



Monitoring und Fehlerbehebung

StorageGRID

NetApp
April 10, 2024

Inhalt

Monitoring und Fehlerbehebung	1
Überwachung und Fehlerbehebung: Übersicht	1
Zeigen Sie das Dashboard an	1
Zeigen Sie die Seite Knoten an	5
Informationen, die Sie regelmäßig überwachen sollten	40
Verwalten von Meldungen und Alarmen	77
Konfigurieren von Überwachungsmeldungen und Protokollzielen	126
Verwenden Sie einen externen Syslog-Server	131
Verwenden Sie SNMP-Überwachung	146
Erfassung zusätzlicher StorageGRID-Daten	161
Fehler in einem StorageGRID System beheben	195
Alerts Referenz	264
Häufig verwendete Prometheus-Kennzahlen	304
Alarmreferenz (Altsystem)	310
Referenz für Protokolldateien	343

Monitoring und Fehlerbehebung

Überwachung und Fehlerbehebung: Übersicht

Anhand dieser Anweisungen können Sie ein StorageGRID System überwachen sowie eventuelle Probleme bewerten und beheben.

Informationen zu diesen Anweisungen

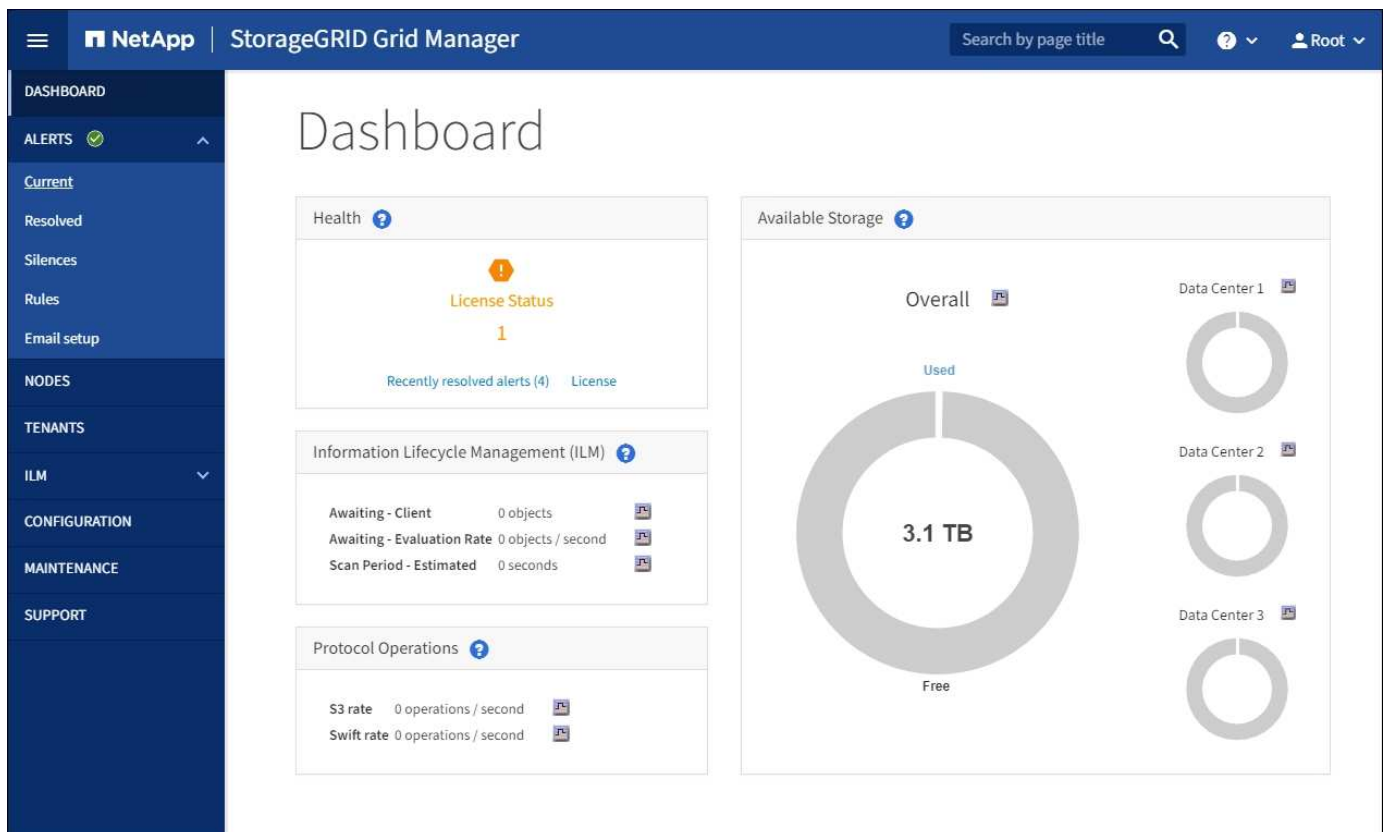
In diesen Anweisungen wird die Verwendung von Grid Manager zum Überwachen eines StorageGRID-Systems beschrieben. Sie erfahren, welche Informationen Sie regelmäßig überwachen sollten, wie Sie Warnmeldungen und ältere Alarme verwalten, wie Sie SNMP für das Monitoring verwenden und wie Sie zusätzliche StorageGRID-Daten erhalten, einschließlich Metriken und Diagnosen.

Sie beschreiben außerdem die Fehlerbehebung für ein StorageGRID System und beschreiben alle Systemmeldungen, ältere Alarme und Protokolldateien.

Befolgen Sie diese Anweisungen, wenn Sie nach der Installation ein StorageGRID-System überwachen und unterstützen.

Zeigen Sie das Dashboard an

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.




Suchfeld

Mit dem Feld **Suche** in der Kopfzeile können Sie schnell zu einem bestimmten Seiten- oder Seitenleiste-Eintrag im Grid Manager navigieren. Sie können beispielsweise **key** eingeben, um auf die Seite Key Management Server zuzugreifen.

Systemzustand

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
<p>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.</p>	<p>Möglicherweise werden mindestens ein der folgenden Links angezeigt:</p> <ul style="list-style-type: none"> • 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 ALERTS Current 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 MAINTENANCE System Lizenz anzuzeigen. 	<ul style="list-style-type: none"> • Überwachen Sie die Status der Node-Verbindung • Anzeigen aktueller Warnmeldungen • Anzeigen von behobenen Warnmeldungen • Anzeigen von älteren Alarmen • StorageGRID verwalten


Bereich „Verfügbare Lagerung“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
<p>Zeigt die verfügbare und genutzte Speicherkapazität im gesamten Grid an, nicht einschließlich Archivmedien.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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 NODES. Anschließend können Sie die Registerkarte „Storage“ für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen. 	<ul style="list-style-type: none"> • Öffnen Sie die Registerkarte „Speicher“ • Monitoring der Storage-Kapazität

Bereich „Information Lifecycle Management“ (ILM)

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
<p>Zeigt die aktuellen ILM-Vorgänge und ILM-Warteschlangen für das System an. Sie können diese Informationen für das Monitoring der Arbeitsbelastung Ihres Systems verwenden.</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Um Details anzuzeigen, wählen Sie NODES. 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. 	<ul style="list-style-type: none"> • Zeigen Sie die Registerkarte ILM an • StorageGRID verwalten.

Bereich „Protokollbetrieb“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
<p>Zeigt die Anzahl der protokollspezifischen Vorgänge (S3 und Swift) an, die vom System durchgeführt werden.</p> <p>Sie können diese Informationen nutzen, um die Workloads und die Effizienz Ihres Systems zu überwachen. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.</p>	<ul style="list-style-type: none"> • Um Details anzuzeigen, wählen Sie NODES. 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. 	<ul style="list-style-type: none"> • Zeigen Sie die Registerkarte Objekte an • S3 verwenden • Verwenden Sie Swift

Zeigen Sie die Seite Knoten an


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.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
DC1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	6%
DC1-ARC1	Archive Node	—	—	1%
DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%
DC2	Site	0%	0%	—


Die Tabelle Knoten enthält alle Standorte und Knoten Ihres StorageGRID Systems. Für jeden Node werden zusammenfassende Informationen angezeigt. Wenn ein Node über eine aktive Warnmeldung verfügt, wird neben dem Node-Namen ein Symbol angezeigt. Wenn der Knoten verbunden ist und keine aktiven Warnmeldungen enthält, wird kein Symbol angezeigt.

Symbole für Verbindungsstatus

- **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekanntem 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.

Wenn ein Knoten vom Raster getrennt wird, wird möglicherweise eine zugrunde liegende Warnmeldung angezeigt, aber nur das Symbol „not connected“ wird angezeigt. Um die aktiven Warnmeldungen für einen Node anzuzeigen, wählen Sie den Node aus.

Warnungssymbole

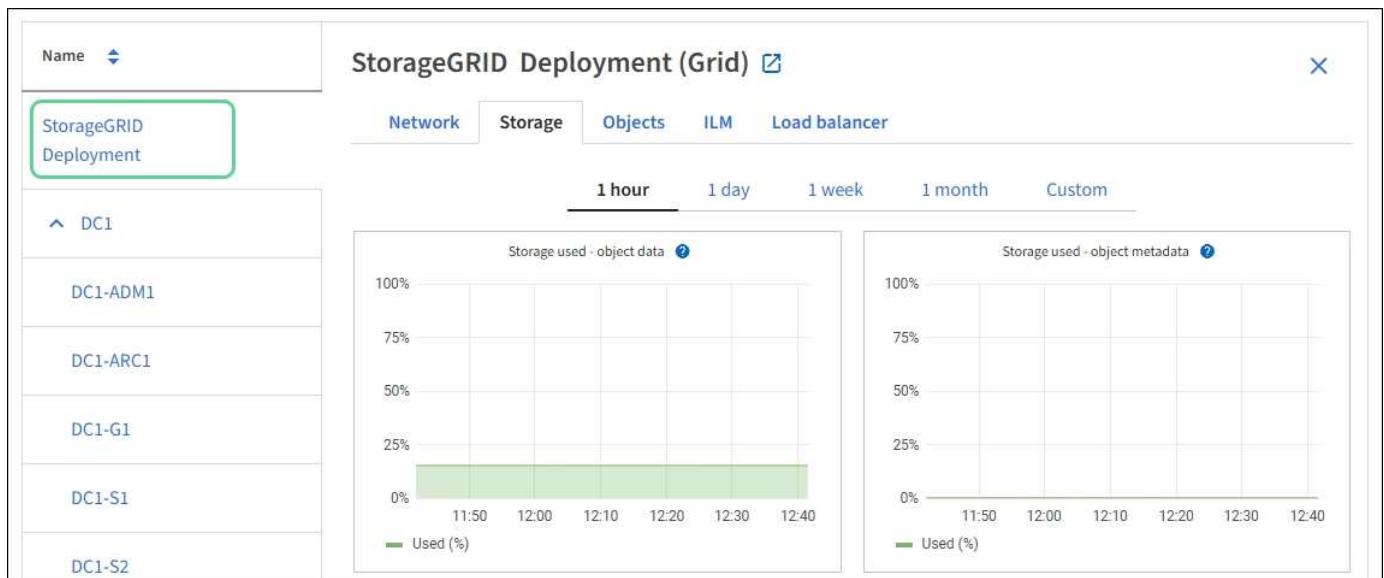
Wenn eine aktive Warnmeldung für einen Node vorhanden ist, wird neben dem Node-Namen eines der folgenden Symbole angezeigt:

- **Kritisch** : Es 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 schwerwiegenden Problem führen.

Anzeigen von Details zu einem System, Standort oder Node

Um die verfügbaren Informationen anzuzeigen, wählen Sie den Namen des Rasters, des Standorts oder Nodes wie folgt aus:

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



Zeigen Sie die Registerkarte Übersicht an

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

Die Registerkarte Übersicht wird für alle Knoten angezeigt.

Node-Informationen

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

The screenshot displays the 'Overview' tab for a Storage Node named 'DC1-S2'. The node is currently 'Connected'. Storage usage is shown as 26% for Object data and 0% for Object metadata. The software version is 11.6.0 and the IP address is 10.224.1.227 on the eth0 interface.

Field	Value
Name:	DC1-S2
Type:	Storage Node
ID:	e12e3f95-da25-4c56-8ca1-ec796b3fdbd9
Connection state:	Connected
Storage used:	Object data: 26% Object metadata: 0%
Software version:	11.6.0
IP addresses:	10.224.1.227 - eth0 (Grid Network)

Die Übersichtsinformationen für einen Knoten umfassen Folgendes:

- **Name:** Der Hostname, der dem Knoten zugewiesen und im Grid Manager angezeigt wird.
- **Typ:** Node-Typ - Admin-Node, primärer 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.

- * Unbekannt* : Der Knoten ist aus einem unbekanntem 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.

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

◦ * Verbunden* : Der Knoten ist mit dem Raster verbunden.

- **Verwendeter Speicher:** Nur für Speicherknoten.
 - **Objektdaten:** Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der auf dem Speicherknoten verwendet wurde.
 - **Objektmetadaten:** Der Prozentsatz des insgesamt zulässigen Speicherplatzes für Objektmetadaten, die auf dem Speicherknoten verwendet wurden.
- **Software-Version:** Die Version von StorageGRID, die auf dem Knoten installiert ist.
- **HA-Gruppen:** Nur für Admin-Node und Gateway-Nodes. Wird angezeigt, wenn eine Netzwerkschnittstelle auf dem Knoten in einer Hochverfügbarkeitsgruppe enthalten ist und ob diese Schnittstelle die primäre Schnittstelle ist.
- **IP-Adressen:** Die IP-Adressen des Knotens. Klicken Sie auf **zusätzliche IP-Adressen anzeigen**, um die IPv4- und IPv6-Adressen und Schnittstellenzuordnungen des Knotens anzuzeigen.

Meldungen

Im Abschnitt „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.

Alert name	Severity	Time triggered	Current values
Low installed node memory The amount of installed memory on a node is low.	 Critical	11 hours ago	Total RAM size: 8.37 GB

Verwandte Informationen

[Überwachen Sie die Status der Node-Verbindung](#)

[Anzeigen aktueller Warnmeldungen](#)

[Zeigen Sie eine bestimmte Warnmeldung an](#)

Zeigen Sie die Registerkarte Hardware an

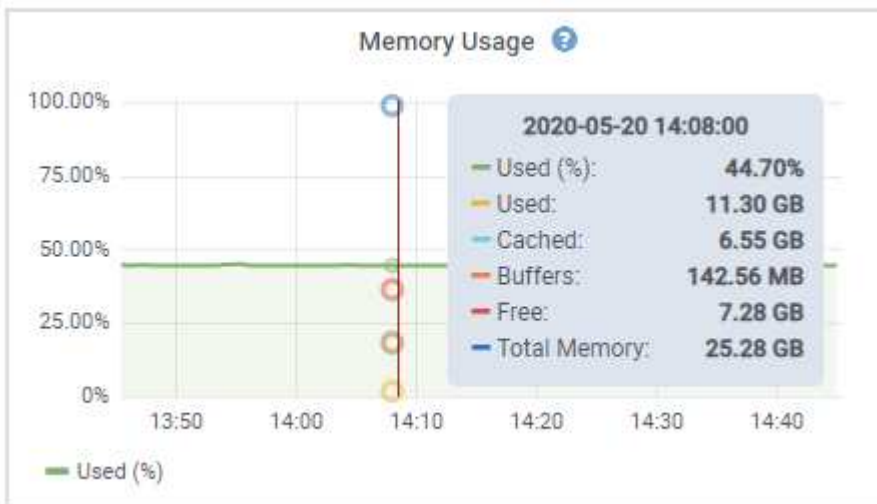
Auf der Registerkarte Hardware werden für jeden Node CPU-Auslastung und Arbeitsspeicherauslastung sowie zusätzliche Hardware-Informationen über Appliances angezeigt.

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.

Zeigen Sie Informationen zu Appliance Storage Nodes an

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

Schritte

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

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

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

DC2-SGA-010-096-106-021 (Storage Node) [↗](#)



Overview Hardware Network Storage Objects ILM Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021
Type: Storage Node
ID: f0890e03-4c72-401f-ae92-245511a38e51
Connection state: Connected
Storage used: Object data 7% [?](#)
Object metadata 5% [?](#)
Software version: 11.6.0 (build 20210915.1941.afce2d9)
IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

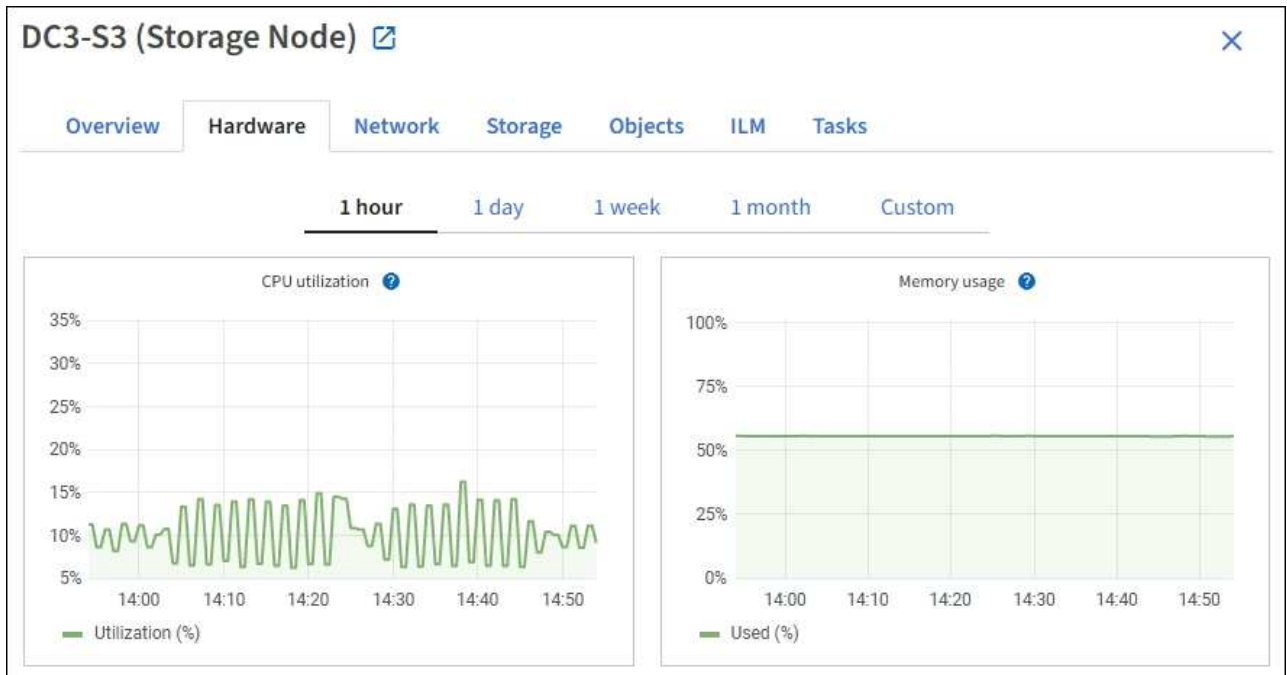
Interface ⌵	IP address ⌵
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ⌵	Severity ? ⌵	Time triggered ⌵	Current values
ILM placement unachievable ↗	Major	2 hours ago ?	A placement instruction in an ILM rule cannot be achieved for certain objects.

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

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



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



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

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

StorageGRID Appliance

Appliance model: ?	SG5660	
Storage controller name: ?	StorageGRID-SGA-Lab11	
Storage controller A management IP: ?	10.224.2.192	
Storage controller WWID: ?	600a098000a4a707000000005e8ed5fd	
Storage appliance chassis serial number: ?	1142FG000135	
Storage controller firmware version: ?	08.40.60.01	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	2.00 TB	
Storage RAID mode: ?	RAID6	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller serial number: ?	SV54365519	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?
SN SV13304553	0	Nominal	N/A

Feld in der Appliance-Tabelle	Beschreibung
Appliance-Modell	Die Modellnummer dieser StorageGRID Appliance, dargestellt in der SANtricity Software.
Name des Storage Controllers	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.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Controller B Management-IP	<p>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.</p> <p>Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B</p>
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.
Version der Storage Controller-Firmware	Die Version der Firmware auf dem Storage Controller für dieses Gerät.
Storage-Hardware	<p>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.</p> <p>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.</p>
Anzahl der Laufwerke bei Ausfall des Storage-Controllers	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 Storage-Controller	Der Status von Netzteil A für den Storage Controller.
Netzteil B für Storage Controller	Der Status von Netzteil B für den Speicher-Controller.
Typ des Speicherdatenspeichers	Die Art der Laufwerke in der Appliance, z. B. HDD (Festplatte) oder SSD (Solid State Drive).
Größe der Speicherdatenlaufwerk	<p>Die effektive Größe eines Datenlaufwerks.</p> <p>Hinweis: Für Knoten mit Erweiterungs-Shelfs, verwenden Sie das Datenlaufwerk-Größe für jedes Shelf Stattdessen. Die effektive Laufwerksgröße kann je nach Shelf abweichen.</p>
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.

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

+

Spalte in der Tabelle „Storage Shelves“	Beschreibung
Seriennummer des Shelf Chassis	Die Seriennummer für das Storage Shelf-Chassis.
Shelf-ID	Die numerische Kennung für das Storage-Shelf. <ul style="list-style-type: none"> • 99: Storage Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf <p>Hinweis: Erweiterungseinschübe gelten nur für SG6060 und SG6060X.</p>
Der Shelf-Status	Der Gesamtstatus des Storage Shelf.
IOM-Status	Der Status der ein-/Ausgangsmodule (IOMs) in beliebigen Erweiterungs-Shelves. K. A., wenn es sich nicht um ein Erweiterungs-Shelf handelt

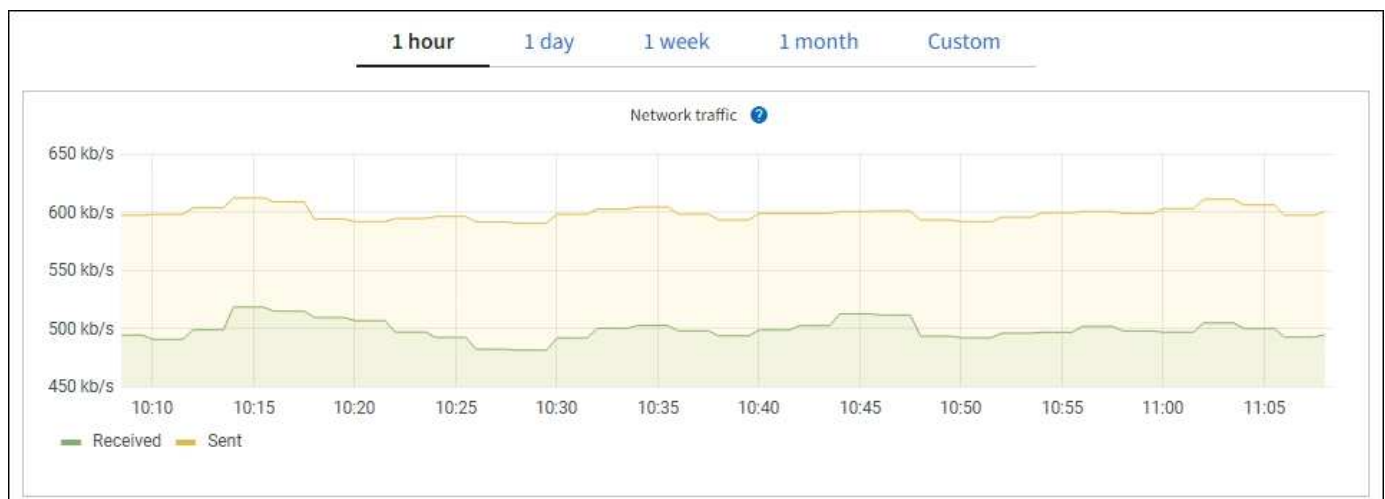
Spalte in der Tabelle „Storage Shelves“	Beschreibung
Netzteilstatus	Der Gesamtstatus der Netzteile für das Storage Shelf.
Status der Schublade	Der Zustand der Schubladen im Lagerregal. N/A, wenn das Regal keine Schubladen enthält.
Lüfterstatus	Der Gesamtstatus der Lüfter im Storage Shelf.
Laufwerksschächte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

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 Netzwerkverkehrs.



1. Lesen Sie den Abschnitt Netzwerkschnittstellen.

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

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



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

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

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

2. Lesen Sie den Abschnitt Netzwerkkommunikation.

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

Network communication

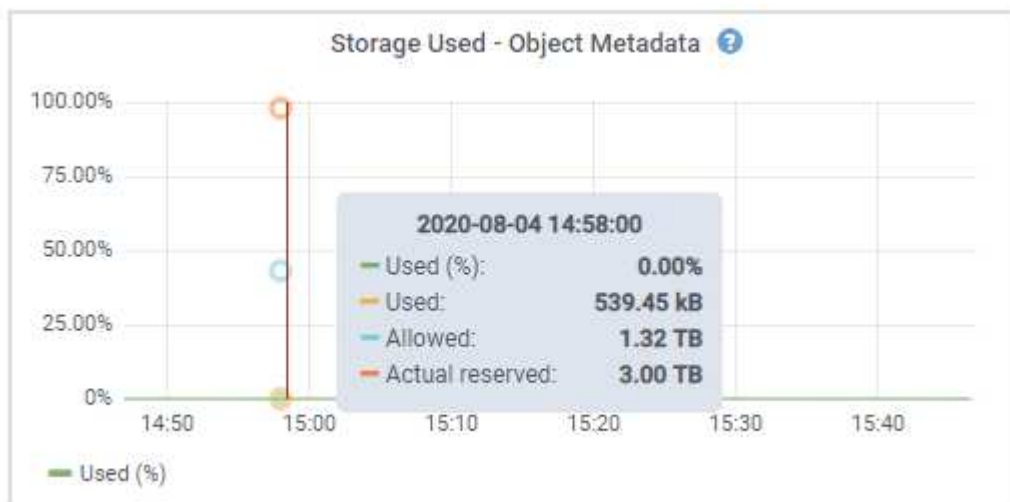
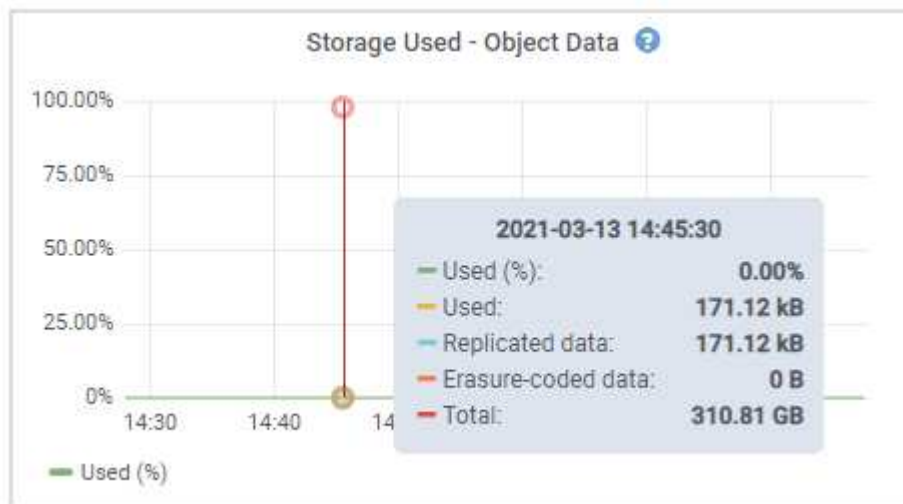
Receive

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

Transmit

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

3. 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	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

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

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

Verwandte Informationen

[SG6000 Storage-Appliances](#)

Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an

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

Schritte

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

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

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

10-224-6-199-ADM1 (Primary Admin Node) [🔗](#) ✕

Overview Hardware Network Storage Load balancer Tasks SANtricity System Manager

Node information ?

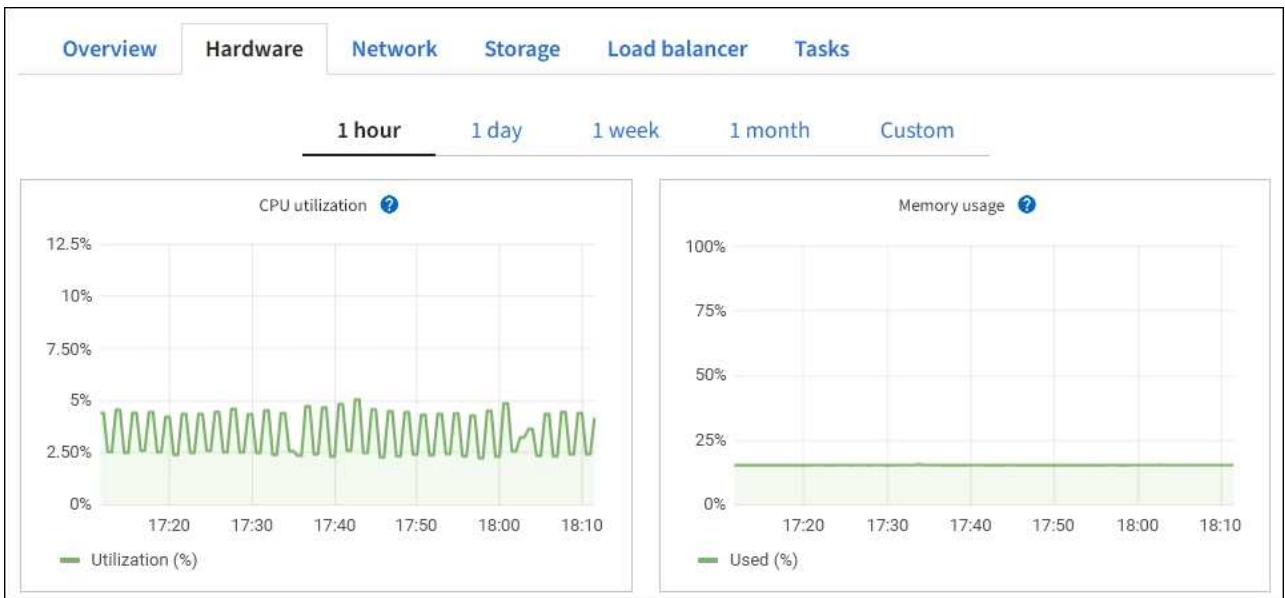
Name: 10-224-6-199-ADM1
 Type: Primary Admin Node
 ID: 6fdc1890-ca0a-4493-acdd-72ed317d95fb
 Connection state: ✔ Connected
 Software version: 11.6.0 (build 20210928.1321.6687ee3)
 IP addresses: 172.16.6.199 - eth0 (Grid Network)
 10.224.6.199 - eth1 (Admin Network)
 47.47.7.241 - eth2 (Client Network)

[Hide additional IP addresses](#) ^

Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

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

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



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

StorageGRID Appliance

Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

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

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

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

Wenn 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 Netzwerkverkehrs.



a. Lesen Sie den Abschnitt Netzwerkschnittstellen.

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

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



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

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

b. Lesen Sie den Abschnitt Netzwerkkommunikation.

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

Network communication							
Receive							
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames	
eth0	2.89 GB	19,421,503	0	24,032	0	0	
Transmit							
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier	
eth0	3.64 GB	18,494,381	0	0	0	0	















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

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Load balancer](#)[Tasks](#)

Disk devices

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

Volumes

Mount point  	Device  	Status  	Size  	Available  	Write cache status  
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB 	Unknown

Verwandte Informationen

[SG100- und SG1000-Services-Appliances](#)

Zeigen Sie die Registerkarte Netzwerk an

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

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

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

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

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

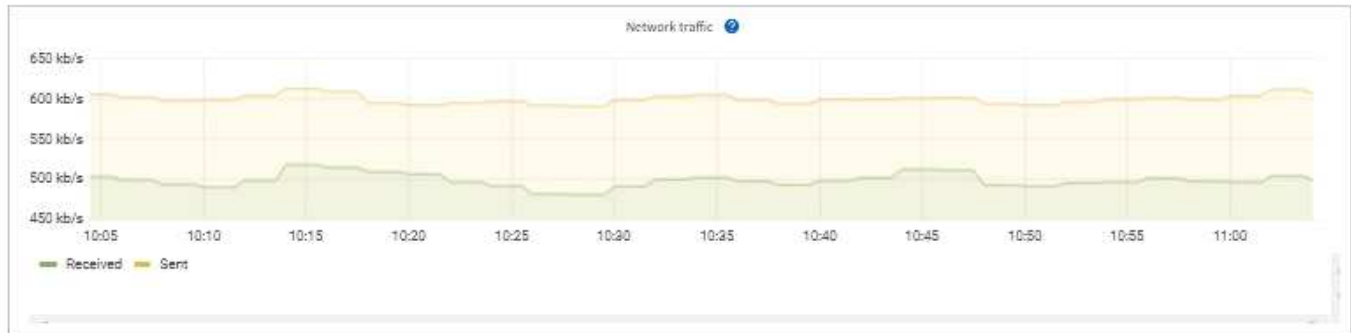
1 hour

1 day

1 week

1 month

Custom



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Verwandte Informationen

[Überwachen Sie Netzwerkverbindungen und Performance](#)

Öffnen Sie die Registerkarte „Speicher“

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

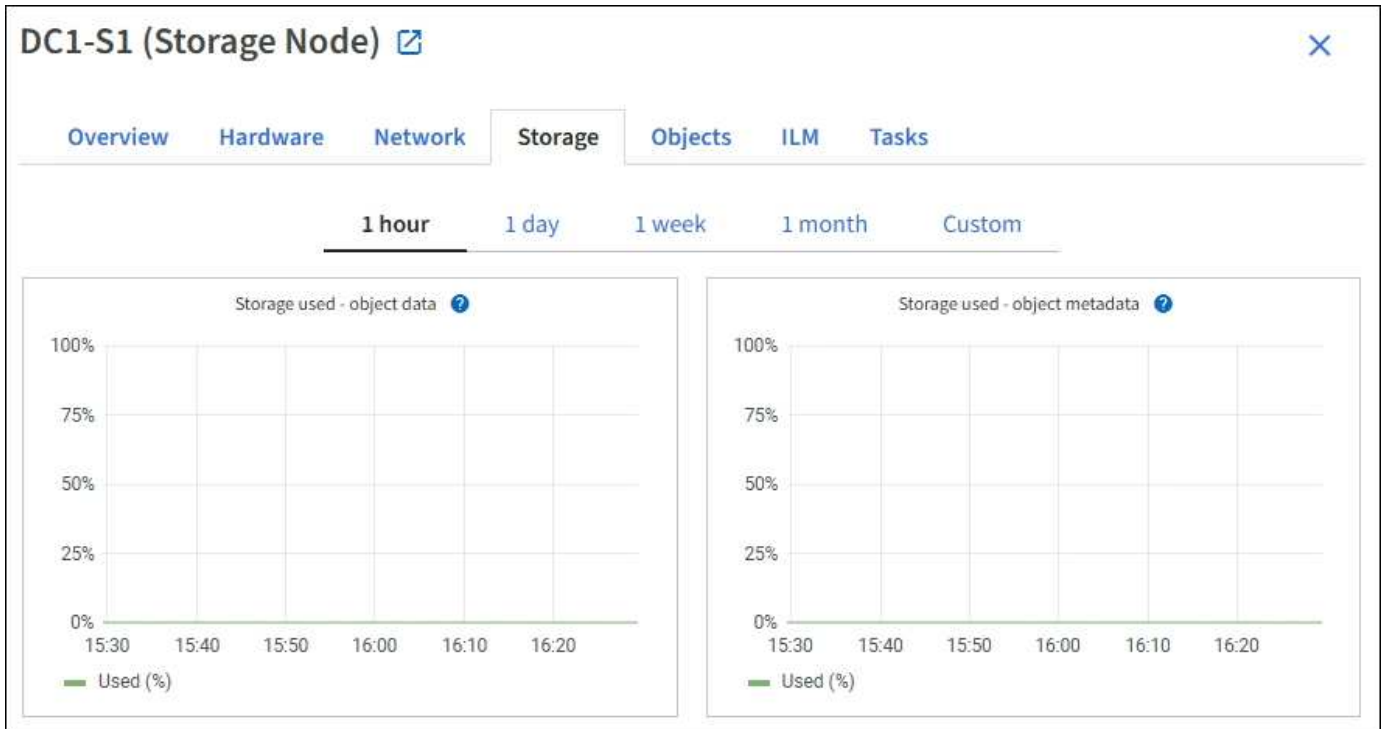
Die Registerkarte Storage wird für alle Nodes, jeden Standort und das gesamte Raster angezeigt.

Verwendete Diagramme im Storage

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



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 Objektspeichern Tabellen

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

Disk devices

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

Volumes

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

Object stores

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

Verwandte Informationen

[Monitoring der Storage-Kapazität](#)

Verwenden Sie die Registerkarte Aufgabe, um einen Grid-Knoten neu zu starten

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

- Sie haben die Berechtigung **Wartung** oder **Stammzugriff**.
- Sie haben die **Provisionierungs-Passphrase**.

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.



In seltenen Fällen kann es vorkommen, dass eine StorageGRID Appliance in den **Wartungsmodus** versetzt wird, damit die Appliance für den Remote-Zugriff nicht verfügbar ist.

Schritte

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

Overview Hardware Network Storage Objects ILM **Tasks**

Reboot

Reboots the node.

Maintenance mode

Places the appliance's compute controller into maintenance mode.

4. Wählen Sie **Neustart**.

Ein Bestätigungsdialogfeld wird angezeigt.

Reboot node SGA-lab11 ✕

Reboot shuts down and restarts a node, based on where the node is installed:

- Rebooting a VMware node reboots the virtual machine.
- Rebooting a Linux node reboots the container.
- Rebooting a StorageGRID Appliance node reboots the compute controller.

Attention: When the primary Admin Node is rebooted, your browser's connection to StorageGRID will be lost temporarily.

If you are ready to reboot this node, enter the provisioning passphrase and select OK.

Provisioning passphrase



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 **Nodes** angezeigt. Wenn alle Dienste wieder gestartet wurden und der Knoten erfolgreich mit dem Raster verbunden ist, sollte die Seite **Nodes** einen normalen Status anzeigen (keine Symbole links neben dem Knotennamen), was darauf hinweist, dass keine Alarme aktiv sind und der Knoten mit dem Raster verbunden ist.

Verwandte Informationen

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[SG5600 Storage Appliances](#)

[SG100- und SG1000-Services-Appliances](#)

Zeigen Sie die Registerkarte Objekte an

Die Registerkarte Objekte enthält Informationen zu [S3](#) Und [Swift](#) Einspielraten und Abrufen.

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

- Overview
- Hardware
- Network
- Storage
- Objects
- ILM
- Tasks

- 1 hour
- 1 day
- 1 week
- 1 month
- Custom



Object counts

Total objects: ?	1,295	
Lost objects: ?	0	
S3 buckets and Swift containers: ?	161	

Metadata store queries

Average latency: ?	10.00 milliseconds	
Queries - successful: ?	14,587	
Queries - failed (timed out): ?	0	
Queries - failed (consistency level unmet): ?	0	

Verification

Status: ?	No errors	
Percent complete: ?	47.14%	
Average stat time: ?	0.00 microseconds	
Objects verified: ?	0	
Object verification rate: ?	0.00 objects / second	
Data verified: ?	0 bytes	
Data verification rate: ?	0.00 bytes / second	
Missing objects: ?	0	
Corrupt objects: ?	0	
Corrupt objects unidentified: ?	0	
Quarantined objects: ?	0	

Zeigen Sie die Registerkarte ILM an

Die Registerkarte ILM 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.

DC2-S1 (Storage Node) [↗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) **ILM** [Tasks](#)

Evaluation

Awaiting - all: ?	0 objects	
Awaiting - client: ?	0 objects	
Evaluation rate: ?	0.00 objects / second	
Scan rate: ?	0.00 objects / second	

Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-09-09 17:36:44 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Verwandte Informationen

[Überwachung des Information Lifecycle Management](#)

[StorageGRID verwalten](#)

Zeigen Sie die Registerkarte Load Balancer an

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

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

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



Datenverkehr anfordern

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



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

Eingehende Anfragerate

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

Durchschnittliche Anfragedauer (fehlerfrei)

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

Fehlerantwortrate

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

Verwandte Informationen

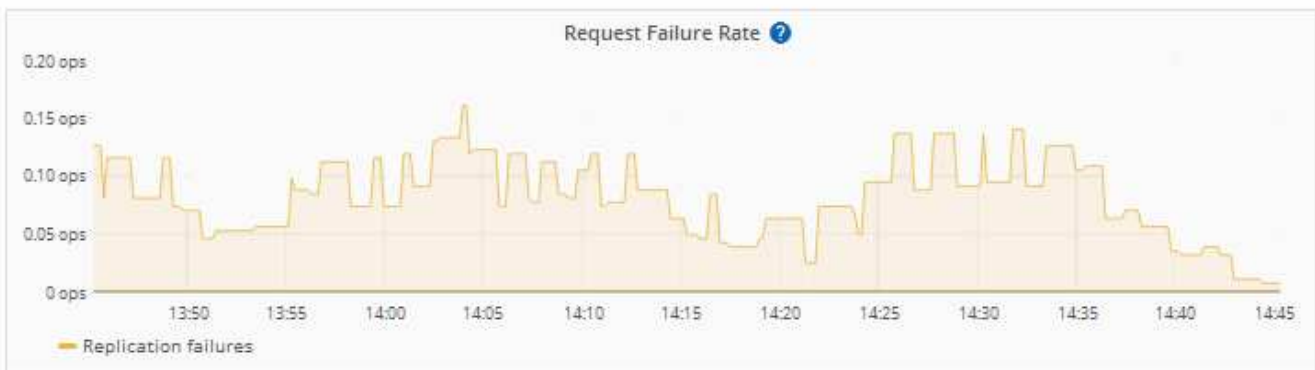
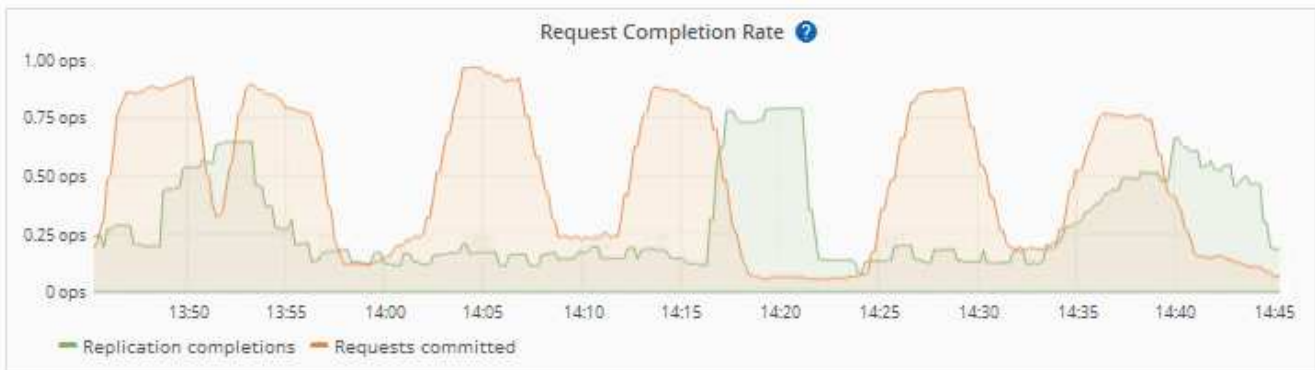
[Monitoring von Lastverteilungsvorgängen](#)

[StorageGRID verwalten](#)

Zeigen Sie die Registerkarte Plattformdienste an

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

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



Weitere Informationen zu S3-Platformservices, einschließlich Details zur Fehlerbehebung, finden Sie im [Anweisungen für die Administration von StorageGRID](#).

Zeigen Sie die Registerkarte SANtricity System Manager an

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 benötigen SANtricity-Firmware 8.70 (11.70) oder höher, um mithilfe des Grid Managers auf SANtricity System Manager zuzugreifen.



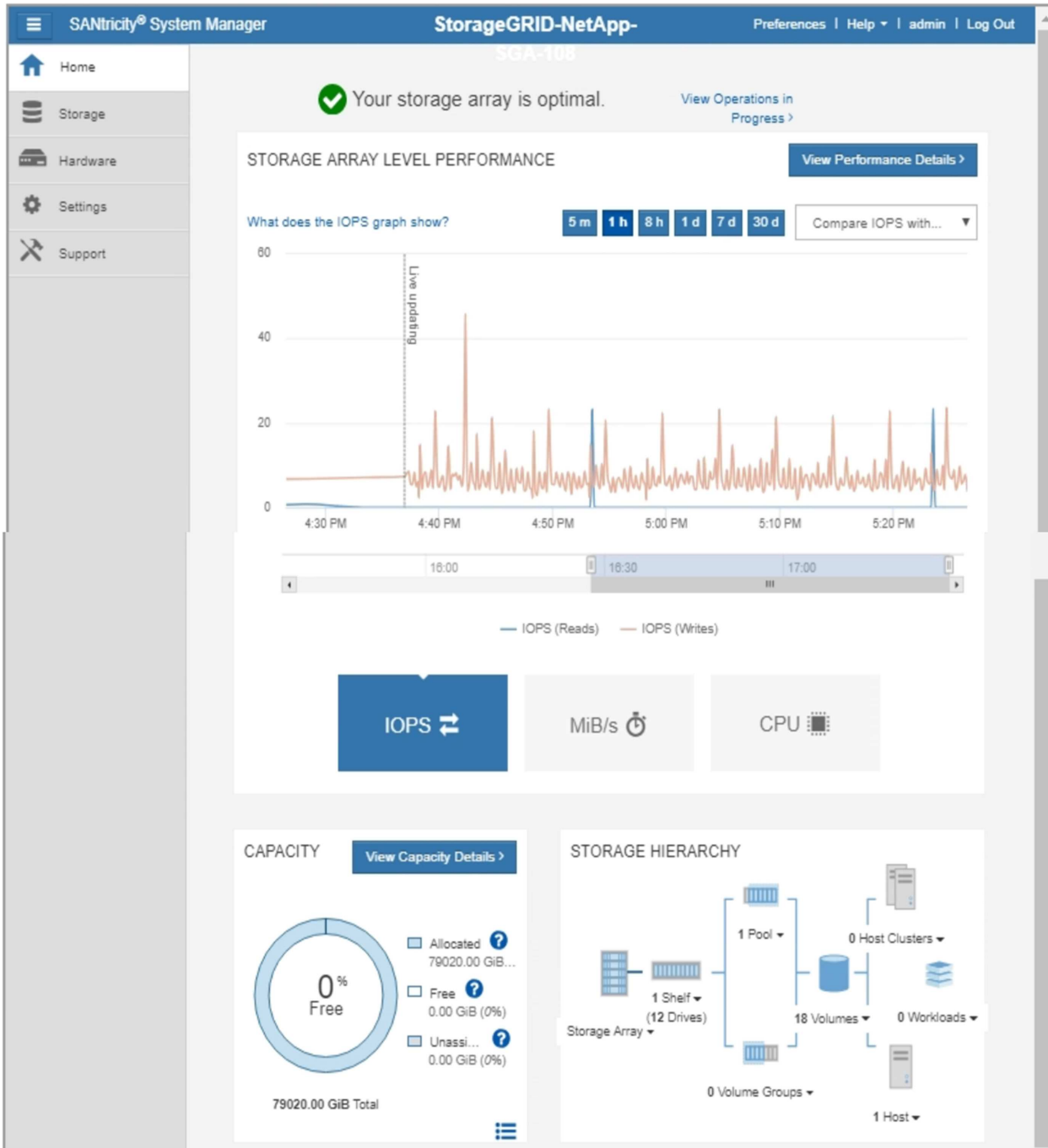
Der Zugriff auf den SANtricity System Manager über den Grid Manager erlaubt in der Regel nur die Überwachung der Appliance-Hardware und die Konfiguration der E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring Ihrer 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.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.



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 unter "[NetApp E-Series und SANtricity Dokumentation](#)".

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.

Was überwacht werden soll	Frequenz
Der Daten für den Systemzustand Wird auf dem Grid Manager Dashboard angezeigt. Beachten Sie, dass sich etwas vom Vortag geändert hat.	Täglich
Tarif Objekt- und Metadatenkapazität des Storage-Node Wird verbraucht	Wöchentlich
Information Lifecycle Management-Operationen	Wöchentlich
Netzwerkverbindungen und Performance	Wöchentlich
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

Systemzustand überwachen

Sie sollten täglich den allgemeinen Zustand Ihres StorageGRID Systems überwachen.

Über diese Aufgabe

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.

Schritte

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 ALERTS Current 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.
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 MAINTENANCE System Lizenz anzuzeigen.

Verwandte Informationen

- [StorageGRID verwalten](#)

- [Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein](#)
- [Verwenden Sie SNMP-Überwachung](#)

Überwachen Sie die Status der Node-Verbindung


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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).



Über diese Aufgabe

Nodes können einen von drei Verbindungszuständen haben:

- **Nicht verbunden - Unbekannt** : Der Knoten ist aus einem unbekanntem 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](#)

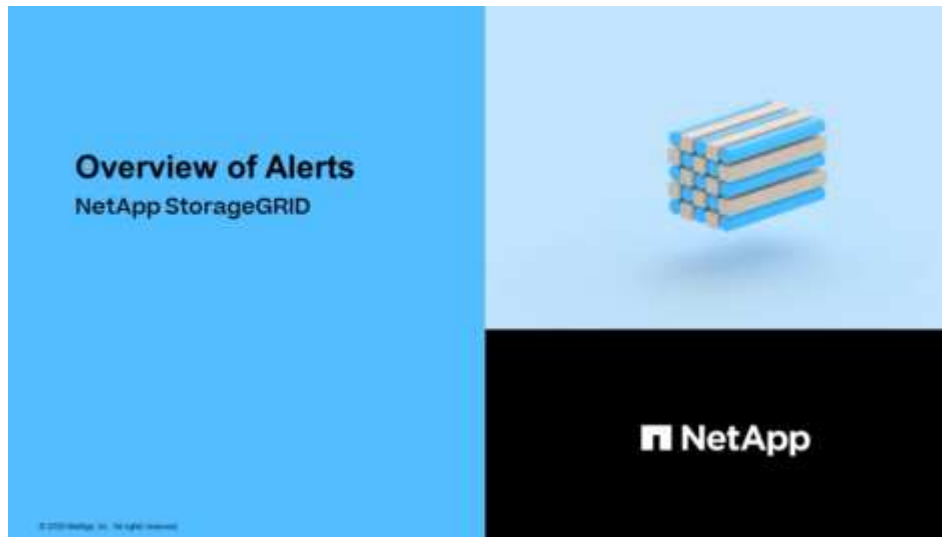
[Recovery und Wartung](#)

Anzeigen aktueller Warnmeldungen

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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Optional haben Sie sich das Video angesehen: "[Video: Übersicht über Warnungen](#)".



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 **ALERTS Current**.

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

Current Alerts [Learn more](#)

View the current alerts affecting your StorageGRID system.




Name	Severity	Time triggered	Site / Node	Status	Current values
Unable to communicate with node One or more services are unresponsive or cannot be reached by the metrics collection job.	2 Major	9 minutes ago (<i>newest</i>) 19 minutes ago (<i>oldest</i>)		2 Active	
Low root disk capacity The space available on the root disk is low.	Minor	25 minutes ago	Data Center 1 / DC1-S1-99-51	Active	Disk space available: 2.00 GB Total disk space: 21.00 GB
Expiration of server certificate for Storage API Endpoints The server certificate used for the storage API endpoints is about to expire.	Major	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 14
Expiration of server certificate for Management Interface The server certificate used for the management interface is about to expire.	Minor	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 30
Low installed node memory The amount of installed memory on a node is low.	8 Critical	a day ago (<i>newest</i>) a day ago (<i>oldest</i>)		8 Active	

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.
Schweregrad	<p>Der Schweregrad der Meldung. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten.</p> <ul style="list-style-type: none"> • * 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 schwerwiegenden 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 (<i>neueste</i>) und die älteste Instanz der Warnmeldung (<i>älteste</i>) 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.

							<input checked="" type="checkbox"/> Group alerts	Active ▼
Name	Severity	Time triggered	Site / Node	Status	Current values			
▲ Low object data storage The disk space available for storing object data is low.	▲ 5 Minor	a day ago (newest) a day ago (oldest)		5 Active				
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC2 231-236 / DC2-S2-233	Active	Disk space remaining: 525.17 GB Disk space used: 243.06 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC1 225-230 / DC1-S1-226	Active	Disk space remaining: 525.17 GB Disk space used: 325.65 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC2 231-236 / DC2-S3-234	Active	Disk space remaining: 525.17 GB Disk space used: 381.55 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC1 225-230 / DC1-S2-227	Active	Disk space remaining: 525.17 GB Disk space used: 282.19 KB Disk space used (%): 0.000%			
Low object data storage The disk space available for storing object data is low.	▲ Minor	a day ago	DC2 231-236 / DC2-S1-232	Active	Disk space remaining: 525.17 GB Disk space used: 189.24 KB Disk space used (%): 0.000%			

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

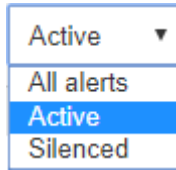


5. Zum Sortieren von Warnungen oder Warnungsgruppen klicken Sie auf die nach-oben/unten-Pfeile ↑↓ In jeder Spaltenüberschrift.

- 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. Siehe [Benachrichtigung über Stille](#).

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

Ein Dialogfeld für die Meldung wird angezeigt. Siehe [Zeigen Sie eine bestimmte Warnmeldung an](#).

Anzeigen von behobenen Warnmeldungen

Sie können den Verlauf der behobenen Warnungen suchen und anzeigen.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

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 **ALERTS 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.

Resolved Alerts




Search and view alerts that have been resolved.


When triggered ✕ Severity ✕ Alert rule ✕ Node ✕

Name	Severity	Time triggered	Time resolved	Site / Node	Triggered values
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S2	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S3	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S4	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-ADM1	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-ADM2	Total RAM size: 8.37 GB
Low installed node memory The amount of installed memory on a node is low.	Critical	2 days ago	a day ago	Data Center 1 / DC1-S1	Total RAM size: 8.37 GB

2. Überprüfen Sie die Informationen in der Tabelle.

Spaltenüberschrift	Beschreibung
Name	Der Name der Warnmeldung und deren Beschreibung.

Spaltenüberschrift	Beschreibung
Schweregrad	<p>Der Schweregrad der Meldung.</p> <ul style="list-style-type: none"> • * 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.
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.

- 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.

- Optional können Sie die Liste der aufgelösten Warnmeldungen mithilfe der Dropdown-Menüs oben in der Tabelle filtern.
 - 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)

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

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

Ein Dialogfeld für die Meldung wird angezeigt. Siehe [Zeigen Sie eine bestimmte Warnmeldung an](#).

Zeigen Sie eine bestimmte Warnmeldung an

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 [Stummschalten einer aktuellen Warnmeldung](#) Oder [Aktualisieren Sie die Meldungsregel](#).

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

Schritte

- Führen Sie einen der folgenden Schritte aus, je nachdem, ob Sie eine aktuelle oder behobene

Warnmeldung anzeigen möchten:

Spaltenüberschrift	Beschreibung
Aktuelle Meldung	<ul style="list-style-type: none"> • 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 ALERTS Current. • 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.
Warnung wurde behoben	<ul style="list-style-type: none"> • 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 ALERTS 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.

^ Low installed node memory The amount of installed memory on a node is low.	8 Critical	a day ago (newest) a day ago (oldest)		8 Active	
<u>Low installed node memory</u> The amount of installed memory on a node is low.	8 Critical	a day ago	Data Center 2 / DC2-S1-99-56	Active	Total RAM size: 8.38 GB

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

Low installed node memory

The amount of installed memory on a node is low.

Recommended actions

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Time triggered

2019-07-15 17:07:41 MDT (2019-07-15 23:07:41 UTC)

Status

Active ([silence this alert](#) )

Site / Node

Data Center 2 / DC2-S1-99-56

Severity

 Critical

Total RAM size

8.38 GB




Condition

[View conditions](#) | [Edit rule](#) 

Close

3. Prüfen Sie die Warnmeldungsdetails.

Informationsdaten	Beschreibung
<i>Titel</i>	Der Name der Warnmeldung.
<i>Erster Absatz</i>	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.

Informationsdaten	Beschreibung
Schweregrad	<p>Der Schweregrad der Meldung.</p> <ul style="list-style-type: none"> • * 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 schwerwiegenden Problem führen.
<i>Datenwerte</i>	<p>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.</p>

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.

Low installed node memory

Major `node_memory_MemTotal_bytes < 24000000000`

Critical `node_memory_MemTotal_bytes < 12000000000`

Total RAM size
8.38 GB

Condition
[View conditions](#) | [Edit rule](#)

- 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**.

Anzeigen von älteren Alarmen

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



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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

Schritte

1. Wählen Sie **SUPPORT Alarme (alt) Aktuelle Alarme**.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Current Alarms





Last Refreshed: 2020-05-27 09:41:39 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

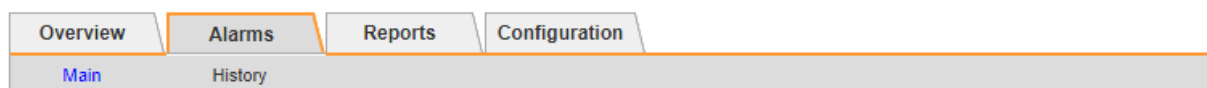
Show Records Per Page Previous < 1 > Next

Das Alarmsymbol zeigt den Schweregrad jedes Alarms wie folgt an:

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


- Um mehr über das Attribut zu erfahren, das den Alarm ausgelöst hat, klicken Sie mit der rechten Maustaste auf den Attributnamen in der Tabelle.
- 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**).



Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
 Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes 

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

Verwandte Informationen

[Alarmreferenz \(Altsystem\)](#)

[Quittierung aktueller Alarme \(Legacy-System\)](#)

[Deaktivieren von Alarmen \(Legacy-System\)](#)

Monitoring der Storage-Kapazität

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

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

Das können Sie [Informationen zur Storage-Kapazität anzeigen](#) Für das gesamte Grid, für jeden Standort und für jeden Storage-Node im StorageGRID-System.

Überwachung der Speicherkapazität für das gesamte Grid

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

Über diese Aufgabe

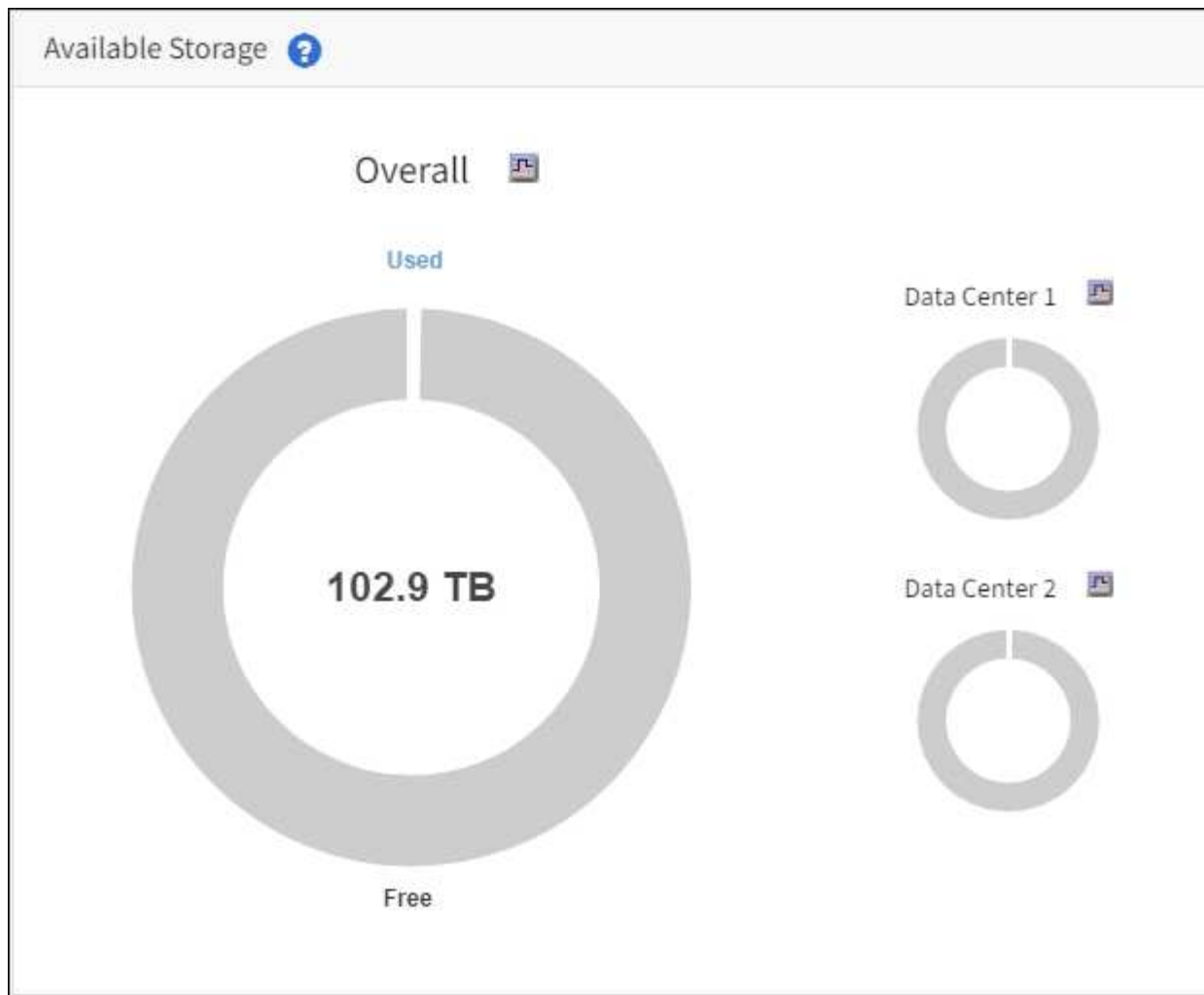
Über das Dashboard im Grid Manager können Sie schnell ermitteln, wie viel Storage für das gesamte Grid und für jedes Datacenter zur Verfügung steht. Die Seite Knoten enthält detailliertere Werte für Objektdaten und Objektmetadaten.

Schritte

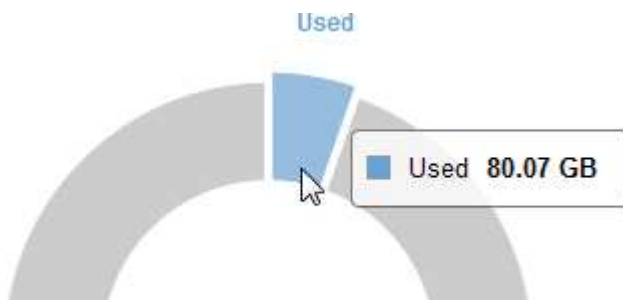
1. Beurteilen Sie, wie viel Storage für das gesamte Grid und das jeweilige Datacenter verfügbar ist.
 - a. Wählen Sie **Dashboard**.
 - b. Notieren Sie sich im Fenster Verfügbare Speicherkapazität die Zusammenfassung der freien und genutzten Speicherkapazität.




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.

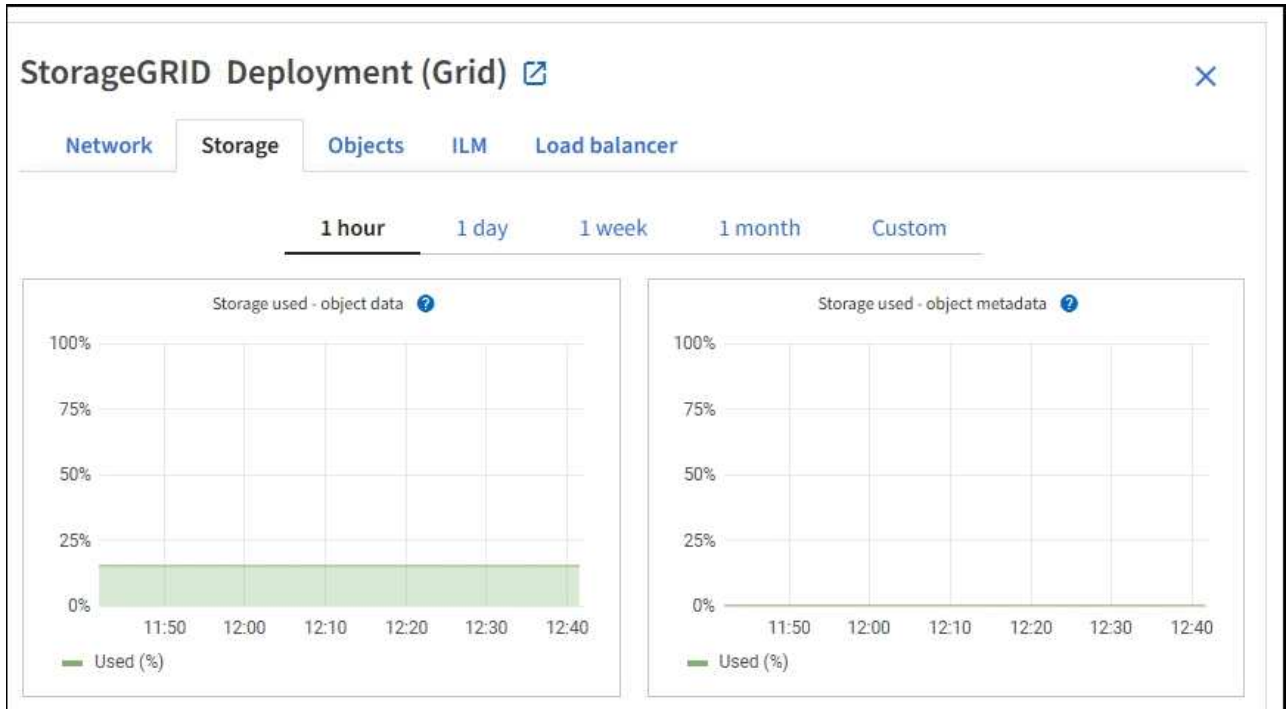


- b. Sehen Sie sich das Diagramm für die einzelnen Datacenter an, um Grids für mehrere Standorte zu verwenden.
- c. Klicken Sie auf das Diagrammsymbol  Für das Gesamtdiagramm oder für ein einzelnes Datacenter, um ein Diagramm anzuzeigen, in dem die Kapazitätsauslastung im Laufe der Zeit dargestellt wird.

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 Cursor über die Diagramme **verwendeter Speicher - Objektdaten** und **verwendeter Speicher - Objektmetadaten**, um zu sehen, wie viel Objekt-Storage und Objekt-Metadaten für das gesamte Grid zur Verfügung stehen und wie viel über die Zeit genutzt 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. Planung, eine Erweiterung zum Hinzufügen von Storage-Nodes oder Storage-Volumes durchzuführen, bevor die nutzbare Storage-Kapazität des Grid genutzt wird

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



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

Weitere Informationen zur Planung einer Speichererweiterung finden Sie im [Anweisungen zur Erweiterung von StorageGRID](#).

Überwachen Sie die Storage-Kapazität für jeden Storage-Node

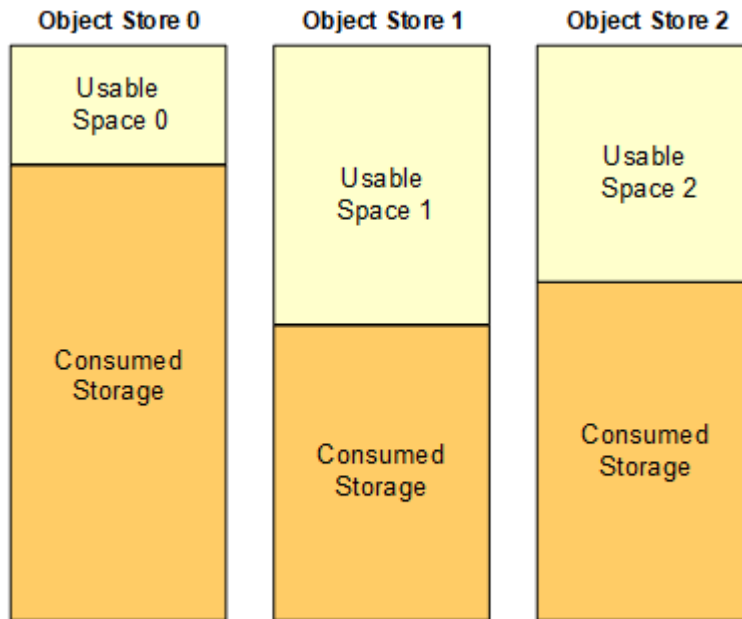
Überwachen Sie den insgesamt nutzbaren Speicherplatz für jeden Storage-Node, um sicherzustellen, dass der Node über ausreichend Speicherplatz für neue Objektdaten verfügt.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

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.



$$\text{Total Usable Space} = \text{Usable Space 0} + \text{Usable Space 1} + \text{Usable Space 2}$$

Schritte

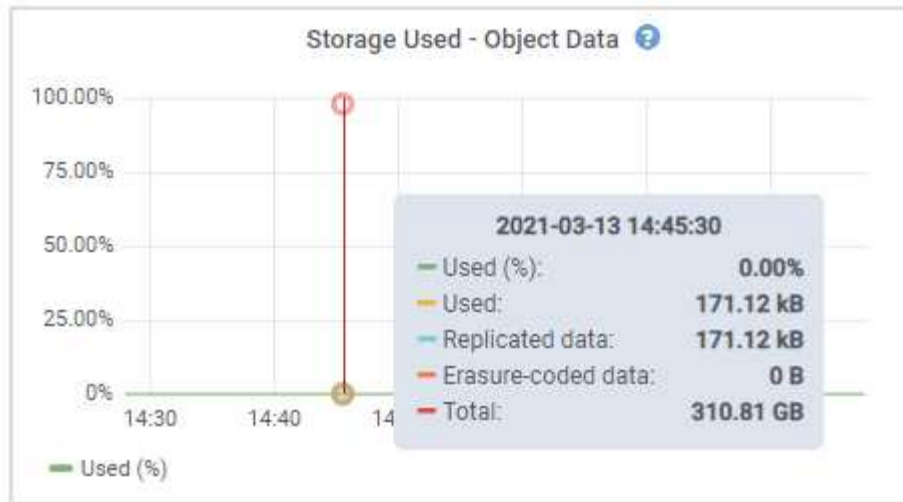
1. Wählen Sie **NODES Storage Node Storage** aus.

Die Diagramme und Tabellen für den Node werden angezeigt.

2. Halten Sie den Mauszeiger über das Diagramm „verwendete Objekte – 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.
- **Erase-codierte Daten:** Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt:** Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` Metrisch.



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



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

Disk devices

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

Volumes

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

Object stores

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

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

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



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

Weitere Informationen zur Planung einer Speichererweiterung finden Sie im [Anweisungen zur Erweiterung](#)

von StorageGRID.

Der **Niederer Objektspeicher** Die Meldung wird ausgelöst, wenn nicht genügend Speicherplatz zum Speichern von Objektdaten auf einem Storage-Node verbleibt.

Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

Über diese Aufgabe

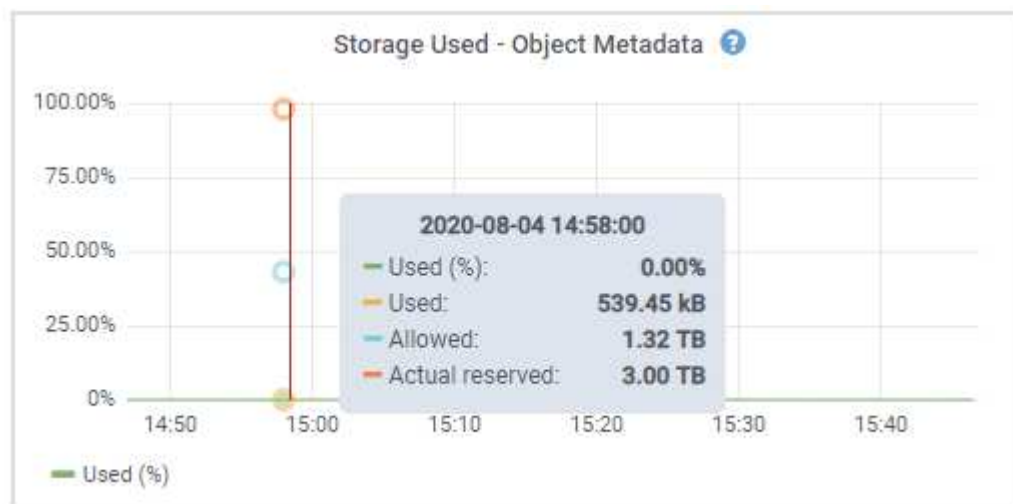
StorageGRID behält drei Kopien von Objektmetadaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem Storage 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 Metadatenutzung 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. Halten Sie den Mauszeiger über das Diagramm „verwendete Werte – Objektmetadaten“, 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. Informationen darüber, wie dieser Wert für jeden Storage-Node bestimmt wird, finden Sie im Anweisungen für die Administration 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 jeden Storage-Node berechnet wird, finden Sie im Anweisungen für die Administration von StorageGRID .	<i>Metric wird in einer zukünftigen Version hinzugefügt.</i>



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. Siehe [Anweisungen zum erweitern eines StorageGRID-Systems](#).

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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

Über diese Aufgabe

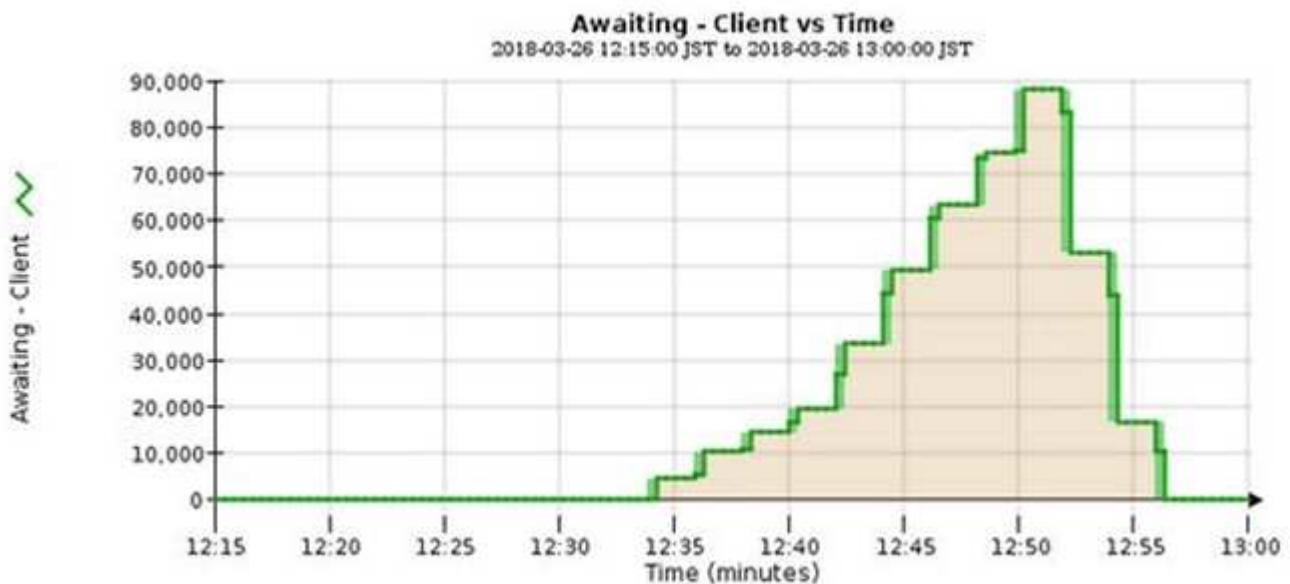
Das StorageGRID System managt Objekte mithilfe der aktiven ILM-Richtlinie. Die ILM-Richtlinie und die zugehörigen ILM-Regeln bestimmen die Anzahl der Kopien, die Art der erstellten Kopien, das Erstellen von Kopien und die Dauer der Aufbewahrung jeder Kopie.

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.

Mithilfe der Seite **NODES** können Sie sich weiter mit ILM-Warteschlangen beschäftigen.

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.

- **Repairs 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.

Überwachen Sie 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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Netzwerkonnektivität 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

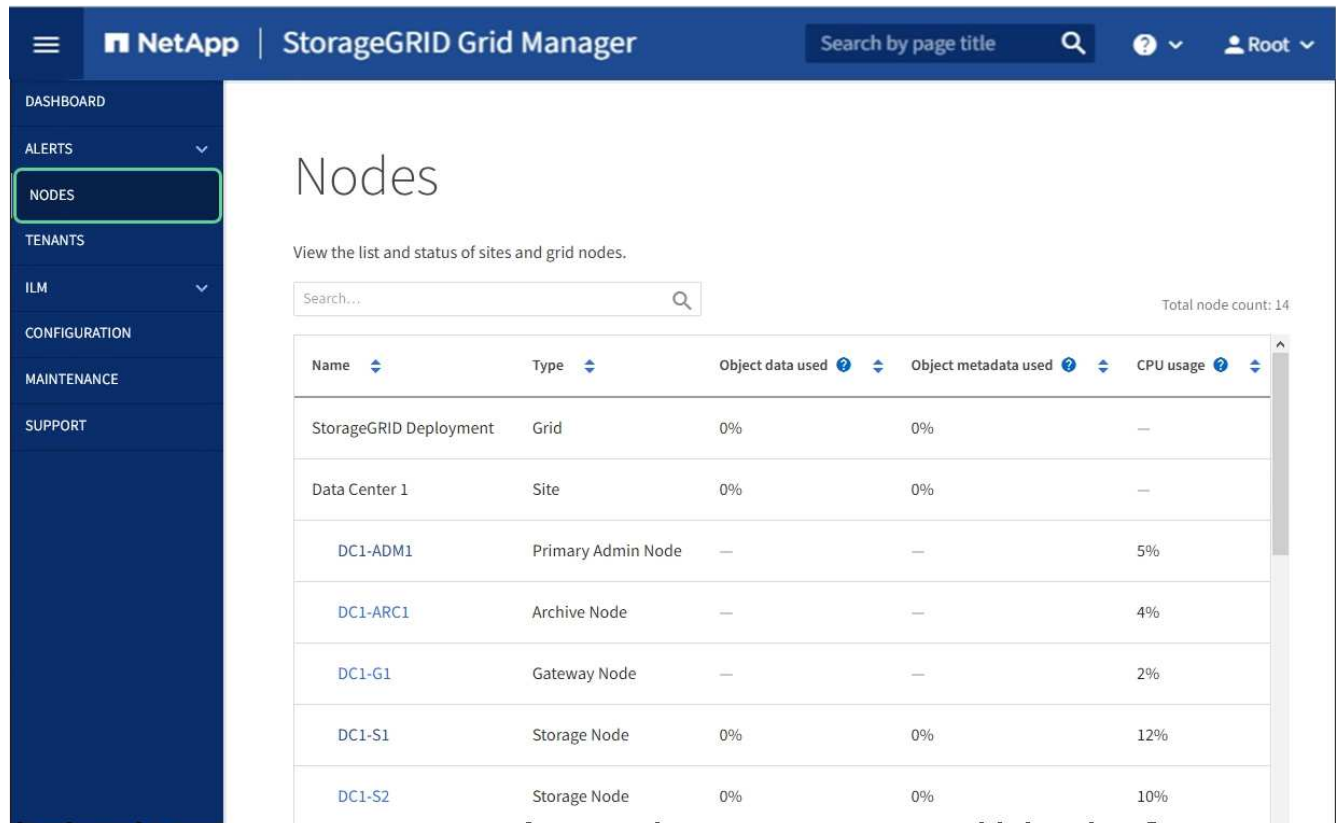
Probleme umgehend beheben können.

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. Siehe [Anweisungen für die Administration von StorageGRID](#).

Schritte

1. Wählen Sie **KNOTEN**.

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



The screenshot shows the NetApp StorageGRID Grid Manager interface. The left sidebar contains a navigation menu with the following items: DASHBOARD, ALERTS, **NODES** (highlighted with a green box), TENANTS, ILM, CONFIGURATION, MAINTENANCE, and SUPPORT. The main content area is titled 'Nodes' and includes a search bar and a table of nodes. The table has the following data:

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	5%
DC1-ARC1	Archive Node	—	—	4%
DC1-G1	Gateway Node	—	—	2%
DC1-S1	Storage Node	0%	0%	12%
DC1-S2	Storage Node	0%	0%	10%

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 Netzwerkverkehrs für das gesamte Grid, den Datacenter-Standort oder für den Node.



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

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

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

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

Network communication						
Receive						
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

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

- a. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

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

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

- 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**.
- 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 zur Verkehrsklassifizierung finden Sie im [Anweisungen für die Administration von StorageGRID](#).

Verwandte Informationen

[Zeigen Sie die Registerkarte Netzwerk an](#)

[Überwachen Sie die Status der Node-Verbindung](#)

Monitoring von Ressourcen auf Node-Ebene

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

Was Sie benötigen

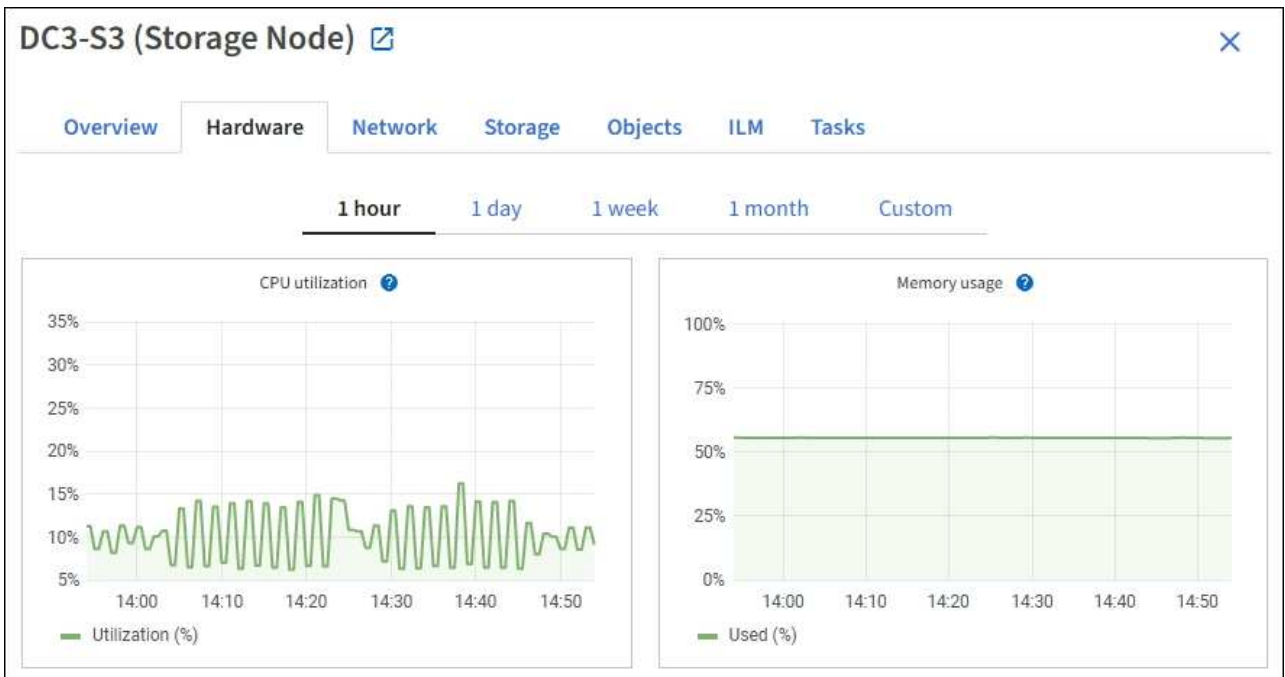
- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

Über diese Aufgabe

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

Schritte

- So zeigen Sie Informationen zur Hardwareauslastung eines Grid-Node an:
 - Wählen Sie auf der Seite **NODES** den Knoten aus.
 - 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

[Zeigen Sie Informationen zu Appliance Storage Nodes an](#)

[Zeigen Sie Informationen zu Appliance Admin Nodes und Gateway Nodes an](#)

Überwachen Sie die Mandantenaktivität

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Berechtigung Root Access oder Administrator.



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 verwendete logische Speicherplatz, die Kontingentnutzung, Kontingente und Objektanzahl aufgelistet. Wenn kein Kontingent für einen Mandanten festgelegt ist, enthalten die Felder Quotenauslastung und Quota einen Strich (#8212;).

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;">10%</div>	20.00 GB	100	→ 📄
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;">85%</div>	100.00 GB	500	→ 📄
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;">50%</div>	1.00 PB	10,000	→ 📄
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;">95%</div>	500.00 TB	50,000	→ 📄
<input type="checkbox"/>	Tenant 05	5.00 GB	–	–	500	→ 📄

Sie können sich bei einem Mandantenkonto anmelden, indem Sie auf den Anmelde-link klicken [→](#) In der Spalte **Anmelden/Kopieren URL** der Tabelle.

Sie können die URL für die Anmeldeseite eines Mandanten kopieren, indem Sie den Link URL kopieren auswählen [📄](#) In der Spalte **Anmelden/Kopieren URL** der Tabelle.

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 Mandanten einschließlich Nutzungsdiagramme anzuzeigen, wählen Sie auf der Seite „Mandanten“ den Kontonamen für den Mandanten aus.

Tenant 02

Tenant ID: 4103 1879 2208 5551 2180  Quota utilization: 85%
Protocol: S3 Logical space used: 85.00 GB
Object count: 500 Quota: 100.00 GB

[Sign in](#) [Edit](#) [Actions](#) 

[Space breakdown](#) [Allowed features](#)

Bucket space consumption

85.00 GB of 100.00 GB used

15.00 GB remaining (15%).











Bucket details

[Export to CSV](#)

Search buckets by name



Displaying 3 results

Name  	Region  	Space used  	Object count  
bucket-01		40.00 GB	250
bucket-02		30.00 GB	200
bucket-03		15.00 GB	50

Übersicht der Mieter

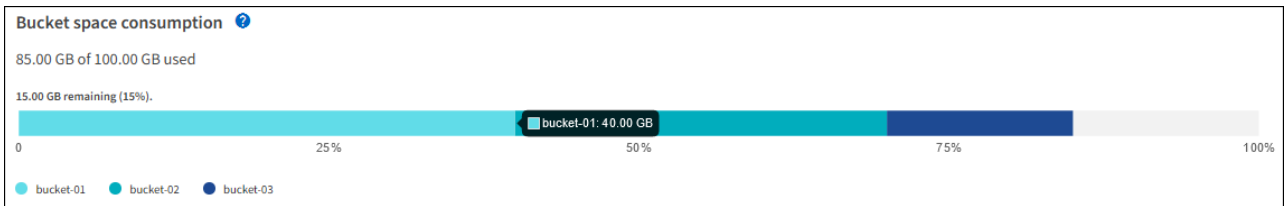
Der Übersichtsbereich für den Mandanten enthält Werte für die Objektanzahl, die Kontingentnutzung, der verwendete logische Speicherplatz und die Kontingenteinstellung.

Raumaufteilung — Raumverbrauch

Die Registerkarte „Space breakdown“ enthält Werte für den Gesamtverbrauch an Bucket (S3) oder Container (Swift) sowie den verwendeten Speicherplatz und die Objektanzahl für die einzelnen Buckets oder Container.

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

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



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



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



Sie können die 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.

◦ Raumaufteilung — Eimer- oder Behälterdetails

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

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

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.

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

- a. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen

Richtlinien sind in der Tabelle aufgeführt.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b

Displaying 2 traffic classification policies.

- Anhand der Liste der Richtlinien können Sie diejenigen ermitteln, die für einen bestimmten Mandanten gelten.
- Um Metriken anzuzeigen, die mit einer Richtlinie verknüpft sind, wählen Sie das Optionsfeld links neben der Richtlinie aus, und klicken Sie dann auf **Metriken**.
- 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.

- 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.

- Optional können Sie mit den Prometheus Kennzahlen die Mandantenaktivität erfassen:

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

Verwandte Informationen

Überwachen Sie die Archivierungskapazität

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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-Topologie** aus.
2. Wählen Sie **Archivnoten ARC Übersicht Haupt**.
3. Überprüfen Sie die Attribute „Speicherstatus“ und „Speicherstatus“, um zu bestätigen, dass die Komponente „Speicher“ ohne Fehler online ist.

The screenshot shows the 'Overview' tab of the ARC (DC1-ARC1-98-165) configuration page. The 'Store State' and 'Store Status' are highlighted with a blue box, indicating they are 'Online' and 'No Errors'. Other components like ARC State, Tivoli Storage Manager, and Replication Status are also shown as 'Online' and 'No Errors'.

Component	State	Status	Icons
ARC State:	Online		[OK] [Green Check]
ARC Status:	No Errors		[OK] [Green Check]
Tivoli Storage Manager State:	Online		[OK] [Green Check]
Tivoli Storage Manager Status:	No Errors		[OK] [Green Check]
Store State:	Online		[OK] [Green Check]
Store Status:	No Errors		[OK] [Green Check]
Retrieve State:	Online		[OK] [Green Check]
Retrieve Status:	No Errors		[OK] [Green Check]
Inbound Replication Status:	No Errors		[OK] [Green Check]
Outbound Replication Status:	No Errors		[OK] [Green Check]

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.

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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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-Knoten, der Clientanforderungen aktiv verteilen soll, **SUPPORT Tools Grid-Topologie** aus.
 - e. Wählen Sie **Gateway Node CLB HTTP Übersicht Main**.
 - 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](#)

[Zeigen Sie die Registerkarte Load Balancer an](#)

Anwendung von Hotfixes oder ggf. Upgrade-Software

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:

- Wählen Sie die Version aus dem Pulldown-Menü aus und klicken Sie auf **Go**.
- Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
- Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Weiter akzeptieren**.

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](#)

[Recovery und Wartung](#)

Verwalten von Meldungen und Alarmen

Alarme und Alarme verwalten: Übersicht

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

Meldungssystem

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

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

- Im Dashboard im Grid Manager wird ein Symbol für den Schweregrad „Meldungen“ angezeigt, und die Anzahl der aktuellen Meldungen wird erhöht.
- Der Alarm wird auf der Seite **NODES** Zusammenfassung und auf der Registerkarte **NODES Node Übersicht** angezeigt.
- Es wird eine E-Mail-Benachrichtigung gesendet, vorausgesetzt, Sie haben einen SMTP-Server konfiguriert und E-Mail-Adressen für die Empfänger bereitgestellt.

- Es wird eine SNMP-Benachrichtigung (Simple Network Management Protocol) gesendet, vorausgesetzt, Sie haben den StorageGRID SNMP-Agent konfiguriert.

Altes Alarmsystem

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



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

Wenn ein Alarm ausgelöst wird, treten folgende Aktionen auf:

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

Vergleichen von Warnungen 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?	<ul style="list-style-type: none"> • Klicken Sie auf dem Dashboard auf den Link Aktuelle Alarme. • Wählen Sie die Warnmeldung auf der Seite NODES Übersicht aus. • Wählen Sie ALERTS Current. <p>Anzeigen aktueller Warnmeldungen</p>	<p>Wählen Sie SUPPORT Alarme (alt) Aktuelle Alarme.</p> <p>Verwalten von Alarmen (Altsystem)</p>
Was bewirkt, dass eine Warnung oder ein Alarm ausgelöst wird?	<p>Alarme werden ausgelöst, wenn ein Prometheus-Ausdruck in einer Alarmregel für die spezifische Triggerbedingung und -Dauer als wahr bewertet wird.</p> <p>Zeigen Sie Alarmregeln an</p>	<p>Alarme werden ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht.</p> <p>Verwalten von Alarmen (Altsystem)</p>

	Meldungen	Alarmer (Altsystem)
Wie kann ich das zugrunde liegende Problem lösen, wenn eine Meldung oder ein Alarm ausgelöst wird?	<p>Die empfohlenen Aktionen für eine Warnmeldung sind in E-Mail-Benachrichtigungen enthalten und stehen auf den Alerts-Seiten im Grid Manager zur Verfügung.</p> <p>Falls erforderlich, werden weitere Informationen in der StorageGRID-Dokumentation bereitgestellt.</p> <p>Alerts Referenz</p>	<p>Sie können sich über einen Alarm informieren, indem Sie den Attributnamen auswählen oder in der StorageGRID-Dokumentation nach einem Alarmcode suchen.</p> <p>Alarmreferenz (Altsystem)</p>
Wo kann ich eine Liste der Alarme oder Alarme sehen, die gelöst wurden?	<p>Wählen Sie ALERTS aufgelöst.</p> <p>Anzeigen von behobenen Warnmeldungen</p>	<p>Wählen Sie SUPPORT Alarme (alt) Historische Alarme aus.</p> <p>Verwalten von Alarmen (Altsystem)</p>
Wo kann ich die Einstellungen verwalten?	<p>Wählen Sie ALERTS Regeln.</p> <p>Verwalten von Meldungen</p>	<p>Wählen Sie SUPPORT. Verwenden Sie dann die Optionen im Abschnitt Alarme (alt) des Menüs.</p> <p>Verwalten von Alarmen (Altsystem)</p>
Welche Benutzergruppenberechtigungen brauche ich?	<ul style="list-style-type: none"> • 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. <p>StorageGRID verwalten</p>	<ul style="list-style-type: none"> • 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. <p>StorageGRID verwalten</p>

	Meldungen	Alarmer (Altsystem)
Wie managt ich E-Mail-Benachrichtigungen?	<p>Wählen Sie ALERTS E-Mail-Einrichtung.</p> <p>Hinweis: Da Alarmer und Alarmer 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.</p> <p>Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein</p>	<p>Wählen Sie SUPPORT Alarmer (alt) Legacy E-Mail-Einrichtung.</p> <p>Verwalten von Alarmen (Altsystem)</p>
Wie verwalte ich SNMP Benachrichtigungen?	<p>Wählen Sie KONFIGURATION Überwachung SNMP-Agent.</p> <p>Verwenden Sie SNMP-Überwachung</p>	<p>Wählen Sie KONFIGURATION Überwachung SNMP-Agent.</p> <p>Verwenden Sie SNMP-Überwachung</p> <p>Hinweis: SNMP-Benachrichtigungen werden nicht für jeden Alarm oder Alarm Schweregrad gesendet.</p> <p>Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)</p>
Wie kontrolliere ich, wer Benachrichtigungen erhält?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS 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. <p>Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT Alarmer (alt) Legacy E-Mail-Einrichtung. 2. Mailingliste wird erstellt. 3. Wählen Sie Benachrichtigungen. 4. Wählen Sie die Mailingliste aus. <p>Verwalten von Alarmen (Altsystem)</p>
Welche Admin Nodes senden Benachrichtigungen?	<p>Ein einziger Admin-Node (der „bevorzugte Absender“).</p> <p>StorageGRID verwalten</p>	<p>Ein einziger Admin-Node (der „bevorzugte Absender“).</p> <p>StorageGRID verwalten</p>

	Meldungen	Alarme (Altsystem)
Wie kann ich einige Benachrichtigungen unterdrücken?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS stumm. 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. <p>Hinweis: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.</p> <p>Benachrichtigung über Stille</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT Alarme (alt) Legacy E-Mail-Einrichtung. 2. Wählen Sie Benachrichtigungen. 3. Wählen Sie eine Mailingliste aus, und wählen Sie unterdrücken. <p>Verwalten von Alarmen (Altsystem)</p>
Wie kann ich alle Benachrichtigungen unterdrücken?	<p>Wählen Sie ALERTS stumm und dann Alle Regeln.</p> <p>Hinweis: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren.</p> <p>Benachrichtigung über Stille</p>	<ol style="list-style-type: none"> 1. Wählen Sie KONFIGURATION System Anzeigoptionen. 2. Aktivieren Sie das Kontrollkästchen Benachrichtigung Alle unterdrücken. <p>Hinweis: Das Unterdrückung von E-Mail-Benachrichtigungen systemweit unterdrückt auch ereignisgesteuerte AutoSupport-E-Mails.</p> <p>Verwalten von Alarmen (Altsystem)</p>
Wie kann ich die Bedingungen und Trigger anpassen?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS Regeln. 2. Wählen Sie eine Standardregel zum Bearbeiten aus, oder wählen Sie benutzerdefinierte Regel erstellen. <p>Bearbeiten von Meldungsregeln</p> <p>Erstellen benutzerdefinierter Warnungsregeln</p>	<ol style="list-style-type: none"> 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. <p>Verwalten von Alarmen (Altsystem)</p>

	Meldungen	Alarme (Altsystem)
Wie deaktiviere ich eine einzelne Warnung oder einen einzelnen Alarm?	<ol style="list-style-type: none"> 1. Wählen Sie ALERTS Regeln. 2. Wählen Sie die Regel aus, und wählen Sie Regel bearbeiten. 3. Deaktivieren Sie das Kontrollkästchen aktiviert. <p>Deaktivieren von Meldungsregeln</p>	<ol style="list-style-type: none"> 1. Wählen Sie SUPPORT Alarme (alt) Globale Alarme. 2. Wählen Sie die Regel aus, und wählen Sie das Symbol Bearbeiten aus. 3. Deaktivieren Sie das Kontrollkästchen aktiviert. <p>Verwalten von Alarmen (Altsystem)</p>

Verwalten von Meldungen

Benachrichtigungen verwalten: Übersicht

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.

Allgemeines zu StorageGRID-Meldungen

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. Bei Ereignissen, die eine sofortige Aktion erfordern, werden 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.

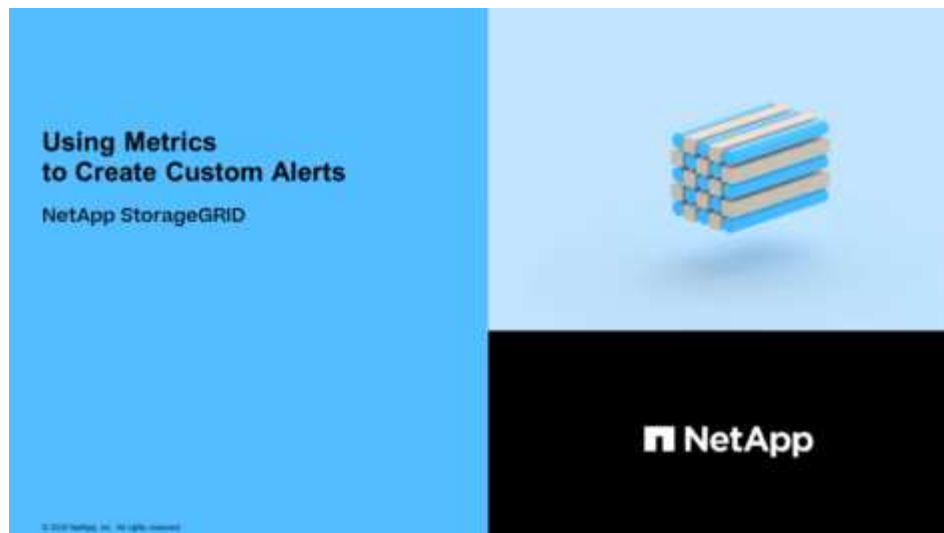
Weitere Informationen .

Sehen Sie sich die folgenden Videos an, um mehr zu erfahren:

- ["Video: Übersicht über Warnungen"](#)



- ["Video: Verwenden von Metriken, um benutzerdefinierte Warnmeldungen zu erstellen"](#)



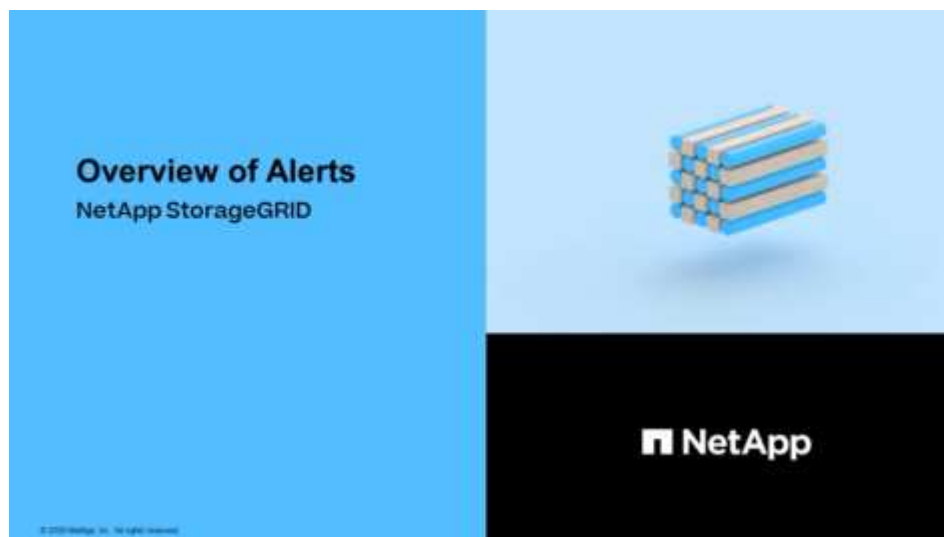
Zeigen Sie Alarmregeln an

Alarmregeln definieren die Bedingungen, die ausgelöst werden [Spezifische Warnmeldungen](#). StorageGRID enthält eine Reihe von Standardwarnregeln, die Sie unverändert verwenden oder ändern können, oder Sie können individuelle Alarmregeln erstellen.

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.
- Optional haben Sie sich das Video angesehen: "[Video: Übersicht über Warnungen](#)"



Schritte

1. Wählen Sie **ALERTS** Regeln.

Die Seite Alarmregeln wird angezeigt.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.


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

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

Displaying 62 alert rules.

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

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

Spaltenüberschrift	Beschreibung
Bestimmten Bedingungen	<p>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.</p> <ul style="list-style-type: none"> • * 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 schwerwiegenden Problem führen.
Typ	<p>Der Typ der Warnregel:</p> <ul style="list-style-type: none"> • 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.
Status	<p>Gibt an, ob diese Warnungsregel derzeit aktiviert oder deaktiviert ist. Die Bedingungen für deaktivierte Warnregeln werden nicht ausgewertet, sodass keine Warnmeldungen ausgelöst werden.</p>

Erstellen benutzerdefinierter Warnungsregeln

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#)

- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff
- Sie kennen das [Häufig verwendete Prometheus-Kennzahlen](#)
- Sie verstehen den ["Syntax der Prometheus-Abfragen"](#)
- Optional haben Sie sich das Video angesehen: ["Video: Verwenden von Metriken, um benutzerdefinierte Warnmeldungen zu erstellen"](#)



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 **ALERTS Regeln**.

Die Seite Alarmregeln wird angezeigt.

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

Das Dialogfeld „Benutzerdefinierte Regel erstellen“ wird angezeigt.

Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions (optional)

Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

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 Formatierungs-codes). 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 Grundaussdruck ist in der Regel die Form:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

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

Der Standardwert ist 5 Minuten.

7. Wählen Sie **Speichern**.

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

Bearbeiten von Meldungsregeln

Sie können eine Meldungsregel bearbeiten, um die Triggerbedingungen zu ändern. Für eine benutzerdefinierte Warnungsregel können Sie auch den Regelnamen, die

Beschreibung und die empfohlenen Aktionen aktualisieren.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.

Über diese Aufgabe

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



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

Schritte

1. Wählen Sie **ALERTS Regeln**.

Die Seite Alarmregeln wird angezeigt.

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

Das Dialogfeld Regel bearbeiten wird angezeigt. In diesem Beispiel wird eine Standardwarnregel angezeigt: Die Felder eindeutiger Name, Beschreibung und empfohlene Aktionen sind deaktiviert und können nicht bearbeitet werden.

Edit Rule - Low installed node memory

Enabled

Unique Name

Description

Recommended Actions (optional) VMware installation- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)
"/>

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

Cancel

Save

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 Formatierungs-codes). Die empfohlenen Aktionen für Warnungsregeln können zwischen 0 und 1,024 Zeichen liegen.

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



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

Conditions

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes < 24000000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes <= 14000000000"/>



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

Ein Grundausdruck ist in der Regel die Form:

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

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

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

Der Standardwert ist 5 Minuten.

8. Wählen Sie **Speichern**.

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

Deaktivieren von Meldungsregeln

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.

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 **ALERTS Regeln**.

Die Seite Alarmregeln wird angezeigt.

2. Wählen Sie das Optionsfeld für die Warnungsregel, die deaktiviert oder aktiviert werden soll.

3. Wählen Sie **Regel bearbeiten**.

Das Dialogfeld Regel bearbeiten wird angezeigt.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **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. Wählen Sie **Speichern**.

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

Entfernen Sie benutzerdefinierte Warnungsregeln

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.

Schritte

1. Wählen Sie **ALERTS Regeln**.

Die Seite Alarmregeln wird angezeigt.

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

Sie können keine Standardwarnregel entfernen.

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

Ein Bestätigungsdialogfeld wird angezeigt.

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

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

Verwalten von Warnmeldungen

Einrichten von SNMP-Benachrichtigungen für Warnmeldungen

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

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

Informationen zum Konfigurieren des SNMP-Agenten finden Sie unter [Verwenden Sie SNMP-Überwachung](#).

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

- Traps sind Benachrichtigungen, die vom SNMP-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. Siehe [Benachrichtigung über Stille](#).

Benachrichtigungen werden von jedem Admin-Node gesendet, der als bevorzugter Absender konfiguriert wurde. Standardmäßig ist der primäre Admin-Node ausgewählt. Siehe [Anweisungen für die Administration 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. Siehe [Warnmeldungen, die SNMP-Benachrichtigungen generieren \(Legacy-System\)](#).

Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.

Über diese Aufgabe

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 im [Anweisungen für die Administration von StorageGRID](#).

Schritte

1. Wählen Sie **ALERTS E-Mail-Einrichtung**.

Die Seite E-Mail-Einrichtung wird angezeigt.

Email Setup

You can configure the email server for alert notifications, define filters to limit the number of notifications, and enter email addresses for alert recipients.

Use these settings to define the email server used for alert notifications. These settings are not used for alarm notifications and AutoSupport. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Enable Email Notifications

Save

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.

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

Email (SMTP) Server

Mail Server ?	<input type="text" value="10.224.1.250"/>
Port ?	<input type="text" value="25"/>
Username (optional) ?	<input type="text" value="smtpuser"/>
Password (optional) ?	<input type="password" value="*****"/>

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

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

Beispiel: `storagegrid-alerts@example.com`

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

Wählen Sie das Plus-Symbol **+** Um Empfänger hinzuzufügen.

Email Addresses

Sender Email Address	<input type="text" value="storagegrid-alerts@example.com"/>	
Recipient 1	<input type="text" value="recipient1@example.com"/>	✕
Recipient 2	<input type="text" value="recipient2@example.com"/>	+ ✕

5. Wenn Transport Layer Security (TLS) für die Kommunikation mit dem SMTP-Server erforderlich ist, wählen Sie im Abschnitt Transport Layer Security (TLS) die Option **TLS erforderlich** aus.

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

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

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

- b. Aktivieren Sie das Kontrollkästchen **Client-Zertifikat senden**, wenn Ihr SMTP-E-Mail-Server E-Mail-Absender benötigt, um Clientzertifikate 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 wählen Sie **Durchsuchen** und wählen Sie die Datei aus.

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

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



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

Transport Layer Security (TLS)

Require TLS [?](#)

CA Certificate [?](#)

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Send Client Certificate [?](#)

Client Certificate [?](#)

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Private Key [?](#)

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890  
-----BEGIN PRIVATE KEY-----
```

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.

Filters

Severity ⓘ Minor, major, critical Major, critical Critical only

Send Test Email

Save

7. Wenn Sie bereit sind, Ihre E-Mail-Einstellungen zu testen, führen Sie die folgenden Schritte aus:

a. Wählen Sie **Test-E-Mail Senden**.

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

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



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

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



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

8. Wählen Sie **Speichern**.

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

Die E-Mail-Einstellungen werden gespeichert.

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

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

E-Mail-Benachrichtigungen enthalten die folgenden Informationen:

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 4
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

Sent from: DC1-ADM1-225 5

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

Gruppierung von Warnungen

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

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

Verhalten	Beispiel
<p>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.</p>	<ul style="list-style-type: none"> • 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.
<p>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.</p>	<ul style="list-style-type: none"> • Die Warnmeldung A wird ausgelöst und die kleineren, größeren und kritischen Alarmschwellenwerte werden erreicht. Eine Benachrichtigung wird für die kritische Warnmeldung gesendet.
<p>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.</p>	<ol style="list-style-type: none"> 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.
<p>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.</p>	<ol style="list-style-type: none"> 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.
<p>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.</p>	<ol style="list-style-type: none"> 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.

Verhalten	Beispiel
StorageGRID sendet weiterhin alle 7 Tage E-Mail-Benachrichtigungen, bis alle Instanzen der Warnmeldung gelöst oder die Alarmregel stummgeschaltet wurde.	<ol style="list-style-type: none"> 1. Am 8. März wird Alarm A für Knoten 1 ausgelöst. Eine Benachrichtigung wird gesendet. 2. Warnung A ist nicht gelöst oder stummgeschaltet. Weitere Benachrichtigungen erhalten Sie am 15. März, 22. März 29 usw.

Beheben Sie Warnmeldungen bei E-Mail-Benachrichtigungen

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.

Schritte

1. Überprüfen Sie Ihre Einstellungen.
 - a. Wählen Sie **ALERTS 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.

Siehe [Erfassen von Protokolldateien und Systemdaten](#).

Benachrichtigung über Stille

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

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten von Warnungen oder Stammzugriff.

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 **ALERTS stumm**.

Die Seite „Stille“ wird angezeigt.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create Edit Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
<i>No results found.</i>				

2. Wählen Sie **Erstellen**.

Das Dialogfeld Stille erstellen wird angezeigt.

Create Silence

Alert Rule

Description (optional)

Duration

Severity Minor only Minor, major Minor, major, critical

Nodes

- StorageGRID Deployment
 - Data Center 1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3

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

Feld	Beschreibung
Meldungsregel	<p>Der Name der Alarmregel, die Sie stumm schalten möchten. Sie können eine beliebige Standard- oder benutzerdefinierte Warnungsregel auswählen, auch wenn die Alarmregel deaktiviert ist.</p> <p>Hinweis: Wählen Sie Alle Regeln aus, wenn Sie alle Alarmregeln mit den in diesem Dialogfeld angegebenen Kriterien stummschalten möchten.</p>
Beschreibung	<p>Optional eine Beschreibung der Stille. Beschreiben Sie zum Beispiel den Zweck dieser Stille.</p>
Dauer	<p>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.</p> <p>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.</p>

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	<p>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.</p> <p>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.</p>

4. Wählen Sie **Speichern**.

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

Option	Beschreibung
Stille bearbeiten	<ol style="list-style-type: none"> Wählen Sie ALERTS stumm. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie bearbeiten möchten. Wählen Sie Bearbeiten. Ändern Sie die Beschreibung, die verbleibende Zeit, die ausgewählten Schweregrade oder den betroffenen Knoten. Wählen Sie Speichern.
Entfernen Sie eine Stille	<ol style="list-style-type: none"> Wählen Sie ALERTS stumm. Wählen Sie in der Tabelle das Optionsfeld für die Stille, die Sie entfernen möchten. Wählen Sie Entfernen. Wählen Sie OK, um zu bestätigen, dass Sie diese Stille entfernen möchten. <p>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.</p>

Verwandte Informationen

- [Konfigurieren Sie den SNMP-Agent](#)

Verwalten von Alarmen (Altsystem)

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



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

Alarmklassen (altes System)

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

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

Alarmauslöselogik (Älteres System)

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

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

Für jedes numerische Attribut kann der Alarmschwerwert und der entsprechende Schwellenwert 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.

Alarmer desselben Schweregrades

Wenn zwei globale benutzerdefinierte Alarmer für dasselbe Attribut den gleichen Schweregrad haben, werden die Alarmer 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
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

Default Alarms

Filter by

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 Alarmer und Benachrichtigungen gesendet werden, wird der Schweregrad des Alarms anhand des aktuellen Alarmschwerfalls für das Attribut

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

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

Neuer Services

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

Alarme und Tabellen

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

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

Sie können den VMFI-Alarm so deaktivieren, dass der VMFI-Alarm 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

Quittierung aktueller Alarme (Legacy-System)

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Alarme quittieren verfügen.

Über diese Aufgabe

Da das alte Alarmsystem weiterhin unterstützt wird, wird die Liste der alten Alarme auf der Seite Aktuelle Alarme bei jedem neuen Alarm erhöht. Sie können die Alarme in der Regel ignorieren (da 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 auf der Seite „Aktuelle Alarme“ im Grid Manager aufgeführt, es sei denn, der Alarm wird auf der nächsten Schweregrade ausgelöst oder behoben und tritt erneut auf.



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

Schritte

1. Wählen Sie **SUPPORT Alarme (alt) Aktuelle Alarme**.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data_Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show Records Per Page Previous < 1 > Next

2. Wählen Sie in der Tabelle den Dienstnamen aus.

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

Overview | **Alarms** | Reports | Configuration

Main | History



Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes

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.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 17:38:58 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable	2020-05-27 17:38:14 MDT

Show Records Per Page Previous « 1 » Next

Standardalarme anzeigen (Altsystem)

Sie können die Liste aller älteren Standardalarme anzeigen.


Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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.



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by equals

221 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Major	Greater than 10,000,000	>=	10000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Minor	Greater than 1,000,000	>=	1000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Notice	Greater than 150,000	>=	150000	
<input checked="" type="checkbox"/>		XCVP (% Completion)	Notice	Foreground Verification Completed	=	100	
<input checked="" type="checkbox"/>	ADC	ADCA (ADC Status)	Minor	Error	>=	10	
<input checked="" type="checkbox"/>	ADC	ADCE (ADC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ADC	ALIS (Inbound Attribute Sessions)	Notice	Over 100	>=	100	
<input checked="" type="checkbox"/>	ADC	ALOS (Outbound Attribute Sessions)	Notice	Over 200	>=	200	

Prüfen historischer Alarme und Alarmfrequenz (altes System)

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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** aus.
 - b. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf einen der Zeiträume.

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

Die Alarme werden in umgekehrter chronologischer Reihenfolge aufgeführt.

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

Globale benutzerdefinierte Alarme erstellen (altes System)

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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** .



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000		

Default Alarms

Filter by Attribute Code equals AR*

9 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000	
<input checked="" type="checkbox"/>	ARC	ARRF (Request Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARRV (Verification Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARVF (Store Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	NMS	ARRC (Remaining Capacity)	Notice	Below 10	<=	10	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Major	Disconnected	<=	9	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Notice	Standby	<=	19	

Apply Changes

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







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

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

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

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

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

Überschrift	Beschreibung
Attribut	Wählen Sie den Namen und den Code des zu überwachenden Attributs aus der Liste aller Attribute aus, die für den ausgewählten Dienst oder die ausgewählte Komponente gelten. Um Informationen über das Attribut anzuzeigen, klicken Sie auf Info  Neben dem Namen des Attributs.
Schweregrad	Das Symbol und der Text, der die Alarmstufe angibt.
Nachricht	Der Grund für den Alarm (Verbindung unterbrochen, Lagerraum unter 10 % usw.).
Operator	Operatoren für das Testen des aktuellen Attributwerts gegen den Wert-Schwellenwert: <ul style="list-style-type: none"> • = gleich • Größer als • Kleiner als • = größer als oder gleich • \= kleiner als oder gleich • ≠ ist nicht gleich
Wert	Der Schwellenwert 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 kommasetrennte 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. <p>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.</p>
Aktionen	Steuertasten zu:  Bearbeiten Sie eine Zeile <ul style="list-style-type: none"> +  Eine Zeile einfügen +  Löschen Sie eine Zeile +  Ziehen Sie eine Zeile nach oben oder unten +  Kopieren Sie eine Zeile

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

Deaktivieren von Alarmen (Legacy-System)

Die Alarme im alten Alarmsystem sind standardmäßig aktiviert, 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 (Legacy-System)

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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 **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.



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by equals

3 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Critical	Under 10000000	<=	10000000	
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Major	Under 50000000	<=	50000000	
<input type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 100000000	<=	100000000	

Apply Changes

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.

Globale benutzerdefinierte Alarme deaktivieren (Legacy-System)

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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**.



Global Custom Alarms (1 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>	All	RDTE (Tivoli Storage Manager State)	Major	Offline	=	10		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

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.

Benachrichtigungen für Alarme konfigurieren (Altsystem)

StorageGRID System kann automatisch E-Mails und senden [SNMP-Benachrichtigungen](#) Wenn ein Alarm ausgelöst wird oder sich ein Servicenstatus ändert.

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

Arten von Alarmanmeldungen (Legacy-System)

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

Benachrichtigungen auf Schweregraden

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

- Hinweis
- Gering
- Major
- Kritisch

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

Service-Status-Benachrichtigungen

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

- Unbekannt
- Administrativ Nach Unten

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

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

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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. Siehe [Anweisungen für die Administration von StorageGRID](#).

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

Schritte

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

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

Use these settings to define the email server used for alarm notifications and for AutoSupport messages. These settings are not used for alert notifications. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).



Email Server

Updated: 2016-03-17 11:11:59 PDT

E-mail Server (SMTP) Information

Mail Server	<input type="text"/>
Port	<input type="text"/>
Authentication	<input type="button" value="Off"/>
Authentication Credentials	Username: <input type="text" value="root"/>
	Password: <input type="password" value="....."/>
From Address	<input type="text"/>
Test E-mail	To: <input type="text"/>
	<input type="checkbox"/> Send Test E-mail

Apply Changes

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

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

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

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

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

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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 Alarmer (alt) Legacy E-Mail-Einrichtung**.

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



Email Templates

Updated: 2016-03-17 11:21:54 PDT

Template (0 - 0 of 0)

Template Name	Subject Prefix	Header	Footer	Actions
Template One	Notifications	All Email Lists	From SGWS	  

Show Records Per Page



- 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.

- 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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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).



Email Lists

Updated: 2016-03-17 11:56:24 PDT

Lists (0 - 0 of 0)

Group Name	Recipients	Template	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	  

Show Records Per Page

« »



4. Fügen Sie in der neuen Zeile Folgendes hinzu:

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

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

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

Es wird eine neue Mailingliste erstellt.

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

Um E-Mail-Benachrichtigungen für das 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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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.

Alarmbenachrichtigungen für eine Mailingliste unterdrücken (Älteres System)

Sie können Alarmbenachrichtigungen für eine Mailingliste unterdrücken, wenn Sie nicht mehr möchten, dass

die Mailingliste Benachrichtigungen über Alarme erhalten. Beispielsweise möchten Sie Benachrichtigungen über ältere Alarme unterdrücken, nachdem Sie zu Warnmeldungen gewechselt haben.

Was Sie benötigen


- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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.

E-Mail-Benachrichtigungen systemweit unterdrücken

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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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**.



Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input checked="" type="checkbox"/>

[Apply Changes](#) 

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

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

Konfigurieren von Überwachungsmeldungen und Protokollzielen

Audit-Meldungen und -Protokolle zeichnen Systemaktivitäten und Sicherheitsereignisse auf und sind wichtige Tools für das Monitoring und die Fehlerbehebung. Sie können die Audiorelevel anpassen, um die Art und Anzahl der aufgezeichneten Audit-Meldungen zu erhöhen oder zu verringern. Optional können Sie alle HTTP-Anforderungs-Header definieren, die Sie in Client-Audit-Nachrichten lesen und schreiben möchten. Sie können auch einen externen Syslog-Server konfigurieren und das Ziel der Audit-Informationen ändern.

Weitere Informationen zu Audit-Meldungen finden Sie unter [Prüfung von Audit-Protokollen](#).

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.

Über diese Aufgabe

Alle StorageGRID Nodes generieren Audit-Meldungen und -Protokolle, um die Systemaktivität und -Ereignisse nachzuverfolgen. Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können die Überwachungsstufen anpassen, um die Art und Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu erhöhen oder zu verringern. Optional können Sie die Audit-Informationen konfigurieren, die an einen Remote-Syslog-Server gesendet oder temporär auf den ausnehmenden Nodes zur manuellen Erfassung gespeichert werden sollen.

Ändern Sie die Meldungsebenen im Auditprotokoll

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

Audit-Kategorie	Beschreibung
System	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe Systemaudits Meldungen .
Storage	Diese Ebene ist standardmäßig auf Fehler festgelegt. Siehe Audit-Meldungen zu Objekt-Storage .
Vereinfachtes	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe Management-Audit-Nachricht .
Client Liest	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe Client liest Audit-Meldungen .
Client-Schreibvorgänge	Standardmäßig ist diese Ebene auf „Normal“ eingestellt. Siehe Audit-Meldungen des Clients schreiben .



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- und Syslog-Server**.

Audit and syslog server

Audit messages and logs record system activities and security events and are an essential tool for monitoring and troubleshooting.

Audit levels

Adjust audit levels to increase or decrease the type and number of audit messages recorded.

System	Normal
Storage	Error
Management	Normal
Client reads	Normal
Client writes	Normal

Audit protocol headers

Optionally, define any HTTP request headers you want to include in client read and write audit messages.

Header name 1

[Add another header](#)

Use external syslog server

By default, audit messages are saved on Admin Nodes and logs are saved on the nodes where they were generated. If you want to save audit messages and a subset of logs externally, configure an external syslog server.

i If you want to use an external syslog server, you must configure it first.

[Configure external syslog server](#)

If you want to change these log locations, select a different option below.

Log type	Log location
Audit log	Admin Nodes
Security events	Local nodes
Application logs	Local nodes

- Default (Admin Nodes/local nodes)
- External syslog server
- Admin Nodes and external syslog server
- Local nodes only

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.

Audit-Level	Beschreibung
Fehler	Nur Fehlermeldungen sind protokollierte - Audit-Meldungen, für die der Ergebniscode nicht „erfolgreich“ (SUCS) war.
Normal	Standardtransaktionsmeldungen werden protokolliert – die in diesen Anweisungen für die Kategorie aufgeführten Nachrichten.
Debuggen	Veraltet. Dieser Level verhält sich mit dem normalen Prüfstand.

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

3. Definieren Sie optional unter **Prüfprotokoll-Header** alle HTTP-Anforderungsheader, die Sie in die Lese- und Schreibnachrichten des Clients einbeziehen möchten. Verwenden Sie ein Sternchen (*) als Platzhalter, um Null oder mehr Zeichen zu entsprechen. Verwenden Sie die Escape-Sequenz (*), um mit einem wortwörtliche Sternchen überein.



Header für Prüfprotokolle sind nur auf S3 und Swift Anfragen anwendbar.

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

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



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

5. Wählen Sie **Speichern**

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

Verwenden Sie einen externen Syslog-Server

Sie können einen externen Syslog-Server konfigurieren, wenn Sie Audit-Informationen Remote speichern möchten.

- Wenn Sie Audit-Informationen auf einem externen Syslog-Server speichern möchten, gehen Sie zu [Konfigurieren Sie einen externen Syslog-Server](#).
- Wenn Sie keinen externen Syslog-Server verwenden, fahren Sie mit fort [Wählen Sie Ziele für Audit-Informationen aus](#).

Wählen Sie Ziele für Audit-Informationen aus

Sie können festlegen, wo Audit-Protokolle, Sicherheitsereignisprotokolle und Anwendungsprotokolle gesendet werden.



Einige Ziele sind nur verfügbar, wenn Sie einen externen Syslog-Server verwenden. Siehe [Konfigurieren Sie einen externen Syslog-Server](#) So konfigurieren Sie einen externen Syslog-Server:



Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter [StorageGRID-Softwareprotokolle](#).

1. Wählen Sie auf der Seite Audit- und Syslog-Server aus den aufgeführten Optionen das Ziel für Audit-Informationen aus:

Option	Beschreibung
Standard (Admin-Nodes/lokale Nodes)	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten werden Sicherheitsereignisprotokolle und Anwendungsprotokolle auf den Knoten gespeichert, in denen sie erzeugt wurden (auch als "der lokale Knoten" bezeichnet).
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Node und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Nur lokale Nodes	Es werden keine Audit-Informationen an einen Admin-Node oder Remote-Syslog-Server gesendet. Audit-Informationen werden nur auf den generierten Nodes gespeichert. Hinweis: StorageGRID entfernt regelmäßig diese lokalen Protokolle in einer Drehung, um Speicherplatz freizugeben. Wenn die Protokolldatei für einen Knoten 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet. Die Rotationsgrenze für das Protokoll beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Auf jedem Node werden durchschnittlich etwa 20 GB an Protokoll Daten gespeichert.



In werden Audit-Informationen, die für jeden lokalen Node generiert werden, gespeichert
`/var/local/log/localaudit.log`

1. Wählen Sie **Speichern**.

Es wird eine Warnmeldung angezeigt:



Protokollziel ändern?

1. Bestätigen Sie, dass Sie das Ziel für Audit-Informationen ändern möchten, indem Sie **OK** wählen.

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

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

Verwandte Informationen

[Überlegungen für externen Syslog-Server](#)

[StorageGRID verwalten](#)

[Fehlerbehebung für den externen Syslog-Server](#)

Verwenden Sie einen externen Syslog-Server

Überlegungen für externen Syslog-Server

Anhand der folgenden Richtlinien können Sie die Größe des benötigten externen Syslog-Servers einschätzen.

Was ist ein externer Syslog-Server?

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID, mit dem Sie Audit-Informationen zum System an einem Ort sammeln können. Mithilfe eines externen Syslog-Servers können Sie die Ziele Ihrer Audit-Informationen konfigurieren, sodass Sie den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten können. Folgende Arten von Audit-Informationen können Sie an den externen Syslog-Server senden:

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

Wie schätzen Sie die Größe des externen Syslog-Servers ein

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

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

In Schätzformeln S3-Operationen pro Sekunde verwenden

Wenn Ihr Grid für einen Durchsatz in Byte pro Sekunde ausgedrückt wurde, müssen Sie diese Größe in S3-Vorgänge pro Sekunde konvertieren, um die Abschätzung-Formeln zu verwenden. Um den Grid-Durchsatz zu konvertieren, müssen Sie zunächst die durchschnittliche Objektgröße festlegen, die Sie anhand der

Informationen in vorhandenen Audit-Protokollen und -Metriken (falls vorhanden) durchführen können, oder indem Sie Ihre Kenntnisse über die Anwendungen nutzen, die StorageGRID verwenden. Beispiel: Wenn Ihr Grid einen Durchsatz von 2,000 MB/s erreicht hat und die durchschnittliche Objektgröße 2 MB beträgt, wurde das Grid so dimensioniert, dass es 1,000 S3-Operationen pro Sekunde (2,000 MB/2 MB) verarbeiten kann.



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

Schätzformeln für Prüfprotokolle

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

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

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

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Die wichtigsten zusätzlichen Variablen sind für Audit-Protokolle der Prozentsatz der am häufigsten verwendeten S3-Vorgänge (im Vergleich zu RUFT) und die mittlere Größe der folgenden S3-Felder in Byte (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

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

Verwenden wir P, um den Prozentsatz der an Put-Vorgängen abzubilden, wobei $0 \leq P \leq 1$ (für einen 100 %

PUT-Workload, $P = 1$ und für einen 100 % GET-Workload, $P = 0$).

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

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

$$\text{Audit Log Rate} = ((2 \times P) + (1 - P)) \times \text{S3 Operations Rate}$$
$$\text{Audit Log Average Size} = (570 + K) \text{ bytes}$$

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

Schätzformeln für nicht standardmäßige Audit-Level

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

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

Schätzformeln für Sicherheitsereignisse

Sicherheitsereignisse werden nicht mit S3-Vorgängen korreliert und erzeugen in der Regel ein unvernachlässigbares Volume an Protokollen und Daten. Aus diesen Gründen werden keine Schätzformeln bereitgestellt.

Schätzformeln für Anwendungsprotokolle

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

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

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

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

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

Beispiel für eine Einschätzung der Dimensionierung

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

- Replizierung
- Verfahren Zur Einhaltung Von Datenkonsistenz

Wenn Sie Replizierung für die Datensicherung verwenden

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

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

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen,

die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss.

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

Wenn Ihr Grid beispielsweise für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, beträgt der Workload 50 % und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte, sollte der externe Syslog-Server entsprechend angepasst werden, um 1800 Applikations-Logs pro Sekunde zu unterstützen, Und erhalten Applikationsdaten mit einer Rate von 0.5 MB pro Sekunde (und in der Regel auch dort).

Bei Verwendung von Erasure Coding zur Datensicherung

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

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

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss.

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

Wenn Ihr Grid beispielsweise 1,000 S3-Vorgänge pro Sekunde beträgt, beträgt der Workload 50 % der Put-Vorgänge sowie Ihre S3-Kontonamen und Bucket-Namen Und Objektnamen durchschnittlich 90 Byte, Ihr externer Syslog-Server sollte Größe haben, um 2,250 Anwendungsprotokolle pro Sekunde zu unterstützen. Sie sollten in der Lage sein, Anwendungsdaten zu empfangen und zu empfangen (und in der Regel speichern) mit einer Rate von 0.6 MB pro Sekunde.

Weitere Informationen zur Konfiguration von Meldungsebenen und einem externen Syslog-Server finden Sie unter:

- [Konfigurieren Sie einen externen Syslog-Server](#)
- [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)

Konfigurieren Sie einen externen Syslog-Server

Wenn Sie Audit-Protokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Speicherort außerhalb des Grid speichern möchten, konfigurieren Sie einen externen Syslog-Server mithilfe dieses Verfahrens.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie verfügen über einen Syslog-Server mit der Kapazität, die Protokolldateien zu empfangen und zu speichern. Weitere Informationen finden Sie unter [Überlegungen für externen Syslog-Server](#).
- Sie haben die richtigen Server- und Client-Zertifizierungen, wenn Sie TLS oder RELP/TLS verwenden möchten.

Über diese Aufgabe

Wenn Sie Audit-Informationen an einen externen Syslog-Server senden möchten, müssen Sie zuerst den externen Server konfigurieren.

Durch das Senden von Audit-Informationen an einen externen Syslog-Server können Sie:

- Effizientere Erfassung und Verwaltung von Audit-Informationen wie Audit-Nachrichten, Applikationsprotokollen und Sicherheitsereignissen
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da Audit-Informationen direkt von den verschiedenen Speicherknoten auf den externen Syslog-Server übertragen werden, ohne über einen Admin-Knoten gehen zu müssen



Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit einer Größe von mehr als 8192 Byte am Ende der Nachricht gekürzt, um den allgemeinen Einschränkungen in externen Syslog-Server-Implementierungen zu entsprechen.



Um die Optionen für eine vollständige Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers zu maximieren, werden auf jedem Knoten bis zu 20 GB an lokalen Protokollen von Audit-Datensätzen (localaudit.log) aufbewahrt.



Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können zusätzliche Konfigurationsoptionen mithilfe der privaten API angewendet werden `audit-destinations` Endpunkte: So ist es beispielsweise möglich, unterschiedliche Syslog-Server für unterschiedliche Node-Gruppen zu verwenden.

Greifen Sie auf den Syslog-Server-Konfigurationsassistenten zu

Schritte

1. Wählen Sie **KONFIGURATION Überwachung Audit- und Syslog-Server**.

Audit and syslog server

Audit messages and logs record system activities and security events and are an essential tool for monitoring and troubleshooting.

Audit levels

Adjust audit levels to increase or decrease the type and number of audit messages recorded.

System	Normal
Storage	Error
Management	Normal
Client reads	Normal
Client writes	Normal

Audit protocol headers

Optionally, define any HTTP request headers you want to include in client read and write audit messages.

Header name 1

[Add another header](#)

Use external syslog server

By default, audit messages are saved on Admin Nodes and logs are saved on the nodes where they were generated. If you want to save audit messages and a subset of logs externally, configure an external syslog server.

i If you want to use an external syslog server, you must configure it first.

[Configure external syslog server](#)

If you want to change these log locations, select a different option below.

Log type	Log location
Audit log	Admin Nodes
Security events	Local nodes
Application logs	Local nodes

- Default (Admin Nodes/local nodes)
- External syslog server
- Admin Nodes and external syslog server
- Local nodes only

- Wählen Sie auf der Seite Audit- und Syslog-Server die Option **externen Syslog-Server konfigurieren** aus. Wenn Sie zuvor einen externen Syslog-Server konfiguriert haben, wählen Sie **Externe Syslog-Server bearbeiten**.

Syslog-Informationen eingeben

Configure external syslog server

1 Enter syslog info

2 Manage syslog content

3 Send test messages

External syslog server configuration

Host ?

syslog.test.com

A valid FQDN or IP address.

Port ?

514

An integer between 1 and 65535.

Protocol ?



TCP



TLS



RELP/TCP



RELP/TLS



UDP

Server CA certificates ?

Browse

Client certificate ?

Browse

Client private key ?

Browse

Cancel

Continue

1. Geben Sie im Feld **Host** einen gültigen vollständig qualifizierten Domännennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server ein.
2. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine Ganzzahl zwischen 1 und 65535 sein). Der Standardport ist 514.
3. Wählen Sie das Protokoll aus, das zum Senden von Audit-Informationen an den externen Syslog-Server verwendet wird.

TLS oder RELP/TLS wird empfohlen. Sie müssen ein Serverzertifikat hochladen, um eine dieser Optionen verwenden zu können.

Mithilfe von Zertifikaten lassen sich die Verbindungen zwischen dem Grid und dem externen Syslog-Server sichern. Weitere Informationen finden Sie unter [StorageGRID-Sicherheitszertifikate verwenden](#).

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



Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls für eine zuverlässige Bereitstellung von Ereignismeldungen. Mithilfe von RELP können Sie den Verlust von Audit-Informationen verhindern, wenn Ihr externer Syslog-Server neu gestartet werden muss.

4. Wählen Sie **Weiter**.

5. Wenn Sie **TLS** oder **RELPL/TLS** ausgewählt haben, laden Sie die folgenden Zertifikate hoch:

- **Server CA-Zertifikate:** Ein oder mehrere vertrauenswürdige CA-Zertifikate zur Überprüfung des externen Syslog-Servers (in PEM-Codierung). Wenn nicht angegeben, wird das Standard-Grid-CA-Zertifikat verwendet. Die Datei, die Sie hier hochladen, kann ein CA-Bundle sein.
- **Clientzertifikat:** Das Clientzertifikat zur Authentifizierung an den externen Syslog-Server (in PEM-Codierung).
- **Privater Client-Schlüssel:** Privater Schlüssel für das Clientzertifikat (in PEM-Kodierung).



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

- i. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel, das Sie verwenden möchten.
- ii. Wählen Sie die Zertifikatdatei oder die Schlüsseldatei aus.
- iii. Wählen Sie **Öffnen**, um die Datei hochzuladen.

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

6. Wählen Sie **Weiter**.

Syslog-Inhalte managen

Configure external syslog server

✓ Enter syslog info

2 Manage syslog content

✓ Send test messages

Manage syslog content

Send audit logs ?

Severity ? Informational (6) ▼

Facility ? local7 (23) ▼

Send security events ?

Severity ? Passthrough ▼

Facility ? Passthrough ▼

Send application logs ?

Severity ? Passthrough ▼

Facility ? Passthrough ▼

Previous

Continue

1. Wählen Sie die einzelnen Arten von Audit-Informationen aus, die Sie an den externen Syslog-Server senden möchten.

- **Prüfprotokolle senden:** StorageGRID-Ereignisse und Systemaktivitäten
- **Sicherheitsereignisse senden:** Sicherheitsereignisse wie z. B. wenn ein unberechtigter Benutzer versucht sich anzumelden oder sich ein Benutzer als Root anmeldet
- **Anwendungsprotokolle senden:** Log-Dateien nützlich für die Fehlerbehebung einschließlich:
 - bycast-err.log
 - bycast.log
 - jaeger.log
 - nms.log (nur Admin-Nodes)
 - prometheus.log
 - raft.log
 - hagroups.log

2. Verwenden Sie die Dropdown-Menüs, um den Schweregrad und die Einrichtung (Nachrichtentyp) für die Kategorie der zu sendenden Audit-Informationen auszuwählen.

Wenn Sie **Passthrough** für Schweregrad und Einrichtung auswählen, erhalten die an den Remote-Syslog-Server gesendeten Informationen denselben Schweregrad und dieselbe Einrichtung wie bei der lokalen Anmeldung am Node. Durch die Festlegung von Standort und Schweregrad können Sie die Protokolle individuell zusammenlegen und so die Analyse erleichtern.



Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter [StorageGRID-Softwareprotokolle](#).

- a. Wählen Sie für **Severity Passthrough** aus, wenn jede Nachricht, die an das externe Syslog gesendet wird, den gleichen Schweregrad wie im lokalen Syslog hat.

Wenn Sie für Prüfprotokolle **Passthrough** wählen, lautet der Schweregrad „Info“.

Wenn Sie bei Sicherheitsereignissen **Passthrough** auswählen, werden die Schweregrade von der linux-Distribution auf den Knoten erzeugt.

Wenn Sie bei Anwendungsprotokollen **Passthrough** auswählen, variieren die Schweregrade je nach Problem zwischen 'info' und 'Hinweis'. Zum Beispiel gibt das Hinzufügen eines NTP-Servers und die Konfiguration einer HA-Gruppe einen Wert von 'Info', während der ssm oder rsm-Service absichtlich gestoppt wird, einen Wert von 'Hinweis'.

- b. Wenn Sie den Passthrough-Wert nicht verwenden möchten, wählen Sie einen Schweregrad zwischen 0 und 7 aus.

Der ausgewählte Wert wird auf alle Meldungen dieses Typs angewendet. Informationen zu den verschiedenen Schweregraden gehen verloren, wenn Sie den Schweregrad mit einem festen Wert überschreiben.

Schweregrad	Beschreibung
0	Notfall: System ist unbrauchbar
1	Warnung: Maßnahmen müssen sofort ergriffen werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber bedeutender Zustand
6	Information: Informationsmeldungen
7	Debug: Debug-Level-Meldungen

- c. Wählen Sie für **Einrichtung Passthrough** aus, wenn jede Nachricht, die an das externe Syslog gesendet wird, den gleichen Wert wie im lokalen Syslog hat.

Wenn Sie für Prüfprotokolle **Passthrough** wählen, lautet die an den externen Syslog-Server gesendete Funktion „local7“.

Wenn Sie bei Sicherheitsereignissen **Passthrough** wählen, werden die Facility-Werte durch die linux-Distribution auf den Knoten generiert.

Wenn Sie bei Anwendungsprotokollen **Passthrough** auswählen, haben die an den externen Syslog-

Server gesendeten Anwendungsprotokolle die folgenden Facility-Werte:

Applikationsprotokoll	Durchlasswert
bycast.log	Benutzer oder Daemon
bycast-err.log	Benutzer, Daemon, local3 oder local4
jaeger.log	local2
nms.log	Lokalisierung 3
prometheus.log	local4
raft.log	Lokalisierung 5
hagroups.log	Lokalisierung 6

- d. Wenn Sie den Passthrough-Wert nicht verwenden möchten, wählen Sie den Facility-Wert zwischen 0 und 23 aus.

Der ausgewählte Wert wird auf alle Meldungen dieses Typs angewendet. Informationen über verschiedene Einrichtungen gehen verloren, wenn Sie eine Anlage mit einem festen Wert überschreiben möchten.

Anlage	Beschreibung
0	kern (Kernelmeldungen)
1	Benutzer (Meldungen auf Benutzerebene)
2	E-Mail
3	Daemon (Systemdemonen)
4	Auth (Sicherheits-/Autorisierungsmeldungen)
5	Syslog (intern erzeugte Nachrichten durch syslogd)
6	lpr (Liniendrucker-Subsystem)
7	nachrichten (Netzwerk-News-Subsystem)
8	UUCP
9	Cron (Clock Daemon)

Anlage	Beschreibung
10	Sicherheit (Sicherheits-/Autorisierungsmeldungen)
11	FTP
12	NTP
13	Logaudit (Protokollaudit)
14	Logalert (Protokollwarnung)
15	Uhr (Uhrzeitdaemon)
16	Local0
17	local1
18	local2
19	Lokalisierung 3
20	local4
21	Lokalisierung 5
22	Lokalisierung 6
23	Local7

3. Wählen Sie **Weiter**.

Versenden von Testmeldungen

Configure external syslog server



Enter syslog info



Manage syslog content



Send test messages

Send test messages from all nodes



After updating the syslog server configuration, confirm that the external syslog server can receive test StorageGRID messages. If the test messages cannot be delivered and you use this configuration, you might lose important messages regarding StorageGRID events and activities.

Before using the syslog server configuration, confirm that all nodes can send messages to the external server. Select **Send test messages** and then check the syslog server. Make sure it receives a test message from each node in your grid. As required, correct any reported errors and try again.

Send test messages

Previous

Skip and finish

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



Verwenden Sie die Konfiguration des externen Syslog-Servers erst, wenn Sie bestätigen, dass der externe Syslog-Server von jedem Knoten in Ihrem Raster eine Testmeldung empfangen hat und dass die Meldung wie erwartet verarbeitet wurde.

1. Wenn Sie keine Testmeldungen senden möchten und Sie sicher sind, dass Ihr externer Syslog-Server richtig konfiguriert ist und Audit-Informationen von allen Knoten in Ihrem Raster erhalten kann, wählen Sie **Überspringen und beenden**.

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

2. Wählen Sie **andernfalls * Testmeldungen senden*** aus.

Die Testergebnisse werden kontinuierlich auf der Seite angezeigt, bis Sie den Test beenden. Während der Test läuft, werden Ihre Audit-Meldungen weiterhin an Ihre zuvor konfigurierten Ziele gesendet.

3. Wenn Sie Fehler erhalten, korrigieren Sie diese und wählen Sie **Testmeldungen senden** erneut. Siehe [Fehlerbehebung beim externen Syslog-Server](#) Um Ihnen bei der Behebung von Fehlern zu helfen.
4. Warten Sie, bis ein grünes Banner angezeigt wird, dass alle Nodes die Tests bestanden haben.
5. Überprüfen Sie den Syslog-Server, ob Testmeldungen empfangen und verarbeitet werden wie erwartet.



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

6. Wählen Sie **Stop and Finish**.

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



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

Wählen Sie Ziele für Audit-Informationen aus

Sie können festlegen, wo Sicherheitsereignisprotokolle, Anwendungsprotokolle und Prüfmeldungsprotokolle gesendet werden.



Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter [StorageGRID-Softwareprotokolle](#).

1. Wählen Sie auf der Seite Audit- und Syslog-Server aus den aufgeführten Optionen das Ziel für Audit-Informationen aus:

Option	Beschreibung
Standard (Admin-Nodes/lokale Nodes)	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten werden Sicherheitsereignisprotokolle und Anwendungsprotokolle auf den Knoten gespeichert, in denen sie erzeugt wurden (auch als "der lokale Knoten" bezeichnet).
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Node und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>audit.log</code>) Auf dem Admin-Knoten und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Nur lokale Nodes	Es werden keine Audit-Informationen an einen Admin-Node oder Remote-Syslog-Server gesendet. Audit-Informationen werden nur auf den generierten Nodes gespeichert. Hinweis: StorageGRID entfernt regelmäßig diese lokalen Protokolle in einer Drehung, um Speicherplatz freizugeben. Wenn die Protokolldatei für einen Knoten 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet. Die Rotationsgrenze für das Protokoll beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Auf jedem Node werden durchschnittlich etwa 20 GB an Protokoll Daten gespeichert.



In werden Audit-Informationen, die für jeden lokalen Node generiert werden, gespeichert
`/var/local/log/localaudit.log`

1. Wählen Sie **Speichern**. Wählen Sie anschließend OK, um die Änderung am Protokollziel zu akzeptieren.
2. Wenn Sie entweder **Externer Syslog-Server** oder **Admin-Knoten und externer Syslog-Server** als Ziel für Audit-Informationen ausgewählt haben, wird eine zusätzliche Warnung angezeigt. Überprüfen Sie den Warntext.



Sie müssen bestätigen, dass der externe Syslog-Server Test-StorageGRID-Meldungen empfangen kann.

1. Bestätigen Sie, dass Sie das Ziel für Audit-Informationen ändern möchten, indem Sie **OK** wählen.

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

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

Verwandte Informationen

[Übersicht über Überwachungsnachrichten](#)

[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)

[Systemaudits Meldungen](#)

[Audit-Meldungen zu Objekt-Storage](#)

[Management-Audit-Nachricht](#)

[Client liest Audit-Meldungen](#)

[StorageGRID verwalten](#)

Verwenden Sie SNMP-Überwachung

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

- [Konfigurieren Sie den SNMP-Agent](#)
- [Aktualisieren Sie den SNMP-Agent](#)

Sorgen

Auf jedem StorageGRID-Knoten wird ein SNMP-Agent oder Daemon ausgeführt, der eine Management Information Base (MIB) bereitstellt. Die StorageGRID MIB enthält Tabellen- und Benachrichtigungsdefinitionen für Alarmer 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.

Jeder Alarm wird einem von drei Trap-Typen basierend auf dem Schweregrad des Alarms zugeordnet: ActiveMinorAlert, activeMajorAlert und activeCriticalAlert. Beschreibungen der Warnmeldungen, die diese Traps auslösen können, finden Sie im [Alerts Referenz](#).

- 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.

Auf die MIB zugreifen

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 \(Legacy-System\)](#)
- [Benachrichtigung über Stille](#)

Konfigurieren Sie den SNMP-Agent

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Berechtigung Root Access.

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.

SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

Enable SNMP

Save

- 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.

SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

Enable SNMP

System Contact

System Location

Enable SNMP Agent Notifications

Enable Authentication Traps

Community Strings

Default Trap Community

Read-Only Community

String 1 +

Other Configurations

Agent Addresses (0)

USM Users (0)

Trap Destinations (0)

+ Create Edit Remove

Internet Protocol	Transport Protocol	StorageGRID Network	Port
-------------------	--------------------	---------------------	------

No results found.

Save

- 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.

- 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 auslieferte 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.

Create Agent Address

Internet Protocol IPv4 IPv6

Transport Protocol UDP TCP

StorageGRID Network

Port

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.

Other Configurations

Agent Addresses (2)

USM Users (2)

Trap Destinations (2)

+ Create **✎** Edit **✕** Remove

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

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.

Create USM User

Username

Read-Only MIB Access

Authoritative Engine ID

Security Level authPriv authNoPriv

Authentication

Protocol

Password

Confirm Password

Privacy

Protocol

Password

Confirm Password

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.

Other Configurations

Agent Addresses (2)

USM Users (3)

Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	<input checked="" type="checkbox"/>	authNoPriv	
<input type="radio"/>	user1	<input type="checkbox"/>	authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3	<input type="checkbox"/>	authPriv	59D39E801256

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.

Create Trap Destination

Version SNMPv1 SNMPv2C SNMPv3

Type ⓘ Trap

Host ⓘ

Port ⓘ 162

Protocol ⓘ UDP TCP

Community String ⓘ Use the default trap community: No default found
(Specify the default on the SNMP Agent page.)
 Use a custom community string

Custom Community String

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	<p>Hinweis: für SNMPv1 kann der SNMP-Agent nur Traps senden. Informationen werden nicht unterstützt.</p> <ol style="list-style-type: none"> 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. <p>Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.</p>
SNMPv2c	<ol style="list-style-type: none"> 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. <p>Die benutzerdefinierte Community-Zeichenfolge kann maximal 32 Zeichen lang sein und darf kein Leerzeichen enthalten.</p>

Version	Geben Sie diese Informationen an
SNMPv3	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> ◦ 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.

Other Configurations

Agent Addresses (1) USM Users (2) **Trap Destinations (2)**

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>						
	Version	Type	Host	Port	Protocol	Community/USM User
<input type="radio"/>	SNMPv3	Trap	local		UDP	User: Read only user
<input type="radio"/>	SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user

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

Die neue SNMP-Agent-Konfiguration wird aktiv.

Verwandte Informationen

[Benachrichtigung über Stille](#)

Aktualisieren Sie den SNMP-Agent

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

Jedes Mal, wenn Sie den aktualisieren [SNMP-Agent-Konfiguration](#), Beachten Sie, dass Sie unten auf der Seite SNMP Agent auf **Speichern** klicken müssen, um alle Änderungen zu übernehmen, 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.

Other Configurations

Agent Addresses (2) USM Users (2) Trap Destinations (2)

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

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.

- Um eine Agentenadresse hinzuzufügen, klicken Sie auf **Erstellen**. Lesen Sie dann den Schritt für Agent-Adressen in den Anweisungen zur Konfiguration des SNMP-Agenten.
 - 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.
 - 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.
 - 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.

Other Configurations

Agent Addresses (2) USM Users (3) Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	<input checked="" type="checkbox"/>	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

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

- 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.

Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Undefined trap destination usmUser 'user1'

OK

- a. Um Ihre Änderungen zu speichern, klicken Sie unten auf der Seite SNMP Agent auf **Speichern**.

9. Wenn Sie Trap-Ziele aktualisieren möchten, wählen Sie im Abschnitt andere Konfigurationen die Registerkarte Trap-Ziele aus.

Other Configurations

Agent Addresses (1)

USM Users (2)

Trap Destinations (2)

[+ Create](#) [✎ Edit](#) [✕ Remove](#)

	Version	Type	Host	Port	Protocol	Community/USM User
<input type="radio"/>	SNMPv3	Trap	local		UDP	User: Read only user
<input type="radio"/>	SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user

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**.
10. Wenn Sie die SNMP-Agent-Konfiguration aktualisiert haben, klicken Sie auf **Speichern**.

Erfassung zusätzlicher StorageGRID-Daten

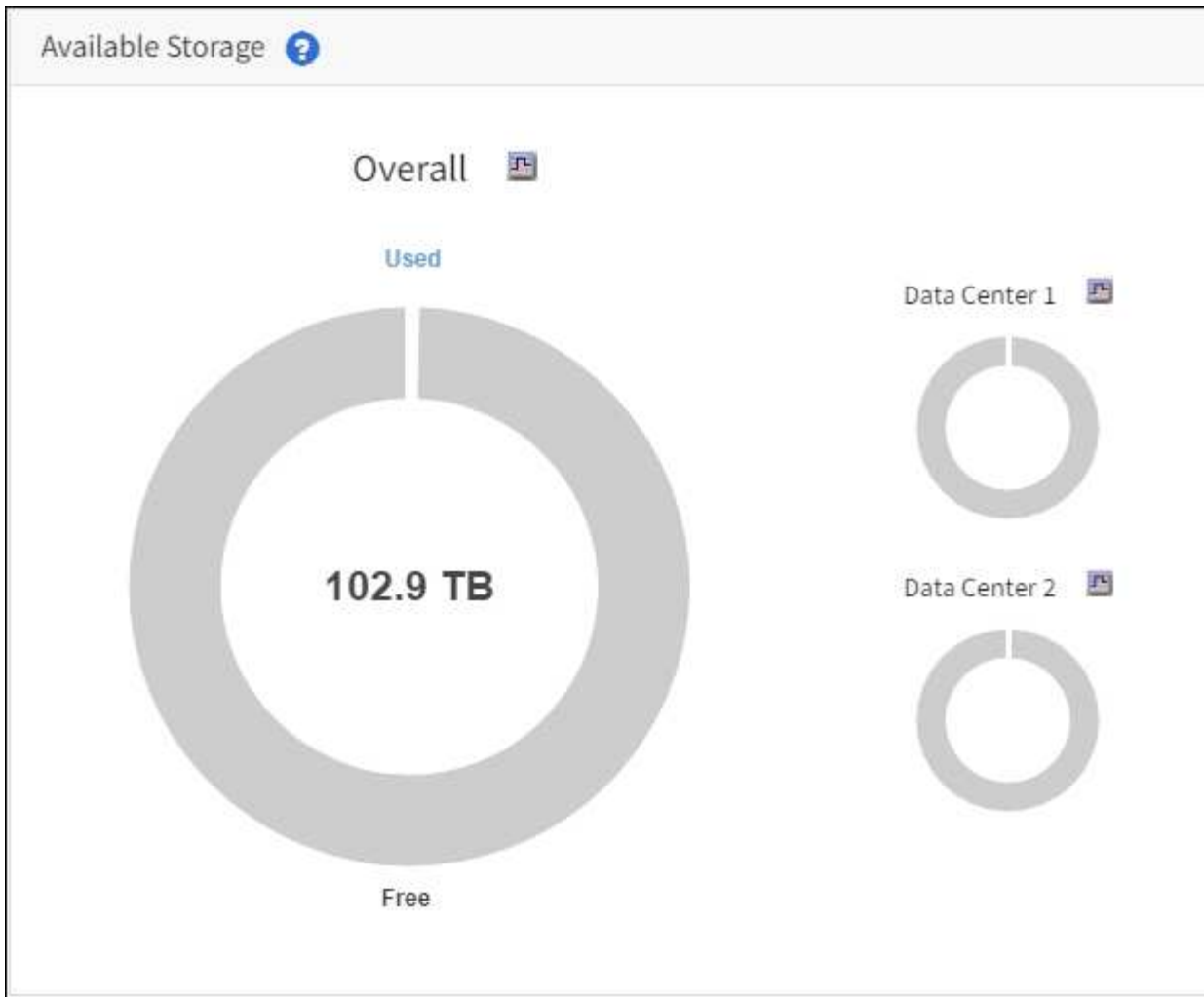
Verwenden Sie Diagramme und Diagramme

Mithilfe von Diagrammen und Berichten lässt sich der Zustand des StorageGRID Systems überwachen und Probleme beheben. Die im Grid Manager verfügbaren Diagrammtypen und Berichte umfassen Donut-Diagramme (nur auf dem Dashboard), Diagramme und Textberichte.

Diagrammtypen

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

Das Grid Manager Dashboard enthält Donut-Diagramme, die den verfügbaren Speicherplatz für das Grid und jeden Standort zusammenfassen.



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

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

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

Es gibt vier Arten von Diagrammen:

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

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

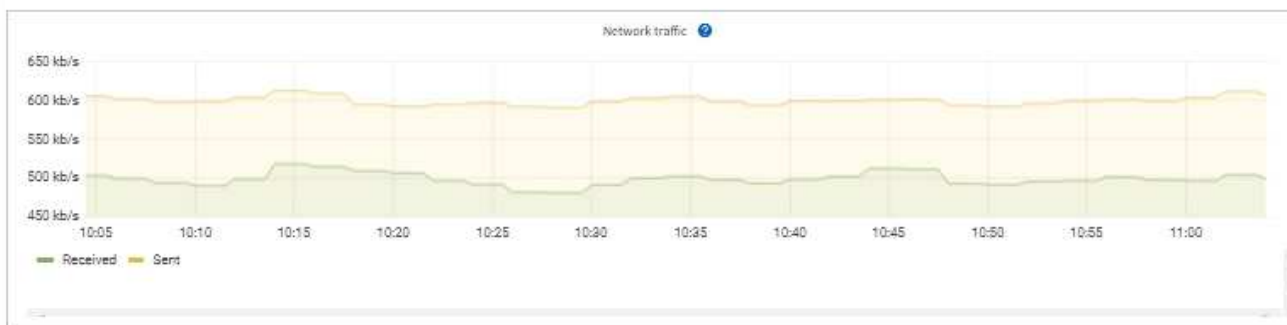
1 hour

1 day

1 week

1 month

Custom



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive


Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

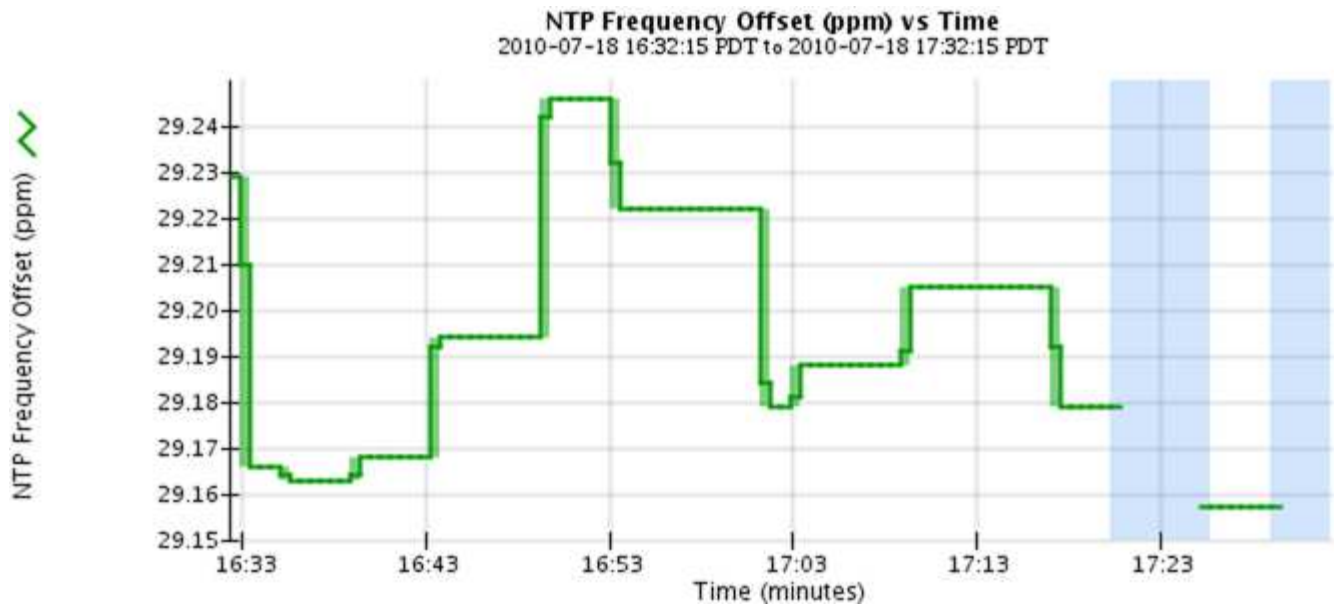
Transmit


Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

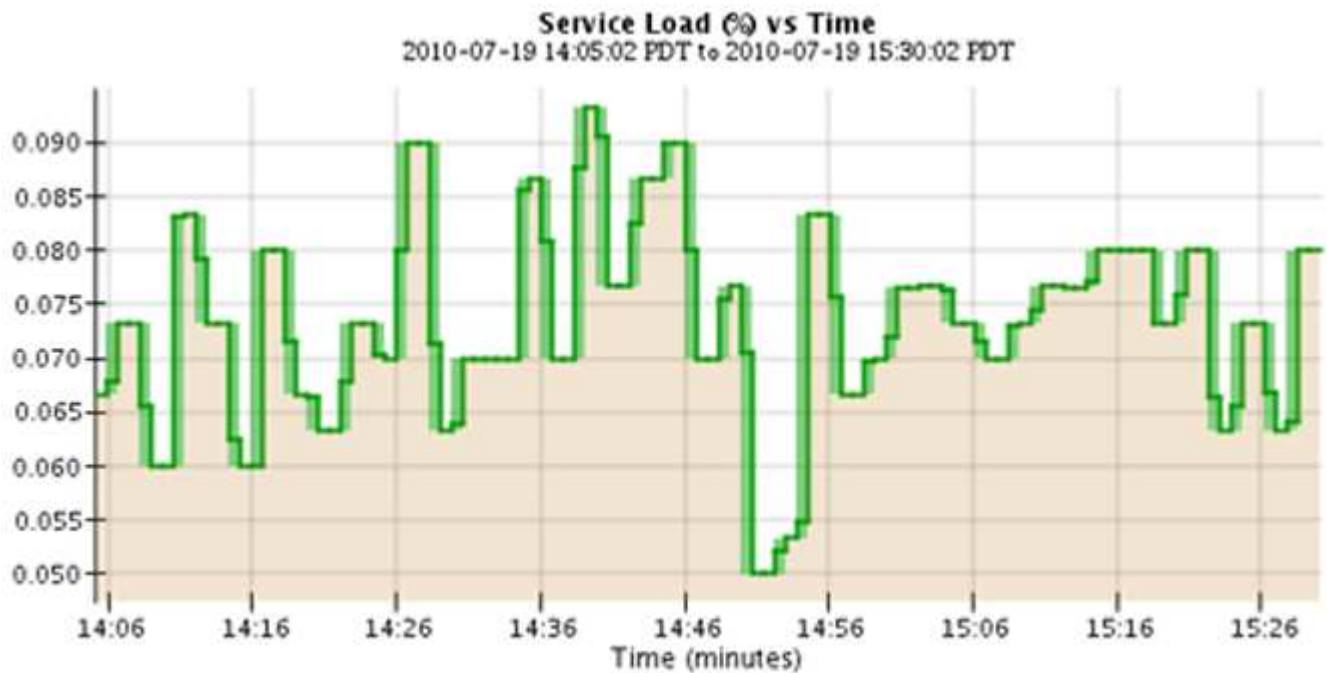



Grafana-Diagramme sind auch auf den vorgebauten Dashboards enthalten, die auf der Seite **SUPPORT Tools Metrics** zur Verfügung stehen.

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



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



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

1 hour 1 day 1 week 1 month Custom

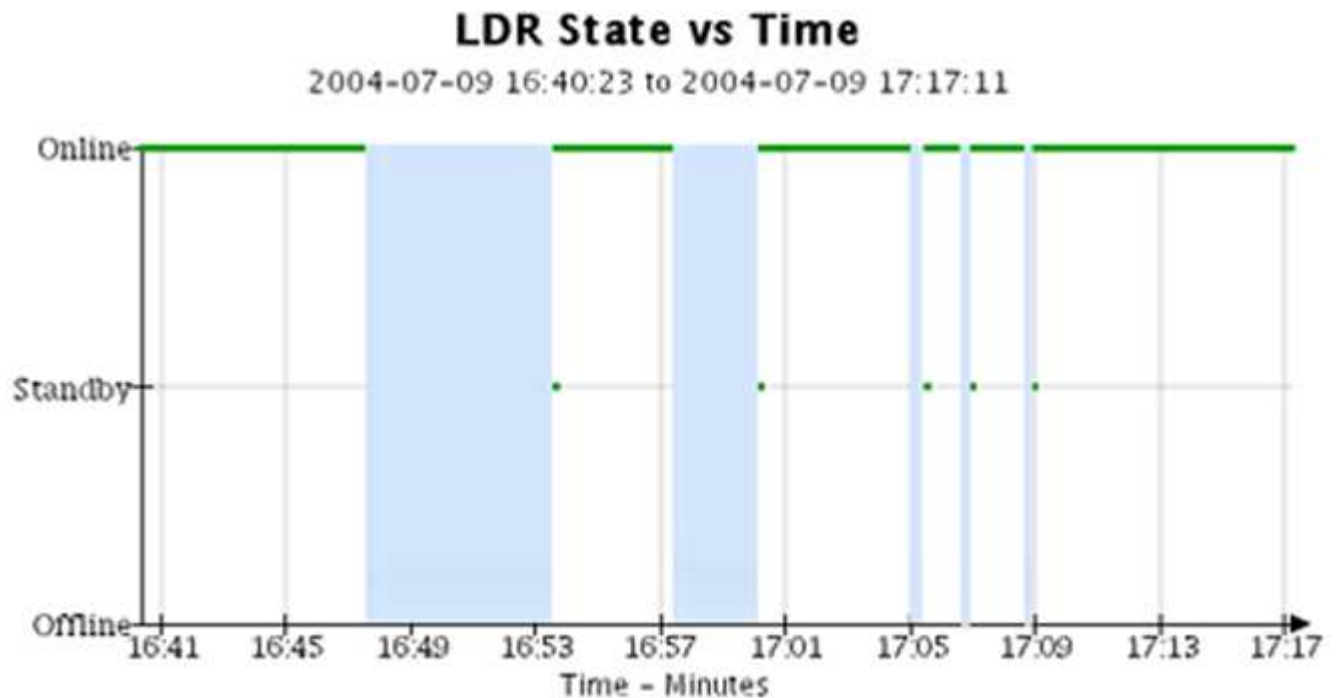
From: 2020-10-01 [calendar icon] 12 : 45 PM PDT

To: 2020-10-01 [calendar icon] 01 : 10 PM PDT Apply



Close

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



Verwandte Informationen







[Zeigen Sie die Seite Knoten an](#)

[Sehen Sie sich den Baum der Grid Topology an](#)

[Prüfen von Support-Kennzahlen](#)

Diagrammlegende

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

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 unbekanntem 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 unbekanntem Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldet, administrativ nach unten lag.

Zeigen Sie Diagramme und Diagramme an

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

Was Sie benötigen

Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

Schritte

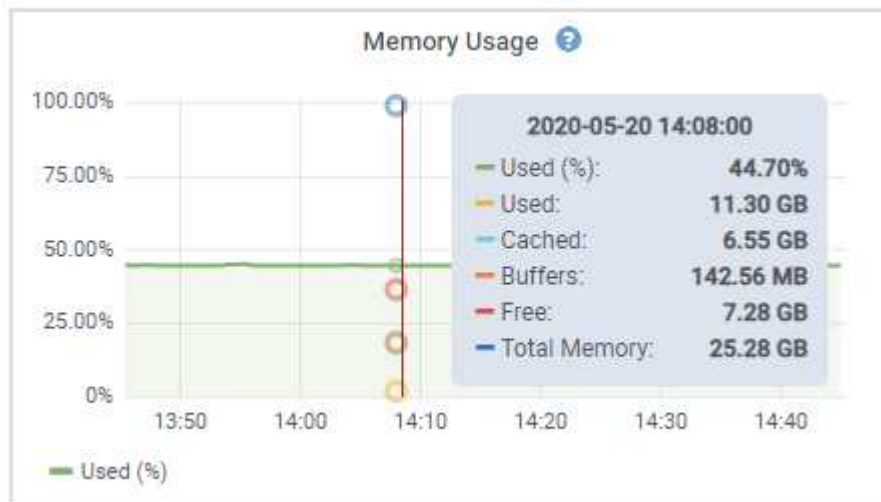
1. Wählen Sie **KNOTEN**. Wählen Sie dann einen Knoten, einen Standort oder das gesamte Raster aus.

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

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



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




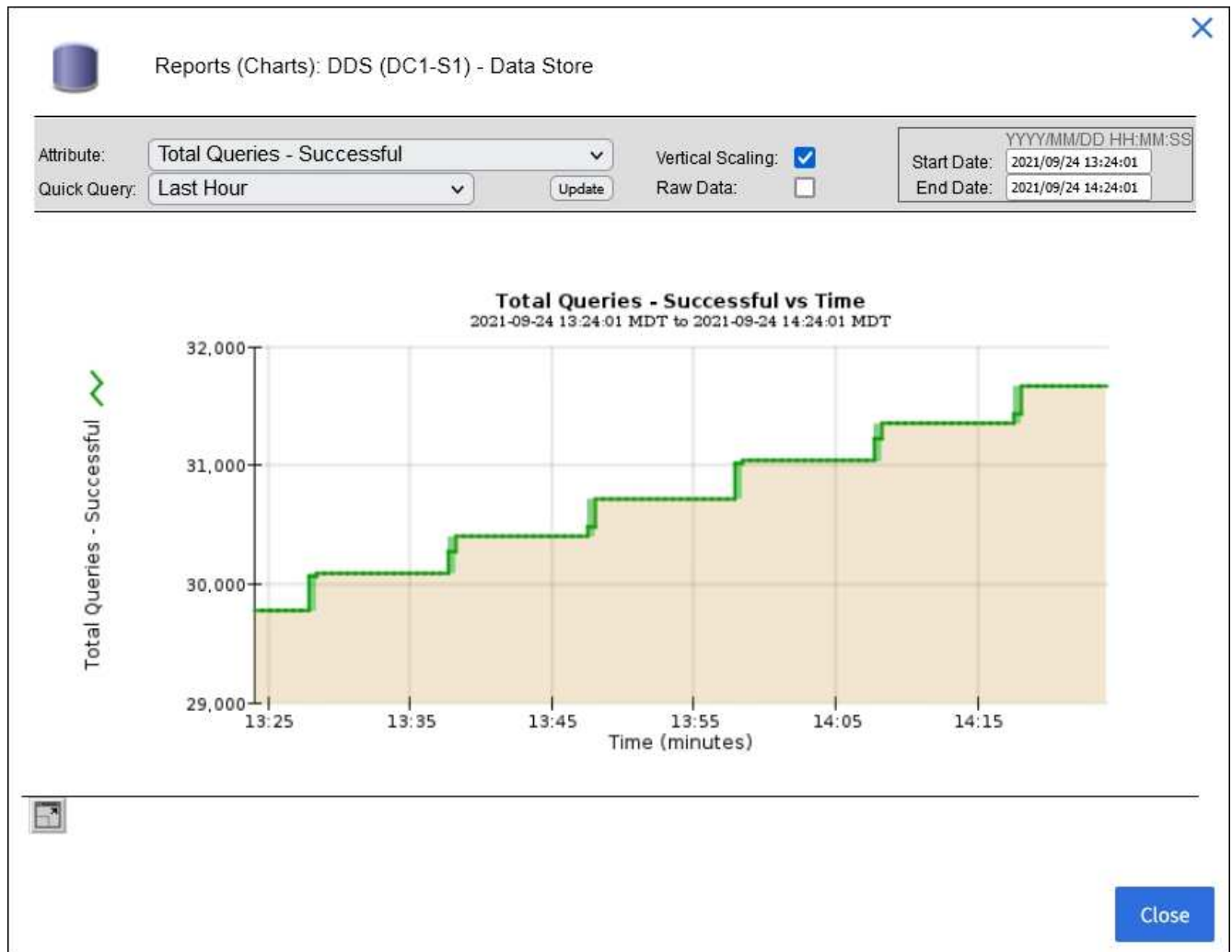
4. Bei Bedarf können Sie oft ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Wählen Sie in der Tabelle auf der Seite Knoten das Diagrammsymbol aus  Rechts neben dem Attributnamen.

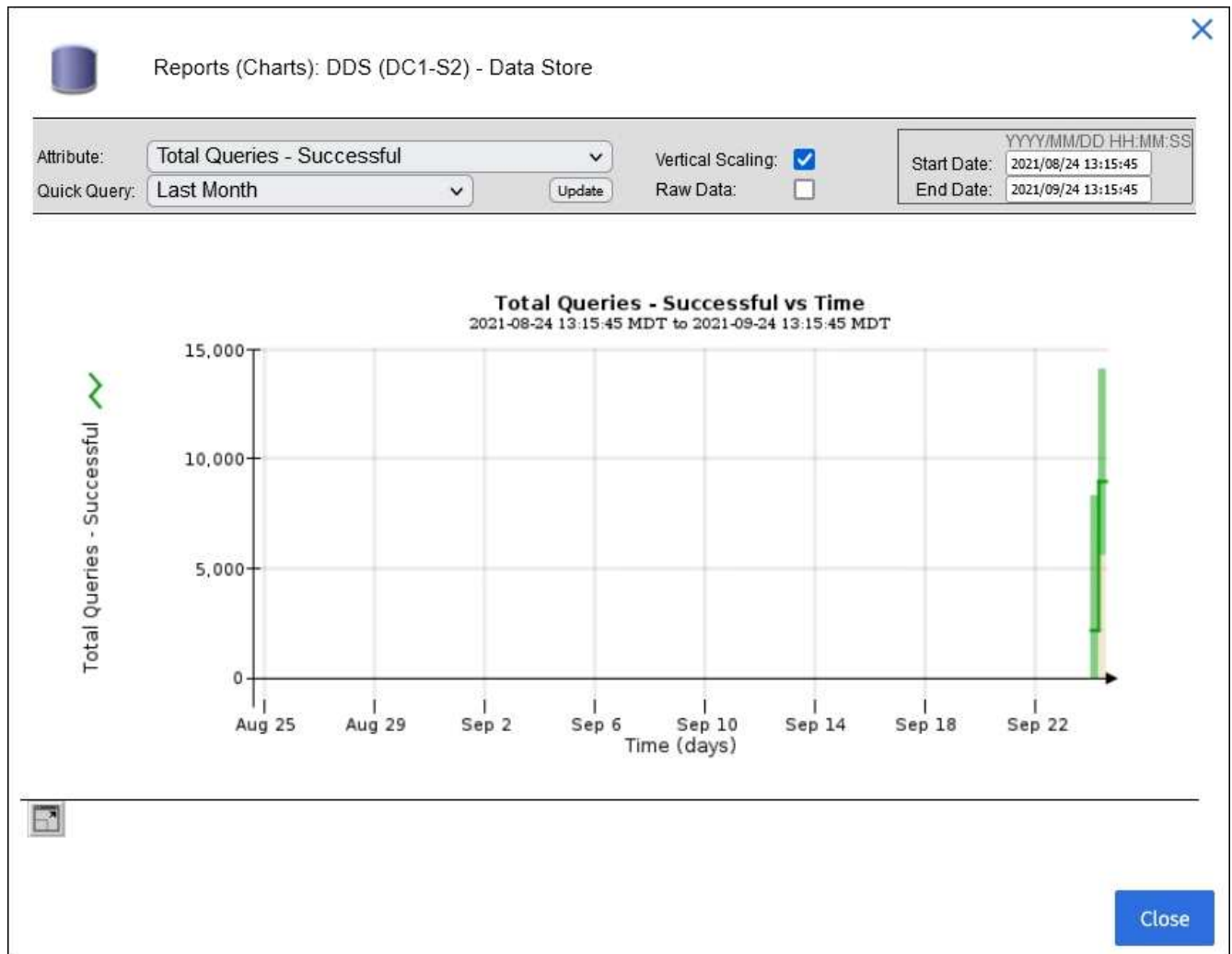



Diagramme sind nicht für alle Metriken und Attribute verfügbar.

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


anzuzeigen.

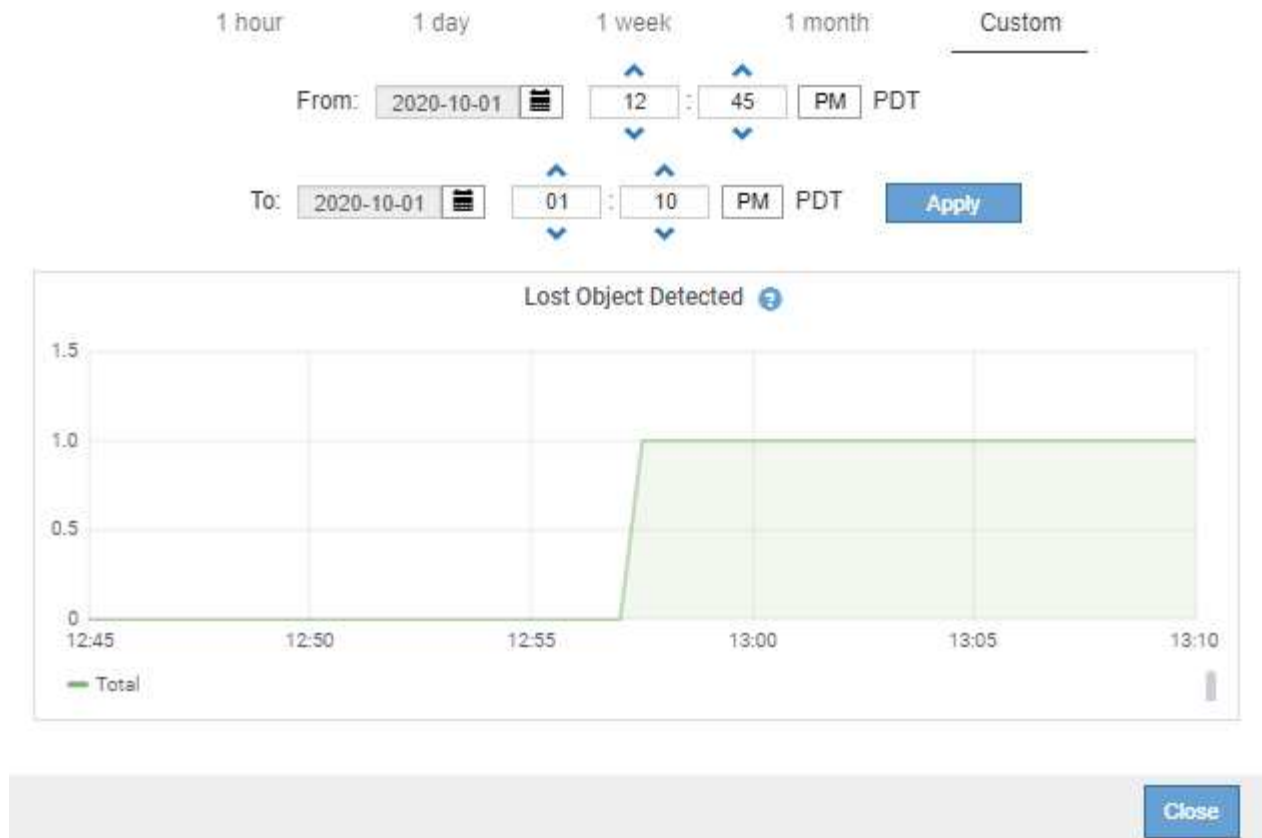





Beispiel 2: Auf der Registerkarte Objekte für einen Speicherknoten können Sie das Diagrammsymbol auswählen  Zeigt die Grafana-Grafik der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte an.

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





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

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

Diagramme generieren

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Grid Node Component oder Service Berichte Diagramme** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Um 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. Wählen Sie **Aktualisieren**.

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

Verwenden Sie Textberichte

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

RAW-Textberichte

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

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

Text Results for Services: Load - System Logging

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

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

Zusammenfassen von Textberichten

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

In jedem Eintrag werden die folgenden Informationen angezeigt:

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

Text Results for Attribute Send to Relay Rate

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

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

Erstellen von Textberichten

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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 unbekanntem Zustand war.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Grid Node Component oder Service Berichte Text** aus.
3. Wählen Sie das Attribut aus der Dropdown-Liste **Attribut** aus, für das ein Bericht erstellt werden soll.
4. Wählen Sie aus der Dropdown-Liste **Ergebnisse pro Seite** die Anzahl der Ergebnisse pro Seite aus.
5. Um Werte auf maximal drei Dezimalstellen (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.


Exportieren von Textberichten

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

Über diese Aufgabe

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

Schritte

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

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

Grid ID: 000 000

OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200

Node Path: Site/170-176/SSM/Events

Attribute: Attribute Send to Relay Rate (ABSR)

Query Start Date: 2010-07-19 08:42:09 PDT

Query End Date: 2010-07-20 08:42:09 PDT

Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type

2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U

2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U

2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U

2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U

2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U

2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U

2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U

2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U

2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U

2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U

2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U

2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U

2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

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

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

PUT- und GET-Performance werden überwacht

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

Über diese Aufgabe

Um DIE PUT- und GET-Leistung zu überwachen, können Sie S3- und Swift-Befehle direkt von einer Workstation aus oder über die Open-Source S3tester-Anwendung ausführen. Mit diesen Methoden können Sie die Leistung unabhängig von Faktoren bewerten, die außerhalb von StorageGRID liegen, z. B. Probleme mit einer Client-Applikation oder Probleme mit einem externen Netzwerk.

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

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

Meldungen in [Prüfprotokoll](#) Geben Sie die Gesamtzeit an, die für die Ausführung bestimmter Vorgänge erforderlich ist. Um z. B. die Gesamtverarbeitungszeit für eine S3-GET-Anforderung zu bestimmen, können Sie den Wert des ZEITATTRIBUTS in der SGET-Audit-Nachricht prüfen. Das ZEITATTRIBUT finden Sie auch in den Audit-Meldungen für die folgenden Vorgänge:

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

Bei der Analyse von Ergebnissen sollten Sie die durchschnittliche Zeit zur Erfüllung einer Anfrage sowie den Gesamtdurchsatz betrachten, den Sie erreichen können. Wiederholen Sie die gleichen Tests regelmäßig, und

notieren Sie die Ergebnisse, damit Sie Trends erkennen können, die möglicherweise untersucht werden müssen.

- Das können Sie ["Laden Sie S3tester von Github herunter"](#).

Überwachen von Objektverifizierungsvorgängen

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.

Über diese Aufgabe

Zwei [Verifizierungsprozesse](#) Gewährleisten Sie gemeinsam die Datenintegrität:

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

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



Die Warnung **nicht identifiziertes korruptes Objekt erkannt** wird ausgelöst, wenn das System ein korruptes Objekt erkennt, das nicht automatisch korrigiert werden kann.

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

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

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

Schritte

1. Prüfen Sie die Ergebnisse aus Hintergrundverifizierungen:

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

b. Überprüfen Sie die Überprüfungsergebnisse:

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

Verification

Status: ?	No errors	
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	

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

Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

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

2. Überprüfen Sie die Ergebnisse von Objektprüfaufträgen:

- Wählen Sie **WARTUNG Objekt Existenzprüfung Jobverlauf**.
- Scannen Sie die Spalte „fehlende Objektkopien erkannt“. Wenn Aufträge zu 100 oder mehr fehlenden Objektkopien und dem geführt haben [Warnmeldung für Objekte verloren](#) Wurde ausgelöst, wenden Sie sich an den technischen Support.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job | **Job history**

Delete | Search...

<input type="checkbox"/>	Job ID [?]	Status [⬇]	Nodes (volumes) [?]	Missing object copies detected [?]
<input type="checkbox"/>	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
<input type="checkbox"/>	12538643155010477372	Completed	DC1-S3 (1 volume)	0
<input type="checkbox"/>	5490044849774982476	Completed	DC1-S2 (1 volume)	0
<input type="checkbox"/>	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and <u>7 more</u>	0

Monitoring von Ereignissen

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

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log` Protokolldatei. Siehe [Referenz für Protokolldateien](#).

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

Schritte

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

- Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- Wählen Sie **site Grid Node SSM Ereignisse Berichte** aus.
- Wählen Sie **Text**.

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

- Ändern Sie **Attribut** in **Letztes Ereignis**.
- Wählen Sie optional einen Zeitraum für **Quick Query** aus.
- Wählen Sie **Aktualisieren**.

Text Results for Last Event
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Erstellen benutzerdefinierter Syslog-Ereignisse

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

Über diese Aufgabe



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

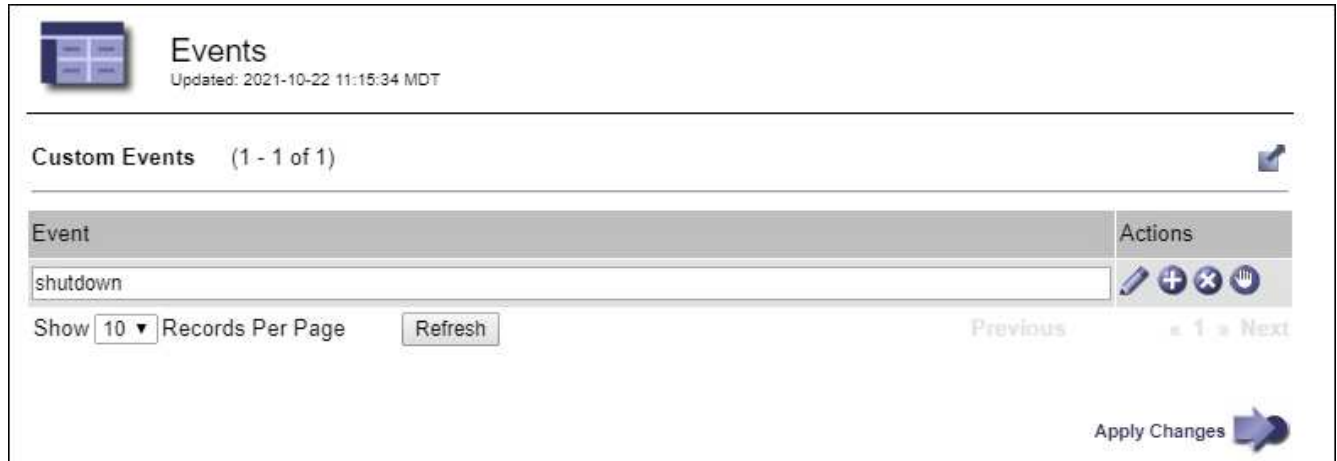
- Nach der Erstellung eines benutzerdefinierten Ereignisses wird jeder Vorgang überwacht.
- So erstellen Sie ein benutzerdefiniertes Ereignis basierend auf Schlüsselwörtern im `/var/local/log/messages` Dateien, die Protokolle in diesen Dateien müssen:
 - Vom Kernel generiert
 - Wird vom Daemon oder vom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

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

Schritte





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

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




Events
Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1)

Event	Actions
shutdown	   

Show 10 Records Per Page Refresh Previous 1 Next

Apply Changes 

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

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

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC1-ADM1) - Events

Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State:	Connected	
Total Events:	0	
Last Event:	No Events	

Description	Count	
Abnormal Software Events	0	
Account Service Events	0	
Cassandra Errors	0	
Cassandra Heap Out Of Memory Errors	0	
Chunk Service Events	0	
Custom Events	0	
Data-Mover Service Events	0	
File System Errors	0	
Forced Termination Events	0	
Grid Node Errors	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	
Out Of Memory Errors	0	
Replicated State Machine Service Events	0	
SCSI Errors	0	


Setzen Sie die Anzahl der benutzerdefinierten Ereignisse auf Null zurück

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

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

Overview			Alarms			Reports			Configuration		
Main			Alarms								
 Configuration: SSM (DC2-ADM1) - Events Updated: 2018-04-11 10:35:44 MDT											
Description	Count	Reset									
Abnormal Software Events	0	<input type="checkbox"/>									
Account Service Events	0	<input type="checkbox"/>									
Cassandra Errors	0	<input type="checkbox"/>									
Cassandra Heap Out Of Memory Errors	0	<input type="checkbox"/>									
Custom Events	0	<input checked="" type="checkbox"/>									
File System Errors	0	<input type="checkbox"/>									
Forced Termination Events	0	<input type="checkbox"/>									

4. Wählen Sie **Änderungen Anwenden**.

Audit-Meldungen prüfen

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

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

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

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

Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf die Audit-Share sowohl für NFS als auch für CIFS konfigurieren (CIFS ist veraltet). Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#).

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](#)

Erfassen von Protokolldateien und Systemdaten

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

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Über diese Aufgabe

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

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#).

Schritte

1. Wählen Sie **SUPPORT Tools Logs**.

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

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

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

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

4. Wählen Sie die Protokolltypen aus, die Sie sammeln möchten.

- **Anwendungsprotokolle:** Anwendungsspezifische Protokolle, die der technische Support am häufigsten für die Fehlerbehebung verwendet. Die gesammelten Protokolle sind eine Teilmenge der verfügbaren Anwendungsprotokolle.
- **Audit Logs:** Protokolle, die die während des normalen Systembetriebs erzeugten Audit-Meldungen enthalten.
- **Network Trace:** Protokolle, die für das Debuggen von Netzwerken verwendet werden.
- **Prometheus Datenbank:** Zeitreihenkenzahlen aus den Diensten auf allen Knoten.

5. Geben Sie optional Notizen zu den Protokolldateien ein, die Sie im Textfeld **Hinweise** sammeln.

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

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

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

7. Wählen Sie **Protokolle Sammeln**.

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

Auf der Seite „Protokolle“ können Sie den Fortschritt der Sammlung von Protokolldateien für jeden Grid-Knoten überwachen.

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

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

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

Nachdem Sie fertig sind

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

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

Senden Sie manuell eine AutoSupport Meldung aus

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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Root Access oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **SUPPORT Tools 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.

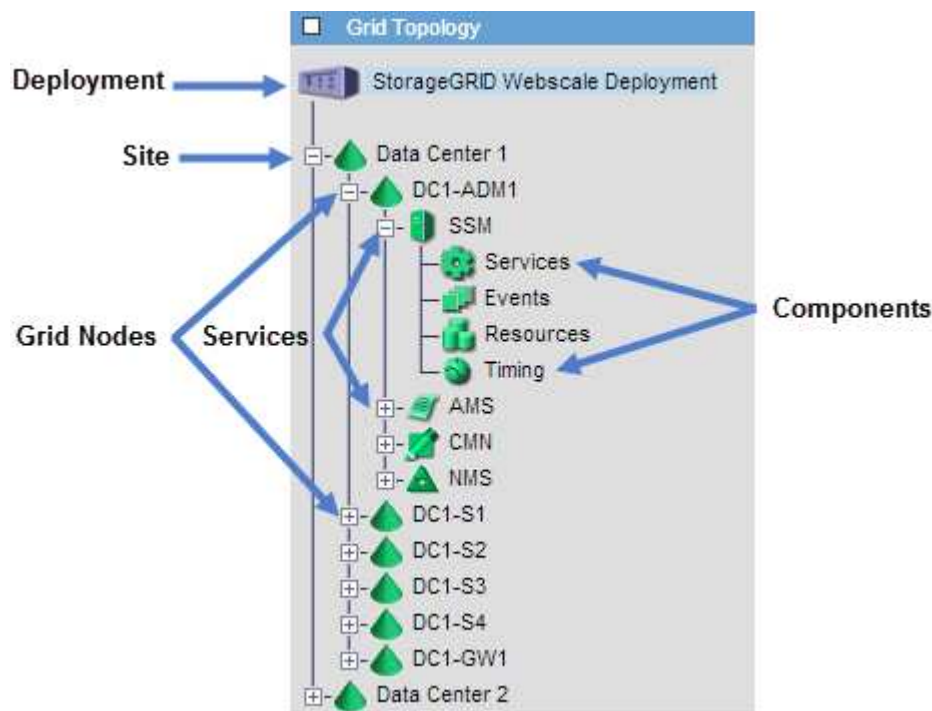
Verwandte Informationen

[E-Mail-Servereinstellungen für Alarme konfigurieren \(Legacy-System\)](#)

Sehen Sie sich den Baum der Grid Topology an

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

Um auf den Grid Topology-Baum zuzugreifen, wählen Sie **SUPPORT Tools Grid-Topologie**.



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

Prüfen von Support-Kennzahlen

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support detaillierte Metriken und Diagramme für Ihr StorageGRID System prüfen.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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. Siehe Liste von [Häufig verwendete Prometheus-Kennzahlen](#).

Schritte

1. Wählen Sie nach Anweisung des technischen Supports **SUPPORT Tools Metriken** aus.

Ein Beispiel für die Seite Metriken ist hier aufgeführt:

2. Um die aktuellen Werte der StorageGRID-Metriken abzufragen und Diagramme der Werte im Zeitverlauf anzuzeigen, klicken Sie im Abschnitt Prometheus auf den Link.

Das Prometheus-Interface wird angezeigt. Sie können über diese Schnittstelle Abfragen für die verfügbaren StorageGRID-Metriken ausführen und StorageGRID-Metriken im Laufe der Zeit grafisch darstellen.

Prometheus Alerts Graph Status Help

Enable query history

Expression (press Shift+Enter for newlines)

Execute - insert metric at cursor -

Graph Console

Element	Value
no data	

Remove Graph

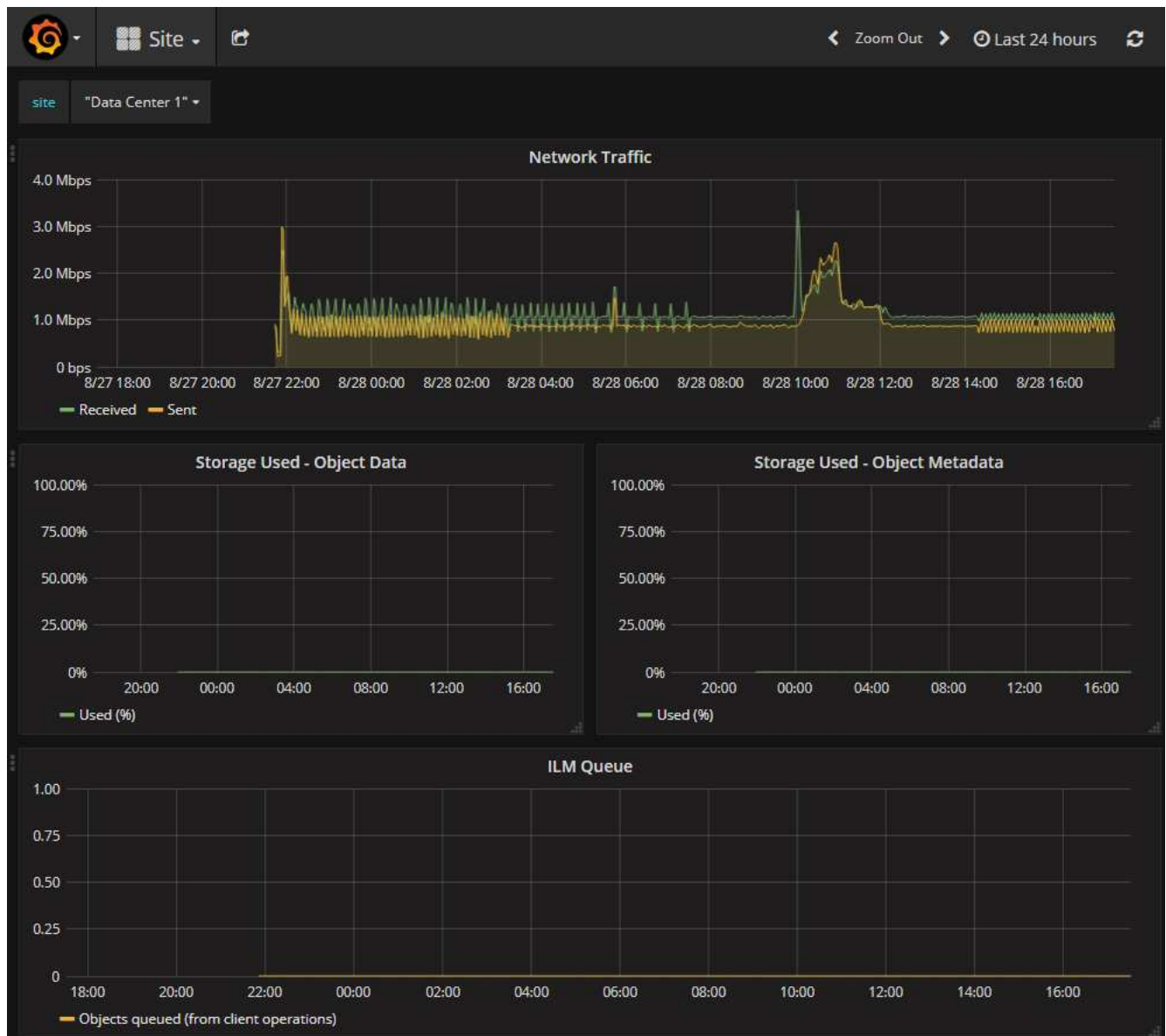
Add Graph



Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

- Um über einen längeren Zeitraum auf vorkonfigurierte Dashboards mit Diagrammen zu StorageGRID-Kennzahlen zuzugreifen, klicken Sie im Abschnitt „Grafana“ auf die Links.

Die Grafana-Schnittstelle für den ausgewählten Link wird angezeigt.



Führen Sie eine Diagnose aus

Bei der Fehlerbehebung eines Problems können Sie gemeinsam mit dem technischen Support eine Diagnose auf Ihrem StorageGRID-System durchführen und die Ergebnisse überprüfen.




- [Prüfen von Support-Kennzahlen](#)
- [Häufig verwendete Prometheus-Kennzahlen](#)

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Seite Diagnose führt eine Reihe von diagnostischen Prüfungen zum aktuellen Status des Rasters durch. Jede diagnostische Prüfung kann einen von drei Zuständen haben:

-  **Normal:** Alle Werte liegen im Normalbereich.
-  **Achtung:** Ein oder mehrere Werte liegen außerhalb des normalen Bereichs.
-  **Achtung:** Ein oder mehrere der Werte liegen deutlich außerhalb des normalen Bereichs.

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

Schritte




1. Wählen Sie **SUPPORT Tools Diagnose**.

Die Seite Diagnose wird angezeigt und zeigt die Ergebnisse für jede Diagnostiktest an. Die Ergebnisse sind nach Schweregrad (Achtung, Achtung und dann normal) sortiert. Innerhalb jedes Schweregrads werden die Ergebnisse alphabetisch sortiert.

In diesem Beispiel haben alle Diagnosen einen normalen Status.









Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

-  **Normal:** All values are within the normal range.
-  **Attention:** One or more of the values are outside of the normal range.
-  **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

[Run Diagnostics](#)

-  **Cassandra blocked task queue too large** 
-  **Cassandra commit log latency** 
-  **Cassandra commit log queue depth** 
-  **Cassandra compaction queue too large** 

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

Details zur Diagnose und ihren aktuellen Ergebnissen werden angezeigt. Folgende Details sind aufgelistet:

- **Status:** Der aktuelle Status dieser Diagnose: Normal, Achtung oder Achtung.
- **Prometheus query:** Bei Verwendung für die Diagnose, der Prometheus Ausdruck, der verwendet wurde, um die Statuswerte zu generieren. (Ein Prometheus-Ausdruck wird nicht für alle Diagnosen verwendet.)
- **Schwellenwerte:** Wenn für die Diagnose verfügbar, die systemdefinierten Schwellenwerte für jeden anormalen Diagnosestatus. (Schwellenwerte werden nicht für alle Diagnosen verwendet.)



Sie können diese Schwellenwerte nicht ändern.

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

✓ **CPU utilization**
⤴

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status ✓ Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`
[View in Prometheus](#)

Thresholds ⚠ Attention >= 75%
 ⚠ Caution >= 95%

Status	Instance	CPU Utilization
✓	DC1-ADM1	2.598%
✓	DC1-ARC1	0.937%
✓	DC1-G1	2.119%
✓	DC1-S1	8.708%
✓	DC1-S2	8.142%
✓	DC1-S3	9.669%
✓	DC2-ADM1	2.515%
✓	DC2-ARC1	1.152%
✓	DC2-S1	8.204%
✓	DC2-S2	5.000%
✓	DC2-S3	10.469%

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 Metrics** auf die vorgebauten Grafana Dashboards zugreifen.



4. **Optional:** Um ein Diagramm des Prometheus-Ausdrucks über die Zeit zu sehen, klicken Sie auf **Anzeigen in Prometheus**.

Es wird ein Prometheus-Diagramm des in der Diagnose verwendeten Ausdrucks angezeigt.

Enable query history

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

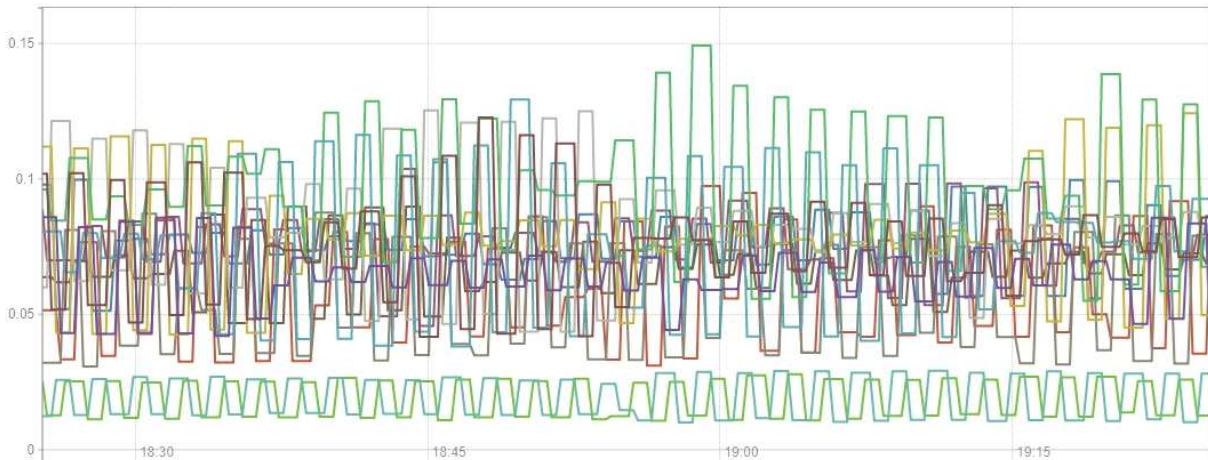
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor -

Graph Console

1h + << Until >> Res. (s) stacked



- {instance="DC3-S3"}
- {instance="DC3-S2"}
- {instance="DC3-S1"}
- {instance="DC2-S3"}
- {instance="DC2-S2"}
- {instance="DC2-S1"}
- {instance="DC2-ADM1"}
- {instance="DC1-S3"}
- {instance="DC1-S2"}
- {instance="DC1-S1"}
- {instance="DC1-G1"}
- {instance="DC1-ARC1"}
- {instance="DC1-ADM1"}

Remove Graph

Add Graph

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. Siehe [Anweisungen für die Administration von StorageGRID](#).

Informationen zu den Kennzahlen-API-Vorgängen, einschließlich der vollständigen Liste der verfügbaren Metriken, finden Sie im Grid Manager. Wählen Sie oben auf der Seite das Hilfesymbol aus und wählen Sie **API Dokumentation Metriken** aus.



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

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

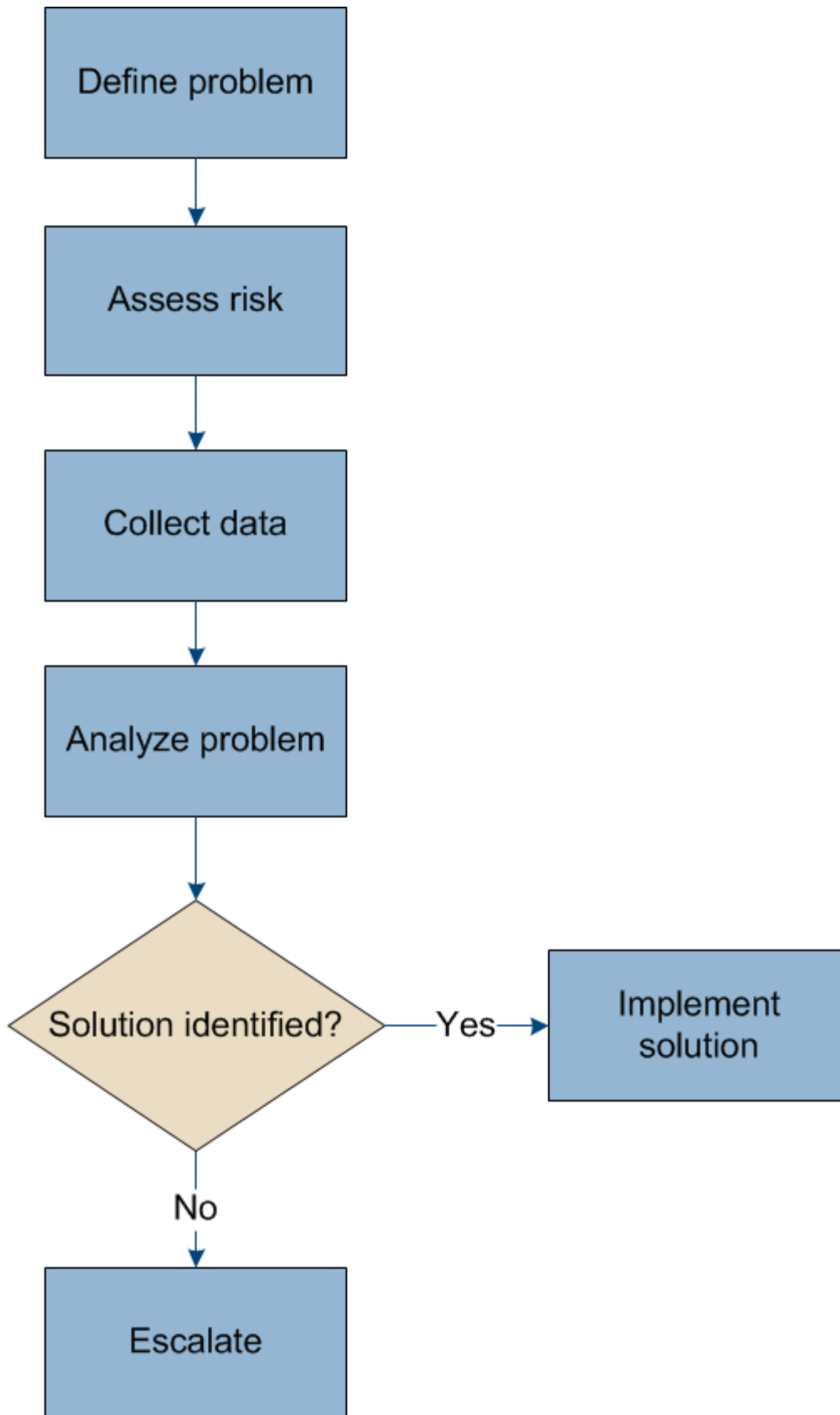
Fehler in einem StorageGRID System beheben

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 Ihnen ein Problem auftritt [Verwalten eines StorageGRID-Systems](#), Sie können den in dieser Abbildung beschriebenen Prozess verwenden, um das Problem zu identifizieren und zu analysieren. In vielen Fällen können Sie Probleme selbstständig lösen. In diesem Fall müssen Sie jedoch einige Probleme an den technischen Support eskalieren.



Definieren Sie das Problem

Der erste Schritt zur Lösung eines Problems besteht darin, das Problem klar zu definieren.

Diese Tabelle enthält Beispiele für die Arten von Informationen, die Sie erfassen können, um ein Problem zu definieren:

Frage	Beispielantwort
Was macht das StorageGRID-System? Was sind die Symptome?	Client-Applikationen 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.

Bewerten Sie das Risiko und die Auswirkungen auf das System

Bewerten Sie nach Definition des Problems sein Risiko und die Auswirkungen auf das StorageGRID System. Beispielsweise bedeutet das Vorhandensein kritischer Warnmeldungen nicht zwangsläufig, dass das System keine Kernservices liefert.

In dieser Tabelle sind die Auswirkungen eines Beispielproblems auf Systemvorgänge zusammengefasst:

Frage	Beispielantwort
Kann das StorageGRID System Inhalte aufnehmen?	Nein
Können Client-Anwendungen Inhalte abrufen?	Einige Objekte können abgerufen werden, andere 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.

Datenerfassung

Nach der 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 diesen Dat sammeln	Anweisungen
Zeitplan der neuesten Änderungen erstellen	Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.	<ul style="list-style-type: none">• Erstellen Sie eine Zeitleiste der neuesten Änderungen
Prüfen von Warnungen und Alarmen	<p>Mithilfe von Warnfunktionen und Alarmen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme geben.</p> <p>Überprüfen Sie die Liste der aktuellen Warnungen und Alarme, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat.</p> <p>Prüfen Sie die in der Vergangenheit ausgelösten Warnmeldungen und Alarme, um zusätzliche Einblicke zu erhalten.</p>	<ul style="list-style-type: none">• Anzeigen aktueller Warnmeldungen• Anzeigen von älteren Alarmen• Anzeigen von behobenen Warnmeldungen• Prüfen historischer Alarme und Alarmfrequenz (altes System)
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.	<ul style="list-style-type: none">• Monitoring von Ereignissen
Identifizieren von Trends mithilfe von Diagrammen und Textberichten	Trends liefern wertvolle Hinweise darauf, wann Probleme zuerst auftraten, und können Ihnen helfen zu verstehen, wie schnell sich die Dinge ändern.	<ul style="list-style-type: none">• Verwenden Sie Diagramme und Diagramme• Verwenden Sie Textberichte
Basispläne erstellen	Sammeln von Informationen über die normalen Stufen verschiedener Betriebswerte. Diese Basiswerte und Abweichungen von diesen Grundlinien können wertvolle Hinweise liefern.	<ul style="list-style-type: none">• Basispläne erstellen
Durchführen von Einspeisung und Abruf von Tests	Zur Fehlerbehebung von Performance-Problemen bei Aufnahme und Abruf können Objekte auf einer Workstation gespeichert und abgerufen werden. Vergleichen Sie die Ergebnisse mit denen, die bei der Verwendung der Client-Anwendung angezeigt werden.	<ul style="list-style-type: none">• PUT- und GET-Performance werden überwacht

Art der zu erfassenden Daten	Warum diesen Dat 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.	<ul style="list-style-type: none"> • Audit-Meldungen prüfen
Überprüfen Sie Objektstandorte und Storage-Integrität	Wenn Sie Speicherprobleme haben, stellen Sie sicher, dass Objekte an der gewünschten Stelle platziert werden. Überprüfen Sie die Integrität von Objektdaten auf einem Storage-Node.	<ul style="list-style-type: none"> • Überwachen von Objektverifizierungsvorgängen • Bestätigen Sie den Speicherort der Objektdaten • Überprüfen Sie die Objektintegrität
Datenerfassung für technischen Support	Vom technischen Support werden Sie möglicherweise aufgefordert, Daten zu sammeln oder bestimmte Informationen zu überprüfen, um Probleme zu beheben.	<ul style="list-style-type: none"> • Erfassen von Protokolldateien und Systemdaten • Senden Sie manuell eine AutoSupport Meldung aus • Prüfen von Support-Kennzahlen

Erstellen Sie eine Zeitleiste der neuesten Änderungen

Wenn ein Problem auftritt, sollten Sie berücksichtigen, was sich kürzlich geändert hat und wann diese Änderungen aufgetreten sind.

- Änderungen an Ihrem StorageGRID System, seiner Konfiguration oder seiner Umgebung können zu neuem Verhalten führen.
- Durch eine Zeitleiste von Änderungen können Sie feststellen, welche Änderungen für ein Problem verantwortlich sein könnten und wie jede Änderung ihre Entwicklung beeinflusst haben könnte.

Erstellen Sie eine Tabelle mit den letzten Änderungen an Ihrem System, die Informationen darüber enthält, wann jede Änderung stattgefunden hat und welche relevanten Details über die Änderung angezeigt werden, und Informationen darüber, was während der Änderung noch passiert ist:

Zeit der Änderung	Art der Änderung	Details
<p>Beispiel:</p> <ul style="list-style-type: none"> • Wann haben Sie die Node-Wiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Prozess unterbrochen? 	<p>Was ist los? Was haben Sie gemacht?</p>	<p>Dokumentieren Sie alle relevanten Details zu der Änderung. Beispiel:</p> <ul style="list-style-type: none"> • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Änderungen bei Client-Workloads <p>Achten Sie darauf, zu beachten, ob mehrere Änderungen gleichzeitig durchgeführt wurden. Wurde diese Änderung beispielsweise vorgenommen, während ein Upgrade durchgeführt wurde?</p>

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?

]**Basispläne erstellen**

Sie können Basislinien für Ihr System einrichten, indem Sie die normalen Ebenen verschiedener Betriebswerte erfassen. In Zukunft können Sie aktuelle Werte mit diesen Basiswerten vergleichen, um ungewöhnliche Werte zu erkennen und zu beheben.

Eigenschaft	Wert	Wie zu erhalten
Durchschnittlicher Storage-Verbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	<p>Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher.</p> <p>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</p> <p>Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.</p>
Durchschnittlicher Metadatenverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	<p>Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher.</p> <p>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</p> <p>Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.</p>

Eigenschaft	Wert	Wie zu erhalten
Geschwindigkeit von S3/Swift Operationen	Vorgänge/Sekunde	<p>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.</p> <p>Wählen Sie NODES site oder Storage Node Objects aus, um die Einspeisungs- und Abrufraten und Zählungen für einen bestimmten Standort oder Knoten anzuzeigen. Halten Sie den Mauszeiger über das Diagramm Aufnahme und Abruf für S3 oder Swift.</p>
S3/Swift-Vorgänge sind fehlgeschlagen	Betrieb	<p>Wählen Sie SUPPORT Tools Grid-Topologie aus. Zeigen Sie auf der Registerkarte Übersicht im Abschnitt API-Vorgänge den Wert für S3-Operationen an – Fehlgeschlagen oder Swift-Vorgänge – Fehlgeschlagen.</p>
ILM-Auswertungsrage	Objekte/Sekunde	<p>Wählen Sie auf der Seite Knoten GRID ILM aus.</p> <p>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.</p>
ILM-Scan-Rate	Objekte/Sekunde	<p>Wählen Sie NODES Grid ILM aus.</p> <p>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.</p>

Eigenschaft	Wert	Wie zu erhalten
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 NODES Storage Node Objekte aus. Zeigen Sie in der Tabelle Abfragen den Wert für durchschnittliche Latenz an.

Analysieren von Daten


Verwenden Sie die gesammelten Informationen, um die Ursache des Problems und der potenziellen Lösungen zu ermitteln.

Die Analyse ist Problem-abhängig, aber im Allgemeinen:

- 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? Definieren Sie das Problem

✓	Element	Hinweise
	Folgenabschätzung	<p>Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation?</p> <ul style="list-style-type: none"> • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	<p>Wählen Sie WARTUNG System Lizenz. Die StorageGRID System-ID wird im Rahmen der aktuellen Lizenz angezeigt.</p>
	Softwareversion	<p>Wählen Sie oben im Grid Manager das Hilfesymbol aus, und wählen Sie über, um die StorageGRID-Version anzuzeigen.</p>
	Anpassbarkeit	<p>Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf:</p> <ul style="list-style-type: none"> • 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	<p>Erfassen von Protokolldateien und Systemdaten für Ihr System Wählen Sie SUPPORT Tools Logs.</p> <p>Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln.</p> <p>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.)</p> <p>Erfassen von Protokolldateien und Systemdaten</p>
	Basisinformationen	<p>Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch</p> <p>Basispläne erstellen</p>

✓	Element	Hinweise
	Zeitachse der letzten Änderungen	Erstellen Sie eine Zeitleiste, in der alle letzten Änderungen am System oder seiner Umgebung zusammengefasst sind. Erstellen Sie eine Zeitleiste der neuesten Änderungen
	Verlauf der Bemühungen zur Diagnose des Problems	Wenn Sie Schritte zur Diagnose oder Behebung des Problems selbst ergriffen haben, achten Sie darauf, die Schritte und das Ergebnis zu notieren.

Behebung von Objekt- und Storage-Problemen

Bestätigen Sie den Speicherort der Objektdaten

Je nach 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. Wenn Sie eine bestimmte Version des Objekts suchen möchten, geben Sie die Version-ID ein (optional).

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

Version ID (optional)

4. Wählen Sie **Look Up**.

Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

- Systemmetadaten, einschließlich Objekt-ID (UUID), Version-ID (optional), Objektname, Name des Containers, Mandantenkontoname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "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. 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  
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point  	Device  	Status  	Size  	Available  	Write cache status  
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID  	Size  	Available  	Replicated data  	EC data  	Object data (%)  	Health  
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Führen Sie die folgenden Schritte aus, um weitere Details zu jedem Storage-Node anzuzeigen:

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **site Speicherknoten LDR Storage Übersicht Haupt**.



Overview: LDR (DC1-S1) - Storage

Updated: 2020-01-29 15:03:39 PST

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors

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 Speicher-knoten so bald wie möglich wieder voll zu machen. Wenn nötig, können Sie auf die Registerkarte **Konfiguration** gehen und den Speicher-knoten 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

[Recovery und Wartung](#)

Überprüfen Sie die Objektintegrität

Das StorageGRID System überprüft die Integrität der Objektdaten auf Storage-Nodes und überprüft sowohl beschädigte als auch fehlende Objekte.

Es gibt zwei Verifizierungsverfahren: Hintergrundüberprüfung und Objektexistenz-Prüfung (früher als Vordergrundüberprüfung bezeichnet). Sie arbeiten zusammen, um die Datenintegrität sicherzustellen. Die Hintergrundüberprüfung wird automatisch ausgeführt und überprüft kontinuierlich die Korrektheit von Objektdaten. Die Überprüfung der ObjektExistenz kann von einem Benutzer ausgelöst werden, um die Existenz (obwohl nicht die Richtigkeit) von Objekten schneller zu überprüfen.

Was ist Hintergrundüberprüfung?

Die Hintergrundüberprüfung überprüft Storage Nodes automatisch und kontinuierlich auf beschädigte Kopien von Objektdaten und versucht automatisch, alle gefundenen Probleme zu beheben.

Bei der Hintergrundüberprüfung werden die Integrität replizierter Objekte und Objekte mit Erasure-Coding-Verfahren überprüft:

- **Replizierte Objekte:** Findet der Hintergrundverifizierungsvorgang ein beschädigtes Objekt, wird die beschädigte Kopie vom Speicherort entfernt und an anderer Stelle auf dem Speicherknoten isoliert. Anschließend wird eine neue, nicht beschädigte Kopie 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 versucht, eine andere 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 Alarmer (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, weil es keine andere Kopie finden kann, wird die Warnung **Objekte verloren** ausgelöst.

Ändern Sie die 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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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-Topologie** 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 **Prüfrate adaptiv** aus.

The screenshot shows a web interface for configuring LDR verification. At the top, there are tabs for 'Overview', 'Alarms', 'Reports', and 'Configuration'. Below the tabs is a 'Main' header. The main content area is titled 'Configuration: LDR (Storage-Node) - Verification' with a sub-header 'Updated: 2021-11-11 07:13:00 MST'. There are three sections: 'Reset Missing Objects Count' with a checkbox, 'Background Verification' with a dropdown menu for 'Verification Rate' set to 'Adaptive', and 'Reset Corrupt Objects Count' with a checkbox. Below that is 'Quarantined Objects' with a checkbox for 'Delete Quarantined Objects'. An 'Apply Changes' button with a right-pointing arrow is at the bottom right.



Wenn Sie die Verifizierungsrate auf hoch setzen, wird der alte Alarm VPRI (Verification Rate) auf der Melderebene ausgelöst.

6. Klicken Sie Auf **Änderungen Übernehmen**.
7. 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.
8. 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-Topologie** 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).
9. Nachdem das StorageGRID System beschädigte Objekte automatisch wiederhergestellt hat, setzen Sie die Anzahl beschädigter Objekte zurück.
- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Speicherknoten LDR Verifizierung Konfiguration**.
 - c. Wählen Sie **Anzahl Der Beschädigten Objekte Zurücksetzen**.
 - d. Klicken Sie Auf **Änderungen Übernehmen**.
10. 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.

- a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- b. Wählen Sie **Speicherknoten LDR Verifizierung Konfiguration**.
- c. Wählen Sie **Gesperrte Objekte Löschen**.
- d. Wählen Sie **Änderungen Anwenden**.

Was ist Objektexistenz-Prüfung?

Die ObjektExistenz überprüft, ob alle erwarteten replizierten Kopien von Objekten und mit Erasure Coding verschlüsselten Fragmenten auf einem Storage Node vorhanden sind. Die Objektüberprüfung überprüft nicht die Objektdaten selbst (Hintergrundüberprüfung führt das durch); stattdessen bietet sie eine Möglichkeit, die Integrität von Speichergeräten zu überprüfen, insbesondere wenn ein kürzlich auftretende Hardwareproblem die Datenintegrität beeinträchtigen könnte.

Im Gegensatz zur automatischen Hintergrundüberprüfung müssen Sie einen Auftrag zur Überprüfung der Objektexistenz manuell starten.

Die Objektexistenz prüft die Metadaten für jedes in StorageGRID gespeicherte Objekt und überprüft, ob es sich um replizierte Objektkopien sowie um Erasure Coding verschlüsselte Objektfragmente handelt. Fehlende Daten werden wie folgt behandelt:

- **Replizierte Kopien:** Fehlt eine Kopie replizierter Objektdaten, versucht StorageGRID automatisch, die Kopie von einer an anderer Stelle im System gespeicherten Kopie zu ersetzen. Der Storage-Node führt eine vorhandene Kopie durch eine ILM-Evaluierung aus. Damit wird festgestellt, dass die aktuelle ILM-Richtlinie für dieses Objekt nicht mehr erfüllt wird, da eine weitere Kopie fehlt. Eine neue Kopie wird erstellt und platziert, um die aktive ILM-Richtlinie des Systems zu erfüllen. Diese neue Kopie kann nicht an derselben Stelle platziert werden, an der die fehlende Kopie gespeichert wurde.
- **Erasure-codierte Fragmente:** Fehlt ein Fragment eines Objekts mit Löschungscode, versucht StorageGRID automatisch, das fehlende Fragment auf demselben Speicherknoten mithilfe der verbleibenden Fragmente neu zu erstellen. Wenn das fehlende Fragment nicht wiederhergestellt werden kann (weil zu viele Fragmente verloren gegangen sind), versucht ILM, eine andere Kopie des Objekts zu finden, mit der es ein neues Fragment mit Löschungscode generieren kann.

Überprüfung der ObjektExistenz ausführen

Sie erstellen und führen jeweils einen Job für die Überprüfung der Objektexistenz aus. Wenn Sie einen Job erstellen, wählen Sie die Speicherknoten und -Volumes aus, die Sie überprüfen möchten. Sie wählen auch das Consistency Control für den Job aus.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben sichergestellt, dass die zu prüfenden Speicherknoten online sind. Wählen Sie **NODES**, um die Tabelle der Knoten anzuzeigen. Stellen Sie sicher, dass neben dem Knotennamen für die Knoten, die Sie überprüfen möchten, keine Warnsymbole angezeigt werden.
- Sie haben sichergestellt, dass die folgenden Verfahren auf den Knoten, die Sie überprüfen möchten, **nicht** ausgeführt werden:
 - Grid-Erweiterung, um einen Storage-Node hinzuzufügen
 - Deaktivierung des Storage Node
 - Recovery eines ausgefallenen Storage-Volumes
 - Wiederherstellung eines Speicherknoten mit einem ausgefallenen Systemlaufwerk
 - EC-Ausgleich
 - Appliance-Node-Klon

Die Objektprüfung bietet keine nützlichen Informationen, während diese Verfahren ausgeführt werden.

Über diese Aufgabe

Die Fertigstellung eines Objektes kann je nach Anzahl der Objekte im Raster, der ausgewählten Storage-Nodes und Volumes und der ausgewählten Konsistenzgruppe Tage oder Wochen dauern. Sie können nur einen Job gleichzeitig ausführen, aber Sie können mehrere Speicherknoten und Volumes gleichzeitig auswählen.

Schritte

1. Wählen Sie **WARTUNG Aufgaben Objektexistenz prüfen**.
2. Wählen Sie **Job erstellen**. Der Assistent Job-Prüfung für Objektexistenz erstellen wird angezeigt.
3. Wählen Sie die Nodes aus, die die Volumes enthalten, die Sie überprüfen möchten. Um alle Online-Knoten auszuwählen, aktivieren Sie in der Spaltenüberschrift das Kontrollkästchen **Node Name**.

Sie können nach Node-Namen oder Site suchen.

Sie können keine Nodes auswählen, die nicht mit dem Raster verbunden sind.

4. Wählen Sie **Weiter**.
5. Wählen Sie für jeden Knoten in der Liste ein oder mehrere Volumes aus. Sie können mithilfe der Storage-Volume-Nummer oder des Node-Namens nach Volumes suchen.

Um alle Volumes für jeden ausgewählten Knoten auszuwählen, aktivieren Sie in der Spaltenüberschrift das Kontrollkästchen **Speichervolumen**.

6. Wählen Sie **Weiter**.
7. Wählen Sie das Consistency Control für den Job aus.

Die Konsistenzkontrolle bestimmt, wie viele Kopien von Objektmetadaten für die Objektüberprüfung verwendet werden.

- **Strong-site**: Zwei Kopien von Metadaten an einem einzigen Standort.
- **Stark-global**: Zwei Kopien von Metadaten an jedem Standort.
- **Alle** (Standard): Alle drei Kopien von Metadaten an jedem Standort.

Weitere Informationen zur Consistency Control finden Sie in den Beschreibungen im Assistenten.

8. Wählen Sie **Weiter**.
9. Ihre Auswahl überprüfen und überprüfen. Sie können **Zurück** auswählen, um zu einem vorherigen Schritt im Assistenten zu wechseln, um Ihre Auswahl zu aktualisieren.

Ein Job zur Überprüfung der Objektexistenz wird erstellt und wird ausgeführt, bis einer der folgenden Aktionen ausgeführt wird:

- Der Job ist abgeschlossen.
- Sie unterbrechen oder abbrechen den Job. Sie können einen Job, den Sie angehalten haben, fortsetzen, aber einen Job, den Sie abgebrochen haben, nicht mehr fortsetzen.
- Der Job wird abgestellt. Die Warnung * Objektexistenz ist blockiert* wird ausgelöst. Befolgen Sie die für die Meldung angegebenen Korrekturmaßnahmen.
- Der Job schlägt fehl. Die Warnung * Objektexistenz ist fehlgeschlagen* wird ausgelöst. Befolgen Sie die für die Meldung angegebenen Korrekturmaßnahmen.
- Es wird eine Meldung „SService nicht verfügbar“ oder „interner Serverfehler“ angezeigt. Aktualisieren Sie nach einer Minute die Seite, um mit der Überwachung des Jobs fortzufahren.



Sie können bei Bedarf von der Seite „Objektexistenz“ wegnavigieren und mit der Überwachung des Jobs fortfahren.

10. Zeigen Sie während der Ausführung des Jobs die Registerkarte **aktiver Job** an, und notieren Sie den Wert

fehlender Objektkopien.

Dieser Wert stellt die Gesamtzahl der fehlenden Kopien replizierter Objekte und Objekte mit Erasure-Coding-Code mit einem oder mehreren fehlenden Fragmenten dar.

Wenn die Anzahl der erkannten fehlenden Objektkopien größer als 100 ist, kann es zu einem Problem mit dem Speicher des Speicherknosens kommen.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job Job history

Status: Accepted Consistency control: All
Job ID: 2334602652907829302 Start time: 2021-11-10 14:43:02 MST
Missing object copies detected: 0 Elapsed time: --
Progress: 0% Estimated time to completion: --

Pause Cancel

Volumes Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Nehmen Sie nach Abschluss des Jobs alle weiteren erforderlichen Maßnahmen vor:

- Wenn fehlende Objektkopien gefunden wurden, ist Null, dann wurden keine Probleme gefunden. Es ist keine Aktion erforderlich.
- Wenn fehlende Objektkopien erkannt sind größer als Null und die Warnung **Objekte verloren** nicht ausgelöst wurde, wurden alle fehlenden Kopien vom System repariert. Überprüfen Sie, ob Hardwareprobleme behoben wurden, um zukünftige Schäden an Objektkopien zu vermeiden.
- Wenn fehlende Objektkopien erkannt sind größer als Null und die Warnung **Objekte verloren** ausgelöst wurde, könnte die Datenintegrität beeinträchtigt werden. Wenden Sie sich an den technischen Support.
- Sie können verlorene Objektkopien untersuchen, indem Sie die LLST-Audit-Meldungen mit grep extrahieren: `grep LLST audit_file_name`.

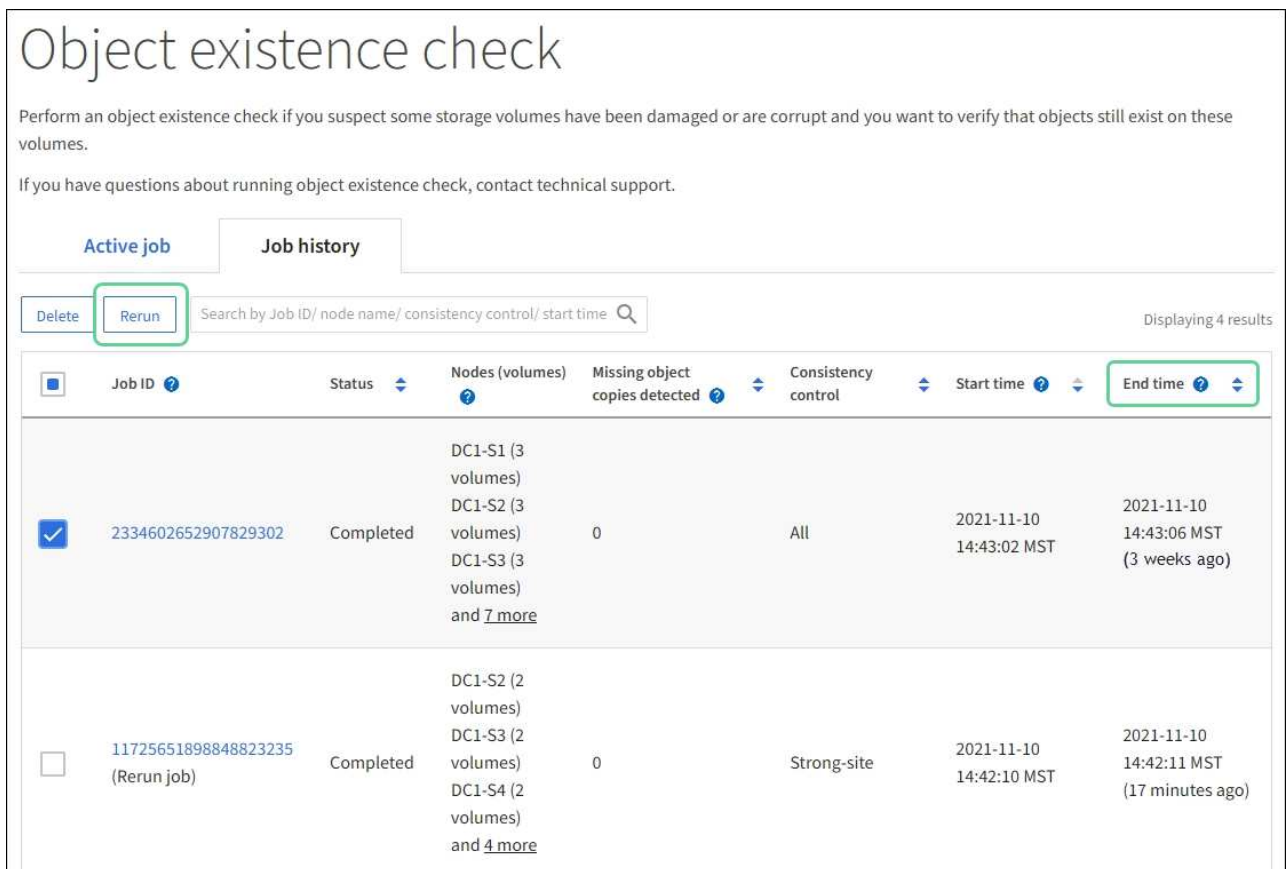
Dieses Verfahren ähnelt dem Verfahren für [Untersuchung verlorener Objekte](#), Obwohl für Objektkopien Sie suchen LLST Statt OLST.

12. Wenn Sie für den Job die Kontrolle der Konsistenz vor Ort oder stark-global ausgewählt haben, warten Sie

ungefähr drei Wochen auf die Metadatenkonsistenz, und führen Sie den Job erneut auf denselben Volumes aus.

Wenn StorageGRID Zeit hatte, konsistente Metadaten für die im Job enthaltenen Nodes und Volumes zu erzielen, konnte eine erneute Ausführung des Jobs fälschlicherweise gemeldete fehlende Objektkopien löschen oder zusätzliche Objektkopien veranlassen, dass sie nicht verwendet wurden.

- a. Wählen Sie **WARTUNG Objekt Existenzprüfung Jobverlauf**.
- b. Legen Sie fest, welche Jobs für die erneute Ausführung bereit sind:
 - i. Sehen Sie sich die Spalte **Endzeit** an, um festzustellen, welche Jobs vor mehr als drei Wochen ausgeführt wurden.
 - ii. Überprüfen Sie für diese Jobs die Spalte Consistency Control auf Strong-site oder strong-global.
- c. Aktivieren Sie das Kontrollkästchen für jeden Job, den Sie erneut ausführen möchten, und wählen Sie dann **Rerun**.



<input type="checkbox"/>	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Überprüfen Sie im Assistenten für Rerun-Jobs die ausgewählten Knoten und Volumes und die Konsistenzsteuerung.
- e. Wenn Sie bereit sind, die Jobs erneut auszuführen, wählen Sie **Rerun**.

Die Registerkarte „aktiver Job“ wird angezeigt. Alle ausgewählten Jobs werden als ein Job bei einer Consistency Control von strong-site erneut ausgeführt. In einem Feld mit * Related Jobs* im Bereich Details werden die Job-IDs für die ursprünglichen Jobs angezeigt.

Nachdem Sie fertig sind

Wenn Sie noch Bedenken bezüglich der Datenintegrität haben, gehen Sie zu **SUPPORT Tools Grid-Topologie Site Storage-Node 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.

Fehlerbehebung bei verlorenen und fehlenden Objektdaten

Objekte können aus verschiedenen Gründen abgerufen werden, darunter Leseanforderungen von einer Client-Applikation, Hintergrundverifizierungen replizierter Objektdaten, ILM-Neubewertungen und die Wiederherstellung von Objektdaten während der Recovery eines Storage Node.

Das StorageGRID System verwendet 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 wird wie folgt die Warnung **Objekte verloren** ausgelöst:

- Wenn bei replizierten Kopien keine weitere Kopie abgerufen werden kann, gilt das Objekt als verloren und die Meldung wird 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. Falls keine weitere Kopie gefunden wird, wird die Meldung 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 Objects“ zurücksetzen, um zu verhindern, dass bekannte verlorene Objekte neue verlorene Objekte maskieren.

Verwandte Informationen

[Untersuchen Sie verlorene Objekte](#)

[Verlorene und fehlende Objektanzahl zurücksetzen](#)

Untersuchen Sie verlorene Objekte

Wenn der Alarm **Objekte verloren** ausgelöst wird, müssen Sie sofort untersuchen. Sammeln Sie Informationen zu den betroffenen Objekten und wenden Sie sich an den technischen Support.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

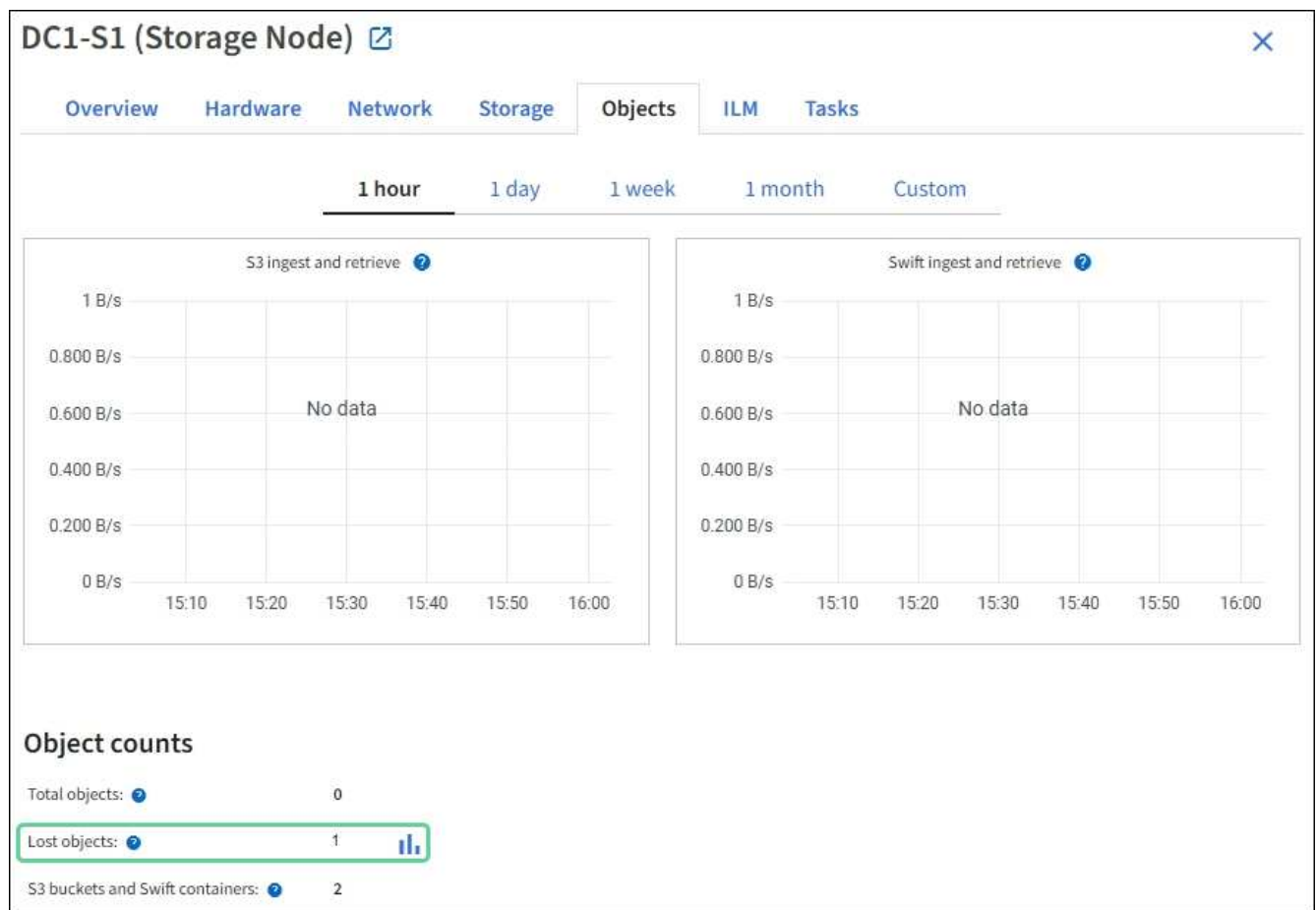
Die Warnung **Objects lost** zeigt an, dass StorageGRID glaubt, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

Untersuchen Sie verlorene Objektwarnungen sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. In einigen Fällen können Sie ein verlorenes Objekt wiederherstellen, wenn Sie eine sofortige Aktion ausführen.

Schritte

1. Wählen Sie **KNOTEN**.
2. Wählen Sie **Speicherknoten Objekte** Aus.
3. Überprüfen Sie die Anzahl der verlorenen Objekte, die in der Tabelle Objektanzahl angezeigt werden.

Diese Nummer gibt die Gesamtzahl der Objekte an, die dieser Grid-Node im gesamten StorageGRID-System als fehlend erkennt. Der Wert ist die Summe der Zähler Lost Objects der Data Store Komponente innerhalb der LDR- und DDS-Dienste.



4. Greifen Sie von einem Admin-Node aus auf das Audit-Protokoll zu, um die eindeutige Kennung (UUID) des Objekts zu bestimmen, das die Warnung **Objekte verloren** 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 aufgeführten Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführten 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][AMID(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“:“)	<p>Wenn das Objekt nicht gefunden wird, wird die Meldung „FEHLER“:“ zurückgegeben.</p> <p>Wenn das Objekt nicht gefunden wird, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen. Das Fehlen eines Objekts bedeutet, dass das Objekt absichtlich gelöscht wurde.</p>
Standorte 0	<p>Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung Objects Lost falsch positiv sein.</p> <p>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.</p> <p>(Verfahren für Suche nach möglicherweise verlorenen Objekten Erläutert, wie Sie die Knoten-ID verwenden, um den richtigen Speicherknoten zu finden.)</p> <p>Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen.</p>
Standorte = 0	<p>Wenn in der Ausgabe keine Positionen aufgeführt sind, fehlt das Objekt möglicherweise. Versuchen Sie es Suchen Sie das Objekt und stellen Sie es wieder her Selbst oder Sie können sich an den technischen Support wenden.</p> <p>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 „<i>Repair-Data</i>“ ausgegeben, und läuft die Recovery noch? Weitere Informationen finden Sie unter Wiederherstellung von Objektdateien auf einem Storage-Volumen.</p>

Verwandte Informationen

[Prüfung von Audit-Protokollen](#)

Suche nach potenziell verlorenen Objekten und Wiederherstellung

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 „potenziell 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 **SUPPORT Tools Grid-Topologie** aus. Wählen Sie anschließend **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 `#`.

1. 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 Objektdateipfad nicht gefunden wurde, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektdateipfad 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.
 - a. Wenn der Objektdateipfad gefunden wurde, versuchen Sie, das Objekt in StorageGRID wiederherzustellen:
 - i. 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'`

- ii. Telnet für localhost 1402 für den Zugriff auf die LDR-Konsole. Geben Sie Ein: `telnet 0 1402`
- iii. Geben Sie Ein: `cd /proc/STOR`
- iv. 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](#)

- v. Wenn das Objekt erfolgreich in StorageGRID wiederhergestellt wurde, überprüfen Sie, ob 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"
  }
]
}
```

1. Melden Sie sich von der LDR-Konsole ab. Geben Sie Ein: `exit`
 - a. 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.
2. Melden Sie sich beim Grid-Node an:
 - 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 `#`.
3. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`
4. 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
```

5. 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]]
```

6. 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. . Setzen Sie die Anzahl der verlorenen Objekte im Grid Manager zurück.

Verwandte Informationen

[Untersuchen Sie verlorene Objekte](#)

[Verlorene und fehlende Objektanzahl zurücksetzen](#)

[Prüfung von Audit-Protokollen](#)

Verlorene und fehlende Objektanzahl zurücksetzen

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 mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **UNTERSTÜTZUNG Tools Grid-Topologie Site Storage-Node LDR Data Store Übersicht Haupt**
- **UNTERSTÜTZUNG Tools Grid-Topologie 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-Topologie** 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**.

Overview | Alarms | Reports | **Configuration**

Main | Alarms

 **Configuration: LDR (99-94) - Data Store**
 Updated: 2017-05-11 14:56:13 PDT

Reset Lost Objects Count

Apply Changes 

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.

Beheben Sie die Warnung „Niedrig Object Data Storage“

Der Alarm * Low Object Data Storage* überwacht, wie viel Speicherplatz zum Speichern von Objektdaten auf jedem Storage Node verfügbar ist.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die Warnung * Low Object Data Storage* wird ausgelöst, wenn die Gesamtzahl der replizierten und Erasure codierten Objektdaten auf einem Storage Node einer der Bedingungen entspricht, 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 **ALERTS Current**.

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

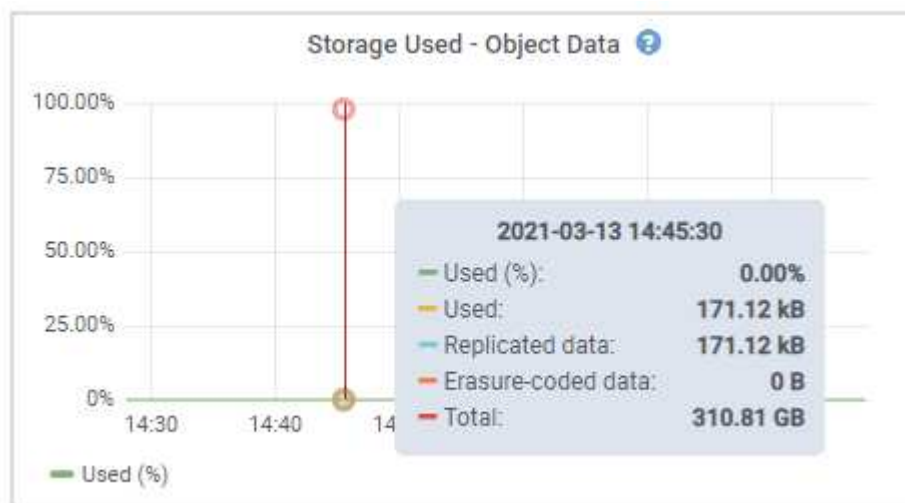
4. Wählen Sie **NODES Storage Node oder Standort Storage** aus.

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

[Fehlersuche im SSTS-Alarm \(Storage Status\) durchführen](#)

[Erweitern Sie Ihr Raster](#)

[StorageGRID verwalten](#)

Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, müssen Sie möglicherweise die Warnung **Low read-only Watermark override** auflösen. Wenn möglich, sollten Sie Ihr System aktualisieren, um mit den optimierten Werten zu beginnen.

In vorherigen Versionen, die drei [Wasserzeichen für Storage-Volumes](#) wurden globale Einstellungen #8212 durchgeführt. Dieselben Werte werden auf jedes Storage-Volume auf jedem Storage Node angewendet. Ab StorageGRID 11.6 kann die Software diese Wasserzeichen für jedes Storage Volume optimieren, basierend auf der Größe des Storage-Nodes und der relativen Kapazität des Volumes.

Wenn Sie ein Upgrade auf StorageGRID 11.6 durchführen, werden optimierte Read- und Write-Wasserzeichen automatisch auf alle Storage Volumes angewendet, sofern keine der folgenden Optionen zutrifft:

- Ihr System ist in der Nähe der Kapazität und kann keine neuen Daten akzeptieren, wenn optimierte Wasserzeichen angewendet wurden. StorageGRID ändert in diesem Fall keine Wasserzeichen-Einstellungen.
- Sie haben zuvor eine der Storage-Volume-Wasserzeichen auf einen benutzerdefinierten Wert gesetzt. StorageGRID überschreibt keine benutzerdefinierten Wasserzeichen-Einstellungen mit optimierten Werten. Allerdings kann StorageGRID die Warnung **Low read-only Watermark override** auslösen, wenn Ihr benutzerdefinierter Wert für das Speichervolumen Soft Read-Only Watermark zu klein ist.

Analysieren Sie die Meldung

Wenn Sie benutzerdefinierte Werte für Speichervolumen-Wasserzeichen verwenden, wird möglicherweise für einen oder mehrere Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

Jede Instanz des Alarms weist darauf hin, dass der benutzerdefinierte Wert des **Storage Volume Soft Read-Only Watermark** kleiner als der für diesen Speicherknoten optimierte Mindestwert ist. Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Speicherknoten möglicherweise kritisch wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergehen kann. Einige Speicher-Volumes sind möglicherweise nicht mehr zugänglich (automatisch abgehängt), wenn der Node die Kapazität erreicht.

Angenommen, Sie haben zuvor den **Speichervolumen Soft Read-Only-Wasserzeichen** auf 5 GB gesetzt. Nehmen Sie nun an, dass StorageGRID die folgenden optimierten Werte für die vier Storage-Volumes in Storage Node A berechnet hat:

Lautstärke 0	12 GB
Band 1	12 GB
Lautstärke 2	11 GB
Lautstärke 3	15 GB

Die Warnung **Low read-only Watermark override** wird für Storage Node A ausgelöst, da Ihr benutzerdefinierter Wasserzeichen (5 GB) kleiner als der für alle Volumes in diesem Knoten optimierte Mindestwert ist (11 GB). Wenn Sie die benutzerdefinierte Einstellung weiterhin verwenden, wird der Node möglicherweise schwer mit wenig Speicherplatz ausgeführt, bevor er sicher in den schreibgeschützten Zustand übergeht.

Beheben Sie die Meldung

Befolgen Sie diese Schritte, wenn eine oder mehrere **Low Read-Only-Wasserzeichen überschreiben** -Warnungen ausgelöst wurden. Sie können diese Anweisungen auch verwenden, wenn Sie derzeit benutzerdefinierte Wasserzeichen-Einstellungen verwenden und optimierte Einstellungen auch dann verwenden möchten, wenn keine Warnungen ausgelöst wurden.

Was Sie benötigen

- Sie haben das Upgrade auf StorageGRID 11.6 abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Sie können die Warnung **Low read-only Watermark override** lösen, indem Sie benutzerdefinierte Wasserzeichen-Einstellungen auf die neuen Wasserzeichen-Überschreibungen aktualisieren. Wenn jedoch ein oder mehrere Speicherknoten nahe voll sind oder Sie spezielle ILM-Anforderungen haben, sollten Sie zunächst die optimierten Speicherabdrücke anzeigen und feststellen, ob sie sicher verwendet werden können.

Bewertung der Nutzung von Objektdaten für das gesamte Grid

1. Wählen Sie **KNOTEN**.
2. Erweitern Sie für jeden Standort im Raster die Liste der Nodes.
3. Überprüfen Sie die Prozentwerte, die in der Spalte **Objektdaten verwendet** für jeden Speicherknoten an jedem Standort angezeigt werden.
4. Wenn keiner der Speicherknoten fast voll ist (zum Beispiel sind alle **Objektdaten verwendet** Werte kleiner als 80%), können Sie die Überschreibeeinstellungen verwenden. Gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#).



Es gibt einige Ausnahmen von dieser allgemeinen Regel. Wenn ILM-Regeln beispielsweise ein strenges Aufnahmeverhalten verwenden oder bestimmte Storage-Pools nahezu vollständig sind, sollten Sie zuerst die Schritte in durchführen [Anzeigen optimierter Speicherabdrücke](#) Und [ob Sie optimierte Wasserzeichen verwenden können](#).

5. Wenn mehrere Speicherknoten nahezu voll sind, führen Sie die Schritte unter aus [Anzeigen optimierter Speicherabdrücke](#) Und [ob Sie optimierte Wasserzeichen verwenden können](#).

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

1. Wählen Sie **SUPPORT Tools Kennzahlen** aus.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

4. Um das empfohlene maximale Softread-only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

5. Beachten Sie den maximal optimierten Wert für jeden Speicherknoten.

Bestimmen Sie, ob Sie optimierte Wasserzeichen verwenden können

1. Wählen Sie **KNOTEN**.
2. Wiederholen Sie diese Schritte für jeden Online-Speicherknoten:
 - a. Wählen Sie **Storage-Node Storage** Aus.
 - b. Scrollen Sie nach unten zur Tabelle „Objektspeichern“.
 - c. Vergleichen Sie den **verfügbaren**-Wert für jeden Objektspeicher (Volumen) mit dem für diesen Speicherknoten angegebenen maximalen optimierten Wasserzeichen.
3. Wenn mindestens ein Volume auf jedem Online-Speicherknoten mehr Speicherplatz als das maximal optimierte Wasserzeichen für diesen Knoten hat, gehen Sie zu [Verwenden Sie optimierte Wasserzeichen](#) Um die optimierten Wasserzeichen zu verwenden.

Andernfalls [Erweitern Sie Ihr Raster](#) So bald wie möglich. Fügen Sie einem vorhandenen Node entweder Storage Volumes hinzu oder fügen Sie neue Storage-Nodes hinzu. Fahren Sie dann mit fort [Verwenden Sie optimierte Wasserzeichen](#) Zum Aktualisieren der Einstellungen für Wasserzeichen.

4. Wenn Sie mit der Verwendung benutzerdefinierter Werte für die Speichervolumen-Wasserzeichen fortfahren müssen, [Stille](#) Oder [Deaktivieren](#) Die Warnung * Low read-only Watermark override*.



Auf jedes Storage Volume auf jedem Storage Node werden dieselben benutzerdefinierten Werte angewendet. Die Verwendung kleinerer Werte als empfohlen für Speichervolumen-Wasserzeichen kann dazu führen, dass einige Speicher-Volumes nicht mehr zugänglich sind (automatisch abgehängt), wenn der Node die Kapazität erreicht.


Verwenden Sie optimierte Wasserzeichen

1. Gehen Sie zu **KONFIGURATION System Speicheroptionen**.
2. Wählen Sie im Menü Speicheroptionen die Option **Konfiguration** aus.
3. Ändern Sie alle drei Wasserzeichen-Überschreibungen auf 0.
4. Wählen Sie **Änderungen Anwenden**.

Für jedes Storage Volume gelten nun optimierte Wasserzeichen, basierend auf der Größe des Storage Nodes und der relativen Kapazität des Volumes.

Storage Options

- Overview
- Configuration



Storage Options Overview

Updated: 2021-11-22 13:57:51 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0 B
Storage Volume Soft Read-Only Watermark Override	0 B
Storage Volume Hard Read-Only Watermark Override	0 B
Metadata Reserved Space	3,000 GB

Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

Fehlersuche im SSTS-Alarm (Storage Status) durchführen

Der SSTS-Alarm (Storage Status) wird ausgelöst, wenn ein Speicherknoten über nicht genügend freien Speicherplatz für den Objektspeicher verfügt.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Der SSTS-Alarm (Speicherstatus) wird auf der Meldeebene ausgelöst, wenn die Menge an freiem Speicherplatz auf jedem Volume in einem Speicherknoten unter den Wert des Speichervolumen-SoftRead-Only-Wasserzeichens (**KONFIGURATION System Speicheroptionen**) 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

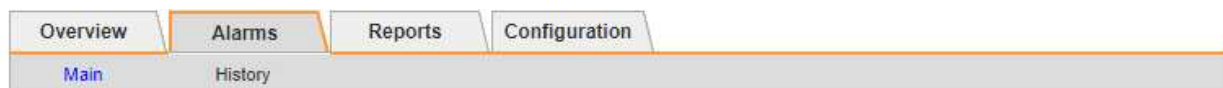
Angenommen, das Speichervolumen-Soft-Read-Only-Wasserzeichen ist auf 10 GB gesetzt, das ist der Standardwert. Der SSTS-Alarm wird ausgelöst, wenn auf jedem Speicher-Volumen im Storage-Node weniger als 10 GB nutzbarer Speicherplatz verbleibt. Wenn eines der Volumes über 10 GB oder mehr verfügbaren Speicherplatz 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.



Alarms: LDR (DC1-S3-101-195) - Storage

Updated: 2019-10-09 12:52:43 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
Normal	SHLH (Health)						<input type="checkbox"/>

Apply Changes

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.

- Um festzustellen, wie viel nutzbarer Speicherplatz tatsächlich verfügbar ist, wählen Sie **LDR Storage Übersicht**, und suchen Sie das Attribut Total Usable Space (STAS).

The screenshot shows the 'Overview: LDR (:DC1-S1-101-193) - Storage' page. The 'Storage State - Current' is 'Read-only' and 'Storage Status' is 'Insufficient Free Space'. Under 'Utilization', 'Total Usable Space' is 19.6 GB. Under 'Replication', 'Delete Service State' is 'Enabled'. The 'Object Store Volumes' table shows three volumes with 'Available' space values of 2.93 GB, 8.32 GB, and 8.36 GB.

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	54.7 GB	2.93 GB	46.2 GB	0 B	84.486 %	No Errors
0001	54.7 GB	8.32 GB	46.3 GB	0 B	84.644 %	No Errors
0002	54.7 GB	8.36 GB	46.3 GB	0 B	84.57 %	No Errors

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.

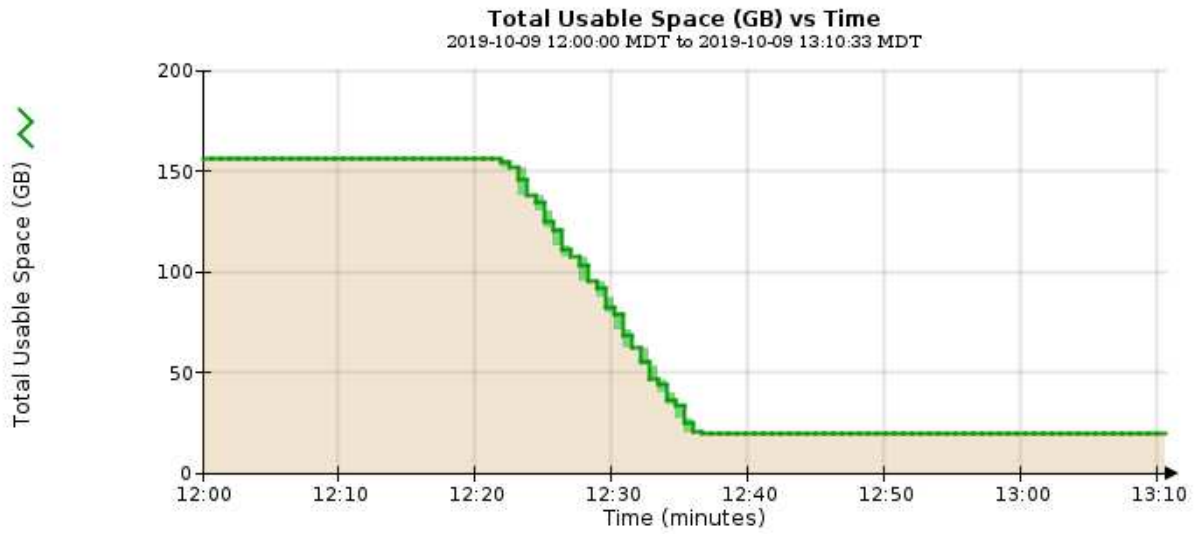
- Um zu verstehen, wie Speicher im Laufe der Zeit genutzt wurde, wählen Sie die Registerkarte **Berichte** und zeichnen den gesamten nutzbaren Speicherplatz in den letzten Stunden.

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.



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33
		<input type="button" value="Update"/>			




5. Um zu verstehen, wie Speicher als Prozentsatz der Gesamtmenge genutzt wird, geben Sie den gesamten nutzbaren Speicherplatz (Prozent) in den letzten Stunden an.

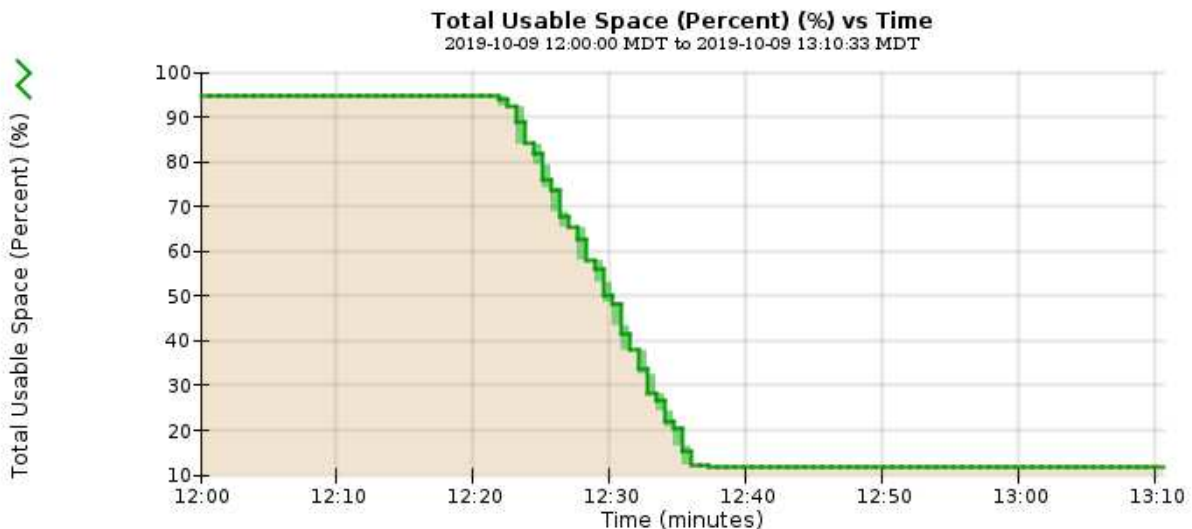
In diesem Beispiel sank der nutzbare Gesamtspeicherplatz von 95 % auf etwa 10 % zur selben Zeit.

Overview | Alarms | **Reports** | Configuration

Charts | Text

 Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute: Total Usable Space (Percent) Vertical Scaling: Start Date: 2019/10/09 12:00:00
 Quick Query: Custom Query Update Raw Data: End Date: 2019/10/09 13:10:33



6. Fügen Sie bei Bedarf die Storage-Kapazität um hinzu [Erweitern des StorageGRID Systems](#).

Informationen zu Verfahren zum Verwalten eines vollständigen Speicherknoten finden Sie im [Anweisungen für die Administration von StorageGRID](#).

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.

Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log` Protokolldatei. Siehe [Referenz für Protokolldateien](#).

Weitere Informationen zur Fehlerbehebung von Plattformdiensten finden Sie im [Anweisungen für die Administration von StorageGRID](#). Möglicherweise müssen Sie es [Greifen Sie über den Tenant Manager auf den Mandanten zu](#) So beheben Sie einen Plattformdienstfehler.

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. Wählen Sie **Anzahl der Ereignisse 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.

Behebung von Metadatenproblemen

Sie können mehrere Aufgaben durchführen, um die Ursache von Metadatenproblemen zu ermitteln.

Beheben Sie die Warnmeldung zu niedrigen Metadaten-Storage

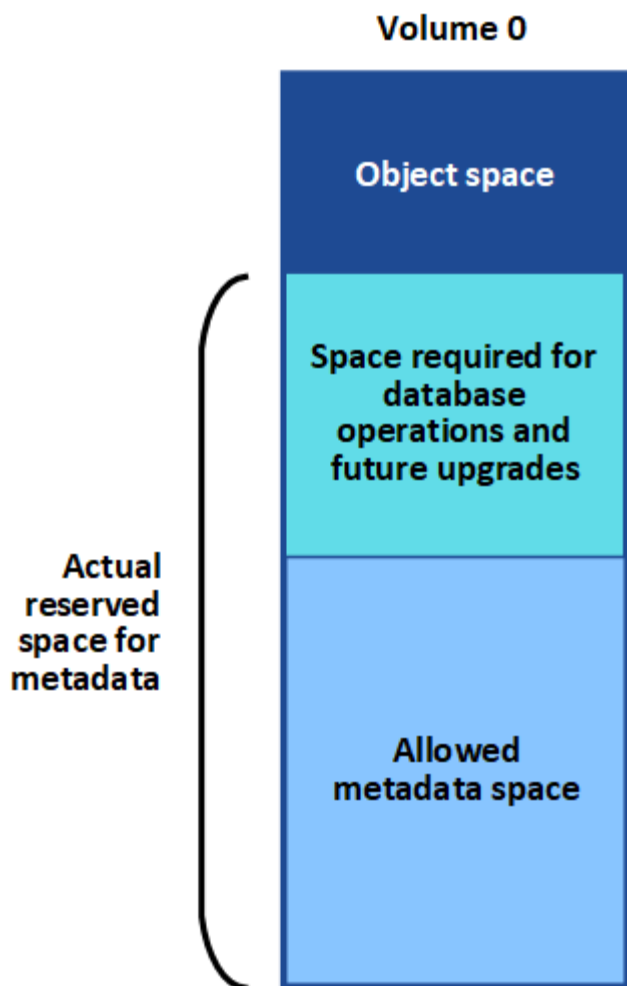
Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

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.

Das können Sie [Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node](#) Um Ihnen zu helfen, Fehler frühzeitig zu erkennen und zu beheben, bevor sie auftreten.

StorageGRID verwendet die folgende Prometheus Kennzahl, um den vollen Umfang des zulässigen Metadaten-Speicherplatzes zu messen:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_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.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.



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 **ALERTS Current**.
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 Metadaten an einem Standort hinzufügen müssen, sollten Sie auch [Erweitern Sie alle anderen Standorte](#) An die gleiche Anzahl von Storage-Nodes.

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.

Fehlersuche im Alarm Services: Status - Cassandra (SVST) durchführen

Der Alarm Services: Status – Cassandra (SVST) gibt an, dass Sie die Cassandra-Datenbank für einen Storage-Node möglicherweise neu aufbauen müssen. Cassandra dient als Metadaten-Speicher für StorageGRID.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- 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.

Das können Sie [Führen Sie eine Diagnose aus](#) Um zusätzliche Informationen über den aktuellen Status Ihres Rasters zu erhalten.



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-Topologie** aus.
2. Wählen Sie **Site Storage Node SSM Services Alarme Main**, um Alarme anzuzeigen.

Dieses Beispiel zeigt, dass der SVST-Alarm ausgelöst wurde.

Severity Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running		<input type="checkbox"/>

Auf der SSM Services-Hauptseite wird auch angezeigt, dass Cassandra nicht ausgeführt wird.

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC2-S1) - Services

Updated: 2017-03-30 09:53:53 MDT

Operating System: Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running	4	3.58 %	19.1 MB

3. Neustarten von Cassandra aus dem Storage-Node:
 - 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`
4. 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.

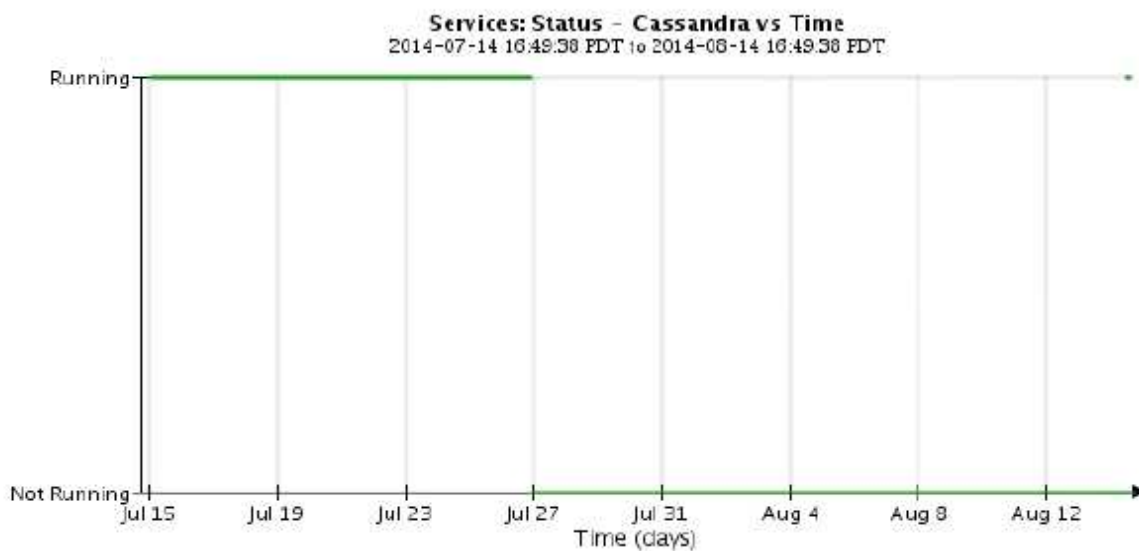
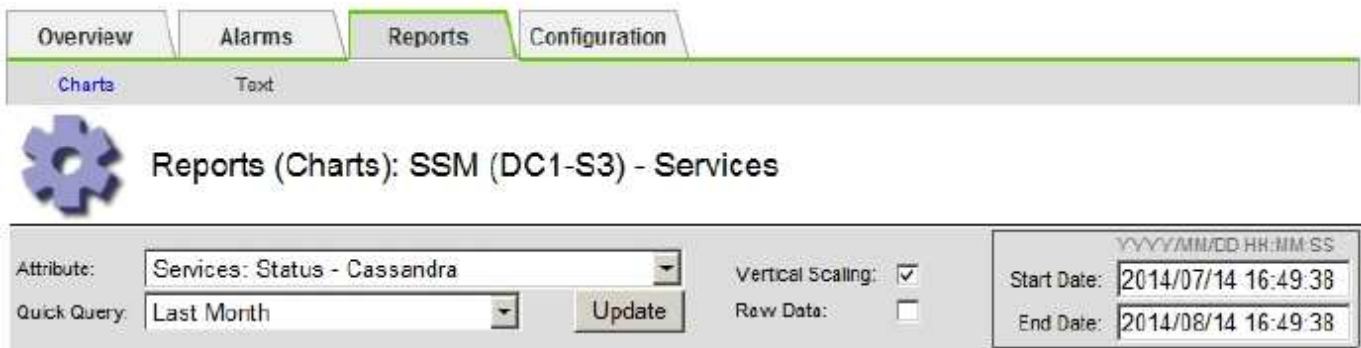
Sie können feststellen, wie lange Cassandra ausgefallen ist, indem Sie sie aufschreiben oder die Datei `servermanager.log` lesen.

5. Cassandra Diagramm:
 - a. Wählen Sie **SUPPORT Tools Grid-Topologie** 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 [Stellen Sie Storage Node länger als 15 Tage wieder her](#).

- c. Wenden Sie sich an den technischen Support, wenn die Alarme nach dem Wiederaufbau von Cassandra nicht gelöscht werden.

Fehlerbehebung bei Cassandra-Fehlern außerhalb des Speichers (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 **SUPPORT Tools Grid-Topologie Konfiguration**.
2. Stellen Sie sicher, dass die Anzahl der Cassandra Heap-Fehler bei einem Speicherfehler mindestens 1 beträgt.

Das können Sie [Führen Sie eine Diagnose aus](#) Um zusätzliche Informationen über den aktuellen Status Ihres Rasters zu erhalten.

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. Nachdem das Problem behoben wurde, aktivieren Sie das Kontrollkästchen **Zurücksetzen** für die Anzahl der Cassandra-Heap-Fehler aus dem Speicher. Wählen Sie dann **Änderungen anwenden**.



Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen.

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.

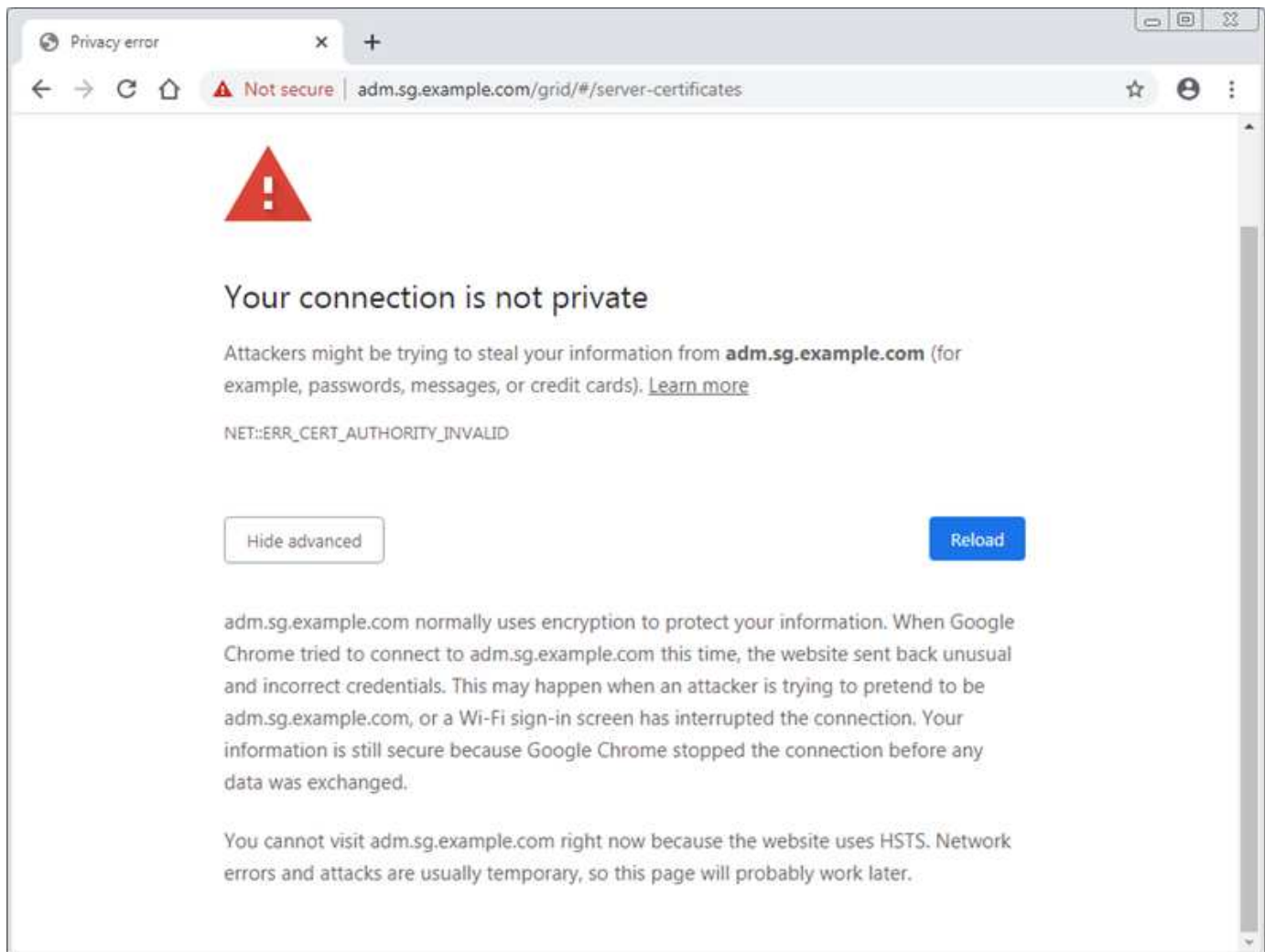
Über diese Aufgabe

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 Domännennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für die benutzerdefinierte Managementoberfläche läuft ab.
- Sie werden von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Im folgenden Beispiel ist ein Zertifikatfehler angezeigt, wenn das Zertifikat der benutzerdefinierten Managementoberfläche abgelaufen ist:



Um sicherzustellen, dass 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 Zertifikat der StorageGRID-Verwaltungsschnittstelle oder durch Clientzertifikate verursacht werden. Die auf der Seite [Zertifikate*](#) konfigurierte Warnung ***Ablauf von Clientzertifikaten** wird ausgelöst, wenn ein Clientzertifikat abläuft.

Schritte

Wenn Sie eine Benachrichtigung über ein abgelaufenes Zertifikat erhalten haben, rufen Sie die Zertifikatsdetails auf: . Wählen Sie **KONFIGURATION Sicherheit Zertifikate** und dann [Wählen Sie die entsprechende Registerkarte Zertifikat aus](#).

1. Überprüfen Sie die Gültigkeitsdauer des Zertifikats. + einige Webbrowser und S3- oder Swift-Clients akzeptieren keine Zertifikate mit einer Gültigkeitsdauer von mehr als 398 Tagen.
2. Wenn das Zertifikat abgelaufen ist oder bald abläuft, laden Sie ein oder generieren Sie ein neues Zertifikat.
 - Ein Serverzertifikat finden Sie in den Schritten für [Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#).
 - Ein Client-Zertifikat finden Sie in den Schritten für [Konfigurieren eines Client-Zertifikats](#).
3. Versuchen Sie bei Serverzertifikatfehlern oder beiden der folgenden Optionen:
 - Stellen Sie sicher, dass der Alternative Name (SAN) des Zertifikats ausgefüllt ist und dass das SAN mit der IP-Adresse oder dem Hostnamen des Node übereinstimmt, mit dem Sie eine Verbindung herstellen.
 - Wenn Sie versuchen, eine Verbindung zu StorageGRID mit einem Domain-Namen herzustellen:
 - i. Geben Sie die IP-Adresse des Admin-Knotens anstelle des Domain-Namens ein, um den Verbindungsfehler zu umgehen und auf den Grid-Manager zuzugreifen.
 - ii. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und dann [Wählen Sie die entsprechende Registerkarte Zertifikat aus](#) So installieren Sie ein neues benutzerdefiniertes Zertifikat oder fahren mit dem Standardzertifikat fort.
 - iii. Lesen Sie in der Anleitung zum Verwalten von StorageGRID die Schritte für [Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager](#).

Fehlerbehebung bei Problemen mit Admin-Node 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.

Fehler bei der Anmeldung beheben

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 Alarmer.
 - ii. Wählen Sie **KONFIGURATION Zugangskontrolle Identitätsverbund**.
 - 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 nginx-gw-Dienst ausgeführt wird # `service nginx-gw status`

9. Lumberjack zum Sammeln von Protokollen verwenden: # `/usr/local/sbin/lumberjack.rb`

Wenn die fehlgeschlagene Authentifizierung in der Vergangenheit stattgefunden hat, können Sie die Skriptoptionen `--start` und `--end` Lumberjack verwenden, um den entsprechenden Zeitbereich festzulegen. Verwenden Sie die `lumberjack -h` für Details zu diesen Optionen.

Die Ausgabe an das Terminal gibt an, wo das Protokollarchiv kopiert wurde.

10. folgende Protokolle prüfen:

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Wenn Sie keine Probleme mit dem Admin-Knoten feststellen konnten, geben Sie einen der folgenden Befehle ein, um die IP-Adressen der drei Speicherknoten zu ermitteln, die den ADC-Dienst an Ihrem Standort ausführen. In der Regel handelt es sich dabei um die ersten drei Storage-Nodes, die am Standort installiert wurden.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Admin-Knoten verwenden den ADC-Dienst während des Authentifizierungsprozesses.

12. 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 `#`.

13. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Stellen Sie sicher, dass die Services `idnt`, `acct`, `nginx` und `cassandra` ausgeführt werden.

14. Wiederholen Sie die Schritte [Verwenden Sie Lumberjack, um Protokolle zu sammeln](#) Und [Protokolle prüfen](#) So prüfen Sie die Protokolle auf den Speicherknoten.

15. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Stellen Sie die Protokolle bereit, die Sie für den technischen Support gesammelt haben. Siehe auch [Referenz für Protokolldateien](#).

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 ein verwenden [Unterstützter Webbrowser](#).



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.

Überprüfen Sie den 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 bei Grid Manager an [Unterstützter Webbrowser](#).
2. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
3. Wählen Sie **Site nicht verfügbar 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](#)

Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen

Sie können verschiedene Aufgaben durchführen, um die Ursache von Problemen im Zusammenhang mit dem StorageGRID Netzwerk-, Hardware- und Plattformproblemen zu ermitteln.

Fehler bei „422: Unbearbeitbare Einheit“ beheben

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
<pre>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</pre>	<p>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.</p> <p>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.</p>
<pre>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)</pre>	<p>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.</p> <p>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.</p>

Verwandte Informationen

[StorageGRID verwalten](#)

Fehlerbehebung bei der MTU-Warnung für das Grid Network

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-ip.py [-h] [-n node] mtu network [network...]`
 - Beispiel*: `change-ip.py -n node 1500 grid admin`

Hinweis: Wenn auf Linux-basierten Knoten der gewünschte MTU-Wert für das Netzwerk im Container den bereits auf der Hostschnittstelle konfigurierten Wert überschreitet, müssen Sie zuerst die Hostschnittstelle so konfigurieren, dass sie den gewünschten MTU-Wert hat, und dann den verwenden `change-ip.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
<code>mtu</code>	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
<code>network</code>	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: <ul style="list-style-type: none">• Raster• Admin• Client

+

Optionale Argumente	Beschreibung
-h, - help	Hilfemeldung anzeigen und beenden.
-n node, --node node	Der Node. Die Standardeinstellung ist der lokale Knoten.

Verwandte Informationen

[SG100- und SG1000-Services-Appliances](#)

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[SG5600 Storage Appliances](#)

Beheben Sie die Fehlerbehebung im NRER-Alarm (Network Receive Error)

NRER-Alarmer (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-Alarmer 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 Netzkabel 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-Topologie** aus.
 - b. Wählen Sie **site Grid Node SSM Ressourcen Konfiguration Main**.

c. Wählen Sie **Empfangspunkt zurücksetzen** und klicken Sie auf **Änderungen anwenden**.

Verwandte Informationen

[Fehler bei der Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU](#)

[Alarmreferenz \(Altsystem\)](#)

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[SG5600 Storage Appliances](#)

[SG100- und SG1000-Services-Appliances](#)

Fehler bei der Zeitsynchronisierung beheben

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

[Recovery und Wartung](#)

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 promiscuous-Modus auf dem Hypervisor nicht aktiviert wurde.

Weitere Informationen zum Aktivieren des MAC-Klonens finden Sie in den Anweisungen im Installationshandbuch für Ihre Plattform.

Promiscuous 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 Befehle der Container-Engine, um den vorhandenen Node-Container zu beenden.
- Starten Sie den Node neu.

Schritte

1. Überprüfen Sie die Protokolle sowohl für den Service-Daemon als auch für den verwaisten Node auf offensichtliche Fehler oder Meldungen zum unerwarteten Beenden.
2. Melden Sie sich beim Host als Root an oder verwenden Sie ein Konto mit sudo-Berechtigung.
3. Versuchen Sie, den Node erneut zu starten, indem Sie den folgenden Befehl ausführen: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Wenn der Node verwaiste ist, wird die Antwort angezeigt

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Stoppen Sie von Linux die Container-Engine und alle kontrollierenden storagegrid Node-Prozesse. Beispiel: `sudo docker stop --time secondscontainer-name`

Für `seconds` Geben Sie die Anzahl der Sekunden ein, die Sie warten möchten, bis der Container angehalten wird (normalerweise 15 Minuten oder weniger). Beispiel:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Starten Sie den Knoten neu: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

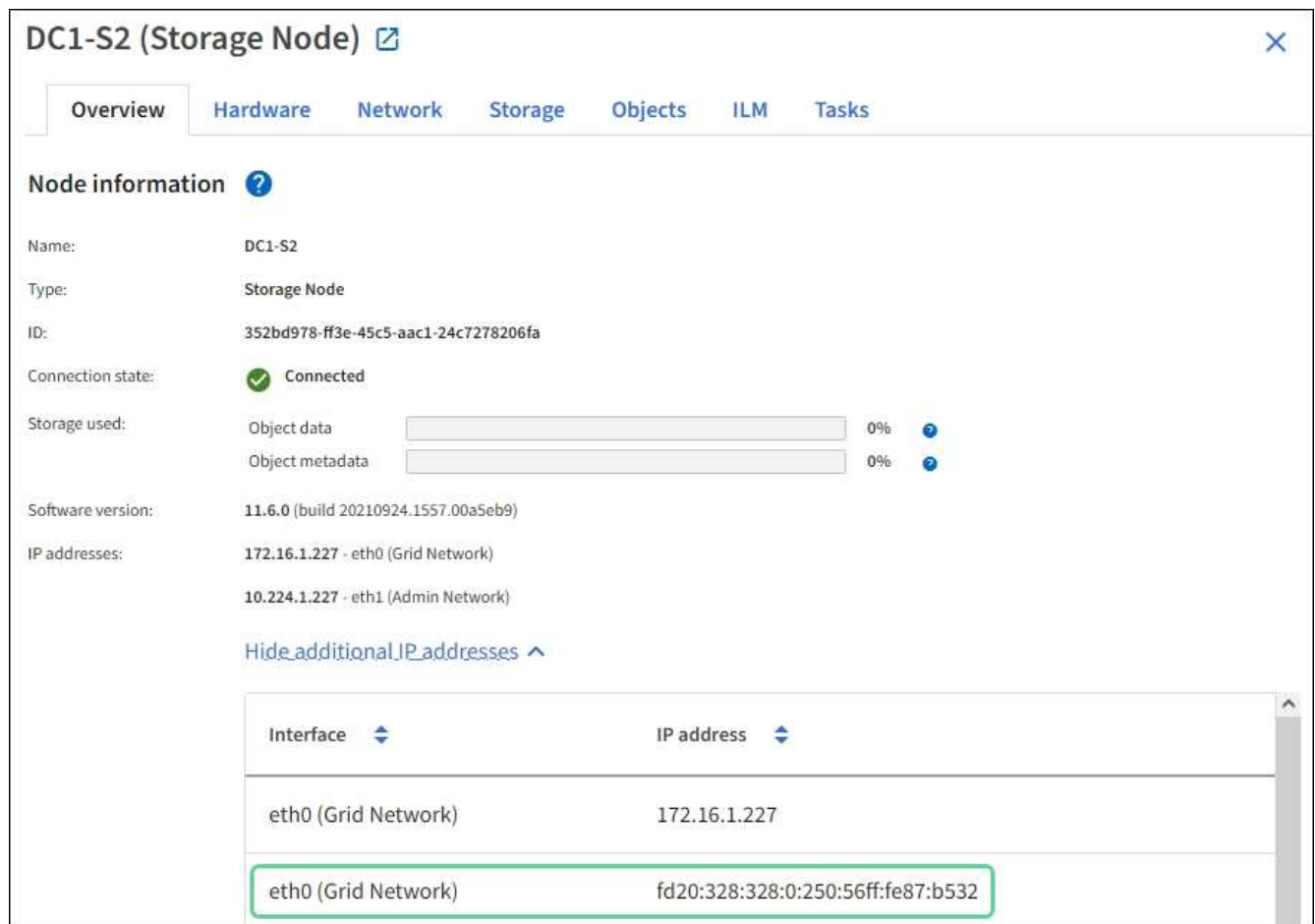
Linux: Fehlerbehebung bei der IPv6-Unterstützung

Möglicherweise müssen Sie die IPv6-Unterstützung im Kernel aktivieren, wenn Sie StorageGRID-Knoten auf Linux-Hosts installiert haben und Sie bemerken, dass den Knoten-Containern keine IPv6-Adressen wie erwartet zugewiesen wurden.

Über diese Aufgabe

Die IPv6-Adresse, die einem Grid-Node zugewiesen wurde, wird in den folgenden Speicherorten im Grid Manager angezeigt:

- Wählen Sie **NODES** aus, und wählen Sie den Knoten aus. Wählen Sie dann auf der Registerkarte Übersicht neben **IP-Adressen** die Option **Mehr anzeigen** aus.



The screenshot shows the 'DC1-S2 (Storage Node)' page in the Grid Manager. The 'Node information' section is expanded to show 'IP addresses'. The 'eth0 (Grid Network)' interface is highlighted with a green box, showing the IPv6 address `fd20:328:328:0:250:56ff:fe87:b532`.

Interface	IP address
eth0 (Grid Network)	172.16.1.227
eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532

- Wählen Sie **SUPPORT Tools Grid-Topologie** 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
```

Fehlerbehebung für einen externen Syslog-Server

In der folgenden Tabelle werden Fehlermeldungen des externen Syslog-Servers beschrieben und Korrekturmaßnahmen aufgeführt.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Hostname kann nicht aufgelöst werden	<p>Der für den Syslog-Server eingegebene FQDN konnte nicht in eine IP-Adresse aufgelöst werden.</p> <ol style="list-style-type: none">Überprüfen Sie den eingegebenen Hostnamen. Wenn Sie eine IP-Adresse eingegeben haben, stellen Sie sicher, dass es sich um eine gültige IP-Adresse in der Schreibweise W.X.Y.Z („gepunktete Dezimalstelle“) handelt.Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind.Vergewissern Sie sich, dass jeder Knoten auf die IP-Adressen des DNS-Servers zugreifen kann.
Verbindung abgelehnt	<p>Eine TCP- oder TLS-Verbindung zum Syslog-Server wurde abgelehnt. Möglicherweise ist auf dem TCP- oder TLS-Port für den Host kein Service verfügbar, oder eine Firewall blockiert möglicherweise den Zugriff.</p> <ol style="list-style-type: none">Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben.Vergewissern Sie sich, dass der Host für den syslog-Service einen Syslog-Daemon ausführt, der auf dem angegebenen Port abhört.Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten auf die IP und den Port des Syslog-Servers blockiert.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Netzwerk nicht erreichbar	<p>Der Syslog-Server befindet sich nicht in einem direkt verbundenen Subnetz. Ein Router hat eine ICMP-Fehlermeldung zurückgegeben, um anzuzeigen, dass die Testmeldungen von den aufgeführten Knoten nicht an den Syslog-Server weitergeleitet werden konnten.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Node die Liste des Grid-Netzwerksubnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese konfiguriert sind, um Datenverkehr zum Syslog-Server über die erwartete Netzwerkschnittstelle und das erwartete Gateway (Grid, Administrator oder Client) zu leiten.
Host nicht erreichbar	<p>Der Syslog-Server befindet sich in einem direkt verbundenen Subnetz (Subnetz, das von den aufgeführten Knoten für ihre Grid-, Admin- oder Client-IP-Adressen verwendet wird). Die Knoten versuchten, Testmeldungen zu senden, erhielten aber keine Antworten auf ARP-Anfragen für die MAC-Adresse des Syslog-Servers.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie, ob der Host, auf dem der Syslog-Service ausgeführt wird, ausgeführt wird.
Zeitüberschreitung bei Verbindung	<p>Es wurde ein TCP/TLS-Verbindungsversuch unternommen, aber für lange Zeit wurde vom Syslog-Server keine Antwort empfangen. Möglicherweise gibt es eine Fehlkonfiguration bei Routing oder eine Firewall könnte den Datenverkehr ohne jede Antwort löschen (eine häufige Konfiguration).</p> <ol style="list-style-type: none"> 1. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse für den Syslog-Server eingegeben haben. 2. Überprüfen Sie für jeden aufgeführten Node die Liste des Grid-Netzwerksubnetz, die Subnetz-Listen von Admin-Netzwerken und die Client-Netzwerk-Gateways. Vergewissern Sie sich, dass diese konfiguriert sind, um Datenverkehr über die Netzwerkschnittstelle und das Gateway (Grid, Admin oder Client) an den Syslog-Server weiterzuleiten, über den Sie erwarten, dass der Syslog-Server erreicht wird. 3. Vergewissern Sie sich, dass eine Firewall keinen Zugriff auf TCP/TLS-Verbindungen von den Knoten blockiert, die in der IP und dem Port des Syslog-Servers aufgeführt sind.

Fehlermeldung	Beschreibung und empfohlene Aktionen
Verbindung vom Partner geschlossen	<p>Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, wurde aber später geschlossen. Gründe hierfür sind u. a.:</p> <ul style="list-style-type: none"> • Der Syslog-Server wurde möglicherweise neu gestartet oder neu gestartet. • Der Node und der Syslog-Server verfügen möglicherweise über unterschiedliche TCP/TLS-Einstellungen. • Bei einer Zwischenfirewall werden möglicherweise inaktive TCP-Verbindungen geschlossen. • Ein nicht-Syslog-Server, der auf dem Syslog-Server-Port hört, hat die Verbindung möglicherweise geschlossen. <ul style="list-style-type: none"> a. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. b. Wenn Sie TLS verwenden, bestätigen Sie, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, bestätigen Sie, dass der Syslog-Server auch TCP verwendet. c. Überprüfen Sie, ob eine Zwischenfirewall nicht für das Schließen inaktiver TCP-Verbindungen konfiguriert ist.
Fehler beim TLS-Zertifikat	<p>Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen angegebenen CA-Zertifikatspaket und dem von Ihnen angegebenen Clientzertifikat kompatibel.</p> <ol style="list-style-type: none"> 1. Vergewissern Sie sich, dass das CA-Zertifikatsbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat auf dem Syslog-Server kompatibel sind. 2. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Weiterleitung angehalten	<p>Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet, und StorageGRID kann den Grund nicht erkennen.</p> <p>Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln.</p>

Fehlermeldung	Beschreibung und empfohlene Aktionen
TLS-Sitzung beendet	<p>Der Syslog-Server hat die TLS-Sitzung beendet und StorageGRID kann den Grund nicht erkennen.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln. 2. Überprüfen Sie, ob Sie den richtigen FQDN oder die richtige IP-Adresse, den richtigen Port und das richtige Protokoll für den Syslog-Server eingegeben haben. 3. Wenn Sie TLS verwenden, bestätigen Sie, dass der Syslog-Server auch TLS verwendet. Wenn Sie TCP verwenden, bestätigen Sie, dass der Syslog-Server auch TCP verwendet. 4. Vergewissern Sie sich, dass das CA-Zertifikatbündel und das Clientzertifikat (falls vorhanden) mit dem Serverzertifikat vom Syslog-Server kompatibel sind. 5. Vergewissern Sie sich, dass die Identitäten im Serverzertifikat vom Syslog-Server die erwarteten IP- oder FQDN-Werte enthalten.
Abfrage der Ergebnisse fehlgeschlagen	<p>Der für die Konfiguration und Tests des Syslog-Servers verwendete Admin-Node kann die Testergebnisse nicht von den aufgeführten Nodes anfordern. Mindestens ein Node ist ausgefallen.</p> <ol style="list-style-type: none"> 1. Befolgen Sie die Standardschritte zur Fehlerbehebung, um sicherzustellen, dass die Knoten online sind und alle erwarteten Services ausgeführt werden. 2. Starten Sie den falsch-Dienst auf den aufgeführten Knoten neu.

Alerts Referenz

In der folgenden Tabelle sind alle standardmäßigen StorageGRID-Warnmeldungen aufgeführt. Bei Bedarf können Sie benutzerdefinierte Alarmregeln erstellen, die Ihrem Systemmanagement entsprechen.

Weitere Informationen finden Sie unter [Häufig verwendete 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	<p>Der Akku im Speicher-Controller des Geräts ist abgelaufen.</p> <ol style="list-style-type: none"> 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Akku des Geräts fehlgeschlagen	<p>Der Akku im Speicher-Controller des Geräts ist ausgefallen.</p> <ol style="list-style-type: none"> 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 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	<p>Der Akku im Speicher-Controller des Geräts weist nicht genügend Kapazität auf.</p> <ol style="list-style-type: none"> 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Akku des Geräts befindet sich nahe dem Ablauf	<p>Der Akku im Speicher-Controller des Geräts läuft langsam ab.</p> <ol style="list-style-type: none"> 1. Setzen Sie die Batterie bald wieder ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Akku des Geräts entfernt	<p>Der Akku im Speicher-Controller des Geräts fehlt.</p> <ol style="list-style-type: none"> 1. Setzen Sie eine Batterie ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Akku des Geräts ist zu heiß	<p>Die Batterie im Speicher-Controller des Geräts ist überhitzt.</p> <ol style="list-style-type: none"> 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.

Alarmname	Beschreibung und empfohlene Aktionen
Fehler bei der BMC-Kommunikation des Geräts	<p>Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren.</p> <ol style="list-style-type: none"> 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ SG6000 Storage-Appliances 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Fehler beim Sichern des Appliance-Cache	<p>Ein persistentes Cache-Sicherungsgerät ist fehlgeschlagen.</p> <ol style="list-style-type: none"> 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	<p>Die Kapazität des Cache-Sicherungsgeräts ist nicht ausreichend.</p> <p>Wenden Sie sich an den technischen Support.</p>
Appliance Cache Backup-Gerät schreibgeschützt	<p>Ein Cache-Backup-Gerät ist schreibgeschützt.</p> <p>Wenden Sie sich an den technischen Support.</p>
Die Größe des Appliance-Cache-Speichers stimmt nicht überein	<p>Die beiden Controller im Gerät haben unterschiedliche Cache-Größen.</p> <p>Wenden Sie sich an den technischen Support.</p>

Alarmname	Beschreibung und empfohlene Aktionen
<p>Die Temperatur des Computing-Controller-Chassis des Geräts ist zu hoch</p>	<p>Die Temperatur des Computing-Controllers in einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.</p> <ol style="list-style-type: none"> 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: <ul style="list-style-type: none"> ◦ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
<p>Die CPU-Temperatur des Appliance-Compute-Controllers ist zu hoch</p>	<p>Die Temperatur der CPU im Computing-Controller einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten.</p> <ol style="list-style-type: none"> 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: <ul style="list-style-type: none"> ◦ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Aufmerksamkeit für Compute-Controller ist erforderlich	<p>Im Compute-Controller einer StorageGRID-Appliance wurde ein Hardwarefehler erkannt.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: <ul style="list-style-type: none"> ◦ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances
Ein Problem besteht in der Stromversorgung Des Computercontrollers A des Geräts	<p>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.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: <ul style="list-style-type: none"> ◦ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Das Netzteil B des Compute-Controllers ist ein Problem	<p>Die Stromversorgung B im Compute-Controller hat ein Problem.</p> <p>Diese Warnmeldung weist möglicherweise darauf hin, dass das Netzteil ausgefallen ist oder dass es ein Problem bei der Stromversorgung aufweist.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: <ul style="list-style-type: none"> ◦ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances
Der Service zur Überwachung der Computing-Hardware des Appliances ist ausgesetzt	<p>Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt.</p> <ol style="list-style-type: none"> 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
Fibre-Channel-Fehler des Geräts erkannt	<p>Es wurde ein Fibre Channel-Verbindungsproblem zwischen dem Speicher-Controller des Geräts und dem Compute-Controller erkannt.</p> <p>Diese Warnmeldung weist möglicherweise darauf hin, dass ein Problem bei der Fibre Channel-Verbindung zwischen den Storage- und Computing-Controllern in der Appliance aufgetreten ist.</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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. <p>Hinweis: Wenn dieses Problem weiterhin besteht, kann das StorageGRID-System die problematische Verbindung automatisch offline schalten.</p> 2. Bei Bedarf die Komponenten austauschen. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances
Fehler des Fibre-Channel-HBA-Ports des Geräts	<p>Ein Fibre-Channel-HBA-Port ist ausgefallen oder ist ausgefallen.</p> <p>Wenden Sie sich an den technischen Support.</p>
Appliance Flash Cache Laufwerke sind nicht optimal	<p>Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal.</p> <ol style="list-style-type: none"> 1. Ersetzen Sie die SSD-Cache-Laufwerke. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Geräteverbindung/Batteriebehälter entfernt	<p>Der Verbindungs-/Batteriebehälter fehlt.</p> <ol style="list-style-type: none"> 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Lesen Sie die Anweisungen für Ihre Storage Appliance. <ul style="list-style-type: none"> ◦ SG5600 Storage Appliances ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Geräte-LACP-Port fehlt	<p>Ein Port auf einer StorageGRID-Appliance beteiligt sich nicht an der LACP-Verbindung.</p> <ol style="list-style-type: none"> 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.
Das gesamte Netzteil des Geräts ist heruntergestuft	<p>Die Leistung eines StorageGRID-Geräts ist von der empfohlenen Betriebsspannung abweichen.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie den Status von Netzteil A und B, um festzustellen, welches Netzteil ungewöhnlich funktioniert, und befolgen Sie die empfohlenen Maßnahmen: <ul style="list-style-type: none"> ◦ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ SG100- und SG1000-Services-Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Ausfall des Appliance Storage Controller A	<p>Der Speicher-Controller A in einer StorageGRID-Appliance ist ausgefallen.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Fehler beim Speicher-Controller B des Geräts	<p>Bei Speicher-Controller B in einer StorageGRID-Appliance ist ein Fehler aufgetreten.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Laufwerksausfall des Appliance-Storage-Controllers	<p>Mindestens ein Laufwerk in einer StorageGRID-Appliance ist ausgefallen oder nicht optimal.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Hardwareproblem des Appliance Storage Controllers	<p>SANtricity meldet, dass für eine Komponente einer StorageGRID Appliance ein Hinweis erforderlich ist.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Ausfall der Stromversorgung des Speicher-Controllers	<p>Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abweichen.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Fehler bei Netzteil B des Speicher-Controllers	<p>Stromversorgung B bei einem StorageGRID-Gerät hat von der empfohlenen Betriebsspannung abweichen.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances

Alarmname	Beschreibung und empfohlene Aktionen
<p>Monitordienst der Appliance-Storage-Hardware ist ausgesetzt</p>	<p>Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt.</p> <ol style="list-style-type: none"> 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.
<p>Appliance Storage-Shelfs ist beeinträchtigt</p>	<p>Der Status einer der Komponenten im Storage Shelf für eine Storage Appliance ist beeinträchtigt.</p> <ol style="list-style-type: none"> 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
<p>Gerätetemperatur überschritten</p>	<p>Die nominale oder maximale Temperatur für den Lagercontroller des Geräts wurde überschritten.</p> <ol style="list-style-type: none"> 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.
<p>Temperatursensor des Geräts entfernt</p>	<p>Ein Temperatursensor wurde entfernt. Wenden Sie sich an den technischen Support.</p>

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Auto-Kompaktor-Fehler	<p>Beim Cassandra Auto-Kompaktor ist ein Fehler aufgetreten.</p> <p>Der Cassandra Auto-Kompaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank bei Überschreibungen und Lötten schwerer Workloads. Diese Bedingung bleibt bestehen, aber bei bestimmten Workloads kommt es zu einem unerwartet hohen Metadatenverbrauch.</p> <ol style="list-style-type: none"> 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.
Audit-Protokolle werden der Warteschlange im Speicher hinzugefügt	<p>Der Node kann Protokolle nicht an den lokalen Syslog-Server senden, und die Warteschlange im Speicher wird ausgefüllt.</p> <ol style="list-style-type: none"> 1. Vergewissern Sie sich, dass der rsyslog-Service auf dem Node ausgeführt wird. 2. Falls erforderlich, starten Sie den rsyslog-Service auf dem Node mithilfe des Befehls <code>neu service rsyslog restart</code>. 3. Wenn der rsyslog-Dienst nicht neu gestartet werden kann und Sie keine Audit-Meldungen auf Admin-Knoten speichern, wenden Sie sich an den technischen Support. Prüfprotokolle gehen verloren, wenn diese Bedingung nicht korrigiert wird.
Cassandra Auto-Kompaktor-Kennzahlen veraltet	<p>Die Kennzahlen, die den Cassandra Auto-Kompaktor beschreiben, sind veraltet.</p> <p>Der Cassandra Auto-Kompaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank bei Überschreibungen und Lötten schwerer Workloads. Während diese Warnung weiterhin angezeigt wird, kommt es bei bestimmten Workloads zu einem unerwartet hohen Metadatenverbrauch.</p> <ol style="list-style-type: none"> 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 Kommunikationsfehler	<p>Die Nodes, auf denen der Cassandra-Service ausgeführt wird, haben Probleme bei der Kommunikation untereinander.</p> <p>Diese Warnmeldung zeigt, dass etwas die Kommunikation zwischen Nodes beeinträchtigt. Möglicherweise gibt es ein Netzwerkproblem, oder der Cassandra-Service ist auf einem oder mehreren Storage-Nodes nicht verfügbar.</p> <ol style="list-style-type: none"> 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-Topologie aus. 4. Wählen Sie für jeden Speicherknoten in Ihrem System SSM Services aus. Stellen Sie sicher, dass der Status des Cassandra-Services „läuft“. 5. Falls Cassandra nicht ausgeführt wird, befolgen Sie die Schritte für Starten oder Neustarten eines Dienstes. 6. Wenn jetzt alle Instanzen des Cassandra-Service ausgeführt werden und die Warnmeldung nicht behoben wurde, wenden Sie sich an den technischen Support.
Cassandra-Kompensation überlastet	<p>Der Cassandra-Verdichtungsprozess ist überlastet.</p> <p>Wenn der Verdichtungsprozess überlastet ist, kann die Lese-Performance beeinträchtigt werden und möglicherweise ist der RAM-Speicher erforderlich. Auch der Cassandra-Service reagiert möglicherweise nicht oder stürzt ab.</p> <ol style="list-style-type: none"> 1. Starten Sie den Cassandra-Service neu. Befolgen Sie dazu die Schritte für Neustart eines Dienstes. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Veraltete Reparaturkennzahlen für Cassandra	<p>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.</p> <ol style="list-style-type: none"> 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.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Reparaturfortschritt langsam	<p>Der Fortschritt der Cassandra-Datenbankreparaturen ist langsam.</p> <p>Bei langsamen Datenbankreparaturen wird die Datenkonsistenz im Cassandra behindert. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt.</p> <ol style="list-style-type: none"> 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.
Cassandra Reparaturservice nicht verfügbar	<p>Der Cassandra-Reparaturservice ist nicht verfügbar.</p> <p>Der Cassandra Reparaturservice ist auf allen Storage-Nodes 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.</p> <ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Tools > Grid-Topologie 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. Falls Cassandra Reaper nicht ausgeführt wird, befolgen Sie die Schritte für Starten oder Neustarten eines Dienstes. 4. Wenn jetzt alle Instanzen des Cassandra Reaper Service ausgeführt werden und die Warnmeldung nicht behoben ist, wenden Sie sich an den technischen Support.
Cassandra Tabelle beschädigt	<p>Cassandra hat Tabellenbeschädigungen erkannt.</p> <p>Cassandra wird automatisch neu gestartet, wenn Tabellenbeschädigungen erkannt werden.</p> <p>Wenden Sie sich an den technischen Support.</p>
Verbindungsfehler beim Cloud-Storage-Pool	<p>Bei der Zustandsprüfung für Cloud-Storage-Pools wurde ein oder mehrere neue Fehler erkannt.</p> <ol style="list-style-type: none"> 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. Siehe Anweisungen für Verwalten von Objekten mit Information Lifecycle Management.

Alarmname	Beschreibung und empfohlene Aktionen
DHCP-Leasing abgelaufen	<p>Der DHCP-Leasingvertrag auf einer Netzwerkschnittstelle ist abgelaufen. Wenn der DHCP-Leasing abgelaufen ist, befolgen Sie die empfohlenen Maßnahmen:</p> <ol style="list-style-type: none"> 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. Siehe Anweisungen zur Wiederherstellung und Wartung.
DHCP-Leasing läuft bald ab	<p>Der DHCP-Lease auf einer Netzwerkschnittstelle läuft demnächst aus.</p> <p>Um zu verhindern, dass der DHCP-Leasingraten abläuft, führen Sie die empfohlenen Maßnahmen durch:</p> <ol style="list-style-type: none"> 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. Siehe Anweisungen zur Wiederherstellung und Wartung.
DHCP-Server nicht verfügbar	<p>Der DHCP-Server ist nicht verfügbar.</p> <p>Der StorageGRID-Node kann den DHCP-Server nicht kontaktieren. Das DHCP-Leasing für die IP-Adresse des Node kann nicht validiert werden.</p> <ol style="list-style-type: none"> 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. Siehe Anweisungen zur Wiederherstellung und Wartung.

Alarmname	Beschreibung und empfohlene Aktionen
Die Festplatten-I/O ist sehr langsam	<p>Sehr langsamer Festplatten-I/O könnte sich auf die StorageGRID-Performance auswirken.</p> <ol style="list-style-type: none"> 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. <p>Hinweis: betroffene Knoten könnten Dienste deaktivieren und sich neu starten, um keine Auswirkungen auf die Gesamtleistung des Grids zu haben. Wenn der zugrunde liegende Zustand beseitigt ist und diese Nodes eine normale I/O-Performance erkennen, wird der gesamte Service automatisch wiederhergestellt.</p>
EC-Ausgleichfehler	<p>Der Job zur Neuverteilung von Daten, die mit Lösungs-codes zwischen Speicherknoten codiert wurden, ist fehlgeschlagen oder wurde vom Benutzer angehalten.</p> <ol style="list-style-type: none"> 1. Stellen Sie sicher, dass alle Speicherknoten an der Seite, die ausgeglichen werden, online und verfügbar sind. 2. Stellen Sie sicher, dass am Standort keine Volume-Ausfälle ausgeglichen werden. Wenn dies der Fall ist, beenden Sie den EC-Ausgleichauftrag, sodass Sie einen Reparaturauftrag ausführen können. <p style="margin-left: 40px;"><code>'rebalance-data terminate --job-id <ID>'</code></p> 3. Stellen Sie sicher, dass am Standort keine Serviceausfälle auftreten, die ausgeglichen werden. Wenn ein Dienst nicht ausgeführt wird, befolgen Sie die Schritte zum Starten oder Neustarten eines Dienstes in den Anweisungen zur Wiederherstellung und Wartung. 4. Starten Sie nach der Behebung von Problemen den Job neu, indem Sie den folgenden Befehl auf dem primären Administratorknoten ausführen: <p style="margin-left: 40px;"><code>'rebalance-data start --job-id <ID>'</code></p> 5. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
EC-Reparaturfehler	<p>Ein Reparaturauftrag für Löschungscodierte Daten ist fehlgeschlagen oder wurde angehalten.</p> <ol style="list-style-type: none"> 1. Stellen Sie sicher, dass genügend Storage-Nodes oder -Volumes zur Verfügung stehen, um den fehlerhaften Storage-Node oder das ausgefallene Volume zu übernehmen. 2. Stellen Sie sicher, dass genügend Storage Nodes vorhanden sind, um die aktive ILM-Richtlinie zu erfüllen. 3. Stellen Sie sicher, dass es keine Probleme mit der Netzwerkverbindung gibt. 4. Starten Sie nach der Behebung von Problemen den Job neu, indem Sie den folgenden Befehl auf dem primären Administratorknoten ausführen: <pre data-bbox="639 688 1393 751">'repair-data start-ec-node-repair --repair-id <ID>'</pre> 5. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.
EC-Reparatur blockiert	<p>Ein Reparaturauftrag für Daten, die aufgrund von Erasure-Coding-Verfahren codiert wurden, ist ins Stocken geraten.</p> <ol style="list-style-type: none"> 1. Stellen Sie sicher, dass genügend Storage-Nodes oder -Volumes zur Verfügung stehen, um den fehlerhaften Storage-Node oder das ausgefallene Volume zu übernehmen. 2. Stellen Sie sicher, dass es keine Probleme mit der Netzwerkverbindung gibt. 3. Prüfen Sie nach der Behebung von Problemen, ob die Meldung behoben ist. Um einen detaillierteren Bericht über den Fortschritt der Reparatur anzuzeigen, führen Sie den folgenden Befehl auf dem primären Admin-Knoten aus: <pre data-bbox="639 1381 1409 1444">'repair-data show-ec-repair-status --repair-id <ID>'</pre> 4. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.


Alarmname	Beschreibung und empfohlene Aktionen
E-Mail-Benachrichtigung fehlgeschlagen	<p>Die E-Mail-Benachrichtigung für eine Warnmeldung konnte nicht gesendet werden.</p> <p>Diese Warnung wird ausgelöst, wenn eine Benachrichtigung per E-Mail fehlschlägt oder eine Test-E-Mail (gesendet von der Seite ALERTS E-Mail Setup) nicht zugestellt werden kann.</p> <ol style="list-style-type: none"> 1. Melden Sie sich über den Admin-Node in der Spalte Standort/Node der Warnmeldung bei Grid Manager an. 2. Gehen Sie auf die Seite ALERTS E-Mail-Setup, überprüfen Sie die Einstellungen und ändern Sie diese bei Bedarf. 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 Logs 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 <code>prometheus.log</code> (<code>_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log</code>). 7. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.
Ablauf von Clientzertifikaten, die auf der Seite Zertifikate konfiguriert sind	<p>Ein oder mehrere auf der Seite Zertifikate konfigurierte Clientzertifikate sind kurz vor dem Ablauf.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit Zertifikate und wählen Sie dann die Registerkarte Client aus. 2. Wählen Sie ein Zertifikat aus, das bald abläuft. 3. Wählen Sie * Neues Zertifikat anhängen* an Hochladen oder Generieren eines neuen Zertifikats. 4. Wiederholen Sie diese Schritte für jedes Zertifikat, das bald abläuft.

Alarmname	Beschreibung und empfohlene Aktionen
<p>Ablauf des Endpunktzertifikats des Load Balancer</p>	<p>Ein oder mehrere Load Balancer-Endpunktzertifikate laufen kurz vor dem Ablauf.</p> <ol style="list-style-type: none"> 1. Wählen Sie KONFIGURATION Netzwerk Load Balancer-Endpunkte aus. 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. <p>Weitere Informationen zum Verwalten von Endpunkten für den Load Balancer finden Sie im Anweisungen für die Administration von StorageGRID.</p>
<p>Ablauf des Serverzertifikats für die Managementoberfläche</p>	<p>Das für die Managementoberfläche verwendete Serverzertifikat läuft bald ab.</p> <ol style="list-style-type: none"> 1. Wählen Sie KONFIGURATION Sicherheit Zertifikate. 2. Wählen Sie auf der Registerkarte Global die Option Management Interface Certificate aus. 3. Laden Sie ein neues Zertifikat für die Managementoberfläche hoch.
<p>Ablauf des globalen Serverzertifikats für S3 und Swift API</p>	<p>Das Serverzertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, läuft bald ab.</p> <ol style="list-style-type: none"> 1. Wählen Sie KONFIGURATION Sicherheit Zertifikate. 2. Wählen Sie auf der Registerkarte Global S3 und Swift API Zertifikat. 3. Laden Sie ein neues S3- und Swift-API-Zertifikat hoch.
<p>Ablauf des externen Syslog CA-Zertifikats</p>	<p>Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des externen Syslog-Serverzertifikats verwendet wird, läuft in Kürze ab.</p> <ol style="list-style-type: none"> 1. Aktualisieren des CA-Zertifikats auf dem externen Syslog-Server. 2. Holen Sie sich eine Kopie des aktualisierten CA-Zertifikats. 3. Gehen Sie vom Grid Manager zu KONFIGURATION Überwachung Audit- und Syslog-Server. 4. Wählen Sie externen Syslog-Server bearbeiten. 5. Wählen Sie Durchsuchen, um das neue Zertifikat hochzuladen. 6. Schließen Sie den Konfigurationsassistenten ab, um das neue Zertifikat und den neuen Schlüssel zu speichern.

Alarmname	Beschreibung und empfohlene Aktionen
Ablauf des externen Syslog-Client-Zertifikats	<p>Das Client-Zertifikat für einen externen Syslog-Server läuft kurz vor dem Ablauf.</p> <ol style="list-style-type: none"> 1. Gehen Sie vom Grid Manager zu KONFIGURATION Überwachung Audit- und Syslog-Server. 2. Wählen Sie externen Syslog-Server bearbeiten. 3. Wählen Sie Durchsuchen, um das neue Zertifikat hochzuladen. 4. Wählen Sie Durchsuchen, um den neuen privaten Schlüssel hochzuladen. 5. Schließen Sie den Konfigurationsassistenten ab, um das neue Zertifikat und den neuen Schlüssel zu speichern.
Ablauf des externen Syslog-Serverzertifikats	<p>Das vom externen Syslog-Server präsentierte Serverzertifikat läuft bald ab.</p> <ol style="list-style-type: none"> 1. Aktualisieren des Serverzertifikats auf dem externen Syslog-Server 2. Wenn Sie zuvor die Grid Manager API verwendet haben, um ein Serverzertifikat zur Zertifikatvalidierung bereitzustellen, laden Sie das aktualisierte Serverzertifikat mithilfe der API hoch.
Fehler bei der Weiterleitung des externen Syslog-Servers	<p>Der Node kann Protokolle nicht an den externen Syslog-Server weiterleiten.</p> <ol style="list-style-type: none"> 1. Gehen Sie vom Grid Manager zu KONFIGURATION Überwachung Audit- und Syslog-Server. 2. Wählen Sie externen Syslog-Server bearbeiten. 3. Fahren Sie mit dem Konfigurationsassistenten fort, bis Sie Testmeldungen senden auswählen können. 4. Wählen Sie Testmeldungen senden aus, um festzustellen, warum Protokolle nicht an den externen Syslog-Server weitergeleitet werden können. 5. Beheben Sie alle gemeldeten Probleme.
MTU-Diskrepanz bei dem Grid-Netzwerk	<p>Die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) unterscheidet sich deutlich von den Knoten im Grid.</p> <p>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.</p> <p>Siehe die Anleitung für die Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU in Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen.</p>

Alarmname	Beschreibung und empfohlene Aktionen
Hohe Java-Heap-Nutzung	<p>Es wird ein hoher Prozentsatz von Java Heap Space verwendet.</p> <p>Wenn der Java-Heap voll ist, können Metadatendienste nicht verfügbar sein und Clientanforderungen können fehlschlagen.</p> <ol style="list-style-type: none"> 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	<p>Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang.</p> <p>Eine höhere Abfragelatenz kann durch eine Hardware-Änderung verursacht werden, wie z. B. den Austausch einer Festplatte, eine Workload-Änderung wie die plötzliche Zunahme der Einspeisung oder eine Netzwerkänderung, wie etwa ein Kommunikationsproblem zwischen Nodes und Standorten.</p> <ol style="list-style-type: none"> 1. Ermitteln Sie, ob Hardware-, Workload- oder Netzwerkänderungen vorhanden sind, während die Abfragelatenz erhöht wurde. 2. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.
Synchronisierungsfehler bei der Identitätsföderation	<p>Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren.</p> <ol style="list-style-type: none"> 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 Verwenden Sie den Identitätsverbund Lesen Sie unter Anleitung zum Verwalten 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.

Alarmname	Beschreibung und empfohlene Aktionen
Fehler bei der Synchronisierung der Identitätsföderation für einen Mandanten	<p>Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren, die von einem Mandanten konfiguriert wurde.</p> <ol style="list-style-type: none"> 1. Melden Sie sich beim Tenant Manager an. 2. Vergewissern Sie sich, dass der vom Mandanten konfigurierte LDAP-Server online und verfügbar ist. 3. Überprüfen Sie die Einstellungen auf der Seite Identity Federation. Vergewissern Sie sich, dass alle Werte aktuell sind. Siehe Verwenden Sie den Identitätsverbund In den Anweisungen zur Verwendung eines Mandantenkontos. 4. Klicken Sie auf Verbindung testen, um die Einstellungen für den LDAP-Server zu validieren. 5. Wenden Sie sich an den technischen Support, wenn das Problem nicht gelöst werden kann.
ILM-Platzierung nicht erreichbar	<p>Für bestimmte Objekte kann keine Platzierung in einer ILM-Regel erzielt werden.</p> <p>Diese Meldung gibt an, dass ein für einen Speicherungsanweisung 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.</p> <ol style="list-style-type: none"> 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. Siehe Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management. 3. Aktualisieren Sie bei Bedarf die Regeleinstellungen und aktivieren Sie eine neue Richtlinie. <p>Hinweis: Es kann bis zu 1 Tag dauern, bis der Alarm gelöscht wird.</p> <ol style="list-style-type: none"> 4. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. <p>Hinweis: dieser Alarm kann während eines Upgrades angezeigt werden und kann einen Tag nach dem erfolgreichen Abschluss des Upgrades bestehen. Wenn diese Warnung durch ein Upgrade ausgelöst wird, wird sie von selbst gelöscht.</p>

Alarmname	Beschreibung und empfohlene Aktionen
Der ILM-Scan ist zu lang	<p>Der Zeitaufwand für das Scannen, Bewerten von Objekten und Anwenden von ILM ist zu lang.</p> <p>Wenn die geschätzte Zeit für die Durchführung eines vollständigen ILM-Scans aller Objekte zu lang ist (siehe Scan Period - Estimated im Dashboard), wird die aktive ILM-Richtlinie möglicherweise nicht auf neu aufgenommene Objekte angewendet. Änderungen der ILM-Richtlinie werden möglicherweise nicht auf vorhandene Objekte angewendet.</p> <ol style="list-style-type: none"> 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 zum Beispiel im Grid Manager die Option KONFIGURATION Netzwerk 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. <p>StorageGRID verwalten</p>
ILM-Scan-Rate niedrig	<p>Die ILM-Scan-Rate ist auf weniger als 100 Objekte/Sekunde eingestellt.</p> <p>Diese Warnung zeigt an, dass jemand die ILM-Scanrate 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.</p> <ol style="list-style-type: none"> 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. <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Ändern Sie nie die ILM-Scanrate, ohne den technischen Support zu kontaktieren.</p> </div>

Alarmname	Beschreibung und empfohlene Aktionen
ABLAUF DES KMS-CA-Zertifikats	<p>Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des KMS-Zertifikats (Key Management Server) verwendet wird, läuft bald ab.</p> <ol style="list-style-type: none"> 1. Aktualisieren Sie mithilfe der KMS-Software das CA-Zertifikat für den Schlüsselverwaltungsserver. 2. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit 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. <p>StorageGRID verwalten</p>
ABLAUF DES KMS-Clientzertifikats	<p>Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft bald ab.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit 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. <p>StorageGRID verwalten</p>
KMS-Konfiguration konnte nicht geladen werden	<p>Es ist die Konfiguration für den Verschlüsselungsmanagement-Server vorhanden, konnte aber nicht geladen werden.</p> <ol style="list-style-type: none"> 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	<p>Ein Appliance-Node konnte keine Verbindung zum Schlüsselmanagementserver für seinen Standort herstellen.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit 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	<p>Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt.</p> <ol style="list-style-type: none"> 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	<p>Alle Appliance-Volumes wurden entschlüsselt, aber ein oder mehrere Volumes konnten nicht auf den neuesten Schlüssel rotieren. Kontaktieren Sie den technischen Support.</p>
KM ist nicht konfiguriert	<p>Für diesen Standort ist kein Schlüsselverwaltungsserver vorhanden.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit Schlüsselverwaltungsserver aus. 2. Fügen Sie für diese Site einen KMS hinzu oder fügen Sie einen Standard-KMS hinzu. <p>StorageGRID verwalten</p>

Alarmname	Beschreibung und empfohlene Aktionen
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	<p>Ein oder mehrere Volumes auf einer Appliance mit aktivierter Node-Verschlüsselung konnten nicht mit dem aktuellen KMS-Schlüssel entschlüsselt werden.</p> <ol style="list-style-type: none"> 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	<p>Das vom KMS (Key Management Server) verwendete Serverzertifikat läuft in Kürze ab.</p> <ol style="list-style-type: none"> 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. <p>StorageGRID verwalten</p>
Große Audit-Warteschlange	<p>Die Datenträgerwarteschlange für Überwachungsmeldungen ist voll.</p> <ol style="list-style-type: none"> 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 Client-Schreibvorgänge auf Fehler oder aus lesen (KONFIGURATION Überwachung Audit- und Syslog-Server). <p>Prüfung von Audit-Protokollen</p>

Alarmname	Beschreibung und empfohlene Aktionen
<p>Aktivität des Legacy-CLB-Load-Balancer erkannt</p>	<p>Einige Clients stellen möglicherweise eine Verbindung zum veralteten CLB-Load-Balancer-Service mithilfe des S3- und Swift-API-Standardzertifikats her.</p> <ol style="list-style-type: none"> 1. Um zukünftige Upgrades zu vereinfachen, installieren Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat auf der Registerkarte Global der Seite Zertifikate. Stellen Sie anschließend sicher, dass alle S3- oder Swift-Clients, die sich mit dem älteren CLB verbinden, über das neue Zertifikat verfügen. 2. Erstellen Sie einen oder mehrere Load Balancer-Endpunkte. Anschließend leiten Sie alle vorhandenen S3- und Swift-Clients an diese Endpunkte weiter. Wenden Sie sich an den technischen Support, wenn Sie den Client-Port neu zuordnen müssen. <p>Eine andere Aktivität kann diese Warnmeldung auslösen, einschließlich Port-Scans. Um festzustellen, ob der veraltete CLB-Dienst derzeit verwendet wird, zeigen Sie die an <code>storagegrid_private_clb_http_connection_established_successful</code> Prometheus metrisch.</p> <p>Falls erforderlich, deaktivieren Sie diese Warnregel, wenn der CLB-Dienst nicht mehr verwendet wird.</p>
<p>Protokolle werden der Warteschlange auf der Festplatte hinzugefügt</p>	<p>Der Node kann Protokolle nicht an den externen Syslog-Server weiterleiten, und die Warteschlange auf der Festplatte wird ausgefüllt.</p> <ol style="list-style-type: none"> 1. Gehen Sie vom Grid Manager zu KONFIGURATION Überwachung Audit- und Syslog-Server. 2. Wählen Sie externen Syslog-Server bearbeiten. 3. Fahren Sie mit dem Konfigurationsassistenten fort, bis Sie Testmeldungen senden auswählen können. 4. Wählen Sie Testmeldungen senden aus, um festzustellen, warum Protokolle nicht an den externen Syslog-Server weitergeleitet werden können. 5. Beheben Sie alle gemeldeten Probleme.
<p>Geringe Kapazität der Auditprotokoll-Festplatte</p>	<p>Der für Audit-Protokolle verfügbare Platz ist gering.</p> <ol style="list-style-type: none"> 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 verfügbarer Node-Speicher	<p>Die RAM-Menge, die auf einem Knoten verfügbar ist, ist gering.</p> <p>Ein wenig verfügbarer RAM kann auf eine Änderung der Arbeitslast oder ein Speicherleck bei einem oder mehreren Knoten hinweisen.</p> <ol style="list-style-type: none"> Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. Wenn der verfügbare Speicher unter den Hauptwarnschwellenwert fällt, wenden Sie sich an den technischen Support.
Wenig freier Speicherplatz für den Speicherpool	<p>Der Speicherplatz, der zur Speicherung von Objektdaten in einem Speicherpool verfügbar ist, ist gering.</p> <ol style="list-style-type: none"> Wählen Sie ILM Storage Pools aus. Wählen Sie den Speicherpool aus, der in der Warnmeldung aufgeführt ist, und wählen Sie Details anzeigen. 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. Führen Sie ein Erweiterungsverfahren durch, um die Speicherkapazität zu erhöhen. <p>Erweitern Sie Ihr Raster</p>
Wenig installierter Node-Speicher	<p>Der installierte Arbeitsspeicher auf einem Node ist gering.</p> <p>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:</p> <ul style="list-style-type: none"> Installieren Sie Red hat Enterprise Linux oder CentOS Installieren Sie Ubuntu oder Debian VMware installieren

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger Metadaten-Storage	<p>Der zur Speicherung von Objektmetadaten verfügbare Speicherplatz ist gering.</p> <p>Kritischer Alarm</p> <ol style="list-style-type: none"> 1. Die Aufnahme von Objekten beenden. 2. Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. <p>Großalarm</p> <p>Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt.</p> <ul style="list-style-type: none"> • Kleine Warnung* <ol style="list-style-type: none"> 1. Überwachen Sie die Rate, mit der Objekt-Metadaten Speicherplatz verwendet wird. Wählen Sie NODES Storage Node Storage aus, und zeigen Sie das Diagramm verwendete Speicherdaten - Objektmetadaten an. 2. Fügen Sie Storage-Nodes in einem hinzu Expansionsverfahren So bald wie möglich. <p>Sobald neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht.</p> <p>Siehe Anweisungen für die Warnmeldung zu niedrigem Metadaten-Speicher in Behebung von Metadatenproblemen.</p>
Niedrige Kenngrößen für die Festplattenkapazität	<p>Der für die Kennzahlendatenbank verfügbare Speicherplatz ist gering.</p> <ol style="list-style-type: none"> 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 Objekt-Storage	<p>Der zum Speichern von Objektdaten verfügbare Platz ist gering.</p> <p>Eine Erweiterung durchführen. Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen.</p> <p>Beheben Sie die Warnung „Niedrig Object Data Storage“</p> <p>Erweitern Sie Ihr Raster</p>

Alarmname	Beschreibung und empfohlene Aktionen
Low Read-Only-Wasserzeichen überschreiben	<p>Der Speichervolumen Soft Read-Only-Wasserzeichen-Überschreiben ist kleiner als der für einen Speicherknoten optimierte Mindestwert.</p> <p>Informationen zum Beheben dieser Warnmeldung finden Sie unter Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff.</p>
Niedrige Root-Festplattenkapazität	<p>Der für die Root-Festplatte verfügbare Speicherplatz ist gering.</p> <ol style="list-style-type: none"> Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedrige Datenkapazität des Systems	<p>Der Speicherplatz, der für StorageGRID-Systemdaten auf verfügbar ist <code>/var/local</code> Das Dateisystem ist niedrig.</p> <ol style="list-style-type: none"> Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Geringer Tmp-Telefonspeicherplatz	<p>Der im Verzeichnis <code>/tmp</code> verfügbare Speicherplatz ist gering.</p> <ol style="list-style-type: none"> Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Fehler bei der Node-Netzwerkverbindung	<p>Beim Übertragen der Daten zwischen den Nodes ist ein Fehler aufgetreten.</p> <p>Fehler mit der Netzwerkverbindung können ohne manuelles Eingreifen behoben werden. Wenden Sie sich an den technischen Support, wenn die Fehler nicht behoben sind.</p> <p>Siehe die Anweisungen für den NRER-Alarm (Network Receive Error) in Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen.</p>

Alarmname	Beschreibung und empfohlene Aktionen
Node-Netzwerkannahme-Frame-Fehler	<p>Bei einem hohen Prozentsatz der Netzwerkframes, die von einem Node empfangen wurden, gab es Fehler.</p> <p>Diese Meldung weist möglicherweise auf ein Hardwareproblem hin, z. B. auf ein schlechtes Kabel oder auf einen fehlerhaften Transceiver an beiden Enden der Ethernet-Verbindung.</p> <ol style="list-style-type: none"> 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	<p>Die Zeit des Node ist nicht mit dem NTP-Server (Network Time Protocol) synchronisiert.</p> <ol style="list-style-type: none"> 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	<p>Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt.</p> <ol style="list-style-type: none"> 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	<p>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.</p> <p>Wenden Sie sich an den technischen Support.</p>

Alarmname	Beschreibung und empfohlene Aktionen
Überprüfung der Objektexistenz fehlgeschlagen	<p>Der Job für die Objektexistenzprüfung ist fehlgeschlagen.</p> <ol style="list-style-type: none"> 1. Wählen Sie Prüfung der Existenz DES WARTUNGSOBJEKTS aus. 2. Notieren Sie die Fehlermeldung. Führen Sie die entsprechenden Korrekturmaßnahmen durch: <ul style="list-style-type: none"> Start fehlgeschlagen, Verbindung verloren, Unbekannter Fehler <ol style="list-style-type: none"> a. Stellen Sie sicher, dass die im Job enthaltenen Speicherknoten und -Volumes online und verfügbar sind. b. Stellen Sie sicher, dass auf den Storage-Nodes keine Service- oder Volume-Ausfälle auftreten. Wenn ein Dienst nicht ausgeführt wird, starten Sie den Dienst oder starten Sie ihn neu. Siehe Anweisungen zur Wiederherstellung und Wartung. c. Stellen Sie sicher, dass die ausgewählte Consistency Control erfüllt werden kann. d. Wählen Sie nach der Behebung von Problemen Wiederholen aus. Der Job wird vom letzten gültigen Status wieder aufgenommen. Kritischer Speicherfehler im Volumen <ol style="list-style-type: none"> e. Stellen Sie das ausgefallene Volume wieder her. Siehe Anweisungen zur Wiederherstellung und Wartung. f. Wählen Sie Wiederholen. g. Erstellen Sie nach Abschluss des Jobs einen weiteren Job für die verbleibenden Volumes auf dem Node, um auf zusätzliche Fehler zu überprüfen. 3. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Prüfung der ObjektExistenz ist blockiert	<p>Der Job zur Prüfung der ObjektExistenz ist blockiert.</p> <p>Der Job für die Überprüfung der Objektexistenz kann nicht fortgesetzt werden. Entweder sind ein oder mehrere Storage-Nodes oder Volumes im Job offline oder nicht mehr reagiert, oder das ausgewählte Konsistenzelement kann nicht mehr zufriedenstellend sein, da zu viele Nodes ausgefallen sind oder nicht mehr verfügbar sind.</p> <ol style="list-style-type: none"> 1. Stellen Sie sicher, dass alle zu prüfenden Speicherknoten und Volumes online und verfügbar sind (wählen Sie KNOTEN). 2. Stellen Sie sicher, dass genügend Storage-Nodes online und verfügbar sind, damit der aktuelle Koordinator-Node mithilfe der ausgewählten Konsistenzsteuerung Objektmetadaten lesen kann. Starten oder starten Sie ggf. einen Dienst neu. Siehe Anweisungen zur Wiederherstellung und Wartung. <p>Wenn Sie die Schritte 1 und 2 lösen, beginnt der Job automatisch an der Stelle, an der er aufging.</p> <ol style="list-style-type: none"> 3. Wenn das ausgewählte Consistency Control nicht erfüllt werden kann, brechen Sie den Job ab und starten Sie einen anderen Job mit einer niedrigeren Consistency Control. 4. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.
Objekte verloren	<p>Mindestens ein Objekt ist aus dem Raster verloren gegangen.</p> <p>Diese Meldung kann darauf hindeuten, dass Daten dauerhaft verloren gegangen sind und nicht wieder abgerufen werden können.</p> <ol style="list-style-type: none"> 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. <p>Fehlerbehebung bei verlorenen und fehlenden Objektdaten</p> <ol style="list-style-type: none"> 2. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück: <ol style="list-style-type: none"> a. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. b. Wählen Sie für den Speicherknoten, der die Warnung erhöht hat site Grid Node LDR Data Store Konfiguration Main aus. c. Wählen Sie Anzahl der verlorenen Objekte zurücksetzen und klicken Sie auf Änderungen anwenden.

Alarmname	Beschreibung und empfohlene Aktionen
Plattform-Services nicht verfügbar	<p>Zu wenige Speicherknoten mit dem RSM-Service laufen oder sind an einem Standort verfügbar.</p> <p>Stellen Sie sicher, dass die meisten Speicherknoten, die den RSM-Dienst am betroffenen Standort haben, ausgeführt werden und sich nicht fehlerfrei befinden.</p> <p>Siehe „Fehlerbehebung für Plattforddienste“ im Anweisungen für die Administration von StorageGRID.</p>
S3 PUT Objektgröße zu groß	<p>Ein S3-Client versucht, einen PUT-Objektvorgang auszuführen, der die S3-Größenlimits überschreitet.</p> <ol style="list-style-type: none"> 1. Verwenden Sie die Mandanten-ID, die in den Alarmdetails angegeben ist, um das Mandantenkonto zu identifizieren. 2. Gehen Sie zu Support Tools Logs und sammeln Sie die Anwendungsprotokolle für den Speicherknoten, die in den Warndetails angezeigt werden. Geben Sie einen Zeitraum an, der 15 Minuten vor und nach der Zeit der Warnmeldung liegt. 3. Extrahieren Sie das heruntergeladene Archiv, und navigieren Sie zum Speicherort von <code>bycast.log</code> (<code>/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log</code>). 4. Durchsuchen Sie den Inhalt von <code>bycast.log</code> Für "method=PUT" Und identifizieren Sie die IP-Adresse des S3-Clients, indem Sie den betrachten <code>clientIP</code> Feld. 5. Informieren Sie alle Client-Benutzer, dass die maximale PUT-Objektgröße 5 gib beträgt. 6. Verwenden Sie mehrteilige Uploads für Objekte mit einer Größe von mehr als 5 gib.
Services-Appliance-Verbindung am Admin-Netzwerkanschluss 1 getrennt	<p>Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden.</p> <ol style="list-style-type: none"> 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 ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
Services-Appliance-Link im Admin-Netzwerk (oder Client-Netzwerk) herunter	<p>Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden.</p> <ol style="list-style-type: none"> 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 ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ Deaktivieren von Meldungsregeln
Services-Appliance-Verbindung an Netzwerkport 1, 2, 3 oder 4 getrennt	<p>Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden.</p> <ol style="list-style-type: none"> 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 ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. <ul style="list-style-type: none"> ◦ SG100- und SG1000-Services-Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
<p>Die Speicherkonnektivität der Services-Appliance ist herabgesetzt</p>	<p>Eine der beiden SSDs in einer Services-Appliance ist ausgefallen oder nicht mit der anderen synchronisiert.</p> <p>Die Funktionalität der Appliance ist nicht beeinträchtigt, Sie sollten das Problem jedoch sofort beheben. Wenn beide Laufwerke ausfallen, funktioniert die Appliance nicht mehr.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option NODES Services Appliance und 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. <p>Anweisungen zum Austauschen eines Laufwerks in einer Services Appliance finden Sie im Installations- und Wartungshandbuch für SG100- und SG1000-Geräte.</p> <p>SG100- und SG1000-Services-Appliances</p>
<p>Verknüpfung der Speicher-Appliance auf Admin-Netzwerk-Port 1 ausgefallen</p>	<p>Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden.</p> <ol style="list-style-type: none"> 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 ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
<p>Link der Storage Appliance ist im Admin-Netzwerk (oder Client-Netzwerk) inaktiv.</p>	<p>Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden.</p> <ol style="list-style-type: none"> 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 ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ Deaktivieren von Meldungsregeln
<p>Verbindung der Storage Appliance über Netzwerkport 1, 2, 3 oder 4 getrennt</p>	<p>Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden.</p> <ol style="list-style-type: none"> 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 ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
Die Storage-Konnektivität der Storage-Appliance ist herabgesetzt	<p>Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller.</p> <ol style="list-style-type: none"> 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. <p>Hinweis: Wenn ein zweites Kabel ersetzt werden muss, ziehen Sie es mindestens 5 Minuten nicht ab. Andernfalls kann das Root-Volume schreibgeschützt sein und die Hardware neu starten.</p> <ol style="list-style-type: none"> 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.
Speichergerät nicht zugänglich	<p>Auf ein Speichergerät kann nicht zugegriffen werden.</p> <p>Diese Meldung gibt an, dass ein Volume nicht angehängt oder auf dieses zugegriffen werden kann, weil ein Problem mit einem zugrunde liegenden Speichergerät vorliegt.</p> <ol style="list-style-type: none"> 1. Überprüfen Sie den Status aller für den Knoten verwendeten Speichergeräte: <ul style="list-style-type: none"> ◦ 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. <ul style="list-style-type: none"> ▪ 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. Beachten Sie die Anweisungen für Ihr Gerät: <ul style="list-style-type: none"> ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Hohe Kontingentnutzung für Mandanten	<p>Ein hoher Prozentsatz des Kontingentspeichers wird verwendet. Wenn ein Mieter seine Quote überschreitet, werden Neuanlässe abgelehnt.</p> <p>Hinweis: Diese Alarmregel ist standardmäßig deaktiviert, da sie viele Benachrichtigungen erzeugen kann.</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ◦ Wählen Sie Bearbeiten, um das Speicherkontingent für den Mieter zu erhöhen. ◦ Benachrichtigen Sie den Mandanten, dass seine Kontingentauslastung hoch ist.
Kommunikation mit Knoten nicht möglich	<p>Mindestens ein Service reagiert nicht oder der Node kann nicht erreicht werden.</p> <p>Diese Warnmeldung gibt an, dass ein Knoten aus einem unbekanntem 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.</p> <p>Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. Wenn das Problem weiterhin besteht:</p> <ol style="list-style-type: none"> 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. Siehe Anweisungen zur Wiederherstellung und Wartung. 3. Stellen Sie sicher, dass der Host für den Node eingeschaltet ist. Falls nicht, starten Sie den Host. <p>Hinweis: Wenn mehr als ein Host ausgeschaltet ist, lesen Sie den Anweisungen zur Wiederherstellung und Wartung.</p> <ol style="list-style-type: none"> 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.

Alarmname	Beschreibung und empfohlene Aktionen
Unerwarteter Node-Neustart	<p>Ein Node wurde in den letzten 24 Stunden unerwartet neu gebootet.</p> <ol style="list-style-type: none"> Überwachen Sie diesen Alarm. Der Alarm wird nach 24 Stunden gelöscht. Wenn der Node jedoch unerwartet neu gebootet wird, wird die Warnmeldung erneut ausgelöst. Wenn Sie die Meldung nicht beheben können, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.
Nicht identifizierte beschädigte Objekte erkannt	<p>Im replizierten Objekt-Storage wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte.</p> <ol style="list-style-type: none"> 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. Nach der Lösung von Storage-Problemen Überprüfung der ObjektExistenz ausführen Um festzustellen, ob replizierte Kopien, wie in Ihren ILM-Richtlinien definiert, fehlen. Überwachen Sie diesen Alarm. Die Warnmeldung wird nach 24 Stunden gelöscht, wird jedoch erneut ausgelöst, wenn das Problem noch nicht behoben wurde. Wenn Sie die Meldung nicht beheben können, wenden Sie sich an den technischen Support.

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.

Metriken werden auf jedem Admin-Node gespeichert, bis der für Prometheus-Daten reservierte Speicherplatz voll ist. Wenn der `/var/local/mysql_ibdata/` Volume erreicht die Kapazität, zuerst werden die ältesten Metriken gelöscht.

Um die vollständige Liste der Metriken zu erhalten, verwenden Sie die Grid Management API.

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

Die folgende Tabelle enthält die am häufigsten verwendeten Prometheus-Kennzahlen. Sie können diese Liste nutzen, um die Bedingungen in den Standardwarnregeln besser zu verstehen oder die Bedingungen für benutzerdefinierte Alarmregeln zu erstellen.



Metriken, die *privat* in ihren Namen enthalten, sind nur zur internen Verwendung vorgesehen und können ohne Ankündigung zwischen StorageGRID Versionen geändert werden.

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.

Prometheus metrisch	Beschreibung
storagegrid_Content_Objects_Lost	<p>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.</p> <p>Fehlerbehebung bei verlorenen und fehlenden Objektdaten</p>
storagegrid_http_Sessions_Incoming_versuchte	Die Gesamtzahl der HTTP-Sitzungen, die zu einem Speicherknoten versucht wurden.
storagegrid_http_Sessions_Incoming_derzeit_etabliertes	Die Anzahl der derzeit aktiven HTTP-Sitzungen (offen) auf dem Speicherknoten.
storagegrid_http_Sessions_INCOMING_FAILED	Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen wurden, entweder aufgrund einer fehlerhaften HTTP-Anfrage oder aufgrund eines Fehlers bei der Verarbeitung eines Vorgangs.
storagegrid_http_Sessions_Incoming_successful	Die Gesamtzahl der erfolgreich abgeschlossenen HTTP-Sitzungen.
storagegrid_ilm_awaiting_background_Objects	Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus dem Scan warten
storagegrid_ilm_awaiting_Client_Evaluation_Objects_per_Second	Die aktuelle Rate, mit der Objekte im Vergleich zur ILM-Richtlinie auf diesem Node bewertet werden.
storagegrid_ilm_awaiting_Client_Objects	Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus den Client-Vorgängen (z. B. Aufnahme) warten
storagegrid_ilm_awaiting_total_Objects	Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten
storagegrid_ilm_Scan_Objects_per_Second	Die Geschwindigkeit, mit der Objekte des Node gescannt und für ILM in der Warteschlange gestellt werden.
storagegrid_ilm_Scan_Period_Geschätzter_Minuten	<p>Die geschätzte Zeit zum Abschließen eines vollständigen ILM-Scans auf diesem Node.</p> <p>Hinweis: Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die sich im Besitz dieses Knotens befinden.</p>

Prometheus metrisch	Beschreibung
storagegrid_Load_Balancer_Endpoint_cert_expiry_time	Die Ablaufzeit des Endpunktzertifikats des Load Balancer in Sekunden seit der Epoche.
storagegrid_Metadatenabfragen_average_Latency_Millisekunden	Die durchschnittliche Zeit, die zum Ausführen einer Abfrage des MetadatenSpeichers über diesen Service benötigt wird.
storagegrid_Network_received_Byte	Die Gesamtmenge der seit der Installation empfangenen Daten.
storagegrid_Network_transmitted_Byte	Die Gesamtmenge der seit der Installation gesendeten Daten.
storagegrid_Node_cpu_Utilization_percent	Der Prozentsatz der verfügbaren CPU-Zeit, die derzeit von diesem Service genutzt wird. Gibt an, wie beschäftigt der Dienst ist. Die verfügbare CPU-Zeit hängt von der Anzahl der CPUs für den Server ab.
storagegrid_ntp_Chosen_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.

Prometheus metrisch	Beschreibung
storagegrid_Servercertifikat_Management_Interface_cert_expiry_days	Die Anzahl der Tage vor Ablauf des Managementschnittstelle-Zertifikats.
storagegrid_Servercertifikat_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_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_transmitted_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	<p>Der aktuelle Status der Storage-Services. Attributwerte sind:</p> <ul style="list-style-type: none"> • 10 = Offline • 15 = Wartung • 20 = schreibgeschützt • 30 = Online
storagegrid_Storage_Status	<p>Der aktuelle Status der Storage-Services. Attributwerte sind:</p> <ul style="list-style-type: none"> • 0 = Keine Fehler • 10 = In Transition • 20 = Nicht Genügend Freier Speicherplatz • 30 = Volume(s) nicht verfügbar • 40 = Fehler

Prometheus metrisch	Beschreibung
storagegrid_Storage_Utifficienfficienoy_Bytes	Schätzung der Gesamtgröße der replizierten und Erasure-codierten Objektdaten auf dem Storage-Node
storagegrid_Storage_Utiffici“_Metadata_allowed_Bytes	Der gesamte Speicherplatz auf Volume 0 jedes Storage-Node, der für Objekt-Metadaten zulässig ist. Dieser Wert ist immer kleiner als der tatsächlich für Metadaten auf einem Node reservierte Speicherplatz, da für grundlegende Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades ein Teil des reservierten Speicherplatzes benötigt wird. Der zulässige Speicherplatz für Objektmetadaten steuert die allgemeine Objektkapazität.
storagegrid_Storage_Utifficiendatij_Metadaten_Bytes	Die Menge der Objekt-Metadaten auf dem Storage-Volume 0 in Bytes.
storagegrid_Storage_Utifficienfficienals_total_space_Bytes	Der gesamte Speicherplatz, der allen Objektspeichern zugewiesen ist.
storagegrid_Storage_Utiabile_space_Bytes	Die verbleibende Menge an Objekt-Storage. Berechnet durch Hinzufügen der verfügbaren Menge an Speicherplatz für alle Objektspeichern auf dem Storage-Node.
storagegrid_Swift_Data_Transfers_Bytes_aufgenommen	Die Gesamtmenge der Daten, die Swift-Clients seit dem letzten Zurücksetzen des Attributs von diesem Storage-Node aufgenommen haben.
storagegrid_Swift_Data_Transfers_Bytes_abgerufen	Die Gesamtanzahl der Daten, die Swift-Clients von diesem Speicherknoten seit dem letzten Zurücksetzen des Attributs abgerufen haben.
storagegrid_Swift_Operations_fehlgeschlagen	Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge (HTTP-Statuscodes 4xx und 5xx), ausgenommen solche, die durch Swift-Autorisierungsfehler verursacht wurden.
storagegrid_Swift_Operations_erfolgreich	Die Gesamtzahl der erfolgreichen Swift-Vorgänge (HTTP-Statuscode 2xx).
storagegrid_Swift_Operations_nicht autorisiert	Die Gesamtzahl der fehlgeschlagenen Swift-Vorgänge, die auf einen Autorisierungsfehler zurückzuführen sind (HTTP-Statuscodes 401, 403, 405).

Prometheus metrisch	Beschreibung
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	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
ACMS	Verfügbare Metadaten	BARC, BLDR, BCMN	<p>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.</p> <p>Überprüfen und Wiederherstellen der Verbindungen zu einem DDS-Dienst, um diesen Alarm zu löschen und den Service auf die volle Funktionalität zurückzugeben.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
AKTE	Status Des Cloud Tiering Service	LICHTBOGEN	<p>Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Cloud Tiering - Simple Storage Service (S3).</p> <p>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.</p> <p>Wenn ein Hauptalarm aufgrund eines Authentifizierungsfehlers ausgelöst wird, überprüfen Sie ggf. die mit dem Ziel-Bucket verknüpften Anmeldeinformationen und aktualisieren Sie Werte.</p> <p>Wenn aus irgendeinem anderen Grund ein Großalarm ausgelöst wird, wenden Sie sich an den technischen Support.</p>
ADCA	ADC-Status	ADU	<p>Wenn ein Alarm ausgelöst wird, wählen Sie SUPPORT Tools Grid-Topologie. Wählen Sie dann site Grid Node ADC Übersicht Main und ADC Alarme Main, um die Ursache des Alarms zu bestimmen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
ADCE	ADC-Status	ADU	<p>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.</p> <p>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.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
AITE	Status Abrufen	BARC	<p>Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>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.</p> <p>Wenn der Wert des Status „Archivabrueve“ Offline lautet, versuchen Sie, den Status auf Online zu aktualisieren. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node ARC Abruf Konfiguration Main, wählen Sie Archiv Status abrufen Online, und klicken Sie auf Änderungen anwenden.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AITU	Status Abrufen	BARC	<p>Wenn der Wert für „Status abrufen“ als Zielfehler gilt, prüfen Sie das ausgewählte externe Archivspeichersystem auf Fehler.</p> <p>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.</p> <p>Wenn der Wert des Status „Archiv abrufen“ Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.</p>
ALIS	Eingehende Attributsitzungen	ADU	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ALOS	Ausgehende Attributsitzungen	ADU	Der ADC-Dienst verfügt über eine hohe Anzahl von Attributsitzungen und wird überlastet. Wenn dieser Alarm ausgelöst wird, wenden Sie sich an den technischen Support.
ALUR	Nicht Erreichbare Attributdatenbanken	ADU	Überprüfen Sie die Netzwerkverbindung mit dem NMS-Service, um sicherzustellen, dass der Dienst das Attribut-Repository kontaktieren kann. Wenn dieser Alarm ausgelöst wird und die Netzwerkverbindung gut ist, wenden Sie sich an den technischen Support.
AMQS	Audit-Nachrichten In Queued	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn Audit-Meldungen nicht sofort an ein Audit-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: <ul style="list-style-type: none"> • Hinweis: Mehr als 100,000 Nachrichten • Minor: Mindestens 500,000 Nachrichten • Major: Mindestens 2,000,000 Nachrichten • Kritisch: Mindestens 5,000,000 Nachrichten Wenn ein AMQS-Alarm ausgelöst wird, überprüfen Sie die Belastung des Systems. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen. In diesem Fall können Sie den Alarm ignorieren. Wenn der Alarm weiterhin besteht und der Schweregrad erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. Verringern Sie die Betriebsrate des Clients oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie den Audit-Level auf Fehler oder aus ändern. Siehe Konfigurieren von Überwachungsmeldungen und Protokollzielen .

Codieren	Name	Service	Empfohlene Maßnahmen
AOTE	Store State	BARC	<p>Nur verfügbar für Archive Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>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.</p> <p>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.</p>
AOTU	Speicherstatus	BARC	<p>Wenn der Wert des Speicherstatus „Sitzung verloren“ lautet, prüfen Sie, ob das externe Archivspeichersystem verbunden und online ist.</p> <p>Wenn der Wert von Zielfehler ist, überprüfen Sie das externe Archivspeichersystem auf Fehler.</p> <p>Wenn der Wert des Speicherstatus Unbekannter Fehler lautet, wenden Sie sich an den technischen Support.</p>
APMS	Storage Multipath-Konnektivität	SSM	<p>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:</p> <ol style="list-style-type: none"> 1. Schließen Sie das Kabel an, das keine Kontrollleuchten anzeigt, oder ersetzen Sie es. 2. Warten Sie eine bis fünf Minuten. <p>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.</p> <ol style="list-style-type: none"> 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	BOGENZUSTAN D	LICHTBOGEN	<p>Der ARC-Dienst verfügt über einen Standby-Status, bis alle ARC-Komponenten (Replikation, Speicher, Abrufen, Ziel) gestartet wurden. Dann geht es zu Online.</p> <p>Wenn der Wert des ARC-Status nicht von Standby auf Online übergeht, überprüfen Sie den Status der ARC-Komponenten.</p> <p>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.</p>
AROQ	Objekte In Queued	LICHTBOGEN	<p>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.</p> <p>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.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ARRF	Anfragefehler	LICHTBOGEN	<p>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.</p> <p>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.</p> <p>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.</p> <p>Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node ARC Abruf Konfiguration Main, wählen Sie Fehleranzahl der Anforderung zurücksetzen und klicken Sie auf Änderungen anwenden.</p>
ARRV	Verifizierungsfehler	LICHTBOGEN	<p>Wenden Sie sich an den technischen Support, um das Problem zu diagnostizieren und zu beheben.</p> <p>Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node ARC Abruf Konfiguration Main, wählen Sie Anzahl der fehlgeschlagene Verifikation zurücksetzen und klicken Sie auf Änderungen anwenden.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
ARVF	Speicherfehler	LICHTBOGEN	<p>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.</p> <p>Sobald das Problem behoben ist, das diesen Alarm ausgelöst hat, setzen Sie die Anzahl der Fehler zurück. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node ARC Abruf Konfiguration Main, wählen Sie Anzahl der fehlgeschlagene Store zurücksetzen und klicken Sie auf Änderungen anwenden.</p>
ASXP	Revisionsfreigaben	AMS	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AUMA	AMS-Status	AMS	<p>Wenn der Wert für AMS Status DB-Verbindungsfehler ist, starten Sie den Grid-Node neu.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
AUME	AMS-Status	AMS	<p>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.</p> <p>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.</p>
AUXS	Exportstatus Prüfen	AMS	<p>Wenn ein Alarm ausgelöst wird, beheben Sie das zugrunde liegende Problem und starten Sie dann den AMS-Dienst neu.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
HINZUFÜGEN	Anzahl Ausgefallener Speicher-Controller-Laufwerke	SSM	<p>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.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
BASF	Verfügbare Objektkennungen	CMN	<p>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.</p> <p>Wenden Sie sich an den technischen Support, um weitere Kennungen zuzuweisen.</p>
BASS	Identifizier Block Zuordnungsstatus	CMN	<p>Standardmäßig wird ein Alarm ausgelöst, wenn Objektkennungen nicht zugewiesen werden können, da ADC Quorum nicht erreicht werden kann.</p> <p>Die Zuweisung von Identifizier-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.</p> <p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
BRDT	Temperatur Im Computing-Controller-Chassis	SSM	<p>Ein Alarm wird ausgelöst, wenn die Temperatur des Compute-Controllers in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet.</p> <p>Prüfen Sie die Hardware-Komponenten und Umweltprobleme auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
BTSE	Uhrstatus	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
CAHP	Java Heap-Nutzung In Prozent	DDS	<p>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-Metadatenpeicher überschreitet. Überprüfen Sie die ILM-Aktivität im Dashboard, oder wählen Sie SUPPORT Tools Grid-Topologie und dann site Grid-Knoten DDS Ressourcen Übersicht Main.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
CAIH	Anzahl Der Verfügbaren Aufnahmeziele	CLB	Dieser Alarm ist veraltet.
CAQH	Anzahl Der Verfügbaren Ziele	CLB	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
CASA	Data Store-Status	DDS	<p>Wenn der Cassandra-Metadatenpeicher nicht mehr verfügbar ist, wird ein Alarm ausgelöst.</p> <p>Den Status von Cassandra überprüfen:</p> <ol style="list-style-type: none"> 1. Melden Sie sich beim Storage-Node als admin und an <code>su</code> Um das Root-Kennwort zu verwenden, das in der Datei <code>Passwords.txt</code> angegeben ist. 2. Geben Sie Ein: <code>service cassandra status</code> 3. Falls Cassandra nicht ausgeführt wird, starten Sie es neu: <code>service cassandra restart</code> <p>Dieser Alarm kann auch zeigen, dass der Metadatenpeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert.</p> <p>Weitere Informationen zur Fehlerbehebung im Alarm Services: Status - Cassandra (SVST) in Behebung von Metadatenproblemen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
FALL	Datenspeicherstatus	DDS	<p>Dieser Alarm wird während der Installation oder Erweiterung ausgelöst, um anzuzeigen, dass ein neuer Datenspeicher in das Raster eingespeist wird.</p>
CES	Eingehende Sitzungen – Eingerichtet	CLB	<p>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.</p>
CCNA	Computing-Hardware	SSM	<p>Dieser Alarm wird ausgelöst, wenn der Status der Hardware des Computing-Controllers in einer StorageGRID-Appliance zu beachten ist.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
CDLP	Belegter Speicherplatz Für Metadaten (Prozent)	DDS	<p>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.</p> <p>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. Siehe Erweitern Sie Ihr Raster.</p> <p>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.</p> <p>Hinweis: Wenden Sie sich an den technischen Support, wenn Sie keine Speicherknoten hinzufügen können.</p> <p>Nachdem neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht.</p> <p>Siehe auch Informationen zur Fehlerbehebung für die Warnmeldung zu niedrigem Metadaten-Speicher in Behebung von Metadatenproblemen.</p>
CLBA	CLB-Status	CLB	<p>Wenn ein Alarm ausgelöst wird, wählen Sie SUPPORT Tools Grid Topology und wählen Sie <i>site Grid Node CLB Übersicht Main</i> und CLB Alarme Main um die Ursache des Alarms zu ermitteln und das Problem zu beheben.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
CLBE	Der Status des CLB	CLB	<p>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.</p> <p>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.</p>
CMNA	CMN-Status	CMN	<p>Wenn der Wert von CMN Status Fehler ist, wählen Sie SUPPORT Tools Grid Topology und wählen Sie site Grid Node CMN Übersicht Main und CMN Alarme Main aus, um die Fehlerursache zu ermitteln und das Problem zu beheben.</p> <p>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).</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
CPRC	Verbleibende Kapazität	NMS	<p>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.</p> <p>Wenn ein Alarm ausgelöst wird, wenden Sie sich an den technischen Support.</p>
CPSA	Compute Controller Netzteil A	SSM	<p>Wenn ein Problem mit der Stromversorgung A im Rechencontroller eines StorageGRID-Geräts auftritt, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p>
CPSB	Compute Controller Netzteil B	SSM	<p>Bei einem StorageGRID-Gerät wird ein Alarm ausgelöst, wenn ein Problem mit der Stromversorgung B im Compute-Controller auftritt.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
KFUT	CPU-Temperatur für Compute Controller	SSM	<p>Ein Alarm wird ausgelöst, wenn die Temperatur der CPU im Compute-Controller in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet.</p> <p>Wenn es sich bei dem Speicherknoten um eine StorageGRID-Appliance handelt, gibt das StorageGRID-System an, dass eine Warnung für den Controller erforderlich ist.</p> <p>Prüfen Sie die Probleme mit den Hardwarekomponenten und der Umgebung auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.</p>
DNST	DNS-Status	SSM	<p>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.</p>
ECCD	Beschädigte Fragmente Erkannt	LDR	<p>Ein Alarm wird ausgelöst, wenn die Hintergrundüberprüfung ein korruptes Fragment mit Lösungscode 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 Lösungscode wird erst dann als fehlend betrachtet, wenn die Anzahl der verlorenen oder korrupten Fragmente die Fehlertoleranz des Lösungscode verletzt. Daher ist es möglich, ein korruptes Fragment zu haben und das Objekt trotzdem abrufen zu können.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
ACST	Verifizierungsstatus	LDR	<p>Dieser Alarm zeigt den aktuellen Status des Hintergrundverifizierungsverfahrens für das Löschen codierter Objektdaten auf diesem Speicherknoten an.</p> <p>Bei der Hintergrundüberprüfung wird ein Großalarm ausgelöst.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
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.
HSTU	HTTP-Status	BLDR	<p>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:</p> <ul style="list-style-type: none"> • Das HTTP-Protokoll wurde manuell in den Offline-Modus versetzt. • Das Attribut Auto-Start HTTP wurde deaktiviert. • Der LDR-Service wird heruntergefahren. <p>Das Attribut Auto-Start HTTP ist standardmäßig aktiviert. Wenn diese Einstellung geändert wird, kann HTTP nach einem Neustart offline bleiben.</p> <p>Warten Sie gegebenenfalls, bis der LDR-Service neu gestartet wurde.</p> <p>Wählen Sie SUPPORT Tools Grid-Topologie 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.</p> <p>Wenden Sie sich an den technischen Support, wenn das HTTP-Protokoll offline bleibt.</p>
HTAS	Automatisches Starten von HTTP	LDR	Gibt an, ob HTTP-Dienste beim Start automatisch gestartet werden sollen. Dies ist eine vom Benutzer angegebene Konfigurationsoption.
IRSU	Status Der Eingehenden Replikation	BLDR, BARC	Ein Alarm zeigt an, dass die eingehende Replikation deaktiviert wurde. Konfigurationseinstellungen bestätigen: Wählen Sie SUPPORT Tools Grid-Topologie . Wählen Sie dann site Grid Node LDR Replikation Konfiguration Main aus.

Codieren	Name	Service	Empfohlene Maßnahmen
LATA	Durchschnittliche Latenz	NMS	<p>Überprüfen Sie auf Verbindungsprobleme.</p> <p>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.</p> <p>Auf mehrere Alarmer prüfen. Eine Erhöhung der durchschnittlichen Latenzzeit kann durch eine übermäßige Anzahl von ausgelösten Alarmen angezeigt werden.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
LDRE	LDR-Status	LDR	<p>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.</p> <p>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.</p>
VERLOREN	Verlorene Objekte	DDS, LDR	<p>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.</p> <p>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.</p> <p>Untersuchen SIE VERLORENE (VERLORENE Objekte) Alarme sofort. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p> <p>Fehlerbehebung bei verlorenen und fehlenden Objektdaten</p>

Codieren	Name	Service	Empfohlene Maßnahmen
MCEP	Ablauf Des Managementschnittstelle-Zertifikats	CMN	<p>Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf die Managementoberfläche verwendet wird, kurz vor Ablauf steht.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit Zertifikate. 2. Wählen Sie auf der Registerkarte Global die Option Management Interface Certificate aus. 3. Laden Sie ein neues Zertifikat für die Managementoberfläche hoch.
MINQ	E-Mail-Benachrichtigungen in Warteschlange	NMS	<p>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.</p> <p>E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)</p>
MIN	E-Mail-Benachrichtigungsstatus	BNMS	<p>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.</p> <p>E-Mail-Servereinstellungen für Alarme konfigurieren (Legacy-System)</p>
MISS	Status der NMS-Schnittstellen-Engine	BNMS	<p>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.</p>
NANG	Einstellung Für Automatische Netzwerkaushandlung	SSM	<p>Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen.</p> <p>Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.</p>

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: <ul style="list-style-type: none"> • Fehler bei der Vorwärtskorrektur (FEC) stimmen nicht überein • Switch-Port und MTU-NIC stimmen nicht überein • Hohe Link-Fehlerraten • NIC-Klingelpuffer überlaufen Weitere Informationen zur Fehlerbehebung im NRER-Alarm (Network Receive Error) in finden Sie unter Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen .
NRLY	Verfügbare Audit-Relais	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn 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.

Codieren	Name	Service	Empfohlene Maßnahmen
NSCE	Bundesland des NMS	NMS	<p>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.</p> <p>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.</p>
NSPD	Schnell	SSM	<p>Dies kann durch Probleme mit der Netzwerkverbindung oder der Treiberkompatibilität verursacht werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
NTBR	Freie Tablespace	NMS	<p>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.</p> <p>Durch das Anpassen des Alarmschwellenwerts können Sie proaktiv verwalten, wenn zusätzlicher Storage zugewiesen werden muss.</p> <p>Wenn der verfügbare Speicherplatz einen niedrigen Schwellenwert erreicht (siehe Alarmschwelle), wenden Sie sich an den technischen Support, um die Datenbankanweisung zu ändern.</p>
NTER	Übertragungsfehler	SSM	<p>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.</p> <p>Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node SSM Ressourcen Konfiguration Main, wählen Sie Anzahl der Übertragungsfehler zurücksetzen und klicken Sie auf Änderungen anwenden.</p>

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

Codieren	Name	Service	Empfohlene Maßnahmen
OQRT	Objekte Isoliert	LDR	<p>Nachdem die Objekte automatisch vom StorageGRID-System wiederhergestellt wurden, können die isolierten Objekte aus dem Quarantäneverzeichnis entfernt werden.</p> <ol style="list-style-type: none"> 1. Wählen Sie SUPPORT > Tools > Grid-Topologie aus. 2. Wählen Sie Standort Speicherknoten LDR Verifizierung Konfiguration Haupt. 3. Wählen Sie Gesperpte Objekte Löschen. 4. Klicken Sie Auf Änderungen Übernehmen. <p>Die isolierten Objekte werden entfernt und die Zählung wird auf Null zurückgesetzt.</p>
ORSU	Status Der Ausgehenden Replikation	BLDR, BARC	<p>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-Topologie aus. Wählen Sie dann site Grid Node LDR Replikation Konfiguration aus.</p> <p>Wenn der LDR-Dienst nicht zur Replikation verfügbar ist, wird ein Alarm ausgelöst. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node LDR Storage aus.</p>
OSLF	Shelf-Status	SSM	<p>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.</p>


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

Codieren	Name	Service	Empfohlene Maßnahmen
RDTU	Status Von Tivoli Storage Manager	BARC	<p>Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Tivoli Storage Manager (TSM).</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Wenn der Wert des Tivoli Storage Manager Status als Sitzungsfehler lautet, ist eine etablierte Sitzung unerwartet verloren gegangen. Überprüfen Sie die Netzwerkverbindung zwischen dem TSM Middleware-Server und dem StorageGRID-System. Überprüfen Sie den Middleware-Server auf Fehler.</p> <p>Wenn der Wert von Tivoli Storage Manager Status Unbekannt Fehler lautet, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
RIRF	Eingehende Replikationen — Fehlgeschlagen	BLDR, BARC	<p>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.</p> <p>Um die Zählung zurückzusetzen, wählen Sie SUPPORT Tools Grid-Topologie und dann site Grid-Knoten LDR Replikation Konfiguration Main aus. Wählen Sie Anzahl der fehlgeschlagene Inbound-Replikation zurücksetzen und klicken Sie auf Änderungen anwenden.</p>
RIRQ	Eingehende Replikationen — In Warteschlange	BLDR, BARC	<p>Alarmer 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.</p>
RORQ	Ausgehende Replikationen — In Warteschlange	BLDR, BARC	<p>Die Warteschlange für ausgehende Replizierung enthält Objektdaten, die kopiert werden, um ILM-Regeln und von Clients angeforderte Objekte zu erfüllen.</p> <p>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.</p>
SAVP	Nutzbarer Speicherplatz (Prozent)	LDR	<p>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.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SCAS	Status	CMN	<p>Wenn der Wert des Status für die aktive Grid-Aufgabe Fehler ist, suchen Sie die Grid-Task-Meldung. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node CMN Grid Tasks Übersicht Main. Die Grid-Aufgabenmeldung zeigt Informationen zum Fehler an (z. B. „Check failed on Node 12130011“).</p> <p>Nachdem Sie das Problem untersucht und behoben haben, starten Sie die Grid-Aufgabe neu. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node CMN Grid Tasks Konfiguration Main und wählen Sie Aktionen Ausführen.</p> <p>Wenn der Wert des Status für einen abgebrochenen Grid-Task Fehler ist, versuchen Sie, den Grid-Task zu abbrechen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SCEP	Ablaufdatum des Storage API-Service-Endpoints-Zertifikats	CMN	<p>Dieser Vorgang wird ausgelöst, wenn das Zertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, kurz vor Ablauf steht.</p> <ol style="list-style-type: none"> 1. Wählen Sie KONFIGURATION Sicherheit Zertifikate. 2. Wählen Sie auf der Registerkarte Global S3 und Swift API Zertifikat. 3. Laden Sie ein neues S3- und Swift-API-Zertifikat hoch.
SCHR	Status	CMN	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SCSA	Storage Controller A	SSM	<p>Wenn in einer StorageGRID-Appliance ein Problem mit Storage Controller A auftritt, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SCSB	Storage Controller B	SSM	<p>Wenn ein Problem mit dem Storage Controller B in einer StorageGRID-Appliance auftritt, wird ein Alarm ausgelöst.</p> <p>Ersetzen Sie die Komponente bei Bedarf.</p> <p>Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B</p>
SHLH.	Systemzustand	LDR	<p>Wenn der Wert „Systemzustand“ für einen Objektspeicher „Fehler“ lautet, prüfen und korrigieren Sie Folgendes:</p> <ul style="list-style-type: none"> • Probleme mit dem zu montiertem Volume • Fehler im Filesystem
SLSA	CPU-Auslastung durchschnittlich	SSM	<p>Je höher der Wert des Busiers des Systems.</p> <p>Wenn der CPU-Lastdurchschnitt weiterhin mit einem hohen Wert besteht, sollte die Anzahl der Transaktionen im System untersucht werden, um zu ermitteln, ob dies zu diesem Zeitpunkt aufgrund einer hohen Last liegt. Ein Diagramm des CPU-Lastdurchschnitts anzeigen: Wählen Sie SUPPORT Tools Grid-Topologie. Wählen Sie dann site Grid Node SSM Ressourcen Berichte Diagramme aus.</p> <p>Wenn die Belastung des Systems nicht hoch ist und das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SMST	Überwachungsstatus protokollieren	SSM	<p>Wenn der Wert des Protokollüberwachungsstatus für einen anhaltenden Zeitraum nicht verbunden ist, wenden Sie sich an den technischen Support.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SMTT	Ereignisse Insgesamt	SSM	<p>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 Alarmer für Ereignisse insgesamt ausgelöst werden.</p> <p>Wenn ein Problem behoben ist, setzen Sie den Zähler zurück, um den Alarm zu löschen. Wählen Sie NODES site Grid Node Events Anzahl der Ereignisse zurücksetzen.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  Um die Anzahl der Ereignisse zurückzusetzen, müssen Sie über die Berechtigung für die Konfiguration der Grid-Topologie-Seite verfügen. </div> <p>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.</p>
SNST	Status	CMN	<p>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.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SOSS	Status Des Storage- Betriebssystems	SSM	<p>Ein Alarm wird ausgelöst, wenn die SANtricity-Software angibt, dass bei einer Komponente in einer StorageGRID-Appliance ein „muss beachtet werden“-Problem vorliegt.</p> <p>Wählen Sie KNOTEN. Wählen Sie dann Appliance Storage Node Hardware aus. 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.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SSMA	SSM-Status	SSM	<p>Wenn der Wert des SSM Status Fehler ist, wählen Sie SUPPORT Tools Grid Topologie, und wählen Sie dann site Grid Node SSM Übersicht Main und SSM Übersicht Alarme, um die Ursache des Alarms zu bestimmen.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>
SSME	SSM-Status	SSM	<p>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.</p> <p>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.</p>
SSTS	Storage-Status	BLDR	<p>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.</p> <p>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.</p> <p>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 finden Sie im Health des Volumes: Wählen Sie SUPPORT Tools Grid-Topologie. Wählen Sie dann site Grid Node LDR Storage Übersicht Haupt. Die Gesundheit des Volumes ist unter Objektspeichern aufgeführt.</p> <p>Wenn der Wert des Speicherstatus Fehler ist, wenden Sie sich an den technischen Support.</p> <p>Fehlersuche im SSTS-Alarm (Storage Status) durchführen</p>

Codieren	Name	Service	Empfohlene Maßnahmen
SVST	Status	SSM	<p>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.</p> <p>Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node SSM Services Übersicht Main. 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:</p> <ul style="list-style-type: none"> • Der Dienst wurde manuell beendet (<code>/etc/init.d/<service> stop</code>). • 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. <p>Wenn ein Dienst als nicht ausgeführt aufgeführt ist, starten Sie den Dienst neu (<code>/etc/init.d/<service> restart</code>).</p> <p>Dieser Alarm kann auch zeigen, dass der Metadatenpeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p> <p>Fehlersuche im Alarm Services: Status - Cassandra (SVST) durchführen</p>
TMEM.	Installierter Speicher	SSM	<p>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.</p>

Codieren	Name	Service	Empfohlene Maßnahmen
POP	Ausstehende Vorgänge	ADU	Eine Meldungswarteschlange kann darauf hinweisen, dass der ADC-Dienst überlastet ist. Es können zu wenige ADC-Dienste an das StorageGRID-System angeschlossen werden. In einer großen Implementierung kann der ADC-Service Computing-Ressourcen hinzufügen oder das System benötigt zusätzliche ADC-Services.
UMEM	Verfügbarer Speicher	SSM	Wenn der verfügbare RAM knapp wird, prüfen Sie, ob es sich um ein Hardware- oder Softwareproblem handelt. Wenn es sich nicht um ein Hardwareproblem handelt oder wenn der verfügbare Speicher unter 50 MB liegt (der Standard-Alarmschwellenwert), wenden Sie sich an den technischen Support.
VMFI	Einträge Verfügbar	SSM	Dies deutet darauf hin, dass zusätzlicher Speicherplatz benötigt wird. Wenden Sie sich an den technischen Support.
VMFR	Speicherplatz Verfügbar	SSM	Wenn der Wert des verfügbaren Speicherplatzes zu niedrig wird (siehe Alarmschwellen), muss untersucht werden, ob sich die Log-Dateien aus dem Verhältnis heraus entwickeln oder Objekte, die zu viel Speicherplatz beanspruchen (siehe Alarmschwellen), die reduziert oder gelöscht werden müssen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
VMST	Status	SSM	Ein Alarm wird ausgelöst, wenn der Wert Status für das Bereitstellungsvolumen Unbekannt ist. 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	<p>Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node LDR Storage Übersicht Haupt.</p> <p>Überprüfen Sie das Betriebssystem auf Anzeichen von Block- oder Dateisystemfehlern.</p> <p>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.</p>
XAMS	Nicht Erreichbare Audit-Repositorys	BADC, BARC, BCLB, BCMN, BLDR, BNMS	<p>Überprüfen Sie die Netzwerkverbindung mit dem Server, der den Admin-Node hostet.</p> <p>Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.</p>

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

Codieren	Name	Schweregrad
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
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

Codieren	Name	Schweregrad
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
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

Codieren	Name	Schweregrad
TMEM.	Installierter Speicher	Gering
UMEM	Verfügbarer Speicher	Gering
VMST	Status	Gering
VPRI	Überprüfungspriorität	Hinweis
VSTU	Status Der Objektüberprüfung	Hinweis

Referenz für Protokolldateien

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

Die Protokolle werden wie folgt kategorisiert:

- [StorageGRID-Softwareprotokolle](#)
- [Protokoll für Implementierung und Wartung](#)
- [Protokolle für Drittanbietersoftware](#)
- [Etwa bycast.log](#)



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

Um auf die Protokolle zuzugreifen, können Sie Logfiles und Systemdaten von einem oder mehreren Knoten als ein einziges Log-File-Archiv (**SUPPORT Tools Logs**) sammeln. Wenn der primäre Admin-Node nicht verfügbar ist oder einen bestimmten Knoten nicht erreichen kann, können Sie für jeden Grid-Knoten wie folgt auf einzelne Protokolldateien zugreifen:

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

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

Speicherort der Archivierung	Beschreibung
Prüfung	Während des normalen Systembetriebs erzeugte Überwachungsmeldungen.
Protokolle von Base-os	Informationen zu Betriebssystemen, einschließlich StorageGRID-Image-Versionen
Pakete	Globale Konfigurationsinformationen (Bundles)
cassandra	Cassandra Datenbankinformationen und Reaper Reparaturprotokolle.
eg	VCSs-Informationen zu den aktuellen Knoten- und EC-Gruppeninformationen nach Profil-ID.
Raster	Allgemeine Grid-Protokolle einschließlich Debug (<code>broadcast.log</code>) Und <code>servermanager</code> Protokolle:
grid.xml	Die Grid-Konfigurationsdatei ist über alle Nodes hinweg freigegeben.
Hagroups	Hochverfügbarkeitsgruppen – Kennzahlen und Protokolle
Installieren	<code>gdu-server</code> Und installieren Protokolle.
lumberjack.log	Debug-Meldungen im Zusammenhang mit Protokollerfassung.
Lambda-Schiedsrichter	Protokolle in Verbindung mit der S3 Select Proxy-Anforderung.
Metriken	Service-Protokolle für Grafana, Jaeger, Node Exporter und Prometheus.
Falsch	Miscd-Zugriffs- und Fehlerprotokolle.
mysql	Die Konfiguration der MariaDB-Datenbank und die zugehörigen Protokolle.
Netz	Protokolle, die von netzwerkbezogenen Skripten und dem dynIP-Dienst erstellt werden.
Nginx	Konfigurationsdateien und Protokolle für den Load Balancer. Beinhaltet außerdem Traffic-Protokolle: Grid Manager und Tenant Manager.
Nginx-gw	Konfigurationsdateien und Protokolle für den Load Balancer.
ntp	NTP-Konfigurationsdatei und -Protokolle
betriebssystem	Node- und Grid-Statusdatei, einschließlich Services <code>pid</code> .

Speicherort der Archivierung	Beschreibung
Andere	Log-Dateien unter <code>/var/local/log</code> Die nicht in anderen Ordnern erfasst werden.
perf-	Performance-Informationen für CPU-, Netzwerk- und Festplatten-I/O.
prometheus-Data	Aktuelle Prometheus-Kennzahlen, wenn die Log-Sammlung Prometheus-Daten enthält.
Bereitstellung	Protokolle im Zusammenhang mit dem Grid-Bereitstellungsprozess.
Floß	Protokolle aus dem in Plattformservices verwendeten Raft-Cluster.
snmp	SNMP-Agent-Konfiguration und Alarmzulassungs-/Deny-Listen, die für das Senden von SNMP-Benachrichtigungen verwendet werden.
Steckdosen-Daten	Sockendaten für Netzwerk-Debug.
system-commands.txt	Ausgabe von StorageGRID-Containerbefehlen. Enthält Systeminformationen wie z. B. Netzwerk- und Festplattenverwendung.

Verwandte Informationen

[Erfassen von Protokolldateien und Systemdaten](#)

StorageGRID-Softwareprotokolle


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



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

Allgemeine StorageGRID-Protokolle

Dateiname	Hinweise	Gefunden am
<code>/var/local/log/bycast.log</code>	Die primäre StorageGRID-Fehlerbehebungsdatei. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann Site Node SSM Events aus.	Alle Nodes

Dateiname	Hinweise	Gefunden am
/var/local/log/bycast-err.log	Enthält eine Untergruppe von bycast.log (Meldungen mit dem Schweregrad „FEHLER“ und „KRITISCH“). WICHTIGE Meldungen werden auch im System angezeigt. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann Site Node SSM Events aus.	Alle Nodes
/var/local/core/	Enthält alle Core Dump-Dateien, die erstellt wurden, wenn das Programm normal beendet wird. Mögliche Ursachen sind Assertion Failures, Verstöße oder Thread Timeouts. <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  Die Datei <code>\var/local/core/kexec_cmd</code> ist normalerweise auf Appliance-Knoten vorhanden und weist keinen Fehler auf. </div>	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

Dateiname	Hinweise	Gefunden am
/var/local/log/ams.errlog		Admin-Nodes
/var/local/log/arc.errlog		Archiv-Nodes
/var/local/log/cassandra/system.log	Informationen für den Metadatenpeicher (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
/var/local/log/dynip*	Enthält Protokolle zum Dynap-Dienst, der das Grid auf dynamische IP-Änderungen überwacht und die lokale Konfiguration aktualisiert.	Alle Nodes

Dateiname	Hinweise	Gefunden am
/var/local/log/grafana.log	Das mit dem Grafana-Service verknüpfte Protokoll, das für die Visualisierung von Kennzahlen im Grid Manager verwendet wird.	Admin-Nodes
/var/local/log/hagroups.log	Das Protokoll, das mit Hochverfügbarkeitsgruppen verknüpft ist.	Admin-Nodes und Gateway-Nodes
/var/local/log/hagroups_events.log	Verfolgt Statusänderungen, beispielsweise den Übergang von BACKUP zu MASTER oder FEHLER.	Admin-Nodes und Gateway-Nodes
/var/local/log/idnt.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/var/local/log/jaeger.log	Das Protokoll, das mit dem jaeger-Dienst verknüpft ist, das für die Trace-Erfassung verwendet wird.	Alle Nodes
/var/local/log/kstn.errlog		Speicherknoten, auf denen der ADC-Service ausgeführt wird
/var/local/log/lambda*	Enthält Protokolle für den S3 Select-Service.	Admin- und Gateway-Nodes Dieses Protokoll enthält nur bestimmte Admin- und Gateway-Knoten. Siehe S3 Select Anforderungen und Einschränkungen für Admin und Gateway Nodes .
/var/local/log/ldr.errlog		Storage-Nodes
/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
<code>/var/local/log/nginx/*.log</code>	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
<code>/var/local/log/nginx-gw/*.log</code>	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
<code>/var/local/log/persistence*</code>	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Root-Festplatte verwaltet, die bei einem Neustart erhalten bleiben müssen.	Alle Nodes
<code>/var/local/log/prometheus.log</code>	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
<code>/var/local/log/raft.log</code>	Enthält die Ausgabe der Bibliothek, die vom RSM-Dienst für das Raft-Protokoll verwendet wird.	Storage-Nodes mit RSM-Service
<code>/var/local/log/rms.errlog</code>	Enthält Protokolle für den RSM-Service (Replicated State Machine Service), der für S3-Platformservices verwendet wird.	Storage-Nodes mit RSM-Service
<code>/var/local/log/ssm.errlog</code>		Alle Nodes
<code>/var/local/log/update-s3vs-domains.log</code>	Enthält Protokolle zur Verarbeitung von Updates für die Konfiguration virtueller gehosteter S3-Domännennamen. Siehe Anweisungen für die Implementierung von S3-Client-Applikationen.	Admin- und Gateway-Nodes

Dateiname	Hinweise	Gefunden am
/var/local/log/update-snmpp-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	<ul style="list-style-type: none"> 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	<p>Enthält Fehlermeldungen bezüglich der MySQL-Datenbank-Upgrades.</p> <p>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.</p>	Admin-Nodes

Dateiname	Hinweise	Gefunden am
/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 Softwareaktualisierungsereignisse.	Alle Nodes

Protokolle für Drittanbietersoftware

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

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

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#).

Dateirotation für bycast.log

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

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

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

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



Wenn eine Protokolldatei komprimiert wurde, dürfen Sie sie nicht auf den gleichen Speicherort dekomprimieren, an dem sie geschrieben wurde. Die Dekomprimierung der Datei an demselben Speicherort kann die Drehskripte des Protokolls beeinträchtigen.

Optional können Sie das Ziel der Audit-Protokolle ändern und Audit-Informationen an einen externen Syslog-Server senden. Lokale Protokolle von Audit-Datensätzen werden weiterhin generiert und gespeichert, wenn ein externer Syslog-Server konfiguriert ist. Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#).

Verwandte Informationen

[Erfassen von Protokolldateien und Systemdaten](#)

Nachrichten in bycast.log

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

Beispielmeldung für ADE:

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

ADE-Meldungen enthalten die folgenden Informationen:

Nachrichtensegment	Wert im Beispiel
Node-ID	12455685
PROZESS-ID WIRD ADDIEREN	0357819531

Nachrichtensegment	Wert im Beispiel
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-Topologie** aus. Wählen Sie dann **Standort Knoten SSM Events** aus.

Fehlercodes in bycast.log

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

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

Fehlercode	Bedeutung
SUKZ	Kein Fehler
GERR	Unbekannt
STORNO	Storniert
ABRT	Abgebrochen

Fehlercode	Bedeutung
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
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

Fehlernummer	Fehlercode	Bedeutung
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
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

Fehlernummer	Fehlercode	Bedeutung
034	ERANGE	Math Ergebnis nicht darstellbar
035	EDEADLK	Ressourcen-Deadlock würde eintreten
036	ENAMETOOLONG	Dateiname zu lang
037	ENOLCK	Keine Datensatzsperrern 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
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

Fehlernummer	Fehlercode	Bedeutung
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
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

Fehlernummer	Fehlercode	Bedeutung
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
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

Fehlernummer	Fehlercode	Bedeutung
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	ECONNRESET	Verbindungsrücksetzung durch Peer
105	ENOBUFS	Kein Pufferspeicher verfügbar
106	EISCONN	Transportendpunkt ist bereits verbunden
107	ENOTCONN	Transportendpunkt ist nicht verbunden
108	ESHUTDOWN	Senden nach dem Herunterfahren des Transportendpunkts nicht möglich
109	ETOMANYREFS	Zu viele Referenzen: Keine Spleißung möglich
110	ETIMEDOUT	Zeitüberschreitung bei Verbindung
111	ECONNREFUSED	Verbindung abgelehnt
112	EHOSTDOWN	Host ist ausgefallen
113	EHOSTUNREACH	Keine Route zum Host
114	EALREADY	Der Vorgang wird bereits ausgeführt
115	EINPROGRESS	Vorgang wird jetzt ausgeführt
116		
117	EUCLEAN	Struktur muss gereinigt werden

Fehlernummer	Fehlercode	Bedeutung
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
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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.