeit repariert oder geändert?
- Wurde die ILM-Richtlinie aktualisiert?
- Hat sich der Client-Workload geändert?
- Hat sich die Client-Applikation oder deren Verhalten geändert?
- Haben Sie den Lastausgleich geändert oder eine Hochverfügbarkeitsgruppe aus Admin-Nodes oder Gateway-Nodes hinzugefügt oder entfernt?
- Wurden Aufgaben gestartet, die ein sehr langer Zeitaufwand beanspruchen können? Beispiele:
  - Wiederherstellung eines fehlerhaften Speicherknotens
  - Ausmusterung von Storage-Nodes
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, beispielsweise beim Hinzufügen eines Mandanten oder bei der Änderung der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattform-Services kürzlich aktiviert oder geändert?
- Wurde die Compliance in letzter Zeit aktiviert?
- Wurden Cloud-Storage-Pools hinzugefügt oder entfernt?
- Wurden Änderungen an der Storage-Komprimierung oder -Verschlüsselung vorgenommen?
- Wurden Änderungen an der Netzwerkinfrastruktur vorgenommen? Beispiel: VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?
- Wurden Konfigurationsänderungen am Archiv-Node vorgenommen?
- Wurden weitere Änderungen am StorageGRID System bzw. an der zugehörigen Umgebung

vorgenommen?

Basisvorgänge werden erstellt

Sie können Basislinien für Ihr System einrichten, indem Sie die normalen Ebenen verschiedener Betriebswerte erfassen. In Zukunft können Sie aktuelle Werte mit diesen Basiswerten vergleichen, um ungewöhnliche Werte zu erkennen und zu beheben.

Eigenschaft	Wert	Wie zu erhalten
Durchschnittlicher Storage-Verbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm Speicher verwendet - Objektdaten einen Zeitraum, in dem die Linie ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Storage täglich belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenkverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm „verwendete Speicher - Objektmetadaten“ einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Metadaten-Storage jeden Tag belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Geschwindigkeit von S3/Swift Operationen	Vorgänge/Sekunde	Wechseln Sie im Grid Manager zum Fenster Dashboard. Sehen Sie sich im Abschnitt Protokollvorgänge die Werte für die S3-Rate und die Swift-Rate an. Um Einspeis- und Abrufraten und Zählungen für einen bestimmten Standort oder Knoten anzuzeigen, wählen Sie **Knoten** > ***Standort oder Storage Node*** > **Objekte**. Halten Sie den Mauszeiger über das Diagramm Aufnahme und Abruf für S3 oder Swift.
S3/Swift-Vorgänge sind fehlgeschlagen	Betrieb	Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Zeigen Sie auf der Registerkarte Übersicht im Abschnitt API-Vorgänge den Wert für S3-Operationen an – Fehlgeschlagen oder Swift-Vorgänge – Fehlgeschlagen.

Eigenschaft	Wert	Wie zu erhalten
ILM-Auswertungsrate	Objekte/Sekunde	Wählen Sie auf der Seite Knoten ***GRID*** > **ILM** aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um einen Basiswert für **Evaluierungsrate** für Ihr System zu schätzen.
ILM-Scan-Rate	Objekte/Sekunde	Wählen Sie **Nodes** > ***GRID*** > **ILM** aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basiswert für **Scanrate** für Ihr System zu schätzen.
Objekte, die sich aus Client-Vorgängen in Warteschlange befinden	Objekte/Sekunde	Wählen Sie **Nodes** > ***GRID*** > **ILM** aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um einen Basiswert für **Objekte in der Warteschlange (aus Client-Operationen)** für Ihr System zu schätzen.
Durchschnittliche Abfragelatenz	Millisekunden	Wählen Sie **Knoten** > ***Speicherknoten*** > **Objekte** Aus. Zeigen Sie in der Tabelle Abfragen den Wert für durchschnittliche Latenz an.

Datenanalyse

Verwenden Sie die gesammelten Informationen, um die Ursache des Problems und der potenziellen Lösungen zu ermitteln.

Die Analyse ist Problem-abhängig, aber im Allgemeinen:

- Erkennen von Fehlerpunkten und Engpässen mithilfe der Alarme.
- Rekonstruieren Sie den Problemverlauf mithilfe der Alarmhistorie und -Diagramme.
- Verwenden Sie Diagramme, um Anomalien zu finden und die Problemsituation mit dem normalen Betrieb zu vergleichen.

Checkliste für Eskalationsinformationen

Wenn Sie das Problem nicht selbst lösen können, wenden Sie sich an den technischen Support. Bevor Sie sich an den technischen Support wenden, müssen Sie die in der folgenden Tabelle aufgeführten Informationen zur Erleichterung der Problembehebung nutzen.

✔	Element	Hinweise
	Problemstellung	Was sind die Problemsymptome? Wann hat das Problem begonnen? Passiert es konsequent oder intermittierend? Welche Zeiten hat es gelegentlich gegeben? "Definition des Problems"
	Folgenabschätzung	Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation? • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	Wählen Sie **Wartung** > **System** > **Lizenz**. Die StorageGRID System-ID wird im Rahmen der aktuellen Lizenz angezeigt.
	Softwareversion	Klicken Sie auf **Hilfe** > **Info**, um die StorageGRID-Version anzuzeigen.
	Anpassbarkeit	Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf: • Verwendet das Grid Storage-Komprimierung, Storage-Verschlüsselung oder Compliance? • Erstellt ILM replizierte oder Erasure Coding Objekte? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das strenge, ausgewogene oder duale Ingest-Verhalten?
	Log-Dateien und Systemdaten	Erfassen von Protokolldateien und Systemdaten für Ihr System Wählen Sie **Support** > **Extras** > **Protokolle**. Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln. Wenn Sie Protokolle nur für ausgewählte Knoten erfassen, müssen Sie mindestens einen Speicherknoten mit dem ADC-Service einschließen. (Die ersten drei Storage-Nodes an einem Standort enthalten den ADC-Service.) "Protokolldateien und Systemdaten werden erfasst"
	Basisinformationen	Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch "Basisvorgänge werden erstellt"

✔	Element	Hinweise
	Zeitachse der letzten Änderungen	Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind. "Erstellen einer Chronik der neuesten Änderungen"
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie Schritte zur Diagnose oder Behebung des Problems selbst ergriffen haben, achten Sie darauf, die Schritte und das Ergebnis zu notieren.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei Objekt- und Storage-Problemen

Sie können verschiedene Aufgaben ausführen, um die Ursachen von Objekt- und Storage-Problemen zu ermitteln.

Bestätigen der Speicherorte von Objektdaten

Je nach Problem sollten Sie überprüfen, wo Objektdaten gespeichert werden. Beispielsweise möchten Sie überprüfen, ob die ILM-Richtlinie wie erwartet funktioniert und Objektdaten dort gespeichert werden, wo sie geplant sind.

Was Sie benötigen

- Sie müssen über eine Objektkennung verfügen, die einer der folgenden sein kann:
  - **UUID**: Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.
  - **CBID**: Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in allen Großbuchstaben ein.
  - **S3-Bucket und Objektschlüssel**: Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
  - **Swift Container und Objektname**: Wenn ein Objekt über die Swift-Schnittstelle aufgenommen wird, verwendet die Client-Anwendung eine Container- und Objektname-Kombination, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Wählen Sie **ILM** > **Objekt Metadaten Lookup** aus.
2. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

   Sie können eine UUID, CBID, S3 Bucket/Objektschlüssel oder Swift Container/Objektname eingeben.

3. Klicken Sie Auf **Look Up**.

   Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

   - Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
   - Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
   - Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
   - Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
   - Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
   - Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
   - Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
   - Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

     Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Verwandte Informationen

"Objektmanagement mit ILM"

"S3 verwenden"

"Verwenden Sie Swift"

Fehler beim Objektspeicher (Storage Volume)

Der zugrunde liegende Storage auf einem Storage-Node ist in Objektspeicher unterteilt. Diese Objektspeicher sind physische Partitionen, die als Bereitstellungspunkte für den Storage des StorageGRID Systems fungieren. Objektspeicher werden auch als Storage Volumes bezeichnet.

Sie können die Objektspeicherinformationen für jeden Speicherknoten anzeigen. Objektspeicher werden unten auf der Seite **Nodes** > ***Storage Node*** > **Storage** angezeigt.

Disk Devices

Name	World Wide Name	I/O Load	Read Rate	Write Rate
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s

Volumes

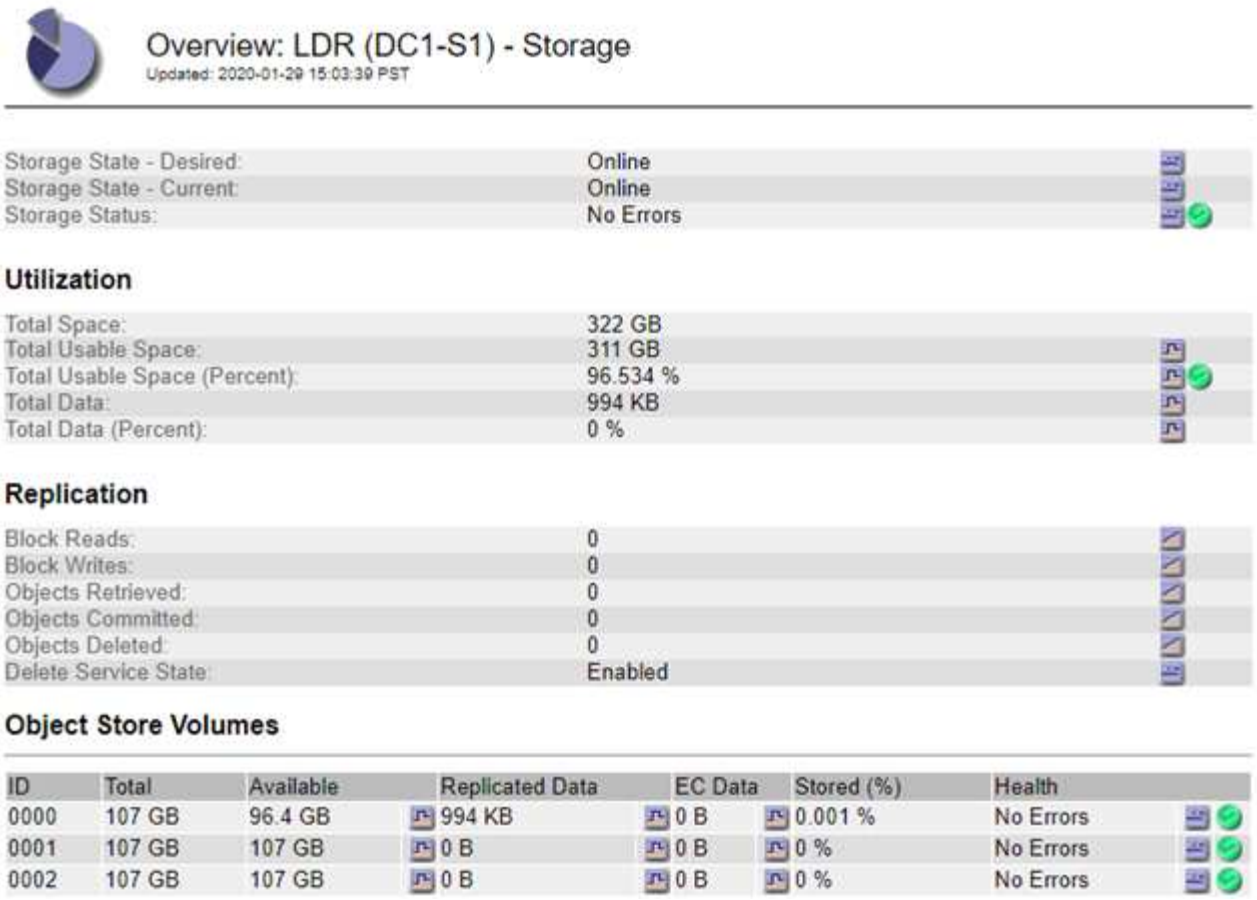
Mount Point	Device	Status	Size	Available	Write Cache Status
/	croot	Online	21.00 GB	14.25 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB	Enabled

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 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

Führen Sie die folgenden Schritte aus, um weitere Details zu jedem Storage-Node anzuzeigen:

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Übersicht** > **Haupt**.



Je nach Art des Ausfalls können Fehler bei einem Storage-Volume in einem Alarm über den Storage-Status oder den Zustand eines Objektspeicher gespiegelt werden. Wenn ein Speichervolume ausfällt, sollten Sie das ausgefallene Speichervolume reparieren, um den Speicherknoten so bald wie möglich wieder voll zu machen. Wenn nötig, können Sie auf die Registerkarte **Konfiguration** gehen und den Speicherknoten in einen Read -only Zustand setzen, so dass das StorageGRID System ihn für den Datenabruf verwenden kann, während Sie sich auf eine vollständige Wiederherstellung des Servers vorbereiten.

Verwandte Informationen

"Verwalten Sie erholen"

Überprüfen der Objektintegrität

Das StorageGRID System überprüft die Integrität der Objektdaten auf Storage-Nodes und überprüft sowohl beschädigte als auch fehlende Objekte.

Es gibt zwei Verifizierungsverfahren: Hintergrund- und Vordergrundüberprüfung. Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung wird automatisch ausgeführt und überprüft kontinuierlich die Korrektheit von Objektdaten. Die Vordergrundüberprüfung kann von einem Benutzer ausgelöst werden, um die Existenz (obwohl nicht die Korrektheit) von Objekten schneller zu überprüfen.

Was ist Hintergrundüberprüfung

Die Hintergrundüberprüfung überprüft Storage Nodes automatisch und kontinuierlich auf beschädigte Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Bei der Hintergrundüberprüfung werden die Integrität replizierter Objekte und Objekte mit Erasure-Coding-Verfahren überprüft:

- **Replizierte Objekte**: Findet der Hintergrundverifizierungsvorgang ein beschädigtes Objekt, wird die beschädigte Kopie vom Speicherort entfernt und an anderer Stelle auf dem Speicherknoten isoliert. Anschließend wird eine neue, nicht beschädigte Kopie erstellt und gemäß der aktiven ILM-Richtlinie platziert. Die neue Kopie wird möglicherweise nicht auf dem Speicherknoten abgelegt, der für die ursprüngliche Kopie verwendet wurde.

> Beschädigte Objektdaten werden nicht aus dem System gelöscht, sondern in Quarantäne verschoben, sodass weiterhin darauf zugegriffen werden kann. Weitere Informationen zum Zugriff auf isolierte Objektdaten erhalten Sie vom technischen Support.

- **Erasure-codierte Objekte**: Erkennt der Hintergrund-Verifizierungsprozess, dass ein Fragment eines Löschungscodierten Objekts beschädigt ist, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Daten- und Paritätsfragmente neu zu erstellen. Wenn das beschädigte Fragment nicht wiederhergestellt werden kann, wird das Attribut „Corrupt Copies detected (ECOR)“ um eins erhöht und es wird versucht, eine weitere Kopie des Objekts abzurufen. Wenn der Abruf erfolgreich ist, wird eine ILM-Bewertung durchgeführt, um eine Ersatzkopie des Objekts, das mit der Fehlerkorrektur codiert wurde, zu erstellen.

  Bei der Hintergrundüberprüfung werden nur Objekte auf Speicherknoten überprüft. Es überprüft keine Objekte auf Archiv-Nodes oder in einem Cloud-Speicherpool. Objekte müssen älter als vier Tage sein, um sich für die Hintergrundüberprüfung zu qualifizieren.

Die Hintergrundüberprüfung läuft mit einer kontinuierlichen Geschwindigkeit, die nicht auf normale Systemaktivitäten ausgerichtet ist. Hintergrundüberprüfung kann nicht angehalten werden. Sie können jedoch die Hintergrundverifizierungsrate erhöhen, um falls Sie vermuten, dass ein Problem vorliegt, den Inhalt eines Storage-Nodes schneller zu überprüfen.

Warnmeldungen und Alarme (alt) im Zusammenhang mit der Hintergrundüberprüfung

Wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann (weil die Beschädigung verhindert, dass das Objekt identifiziert wird), wird die Warnung **Unerkannter beschädigter Gegenstand erkannt** ausgelöst.

Wenn die Hintergrundüberprüfung ein beschädigtes Objekt nicht ersetzen kann, da es keine andere Kopie finden kann, werden die Meldung **Objekte verloren** und der ältere Alarm VERLOREN GEGANGENE (verlorene Objekte) ausgelöst.

Ändern der Hintergrundverifizierungsrate

Sie können die Rate ändern, mit der die Hintergrundüberprüfung replizierte Objektdaten auf einem Storage-Node überprüft, wenn Sie Bedenken hinsichtlich der Datenintegrität haben.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Sie können die Verifizierungsrate für die Hintergrundüberprüfung eines Speicherknoten ändern:

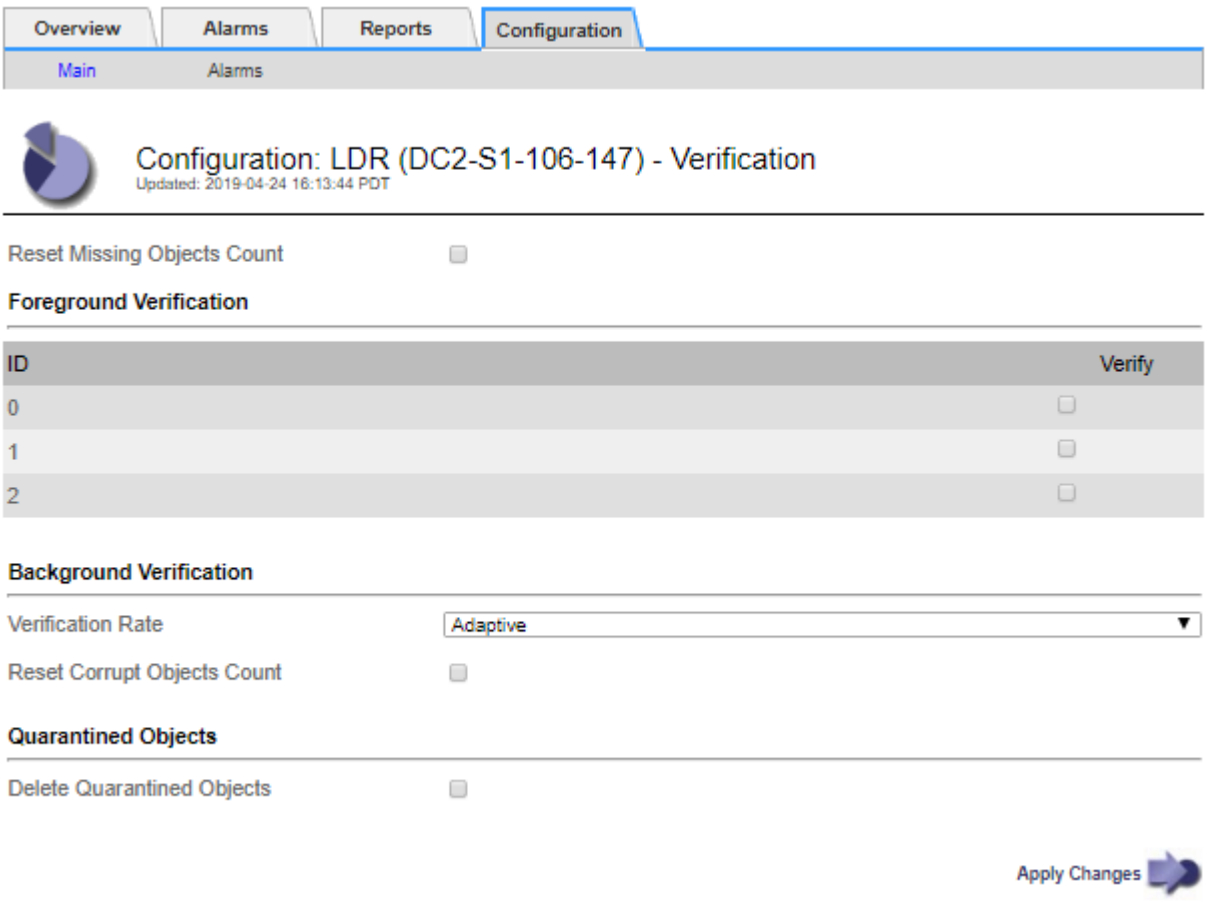
- Adaptiv: Standardeinstellung. Die Aufgabe wurde entwickelt, um maximal 4 MB/s oder 10 Objekte/s zu überprüfen (je nachdem, welcher Wert zuerst überschritten wird).
- Hoch: Die Storage-Verifizierung verläuft schnell und kann zu einer Geschwindigkeit führen, die normale

Systemaktivitäten verlangsamen kann.

Verwenden Sie die hohe Überprüfungsrate nur, wenn Sie vermuten, dass ein Hardware- oder Softwarefehler beschädigte Objektdaten aufweisen könnte. Nach Abschluss der Hintergrundüberprüfung mit hoher Priorität wird die Verifizierungsrate automatisch auf Adaptive zurückgesetzt.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Storage-Node* > LDR > Verifizierung** aus.
3. Wählen Sie **Konfiguration** > **Main**.
4. Gehen Sie zu **LDR** > **Verifizierung** > **Konfiguration** > **Main**.
5. Wählen Sie unter Hintergrundüberprüfung die Option **Verifizierungsrate** > **hoch** oder **Verifizierungsrate** > **adaptiv** aus.



Wenn Sie die Verifizierungsrate auf hoch setzen, wird der alte Alarm VPRI (Verification Rate) auf der Melderebene ausgelöst.

1. Klicken Sie Auf **Änderungen Übernehmen**.
2. Überwachen der Ergebnisse der Hintergrundüberprüfung replizierter Objekte
   a. Gehen Sie zu **Nodes** > ***Storage Node*** > **Objects**.
   b. Überwachen Sie im Abschnitt Überprüfung die Werte für **beschädigte Objekte** und **beschädigte Objekte nicht identifiziert**.

Wenn bei der Hintergrundüberprüfung beschädigte replizierte Objektdaten gefunden werden, wird die Metrik **beschädigte Objekte** erhöht und StorageGRID versucht, die Objektkennung aus den Daten zu extrahieren, wie folgt:

- Wenn die Objekt-ID extrahiert werden kann, erstellt StorageGRID automatisch eine neue Kopie der Objektdaten. Die neue Kopie kann an jedem beliebigen Ort im StorageGRID System erstellt werden, der die aktive ILM-Richtlinie erfüllt.
- Wenn die Objektkennung nicht extrahiert werden kann (weil sie beschädigt wurde), wird die Metrik **korrupte Objekte nicht identifiziert** erhöht und die Warnung **nicht identifiziertes korruptes Objekt erkannt** ausgelöst.

c. Wenn beschädigte replizierte Objektdaten gefunden werden, wenden Sie sich an den technischen Support, um die Ursache der Beschädigung zu ermitteln.

3. Überwachen Sie die Ergebnisse der Hintergrundüberprüfung von Objekten, die mit Erasure Coding codiert wurden.

   Wenn bei der Hintergrundüberprüfung beschädigte Fragmente von Objektdaten gefunden werden, die mit dem Erasure-Coding-Verfahren codiert wurden, wird das Attribut „beschädigte Fragmente erkannt“ erhöht. StorageGRID stellt sich wieder her, indem das beschädigte Fragment auf demselben Speicherknoten wiederhergestellt wird.

   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***Storage Node* > LDR > Erasure Coding** aus.
   c. Überwachen Sie in der Tabelle „Ergebnisse der Überprüfung“ das Attribut „beschädigte Fragmente erkannt“ (ECCD).

4. Nachdem das StorageGRID System beschädigte Objekte automatisch wiederhergestellt hat, setzen Sie die Anzahl beschädigter Objekte zurück.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***Storage Node* > LDR > Verifizierung > Konfiguration** aus.
   c. Wählen Sie **Anzahl Der Beschädigten Objekte Zurücksetzen**.
   d. Klicken Sie Auf **Änderungen Übernehmen**.
5. Wenn Sie sicher sind, dass isolierte Objekte nicht erforderlich sind, können Sie sie löschen.

> Wenn der Alarm **Objects lost** oder der Legacy-Alarm LOST (Lost Objects) ausgelöst wurde, möchte der technische Support möglicherweise auf isolierte Objekte zugreifen, um das zugrunde liegende Problem zu beheben oder eine Datenwiederherstellung zu versuchen.

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Storage Node*** > **LDR** > **Verifizierung** > **Konfiguration**.
3. Wählen Sie **Gesperrte Objekte Löschen**.
4. Klicken Sie Auf **Änderungen Übernehmen**.

Was ist die Vordergrundüberprüfung

Vordergrundüberprüfung ist ein vom Benutzer initiierter Prozess, der überprüft, ob alle erwarteten Objektdaten auf einem Storage-Node vorhanden sind. Vordergrundüberprüfung wird verwendet, um die Integrität eines Speichergeräts zu überprüfen.

Die Vordergrundüberprüfung ist eine schnellere Alternative zur Hintergrundüberprüfung, die die Existenz von

Objektdaten auf einem Storage-Node, jedoch nicht die Integrität überprüft. Wenn bei der Überprüfung im Vordergrund festgestellt wird, dass viele Elemente fehlen, kann es zu Problemen mit dem gesamten oder einem Teil eines Speichergeräts, das mit dem Speicherknoten verknüpft ist, kommen.

Bei der Vordergrundüberprüfung werden sowohl replizierte Objektdaten als auch mit Erasure-Coding-Objektdaten überprüft:

- **Replizierte Objekte**: Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, die Kopie von an anderer Stelle im System gespeicherten Kopien zu ersetzen. Der Storage Node führt eine vorhandene Kopie durch eine ILM-Bewertung aus. Damit wird ermittelt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da die fehlende Kopie nicht mehr am erwarteten Standort vorhanden ist. Eine neue Kopie wird erstellt und platziert, um die aktive ILM-Richtlinie des Systems zu erfüllen. Diese neue Kopie kann nicht an demselben Speicherort abgelegt werden, an dem die fehlende Kopie gespeichert wurde.
- **Erasure-codierte Objekte**: Wenn ein Fragment eines Löschungskodierten Objekts gefunden wird, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten unter Verwendung der verbleibenden Fragmente neu zu erstellen. Wenn das fehlende Fragment nicht wieder aufgebaut werden kann (weil zu viele Fragmente verloren sind), wird das Attribut Corrupt Copies detected (ECOR) um eins erhöht. ILM versucht anschließend, eine andere Kopie des Objekts zu finden, mit der das Unternehmen eine neue Kopie mit Verfahren zur Fehlerkorrektur erstellen kann.

  Wenn bei der Vordergrundüberprüfung ein Problem mit dem Erasure Coding für ein Storage-Volume erkannt wird, wird bei der Vordergrundverifizierung eine Fehlermeldung angehalten, die das betroffene Volume identifiziert. Sie müssen ein Recovery-Verfahren für alle betroffenen Storage Volumes durchführen.

Wenn im Raster keine weiteren Kopien eines fehlenden replizierten Objekts oder eines beschädigten Erasure-codierten Objekts gefunden werden, werden die Meldung **Objekte verloren** und der Legacy-Alarm FÜR VERLORENE (verlorene Objekte) ausgelöst.

Vordergrundüberprüfung wird ausgeführt

Mit der Vordergrundüberprüfung können Sie die Existenz von Daten auf einem Speicherknoten überprüfen. Fehlende Objektdaten können darauf hindeuten, dass beim zugrunde liegenden Speichergerät ein Problem vorliegt.

Was Sie benötigen

- Sie haben sichergestellt, dass die folgenden Grid-Aufgaben nicht ausgeführt werden:
  - Grid Expansion: Add Server (GEXP), wenn ein Storage Node hinzugefügt wird
  - Storage Node Deaktivierungsfunktion (LDCM) auf demselben Storage-Node Wenn diese Grid-Aufgaben ausgeführt werden, warten Sie, bis sie abgeschlossen sind oder lassen Sie die Sperre frei.
- Sie haben sichergestellt, dass die Speicherung online ist. (Wählen Sie **Support** > **Tools** > **Grid Topology**. Wählen Sie dann ***Storage Node*** > **LDR** > **Storage** > **Übersicht** > **Haupt** aus. Vergewissern Sie sich, dass **Speicherstatus - Aktuell** online ist.)
- Sie haben sichergestellt, dass die folgenden Wiederherstellungsverfahren nicht auf demselben Speicherknoten ausgeführt werden:
  - Recovery eines ausgefallenen Storage-Volumes
  - Die Recovery eines Storage-Knotens mit einer fehlgeschlagenen Systemlaufwerk-Vordergrundüberprüfung bietet keine nützlichen Informationen, während Recovery-Verfahren ausgeführt werden.

Über diese Aufgabe

Vordergrundüberprüfung werden sowohl fehlende replizierte Objektdaten als auch fehlende, mit Erasure Coding versehenen Objektdaten überprüft:

- Wenn bei der Überprüfung im Vordergrund große Mengen fehlender Objektdaten festgestellt werden, liegt es wahrscheinlich vor, dass der Storage-Node analysiert und behoben werden muss.
- Wenn bei der Überprüfung im Vordergrund ein schwerwiegender Storage-Fehler bei der Datenlöschung festgestellt wird, werden Sie darüber informiert. Sie müssen die Wiederherstellung des Speichervolumes durchführen, um den Fehler zu beheben.

Sie können die Vordergrundüberprüfung so konfigurieren, dass alle Objektspeicher eines Storage Node oder nur bestimmte Objektspeichern überprüft werden.

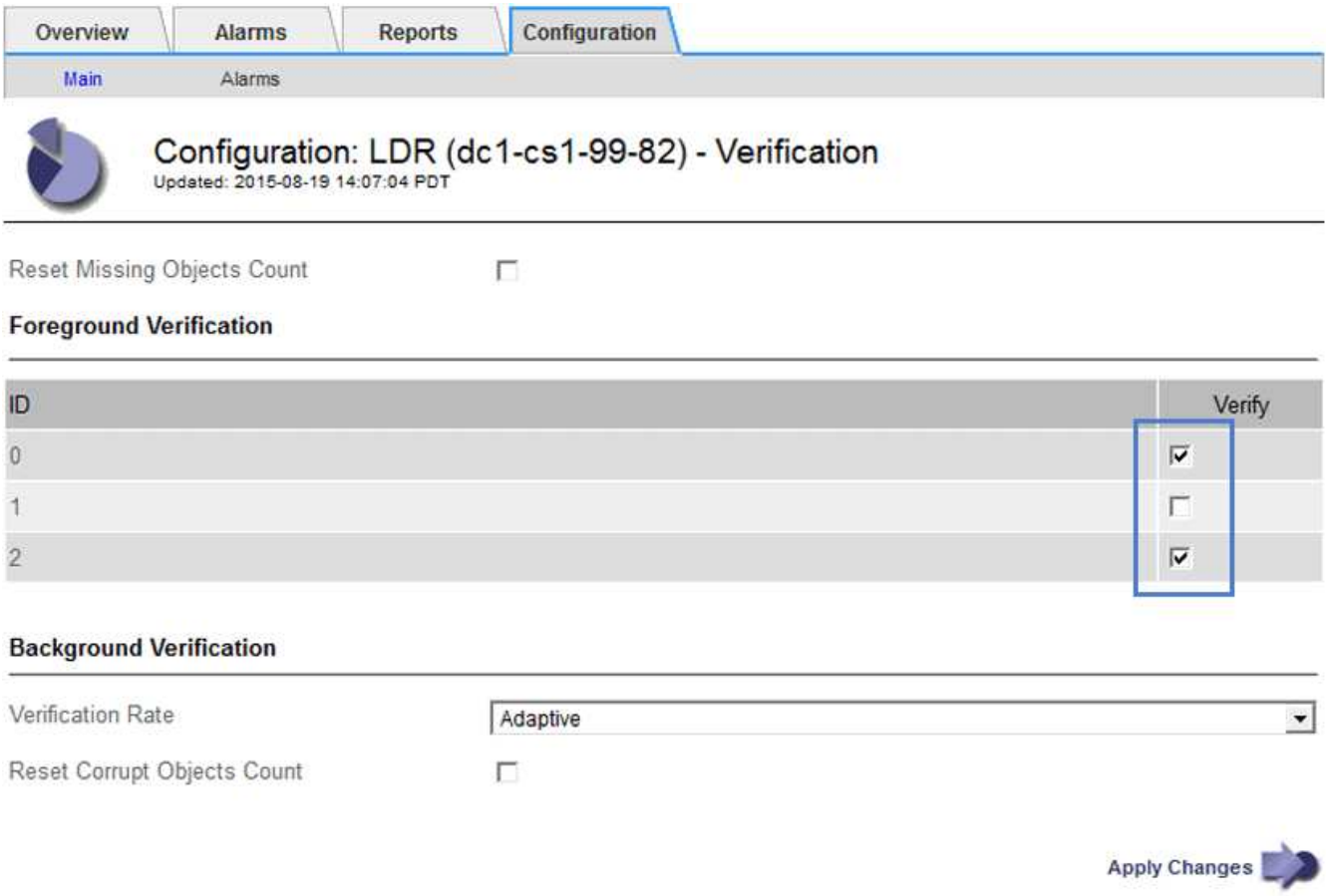
Wenn die Vordergrundüberprüfung fehlende Objektdaten findet, versucht das StorageGRID-System, sie zu ersetzen. Wenn keine Ersatzkopie erstellt werden kann, kann der Alarm „VERLORENE Objekte“ ausgelöst werden.

Die Vordergrundüberprüfung generiert eine LDR-Vordergrundverifizierung, die je nach Anzahl der auf einem Storage-Node gespeicherten Objekte Tage- oder wochenlang dauern kann. Es ist möglich, mehrere Storage-Nodes gleichzeitig auszuwählen. Diese Grid-Aufgaben werden jedoch nicht gleichzeitig ausgeführt. Stattdessen werden sie in eine Warteschlange gestellt und bis zum Abschluss nacheinander ausgeführt. Wenn die Vordergrundüberprüfung auf einem Storage-Node ausgeführt wird, können Sie auf diesem Storage-Node keine andere Überprüfungsaufgabe im Vordergrund starten, obwohl die Option zum Überprüfen zusätzlicher Volumes für den Storage-Node möglicherweise verfügbar ist.

Wenn ein anderer Storage-Node als der, auf dem die Vordergrundüberprüfung ausgeführt wird, offline geschaltet wird, wird die Grid-Aufgabe weiter ausgeführt, bis das Attribut **% complete** 99.99 Prozent erreicht. Das Attribut **% complete** wird dann auf 50 Prozent zurückgestellt und wartet, bis der Speicherknoten wieder in den Online-Status zurückkehrt. Wenn der Status des Speicherknotens wieder online geschaltet wird, wird die Grid-Aufgabe für die Überprüfung des LDR-Vordergrunds fortgesetzt, bis sie abgeschlossen ist.

Schritte

1. Wählen Sie ***Storage Node*** > **LDR** > **Verifizierung** aus.
2. Wählen Sie **Konfiguration** > **Main**.
3. Aktivieren Sie unter **Vordergrundüberprüfung** das Kontrollkästchen für jede Speicher-Volume-ID, die Sie überprüfen möchten.



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

   Warten Sie, bis die Seite automatisch aktualisiert und neu geladen wird, bevor Sie die Seite verlassen. Sobald die Aktualisierung abgeschlossen ist, stehen Objektspeicher zur Auswahl auf diesem Speicherknoten nicht mehr zur Verfügung.

   Eine LDR-Vordergrundüberprüfungsraster-Aufgabe wird erstellt und ausgeführt, bis sie abgeschlossen, unterbrochen oder abgebrochen wird.

5. Fehlende Objekte oder fehlende Fragmente überwachen:

   a. Wählen Sie ***Storage Node*** > **LDR** > **Verifizierung** aus.

   b. Notieren Sie auf der Registerkarte Übersicht unter **Ergebnisse der Überprüfung** den Wert von **fehlenden Objekten erkannt**.

      Hinweis: Der gleiche Wert wird auf der Seite Knoten als **Lost Objects** angegeben. Gehen Sie zu **Nodes** > ***Storage Node*** und wählen Sie die Registerkarte **Objects** aus.

      Wenn die Anzahl der **fehlenden Objekte erkannt** groß ist (wenn Hunderte von fehlenden Objekten vorhanden sind), liegt wahrscheinlich ein Problem mit dem Speicher des Speicherknoten vor. Wenden Sie sich an den technischen Support.

   c. Wählen Sie ***Storage Node*** > **LDR** > **Erasure Coding** aus.

   d. Notieren Sie auf der Registerkarte Übersicht unter **Ergebnisse der Überprüfung** den Wert von **fehlenden Fragmenten erkannt**.

      Wenn die Anzahl **fehlendes Fragment** groß ist (wenn hunderte von fehlenden Fragmenten vorhanden

sind), liegt wahrscheinlich ein Problem mit dem Speicher des Speicherknoten vor. Wenden Sie sich an den technischen Support.

Wenn die Vordergrundüberprüfung keine beträchtliche Anzahl an fehlenden replizierten Objektkopien oder eine beträchtliche Anzahl an fehlenden Fragmenten erkennt, funktioniert der Speicher normal.

6. Überwachen Sie den Abschluss der Vordergrundüberprüfungsraster-Aufgabe:
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann **site** > ***Admin Node*** > **CMN** > **Grid Task** > **Übersicht** > **Main**.
   b. Stellen Sie sicher, dass das Raster für die Vordergrundverifizierung fehlerfrei fortschreitet.

      Hinweis: Bei Unterbrechung des Vordergrundverifizierungsgitters wird ein Alarm auf Notice-Ebene am Grid Task Status (SCAS) ausgelöst.

   c. Wenn die Rasteraufgabe mit einem angehalten wird `critical storage error`, Das betroffene Volumen wiederherstellen und dann die Vordergrundüberprüfung auf den verbleibenden Volumes ausführen, um auf zusätzliche Fehler zu überprüfen.

      Achtung: Wenn die Aufgabe Vordergrundverifizierung mit der Meldung unterbricht `Encountered a critical storage error in volume volID`, Sie müssen das Verfahren für die Wiederherstellung eines fehlerhaften Speichervolume. Weitere Informationen finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **LDR** > **Verifizierung** > **Konfiguration** > **Main** und erhöhen Sie die Hintergrundverifizierungsrate. Die Hintergrundüberprüfung überprüft die Richtigkeit aller gespeicherten Objektdaten und repariert sämtliche gefundenen Probleme. Das schnelle Auffinden und Reparieren potenzieller Probleme verringert das Risiko von Datenverlusten.

Verwandte Informationen

"Verwalten Sie erholen"

Fehlerbehebung verloren gegangene und fehlende Objektdaten

Objekte können aus verschiedenen Gründen abgerufen werden, darunter Leseanforderungen von einer Client-Applikation, Hintergrundverifizierungen replizierter Objektdaten, ILM-Neubewertungen und die Wiederherstellung von Objektdaten während der Recovery eines Storage Node.

Das StorageGRID System verwendet Positionsinformationen in den Metadaten eines Objekts, um von welchem Speicherort das Objekt abzurufen. Wenn eine Kopie des Objekts nicht am erwarteten Speicherort gefunden wird, versucht das System, eine andere Kopie des Objekts von einer anderen Stelle im System abzurufen, vorausgesetzt, die ILM-Richtlinie enthält eine Regel zum Erstellen von zwei oder mehr Kopien des Objekts.

Wenn der Abruf erfolgreich ist, ersetzt das StorageGRID System die fehlende Kopie des Objekts. Andernfalls werden die Warnung **Objekte verloren** und der Alarm für verlorene Objekte (verlorene Objekte) ausgelöst, wie folgt:

- Wenn bei replizierten Kopien eine andere Kopie nicht abgerufen werden kann, gilt das Objekt als verloren, und die Warnung und der Alarm werden ausgelöst.

- Wenn beim Löschen codierter Kopien eine Kopie nicht vom erwarteten Speicherort abgerufen werden kann, wird das Attribut „Corrupt Copies Detected (ECOR)“ um eins erhöht, bevor versucht wird, eine Kopie von einem anderen Speicherort abzurufen. Wenn keine weitere Kopie gefunden wird, werden die Warnung und der Alarm ausgelöst.

Sie sollten alle **Objekte Lost**-Warnungen sofort untersuchen, um die Ursache des Verlusts zu ermitteln und zu ermitteln, ob das Objekt noch in einem Offline-oder anderweitig derzeit nicht verfügbar ist, Storage Node oder Archive Node.

Wenn Objekt-Daten ohne Kopien verloren gehen, gibt es keine Recovery-Lösung. Sie müssen jedoch den Zähler „Lost Object“ zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren.

Verwandte Informationen

"Untersuchung verlorener Objekte"

"Zurücksetzen verlorener und fehlender Objektanzahl"

Untersuchung verlorener Objekte

Wenn der Alarm * Objects lost* und der Alarm Legacy LOST Objects (Lost Objects) ausgelöst werden, müssen Sie sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Die Warnung **Objekte verloren** und der VERLORENE Alarm zeigen an, dass StorageGRID der Ansicht ist, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

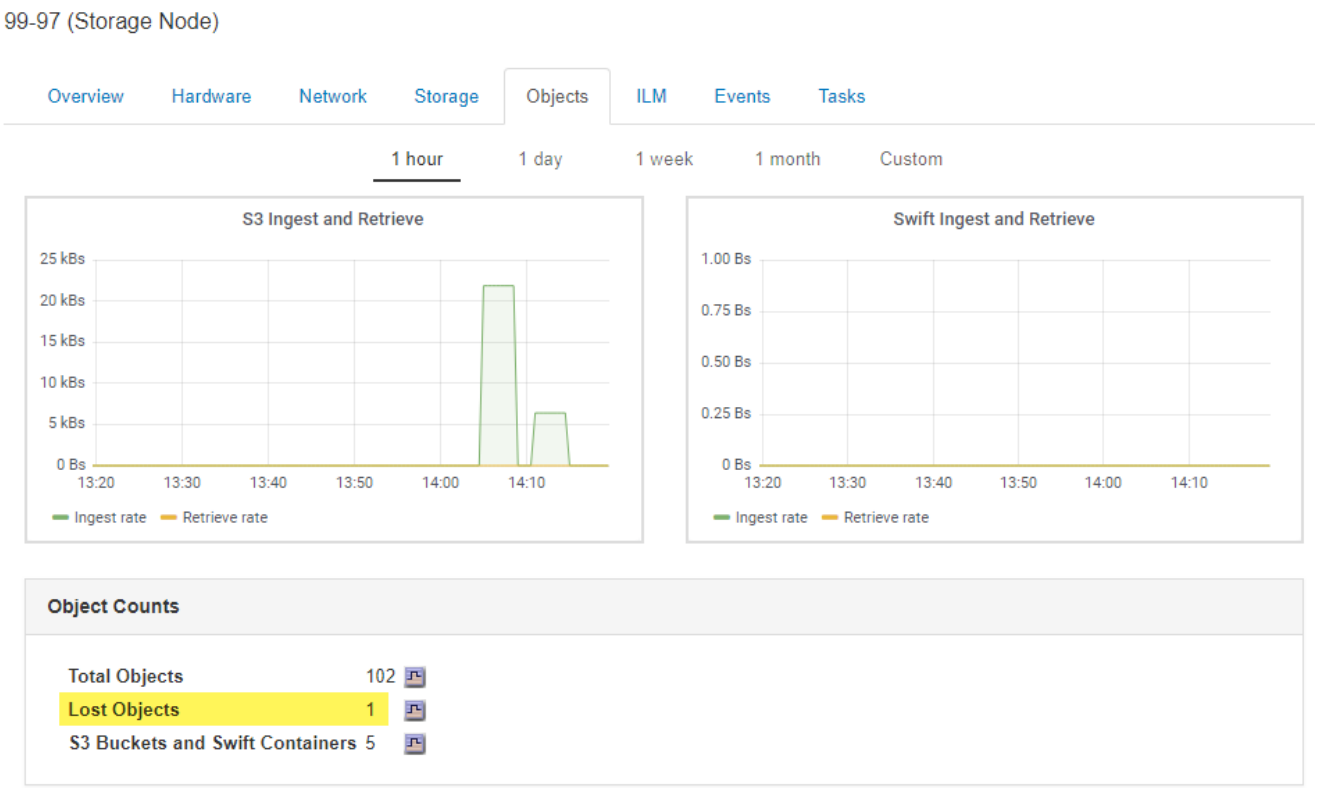
Untersuchen Sie verlorene Objektalarme oder -Warnmeldungen sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. In einigen Fällen können Sie ein verlorenes Objekt wiederherstellen, wenn Sie eine sofortige Aktion ausführen.

Die Anzahl der verlorenen Objekte kann im Grid Manager angezeigt werden.

Schritte

1. Wählen Sie **Knoten**.
2. Wählen Sie ***Speicherknoten*** > **Objekte** Aus.
3. Überprüfen Sie die Anzahl der in der Tabelle Objektanzahl angezeigten verlorenen Objekte.

   Diese Nummer gibt die Gesamtzahl der Objekte an, die dieser Grid-Node im gesamten StorageGRID-System als fehlend erkennt. Der Wert ist die Summe der Zähler Lost Objects der Data Store Komponente innerhalb der LDR- und DDS-Dienste.



4. Greifen Sie von einem Admin-Node aus auf das Audit-Protokoll zu, um die eindeutige Kennung (UUID) des Objekts zu bestimmen, das die Meldung **Objekte verloren** und DEN VERLORENEN Alarm ausgelöst hat:
   a. Melden Sie sich beim Grid-Node an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
   b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden. Geben Sie Ein: `cd /var/local/audit/export/`
   c. Verwenden Sie grep, um die Audit-Meldungen zu „Objekt verloren“ (OLST) zu extrahieren. Geben Sie Ein: `grep OLST audit_file_name`
   d. Beachten Sie den in der Meldung enthaltenen UUID-Wert.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Verwenden Sie die `ObjectByUUID` Befehl zum Suchen des Objekts anhand seiner ID (UUID) und bestimmen Sie, ob die Daten gefährdet sind.

   a. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole.

   b. Geben Sie Ein: `/proc/OBRP/ObjectByUUID UUID_value`

      In diesem ersten Beispiel, das Objekt mit `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` Hat zwei Standorte aufgelistet.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
```

```
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

Im zweiten Beispiel das Objekt mit `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` Hat keine Standorte aufgelistet.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Überprüfen Sie die Ausgabe von /proc/OBRP/ObjectByUUID, und ergreifen Sie die entsprechenden Maßnahmen:

Metadaten	Schlussfolgerung
Kein Objekt gefunden („FEHLER“:“)	Wenn das Objekt nicht gefunden wird, wird die Meldung „FEHLER“:“ zurückgegeben. Wenn das Objekt nicht gefunden wird, kann der Alarm sicher ignoriert werden. Das Fehlen eines Objekts bedeutet, dass das Objekt absichtlich gelöscht wurde.
Standorte 0	Wenn im Ausgang Positionen aufgeführt sind, kann der Alarm Lost Objects falsch positiv sein. Vergewissern Sie sich, dass die Objekte vorhanden sind. Verwenden Sie die Knoten-ID und den Dateipfad, der in der Ausgabe aufgeführt ist, um zu bestätigen, dass sich die Objektdatei am aufgelisteten Speicherort befindet. (Das Verfahren zum Auffinden potenziell verlorener Objekte erläutert, wie Sie die Node-ID verwenden, um den richtigen Storage-Node zu finden.) "Suche nach und Wiederherstellung möglicherweise verlorenen Objekten" Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um den Alarm und die Warnung zu löschen.
Standorte = 0	Wenn in der Ausgabe keine Positionen aufgeführt sind, fehlt das Objekt möglicherweise. Sie können versuchen, das Objekt selbst zu finden und wiederherzustellen, oder Sie können sich an den technischen Support wenden. "Suche nach und Wiederherstellung möglicherweise verlorenen Objekten" Vom technischen Support bitten Sie möglicherweise, zu bestimmen, ob ein Verfahren zur Storage-Recovery durchgeführt wird. Das heißt, wurde auf jedem Storage Node ein Befehl „ *Repair-Data*“ ausgegeben, und läuft die Recovery noch? Weitere Informationen zum Wiederherstellen von Objektdaten auf einem Storage-Volume finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.

Verwandte Informationen

"Verwalten Sie erholen"

"Prüfung von Audit-Protokollen"

Suche nach und Wiederherstellung möglicherweise verlorenen Objekten

Möglicherweise können Objekte gefunden und wiederhergestellt werden, die einen Alarm

„Lost Objects“ (LOST Objects – LOST) und einen „Object Lost*“-Alarm ausgelöst haben und die Sie als „potentiell verloren“ identifiziert haben.

Was Sie benötigen

- Sie müssen über die UUID eines verlorenen Objekts verfügen, wie in „`Untersuchung verlorener Objekte`“ angegeben.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Im Anschluss an dieses Verfahren können Sie sich nach replizierten Kopien des verlorenen Objekts an einer anderen Stelle im Grid suchen. In den meisten Fällen wird das verlorene Objekt nicht gefunden. In einigen Fällen können Sie jedoch ein verlorenes repliziertes Objekt finden und wiederherstellen, wenn Sie umgehend Maßnahmen ergreifen.

Wenden Sie sich an den technischen Support, wenn Sie Hilfe bei diesem Verfahren benötigen.

Schritte

1. Suchen Sie in einem Admin-Knoten die Prüfprotokolle nach möglichen Objektspeichern:
   a. Melden Sie sich beim Grid-Node an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
   b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`
   c. Verwenden Sie grep, um die mit dem potenziell verlorenen Objekt verknüpften Audit-Nachrichten zu extrahieren und sie an eine Ausgabedatei zu senden. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

      Beispiel:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. Verwenden Sie grep, um die Meldungen zum Lost Location (LLST) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep LLST output_file_name`

      Beispiel:

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      Eine LLST-Überwachungsmeldung sieht wie diese Beispielmeldung aus.

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. Suchen Sie in der LLST-Meldung das Feld PCLD und das Feld NOID.

Falls vorhanden, ist der Wert von PCLD der vollständige Pfad auf der Festplatte zur fehlenden replizierten Objektkopie. Der Wert von NOID ist die Knoten-id des LDR, wo eine Kopie des Objekts gefunden werden kann.

Wenn Sie einen Speicherort für ein Objekt finden, kann das Objekt möglicherweise wiederhergestellt werden.

f. Suchen Sie den Speicherknoten für diese LDR-Knoten-ID.

Es gibt zwei Möglichkeiten, die Node-ID zum Suchen des Storage Node zu verwenden:

- Wählen Sie im Grid Manager die Option **Support** > **Tools** > **Grid Topology** aus. Wählen Sie dann ***Data Center*** > ***Storage Node*** > **LDR** aus. Die LDR-Knoten-ID befindet sich in der Node-Informationstabelle. Überprüfen Sie die Informationen für jeden Speicherknoten, bis Sie den gefunden haben, der dieses LDR hostet.
- Laden Sie das Wiederherstellungspaket für das Grid herunter und entpacken Sie es. Das PAKET enthält ein Verzeichnis *\docs*. Wenn Sie die Datei index.html öffnen, zeigt die Serverübersicht alle Knoten-IDs für alle Grid-Knoten an.

2. Stellen Sie fest, ob das Objekt auf dem in der Meldung „Audit“ angegebenen Speicherknoten vorhanden ist:

a. Melden Sie sich beim Grid-Node an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

b. Stellen Sie fest, ob der Dateipfad für das Objekt vorhanden ist.

Verwenden Sie für den Dateipfad des Objekts den Wert von PCLD aus der LLST-Überwachungsmeldung.

Geben Sie beispielsweise Folgendes ein:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Hinweis: Fügen Sie den Objektdateipfad immer in einzelne Anführungszeichen, um Sonderzeichen zu entkommen.

- Wenn der Objektpfad nicht gefunden wurde, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wurde, fahren Sie mit Schritt fort Stellen Sie das Objekt in StorageGRID wieder her. Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.

1. Wenn der Objektpfad gefunden wurde, versuchen Sie, das Objekt in StorageGRID wiederherzustellen:
   a. Ändern Sie vom gleichen Speicherknoten aus die Eigentumsrechte an der Objektdatei, so dass sie von StorageGRID gemanagt werden kann. Geben Sie Ein: `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole. Geben Sie Ein: `telnet 0 1402`
   c. Geben Sie Ein: `cd /proc/STOR`
   d. Geben Sie Ein: `Object_Found 'file_path_of_object'`

      Geben Sie beispielsweise Folgendes ein:

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Ausstellen der `Object\_Found` Durch den Befehl wird das Raster des Speicherorts des Objekts benachrichtigt. Zudem wird die aktive ILM-Richtlinie ausgelöst, die zusätzliche Kopien gemäß den Angaben in der Richtlinie erstellt.

      Hinweis: Wenn der Speicherknoten, in dem Sie das Objekt gefunden haben, offline ist, können Sie das Objekt auf einen beliebigen Speicherknoten kopieren, der online ist. Platzieren Sie das Objekt in einem beliebigen /var/local/rangedb-Verzeichnis des Online-Storage-Node. Geben Sie dann den aus `Object\_Found` Befehl mit diesem Dateipfad zum Objekt.

      - Wenn das Objekt nicht wiederhergestellt werden kann, wird das angezeigt `Object\_Found` Befehl schlägt fehl. Wenden Sie sich an den technischen Support.
      - Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, wird eine Erfolgsmeldung angezeigt. Beispiel:

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

      Mit Schritt fortfahren Überprüfen Sie, ob neue Standorte erstellt wurden

1. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, vergewissern Sie sich, dass neue

Speicherorte erstellt wurden.

a. Geben Sie Ein: `cd /proc/OBRP`

b. Geben Sie Ein: `ObjectByUUID UUID_value`

   Das folgende Beispiel zeigt, dass es zwei Standorte für das Objekt mit UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 gibt.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
```

```
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Melden Sie sich von der LDR-Konsole ab. Geben Sie Ein: `exit`

2. Durchsuchen Sie von einem Admin-Node aus die Prüfprotokolle für die ORLM-Überwachungsmeldung für dieses Objekt, um zu bestätigen, dass Information Lifecycle Management (ILM) Kopien nach Bedarf platziert hat.

   a. Melden Sie sich beim Grid-Node an:

      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

   b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`

   c. Verwenden Sie grep, um die mit dem Objekt verknüpften Überwachungsmeldungen in eine Ausgabedatei zu extrahieren. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

      Beispiel:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_restored_object.txt
      ```

   d. Verwenden Sie grep, um die ORLM-Audit-Meldungen (Object Rules met) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep ORLM output_file_name`

      Beispiel:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

Eine ORLM-Überwachungsmeldung sieht wie diese Beispielmeldung aus.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Suchen Sie das FELD LOKS in der Überwachungsmeldung.

   Wenn vorhanden, ist der Wert von CLDI in LOCS die Node-ID und die Volume-ID, in der eine Objektkopie erstellt wurde. Diese Meldung zeigt, dass das ILM angewendet wurde und dass an zwei Standorten im Grid zwei Objektkopien erstellt wurden.

b. Setzen Sie die Anzahl der verlorenen Objekte im Grid Manager zurück.

Verwandte Informationen

"Untersuchung verlorener Objekte"

"Bestätigen der Speicherorte von Objektdaten"

"Zurücksetzen verlorener und fehlender Objektanzahl"

"Prüfung von Audit-Protokollen"

Zurücksetzen verlorener und fehlender Objektanzahl

Nachdem Sie das StorageGRID-System untersucht und überprüft haben, ob alle aufgezeichneten verlorenen Objekte dauerhaft verloren gehen oder dass es sich um einen falschen Alarm handelt, können Sie den Wert des Attributs Lost Objects auf Null zurücksetzen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

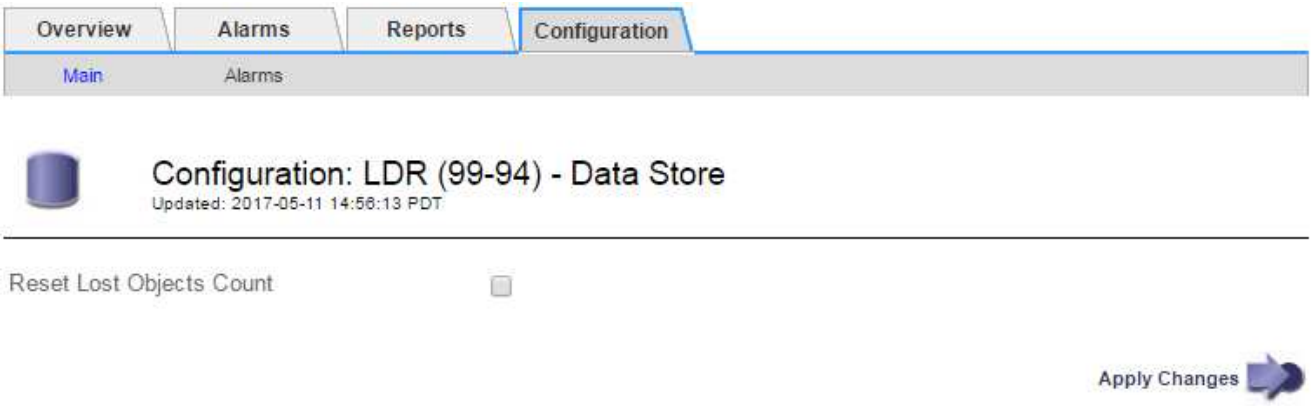
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **Support** > **Tools** > **Grid Topology** > ***site*** **>** ***Storage Node*** > **LDR** > **Data Store** > **Übersicht** > **Main**
- **Support** > **Tools** > **Grid Topology** > ***site*** **>** ***Storage Node*** > **DDS** > **Data Store** > **Übersicht** > **Main**

Diese Anleitung zeigt das Zurücksetzen des Zählers von der Seite **LDR** > **Data Store**.

Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***Site* > *Storage Node*** > **LDR** > **Data Store** > **Konfiguration** für den Speicherknoten, der die Meldung **Objekte verloren** oder DEN VERLORENEN Alarm hat.
3. Wählen Sie **Anzahl Der Verlorenen Objekte Zurücksetzen**.



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

   Das Attribut Lost Objects wird auf 0 zurückgesetzt und die Warnung **Objects lost** und DIE VERLORENE Alarmfunktion werden gelöscht, was einige Minuten dauern kann.

5. Setzen Sie optional andere zugehörige Attributwerte zurück, die beim Identifizieren des verlorenen Objekts möglicherweise erhöht wurden.

   a. Wählen Sie ***Site* > *Storage Node*** > **LDR** > **Erasure Coding** > **Konfiguration** aus.
   b. Wählen Sie **Reset reads Failure Count** und **Reset corrupte Kopien Detected Count** aus.
   c. Klicken Sie Auf **Änderungen Übernehmen**.
   d. Wählen Sie ***Site* > *Storage Node*** > **LDR** > **Verifizierung** > **Konfiguration**.
   e. Wählen Sie **Anzahl der fehlenden Objekte zurücksetzen** und **Anzahl der beschädigten Objekte zurücksetzen**.
   f. Wenn Sie sicher sind, dass keine isolierten Objekte erforderlich sind, können Sie **Quarantäne-Objekte löschen** auswählen.

      Isolierte Objekte werden erstellt, wenn die Hintergrundüberprüfung eine beschädigte replizierte Objektkopie identifiziert. In den meisten Fällen ersetzt StorageGRID das beschädigte Objekt automatisch, und es ist sicher, die isolierten Objekte zu löschen. Wenn jedoch die Meldung **Objects lost** oder DER VERLORENE Alarm ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen.

   g. Klicken Sie Auf **Änderungen Übernehmen**.

   Es kann einige Momente dauern, bis die Attribute zurückgesetzt werden, nachdem Sie auf **Änderungen anwenden** klicken.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei der Warnung „niedriger Objektdatenspeicher“

Der Alarm * Low Object Data Storage* überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Storage Node verfügbar ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Der **Low Object Datenspeicher** wird ausgelöst, wenn die Gesamtzahl der replizierten und Erasure codierten Objektdaten auf einem Storage Node eine der Bedingungen erfüllt, die in der Warnungsregel konfiguriert sind.

Standardmäßig wird eine wichtige Warnmeldung ausgelöst, wenn diese Bedingung als „true“ bewertet wird:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In diesem Zustand:

- `storagegrid_storage_utilization_data_bytes` Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten für einen Storage-Node
- `storagegrid_storage_utilization_usable_space_bytes` Ist die Gesamtmenge an verbleibendem Objekt-Speicherplatz für einen Storage-Node.

Wenn ein Major oder Minor **Low Object Data Storage**-Alarm ausgelöst wird, sollten Sie so schnell wie möglich eine Erweiterung durchführen.

Schritte

1. Wählen Sie **Alarme** > **Aktuell**.

   Die Seite „Meldungen“ wird angezeigt.

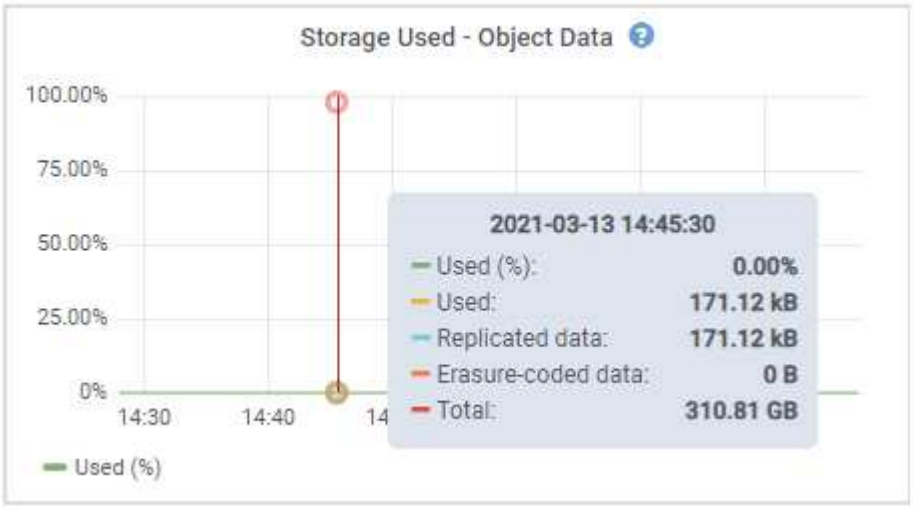
2. Erweitern Sie bei Bedarf aus der Warnmeldungstabelle die Warnungsgruppe **Low Object Data Storage** und wählen Sie die Warnung aus, die angezeigt werden soll.

   Wählen Sie die Meldung und nicht die Überschrift einer Gruppe von Warnungen aus.

3. Überprüfen Sie die Details im Dialogfeld, und beachten Sie Folgendes:
   - Auslösezeit
   - Der Name des Standorts und des Nodes
   - Die aktuellen Werte der Metriken für diese Meldung
4. Wählen Sie **Nodes** > ***Storage Node oder Standort*** > **Storage** aus.
5. Bewegen Sie den Mauszeiger über das Diagramm „verwendete Daten – Objektdaten“.

   Die folgenden Werte werden angezeigt:

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



6. Wählen Sie die Zeitsteuerelemente über dem Diagramm aus, um die Speichernutzung über verschiedene Zeiträume anzuzeigen.

   Mit einem Blick auf die Storage-Nutzung im Laufe der Zeit können Sie nachvollziehen, wie viel Storage vor und nach der Warnmeldung genutzt wurde, und Sie können schätzen, wie lange es dauern könnte, bis der verbleibende Speicherplatz des Node voll ist.

7. So bald wie möglich, ein Erweiterungsverfahren für zusätzliche Speicherkapazität durchführen.

   Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen.

   Informationen zum Verwalten eines vollständigen Speicherknoten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"Fehlerbehebung beim SSTS-Alarm (Storage Status)"

"Erweitern Sie Ihr Raster"

"StorageGRID verwalten"

Fehlerbehebung beim SSTS-Alarm (Storage Status)

Der SSTS-Alarm (Storage Status) wird ausgelöst, wenn ein Speicherknoten über nicht

genügend freien Speicherplatz für den Objektspeicher verfügt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Der SSTS-Alarm (Speicherstatus) wird auf Notice-Ebene ausgelöst, wenn die Menge an freiem Speicherplatz auf jedem Volume in einem Speicherknoten unter den Wert des Speichervolumen-Soft-Read-Only-Wasserzeichens (**Konfiguration Speicheroptionen Übersicht**) fällt.

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

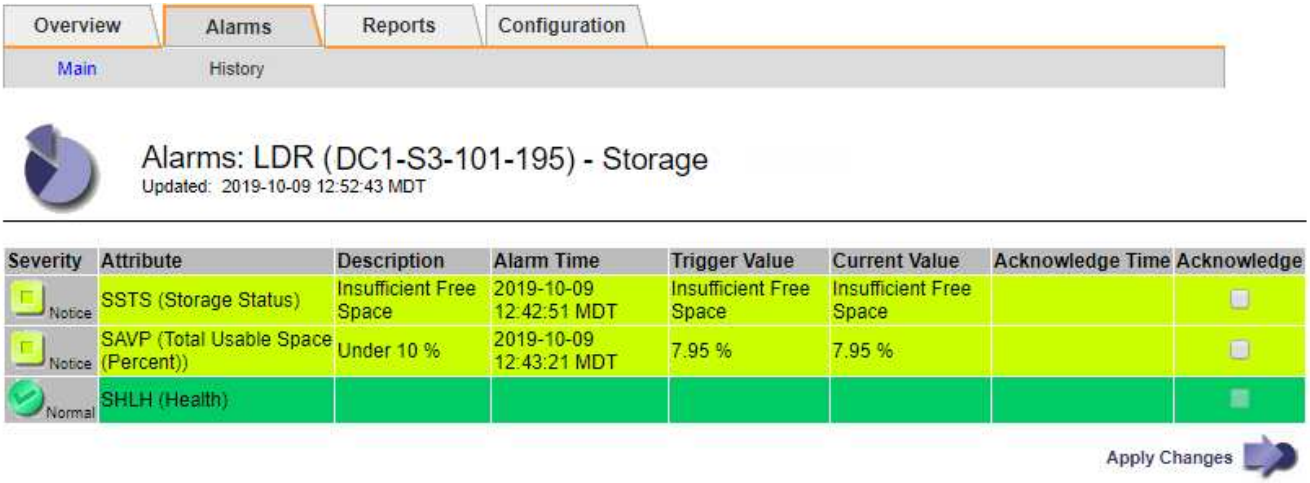
Angenommen, das Speichervolumen-Soft-Read-Only-Wasserzeichen ist auf 10 GB gesetzt, das ist der Standardwert. Der SSTS-Alarm wird ausgelöst, wenn auf jedem Speicher-Volume im Storage-Node weniger als 10 GB nutzbarer Speicherplatz verbleibt. Wenn eines der Volumes über 10 GB oder mehr verfügbaren Speicherplatz verfügt, wird der Alarm nicht ausgelöst.

Wenn ein SSTS-Alarm ausgelöst wurde, können Sie diese Schritte ausführen, um das Problem besser zu verstehen.

Schritte

1. Wählen Sie **Support** > **Alarme (alt)** > **Aktuelle Alarme**.
2. Wählen Sie in der Spalte Service das Rechenzentrum, den Node und den Service aus, die dem SSTS-Alarm zugeordnet sind.

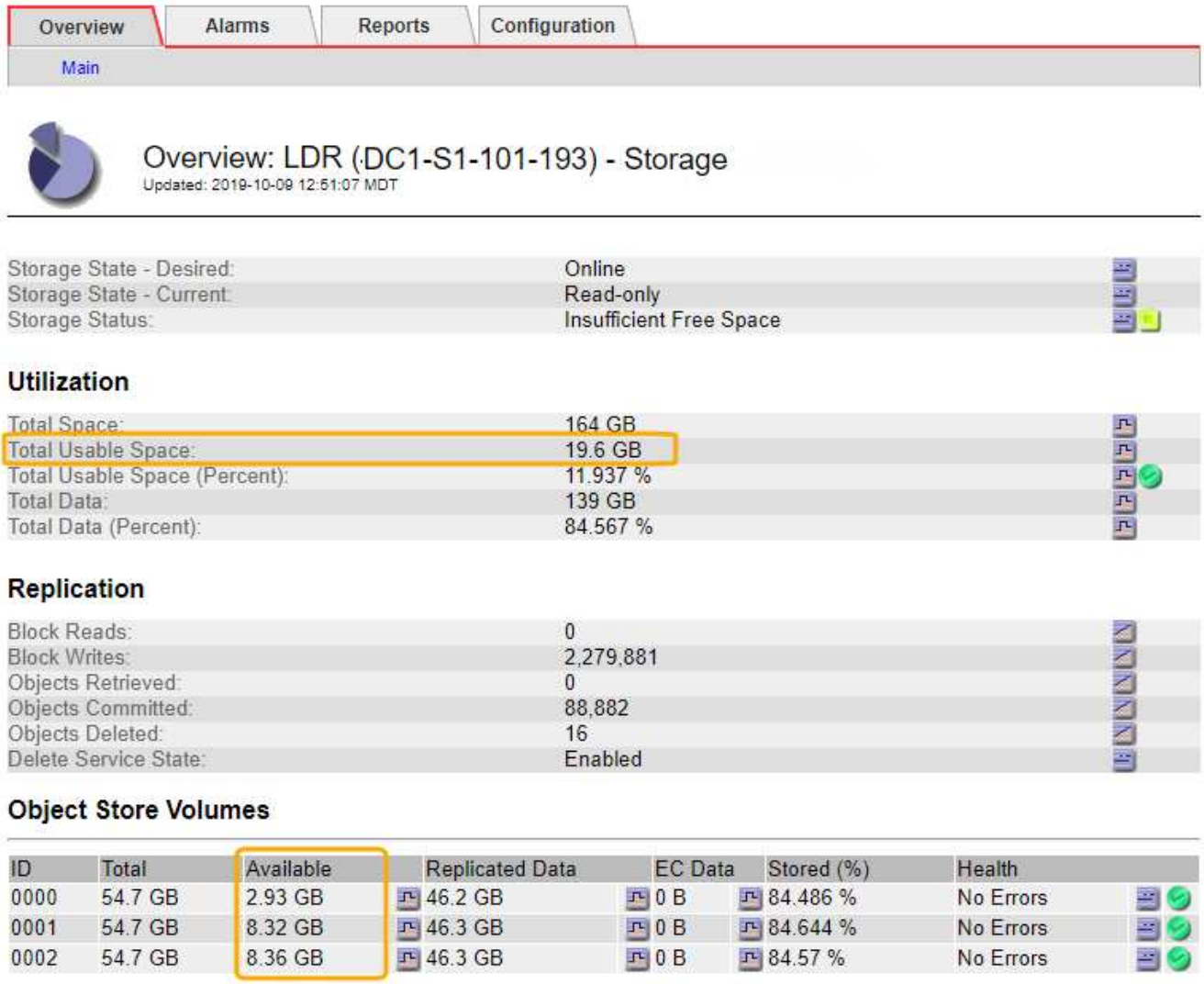
   Die Seite Grid Topology wird angezeigt. Auf der Registerkarte „Alarme“ werden die aktiven Alarme für den ausgewählten Knoten und Dienst angezeigt.



In diesem Beispiel wurden sowohl die SSTS-Alarme (Speicherstatus) als auch die SAVP (Total Usable Space (Prozent)) auf der Notice-Ebene ausgelöst.

> Typischerweise werden sowohl der SSTS-Alarm als auch der SAVP-Alarm etwa gleichzeitig ausgelöst. Ob jedoch beide Alarme ausgelöst werden, hängt von der Wasserzeichen-Einstellung in GB und der SAVP-Alarmeinstellung in Prozent ab.

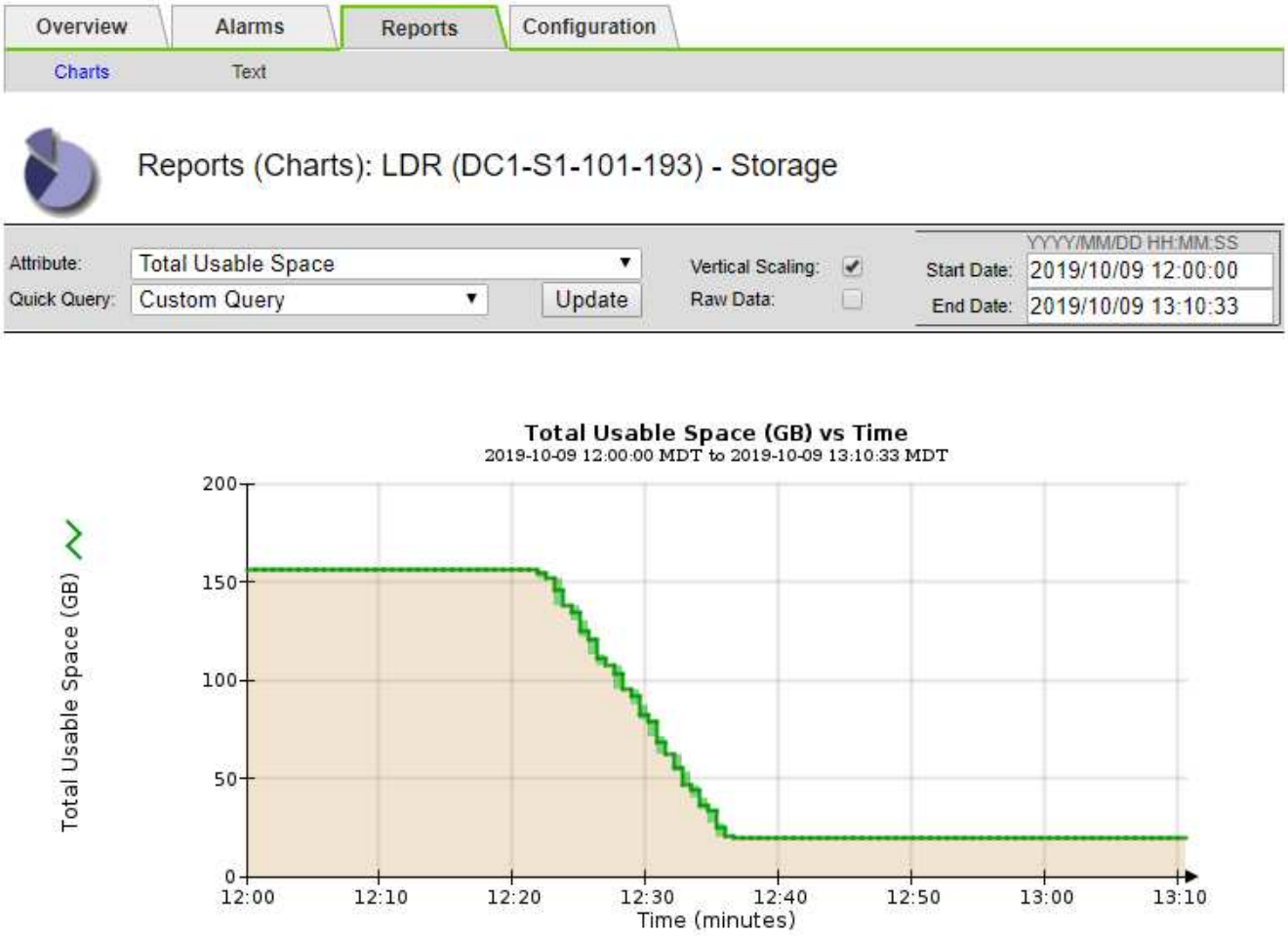
3. Um festzustellen, wie viel nutzbarer Speicherplatz tatsächlich verfügbar ist, wählen Sie **LDR Storage Übersicht**, und suchen Sie das Attribut Total Usable Space (STAS).



In diesem Beispiel bleiben nur 19.6 GB des 164 GB Speicherplatzes auf diesem Speicherknoten verfügbar. Beachten Sie, dass der Gesamtwert die Summe der **verfügbaren**-Werte für die drei Objektspeicher-Volumes ist. Der SSTS-Alarm wurde ausgelöst, weil jedes der drei Speicher-Volumes weniger als 10 GB verfügbaren Speicherplatz hatte.

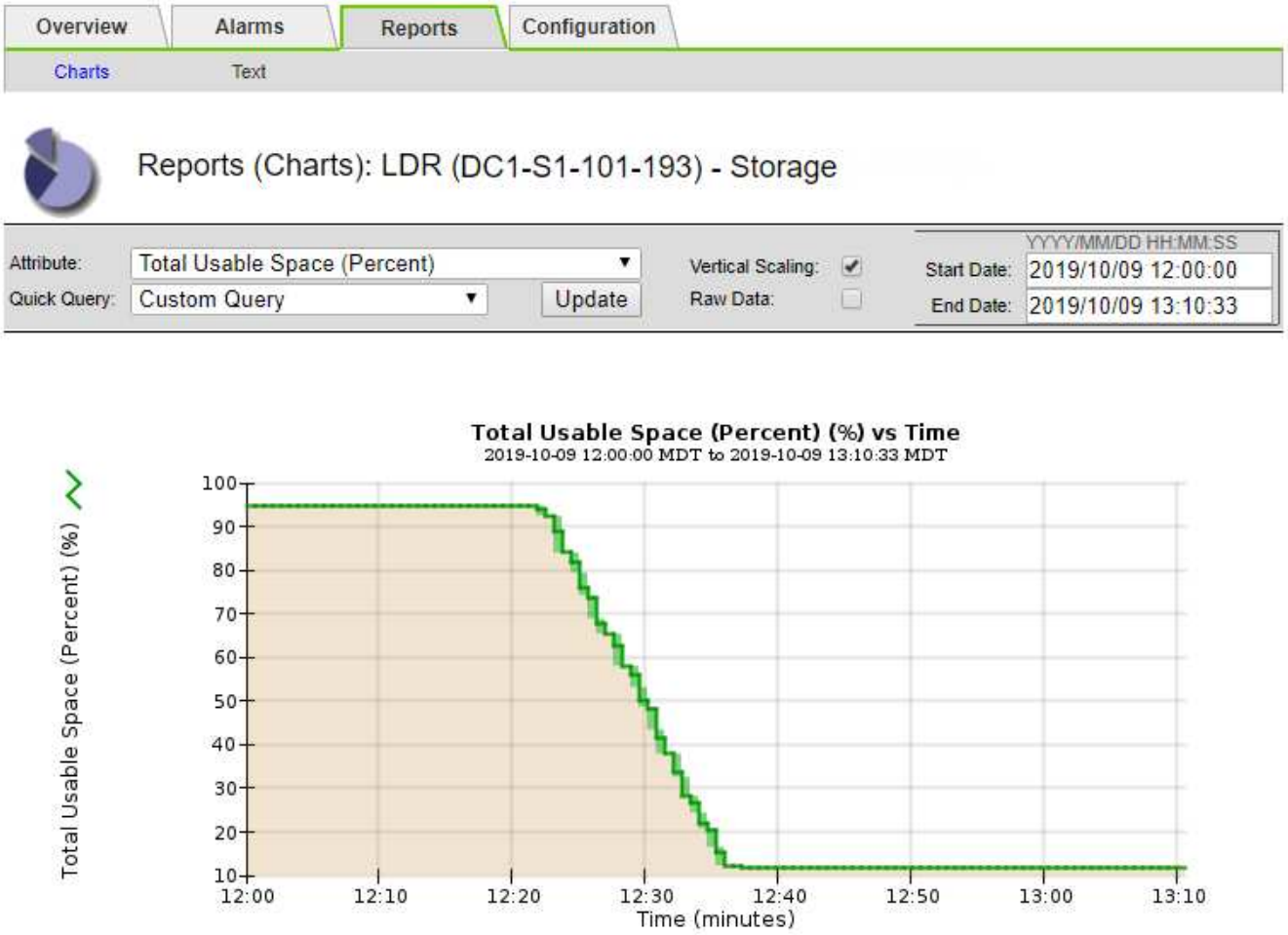
4. Um zu verstehen, wie Speicher im Laufe der Zeit genutzt wurde, wählen Sie die Registerkarte **Berichte** und zeichnen den gesamten nutzbaren Speicherplatz in den letzten Stunden.

   In diesem Beispiel sank der gesamte nutzbare Speicherplatz von etwa 155 GB bei 12:00 auf 20 GB bei 12:35, was der Zeit entspricht, zu der der SSTS-Alarm ausgelöst wurde.



5. Um zu verstehen, wie Speicher als Prozentsatz der Gesamtmenge genutzt wird, geben Sie den gesamten nutzbaren Speicherplatz (Prozent) in den letzten Stunden an.

   In diesem Beispiel sank der nutzbare Gesamtspeicherplatz von 95 % auf etwa 10 % zur selben Zeit.



6. Bei Bedarf Erweiterung des StorageGRID Systems Storage-Kapazität hinzufügen.

   Anweisungen zum Verwalten eines vollständigen Speicherknoten finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"Erweitern Sie Ihr Raster"

"StorageGRID verwalten"

Fehlerbehebung bei der Bereitstellung von Plattform-Services-Meldungen (SMTT-Alarm)

Der SMTT-Alarm (Total Events) wird im Grid Manager ausgelöst, wenn eine Plattformdienstnachricht an ein Ziel gesendet wird, das die Daten nicht annehmen kann.

Über diese Aufgabe

So kann beispielsweise ein S3-Multipart-Upload erfolgreich sein, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsmeldung nicht an den konfigurierten Endpunkt gesendet werden kann. Alternativ kann eine Nachricht für die CloudMirror Replizierung nicht bereitgestellt werden, wenn die Metadaten zu lang sind.

Der SMTT-Alarm enthält eine Meldung „Letztes Ereignis“, die lautet: `Failed to publish notifications for bucket-name object key` Für das letzte Objekt, dessen Benachrichtigung fehlgeschlagen ist.

Weitere Informationen zur Fehlerbehebung bei Plattform-Services finden Sie in den Anweisungen für die

Administration von StorageGRID. Möglicherweise müssen Sie über den Tenant Manager auf den Mandanten zugreifen, um einen Plattformdienstfehler zu beheben.

Schritte

1. Um den Alarm anzuzeigen, wählen Sie **Nodes *site Grid Node* Events** aus.
2. Letztes Ereignis oben in der Tabelle anzeigen.

   Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

3. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
4. Klicken Sie auf **Ereignisanzahl zurücksetzen**.
5. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.
6. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts auszulösen.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"Referenz für Protokolldateien"

"Ereignisanzahl wird zurückgesetzt"

Behebung von Metadatenproblemen

Sie können verschiedene Aufgaben ausführen, um die Ursache von Metadatenproblemen zu ermitteln.

Fehlerbehebung für Storage-Warnmeldungen bei niedrigen Metadaten

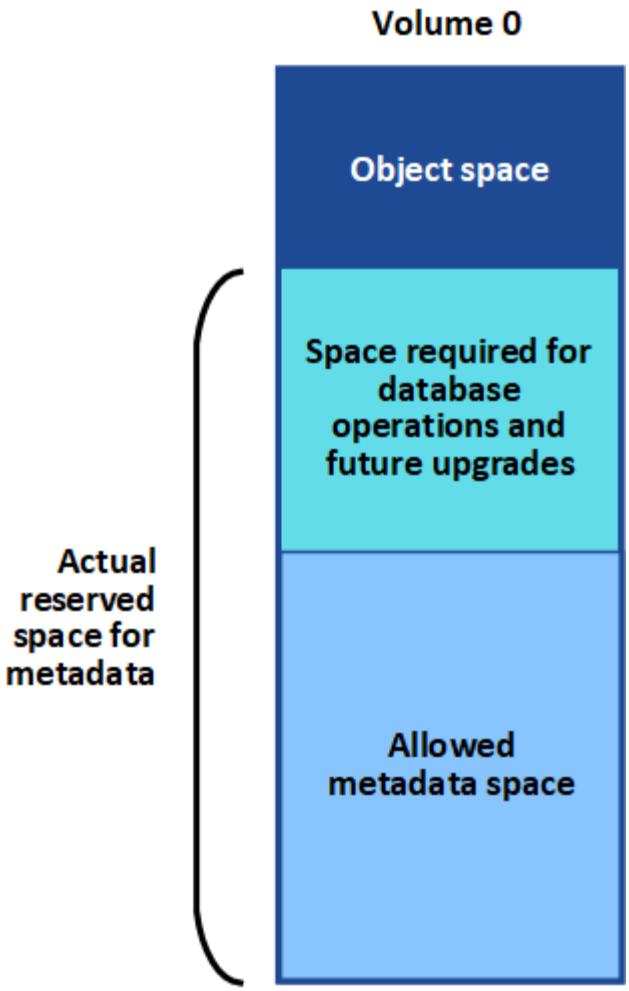
Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

StorageGRID reserviert eine bestimmte Menge an Speicherplatz auf Volume 0 jedes Storage-Nodes für Objekt-Metadaten. Dieser Speicherplatz wird als tatsächlicher reservierter Speicherplatz bezeichnet und in den Speicherplatz für Objekt-Metadaten (zulässiger Metadatenspeicherplatz) und den für wichtige Datenbankvorgänge wie Data-Compaction und Reparatur erforderlichen Speicherplatz unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.



Wenn Objekt-Metadaten mehr als 100 % des für Metadaten zulässigen Speicherplatzes belegen, können Datenbankvorgänge nicht effizient ausgeführt werden und es treten Fehler auf.

StorageGRID verwendet die folgende Prometheus Kennzahl, um den vollen Umfang des zulässigen Metadaten-Speicherplatzes zu messen:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

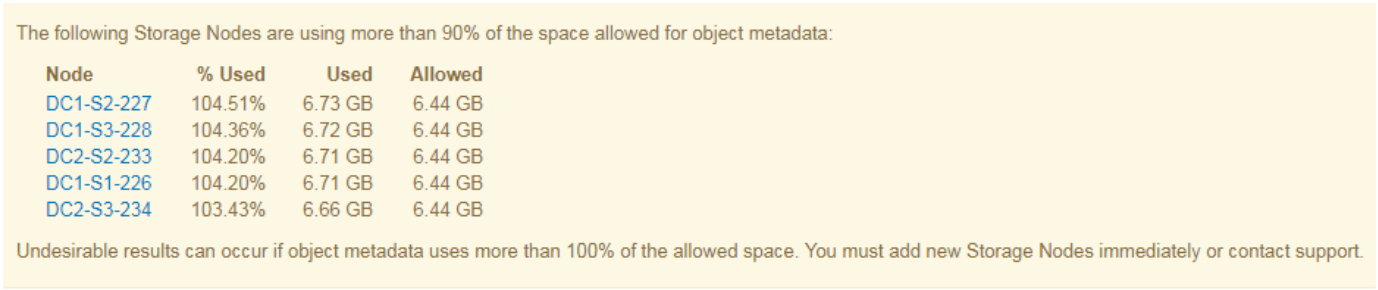
Wenn dieser Prometheus-Ausdruck bestimmte Schwellenwerte erreicht, wird die Warnung **Low Metadaten Storage** ausgelöst.

- **Minor**: Objektmetadaten verwenden 70% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie sollten so bald wie möglich neue Storage-Nodes hinzufügen.
- **Major**: Objektmetadaten verwenden 90% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie müssen sofort neue Storage-Nodes hinzufügen.

> Wenn Objektmetadaten 90 % oder mehr des zulässigen Metadaten-Speicherplatzes beanspruchen, wird im Dashboard eine Warnung angezeigt. Wenn diese Warnung angezeigt wird, müssen Sie sofort neue Speicherknoten hinzufügen. Es ist nicht zulässig, dass Objektmetadaten mehr als 100 % des zulässigen Speicherplatzes nutzen.

- **Kritisch**: Objektmetadaten verbrauchen 100% oder mehr des zulässigen Metadaten-Speicherplatzes und verbrauchen den für wichtige Datenbankvorgänge erforderlichen Speicherplatz. Sie müssen die Aufnahme neuer Objekte beenden und sofort neue Speicherknoten hinzufügen.

In dem folgenden Beispiel belegen die Objektmetadaten mehr als 100 % des zulässigen Metadaten-Speicherplatzes. Hierbei handelt es sich um eine kritische Situation, die zu einem ineffizienten und ineffizienten Datenbankbetrieb und zu Fehlern führt.



Wenn die Größe von Volume 0 kleiner ist als die Option „Metadatenreservierter Speicherplatz“ (z. B. in einer nicht-Produktionsumgebung), kann die Berechnung für die Warnmeldung * Low Metadaten Storage* fehlerhaft sein.

Schritte

1. Wählen Sie **Alarme** > **Aktuell**.
2. Erweitern Sie, falls erforderlich, aus der Warnmeldungstabelle die Warnungsgruppe **Low-Metadaten-Speicher** und wählen Sie die spezifische Warnung aus, die Sie anzeigen möchten.
3. Überprüfen Sie die Details im Dialogfeld „Warnung“.
4. Wenn eine wichtige oder kritische Warnung für * Storage-Systeme mit niedrigen Metadaten* ausgelöst wurde, führen Sie eine Erweiterung durch, um Storage-Nodes sofort hinzuzufügen.

   Da StorageGRID komplette Kopien aller Objektmetadaten an jedem Standort speichert, wird die Metadaten-Kapazität des gesamten Grid durch die Metadaten-Kapazität des kleinsten Standorts begrenzt. Wenn Sie einem Standort Metadatenkapazität hinzufügen möchten, sollten Sie auch alle anderen Standorte um dieselbe Anzahl von Storage-Nodes erweitern.

   Nach der Erweiterung verteilt StorageGRID die vorhandenen Objekt-Metadaten neu auf die neuen Nodes, wodurch die allgemeine Metadaten des Grid erhöht werden. Es ist keine Benutzeraktion erforderlich. Die Warnung * Speicherung von niedrigen Metadaten* wird gelöscht.

Verwandte Informationen

"Monitoring der Objekt-Metadaten-Kapazität für jeden Storage Node"

"Erweitern Sie Ihr Raster"

Fehlerbehebung im Alarm Services: Status - Cassandra (SVST)

Der Alarm Services: Status – Cassandra (SVST) gibt an, dass Sie die Cassandra-Datenbank für einen Storage-Node möglicherweise neu aufbauen müssen. Cassandra dient als Metadatenspeicher für StorageGRID.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Wenn Cassandra länger als 15 Tage angehalten wird (z. B. ausgeschaltet), startet Cassandra nicht, wenn der Node wieder online geschaltet wird. Sie müssen die Cassandra-Datenbank für den betroffenen DDS-Dienst neu erstellen.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen.

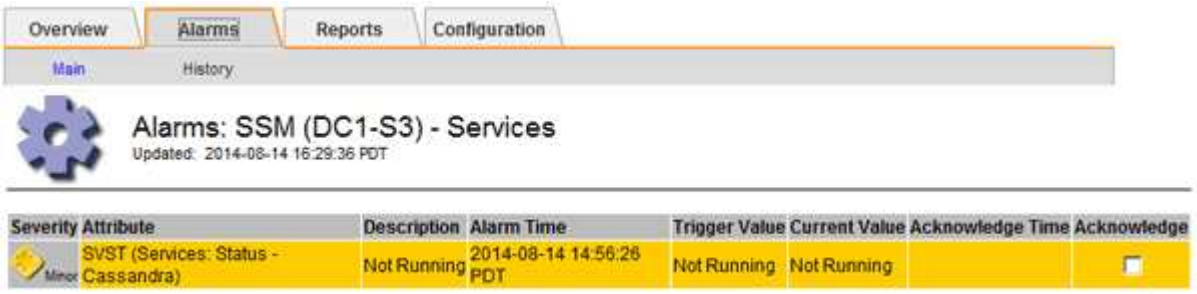
"Diagnose wird ausgeführt"

> Wenn mindestens zwei der Cassandra-Datenbankdienste länger als 15 Tage ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

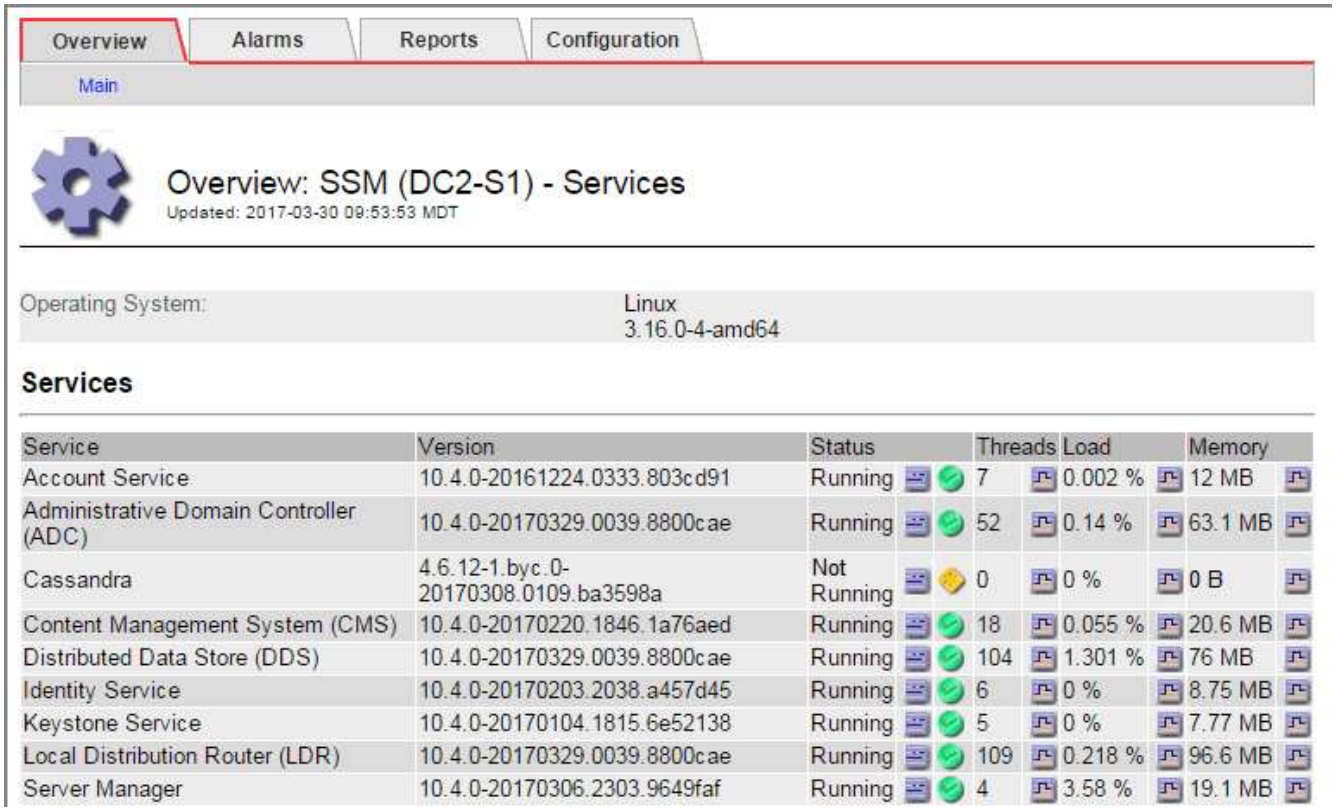
Schritte

1. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
2. Wählen Sie ***site*** **>** ***Storage Node*** > **SSM** > **Services** > **Alarme** > **Main**, um Alarme anzuzeigen.

   Dieses Beispiel zeigt, dass der SVST-Alarm ausgelöst wurde.



   Auf der SSM Services-Hauptseite wird auch angezeigt, dass Cassandra nicht ausgeführt wird.



1. Versuchen Sie, Cassandra vom Storage-Node neu zu starten:
   a. Melden Sie sich beim Grid-Node an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
   b. Geben Sie Ein: `/etc/init.d/cassandra status`
   c. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: `/etc/init.d/cassandra restart`
2. Falls Cassandra nicht neu startet, bestimmen Sie, wie lange Cassandra ausgefallen ist. Wenn Cassandra länger als 15 Tage ausfällt, müssen Sie die Cassandra-Datenbank neu aufbauen.

   Wenn zwei oder mehr der Cassandra-Datenbankdienste ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

   Sie können feststellen, wie lange Cassandra ausgefallen ist, indem Sie sie aufschreiben oder die Datei servermanager.log lesen.

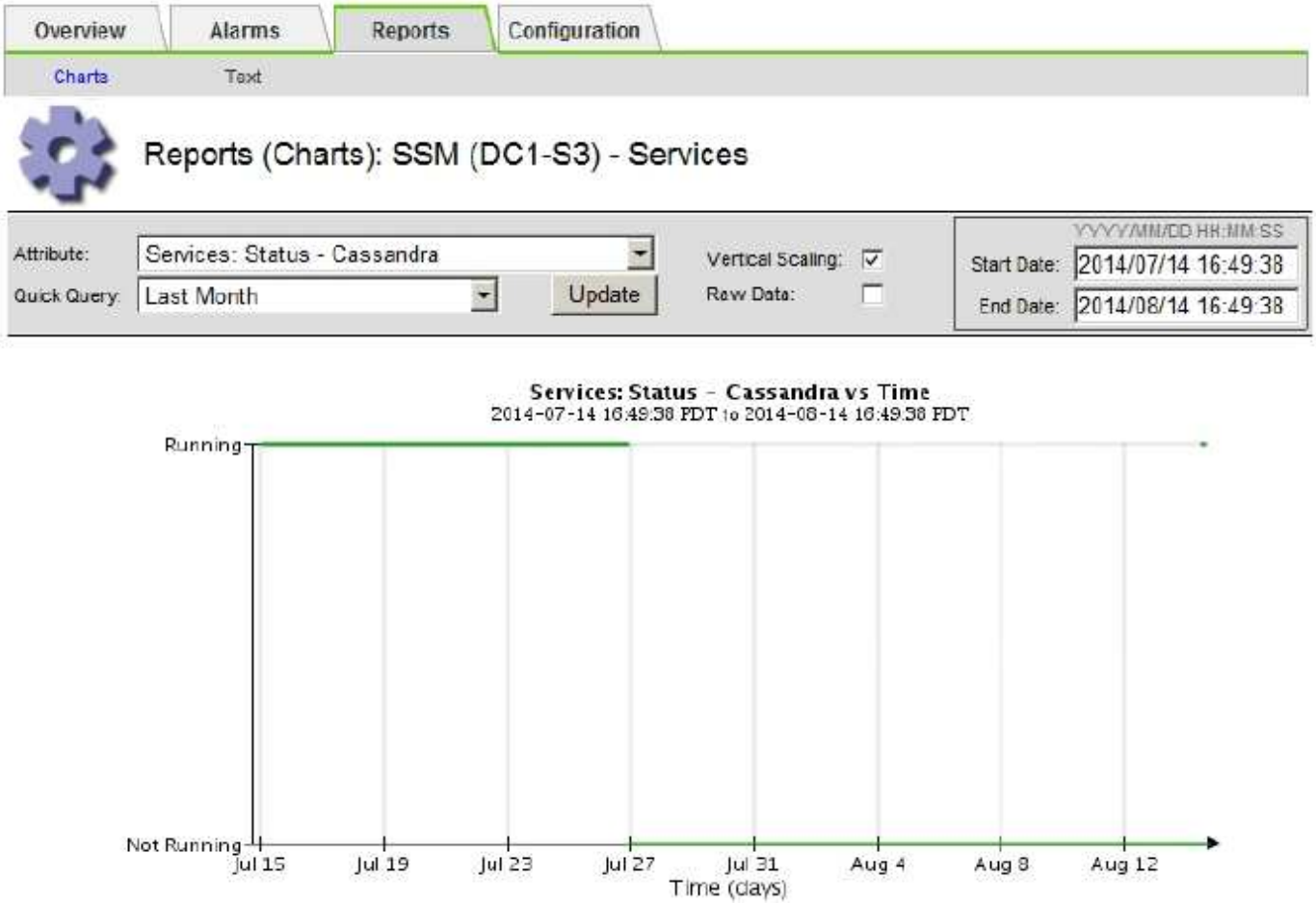
3. Cassandra Diagramm:
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***site*** > ***Storage Node*** > **SSM** > **Services** > **Berichte** > **Diagramme** aus.
   b. Wählen Sie **Attribut** > **Service: Status - Cassandra**.
   c. Geben Sie für **Startdatum** ein Datum ein, das mindestens 16 Tage vor dem aktuellen Datum liegt.

Geben Sie für **Enddatum** das aktuelle Datum ein.

d. Klicken Sie Auf **Aktualisieren**.

e. Wenn Cassandra für mehr als 15 Tage nicht verfügbar ist, bauen Sie die Cassandra-Datenbank erneut aus.

Das folgende Diagramm zeigt, dass Cassandra seit mindestens 17 Tagen ausgefallen ist.



1. So prüfen Sie die Datei servermanager.log auf dem Speicherknoten:

   a. Melden Sie sich beim Grid-Node an:

      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

   b. Geben Sie Ein: `cat /var/local/log/servermanager.log`

      Der Inhalt der Datei servermanager.log wird angezeigt.

      Wenn Cassandra länger als 15 Tage ausfällt, wird die folgende Meldung in der Datei servermanager.log angezeigt:

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

a. Stellen Sie sicher, dass der Zeitstempel dieser Nachricht der Zeitpunkt ist, zu dem Sie versucht haben, Cassandra wie in Schritt angegeben neu zu starten Starten Sie Cassandra vom Storage-Node aus neu.

   Für Cassandra gibt es mehrere Einträge; Sie müssen den letzten Eintrag finden.

b. Wenn Cassandra länger als 15 Tage ausfällt, müssen Sie die Cassandra-Datenbank neu aufbauen.

   Anweisungen hierzu finden Sie unter „`Wiederherstellen von einem einzelnen Speicherknoten nach unten mehr als 15 Tage`“ in den Anweisungen zur Wiederherstellung und Wartung.

c. Wenden Sie sich an den technischen Support, wenn die Alarme nach dem Wiederaufbau von Cassandra nicht gelöscht werden.

Verwandte Informationen

"Verwalten Sie erholen"

Fehlerbehebung bei Cassandra-Speicherfehlern (SMTT-Alarm)

Ein Alarm für Total Events (SMTT) wird ausgelöst, wenn die Cassandra-Datenbank einen Fehler außerhalb des Arbeitsspeichers hat. Wenn dieser Fehler auftritt, wenden Sie sich an den technischen Support, um das Problem zu bearbeiten.

Über diese Aufgabe

Wenn für die Cassandra-Datenbank ein Fehler außerhalb des Arbeitsspeichers auftritt, wird ein Heap Dump erstellt, ein SMTT-Alarm (Total Events) ausgelöst und die Anzahl der Cassandra Heap Out of Memory-Fehler wird um eins erhöht.

Schritte

1. Um das Ereignis anzuzeigen, wählen Sie **Knoten** > ***Grid Node*** > **Ereignisse**.
2. Stellen Sie sicher, dass die Anzahl der Cassandra Heap-Fehler bei einem Speicherfehler mindestens 1 beträgt.

   Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen.

   "Diagnose wird ausgeführt"

3. Gehen Sie zu `/var/local/core/`, Komprimieren Sie die `Cassandra.hprof` Datei erstellen und an den technischen Support senden.
4. Erstellen Sie ein Backup der `Cassandra.hprof` Datei und löschen Sie sie aus dem `/var/local/core/directory`.

   Diese Datei kann bis zu 24 GB groß sein, so sollten Sie sie entfernen, um Speicherplatz freizugeben.

5. Wenn das Problem behoben ist, klicken Sie auf **Ereignisanzahl zurücksetzen**.

Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen.

Verwandte Informationen

"Ereignisanzahl wird zurückgesetzt"

Fehlerbehebung bei Zertifikatfehlern

Wenn beim Versuch, eine Verbindung mit StorageGRID über einen Webbrowser, einen S3- oder Swift-Client oder ein externes Monitoring-Tool herzustellen, ein Problem mit der Sicherheit oder dem Zertifikat auftritt, sollten Sie das Zertifikat überprüfen.

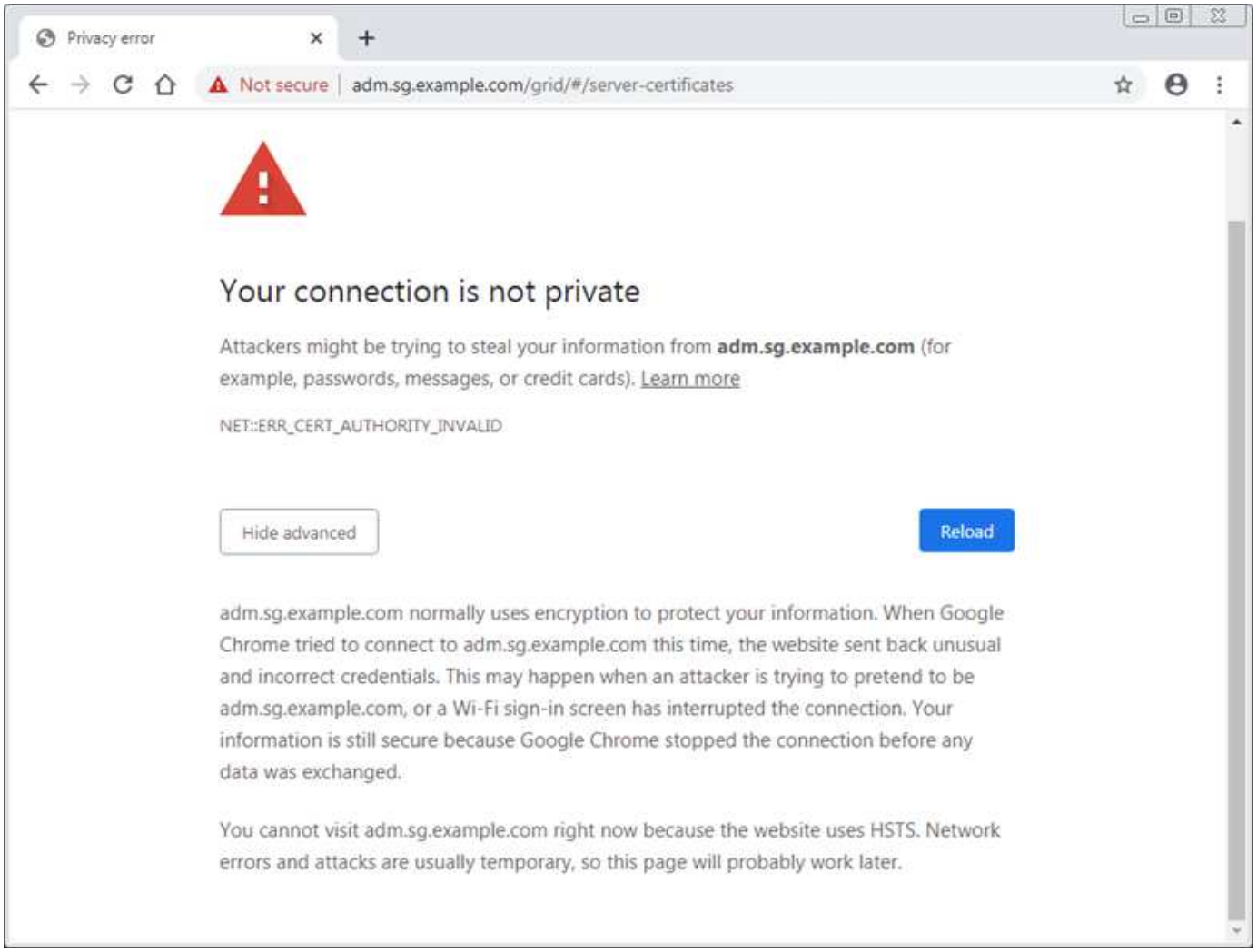
Über diese Aufgabe

Zertifikatfehler können Probleme verursachen, wenn Sie versuchen, eine Verbindung mit StorageGRID mithilfe des Grid Managers, der Grid Management API, des Mandantenmanagers oder der Mandantenmanagement-API herzustellen. Zertifikatfehler können auch auftreten, wenn Sie eine Verbindung mit einem S3- oder Swift-Client oder einem externen Monitoring-Tool herstellen.

Wenn Sie mit einem Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für den benutzerdefinierten Verwaltungsserver läuft ab.
- Sie werden von einem Server-Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Das folgende Beispiel zeigt einen Zertifikatfehler, wenn das Zertifikat des benutzerdefinierten Verwaltungsservers abgelaufen ist:



Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn das Serverzertifikat abläuft.

Wenn Sie Clientzertifikate für die externe Prometheus-Integration verwenden, können Zertifikatfehler durch das StorageGRID Management Interface Server Zertifikat oder durch Client-Zertifikate verursacht werden. Die Warnung **Ablauf von Zertifikaten, die auf der Seite Clientzertifikate** konfiguriert sind, wird ausgelöst, wenn ein Clientzertifikat abläuft.

Schritte

1. Wenn Sie eine Benachrichtigung über ein abgelaufenes Zertifikat erhalten haben, rufen Sie die Zertifikatsdetails auf:
   - Wählen Sie für ein Serverzertifikat **Konfiguration Netzwerkeinstellungen Serverzertifikate** aus.
   - Wählen Sie für ein Clientzertifikat **Konfiguration Zugangskontrolle Clientzertifikate** aus.
2. Überprüfen Sie die Gültigkeitsdauer des Zertifikats.

   Einige Webbrowser und S3- oder Swift-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.

3. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein oder generieren Sie ein neues Zertifikat.
   - Informationen zum Serverzertifikat finden Sie in den Schritten zum Konfigurieren eines

benutzerdefinierten Serverzertifikats für den Grid Manager und den Mandantenmanager in den Anweisungen für die Administration von StorageGRID.

- Informationen zum Konfigurieren eines Client-Zertifikats finden Sie in den Schritten zum Konfigurieren eines Client-Zertifikats in den Anleitungen zum Verwalten von StorageGRID.

4. Versuchen Sie bei Serverzertifikatfehlern oder beiden der folgenden Optionen:
   - Stellen Sie sicher, dass der Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass das SAN mit der IP-Adresse oder dem Hostnamen des Node übereinstimmt, mit dem Sie eine Verbindung herstellen.
   - Wenn Sie versuchen, eine Verbindung zu StorageGRID mit einem Domain-Namen herzustellen:
     i. Geben Sie die IP-Adresse des Admin-Knotens anstelle des Domain-Namens ein, um den Verbindungsfehler zu umgehen und auf den Grid-Manager zuzugreifen.
     ii. Wählen Sie im Grid Manager **Konfiguration Netzwerkeinstellungen Server-Zertifikate** aus, um ein neues benutzerdefiniertes Zertifikat zu installieren oder mit dem Standardzertifikat fortzufahren.
     iii. Lesen Sie in den Anweisungen zum Verwalten von StorageGRID die Schritte zum Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Mandanten-Manager.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei Problemen mit Admin-Knoten und Benutzeroberfläche

Es gibt verschiedene Aufgaben, die Sie durchführen können, um die Ursache von Problemen im Zusammenhang mit Admin-Knoten und der StorageGRID-Benutzeroberfläche zu ermitteln.

Fehlerbehebung bei Anmeldefehlern

Wenn beim Anmelden bei einem StorageGRID-Admin-Node ein Fehler auftritt, weist Ihr System möglicherweise ein Problem mit der Konfiguration des Identitätsverbunds auf, ein Netzwerk- oder Hardwareproblem, ein Problem mit den Admin-Node-Services oder ein Problem mit der Cassandra-Datenbank auf verbundenen Speicherknoten.

Was Sie benötigen

- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Verwenden Sie diese Hinweise zur Fehlerbehebung, wenn eine der folgenden Fehlermeldungen angezeigt wird, wenn Sie versuchen, sich bei einem Admin-Knoten anzumelden:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Schritte

1. Warten Sie 10 Minuten, und melden Sie sich erneut an.

   Wenn der Fehler nicht automatisch behoben wird, fahren Sie mit dem nächsten Schritt fort.

2. Wenn Ihr StorageGRID-System mehr als einen Admin-Knoten hat, melden Sie sich von einem anderen Admin-Knoten beim Grid-Manager an.
   - Wenn Sie sich anmelden können, können Sie die Optionen **Dashboard**, **Nodes**, **Alerts** und **Support** verwenden, um die Ursache des Fehlers zu ermitteln.
   - Wenn Sie nur einen Admin-Node haben oder sich dennoch nicht anmelden können, fahren Sie mit dem nächsten Schritt fort.
3. Ermitteln, ob die Hardware des Node offline ist
4. Wenn SSO (Single Sign On) für Ihr StorageGRID-System aktiviert ist, lesen Sie in den Anweisungen zur Administration von StorageGRID die Schritte zur Konfiguration der Single Sign-On.

   Unter Umständen müssen Sie SSO für einen einzelnen Admin-Node vorübergehend deaktivieren und erneut aktivieren, um Probleme zu beheben.

   > Wenn SSO aktiviert ist, können Sie sich nicht mit einem eingeschränkten Port anmelden. Sie müssen Port 443 verwenden.

5. Ermitteln Sie, ob das verwendete Konto einem föderierten Benutzer angehört.

   Wenn das verbundene Benutzerkonto nicht funktioniert, melden Sie sich beim Grid Manager als lokaler Benutzer, z. B. als Root, an.

   - Wenn sich der lokale Benutzer anmelden kann:
     i. Überprüfen Sie alle angezeigten Alarme.
     ii. Wählen Sie **Konfiguration** > **Identitätsföderation**.
     iii. Klicken Sie auf **Verbindung testen**, um die Verbindungseinstellungen für den LDAP-Server zu validieren.
     iv. Wenn der Test fehlschlägt, beheben Sie alle Konfigurationsfehler.
   - Wenn sich der lokale Benutzer nicht anmelden kann und Sie sich sicher sind, dass die Anmeldeinformationen korrekt sind, fahren Sie mit dem nächsten Schritt fort.
6. Verwenden Sie Secure Shell (SSH), um sich beim Admin-Knoten anzumelden:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

7. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

   Stellen Sie sicher, dass die nms-, mi-, nginx- und Management-API-Services ausgeführt werden.

   Die Ausgabe wird sofort aktualisiert, wenn sich der Status eines Dienstes ändert.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Vergewissern Sie sich, dass der Apache-Webserver ausgeführt wird: `# service apache2 status`

1. Verwenden Sie Lumberjack, um Protokolle zu sammeln: `# /usr/local/sbin/lumberjack.rb`

   Wenn die fehlgeschlagene Authentifizierung in der Vergangenheit stattgefunden hat, können Sie die Skriptoptionen --Start und --end Lumberjack verwenden, um den entsprechenden Zeitbereich festzulegen. Verwenden Sie die lumberjack -h für Details zu diesen Optionen.

   Die Ausgabe an das Terminal gibt an, wo das Protokollarchiv kopiert wurde.

1. Überprüfen Sie die folgenden Protokolle:
   - `/var/local/log/bycast.log`
   - `/var/local/log/bycast-err.log`
   - `/var/local/log/nms.log`

- `**/*commands.txt`

2. Wenn Sie keine Probleme mit dem Admin-Knoten feststellen konnten, geben Sie einen der folgenden Befehle ein, um die IP-Adressen der drei Speicherknoten zu ermitteln, die den ADC-Dienst an Ihrem Standort ausführen. In der Regel handelt es sich dabei um die ersten drei Storage-Nodes, die am Standort installiert wurden.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Admin-Knoten verwenden den ADC-Dienst während des Authentifizierungsprozesses.

3. Melden Sie sich über den Admin-Node bei jedem der ADC-Speicherknoten an. Verwenden Sie dazu die IP-Adressen, die Sie identifiziert haben.
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

   Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

4. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

   Stellen Sie sicher, dass die Services idnt, acct, nginx und cassandra ausgeführt werden.

5. Wiederholen Sie die Schritte Verwenden Sie Lumberjack, um Protokolle zu sammeln Und Protokolle prüfen So prüfen Sie die Protokolle auf den Speicherknoten.
6. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

   Stellen Sie die Protokolle bereit, die Sie für den technischen Support gesammelt haben.

Verwandte Informationen

"StorageGRID verwalten"

"Referenz für Protokolldateien"

Fehlerbehebung bei Problemen mit der Benutzeroberfläche

Nach dem Upgrade auf eine neue Version der StorageGRID-Software sind möglicherweise Probleme mit dem Grid Manager oder dem Tenant Manager zu sehen.

Web-Oberfläche reagiert nicht wie erwartet

Der Grid-Manager oder der Mandantenmanager reagieren nach einem Upgrade der StorageGRID-Software möglicherweise nicht wie erwartet.

Wenn Probleme mit der Weboberfläche auftreten:

- Stellen Sie sicher, dass Sie einen unterstützten Browser verwenden.

  > Die Browser-Unterstützung wurde für StorageGRID 11.5 geändert. Vergewissern Sie sich, dass Sie eine unterstützte Version verwenden.

- Löschen Sie den Cache Ihres Webbrowsers.

  Beim Löschen des Caches werden veraltete Ressourcen entfernt, die von der vorherigen Version der StorageGRID-Software verwendet werden, und die Benutzeroberfläche kann wieder ordnungsgemäß ausgeführt werden. Anweisungen hierzu finden Sie in der Dokumentation Ihres Webbrowsers.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"StorageGRID verwalten"

Überprüfen des Status eines nicht verfügbaren Admin-Knotens

Wenn das StorageGRID-System mehrere Administratorknoten enthält, können Sie den Status eines nicht verfügbaren Admin-Knotens mit einem anderen Admin-Knoten überprüfen.

Was Sie benötigen

Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Melden Sie sich bei einem verfügbaren Admin-Node mit einem unterstützten Browser beim Grid Manager an.
2. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
3. Wählen Sie ***Site*** **> nicht verfügbarer Admin-Node** > **SSM** > **Services** > **Übersicht** > **Main**.
4. Suchen Sie nach Diensten, die den Status nicht aktiv haben und die möglicherweise auch blau angezeigt werden.
5. Bestimmen Sie, ob Alarme ausgelöst wurden.
6. Ergreifen Sie die entsprechenden Maßnahmen, um das Problem zu lösen.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei Netzwerk-, Hardware- und Plattformproblemen

Sie können verschiedene Aufgaben durchführen, um die Ursache von Problemen im Zusammenhang mit dem StorageGRID Netzwerk-, Hardware- und Plattformproblemen zu ermitteln.

Fehlerbehebung „`422: Unprocessable Entity`“-Fehler

Der Fehler 422: Unbearbeitbare Einheit kann unter verschiedenen Umständen auftreten. Überprüfen Sie die Fehlermeldung, um festzustellen, welche Ursache Ihr Problem verursacht hat.

Wenn eine der aufgeführten Fehlermeldungen angezeigt wird, führen Sie die empfohlene Aktion durch.

Fehlermeldung	Ursache und Korrekturmaßnahme

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Diese Meldung kann auftreten, wenn Sie bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option **TLS nicht verwenden** für Transport Layer Security (TLS) auswählen.
	
	Die Verwendung der Option **keine Verwendung von TLS** wird nicht für die Verwendung mit AD-Servern unterstützt, die LDAP-Signatur erzwingen. Sie müssen entweder die Option **STARTTLS verwenden** oder die Option **LDAPS verwenden** für TLS auswählen.

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte Chiffre zu verwenden, um eine TLS-Verbindung (Transport Layer Security) von StorageGRID zu einem externen System herzustellen, das für Identify Federation oder Cloud Storage Pools verwendet wird.
	
	Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eine der von StorageGRID unterstützten Chiffren für ausgehende TLS-Verbindungen verwenden, wie in den Anleitungen zur StorageGRID-Verwaltung dargestellt.

Verwandte Informationen

"StorageGRID verwalten"

Fehlerbehebung bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU

Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) über Knoten im Grid deutlich unterscheidet.

Über diese Aufgabe

Die Unterschiede in den MTU-Einstellungen könnten darauf hinweisen, dass einige, aber nicht alle, eth0-Netzwerke für Jumbo Frames konfiguriert sind. Eine MTU-Größe von mehr als 1000 kann zu Problemen mit der Netzwerkleistung führen.

Schritte

1. Führen Sie die MTU-Einstellungen für eth0 auf allen Knoten auf.
   - Verwenden Sie die im Grid Manager angegebene Abfrage.
   - Navigieren Sie zu *primary Admin Node IP address*`/metrics/graph` Und geben Sie die folgende Abfrage ein: `node_network_mtu_bytes{interface='eth0'}`
2. Ändern Sie die MTU-Einstellungen nach Bedarf, um sicherzustellen, dass sie für die Grid Network Interface (eth0) auf allen Knoten identisch sind.
   - Informationen zu Appliance-Knoten finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.
   - Verwenden Sie für Linux- und VMware-basierte Knoten den folgenden Befehl: `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`
     - Beispiel*: `change-mtu.py -n node 1500 grid admin`

       Hinweis: Wenn auf Linux-basierten Knoten der gewünschte MTU-Wert für das Netzwerk im Container den bereits auf der Hostschnittstelle konfigurierten Wert überschreitet, müssen Sie zuerst die Hostschnittstelle so konfigurieren, dass sie den gewünschten MTU-Wert hat, und dann den verwenden `change-mtu.py` Skript zum Ändern des MTU-Werts des Netzwerks im Container.

     Verwenden Sie die folgenden Argumente, um die MTU auf Linux- oder VMware-basierten Knoten zu ändern.

Positionsargumente	Beschreibung
`mtu`	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
`network`	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: • Raster • Admin • Client

+

Optionale Argumente	Beschreibung
`-h, – help`	HilMeldung anzeigen und beenden.
`-n node, --node node`	Der Node. Die Standardeinstellung ist der lokale Knoten.

Verwandte Informationen

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

Fehlerbehebung bei dem NRER-Alarm (Network Receive Error)

NRER-Alarme (Network Receive Error) können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerk-Hardware verursacht werden. In einigen Fällen können NRER-Fehler ohne manuelles Eingreifen gelöscht werden. Wenn die Fehler nicht behoben werden, führen Sie die empfohlenen Maßnahmen durch.

Über diese Aufgabe

NRER-Alarme können durch die folgenden Probleme mit Netzwerk-Hardware verursacht werden, die eine Verbindung mit StorageGRID herstellt:

- Eine Vorwärtsfehlerkorrektur (FEC) ist erforderlich und wird nicht verwendet
- Switch-Port und MTU-NIC stimmen nicht überein
- Hohe Link-Fehlerraten
- NIC-Klingelpuffer überlaufen

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle möglichen Ursachen des NRER-Alarms bei der Netzwerkkonfiguration.
    - Wenn der Fehler durch eine nicht übereinstimmende FEC verursacht wird, führen Sie die folgenden Schritte aus:

      Hinweis: Diese Schritte gelten nur für NRER-Fehler, die durch FEC-Diskrepanz auf StorageGRID-Geräten verursacht werden.

        i. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID-Gerät angeschlossen ist.

        ii. Überprüfen Sie die physikalische Integrität der Kabel vom Gerät zum Switch.

        iii. Wenn Sie die FEC-Einstellungen ändern möchten, um den NRER-Alarm zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Konfiguration verknüpfen“ des Installationsprogramms von StorageGRID-Geräten für den **Auto**-Modus konfiguriert ist (siehe Installations- und Wartungsanweisungen für Ihr Gerät). Ändern Sie dann die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

        (Sie können FEC-Einstellungen auf StorageGRID-Geräten nicht konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu erkennen und zu spiegeln, an denen sie angeschlossen sind. Wenn die Verbindungen zu 25-GbE- oder 100-GbE-Netzwerkgeschwindigkeiten gezwungen sind, können Switch und NIC eine gemeinsame FEC-Einstellung nicht aushandeln. Ohne eine gemeinsame FEC-Einstellung kehrt das Netzwerk in den Modus „`no-FEC`“ zurück. Wenn FEC nicht aktiviert ist, sind die Anschlüsse anfälliger für Fehler, die durch elektrische Geräusche verursacht werden.)

Hinweis: StorageGRID-Geräte unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie kein FEC.

- Wenn der Fehler durch einen Switch Port und eine nicht übereinstimmende NIC MTU verursacht wird, überprüfen Sie, ob die auf dem Node konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port identisch ist.

  Die auf dem Node konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung am Switch-Port, mit dem der Node verbunden ist. Wenn ein StorageGRID-Knoten einen Ethernet-Frame empfängt, der größer ist als seine MTU, was mit dieser Konfiguration möglich ist, wird möglicherweise der NRR-Alarm gemeldet. Wenn Sie der Ansicht sind, dass dies geschieht, ändern Sie entweder die MTU des Switch Ports entsprechend der StorageGRID Netzwerkschnittstelle MTU oder ändern Sie die MTU der StorageGRID-Netzwerkschnittstelle je nach Ihren End-to-End-Zielen oder Anforderungen an den Switch-Port.

  > Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen identisch sein.

  > Informationen zum Ändern der MTU-Einstellung finden Sie im Installations- und Wartungshandbuch für Ihre Appliance.

- Wenn der Fehler durch hohe Verbindungsfehlerraten verursacht wird, führen Sie die folgenden Schritte aus:

  i. Aktivieren Sie FEC, falls nicht bereits aktiviert.

  ii. Stellen Sie sicher, dass Ihre Netzwerkkabel von guter Qualität sind und nicht beschädigt oder nicht ordnungsgemäß angeschlossen sind.

  iii. Falls die Kabel nicht das Problem darstellen, wenden Sie sich an den technischen Support.

  > In einer Umgebung mit hohem elektrischen Rauschen können hohe Fehlerraten festgestellt werden.

- Wenn es sich bei dem Fehler um einen NIC-Ringpuffer handelt, wenden Sie sich an den technischen Support.

  Der Ruffuffer kann bei Überlastung des StorageGRID-Systems überlaufen werden und kann Netzwerkereignisse nicht zeitnah verarbeiten.

2. Nachdem Sie das zugrunde liegende Problem gelöst haben, setzen Sie den Fehlerzähler zurück.
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***site*** > ***GRID Node*** > **SSM** > **Ressourcen** > **Konfiguration** > **Main** aus.
   c. Wählen Sie **Empfangspunkt zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Verwandte Informationen

"Fehlerbehebung bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU"

"Alarmreferenz (Altsystem)"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

"SG100 SG1000 Services-Appliances"

Fehlerbehebung bei Fehlern bei der Zeitsynchronisierung

Möglicherweise treten Probleme mit der Zeitsynchronisierung in Ihrem Raster auf.

Wenn Probleme mit der Zeitsynchronisierung auftreten, stellen Sie sicher, dass Sie mindestens vier externe NTP-Quellen angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern, und dass alle externen NTP-Quellen normal funktionieren und von Ihren StorageGRID-Knoten zugänglich sind.

> Wenn Sie die externe NTP-Quelle für eine StorageGRID-Installation auf Produktionsebene angeben, verwenden Sie den Windows Time-Dienst (W32Time) nicht auf einer Windows-Version als Windows Server 2016. Der Zeitdienst für ältere Windows Versionen ist nicht ausreichend genau und wird von Microsoft nicht für die Verwendung in Umgebungen mit hoher Genauigkeit, wie z. B. StorageGRID, unterstützt.

Verwandte Informationen

"Verwalten Sie erholen"

Linux: Probleme mit der Netzwerkverbindung

Möglicherweise werden Probleme mit der Netzwerkverbindung für StorageGRID Grid-Nodes auftreten, die auf Linux-Hosts gehostet werden.

Klonen VON MAC Adressen

In einigen Fällen können Netzwerkprobleme mithilfe des Klonens von MAC-Adressen behoben werden. Wenn Sie virtuelle Hosts verwenden, legen Sie den Wert des MAC-Adressenklonens für jedes Ihrer Netzwerke in der Node-Konfigurationsdatei auf „true“ fest. Diese Einstellung bewirkt, dass die MAC-Adresse des StorageGRID-Containers die MAC-Adresse des Hosts verwendet. Informationen zum Erstellen von Node-Konfigurationsdateien finden Sie in den Anweisungen im Installationshandbuch für Ihre Plattform.

> Erstellen Sie separate virtuelle Netzwerkschnittstellen, die vom Linux Host-Betriebssystem verwendet werden können. Die Verwendung derselben Netzwerkschnittstellen für das Linux-Hostbetriebssystem und den StorageGRID-Container kann dazu führen, dass das Host-Betriebssystem nicht mehr erreichbar ist, wenn der promiskuious-Modus auf dem Hypervisor nicht aktiviert wurde.

Weitere Informationen zum Aktivieren des MAC-Klonens finden Sie in den Anweisungen im Installationshandbuch für Ihre Plattform.

Promiskuous Modus

Wenn Sie kein Klonen der MAC-Adresse verwenden möchten und lieber alle Schnittstellen Daten für andere MAC-Adressen als die vom Hypervisor zugewiesenen empfangen und übertragen möchten, Stellen Sie sicher, dass die Sicherheitseigenschaften auf der Ebene der virtuellen Switch- und Portgruppen auf **Accept** für den Promiscuous-Modus, MAC-Adressänderungen und Forged-Übertragungen eingestellt sind. Die auf dem virtuellen Switch eingestellten Werte können von den Werten auf der Portgruppenebene außer Kraft gesetzt

werden. Stellen Sie also sicher, dass die Einstellungen an beiden Stellen identisch sind.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

Linux: Node-Status lautet „`verwaiste`“

Ein Linux-Node in einem verwaisten Status gibt in der Regel an, dass entweder der StorageGRID-Service oder der StorageGRID-Node-Daemon, der den Container steuert, unerwartet gestorben ist.

Über diese Aufgabe

Wenn ein Linux-Knoten meldet, dass er sich in einem verwaisten Status befindet, sollten Sie Folgendes tun:

- Überprüfen Sie die Protokolle auf Fehler und Meldungen.
- Versuchen Sie, den Node erneut zu starten.
- Verwenden Sie bei Bedarf Docker-Befehle, um den vorhandenen Node-Container zu beenden.
- Starten Sie den Node neu.

Schritte

1. Überprüfen Sie die Protokolle sowohl für den Service-Daemon als auch für den verwaisten Node auf offensichtliche Fehler oder Meldungen zum unerwarteten Beenden.
2. Melden Sie sich beim Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung.
3. Versuchen Sie, den Node erneut zu starten, indem Sie den folgenden Befehl ausführen: `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   Wenn der Node verwaiste ist, wird die Antwort angezeigt

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. Beenden Sie unter Linux den Docker Container und alle steuernden storagegrid Node-Prozesse:`sudo docker stop --time secondscontainer-name`

   Für `seconds`Geben Sie die Anzahl der Sekunden ein, die Sie warten möchten, bis der Container angehalten wird (normalerweise 15 Minuten oder weniger).

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. Starten Sie den Knoten neu: `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

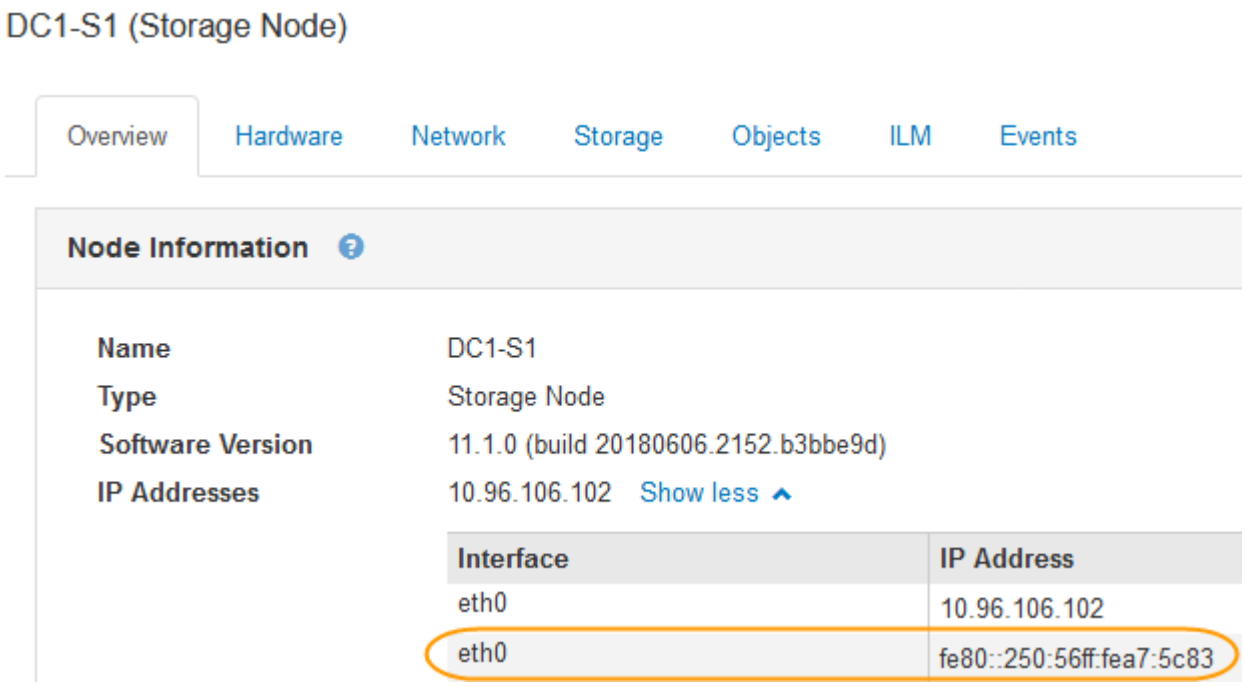
Linux: Fehlerbehebung von IPv6-Unterstützung

Möglicherweise müssen Sie die IPv6-Unterstützung im Kernel aktivieren, wenn Sie StorageGRID-Knoten auf Linux-Hosts installiert haben und Sie bemerken, dass den Knoten-Containern keine IPv6-Adressen wie erwartet zugewiesen wurden.

Über diese Aufgabe

Die IPv6-Adresse, die einem Grid-Node zugewiesen wurde, wird in den folgenden Speicherorten im Grid Manager angezeigt:

- Wählen Sie **Knoten** aus, und wählen Sie den Knoten aus. Klicken Sie dann auf der Registerkarte Übersicht neben **IP-Adressen** auf **Mehr anzeigen**.



- Wählen Sie **Support** > **Tools** > **Grid Topology** Aus. Wählen Sie dann ***Node*** > **SSM** > **Ressourcen** aus. Wenn eine IPv6-Adresse zugewiesen wurde, wird sie unter der IPv4-Adresse im Abschnitt **Netzwerkadressen** aufgelistet.

Wenn die IPv6-Adresse nicht angezeigt wird und der Knoten auf einem Linux-Host installiert ist, führen Sie diese Schritte aus, um die IPv6-Unterstützung im Kernel zu aktivieren.

Schritte

1. Melden Sie sich beim Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung.
2. Führen Sie den folgenden Befehl aus: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Das Ergebnis sollte 0 sein.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

Wenn das Ergebnis nicht 0 ist, lesen Sie die Dokumentation zum Ändern des Betriebssystems `sysctl` Einstellungen. Ändern Sie dann den Wert in 0, bevor Sie fortfahren.

3. Geben Sie den StorageGRID-Node-Container ein: `storagegrid node enter node-name`
4. Führen Sie den folgenden Befehl aus: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Das Ergebnis sollte 1 sein.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

Wenn das Ergebnis nicht 1 ist, gilt dieses Verfahren nicht. Wenden Sie sich an den technischen Support.

5. Verlassen Sie den Behälter: `exit`

```
root@DC1-S1:~ # exit
```

6. Bearbeiten Sie als root die folgende Datei: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Suchen Sie die folgenden beiden Zeilen, und entfernen Sie die Kommentar-Tags. Speichern und schließen Sie anschließend die Datei.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Führen Sie folgende Befehle aus, um den StorageGRID-Container neu zu starten:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Prüfung von Audit-Protokollen

Machen Sie sich mit den StorageGRID Systemaudits-Protokollen vertraut und sehen Sie eine Liste aller Audit-Meldungen an.

- "Übersicht über Überwachungsnachrichten"
- "Audit-Log-Datei und Nachrichtenformate"
- "Überwachungsmeldungen und der Lebenszyklus von Objekten"
- "Audit-Meldungen"

Übersicht über Überwachungsnachrichten

Diese Anweisungen enthalten Informationen zur Struktur und zum Inhalt der StorageGRID-Prüfmeldungen und Prüfprotokolle. Sie können diese Informationen zum Lesen und Analysieren des Prüfprotokolls der Systemaktivität verwenden.

Diese Anweisungen richten sich an Administratoren, die für die Erstellung von Berichten zu Systemaktivitäten und -Nutzung verantwortlich sind, für die eine Analyse der Audit-Meldungen des StorageGRID Systems erforderlich ist.

Es wird davon ausgegangen, dass Sie die Art der geprüften Aktivitäten innerhalb des StorageGRID-Systems genau kennen. Um die Text-Log-Datei verwenden zu können, müssen Sie auf die konfigurierte Revisionsfreigabe im Admin-Knoten zugreifen können.

Verwandte Informationen

"StorageGRID verwalten"

Meldungsfluss und -Aufbewahrung von Audits

Alle StorageGRID-Services generieren während des normalen Systembetriebs Audit-Meldungen. Sie sollten verstehen, wie diese Audit-Meldungen über das StorageGRID-System in das übertragen werden `audit.log` Datei:

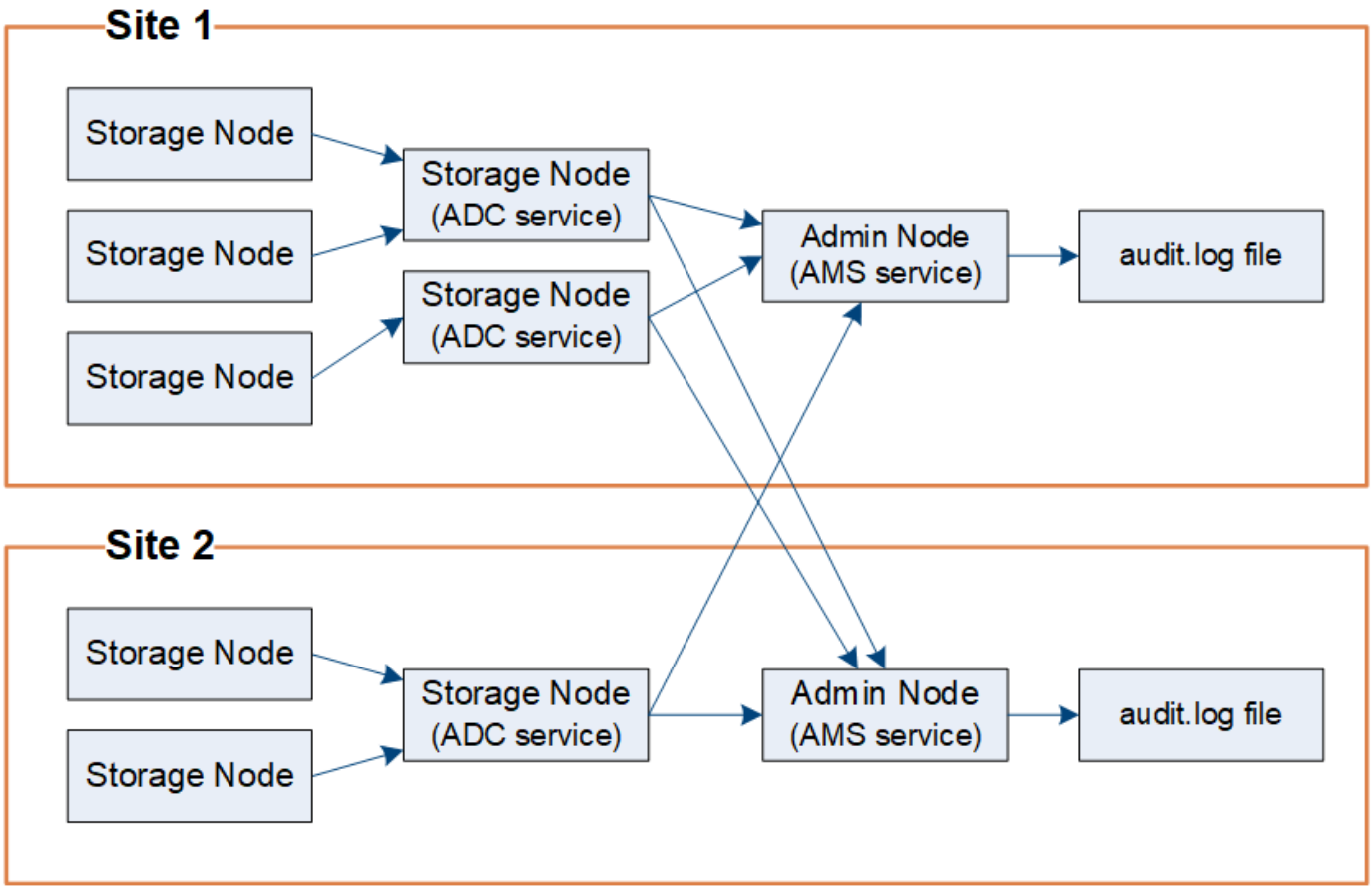
Audit-Nachrichtenfluss

Überwachungsmeldungen werden von Admin-Nodes und Storage-Nodes verarbeitet, die über einen ADC-Dienst (Administrative Domain Controller) verfügen.

Wie im Überwachungsmeldung-Flow-Diagramm dargestellt, sendet jeder StorageGRID Node seine Audit-Meldungen an einen der ADC-Services am Datacenter-Standort. Der ADC-Dienst wird automatisch für die ersten drei Speicherknoten aktiviert, die an jedem Standort installiert sind.

Jeder ADC-Dienst fungiert wiederum als Relais und sendet seine Sammlung von Audit-Meldungen an jeden Admin-Knoten im StorageGRID-System, wodurch jeder Admin-Knoten einen vollständigen Datensatz der Systemaktivität erhält.

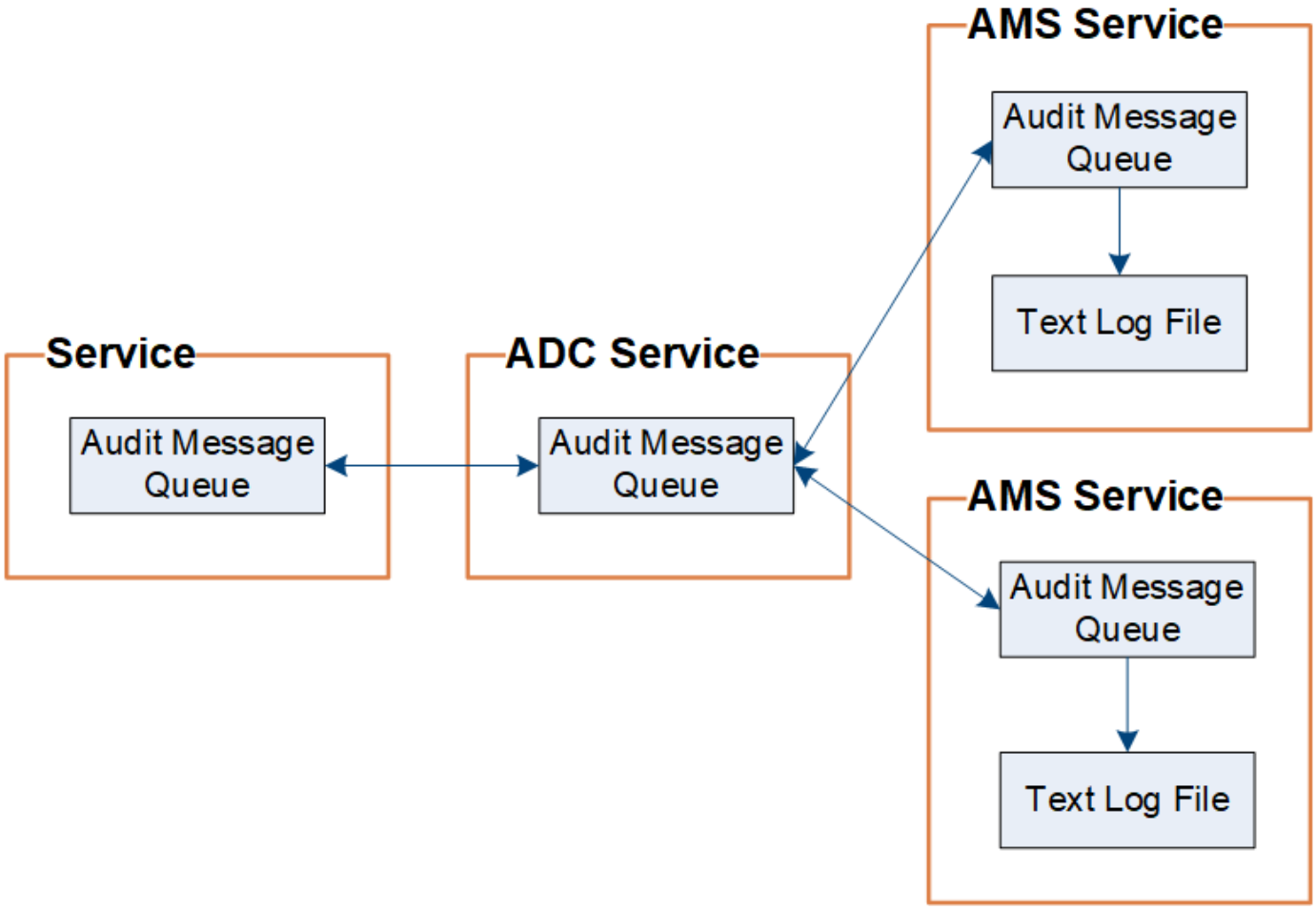
Jeder Admin-Knoten speichert Audit-Meldungen in Text-Log-Dateien; die aktive Protokolldatei wird benannt `audit.log`.



Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschprozess, um sicherzustellen, dass keine Audit-Meldungen verloren gehen, bevor sie in das Audit-Protokoll geschrieben werden.

Wenn ein Knoten eine Überwachungsmeldung generiert oder sendet, wird die Meldung in einer Meldungswarteschlange auf der Systemfestplatte des Grid-Node gespeichert. Eine Kopie der Nachricht wird immer in einer Warteschlange mit Überwachungsmeldung gespeichert, bis die Nachricht in die Audit-Log-Datei des Admin-Knotens geschrieben wird `/var/local/audit/export` Verzeichnis. Dadurch wird der Verlust einer Prüfmeldung während des Transports verhindert.



Die Warteschlange für Überwachungsnachrichten kann aufgrund von Problemen mit der Netzwerkverbindung oder aufgrund unzureichender Audit-Kapazität vorübergehend erhöht werden. Wenn die Warteschlangen steigen, verbrauchen sie mehr des verfügbaren Speicherplatzes in den einzelnen Nodes `/var/local/` Verzeichnis. Wenn das Problem weiterhin besteht und das Verzeichnis der Überwachungsmeldungen eines Knotens zu voll ist, werden die einzelnen Knoten die Verarbeitung ihres Rückstands priorisieren und für neue Meldungen vorübergehend nicht verfügbar sein.

Sie können insbesondere folgende Verhaltensweisen erkennen:

- Wenn der `/var/local/audit/export` Verzeichnis, das von einem Admin-Knoten verwendet wird, wird voll, der Admin-Knoten wird als nicht verfügbar für neue Audit-Meldungen markiert, bis das Verzeichnis nicht mehr voll ist. S3- und Swift-Client-Anforderungen sind nicht betroffen. Der Alarm XAMS (Unreachable Audit Repositories) wird ausgelöst, wenn ein Audit-Repository nicht erreichbar ist.
- Wenn der `/var/local/` Das von einem Speicherknoten mit dem ADC-Dienst verwendete Verzeichnis wird zu 92 % voll, der Knoten wird als nicht verfügbar markiert, um Meldungen zu prüfen, bis das Verzeichnis nur zu 87 % voll ist. S3- und Swift-Client-Anfragen zu anderen Nodes sind nicht betroffen. Der Alarm NRLY (Available Audit Relays) wird ausgelöst, wenn Audit-Relais nicht erreichbar sind.

  > Wenn keine Speicherknoten mit dem ADC-Dienst verfügbar sind, werden die Überwachungsmeldungen von den Speicherknoten lokal gespeichert.

- Wenn der `/var/local/` Das von einem Storage-Node verwendete Verzeichnis ist zu 85 % voll, wobei der Node die S3- und Swift-Client-Anforderungen ablehnen wird `503 Service Unavailable`.

Die folgenden Arten von Problemen können dazu führen, dass die Warteschlangen für Überwachungsnachrichten sehr groß werden:

- Der Ausfall eines Admin-Knotens oder Speicherknoten mit dem ADC-Dienst. Wenn einer der Systemknoten ausgefallen ist, werden die übrigen Knoten möglicherweise rückgemeldet.
- Eine nachhaltige Aktivitätsrate, die die Audit-Kapazität des Systems übersteigt.
- Der `/var/local/` Speicherplatz auf einem ADC-Speicherknoten wird aus Gründen voll, die nicht mit Audit-Meldungen zusammenhängen. In diesem Fall hört der Knoten auf, neue Überwachungsmeldungen zu akzeptieren und priorisiert seinen aktuellen Rückstand, was zu Backlogs auf anderen Knoten führen kann.

Großer Alarm für Überwachungswarteschlangen und Überwachungsmeldungen in Queued (AMQS)

Um Ihnen dabei zu helfen, die Größe der Überwachungsmeldungswarteschlangen im Laufe der Zeit zu überwachen, werden die Warnung **große Prüfwarteschlange** und der ältere AMQS-Alarm ausgelöst, wenn die Anzahl der Nachrichten in einer Speicherknotenwarteschlange oder Admin-Knoten-Warteschlange bestimmte Schwellenwerte erreicht.

Wenn der Alarm * Large Audit queue* oder der alte AMQS-Alarm ausgelöst wird, prüfen Sie zunächst die Auslastung des Systems – wenn eine beträchtliche Anzahl aktueller Transaktionen vorliegt, sollten sich die Warnung und der Alarm im Laufe der Zeit lösen und können ignoriert werden.

Wenn die Warnung oder der Alarm weiterhin besteht und die Schwere erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. Verringern Sie die Betriebsrate des Clients, oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie das Audit-Level für Client-Schreibvorgänge und Client-Lesevorgänge auf Fehler oder aus ändern. Siehe „“"Ändern der Level von Überwachungsnachrichten".“

Duplizieren von Nachrichten

Bei einem Netzwerk- oder Node-Ausfall ist das StorageGRID System konservativ. Aus diesem Grund können doppelte Nachrichten im Audit-Protokoll vorhanden sein.

Ändern der Level von Überwachungsnachrichten

Sie können die Audiorelevel anpassen, um die Anzahl der im Audit-Protokoll für jede Kategorie von Überwachungsmeldungen aufgezeichneten Audit-Meldungen zu erhöhen oder zu verringern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die im Auditprotokoll aufgezeichneten Überwachungsmeldungen werden basierend auf den Einstellungen auf der Seite **Konfiguration** > **Überwachung** > **Audit** gefiltert.

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

- **System**: Standardmäßig ist dieser Level auf Normal gesetzt.
- **Speicherung**: Standardmäßig ist diese Ebene auf Fehler gesetzt.

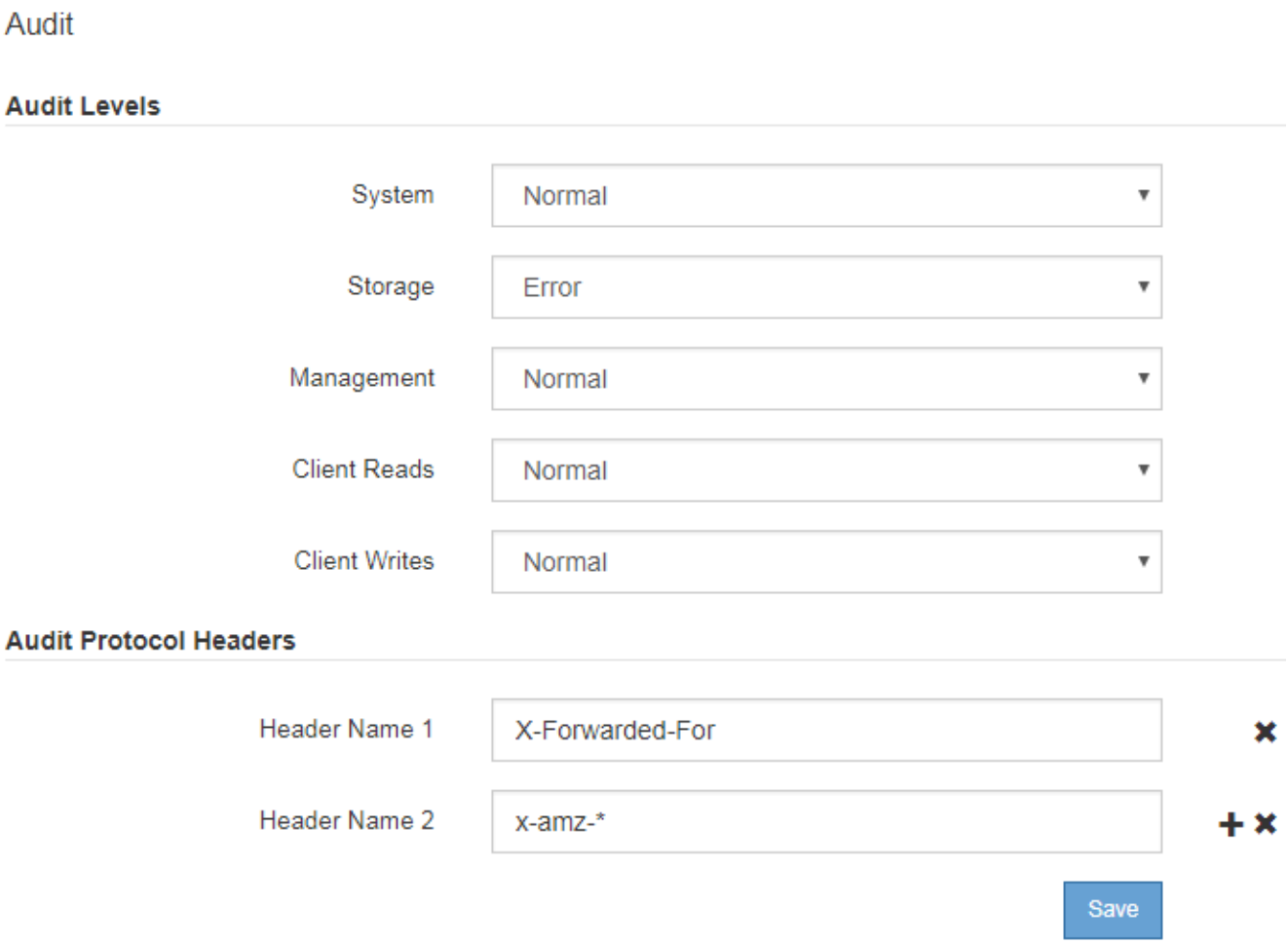
- **Verwaltung**: Standardmäßig ist diese Ebene auf Normal gesetzt.
- **Client liest**: Standardmäßig ist diese Ebene auf Normal gesetzt.
- **Client schreibt**: Standardmäßig ist diese Ebene auf Normal gesetzt.

Diese Standardeinstellungen gelten, wenn Sie StorageGRID ursprünglich mit Version 10.3 oder höher installiert haben. Wenn Sie ein Upgrade von einer früheren Version von StorageGRID durchgeführt haben, ist die Standardeinstellung für alle Kategorien auf „Normal“ gesetzt.

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

Schritte

1. Wählen Sie **Konfiguration** > **Überwachung** > **Audit**.



2. Wählen Sie für jede Kategorie der Überwachungsmeldung eine Überwachungsstufe aus der Dropdown-Liste aus:

Audit-Level	Beschreibung
Aus	Es werden keine Überwachungsmeldungen aus der Kategorie protokolliert.
Fehler	Nur Fehlermeldungen sind protokollierte - Audit-Meldungen, für die der Ergebniscode nicht „erfolgreich“ (SUCS) war.

Audit-Level	Beschreibung
Normal	Standardtransaktionsmeldungen werden protokolliert – die in diesen Anweisungen für die Kategorie aufgeführten Nachrichten.
Debuggen	Veraltet. Dieser Level verhält sich mit dem normalen Prüfstand.

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

3. Geben Sie unter **Audit Protocol Headern** den Namen der HTTP-Request-Header ein, die in den Audit-Meldungen Client Read und Client Write enthalten sein sollen. Verwenden Sie ein Sternchen (*) als Platzhalter, oder verwenden Sie die Escape-Sequenz (*) als wortwörtliche Sternchen. Klicken Sie auf das Pluszeichen, um eine Liste der Kopfzeilennamen-Felder zu erstellen.

   Header für Prüfprotokolle sind nur auf S3 und Swift Anfragen anwendbar.

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

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

4. Klicken Sie Auf **Speichern**.

Verwandte Informationen

"Systemaudits Meldungen"

"Audit-Meldungen zu Objekt-Storage"

"Management-Audit-Nachricht"

"Client liest Audit-Meldungen"

"StorageGRID verwalten"

Zugriff auf die Audit-Log-Datei

Die Revisionsfreigabe enthält die aktive `audit.log` Datei und alle komprimierten Audit-Log-Dateien. Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf Audit-Shares sowohl für NFS als auch für CIFS (veraltet) konfigurieren. Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:

```
cd /var/local/audit/export
```

3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

Verwandte Informationen

"StorageGRID verwalten"

Drehung der Audit-Log-Dateien

Audit-Log-Dateien werden auf einem Admin-Node gespeichert `/var/local/audit/export` Verzeichnis. Die aktiven Audit-Log-Dateien werden benannt `audit.log`.

Einmal am Tag, die aktive `audit.log` Die Datei wird gespeichert und eine neue `audit.log` Datei wird gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format *`yyyy-mm-dd.txt`*. Wenn an einem Tag mehrere Auditprotokolle erstellt werden, verwenden die Dateinamen das Datum, an dem die Datei im Format gespeichert wurde *`yyyy-mm-dd.txt.n`*. Beispiel: `2018-04-15.txt` Und `2018-04-15.txt.1` Sind die ersten und zweiten Log-Dateien, die am 15. April 2018 erstellt und gespeichert wurden.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt *`yyyy-mm-dd.txt.gz`*, Die das ursprüngliche Datum bewahrt. Im Lauf der Zeit führt dies zu einem Verbrauch von für Prüfprotokolle auf dem Admin-Node zugewiesenem Storage. Ein Skript überwacht den Verbrauch von Speicherplatz im Überwachungsprotokoll und löscht die Protokolldateien nach Bedarf, um Speicherplatz im freizugeben `/var/local/audit/export` Verzeichnis. Audit-Protokolle werden nach dem Erstellungsdatum der Prüfprotokolle gelöscht, wobei der älteste zuerst gelöscht wird. Sie können die Aktionen des Skripts in der folgenden Datei überwachen: `/var/local/log/manage-audit.log`.

Dieses Beispiel zeigt die aktive `audit.log` Datei, Datei des Vortags (`2018-04-15.txt`), und die komprimierte Datei für den Vortag (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Audit-Log-Datei und Nachrichtenformate

Mit Audit-Protokollen können Informationen zu Ihrem System erfasst und Probleme behoben werden. Sie sollten das Format der Audit-Log-Datei und das allgemeine Format für Audit-Meldungen verstehen.

Format der Auditprotokolldatei

Die Audit-Log-Dateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Nachrichten.

Jede Überwachungsmeldung enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Meldung (ATIM) im ISO 8601-Format auslöste, gefolgt von einem Leerzeichen:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, Wo *UUUUUU* Nur Mikrosekunden.

- Die Meldung selbst, die in eckigen Klammern eingeschlossen ist und mit beginnt `AUDT`.

Das folgende Beispiel zeigt drei Audit-Nachrichten in einer Audit-Log-Datei (Zeilenumbrüche zur Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, wenn ein Mandant einen S3-Bucket erstellt und diesem Bucket zwei Objekte hinzugefügt hat.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

In ihrem Standardformat sind die Audit-Meldungen in den Audit-Log-Dateien nicht einfach zu lesen oder zu interpretieren. Sie können das verwenden `audit-explain` Tool zum Abrufen vereinfachter Zusammenfassungen der Audit-Meldungen im Audit-Protokoll. Sie können das verwenden `audit-sum` Tool zum Zusammenfassen, wie viele Schreibvorgänge, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

Verwandte Informationen

"Verwenden des Tools zur Erläuterung von Audits"

"Verwenden des Tools Audit-Sum"

Verwenden des Tools zur Erläuterung von Audits

Sie können das verwenden `audit-explain` Tool zum Übersetzen der Audit-Meldungen im Audit-Protokoll in ein einfach zu lesendes Format.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

Der `audit-explain` Das auf dem primären Admin-Knoten verfügbare Tool bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Audit-Protokoll.

> Der `audit-explain` Das Tool ist hauptsächlich für den technischen Support bei der Fehlerbehebung vorgesehen. Wird Verarbeitet `audit-explain` Abfragen können eine große Menge an CPU-Energie verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt die typische Ausgabe von der `audit-explain` Werkzeug. Diese vier SPUT-Audit-Nachrichten wurden generiert, als der S3-Mandant mit Konto-ID 92484777680322627870 S3-PUT-Anforderungen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und diesem Bucket drei Objekte hinzuzufügen.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Der `audit-explain` Das Tool kann einfache oder komprimierte Prüfprotokolle verarbeiten. Beispiel:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

Der `audit-explain` Das Tool kann auch mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Schließlich das `audit-explain` Das Tool kann Eingaben aus einer Leitung annehmen, sodass Sie die Eingabe mit dem filtern und vorverarbeiten können `grep` Befehl oder andere Mittel. Beispiel:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Da Audit-Protokolle sehr groß und langsam zu analysieren sein können, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen und ausführen möchten `audit-explain` Auf die Teile, statt der gesamten Datei.

> Der `audit-explain` Das Werkzeug akzeptiert keine komprimierten Dateien als Piper-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente an, oder verwenden Sie das `zcat` Werkzeug, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
zcat audit.log.gz | audit-explain
```

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-explain -h
```

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` Gibt den Namen und den Speicherort der zu analysierenden Datei oder der zu analysierenden Dateien an:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   Der `audit-explain` Werkzeug druckt menschliche Interpretationen aller Nachrichten in der angegebenen Datei oder Datei.

   > Um die Zeilenlänge zu verringern und die Lesbarkeit zu erleichtern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel anzeigen möchten, verwenden Sie den Zeitstempel (`-t`) Option.

Verwandte Informationen

"SPUT: S3 PUT"

Sie können das verwenden `audit-sum` Tool zum Zählen der Schreib-, Lese-, Kopf- und Löschmeldungen und zum Anzeigen der minimalen, maximalen und durchschnittlichen Zeit (oder Größe) für jeden Operationstyp.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

Der `audit-sum` Tool, das auf dem primären Admin-Knoten verfügbar ist, fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

> Der `audit-sum` Das Tool ist hauptsächlich für den technischen Support bei der Fehlerbehebung vorgesehen. Wird Verarbeitet `audit-sum` Abfragen können eine große Menge an CPU-Energie verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt die typische Ausgabe von der `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

Der `audit-sum` Das Tool bietet Zählung und Zeiten für die folgenden S3, Swift und ILM-Audit-Meldungen in einem Prüfprotokoll:

Codieren	Beschreibung	Siehe
ARCT	Archivieren von Cloud-Tier	"ARCT: Archiv Abrufen aus Cloud-Tier"
ASCT	Archivspeicher Cloud-Tier	"ASCT: Archivspeicher Cloud-Tier"

Codieren	Beschreibung	Siehe
IDEL	ILM initiated Delete: Protokolliert, wenn ILM den Prozess des Löschens eines Objekts startet.	"IDEL: ILM gestartet Löschen"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3 LÖSCHEN"
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten.	"SGET S3 ABRUFEN"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	"SHEA: S3 KOPF"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	"WDEL: Swift LÖSCHEN"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten.	"WGET: Schneller ERHALTEN"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.	"WHEA: Schneller KOPF"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.	"WPUT: Schnell AUSGEDRÜCKT"

Der `audit-sum` Das Tool kann einfache oder komprimierte Prüfprotokolle verarbeiten. Beispiel:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

Der `audit-sum` Das Tool kann auch mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Schließlich das `audit-sum` Das Tool kann auch Eingaben aus einer Leitung annehmen, sodass Sie die Eingabe mit dem filtern und vorverarbeiten können `grep` Befehl oder andere Mittel. Beispiel:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

> Dieses Tool akzeptiert keine komprimierten Dateien als Piper Input. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente an, oder verwenden Sie das `zcat` Werkzeug, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Mit Befehlszeilenoptionen können Operationen für Buckets separat von Operationen für Objekte zusammengefasst oder Nachrichtenübersichten nach Bucket-Namen, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden in den Zusammenfassungen die minimale, maximale und durchschnittliche Betriebszeit angezeigt, Sie können jedoch die verwenden `size (-s)` Option, stattdessen die Objektgröße zu betrachten.

Verwenden Sie die `help (-h)` Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-sum -h
```

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Wenn Sie alle Nachrichten analysieren möchten, die mit Schreibvorgängen, Lese-, Kopf- und Löschvorgängen zusammenhängen, führen Sie die folgenden Schritte aus:

a. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` Gibt den Namen und den Speicherort der zu analysierenden Datei oder der zu analysierenden Dateien an:

```
$ audit-sum /var/local/audit/export/audit.log
```

Dieses Beispiel zeigt die typische Ausgabe von der `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

In diesem Beispiel sind SGET (S3 GET) Vorgänge im Durchschnitt mit 1.13 Sekunden die langsamsten. SGET und SPUT (S3 PUT) Vorgänge weisen jedoch lange Schlimmstfallszeiten von etwa 1,770 Sekunden auf.

b. Um die langsamsten 10 Abruffunktionen anzuzeigen, wählen Sie mit dem grep-Befehl nur SGET-Nachrichten aus und fügen Sie die Long-Output-Option hinzu (`-l`) So fügen Sie Objektpfade ein: `grep SGET audit.log | audit-sum -l`

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, mit dem Sie das Audit-Protokoll für andere Meldungen zu diesen speziellen Objekten grep erstellen können.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+ Aus diesem Beispielausgang sehen Sie, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von ca. 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe berücksichtigt die langsamen Abrufzeiten im schlimmsten Fall.

3. Wenn Sie feststellen möchten, welche Größe von Objekten in Ihr Raster aufgenommen und aus diesem abgerufen werden soll, verwenden Sie die Option „Größe“ (`-s`):

```
audit-sum -s audit.log
```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

In diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2.5 MB, die durchschnittliche Größe für SGET ist jedoch deutlich größer. Die Anzahl der SPUT-Meldungen ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hinweist, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufvorgänge gestern langsam waren:
   a. Geben Sie den Befehl für das entsprechende Prüfprotokoll ein und verwenden Sie die Option „Gruppe für Zeit“ (`-gt`), gefolgt von dem Zeitraum (z. B. 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Diese Ergebnisse zeigen, dass S3 VERKEHR zwischen 06:00 und 07:00 Spikes. Auch die max- und Durchschnittszeiten sind zu diesen Zeiten deutlich höher, und sie stiegen nicht schrittweise auf, wenn die Zahl erhöht wurde. Dies deutet darauf hin, dass die Kapazität irgendwo überschritten wurde, vielleicht im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

b. Um zu bestimmen, welche Objekte in der Größe gestern jede Stunde abgerufen wurden, fügen Sie die Option Größe hinzu (`-s`) Zum Befehl:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Diese Ergebnisse zeigen, dass einige sehr große Rückrufe auftraten, als der gesamte Abrufverkehr seinen maximalen Wert hatte.

c. Verwenden Sie zum Anzeigen weiterer Details die `audit-explain` Tool zur Überprüfung aller SGET-Vorgänge während dieser Stunde:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Wenn die Ausgabe des grep-Befehls viele Zeilen sein soll, fügen Sie den hinzu `less` Befehl zum Anzeigen des Inhalts der Audit-Log-Datei eine Seite (ein Bildschirm) gleichzeitig.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen auf Buckets langsamer sind als SPUT-Vorgänge für Objekte:

a. Verwenden Sie als erstes die `-go` Bei dieser Option werden Meldungen für Objekt- und Bucket-Vorgänge getrennt gruppiert:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets unterschiedliche Leistungseigenschaften haben als SPUT-Operationen für Objekte.

b. Um festzustellen, welche Buckets die langsamsten SPUT-Operationen haben, verwenden Sie den `-gb` Option, die Meldungen nach Bucket gruppiert:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Um zu bestimmen, welche Buckets die größte SPUT-Objektgröße haben, verwenden Sie beide `-gb` Und das `-s` Optionen:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Verwandte Informationen

"Verwenden des Tools zur Erläuterung von Audits"

Überwachungsmeldungsformat

Im StorageGRID-System ausgetauschte Audit-Meldungen enthalten Standardinformationen, die für alle Meldungen und spezifische Inhalte zur Beschreibung des Ereignisses oder der Aktivität üblich sind.

Wenn die von bereitgestellten Zusammenfassungsdaten angezeigt werden `audit-explain` Und `audit-sum` Tools reichen nicht aus. Lesen Sie in diesem Abschnitt, um das allgemeine Format aller Audit-Meldungen zu verstehen.

Im Folgenden finden Sie eine Beispielmeldung, wie sie in der Audit-Log-Datei angezeigt werden kann:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Jede Überwachungsmeldung enthält eine Zeichenfolge von Attributelementen. Der gesamte String ist in Klammern eingeschlossen (`[ ]`), und jedes Attributelement in der Zeichenfolge weist folgende Merkmale auf:

- In Halterungen eingeschlossen `[ ]`
- Eingeführt durch den String `AUDT`, Das eine Audit-Nachricht anzeigt
- Ohne Trennzeichen (keine Kommata oder Leerzeichen) vor oder nach
- Wird durch ein Zeilenvorschub-Zeichen beendet `\n`

Jedes Element umfasst einen Attributcode, einen Datentyp und einen Wert, der in diesem Format angegeben wird:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Die Anzahl der Attributelemente in der Nachricht hängt vom Ereignistyp der Nachricht ab. Die Attributelemente werden in keiner bestimmten Reihenfolge aufgeführt.

In der folgenden Liste werden die Attributelemente beschrieben:

- `ATTR` Ist ein 4-Zeichen-Code für das Attribut, das gemeldet wird. Es gibt einige Attribute, die für alle Audit-Meldungen und andere, die ereignisspezifisch sind, gelten.
- `type` Ist eine 4-Zeichen-Kennung des Programmierdatentyps des Wertes, wie UI64, FC32 usw. Der Typ ist in Klammern eingeschlossen `( )`.
- `value` Ist der Inhalt des Attributs, in der Regel ein numerischer Wert oder Textwert. Werte folgen immer einem Doppelpunkt (`:`). Werte des Datentyps CSTR werden von doppelten Anführungszeichen umgeben `" "`.

Verwandte Informationen

"Verwenden des Tools zur Erläuterung von Audits"

"Verwenden des Tools Audit-Sum"

"Audit-Meldungen"

"Gemeinsame Elemente in Audit-Meldungen"

"Datentypen"

"Beispiele für Überwachungsnachrichten"

Datentypen

Verschiedene Datentypen werden zur Speicherung von Informationen in Audit-Meldungen verwendet.

Typ	Beschreibung
UI32	Unsigned long integer (32 Bit); es kann die Zahlen 0 bis 4,294,967,295 speichern.
UI64	Unsigned double long integer (64 Bit); es kann die Zahlen 0 bis 18,446,744,073,709,551,615 speichern.
FC32	Vierklarlige Konstante; ein 32-Bit unsigned integer Wert, der als vier ASCII-Zeichen wie "ABCD" dargestellt wird.
IPAD	Wird für IP-Adressen verwendet.

Typ	Beschreibung
CSTR	Ein Array mit variabler Länge von UTF-8 Zeichen. Zeichen können mit den folgenden Konventionen entgangen werden: • Backslash ist \\. • Der Schlittenrücklauf beträgt \r • Doppelte Anführungszeichen sind \". • Zeilenvorschub (neue Zeile) ist \n. • Zeichen können durch ihre hexadezimalen Äquivalente ersetzt werden (im Format \xHH, wobei HH der hexadezimale Wert ist, der das Zeichen darstellt).

Ereignisspezifische Daten

Jede Überwachungsmeldung im Prüfprotokoll zeichnet Daten auf, die für ein Systemereignis spezifisch sind.

Nach der Öffnung `[AUDT:` Container, der die Meldung selbst identifiziert, die nächsten Attribute liefern Informationen über das Ereignis oder die Aktion, die durch die Überwachungsmeldung beschrieben werden. Diese Attribute sind im folgenden Beispiel hervorgehoben:

```
2018-12-05T08:24:45.921845 [AUDT:[RSLT(FC32):SUCS]
[TIME(UI64):11454] [SAIP(IPAD):"10.224.0.100"]
[S3AI(CSTR):"60025621595611246499"] [SACC(CSTR):"account"]
[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="]
[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]
[SBAI(CSTR):"60025621595611246499"] [SBAC(CSTR):"account"] [S3BK(CSTR):"bucket"]
[S3KY(CSTR):"object"] [CBID(UI64):0xCC128B9B9E428347]
[UUID(CSTR):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"] [CSIZ(UI64):30720]
[AVER(UI32):10] [ATIM(UI64):1543998285921845] [ATYP(FC32):SHEA]
[ANID(UI32):12281045] [AMID(FC32):S3RQ] [ATID(UI64):15552417629170647261]]
```

Der `ATYP` Element (unterstrichen im Beispiel) identifiziert, welches Ereignis die Nachricht erzeugt hat. Diese Beispielmeldung enthält den SHEA-Nachrichtencode ([ATYP(FC32):SHEA]), der angibt, dass er von einer erfolgreichen S3-KOPFANFORDERUNG generiert wurde.

Verwandte Informationen

"Gemeinsame Elemente in Audit-Meldungen"

"Audit-Meldungen"

Gemeinsame Elemente in Audit-Meldungen

Alle Meldungen enthalten die allgemeinen Elemente.

Codieren	Typ	Beschreibung
INMITTEN	FC32	Modul-ID: Eine vier-Zeichen-ID der Modul-ID, die die Nachricht generiert hat. Dies gibt das Codesegment an, in dem die Überwachungsmeldung generiert wurde.
ANID	UI32	Node-ID: Die Grid-Node-ID, die dem Service zugewiesen wurde, der die Meldung generiert hat. Jedem Service wird bei Konfiguration und Installation des StorageGRID-Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.
ASES	UI64	Kennung der Auditsitzung: In vorherigen Releases gab dieses Element die Zeit an, zu der das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit der Betriebssystemepoche gemessen (00:00:00 UTC am 1. Januar 1970). **Hinweis:** Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ASQN	UI64	Sequenzanzahl: In vorherigen Releases wurde dieser Zähler für jede erzeugte Überwachungsmeldung auf dem Grid-Node (ANID) erhöht und beim Neustart des Dienstes auf Null zurückgesetzt. **Hinweis:** Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ATID	UI64	Trace-ID: Eine Kennung, die von den Nachrichten, die von einem einzelnen Ereignis ausgelöst wurden, gemeinsam genutzt wird.
ATIM	UI64	Zeitstempel: Die Zeit, zu der das Ereignis generiert wurde, das die Audit-Nachricht auslöste, gemessen in Mikrosekunden seit der Betriebssystemepoche (00:00:00 UTC am 1. Januar, 1970). Beachten Sie, dass die meisten verfügbaren Tools zum Konvertieren des Zeitstempels in lokales Datum und Uhrzeit auf Millisekunden basieren. Möglicherweise ist ein Aufrundung oder Verkürzung des protokollierten Zeitstempels erforderlich. Die lesbare Zeit des Menschen, die zu Beginn der Überwachungsmeldung-angezeigt wird `audit.log` Die Datei ist das ATIM-Attribut im ISO 8601-Format. Das Datum und die Uhrzeit werden als dargestellt *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, Wo der `T` Ist ein Literalzeichenzeichen, das den Beginn des Zeitsegments des Datums angibt. *`UUUUUU`* Nur Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine 4-Zeichen-Kennung des zu protokollierenden Ereignisses. Dies regelt den "Nutzlastinhalt" der Nachricht: Die Attribute, die enthalten sind.
AVER	UI32	Version: Die Version der Audit-Nachricht. Wenn die StorageGRID Software weiterentwickelt wird, können neue Serviceversionen neue Funktionen in die Audit-Berichte integrieren. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst zur Verarbeitung von Meldungen aus älteren Serviceversionen.

Codieren	Typ	Beschreibung
RSLT	FC32	Ergebnis: Das Ergebnis von Ereignis, Prozess oder Transaktion. Wenn für eine Nachricht nicht relevant ist, WIRD KEINE verwendet, sondern SUCS, damit die Nachricht nicht versehentlich gefiltert wird.

Beispiele für Überwachungsnachrichten

Detaillierte Informationen finden Sie in jeder Audit-Nachricht. Alle Überwachungsmeldungen verwenden das gleiche Format.

Im Folgenden finden Sie eine Beispielmeldung für Audits, wie sie im angezeigt werden kann `audit.log` Datei:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Die Überwachungsmeldung enthält Informationen über das zu protokollierte Ereignis sowie Informationen über die Meldung selbst.

Um festzustellen, welches Ereignis durch die Überwachungsmeldung aufgezeichnet wird, suchen Sie nach dem ATYP-Attribut (unten hervorgehoben):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

Der Wert des ATYP-Attributs ist SPUT. SPUT stellt eine S3-PUT-Transaktion dar, die die Aufnahme eines Objekts in einen Bucket protokolliert.

Die folgende Meldung des Audits zeigt auch den Bucket an, dem das Objekt zugeordnet ist:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Um zu ermitteln, wann das PUT-Ereignis aufgetreten ist, notieren Sie den UTC-Zeitstempel (Universal Coordinated Time, Universal Coordinated Time, koordinierte Zeit) zu Beginn der Überwachungsmeldung. Dieser Wert ist eine menschliche-lesbare Version des ATIM-Attributs der Prüfmeldung selbst:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM zeichnet die Zeit in Mikrosekunden, seit Beginn der UNIX-Epoche. Im Beispiel der Wert `1405631878959669` Übersetzt bis Donnerstag, 17. Juli 2014 21:17:59 UTC.

Verwandte Informationen

"SPUT: S3 PUT"

"Gemeinsame Elemente in Audit-Meldungen"

Überwachungsmeldungen und der Lebenszyklus von Objekten

Audit-Nachrichten werden bei jeder Aufnahme, jedem Abruf oder jedem Löschen eines Objekts generiert. Sie können diese Transaktionen im Audit-Protokoll identifizieren, indem Sie API-spezifische (S3 oder Swift) Audit-Nachrichten suchen.

Überwachungsmeldungen werden durch Kennungen verknüpft, die für jedes Protokoll spezifisch sind.

Protokoll	Codieren
Verknüpfen von S3-Vorgängen	S3BK (S3-Bucket) und/oder S3KY (S3-Schlüssel)
Swift-Vorgänge verknüpfen	WCON (Swift-Container) und/oder WOBJ (Swift-Objekt)

Protokoll	Codieren
Verknüpfen interner Vorgänge	CBID (interne Kennung des Objekts)

Timing von Audit-Meldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Nodes, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der durch die verschiedenen Services erzeugten Audit-Meldungen von den Beispielen in diesem Abschnitt abweichen.

Konfiguration der Richtlinien für das Informationslebenszyklus-Management

Bei der ILM-Standardrichtlinie (Baseline 2 Copy) werden Objektdaten einmal für insgesamt zwei Kopien kopiert. Wenn die ILM-Richtlinie mehr als zwei Kopien erfordert, gibt es für jede zusätzliche Kopie einen zusätzlichen Satz von CBRE-, CBSE- und SCMT-Meldungen. Weitere Informationen zu ILM-Richtlinien finden Sie unter Informationen zum Managen von Objekten mit Information Lifecycle Management.

Archiv-Nodes

Die Reihe von Meldungen, die beim Senden von Objektdaten an ein externes Archiv-Speichersystem generiert werden, ist ähnlich wie bei Storage-Nodes, es sei denn, es gibt keine SCMT-Meldung (Store Object Commit). Und die ATCE (Archive Object Store Begin) und ASCE (Archive Object Store End) Nachrichten werden für jede archivierte Kopie von Objektdaten generiert.

Die Reihe von Audit-Meldungen, die beim Abrufen von Objektdaten aus einem externen Archiv-Storage-System generiert werden, ähnelt der für Storage-Nodes, jedoch werden für jede abgerufene Kopie von Objektdaten ARCB (Archivobjekt Retrieve Begin) und ARCE (Archive Object Retrieve End) Nachrichten generiert.

Die beim Löschen von Objektdaten aus einem externen Archivspeichersystem generierte Reihe von Überwachungsmeldungen ähnelt der für Speicherknoten, es sei denn, ES gibt keine SREM (Object Store Remove)-Nachricht und für jede Löschanforderung gibt es eine AREM-Nachricht (Archive Object Remove).

Verwandte Informationen

"Objektmanagement mit ILM"

Objektaufnahme von Transaktionen

Sie können Transaktionen zur Client-Aufnahme im Prüfprotokoll identifizieren, indem API-spezifische (S3 oder Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Aufnahmetransaktion generierten Audit-Meldungen aufgeführt. Es sind nur die Nachrichten enthalten, die für die Aufzeichnung der Transaktion erforderlich sind.

S3 Aufnahme von Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3-PUT-Aufnahmerate wurde erfolgreich abgeschlossen.	CBID, S3BK, S3KY	"SPUT: S3 PUT"

Codieren	Name	Beschreibung	Verfolgen	Siehe
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Swift Ingest-Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
WPUT	Swift PUT-Transaktion	EINE Swift PUT-Aufnahme-Transaktion wurde erfolgreich abgeschlossen.	CBID, WCON, WOBJ	"WPUT: Schnell AUSGEDRÜCKT"
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Beispiel: S3-Objektaufnahme

Die folgende Serie von Audit-Meldungen ist ein Beispiel für die im Revisionsprotokoll generierten und gespeicherten Audit-Meldungen, wenn ein S3-Client ein Objekt in einen Storage-Node (LDR-Service) einspeist.

In diesem Beispiel umfasst die aktive ILM-Richtlinie die ILM-Regel für das Lager, erstellen Sie 2 Kopien.

> Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Audit-Meldungen aufgeführt. Es werden nur solche aufgeführt, die sich auf die S3-Aufnahmetransaktion (SPUT) beziehen.

In diesem Beispiel wird vorausgesetzt, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Meldung gibt an, dass eine S3-PUT-Transaktion ausgegeben wurde, um ein Objekt in einem bestimmten Bucket zu erstellen.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"]<strong
class="S3KY(CSTR):"testobject-0-
3"">[CBID(UI64):0x8EF52DF8025E63A8]</strong>[CSIZ(UI64):30720][AVER(UI32):
10]<strong
class="ATIM(UI64):150032627859669">[ATYP(FC32):SPUT]</strong>[ANID(UI32):1
2086324][AMID(FC32):S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Objektregeln erfüllt

Die ORLM-Meldung gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Meldung enthält die CBID des Objekts und den Namen der verwendeten ILM-Regel.

Bei replizierten Objekten umfasst das Feld LOCS die LDR-Node-ID und Volume-ID der Objektstandorte.

```
2019-07-17T21:18:31.230669[AUDT:
<strong>[CBID(UI64):0x50C4F7AC2BC8EDF7]</strong> [RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]<strong class="LOCS(CSTR): *"CLDI 12828634
2148730112">[RSLT(FC32):SUCS][AVER(UI32):10] [ATYP(FC32):ORLM]</strong>
[ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):131
00453][AMID(FC32):BCMS]]
```

Bei Objekten mit Erasure Coding enthält das Feld LOCS die Profile-ID für Erasure Coding und die Gruppen-ID für Erasure Coding

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR): "CLEC 1 A471E45D-A400-47C7-86AC-12E77F229831"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ANID(UI32):12355278][AMI
D(FC32):ILMX][ATID(UI64):41685590464737255 60]]
```

Das PFADFELD umfasst S3-Bucket und wichtige Informationen sowie Swift-Container- und Objektinformationen, je nachdem, welche API verwendet wurde.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Löschen von Objekttransaktionen

Sie können Transaktionen zum Löschen von Objekten im Prüfprotokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Meldungen angezeigt werden.

In den folgenden Tabellen sind nicht alle während einer Löschtransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die zum Verfolgen der Löschtransaktion erforderlich sind.

S3-Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Anforderung zum Löschen des Objekts aus einem Bucket gemacht.	CBID, S3KY	"SDEL: S3 LÖSCHEN"

Swift Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WDEL	Swift Löschen	Anforderung gemacht, das Objekt aus einem Container oder Container zu löschen.	CBID, WOBJ	"WDEL: Swift LÖSCHEN"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt aus einem Storage-Node (LDR-Service) löscht, wird eine Überwachungsmeldung generiert und im Revisionsprotokoll gespeichert.

Im folgenden Beispiel sind nicht alle während einer Löschtransaktion generierten Audit-Meldungen aufgeführt. Es werden nur diejenigen aufgelistet, die mit der S3-Löschtransaktion (SDEL) in Verbindung stehen.

SDEL: S3 Löschen

Die Objektlöschung beginnt, wenn der Client eine LÖSCHANFORDERUNG an einen LDR-Dienst sendet. Die Meldung enthält den Bucket, aus dem das Objekt gelöscht werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"] <strong>[S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
7"][CBID(UI64):0x339F21C5A6964D89]</strong>
[CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669]
<strong>[ATYP(FC32):SDEL]</strong>[ANID(UI32):12086324][AMID(FC32):S3RQ][A
TID(UI64):4727861330952970593]]
```

Abrufen von Objekttransaktionen

Sie können Transaktionen zum Abrufen von Objekten im Audit-Protokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Abruftransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die für die Rückrufs-Transaktion erforderlich sind.

S3-Abruf von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 ABRUFEN	Anforderung zum Abrufen eines Objekts aus einem Bucket	CBID, S3BK, S3KY	"SGET S3 ABRUFEN"

Schnelles Abrufen von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WGET	Swift GET	Anforderung gemacht, ein Objekt aus einem Container abzurufen.	CBID, WCON, WOBJ	"WGET: Schneller ERHALTEN"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Storage-Node (LDR-Service) abruft, wird eine Audit-Meldung erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET S3 ABRUFEN

Der Objektabruf beginnt, wenn der Client eine GET Object-Anforderung an einen LDR-Service sendet. Die Meldung enthält den Bucket, aus dem das Objekt abgerufen werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]
[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947988782605][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]]
```

Wenn die Bucket-Richtlinie ermöglicht, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört, Die Überwachungsmeldung enthält Informationen über das Mandantenkonto des Bucket-Inhabers, sodass Sie diese anonymen und Cross-Account-Anforderungen verfolgen können.

In der folgenden Beispielmeldung sendet der Client eine GET Object-Anforderung für ein in einem Bucket gespeichertes Objekt, das ihnen nicht gehören. Die Werte für SBAI und SBAC zeichnen die Konto-ID und den Namen des Mandanten des Bucket-Besitzers auf. Diese Werte unterscheiden sich von der Konto-ID und dem Namen des in S3AI und SACC aufgezeichneten Clients.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]
<strong>[S3AI(CSTR):"17915054115450519830"][SACC(CSTR):"s3-account-
b"]</strong>[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="]<st
rong
class="SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"">[SBAI(CS
TR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]</strong>[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Nachrichten zum Metadatenupdate

Audit-Meldungen werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zu S3-Metadaten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten wurden aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3-Metadaten wurden aktualisiert"

Beispiel: S3-Metadatenaktualisierung

Das Beispiel zeigt eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadatenaktualisierung

Der S3-Client fordert eine SUPD (SUPD) auf, die angegebenen Metadaten zu aktualisieren (`x-amz-meta-*`) Für das S3-Objekt (S3KY). In diesem Beispiel sind Anforderungsheader im Feld HTRH enthalten, da sie als Audit-Protokoll-Header konfiguriert wurde (**Konfiguration** > **Monitoring** > **Audit**).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Verwandte Informationen

"Ändern der Level von Überwachungsnachrichten"

Audit-Meldungen

Detaillierte Beschreibungen der vom System zurückgegebenen Audit-Meldungen finden Sie in den folgenden Abschnitten. Jede Überwachungsmeldung wird zuerst in einer Tabelle aufgeführt, in der verwandte Nachrichten nach der Aktivitätsklasse gruppiert werden, für die die Meldung steht. Diese Gruppierungen sind sowohl für das Verständnis der Arten von Aktivitäten, die geprüft werden, als auch für die Auswahl der gewünschten Art der Filterung von Überwachungsnachrichten nützlich.

Die Überwachungsmeldungen werden auch alphabetisch nach ihren vier-Zeichen-Codes aufgelistet. Mit dieser alphabetischen Auflistung können Sie Informationen zu bestimmten Nachrichten suchen.

Die in diesem Kapitel verwendeten 4-Zeichen-Codes sind die ATYP-Werte, die in den Audit-Meldungen gefunden werden, wie in der folgenden Beispielmeldung dargestellt:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][<stro
ng>ATYP\(FC32\):SYSU</strong>][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(
UI64):9445736326500603516]]
```

Verwandte Informationen

"Audit-Meldungen"

"Ändern der Level von Überwachungsnachrichten"

Kategorien von Überwachungsnachrichten

Sie sollten mit den verschiedenen Kategorien vertraut sein, in denen Audit-Meldungen gruppiert werden. Diese Gruppen sind auf der Grundlage der Aktivitätsklasse organisiert, für die die Nachricht steht.

Systemaudits Meldungen

Sie sollten mit Audit-Meldungen vertraut sein, die zur Systemaudit-Kategorie gehören. Dies sind Ereignisse in Bezug auf das Auditing von Systemen selbst, den Status von Grid-Nodes, systemweite Task-Aktivitäten (Grid-Aufgaben) und Service-Backup-Vorgänge, sodass Sie potenzielle Probleme beheben können.

Codieren	Titel und Beschreibung der Nachricht	Siehe
ECOC	Beschädigte Datenfragment mit Erasure-Code: Zeigt an, dass ein korruptes Datenfragment mit Löschungscode erkannt wurde.	"ECOC: Korrupte, mit Erasure codierte Datenfragment"

Codieren	Titel und Beschreibung der Nachricht	Siehe
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Verbindungsversuch mit TLS (Transport Layer Security) fehlgeschlagen.	"ETAF: Sicherheitsauthentifizierung fehlgeschlagen"
GNRG	GNDS Registrierung: Ein Dienst aktualisiert oder registriert Informationen über sich selbst im StorageGRID-System.	"GNRG: GNDS Registrierung"
GNUR	GNDS Unregistrierung: Ein Dienst hat sich vom StorageGRID-System nicht registriert.	"GNUR: GNDS Registrierung aufheben"
GTED	Grid Task beendet: Der CMN-Dienst hat die Verarbeitung der Grid-Aufgabe abgeschlossen.	"GTED: Grid Task beendet"
GTST	Grid Task gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid-Aufgabe begonnen.	"GTST: Grid Task gestartet"
GSU	Grid Task übermittelt: Eine Grid-Aufgabe wurde an den CMN-Dienst übermittelt.	"GTSU: Grid Task übermittelt"
IDEL	ILM-Initiated Delete: Diese Audit-Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.	"IDEL: ILM gestartet Löschen"
LKCU	Bereinigung Des Objekts Überschrieben. Diese Überwachungsmeldung wird erzeugt, wenn ein überschreibtes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	"LKCU: Objektbereinigung überschrieben"
LLST	Standort verloren: Diese Überwachungsmeldung wird generiert, wenn ein Standort verloren geht.	"LLST: Standort verloren"

Codieren	Titel und Beschreibung der Nachricht	Siehe
OLST	Objekt verloren: Ein angeforderter Gegenstand kann nicht innerhalb des StorageGRID Systems gefunden werden.	"OLST: System hat Lost Object erkannt"
ORLM	Objektregeln erfüllt: Objektdaten werden gemäß den ILM-Regeln gespeichert.	"ORLM: Objektregeln erfüllt"
SADD	Sicherheitsüberprüfung deaktivieren: Die Protokollierung von Überwachungsnachrichten wurde deaktiviert.	"SADD: Security Audit deaktiviert"
SADE	Sicherheitsüberprüfung aktivieren: Die Protokollierung von Prüfnachrichten wurde wiederhergestellt.	"SADE: Sicherheits-Audit aktivieren"
SVRF	Objektspeicherüberprüfung fehlgeschlagen: Überprüfung durch einen Inhaltsblock fehlgeschlagen.	"SVRF: Objektspeicherüberprüfung fehlgeschlagen"
SVRU	Objektspeicher Verify Unbekannt: Unerwartete Objektdaten im Objektspeicher erkannt.	"SVRU: Objektspeicher überprüfen Unbekannt"
SYSD	Knotenstopp: Es wurde ein Herunterfahren angefordert.	"SYSD: Knoten stoppen"
SYST	Knoten stoppen: Ein Dienst hat einen graziösen Stopp initiiert.	"SYST: Knoten wird angehalten"
SYSU	Node Start: Ein Dienst gestartet. In der Meldung wird der Charakter des vorherigen Herunterfahrens angezeigt.	"SYSU: Knoten Start"
VLST	Vom Benutzer Initiiertes Volume Verloren: Das `/proc/CMSI/Volume_Lost` Befehl wurde ausgeführt.	"VLST: Vom Benutzer initiiertes Volumen verloren"

Verwandte Informationen

"LKCU: Objektbereinigung überschrieben"

Sie sollten mit Audit-Meldungen vertraut sein, die zur Objektspeicheraudits-Kategorie gehören. Dies sind Ereignisse, die mit der Speicherung und dem Management von Objekten innerhalb des StorageGRID Systems zusammenhängen. Dazu zählen Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Verifizierungen.

Codieren	Beschreibung	Siehe
APCT	Archiv aus Cloud-Tier: Archivierte Objektdaten werden aus einem externen Archiv-Storage-System gelöscht, das über die S3-API eine Verbindung zur StorageGRID herstellt.	"APCT: Löschen von Archiven aus der Cloud-Ebene"
ARCB	Archiv Objekt abrufen Begin: Der ARC-Dienst beginnt den Abruf von Objektdaten aus dem externen Archivspeichersystem.	"ARCB: Archiv Objekt abrufen beginnen"
ARCE	Archivobjekt Retrieve End: Objektdaten wurden von einem externen Archivspeichersystem abgerufen, und der ARC-Dienst meldet den Status des Abruffvorgangs.	"ARCE: Archiv Objekt abrufen Ende"
ARCT	Archive Retrieve von Cloud-Tier: Archivierte Objektdaten werden von einem externen Archiv-Storage-System abgerufen, das über die S3-API eine Verbindung zur StorageGRID herstellt.	"ARCT: Archiv Abrufen aus Cloud-Tier"
AREM	Archiv Objekt entfernen: Ein Inhaltsblock wurde erfolgreich oder erfolglos aus dem externen Archiv-Speichersystem gelöscht.	"ARM: Archivobjekt Entfernen"
ASCE	Archiv Objekt Store Ende: Ein Inhaltsblock wurde auf das externe Archivspeichersystem geschrieben und der ARC-Dienst meldet den Status des Schreibvorgangs.	"ASCE: Archiv-Objektspeicher Ende"

Codieren	Beschreibung	Siehe
ASCT	Archivspeicher Cloud-Tier: Objektdaten werden in einem externen Archiv-Storage-System gespeichert, das über die S3-API eine Verbindung zur StorageGRID herstellt.	"ASCT: Archivspeicher Cloud-Tier"
ATCE	Archive Object Store Begin: Das Schreiben eines Inhaltsblocks in einen externen Archiv-Speicher hat begonnen.	"ATCE: Archiv-Objektspeicher beginnen"
AVCC	Archiv Validierung der Cloud-Tier-Konfiguration: Die angegebenen Account- und Bucket-Einstellungen wurden erfolgreich oder nicht erfolgreich validiert.	"AVCC: Archiv Validierung der Cloud-Tier-Konfiguration"
CBSES	Objekt Send End: Die Quelleinheit hat einen Grid-Node zum Grid-Node-Datentransfer abgeschlossen.	"CBSE: Objekt Senden Ende"
CBRE	Empfang des Objekts: Die Zieleinheit hat einen Grid-Node zum Datentransfer des Grid-Node abgeschlossen.	"CBRE: Das Objekt erhält das Ende"
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	"SCMT: Objekt Store Commit"
SREM	Objektspeicher Remove: Ein Inhaltsblock wurde von einem Grid-Knoten gelöscht und kann nicht mehr direkt angefordert werden.	"SREM: Objektspeicher Entfernen"

Client liest Audit-Meldungen

Client-Read-Audit-Meldungen werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Abrufen eines Objekts vorgibt.

Codieren	Beschreibung	Verwendet von	Siehe
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SGET S3 ABRUFEN"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	S3-Client	"SHEA: S3 KOPF"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten.	Swift Client	"WGET: Schneller ERHALTEN"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.	Swift Client	"WHEA: Schneller KOPF"

Audit-Meldungen des Clients schreiben

Audit-Meldungen zu Clientschreibmeldungen werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Erstellen oder Ändern eines Objekts macht.

Codieren	Beschreibung	Verwendet von	Siehe
OVWR	Objekt-Überschreiben: Protokolliert eine Transaktion, um ein Objekt mit einem anderen Objekt zu überschreiben.	S3-Clients Swift Clients	"OVWR: Objektüberschreibung"

Codieren	Beschreibung	Verwendet von	Siehe
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SDEL: S3 LÖSCHEN"
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zur Wiederherstellung eines Objekts aus AWS Glacier Storage in einem Cloud Storage Pool.	S3-Client	"SPOS: S3-BEITRAG"
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen. **Hinweis:** Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	"SPUT: S3 PUT"
SUPD	Aktualisierte S3 Metadaten: Protokolliert eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes Objekt oder Bucket.	S3-Client	"SUPD: S3-Metadaten wurden aktualisiert"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	Swift Client	"WDEL: Swift LÖSCHEN"

Codieren	Beschreibung	Verwendet von	Siehe
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.	Swift Client	"WPUT: Schnell AUSGEDRÜCKT"

Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API.

Codieren	Titel und Beschreibung der Nachricht	Siehe
MGAU	Management-API-Audit-Nachricht: Ein Protokoll von Benutzeranfragen.	"MGAU: Management-Audit-Nachricht"

Audit-Meldungen

Wenn Systemereignisse auftreten, generiert das StorageGRID System Audit-Meldungen und zeichnet sie im Revisionsprotokoll auf.

APCT: Löschen von Archiven aus der Cloud-Ebene

Diese Meldung wird erzeugt, wenn archivierte Objektdaten aus einem externen Storage-System gelöscht werden, das eine Verbindung zur StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den gelöschten Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte. Gibt immer 0 zurück.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Eindeutige Kennung (UUID) des Cloud-Tiers, aus dem das Objekt gelöscht wurde.

ARCB: Archiv Objekt abrufen beginnen

Diese Meldung wird erzeugt, wenn eine Anfrage zum Abrufen der archivierten Objektdaten gestellt wird und der Abrufvorgang beginnt. Abrufanfragen werden sofort bearbeitet, können jedoch neu geordnet werden, um die Effizienz des Abrufs von linearen Medien wie z. B. Bandmedien zu verbessern.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivspeichersystem abgerufen werden soll.
RSLT	Ergebnis	Zeigt das Ergebnis des Speicherabrufs an. Aktuell definierter Wert ist:SUCS: Die Inhaltsanforderung wurde empfangen und zum Abruf in die Warteschlange gestellt.

Diese Überwachungsmeldung markiert den Zeitpunkt eines Archivabrufs. Damit können Sie die Nachricht mit einer entsprechenden ARCE-End-Nachricht abgleichen, um die Dauer des Archivabrufs zu bestimmen und ob der Vorgang erfolgreich war.

ARCE: Archiv Objekt abrufen Ende

Diese Meldung wird erzeugt, wenn ein Versuch des Archiv-Knotens, Objektdaten von einem externen Archivspeichersystem abzurufen, abgeschlossen wird. Wenn die Meldung erfolgreich ist, zeigt die Meldung an, dass die angeforderten Objektdaten vollständig aus dem Archivverzeichnis gelesen und erfolgreich verifiziert wurden. Nachdem die Objektdaten abgerufen und verifiziert wurden, werden sie an den anfragenden Service geliefert.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivspeichersystem abgerufen werden soll.
VLID	Volume-Kennung	Die Kennung des Volumes, auf dem die Daten archiviert wurden.Wenn kein Archivverzeichnis für den Inhalt gefunden wird, wird eine Volume-ID von 0 zurückgegeben.

Codieren	Feld	Beschreibung
RSLT	Abrufergebnis	Der Abschlussstatus des Archivabrufs: • ERFOLGREICH • VRFL: Fehlgeschlagen (Objektverifizierung fehlgeschlagen) • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • STORNO: Fehlgeschlagen (Abrufvorgang abgebrochen) • GERR: Fehlgeschlagen (allgemeiner Fehler)

Wenn Sie diese Nachricht mit der entsprechenden ARCB-Nachricht abstimmen, können Sie die Zeit angeben, die für den Archivabruf benötigt wurde. Diese Meldung gibt an, ob der Abruf erfolgreich war, und im Falle eines Fehlers die Ursache für das Abrufen des Inhaltsblocks.

ARCT: Archiv Abrufen aus Cloud-Tier

Diese Meldung wird generiert, wenn archivierte Objektdaten von einem externen Archiv-Storage-System abgerufen werden, das eine Verbindung mit der StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den abgerufenen Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte. Der Wert ist nur für erfolgreiche Abrufen genau.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Unique Identifier (UUID) des externen Archivspeichersystems.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

ARM: Archivobjekt Entfernen

Die Meldung „Archiv Objekt entfernen“ zeigt an, dass ein Inhaltsblock erfolgreich oder nicht erfolgreich von einem Archiv-Knoten gelöscht wurde. Wenn das Ergebnis erfolgreich ist, hat der Archivknoten das externe Archivspeichersystem erfolgreich darüber informiert, dass StorageGRID einen Objektspeicherort freigegeben hat. Ob das Objekt aus dem externen Archivspeichersystem entfernt wird, hängt vom Systemtyp und dessen Konfiguration ab.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivmediensystem abgerufen werden soll.
VLID	Volume-Kennung	Die Kennung des Volumes, auf dem die Objektdaten archiviert wurden.
RSLT	Ergebnis	Der Abschlussstatus des Löschvorgangs für das Archiv: • ERFOLGREICH • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • GERR: Fehlgeschlagen (allgemeiner Fehler)

ASCE: Archiv-Objektspeicher Ende

Diese Meldung zeigt an, dass das Schreiben eines Inhaltsblocks in ein externes Archiv-Speichersystem beendet ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die Kennung des Inhaltsblocks, der auf dem externen Archivspeichersystem gespeichert ist.
VLID	Volume-Kennung	Die eindeutige Kennung des Archiv-Volume, auf das die Objektdaten geschrieben werden.

Codieren	Feld	Beschreibung
VREN	Überprüfung Aktiviert	Zeigt an, ob eine Überprüfung für Inhaltsblöcke durchgeführt wird. Aktuell definierte Werte sind: • VENA: Die Überprüfung ist aktiviert • VDSA: Die Überprüfung ist deaktiviert
MCLS	Management-Klasse	Eine Zeichenfolge, die die TSM-Managementklasse identifiziert, der der Inhaltsblock zugeordnet ist, falls zutreffend.
RSLT	Ergebnis	Zeigt das Ergebnis des Archivierungsvorgangs an. Aktuell definierte Werte sind: • ERFOLGREICH (Archivierungsprozess erfolgreich) • OFFL: Fehlgeschlagen (Archivierung ist offline) • VRFL: Fehlgeschlagen (Objektüberprüfung fehlgeschlagen) • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • GERR: Fehlgeschlagen (allgemeiner Fehler)

Diese Überwachungsmeldung bedeutet, dass der angegebene Inhaltsblock auf das externe Archivspeichersystem geschrieben wurde. Wenn der Schreibvorgang fehlschlägt, liefert das Ergebnis grundlegende Informationen zur Fehlerbehebung über den Fehlerort. Ausführlichere Informationen zu Archivfehlern finden Sie unter Untersuchung der Attribute von Archivierungs-Knoten im StorageGRID System.

ASCT: Archivspeicher Cloud-Tier

Diese Meldung wird generiert, wenn archivierte Objektdaten in einem externen Storage-System gespeichert werden, das eine Verbindung mit StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den abgerufenen Inhaltsblock.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Unique Identifier (UUID) des Cloud-Tiers, in dem der Inhalt gespeichert wurde.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

ATCE: Archiv-Objektspeicher beginnen

Diese Meldung weist darauf hin, dass das Schreiben eines Inhaltsblocks in einen externen Archivspeicher gestartet wurde.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des zu archivierenden Inhaltsblocks.
VLID	Volume-Kennung	Die eindeutige Kennung des Volumes, auf das der Inhaltsblock geschrieben wird. Wenn der Vorgang fehlschlägt, wird eine Volume-ID von 0 zurückgegeben.
RSLT	Ergebnis	Gibt das Ergebnis der Übertragung des Inhaltsblocks an. Aktuell definierte Werte sind: • ERFOLGREICH (Inhaltsblock erfolgreich gespeichert) • EXIS: Ignoriert (Inhaltsblock wurde bereits gespeichert) • ISFD: Fehlgeschlagen (nicht genügend Speicherplatz) • STER: Fehlgeschlagen (Fehler beim Speichern der CBID) • OFFL: Fehlgeschlagen (Archivierung ist offline) • GERR: Fehlgeschlagen (allgemeiner Fehler)

AVCC: Archiv Validierung der Cloud-Tier-Konfiguration

Diese Meldung wird generiert, wenn die Konfigurationseinstellungen für einen Cloud Tiering – Simple Storage Service (S3)-Zieltyp validiert werden.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	UUID, die dem validierten externen Archivspeichersystem zugeordnet ist.

CBRB: Objekt empfangen beginnen

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn der Transfer eines Inhaltsblocks von einem Node zum anderen initiiert wird, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.

Codieren	Feld	Beschreibung
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBRE: Das Objekt erhält das Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.

Codieren	Feld	Beschreibung
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung endete aufgrund des Empfangs von beschädigten oder ungültigen Daten (kann auf Manipulation hinweisen)

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu

lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

CBSB: Objektsendebeginn

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen initiiert wird, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.

Codieren	Feld	Beschreibung
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBSE: Objekt Senden Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.

Codieren	Feld	Beschreibung
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung endete aufgrund des Empfangs von beschädigten oder ungültigen Daten (kann auf Manipulation hinweisen)

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

ECOC: Korrupte, mit Erasure codierte Datenfragment

Diese Meldung zeigt an, dass das System ein korruptes Datenfragment mit Löschungscode erkannt hat.

Codieren	Feld	Beschreibung
VCCO	VCS-ID	Der Name des VCS, der den beschädigten Teil enthält.
VLID	Volume-ID	Das RangeDB-Volume, das das korrupte Fragment mit Löschungscode enthält.
CCID	Block-ID	Der Identifier des beschädigten Fragments zur Löschung.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ETAF: Sicherheitsauthentifizierung fehlgeschlagen

Diese Meldung wird erzeugt, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung, über die die Authentifizierung fehlgeschlagen ist.
RUID	Benutzeridentität	Eine dienstabhängige Kennung, die die Identität des Remote-Benutzers darstellt.

Codieren	Feld	Beschreibung
RSLT	Ursachencode	Der Grund für den Fehler: SCNI: Sichere Verbindungseinrichtung fehlgeschlagen. CERM: Zertifikat fehlt. Zertifikat: Zertifikat war ungültig. CERE: Das Zertifikat ist abgelaufen. CERR: Zertifikat wurde widerrufen. CSGN: Die Zertifikatsignatur war ungültig. CSGU: Zertifikatssignator war unbekannt. UCRM: Benutzerkennungen fehlten. UCRI: Die Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht zulässig. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wenn eine Verbindung zu einem sicheren Service hergestellt wird, der TLS verwendet, werden die Anmeldeinformationen der Remote-Einheit mithilfe des TLS-Profils und der zusätzlichen Logik, die in den Service integriert ist, überprüft. Wenn diese Authentifizierung aufgrund ungültiger, unerwarteter oder unzulässiger Zertifikate oder Anmeldeinformationen fehlschlägt, wird eine Überwachungsmeldung protokolliert. Dies ermöglicht Abfragen für nicht autorisierte Zugriffsversuche und andere sicherheitsrelevante Verbindungsprobleme.

Die Meldung kann dazu führen, dass eine Remoteineinheit eine falsche Konfiguration hat oder dass versucht wird, ungültige oder unzulässige Anmeldedaten für das System vorzulegen. Diese Überwachungsmeldung sollte überwacht werden, um Versuche zu erkennen, unbefugten Zugriff auf das System zu erlangen.

GNRG: GNDS Registrierung

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst Informationen über sich selbst im StorageGRID-System aktualisiert oder registriert hat.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.
GNTP	Gerätetyp	Der Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Modellversion des Geräts	Der String, der die Gerätemodellversion des Grid-Knotens im DMDL-Bundle identifiziert.
GNGP	Gruppieren	Die Gruppe, zu der der Grid-Knoten gehört (im Zusammenhang mit Verbindungskosten und Service-Query-Ranking).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Node.

Diese Meldung wird generiert, wenn ein Grid-Knoten seinen Eintrag im Grid-Knoten-Paket aktualisiert.

GNUR: GNDS Registrierung aufheben

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst nicht registrierte Informationen über sich selbst vom StorageGRID-System enthält.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.

GTED: Grid Task beendet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst die Verarbeitung der angegebenen Rasteraufgabe abgeschlossen hat und die Aufgabe in die Tabelle „Historisch“ verschoben hat. Wenn es sich um SUCS, ABRT oder ROLF handelt, wird eine entsprechende Überwachungsmeldung für die mit Grid Task gestartete Aufgabe angezeigt. Die anderen Ergebnisse zeigen, dass die Verarbeitung dieser Grid-Aufgabe nie gestartet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über den gesamten Lebenszyklus. **Hinweis:** die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: • SUCS: Die Grid-Aufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne einen Rollback-Fehler abgebrochen. • ROLF: Die Grid-Aufgabe wurde abgebrochen und konnte den Rollback-Vorgang nicht abschließen. • STORNO: Die Grid-Aufgabe wurde vom Benutzer vor dem Start abgebrochen. • EXPR: Der Grid-Task ist vor dem Start abgelaufen. • IVLD: Die Grid-Aufgabe war ungültig. • AUTH: Die Grid-Aufgabe war nicht zulässig. • DUPL: Die Grid-Aufgabe wurde als Duplikat abgelehnt.

GTST: Grid Task gestartet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst mit der Verarbeitung der angegebenen Grid-Aufgabe begonnen hat. Die Meldung „Audit“ folgt unmittelbar der Nachricht „Grid Task Submission Submitted“ für Grid-Aufgaben, die vom internen Grid Task Submission Service initiiert und für die automatische Aktivierung ausgewählt wurde. Für Grid-Aufgaben, die in die Tabelle „Ausstehend“ eingereicht werden, wird diese Meldung generiert, wenn der Benutzer die Grid-Aufgabe startet.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. **Hinweis:** die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: • SUCS: Die Grid-Aufgabe wurde erfolgreich gestartet.

GTSU: Grid Task übermittelt

Diese Überwachungsmeldung zeigt an, dass eine Grid-Aufgabe an den CMN-Dienst gesendet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Identifiziert eindeutig eine generierte Grid-Aufgabe und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. **Hinweis:** die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.

Codieren	Feld	Beschreibung
TTYP	Aufgabentyp	Der Typ der Rasteraufgabe.
TVER	Aufgabenversion	Eine Zahl, die die Version der Grid-Aufgabe angibt.
TDSC	Aufgabenbeschreibung	Eine vom Menschen lesbare Beschreibung der Grid-Aufgabe.
VATS	Gültig Nach Zeitstempel	Die früheste Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX-Zeit), zu der die Grid-Aufgabe gültig ist.
VBTS	Gültig Vor Zeitstempel	Die letzte Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX Zeit), zu der die Grid-Aufgabe gültig ist.
TSRC	Quelle	Die Quelle der Aufgabe: • TXTB: Die Grid-Aufgabe wurde über das StorageGRID-System als signierter Textblock gesendet. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submit Service übermittelt.
ACTV	Aktivierungstyp	Die Art der Aktivierung: • AUTO: Die Grid-Aufgabe wurde zur automatischen Aktivierung eingereicht. • PEND: Die Grid-Aufgabe wurde in die ausstehende Tabelle übermittelt. Dies ist die einzige Möglichkeit für die TXTB-Quelle.
RSLT	Ergebnis	Das Ergebnis der Einreichung: • SUCS: Die Grid-Aufgabe wurde erfolgreich übermittelt. • FAIL: Die Aufgabe wurde direkt in die historische Tabelle verschoben.

IDEL: ILM gestartet Löschen

Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.

Die IDEL-Nachricht wird in einer der folgenden Situationen erzeugt:

- **Für Objekte in konformen S3-Buckets**: Diese Meldung wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, da der Aufbewahrungszeitraum abgelaufen ist (vorausgesetzt, die Einstellung zum automatischen Löschen ist aktiviert und die Legal Hold ist deaktiviert).
- **Für Objekte in nicht konformen S3 Buckets oder Swift Containern**. Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet, da derzeit keine Platzierungsanweisungen in der aktiven ILM-Richtlinie für das Objekt gelten.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CMPA	Compliance: Automatisches Löschen	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true) geben an, ob ein konformes Objekt automatisch gelöscht werden soll, wenn der Aufbewahrungszeitraum endet, es sei denn, der Bucket befindet sich unter einer gesetzlichen Aufbewahrungspflichten.
CMPL	Einhaltung: Gesetzliche Aufbewahrungspflichten	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true), die angeben, ob der Bucket derzeit unter einer gesetzlichen Aufbewahrungspflichten steht.
CMPR	Compliance: Aufbewahrungszeitraum	Nur für Objekte in S3-konformen Buckets. Die Länge der Aufbewahrungsdauer des Objekts in Minuten.
CTME	Compliance: Aufnahmezeit	Nur für Objekte in S3-konformen Buckets. Die Aufnahmezeit des Objekts. Sie können den Aufbewahrungszeitraum in Minuten zu diesem Wert hinzufügen, um zu bestimmen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte mit Erasure-Coding-Verfahren, die Profil-ID für das Erasure-Coding-Verfahren und die Gruppen-ID für das Erasure-Coding-Verfahren, die auf die Daten des Objekts angewendet werden. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	• Wenn ein Objekt in einem konformen S3-Bucket automatisch gelöscht wird, weil der Aufbewahrungszeitraum abgelaufen ist, ist dieses Feld leer. • Wenn das Objekt gelöscht wird, da derzeit keine Anweisungen zur Platzierung für das Objekt vorhanden sind, zeigt dieses Feld den vom Menschen lesbaren Namen der letzten ILM-Regel an, die auf das Objekt angewendet wurde.

Codieren	Feld	Beschreibung
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

LKCU: Objektbereinigung überschrieben

Diese Meldung wird generiert, wenn StorageGRID ein überschreibtes Objekt entfernt, das zuvor zur Freigabe von Speicherplatz erforderlich war. Ein Objekt wird überschrieben, wenn ein S3- oder Swift-Client ein Objekt in einen Pfad schreibt, der bereits ein Objekt enthält. Die Entfernung erfolgt automatisch und im Hintergrund.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
LTYP	Art der Bereinigung	*Nur zur internen Verwendung.*
LUID	Objekt-UUID entfernt	Die Kennung des entfernten Objekts.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell Eindeutige Kennung	Die Kennung des noch vorhandenen Objekts. Dieser Wert ist nur verfügbar, wenn das Objekt nicht gelöscht wurde.

LLST: Standort verloren

Diese Meldung wird immer dann erzeugt, wenn ein Speicherort für eine Objektkopie (repliziert oder Erasure Coding) nicht gefunden werden kann.

Codieren	Feld	Beschreibung
CBIL	CBID	Die betroffene CBID.
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
UUID	Universally Unique ID	Die Kennung des betroffenen Objekts im StorageGRID-System.
ECPR	Verfahren Zur Einhaltung Von Datenkonsistenz	Für Erasure-Coding-Objektdaten. Die ID des verwendeten Erasure Coding-Profils.
LTYP	Positionstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für Erasure-codierte Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten
PCLD	Pfad zu repliziertem Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten. Wird nur zurückgegeben, wenn LTYP einen Wert von CLDI (d.h. für replizierte Objekte) hat. Nimmt das Formular an `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Ergebnis	Immer KEINE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
TSRC	Auslösequelle	BENUTZER: Benutzer ausgelöst SYST: System ausgelöst

MGAU: Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API. Jede Anfrage, die keine GET- oder HEAD-Anforderung an die API ist, protokolliert eine Antwort mit dem Benutzernamen, der IP und der Art der Anfrage an die API.

Codieren	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domain-Name	Der Host-Domain-Name.
MPAT	AnfraPfad	Der Anfraspfad.
MPQP	Abfrageparameter anfordern	Die Abfrageparameter für die Anforderung.
MRBD	Text anfordern	Der Inhalt des Anforderungsinstanz. Während der Antwortkörper standardmäßig protokolliert wird, wird der Anforderungskörper in bestimmten Fällen protokolliert, wenn der Antwortkörper leer ist. Da die folgenden Informationen im Antwortkörper nicht verfügbar sind, werden sie von der Anforderungsstelle für die folgenden POST-Methoden übernommen: • Benutzername und Konto-ID in **POST authorize** • Neue Subnetze-Konfiguration in **POST /Grid/Grid-Networks/Update** • Neue NTP-Server in **POST /grid/ntp-Servers/Update** • Ausgemusterte Server-IDs in **POST /Grid/Servers/Decommission** **Hinweis:** sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MRMD	Anforderungsmethode	Die HTTP-Anforderungsmethode: • POST • PUT • Löschen • PATCH

Codieren	Feld	Beschreibung
MRSC	Antwortcode	Der Antwortcode.
MRSP	Antwortkörper	Der Inhalt der Antwort (der Antwortkörper) wird standardmäßig protokolliert. **Hinweis:** sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MSIP	Quell-IP-Adresse	Die Client (Quell-) IP-Adresse.
MUUN	User-URN	Der URN (einheitlicher Ressourcenname) des Benutzers, der die Anforderung gesendet hat.
RSLT	Ergebnis	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.

OLST: System hat Lost Object erkannt

Diese Meldung wird erzeugt, wenn der DDS-Dienst keine Kopien eines Objekts im StorageGRID-System finden kann.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des verlorenen Objekts.
NID	Node-ID	Falls verfügbar, der letzte bekannte direkte oder Nearline-Speicherort des verlorenen Objekts. Es ist möglich, nur die Knoten-ID ohne eine Volume-ID zu haben, wenn die Volume-Informationen nicht verfügbar sind.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Falls verfügbar: Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
UUID	Universally Unique ID	Die Kennung des verlorenen Objekts im StorageGRID System.
VOLI	Volume-ID	Falls verfügbar, die Volume-ID des Speicherknoten oder Archiv-Knotens für den letzten bekannten Speicherort des verlorenen Objekts.

ORLM: Objektregeln erfüllt

Diese Meldung wird generiert, wenn das Objekt erfolgreich gespeichert und wie durch die ILM-Regeln festgelegt kopiert wird.

> Die ORLM-Meldung wird nicht generiert, wenn ein Objekt erfolgreich mit der Regel 2 Kopien erstellen gespeichert wird, wenn eine andere Regel in der Richtlinie den erweiterten Filter Objektgröße verwendet.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.

Codieren	Feld	Beschreibung
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte mit Erasure-Coding-Verfahren, die Profil-ID für das Erasure-Coding-Verfahren und die Gruppen-ID für das Erasure-Coding-Verfahren, die auf die Daten des Objekts angewendet werden. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	Das von Menschen lesbare Etikett, das der ILM-Regel gegeben wurde, die auf dieses Objekt angewendet wurde.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Container-CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.

Codieren	Feld	Beschreibung
STAT	Status	Der Status des ILM-Betriebs. FERTIG: ILM-Vorgänge für das Objekt wurden abgeschlossen. DFER: Das Objekt wurde für zukünftige ILM-Neuevaluierungen markiert. PRGD: Das Objekt wurde aus dem StorageGRID-System gelöscht. NLOC: Die Objektdaten können nicht mehr im StorageGRID-System gefunden werden. Dieser Status kann darauf hinweisen, dass alle Kopien von Objektdaten fehlen oder beschädigt sind.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.

Die ORLM-Überwachungsmeldung kann für ein einzelnes Objekt mehrmals ausgegeben werden. Sie wird beispielsweise ausgegeben, wenn eines der folgenden Ereignisse stattfindet:

- ILM-Regeln für das Objekt sind dauerhaft erfüllt.
- ILM-Regeln für das Objekt werden für diese Epoche erfüllt.
- Das Objekt wurde durch ILM-Regeln gelöscht.
- Bei der Hintergrundüberprüfung wird erkannt, dass eine Kopie replizierter Objektdaten beschädigt ist. Das StorageGRID System führt eine ILM-Bewertung durch, um das beschädigte Objekt zu ersetzen.

Verwandte Informationen

"Objektaufnahme von Transaktionen"

"Löschen von Objekttransaktionen"

OVWR: Objektüberschreibung

Diese Meldung wird erzeugt, wenn ein externer (Client-angeforderter) Vorgang ein Objekt durch ein anderes Objekt überschrieben.

Codieren	Feld	Beschreibung
CBID	Kennung für Inhaltsblock (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des Objekts in Byte, das überschrieben wird.

Codieren	Feld	Beschreibung
OCBD	Kennung für Inhaltsblock (vorherige)	Die CBID für das vorherige Objekt.
UUID	Universally Unique ID (neu)	Die Kennung des neuen Objekts im StorageGRID System.
OUID	Universally Unique ID (vorherige)	Die Kennung für das vorherige Objekt innerhalb des StorageGRID-Systems.
PFAD	S3 oder Swift Objektpfad	Der S3- oder Swift-Objektpfad wird sowohl für das vorherige als auch für das neue Objekt verwendet
RSLT	Ergebniscode	Ergebnis der Transaktion Objekt überschreiben. Das Ergebnis ist immer: ERFOLGREICH

SADD: Security Audit deaktiviert

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung der Überwachungsmeldungen deaktiviert hat; Audit-Meldungen werden nicht mehr erfasst oder geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, mit der das Audit deaktiviert wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Deaktivieren der Revisionsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Meldung besagt, dass die Protokollierung zuvor aktiviert, aber jetzt deaktiviert wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt (SADE) und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SADE: Sicherheits-Audit aktivieren

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung von Überwachungsmeldungen wiederhergestellt hat; Audit-Meldungen werden erneut erfasst und geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, die zum Aktivieren des Audits verwendet wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Aktivieren der Audit-Protokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Nachricht bedeutet, dass die Protokollierung vorher deaktiviert (SADD) war, aber jetzt wiederhergestellt wurde. Dies wird in der Regel nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SCMT: Objekt Store Commit

Grid-Inhalte werden erst dann zur Verfügung gestellt oder als gespeichert erkannt, wenn sie bereitgestellt wurden (was bedeutet, dass sie dauerhaft gespeichert wurden). Dauerhaft gespeicherte Inhalte wurden vollständig auf Festplatte geschrieben und haben entsprechende Integritätsprüfungen bestanden. Diese Meldung wird ausgegeben, wenn ein Inhaltsblock auf den Speicher gesetzt wird.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der zu permanentem Speicher verpflichtet ist.
RSLT	Ergebniscode	Status zum Zeitpunkt, zu dem das Objekt auf Festplatte gespeichert wurde: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und überprüft wurde und nun angefordert werden kann. Er kann zur Nachverfolgung des Datenflusses im System eingesetzt werden.

SDEL: S3 LÖSCHEN

Wenn ein S3-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anfrage gestellt, um das angegebene Objekt oder den angegebenen Bucket zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.

Codieren	Feld	Beschreibung
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SGET S3 ABRUFEN

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anfrage gestellt, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
KLINGELTE	Bereichsleser	Nur für Bereichslesevorgänge. Gibt den Bereich der Bytes an, die von dieser Anforderung gelesen wurden. Der Wert nach dem Schrägstrich (/) zeigt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name

Codieren	Feld	Beschreibung
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.

Codieren	Feld	Beschreibung
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SHEA: S3 KOPF

Wenn ein S3-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, ob es sich um ein Objekt oder einen Bucket handelt und die Metadaten zu einem Objekt abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des überprüften Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.

Codieren	Feld	Beschreibung
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SPOS: S3-BEITRAG

Wenn ein S3-Client eine Anfrage zur WIEDERHERSTELLUNG NACH dem Objekt ausgibt, wird eine Anfrage gestellt, um ein Objekt aus AWS Glacier Storage in einem Cloud Storage Pool wiederherzustellen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der Anforderung ZUR Wiederherstellung DES POSTOBJEKTS. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Stellen Sie Informationen wieder her.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.

Codieren	Feld	Beschreibung
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Buckets gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern diese in der PUT Bucket-Anforderung vorhanden sind (gekürzt auf die ersten 1024 Zeichen)
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
LKEN	Objektsperre Aktiviert	Der Wert der Anfrageüberschrift `x-amz-bucket-object-lock-enabled`, Wenn vorhanden in DER PUT Bucket Anforderung.
LKLH	Gesetzliche Sperren Für Objekte	Der Wert der Anfrageüberschrift `x-amz-object-lock-legal-hold`, Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKMD	Aufbewahrungsmodus Für Objektsperre	Der Wert der Anfrageüberschrift `x-amz-object-lock-mode`, Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKRU	Objektsperre Bis Datum Beibehalten	Der Wert der Anfrageüberschrift `x-amz-object-lock-retain-until-date`, Wenn vorhanden in DER PUT-Objekt-Anforderung.
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.

Codieren	Feld	Beschreibung
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3KY	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Die neue Subressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).

Codieren	Feld	Beschreibung
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
ULID	Upload-ID	Nur in SPUT-Nachrichten für komplette mehrteilige Uploadvorgänge enthalten. Zeigt an, dass alle Teile hochgeladen und zusammengesetzt wurden.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Versionsnummer eines neuen Objekts, das in einem versionierten Bucket erstellt wurde Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.
VSST	Status Der Versionierung	Der neue Versionierungs-Status eines Buckets. Es werden zwei Zustände verwendet: "Aktiviert" oder "ausgesetzt". Operationen für Objekte enthalten dieses Feld nicht.

SREM: Objektspeicher Entfernen

Diese Meldung wird ausgegeben, wenn Inhalte aus einem persistenten Storage entfernt werden und nicht mehr über regelmäßige APIs zugänglich sind.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der aus dem permanenten Speicher gelöscht wurde.
RSLT	Ergebniscode	Gibt das Ergebnis der Aktionen zum Entfernen von Inhalten an. Der einzige definierte Wert ist: SUCS: Inhalt aus persistentem Storage entfernt

Diese Überwachungsmeldung bedeutet, dass ein bestimmter Inhaltsblock von einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Die Nachricht kann verwendet werden, um den Fluss gelöschter Inhalte innerhalb des Systems zu verfolgen.

SUPD: S3-Metadaten wurden aktualisiert

Diese Nachricht wird von der S3-API generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert. Die Meldung wird vom Server ausgegeben, wenn die Metadatenaktualisierung erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert des HTTP-Anfrageheaders Consistency-Control, falls in der Anfrage vorhanden, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: `urn:sgws:identity::03393893651506583485:root` Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Versionsnummer der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SVRF: Objektspeicherüberprüfung fehlgeschlagen

Diese Meldung wird ausgegeben, wenn ein Inhaltsblock den Verifizierungsprozess nicht erfolgreich durchführt. Jedes Mal, wenn replizierte Objektdaten von der Festplatte gelesen oder auf die Festplatte geschrieben werden, werden verschiedene Verifizierungsprüfungen durchgeführt, um sicherzustellen, dass die an den anfordernden Benutzer gesendeten Daten mit den ursprünglich im System aufgenommenen Daten

identisch sind. Wenn eine dieser Prüfungen fehlschlägt, werden die beschädigten replizierten Objektdaten vom System automatisch gesperrt, um ein erneuten Abruf der Daten zu verhindern.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, bei der die Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Fehlertyp Verifikation: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Prüfung des Hashbasierten Nachrichtenauthentifizierungscodes (HMAC) fehlgeschlagen. EHSH: Unerwarteter verschlüsselter Content-Hash. PHSH: Unerwarteter Originalinhalt Hash. SEQC: Falsche Datensequenz auf der Festplatte. PERR: Ungültige Struktur der Festplattendatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.

Hinweis: Diese Nachricht sollte genau überwacht werden. Fehler bei der Inhaltsprüfung können auf Manipulationen an Inhalten oder drohende Hardwareausfälle hinweisen.

Um zu bestimmen, welcher Vorgang die Meldung ausgelöst hat, lesen Sie den Wert des FELDS AMID (Modul-ID). Beispielsweise gibt ein SVFY-Wert an, dass die Meldung vom Storage Verifier-Modul generiert wurde, d. h. eine Hintergrundüberprüfung und STOR zeigt an, dass die Meldung durch den Abruf von Inhalten ausgelöst wurde.

SVRU: Objektspeicher überprüfen Unbekannt

Die Storage-Komponente des LDR-Service scannt kontinuierlich alle Kopien replizierter Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Codieren	Feld	Beschreibung
FPTH	Dateipfad	Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

Hinweis: die SVRU: Objektspeicher überprüfen Unbekannte Überwachungsmeldung sollte genau überwacht werden. Es bedeutet, dass im Objektspeicher unerwartete Kopien von Objektdaten erkannt wurden. Diese Situation sollte sofort untersucht werden, um festzustellen, wie diese Kopien erstellt wurden, da sie auf den Versuch hinweisen können, Inhalte zu manipulieren oder Hardware-Ausfälle anzufangen.

SYSD: Knoten stoppen

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde. Normalerweise wird diese Meldung erst nach einem späteren Neustart gesendet, da die Warteschlange für die Überwachungsmeldung vor dem Herunterfahren nicht gelöscht wird. Suchen Sie nach der SYST-Meldung, die zu Beginn der Abschaltsequenz gesendet wird, wenn der Dienst nicht neu gestartet wurde.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Das RSLT eines SYSD kann nicht auf ein „nicht ordnungsgemäßes“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYST: Knoten wird angehalten

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde und dass der Dienst seine Abschaltsequenz initiiert hat. SYST kann verwendet werden, um festzustellen, ob das Herunterfahren angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das normalerweise nach dem Neustart des Dienstes gesendet wird).

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Der RSLT-Code einer SYST-Meldung kann nicht auf ein „nicht ordnungsgemäßes“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYSU: Knoten Start

Wenn ein Dienst neu gestartet wird, wird diese Meldung erzeugt, um anzugeben, ob die vorherige Abschaltung sauber (befahl) oder ungeordnet (unerwartet) war.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SUCS: Das System wurde sauber abgeschaltet. DSDN: Das System wurde nicht sauber heruntergefahren. VRGN: Das System wurde erstmals nach der Server-Installation (oder Neuinstallation) gestartet.

Die Meldung gibt nicht an, ob der Host-Server gestartet wurde, sondern nur der Reporting-Service. Diese Meldung kann verwendet werden, um:

- Diskontinuität im Prüfprotokoll erkennen.
- Ermitteln Sie, ob ein Service während des Betriebs ausfällt (da die verteilte Natur des StorageGRID Systems diese Fehler maskieren kann). Der Server Manager startet einen fehlgeschlagenen Dienst automatisch neu.

VLST: Vom Benutzer initiiertes Volumen verloren

Diese Meldung wird ausgegeben, wenn der `/proc/CMSI/Volume_Lost` Befehl wird ausgeführt.

Codieren	Feld	Beschreibung
VOLL	Volume Identifier Lower	Das untere Ende des betroffenen Volumenbereichs oder eines einzelnen Volumens.

Codieren	Feld	Beschreibung
VOLU	Volume Identifier Ober	Das obere Ende des betroffenen Volumenbereichs. Gleich VOLL wenn ein einzelnes Volume ist.
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
LTYP	Positionstyp	„CLDI“ (Online) oder „CLNL“ (Nearline). Wenn nicht angegeben, ist die Standardeinstellung „CLDI“.
RSLT	Ergebnis	Immer „KEINE“. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

WDEL: Swift LÖSCHEN

Wenn ein Swift-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anfrage zum Entfernen des angegebenen Objekts oder Containers gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.

Codieren	Feld	Beschreibung
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WGET: Schneller ERHALTEN

Wenn ein Swift-Client eine GET-Transaktion ausgibt, wird eine Anfrage gestellt, um ein Objekt abzurufen, die Objekte in einem Container aufzulisten oder die Container in einem Konto aufzulisten. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername. Dieses Feld wird nicht von Operationen für Accounts berücksichtigt.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WHEA: Schneller KOPF

Wenn ein Swift-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, ob ein Konto, Container oder Objekt vorhanden ist, und alle relevanten Metadaten abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der HAUPTTRANSAKTION. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername. Dieses Feld wird nicht von Operationen für Accounts berücksichtigt.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.

Codieren	Feld	Beschreibung
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WPUT: Schnell AUSGEDRÜCKT

Wenn ein Swift-Client eine PUT-Transaktion ausgibt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Containers gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. **Hinweis:** `X-Forwarded-For` Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der `X-Forwarded-For` Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH

Codieren	Feld	Beschreibung
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.