



Überwachung und Wartung von StorageGRID

StorageGRID

NetApp
October 03, 2025

Inhalt

Überwachung und Wartung von StorageGRID	1
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
Erweitern Sie Ihr Raster	361
Raster erweitern: Übersicht	361
Planen Sie eine Erweiterung von StorageGRID	363
Sammeln Sie die erforderlichen Materialien	376
Hinzufügen von Storage-Volumes	382
Grid-Nodes oder Standort hinzufügen	391
Erweitertes System konfigurieren	407
Wenden Sie sich an den technischen Support	417
Recovery und Wartung	417
Recovery and Maintain: Übersicht	417
StorageGRID Hotfix Verfahren	419
Verfahren zur Recovery von Grid-Nodes	427
Durchführen der Standortwiederherstellung durch den technischen Support	543
Verfahren zur Deaktivierung	545
Netzwerkwartungsverfahren	599
Verfahren auf Host-Ebene und Middleware	625
Verfahren für den Grid-Node	633
Klonen von Appliance-Nodes	659
Prüfung von Audit-Protokollen	668
Audit-Protokolle: Übersicht	668
Audit-Log-Datei und Nachrichtenformate	672
Überwachungsmeldungen und der Lebenszyklus von Objekten	691
Audit-Meldungen	699

Überwachung und Wartung von StorageGRID

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

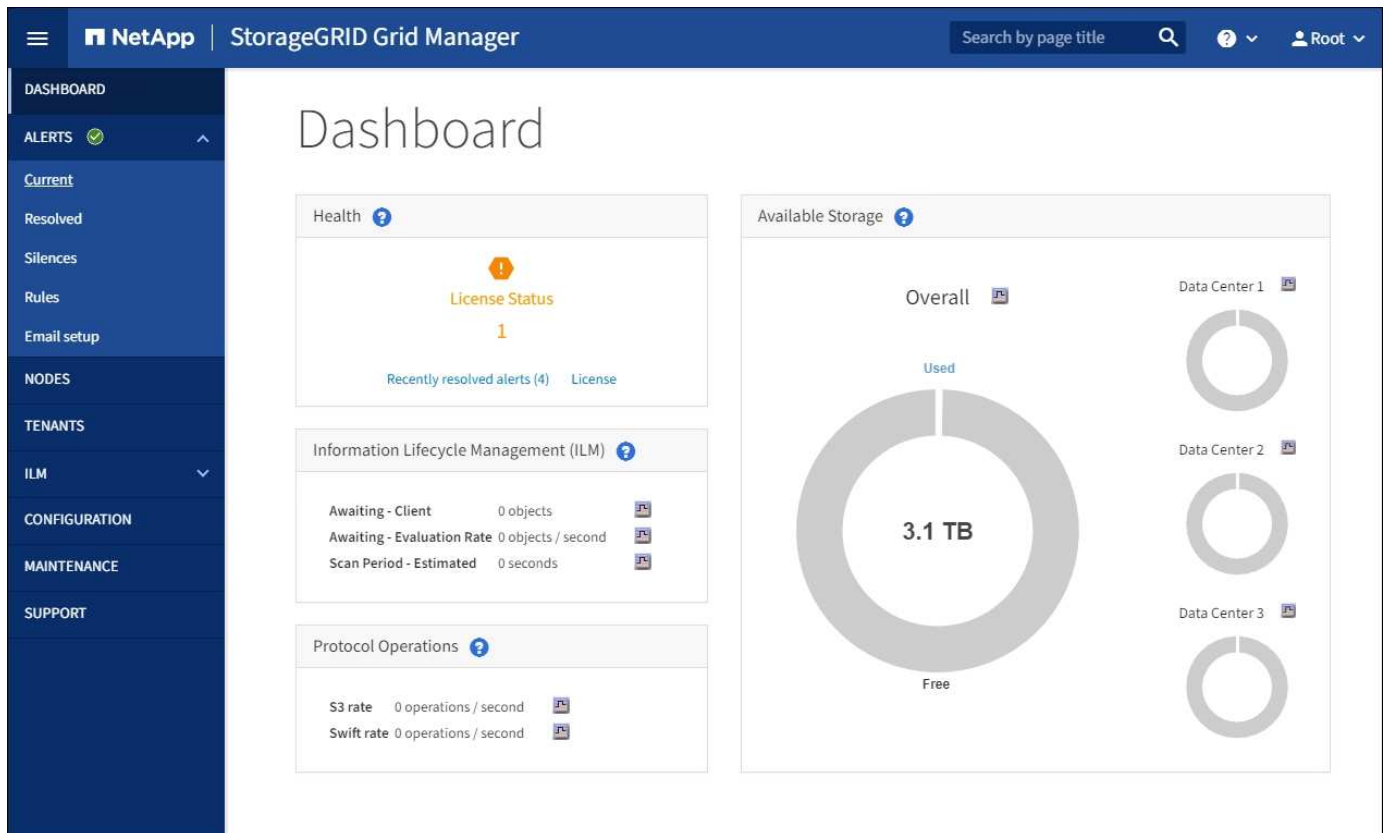
In diesen Anweisungen wird die Verwendung von Grid Manager zum Überwachen eines StorageGRID-Systems beschrieben. Sie erfahren, welche Informationen Sie regelmäßig überwachen sollten, wie Sie Warnmeldungen und ältere Alarmer verwalten, wie Sie SNMP für das Monitoring verwenden und wie Sie zusätzliche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

Sie beschreiben außerdem die Fehlerbehebung für ein StorageGRID System und beschreiben alle Systemmeldungen, ältere Alarmer 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 .
Fasst den Systemzustand zusammen. Ein grünes Häkchen bedeutet, dass keine aktuellen Warnmeldungen vorhanden sind und alle Grid-Nodes verbunden sind. Jedes andere Symbol bedeutet, dass mindestens eine aktuelle Warnung oder ein nicht getrennter Knoten vorhanden ist.	Möglicherweise werden mindestens ein der folgenden Links angezeigt: • Grid Details: Wird angezeigt, wenn Knoten getrennt sind (Verbindungsstatus unbekannt oder Administrativ ausgefallen). Klicken Sie auf den Link oder klicken Sie auf das blaue oder graue Symbol, um zu ermitteln, welche Nodes betroffen sind. • Aktuelle Meldungen: Wird angezeigt, wenn derzeit Alarmer 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 Alarmer: 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-Alarmer: Wird angezeigt, wenn derzeit Alarmer (Legacy-System) aktiv sind. Klicken Sie auf den Link, um die Details auf der Seite SUPPORT Alarmer (alt) Aktuelle Alarmer 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.	• 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 .
Zeigt die verfügbare und genutzte Speicherkapazität im gesamten Grid an, nicht einschließlich Archivmedien. Das Gesamtdiagramm stellt die Gesamtgesamtwerte für das gesamte Grid dar. Ist dies ein Grid mit mehreren Standorten, werden für jeden Datacenter-Standort zusätzliche Diagramme angezeigt. Anhand dieser Informationen können Sie den verwendeten Speicher mit dem verfügbaren Speicher vergleichen. Wenn Sie ein Grid mit mehreren Standorten verwenden, können Sie feststellen, welcher Standort mehr Storage verbraucht.	• Um die Kapazität anzuzeigen, platzieren Sie den Cursor über die verfügbaren und genutzten Kapazitätsbereiche des Diagramms. • Um Kapazitätstrends über einen Datumsbereich anzuzeigen, klicken Sie auf das Diagrammsymbol  Für das Gesamtraster oder einen Standort im Datacenter. • Um Details anzuzeigen, wählen Sie NODES. Anschließend können Sie die Registerkarte „Storage“ für das gesamte Grid, eine gesamte Site oder einen einzelnen Storage-Node anzeigen.	• Öffnen Sie die Registerkarte „Speicher“ • Monitoring der Storage-Kapazität

Bereich „Information Lifecycle Management“ (ILM)

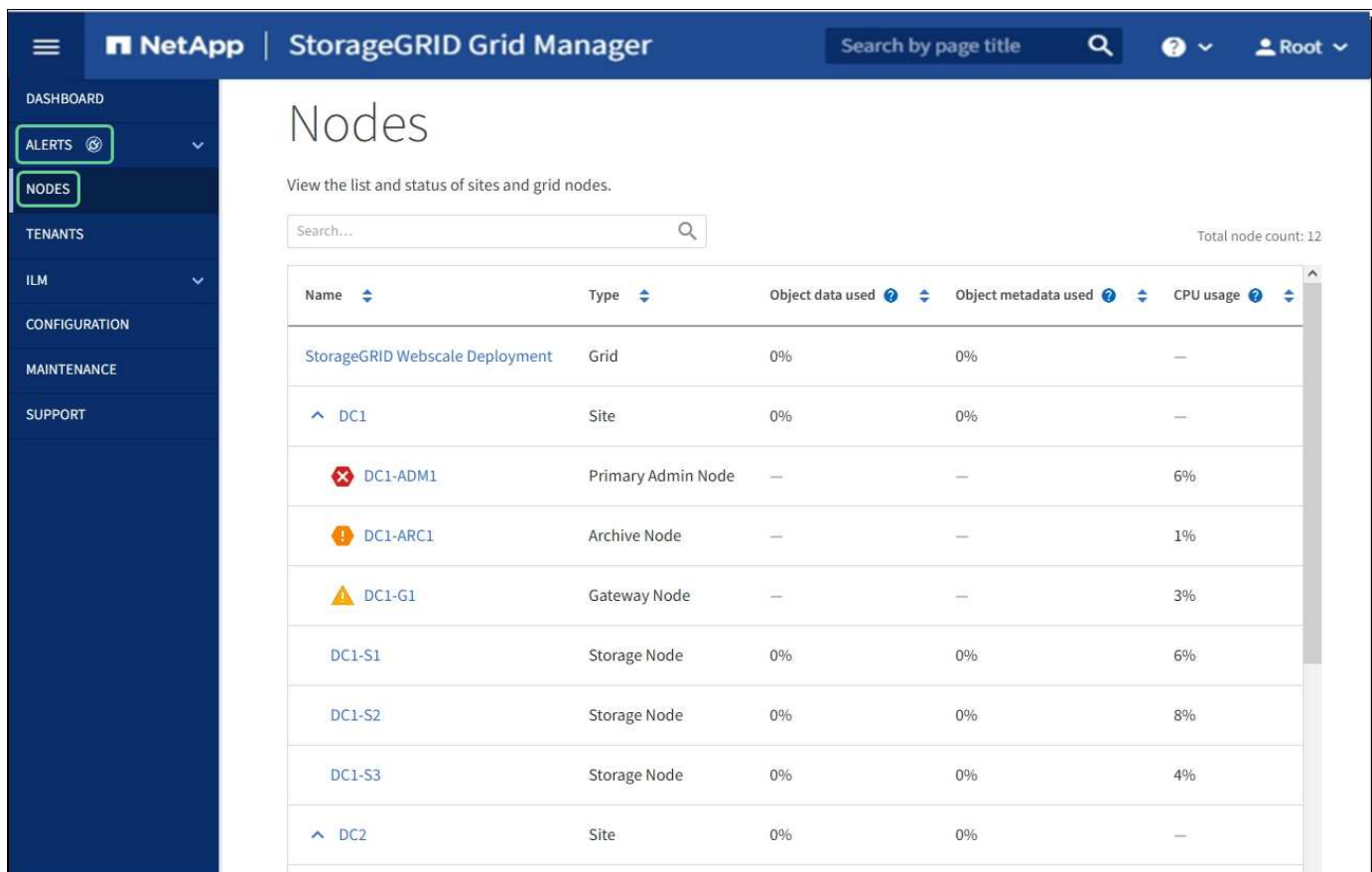
Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die aktuellen ILM-Vorgänge und ILM-Warteschlangen für das System an. Sie können diese Informationen für das Monitoring der Arbeitsbelastung Ihres Systems verwenden. • Ausstehend - Client: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung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

Bereich „Protokollbetrieb“

Beschreibung	Weitere Details anzeigen	Weitere Informationen .
Zeigt die Anzahl der protokollspezifischen Vorgänge (S3 und Swift) an, die vom System durchgeführt werden. Sie können diese Informationen nutzen, um die Workloads und die Effizienz Ihres Systems zu überwachen. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.	• Um Details anzuzeigen, wählen Sie 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.	• 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 unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.



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

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

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

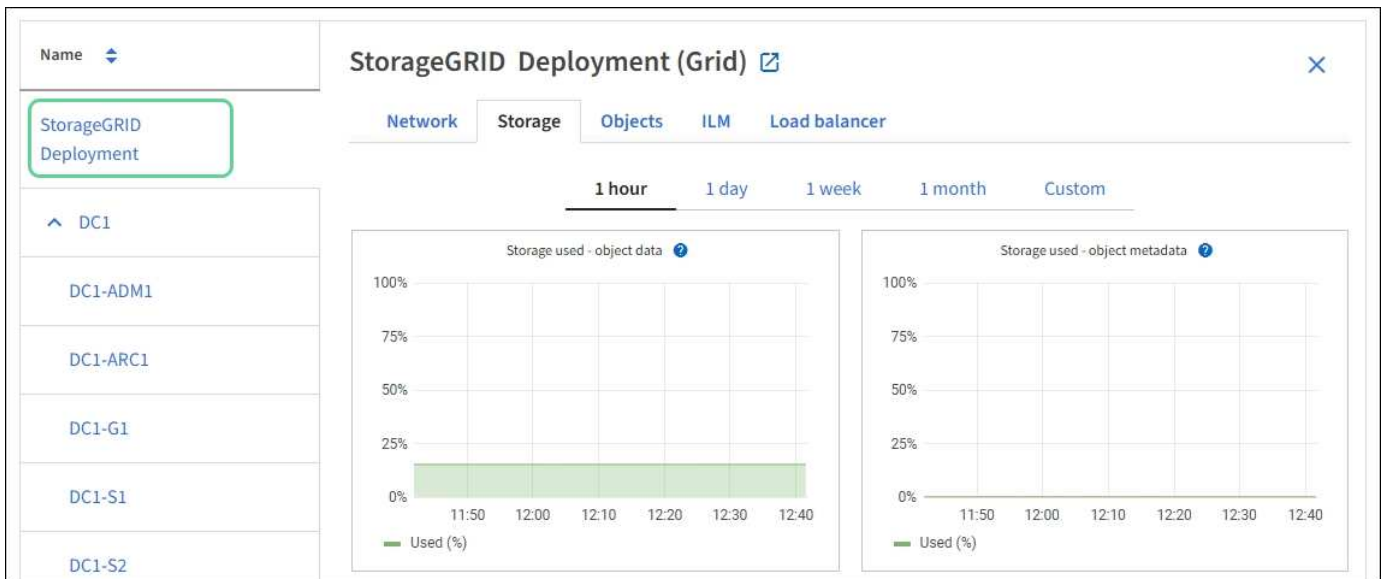
Wenn eine aktive Warnmeldung für einen Node vorhanden ist, wird neben dem Node-Namen eines der folgenden Symbole angezeigt:

- *** 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.



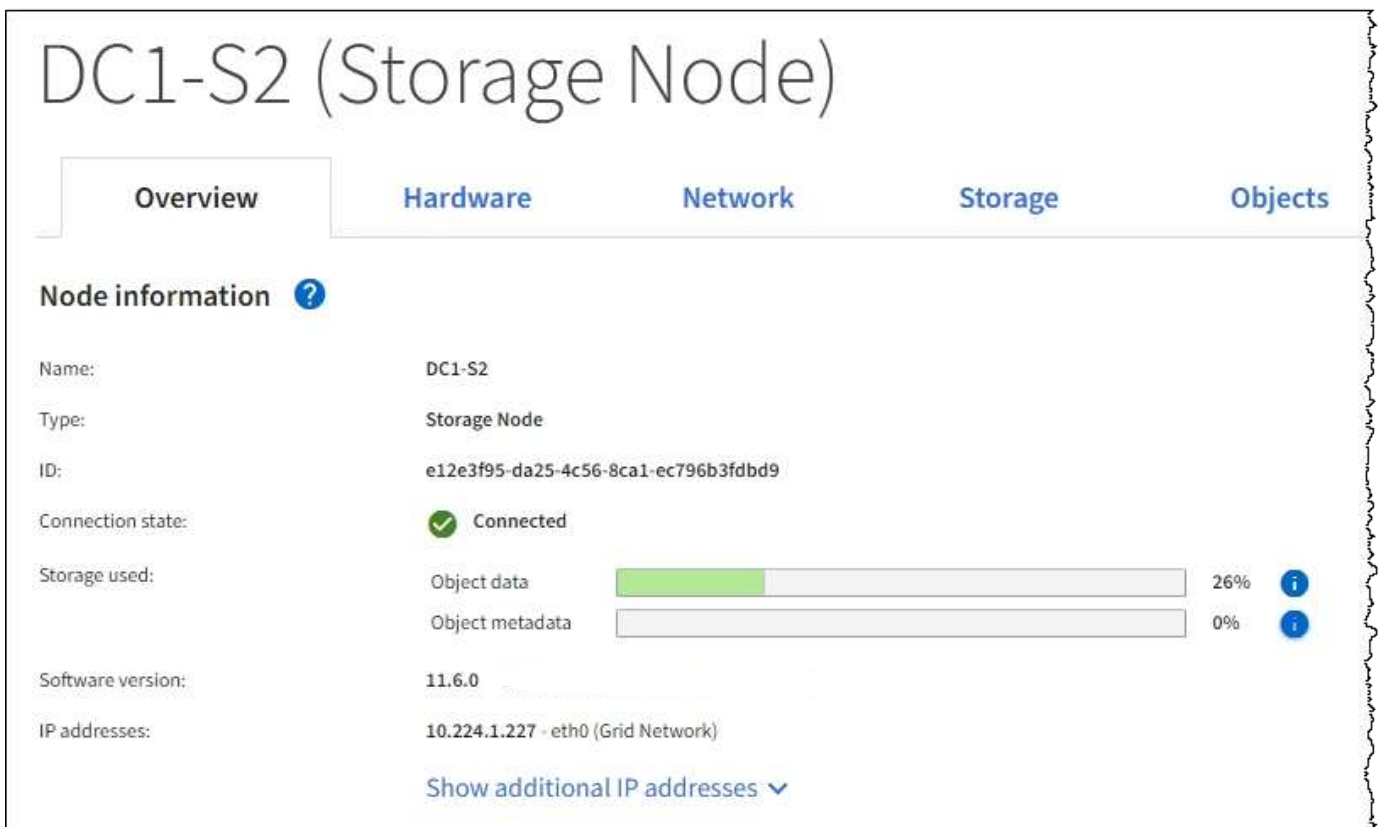
Zeigen Sie die Registerkarte Übersicht an

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.



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



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

- **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.

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

Verwandte Informationen

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

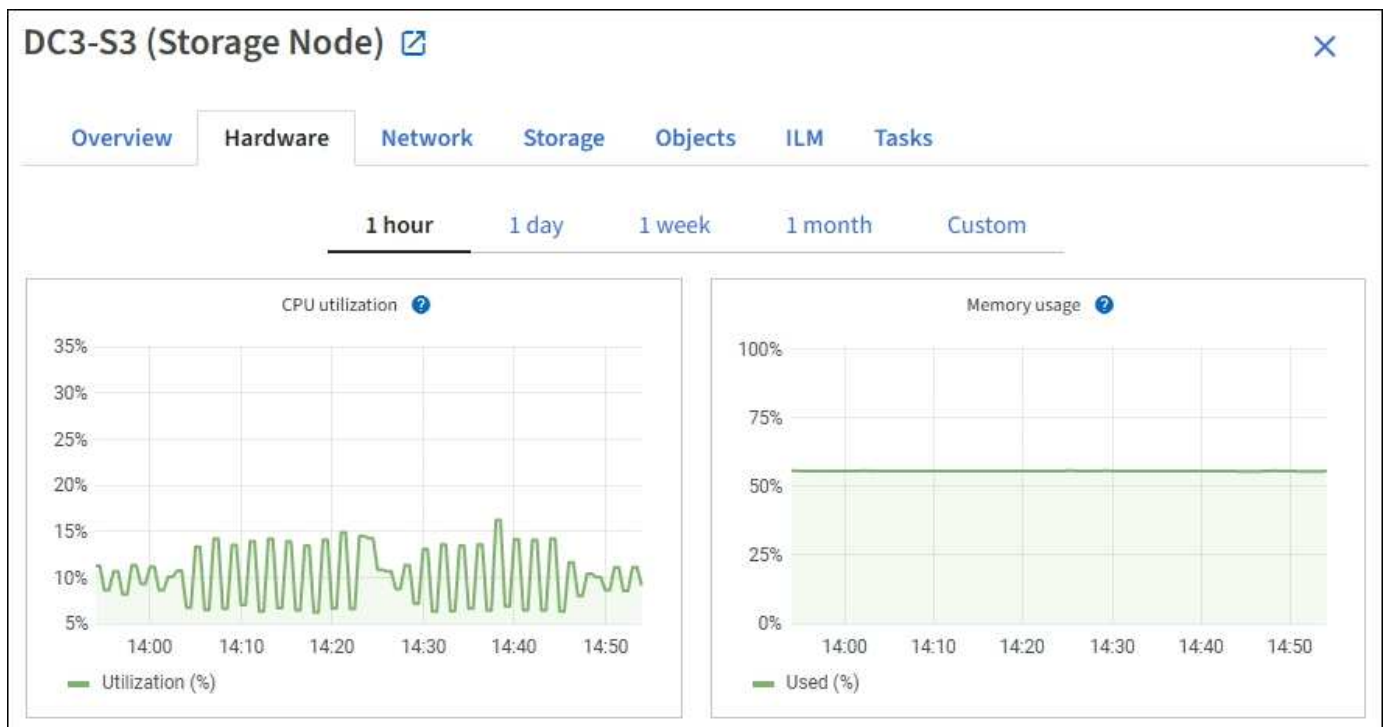
[Anzeigen aktueller Warnmeldungen](#)

[Zeigen Sie eine bestimmte Warnmeldung an](#)

Zeigen Sie die Registerkarte Hardware an

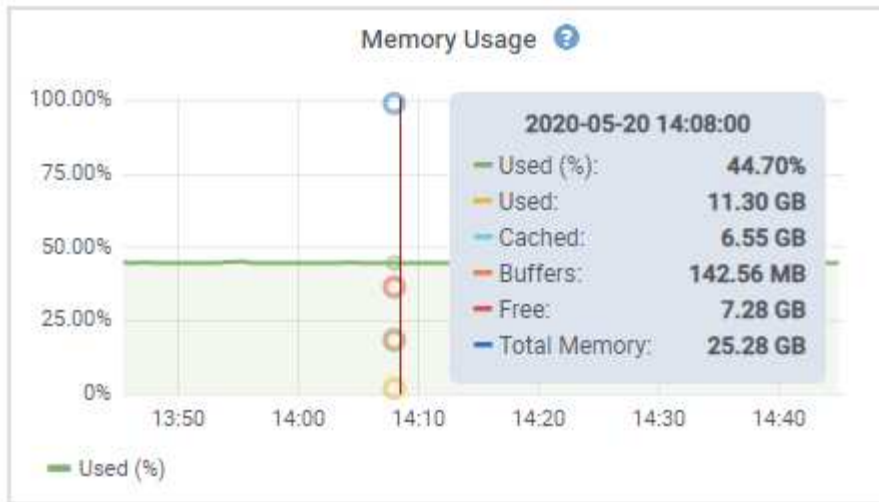
Auf der Registerkarte Hardware werden für jeden Node CPU-Auslastung und Arbeitsspeicherauslastung sowie zusätzliche Hardware-Informationen über Appliances angezeigt.

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.

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](#) [^](#)

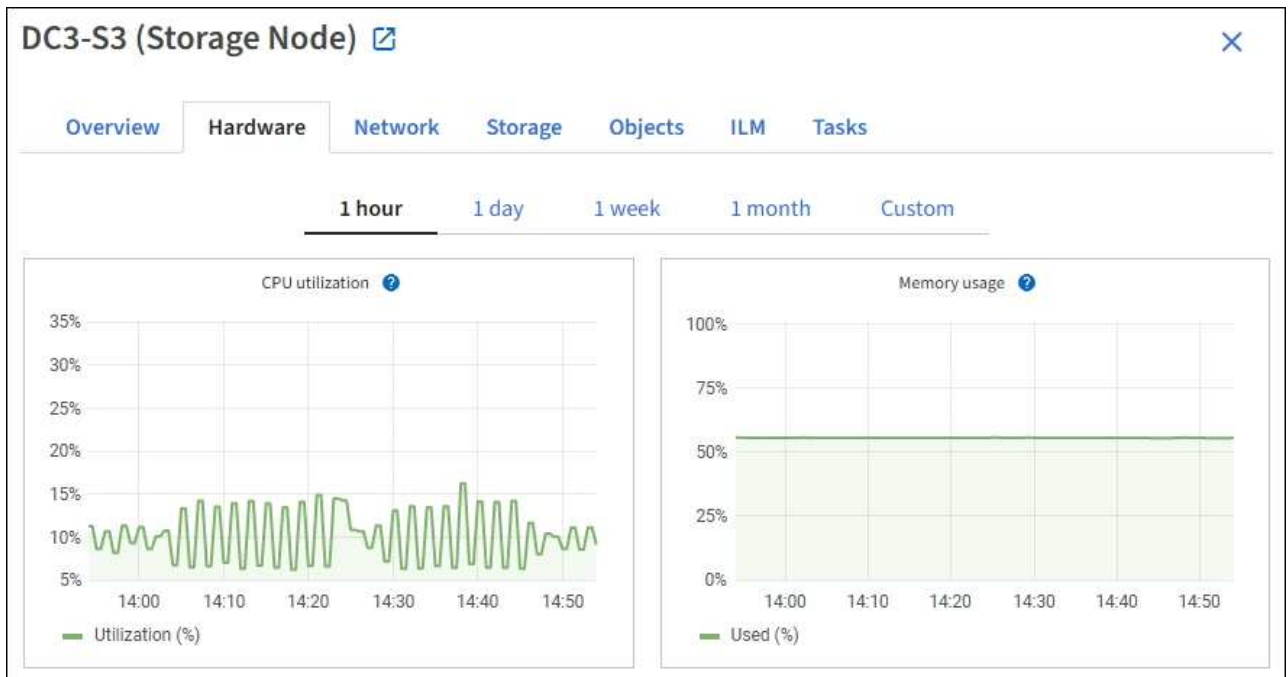
Interface ⬆	IP address ⬆
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

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	IP-Adresse für Management Port 1 auf Storage Controller B Sie verwenden diese IP für den Zugriff auf die SANtricity Software zur Fehlerbehebung bei Speicherproblemen. Einige Gerätemodelle verfügen nicht über einen Speicher-Controller B
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	Der Gesamtstatus der Hardware des Storage Controllers. Wenn SANtricity System Manager einen Status als Warnung für die Storage-Hardware meldet, meldet das StorageGRID System diesen Wert ebenfalls. Wenn der Status „Anforderungen einer Warnung erfüllt,“ zunächst den Storage Controller mithilfe der SANtricity Software prüfen. Stellen Sie dann sicher, dass keine weiteren Alarme vorhanden sind, die für den Rechencontroller gelten.
Anzahl 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	Die effektive Größe eines Datenlaufwerks. Hinweis: Für Knoten mit Erweiterungs-Shelfs, verwenden Sie das Datenlaufwerk-Größe für jedes Shelf Stattdessen. Die effektive Laufwerksgröße kann je nach Shelf abweichen.
Storage RAID-Modus	Der für die Appliance konfigurierte RAID-Modus.

Feld in der Appliance-Tabelle	Beschreibung
Storage-Konnektivität	Der Status der Storage-Konnektivität.
Gesamtnetzteil	Der Status aller Netzteile für das Gerät.
BMC IP für Computing Controller	Die IP-Adresse des Ports für das Baseboard Management Controller (BMC) im Computing-Controller. Mit dieser IP können Sie eine Verbindung zur BMC-Schnittstelle herstellen, um die Appliance-Hardware zu überwachen und zu diagnostizieren. Dieses Feld wird nicht für 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. • 99: Storage Controller Shelf • 0: Erstes Erweiterungs-Shelf • 1: Zweites Erweiterungs-Shelf Hinweis: Erweiterungseinschübe gelten nur für SG6060 und SG6060X.
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

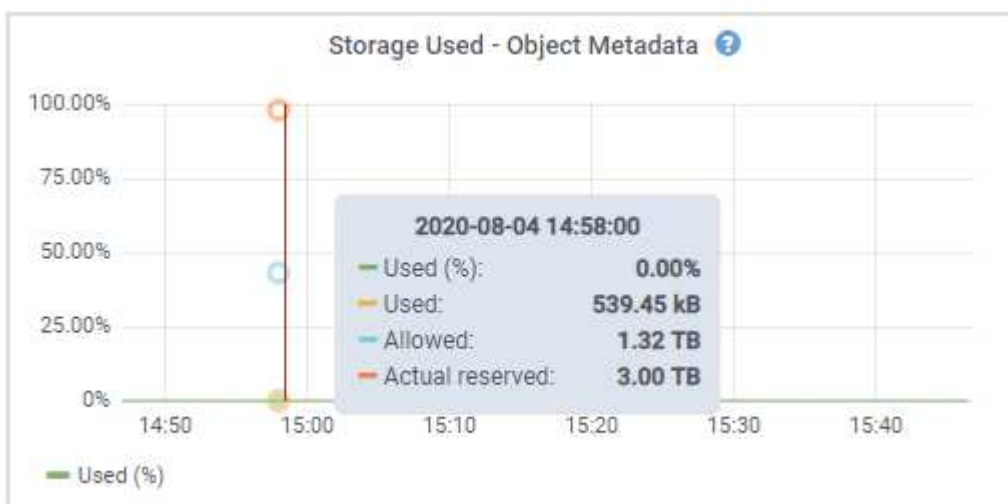
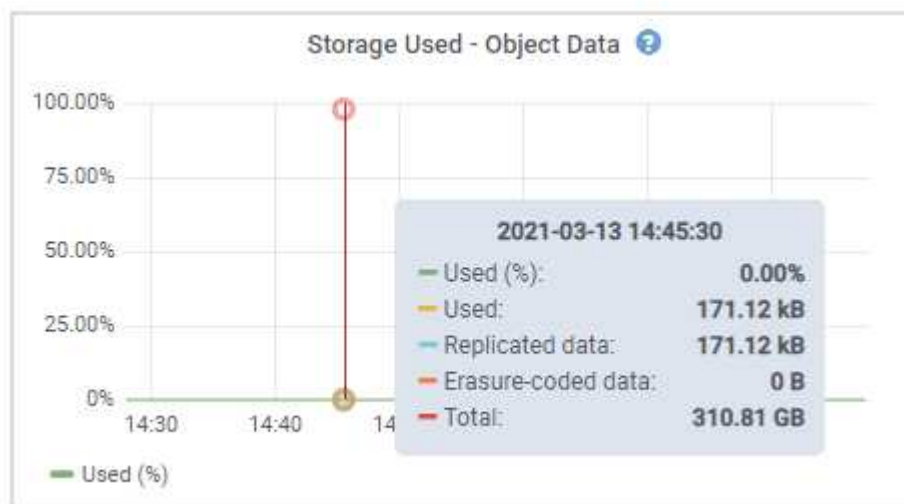
Receive

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

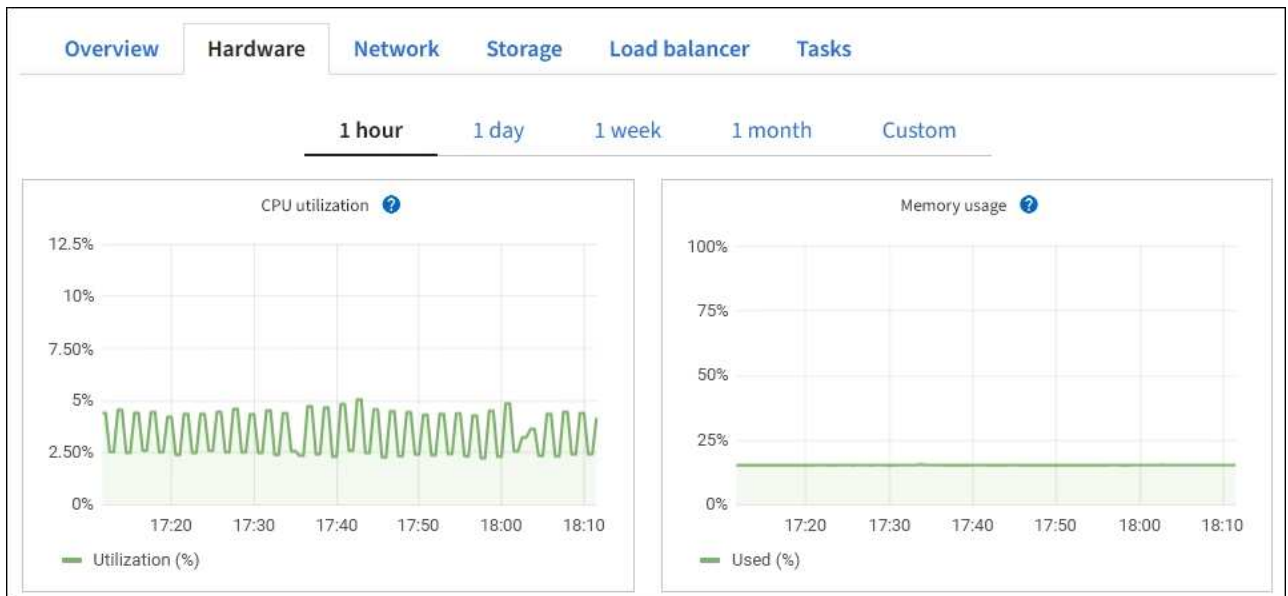
Node information

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.

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.

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

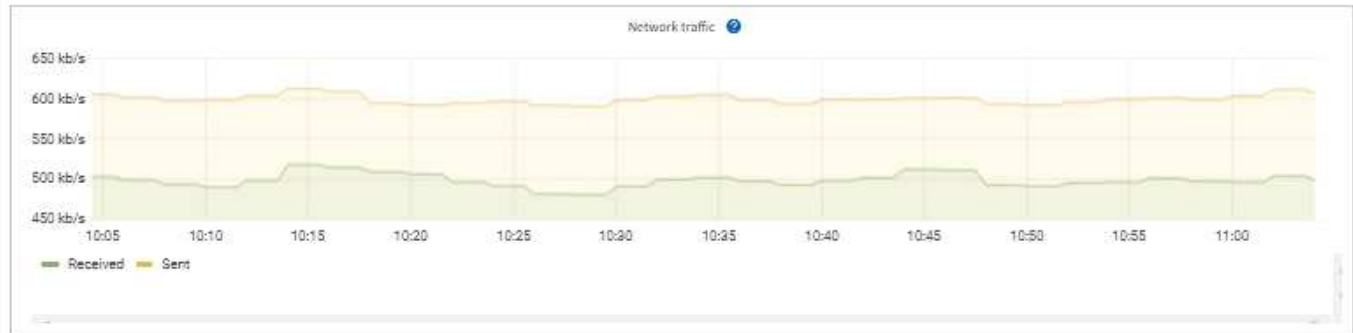
Auf der Registerkarte Netzwerk wird ein Diagramm angezeigt, in dem der empfangene und gesendete Netzwerkdatenverkehr über alle Netzwerkschnittstellen auf dem Node, am Standort oder im Raster angezeigt wird.

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.

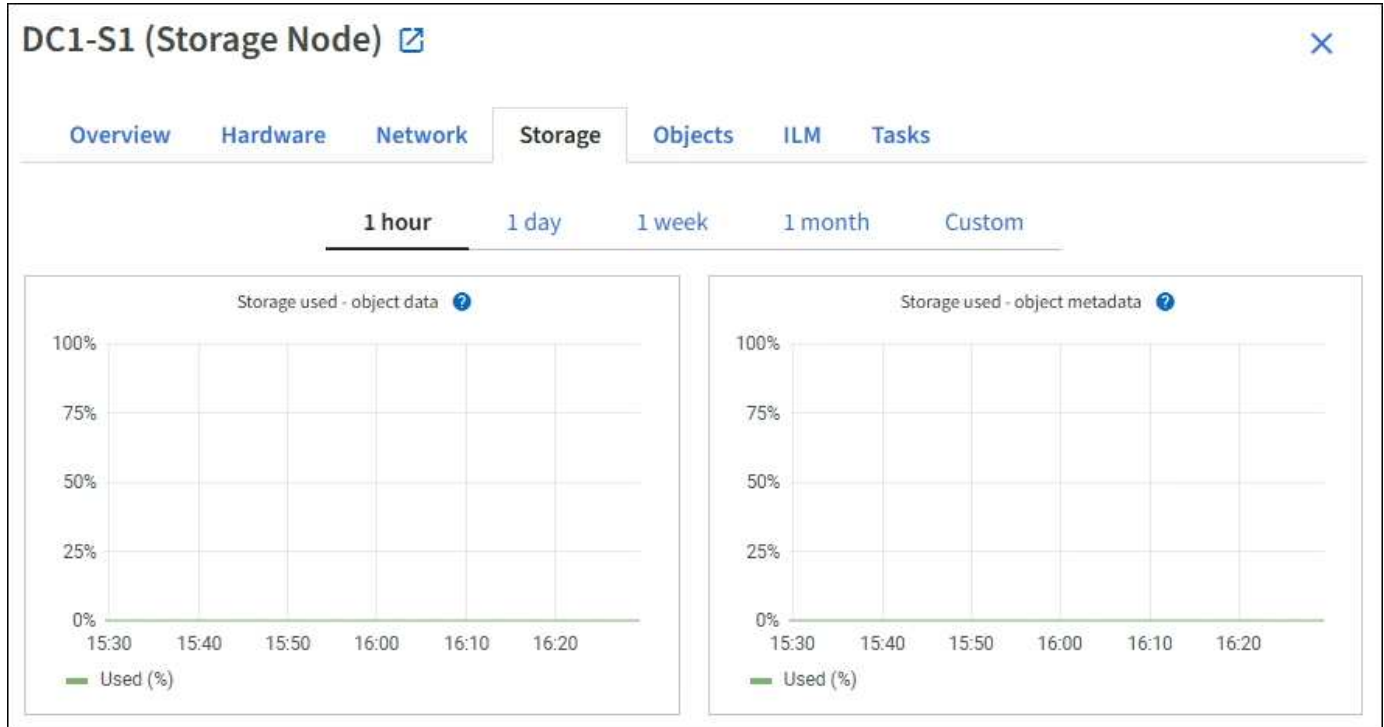
Die Registerkarte Storage wird für alle Nodes, jeden Standort und das gesamte Raster angezeigt.

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:

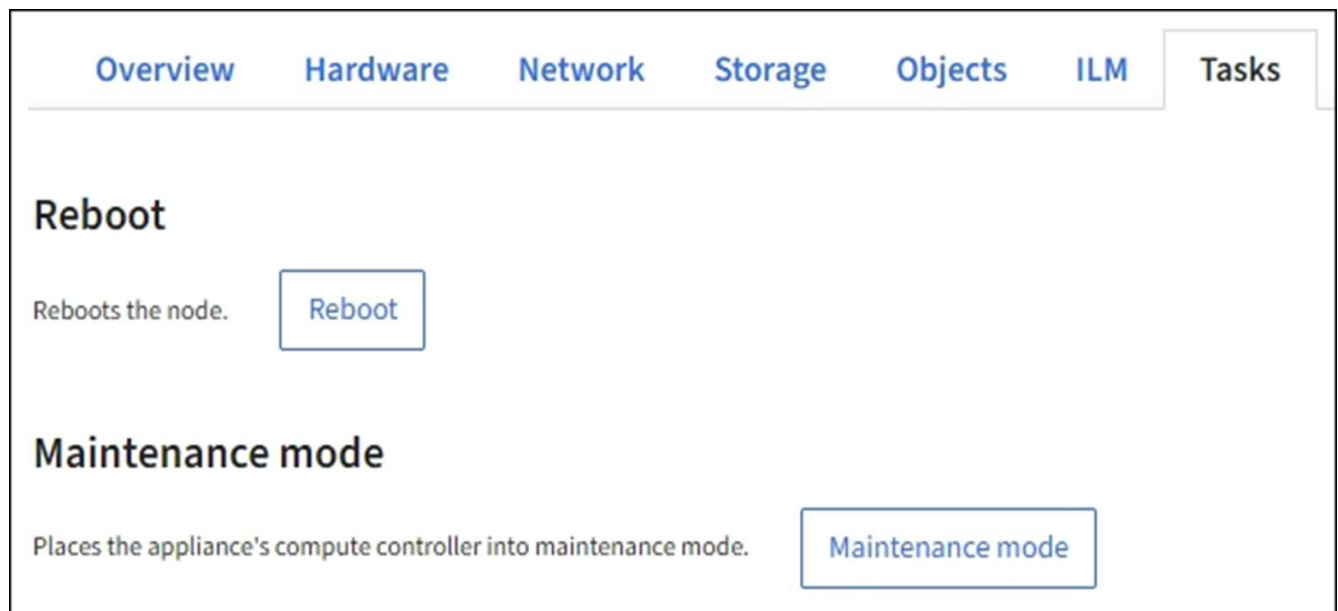
- Wenn eine ILM-Regel ein Aufnahmeverhalten von Dual-Commit angibt oder die Regel einen Ausgleich angibt und nicht sofort alle erforderlichen Kopien erstellen kann, werden neu aufgenommenen Objekte sofort von StorageGRID auf zwei Storage-Nodes am selben Standort übertragen und ILM wird später ausgewertet. 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.

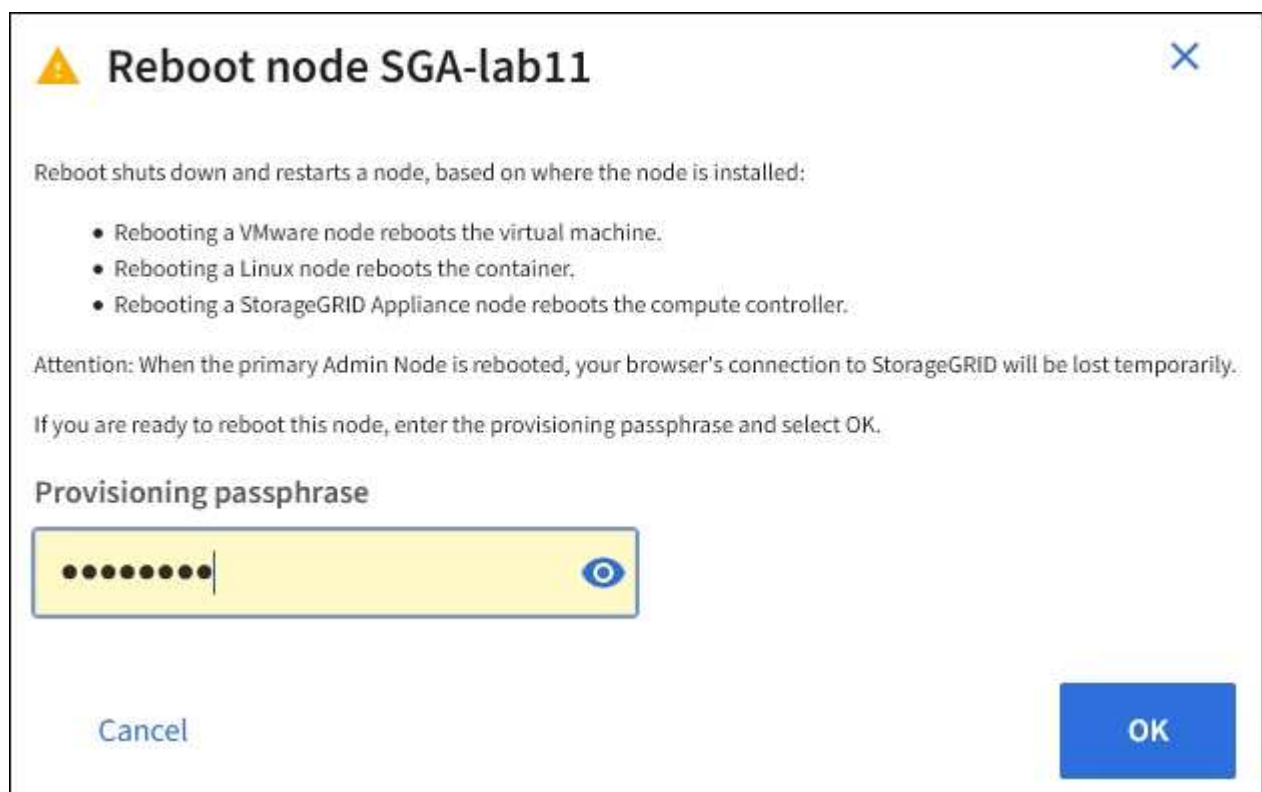
Schritte

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



4. Wählen Sie **Neustart**.

Ein Bestätigungsdialogfeld wird angezeigt.



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

5. Geben Sie die Provisionierungs-Passphrase ein, und klicken Sie auf **OK**.

6. Warten Sie, bis der Node neu gebootet wird.

Es kann einige Zeit dauern, bis Dienste heruntergefahren werden.

Wenn der Knoten neu gestartet wird, wird das graue Symbol (Administrativ Down) auf der linken Seite der Seite **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.

DC1-S1 (Storage Node) [🔗](#)

[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

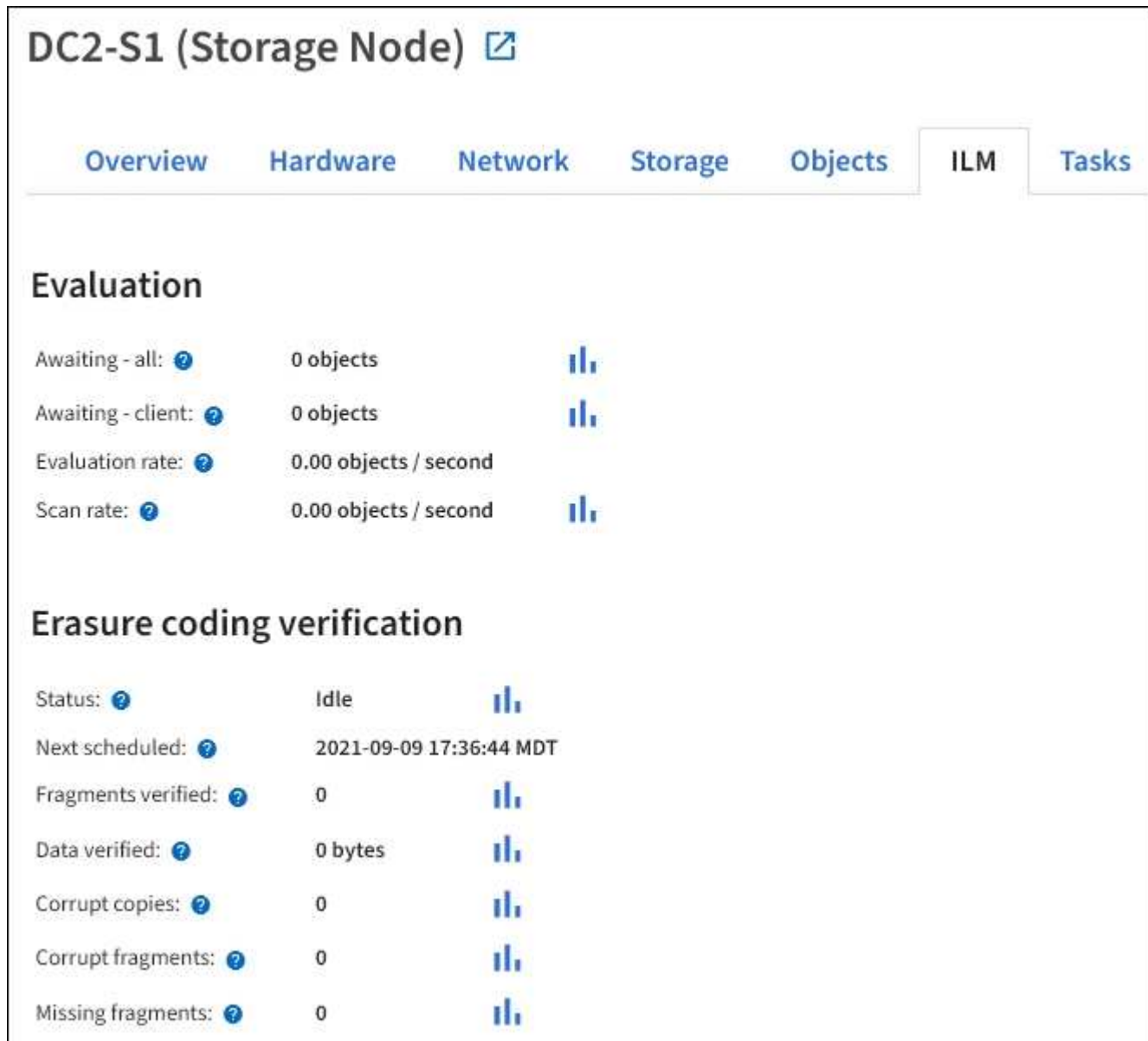
Quarantined objects: [?](#) 0

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.



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.

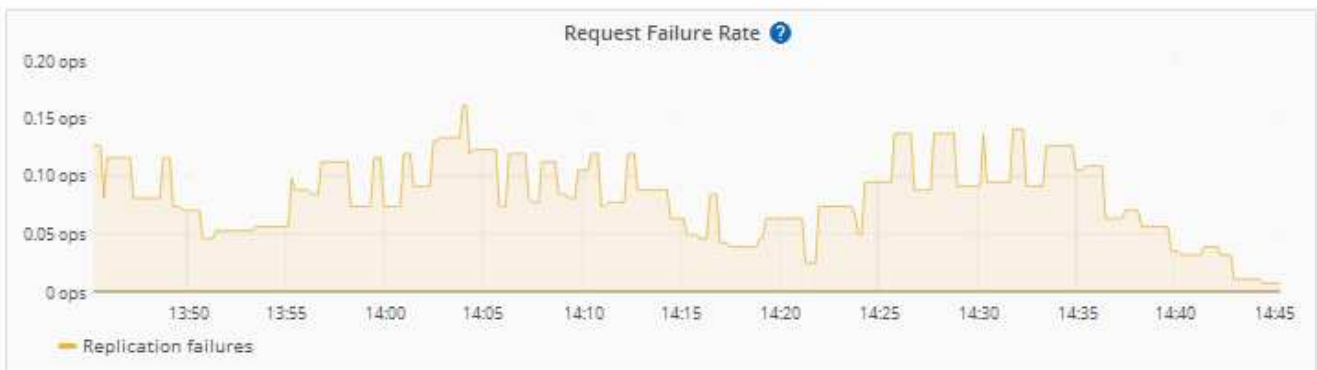
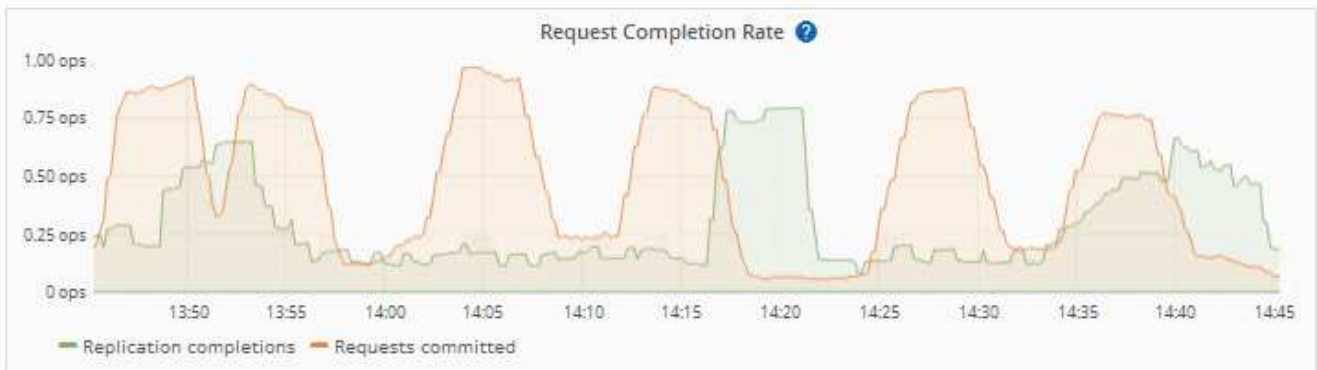
1 hour

1 day

1 week

1 month

Custom



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.



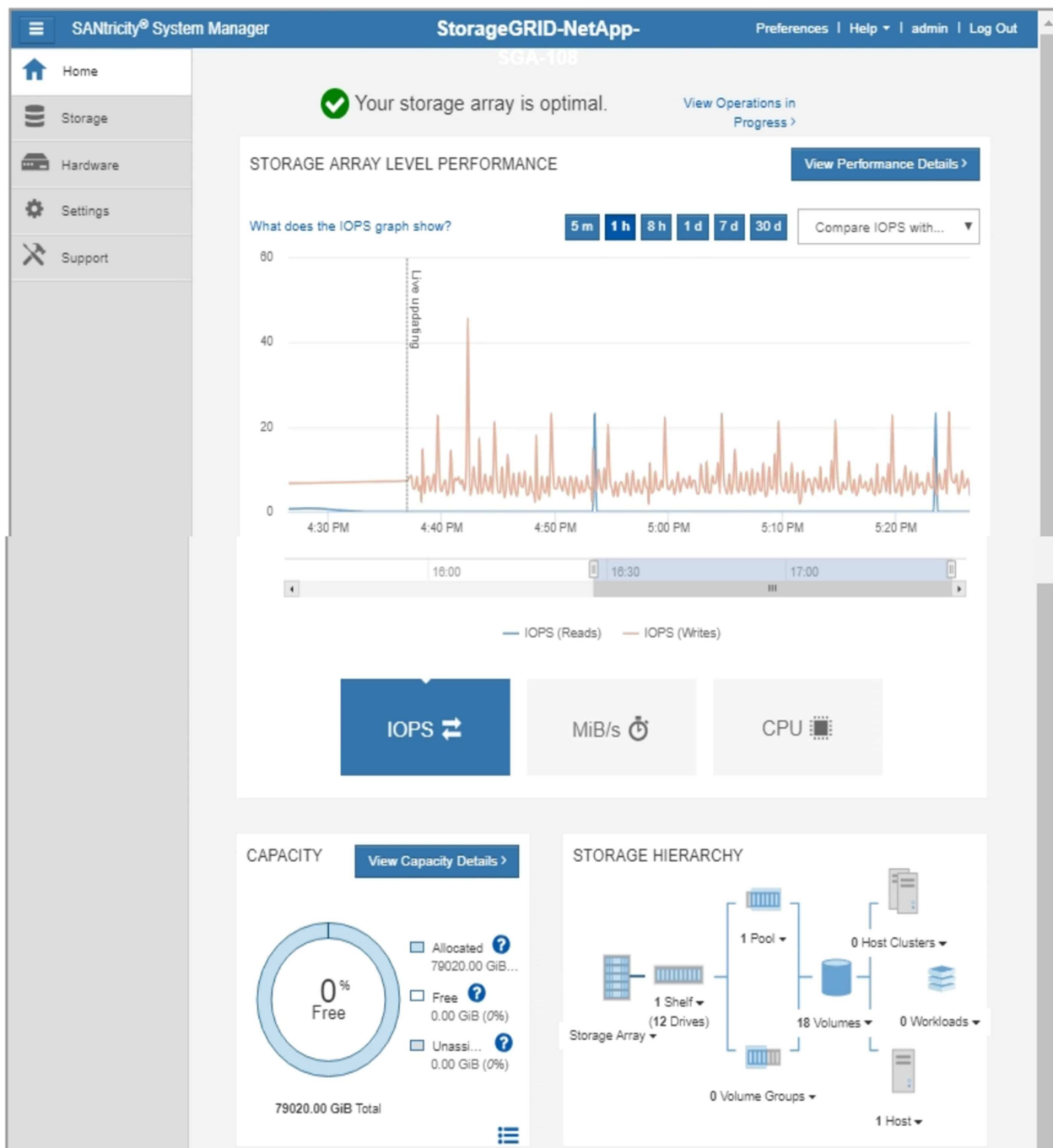
Der Zugriff auf den SANtricity System Manager über den Grid Manager erlaubt in der Regel nur die Überwachung der Appliance-Hardware und die Konfiguration der E-Series AutoSupport. Viele Funktionen und Vorgänge in SANtricity System Manager, z. B. ein Firmware-Upgrade, gelten nicht für das Monitoring Ihrer 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 unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen. Die Warnung * kann nicht mit Node* kommunizieren. Auch andere Warnmeldungen können aktiv sein. Diese Situation erfordert sofortige Aufmerksamkeit.



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

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

Schritte

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

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

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

Name

StorageGRID Webscale Deployment

DC1

DC1-ADM1

DC1-ARC1

DC1-G1

DC1-S1

DC1-S2

DC1-S3

DC2

DC2-ADM1

DC2-ARC1

DC2-ARC1 (Archive Node)

Overview Hardware Network Storage Tasks

Node information

Name: DC2-ARC1

Type: Archive Node

ID: 202ef603-db47-4c90-8b19-afba46e82393

Connection state: Unknown

Software version: 11.6.0 (build 20210924.1557.00a5eb9)

IP addresses: 172.16.1.236 - eth0 (Grid Network)
10.224.1.236 - eth1 (Admin Network)

Show additional IP addresses

Alerts

Alert name	Severity	Time triggered	Current values
Unable to communicate with node	Major	9 days ago	Unresponsive services: arc, dynip, ssm

2. Wenn ein Knoten über ein blaues Symbol verfügt, führen Sie die folgenden Schritte aus:

- 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.

- 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.

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

Verwandte Informationen

[Alerts Referenz](#)

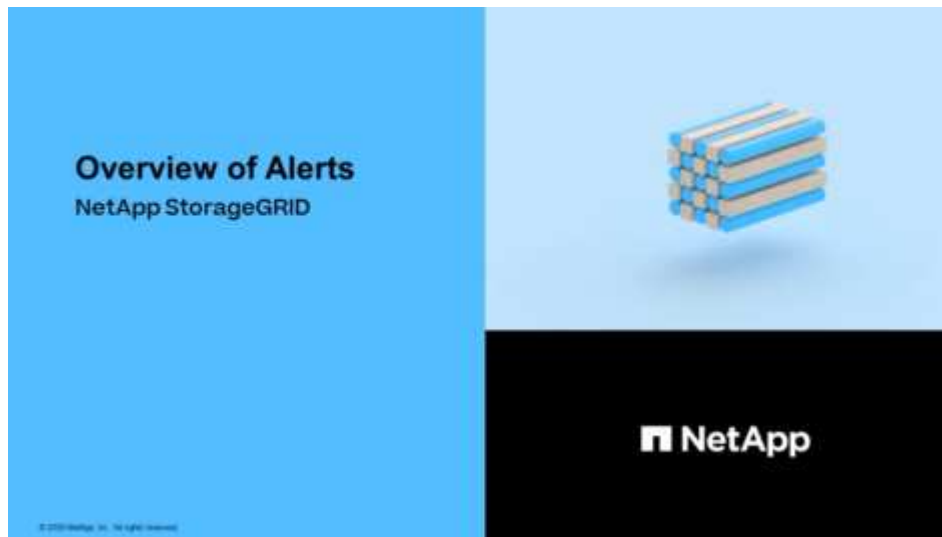
[Recovery und Wartung](#)

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.

☒ Group alerts Active							
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 (newest) 19 minutes ago (oldest)		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 (newest) a day ago (oldest)		8 Active			

Standardmäßig werden Alarmer 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	Der Schweregrad der Meldung. Wenn mehrere Warnungen gruppiert sind, zeigt die Titelzeile an, wie viele Instanzen dieser Warnung bei jedem Schweregrad auftreten. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • Major : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • Klein : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem 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.

☒ 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.

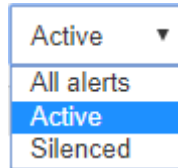
☐ Group alerts
 Active ▼

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

Last week

Filter by severity

Filter by rule

Filter by node

Search

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

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

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

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

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

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

- b. Wählen Sie im Dropdown-Menü **Severity** einen oder mehrere Schweregrade aus, um nach gelösten Warnmeldungen eines bestimmten Schweregrads zu filtern.

- c. Wählen Sie im Dropdown-Menü **Warnregel** eine oder mehrere Standard- oder benutzerdefinierte Warnungsregeln aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einer bestimmten Alarmregel zusammenhängen.

- d. Wählen Sie im Dropdown-Menü **Node** einen oder mehrere Knoten aus, um nach aufgelösten Warnmeldungen zu filtern, die mit einem bestimmten Knoten verbunden sind.

- e. Klicken Sie Auf **Suchen**.

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

Ein Dialogfeld für die Meldung wird angezeigt. Siehe [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

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

Warnmeldung anzeigen möchten:

Spaltenüberschrift	Beschreibung
Aktuelle Meldung	- 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	- 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	
Low installed node memory The amount of installed memory on a node is low.	✖ 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	Der Schweregrad der Meldung. • * Kritisch* : Es besteht eine anormale Bedingung, die die normalen Vorgänge eines StorageGRID-Knotens oder -Dienstes gestoppt hat. Sie müssen das zugrunde liegende Problem sofort lösen. Wenn das Problem nicht behoben ist, kann es zu Serviceunterbrechungen und Datenverlusten kommen. • Major : Es besteht eine anormale Bedingung, die entweder die aktuellen Operationen beeinflusst oder sich dem Schwellenwert für eine kritische Warnung nähert. Sie sollten größere Warnmeldungen untersuchen und alle zugrunde liegenden Probleme beheben, um sicherzustellen, dass die anormale Bedingung den normalen Betrieb eines StorageGRID Node oder Service nicht beendet. • Klein : Das System funktioniert normal, aber es besteht eine anormale Bedingung, die die Fähigkeit des Systems beeinträchtigen könnte, zu arbeiten, wenn es fortgesetzt wird. Sie sollten kleinere Warnmeldungen überwachen und beheben, die sich nicht selbst beheben lassen, um sicherzustellen, dass sie nicht zu einem schwerwiegenden Problem führen.
Datenwerte	Der aktuelle Wert der Metrik für diese Meldung. Für manche Warnmeldungen werden zusätzliche Werte angezeigt, die Ihnen helfen, die Warnmeldung zu verstehen und zu untersuchen. Die Werte für eine Warnung für Low-Metadaten-Speicher enthalten beispielsweise den Prozentsatz des belegten Speicherplatzes, den gesamten Speicherplatz und die Menge des verwendeten Festplattenspeichers.

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

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



Seien Sie vorsichtig, wenn Sie sich entscheiden, eine Alarmregel zu stummschalten. 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 50 Records Per Page

Previous 1 Next

Das Alarmsymbol zeigt den Schweregrad jedes Alarms wie folgt an:

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

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		☐

Apply Changes 

- Wenn Sie die Anzahl der aktuellen Alarmer löschen möchten, können Sie optional Folgendes tun:
 - Bestätigen Sie den Alarm. Ein bestätigter Alarm wird nicht mehr in die Anzahl der älteren Alarmer 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

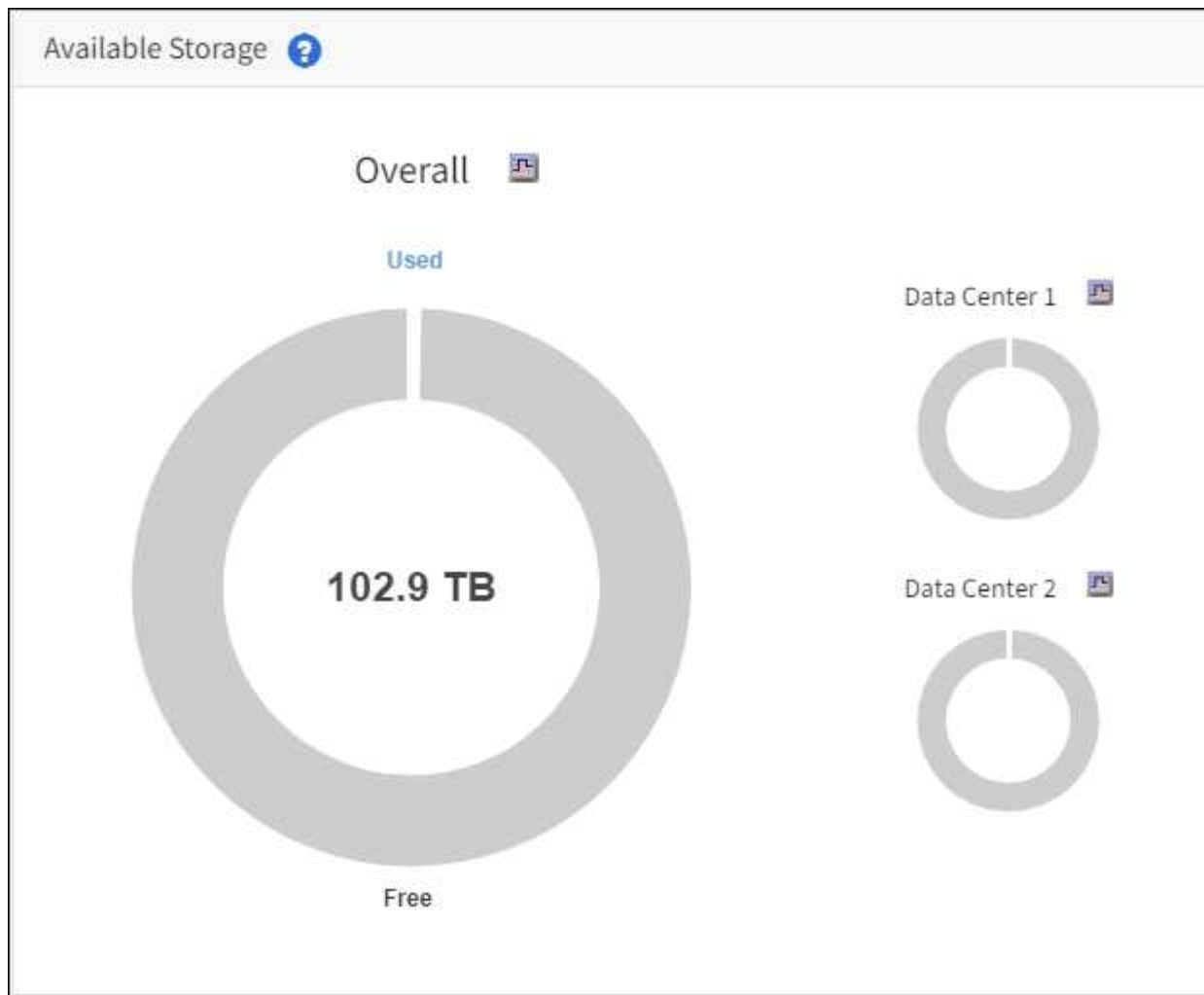
Über das Dashboard im Grid Manager können Sie schnell ermitteln, wie viel Storage für das gesamte Grid und für jedes Datacenter zur Verfügung steht. Die Seite Knoten enthält detailliertere Werte für Objektdaten und Objektmetadaten.

Schritte

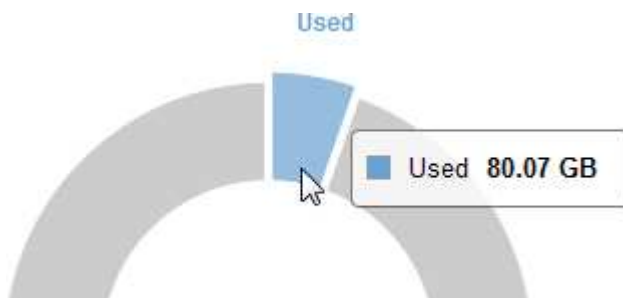
1. Beurteilen Sie, wie viel Storage für das gesamte Grid und das jeweilige Datacenter verfügbar ist.
 - a. Wählen Sie **Dashboard**.
 - b. Notieren Sie sich im Fenster Verfügbare Speicherkapazität die Zusammenfassung der freien und genutzten Speicherkapazität.



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.

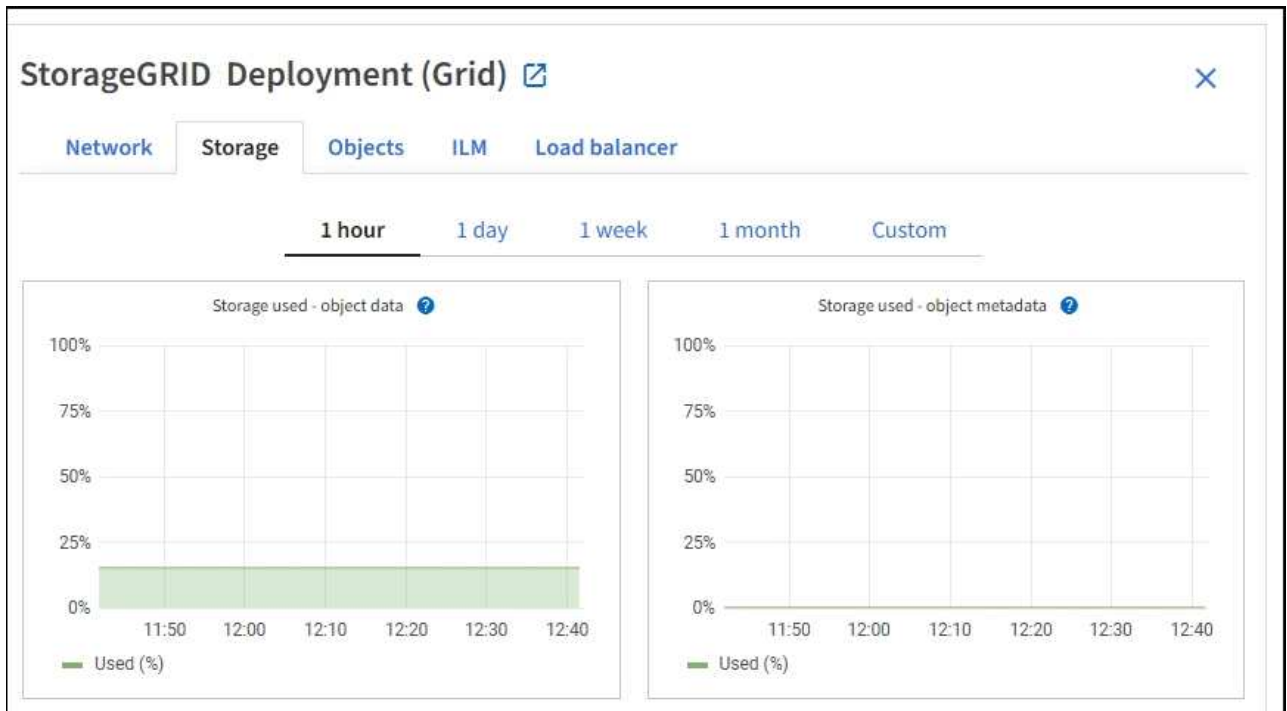


- b. Sehen Sie sich das Diagramm für die einzelnen Datacenter an, um Grids für mehrere Standorte zu verwenden.
- c. Klicken Sie auf das Diagrammsymbol  Für das Gesamtdiagramm oder für ein einzelnes Datacenter, um ein Diagramm anzuzeigen, in dem die Kapazitätsauslastung im Laufe der Zeit dargestellt wird.

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.

- Wählen Sie **KNOTEN**.
- Wählen Sie **Grid Storage** aus.



- 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.

- 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

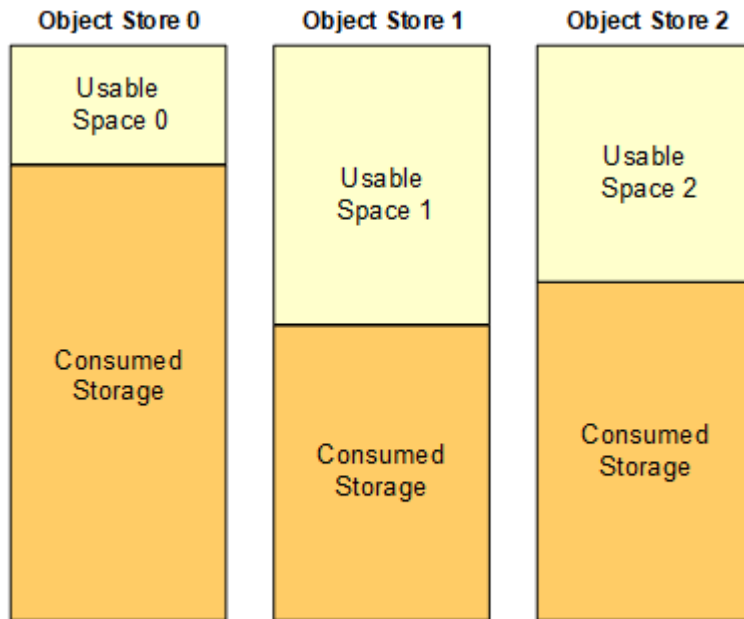
Überwachen Sie den insgesamt nutzbaren Speicherplatz für jeden Storage-Node, um sicherzustellen, dass der Node über ausreichend Speicherplatz für neue Objektdaten verfügt.

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

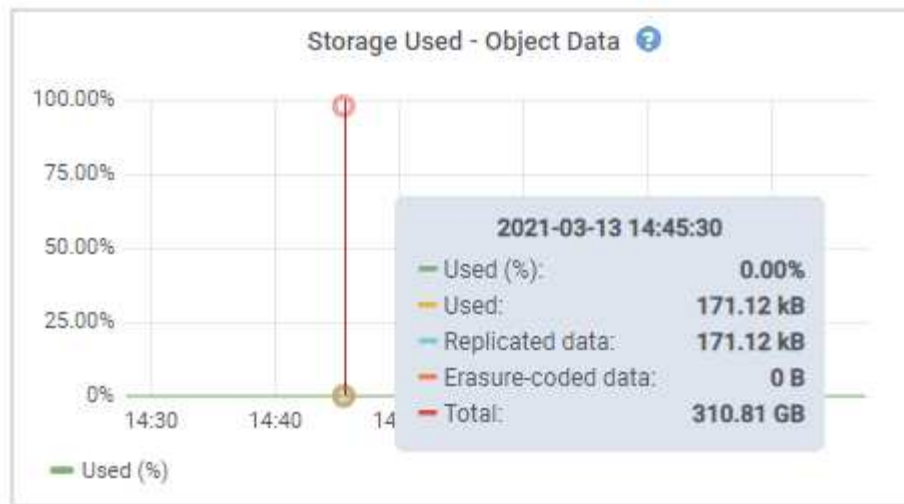
1. Wählen Sie **NODES Storage Node Storage** aus.

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.
- **Erasure-codierte Daten:** Eine Schätzung der Menge der mit der Löschung codierten Objektdaten auf diesem Knoten, Standort oder Grid.
- **Gesamt:** Die Gesamtmenge an nutzbarem Speicherplatz auf diesem Knoten, Standort oder Grid. Der verwendete Wert ist der `storagegrid_storage_utilization_data_bytes` Metrisch.



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



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

Disk devices

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

Volumes

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

Object stores

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

- 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 Objektmeterdaten 100 % des zulässigen Metadaten-Speicherplatzes übersteigen.

Was Sie benötigen

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

Über diese Aufgabe

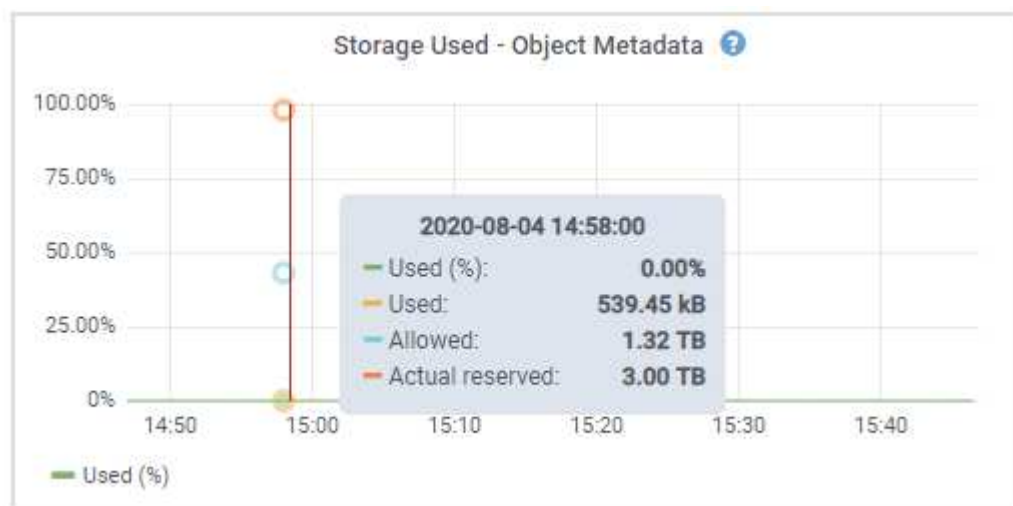
StorageGRID behält drei Kopien von Objektmeterdaten an jedem Standort vor, um Redundanz zu gewährleisten und Objekt-Meterdaten vor Verlust zu schützen. Die drei Kopien werden gleichmäßig über alle Storage-Nodes an jedem Standort verteilt. Dabei wird der für Metadaten reservierte Speicherplatz auf dem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

In einigen Fällen wird die Kapazität der Objektmeterdaten 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 – Objektmeterdaten“, 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.

- 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

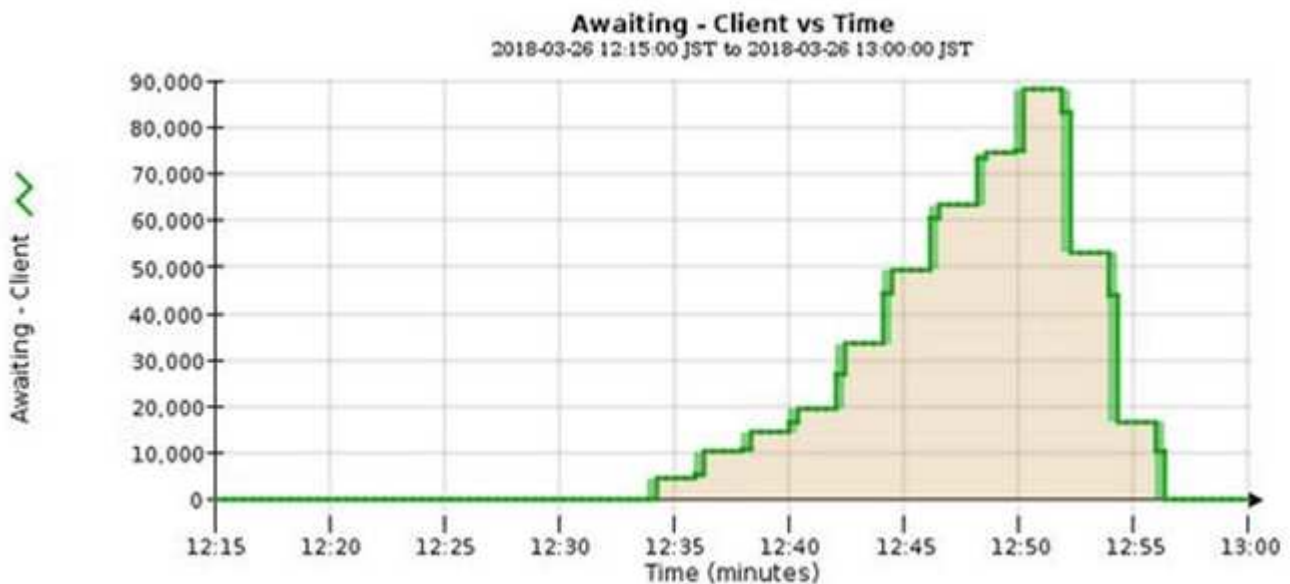
Das StorageGRID System managt Objekte mithilfe der aktiven ILM-Richtlinie. Die ILM-Richtlinie und die zugehörigen ILM-Regeln bestimmen die Anzahl der Kopien, die Art der erstellten Kopien, das Erstellen von Kopien und die Dauer der Aufbewahrung jeder Kopie.

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

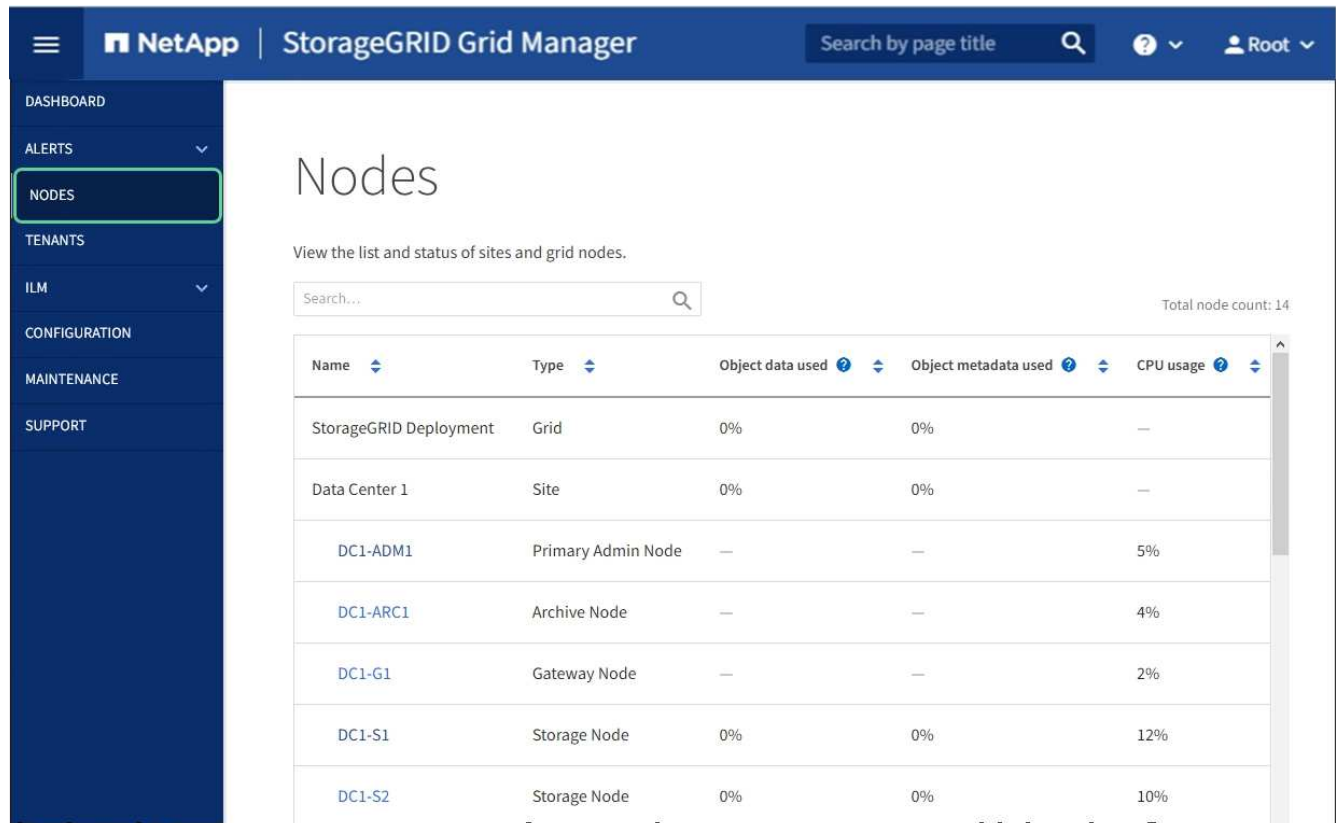
Probleme umgehend beheben können.

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.



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.

+ Create ✎ Edit ✕ Remove 📊 Metrics			
	Name	Description	ID
☐	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒	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

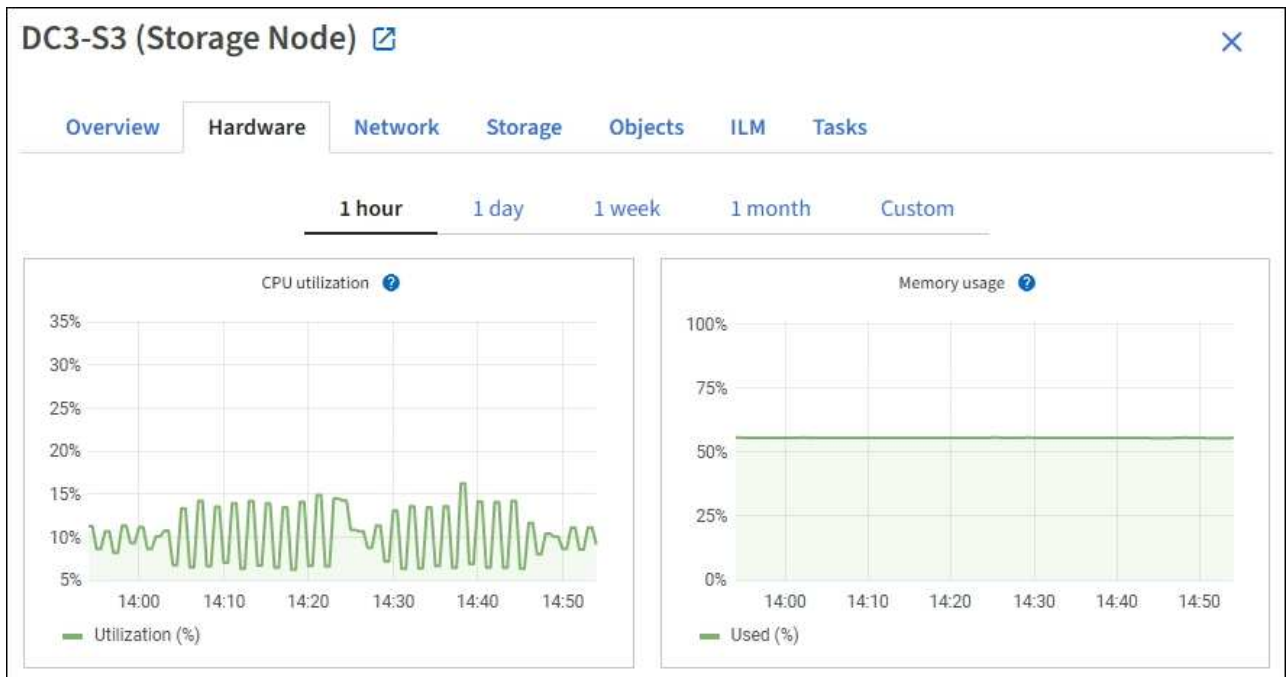
- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

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.

Create
Export to CSV
Actions ▾

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

Sie können sich bei einem Mandantenkonto anmelden, indem Sie auf den Anmeldelink 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.

- 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.

- 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 
Protocol: S3
Object count: 500

Quota utilization: 85%
Logical space used: 85.00 GB
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

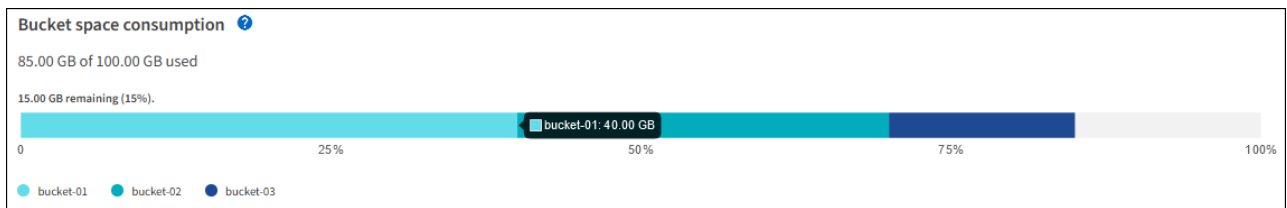
Der Übersichtsbereich für den Mandanten enthält Werte für die Objektanzahl, die Kontingentnutzung, der verwendete logische Speicherplatz und die Kontingenteinstellung.

◦ 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.

+ Create Edit ✕ Remove Metrics			
	Name	Description	ID
☐	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒	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

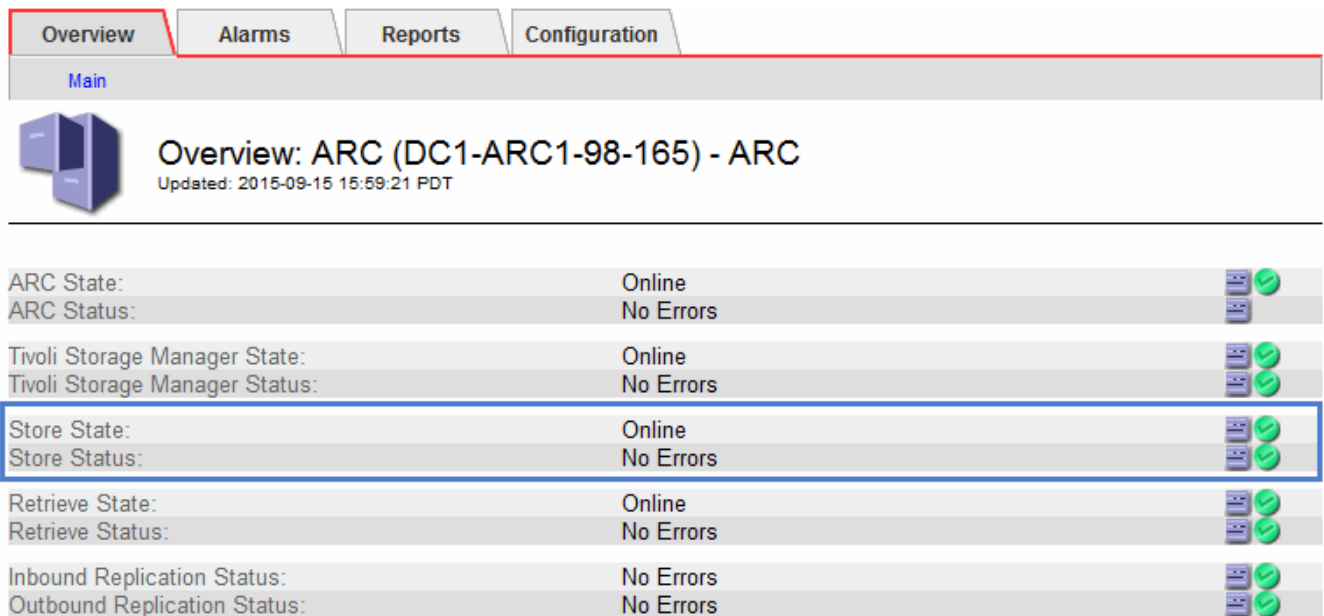
- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 **Archivknoten ARC Übersicht Haupt**.
3. Überprüfen Sie die Attribute „Speicherstatus“ und „Speicherstatus“, um zu bestätigen, dass die Komponente „Speicher“ ohne Fehler online ist.



Overview	Alarms	Reports	Configuration
Main			
 Overview: ARC (DC1-ARC1-98-165) - ARC Updated: 2015-09-15 15:59:21 PDT			
ARC State:	Online		
ARC Status:	No Errors		
Tivoli Storage Manager State:	Online		
Tivoli Storage Manager Status:	No Errors		
Store State:	Online		
Store Status:	No Errors		
Retrieve State:	Online		
Retrieve Status:	No Errors		
Inbound Replication Status:	No Errors		
Outbound Replication Status:	No Errors		

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 Lastausgleichsvorgänge 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

Alarmer und Alarmer 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?	• Klicken Sie auf dem Dashboard auf den Link Aktuelle Alarme. • Wählen Sie die Warnmeldung auf der Seite NODES Übersicht aus. • Wählen Sie ALERTS Current. Anzeigen aktueller Warnmeldungen	Wählen Sie SUPPORT Alarme (alt) Aktuelle Alarme. Verwalten von Alarmen (Altsystem)
Was bewirkt, dass eine Warnung oder ein Alarm ausgelöst wird?	Alarme werden ausgelöst, wenn ein Prometheus-Ausdruck in einer Alarmregel für die spezifische Triggerbedingung und -Dauer als wahr bewertet wird. Zeigen Sie Alarmregeln an	Alarme werden ausgelöst, wenn ein StorageGRID-Attribut einen Schwellenwert erreicht. Verwalten von Alarmen (Altsystem)

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

	Meldungen	Alarme (Altsystem)
Wie managt ich E-Mail-Benachrichtigungen?	Wählen Sie ALERTS E-Mail-Einrichtung. Hinweis: Da Alarme und Alarme unabhängige Systeme sind, wird das E-Mail-Setup für Alarm- und AutoSupport-Benachrichtigungen nicht für Benachrichtigungen verwendet. Sie können jedoch denselben E-Mail-Server für alle Benachrichtigungen verwenden. Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein	Wählen Sie SUPPORT Alarme (alt) Legacy E-Mail-Einrichtung. Verwalten von Alarmen (Altsystem)
Wie verwalte ich SNMP Benachrichtigungen?	Wählen Sie KONFIGURATION Überwachung SNMP-Agent. Verwenden Sie SNMP-Überwachung	Wählen Sie KONFIGURATION Überwachung SNMP-Agent. Verwenden Sie SNMP-Überwachung Hinweis: SNMP-Benachrichtigungen werden nicht für jeden Alarm oder Alarm Schweregrad gesendet. Warnmeldungen, die SNMP-Benachrichtigungen generieren (Legacy-System)
Wie kontrolliere ich, wer Benachrichtigungen erhält?	1. Wählen Sie 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. Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein	1. Wählen Sie SUPPORT Alarme (alt) Legacy E-Mail-Einrichtung. 2. Mailingliste wird erstellt. 3. Wählen Sie Benachrichtigungen. 4. Wählen Sie die Mailingliste aus. Verwalten von Alarmen (Altsystem)
Welche Admin Nodes senden Benachrichtigungen?	Ein einziger Admin-Node (der „bevorzugte Absender“). StorageGRID verwalten	Ein einziger Admin-Node (der „bevorzugte Absender“). StorageGRID verwalten

	Meldungen	Alarme (Altsystem)
Wie kann ich einige Benachrichtigungen unterdrücken?	1. Wählen Sie 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. Hinweis: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. Benachrichtigung über Stille	1. Wählen Sie SUPPORT Alarme (alt) Legacy E-Mail-Einrichtung. 2. Wählen Sie Benachrichtigungen. 3. Wählen Sie eine Mailingliste aus, und wählen Sie unterdrücken. Verwalten von Alarmen (Altsystem)
Wie kann ich alle Benachrichtigungen unterdrücken?	Wählen Sie ALERTS stumm und dann Alle Regeln. Hinweis: Wenn Sie den SNMP-Agent aktiviert haben, unterdrücken Stille auch SNMP-Traps und informieren. Benachrichtigung über Stille	1. Wählen Sie KONFIGURATION System Anzeigeeoptionen. 2. Aktivieren Sie das Kontrollkästchen Benachrichtigung Alle unterdrücken. Hinweis: Das Unterdrückung von E-Mail-Benachrichtigungen systemweit unterdrückt auch ereignisgesteuerte AutoSupport-E-Mails. Verwalten von Alarmen (Altsystem)
Wie kann ich die Bedingungen und Trigger anpassen?	1. Wählen Sie ALERTS Regeln. 2. Wählen Sie eine Standardregel zum Bearbeiten aus, oder wählen Sie benutzerdefinierte Regel erstellen. Bearbeiten von Meldungsregeln Erstellen benutzerdefinierter Warnungsregeln	1. Wählen Sie SUPPORT Alarme (alt) Globale Alarme. 2. Erstellen Sie einen globalen benutzerdefinierten Alarm, um einen Standardalarm zu überschreiben oder ein Attribut zu überwachen, das keinen Standardalarm hat. Verwalten von Alarmen (Altsystem)

	Meldungen	Alarme (Altsystem)
Wie deaktiviere ich eine einzelne Warnung oder einen einzelnen Alarm?	1. Wählen Sie ALERTS Regeln. 2. Wählen Sie die Regel aus, und wählen Sie Regel bearbeiten. 3. Deaktivieren Sie das Kontrollkästchen aktiviert. Deaktivieren von Meldungsregeln	1. Wählen Sie SUPPORT Alarme (alt) Globale Alarme. 2. Wählen Sie die Regel aus, und wählen Sie das Symbol Bearbeiten aus. 3. Deaktivieren Sie das Kontrollkästchen aktiviert. Verwalten von Alarmen (Altsystem)

Verwalten von Meldungen

Benachrichtigungen verwalten: Übersicht

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

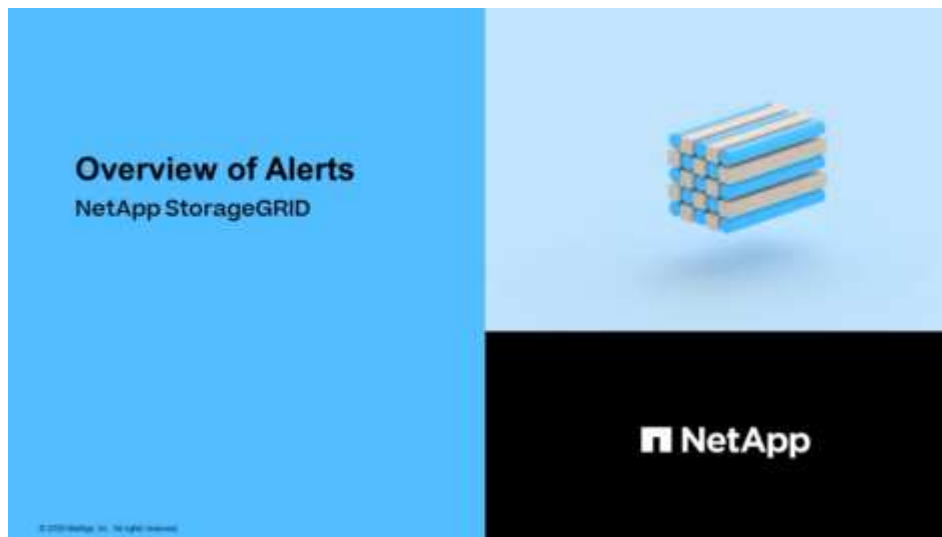
Warnmeldungen“ angezeigten Warnmeldungen enthalten empfohlene Aktionen zur Behebung von Warnmeldungen. Dazu gehören häufig direkte Links zum StorageGRID Dokumentationszentrum, damit detailliertere Fehlerbehebungsmaßnahmen leichter gefunden und zugänglich sind.

- 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.

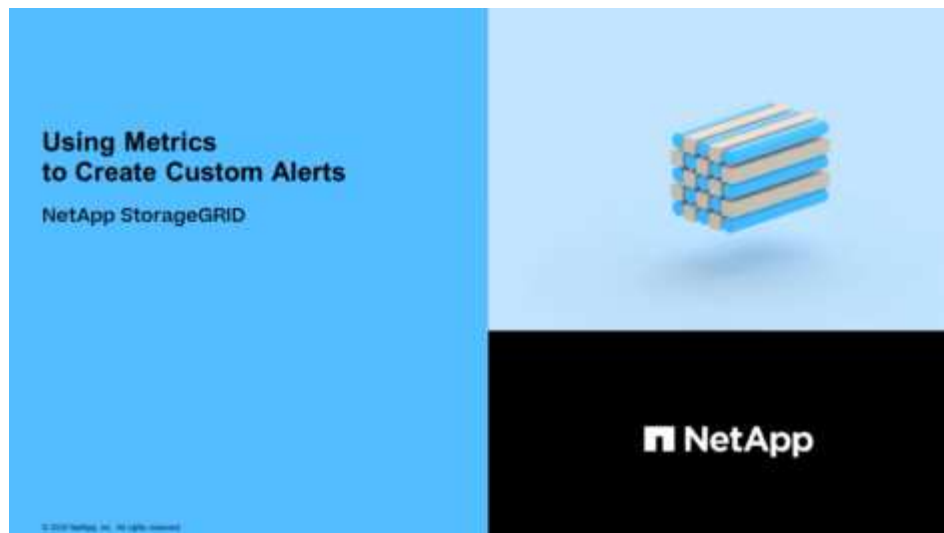
Weitere Informationen .

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

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



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



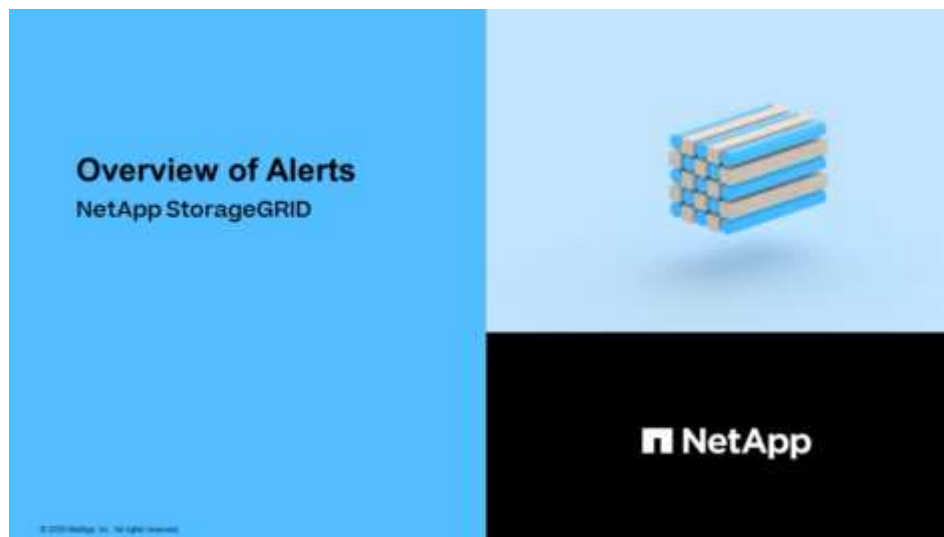
Zeigen Sie Alarmregeln an

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

Create custom rule

Edit rule

Remove custom rule

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

Displaying 62 alert rules.

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

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

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

Erstellen benutzerdefinierter Warnungsregeln

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

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 Formatierungscode). 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 Low installed node memory

Description The amount of installed memory on a node is low.

Recommended Actions (optional)

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](#)

Conditions

Minor

Major

Critical

node_memory_MemTotal_bytes < 24000000000

node_memory_MemTotal_bytes <= 12000000000

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

Duration

2

minutes

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 Formatierungscode). 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	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	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 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
```

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 ?	10.224.1.250
Port ?	25
Username (optional) ?	smtpuser
Password (optional) ?	*****

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 ?	storagegrid-alerts@example.com	
Recipient 1 ?	recipient1@example.com	✕
Recipient 2 ?	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-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Send Client Certificate  ☒

Client Certificate 

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

Private Key 

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----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
Jede Warnbenachrichtigung gilt nur für Warnungen, die denselben Namen haben. Wenn zwei Benachrichtigungen mit verschiedenen Namen gleichzeitig ausgelöst werden, werden zwei E-Mail-Benachrichtigungen gesendet.	- Bei zwei Nodes wird gleichzeitig ein Alarm A ausgelöst. Es wird nur eine Benachrichtigung gesendet. - Bei Knoten 1 wird die Warnmeldung A ausgelöst, und gleichzeitig wird auf Knoten 2 die Warnmeldung B ausgelöst. Für jede Warnung werden zwei Benachrichtigungen gesendet.
Wenn für eine bestimmte Warnmeldung auf einem bestimmten Node die Schwellenwerte für mehr als einen Schweregrad erreicht werden, wird eine Benachrichtigung nur für die schwerste Warnmeldung gesendet.	Die Warnmeldung A wird ausgelöst und die kleineren, größeren und kritischen Alarmschwellenwerte werden erreicht. Eine Benachrichtigung wird für die kritische Warnmeldung gesendet.
Bei der ersten Alarmauslösung wartet StorageGRID zwei Minuten, bevor eine Benachrichtigung gesendet wird. Wenn während dieser Zeit andere Warnmeldungen mit demselben Namen ausgelöst werden, gruppiert StorageGRID alle Meldungen in der ersten Benachrichtigung.	- An Knoten 1 um 08:00 wird eine Warnmeldung A ausgelöst. Es wird keine Benachrichtigung gesendet. - An Knoten 2 um 08:01 wird eine Warnmeldung A ausgelöst. Es wird keine Benachrichtigung gesendet. - Um 08:02 Uhr wird eine Benachrichtigung gesendet, um beide Instanzen der Warnmeldung zu melden.
Falls eine weitere Benachrichtigung mit demselben Namen ausgelöst wird, wartet StorageGRID 10 Minuten, bevor eine neue Benachrichtigung gesendet wird. Die neue Benachrichtigung meldet alle aktiven Warnungen (aktuelle Warnungen, die nicht stummgeschaltet wurden), selbst wenn sie zuvor gemeldet wurden.	- An Knoten 1 um 08:00 wird eine Warnmeldung A ausgelöst. Eine Benachrichtigung wird um 08:02 Uhr gesendet. - 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.
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.	- Für Knoten 1 wird eine Warnmeldung A ausgelöst. Eine Benachrichtigung wird gesendet. - Für Knoten 2 wird eine Warnmeldung A ausgelöst. Eine zweite Benachrichtigung wird gesendet. - Die Warnung A wird für Knoten 2 behoben, bleibt jedoch für Knoten 1 aktiv. - Für Node 2 wird erneut eine Warnmeldung A ausgelöst. Es wird keine neue Benachrichtigung gesendet, da die Meldung für Node 1 noch aktiv ist.

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

Beheben Sie Warnmeldungen bei E-Mail-Benachrichtigungen

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

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
No results found.				

2. Wählen Sie **Erstellen**.

Das Dialogfeld Stille erstellen wird angezeigt.

Create Silence

Alert Rule

Description (optional)

Duration Minutes ▼

Severity ☐ Minor only ☐ Minor, major ☐ Minor, major, critical

Nodes ☐ StorageGRID Deployment

- ☐ Data Center 1
 - ☐ DC1-ADM1
 - ☐ DC1-G1
 - ☐ DC1-S1
 - ☐ DC1-S2
 - ☐ DC1-S3

Cancel Save

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

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

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

4. 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	- 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	- 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. Hinweis: Benachrichtigungen werden jetzt gesendet, wenn diese Warnung ausgelöst wird (es sei denn, sie werden durch eine andere Stille unterdrückt). Wenn diese Warnmeldung derzeit ausgelöst wird, kann es einige Minuten dauern, bis E-Mail- oder SNMP-Benachrichtigungen gesendet werden und die Seite „Meldungen“ aktualisiert wird.

Verwandte Informationen

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

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 Schwellwert eingestellt werden. Der NMS-Service auf jedem Admin-Node überwacht kontinuierlich die aktuellen Attributwerte im

Vergleich zu konfigurierten Schwellenwerten. Wenn ein Alarm ausgelöst wird, wird eine Benachrichtigung an alle designierten Mitarbeiter gesendet.

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

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

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

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

Beispiel für Alarmauslösung

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

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

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

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

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

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

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

Alarme desselben Schweregrades

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

Wenn UMEM beispielsweise auf 50 MB abfällt, wird der erste Alarm ausgelöst (= 500000000), nicht jedoch der untere Alarm (\=100000000).



Global Alarms

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

Global Custom Alarms (0 Result(s))

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

Wird die Reihenfolge umgekehrt, wenn UMEM auf 100MB fällt, wird der erste Alarm (\=100000000) ausgelöst, nicht jedoch der darunter stehende Alarm (= 500000000).



Global Alarms

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

Global Custom Alarms (0 Result(s))

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

Default Alarms

Filter by Disabled Defaults 

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions

Apply Changes 

Benachrichtigungen

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

Um zu vermeiden, dass bei Erreichen eines Alarmschwellenwerts mehrere Alarme und Benachrichtigungen gesendet werden, wird der Schweregrad des Alarms anhand des aktuellen Alarmschwerfalls für das Attribut

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

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

Neuer Services

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

Alarme und Tabellen

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

Die folgende Tabelle zeigt beispielsweise zwei kritische Einträge (VMFI)-Alarme. (Wählen Sie **SUPPORT Tools Grid-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 50 Records Per Page Refresh 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		☐

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
☐								

Default Alarms

Filter by equals

221 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
☒		IQSZ (Number of Objects)	Major	Greater than 10,000,000	>=	10000000	
☒		IQSZ (Number of Objects)	Minor	Greater than 1,000,000	>=	1000000	
☒		IQSZ (Number of Objects)	Notice	Greater than 150,000	>=	150000	
☒		XCVP (% Completion)	Notice	Foreground Verification Completed	=	100	
☒	ADC	ADCA (ADC Status)	Minor	Error	>=	10	
☒	ADC	ADCE (ADC State)	Notice	Standby	=	10	
☒	ADC	ALIS (Inbound Attribute Sessions)	Notice	Over 100	>=	100	
☒	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
☒	ARC	ARCE (ARC State)	Notice	Standby	=	10		
☒	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000		
☒	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
☒	ARC	ARCE (ARC State)	Notice	Standby	=	10	
☒	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000	
☒	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000	
☒	ARC	ARRF (Request Failures)	Major	At least 1	>=	1	
☒	ARC	ARRV (Verification Failures)	Major	At least 1	>=	1	
☒	ARC	ARVF (Store Failures)	Major	At least 1	>=	1	
☒	NMS	ARRC (Remaining Capacity)	Notice	Below 10	<=	10	
☒	NMS	ARRS (Repository Status)	Major	Disconnected	<=	9	
☒	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 Alarmer“ kopiert.

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

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

Überschrift	Beschreibung
Attribut	Wählen Sie den Namen und den Code des zu überwachenden Attributs aus der Liste aller Attribute aus, die für den ausgewählten Dienst oder die ausgewählte Komponente gelten. Um Informationen über das Attribut anzuzeigen, klicken Sie auf Info  Neben dem Namen des Attributs.
Schweregrad	Das Symbol und der Text, der die Alarmstufe angibt.
Nachricht	Der Grund für den Alarm (Verbindung unterbrochen, Lagerraum unter 10 % usw.).
Operator	Operatoren für das Testen des aktuellen Attributwerts gegen den Wert-Schwellenwert: • = gleich • Größer als • Kleiner als • = größer als oder gleich • \= kleiner als oder gleich • ≠ ist nicht gleich
Wert	Der 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. 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.
Aktionen	Steuertasten zu:  Bearbeiten Sie eine Zeile +  Eine Zeile einfügen +  Löschen Sie eine Zeile +  Ziehen Sie eine Zeile nach oben oder unten +  Kopieren Sie eine Zeile

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

Deaktivieren von Alarmen (Legacy-System)

Die Alarme im alten Alarmsystem sind standardmäßig aktiviert, 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
☐								   

Default Alarms

Filter by equals 

3 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
☒	SSM	UMEM (Available Memory)	 Critical	Under 10000000	<=	10000000	 
☒	SSM	UMEM (Available Memory)	 Major	Under 50000000	<=	50000000	 
☐	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 Alarmer 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 Alarmer (alt) Globale Alarmer**.
2. Klicken Sie in der Tabelle Globale benutzerdefinierte Alarmer 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
☐	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

Port

Authentication

Authentication Credentials

From Address

Test E-mail

Off

Username: root

Password:

To:

☐ 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 kommasetrennte 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
		All Email Lists	From SGWS	
Template One	Notifications			  

Show Records Per Page

« »

Apply Changes 

- 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-Nachrichtentextes 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
			  

Show Records Per Page

« »

Apply Changes



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 Alarmer 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 Alarmer 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 Alarmer unabhängig vom Schweregrad erhalten. Eine andere Gruppe benötigt möglicherweise nur Benachrichtigungen für Alarmer 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 Alarmer (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 Alarmer 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 Anzeigoptionen**.
2. Wählen Sie im Menü Anzeigoptionen 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	☒

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.

- 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.

- 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.

- 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 Protokolldaten 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):

Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate

Audit Log Average Size = (570 + K) bytes

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

Schätzformeln für nicht standardmäßige Audit-Level

Die für Prüfprotokolle bereitgestellten Formeln setzen voraus, dass die standardmäßigen Einstellungen für die Revisionsstufe verwendet werden (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist). Detaillierte Formeln zur Schätzung der Rate und der durchschnittlichen Größe von 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-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

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

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

Wenn Ihr Grid beispielsweise 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.

 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



REL/TCP



REL/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
broadcast.log	Benutzer oder Daemon
broadcast-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	Demon (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
3 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 Protokolldaten 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 Alarme und Alarme. Die MIB enthält auch Informationen zur Systembeschreibung wie Plattform und Modellnummer für jeden Knoten. Jeder StorageGRID-Knoten unterstützt auch eine Untergruppe von MIB-II-Objekten.

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

StorageGRID-Knoten die gleiche Konfiguration.

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

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

Traps werden in allen drei Versionen von SNMP unterstützt.

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

Die Informationsunterstützung wird in SNMPv2c und SNMPv3 unterstützt.

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

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

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 Alarmer (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.

The screenshot shows a dialog box titled "Create Agent Address". It has four main sections: "Internet Protocol" with radio buttons for "IPv4" (selected) and "IPv6"; "Transport Protocol" with radio buttons for "UDP" (selected) and "TCP"; "StorageGRID Network" with a dropdown menu showing "Grid, Admin, and Client Networks"; and "Port" with a text input field containing "161". At the bottom right, there are two buttons: "Cancel" and "Create".

- 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
☐	IPv4	UDP	Grid Network	161
☒	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

SHA

Password

Confirm Password

Privacy

Protocol

AES

Password

Confirm Password

Cancel

Create

- 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 **authoritative 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 **authoritative 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)

+ Create

Edit

Remove

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
☐	user2		authNoPriv	
☐	user1		authNoPriv	B3A73C2F3D6
☒	user3		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

Cancel

Create

b. Wählen Sie im Feld **Version** die SNMP-Version für diese Benachrichtigung aus.

c. Füllen Sie das Formular aus, basierend auf der ausgewählten Version

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

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

d. Klicken Sie Auf **Erstellen**.

Das Trap-Ziel wird erstellt und der Tabelle hinzugefügt.

Other Configurations

Agent Addresses (1) USM Users (2) Trap Destinations (2)						
+ Create Edit Remove						
Version	Type	Host	Port	Protocol	Community/USM User	
SNMPv3	Trap	local		UDP	User: Read only user	
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)

+ Create **Edit** **Remove**

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
☐	IPv4	UDP	Grid Network	161
☒	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)

+ Create **Edit** **Remove**

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
☐	user2	☒	authNoPriv	
☐	user1		authNoPriv	B3A73C2F3D6
☒	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
☐	SNMPv3	Trap	local		UDP	User: Read only user
☐	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

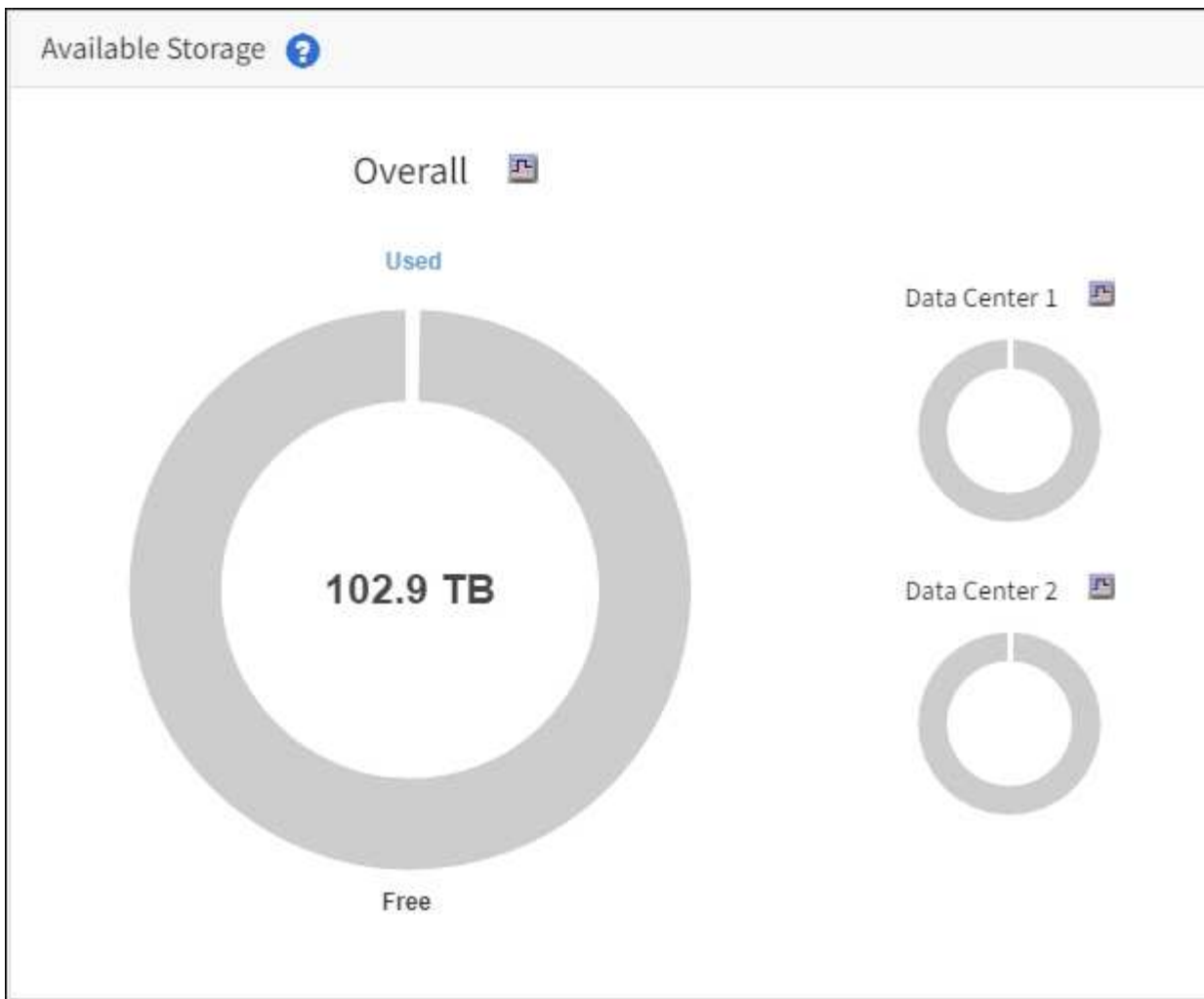
Verwenden Sie Diagramme und Diagramme

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-Topology**.

Es gibt vier Arten von Diagrammen:

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

DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

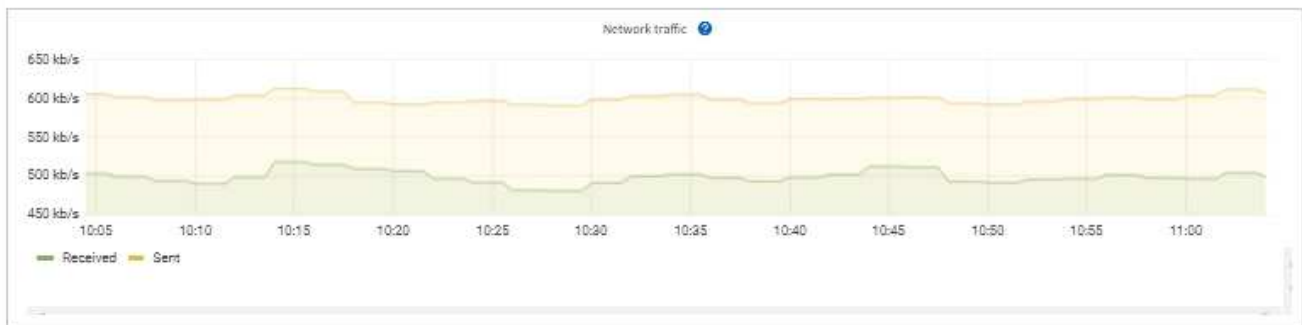
1 hour

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

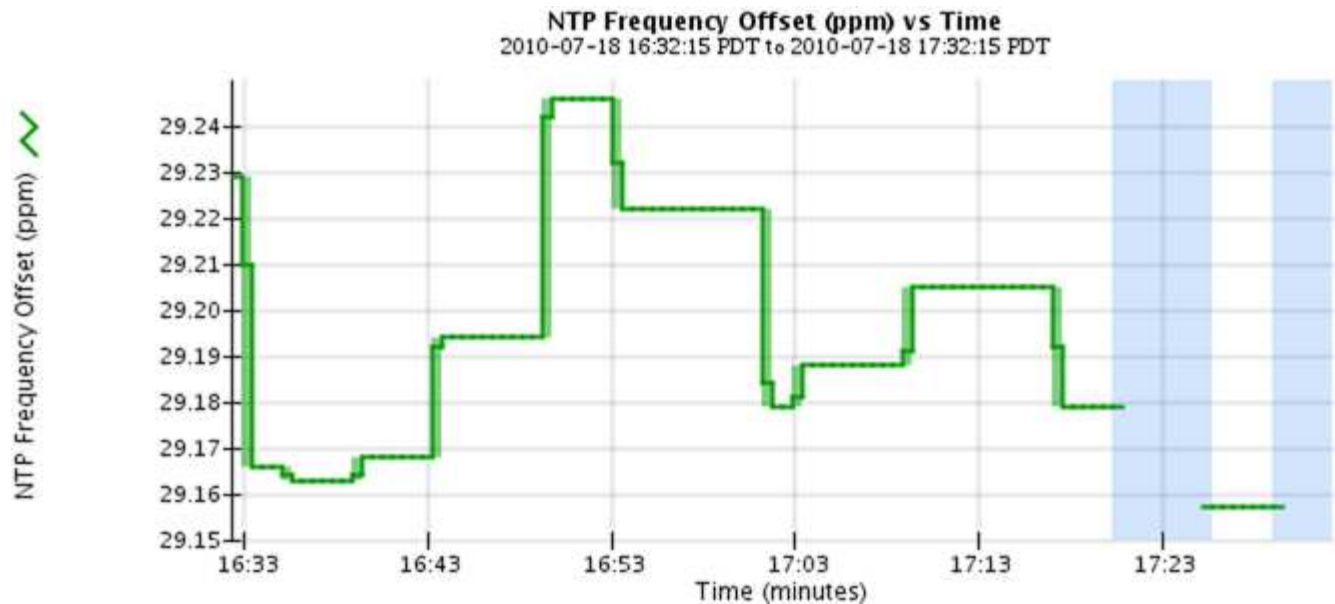
Transmit

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

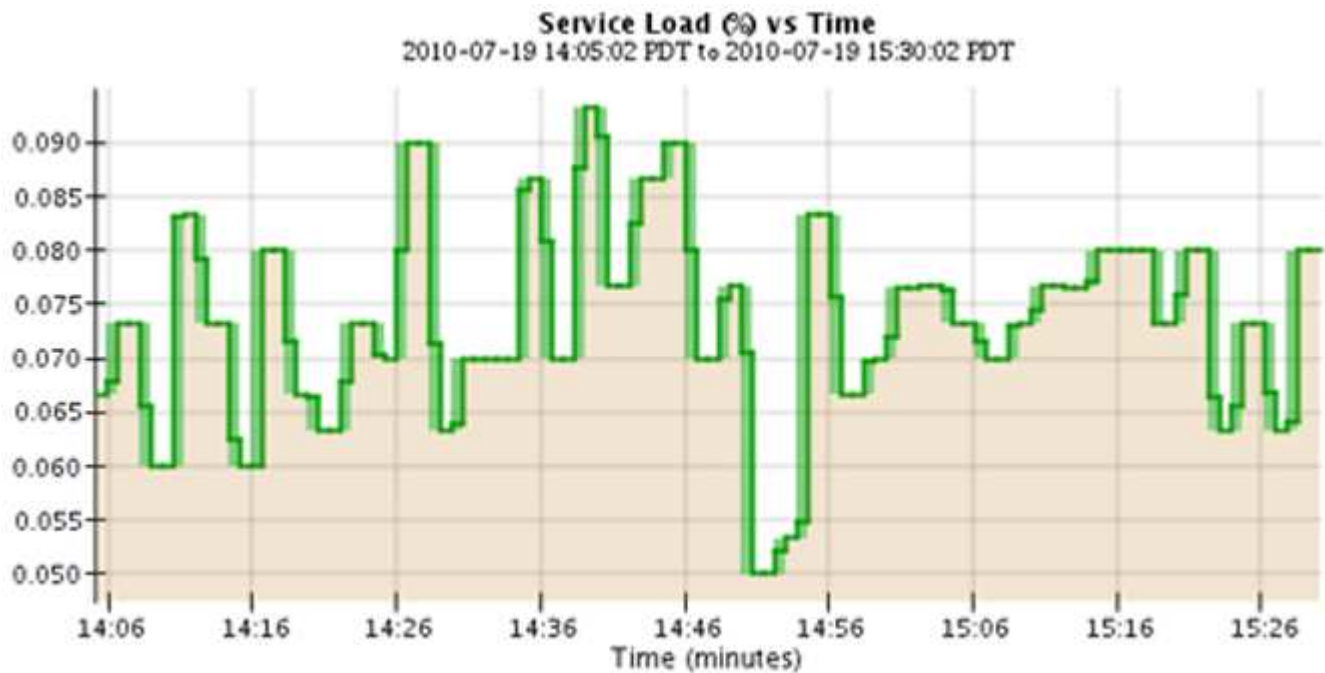


Grafana-Diagramme sind auch auf den vorgebauten Dashboards enthalten, die auf der Seite **SUPPORT Tools Metrics** zur Verfügung stehen.

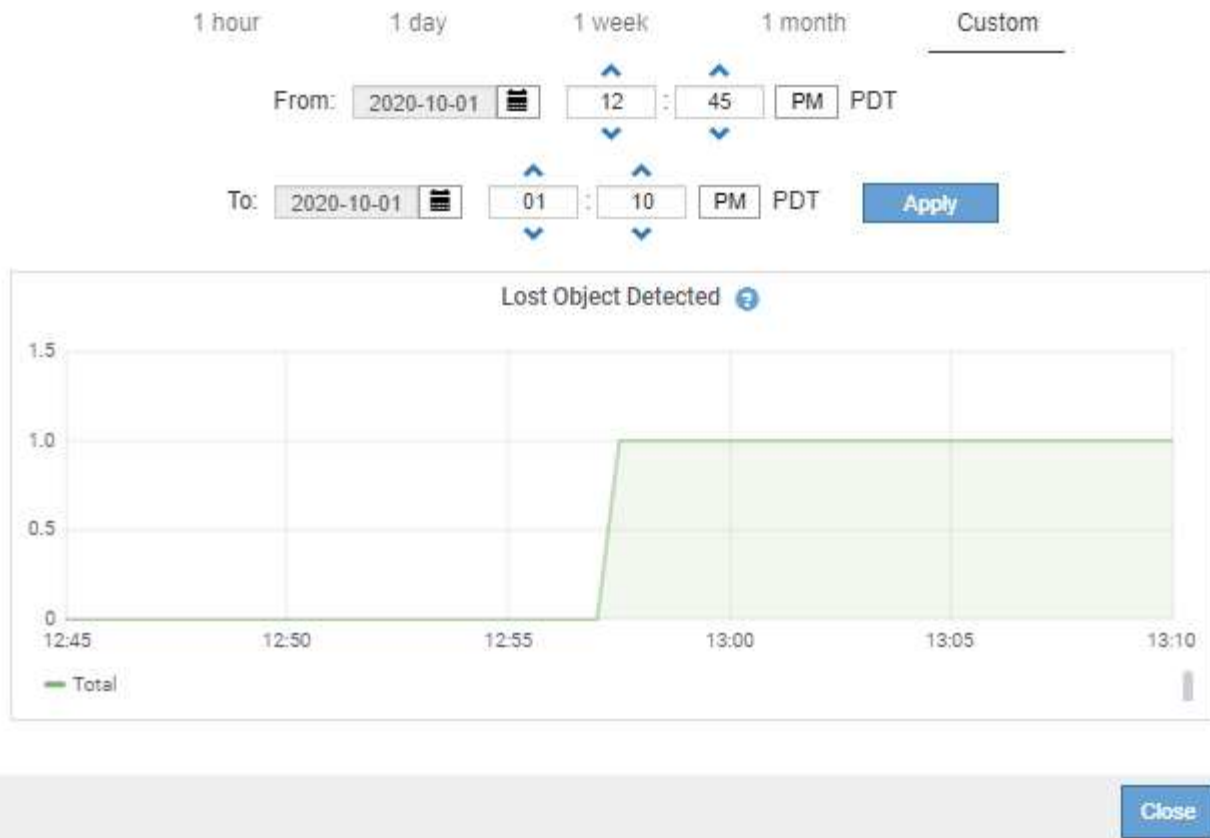
- **Liniendiagramme:** Verfügbar auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG Tools Grid Topologie** (wählen Sie das Diagrammsymbol  Nach einem Datenwert) werden Liniendiagramme verwendet, um die Werte von StorageGRID-Attributen zu zeichnen, die einen Einheitenwert haben (z. B. NTP-Frequenzversatz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



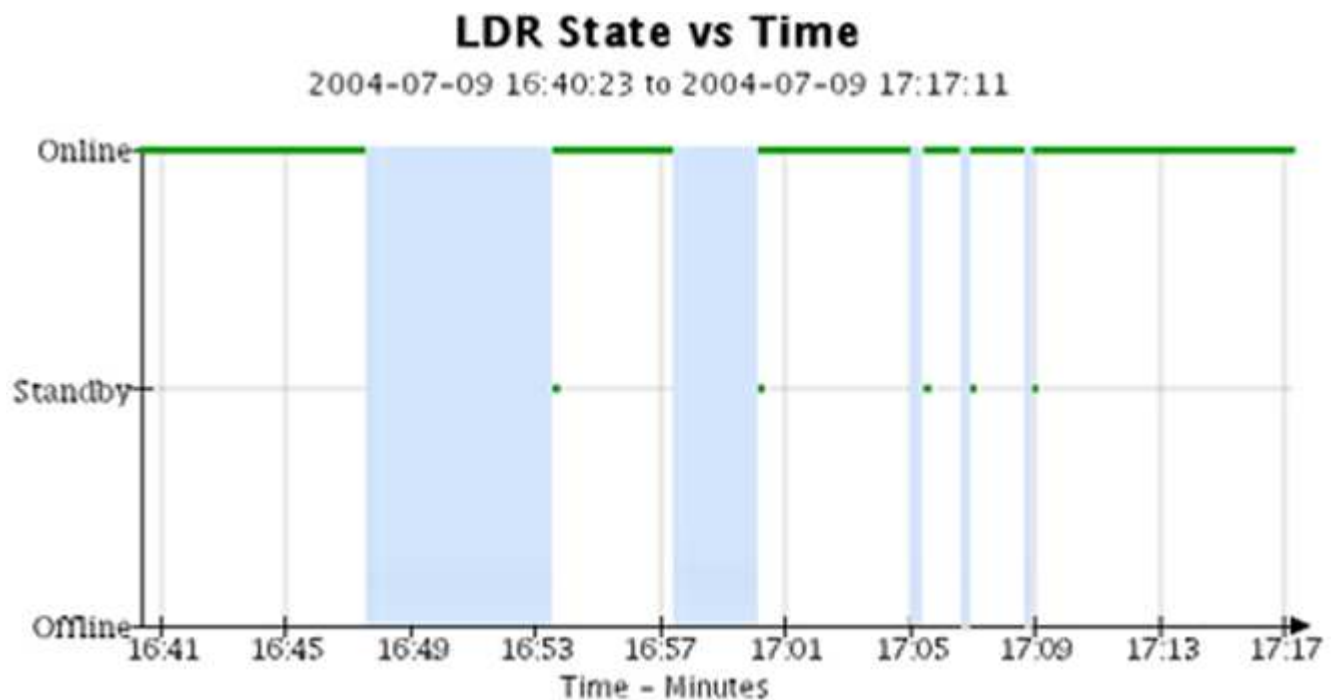
- **Flächendiagramme:** Verfügbar auf der Seite Knoten und auf der Seite **UNTERSTÜTZUNG Tools Grid-Topology** (wählen Sie das Diagrammsymbol  Nach einem Datenwert) werden Flächendiagramme verwendet, um volumetrische Attributmengen zu zeichnen, z. B. Objektanzahl oder Dienstlastwerte. Die Flächendiagramme 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:



- **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 unbekannten Zustand befand.
	Graue Schattierung zeigt an, dass einige oder alle Attributwerte zu diesem Zeitpunkt nicht bekannt waren, da der Dienst, der die Attribute meldet, administrativ herabgesetzt war.
	Eine Mischung aus grauem und blauem Schatten zeigt an, dass einige der Attributwerte zu diesem Zeitpunkt unbestimmt waren (weil der Dienst sich in einem unbekannten Zustand befand), während andere nicht bekannt waren, weil der Dienst, der die Attribute meldet, administrativ nach unten lag.

Zeigen Sie Diagramme und Diagramme an

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

Was Sie benötigen

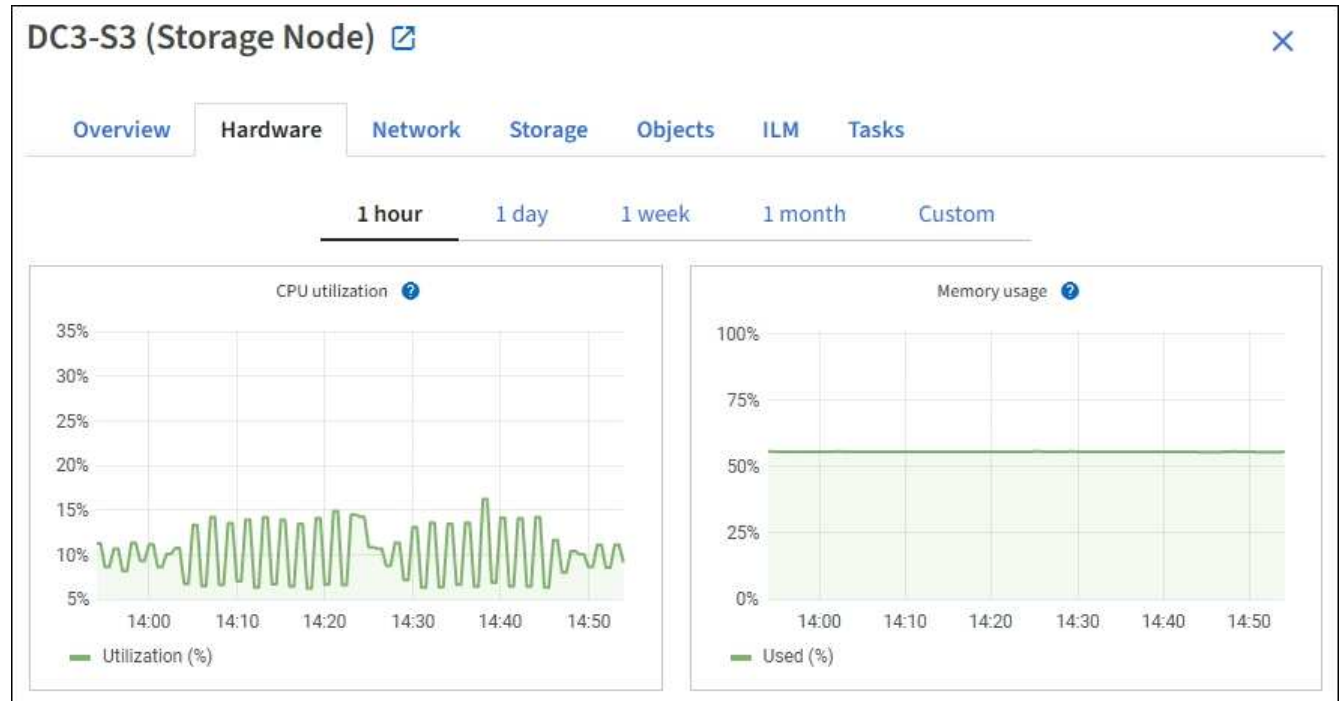
Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).

Schritte

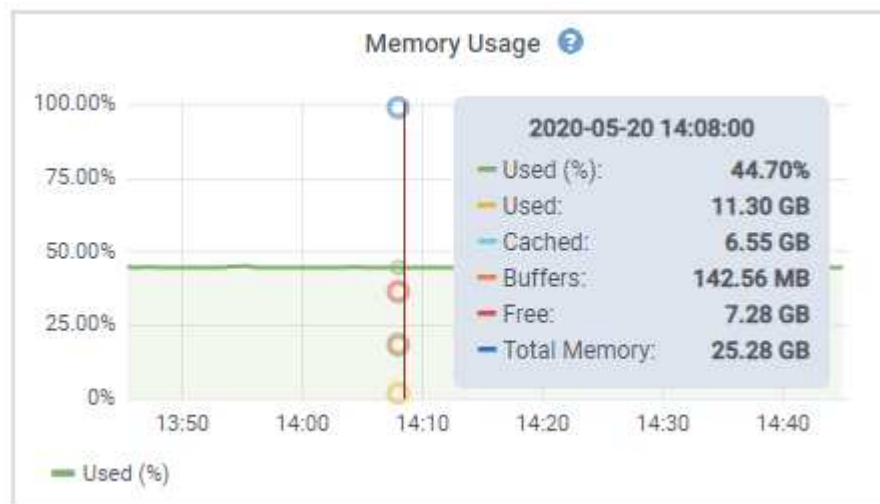
1. Wählen Sie **KNOTEN**. Wählen Sie dann einen Knoten, einen Standort oder das gesamte Raster aus.

- 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.



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



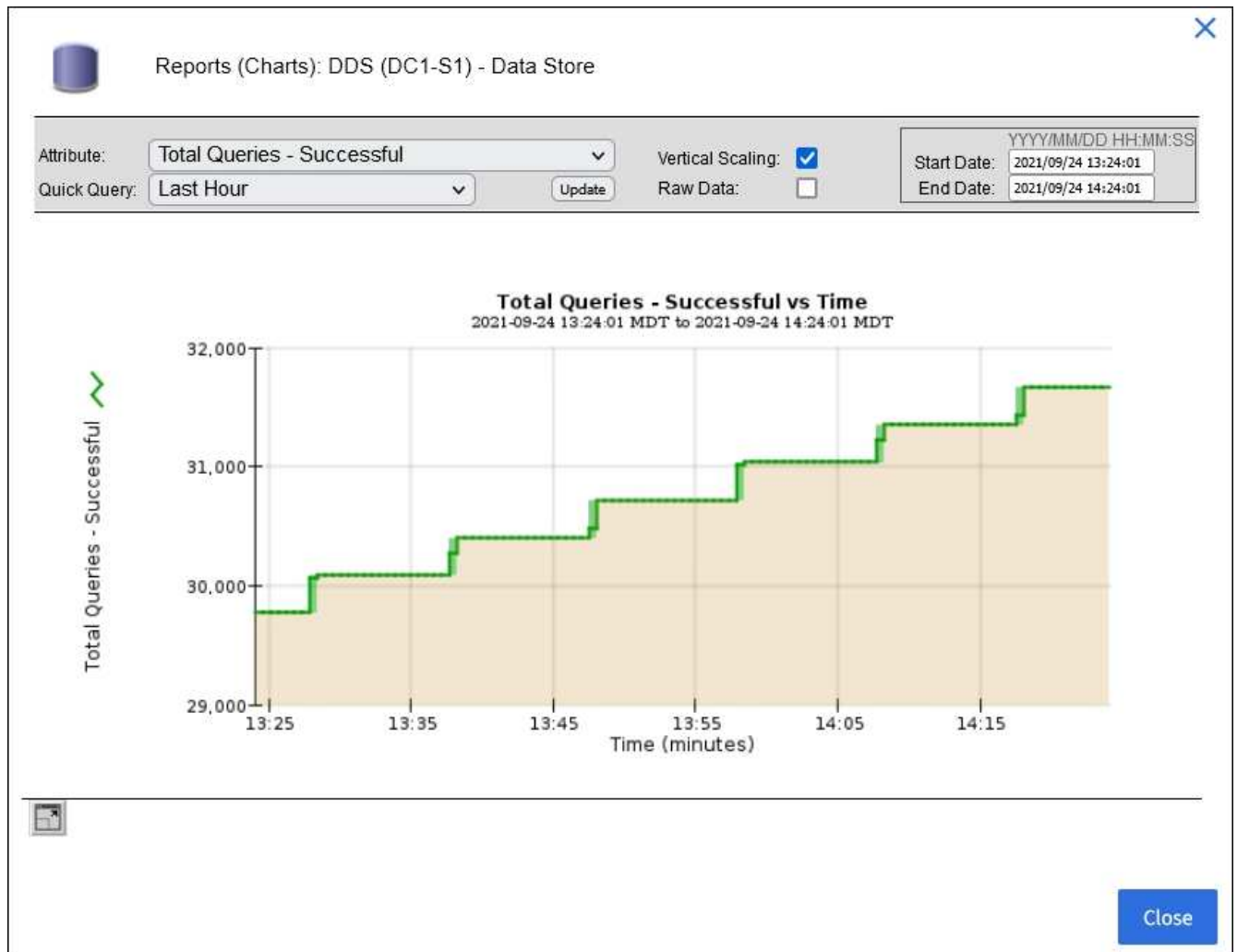
- Bei Bedarf können Sie oft ein Diagramm für ein bestimmtes Attribut oder eine bestimmte Metrik anzeigen. Wählen Sie in der Tabelle auf der Seite Knoten das Diagrammsymbol aus. Rechts neben dem Attributnamen.

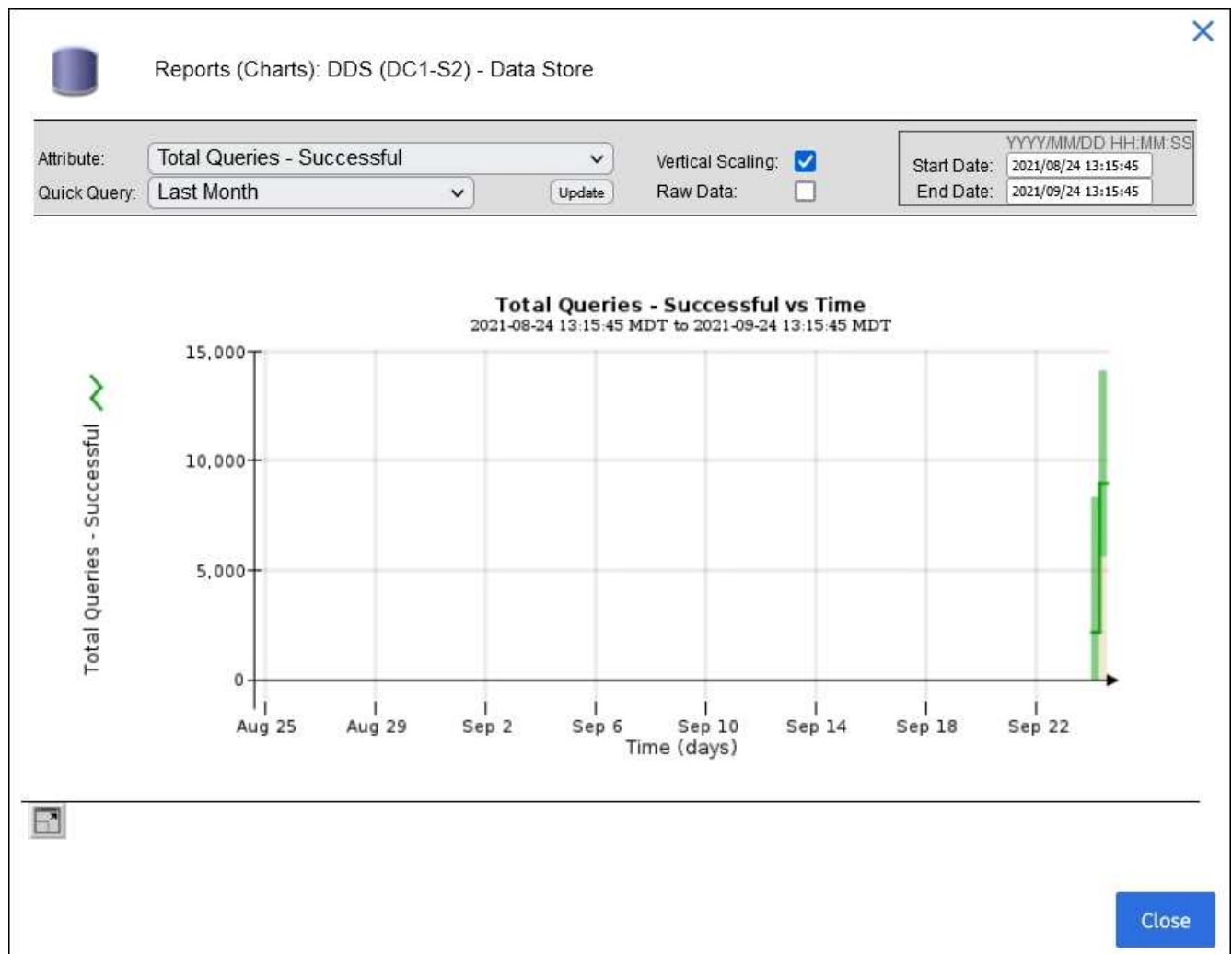


Diagramme sind nicht für alle Metriken und Attribute verfügbar.

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.

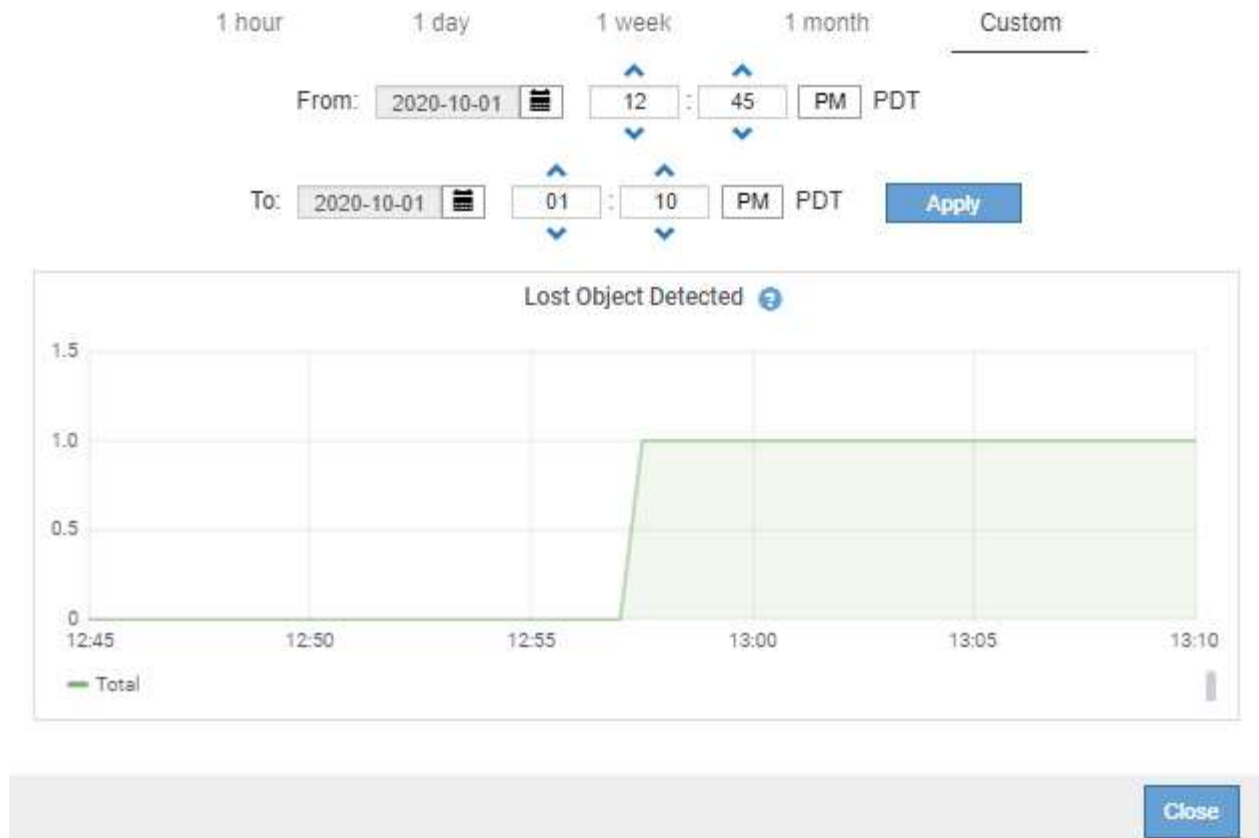




Beispiel 2: Auf der Registerkarte Objekte für einen Speicherknoten können Sie das Diagrammsymbol auswählen Zeigt die Grafana-Grafik der Anzahl der im Laufe der Zeit erkannten verlorenen Objekte an.

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 unbekannten Zustand war.

Schritte

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

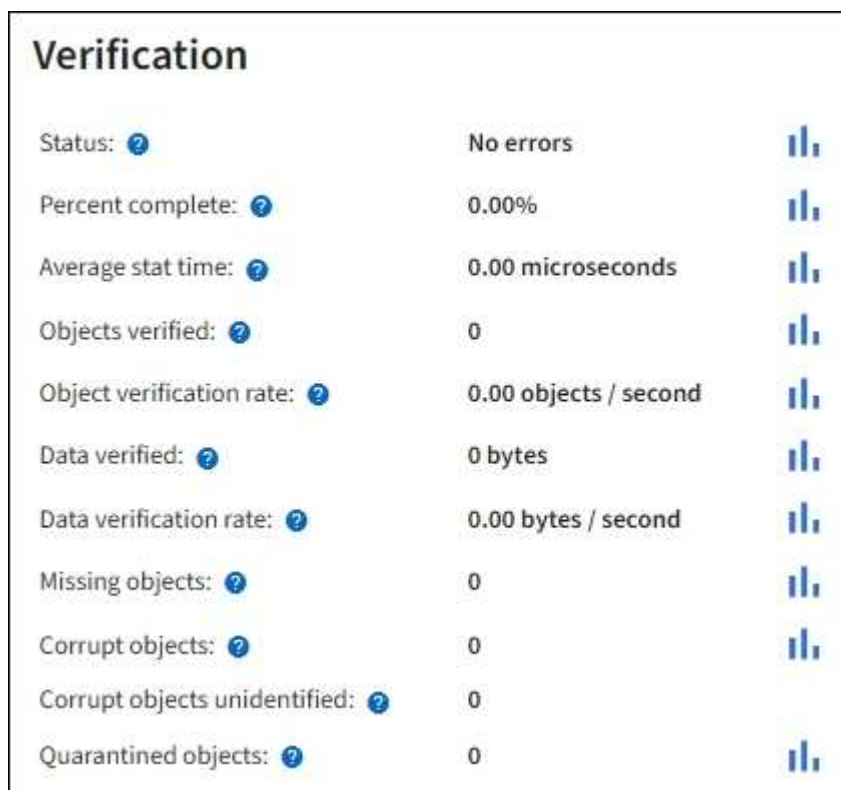
Schritte

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.



- 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...

☐

Job ID ?

Status ⬆

Nodes (volumes) ?

Missing object copies detected ?

☐

15816859223101303015

Completed

DC2-S1 (3 volumes)

0

☐

12538643155010477372

Completed

DC1-S3 (1 volume)

0

☐

5490044849774982476

Completed

DC1-S2 (1 volume)

0

☐

3395284277055907678

Completed

DC1-S1 (3 volumes)
DC1-S2 (3 volumes)
DC1-S3 (3 volumes)
and 7 more

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 `/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**.

Reports (Text): SSM (170-41) - Events

Attribute: Last Event Results Per Page: 20 Start Date: 2009/04/15 15:19:53
 Quick Query: Last 5 Minutes Update Raw Data: ☒ End Date: 2009/04/15 15:24:53

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

1 - 2 of 2

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

- 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 Records Per Page

Previous
« 1 »
Next



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	☐
Account Service Events	0	☐
Cassandra Errors	0	☐
Cassandra Heap Out Of Memory Errors	0	☐
Custom Events	0	☒
File System Errors	0	☐
Forced Termination Events	0	☐

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:** Zeitreihenkennczahlen 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.

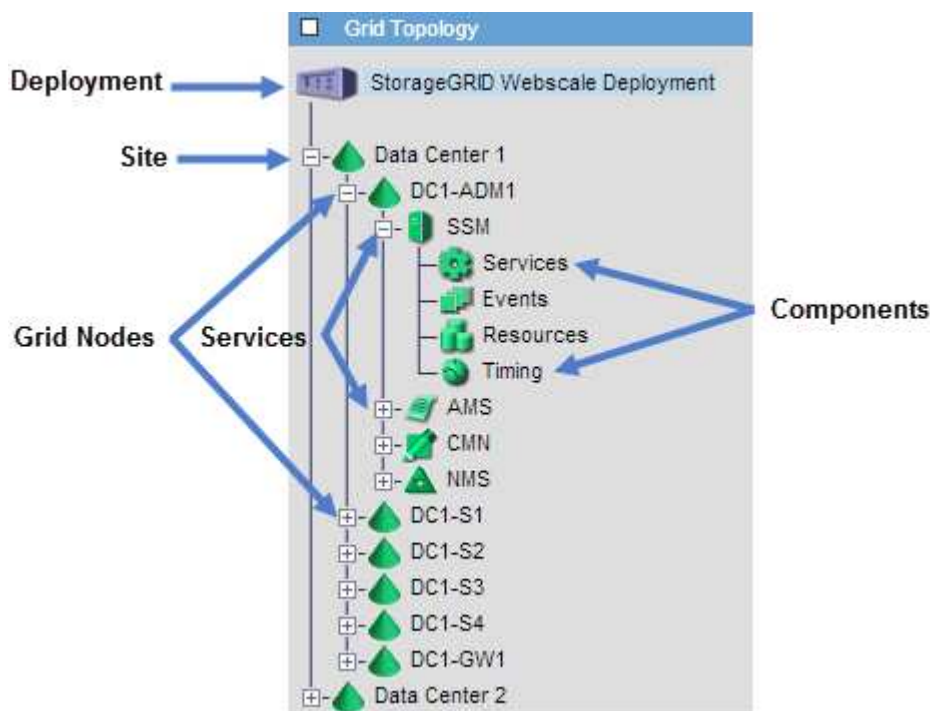
Verwandte Informationen

[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:

Metrics

Access charts and metrics to help troubleshoot issues.

i The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- [https://\[redacted\]/metrics/graph](https://[redacted]/metrics/graph)

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	Grid	S3 - Node
Account Service Overview	ILM	S3 Overview
Alertmanager	Identity Service Overview	S3 Select
Audit Overview	Ingests	Site
Cassandra Cluster Overview	Node	Support
Cassandra Network Overview	Node (Internal Use)	Traces
Cassandra Node Overview	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	
EC Overview	Replicated Read Path Overview	

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.

PrometheusAlertsGraphStatus ▾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 Diagnosetest an. Die Ergebnisse sind nach Schweregrad (Achtung, Achtung und dann normal) sortiert. Innerhalb jedes Schweregrads werden die Ergebnisse alphabetisch sortiert.

In diesem Beispiel haben alle Diagnosen einen normalen Status.

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 $\geq 75\%$
- Caution $\geq 95\%$

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))
```

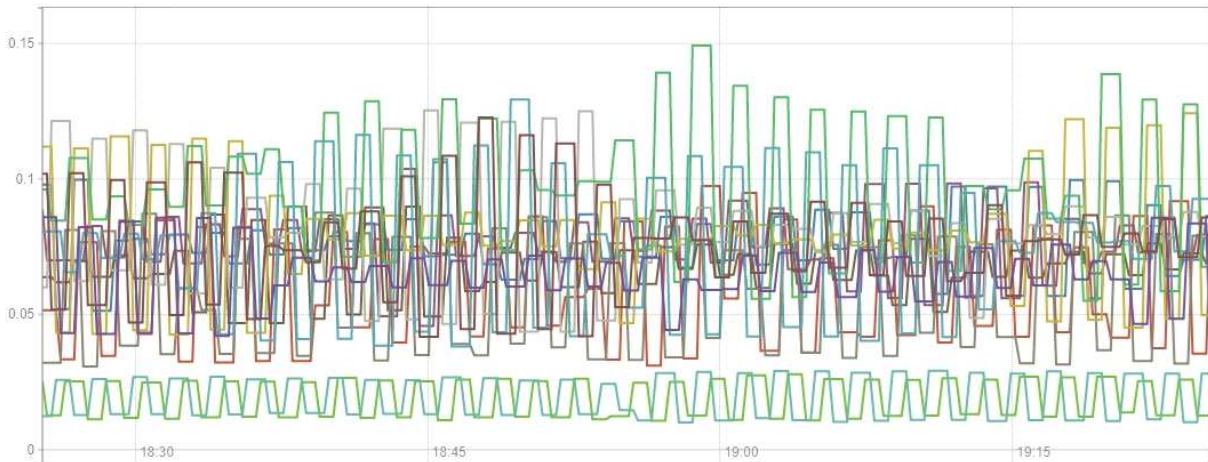
Load time: 547ms
Resolution: 14s
Total time series: 13

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.

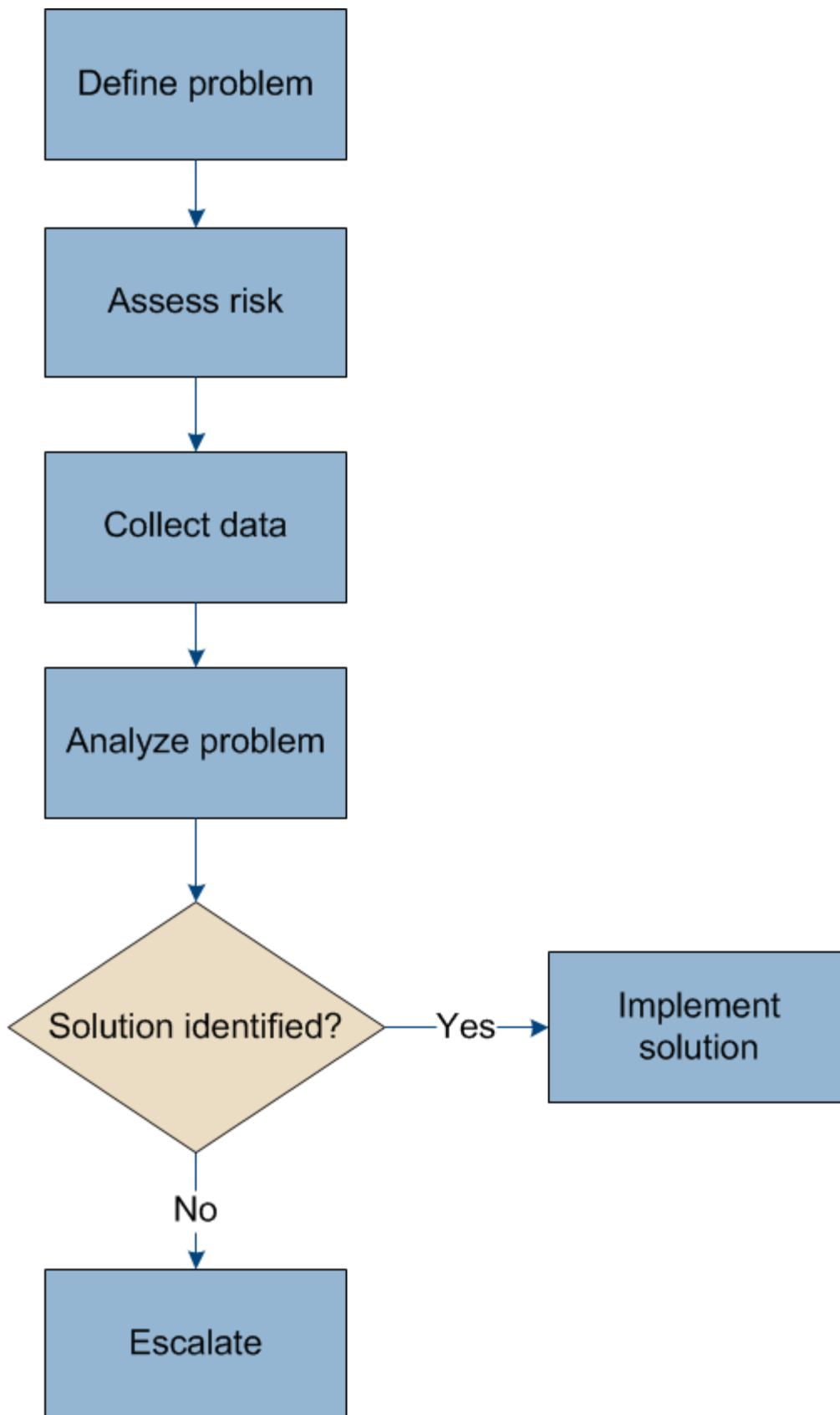
Fehler in einem StorageGRID System beheben

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.	• Erstellen Sie eine Zeitleiste der neuesten Änderungen
Prüfen von Warnungen und Alarmen	Mithilfe von Warnfunktionen und Alarmen können Sie die Ursache eines Problems schnell ermitteln, indem Sie wichtige Hinweise auf die zugrunde liegenden Probleme geben. Überprüfen Sie die Liste der aktuellen Warnungen und Alarme, um festzustellen, ob StorageGRID die Ursache eines Problems für Sie ermittelt hat. Prüfen Sie die in der Vergangenheit ausgelösten Warnmeldungen und Alarme, um zusätzliche Einblicke zu erhalten.	• Anzeigen aktueller 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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
Beispiel: • Wann haben Sie die Node-Wiederherstellung gestartet? • Wann wurde das Software-Upgrade abgeschlossen? • Haben Sie den Prozess unterbrochen?	Was ist los? Was haben Sie gemacht?	Dokumentieren Sie alle relevanten Details zu der Änderung. Beispiel: • Details zu den Netzwerkänderungen. • Welcher Hotfix wurde installiert. • Änderungen bei Client-Workloads Achten Sie darauf, zu beachten, ob mehrere Änderungen gleichzeitig durchgeführt wurden. Wurde diese Änderung beispielsweise vorgenommen, während ein Upgrade durchgeführt wurde?

Beispiele für signifikante aktuelle Änderungen

Hier einige Beispiele für potenziell signifikante Änderungen:

- Wurde das StorageGRID System kürzlich installiert, erweitert oder wiederhergestellt?
- Wurde kürzlich ein Upgrade des Systems durchgeführt? Wurde ein Hotfix angewendet?
- Wurde irgendeine Hardware in letzter Zeit repariert oder geändert?
- Wurde die ILM-Richtlinie aktualisiert?
- Hat sich der Client-Workload geändert?
- Hat sich die Client-Applikation oder deren Verhalten geändert?
- Haben Sie den Lastausgleich geändert oder eine Hochverfügbarkeitsgruppe aus Admin-Nodes oder Gateway-Nodes hinzugefügt oder entfernt?
- Wurden Aufgaben gestartet, die ein sehr langer Zeitaufwand beanspruchen können? Beispiele:
 - Wiederherstellung eines fehlerhaften Speicherknotens
 - Ausmusterung von Storage-Nodes
- Wurden Änderungen an der Benutzerauthentifizierung vorgenommen, beispielsweise beim Hinzufügen eines Mandanten oder bei der Änderung der LDAP-Konfiguration?
- Findet eine Datenmigration statt?
- Wurden Plattform-Services kürzlich aktiviert oder geändert?
- Wurde die Compliance in letzter Zeit aktiviert?
- Wurden Cloud-Storage-Pools hinzugefügt oder entfernt?
- Wurden Änderungen an der Storage-Komprimierung oder -Verschlüsselung vorgenommen?
- Wurden Änderungen an der Netzwerkinfrastruktur vorgenommen? Beispiel: VLANs, Router oder DNS.
- Wurden Änderungen an NTP-Quellen vorgenommen?
- Wurden Änderungen an den Grid-, Admin- oder Client-Netzwerkschnittstellen vorgenommen?
- Wurden Konfigurationsänderungen am Archiv-Node vorgenommen?

- Wurden weitere Änderungen am StorageGRID System bzw. an der zugehörigen Umgebung vorgenommen?

]**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	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm Speicher verwendet - Objektdaten einen Zeitraum, in dem die Linie ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Storage täglich belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.
Durchschnittlicher Metadatenverbrauch	GB verbrauchen/Tag Prozent verbraucht/Tag	Wechseln Sie zum Grid Manager. Wählen Sie auf der Seite Knoten das gesamte Raster oder eine Site aus, und wechseln Sie zur Registerkarte Speicher. Suchen Sie im Diagramm „verwendete Speicher - Objektmetadaten“ einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um zu schätzen, wie viel Metadaten-Storage jeden Tag belegt wird Sie können diese Informationen für das gesamte System oder für ein bestimmtes Rechenzentrum erfassen.

Eigenschaft	Wert	Wie zu erhalten
Geschwindigkeit von S3/Swift Operationen	Vorgänge/Sekunde	Wechseln Sie im Grid Manager zum Fenster Dashboard. Sehen Sie sich im Abschnitt Protokollvorgänge die Werte für die S3-Rate und die Swift-Rate an. 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.
S3/Swift-Vorgänge sind fehlgeschlagen	Betrieb	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.
ILM-Auswertungsrates	Objekte/Sekunde	Wählen Sie auf der Seite Knoten GRID ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Mauszeiger über das Diagramm, um einen Basiswert für Evaluierungsrate für Ihr System zu schätzen.
ILM-Scan-Rate	Objekte/Sekunde	Wählen Sie NODES Grid ILM aus. Suchen Sie im ILM-Queue-Diagramm einen Zeitraum, in dem die Zeile ziemlich stabil ist. Bewegen Sie den Cursor über das Diagramm, um einen Basiswert für Scanrate für Ihr System zu schätzen.

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	Wo liegt der Schweregrad des Problems? Welche Auswirkungen hat dies auf die Client-Applikation? • Ist der Client bereits erfolgreich verbunden? • Kann der Client Daten aufnehmen, abrufen und löschen?
	StorageGRID System-ID	Wählen Sie WARTUNG System Lizenz . Die StorageGRID System-ID wird im Rahmen der aktuellen Lizenz angezeigt.
	Softwareversion	Wählen Sie oben im Grid Manager das Hilfesymbol aus, und wählen Sie über , um die StorageGRID-Version anzuzeigen.
	Anpassbarkeit	Fassen Sie zusammen, wie Ihr StorageGRID System konfiguriert ist. Nehmen Sie z. B. Folgendes auf: • Verwendet das Grid Storage-Komprimierung, Storage-Verschlüsselung oder Compliance? • Erstellt ILM replizierte oder Erasure Coding Objekte? Stellt ILM Standortredundanz sicher? Nutzen ILM-Regeln das strenge, ausgewogene oder duale Ingest-Verhalten?
	Log-Dateien und Systemdaten	Erfassen von Protokolldateien und Systemdaten für Ihr System Wählen Sie SUPPORT Tools Logs. Sie können Protokolle für das gesamte Grid oder für ausgewählte Nodes sammeln. Wenn Sie Protokolle nur für ausgewählte Knoten erfassen, müssen Sie mindestens einen Speicherknoten mit dem ADC-Service einschließen. (Die ersten drei Storage-Nodes an einem Standort enthalten den ADC-Service.) Erfassen von Protokolldateien und Systemdaten
	Basisinformationen	Sammeln von Basisinformationen über Erfassungs-, Abrufvorgänge und Storage-Verbrauch Basispläne erstellen

	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)

Look Up

4. Wählen Sie **Look Up**.

Die Ergebnisse der Objektmeldaten 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 Objektmeldaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAHS": "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

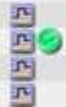
Total Space: 322 GB

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 Speicherknoten so bald wie möglich wieder voll zu machen. Wenn nötig, können Sie auf die Registerkarte **Konfiguration** gehen und den Speicherknoten in einen Read-only Zustand setzen, so dass das StorageGRID System ihn für den Datenabruf verwenden kann, während Sie sich auf eine vollständige Wiederherstellung des Servers vorbereiten.

Verwandte Informationen

[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.

Overview Alarms Reports **Configuration**

Main

Configuration: LDR (Storage-Node-1) - Verification
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count ☐

Background Verification

Verification Rate Adaptive ▼

Reset Corrupt Objects Count ☐

Quarantined Objects

Delete Quarantined Objects ☐

Apply Changes



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 Lösungscode, 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 Lösungscode 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 Speicherknotens 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**.

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

Delete

Rerun

Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

☐	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
☒	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)
☐	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

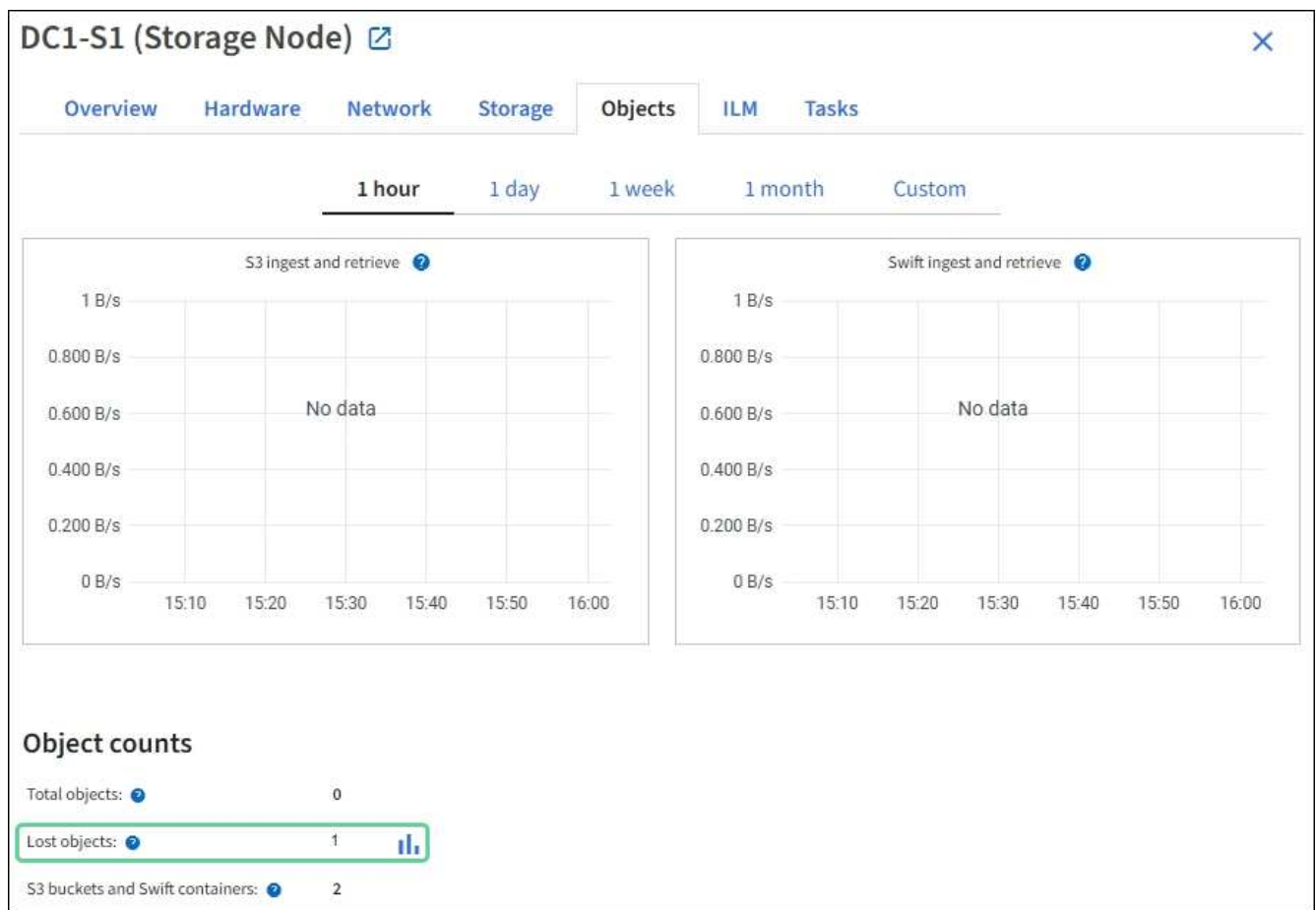
Die Warnung **Objects lost** zeigt an, dass StorageGRID glaubt, dass es keine Kopien eines Objekts im Raster gibt. Möglicherweise sind Daten dauerhaft verloren gegangen.

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“:“)	Wenn das Objekt nicht gefunden wird, wird die Meldung „FEHLER“:“ zurückgegeben. 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.
Standorte 0	Wenn in der Ausgabe Standorte aufgeführt sind, kann die Warnung Objects Lost falsch positiv sein. Vergewissern Sie sich, dass die Objekte vorhanden sind. Verwenden Sie die Knoten-ID und den Dateipfad, der in der Ausgabe aufgeführt ist, um zu bestätigen, dass sich die Objektdatei am aufgelisteten Speicherort befindet. (Verfahren für Suche nach möglicherweise verlorenen Objekten Erläutert, wie Sie die Knoten-ID verwenden, um den richtigen Speicherknoten zu finden.) Wenn die Objekte vorhanden sind, können Sie die Anzahl der verlorenen Objekte zurücksetzen, um die Warnung zu löschen.
Standorte = 0	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. 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 Objektdaten auf einem Storage-Volume.

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 „potentiell verloren“ identifiziert haben.

Was Sie benötigen

- Sie müssen über die UUID eines verlorenen Objekts verfügen, wie in „Untersuchung verlorener Objekte“ angegeben.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Im Anschluss an dieses Verfahren können Sie sich nach replizierten Kopien des verlorenen Objekts an einer anderen Stelle im Grid suchen. In den meisten Fällen wird das verlorene Objekt nicht gefunden. In einigen Fällen können Sie jedoch ein verlorenes repliziertes Objekt finden und wiederherstellen, wenn Sie umgehend Maßnahmen ergreifen.



Wenden Sie sich an den technischen Support, wenn Sie Hilfe bei diesem Verfahren benötigen.

Schritte

1. Suchen Sie in einem Admin-Knoten die Prüfprotokolle nach möglichen Objektspeichern:
 - a. Melden Sie sich beim Grid-Node an:
 - i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei: Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.
 - b. Wechseln Sie in das Verzeichnis, in dem sich die Audit-Protokolle befinden: `cd /var/local/audit/export/`
 - c. Verwenden Sie `grep`, um die mit dem potenziell verlorenen Objekt verknüpften Audit-Nachrichten zu extrahieren und sie an eine Ausgabedatei zu senden. Geben Sie Ein: `grep uuid-valueaudit_file_name > output_file_name`

Beispiel:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_lost_object.txt
```

- d. Verwenden Sie `grep`, um die Meldungen zum Lost Location (LLST) aus dieser Ausgabedatei zu extrahieren. Geben Sie Ein: `grep LLST output_file_name`

Beispiel:

```
Admin: # grep LLST messages_about_lost_objects.txt
```

Eine LLST-Überwachungsmeldung sieht wie diese Beispielmeldung aus.

```
[AUDT:\[NOID\ (UI32\):12448208\] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) : "926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTP (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 `ldocs`. 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 Objektpfad immer in einzelne Anführungszeichen, um Sonderzeichen zu entkommen.

- Wenn der Objektpfad nicht gefunden wurde, geht das Objekt verloren und kann mit diesem Verfahren nicht wiederhergestellt werden. Wenden Sie sich an den technischen Support.
- Wenn der Objektpfad gefunden wurde, fahren Sie mit Schritt fort [Stellen Sie das Objekt in StorageGRID wieder her](#). Sie können versuchen, das gefundene Objekt wieder in StorageGRID wiederherzustellen.
 - a. Wenn der Objektpfad 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

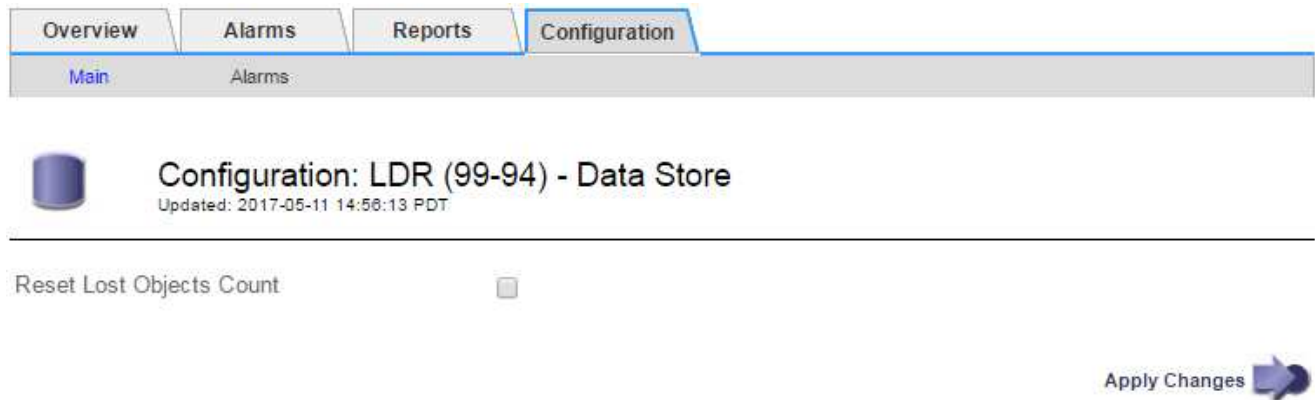
Sie können den Zähler „Lost Objects“ von einer der folgenden Seiten zurücksetzen:

- **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**.



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

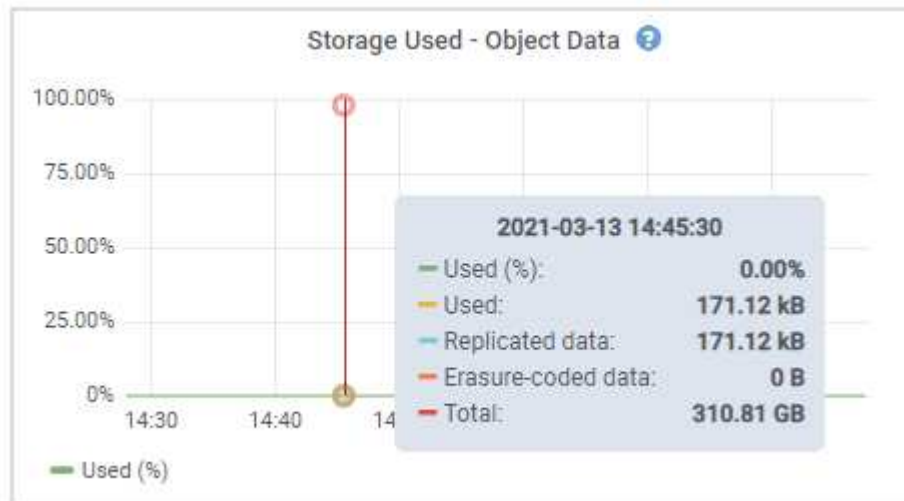
4. Wählen Sie **NODES Storage Node oder Standort Storage** aus.

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.



- 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.

- 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-Volume im Storage-Node weniger als 10 GB nutzbarer Speicherplatz verbleibt. Wenn eines der Volumes über 10 GB oder mehr verfügbaren Speicherplatz verfügt, wird der Alarm nicht ausgelöst.

Wenn ein SSTS-Alarm ausgelöst wurde, können Sie diese Schritte ausführen, um das Problem besser zu verstehen.

Schritte

1. Wählen Sie **SUPPORT Alarme (alt) Aktuelle Alarme**.
2. Wählen Sie in der Spalte Service das Rechenzentrum, den Node und den Service aus, die dem SSTS-Alarm zugeordnet sind.

Die Seite Grid Topology wird angezeigt. Auf der Registerkarte „Alarme“ werden die aktiven Alarme für den ausgewählten Knoten und Dienst angezeigt.

OverviewAlarmsReportsConfiguration

MainHistory

**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		☐
 Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		☐
 Normal	SHLH (Health)						☐

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).

Overview

Alarms

Reports

Configuration

Main

Overview: LDR (.DC1-S1-101-193) - Storage

Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:

Online

Storage State - Current:

Read-only

Storage Status:

Insufficient Free Space

Utilization

Total Space:

164 GB

Total Usable Space:

19.6 GB

Total Usable Space (Percent):

11.937 %

Total Data:

139 GB

Total Data (Percent):

84.567 %

Replication

Block Reads:

0

Block Writes:

2,279,881

Objects Retrieved:

0

Objects Committed:

88,882

Objects Deleted:

16

Delete Service State:

Enabled

Object Store Volumes

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.

Overview

Alarms

Reports

Configuration

Charts

Text



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:

Total Usable Space

Quick Query:

Custom Query

Update

Vertical Scaling:
☒

Raw Data:
☐

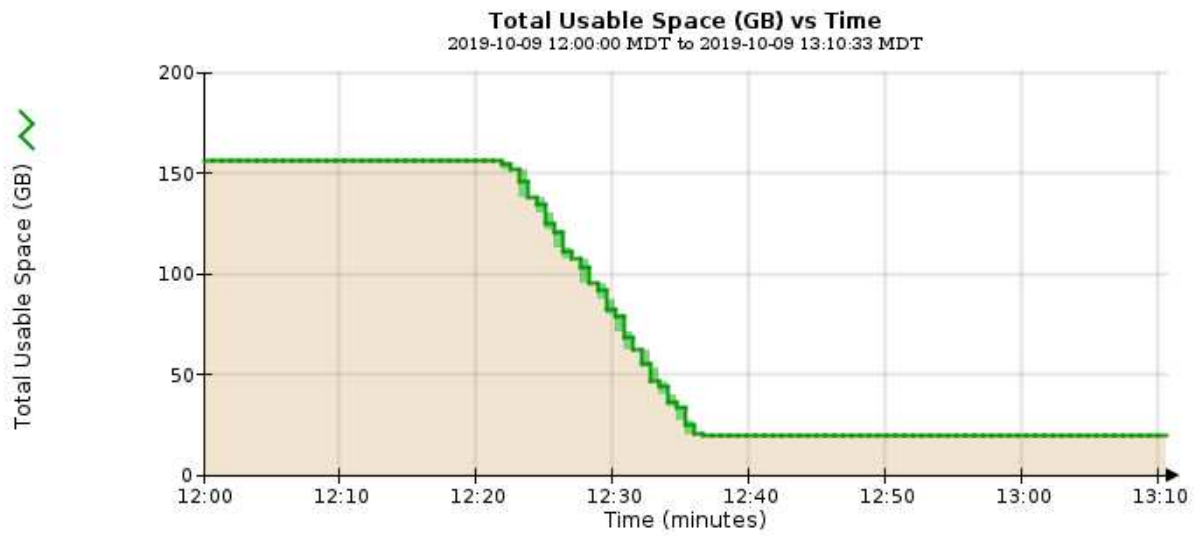
YYYY/MM/DD HH:MM:SS

Start Date:

2019/10/09 12:00:00

End Date:

2019/10/09 13:10:33



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)

Quick Query:

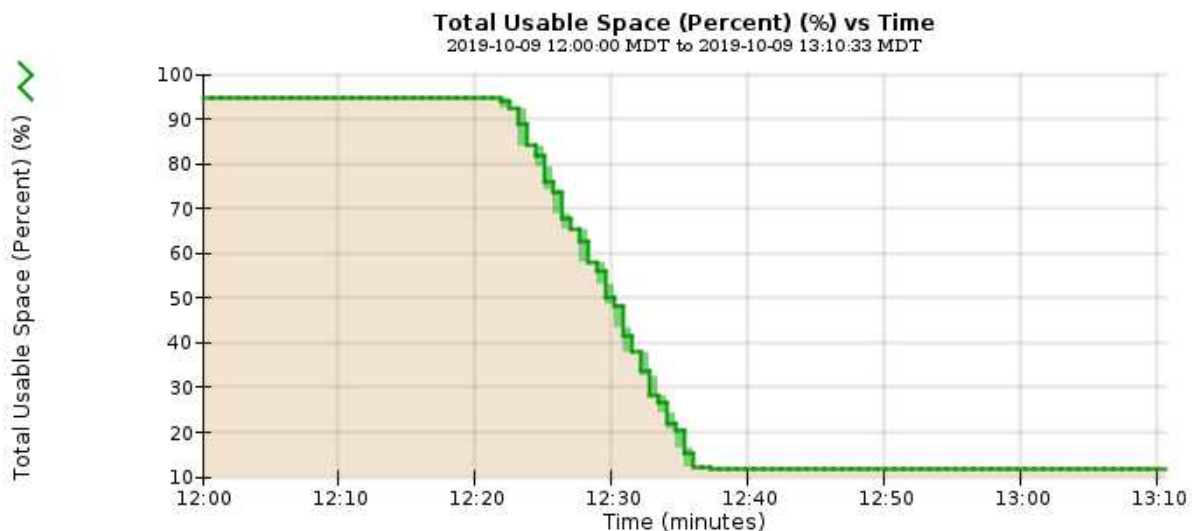
Custom Query

Update

Vertical Scaling: ☒
Raw Data: ☐

YYYY/MM/DD HH:MM:SS

Start Date: 2019/10/09 12:00:00
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

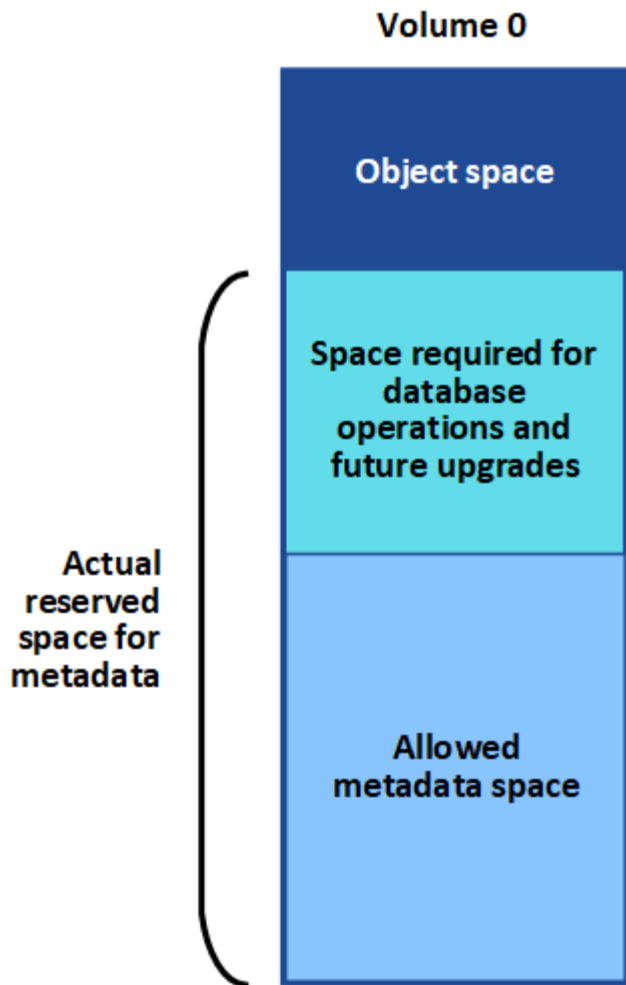
Wenn die Warnung * Storage* mit niedrigen Metadaten ausgelöst wird, müssen Sie neue Storage-Nodes hinzufügen.

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:** Objektmeteradaten verwenden 70% oder mehr des zulässigen Metadaten-Speicherplatzes. Sie sollten so bald wie möglich neue Storage-Nodes hinzufügen.
- **Major:** Objektmeteradaten 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 Metadatenpeicher 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.

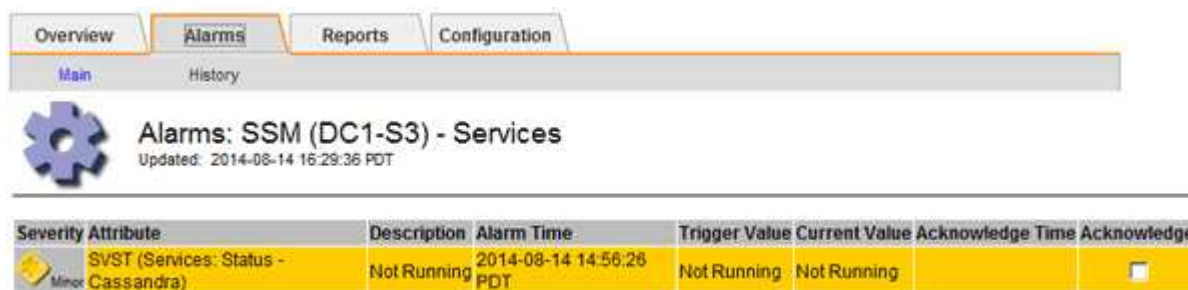


Wenn mindestens zwei der Cassandra-Datenbankdienste länger als 15 Tage ausgefallen sind, wenden Sie sich an den technischen Support, und fahren Sie nicht mit den folgenden Schritten fort.

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		☐

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.

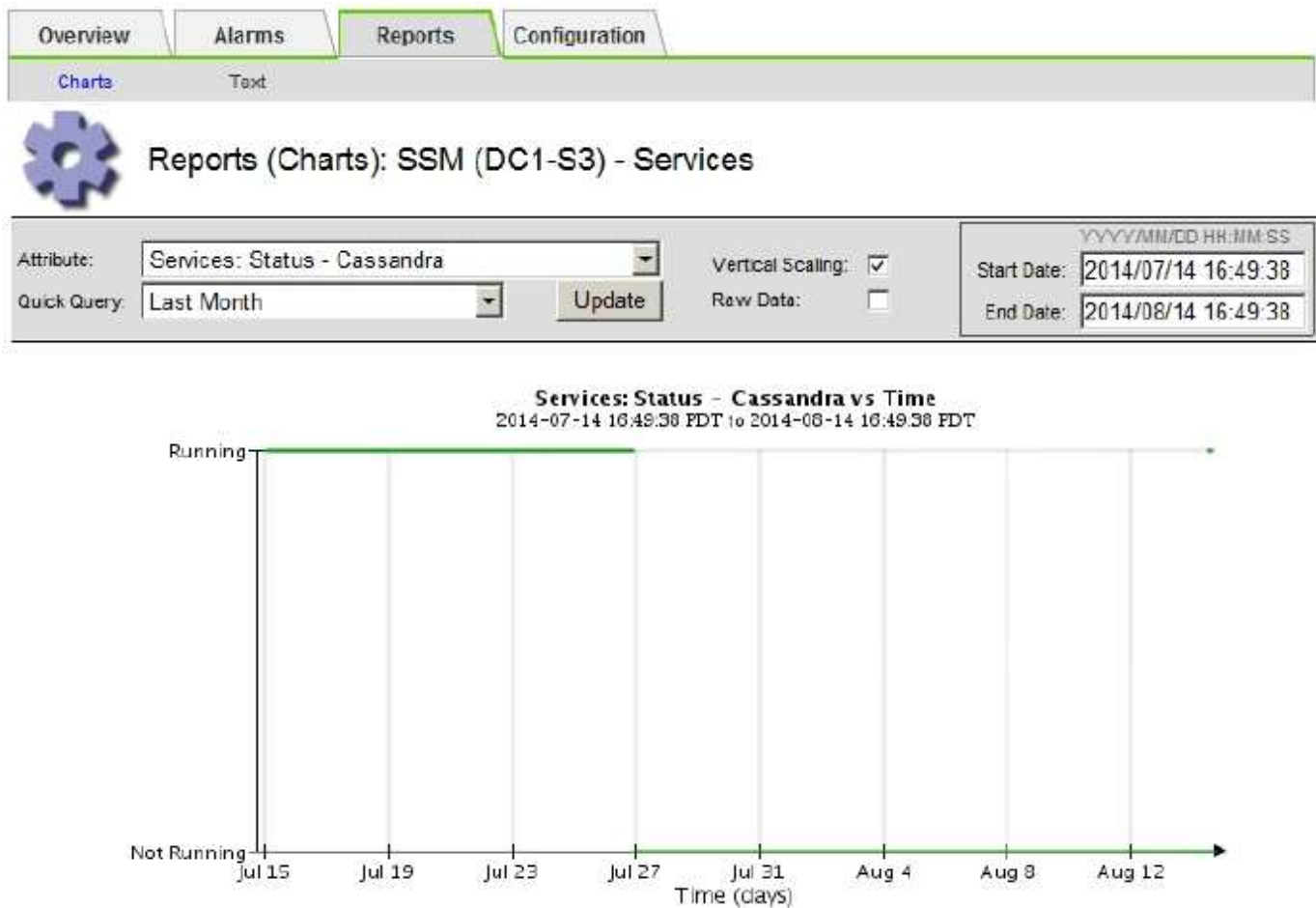
Sie können feststellen, wie lange Cassandra ausgefallen ist, indem Sie sie aufschreiben oder die Datei `servermanager.log` lesen.

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:

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

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.

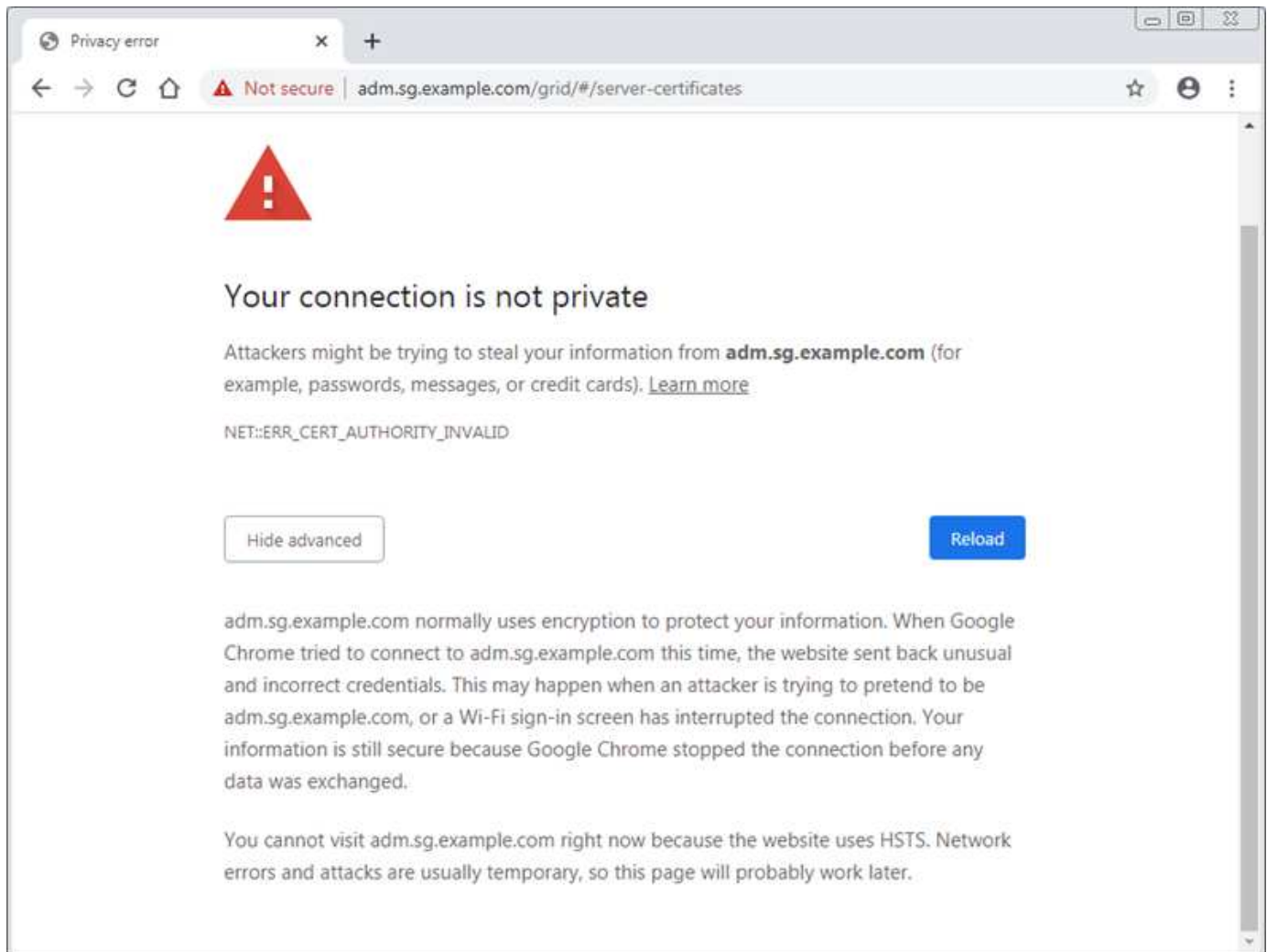
Über diese Aufgabe

Zertifikatsfehler 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. Zertifikatsfehler 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 Zertifikatsfehler 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 Zertifikatsfehler 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 Zertifikatsfehler 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 Serverzertifikatsfehlern 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 Speicher-knoten.

Was Sie benötigen

- Sie müssen die `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:

- Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
- Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- 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
422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839	Diese Meldung kann auftreten, wenn Sie bei der Konfiguration der Identitätsföderation mit Windows Active Directory (AD) die Option TLS nicht verwenden für Transport Layer Security (TLS) auswählen. Die Verwendung der Option keine Verwendung von TLS wird nicht für die Verwendung mit AD-Servern unterstützt, die LDAP-Signatur erzwingen. Sie müssen entweder die Option STARTTLS verwenden oder die Option LDAPS verwenden für TLS auswählen.
422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)	Diese Meldung wird angezeigt, wenn Sie versuchen, eine nicht unterstützte Chiffre zu verwenden, um eine TLS-Verbindung (Transport Layer Security) von StorageGRID zu einem externen System herzustellen, das für Identify Federation oder Cloud Storage Pools verwendet wird. Überprüfen Sie die vom externen System angebotenen Chiffren. Das System muss eine der von StorageGRID unterstützten Chiffren für ausgehende TLS-Verbindungen verwenden, wie in den Anleitungen zur StorageGRID-Verwaltung dargestellt.

Verwandte Informationen

[StorageGRID verwalten](#)

Fehlerbehebung bei der 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
mtu	Die MTU, die eingestellt werden soll. Muss zwischen 1280 und 9216 liegen.
network	Die Netzwerke, auf die die MTU angewendet werden soll. Geben Sie einen oder mehrere der folgenden Netzwerktypen an: • Raster • Admin • Client

+

Optionale Argumente	Beschreibung
-h, - help	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-Alarme (Network Receive Error) können durch Verbindungsprobleme zwischen StorageGRID und Ihrer Netzwerk-Hardware verursacht werden. In einigen Fällen können NRER-Fehler ohne manuelles Eingreifen gelöscht werden. Wenn die Fehler nicht behoben werden, führen Sie die empfohlenen Maßnahmen durch.

Über diese Aufgabe

NRER-Alarme können durch die folgenden Probleme mit Netzwerk-Hardware verursacht werden, die eine Verbindung mit StorageGRID herstellt:

- Eine Vorwärtsfehlerkorrektur (FEC) ist erforderlich und wird nicht verwendet
- Switch-Port und MTU-NIC stimmen nicht überein
- Hohe Link-Fehlerraten
- NIC-Klingelpuffer überlaufen

Schritte

1. Befolgen Sie die Schritte zur Fehlerbehebung für alle möglichen Ursachen des NRER-Alarms bei der Netzwerkkonfiguration.
 - Wenn der Fehler durch eine nicht übereinstimmende FEC verursacht wird, führen Sie die folgenden Schritte aus:

Hinweis: Diese Schritte gelten nur für NRER-Fehler, die durch FEC-Diskrepanz auf StorageGRID-Geräten verursacht werden.

- i. Überprüfen Sie den FEC-Status des Ports im Switch, der an Ihr StorageGRID-Gerät angeschlossen ist.
- ii. Überprüfen Sie die physikalische Integrität der Kabel vom Gerät zum Switch.
- iii. Wenn Sie die FEC-Einstellungen ändern möchten, um den NRER-Alarm zu beheben, stellen Sie zunächst sicher, dass das Gerät auf der Seite „Konfiguration verknüpfen“ des Installationsprogramms von StorageGRID-Geräten für den **Auto**-Modus konfiguriert ist (siehe Installations- und Wartungsanweisungen für Ihr Gerät). Ändern Sie dann die FEC-Einstellungen an den Switch-Ports. Die StorageGRID-Appliance-Ports passen ihre FEC-Einstellungen nach Möglichkeit an.

(Sie können FEC-Einstellungen auf StorageGRID-Geräten nicht konfigurieren. Stattdessen versuchen die Geräte, die FEC-Einstellungen an den Switch-Ports zu erkennen und zu spiegeln, an denen sie angeschlossen sind. Wenn die Verbindungen zu 25-GbE- oder 100-GbE-Netzwerkgeschwindigkeiten gezwungen sind, können Switch und NIC eine gemeinsame FEC-Einstellung nicht aushandeln. Ohne eine gemeinsame FEC-Einstellung kehrt das Netzwerk in den Modus „no-FEC“ zurück. Wenn FEC nicht aktiviert ist, sind die Anschlüsse anfälliger für Fehler, die durch elektrische Geräusche verursacht werden.)

Hinweis: StorageGRID-Geräte unterstützen Firecode (FC) und Reed Solomon (RS) FEC sowie kein FEC.

- Wenn der Fehler durch einen Switch Port und eine nicht übereinstimmende NIC MTU verursacht wird, überprüfen Sie, ob die auf dem Node konfigurierte MTU-Größe mit der MTU-Einstellung für den Switch-Port identisch ist.

Die auf dem Node konfigurierte MTU-Größe ist möglicherweise kleiner als die Einstellung am Switch-Port, mit dem der Node verbunden ist. Wenn ein StorageGRID-Knoten einen Ethernet-Frame empfängt, der größer ist als seine MTU, was mit dieser Konfiguration möglich ist, wird möglicherweise der NRR-Alarm gemeldet. Wenn Sie der Ansicht sind, dass dies geschieht, ändern Sie entweder die MTU des Switch Ports entsprechend der StorageGRID Netzwerkschnittstelle MTU oder ändern Sie die MTU der StorageGRID-Netzwerkschnittstelle je nach Ihren End-to-End-Zielen oder Anforderungen an den Switch-Port.



Für die beste Netzwerkleistung sollten alle Knoten auf ihren Grid Network Interfaces mit ähnlichen MTU-Werten konfiguriert werden. Die Warnung **Grid Network MTU mismatch** wird ausgelöst, wenn sich die MTU-Einstellungen für das Grid Network auf einzelnen Knoten erheblich unterscheiden. Die MTU-Werte müssen nicht für alle Netzwerktypen identisch sein.



Informationen zum Ändern der MTU-Einstellung finden Sie im Installations- und Wartungshandbuch für Ihre Appliance.

- Wenn der Fehler durch hohe Verbindungsfehlerraten verursacht wird, führen Sie die folgenden Schritte aus:
 - i. Aktivieren Sie FEC, falls nicht bereits aktiviert.
 - ii. Stellen Sie sicher, dass Ihre 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.

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

DC1-S2 (Storage Node)

Overview Hardware Network Storage Objects ILM Tasks

Node information

Name: DC1-S2

Type: Storage Node

ID: 352bd978-ff3e-45c5-aac1-24c7278206fa

Connection state: ✓ Connected

Storage used:

Object data	0%
Object metadata	0%

Software version: 11.6.0 (build 20210924.1557.00aSeb9)

IP addresses:

172.16.1.227 - eth0 (Grid Network)

10.224.1.227 - eth1 (Admin Network)

[Hide additional IP addresses](#)

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	Der für den Syslog-Server eingegebene FQDN konnte nicht in eine IP-Adresse aufgelöst werden. 1. 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. 2. Überprüfen Sie, ob die DNS-Server richtig konfiguriert sind. 3. Vergewissern Sie sich, dass jeder Knoten auf die IP-Adressen des DNS-Servers zugreifen kann.
Verbindung abgelehnt	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. 1. 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. 2. Vergewissern Sie sich, dass der Host für den syslog-Service einen Syslog-Daemon ausführt, der auf dem angegebenen Port abhört. 3. 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	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. 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-Netzwerksnetz, 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	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. 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	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). 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-Netzwerksnetz, 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	Eine TCP-Verbindung zum Syslog-Server wurde erfolgreich hergestellt, wurde aber später geschlossen. Gründe hierfür sind u. a.: • 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. 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	Das vom Syslog-Server empfangene Serverzertifikat war nicht mit dem von Ihnen angegebenen CA-Zertifikatspaket und dem von Ihnen angegebenen Clientzertifikat kompatibel. 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	Syslog-Datensätze werden nicht mehr an den Syslog-Server weitergeleitet, und StorageGRID kann den Grund nicht erkennen. Überprüfen Sie die mit diesem Fehler bereitgestellten Debugging-Protokolle, um zu versuchen, die Grundursache zu ermitteln.

Fehlermeldung	Beschreibung und empfohlene Aktionen
TLS-Sitzung beendet	Der Syslog-Server hat die TLS-Sitzung beendet und StorageGRID kann den Grund nicht erkennen. 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	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. 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	Der Akku im Speicher-Controller des Geräts ist abgelaufen. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: ◦ 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	Der Akku im Speicher-Controller des Geräts ist ausgefallen. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: ◦ 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	Der Akku im Speicher-Controller des Geräts weist nicht genügend Kapazität auf. 1. Tauschen Sie die Batterie aus. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: ◦ 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	Der Akku im Speicher-Controller des Geräts läuft langsam ab. 1. Setzen Sie die Batterie bald wieder ein. Die Schritte zum Entfernen und Austauschen einer Batterie sind in dem Verfahren zum Austausch eines Speichercontrollers enthalten. Beachten Sie die Anweisungen für Ihre Storage Appliance: ◦ 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	Der Akku im Speicher-Controller des Geräts fehlt. 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: ◦ 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	Die Batterie im Speicher-Controller des Geräts ist überhitzt. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Mögliche Gründe für die Temperaturerhöhung wie Lüfter- oder HLK-Ausfall untersuchen. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Fehler bei der BMC-Kommunikation des Geräts	Die Kommunikation mit dem Baseboard Management Controller (BMC) wurde verloren. 1. Vergewissern Sie sich, dass der BMC ordnungsgemäß funktioniert. Wählen Sie NODES, und wählen Sie dann die Registerkarte Hardware für den Geräteknoten aus. Suchen Sie das BMC IP-Feld für den Compute Controller, und navigieren Sie zu dieser IP-Adresse. 2. Versuchen Sie, BMC-Kommunikation wiederherzustellen, indem Sie den Knoten in den Wartungsmodus versetzen und dann das Gerät aus- und wieder einschalten. Beachten Sie die Anweisungen für Ihr Gerät: ◦ 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	Ein persistentes Cache-Sicherungsgerät ist fehlgeschlagen. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.
Gerät-Cache-Backup-Gerät unzureichende Kapazität	Die Kapazität des Cache-Sicherungsgeräts ist nicht ausreichend. Wenden Sie sich an den technischen Support.
Appliance Cache Backup-Gerät schreibgeschützt	Ein Cache-Backup-Gerät ist schreibgeschützt. Wenden Sie sich an den technischen Support.
Die Größe des Appliance-Cache-Speichers stimmt nicht überein	Die beiden Controller im Gerät haben unterschiedliche Cache-Größen. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Die Temperatur des Computing-Controller-Chassis des Geräts ist zu hoch	Die Temperatur des Computing-Controllers in einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten. 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG100- und SG1000-Services-Appliances ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Die CPU-Temperatur des Appliance-Compute-Controllers ist zu hoch	Die Temperatur der CPU im Computing-Controller einer StorageGRID Appliance hat einen nominalen Schwellenwert überschritten. 1. Prüfen Sie die Hardwarekomponenten auf Überhitzungsbedingungen, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ 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	Im Compute-Controller einer StorageGRID-Appliance wurde ein Hardwarefehler erkannt. - Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: - Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. - Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. - Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: 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	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. - Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: - Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. - Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. - Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: 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	Die Stromversorgung B im Compute-Controller hat ein Problem. Diese Warnmeldung weist möglicherweise darauf hin, dass das Netzteil ausgefallen ist oder dass es ein Problem bei der Stromversorgung aufweist. - Überprüfen Sie die Hardwarekomponenten auf Fehler, und befolgen Sie die empfohlenen Maßnahmen: - Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. - Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. - Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: 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	Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt. - Überprüfen Sie den Status des eos-Systemstatusdienstes in der Basis-os. - Wenn sich der Dienst im Status „angehalten“ oder „Fehler“ befindet, starten Sie den Dienst neu. - Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Fibre-Channel-Fehler des Geräts erkannt	Es wurde ein Fibre Channel-Verbindungsproblem zwischen dem Speicher-Controller des Geräts und dem Compute-Controller erkannt. 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. 1. Prüfen Sie die Hardwarekomponenten auf Fehler (NODES Appliance Node Hardware). Wenn der Status einer der Komponenten nicht „nominal“ lautet, führen Sie folgende Schritte aus: a. Stellen Sie sicher, dass die Fibre Channel-Kabel zwischen den Controllern vollständig verbunden sind. b. Stellen Sie sicher, dass die Fibre-Channel-Kabel frei von übermäßigen Kurven sind. c. Vergewissern Sie sich, dass die SFP+-Module richtig eingesetzt sind. Hinweis: Wenn dieses Problem weiterhin besteht, kann das StorageGRID-System die problematische Verbindung automatisch offline schalten. 2. Bei Bedarf die Komponenten austauschen. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG5700 Storage-Appliances ◦ SG6000 Storage-Appliances
Fehler des Fibre-Channel-HBA-Ports des Geräts	Ein Fibre-Channel-HBA-Port ist ausgefallen oder ist ausgefallen. Wenden Sie sich an den technischen Support.
Appliance Flash Cache Laufwerke sind nicht optimal	Die für den SSD-Cache verwendeten Laufwerke sind nicht optimal. 1. Ersetzen Sie die SSD-Cache-Laufwerke. Beachten Sie die Anweisungen für Ihr Gerät: ◦ 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	Der Verbindungs-/Batteriebehälter fehlt. 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. ◦ 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	Ein Port auf einer StorageGRID-Appliance beteiligt sich nicht an der LACP-Verbindung. 1. Überprüfen Sie die Konfiguration für den Switch. Stellen Sie sicher, dass die Schnittstelle in der richtigen Link-Aggregationsgruppe konfiguriert ist. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Das gesamte Netzteil des Geräts ist heruntergestuft	Die Leistung eines StorageGRID-Geräts ist von der empfohlenen Betriebsspannung abweichen. 1. Überprüfen Sie den Status von Netzteil A und B, um festzustellen, welches Netzteil ungewöhnlich funktioniert, und befolgen Sie die empfohlenen Maßnahmen: ◦ Wenn Sie über ein SG100, SG1000 oder SG6000 verfügen, verwenden Sie das BMC. ◦ Wenn Sie eine SG5600 oder SG5700 haben, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ 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	Der Speicher-Controller A in einer StorageGRID-Appliance ist ausgefallen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Fehler beim Speicher-Controller B des Geräts	Bei Speicher-Controller B in einer StorageGRID-Appliance ist ein Fehler aufgetreten. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Laufwerksausfall des Appliance-Storage-Controllers	Mindestens ein Laufwerk in einer StorageGRID-Appliance ist ausgefallen oder nicht optimal. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Hardwareproblem des Appliance Storage Controllers	SANtricity meldet, dass für eine Komponente einer StorageGRID Appliance ein Hinweis erforderlich ist. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Ausfall der Stromversorgung des Speicher-Controllers	Die Stromversorgung A in einem StorageGRID Gerät hat von der empfohlenen Betriebsspannung abweichen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Fehler bei Netzteil B des Speicher-Controllers	Stromversorgung B bei einem StorageGRID-Gerät hat von der empfohlenen Betriebsspannung abweichen. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Monitordienst der Appliance-Storage-Hardware ist ausgesetzt	Der Service, der den Status der Speicherhardware überwacht, hat die Meldung von Daten gestoppt. 1. Überprüfen Sie den Status des eos-Systemstatusdienstes in der Basis-os. 2. Wenn sich der Dienst im Status „angehalten“ oder „Fehler“ befindet, starten Sie den Dienst neu. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Appliance Storage-Shelfs ist beeinträchtigt	Der Status einer der Komponenten im Storage Shelf für eine Storage Appliance ist beeinträchtigt. 1. Verwenden Sie SANtricity System Manager, um Hardwarekomponenten zu überprüfen und die empfohlenen Maßnahmen zu befolgen. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances
Gerätetemperatur überschritten	Die nominale oder maximale Temperatur für den Lagercontroller des Geräts wurde überschritten. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Mögliche Gründe für die Temperaturerhöhung wie Lüfter- oder HLK-Ausfall untersuchen. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Temperatursensor des Geräts entfernt	Ein Temperatursensor wurde entfernt. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Auto-Kompaktor-Fehler	Beim Cassandra Auto-Kompaktor ist ein Fehler aufgetreten. Der Cassandra Auto-Kompaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank bei Überschreibungen und Löten schwerer Workloads. Diese Bedingung bleibt bestehen, aber bei bestimmten Workloads kommt es zu einem unerwartet hohen Metadatenverbrauch. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.
Audit-Protokolle werden der Warteschlange im Speicher hinzugefügt	Der Node kann Protokolle nicht an den lokalen Syslog-Server senden, und die Warteschlange im Speicher wird ausgefüllt. 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>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	Die Kennzahlen, die den Cassandra Auto-Kompaktor beschreiben, sind veraltet. Der Cassandra Auto-Kompaktor ist auf allen Storage-Nodes vorhanden und verwaltet die Größe der Cassandra-Datenbank bei Überschreibungen und Löten schwerer Workloads. Während diese Warnung weiterhin angezeigt wird, kommt es bei bestimmten Workloads zu einem unerwartet hohen Metadatenverbrauch. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Kommunikationsfehler	Die Nodes, auf denen der Cassandra-Service ausgeführt wird, haben Probleme bei der Kommunikation untereinander. 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. 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	Der Cassandra-Verdichtungsprozess ist überlastet. Wenn der Verdichtungs Vorgang 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. 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	Die Kennzahlen, die Cassandra-Reparaturaufträge beschreiben, sind veraltet. Wenn dieser Zustand mehr als 48 Stunden besteht, werden bei Client-Anfragen, z. B. Bucket-Listen, gelöschte Daten angezeigt. 1. Booten Sie den Node neu. Gehen Sie im Grid Manager zu NODES, wählen Sie den Knoten und wählen Sie die Registerkarte Aufgaben aus. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
Cassandra Reparaturfortschritt langsam	Der Fortschritt der Cassandra-Datenbankreparaturen ist langsam. 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. 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	Der Cassandra-Reparaturservice ist nicht verfügbar. 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. 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	Cassandra hat Tabellenbeschädigungen erkannt. Cassandra wird automatisch neu gestartet, wenn Tabellenbeschädigungen erkannt werden. Wenden Sie sich an den technischen Support.
Verbindungsfehler beim Cloud-Storage-Pool	Bei der Zustandsprüfung für Cloud-Storage-Pools wurde ein oder mehrere neue Fehler erkannt. 1. Wechseln Sie auf der Seite „Speicherpools“ zum Abschnitt „Cloud-Speicherpools“. 2. Sehen Sie sich die Spalte Letzter Fehler an, um zu ermitteln, welcher Cloud Storage Pool einen Fehler hat. 3. Siehe Anweisungen für Verwalten von Objekten mit Information Lifecycle Management.

Alarmname	Beschreibung und empfohlene Aktionen
DHCP-Leasing abgelaufen	Der DHCP-Leasingvertrag auf einer Netzwerkschnittstelle ist abgelaufen. Wenn der DHCP-Leasing abgelaufen ist, befolgen Sie die empfohlenen Maßnahmen: 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Siehe Anweisungen zur Wiederherstellung und Wartung.
DHCP-Leasing läuft bald ab	Der DHCP-Lease auf einer Netzwerkschnittstelle läuft demnächst aus. Um zu verhindern, dass der DHCP-Leasingraten abläuft, führen Sie die empfohlenen Maßnahmen durch: 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	Der DHCP-Server ist nicht verfügbar. Der StorageGRID-Node kann den DHCP-Server nicht kontaktieren. Das DHCP-Leasing für die IP-Adresse des Node kann nicht validiert werden. 1. Stellen Sie sicher, dass die Verbindung zwischen diesem Knoten und dem DHCP-Server auf der betroffenen Schnittstelle besteht. 2. Stellen Sie sicher, dass im betroffenen Subnetz auf dem DHCP-Server IP-Adressen zugewiesen werden können. 3. Stellen Sie sicher, dass eine permanente Reservierung für die im DHCP-Server konfigurierte IP-Adresse vorhanden ist. Oder verwenden Sie das StorageGRID-Tool zur IP-Änderung, um außerhalb des DHCP-Adressenpools eine statische IP-Adresse zuzuweisen. Siehe Anweisungen zur Wiederherstellung und Wartung.

Alarmname	Beschreibung und empfohlene Aktionen
Die Festplatten-I/O ist sehr langsam	Sehr langsamer Festplatten-I/O könnte sich auf die StorageGRID-Performance auswirken. 1. Wenn das Problem mit einem Storage Appliance-Node zusammenhängt, überprüfen Sie mithilfe von SANtricity System Manager auf fehlerhafte Laufwerke, Laufwerke mit prognostizierte Fehler oder laufende Festplattenreparaturen. Überprüfen Sie auch den Status der Fibre Channel- oder SAS-Links zwischen den Computing-Ressourcen und den Storage Controllern der Appliance, um zu überprüfen, ob Links ausgefallen sind oder übermäßige Fehlerraten angezeigt werden. 2. Überprüfen Sie das Storage-System, das die Volumes dieses Nodes hostet, um die Ursache des langsamen I/O zu ermitteln und zu korrigieren 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird. 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.
EC-Ausgleichfehler	Der Job zur Neuverteilung von Daten, die mit Löschungs-codes zwischen Speicherknoten codiert wurden, ist fehlgeschlagen oder wurde vom Benutzer angehalten. 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. <pre>'rebalance-data terminate --job-id <ID>'</pre> 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: <pre>'rebalance-data start --job-id <ID>'</pre> 5. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
EC-Reparaturfehler	Ein Reparaturauftrag für Löschungscodierte Daten ist fehlgeschlagen oder wurde angehalten. 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>'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	Ein Reparaturauftrag für Daten, die aufgrund von Erasure-Coding-Verfahren codiert wurden, ist ins Stocken geraten. 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>'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	Die E-Mail-Benachrichtigung für eine Warnmeldung konnte nicht gesendet werden. 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. 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	Ein oder mehrere auf der Seite Zertifikate konfigurierte Clientzertifikate sind kurz vor dem Ablauf. 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
Ablauf des Endpunktzertifikats des Load Balancer	Ein oder mehrere Load Balancer-Endpunktzertifikate laufen kurz vor dem Ablauf. 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. Weitere Informationen zum Verwalten von Endpunkten für den Load Balancer finden Sie im Anweisungen für die Administration von StorageGRID.
Ablauf des Serverzertifikats für die Managementoberfläche	Das für die Managementoberfläche verwendete Serverzertifikat läuft bald ab. 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.
Ablauf des globalen Serverzertifikats für S3 und Swift API	Das Serverzertifikat, das für den Zugriff auf Storage-API-Endpunkte verwendet wird, läuft bald ab. 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.
Ablauf des externen Syslog CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des externen Syslog-Serverzertifikats verwendet wird, läuft in Kürze ab. 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	Das Client-Zertifikat für einen externen Syslog-Server läuft kurz vor dem Ablauf. 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	Das vom externen Syslog-Server präsentierte Serverzertifikat läuft bald ab. 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	Der Node kann Protokolle nicht an den externen Syslog-Server weiterleiten. 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	Die MTU-Einstellung (Maximum Transmission Unit) für die Grid Network Interface (eth0) unterscheidet sich deutlich von den Knoten im Grid. Die Unterschiede in den MTU-Einstellungen könnten darauf 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. Siehe die Anleitung für die Warnmeldung zur Nichtübereinstimmung bei Grid Network MTU in Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen.

Alarmname	Beschreibung und empfohlene Aktionen
Hohe Java-Heap-Nutzung	Es wird ein hoher Prozentsatz von Java Heap Space verwendet. Wenn der Java-Heap voll ist, können Metadatendienste nicht verfügbar sein und Clientanforderungen können fehlschlagen. 1. Überprüfen Sie die ILM-Aktivitäten auf dem Dashboard. Diese Warnmeldung kann sich selbst beheben, wenn der ILM-Workload abnimmt. 2. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 3. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Hohe Latenz bei Metadatenanfragen	Die durchschnittliche Zeit für Cassandra-Metadatenabfragen ist zu lang. 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. 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	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren. 1. Vergewissern Sie sich, dass der konfigurierte LDAP-Server online und verfügbar ist. 2. Überprüfen Sie die Einstellungen auf der Seite Identity Federation. Vergewissern Sie sich, dass alle Werte aktuell sind. Siehe 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	Es ist nicht möglich, föderierte Gruppen und Benutzer von der Identitätsquelle zu synchronisieren, die von einem Mandanten konfiguriert wurde. 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	Für bestimmte Objekte kann keine Platzierung in einer ILM-Regel erzielt werden. 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. 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. Hinweis: Es kann bis zu 1 Tag dauern, bis der Alarm gelöscht wird. 4. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. 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.

Alarmname	Beschreibung und empfohlene Aktionen
Der ILM-Scan ist zu lang	Der Zeitaufwand für das Scannen, Bewerten von Objekten und Anwenden von ILM ist zu lang. 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. 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. StorageGRID verwalten
ILM-Scan-Rate niedrig	Die ILM-Scan-Rate ist auf weniger als 100 Objekte/Sekunde eingestellt. 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. 1. Ermitteln, ob im Rahmen einer laufenden Support-Untersuchung eine temporäre Änderung der ILM-Scanrate vorgenommen wurde. 2. Wenden Sie sich an den technischen Support.  Ändern Sie nie die ILM-Scanrate, ohne den technischen Support zu kontaktieren.

Alarmname	Beschreibung und empfohlene Aktionen
ABLAUF DES KMS-CA-Zertifikats	Das Zertifikat der Zertifizierungsstelle (CA), das zum Signieren des KMS-Zertifikats (Key Management Server) verwendet wird, läuft bald ab. 1. Aktualisieren Sie mithilfe der KMS-Software das CA-Zertifikat für den Schlüsselverwaltungsserver. 2. Wählen Sie im Grid Manager die Option KONFIGURATION 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. StorageGRID verwalten
ABLAUF DES KMS-Clientzertifikats	Das Clientzertifikat für einen Schlüsselverwaltungsserver läuft bald ab. 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. StorageGRID verwalten
KMS-Konfiguration konnte nicht geladen werden	Es ist die Konfiguration für den Verschlüsselungsmanagement-Server vorhanden, konnte aber nicht geladen werden. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.

Alarmname	Beschreibung und empfohlene Aktionen
KMS-Verbindungsfehler	Ein Appliance-Node konnte keine Verbindung zum Schlüsselmanagementserver für seinen Standort herstellen. 1. Wählen Sie im Grid Manager die Option KONFIGURATION 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	Der konfigurierte Schlüsselverwaltungsserver verfügt nicht über einen Verschlüsselungsschlüssel, der mit dem angegebenen Namen übereinstimmt. 1. Vergewissern Sie sich, dass der dem Standort zugewiesene KMS den korrekten Namen für den Verschlüsselungsschlüssel und alle vorherigen Versionen verwendet. 2. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen	Alle Appliance-Volumes wurden entschlüsselt, aber ein oder mehrere Volumes konnten nicht auf den neuesten Schlüssel rotieren. Kontaktieren Sie den technischen Support.
KM ist nicht konfiguriert	Für diesen Standort ist kein Schlüsselverwaltungsserver vorhanden. 1. Wählen Sie im Grid Manager die Option KONFIGURATION Sicherheit Schlüsselverwaltungsserver aus. 2. Fügen Sie für diese Site einen KMS hinzu oder fügen Sie einen Standard-KMS hinzu. StorageGRID verwalten

Alarmname	Beschreibung und empfohlene Aktionen
KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln	Ein oder mehrere Volumes auf einer Appliance mit aktivierter Node-Verschlüsselung konnten nicht mit dem aktuellen KMS-Schlüssel entschlüsselt werden. 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Stellen Sie sicher, dass auf dem Verschlüsselungsmanagement-Server (KMS) der konfigurierte Verschlüsselungsschlüssel und alle vorherigen Schlüsselversionen vorhanden sind. 3. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird.
Ablauf DES KMS-Serverzertifikats	Das vom KMS (Key Management Server) verwendete Serverzertifikat läuft in Kürze ab. 1. Aktualisieren Sie mithilfe der KMS-Software das Serverzertifikat für den Schlüsselverwaltungsserver. 2. Wenden Sie sich an den technischen Support, wenn Sie Hilfe benötigen oder diese Meldung weiterhin angezeigt wird. StorageGRID verwalten
Große Audit-Warteschlange	Die Datenträgerwarteschlange für Überwachungsmeldungen ist voll. 1. Prüfen Sie die Last auf dem System. Wenn eine beträchtliche Anzahl von Transaktionen vorhanden ist, sollte sich der Alarm im Laufe der Zeit lösen und Sie können die Warnung ignorieren. 2. Wenn die Meldung weiterhin angezeigt wird und der Schweregrad erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. 3. Verringern Sie die Betriebsrate des Clients oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie das Audit-Level für Client-Schreibvorgänge ändern und Client-Schreibvorgänge auf Fehler oder aus lesen (KONFIGURATION Überwachung Audit- und Syslog-Server). Prüfung von Audit-Protokollen

Alarmname	Beschreibung und empfohlene Aktionen
Aktivität des Legacy-CLB-Load-Balancer erkannt	Einige Clients stellen möglicherweise eine Verbindung zum veralteten CLB-Load-Balancer-Service mithilfe des S3- und Swift-API-Standardzertifikats her. 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. 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. Falls erforderlich, deaktivieren Sie diese Warnregel, wenn der CLB-Dienst nicht mehr verwendet wird.
Protokolle werden der Warteschlange auf der Festplatte hinzugefügt	Der Node kann Protokolle nicht an den externen Syslog-Server weiterleiten, und die Warteschlange auf der Festplatte wird ausgefüllt. 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.
Geringe Kapazität der Auditprotokoll-Festplatte	Der für Audit-Protokolle verfügbare Platz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger verfügbarer Node-Speicher	Die RAM-Menge, die auf einem Knoten verfügbar ist, ist gering. Ein wenig verfügbarer RAM kann auf eine Änderung der Arbeitslast oder ein Speicherleck bei einem oder mehreren Knoten hinweisen. 1. Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. 2. Wenn der verfügbare Speicher unter den Hauptwarnschwellenwert fällt, wenden Sie sich an den technischen Support.
Wenig freier Speicherplatz für den Speicherpool	Der Speicherplatz, der zur Speicherung von Objektdaten in einem Speicherpool verfügbar ist, ist gering. 1. Wählen Sie ILM Storage Pools aus. 2. Wählen Sie den Speicherpool aus, der in der Warnmeldung aufgeführt ist, und wählen Sie Details anzeigen. 3. Ermitteln, wo zusätzliche Storage-Kapazität erforderlich ist Sie können entweder jedem Standort im Speicherpool Storage-Nodes hinzufügen oder einem oder mehreren vorhandenen Storage-Nodes Storage-Volumes (LUNs) hinzufügen. 4. Führen Sie ein Erweiterungsverfahren durch, um die Speicherkapazität zu erhöhen. Erweitern Sie Ihr Raster
Wenig installierter Node-Speicher	Der installierte Arbeitsspeicher auf einem Node ist gering. Erhöhen Sie die RAM-Menge, die für die virtuelle Maschine oder den Linux-Host verfügbar ist. Überprüfen Sie den Schwellenwert für die Hauptwarnung, um die standardmäßige Mindestanforderung für einen StorageGRID-Node zu bestimmen. Die Installationsanweisungen für Ihre Plattform finden Sie unter: • Installieren Sie Red hat Enterprise Linux oder CentOS • Installieren Sie Ubuntu oder Debian • VMware installieren

Alarmname	Beschreibung und empfohlene Aktionen
Niedriger Metadaten-Storage	Der zur Speicherung von Objektmetadaten verfügbare Speicherplatz ist gering. Kritischer Alarm 1. Die Aufnahme von Objekten beenden. 2. Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. Großalarm Speicherknoten werden sofort in einem Erweiterungsverfahren hinzugefügt. • Kleine Warnung* 1. Überwachen Sie die Rate, mit der Objekt-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. Sobald neue Speicherknoten hinzugefügt wurden, gleicht das System die Objektmetadaten automatisch auf alle Speicherknoten aus, und der Alarm wird gelöscht. Siehe Anweisungen für die Warnmeldung zu niedrigem Metadaten-Speicher in Behebung von Metadatenproblemen.
Niedrige Kenngrößen für die Festplattenkapazität	Der für die Kennzahlendatenbank verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedriger Objekt-Storage	Der zum Speichern von Objektdaten verfügbare Platz ist gering. Eine Erweiterung durchführen. Sie können Storage-Volumes (LUNs) zu vorhandenen Storage-Nodes hinzufügen oder neue Storage-Nodes hinzufügen. Beheben Sie die Warnung „Niedrig Object Data Storage“ Erweitern Sie Ihr Raster

Alarmname	Beschreibung und empfohlene Aktionen
Low Read-Only-Wasserzeichen überschreiben	Der Speichervolumen Soft Read-Only-Wasserzeichen-Überschreiben ist kleiner als der für einen Speicherknoten optimierte Mindestwert. Informationen zum Beheben dieser Warnmeldung finden Sie unter Fehlerbehebung bei Warnungen zur Überbrückung von nur geringem Lesezugriff.
Niedrige Root-Festplattenkapazität	Der für die Root-Festplatte verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Niedrige Datenkapazität des Systems	Der Speicherplatz, der für StorageGRID-Systemdaten auf verfügbar ist <code>/var/local</code> Das Dateisystem ist niedrig. 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.
Geringer Tmp-Telefonspeicherplatz	Der im Verzeichnis <code>/tmp</code> verfügbare Speicherplatz ist gering. 1. Überwachen Sie diese Meldung, um zu prüfen, ob das Problem selbst behoben wird und der Festplattenspeicher wieder verfügbar ist. 2. Wenden Sie sich an den technischen Support, wenn der verfügbare Speicherplatz weiterhin abnehmen wird.
Fehler bei der Node-Netzwerkverbindung	Beim Übertragen der Daten zwischen den Nodes ist ein Fehler aufgetreten. Fehler mit der Netzwerkverbindung können ohne manuelles Eingreifen behoben werden. Wenden Sie sich an den technischen Support, wenn die Fehler nicht behoben sind. Siehe die Anweisungen für den NRER-Alarm (Network Receive Error) in Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen.

Alarmname	Beschreibung und empfohlene Aktionen
Node-Netzwerkannahme-Frame-Fehler	Bei einem hohen Prozentsatz der Netzwerkframes, die von einem Node empfangen wurden, gab es Fehler. 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. 1. Wenn Sie eine Appliance verwenden, versuchen Sie, jeden SFP+ oder SFP28 Transceiver und jedes Kabel nacheinander auszutauschen, um zu prüfen, ob die Warnmeldung gelöscht wird. 2. Wenden Sie sich an den technischen Support, wenn diese Meldung weiterhin angezeigt wird.
Der Node ist nicht mit dem NTP-Server synchronisiert	Die Zeit des Node ist nicht mit dem NTP-Server (Network Time Protocol) synchronisiert. 1. Vergewissern Sie sich, dass Sie mindestens vier externe NTP-Server angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern. 2. Überprüfen Sie, ob alle NTP-Server normal funktionieren. 3. Überprüfen Sie die Verbindungen zu den NTP-Servern. Stellen Sie sicher, dass sie nicht durch eine Firewall blockiert sind.
Der Node ist nicht mit dem NTP-Server gesperrt	Der Node ist nicht auf einen NTP-Server (Network Time Protocol) gesperrt. 1. Vergewissern Sie sich, dass Sie mindestens vier externe NTP-Server angegeben haben, die jeweils eine Stratum 3 oder eine bessere Referenz liefern. 2. Überprüfen Sie, ob alle NTP-Server normal funktionieren. 3. Überprüfen Sie die Verbindungen zu den NTP-Servern. Stellen Sie sicher, dass sie nicht durch eine Firewall blockiert sind.
Netzwerk außerhalb des Appliance-Node ist ausgefallen	Mindestens ein Netzwerkgerät ist ausgefallen oder nicht verbunden. Diese Warnung zeigt an, dass eine Netzwerkschnittstelle (eth) für einen Knoten, der auf einer virtuellen Maschine oder einem Linux-Host installiert ist, nicht zugänglich ist. Wenden Sie sich an den technischen Support.

Alarmname	Beschreibung und empfohlene Aktionen
Überprüfung der Objektexistenz fehlgeschlagen	Der Job für die Objektexistenzprüfung ist fehlgeschlagen. 1. Wählen Sie Prüfung der Existenz DES WARTUNGSOBJEKTS aus. 2. Notieren Sie die Fehlermeldung. Führen Sie die entsprechenden Korrekturmaßnahmen durch: Start fehlgeschlagen, Verbindung verloren, Unbekannter Fehler 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 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	Der Job zur Prüfung der ObjektExistenz ist blockiert. 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. 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. Wenn Sie die Schritte 1 und 2 lösen, beginnt der Job automatisch an der Stelle, an der er aufging. 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	Mindestens ein Objekt ist aus dem Raster verloren gegangen. Diese Meldung kann darauf hindeuten, dass Daten dauerhaft verloren gegangen sind und nicht wieder abgerufen werden können. 1. Untersuchen Sie diesen Alarm sofort. Möglicherweise müssen Sie Maßnahmen ergreifen, um weiteren Datenverlust zu vermeiden. Sie können auch ein verlorenes Objekt wiederherstellen, wenn Sie eine prompte Aktion ausführen. Fehlerbehebung bei verlorenen und fehlenden Objektdaten 2. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück: 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	Zu wenige Speicherknoten mit dem RSM-Service laufen oder sind an einem Standort verfügbar. Stellen Sie sicher, dass die meisten Speicherknoten, die den RSM-Dienst am betroffenen Standort haben, ausgeführt werden und sich nicht fehlerfrei befinden. Siehe „Fehlerbehebung für Plattformdienste“ im Anweisungen für die Administration von StorageGRID.
S3 PUT Objektgröße zu groß	Ein S3-Client versucht, einen PUT-Objektvorgang auszuführen, der die S3-Größenlimits überschreitet. 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	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie das Kabel und die physische Verbindung zum Admin-Netzwerkanschluss 1. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ SG100- und SG1000-Services-Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
Services-Appliance-Link im Admin-Netzwerk (oder Client-Netzwerk) herunter	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ SG100- und SG1000-Services-Appliances ◦ Deaktivieren von Meldungsregeln
Services-Appliance-Verbindung an Netzwerkport 1, 2, 3 oder 4 getrennt	Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ SG100- und SG1000-Services-Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
Die Speicherkonnektivität der Services-Appliance ist herabgesetzt	Eine der beiden SSDs in einer Services-Appliance ist ausgefallen oder nicht mit der anderen synchronisiert. Die Funktionalität der Appliance ist nicht beeinträchtigt, Sie sollten das Problem jedoch sofort beheben. Wenn beide Laufwerke ausfallen, funktioniert die Appliance nicht mehr. 1. Wählen Sie im Grid Manager die Option NODES Services Appliance und dann die Registerkarte Hardware aus. 2. Überprüfen Sie die Meldung im Feld * Storage RAID Mode*. 3. Wenn die Meldung den Status eines Neusynchronisierung anzeigt, warten Sie, bis der Vorgang abgeschlossen ist, und bestätigen Sie dann, dass die Warnmeldung behoben wurde. Eine Neusynchronisierung bedeutet, dass SSD kürzlich ersetzt oder aus einem anderen Grund erneut synchronisiert wird. 4. Wenn die Meldung angibt, dass eine der SSDs ausgefallen ist, ersetzen Sie das ausgefallene Laufwerk so bald wie möglich. Anweisungen zum Austauschen eines Laufwerks in einer Services Appliance finden Sie im Installations- und Wartungshandbuch für SG100- und SG1000-Geräte. SG100- und SG1000-Services-Appliances
Verknüpfung der Speicher-Appliance auf Admin-Netzwerk-Port 1 ausgefallen	Der Admin-Netzwerkanschluss 1 am Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie das Kabel und die physische Verbindung zum Admin-Netzwerkanschluss 1. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
Link der Storage Appliance ist im Admin-Netzwerk (oder Client-Netzwerk) inaktiv.	Die Appliance-Schnittstelle zum Admin-Netzwerk (eth1) oder dem Client-Netzwerk (eth2) ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ Deaktivieren von Meldungsregeln
Verbindung der Storage Appliance über Netzwerkport 1, 2, 3 oder 4 getrennt	Der Netzwerkanschluss 1, 2, 3 oder 4 auf dem Gerät ist ausgefallen oder ist nicht verbunden. 1. Überprüfen Sie die Kabel, SFPs und physischen Verbindungen zum StorageGRID Netzwerk. 2. Beheben Sie Verbindungsprobleme. Die Installations- und Wartungsanleitung für Ihre Appliance-Hardware finden Sie in der Installations- und Wartungsanleitung. 3. Wenn dieser Port zwecklos getrennt ist, deaktivieren Sie diese Regel. Wählen Sie im Grid Manager ALERTS Regeln, wählen Sie die Regel aus und klicken Sie auf Regel bearbeiten. Deaktivieren Sie dann das Kontrollkästchen * aktiviert*. ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances ◦ Deaktivieren von Meldungsregeln

Alarmname	Beschreibung und empfohlene Aktionen
Die Storage-Konnektivität der Storage-Appliance ist herabgesetzt	Problem mit einer oder mehreren Verbindungen zwischen dem Compute-Controller und dem Storage-Controller. 1. Gehen Sie zum Gerät, um die Port-Kontrollleuchten zu überprüfen. 2. Wenn die LEDs eines Ports nicht leuchten, überprüfen Sie, ob das Kabel ordnungsgemäß angeschlossen ist. Ersetzen Sie bei Bedarf das Kabel. 3. Warten Sie bis zu fünf Minuten. 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. 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	Auf ein Speichergerät kann nicht zugegriffen werden. Diese Meldung gibt an, dass ein Volume nicht angehängt oder auf dieses zugegriffen werden kann, weil ein Problem mit einem zugrunde liegenden Speichergerät vorliegt. 1. Überprüfen Sie den Status aller für den Knoten verwendeten Speichergeräte: ◦ Wenn der Knoten auf einer virtuellen Maschine oder einem Linux-Host installiert ist, befolgen Sie die Anweisungen für Ihr Betriebssystem, um die Hardware-Diagnose auszuführen oder eine Dateisystemprüfung durchzuführen. ▪ Installieren Sie Red hat Enterprise Linux oder CentOS ▪ Installieren Sie Ubuntu oder Debian ▪ VMware installieren ◦ Wenn der Node auf einer SG100-, SG1000- oder SG6000-Appliance installiert ist, verwenden Sie den BMC. ◦ Wenn der Node auf einer SG5600 oder SG5700 Appliance installiert ist, verwenden Sie SANtricity System Manager. 2. Ersetzen Sie die Komponente bei Bedarf. Beachten Sie die Anweisungen für Ihr Gerät: ◦ SG6000 Storage-Appliances ◦ SG5700 Storage-Appliances ◦ SG5600 Storage Appliances

Alarmname	Beschreibung und empfohlene Aktionen
Hohe Kontingentnutzung für Mandanten	Ein hoher Prozentsatz des Kontingentspeichers wird verwendet. Wenn ein Mieter seine Quote überschreitet, werden Neuanlässe abgelehnt. Hinweis: Diese Alarmregel ist standardmäßig deaktiviert, da sie viele Benachrichtigungen erzeugen kann. 1. Wählen Sie im Grid Manager die Option MITERS aus. 2. Sortieren Sie die Tabelle nach Quotenausnutzung. 3. Wählen Sie einen Mandanten aus, dessen Quotenauslastung fast 100 % beträgt. 4. Führen Sie einen oder beide der folgenden Schritte aus: ◦ Wählen Sie Bearbeiten, um das Speicherkontingent für den Mieter zu erhöhen. ◦ Benachrichtigen Sie den Mandanten, dass seine Kontingentauslastung hoch ist.
Kommunikation mit Knoten nicht möglich	Mindestens ein Service reagiert nicht oder der Node kann nicht erreicht werden. Diese Warnmeldung gibt an, dass ein Knoten aus einem unbekannten Grund getrennt ist. Beispielsweise wird ein Service auf dem Node möglicherweise angehalten, oder der Node hat aufgrund eines Stromausfalls oder eines unerwarteten Ausfalls seine Netzwerkverbindung verloren. Überwachen Sie diese Warnung, um zu sehen, ob das Problem selbst behoben wird. Wenn das Problem weiterhin besteht: 1. Stellen Sie fest, ob eine weitere Warnung auf diesen Node wirkt. Dieser Alarm kann möglicherweise gelöst werden, wenn Sie die andere Meldung beheben. 2. Vergewissern Sie sich, dass alle Dienste auf diesem Knoten ausgeführt werden. Wenn ein Dienst angehalten wird, versuchen Sie, ihn zu starten. Siehe Anweisungen zur Wiederherstellung und Wartung. 3. Stellen Sie sicher, dass der Host für den Node eingeschaltet ist. Falls nicht, starten Sie den Host. Hinweis: Wenn mehr als ein Host ausgeschaltet ist, lesen Sie den Anweisungen zur Wiederherstellung und Wartung. 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	Ein Node wurde in den letzten 24 Stunden unerwartet neu gebootet. 1. Überwachen Sie diesen Alarm. Der Alarm wird nach 24 Stunden gelöscht. Wenn der Node jedoch unerwartet neu gebootet wird, wird die Warnmeldung erneut ausgelöst. 2. Wenn Sie die Meldung nicht beheben können, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.
Nicht identifizierte beschädigte Objekte erkannt	Im replizierten Objekt-Storage wurde eine Datei gefunden, die nicht als repliziertes Objekt identifiziert werden konnte. 1. Ermitteln Sie, ob Probleme mit dem zugrunde liegenden Speicher auf einem Speicherknoten auftreten. Führen Sie beispielsweise die Hardwarediagnose aus oder führen Sie eine Dateisystemprüfung durch. 2. Nach der Lösung von Storage-Problemen Überprüfung der ObjektExistenz ausführen Um festzustellen, ob replizierte Kopien, wie in Ihren ILM-Richtlinien definiert, fehlen. 3. Überwachen Sie diesen Alarm. Die Warnmeldung wird nach 24 Stunden gelöscht, wird jedoch erneut ausgelöst, wenn das Problem noch nicht behoben wurde. 4. Wenn Sie die Meldung nicht beheben können, wenden Sie sich an den technischen Support.

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.

1. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API Documentation** aus.
2. Suchen Sie nach den **Metriken**-Vorgängen.
3. Ausführen des `GET /grid/metric-names` Betrieb.
4. 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	Gesamtzahl der vom StorageGRID System erkannten Objekte, die von diesem Service als fehlend erkannt werden. Es sollten Maßnahmen ergriffen werden, um die Ursache des Schadens zu ermitteln und ob eine Erholung möglich ist. Fehlerbehebung bei verlorenen und fehlenden Objektdaten
storagegrid_http_Sessions_Incoming_versuchte	Die Gesamtzahl der HTTP-Sitzungen, die zu einem Speicherknoten versucht wurden.
storagegrid_http_Sessions_Incoming_derzeit_etabliertes	Die Anzahl der derzeit aktiven HTTP-Sitzungen (offen) auf dem Speicherknoten.
storagegrid_http_Sessions_INCOMING_FAILED	Die Gesamtzahl der HTTP-Sitzungen, die nicht erfolgreich abgeschlossen wurden, entweder aufgrund einer fehlerhaften HTTP-Anfrage oder aufgrund eines Fehlers bei der Verarbeitung eines Vorgangs.
storagegrid_http_Sessions_Incoming_successful	Die Gesamtzahl der erfolgreich abgeschlossenen HTTP-Sitzungen.
storagegrid_ilm_awaiting_background_Objects	Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus dem Scan warten
storagegrid_ilm_awaiting_Client_Evaluation_Objects_per_Second	Die aktuelle Rate, mit der Objekte im Vergleich zur ILM-Richtlinie auf diesem Node bewertet werden.
storagegrid_ilm_awaiting_Client_Objects	Die Gesamtzahl der Objekte auf diesem Node, die auf eine ILM-Bewertung aus den Client-Vorgängen (z. B. Aufnahme) warten
storagegrid_ilm_awaiting_total_Objects	Gesamtzahl der Objekte, die auf eine ILM-Bewertung warten
storagegrid_ilm_Scan_Objects_per_Second	Die Geschwindigkeit, mit der Objekte des Node gescannt und für ILM in der Warteschlange gestellt werden.
storagegrid_ilm_Scan_Period_Geschätzter_Minuten	Die geschätzte Zeit zum Abschließen eines vollständigen ILM-Scans auf diesem Node. Hinweis: Ein vollständiger Scan garantiert nicht, dass ILM auf alle Objekte angewendet wurde, die sich im Besitz dieses Knotens befinden.

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_endpunktes_cert_expiry_days	Die Anzahl der Tage, bevor das Objekt-Speicher-API-Zertifikat abläuft.
storagegrid_Service_cpu_Sekunden	Der kumulierte Zeitaufwand, die die CPU seit der Installation bei diesem Service verwendet hat.
storagegrid_Service_Memory_Usage_Byte	Die Speichermenge (RAM), die derzeit von diesem Dienst verwendet wird. Dieser Wert ist identisch mit dem, der vom Linux-Top-Dienstprogramm als RES angezeigt wird.
storagegrid_Service_Network_received_Byte	Die Gesamtanzahl der Daten, die seit der Installation von diesem Service eingehen.
storagegrid_Service_Network_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	Der aktuelle Status der Storage-Services. Attributwerte sind: • 10 = Offline • 15 = Wartung • 20 = schreibgeschützt • 30 = Online
storagegrid_Storage_Status	Der aktuelle Status der Storage-Services. Attributwerte sind: • 0 = Keine Fehler • 10 = In Transition • 20 = Nicht Genügend Freier Speicherplatz • 30 = Volume(s) nicht verfügbar • 40 = Fehler

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_Utifficiendatiy_Metadata_Bytes	Die Menge der Objekt-Metadaten auf dem Storage-Volume 0 in Bytes.
storagegrid_Storage_Utifficienfficienals_total_space_Bytes	Der gesamte Speicherplatz, der allen Objektspeichern zugewiesen ist.
storagegrid_Storage_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	Stellen Sie die Verbindung zu einem Dienst (einem ADC-Dienst) wieder her, der einen Attributrelais-Dienst so schnell wie möglich ausführt. Wenn keine angeschlossenen Attributrelais vorhanden sind, kann der Grid-Node keine Attributwerte an den NMS-Dienst melden. So kann der NMS-Dienst den Status des Dienstes nicht mehr überwachen oder Attribute für den Dienst aktualisieren. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
ACMS	Verfügbare Metadaten	BARC, BLDR, BCMN	Ein Alarm wird ausgelöst, wenn ein LDR- oder ARC-Dienst die Verbindung zu einem DDS-Dienst verliert. In diesem Fall können Transaktionen nicht verarbeitet werden. Wenn die Nichtverfügbarkeit von DDS-Diensten nur ein kurzes vorübergehendes Problem ist, können Transaktionen verzögert werden. Überprüfen und Wiederherstellen der Verbindungen zu einem DDS-Dienst, um diesen Alarm zu löschen und den Service auf die volle Funktionalität zurückzugeben.

Codieren	Name	Service	Empfohlene Maßnahmen
AKTE	Status Des Cloud Tiering Service	LICHTBOGEN	Nur verfügbar für Archiv-Nodes mit einem Zieltyp von Cloud Tiering - Simple Storage Service (S3). Wenn das ATTRIBUT ACTS für den Archiv-Node auf Read-Only aktiviert oder Read-Write deaktiviert ist, müssen Sie das Attribut auf Read-Write aktiviert setzen. Wenn ein Hauptalarm aufgrund eines Authentifizierungsfehlers ausgelöst wird, überprüfen Sie ggf. die mit dem Ziel-Bucket verknüpften Anmeldeinformationen und aktualisieren Sie Werte. Wenn aus irgendeinem anderen Grund ein Großalarm ausgelöst wird, wenden Sie sich an den technischen Support.
ADCA	ADC-Status	ADU	Wenn ein Alarm ausgelöst wird, wählen Sie SUPPORT Tools Grid-Topologie. Wählen Sie dann site Grid Node ADC Übersicht Main und ADC Alarme Main, um die Ursache des Alarms zu bestimmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
ADCE	ADC-Status	ADU	Wenn der Wert des ADC-Status Standby lautet, setzen Sie die Überwachung des Dienstes fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert des ADC-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

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

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

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

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

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

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

Codieren	Name	Service	Empfohlene Maßnahmen
BASF	Verfügbare Objektkennungen	CMN	Wenn ein StorageGRID System bereitgestellt wird, wird dem CMN-Service eine feste Anzahl von Objekt-IDs zugewiesen. Dieser Alarm wird ausgelöst, wenn das StorageGRID-System seine Versorgung mit Objektkennungen ausgibt. Wenden Sie sich an den technischen Support, um weitere Kennungen zuzuweisen.
BASS	Identifizier Block Zuordnungsstatus	CMN	Standardmäßig wird ein Alarm ausgelöst, wenn Objektkennungen nicht zugewiesen werden können, da ADC Quorum nicht erreicht werden kann. 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. Wenn ein Alarm ausgelöst wird, untersuchen Sie den Grund für den Verlust von ADC-Quorum (z. B. ein Netzwerk- oder Speicherknoten-Ausfall) und ergreifen Sie Korrekturmaßnahmen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
BRDT	Temperatur Im Computing-Controller-Chassis	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur des Compute-Controllers in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Prüfen Sie die Hardware-Komponenten und Umweltprobleme auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
BTOF	Offset	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Ein Alarm wird ausgelöst, wenn die Servicezeit (Sekunden) erheblich von der Betriebssystemzeit abweicht. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Servicezeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
BTSE	Uhrstatus	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Ein Alarm wird ausgelöst, wenn die Servicezeit nicht mit der vom Betriebssystem erfassten Zeit synchronisiert wird. Unter normalen Bedingungen sollte sich der Dienst neu synchronisieren. Wenn sich die Zeit zu weit von der Betriebssystemzeit abdriftet, können Systemvorgänge beeinträchtigt werden. Vergewissern Sie sich, dass die Zeitquelle des StorageGRID-Systems korrekt ist. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CAHP	Java Heap-Nutzung In Prozent	DDS	Ein Alarm wird ausgelöst, wenn Java die Garbage-Sammlung nicht mit einer Rate durchführen kann, die genügend Heap-Speicherplatz für eine ordnungsgemäße Funktion des Systems zulässt. Ein Alarm kann einen Benutzer-Workload anzeigen, der die im System verfügbaren Ressourcen für den DDS-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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CAIH	Anzahl Der Verfügbaren Aufnahmeziele	CLB	Dieser Alarm ist veraltet.
CAQH	Anzahl Der Verfügbaren Ziele	CLB	Dieser Alarm wird gelöscht, wenn die zugrunde liegenden Probleme der verfügbaren LDR-Dienste behoben werden. Stellen Sie sicher, dass die HTTP-Komponente der LDR-Dienste online ist und ordnungsgemäß ausgeführt wird. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Codieren	Name	Service	Empfohlene Maßnahmen
CASA	Data Store-Status	DDS	Wenn der Cassandra-Metadatenpeicher nicht mehr verfügbar ist, wird ein Alarm ausgelöst. Den Status von Cassandra überprüfen: 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> Dieser Alarm kann auch zeigen, dass der Metadatenpeicher (Cassandra-Datenbank) für einen Storage-Node eine Neuerstellung erfordert. Weitere Informationen zur Fehlerbehebung im Alarm Services: Status - Cassandra (SVST) in Behebung von Metadatenproblemen. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
FALL	Datenspeicherstatus	DDS	Dieser Alarm wird während der Installation oder Erweiterung ausgelöst, um anzuzeigen, dass ein neuer Datenspeicher in das Raster eingespeist wird.
CES	Eingehende Sitzungen – Eingerichtet	CLB	Dieser Alarm wird ausgelöst, wenn auf dem Gateway Node 20,000 oder mehr HTTP-Sitzungen aktiv (offen) sind. Wenn ein Client zu viele Verbindungen hat, können Verbindungsfehler auftreten. Sie sollten den Workload reduzieren.
CCNA	Computing-Hardware	SSM	Dieser Alarm wird ausgelöst, wenn der Status der Hardware des Computing-Controllers in einer StorageGRID-Appliance zu beachten ist.

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

Codieren	Name	Service	Empfohlene Maßnahmen
CLBE	Der Status des CLB	CLB	Wenn der Wert des CLB-Status Standby lautet, setzen Sie die Überwachung der Situation fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Status Offline lautet und keine bekannten Probleme mit der Serverhardware (z. B. nicht angeschlossen) oder eine geplante Ausfallzeit auftreten, starten Sie den Service neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CMNA	CMN-Status	CMN	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. Ein Alarm wird ausgelöst, und der Wert von CMN Status ist kein Online CMN während einer Hardwareaktualisierung des primären Admin-Knotens, wenn die CMNS geschaltet werden (der Wert des alten CMN-Status ist Standby und das neue ist Online). Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
CPRC	Verbleibende Kapazität	NMS	Ein Alarm wird ausgelöst, wenn die verbleibende Kapazität (Anzahl der verfügbaren Verbindungen, die für die NMS-Datenbank geöffnet werden können) unter den konfigurierten Alarmschwerwert fällt. Wenn ein Alarm ausgelöst wird, wenden Sie sich an den technischen Support.
CPSA	Compute Controller Netzteil A	SSM	Wenn ein Problem mit der Stromversorgung A im Rechencontroller eines StorageGRID-Geräts auftritt, wird ein Alarm ausgelöst. Ersetzen Sie die Komponente bei Bedarf.
CPSB	Compute Controller Netzteil B	SSM	Bei einem StorageGRID-Gerät wird ein Alarm ausgelöst, wenn ein Problem mit der Stromversorgung B im Compute-Controller auftritt. Ersetzen Sie die Komponente bei Bedarf.

Codieren	Name	Service	Empfohlene Maßnahmen
KFUT	CPU-Temperatur für Compute Controller	SSM	Ein Alarm wird ausgelöst, wenn die Temperatur der CPU im Compute-Controller in einem StorageGRID-Gerät einen nominalen Schwellenwert überschreitet. Wenn es sich bei dem Speicherknoten um eine StorageGRID-Appliance handelt, gibt das StorageGRID-System an, dass eine Warnung für den Controller erforderlich ist. Prüfen Sie die Probleme mit den Hardwarekomponenten und der Umgebung auf überhitzte Bedingungen. Ersetzen Sie die Komponente bei Bedarf.
DNST	DNS-Status	SSM	Nach Abschluss der Installation wird im SSM-Service ein DNST-Alarm ausgelöst. Nachdem der DNS konfiguriert wurde und die neuen Serverinformationen alle Grid-Knoten erreichen, wird der Alarm abgebrochen.
ECCD	Beschädigte Fragmente Erkannt	LDR	Ein Alarm wird ausgelöst, wenn die Hintergrundüberprüfung ein korruptes Fragment mit Löschungscode erkennt. Wenn ein beschädigtes Fragment erkannt wird, wird versucht, das Fragment neu zu erstellen. Setzen Sie die beschädigten Fragmente zurück, und kopieren Sie verlorene Attribute auf Null, und überwachen Sie sie, um zu sehen, ob die Zählung wieder hoch geht. Wenn die Anzahl höher ist, kann es zu einem Problem mit dem zugrunde liegenden Speicher des Storage-Nodes kommen. Eine Kopie von Objektdaten mit Löschungscode wird erst dann als fehlend betrachtet, wenn die Anzahl der verlorenen oder korrupten Fragmente die Fehlertoleranz des Löschcodes verletzt. Daher ist es möglich, ein korruptes Fragment zu haben und das Objekt trotzdem abrufen zu können. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
ACST	Verifizierungsstatus	LDR	Dieser Alarm zeigt den aktuellen Status des Hintergrundverifizierungsverfahrens für das Löschen codierter Objektdaten auf diesem Speicherknoten an. Bei der Hintergrundüberprüfung wird ein Großalarm ausgelöst.

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

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

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

Codieren	Name	Service	Empfohlene Maßnahmen
NDUP	Einstellungen Für Den Netzwerkduplex	SSM	Überprüfen Sie die Netzwerkadapter-Konfiguration. Die Einstellung muss den Einstellungen Ihrer Netzwerk-Router und -Switches entsprechen. Eine falsche Einstellung kann schwerwiegende Auswirkungen auf die Systemleistung haben.
NLNK	Network Link Detect	SSM	Überprüfen Sie die Netzwerkverbindungen am Port und am Switch. Überprüfen Sie die Netzwerk-Router-, Switch- und Adapterkonfigurationen. Starten Sie den Server neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
RER	Fehler Beim Empfang	SSM	Die folgenden Ursachen können für NRER-Alarme sein: • Fehler bei der Vorwärtskorrektur (FEC) stimmen nicht überein • Switch-Port und MTU-NIC stimmen nicht überein • Hohe Link-Fehlerraten • NIC-Klingelpuffer überlaufen Weitere Informationen zur Fehlerbehebung im NRER-Alarm (Network Receive Error) in finden Sie unter Beheben Sie Fehler bei Netzwerk-, Hardware- und Plattformproblemen.
NRLY	Verfügbare Audit-Relais	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Wenn 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	Wenn der Wert für den NMS-Status Standby lautet, setzen Sie die Überwachung fort und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für NMS-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NSPD	Schnell	SSM	Dies kann durch Probleme mit der Netzwerkverbindung oder der Treiberkompatibilität verursacht werden. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
NTBR	Freie Tablespace	NMS	Wenn ein Alarm ausgelöst wird, überprüfen Sie, wie schnell sich die Datenbanknutzung geändert hat. Ein plötzlicher Abfall (im Gegensatz zu einer allmählichen Änderung im Laufe der Zeit) weist auf eine Fehlerbedingung hin. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support. Durch das Anpassen des Alarmschwellenwerts können Sie proaktiv verwalten, wenn zusätzlicher Storage zugewiesen werden muss. Wenn der verfügbare Speicherplatz einen niedrigen Schwellenwert erreicht (siehe Alarmschwelle), wenden Sie sich an den technischen Support, um die Datenbankzuweisung zu ändern.
NTER	Übertragungsfehler	SSM	Diese Fehler können beseitigt werden, ohne manuell zurückgesetzt zu werden. Wenn sie nicht klar sind, überprüfen Sie die Netzwerk-Hardware. Überprüfen Sie, ob die Adapterhardware und der Treiber korrekt installiert und konfiguriert sind, um mit Ihren Netzwerk-Routern und Switches zu arbeiten. Wenn das zugrunde liegende Problem gelöst ist, setzen Sie den Zähler zurück. Wählen Sie SUPPORT Tools Grid-Topologie aus. Wählen Sie dann site Grid Node SSM Ressourcen Konfiguration Main, wählen Sie Anzahl der Übertragungsfehler zurücksetzen und klicken Sie auf Änderungen anwenden.

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

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

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

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

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

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

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

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

Codieren	Name	Service	Empfohlene Maßnahmen
SSMA	SSM-Status	SSM	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. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SSME	SSM-Status	SSM	Wenn der Wert des SSM-Status „Standby“ lautet, setzen Sie die Überwachung fort, und wenden Sie sich an den technischen Support, wenn das Problem weiterhin besteht. Wenn der Wert für SSM-Status Offline lautet, starten Sie den Dienst neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.
SSTS	Storage-Status	BLDR	Wenn der Wert des Speicherstatus nicht genügend verwendbarer Speicherplatz ist, ist auf dem Speicherknoten kein verfügbarer Speicherplatz mehr verfügbar. Die Datenausgabewerte werden auf andere verfügbare Speicherknoten umgeleitet. Abruf-Anfragen können weiterhin von diesem Grid-Node bereitgestellt werden. Zusätzlicher Speicher sollte hinzugefügt werden. Sie wirkt sich nicht auf die Funktionen des Endbenutzers aus, aber der Alarm bleibt bestehen, bis zusätzlicher Speicher hinzugefügt wird. Wenn der Wert für den Speicherstatus „Volume(s) nicht verfügbar“ ist, steht ein Teil des Speichers nicht zur Verfügung. Speicher und Abruf von diesen Volumes ist nicht möglich. Weitere Informationen 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. Wenn der Wert des Speicherstatus Fehler ist, wenden Sie sich an den technischen Support. Fehlersuche im SSTS-Alarm (Storage Status) durchführen

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

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

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

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

In der folgenden Tabelle sind die älteren Alarme aufgeführt, die SNMP-Benachrichtigungen generieren. Im Gegensatz zu Warnmeldungen generieren nicht alle Alarme SNMP-Benachrichtigungen. Nur die aufgeführten Alarme erzeugen SNMP-Benachrichtigungen und nur bei dem angegebenen Schweregrad oder höher.



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

Codieren	Name	Schweregrad
ACMS	Verfügbare Metadaten	Kritisch
AITE	Status Abrufen	Gering
AITU	Status Abrufen	Major
AMQS	Audit-Nachrichten In Queued	Hinweis
AOTE	Store State	Gering
AOTU	Speicherstatus	Major
AROQ	Objekte In Queued	Gering

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.  Die Datei <code>`/var/local/core/kexec_cmd</code> ist normalerweise auf Appliance-Knoten vorhanden und weist keinen Fehler auf.	Alle Nodes

Server Manager-Protokolle

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

Protokolle für StorageGRID-Services

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

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
/var/local/log/nginx/*.log	Enthält Protokolle für den nginx-Dienst, der als Authentifizierung und sicherer Kommunikationsmechanismus für verschiedene Grid-Dienste (wie Prometheus und dynIP) fungiert, um über HTTPS-APIs mit Diensten auf anderen Knoten kommunizieren zu können.	Alle Nodes
/var/local/log/nginx-gw/*.log	Enthält Protokolle für die eingeschränkten Admin-Ports an Admin-Nodes und für den Load Balancer Service, der den Lastenausgleich von S3- und Swift-Datenverkehr von Clients zu Storage-Nodes ermöglicht.	Admin-Nodes und Gateway-Nodes
/var/local/log/persistence*	Enthält Protokolle für den Persistenzdienst, der Dateien auf der Root-Festplatte verwaltet, die bei einem Neustart erhalten bleiben müssen.	Alle Nodes
/var/local/log/prometheus.log	Enthält für alle Knoten das Service-Protokoll für den Knoten-Exporter und das Kennzahlungsprotokoll der ade-Exporter. Für Admin-Knoten enthält auch Protokolle für die Prometheus- und Alert Manager-Dienste.	Alle Nodes
/var/local/log/raft.log	Enthält die Ausgabe der Bibliothek, die vom RSM-Dienst für das Raft-Protokoll verwendet wird.	Storage-Nodes mit RSM-Service
/var/local/log/rms.errlog	Enthält Protokolle für den RSM-Service (Replicated State Machine Service), der für S3-Plattformservices verwendet wird.	Storage-Nodes mit RSM-Service
/var/local/log/ssm.errlog		Alle Nodes
/var/local/log/update-s3vs-domains.log	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-snmp-firewall.*	Enthalten Protokolle im Zusammenhang mit den Firewall-Ports, die für SNMP verwaltet werden.	Alle Nodes
/var/local/log/update-sysl.log	Enthält Protokolle in Bezug auf Änderungen an der Syslog-Konfiguration des Systems.	Alle Nodes
/var/local/log/update-traffic-classes.log	Enthält Protokolle, die sich auf Änderungen an der Konfiguration von Traffic-Klassifikatoren beziehen.	Admin- und Gateway-Nodes
/var/local/log/update-utcn.log	Enthält Protokolle, die sich auf diesem Knoten im Netzwerk des nicht vertrauenswürdigen Clients beziehen.	Alle Nodes

NMS-Protokolle

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

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 Erweiterungsereignisse.	Storage-Nodes
/var/local/log/gdu-server.log	Erstellt durch den GDU-Dienst. Enthält Ereignisse im Zusammenhang mit Provisioning- und Wartungsverfahren, die vom primären Admin-Node verwaltet werden.	Primärer Admin-Node
/var/local/log/send_admin_hw.log	Während der Installation erstellt. Enthält Debugging-Informationen zur Kommunikation eines Knotens mit dem primären Admin-Knoten.	Alle Nodes
/var/local/log/upgrade.log	Wird während eines Software-Upgrades erstellt. Enthält eine Aufzeichnung der Softwareaktualisierungs-Ereignisse.	Alle Nodes

Protokolle für Drittanbietersoftware

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

Kategorie	Dateiname	Hinweise	Gefunden am
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 (smb, nmb und winbind) und jeden Client-Hostnamen/jede IP.	Admin-Node für den Export der Revisionsfreigabe über CIFS konfiguriert

Etwa bycast.log

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

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

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 `broadcast.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	ENOC SI	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

Erweitern Sie Ihr Raster

Raster erweitern: Übersicht

Mithilfe dieser Anweisungen können Sie die Kapazität oder die Funktionen Ihres StorageGRID Systems erweitern, ohne den Betrieb des Systems zu unterbrechen.

Informationen zu diesen Anweisungen

Diese Anweisungen beschreiben die Durchführung einer StorageGRID Erweiterung zum Hinzufügen von Storage Volumes zu Storage-Nodes, zu einem vorhandenen Standort neue Grid-Nodes oder einen gesamten neuen Standort.

Diese Anweisungen gelten für technische Mitarbeiter, die nach der Installation für die Konfiguration und den Support des StorageGRID Systems verantwortlich sind.

Überblick über das Expansionsverfahren

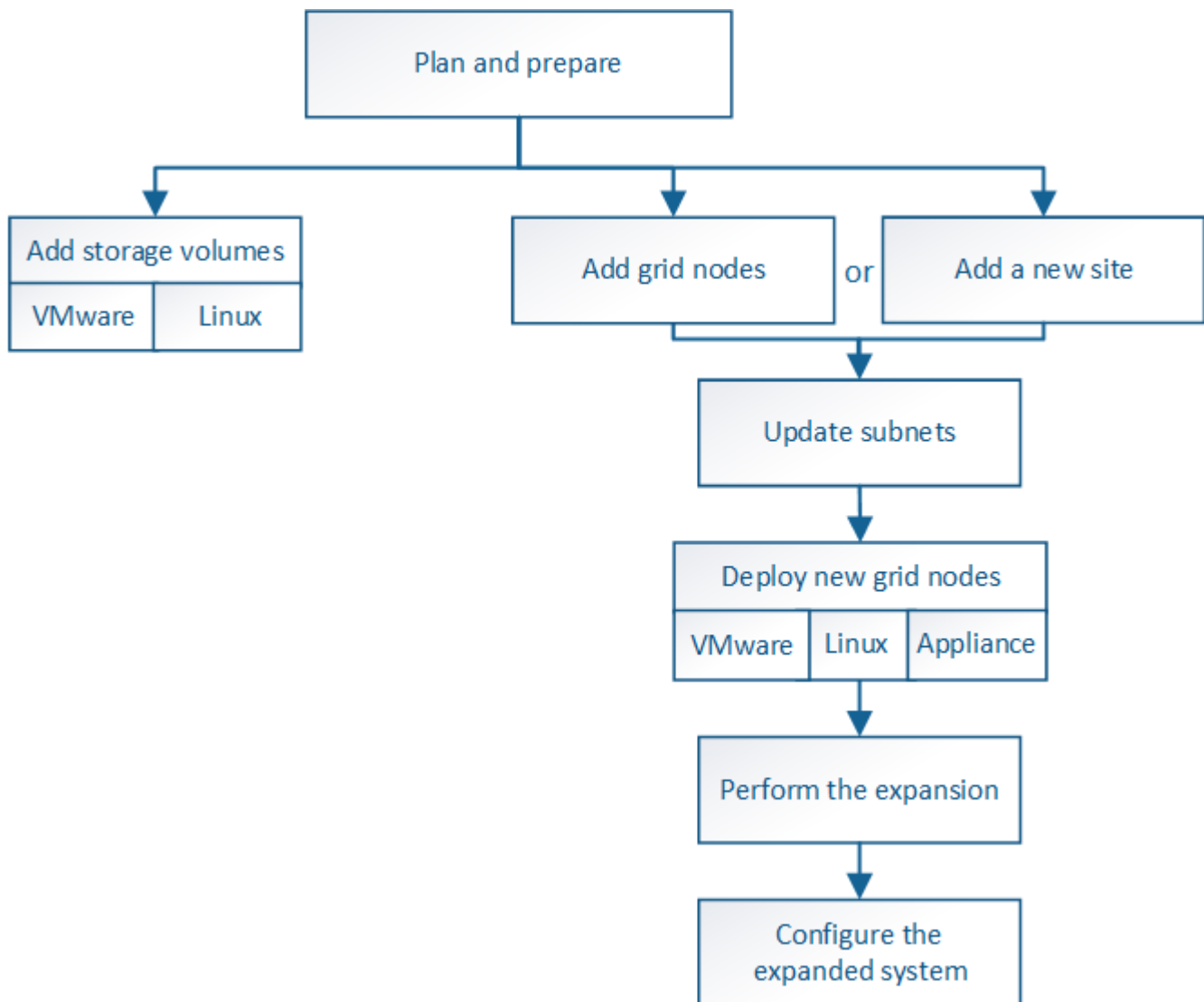
Der Grund für die Erweiterung ist ausschlaggebend dafür, wie viele neue Nodes jeden Typs Sie hinzufügen müssen, und Speicherort dieser neuen Nodes. Beispielsweise bestehen unterschiedliche Node-Anforderungen, wenn Sie eine Erweiterung zur Erhöhung der Storage-Kapazität, das Hinzufügen von Metadaten-Kapazität oder das Hinzufügen von Redundanz oder neuen Funktionen durchführen.

Wie im Workflow-Diagramm dargestellt, hängen die Schritte zur Durchführung einer Erweiterung davon ab, ob Sie Storage-Volumes zu einem Storage Node hinzufügen, einem vorhandenen Standort neue Nodes hinzufügen oder einen neuen Standort hinzufügen. In allen Fällen können Sie die Erweiterung durchführen, ohne den Betrieb des aktuellen Systems zu unterbrechen.

Die Schritte zum Hinzufügen von Nodes hängen auch davon ab, ob Sie StorageGRID-Appliances oder Hosts mit VMware oder Linux hinzufügen.



„Linux“ bezieht sich auf eine Red hat® Enterprise Linux®, Ubuntu®, CentOS- oder Debian®-Bereitstellung. Verwenden Sie die "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Um eine Liste der unterstützten Versionen zu erhalten.



Planen Sie eine Erweiterung von StorageGRID

Erweitern Sie Ihre Storage-Kapazität

Richtlinien zum Hinzufügen von Objektkapazität

Sie können die Objekt-Storage-Kapazität Ihres StorageGRID Systems erweitern, indem Sie vorhandenen Storage-Nodes Storage-Volumes hinzufügen oder vorhandenen Standorten neue Storage-Nodes hinzufügen. Storage-Kapazität muss so hinzugefügt werden, dass sie den Anforderungen Ihrer Information Lifecycle Management (ILM)-Richtlinie entspricht.

Richtlinien für das Hinzufügen von Storage Volumes

Lesen Sie vor dem Hinzufügen von Storage-Volumes zu vorhandenen Storage-Nodes die folgenden Richtlinien und Einschränkungen:

- Sie müssen Ihre aktuellen ILM-Regeln prüfen, um festzustellen, wo und wann Storage-Volumes hinzugefügt werden müssen, um die Storage-Kapazität für replizierte oder Erasure-codierte Objekte zu erhöhen. Siehe Anweisungen für [Verwalten von Objekten mit Information Lifecycle Management](#).
- Die Metadatenkapazität des Systems kann nicht durch Hinzufügen von Storage-Volumes erhöht werden, da Objektmetadaten nur auf Volume 0 gespeichert werden.
- Jeder softwarebasierte Storage Node kann maximal 16 Storage Volumes unterstützen. Wenn Sie darüber hinaus Kapazität hinzufügen möchten, müssen Sie neue Storage-Nodes hinzufügen.
- Jeder SG6060- oder SG6060X-Appliance kann ein oder zwei Erweiterungs-Shelfs hinzugefügt werden. Mit jedem Erweiterungs-Shelf werden 16 Storage-Volumes hinzugefügt. Bei installierten beiden Erweiterungs-Shelfs können SG6060 und SG6060X jeweils insgesamt 48 Storage Volumes unterstützen.
- Sie können keine Speicher-Volumes zu einer anderen Speicher-Appliance hinzufügen.
- Sie können die Größe eines vorhandenen Speichervolumens nicht erhöhen.
- Sie können Storage-Volumes nicht gleichzeitig einem Storage-Node hinzufügen, wenn Sie ein System-Upgrade, Recovery-Vorgang oder eine andere Erweiterung durchführen.

Nachdem Sie sich entschieden haben, Storage Volumes hinzuzufügen und festgestellt haben, welche Storage Nodes Sie erweitern müssen, um Ihre ILM-Richtlinie zu erfüllen, befolgen Sie die Anweisungen für Ihren Storage Node-Typ:

- Um ein oder zwei Erweiterungs-Shelfs zu einer SG6060- oder SG6060X-Storage Appliance hinzuzufügen, gehen Sie zu [Erweiterungs-Shelf für das implementierte SG6060 oder SG6060X hinzufügen](#).
- Befolgen Sie die Anweisungen für [Hinzufügen von Storage-Volumes zu Storage-Nodes](#), um einen softwarebasierten Node zu erhalten.

Richtlinien zum Hinzufügen von Speicherknoten

Lesen Sie vor dem Hinzufügen von Speicherknoten zu vorhandenen Standorten die folgenden Richtlinien und Einschränkungen durch:

- Sie müssen Ihre aktuellen ILM-Regeln prüfen, um festzustellen, wo und wann Storage-Nodes hinzugefügt werden müssen, um den Storage für replizierte oder Erasure-codierte Objekte zu erhöhen. Siehe Anweisungen für [Verwalten von Objekten mit Information Lifecycle Management](#).

- Sie sollten nicht mehr als 10 Speicherknoten in einem einzigen Erweiterungsverfahren hinzufügen.
- Sie können Speicherknoten zu mehr als einem Standort in einem einzigen Erweiterungsverfahren hinzufügen.
- Sie können Storage-Nodes und andere Node-Typen in einem einzigen Erweiterungsverfahren hinzufügen.
- Bevor Sie mit dem Erweiterungsvorgang beginnen, müssen Sie bestätigen, dass alle Datenreparaturvorgänge, die im Rahmen einer Wiederherstellung durchgeführt werden, abgeschlossen sind. Siehe [Prüfen Sie die Reparatur von Daten](#).
- Wenn Sie Storage-Nodes vor oder nach einer Erweiterung entfernen müssen, sollten Sie nicht mehr als 10 Storage-Nodes in einem einzigen Dekommissions-Node-Verfahren außer Betrieb nehmen.

Richtlinien für ADC-Service auf Storage-Nodes

Beim Konfigurieren der Erweiterung müssen Sie festlegen, ob der Dienst Administrative Domain Controller (ADC) auf jedem neuen Speicherknoten enthalten soll. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services.

- Das StorageGRID System erfordert eine [Quorum von ADC-Services](#) Zu jeder Zeit und an jedem Standort verfügbar zu sein.
- Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten.
- Es wird nicht empfohlen, jedem Speicherknoten den ADC-Dienst hinzuzufügen. Die Einbeziehung von zu vielen ADC-Services kann zu Verlangsamungen führen, da die Kommunikation zwischen den Knoten größer ist.
- Ein einzelnes Grid sollte nicht mehr als 48 Storage-Nodes mit dem ADC-Dienst aufweisen. Dies entspricht 16 Standorten mit drei ADC-Diensten an jedem Standort.
- Wenn Sie im Allgemeinen die Einstellung **ADC-Dienst** für einen neuen Knoten auswählen, sollten Sie **automatisch** wählen. Wählen Sie **Ja** nur aus, wenn der neue Knoten einen anderen Speicherknoten ersetzt, der den ADC-Dienst enthält. Da ein Storage-Node nicht stillgelegt werden kann, wenn zu wenige ADC-Dienste verbleiben, wird sichergestellt, dass ein neuer ADC-Service verfügbar ist, bevor der alte Service entfernt wird.
- Der ADC-Dienst kann nicht einem Node hinzugefügt werden, nachdem er bereitgestellt wurde.

Storage-Kapazitäten für replizierte Objekte hinzufügen

Wenn die Information Lifecycle Management-Richtlinie (ILM) für Ihre Implementierung eine Regel umfasst, die replizierte Kopien von Objekten erstellt, müssen Sie berücksichtigen, wie viel Storage hinzugefügt werden muss und wo die neuen Storage Volumes oder Storage-Nodes hinzugefügt werden müssen.

Anweisungen zum Hinzufügen von zusätzlichem Storage finden Sie in den ILM-Regeln, die replizierte Kopien erstellen. Wenn ILM-Regeln zwei oder mehr Objektkopien erstellen, planen Sie das Hinzufügen von Storage an jedem Speicherort, an dem Objektkopien erstellt werden. Wenn Sie ein Grid mit zwei Standorten und eine ILM-Regel haben, die an jedem Standort eine Objektkopie erstellt, müssen Sie jedem Standort Storage hinzufügen, um die allgemeine Objektkapazität des Grids zu erhöhen. Siehe Anweisungen für [Verwalten von Objekten mit Information Lifecycle Management](#).

Aus Performance-Gründen sollten Sie versuchen, die Storage-Kapazität und die Rechenleistung über die Standorte hinweg gleichmäßig zu verteilen. In diesem Beispiel sollten Sie also jedem Standort die gleiche Anzahl an Storage-Nodes oder an jedem Standort zusätzliche Storage-Volumes hinzufügen.

Falls Sie eine komplexere ILM-Richtlinie haben, die Regeln enthält, die Objekte basierend auf Kriterien wie

Bucket-Name oder Regeln, die Objektorte im Laufe der Zeit ändern, wird Ihre Analyse, wo Storage für die Erweiterung erforderlich ist, ähnlich, aber komplexer.

Wenn Sie verstehen, wie schnell die insgesamt genutzte Storage-Kapazität verbraucht wird, können Sie verstehen, wie viel Storage in der Erweiterung hinzugefügt werden muss und wann der zusätzliche Speicherplatz erforderlich ist. Mithilfe des Grid Managers können Sie die Speicherkapazität überwachen und darstellen, wie in den Anweisungen für beschrieben [StorageGRID zur Überwachung und Fehlerbehebung](#).

Denken Sie bei der Planung des Zeitpunkts einer Erweiterung daran, wie lange die Beschaffung und Installation von zusätzlichem Storage dauern könnte.

Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden

Wenn Ihre ILM-Richtlinie eine Regel zur Erstellung von Kopien zur Fehlerkorrektur enthält, müssen Sie planen, wo neuer Storage hinzugefügt werden muss und wann neuer Storage hinzugefügt werden muss. Die Menge des Hinzufügen von Speicherplatz und der Zeitpunkt der Hinzufügung können die nutzbare Speicherkapazität des Grid beeinflussen.

Der erste Schritt bei der Planung einer Storage-Erweiterung ist das untersuchen der Regeln in Ihrer ILM-Richtlinie, die Objekte mit Erasure-Coding-Verfahren erstellt. Da StorageGRID für jedes Objekt, das mit Erasure-Coding-Verfahren codiert wurde, $k+m$ Fragmente erstellt und jedes Fragment auf einem anderen Storage-Node speichert, müssen Sie sicherstellen, dass mindestens $k+m$ Storage-Nodes nach der Erweiterung über Platz für neue Daten mit Erasure-Code verfügen. Wenn das Erasure Coding-Profil einen Site-Loss-Schutz bietet, müssen Sie jedem Standort Storage hinzufügen. Siehe [Objektmanagement mit ILM](#).

Die Anzahl der Nodes, die Sie hinzufügen müssen, hängt auch davon ab, wie voll die vorhandenen Nodes sind, wenn Sie die Erweiterung durchführen.

Allgemeine Empfehlung für die Erweiterung der Storage-Kapazität für Objekte mit Erasure-Coding-Verfahren

Wenn detaillierte Berechnungen vermieden werden sollen, können Sie zwei Storage-Nodes pro Standort hinzufügen, wenn vorhandene Storage-Nodes eine Kapazität von 70 % erreichen.

Diese allgemeine Empfehlung liefert angemessene Ergebnisse für eine Vielzahl von Erasure Coding-Schemata für Grids an einem Standort und für Grids, bei denen ein Erasure Coding-Verfahren einen Site-Loss-Schutz bietet.

Um die Faktoren, die zu dieser Empfehlung führen, besser zu verstehen oder einen genaueren Plan für Ihren Standort zu entwickeln, überprüfen Sie den nächsten Abschnitt. Wenden Sie sich an Ihren NetApp Ansprechpartner, um eine für Ihre Situation optimierte Empfehlung zu erhalten.

Berechnen Sie die Anzahl der Erweiterungs-Storage-Nodes, die für Objekte mit Erasure-Coding-Verfahren hinzugefügt werden sollen

Um die Erweiterung einer Implementierung zur Speicherung von Objekten, die mit Erasure-Coding-Verfahren codiert wurden, zu optimieren, müssen Sie viele Faktoren berücksichtigen:

- Verwendung eines Schemas zur Einhaltung von Datenkonsistenz (Erasure Coding)
- Merkmale des für das Verfahren zur Einhaltung von Datenkonsistenz verwendeten Storage Pools, einschließlich der Anzahl der Nodes an jedem Standort und der Menge an freiem Speicherplatz auf jedem Node

- Gibt an, ob das Grid zuvor erweitert wurde (da sich der freie Speicherplatz pro Storage-Node möglicherweise nicht in etwa auf allen Nodes identisch befindet)
- Die genaue Natur der ILM-Richtlinie, beispielsweise darüber, ob ILM-Regeln replizierte und Erasure-Coding-Objekte erstellen

Die folgenden Beispiele zeigen, welche Auswirkungen das Erasure Coding-Schema hat, die Anzahl der Nodes im Storage-Pool und die Menge an freiem Speicherplatz auf jedem Node.

Ähnliche Überlegungen wirken sich auf die Berechnungen für eine ILM-Richtlinie aus, die sowohl replizierte Daten als auch Daten mit Erasure-Coding-Verfahren speichert und die Berechnungen für ein zuvor erweitertes Grid enthält.



Die Beispiele in diesem Abschnitt stellen die Best Practices für das Hinzufügen von Speicherkapazität zu einem StorageGRID System dar. Wenn Sie die empfohlene Anzahl an Nodes nicht hinzufügen können, müssen Sie möglicherweise das EC-Ausgleichsverfahren durchführen, um zusätzliche, mit Erasure Coding versehenen Objekte zu speichern. Siehe [Ausgleich von Daten, die zur Einhaltung von Datenkonsistenz \(Erasure Coding\)](#).

Beispiel 1: Erweitertes Grid mit einem Standort, das 2+1 Erasure Coding verwendet

Dieses Beispiel zeigt, wie ein einfaches Raster erweitert wird, das nur drei Storage-Nodes enthält.



Dieses Beispiel verwendet nur drei Storage-Nodes zur Vereinfachung. Es wird jedoch nicht empfohlen, nur drei Speicherknoten zu verwenden: Ein tatsächliches Produktionsnetz sollte mindestens $k+m+1$ Speicherknoten verwenden, um Redundanz zu erhalten, was vier Speicherknoten (2+1+1) entspricht.

Gehen Sie folgendermaßen vor:

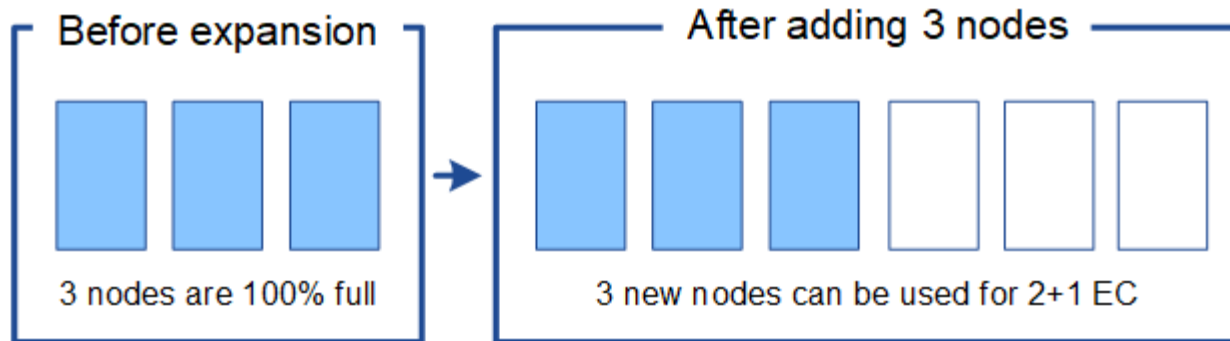
- Alle Daten werden mithilfe des 2+1-Schemas zur Einhaltung von Datenkonsistenz gespeichert. Mit dem Erasure Coding-Schema 2+1 wird jedes Objekt als drei Fragmente gespeichert und jedes Fragment auf einem anderen Storage Node gespeichert.
- Es gibt einen Standort mit drei Storage-Nodes. Jeder Storage-Node hat eine Gesamtkapazität von 100 TB.
- Sie möchten erweitern, indem Sie neue 100-TB-Storage-Nodes hinzufügen.
- Ziel ist es, mithilfe von Erasure Coding Daten auf die alten und neuen Nodes einen Ausgleich zu finden.

Je nachdem, wie voll die Speicherknoten sind, wenn Sie die Erweiterung durchführen, stehen verschiedene Optionen zur Verfügung.

- **Fügen Sie drei 100 TB Storage Nodes hinzu, wenn die vorhandenen Knoten zu 100% voll sind**

In diesem Beispiel sind die vorhandenen Nodes zu 100 % ausgelastet. Da keine freie Kapazität vorhanden ist, müssen Sie sofort drei Nodes hinzufügen, um mit dem Erasure Coding von 2+1 fortzufahren.

Nach Abschluss der Erweiterung werden bei Erasure-Coding von Objekten alle Fragmente auf die neuen Nodes platziert.

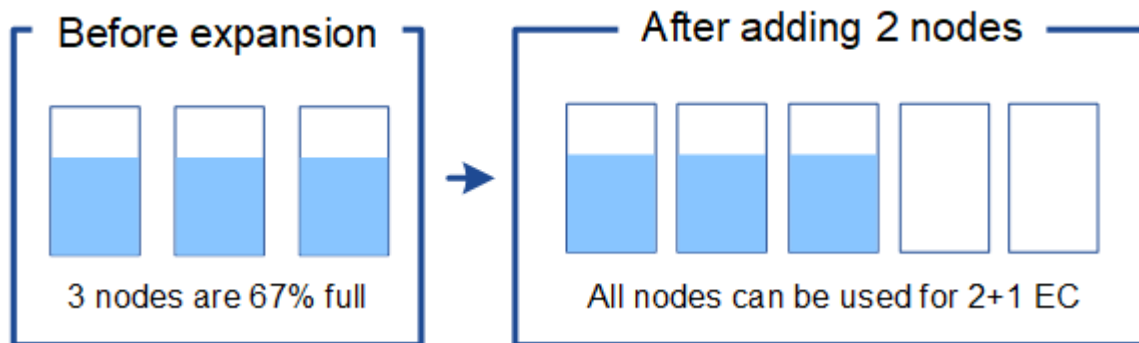


Durch diese Erweiterung werden Nodes $k+m$ hinzugefügt. Das Hinzufügen von vier Nodes wird aus Redundanzgründen empfohlen. Wenn Sie Storage-Nodes mit $k+m$ -Erweiterung hinzufügen, wenn vorhandene Nodes zu 100 % voll sind, werden alle neuen Objekte auf den Erweiterungs-Nodes gespeichert. Wenn einer der neuen Nodes nicht verfügbar ist, kann StorageGRID die ILM-Anforderungen selbst vorübergehend nicht erfüllen.

- **Fügen Sie zwei 100 TB Storage-Nodes hinzu, wenn die vorhandenen Storage-Nodes zu 67 % voll sind**

In diesem Beispiel sind die vorhandenen Nodes zu 67 % ausgelastet. Da auf den vorhandenen Nodes 100 TB an freier Kapazität verfügbar sind (33 TB pro Node), müssen Sie nur noch zwei Nodes hinzufügen, wenn Sie die Erweiterung jetzt durchführen.

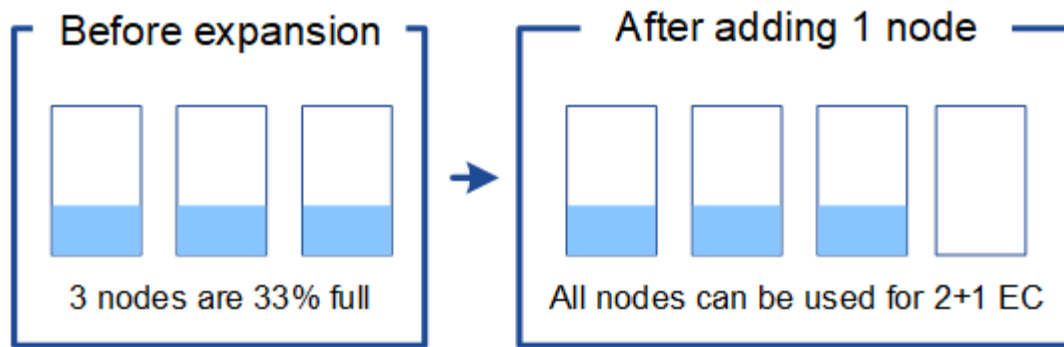
Wenn Sie 200 TB zusätzliche Kapazität hinzufügen, können Sie das 2+1 Erasure Coding fortsetzen und die Daten, die mit Erasure Coding versehen sind, auf allen Nodes einen Ausgleich finden.



- **Fügen Sie einen 100 TB Storage Node hinzu, wenn die vorhandenen Speicherknoten zu 33% voll sind**

In diesem Beispiel sind die vorhandenen Nodes zu 33 % ausgelastet. Da auf den vorhandenen Nodes 200 TB an freier Kapazität verfügbar sind (67 TB pro Node), müssen Sie nur noch einen Node hinzufügen, wenn Sie die Erweiterung jetzt durchführen.

Wenn Sie 100 TB zusätzliche Kapazität hinzufügen, können Sie das 2+1 Erasure Coding fortsetzen und die Daten, die mit Erasure Coding versehen sind, auf allen Nodes einen Ausgleich finden.



Beispiel 2: Erweitern Sie das Grid mit drei Standorten, das Erasure Coding für 6+3 verwendet

Dieses Beispiel zeigt, wie ein Erweiterungsplan für ein Grid mit mehreren Standorten entwickelt wird, das über ein Erasure Coding-Schema mit einer größeren Anzahl von Fragmenten verfügt. Trotz der Unterschiede zwischen diesen Beispielen ist der empfohlene Erweiterungsplan sehr ähnlich.

Gehen Sie folgendermaßen vor:

- Alle Daten werden mithilfe des Erasure Coding-Schemas von 6+3 gespeichert. Mit dem Erasure Coding-Schema 6+3 wird jedes Objekt als 9 Fragmente gespeichert und jedes Fragment wird auf einem anderen Storage Node gespeichert.
- Sie verfügen über drei Standorte und jeder Standort hat vier Storage-Nodes (insgesamt 12 Nodes). Jeder Node hat eine Gesamtkapazität von 100 TB.
- Sie möchten erweitern, indem Sie neue 100-TB-Storage-Nodes hinzufügen.
- Ziel ist es, mithilfe von Erasure Coding Daten auf die alten und neuen Nodes einen Ausgleich zu finden.

Je nachdem, wie voll die Speicherknoten sind, wenn Sie die Erweiterung durchführen, stehen verschiedene Optionen zur Verfügung.

- **Fügen Sie neun 100 TB Storage-Nodes (drei pro Standort) hinzu, wenn vorhandene Knoten zu 100 % voll sind**

In diesem Beispiel sind die 12 vorhandenen Nodes zu 100 % ausgelastet. Da keine freie Kapazität zur Verfügung steht, müssen Sie sofort neun Nodes (900 TB zusätzliche Kapazität) hinzufügen, um mit dem Erasure Coding für 6+3 fortzufahren.

Nach Abschluss der Erweiterung werden bei Erasure-Coding von Objekten alle Fragmente auf die neuen Nodes platziert.



Durch diese Erweiterung werden Nodes $k+m$ hinzugefügt. Das Hinzufügen von 12 Nodes (vier pro Standort) wird aus Redundanzgründen empfohlen. Wenn Sie Storage-Nodes mit $k+m$ -Erweiterung hinzufügen, wenn vorhandene Nodes zu 100 % voll sind, werden alle neuen Objekte auf den Erweiterungs-Nodes gespeichert. Wenn einer der neuen Nodes nicht verfügbar ist, kann StorageGRID die ILM-Anforderungen selbst vorübergehend nicht erfüllen.

- **Hinzufügen von sechs 100 TB Storage-Nodes (zwei pro Standort), wenn vorhandene Knoten zu 75 % voll sind**

In diesem Beispiel sind die 12 vorhandenen Nodes zu 75 % ausgelastet. Da 300 TB freie Kapazität (25 TB pro Node) zur Verfügung stehen, müssen Sie nur sechs Nodes hinzufügen, wenn Sie die Erweiterung jetzt

durchführen. Sie würden jedem der drei Standorte zwei Nodes hinzufügen.

Wenn Sie 600 TB Storage-Kapazität hinzufügen, können Sie das Erasure Coding von 6 und 3 fortsetzen und einen Ausgleich für Daten mit Erasure Coding auf allen Nodes erzielen.

- **Fügen Sie drei 100 TB Storage-Nodes (einer pro Standort) hinzu, wenn vorhandene Knoten zu 50 % voll sind**

In diesem Beispiel sind die 12 vorhandenen Nodes zu 50 % ausgelastet. Da 600 TB freie Kapazität (50 TB pro Node) zur Verfügung stehen, müssen Sie nur drei Nodes hinzufügen, wenn Sie die Erweiterung jetzt durchführen. Sie würden jedem der drei Standorte einen Node hinzufügen.

Wenn Sie 300 TB Storage-Kapazität hinzufügen, können Sie das Erasure Coding von 6 und 3 fortsetzen und einen Ausgleich für Daten mit Erasure Coding auf allen Nodes erzielen.

Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind

Wenn Sie eine Erweiterung zum Hinzufügen von Storage-Nodes durchführen und Ihre ILM-Richtlinie eine oder mehrere ILM-Regeln zum Löschen von Code-Daten enthält, müssen Sie nach Abschluss der Erweiterung möglicherweise das EC-Ausgleichsverfahren durchführen.

Wenn Sie beispielsweise nicht die empfohlene Anzahl von Speicherknoten für das von Ihnen verwendete Erasure Coding-Schema hinzufügen können, müssen Sie möglicherweise das EC-Ausgleichsverfahren ausführen, damit zusätzliche Objekte mit Erasure-Coding-Verfahren gespeichert werden können.

Führen Sie die Erweiterung durch, und fahren Sie mit fort [Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes](#) Zum Ausführen des Verfahrens.

Was ist die Neuausrichtung der EG?

Bei der EC-Ausbalancierung handelt es sich um ein StorageGRID-Verfahren, das nach einer Erweiterung des Storage-Nodes erforderlich sein kann. Das Verfahren wird als Kommandozeilenskript vom primären Admin-Knoten ausgeführt. Bei Ausführung des EC-Ausgleichs verteilt StorageGRID Fragmente, die mit Erasure Coding codiert wurden, auf die vorhandenen und neu erweiterten Storage-Nodes an einem Standort.

Das EC-Ausgleichsverfahren:

- Verschiebt nur Objektdaten, die Erasure Coding verwenden. Es werden keine replizierten Objektdaten verschoben.
- Verteilt die Daten an einem Standort neu. Es werden keine Daten zwischen Standorten verschoben.
- Verteilt Daten auf alle Storage-Nodes an einem Standort neu. Daten werden nicht innerhalb von Storage Volumes neu verteilt.
- Berücksichtigt bei der Verschiebung von Daten, die auf Erasure Coding codiert wurden, nicht die Nutzung replizierter Daten auf jedem Storage Node

Wenn das EC-Ausgleichsverfahren abgeschlossen ist:

- Die Daten, die mithilfe von Erasure-Coding-Verfahren codiert wurden, werden von Storage-Nodes mit weniger verfügbarem Speicherplatz zu Storage-Nodes mit mehr verfügbarem Speicherplatz verschoben.
- Verwendete (%) Werte können sich zwischen Storage Nodes unterscheiden, da der EC-Ausgleichsvorgang keine replizierten Objektkopien verschiebt.

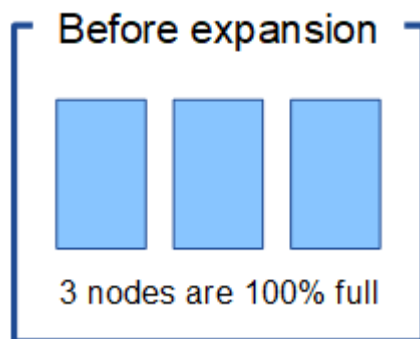
- Die Datensicherung von Objekten, die mit Erasure Coding versehen sind, wird unverändert beibehalten.

Wenn das EC-Ausgleichsverfahren ausgeführt wird, ist die Performance von ILM-Vorgängen sowie S3- und Swift-Client-Operationen wahrscheinlich beeinträchtigt. Aus diesem Grund sollten Sie dieses Verfahren nur in begrenzten Fällen durchführen.

Wann sollte der EC-Ausgleich nicht durchgeführt werden

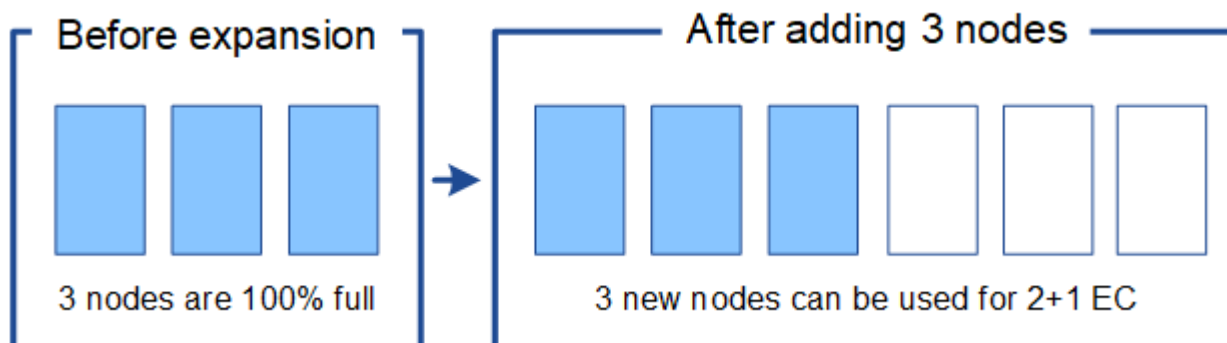
Als Beispiel für den Fall, dass Sie keinen EC-Ausgleich durchführen müssen, sollten Sie Folgendes berücksichtigen:

- StorageGRID wird an einem Standort ausgeführt, der drei Storage-Nodes enthält.
- Die ILM-Richtlinie verwendet eine 2+1-Regel zur Einhaltung von Datenkonsistenz für alle Objekte, die größer als 1.0 MB sind, und eine Replizierungsregel mit 2 Kopien für kleinere Objekte.
- Alle Speicherknoten sind voll geworden, und die Warnung **Low Object Storage** wurde auf dem Hauptschweregrade ausgelöst. Die empfohlene Aktion ist, eine Erweiterungsmaßnahme zum Hinzufügen von Speicherknoten durchzuführen.



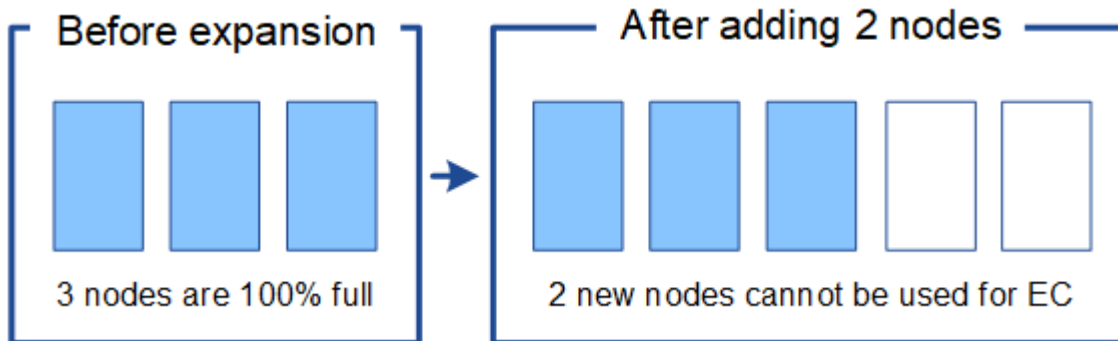
Um den Standort in diesem Beispiel zu erweitern, wird empfohlen, drei oder mehr neue Speicherknoten hinzuzufügen. StorageGRID benötigt drei Storage-Nodes für das Erasure Coding von 2+1, damit die zwei Datenfragmente und das ein Paritätsfragment auf verschiedenen Nodes platziert werden können.

Nachdem Sie die drei Storage-Nodes hinzugefügt haben, bleiben die ursprünglichen Storage-Nodes voll, die Objekte können jedoch weiterhin in das Erasure Coding-Schema 2+1 auf den neuen Nodes aufgenommen werden. Das Ausführen des EC-Ausgleichs-Verfahrens wird in diesem Fall nicht empfohlen: Durch das Ausführen des Verfahrens wird die Performance vorübergehend verringert, was sich auf den Client-Betrieb auswirken könnte.

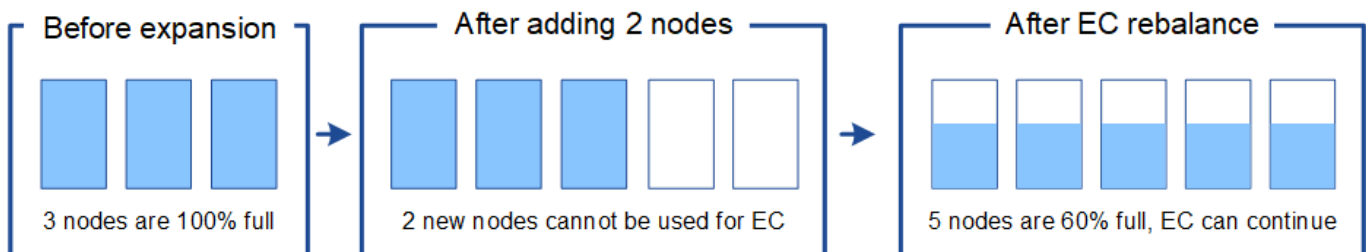


Wann ist die EC-Neuverteilung durchzuführen

Als Beispiel für den Fall, dass Sie den EC-Ausgleichvorgang durchführen sollten, betrachten Sie das gleiche Beispiel, gehen Sie aber davon aus, dass Sie nur zwei Storage-Nodes hinzufügen können. Da für das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) 2+1 mindestens drei Storage-Nodes erforderlich sind, können die neuen Nodes nicht für Daten mit Erasure Coding verwendet werden.



Um dieses Problem zu lösen und die neuen Speicherknoten zu nutzen, können Sie das EC-Ausgleichsverfahren ausführen. Im Rahmen dieses Verfahrens StorageGRID werden Daten und Paritätsfragmente, die mit Datenkonsistenz (Erasure Coding) versehen werden, auf alle Storage-Nodes am Standort neu verteilt. Wenn in diesem Beispiel der EC-Ausgleichvorgang abgeschlossen ist, sind alle fünf Nodes nun nur zu 60 % voll und die Objekte können auf allen Storage-Nodes weiterhin in das Erasure Coding-Schema 2+1 aufgenommen werden.



Anforderungen für die Neuausrichtung der EG

Im Allgemeinen sollten Sie nur in begrenzten Fällen das EC-Ausgleichsverfahren durchführen. Insbesondere sollten Sie eine Neuausrichtung der EG nur durchführen, wenn alle folgenden Aussagen wahr sind:

- Sie verwenden das Erasure Coding für Ihre Objektdaten.
- Die Warnung **Low Object Storage** wurde für einen oder mehrere Storage Nodes an einem Standort ausgelöst, was darauf hinweist, dass die Knoten zu mindestens 80 % voll sind.
- Sie können die empfohlene Anzahl neuer Speicherknoten für das verwendete Erasure-Coding-Schema nicht hinzufügen. Siehe [Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden](#).
- Während das EC-Ausgleichsverfahren läuft, tolerieren Ihre S3- und Swift-Clients eine niedrigere Performance bei Schreib- und Leseoperationen.

Wie EC-Ausgleichs-Verfahren mit anderen Wartungsaufgaben interagiert

Sie können bestimmte Wartungsverfahren nicht gleichzeitig durchführen, während Sie das EC-Ausgleichsverfahren ausführen.

Verfahren	Während des EC-Ausgleichs erlaubt?
Weitere EC-Ausgleichsverfahren	Nein Sie können nur ein EC-Ausgleichsverfahren gleichzeitig ausführen.
Verfahren zur Deaktivierung EC-Datenreparaturauftrag	Nein • Während des EC-Ausgleichs werden Sie daran gehindert, eine Stilllegung oder eine EC-Datenreparatur zu starten. • Sie können den EC-Ausgleichsvorgang nicht starten, während ein Ausmustern von Storage Nodes oder eine EC-Datenreparatur ausgeführt wird.
Expansionsverfahren	Nein Wenn Sie neue Storage-Nodes zu einer Erweiterung hinzufügen müssen, sollten Sie warten, bis Sie alle neuen Nodes hinzugefügt haben. Wenn während des Hinzufügens eines neuen Storage-Nodes ein Verfahren zur Ausgleich der EC ausgeführt wird, werden die Daten nicht zu diesen Nodes verschoben.
Upgrade-Verfahren	Nein Wenn Sie ein Upgrade der StorageGRID-Software durchführen müssen, sollten Sie das Upgrade-Verfahren vor oder nach dem Ausführen des EC-Ausgleichs durchführen. Bei Bedarf können Sie den EC-Ausgleichsvorgang beenden, um ein Software-Upgrade durchzuführen.
Klonvorgang für Appliance-Node	Nein Wenn Sie einen Appliance-Storage-Node klonen müssen, sollten Sie warten, bis der EC-Ausgleichsvorgang ausgeführt wurde, nachdem Sie den neuen Node hinzugefügt haben. Wenn während des Hinzufügens eines neuen Storage-Nodes ein Verfahren zur Ausgleich der EC ausgeführt wird, werden die Daten nicht zu diesen Nodes verschoben.
Hotfix-Verfahren	Ja. Sie können einen StorageGRID-Hotfix anwenden, während der EC-Ausgleichsvorgang ausgeführt wird.
Andere Wartungsarbeiten	Nein Sie müssen das EC-Ausgleichsverfahren beenden, bevor Sie andere Wartungsverfahren durchführen.

Wechselwirkungen zwischen EC-Ausgleichsoperationen und ILM

Während des EC-Ausgleichs ausgeführt wird, vermeiden Sie ILM-Änderungen, die den Standort vorhandener Objekte, die mit Erasure-Coding-Verfahren codiert wurden, ändern könnten. Beginnen Sie beispielsweise nicht

mit der Verwendung einer ILM-Regel, die ein anderes Erasure Coding-Profil hat. Wenn Sie solche ILM-Änderungen vornehmen müssen, sollten Sie den EC-Ausgleichvorgang abbrechen.

Hinzufügen von Metadatenkapazität

Um sicherzustellen, dass ausreichend Speicherplatz für Objektmetadaten verfügbar ist, müssen Sie möglicherweise ein Erweiterungsverfahren durchführen, um neue Storage-Nodes an jedem Standort hinzuzufügen.

StorageGRID reserviert Speicherplatz für Objekt-Metadaten auf Volume 0 jedes Storage-Nodes. An jedem Standort werden drei Kopien aller Objektmetadaten aufbewahrt und gleichmäßig auf alle Storage-Nodes verteilt.

Mit Grid Manager lässt sich die Metadatenkapazität von Storage Nodes überwachen und schätzen, wie schnell Metadaten verbraucht werden. Darüber hinaus wird die Warnung **Low Metadaten Storage** für einen Speicherknoten ausgelöst, wenn der verwendete Metadaten Speicherplatz bestimmte Schwellenwerte erreicht.

Beachten Sie, dass die Objekt-Metadatenkapazität eines Grid je nach Verwendung des Grid möglicherweise schneller belegt als die Objekt-Storage-Kapazität. Wenn Sie beispielsweise normalerweise eine große Anzahl kleiner Objekte aufnehmen oder Objekte mit großen Mengen von Benutzer-Metadaten oder -Tags versehen, müssen Sie möglicherweise Storage-Nodes hinzufügen, um die Metadaten-Kapazität zu erhöhen, obwohl weiterhin ausreichend Objekt-Storage-Kapazität vorhanden ist.

Weitere Informationen finden Sie im Folgenden:

- [Management von Objekt-Metadaten-Storage](#)
- [Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node](#)

Richtlinien zur Erhöhung der Metadaten-Kapazität

Bevor Sie Storage-Nodes hinzufügen, um die Metadatenkapazität zu steigern, lesen Sie die folgenden Richtlinien und Einschränkungen:

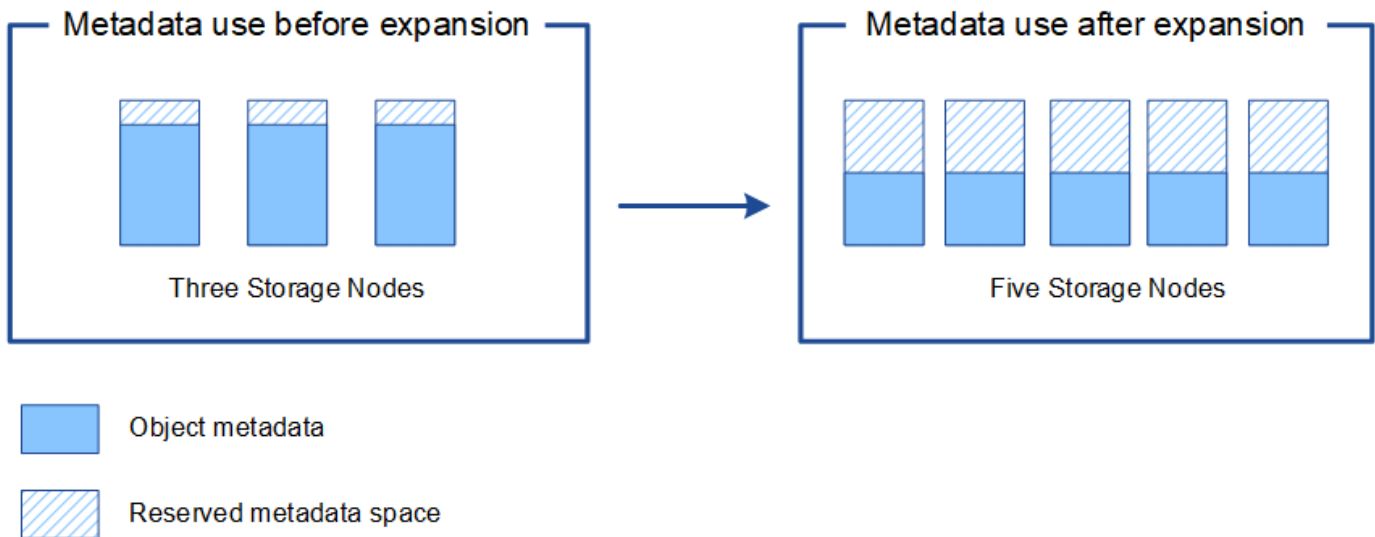
- Wenn eine ausreichende Objekt-Storage-Kapazität verfügbar ist, erhöht sich aufgrund der Verfügbarkeit von mehr Speicherplatz für Objekt-Metadaten die Anzahl der Objekte, die Sie in Ihrem StorageGRID System speichern können.
- Die Metadatenkapazität eines Grids lässt sich erhöhen, indem jedem Standort ein oder mehrere Storage-Nodes hinzugefügt werden.
- Der tatsächlich für Objektmetadaten auf einem bestimmten Storage-Node reservierte Speicherplatz hängt von der Option Metadaten reservierter Speicherplatz (systemweite Einstellung), der RAM-Größe des Node und der Größe des Volumes 0 des Node ab. Siehe Anweisungen für [Administration von StorageGRID](#).
- Vorhandene Storage-Nodes können nicht erhöht werden, da Metadaten nur auf Volume 0 gespeichert werden.
- Sie können die Metadatenkapazität nicht erhöhen, indem Sie einen neuen Standort hinzufügen.
- StorageGRID speichert drei Kopien aller Objektmetadaten an jedem Standort. Daher wird die Metadaten-Kapazität Ihres Systems durch die Metadaten-Kapazität Ihres kleinsten Standorts begrenzt.
- Wenn Sie Metadaten hinzufügen, sollten Sie jedem Standort die gleiche Anzahl an Storage-Nodes hinzufügen.

Verteilung von Metadaten beim Hinzufügen von Storage-Nodes

Wenn Sie Storage-Nodes zu einer Erweiterung hinzufügen, verteilt StorageGRID die vorhandenen Objekt-Metadaten an die neuen Nodes an jedem Standort, wodurch die allgemeine Metadaten des Grid erhöht werden. Es ist keine Benutzeraktion erforderlich.

Die folgende Abbildung zeigt, wie StorageGRID Objektmetadaten neu verteilt, wenn Sie Storage-Nodes in einer Erweiterung hinzufügen. Die linke Seite der Abbildung zeigt das Volumen 0 von drei Storage-Nodes vor einer Erweiterung. Metadaten verbrauchen einen relativ großen Teil des verfügbaren Metadaten-Speicherplatzes jedes Nodes und die Warnung **Low Metadaten Storage** wurde ausgelöst.

Die rechte Seite der Abbildung zeigt, wie die vorhandenen Metadaten nach dem Hinzufügen von zwei Storage-Nodes zum Standort neu verteilt werden. Die Menge der Metadaten auf jedem Node ist gesunken, die Warnung * Storage mit niedrigen Metadaten* wird nicht mehr ausgelöst, und der für Metadaten verfügbare Platz hat sich erhöht.



Grid-Nodes werden hinzugefügt, um Funktionen zu Ihrem System hinzuzufügen

Einem StorageGRID-System können Sie Redundanz oder zusätzliche Funktionen hinzufügen, indem Sie vorhandenen Standorten neue Grid-Nodes hinzufügen.

Sie können beispielsweise zusätzliche Gateway-Nodes hinzufügen, um die Erstellung von Hochverfügbarkeitsgruppen von Gateway-Nodes zu unterstützen, oder Sie können einen Admin-Node an einem Remote-Standort hinzufügen, um die Überwachung über einen lokalen Knoten zu ermöglichen.

In einem einzigen Erweiterungsvorgang können Sie mindestens einen der folgenden Node-Typen zu einem oder mehreren bestehenden Standorten hinzufügen:

- Nicht primäre Admin-Nodes
- Storage-Nodes
- Gateway-Nodes
- Archiv-Nodes

Beachten Sie bei der Vorbereitung des Hinzufügens von Grid-Knoten die folgenden Einschränkungen:

- Der primäre Admin-Node wird während der Erstinstallation bereitgestellt. Sie können während einer

Erweiterung keinen primären Admin-Node hinzufügen.

- Sie können Storage-Nodes und andere Node-Typen in der gleichen Erweiterung hinzufügen.
- Beim Hinzufügen von Speicherknoten müssen Sie die Anzahl und Position der neuen Knoten sorgfältig planen. Siehe [Richtlinien zum Hinzufügen von Objektkapazität](#).
- Wenn Sie Archiv-Nodes hinzufügen, beachten Sie, dass jeder Archiv-Node nur Tape über die TSM Middleware (Tivoli Storage Manager) unterstützt.
- Wenn die Option **New Node Client Network Standard** auf der Seite nicht vertrauenswürdige Clientnetzwerke auf **nicht vertrauenswürdig** gesetzt ist, müssen Client-Anwendungen, die sich mit Erweiterungsknoten über das Client-Netzwerk verbinden, über einen Load Balancer-Endpunkt-Port (**KONFIGURATION Netzwerk nicht vertrauenswürdige Client-Netzwerke**) eine Verbindung herstellen. Siehe Anweisungen für [Administration von StorageGRID](#). So ändern Sie die Einstellung für den neuen Knoten und konfigurieren die Load Balancer-Endpunkte.

Fügen Sie einen neuen Standort hinzu

Sie können Ihr StorageGRID System durch Hinzufügen eines neuen Standorts erweitern.

Richtlinien zum Hinzufügen eines Standorts

Überprüfen Sie vor dem Hinzufügen eines Standorts die folgenden Anforderungen und Einschränkungen:

- Sie können nur einen Standort pro Erweiterungsvorgang hinzufügen.
- Grid-Nodes können einem vorhandenen Standort nicht als Teil derselben Erweiterung hinzugefügt werden.
- Alle Standorte müssen mindestens drei Storage-Nodes enthalten.
- Das Hinzufügen eines neuen Standorts erhöht nicht automatisch die Anzahl der zu speichernden Objekte. Die Gesamtkapazität eines Grids hängt von der Menge des verfügbaren Storage, der ILM-Richtlinie und der Metadatenkapazität an jedem Standort ab.
- Bei der Dimensionierung eines neuen Standorts müssen Sie sicherstellen, dass dieser genügend Metadaten enthält.

Bei StorageGRID werden die Kopien aller Objektmetadaten an jedem Standort gespeichert. Wenn Sie einen neuen Standort hinzufügen, müssen Sie sicherstellen, dass dieser ausreichend Metadaten für die vorhandenen Objektmetadaten und genügend Metadaten für Wachstum enthält.

Weitere Informationen finden Sie im Folgenden:

- [Management von Objekt-Metadaten-Storage](#)
- [Überwachen der Objekt-Metadaten-Kapazität für jeden Storage Node](#)
- Dabei muss die verfügbare Netzwerkbandbreite zwischen Standorten und das Maß der Netzwerklatenz berücksichtigt werden. Metadatenaktualisierungen werden kontinuierlich zwischen Standorten repliziert, selbst wenn alle Objekte nur am Standort gespeichert werden, an dem sie aufgenommen werden.
- Da Ihr StorageGRID System während der Erweiterung betriebsbereit bleibt, müssen Sie ILM-Regeln prüfen, bevor Sie mit dem Erweiterungsverfahren beginnen. Sie müssen sicherstellen, dass Objektkopien nicht auf dem neuen Standort gespeichert werden, bis der Erweiterungsvorgang abgeschlossen ist.

Legen Sie z. B. vor Beginn der Erweiterung fest, ob Regeln den Standardspeicherpool (Alle Speicherknoten) verwenden. In diesem Fall müssen Sie einen neuen Speicherpool erstellen, der die vorhandenen Speicherknoten enthält, und Ihre ILM-Regeln aktualisieren, um den neuen Speicherpool zu verwenden. Andernfalls werden Objekte auf den neuen Standort kopiert, sobald der erste Node an diesem Standort aktiv ist.

Weitere Informationen zum Ändern des ILM beim Hinzufügen eines neuen Standorts finden Sie im Beispiel zum Ändern einer ILM-Richtlinie in den Anweisungen für [Objektmanagement mit ILM](#).

Sammeln Sie die erforderlichen Materialien

Bevor Sie eine Erweiterung durchführen, sammeln Sie die Materialien und installieren und konfigurieren Sie neue Hardware und Netzwerke.

Element	Hinweise
StorageGRID Installationsarchiv	Wenn Sie neue Grid-Nodes oder einen neuen Standort hinzufügen, müssen Sie das StorageGRID Installationsarchiv herunterladen und extrahieren. Sie müssen dieselbe Version verwenden, die derzeit im Raster ausgeführt wird. Weitere Informationen finden Sie in den Anweisungen für Herunterladen und Extrahieren der StorageGRID-Installationsdateien. Hinweis: Sie müssen keine Dateien herunterladen, wenn Sie vorhandenen Speicherknoten neue Speichervolumen hinzufügen oder eine neue StorageGRID Appliance installieren.
Service-Laptop	Der Service-Laptop verfügt über Folgendes: • Netzwerkport • SSH-Client (z. B. PuTTY) • Unterstützter Webbrowser
Passwords.txt Datei	Enthält die Passwörter, die für den Zugriff auf Grid-Nodes in der Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im Passwords.txt Datei:
StorageGRID-Dokumentation	• StorageGRID verwalten • Versionshinweise • Installationsanweisungen für Ihre Plattform ◦ Installieren Sie Red hat Enterprise Linux oder CentOS ◦ Installieren Sie Ubuntu oder Debian ◦ VMware installieren
Aktuelle Dokumentation für Ihre Plattform	Informationen zu unterstützten Versionen finden Sie im "Interoperabilitätsmatrix".

Laden Sie die StorageGRID Installationsdateien herunter und extrahieren Sie sie

Bevor Sie neue Grid-Nodes oder einen neuen Standort hinzufügen können, müssen Sie das entsprechende StorageGRID-Installationsarchiv herunterladen und die Dateien extrahieren.

Über diese Aufgabe

Sie müssen Erweiterungsvorgänge mit der Version von StorageGRID durchführen, die derzeit im Grid ausgeführt wird.

Schritte

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

["NetApp Downloads: StorageGRID"](#)

2. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
4. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Weiter akzeptieren**.
5. Wählen Sie in der Spalte **Install StorageGRID** der Download-Seite die aus .tgz Oder .zip Datei für Ihre Plattform.

Die in der Archivdatei der Installation angezeigte Version muss mit der Version der derzeit installierten Software übereinstimmen.

Verwenden Sie die .zip Datei, wenn Windows auf dem Service-Laptop ausgeführt wird.

Plattform	Installationsarchiv
Red hat Enterprise Linux oder CentOS	StorageGRID-Webscale-version-RPM-uniqueID.zip StorageGRID-Webscale-version-RPM-uniqueID.tgz
Ubuntu oder Debian oder Appliances	StorageGRID-Webscale-version-DEB-uniqueID.zip StorageGRID-Webscale-version-DEB-uniqueID.tgz
VMware	StorageGRID-Webscale-version-VMware-uniqueID.zip StorageGRID-Webscale-version-VMware-uniqueID.tgz
OpenStack/anderer Hypervisor	Um eine vorhandene Implementierung auf OpenStack zu erweitern, müssen Sie eine Virtual Machine mit einer der oben aufgeführten unterstützten Linux-Distributionen implementieren und die entsprechenden Anweisungen für Linux befolgen.

6. Laden Sie die Archivdatei herunter und extrahieren Sie sie.
7. Führen Sie den entsprechenden Schritt für Ihre Plattform aus, um die benötigten Dateien basierend auf Ihrer Plattform, der geplanten Grid-Topologie und der Erweiterung des StorageGRID Systems

auszuwählen.

Die im Schritt für jede Plattform aufgeführten Pfade beziehen sich auf das von der Archivdatei installierte Verzeichnis auf der obersten Ebene.

8. Wenn Sie ein Red hat Enterprise Linux oder CentOS System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	RPM Paket für die Installation der StorageGRID Node Images auf Ihren RHEL- oder CentOS-Hosts.
	RPM Paket für die Installation des StorageGRID Host Service auf Ihren RHEL- oder CentOS-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel für die Ansible-Rolle und das Playbook zur Konfiguration von RHEL- oder CentOS-Hosts für die Implementierung von StorageGRID Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.

Pfad und Dateiname	Beschreibung
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie mit diesen Schemas bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung zum Testen der Upgrade-Kompatibilität besitzen.

1. Wenn Sie ein Ubuntu oder Debian-System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine NetApp Lizenzdatei, die nicht in der Produktionsumgebung enthalten ist und für Tests und Proof of Concept-Implementierungen genutzt werden kann
	DEB-Paket zum Installieren der StorageGRID-Knoten-Images auf Ubuntu oder Debian-Hosts.
	MD5-Prüfsumme für die Datei /debs/storagegrid-webscale-images-version-SHA.deb.
	DEB-Paket zur Installation des StorageGRID-Hostdienstes auf Ubuntu oder Debian-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:

Pfad und Dateiname	Beschreibung
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel-Rolle und Playbook für Ansible zur Konfiguration von Ubuntu oder Debian-Hosts für die Implementierung von StorageGRID-Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie mit diesen Schemas bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung zum Testen der Upgrade-Kompatibilität besitzen.

1. Wenn Sie ein VMware-System erweitern, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	Die Festplattendatei für Virtual Machines, die als Vorlage für die Erstellung von Grid-Node-Virtual Machines verwendet wird.
	Die Vorlagendatei „Open Virtualization Format“ (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung des primären Admin-Knotens.
	Die Vorlagendatei (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung von nicht-primären Admin-Knoten.
	Die Vorlagendatei (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung von Archiv-Knoten.
	Die Vorlagendatei (<code>.ovf</code>) Und Manifest-Datei (<code>.mf</code>) Für die Bereitstellung von Gateway-Knoten.

Pfad und Dateiname	Beschreibung
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Zur Bereitstellung von virtuellen Maschinen-basierten Speicherknoten.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Bash Shell-Skript, das zur Automatisierung der Implementierung virtueller Grid-Nodes verwendet wird.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>deploy-vsphere-ovftool.sh</code> Skript:
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid- Management-API anmelden können.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie mit diesen Schemas bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung zum Testen der Upgrade- Kompatibilität besitzen.

1. Wenn Sie ein Appliance-basiertes StorageGRID System erweitern, wählen Sie die entsprechenden
Dateien aus.

Pfad und Dateiname	Beschreibung
	DEB-Paket zum Installieren der StorageGRID Node Images auf den Geräten.

Pfad und Dateiname	Beschreibung
	Prüfsumme des DEB-Installationspakets, das vom Installationsprogramm der StorageGRID-Appliance verwendet wird, um zu überprüfen, ob das Paket nach dem Hochladen intakt ist.



Für die Installation der Appliance sind diese Dateien nur erforderlich, wenn Sie den Netzwerkverkehr vermeiden müssen. Die Appliance kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Überprüfung der Hardware und des Netzwerks

Stellen Sie vor Beginn der Erweiterung Ihres StorageGRID-Systems Folgendes sicher:

- Die zur Unterstützung der neuen Grid-Nodes erforderliche Hardware oder der neue Standort wurde installiert und konfiguriert.
- Alle neuen Nodes verfügen über bidirektionale Kommunikationspfade zu allen vorhandenen und neuen Nodes (Voraussetzung für das Grid Network).
- Der primäre Admin-Knoten kann mit allen Erweiterungsservern kommunizieren, die das StorageGRID-System hosten sollen.
- Wenn einer der neuen Knoten eine Grid-Netzwerk-IP-Adresse in einem Subnetz hat, das zuvor nicht verwendet wurde, haben Sie bereits [Das neue Subnetz wurde hinzugefügt](#) In die Liste Raster Netzwerk. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und den Vorgang erneut starten.
- Sie verwenden keine NAT (Network Address Translation) im Grid-Netzwerk zwischen Grid-Nodes oder zwischen StorageGRID-Standorten. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt routungsfähig sein. Die Verwendung von NAT zur Brücke des Grid-Netzwerks über ein öffentliches Netzwerksegment wird nur unterstützt, wenn Sie eine Tunneling-Anwendung verwenden, die für alle Knoten im Netz transparent ist, was bedeutet, dass die Grid-Knoten keine Kenntnisse über öffentliche IP-Adressen benötigen.

Diese NAT-Einschränkung gilt für Grid-Knoten und Grid-Netzwerk. Sie können NAT je nach Bedarf zwischen externen Clients und Grid-Nodes verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway-Node bereitzustellen.

Hinzufügen von Storage-Volumes

Fügen Sie Storage-Volumes zu Storage-Nodes hinzu

Sie können die Storage-Kapazität von Storage-Nodes mit maximal 16 Storage-Volumes erweitern, indem Sie zusätzliche Storage-Volumes hinzufügen. Möglicherweise müssen Sie Storage Volumes zu mehr als einem Storage Node hinzufügen, um ILM-Anforderungen für replizierte oder mit Erasure Coding versehenen Kopien zu erfüllen.

Was Sie benötigen

Prüfen Sie vor dem Hinzufügen von Speicher-Volumes den [Richtlinien zum Hinzufügen von Objektkapazität](#) Um sicherzustellen, dass Sie wissen, wo Volumes hinzugefügt werden müssen, um die Anforderungen Ihrer ILM-Richtlinie zu erfüllen.



Diese Anweisungen gelten nur für softwarebasierte Speicherknoten. Siehe [Erweiterungs-Shelf für das implementierte SG6060 oder SG6060X hinzufügen](#) Erfahren Sie, wie Sie Storage Volumes zum SG6060 oder SG6060X durch Installation von Erweiterungs-Shelfs hinzufügen. Andere Appliance-Speicherknoten können nicht erweitert werden.

Über diese Aufgabe

Der zugrunde liegende Storage eines Storage-Node ist in eine Reihe von Storage-Volumes unterteilt. Storage Volumes sind blockbasierte Storage-Geräte, die vom StorageGRID System formatiert und zum Speichern von Objekten gemountet werden. Jeder Storage Node kann bis zu 16 Storage Volumes unterstützen, die im Grid Manager als *Object Stores* bezeichnet werden.



Objekt-Metadaten werden immer im Objektspeicher 0 gespeichert.

Jeder Objektspeicher wird auf einem Volume gemountet, das seiner ID entspricht. Der Objektspeicher mit einer ID von 0000 entspricht zum Beispiel dem `/var/local/rangedb/0` Bereitstellungspunkt.

Bevor Sie neue Speicher-Volumes hinzufügen, zeigen Sie mit Grid Manager die aktuellen Objektspeicher für jeden Storage-Node sowie die entsprechenden Mount-Punkte an. Diese Informationen können Sie beim Hinzufügen von Speicher-Volumes verwenden.

Schritte

1. Wählen Sie **NODES site Storage Node Storage** aus.
2. Blättern Sie nach unten, um die verfügbaren Speichermengen für jedes Volume und jeden Objektspeicher anzuzeigen.

Bei Appliance Storage Nodes entspricht der weltweite Name jedes Laufwerks der weltweiten Kennung (WWID) des Volumes, die angezeigt wird, wenn Sie die standardmäßigen Volume-Eigenschaften in der SANtricity Software anzeigen (die mit dem Storage Controller des Geräts verbundene Managementsoftware).

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. *sd*, *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 ? ⇅
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

3. Befolgen Sie die Anweisungen, mit denen Ihre Plattform dem Storage-Node neue Storage Volumes hinzufügen kann.
 - [VMware: Hinzufügen von Storage Volumes zum Storage-Node](#)
 - [Linux: Hinzufügen von Direct-Attached oder SAN-Volumes zu Storage Node](#)

VMware: Hinzufügen von Storage Volumes zum Storage-Node

Wenn ein Storage-Node weniger als 16 Storage-Volumes enthält, können Sie seine Kapazität mithilfe von VMware vSphere erhöhen, um Volumes hinzuzufügen.

Was Sie benötigen

- Sie haben Zugriff auf die Anweisungen zur Installation von StorageGRID für VMware Implementierungen.
 - [VMware installieren](#)
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, Speicher-Volumes zu einem Speicherknoten hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein anderer Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Der Storage-Node ist für kurze Zeit nicht verfügbar, wenn Sie Storage Volumes hinzufügen. Sie sollten dieses Verfahren jeweils auf einem Storage-Knoten durchführen, um die Grid-Services für Clients zu beeinträchtigen.

Schritte

1. Installieren Sie bei Bedarf neue Storage Hardware und erstellen Sie neue VMware Datenspeicher.
2. Fügen Sie eine oder mehrere Festplatten zur virtuellen Maschine als Speicher hinzu (Objektspeicher).
 - a. Öffnen Sie den VMware vSphere Client.
 - b. Bearbeiten Sie die Einstellungen der virtuellen Maschine, um eine oder mehrere zusätzliche Festplatten hinzuzufügen.

Die Festplatten werden in der Regel als Virtual Machine Disks (VMDKs) konfiguriert. VMDKs sind häufiger verwendet und einfacher zu managen. RDMs können zudem eine bessere Performance für Workloads mit größeren Objektgrößen bieten (z. B. mehr als 100 MB). Weitere Informationen über das Hinzufügen von Festplatten zu virtuellen Maschinen finden Sie in der Dokumentation zu VMware vSphere.

3. Starten Sie die virtuelle Maschine neu, indem Sie im VMware vSphere Client die Option **Gastbetriebssystem neu starten** verwenden oder den folgenden Befehl in einer ssh-Sitzung zur virtuellen Maschine eingeben: `sudo reboot`



Verwenden Sie zum Neustart der virtuellen Maschine nicht **Power Off** oder **Reset**.

4. Konfigurieren Sie den neuen Speicher für die Verwendung durch den 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. Konfiguration der neuen Storage Volumes:

```
sudo add_rangedbs.rb
```

Dieses Skript sucht neue Speicher-Volumes und fordert Sie zur Formatierung auf.

a. Geben Sie **y** ein, um die Formatierung zu akzeptieren.

b. Wenn eines der Volumes zuvor formatiert wurde, entscheiden Sie, ob Sie sie neu formatieren möchten.

- Geben Sie *** y*** ein, um die Formatierung neu zu formatieren.

- Geben Sie **n** ein, um die Neuformatierung zu überspringen.

c. Geben Sie auf Nachfrage **y** ein, um Storage-Services zu beenden.

Die Storage-Services werden angehalten, und das `setup_rangedbs.sh` Skript wird automatisch ausgeführt. Nachdem die Volumes als Rangedbs bereit sind, starten die Dienste erneut.

5. Überprüfen Sie, ob die Dienste richtig starten:

a. Anzeigen einer Liste des Status aller Dienste auf dem Server:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

a. Warten Sie, bis alle Dienste ausgeführt oder verifiziert sind.

b. Statusbildschirm verlassen:

```
Ctrl+C
```

6. Vergewissern Sie sich, dass der Speicherknoten online ist:

a. Melden Sie sich mit einem bei Grid Manager an [Unterstützter Webbrowser](#).

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

c. Wählen Sie **site Storage Node LDR Storage** aus.

d. Wählen Sie die Registerkarte **Konfiguration** und dann die Registerkarte **Main**.

e. Wenn die Dropdown-Liste **Speicherstatus - gewünscht** auf schreibgeschützt oder offline gesetzt ist, wählen Sie **Online** aus.

f. Wählen Sie **Änderungen Anwenden**.

7. So sehen Sie die neuen Objektspeicher:

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

b. Sehen Sie sich die Details in der Tabelle **Object Stores** an.

Ergebnis

Sie können die erweiterte Kapazität der Speicherknoten zum Speichern von Objektdaten verwenden.

Linux: Hinzufügen von Direct-Attached oder SAN-Volumes zu Storage Node

Wenn ein Speicherknoten weniger als 16 Speicher-Volumes umfasst, können Sie seine Kapazität erhöhen, indem Sie neue Block-Speichergeräte hinzufügen, sie für die Linux-Hosts sichtbar machen und die neuen Blockgeräte-Zuordnungen zur StorageGRID-Konfigurationsdatei hinzufügen, die für den Speicherknoten verwendet wurde.

Was Sie benötigen

- Sie haben Zugriff auf die Anweisungen für die Installation von StorageGRID für Ihre Linux-Plattform.
 - [Installieren Sie Red hat Enterprise Linux oder CentOS](#)
 - [Installieren Sie Ubuntu oder Debian](#)
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, Speicher-Volumes zu einem Speicherknoten hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein anderer Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Der Storage-Node ist für kurze Zeit nicht verfügbar, wenn Sie Storage Volumes hinzufügen. Sie sollten dieses Verfahren jeweils auf einem Storage-Knoten durchführen, um die Grid-Services für Clients zu beeinträchtigen.

Schritte

1. Installieren Sie die neue Speicherhardware.

Weitere Informationen finden Sie in der Dokumentation Ihres Hardware-Anbieters.

2. Erstellung neuer Block-Storage-Volumes der gewünschten Größe
 - Schließen Sie die neuen Festplattenlaufwerke an, und aktualisieren Sie die RAID-Controller-Konfiguration nach Bedarf, oder weisen Sie die neuen SAN-LUNs auf den gemeinsam genutzten Speicher-Arrays zu, damit der Linux-Host auf sie zugreifen kann.
 - Verwenden Sie dasselbe persistente Benennungsschema, das Sie für die Storage Volumes auf dem vorhandenen Storage Node verwendet haben.
 - Wenn Sie die Funktion StorageGRID-Node-Migration verwenden, machen Sie die neuen Volumes für andere Linux-Hosts sichtbar, die Migrationsziele für diesen Storage-Node sind. Weitere Informationen finden Sie in den Anweisungen zum Installieren von StorageGRID für Ihre Linux-Plattform.
3. Melden Sie sich beim Linux-Host an, der den Storage-Node als Root unterstützt, oder mit einem Konto, das über sudo-Berechtigung verfügt.
4. Vergewissern Sie sich, dass die neuen Speicher-Volumes auf dem Linux-Host sichtbar sind.

Möglicherweise müssen Sie nach Geräten erneut suchen.

5. Führen Sie den folgenden Befehl aus, um den Speicherknoten vorübergehend zu deaktivieren:

```
sudo storagegrid node stop <node-name>
```

6. Bearbeiten Sie mit einem Texteditor wie vim oder pico die Konfigurationsdatei des Knotens für den Speicherknoten, der unter gefunden werden kann `/etc/storagegrid/nodes/<node-name>.conf`.

7. Suchen Sie den Abschnitt der Node-Konfigurationsdatei, die die vorhandenen Objekt-Storage-Block-Gerätezuordnungen enthält.

Im Beispiel `BLOCK_DEVICE_RANGEDB_00` Bis `BLOCK_DEVICE_RANGEDB_03` Sind die vorhandenen Geräte-Zuordnungen für Objekt-Storage-Blöcke vorhanden.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Fügen Sie neue Objekt-Storage-Block-Gerätezuordnungen hinzu, die den Block-Speicher-Volumes entsprechen, die Sie für diesen Storage-Node hinzugefügt haben.

Stellen Sie sicher, dass Sie bei der nächsten beginnen `BLOCK_DEVICE_RANGEDB_nn`. Lassen Sie keine Lücke.

- Beginnen Sie anhand des obigen Beispiels mit `BLOCK_DEVICE_RANGEDB_04`.
- Im folgenden Beispiel wurden dem Node vier neue Block-Storage-Volumes hinzugefügt:
`BLOCK_DEVICE_RANGEDB_04` Bis `BLOCK_DEVICE_RANGEDB_07`.

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

9. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Node-Konfigurationsdatei für den Storage Node zu validieren:

```
sudo storagegrid node validate <node-name>
```

Beheben Sie Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

Wenn Sie einen ähnlichen Fehler beobachten, bedeutet dies, dass die Knoten-Konfigurationsdatei versucht, das von verwendete Blockgerät zuzuordnen <node-name> Für <PURPOSE> Dem angegebenen <path-name> Im Linux-Dateisystem gibt es jedoch keine gültige Sonderdatei für Blockgeräte (oder Softlink zu einer Sonderdatei für Blockgeräte) an diesem Speicherort.



```

Checking configuration file for node <node-name>...
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device

```

Überprüfen Sie, ob Sie die korrekte Eingabe durchgeführt haben <path-name>.

10. Führen Sie den folgenden Befehl aus, um den Knoten mit den neuen Blockgerätszuordnungen neu zu starten:

```
sudo storagegrid node start <node-name>
```

11. Melden Sie sich mit dem im angegebenen Passwort beim Storage-Node als Administrator an Passwords.txt Datei:
12. Überprüfen Sie, ob die Dienste richtig starten:
- Anzeigen einer Liste des Status aller Dienste auf dem Server:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

- b. Warten Sie, bis alle Dienste ausgeführt oder verifiziert sind.
- c. Statusbildschirm verlassen:

```
Ctrl+C
```

13. Konfigurieren Sie den neuen Speicher für die Verwendung durch den Speicherknoten:

- a. Konfiguration der neuen Storage Volumes:

```
sudo add_rangedbs.rb
```

Dieses Skript sucht neue Speicher-Volumes und fordert Sie zur Formatierung auf.

- a. Geben Sie **y** ein, um die Speicher-Volumes zu formatieren.
- b. Wenn eines der Volumes zuvor formatiert wurde, entscheiden Sie, ob Sie sie neu formatieren möchten.
 - Geben Sie *** y*** ein, um die Formatierung neu zu formatieren.
 - Geben Sie **n** ein, um die Neuformatierung zu überspringen.
- c. Geben Sie auf Nachfrage **y** ein, um Storage-Services zu beenden.

Die Storage-Services werden angehalten, und das `setup_rangedbs.sh` Skript wird automatisch ausgeführt. Nachdem die Volumes als Rangedbs bereit sind, starten die Dienste erneut.

14. Überprüfen Sie, ob die Dienste richtig starten:

- a. Anzeigen einer Liste des Status aller Dienste auf dem Server:

```
sudo storagegrid-status
```

Der Status wird automatisch aktualisiert.

- a. Warten Sie, bis alle Dienste ausgeführt oder verifiziert sind.
- b. Statusbildschirm verlassen:

```
Ctrl+C
```

15. Vergewissern Sie sich, dass der Speicherknoten online ist:

- a. Melden Sie sich mit einem bei Grid Manager an [Unterstützter Webbrowser](#).
- b. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
- c. Wählen Sie **site Storage Node LDR Storage** aus.
- d. Wählen Sie die Registerkarte **Konfiguration** und dann die Registerkarte **Main**.
- e. Wenn die Dropdown-Liste **Speicherstatus - gewünscht** auf schreibgeschützt oder offline gesetzt ist, wählen Sie **Online** aus.
- f. Klicken Sie Auf **Änderungen Übernehmen**.

16. So sehen Sie die neuen Objektspeicher:

- a. Wählen Sie **NODES site Storage Node Storage** aus.
- b. Sehen Sie sich die Details in der Tabelle **Object Stores** an.

Ergebnis

Sie können jetzt die erweiterte Kapazität der Speicherknoten zum Speichern von Objektdaten verwenden.

Grid-Nodes oder Standort hinzufügen

Grid-Nodes zu vorhandenem Standort hinzufügen oder neuen Standort hinzufügen

Gehen Sie folgendermaßen vor, um vorhandenen Standorten Grid-Nodes hinzuzufügen oder einen neuen Standort hinzuzufügen, aber Sie können nicht beide Erweiterungstypen gleichzeitig ausführen.

Was Sie benötigen

- Sie haben die Berechtigung Root-Zugriff oder Wartung.
- Alle bestehenden Nodes im Grid sind über alle Standorte hinweg betriebsbereit.
- Alle vorherigen Erweiterungs-, Upgrade-, Stilllegungs- oder Recovery-Verfahren sind abgeschlossen.



Sie können eine Erweiterung nicht starten, während noch ein weiteres Verfahren zur Erweiterung, Aktualisierung, Wiederherstellung oder aktiven Deaktivierung ausgeführt wird. Sie können jedoch bei Bedarf eine Deaktivierung unterbrechen, um eine Erweiterung zu starten.

Schritte

1. [Subnetze für Grid Network aktualisieren](#).
2. [Neue Grid-Nodes implementieren](#).
3. [Erweiterung durchführen](#).

Subnetze für Grid Network aktualisieren

Wenn Sie Grid-Nodes oder einen neuen Standort in einer Erweiterung hinzufügen, müssen Sie möglicherweise Subnetze zum Grid-Netzwerk aktualisieren oder hinzufügen.

StorageGRID pflegt eine Liste der für die Kommunikation zwischen den Grid-Nodes im Grid-Netzwerk (eth0) verwendeten Subnetze. Zu diesen Einträgen gehören die Subnetze, die von jedem Standort im StorageGRID-System für das Grid-Netzwerk verwendet werden, sowie alle Subnetze, die für NTP, DNS, LDAP oder andere externe Server verwendet werden, auf die über das Grid-Netzwerk-Gateway zugegriffen wird.

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.
- Sie haben die Netzwerkadressen in CIDR-Notation der Subnetze, die Sie konfigurieren möchten.

Über diese Aufgabe

Wenn einer der neuen Knoten eine Grid-Netzwerk-IP-Adresse in einem Subnetz hat, das zuvor nicht

verwendet wurde, müssen Sie das neue Subnetz der Netznetzwerkliste hinzufügen, bevor Sie die Erweiterung starten. Andernfalls müssen Sie die Erweiterung abbrechen, das neue Subnetz hinzufügen und den Vorgang erneut starten.

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > Grid-Netzwerk**.

Grid Network

Configure the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network (eth0) for each site in your StorageGRID system as well as any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnets

Subnet 1



Passphrase

Provisioning
Passphrase

Save

2. Wählen Sie in der Liste Subnetze das Pluszeichen aus, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

Geben Sie beispielsweise 10.96.104.0/22 ein.

3. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **Speichern**.

Die angegebenen Subnetze werden automatisch für Ihr StorageGRID System konfiguriert.

Neue Grid-Nodes implementieren

Die Schritte zur Implementierung neuer Grid-Nodes in einer Erweiterung entsprechen den Schritten, die bei der ersten Installation des Grid verwendet wurden. Sie müssen alle neuen Grid-Nodes implementieren, bevor Sie die Erweiterung durchführen können.

Wenn Sie das Raster erweitern, müssen die hinzuzufügenden Nodes nicht mit den vorhandenen Node-Typen übereinstimmen. VMware Nodes, Linux Container-basierte Nodes oder Appliance-Nodes lassen sich hinzufügen.

VMware: Grid-Nodes implementieren

Sie müssen für jeden VMware Node, den Sie der Erweiterung hinzufügen möchten, eine Virtual Machine in VMware vSphere implementieren.

Schritte

1. [Implementieren Sie den neuen Node als Virtual Machine](#) Und verbinden Sie sie mit einem oder mehreren StorageGRID-Netzwerken.

Bei der Implementierung des Node können Sie optional Node-Ports neu zuordnen oder CPU- oder

Speichereinstellungen erhöhen.

2. Nachdem Sie alle neuen VMware-Nodes implementiert haben, [Das Erweiterungsverfahren durchführen](#).

Linux: Grid-Nodes implementieren

Die Grid-Nodes können auf neuen Linux-Hosts oder auf vorhandenen Linux-Hosts implementiert werden. Wenn Sie zusätzliche Linux-Hosts benötigen, um die CPU-, RAM- und Storage-Anforderungen der StorageGRID-Nodes, die Sie dem Grid hinzufügen möchten, zu unterstützen, bereiten Sie sie auf die gleiche Weise vor, wie Sie die Hosts bei der ersten Installation vorbereitet haben. Anschließend implementieren Sie die Erweiterungs-Nodes auf dieselbe Weise wie bei der Installation die Grid-Nodes.

Was Sie benötigen

- Sie haben Anweisungen zum Installieren von StorageGRID für Ihre Linux-Version und haben die Hardware- und Speicheranforderungen geprüft.
 - [Installieren Sie Red hat Enterprise Linux oder CentOS](#)
 - [Installieren Sie Ubuntu oder Debian](#)
- Wenn Sie neue Grid-Nodes auf vorhandenen Hosts implementieren möchten, haben Sie bestätigt, dass die vorhandenen Hosts über genügend CPU-, RAM- und Storage-Kapazität für die zusätzlichen Nodes verfügen.
- Sie verfügen über einen Plan, um Ausfall-Domains zu minimieren. Beispielsweise sollten nicht alle Gateway-Nodes auf einem einzelnen physischen Host bereitgestellt werden.



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Speicherknoten auf einem einzelnen physischen oder virtuellen Host aus. Die Verwendung eines dedizierten Hosts für jeden Speicherknoten stellt eine isolierte Ausfalldomäne zur Verfügung.

- Wenn der StorageGRID-Node Storage verwendet, der einem NetApp ONTAP System zugewiesen ist, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.

Schritte

1. Wenn Sie neue Hosts hinzufügen, greifen Sie auf die Installationsanweisungen zur Implementierung von StorageGRID Nodes zu.
2. Befolgen Sie zum Bereitstellen der neuen Hosts die Anweisungen zur Vorbereitung der Hosts.
3. Befolgen Sie zum Erstellen von Node-Konfigurationsdateien und zum Validieren der StorageGRID-Konfiguration die Anweisungen für die Bereitstellung von Grid-Nodes.
4. Wenn Sie einem neuen Linux-Host Nodes hinzufügen, starten Sie den StorageGRID-Hostdienst.
5. Wenn Sie einem vorhandenen Linux-Host Nodes hinzufügen, starten Sie die neuen Nodes mithilfe der StorageGRID Host Service-CLI: `sudo storagegrid node start [<node name>]`

Nachdem Sie fertig sind

Nach der Implementierung aller neuen Grid-Nodes können Sie dies gerne nutzen [Die Erweiterung durchführen](#).

Appliances: Implementierung von Storage-, Gateway- oder nicht-primären Admin-Nodes

Um die StorageGRID-Software auf einem Appliance-Knoten zu installieren, verwenden Sie das Installationsprogramm für StorageGRID-Appliances, das in der Appliance enthalten ist. Jede Storage-

Appliance arbeitet als einzelner Storage-Node in einer Erweiterung und jede Services-Appliance fungiert als einzelner Gateway-Node oder als nicht-primärer Admin-Node. Jede Appliance kann eine Verbindung zum Grid-Netzwerk, dem Admin-Netzwerk und dem Client-Netzwerk herstellen.

Was Sie benötigen

- Das Gerät wurde in einem Rack oder Schrank installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Sie haben mit dem Installationsprogramm für StorageGRID-Geräte alle Schritte „Hardware konfigurieren“ in den Installations- und Wartungsanweisungen für die Appliance abgeschlossen.
 - [SG100- und SG1000-Services-Appliances](#)
 - [Hardware konfigurieren \(SG5600\)](#)
 - [Hardware konfigurieren \(SG5700\)](#)
 - [Hardware konfigurieren \(SG6000\)](#)

Das Konfigurieren der Appliance-Hardware umfasst die erforderlichen Schritte zum Konfigurieren von StorageGRID-Verbindungen (Netzwerkverbindungen und IP-Adressen) sowie die optionalen Schritte zum Aktivieren der Node-Verschlüsselung, zum Ändern des RAID-Modus und zum erneuten Zuordnen von Netzwerkports.

- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, wurden in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- Die StorageGRID Appliance Installer-Firmware auf der Ersatzanwendung ist mit der derzeit im Grid ausgeführten StorageGRID-Softwareversion kompatibel. So ist beispielsweise die Version 3.6 des Installationsprogramms für StorageGRID-Geräte mit der Version 11.6 von StorageGRID kompatibel. (Wenn die Versionen nicht kompatibel sind, müssen Sie die StorageGRID Appliance Installer-Firmware aktualisieren.)
- Sie haben einen Service-Laptop mit einem [Unterstützter Webbrowser](#).
- Sie kennen eine der IP-Adressen, die dem Computing-Controller der Appliance zugewiesen sind. Sie können die IP-Adresse für jedes angeschlossene StorageGRID-Netzwerk verwenden.

Über diese Aufgabe

Die Installation von StorageGRID auf einem Appliance-Node erfolgt in folgenden Phasen:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Namen des Appliance-Nodes an oder bestätigen sie.
- Sie starten die Installation und warten, bis Volumes konfiguriert und die Software installiert ist.

Die Installation wird durch Installationsaufgaben des Geräts gepartet. Um die Installation fortzusetzen, melden Sie sich beim Grid Manager an, genehmigen alle Grid-Nodes und schließen den StorageGRID-Installationsprozess ab.



Wenn Sie mehrere Appliance-Nodes gleichzeitig implementieren müssen, können Sie den Installationsprozess mithilfe des automatisierten `configure-sga.py` Installationsskripts für Appliances

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Computing-Controller der Appliance ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt *** Primary Admin Node* Connection** fest, ob Sie die IP-Adresse für den primären Admin Node angeben müssen.

Wenn Sie zuvor andere Knoten in diesem Rechenzentrum installiert haben, kann der StorageGRID-Appliance-Installer diese IP-Adresse automatisch erkennen, vorausgesetzt, dass der primäre Admin-Knoten oder mindestens ein anderer Grid-Node mit ADMIN_IP konfiguriert ist, im selben Subnetz vorhanden ist.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen Admin Node Discovery aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.
Automatische Erkennung aller verbundenen primären Admin-Nodes	a. Aktivieren Sie das Kontrollkästchen Admin Node Discovery aktivieren. b. Warten Sie, bis die Liste der erkannten IP-Adressen angezeigt wird. c. Wählen Sie den primären Admin-Node für das Grid aus, in dem dieser Appliance-Speicher-Node bereitgestellt werden soll. d. Klicken Sie Auf Speichern. e. Warten Sie, bis der Verbindungsstatus bereit ist, bis die neue IP-Adresse einsatzbereit ist.

4. Geben Sie im Feld **Knotenname** den Namen ein, den Sie für diesen Appliance-Knoten verwenden möchten, und wählen Sie **Speichern**.

Der Node-Name wird diesem Appliance-Node im StorageGRID-System zugewiesen. Sie wird im Grid Manager auf der Seite Nodes (Registerkarte Übersicht) angezeigt. Bei Bedarf können Sie den Namen ändern, wenn Sie den Knoten genehmigen.

5. Bestätigen Sie im Abschnitt **Installation**, dass der aktuelle Status „bereit zum Starten der Installation von *Node Name* in das Grid mit primärem Admin-Node *admin_ip*“ lautet und dass die Schaltfläche **Installation starten** aktiviert ist.

Wenn die Schaltfläche **Installation starten** nicht aktiviert ist, müssen Sie möglicherweise die Netzwerkkonfiguration oder die Porteinstellungen ändern. Anweisungen hierzu finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

6. Wählen Sie auf der Startseite des StorageGRID-Appliance-Installationsprogramms die Option **Installation starten**.

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node
discovery ☐

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.

- Wenn Ihre Erweiterung mehrere Appliance-Nodes umfasst, wiederholen Sie die vorherigen Schritte für jede Appliance.



Wenn Sie mehrere Appliance Storage Nodes gleichzeitig bereitstellen müssen, können Sie den Installationsprozess mithilfe des Installationskripts für die configure-sga.py Appliance automatisieren.

- Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, wählen Sie in der Menüleiste die Option **Monitor-Installation** aus.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt wurden, nicht erneut ausgeführt werden. Wenn Sie eine Installation erneut ausführen, werden alle Aufgaben, die nicht erneut ausgeführt werden müssen, mit einer grünen Statusleiste und dem Status „Skipped.“ angezeigt.

9. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

1. Gerät konfigurieren

In dieser Phase tritt eines der folgenden Prozesse auf:

- Bei einer Storage Appliance stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.
- Bei einer Services-Appliance löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken im Compute-Controller und konfiguriert die Hostereinstellungen.

2. Installieren Sie das Betriebssystem

In dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID auf die Appliance.

10. Überwachen Sie den Installationsfortschritt, bis eine Meldung im Konsolenfenster angezeigt wird. Dazu werden Sie aufgefordert, den Knoten mit dem Grid Manager zu genehmigen.



Warten Sie, bis alle Knoten, die Sie in dieser Erweiterung hinzugefügt haben, zur Genehmigung bereit sind, bevor Sie zum Grid Manager gehen, um die Knoten zu genehmigen.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type#: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Erweiterung durchführen

Wenn die Erweiterung durchgeführt wird, werden die neuen Grid-Nodes zu Ihrer bestehenden StorageGRID Implementierung hinzugefügt.

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.
- Sie haben alle Grid-Nodes implementiert, die in dieser Erweiterung hinzugefügt werden.

- Beim Hinzufügen von Speicherknoten haben Sie bestätigt, dass alle Datenreparaturvorgänge im Rahmen einer Wiederherstellung abgeschlossen sind. Siehe [Prüfen Sie die Reparatur von Daten](#).
- Wenn Sie einen neuen Standort hinzufügen, müssen Sie ILM-Regeln prüfen und aktualisieren, bevor Sie die Erweiterung starten, um sicherzustellen, dass Objektkopien erst nach Abschluss der Erweiterung auf dem neuen Standort gespeichert werden. Wenn eine Regel beispielsweise den Standard-Speicherpool (Alle Speicherknoten) verwendet, müssen Sie einen neuen Speicherpool erstellen, der nur die vorhandenen Speicherknoten enthält, und die ILM-Regel aktualisieren, um den neuen Speicherpool zu verwenden. Andernfalls werden Objekte auf den neuen Standort kopiert, sobald der erste Node an diesem Standort aktiv ist. Siehe Anweisungen für [Objektmanagement mit ILM](#).

Über diese Aufgabe

Während der Erweiterung umfasst die folgenden Phasen:

1. Sie konfigurieren die Erweiterung, indem Sie angeben, ob Sie neue Grid-Nodes oder einen neuen Standort hinzufügen und die Grid-Nodes genehmigen, die Sie hinzufügen möchten.
2. Sie starten die Erweiterung.
3. Während der Erweiterungsprozess ausgeführt wird, laden Sie eine neue Wiederherstellungspaket-Datei herunter.
4. Sie überwachen den Status der Gitterkonfigurationsstufen, die automatisch ausgeführt werden. Die Anzahl der Stufen hängt davon ab, welche Typen von Grid-Nodes hinzugefügt werden und ob ein neuer Standort hinzugefügt wird.



Einige Phasen benötigen möglicherweise viel Zeit, um auf einem großen Raster zu laufen. Das Streaming von Cassandra auf einen neuen Storage-Node kann beispielsweise nur wenige Minuten dauern, wenn die Cassandra-Datenbank leer ist. Wenn die Cassandra-Datenbank jedoch eine große Menge an Objekt-Metadaten enthält, kann diese Phase mehrere Stunden oder länger dauern. Starten Sie keine Storage-Nodes entweder während der Phasen „erweitern des Cassandra-Clusters“ oder „Starten von Cassandra und Streaming-Daten“ neu.

Schritte

1. Wählen Sie **WARTUNG Aufgaben Erweiterung**.

Die Seite Rastererweiterung wird angezeigt. Im Abschnitt Ausstehende Knoten werden alle Knoten aufgeführt, die hinzugefügt werden können.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

[Configure Expansion](#)

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve ✕ Remove		Search Q			
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:68:1a	DC2-ADM1-184	Admin Node	VMware VM	172.17.3.184/21
☐	00:50:56:87:f1:fc	DC2-S1-185	Storage Node	VMware VM	172.17.3.185/21
☐	00:50:56:87:54:1e	DC2-S2-186	Storage Node	VMware VM	172.17.3.186/21
☐	00:50:56:87:6f:0c	DC2-S3-187	Storage Node	VMware VM	172.17.3.187/21
☐	00:50:56:87:b6:83	DC2-S4-188	Storage Node	VMware VM	172.17.3.188/21
☐	00:50:56:87:b3:7d	DC2-ARC1-189	Archive Node	VMware VM	172.17.3.189/21

2. Wählen Sie **Erweiterung Konfigurieren**.

Das Dialogfeld Standortauswahl wird angezeigt.

Site Selection

You can add grid nodes to a new site or to existing sites, but you cannot perform both types of expansion at the same time.

Site ☒ New ☐ Existing

Site Name

[Cancel](#) [Save](#)

3. Wählen Sie den Erweiterungstyp aus, den Sie starten:

- Wenn Sie eine neue Site hinzufügen, wählen Sie **Neu**, und geben Sie den Namen der neuen Site ein.
- Wenn Sie einem vorhandenen Standort Rasterknoten hinzufügen, wählen Sie **vorhandene**.

4. Wählen Sie **Speichern**.

5. Überprüfen Sie die Liste **Ausstehende Knoten** und vergewissern Sie sich, dass alle von Ihnen bereitgestellten Grid-Knoten angezeigt werden.

Bei Bedarf können Sie den Cursor über die **Grid Network MAC Address** eines Knotens bewegen, um Details zu diesem Knoten anzuzeigen.

+ Approve

✖ Remove

Grid Network MAC

☐ 00:50:56:87:68:1a
 ☐ 00:50:56:87:54:1e
 ☒ 00:50:56:87:6f:0c
 ☐ 00:50:56:87:b6:83
 ☐ 00:50:56:87:b3:7d

DC2-S3-187

Storage Node

	Address	IP	Name
Network			
Grid Network	172.17.3.187/21	172.17.0.1	kwinters-DC2-ADM1-184
Admin Network			kwinters-DC2-ADM1-184
Client Network	10.224.3.187/21	10.224.0.1	kwinters-DC2-ADM1-184

Hardware

VMware VM 8 CPUs 8 GB RAM

Disks

107 GB 107 GB 107 GB 107 GB 107 GB



Wenn ein Grid-Node fehlt, bestätigen Sie, dass er erfolgreich bereitgestellt wurde.

6. Genehmigen Sie in der Liste der ausstehenden Knoten die Grid-Knoten für diese Erweiterung.
 - a. Aktivieren Sie das Optionsfeld neben dem ersten ausstehenden Rasterknoten, den Sie genehmigen möchten.
 - b. Wählen Sie **Genehmigen**.

Das Konfigurationsformular für den Grid-Node wird angezeigt.

Storage Node Configuration

General Settings

Site	Site A
Name	DC2-S3-187
NTP Role	Automatic
ADC Service	Automatic

Select "Yes" if this node will replace another node at this site that has the ADC service.

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	172.17.3.187/21
Gateway	172.17.0.1

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	
Gateway	
Subnets (CIDR)	+

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	
Gateway	

Cancel

Save

c. Ändern Sie bei Bedarf die allgemeinen Einstellungen:

- **Standort:** Der Name des Standorts, dem der Grid-Node zugeordnet ist. Wenn Sie mehrere Nodes hinzufügen, vergewissern Sie sich, dass Sie für jeden Node den korrekten Standort auswählen. Wenn Sie einen neuen Standort hinzufügen, werden alle Nodes zum neuen Standort hinzugefügt.

- **Name:** Der Hostname, der dem Knoten zugewiesen wird, und der Name, der im Grid Manager angezeigt wird.
- **NTP-Rolle:** Die NTP-Rolle (Network Time Protocol) des Grid-Knotens. Die Optionen sind **Automatic**, **Primary** und **Client**. Bei Auswahl von **automatisch** wird die primäre Rolle Administratorknoten, Speicherknoten mit ADC-Diensten, Gateway-Nodes und beliebigen Grid-Nodes mit nicht statischen IP-Adressen zugewiesen. Allen anderen Grid-Nodes wird die Client-Rolle zugewiesen.



Weisen Sie die primäre NTP-Rolle mindestens zwei Nodes an jedem Standort zu. Dadurch erhalten Sie redundanten Zugriff auf externe Zeitquellen.

- **ADC Service** (nur Speicherknoten): Ob dieser Speicherknoten den Dienst Administrative Domain Controller (ADC) ausführen wird. Der ADC-Dienst verfolgt den Standort und die Verfügbarkeit von Grid-Services. Mindestens drei Storage-Nodes an jedem Standort müssen den ADC-Service enthalten. Der ADC-Dienst kann nicht einem Node hinzugefügt werden, nachdem er bereitgestellt wurde.
 - Wenn Sie diesen Knoten hinzufügen, um einen Speicherknoten zu ersetzen, wählen Sie **Ja** aus, wenn der Knoten, den Sie ersetzen, den ADC-Dienst enthält. Da ein Storage-Node nicht stillgelegt werden kann, wenn zu wenige ADC-Dienste verbleiben, wird sichergestellt, dass ein neuer ADC-Service verfügbar ist, bevor der alte Service entfernt wird.
 - Wählen Sie andernfalls **automatisch** aus, damit das System feststellen kann, ob dieser Knoten den ADC-Dienst erfordert. Erfahren Sie mehr über das ADC-Quorum [Hier](#).

d. Ändern Sie bei Bedarf die Einstellungen für das Grid-Netzwerk, das Admin-Netzwerk und das Client-Netzwerk.

- **IPv4-Adresse (CIDR):** Die CIDR-Netzwerkadresse für die Netzwerkschnittstelle. Beispiel: 172.16.10.100/24
- **Gateway:** Das Standard-Gateway des Grid-Knotens. Beispiel: 172.16.10.1
- **Subnetze (CIDR):** Ein oder mehrere Unternetzwerke für das Admin-Netzwerk.

e. Wählen Sie **Speichern**.

Der genehmigte Grid-Node wird in die Liste der genehmigten Nodes verschoben.

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit Reset Remove Search Q							
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐	00:50:56:87:f1:fc	DC2-S1-185	Site A	Storage Node	VMware VM	172.17.3.185/21	
☐	00:50:56:87:6f:0c	DC2-S3-187	Site A	Storage Node	VMware VM	172.17.3.187/21	

Passphrase

Enter the provisioning passphrase to change the grid topology of your StorageGRID system.

Provisioning Passphrase

Cancel

Expand

- Um die Eigenschaften eines genehmigten Grid-Knotens zu ändern, wählen Sie das entsprechende Optionsfeld aus, und wählen Sie **Bearbeiten**.

- Um einen genehmigten Rasterknoten zurück in die Liste ausstehender Knoten zu verschieben, wählen Sie dessen Optionsfeld aus und wählen Sie **Zurücksetzen**.
 - Um einen genehmigten Grid-Node dauerhaft zu entfernen, schalten Sie den Node aus. Wählen Sie dann das entsprechende Optionsfeld aus, und wählen Sie **Entfernen**.
- f. Wiederholen Sie diese Schritte für jeden ausstehenden Rasterknoten, den Sie genehmigen möchten.



Wenn möglich, sollten Sie alle ausstehenden Grid-Notizen genehmigen und eine einzelne Erweiterung durchführen. Wenn Sie mehrere kleine Erweiterungen durchführen, ist mehr Zeit erforderlich.

7. Wenn Sie alle Grid-Nodes genehmigt haben, geben Sie die **Provisioning-Passphrase** ein, und wählen Sie **Expand**.

Nach einigen Minuten wird diese Seite aktualisiert, um den Status des Erweiterungsverfahrens anzuzeigen. Wenn Aufgaben ausgeführt werden, die sich auf einzelne Grid-Nodes auswirken, enthält der Abschnitt Status des Grid-Knotens den aktuellen Status für jeden Grid-Node.



Während dieses Prozesses zeigt das Installationsprogramm für StorageGRID-Geräte, dass die Installation von Phase 3 auf Stufe 4 verschoben wird, und schließt die Installation ab. Wenn Phase 4 abgeschlossen ist, wird der Controller neu gestartet.

Grid Expansion

Information A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing Grid Nodes
In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Name	Site	Grid Network IPv4 Address	Progress	Stage
DC2-ADM1-184	Site A	172.17.3.184/21		Waiting for NTP to synchronize
DC2-S1-185	Site A	172.17.3.185/21		Waiting for Dynamic IP Service peers
DC2-S2-186	Site A	172.17.3.186/21		Waiting for NTP to synchronize
DC2-S3-187	Site A	172.17.3.187/21		Waiting for NTP to synchronize
DC2-S4-188	Site A	172.17.3.188/21		Waiting for Dynamic IP Service peers
DC2-ARC1-189	Site A	172.17.3.189/21		Waiting for NTP to synchronize

2. Initial Configuration
Pending

3. Distributing the new grid node's certificates to the StorageGRID system.
Pending

4. Starting services on the new grid nodes
Pending

5. Cleaning up unused Cassandra keys
Pending



Eine Standorterweiterung umfasst eine zusätzliche Aufgabe zur Konfiguration von Cassandra für den neuen Standort.

8. Sobald der Link **Download Recovery Package** angezeigt wird, laden Sie die Recovery Package Datei herunter.

Sie müssen eine aktualisierte Kopie der Wiederherstellungspaket-Datei so schnell wie möglich herunterladen, nachdem Grid-Topologieänderungen am StorageGRID-System vorgenommen wurden. Die Recovery Package-Datei ermöglicht es Ihnen, das System wiederherzustellen, wenn ein Fehler auftritt.

- a. Wählen Sie den Download-Link aus.
- b. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **Download starten**.
- c. Wenn der Download abgeschlossen ist, öffnen Sie das .zip Datei und bestätigen Sie, dass es ein enthält `gpt-backup` Verzeichnis und A _SAID.zip Datei: Dann extrahieren Sie den _SAID.zip Wechseln Sie zur Datei /GID*_REV* Telefonbuch und bestätigen Sie, dass Sie das öffnen können `passwords.txt` Datei:
- d. Kopieren Sie die heruntergeladene Recovery Package-Datei (.zip) in zwei sichere und separate Speicherorte.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

9. Befolgen Sie die Anweisungen zum Hinzufügen eines Speicherknoten zu einem vorhandenen Standort oder Hinzufügen eines neuen Standorts.

Fügen Sie dem vorhandenen Standort Storage Node hinzu

Wenn Sie einen oder mehrere Speicherknoten zu einem bestehenden Standort hinzufügen, überwachen Sie den Fortschritt der Phase „Starten von Cassandra und Streamen von Daten“, indem Sie den in der Statusmeldung angezeigten Prozentsatz überprüfen.

4. Starting services on the new grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

⚠ Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Search

Name	Site	Grid Network IPv4 Address	Progress	Stage
DC1-S4	Data Center 1	10.96.99.55/23		Starting Cassandra and streaming data (90.0% streamed)
DC1-S5	Data Center 1	10.96.99.56/23		Complete
DC1-S6	Data Center 1	10.96.99.57/23		Complete

Dieser Prozentsatz schätzt, wie vollständig der Cassandra-Streaming-Vorgang ist, basierend auf der Gesamtmenge der verfügbaren Cassandra-Daten und der bereits auf den neuen Node geschriebenen Menge.



Starten Sie keine Storage-Nodes entweder während der Phasen „Erweiterung des Cassandra-Clusters“ oder „Starten von Cassandra und Streaming-Daten“ neu. Diese Phasen dauern möglicherweise für jeden neuen Storage Node viele Stunden, insbesondere dann, wenn vorhandene Storage-Nodes eine große Menge an Objekt-Metadaten enthalten.

Neuen Standort hinzufügen

Wenn Sie einen neuen Standort hinzufügen, verwenden Sie `nodetool status` Den Fortschritt des Cassandra-Streamings zu überwachen und zu sehen, wie viele Metadaten während der Phase „Erweiterung des Cassandra-Clusters“ auf den neuen Standort kopiert wurden. Die gesamte Datenlast am neuen Standort sollte sich innerhalb von etwa 20 % der Gesamtmenge eines aktuellen Standorts befinden.



Starten Sie keine Storage-Nodes entweder während der Phasen „Erweiterung des Cassandra-Clusters“ oder „Starten von Cassandra und Streaming-Daten“ neu. Diese Phasen dauern möglicherweise für jeden neuen Storage Node viele Stunden, insbesondere dann, wenn vorhandene Storage-Nodes eine große Menge an Objekt-Metadaten enthalten.

1. Fahren Sie mit der Überwachung der Erweiterung fort, bis alle Aufgaben abgeschlossen sind und die Schaltfläche **Erweiterung konfigurieren** erneut angezeigt wird.

Nachdem Sie fertig sind

Je nachdem, welche Typen von Grid-Nodes Sie hinzugefügt haben, müssen Sie zusätzliche Integrations- und Konfigurationsschritte durchführen. Siehe [Konfiguration Schritte nach Erweiterung](#).

Erweitertes System konfigurieren

Konfiguration Schritte nach Erweiterung

Nach Abschluss einer Erweiterung müssen Sie weitere Integrations- und Konfigurationsschritte durchführen.

Über diese Aufgabe

Sie müssen die unten aufgeführten Konfigurationsaufgaben für die Grid-Nodes ausführen, die Sie in Ihrer Erweiterung hinzufügen. Einige Aufgaben können optional sein, je nachdem, welche Optionen bei der Installation und Verwaltung des Systems ausgewählt wurden, und wie Sie die während der Erweiterung hinzugefügten Grid-Nodes konfigurieren möchten.

Schritte

1. Wenn Sie einen Speicherknoten hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus:

- a. Überprüfen Sie die in Ihren ILM-Regeln verwendeten Speicherpools, um sicherzustellen, dass der neue Speicher verwendet wird. Siehe [Objektmanagement mit ILM](#).
 - Wenn Sie einen Standort hinzufügen, erstellen Sie einen Speicherpool für den Standort und aktualisieren Sie ILM-Regeln, um den neuen Speicherpool zu verwenden.
 - Wenn Sie einem vorhandenen Standort einen Speicherknoten hinzugefügt haben, bestätigen Sie, dass der neue Node die richtige Speicherklasse verwendet.



Standardmäßig wird der Speicherklasse Alle Speicherknoten ein neuer Speicherknoten zugewiesen und zu Speicherpools hinzugefügt, die diese Klasse für den Standort verwenden. Wenn ein neuer Knoten eine benutzerdefinierte Speicherklasse verwenden soll, müssen Sie diesen manuell der benutzerdefinierten Klasse zuweisen (**ILM Speicherstufen**).

- b. Vergewissern Sie sich, dass der Speicherknoten Objekte erfasst. Siehe [Vergewissern Sie sich, dass der Speicherknoten aktiv ist](#).
 - c. Ausgleich von Daten mit Verfahren zur Einhaltung von Datenkonsistenz (nur wenn die empfohlene Anzahl von Storage-Nodes nicht hinzugefügt werden konnte) Siehe [Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes](#).
2. Wenn Sie einen Gateway-Node hinzugefügt haben, führen Sie die folgende Konfigurationsaufgabe aus:
- Wenn Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) für Client-Verbindungen verwendet werden, fügen Sie optional den Gateway-Node einer HA-Gruppe hinzu. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen** aus, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe [StorageGRID verwalten](#).
3. Wenn Sie einen Admin-Node hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus:
- a. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist, erstellen Sie für den neuen Admin-Node eine Vertrauensbasis von einer Vertrauensbasis. Sie können sich erst beim Knoten anmelden, wenn Sie dieses Vertrauen der Vertrauensbasis erstellen. Siehe [Konfigurieren Sie Single Sign-On](#).
 - b. Wenn Sie den Load Balancer-Service auf Admin-Nodes verwenden möchten, fügen Sie optional den neuen Admin-Node einer HA-Gruppe hinzu. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen** aus, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe [StorageGRID verwalten](#).
 - c. Kopieren Sie optional die Admin-Node-Datenbank vom primären Admin-Node zum ErweiterungAdmin-

Node, wenn Sie das Attribut und die Audit-Informationen auf jedem Admin-Knoten konsistent halten möchten. Siehe [Kopieren Sie die Admin-Knoten-Datenbank](#).

- d. Kopieren Sie optional die Prometheus-Datenbank vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie die historischen Metriken auf jedem Admin-Knoten konsistent halten möchten. Siehe [Kopieren Sie die Prometheus-Kennzahlen](#).
- e. Kopieren Sie optional die vorhandenen Audit-Protokolle vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie die historischen Protokollinformationen auf jedem Admin-Knoten konsistent halten möchten. Siehe [Prüfprotokolle kopieren](#).
- f. Konfigurieren Sie optional den Zugriff auf das System für Audit-Zwecke über eine NFS- oder CIFS-Dateifreigabe. Siehe [StorageGRID verwalten](#).



Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

- g. Ändern Sie optional den bevorzugten Absender für Benachrichtigungen. Sie können den Erweiterungs-Admin-Knoten zum bevorzugten Absender machen. Andernfalls sendet ein vorhandener als bevorzugter Absender konfigurierter Admin-Node weiterhin Benachrichtigungen, einschließlich AutoSupport-Nachrichten, SNMP-Benachrichtigungen, Alarm-E-Mails und Alarm-E-Mails (Legacy-System). Siehe [StorageGRID verwalten](#).
4. Wenn Sie einen Archivknoten hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus.
- a. Konfigurieren Sie die Verbindung des Archiv-Knotens mit dem angestrebten externen Archiv-Storage-System. Wenn Sie die Erweiterung abgeschlossen haben, befinden sich Archiv-Knoten in einem Alarmzustand, bis Sie die Verbindungsinformationen über die Komponente **ARC Ziel** konfigurieren. Siehe [StorageGRID verwalten](#).
 - b. Aktualisieren Sie die ILM-Richtlinie, um Objektdaten über den neuen Archivierungs-Node zu archivieren. Siehe [Objektmanagement mit ILM](#).
 - c. Konfigurieren Sie benutzerdefinierte Alarmer für die Attribute, die zur Überwachung der Geschwindigkeit und Effizienz des Datenabrufs von Objektdaten von Archiv-Nodes verwendet werden. Siehe [StorageGRID verwalten](#).
5. Um zu prüfen, ob Erweiterungsknoten mit einem nicht vertrauenswürdigen Client-Netzwerk hinzugefügt wurden oder um zu ändern, ob das Client-Netzwerk eines Knotens nicht vertrauenswürdige oder vertrauenswürdige ist, gehen Sie zu **CONFIGURATION Network UnTrusted Client Network**.

Wenn das Client-Netzwerk auf dem Erweiterungsknoten nicht vertrauenswürdige ist, müssen Verbindungen zum Knoten im Client-Netzwerk über einen Load Balancer-Endpunkt hergestellt werden. Siehe [StorageGRID verwalten](#).

6. Konfigurieren Sie das Domain Name System (DNS).

Wenn Sie für jeden Grid-Node DNS-Einstellungen separat angegeben haben, müssen Sie für die neuen Nodes benutzerdefinierte DNS-Einstellungen pro Node hinzufügen. Siehe [Ändern der DNS-Konfiguration für einen einzelnen Grid-Node](#).

Eine Best Practice besteht in der netzweiten DNS-Server-Liste, die einige DNS-Server enthält, auf die von jedem Standort aus lokal zugegriffen werden kann. Wenn Sie gerade einen neuen Standort hinzugefügt haben, fügen Sie der Grid-weiten DNS-Konfiguration neue DNS-Server für den Standort hinzu.



Geben Sie zwei bis sechs IPv4-Adressen für DNS-Server an. Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen. Weitere Informationen finden Sie unter [Ändern der DNS-Konfiguration für einen einzelnen Grid-Node..](#)

7. Wenn Sie einen neuen Standort hinzugefügt haben, vergewissern Sie sich, dass auf die NTP-Server (Network Time Protocol) von diesem Standort aus zugegriffen werden kann. Siehe [Konfigurieren Sie NTP-Server.](#)



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

Vergewissern Sie sich, dass der Speicherknoten aktiv ist

Nachdem ein Erweiterungsvorgang abgeschlossen ist, der neue Speicherknoten hinzugefügt hat, sollte das StorageGRID-System automatisch mit den neuen Speicherknoten beginnen. Sie müssen das StorageGRID-System verwenden, um sicherzustellen, dass der neue Speicherknoten aktiv ist.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an [Unterstützter Webbrowser](#).
2. Wählen Sie **NODES Erweiterungs-Storage-Node Storage** aus.
3. Bewegen Sie den Cursor über das Diagramm **verwendete Speicherung - Objektdaten**, um den Wert für **verwendet** anzuzeigen. Dies ist die Menge des insgesamt nutzbaren Speicherplatzes, der für Objektdaten verwendet wurde.
4. Vergewissern Sie sich, dass der Wert von **verwendet** erhöht wird, wenn Sie den Cursor nach rechts auf dem Diagramm bewegen.

Admin-Knoten-Datenbank kopieren

Beim Hinzufügen von Admin-Nodes durch ein Erweiterungsverfahren können Sie optional die Datenbank vom primären Admin-Node zum neuen Admin-Node kopieren. Durch das Kopieren der Datenbank können Sie historische Informationen über Attribute, Warnmeldungen und Warnmeldungen aufbewahren.

Was Sie benötigen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Der StorageGRID-Softwareaktivierungsprozess erstellt eine leere Datenbank für den NMS-Dienst auf dem Erweiterungs-Admin-Knoten. Wenn der NMS-Dienst auf dem Erweiterungs-Admin-Knoten startet, zeichnet er

Informationen für Server und Dienste auf, die derzeit Teil des Systems sind oder später hinzugefügt werden. Diese Admin-Knoten-Datenbank enthält die folgenden Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT Tools Grid Topology** verfügbar sind

Um sicherzustellen, dass die Admin-Node-Datenbank zwischen den Knoten konsistent ist, können Sie die Datenbank vom primären Admin-Node auf den Erweiterungs-Admin-Node kopieren.



Das Kopieren der Datenbank vom primären Admin-Node (der __Source Admin-Node__) zu einem Erweiterungs-Admin-Node kann bis zu mehrere Stunden dauern. In diesem Zeitraum ist der Grid Manager nicht zugänglich.

Führen Sie diese Schritte aus, um den MI-Dienst und den Management-API-Dienst sowohl auf dem primären Admin-Node als auch auf dem Erweiterungs-Admin-Node zu beenden, bevor Sie die Datenbank kopieren.

Schritte

1. Führen Sie die folgenden Schritte auf dem primären Admin-Knoten aus:

a. Melden Sie sich beim Admin-Knoten an:

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

b. Führen Sie den folgenden Befehl aus: `recover-access-points`

c. Geben Sie die Provisionierungs-Passphrase ein.

d. Beenden SIE DEN MI-Dienst: `service mi stop`

e. Beenden Sie den Management Application Program Interface (Management API) Service: `service mgmt-api stop`

2. Führen Sie die folgenden Schritte auf dem Erweiterungs-Admin-Knoten aus:

a. Melden Sie sich beim Erweiterungs-Admin-Knoten an:

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

b. Beenden SIE DEN MI-Dienst: `service mi stop`

c. Beenden Sie den Management API-Service: `service mgmt-api stop`

d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`

e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den Erweiterungs-Admin-Knoten:


```
/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP
```

- g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem Erweiterungs-Admin-Node überschreiben möchten.

Die Datenbank und ihre historischen Daten werden auf den Erweiterungs-Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den Erweiterungs-Admin-Knoten.

- h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein: `ssh-add -D`

3. Starten Sie die Dienste auf dem primären Admin-Knoten neu: `service servermanager start`

Kopieren Sie die Prometheus-Kennzahlen

Nach dem Hinzufügen eines neuen Admin-Knotens können Sie optional die historischen Metriken kopieren, die von Prometheus vom primären Admin-Node erhalten wurden, zum neuen Admin-Node. Durch das Kopieren der Metriken wird sichergestellt, dass historische Metriken zwischen Admin-Nodes konsistent sind.

Was Sie benötigen

- Der neue Admin-Node wird installiert und ausgeführt.
- Sie haben die `Passwords.txt` Datei:
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn Sie einen Admin-Knoten hinzufügen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Sie können die historischen Kennzahlen zwischen den Knoten konsistent halten, indem Sie die Prometheus-Datenbank vom primären Admin-Node (den `_Source Admin-Node_`) auf den neuen Admin-Node kopieren.



Das Kopieren der Prometheus-Datenbank dauert möglicherweise eine Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-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:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie auf dem neuen Admin-Knoten die folgenden Schritte aus:
 - a. Melden Sie sich beim neuen Admin-Knoten 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:
- b. Stoppen Sie den Prometheus Service: `service prometheus stop`
- c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
- d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
- e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Node auf den neuen Admin-Node:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem neuen Admin-Knoten zerstören möchten.

Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den neuen Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den neuen Admin-Knoten. Der folgende Status wird angezeigt:

```
Database cloned, starting services
```

- a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:

```
ssh-add -D
```

- 4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.

```
service prometheus start
```

Prüfprotokolle kopieren

Wenn Sie einen neuen Admin-Node durch ein Erweiterungsverfahren hinzufügen, protokolliert sein AMS-Service nur Ereignisse und Aktionen, die nach dem Beitritt zum System auftreten. Nach Bedarf können Sie Audit-Protokolle von einem zuvor installierten Admin-Node auf den neuen Erweiterungs-Admin-Node kopieren, sodass er mit dem Rest des StorageGRID Systems synchronisiert ist.

Was Sie benötigen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Um historische Audit-Meldungen auf einem neuen Admin-Knoten verfügbar zu machen, müssen Sie die Audit-Log-Dateien manuell von einem vorhandenen Admin-Knoten in den Erweiterungs-Admin-Knoten kopieren.

Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:



- Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.

Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#) Entsprechende Details.

Schritte

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@_primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- 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 `#`.

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Datei erstellt wird: `service ams stop`
3. Benennen Sie den um `audit.log` Datei um sicherzustellen, dass die Datei auf dem Erweiterungs-Admin-Knoten nicht überschrieben wird, in den Sie sie kopieren:

```
cd /var/local/audit/export
ls -l
mv audit.log new_name.txt
```

4. Kopieren Sie alle Audit-Log-Dateien in den Erweiterungs-Admin-Node:

```
scp -p * IP_address:/var/local/audit/export
```

5. Wenn Sie zur Eingabe der Passphrase für aufgefordert werden `/root/.ssh/id_rsa` Geben Sie das SSH-Zugriffskennwort für den primären Admin-Node ein, der im aufgeführt ist ``Password.txt` Datei:

6. Stellen Sie das Original wieder her `audit.log` Datei:

```
mv new_name.txt audit.log
```

7. AMS-Dienst starten:

```
service ams start
```

8. Melden Sie sich vom Server ab:

```
exit
```

9. Melden Sie sich beim Erweiterungs-Admin-Knoten an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@expansion_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 `#`.

10. Benutzer- und Gruppeneinstellungen für die Audit-Log-Dateien aktualisieren:

```
cd /var/local/audit/export  
chown ams-user:bycast *
```

11. Melden Sie sich vom Server ab:

```
exit
```

Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes

In einigen Fällen müssen Sie möglicherweise nach dem Hinzufügen neuer Storage-Nodes einen Ausgleich für Daten schaffen, die mit Erasure Coding versehen sind.

Was Sie benötigen

- Sie haben die Erweiterungsschritte zum Hinzufügen der neuen Speicherknoten abgeschlossen.
- Sie haben die geprüft [Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind](#).



Führen Sie diesen Vorgang nur aus, wenn die Warnung **Low Object Storage** für einen oder mehrere Speicherknoten an einem Standort ausgelöst wurde und Sie die empfohlene Anzahl neuer Speicherknoten nicht hinzufügen konnten.

- Sie wissen, dass replizierte Objektdaten bei diesem Verfahren nicht verschoben werden und dass beim EC-Ausgleichsverfahren die replizierte Datennutzung auf jedem Storage Node nicht berücksichtigt wird, wenn festgestellt wird, wo Daten mit Erasure Coding verschoben werden.
- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Wenn das EC-Ausgleichsverfahren ausgeführt wird, ist die Performance von ILM-Vorgängen sowie S3- und Swift-Client-Operationen wahrscheinlich beeinträchtigt. Aus diesem Grund sollten Sie dieses Verfahren nur in begrenzten Fällen durchführen.



Das EG-Ausgleichsverfahren reserviert vorübergehend einen großen Speicher. Storage-Warnmeldungen werden möglicherweise ausgelöst, aber nach Abschluss des Ausgleichs werden sie gelöst. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt das EC-Ausgleichsverfahren fehl. Speicherreservierungen werden freigegeben, wenn der EC-Ausgleichsvorgang abgeschlossen ist, unabhängig davon, ob der Vorgang fehlgeschlagen oder erfolgreich war.



S3- und Swift-API-Operationen zum Hochladen von Objekten (oder Objektteilen) können während des EC-Ausgleichs fehlschlagen, wenn sie mehr als 24 Stunden benötigen. Langfristige PUT-Vorgänge funktionieren nicht, wenn die anwendbare ILM-Regel eine strenge oder ausgewogene Platzierung bei der Aufnahme verwendet. Der folgende Fehler wird gemeldet:

```
500 Internal Server Error
```

Schritte

1. Überprüfen Sie die aktuellen Objekt-Storage-Details für den Standort, den Sie ausgleichen möchten.
 - a. Wählen Sie **KNOTEN**.
 - b. Wählen Sie den ersten Speicherknoten am Standort aus.
 - c. Wählen Sie die Registerkarte **Storage** aus.
 - d. Halten Sie den Mauszeiger über das Diagramm „verwendete Daten – Objektdaten“, um die aktuelle Menge der replizierten Daten und mit Erasure Coding versehenen Daten auf dem Storage-Node anzuzeigen.
 - e. Wiederholen Sie diese Schritte, um die anderen Speicherknoten am Standort anzuzeigen.
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. Geben Sie den folgenden Befehl ein:

```
rebalance-data start --site "site-name"
```

Für "site-name" Geben Sie den ersten Standort an, an dem Sie neue Speicherknoten oder Knoten hinzugefügt haben. Umschließen `site-name` In Angeboten.

Der EC-Ausgleichvorgang startet, und eine Job-ID wird zurückgegeben.

4. Kopieren Sie die Job-ID.
5. Überwachen Sie den Status des EC-Ausgleichs.

- So zeigen Sie den Status eines einzelnen EC-Ausgleichs an:

```
rebalance-data status --job-id job-id
```

Für `job-id` Geben Sie die ID an, die beim Start des Verfahrens zurückgegeben wurde.

- So zeigen Sie den Status des aktuellen EC-Ausgleichs und aller zuvor abgeschlossenen Verfahren an:

```
rebalance-data status
```



Hilfe zum Befehl zum Ausgleich von Daten erhalten:

```
rebalance-data --help
```

- Um die geschätzte Zeit bis zum Abschluss und den Prozentsatz für den Abschluss des aktuellen Jobs anzuzeigen, wählen Sie **SUPPORT Tools Metrics**. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.

6. Führen Sie weitere Schritte aus, basierend auf dem zurückgegebenen Status:

- Wenn der Status lautet `In progress`, Der EC-Ausgleichsoperation läuft noch. Sie sollten das Verfahren regelmäßig überwachen, bis es abgeschlossen ist.
- Wenn der Status lautet `Failure`, Führen Sie die [Fehlerschritte](#).
- Wenn der Status lautet `Success`, Führen Sie die [Erfolg](#).

7. Wenn das EC-Ausgleichsverfahren zu viel Last generiert (beispielsweise sind Ingest-Operationen betroffen), unterbrechen Sie den Vorgang.

```
rebalance-data pause --job-id job-id
```

8. Wenn Sie das EC-Ausgleichsverfahren beenden müssen (z. B. um ein StorageGRID-Software-Upgrade durchzuführen), geben Sie Folgendes ein:

```
rebalance-data terminate --job-id job-id
```



Wenn Sie ein EC-Ausgleichsverfahren beenden, verbleiben alle bereits verschobenen Datenfragmente am neuen Standort. Daten werden nicht zurück an den ursprünglichen Speicherort verschoben.

9. Wenn der Status des EC-Ausgleichs lautet `Failure`, Folgen Sie folgenden Schritten:

- Vergewissern Sie sich, dass alle Speicherknoten am Standort mit dem Raster verbunden sind.
- Überprüfen Sie, ob Warnmeldungen vorliegen, die sich auf diese Speicherknoten auswirken könnten, und beheben Sie sie.

Informationen zu bestimmten Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung.

c. Starten Sie das EC-Ausgleichsverfahren neu:

```
rebalance-data start --job-id job-id
```

d. Wenn der Status des EC-Ausgleichs noch immer ist `Failure`, Wenden Sie sich an den technischen Support.

10. Wenn der Status des EC-Ausgleichs-Verfahrens lautet `Success`, Optional [Prüfen von Objekt-Storage](#) Um die aktualisierten Details für die Site anzuzeigen.

Daten mit Erasure-Coding-Verfahren sollten nun besser auf die Storage-Nodes am Standort abgestimmt sein.

11. Wenn Sie Erasure Coding an mehreren Standorten verwenden, führen Sie dieses Verfahren für alle anderen betroffenen Standorte aus.

Wenden Sie sich an den technischen Support

Wenn während des Grid-Erweiterungsprozesses Fehler auftreten, die nicht behoben werden können, oder wenn eine Grid-Aufgabe fehlschlägt, wenden Sie sich an den technischen Support.

Über diese Aufgabe

Wenn Sie sich an den technischen Support wenden, müssen Sie die erforderlichen Protokolldateien bereitstellen, um bei der Fehlerbehebung der Fehler zu helfen, die auftreten.

Schritte

1. Stellen Sie eine Verbindung mit dem Erweiterungs-Node her, bei dem es zu Ausfällen kommt:

a. Geben Sie den folgenden Befehl ein: `ssh -p 8022 admin@grid_node_IP`



Port 8022 ist der SSH-Port des Basis-OS, während Port 22 der SSH-Port der Container-Engine ist, auf der StorageGRID ausgeführt wird.

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:

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

2. Je nach der erreichten Stufe der Installation können Sie eines der folgenden Protokolle abrufen, die auf dem Grid-Knoten verfügbar sind:

Plattform	Protokolle
VMware	• <code>/var/log/daemon.log</code> • <code>/var/log/storagegrid/daemon.log</code> • <code>/var/log/storagegrid/nodes/<node-name>.log</code>
Linux	• <code>/var/log/storagegrid/daemon.log</code> • <code>/etc/storagegrid/nodes/<node-name>.conf</code> (Für jeden ausgefallenen Node) • <code>/var/log/storagegrid/nodes/<node-name>.log</code> (Für jeden ausgefallenen Node; ist möglicherweise nicht vorhanden)

Recovery und Wartung

Recovery and Maintain: Übersicht

Verwenden Sie diese Anweisungen, um Ihr StorageGRID System zu warten und nach Ausfällen eine Wiederherstellung zu ermöglichen.

Informationen zu diesen Anweisungen

In diesen Anweisungen wird beschrieben, wie ein Software-Hotfix angewendet wird, Grid-Nodes wiederhergestellt, ein ausgefallener Standort wiederhergestellt, Grid-Nodes oder einen gesamten Standort ausmustern, Netzwerkwartung durchführen, Wartungsvorgänge auf Host- und Middleware-Ebene durchführen und Grid Node-Verfahren durchführen.



In diesen Anweisungen bezieht sich „Linux“ auf eine Bereitstellung von Red hat® Enterprise Linux®, Ubuntu®, CentOS oder Debian®. Verwenden Sie die ["NetApp Interoperabilitäts-Matrix-Tool"](#) Um eine Liste der unterstützten Versionen zu erhalten.

Bevor Sie beginnen

- Sie verfügen über ein umfassendes Verständnis des StorageGRID Systems.
- Sie haben die Topologie Ihres StorageGRID Systems überprüft und sich mit der Grid-Konfiguration vertraut gemacht.
- Ihr versteht, dass ihr alle Anweisungen genau befolgen und alle Warnungen beachten müsst.
- Sie haben verstanden, dass keine beschriebenen Wartungsmaßnahmen unterstützt oder ein Serviceprojekt erforderlich ist.

Wartungsverfahren für Geräte

Hardwareverfahren finden Sie in der Installations- und Wartungsanleitung für Ihre StorageGRID Appliance.

- [SG100- und SG1000-Services-Appliances](#)
- [SG6000 Storage-Appliances](#)
- [SG5700 Storage-Appliances](#)
- [SG5600 Storage Appliances](#)

Recovery Package Herunterladen

Die Wiederherstellungspakedatei ermöglicht Ihnen die Wiederherstellung des StorageGRID-Systems bei einem Fehler.

Was Sie benötigen

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

Laden Sie die aktuelle Recovery Package-Datei herunter, bevor Sie Grid-Topologieänderungen am StorageGRID-System vornehmen oder bevor Sie Software aktualisieren. Laden Sie anschließend eine neue Kopie des Wiederherstellungspakets herunter, nachdem Sie Änderungen an der Grid-Topologie vorgenommen haben oder nachdem Sie die Software aktualisiert haben.

Schritte

1. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
2. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **Download starten**.

Der Download startet sofort.

3. Wenn der Download abgeschlossen ist:
 - a. Öffnen Sie das `.zip` Datei:
 - b. Bestätigen Sie, dass es ein gpt-Backup-Verzeichnis und eine interne enthält `.zip` Datei:
 - c. Entnehmen Sie die Innenseite `.zip` Datei:
 - d. Bestätigen Sie, dass Sie den öffnen können `Passwords.txt` Datei:
4. Kopieren Sie die heruntergeladene Wiederherstellungspaket-Datei (`.zip`) An zwei sichere und getrennte Stellen.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Verwandte Informationen

[StorageGRID verwalten](#)

StorageGRID Hotfix Verfahren

Möglicherweise müssen Sie einen Hotfix auf Ihr StorageGRID-System anwenden, wenn Probleme mit der Software zwischen Funktionsversionen erkannt und behoben werden.

StorageGRID Hotfixes enthalten Software-Änderungen, die außerhalb einer Feature- oder Patch-Freigabe verfügbar gemacht werden. Die gleichen Änderungen sind in einer zukünftigen Version enthalten. Darüber hinaus enthält jede Hotfix-Version eine Roll-up aller früheren Hotfixes innerhalb der Funktion oder Patch-Freigabe.

Überlegungen für die Anwendung eines Hotfix

Wenn Sie einen Hotfix anwenden, wird eine kumulative Reihe von Softwareupdates auf die Knoten in Ihrem StorageGRID-System angewendet.

Ein StorageGRID-Hotfix kann nicht angewendet werden, wenn ein anderer Wartungsvorgang ausgeführt wird. Sie können beispielsweise keinen Hotfix anwenden, während ein Decommission-, Expansions- oder Wiederherstellungsverfahren ausgeführt wird.



Wenn ein Knoten oder ein Standort stillgelegt wird, können Sie sicher einen Hotfix anwenden. Darüber hinaus können Sie in der Lage sein, einen Hotfix in den letzten Phasen eines StorageGRID-Upgrade-Verfahrens anzuwenden. Weitere Informationen finden Sie in der Anleitung zum Aktualisieren der StorageGRID-Software.

Nachdem Sie den Hotfix im Grid Manager hochgeladen haben, wird der Hotfix automatisch auf den primären Admin-Knoten angewendet. Anschließend können Sie die Anwendung des Hotfix für die übrigen Knoten in Ihrem StorageGRID-System genehmigen.

Wenn ein Hotfix nicht auf einen oder mehrere Knoten angewendet wird, wird der Grund für den Fehler in der Spalte Details der Hotfix-Fortschrittstabelle angezeigt. Sie müssen alle Fehler beheben und den gesamten Prozess wiederholen. Knoten mit einer zuvor erfolgreichen Anwendung des Hotfix werden in nachfolgenden Anwendungen übersprungen. Sie können den Hotfix-Prozess so oft wie erforderlich sicher wiederholen, bis alle Knoten aktualisiert wurden. Der Hotfix muss erfolgreich auf allen Grid-Knoten installiert werden, damit die Anwendung abgeschlossen werden kann.

Während die Grid-Knoten mit der neuen Hotfix-Version aktualisiert werden, können die tatsächlichen Änderungen in einem Hotfix nur bestimmte Dienste auf bestimmte Node-Typen beeinflussen. Ein Hotfix wirkt sich beispielsweise nur auf den LDR-Service auf Storage Nodes aus.

Wie Hotfixes für die Wiederherstellung und Erweiterung eingesetzt werden

Nachdem ein Hotfix auf das Grid angewendet wurde, installiert der primäre Admin-Knoten automatisch die gleiche Hotfix-Version auf alle Knoten, die durch Wiederherstellungsvorgänge wiederhergestellt oder in einer Erweiterung hinzugefügt werden.

Wenn Sie jedoch den primären Admin-Knoten wiederherstellen müssen, müssen Sie manuell die richtige StorageGRID-Version installieren und dann den Hotfix anwenden. Die endgültige StorageGRID-Version des primären Admin-Knotens muss mit der Version der anderen Nodes im Raster übereinstimmen.

Das folgende Beispiel zeigt, wie ein Hotfix bei der Wiederherstellung des primären Admin-Knotens angewendet wird:

1. Angenommen, auf dem Grid wird eine StorageGRID 11.A.B-Version mit dem neuesten Hotfix ausgeführt. Die „GRID Version“ ist 11.A.B.y.
2. Der primäre Admin-Node schlägt fehl.
3. Sie stellen den primären Admin-Node mit StorageGRID 11.A.B neu bereit und führen das Recovery-Verfahren durch.



Je nach Bedarf zur Anpassung der Grid-Version können Sie beim Bereitstellen des Node eine Nebenversion verwenden; es ist nicht erforderlich, das Hauptversion zuerst zu implementieren.

4. Anschließend wenden Sie Hotfix 11.A.B.y auf den primären Admin-Node an.

Verwandte Informationen

[Primären Ersatzadministrator-Knoten konfigurieren](#)

Planen und bereiten Sie sich auf einen Hotfix vor

Sie müssen vor dem Anwenden eines Hotfix planen, um eine minimale Störung Ihres StorageGRID-Systems zu gewährleisten.

Schritte

- [Auswirkungen auf Ihr System beim Anwenden eines Hotfix](#)
- [Beschaffung der erforderlichen Materialien für einen Hotfix](#)
- [Hotfix-Datei wird heruntergeladen](#)
- [Überprüfen Sie den Zustand des Systems, bevor Sie einen Hotfix anwenden](#)

Auswirkungen auf Ihr System beim Anwenden eines Hotfix

Wenn Sie einen Hotfix anwenden, müssen Sie verstehen, wie sich Ihr StorageGRID-System auswirkt.

Bei Client-Applikationen kommt es unter Umständen zu kurzfristigen Unterbrechungen

Das StorageGRID System kann während des Hotfix-Prozesses Daten von Client-Applikationen aufnehmen und abrufen. Client-Verbindungen zu einzelnen Gateway-Nodes oder Storage-Nodes können jedoch vorübergehend unterbrochen werden, wenn der Hotfix Dienste auf diesen Knoten neu starten muss. Die Verbindung wird wiederhergestellt, sobald der Hotfix-Prozess abgeschlossen ist und die Dienste auf den einzelnen Knoten wieder aufgenommen werden.

Möglicherweise müssen Sie Ausfallzeiten planen, um einen Hotfix anzuwenden, wenn ein kurzfristiger Verlust der Verbindung nicht akzeptabel ist. Sie können eine selektive Genehmigung verwenden, um die Planung für die Aktualisierung bestimmter Knoten zu planen.



Dank mehrerer Gateways und Hochverfügbarkeitsgruppen (HA-Gruppen) lassen sich während des Hotfix-Prozesses automatische Failovers durchführen. Siehe Anweisungen für [Konfigurieren von Hochverfügbarkeitsgruppen](#).

Warnmeldungen und SNMP-Benachrichtigungen können ausgelöst werden

Warnmeldungen und SNMP-Benachrichtigungen können ausgelöst werden, wenn Dienste neu gestartet werden und das StorageGRID System als Umgebung mit gemischten Versionen funktioniert (einige Grid-Nodes mit einer früheren Version, während andere auf eine neuere Version aktualisiert wurden). Im Allgemeinen werden diese Warnungen und Benachrichtigungen gelöscht, wenn der Hotfix abgeschlossen ist.

Konfigurationsänderungen sind eingeschränkt

Beim Anwenden eines Hotfix auf StorageGRID:

- Nehmen Sie keine Änderungen an der Grid-Konfiguration vor (z. B. das Angeben von Grid Network Subnets oder das Genehmigen ausstehender Grid-Nodes), bis der Hotfix auf alle Nodes angewendet wurde.
- Aktualisieren Sie die ILM-Konfiguration erst, wenn der Hotfix auf alle Knoten angewendet wurde.

Beschaffung der erforderlichen Materialien für Hotfix

Bevor Sie einen Hotfix anwenden, müssen Sie alle erforderlichen Materialien erhalten.

Element	Hinweise
StorageGRID-Hotfix-Datei	Sie müssen die StorageGRID-Hotfix-Datei herunterladen.
• Netzwerkport • Unterstützter Webbrowser • SSH-Client (z. B. PuTTY)	
Wiederherstellungspaket (.zip) Datei	Vor dem Anwenden eines Hotfix Laden Sie die neueste Recovery Package-Datei herunter Falls während des Hotfix Probleme auftreten, dann, nachdem der Hotfix angewendet wurde, laden Sie eine neue Kopie der Recovery Package-Datei herunter und speichern Sie sie an einem sicheren Ort. Mit der aktualisierten Wiederherstellungspaket-Datei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

Element	Hinweise
Passwords.txt-Datei	Optional und nur verwendet, wenn Sie einen Hotfix manuell mit dem SSH-Client anwenden. Der <code>Passwords.txt</code> Die Datei ist im GENANTTEN Paket enthalten, das Teil des Wiederherstellungspakets ist .zip Datei:
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase wird im nicht aufgeführt <code>Passwords.txt</code> Datei:
Zugehörige Dokumentation	<code>readme.txt</code> Datei für den Hotfix. Diese Datei ist auf der Download-Seite des Hotfix enthalten. Schauen Sie sich die an <code>readme</code> Vor dem Anwenden des Hotfix sorgfältig ablesen.

Verwandte Informationen

[Hotfix-Datei herunterladen](#)

Hotfix-Datei herunterladen

Sie müssen die Hotfix-Datei herunterladen, bevor Sie den Hotfix anwenden können.

Schritte

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

["NetApp Downloads: StorageGRID"](#)

2. Wählen Sie den Pfeil nach unten unter **Verfügbare Software**, um eine Liste der Hotfixes anzuzeigen, die zum Herunterladen verfügbar sind.



Hotfix-Dateiversionen haben das Formular: 11.4.x.y.

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



Wenn Sie gerade den primären Admin-Knoten wiederhergestellt haben und einen Hotfix anwenden müssen, wählen Sie die gleiche Hotfix-Version, die auf den anderen Grid-Knoten installiert ist.

- a. Wählen Sie die Hotfix-Version, die Sie herunterladen möchten, und wählen Sie **Go**.
- b. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
- c. Lesen und akzeptieren Sie die Endnutzer-Lizenzvereinbarung.

Die Download-Seite für die ausgewählte Version wird angezeigt.

- d. Hotfix herunterladen `readme.txt` Datei zum Anzeigen einer Zusammenfassung der Änderungen, die im Hotfix enthalten sind.
4. Wählen Sie die Download-Schaltfläche für den Hotfix, und speichern Sie die Datei.



Ändern Sie den Namen dieser Datei nicht.



Wenn Sie ein macOS-Gerät verwenden, wird die Hotfix-Datei möglicherweise automatisch als gespeichert `.txt` Datei: Wenn dies der Fall ist, müssen Sie die Datei ohne umbenennen `.txt` Erweiterung.

5. Wählen Sie einen Speicherort für den Download aus, und wählen Sie **Speichern**.

Verwandte Informationen

[Primären Ersatzadministrator-Knoten konfigurieren](#)

Überprüfen Sie den Zustand des Systems, bevor Sie Hotfix anwenden

Sie müssen überprüfen, ob das System bereit ist, um den Hotfix aufzunehmen.

1. Melden Sie sich mit einem bei Grid Manager an [Unterstützter Webbrowser](#).
2. Stellen Sie, falls möglich, sicher, dass das System ordnungsgemäß ausgeführt wird und dass alle Grid-Nodes mit dem Grid verbunden sind.

Verbundene Knoten weisen grüne Häkchen auf  Auf der Seite Knoten.

3. Überprüfen Sie, ob und beheben Sie alle aktuellen Warnmeldungen, wenn möglich.

Informationen zu bestimmten Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

4. Stellen Sie sicher, dass keine weiteren Wartungsverfahren wie Upgrades, Wiederherstellungen, Erweiterungen oder Stillstandsmaßnahmen ausgeführt werden.

Sie sollten warten, bis alle aktiven Wartungsvorgänge abgeschlossen sind, bevor Sie einen Hotfix anwenden.

Ein StorageGRID-Hotfix kann nicht angewendet werden, wenn ein anderer Wartungsvorgang ausgeführt wird. Sie können beispielsweise keinen Hotfix anwenden, während ein Decommission-, Expansions- oder Wiederherstellungsverfahren ausgeführt wird.



Wenn ein Knoten oder ein Standort stillgelegt wird, können Sie sicher einen Hotfix anwenden. Darüber hinaus können Sie in der Lage sein, einen Hotfix in den letzten Phasen eines StorageGRID-Upgrade-Verfahrens anzuwenden. Weitere Informationen finden Sie in der Anleitung zum Aktualisieren der StorageGRID-Software.

Verwandte Informationen

[Monitoring und Fehlerbehebung](#)

[Anhalten und Fortsetzen des Stilllegen-Prozesses für Storage-Nodes](#)

Hotfix anwenden

Der Hotfix wird zuerst automatisch auf den primären Admin-Knoten angewendet. Anschließend müssen Sie die Anwendung des Hotfix für andere Grid-Knoten genehmigen, bis alle Knoten dieselbe Softwareversion ausführen. Sie können die Genehmigungssequenz anpassen, indem Sie auswählen, ob einzelne Grid-Nodes,

Gruppen von Grid-Nodes oder alle Grid-Nodes genehmigt werden sollen.

Was Sie benötigen

- Sie haben die Überlegungen geprüft und die Schritte unter ausgeführt [Planen und bereiten Sie sich auf einen Hotfix vor](#).
- Sie haben die Provisionierungs-Passphrase.
- Sie haben Root-Zugriff oder die Wartungsberechtigung.

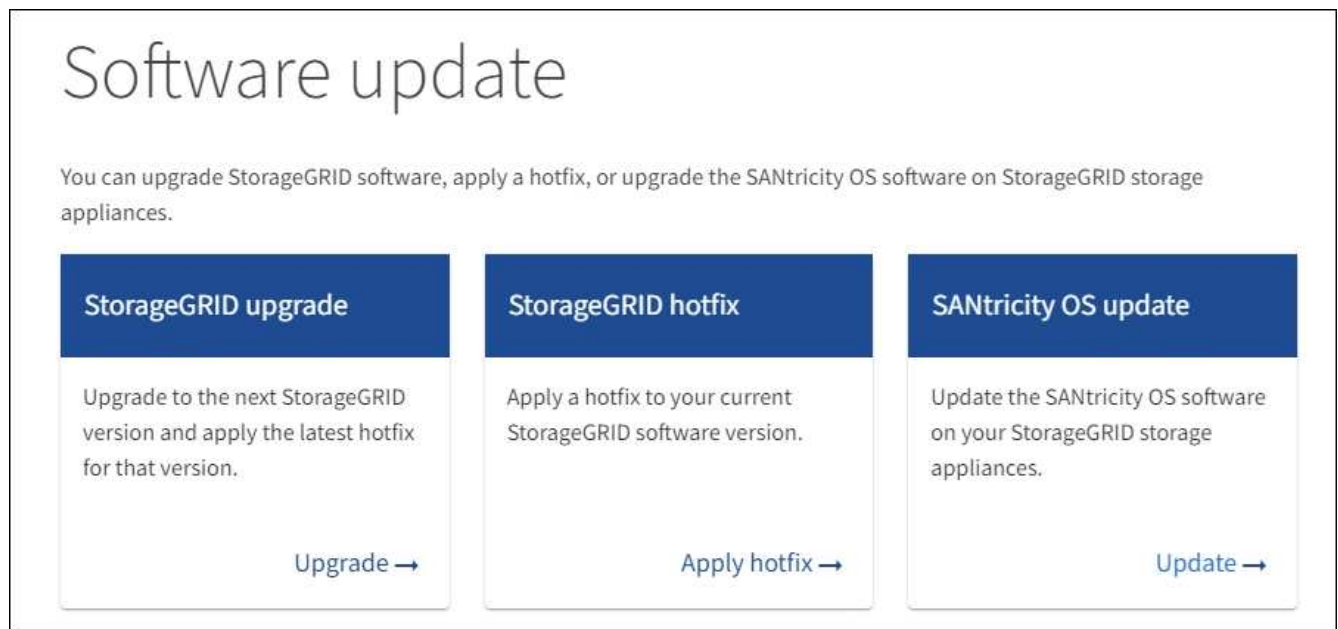
Über diese Aufgabe

- Sie können die Anwendung eines Hotfix auf einen Knoten verzögern. Der Hotfix-Prozess ist jedoch erst abgeschlossen, wenn Sie den Hotfix auf alle Knoten anwenden.
- Sie können erst nach Abschluss des Hotfix-Vorgangs ein StorageGRID Software-Upgrade oder ein SANtricity OS-Upgrade durchführen.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an [Unterstützter Webbrowser](#).
2. Wählen Sie **WARTUNG System Software-Update**.

Die Seite Software-Aktualisierung wird angezeigt.



3. Wählen Sie **Hotfix anwenden**.

Die Seite StorageGRID Hotfix wird angezeigt.

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available.

When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Browse

Passphrase

Provisioning Passphrase ?

Start

4. Wählen Sie die Hotfix-Datei aus, die Sie von der NetApp Support-Webseite heruntergeladen haben.

- a. Wählen Sie **Durchsuchen**.
- b. Suchen und wählen Sie die Datei aus.

`hotfix-install-version`

- c. Wählen Sie **Offen**.

Die Datei wurde hochgeladen. Nach Abschluss des Uploads wird der Dateiname im Feld Details angezeigt.



Ändern Sie den Dateinamen nicht, da er Teil des Verifizierungsvorgangs ist.

5. Geben Sie die Provisionierungs-Passphrase in das Textfeld ein.

Die Schaltfläche **Start** wird aktiviert.

6. Wählen Sie **Start**.

Eine Warnung wird angezeigt, dass die Verbindung Ihres Browsers vorübergehend unterbrochen wird, da Dienste auf dem primären Admin-Knoten neu gestartet werden.

7. Wählen Sie **OK**, um mit der Anwendung des Hotfix auf den primären Admin-Knoten zu beginnen.

Wenn der Hotfix beginnt:

- a. Die Hotfix-Validierungen werden ausgeführt.



Wenn Fehler gemeldet werden, beheben Sie sie, laden Sie die Hotfix-Datei erneut hoch und wählen Sie erneut **Start** aus.

- b. Die Tabelle mit dem Hotfix-Installationsfortschritt wird angezeigt. Diese Tabelle zeigt alle Knoten in

Ihrem Raster und die aktuelle Phase der Hotfix-Installation für jeden Knoten. Die in der Tabelle aufgeführten Nodes sind nach Typ gruppiert:

- Admin-Nodes
- Gateway-Nodes
- Storage-Nodes
- Archiv-Nodes



Der Fortschrittsbalken erreicht den Abschluss, und dann wird der primäre Admin-Node zuerst mit der Phase „Complete“ angezeigt.

Hotfix Installation Progress

Approve All

Remove All

Admin Nodes - 1 out of 1 completed

Search

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191		Complete		

- Sortieren Sie die Listen der Knoten in jeder Gruppierung in aufsteigender oder absteigender Reihenfolge nach **Site**, **Name**, **Progress**, **Stage** oder **Details**. Oder geben Sie einen Begriff in das Feld **Suche** ein, um nach bestimmten Knoten zu suchen.
- Genehmigen Sie die Grid-Knoten, die aktualisiert werden können. Genehmigte Nodes desselben Typs werden nacheinander aktualisiert.



Genehmigen Sie den Hotfix nicht für einen Knoten, es sei denn, Sie sind sicher, dass der Knoten bereit ist, aktualisiert zu werden. Wenn das Hotfix auf einen Grid-Knoten angewendet wird, werden einige Dienste auf diesem Knoten möglicherweise neu gestartet. Diese Vorgänge können zu Serviceunterbrechungen für Clients führen, die mit dem Node kommunizieren.

- Wählen Sie eine oder mehrere **Genehmigen**-Schaltflächen, um einen oder mehrere einzelne Knoten zur Hotfix-Warteschlange hinzuzufügen.
- Wählen Sie in jeder Gruppierung die Schaltfläche **Alle genehmigen** aus, um alle Knoten desselben Typs der Hotfix-Warteschlange hinzuzufügen. Wenn Sie Suchkriterien im Feld **Suche** eingegeben haben, gilt die Schaltfläche **Alle genehmigen** für alle durch die Suchkriterien ausgewählten Knoten.



Die Schaltfläche **Alle genehmigen** oben auf der Seite genehmigt alle Knoten, die auf der Seite aufgeführt sind, während die Schaltfläche **Alle genehmigen** oben in einer Tabellengruppierung nur alle Knoten in dieser Gruppe genehmigt. Wenn die Reihenfolge, in der Knoten aktualisiert werden, wichtig ist, genehmigen Sie Knoten oder Gruppen von Knoten jeweils eins und warten Sie, bis das Upgrade auf jedem Knoten abgeschlossen ist, bevor Sie den nächsten Knoten genehmigen.

- Wählen Sie oben auf der Seite die Schaltfläche **Alle genehmigen** aus, um alle Knoten im Raster zur Hotfix-Warteschlange hinzuzufügen.



Sie müssen den StorageGRID-Hotfix abschließen, bevor Sie ein anderes Softwareupdate starten können. Wenn Sie den Hotfix nicht abschließen können, wenden Sie sich an den technischen Support.

- Wählen Sie **Entfernen** oder **Alle entfernen**, um einen Knoten oder alle Knoten aus der Hotfix-Warteschlange zu entfernen.

Wenn die Bühne über „Queued“ hinausgeht, wird die Schaltfläche **Entfernen** ausgeblendet und Sie können den Knoten nicht mehr aus dem Hotfix-Prozess entfernen.

Storage Nodes - 1 out of 9 completed						Approve All	Remove All
						Search	
Site	Name	Progress	Stage	Details	Action		
Raleigh	RAL-S1-101-196		Queued		Remove		
Raleigh	RAL-S2-101-197		Complete				
Raleigh	RAL-S3-101-198		Queued		Remove		
Sunnyvale	SVL-S1-101-199		Queued		Remove		
Sunnyvale	SVL-S2-101-93		Waiting for you to approve		Approve		
Sunnyvale	SVL-S3-101-94		Waiting for you to approve		Approve		
Vancouver	VTC-S1-101-193		Waiting for you to approve		Approve		
Vancouver	VTC-S2-101-194		Waiting for you to approve		Approve		
Vancouver	VTC-S3-101-195		Waiting for you to approve		Approve		

10. Warten Sie, bis der Hotfix auf jeden genehmigten Grid-Knoten angewendet wird.

Wenn der Hotfix erfolgreich auf allen Knoten installiert wurde, wird die Fortschrittsstabelle für die Hotfix-Installation geschlossen. Ein grünes Banner zeigt das Datum und die Uhrzeit an, zu der der Hotfix abgeschlossen wurde.

11. Wenn der Hotfix nicht auf alle Knoten angewendet werden konnte, überprüfen Sie den Fehler für jeden Knoten, beheben Sie das Problem und wiederholen Sie diese Schritte.

Der Vorgang ist erst abgeschlossen, wenn der Hotfix auf alle Knoten angewendet wurde. Sie können den Hotfix-Prozess so oft wie nötig wiederholen, bis er abgeschlossen ist.

Verwandte Informationen

[StorageGRID verwalten](#)

[Monitoring und Fehlerbehebung](#)

Verfahren zur Recovery von Grid-Nodes

Wenn ein Grid-Node ausfällt, können Sie ihn wiederherstellen, indem Sie den

fehlerhaften physischen oder virtuellen Server ersetzen, die StorageGRID Software neu installieren und wiederherstellbare Daten wiederherstellen.

Grid Nodes können ausfallen, wenn ein Hardware-, Virtualisierungs-, Betriebssystem- oder Softwarefehler den Node funktionsunfähig oder unzuverlässig macht. Es gibt viele Arten von Fehlern, die die Notwendigkeit zur Wiederherstellung eines Grid-Node auslösen können.

Die Schritte zur Wiederherstellung eines Grid-Node sind abhängig von der Plattform, auf der der Grid-Node gehostet wird, und vom Typ des Grid-Nodes. Jeder Grid-Node-Typ verfügt über eine bestimmte Recovery-Prozedur, die Sie genau befolgen müssen.

Im Allgemeinen versuchen Sie, soweit möglich Daten vom ausgefallenen Grid Node aufzubewahren, reparieren oder ersetzen den ausgefallenen Node, verwenden den Grid Manager zum Konfigurieren des Ersatz-Node und stellen die Daten des Node wieder her.



Wenn eine gesamte StorageGRID Site ausfällt, wenden Sie sich an den technischen Support. Der technische Support arbeitet mit Ihnen zusammen an der Entwicklung und Umsetzung eines Site Recovery-Plans, der die wiederherzustellenden Datenmenge maximiert und Ihre Geschäftsziele erreicht.

Verwandte Informationen

[Durchführen der Standortwiederherstellung durch den technischen Support](#)

Warnungen und Überlegungen für die Wiederherstellung von Grid Nodes

Wenn ein Grid-Node ausfällt, müssen Sie ihn so schnell wie möglich wiederherstellen. Bevor Sie beginnen, müssen Sie alle Warnungen und Überlegungen für die Node-Wiederherstellung prüfen.



StorageGRID ist ein verteiltes System, das aus mehreren Knoten besteht, die miteinander arbeiten. Verwenden Sie keine Festplattenschnappschüsse, um Grid-Knoten wiederherzustellen. Beachten Sie stattdessen die Recovery- und Wartungsabläufe für jeden Node-Typ.

Einige der Gründe für die baldige Wiederherstellung eines ausgefallenen Grid-Node sind:

- Ein ausgefallener Grid-Node verringert die Redundanz von System- und Objektdaten, sodass Sie anfällig für dauerhaften Datenverlust sind, wenn ein anderer Node ausfällt.
- Ein ausgefallener Grid-Node kann sich auf die Effizienz des täglichen-bis-täglichen Betriebs auswirken.
- Ein ausgefallener Grid-Node kann die Überwachung des Systembetriebs verringern.
- Ein ausgefallener Grid-Node kann zu einem internen Serverfehler von 500 führen, wenn strenge ILM-Regeln vorhanden sind.
- Wenn ein Grid-Node nicht sofort wiederhergestellt wird, kann es zu einer Zunahme der Recovery-Zeiten kommen. So können sich beispielsweise Warteschlangen entwickeln, die vor Abschluss der Wiederherstellung gelöscht werden müssen.

Befolgen Sie immer das Recovery-Verfahren für den spezifischen Typ des Grid-Node, den Sie wiederherstellen. Die Wiederherstellungsverfahren variieren für primäre oder nicht primäre Admin-Nodes, Gateway-Nodes, Archiv-Nodes, Appliance-Nodes und Storage-Nodes.

Voraussetzungen für die Wiederherstellung von Grid-Nodes

Bei der Wiederherstellung der Grid-Nodes werden alle folgenden Bedingungen vorausgesetzt:

- Die fehlerhafte physische oder virtuelle Hardware wurde ersetzt und konfiguriert.
- Die Version für das Installationsprogramm der StorageGRID Appliance auf der Ersatz-Appliance entspricht der Softwareversion Ihres StorageGRID Systems, wie in der Hardwareinstallation und -Wartung zum Überprüfen und Aktualisieren der Installationsversion der StorageGRID Appliance beschrieben.
 - [SG100- und SG1000-Services-Appliances](#)
 - [SG5600 Storage Appliances](#)
 - [SG5700 Storage-Appliances](#)
 - [SG6000 Storage-Appliances](#)
- Wenn Sie einen anderen Grid-Node als den primären Admin-Node wiederherstellen, besteht die Verbindung zwischen dem wiederherzustellenden Grid-Node und dem primären Admin-Node.

Reihenfolge der Knotenwiederherstellung, wenn ein Server, der mehr als einen Grid-Knoten hostet, ausfällt

Wenn ein Server, der mehr als einen Grid-Node hostet, ausfällt, können Sie die Knoten in beliebiger Reihenfolge wiederherstellen. Wenn der ausgefallene Server jedoch den primären Admin-Node hostet, müssen Sie diesen Knoten zuerst wiederherstellen. Die Wiederherstellung des primären Admin-Knotens verhindert, dass andere Knoten-Wiederherstellungen angehalten werden, während sie warten, bis der primäre Admin-Node kontaktiert wird.

IP-Adressen für wiederhergestellte Knoten

Versuchen Sie nicht, einen Node mithilfe einer IP-Adresse wiederherzustellen, die derzeit einem anderen Node zugewiesen ist. Wenn Sie den neuen Node implementieren, verwenden Sie die aktuelle IP-Adresse des ausgefallenen Nodes oder eine nicht genutzte IP-Adresse.

Wenn Sie für die Implementierung des neuen Knotens eine neue IP-Adresse verwenden und dann den Knoten wiederherstellen, wird die neue IP-Adresse für den wiederhergestellten Knoten weiterhin verwendet. Wenn Sie die ursprüngliche IP-Adresse wiederherstellen möchten, verwenden Sie nach Abschluss der Wiederherstellung das Tool IP ändern.

Sammeln der erforderlichen Materialien für die Grid Node Recovery

Bevor Sie Wartungsmaßnahmen durchführen, müssen Sie sicherstellen, dass die zur Wiederherstellung eines ausgefallenen Grid-Node erforderlichen Materialien vorhanden sind.

Element	Hinweise
StorageGRID Installationsarchiv	Wenn Sie einen Grid-Node wiederherstellen müssen, müssen Sie dies tun Laden Sie die Installationsdateien von StorageGRID herunter Für Ihre Plattform. Hinweis: Sie müssen keine Dateien herunterladen, wenn Sie fehlgeschlagene Speichervolumen auf einem Speicherknoten wiederherstellen.

Element	Hinweise
Service-Laptop	Der Service-Laptop muss Folgendes haben: • Netzwerkport • SSH-Client (z. B. PuTTY) • Unterstützter Webbrowser
Wiederherstellungspaket .zip Datei	Erhalten Sie eine Kopie des aktuellsten Wiederherstellungspakets .zip Datei: <code>sgws-recovery-package-id-revision.zip</code> Der Inhalt des .zip Die Datei wird jedes Mal aktualisiert, wenn das System geändert wird. Sie werden aufgefordert, die aktuellste Version des Wiederherstellungspakets nach dem Speichern dieser Änderungen an einem sicheren Ort zu speichern. Verwenden Sie die neueste Kopie, um nach Grid-Ausfällen eine Wiederherstellung durchzuführen. Wenn der primäre Admin-Node normal funktioniert, können Sie das Wiederherstellungspaket aus dem Grid Manager herunterladen. Wählen Sie WARTUNG System Wiederherstellungspaket. Wenn Sie nicht auf den Grid Manager zugreifen können, können Sie auf einigen Speicherknoten, die den ADC-Dienst enthalten, verschlüsselte Kopien des Wiederherstellungspakets finden. Untersuchen Sie auf jedem Speicherknoten diesen Speicherort für das Wiederherstellungspaket: <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Verwenden Sie das Wiederherstellungspaket mit der höchsten Versionsnummer.
Passwords.txt Datei	Enthält die Passwörter, die für den Zugriff auf Grid-Nodes in der Befehlszeile erforderlich sind. Im Wiederherstellungspaket enthalten.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im Passwords.txt Datei:
Aktuelle Dokumentation für Ihre Plattform	Dokumentation finden Sie auf der Website des Plattformanbieters. Informationen zu den derzeit unterstützten Versionen Ihrer Plattform finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Laden Sie StorageGRID-Installationsdateien herunter und extrahieren Sie sie

Laden Sie die Software herunter und extrahieren Sie die Dateien, sofern Sie nicht sind [Wiederherstellen ausgefallener Speicher-Volumes auf einem Storage-Node](#).

Sie müssen die Version von StorageGRID verwenden, die derzeit im Raster ausgeführt wird.

Schritte

1. Bestimmen Sie, welche Version der Software derzeit installiert ist. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **über** aus.

2. Wechseln Sie zum ["NetApp Download-Seite für StorageGRID"](#).
3. Wählen Sie die Version von StorageGRID aus, die derzeit im Grid ausgeführt wird.

Die StorageGRID-Softwareversionen haben dieses Format: 11.x.y.

4. Melden Sie sich mit Ihrem Benutzernamen und Passwort für Ihr NetApp Konto an.
5. Lesen Sie die Endbenutzer-Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen und wählen Sie dann **Weiter akzeptieren**.
6. Wählen Sie in der Spalte **Install StorageGRID** der Download-Seite die aus .tgz Oder .zip Datei für Ihre Plattform.

Die in der Archivdatei der Installation angezeigte Version muss mit der Version der derzeit installierten Software übereinstimmen.

Verwenden Sie die .zip Datei, wenn Sie Windows ausführen.

Plattform	Installationsarchiv
Red hat Enterprise Linux oder CentOS	StorageGRID-Webscale-version-RPM-uniqueID.zip
	StorageGRID-Webscale-version-RPM-uniqueID.tgz
Ubuntu oder Debian oder Appliances	StorageGRID-Webscale-version-DEB-uniqueID.zip
	StorageGRID-Webscale-version-DEB-uniqueID.tgz
VMware	StorageGRID-Webscale-version-VMware-uniqueID.zip
	StorageGRID-Webscale-version-VMware-uniqueID.tgz

7. Laden Sie die Archivdatei herunter und extrahieren Sie sie.
8. Befolgen Sie den entsprechenden Schritt für Ihre Plattform und wählen Sie die Dateien aus, die Sie benötigen, basierend auf Ihrer Plattform und den Grid-Nodes, die Sie wiederherstellen müssen.

Die im Schritt für jede Plattform aufgeführten Pfade beziehen sich auf das von der Archivdatei installierte Verzeichnis auf der obersten Ebene.

9. Wenn Sie ein wiederherstellen [Red hat Enterprise Linux oder CentOS System](#), Wählen Sie die entsprechenden Dateien.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.

Pfad und Dateiname	Beschreibung
	RPM Paket für die Installation der StorageGRID Node Images auf Ihren RHEL- oder CentOS-Hosts.
	RPM Paket für die Installation des StorageGRID Host Service auf Ihren RHEL- oder CentOS-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel für die Ansible-Rolle und das Playbook zur Konfiguration von RHEL- oder CentOS-Hosts für die Implementierung von StorageGRID Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie mit diesen Schemas bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung zum Testen der Upgrade-Kompatibilität besitzen.

1. Wenn Sie ein wiederherstellen [Ubuntu oder Debian-System](#), Wählen Sie die entsprechenden Dateien.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.

Pfad und Dateiname	Beschreibung
	Eine NetApp Lizenzdatei, die nicht in der Produktionsumgebung enthalten ist und für Tests und Proof of Concept-Implementierungen genutzt werden kann
	DEB-Paket zum Installieren der StorageGRID-Knoten-Images auf Ubuntu oder Debian-Hosts.
	MD5-Prüfsumme für die Datei /debs/storagegrid-webscale-images-version-SHA.deb.
	DEB-Paket zur Installation des StorageGRID-Hostdienstes auf Ubuntu oder Debian-Hosts.
Tool zur Implementierung von Skripten	Beschreibung
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Beispiel-Rolle und Playbook für Ansible zur Konfiguration von Ubuntu oder Debian-Hosts für die Implementierung von StorageGRID-Containern Die Rolle oder das Playbook können Sie nach Bedarf anpassen.

Pfad und Dateiname	Beschreibung
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie mit diesen Schemas bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung zum Testen der Upgrade-Kompatibilität besitzen.

1. Wenn Sie ein wiederherstellen [VMware System](#), Wählen Sie die entsprechenden Dateien.

Pfad und Dateiname	Beschreibung
	Eine Textdatei, die alle in der StorageGRID-Download-Datei enthaltenen Dateien beschreibt.
	Eine kostenlose Lizenz, die keinen Support-Anspruch auf das Produkt bietet.
	Die Festplattendatei für Virtual Machines, die als Vorlage für die Erstellung von Grid-Node-Virtual Machines verwendet wird.
	Die Vorlagendatei „Open Virtualization Format“ (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung des primären Admin-Knotens.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von nicht-primären Admin-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Archiv-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Für die Bereitstellung von Gateway-Knoten.
	Die Vorlagendatei (.ovf) Und Manifest-Datei (.mf) Zur Bereitstellung von virtuellen Maschinen-basierten Speicherknoten.
Tool zur Implementierung von Skripten	Beschreibung

Pfad und Dateiname	Beschreibung
	Ein Bash Shell-Skript, das zur Automatisierung der Implementierung virtueller Grid-Nodes verwendet wird.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>deploy-vsphere-ovftool.sh</code> Skript:
	Ein Python-Skript zur Automatisierung der Konfiguration eines StorageGRID Systems.
	Ein Python-Skript zur Automatisierung der Konfiguration von StorageGRID Appliances
	Ein Beispiel-Python-Skript, mit dem Sie sich bei aktivierter Single-Sign-On-Funktion bei der Grid-Management-API anmelden können.
	Eine Beispielkonfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	Eine leere Konfigurationsdatei für die Verwendung mit dem <code>configure-storagegrid.py</code> Skript:
	API-Schemata für StorageGRID: Hinweis: Bevor Sie ein Upgrade durchführen, können Sie mit diesen Schemas bestätigen, dass jeder Code, den Sie zur Verwendung von StorageGRID Management APIs geschrieben haben, mit der neuen StorageGRID-Version kompatibel ist, wenn Sie keine StorageGRID-Umgebung außerhalb der Produktionsumgebung zum Testen der Upgrade-Kompatibilität besitzen.

1. Wenn Sie ein Appliance-basiertes StorageGRID-System wiederherstellen, wählen Sie die entsprechenden Dateien aus.

Pfad und Dateiname	Beschreibung
	DEB-Paket zum Installieren der StorageGRID Node Images auf den Geräten.
	Prüfsumme des DEB-Installationspakets, das vom Installationsprogramm der StorageGRID-Appliance verwendet wird, um zu überprüfen, ob das Paket nach dem Hochladen intakt ist.



Für die Installation der Appliance sind diese Dateien nur erforderlich, wenn Sie den Netzwerkverkehr vermeiden müssen. Die Appliance kann die erforderlichen Dateien vom primären Admin-Knoten herunterladen.

Wählen Sie die Knotenwiederherstellung aus

Sie müssen den korrekten Wiederherstellungsvorgang für den Typ des fehlgeschlagenen Knotens auswählen.

Grid-Node	Wiederherstellungsvorgang
Mehr als ein Storage-Node	Wenden Sie sich an den technischen Support. Wenn mehrere Storage-Nodes ausgefallen sind, muss der technische Support bei der Recovery Unterstützung leisten, um Inkonsistenzen zu Datenbanken zu vermeiden, die zu Datenverlusten führen können. Möglicherweise ist ein Wiederherstellungsverfahren für Standorte erforderlich. Durchführen der Standortwiederherstellung durch den technischen Support
Ein einzelner Storage-Node	Das Speicherknoten-Wiederherstellungsverfahren hängt vom Typ und der Dauer des Ausfalls ab. Wiederherstellung nach Ausfällen der Storage-Nodes
Admin-Node	Das Verfahren Admin-Knoten hängt davon ab, ob Sie den primären Admin-Knoten oder einen nicht-primären Admin-Knoten wiederherstellen müssen. Wiederherstellung bei Ausfällen des Admin-Nodes
Gateway-Node	Wiederherstellung nach Gateway-Node-Ausfällen.
Archiv-Node	Wiederherstellung nach Ausfällen des Archivierungs-Nodes.



Wenn ein Server, der mehr als einen Grid-Node hostet, ausfällt, können Sie die Knoten in beliebiger Reihenfolge wiederherstellen. Wenn der ausgefallene Server jedoch den primären Admin-Node hostet, müssen Sie diesen Knoten zuerst wiederherstellen. Die Wiederherstellung des primären Admin-Knotens verhindert, dass andere Knoten-Wiederherstellungen angehalten werden, während sie warten, bis der primäre Admin-Node kontaktiert wird.

Wiederherstellung nach Ausfällen der Storage-Nodes

Das Verfahren zur Wiederherstellung eines fehlgeschlagenen Speicherknoten hängt von der Art des Fehlers und dem Typ des fehlgeschlagenen Speicherknoten ab.

Verwenden Sie diese Tabelle, um das Wiederherstellungsverfahren für einen fehlgeschlagenen Speicherknoten auszuwählen.

Problem	Aktion	Hinweise
• Mehr als ein Speicherknoten ist ausgefallen. • Ein zweiter Speicherknoten ist weniger als 15 Tage nach Ausfall oder Wiederherstellung eines Speicherknotens ausgefallen. Dies schließt den Fall ein, dass ein Speicherknoten während der Wiederherstellung eines anderen Speicherknoten noch in Arbeit ist.	Wenden Sie sich an den technischen Support.	Wenn sich alle ausgefallenen Speicherknoten am selben Standort befinden, ist es möglicherweise erforderlich, ein Verfahren zur Standortwiederherstellung durchzuführen. Der technische Support prüft Ihre Situation und erstellt einen Recovery-Plan. Durchführen der Standortwiederherstellung durch den technischen Support Die Wiederherstellung von mehr als einem Storage-Node (oder mehr als einem Storage-Node innerhalb von 15 Tagen) kann die Integrität der Cassandra-Datenbank beeinträchtigen, was zu Datenverlust führen kann. Der technische Support kann bestimmen, wann die Wiederherstellung eines zweiten Storage Node sicher gestartet werden kann. Hinweis: Wenn mehr als ein Speicherknoten, der den ADC-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattfordienstanfragen für diesen Standort.
Ein Speicherknoten ist seit mehr als 15 Tagen offline.	Stellen Sie Storage Node länger als 15 Tage wieder her	Dieses Verfahren ist erforderlich, um die Integrität der Cassandra-Datenbank sicherzustellen.
Ein Appliance-Speicherknoten ist fehlgeschlagen.	Appliance Storage Node wiederherstellen	Das Wiederherstellungsverfahren für Appliance Storage Nodes ist bei allen Ausfällen gleich.
Ein oder mehrere Storage-Volumes sind ausgefallen, das Systemlaufwerk ist jedoch intakt	Wiederherstellung nach einem Storage-Volume-Ausfall bei intaktem Systemlaufwerk	Dieses Verfahren wird für softwarebasierte Speicherknoten verwendet.

Problem	Aktion	Hinweise
Das Systemlaufwerk ist ausgefallen.	Wiederherstellung nach einem Laufwerksausfall	Das Verfahren zum Austausch der Nodes hängt von der Implementierungsplattform ab und ob auch Storage Volumes ausgefallen sind.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die “reaper” oder “Cassandra Reparatur erwähnt.” Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

Stellen Sie Storage Node länger als 15 Tage wieder her

Wenn ein einzelner Storage-Node länger als 15 Tage offline war und nicht mit anderen Storage-Nodes verbunden ist, müssen Sie Cassandra auf dem Node neu aufbauen.

Was Sie benötigen

- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Dekommission.**)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Erweiterung.**)

Über diese Aufgabe

Storage-Nodes verfügen über eine Cassandra Datenbank mit Objekt-Metadaten. Wenn ein Storage-Node seit mehr als 15 Tagen nicht mit anderen Storage-Nodes kommunizieren kann, geht StorageGRID davon aus, dass die Cassandra-Datenbank des Node veraltet ist. Der Storage-Node kann erst wieder dem Grid beitreten, wenn Cassandra mithilfe von Informationen anderer Storage-Nodes neu erstellt wurde.

Verwenden Sie dieses Verfahren, um Cassandra nur dann neu aufzubauen, wenn ein einzelner Storage-Node ausfällt. Wenden Sie sich an den technischen Support, wenn weitere Storage-Nodes offline sind oder wenn Cassandra innerhalb der letzten 15 Tage auf einem anderen Storage-Node neu erstellt wurde. Dazu gehört beispielsweise das Verfahren zur Wiederherstellung ausgefallener Storage-Volumes oder zur Wiederherstellung eines ausgefallenen Storage-Nodes.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie den folgenden Wiederherstellungsvorgang nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Führen Sie den folgenden Wiederherstellungsvorgang nicht durch. Es kann zu Datenverlusten kommen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Wenden Sie sich an den technischen Support.

Durchführen der Standortwiederherstellung durch den technischen Support

Schritte

1. Schalten Sie ggf. den Storage-Node ein, der wiederhergestellt werden muss.
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 `#`.+



Wenn Sie sich beim Grid-Node nicht anmelden können, ist die Systemfestplatte möglicherweise nicht intakt. Gehen Sie zum Verfahren für [Wiederherstellung nach einem Systemausfall](#).

1. Führen Sie die folgenden Prüfungen auf dem Speicherknoten durch:
 - a. Geben Sie diesen Befehl ein: `nodetool status`

Die Ausgabe sollte sein `Connection refused`
 - b. Wählen Sie im Grid Manager **SUPPORT Tools Grid-Topologie** aus.
 - c. Wählen Sie **Site Storage Node SSM Services** aus. Vergewissern Sie sich, dass der Cassandra-Service angezeigt wird `Not Running`.
 - d. Wählen Sie **Storage Node SSM Ressourcen**. Vergewissern Sie sich, dass im Abschnitt Volumes kein Fehlerstatus vorhanden ist.
 - e. Geben Sie diesen Befehl ein: `grep -i Cassandra /var/local/log/servermanager.log`

Die folgende Meldung sollte in der Ausgabe angezeigt werden:

```
Cassandra not started because it has been offline for more than 15 day  
grace period - rebuild Cassandra
```

2. Geben Sie diesen Befehl ein, und überwachen Sie die Skriptaussgabe: `check-cassandra-rebuild`
 - Wenn Speicherservices ausgeführt werden, werden Sie aufgefordert, diese zu beenden. Geben Sie ein: **Y**
 - Überprüfen Sie die Warnungen im Skript. Wenn keine dieser Möglichkeiten gelten, bestätigen Sie, dass Sie Cassandra neu aufbauen möchten. Geben Sie ein: **Y**



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die “reaper” oder “Cassandra Reparatur erwähnt.” Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

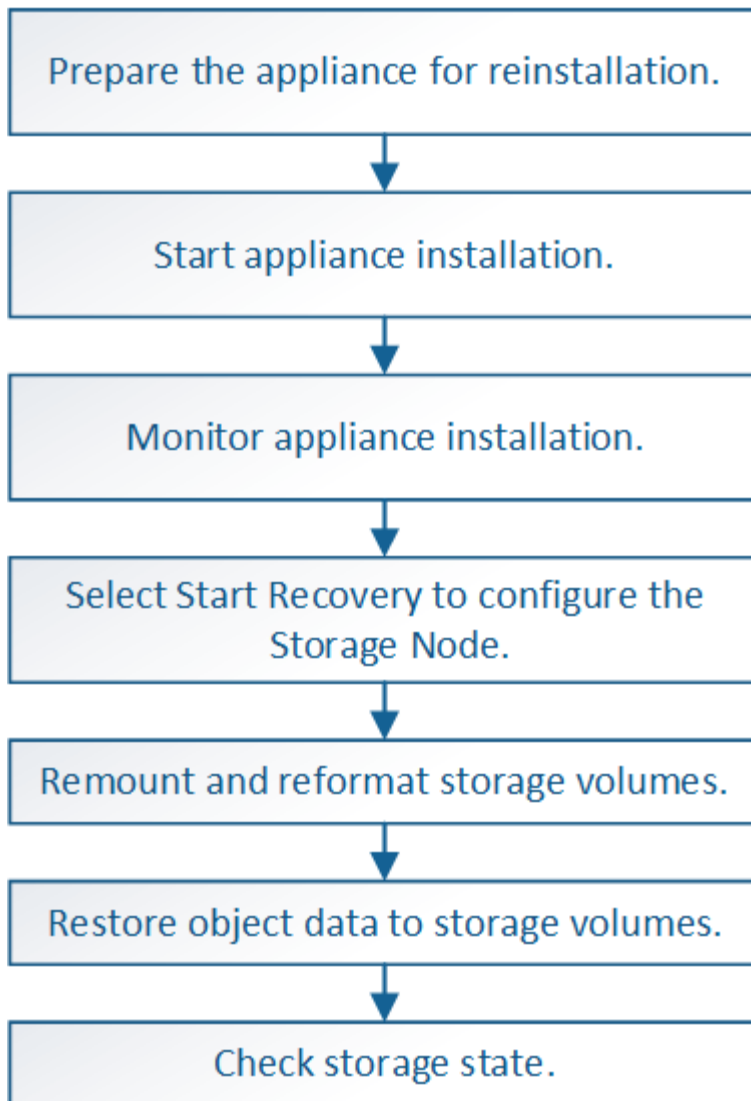
3. Führen Sie nach Abschluss der Neuerstellung die folgenden Prüfungen durch:
 - a. Wählen Sie im Grid Manager **SUPPORT Tools Grid-Topologie** aus.
 - b. Wählen Sie **Site wiederhergestellte Speicherknoten SSM Services** aus.
 - c. Vergewissern Sie sich, dass alle Dienste ausgeführt werden.
 - d. Wählen Sie **DDS Data Store**.
 - e. Bestätigen Sie, dass der **Data Store Status** „up“ und der **Data Store State** „normal“ lautet.

Appliance Storage Node wiederherstellen

Das Verfahren zur Wiederherstellung eines fehlerhaften StorageGRID-Appliance-Speicherknoten ist dieselbe, egal ob Sie eine Wiederherstellung nach dem Verlust des Systemlaufwerks oder nach dem Verlust von Storage-Volumes durchführen.

Über diese Aufgabe

Sie müssen die Appliance vorbereiten und Software neu installieren, den Node so konfigurieren, dass er wieder in das Grid eingespeist wird, Speicher neu formatiert und Objektdaten wiederhergestellt werden.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie den folgenden Wiederherstellungsvorgang nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen kann zu Datenverlust führen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Wenden Sie sich an den technischen Support.

Durchführen der Standortwiederherstellung durch den technischen Support



Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und sich die Kopie auf einem ausgefallenen Storage Volume befindet, können Sie das Objekt nicht wiederherstellen.



Wenn während der Wiederherstellung ein Alarm „Service: Status – Cassandra (SVST)“ (Service: Status – Cassandra) ausgegeben wird, lesen Sie die Überwachungs- und Fehlerbehebungsanweisungen zur Wiederherstellung des Alarms durch Neuaufbau von Cassandra. Nach dem Wiederaufbau von Cassandra sollten die Alarme gelöscht werden. Wenn die Alarme nicht gelöscht werden, wenden Sie sich an den technischen Support.



Informationen zu Hardware-Wartungsarbeiten, wie z. B. Anweisungen zum Austausch eines Controllers oder zur Neuinstallation von SANtricity OS, finden Sie in der Installations- und Wartungsanleitung für Ihre Storage Appliance.

Verwandte Informationen

[Monitoring und Fehlerbehebung](#)

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[SG5600 Storage Appliances](#)

Appliance-Speicherknoten für die Neuinstallation vorbereiten

Wenn Sie einen Appliance-Speicherknoten wiederherstellen, müssen Sie zuerst die Appliance für die Neuinstallation der StorageGRID-Software vorbereiten.

1. Melden Sie sich beim fehlgeschlagenen Speicherknoten 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 `#`.

2. Bereiten Sie den Appliance-Speicherknoten für die Installation der StorageGRID-Software vor.
`sgareinstall`
3. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie Folgendes ein: `y`

Die Appliance wird neu gestartet, und Ihre SSH-Sitzung wird beendet. In der Regel dauert es etwa 5 Minuten, bis das Installationsprogramm für StorageGRID-Appliances verfügbar ist, obwohl in einigen Fällen Sie möglicherweise bis zu 30 Minuten warten müssen.

Der Speicherknoten der StorageGRID-Appliance wird zurückgesetzt, und die Daten auf dem Speicherknoten sind nicht mehr zugänglich. Die während der ursprünglichen Installation konfigurierten IP-Adressen sollten intakt bleiben. Nach Abschluss des Vorgangs wird jedoch empfohlen, dies zu bestätigen.

Nach Ausführung des `sgareinstall` Der Befehl entfernt alle über StorageGRID bereitgestellten Konten, Passwörter und SSH-Schlüssel und generiert neue Host-Schlüssel.

Starten Sie die Installation der StorageGRID Appliance

Um StorageGRID auf einem Appliance-Speicherknoten zu installieren, verwenden Sie das StorageGRID-Appliance-Installationsprogramm, das in der Appliance enthalten ist.

Was Sie benötigen

- Die Appliance wurde in einem Rack installiert, mit Ihren Netzwerken verbunden und eingeschaltet.
- Mithilfe des StorageGRID Appliance Installer wurden Netzwerkverbindungen und IP-Adressen für die Appliance konfiguriert.
- Sie kennen die IP-Adresse des primären Admin-Knotens für das StorageGRID-Raster.
- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, wurden in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert.
- Sie haben diese erforderlichen Aufgaben gemäß den Installations- und Wartungsanweisungen für Ihre Storage Appliance ausgeführt:
 - [SG5600 Storage Appliances](#)
 - [SG5700 Storage-Appliances](#)
 - [SG6000 Storage-Appliances](#)
- Sie verwenden ein [Unterstützter Webbrowser](#).
- Sie kennen eine der IP-Adressen, die dem Computing-Controller in der Appliance zugewiesen sind. Sie können die IP-Adresse für das Admin-Netzwerk (Management-Port 1 auf dem Controller), das Grid-Netzwerk oder das Client-Netzwerk verwenden.

Über diese Aufgabe

Sie installieren Sie StorageGRID auf einem Appliance-Speicherknoten:

- Sie geben die IP-Adresse des primären Admin-Knotens und den Namen des Knotens an oder bestätigen sie.
- Sie starten die Installation und warten, bis Volumes konfiguriert und die Software installiert ist.
- Durch den Prozess partway, die Installation pausiert. Um die Installation fortzusetzen, müssen Sie sich beim Grid Manager anmelden und den ausstehenden Speicherknoten als Ersatz für den ausgefallenen Node konfigurieren.
- Nachdem Sie den Node konfiguriert haben, wird die Installation der Appliance abgeschlossen und die Appliance wird neu gestartet.

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für den Compute-Controller in der Appliance ein.

```
https://Controller_IP:8443
```

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Legen Sie im Abschnitt primäre Administratorknoten-Verbindung fest, ob Sie die IP-Adresse für den primären Admin-Node angeben müssen.

Das Installationsprogramm der StorageGRID-Appliance kann diese IP-Adresse automatisch erkennen, wenn der primäre Admin-Node oder mindestens ein anderer Grid-Node mit Admin_IP konfiguriert ist, sich im selben Subnetz befindet.

3. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Schritte
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen Admin Node Discovery aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.
Automatische Erkennung aller verbundenen primären Admin-Nodes	a. Aktivieren Sie das Kontrollkästchen Admin Node Discovery aktivieren. b. Wählen Sie aus der Liste der ermittelten IP-Adressen den primären Admin-Node für das Grid aus, in dem dieser Appliance-Speicher-Node bereitgestellt wird. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.

4. Geben Sie im Feld **Knotenname** den gleichen Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.
5. Bestätigen Sie im Abschnitt Installation, dass der aktuelle Status „bereit zum Starten der Installation des Knotennamens in das Grid mit Primary Admin Node admin_ip“ lautet und dass die Schaltfläche **Installation starten** aktiviert ist.

Wenn die Schaltfläche **Installation starten** nicht aktiviert ist, müssen Sie möglicherweise die Netzwerkkonfiguration oder die Porteinstellungen ändern. Anweisungen hierzu finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

6. Klicken Sie auf der Startseite des StorageGRID-Appliance-Installationsprogramms auf **Installation starten**.

NetApp® StorageGRID® Appliance Installer

[Home](#)[Configure Networking ▾](#)[Configure Hardware ▾](#)[Monitor Installation](#)[Advanced ▾](#)

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node
discovery ☐

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

Cancel

Save

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**.

Verwandte Informationen

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

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

Überwachen Sie die Installation der StorageGRID Appliance

Das Installationsprogramm der StorageGRID Appliance stellt den Status bereit, bis die Installation abgeschlossen ist. Nach Abschluss der Softwareinstallation wird die Appliance neu gestartet.

1. Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	
2. Install OS			Pending
3. Install StorageGRID			Pending
4. Finalize installation			Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt wurden, nicht erneut ausgeführt werden. Wenn Sie eine Installation erneut ausführen, werden alle Aufgaben, die nicht erneut ausgeführt werden müssen, mit einer grünen Statusleiste und dem Status „Skipped.“ angezeigt.

2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

- **1. Speicher konfigurieren**

In dieser Phase stellt das Installationsprogramm eine Verbindung zum Storage Controller her, löscht jede vorhandene Konfiguration, kommuniziert mit der SANtricity Software, um Volumes zu konfigurieren und die Host-Einstellungen zu konfigurieren.

- **2. Installieren Sie das Betriebssystem**

In dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID auf die Appliance.

3. Überwachen Sie den Installationsfortschritt weiter, bis die Phase **StorageGRID installieren** angehalten wird. Auf der eingebetteten Konsole wird eine Meldung angezeigt, in der Sie aufgefordert werden, diesen Knoten auf dem Admin-Knoten mithilfe des Grid-Managers zu genehmigen.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

4. Gehen Sie zum Verfahren zum Konfigurieren des Appliance-Speicherknoten.

Wählen Sie Wiederherstellung starten, um Appliance Storage Node zu konfigurieren

Sie müssen im Grid Manager die Option Wiederherstellung starten auswählen, um einen Appliance-Speicherknoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Was Sie benötigen

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

- Sie müssen einen Speicher-Node für die Wiederherstellungsanwendung bereitgestellt haben.
- Sie müssen das Startdatum aller Reparaturaufträge für Daten mit Löschungscode kennen.
- Sie müssen überprüft haben, dass der Speicherknoten innerhalb der letzten 15 Tage nicht neu aufgebaut wurde.

Schritte

1. Wählen Sie im Grid Manager die Option **WARTUNG Tasks Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search Q				
Name	IPv4 Address	State	Recoverable	
104-217-S1	10.96.104.217	Unknown	✓	

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.

Wenn der Grid-Knoten die Stufe „Warten auf manuelle Schritte“ erreicht, gehen Sie zum nächsten Thema und führen Sie die manuellen Schritte durch, um Appliance-Storage-Volumes neu zu mounten und neu zu formatieren.



An jedem Punkt während der Wiederherstellung können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Appliance-Knoten durch Ausführen auf einen vorinstallierten Status wiederherstellen `sgareinstall` Auf dem Node.

Speicher-Volumes für Geräte neu mounten und neu formatieren („Manuelle Schritte“)

Führen Sie manuell zwei Skripte aus, um noch intakte Storage-Volumes neu mounten und ausgefallene Storage Volumes neu formatieren zu können. Das erste Skript bindet Volumes wieder ein, die ordnungsgemäß als StorageGRID-Storage-Volumes formatiert sind. Das zweite Skript formatiert alle nicht abgehängt Volumes neu, stellt die Cassandra-Datenbank bei Bedarf wieder her und startet Services.

Was Sie benötigen

- Sie haben bereits die Hardware für alle ausgefallenen Storage Volumes ausgetauscht, die ausgetauscht werden müssen.

Ausführen des `sn-remount-volumes` Skript kann Ihnen helfen, zusätzliche ausgefallene Storage-Volumes zu identifizieren.

- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Dekommission.**)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Erweiterung.**)



Wenden Sie sich an den technischen Support, wenn mehr als ein Speicherknoten offline ist oder wenn ein Speicherknoten in diesem Grid in den letzten 15 Tagen neu aufgebaut wurde. Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript: Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen voneinander kann zu Datenverlust führen.

Über diese Aufgabe

Zum Abschluss dieses Vorgangs führen Sie die folgenden grundlegenden Aufgaben aus:

- Melden Sie sich beim wiederhergestellten Speicherknoten an.
- Führen Sie die aus `sn-remount-volumes` Skript zum Neumounten ordnungsgemäß formatierter Speicher-Volumes. Wenn dieses Skript ausgeführt wird, führt es Folgendes aus:
 - Hängt jedes Storage-Volume an und ab, um das XFS-Journal wiederzugeben.
 - Führt eine Konsistenzprüfung der XFS-Datei durch.
 - Wenn das Dateisystem konsistent ist, bestimmt, ob das Storage Volume ein ordnungsgemäß formatiertes StorageGRID Storage Volume ist.
 - Wenn das Storage Volume ordnungsgemäß formatiert ist, wird das Storage-Volume wieder gemountet. Alle bestehenden Daten auf dem Volume bleiben erhalten.
- Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.
- Führen Sie die aus `sn-recovery-postinstall.sh` Skript: Wenn dieses Skript ausgeführt wird, führt es Folgendes aus.



Starten Sie einen Speicherknoten während der Wiederherstellung nicht neu, bevor Sie ausführen `sn-recovery-postinstall.sh` (Schritt 4) zum Neuformatieren der ausgefallenen Storage Volumes und zum Wiederherstellen von Objekt-Metadaten. Vor dem Neubooten des Speicherknoten `sn-recovery-postinstall.sh` Durch das Abschließen werden Fehler bei Diensten verursacht, die zu starten versuchen, und die Knoten der StorageGRID-Appliance den Wartungsmodus beenden.

- Umformatiert alle Storage-Volumes, die von der `sn-remount-volumes` Das Skript konnte nicht gemountet werden oder es wurde festgestellt, dass es nicht ordnungsgemäß formatiert wurde.



Wenn ein Speicher-Volume neu formatiert wird, gehen alle Daten auf diesem Volume verloren. Sie müssen ein zusätzliches Verfahren durchführen, um Objektdaten von anderen Standorten im Grid wiederherzustellen, vorausgesetzt, dass ILM-Regeln für die Speicherung von mehr als einer Objektkopie konfiguriert wurden.

- Stellt die Cassandra-Datenbank bei Bedarf auf dem Node wieder her.
- Startet die Dienste auf dem Speicherknoten.

Schritte

1. Melden Sie sich beim wiederhergestellten Speicherknoten 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 `#`.

2. Führen Sie das erste Skript aus, um alle ordnungsgemäß formatierten Speicher-Volumes neu zu mounten.



Wenn alle Speicher-Volumes neu sind und formatiert werden müssen, oder wenn alle Speicher-Volumes ausgefallen sind, können Sie diesen Schritt überspringen und das zweite Skript ausführen, um alle nicht abgehängt Speicher-Volumes neu zu formatieren.

- a. Führen Sie das Skript aus: `sn-remount-volumes`

Dieses Skript kann Stunden dauern, bis es auf Storage-Volumes ausgeführt wird, die Daten enthalten.

- b. Überprüfen Sie die Ausgabe, während das Skript ausgeführt wird, und beantworten Sie alle Eingabeaufforderungen.



Nach Bedarf können Sie die verwenden `tail -f` Befehl zum Überwachen des Inhalts der Protokolldatei des Skripts (`/var/local/log/sn-remount-volumes.log`). Die Protokolldatei enthält ausführlichere Informationen als die Befehlsausgabe der Befehlszeile.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.
```

```

===== Device /dev/sdd =====
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sde =====
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

```

In der Beispielausgabe wurde ein Storage-Volume erfolgreich neu eingebunden und drei Storage-Volumes wiesen Fehler auf.

- /dev/sdb Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und hatte eine gültige Volume-Struktur, so dass es erfolgreich neu eingebunden wurde. Daten auf Geräten, die vom Skript neu eingebunden werden, bleiben erhalten.
- /dev/sdc Die Konsistenzprüfung des XFS-Dateisystems ist fehlgeschlagen, da das Speichervolume neu oder beschädigt war.

- `/dev/sdd` Konnte nicht gemountet werden, da die Festplatte nicht initialisiert wurde oder der Superblock der Festplatte beschädigt war. Wenn das Skript kein Speicher-Volume mounten kann, wird gefragt, ob Sie die Konsistenzprüfung des Dateisystems ausführen möchten.
 - Wenn das Speichervolumen an eine neue Festplatte angeschlossen ist, beantworten Sie **N** mit der Eingabeaufforderung. Sie müssen das Dateisystem auf einer neuen Festplatte nicht überprüfen.
 - Wenn das Speichervolumen an eine vorhandene Festplatte angeschlossen ist, beantworten Sie **Y** mit der Eingabeaufforderung. Sie können die Ergebnisse der Dateisystemüberprüfung verwenden, um die Quelle der Beschädigung zu bestimmen. Die Ergebnisse werden im gespeichert `/var/local/log/sn-remount-volumes.log` Protokolldatei.
- `/dev/sde` Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und eine gültige Volume-Struktur hatte; die LDR-Knoten-ID befindet sich jedoch im `valid` Die Datei stimmt nicht mit der ID für diesen Speicher-knoten überein (der `configured LDR noid` Oben angezeigt). Diese Meldung gibt an, dass dieses Volume zu einem anderen Speicher-knoten gehört.

3. Prüfen Sie die Skriptaussgabe und beheben Sie etwaige Probleme.



Wenn ein Speichervolume die Konsistenzprüfung des XFS-Dateisystems fehlgeschlagen ist oder nicht gemountet werden konnte, überprüfen Sie sorgfältig die Fehlermeldungen in der Ausgabe. Sie müssen die Auswirkungen der Ausführung des verstehen `sn-recovery-postinstall.sh` Skript auf diesen Volumen.

- Überprüfen Sie, ob die Ergebnisse einen Eintrag für alle Volumes enthalten, die Sie erwartet haben. Wenn keine Volumes aufgeführt sind, führen Sie das Skript erneut aus.
- Überprüfen Sie die Meldungen für alle angeschlossenen Geräte. Stellen Sie sicher, dass keine Fehler vorliegen, die darauf hinweisen, dass ein Speichervolume nicht zu diesem Speicher-knoten gehört.

Im Beispiel enthält die Ausgabe für `/dev/sde` die folgende Fehlermeldung:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Wenn ein Storage-Volume gemeldet wird, das zu einem anderen Storage Node gehört, wenden Sie sich an den technischen Support. Wenn Sie den ausführen `sn-recovery-postinstall.sh` Skript: Das Speichervolumen wird neu formatiert, was zu Datenverlust führen kann.

- Wenn keine Speichergeräte montiert werden konnten, notieren Sie sich den Gerätenamen und reparieren oder ersetzen Sie das Gerät.



Sie müssen Speichergeräte reparieren oder ersetzen, die nicht montiert werden können.

Sie verwenden den Gerätenamen, um die Volume-ID zu suchen. Dies ist erforderlich, wenn Sie den ausführen `repair-data` Skript zum Wiederherstellen von Objektdaten auf dem Volume (beim nächsten Verfahren).

- Führen Sie nach der Reparatur oder dem Austausch aller nicht montierbaren Geräte den aus `sn-remount-volumes` Skript erneut, um zu bestätigen, dass alle Speicher-Volumes, die neu gemountet werden können, neu eingebunden wurden.



Wenn ein Speicher-Volume nicht angehängt oder nicht ordnungsgemäß formatiert werden kann, und Sie mit dem nächsten Schritt fortfahren, werden das Volume und alle Daten auf dem Volume gelöscht. Falls Sie zwei Kopien von Objektdaten hatten, ist nur eine einzige Kopie verfügbar, bis Sie das nächste Verfahren (Wiederherstellen von Objektdaten) abgeschlossen haben.



Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript, wenn Sie der Meinung sind, dass die in einem ausgefallenen Storage Volume verbliebenen Daten nicht von einer anderen Stelle im Grid wiederhergestellt werden können (falls Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie macht, oder falls Volumes auf mehreren Nodes ausgefallen sind). Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, wie Sie Ihre Daten wiederherstellen können.

4. Führen Sie die aus `sn-recovery-postinstall.sh` Skript: `sn-recovery-postinstall.sh`

Dieses Skript formatiert alle Storage-Volumes, die nicht gemountet werden konnten oder die sich als falsch formatiert herausfanden. Darüber hinaus wird die Cassandra-Datenbank bei Bedarf auf dem Node wiederhergestellt und die Services auf dem Storage-Node gestartet.

Beachten Sie Folgendes:

- Das Skript kann Stunden in Anspruch nehmen.
- Im Allgemeinen sollten Sie die SSH-Sitzung allein lassen, während das Skript ausgeführt wird.
- Drücken Sie nicht **Strg+C**, wenn die SSH-Sitzung aktiv ist.
- Das Skript wird im Hintergrund ausgeführt, wenn eine Netzwerkunterbrechung auftritt und die SSH-Sitzung beendet wird. Sie können jedoch den Fortschritt auf der Seite Wiederherstellung anzeigen.
- Wenn der Storage-Node den RSM-Service verwendet, wird das Skript möglicherweise 5 Minuten lang blockiert, während die Node-Services neu gestartet werden. Diese 5-minütige Verzögerung wird erwartet, wenn der RSM-Dienst zum ersten Mal startet.



Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Service enthalten.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptaussage bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. Als der `sn-recovery-postinstall.sh` Skript wird ausgeführt, überwachen Sie die Wiederherstellungsseite im Grid Manager.

Die Fortschrittsanzeige und die Spalte Phase auf der Seite Wiederherstellung geben einen allgemeinen Status des an `sn-recovery-postinstall.sh` Skript:

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

Nach dem `sn-recovery-postinstall.sh` Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speicher-Volumes wiederherstellen, die durch das Skript formatiert wurden, wie im nächsten Verfahren beschrieben.

Verwandte Informationen

[Prüfen Sie die Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken](#)

[Wiederherstellung von Objektdaten auf Storage Volumes für die Appliance](#)

Wiederherstellung von Objektdaten auf Storage Volumes für die Appliance

Nach der Wiederherstellung von Storage-Volumes für den Appliance-Storage-Node können Sie die Objektdaten wiederherstellen, die bei einem Ausfall des Storage-Node verloren gegangen sind.

Was Sie benötigen

- Sie müssen bestätigt haben, dass der wiederhergestellte Speicherknoten einen Verbindungsstatus von **verbunden** hat  Auf der Registerkarte **NODES Übersicht** im Grid Manager.

Über diese Aufgabe

Objektdaten können von anderen Storage-Nodes, einem Archiv-Node oder einem Cloud Storage-Pool wiederhergestellt werden, wenn die ILM-Regeln des Grid so konfiguriert wurden, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Recovery-Zeitrahmens und der damit verbundenen Kosten zu erhalten.
- Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden

Objektdaten vom Archiv-Node abgerufen. Das Wiederherstellen von Objektdaten auf einem Storage-Node aus einem Archiv-Node dauert länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes, da die Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen zu einer Verzögerung führt.

Informationen zum `repair-data` Skript

Zum Wiederherstellen von Objektdaten führen Sie den `repair-data` Skript: Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans zusammen, um sicherzustellen, dass ILM-Regeln eingehalten werden.

Wählen Sie unten **replizierte Daten** oder **Erasure-codierte (EC) Daten** aus, um die verschiedenen Optionen für das `repair-data` Skript erstellen, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding-Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssets ausführen.



Weitere Informationen zum `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile des primären Admin-Knotens.

Replizierte Daten

Zwei Befehle sind zum Wiederherstellen replizierter Daten verfügbar, unabhängig davon, ob Sie den gesamten Node oder nur bestimmte Volumes auf dem Node reparieren müssen:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Sie können Reparaturen replizierter Daten mit diesem Befehl verfolgen:

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

Zwei Befehle sind zum Wiederherstellen von Erasure-codierten Daten verfügbar. Dabei basiert es darauf, ob Sie den gesamten Node reparieren müssen oder nur bestimmte Volumes auf dem Node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Sie können Reparaturen von Daten, die auf Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```



Der EC-Reparaturauftrag reserviert vorübergehend eine große Menge an Lagerung. Storage-Warnmeldungen können zwar ausgelöst werden, werden aber nach Abschluss der Reparatur behoben. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturauftrag abgeschlossen wurde, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Suchen Sie nach Hostnamen für Speicherknoten

1. Melden Sie sich beim primären Admin-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:
- 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 `#`.

2. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die wiederhergestellten Speicher-Volumes zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`.

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn nur einige Volumes gescheitert sind, gehen Sie zu [wenn nur einige Volumes ausgefallen sind](#).



Sie können nicht ausgeführt werden `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

Replizierte Daten

Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die replizierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Siehe [Monitoring und Fehlerbehebung](#).

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die Erasure-codierte Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zu [wenn alle Volumes ausgefallen sind](#).

Geben Sie die Volume-IDs in hexadezimal ein. Beispiel: `0000` Ist der erste Band und `000F` Ist der sechzehnte Band. Sie können ein Volume, einen Bereich von Volumes oder mehrere Volumes angeben, die sich nicht in einer Sequenz befinden.

Alle Volumes müssen sich auf demselben Speicherknoten befinden. Wenn Sie Volumes für mehr als einen Speicherknoten wiederherstellen müssen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Grid replizierte Daten enthält, verwenden Sie das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf das Volume wieder her 0002 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf alle Volumes im Bereich wieder her 0003 Bis 0009 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Mehrere Volumes nicht in einer Sequenz: Dieser Befehl stellt replizierte Daten in Volumes wieder her 0001, 0005, und 0008 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt die mit dem Löschen kodierte Daten auf das Volume wieder her 0007 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt Daten mit Löschungscode auf alle Volumes im Bereich wieder her 0004 Bis 0006 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Mehrere Volumes nicht in einer Sequenz: Dieser Befehl stellt Erasure-codierte Daten auf Volumes wieder her 000A, 000C, und 000E Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies

`repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Überwachen Sie Reparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beides verwenden.

Replizierte Daten

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES Storage Node wird repariert ILM** aus.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid Speicherknoten, der repariert wird LDR Datenspeicher** aus.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA):** Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM):** Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.
- Wenn Sie optional einen geschätzten Fertigstellungsgrad für die replizierte Reparatur erhalten möchten, fügen Sie den hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:

- Wählen Sie **SUPPORT Tools Kennzahlen** aus, um die voraussichtliche Zeit bis zur Fertigstellung und den Prozentsatz für den Abschluss des aktuellen Jobs anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
- Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data` Betriebliche Gründe:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

```
repair-data show-ec-repair-status
```

Die Ausgabe enthält Informationen, einschließlich `repair ID`, Für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung des Appliance-Speicherknoten

Nach der Wiederherstellung eines Appliance Storage Node müssen Sie überprüfen, ob der gewünschte Status des Appliance Storage Node auf „Online“ gesetzt ist, und vergewissern Sie sich, dass der Status bei jedem Neustart des Storage Node-Servers standardmäßig online ist.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten > LDR > Storage > Speicherzustand — gewünscht** und **Speicherstatus — Strom**.

Der Wert beider Attribute sollte Online sein.

3. Wenn der Speicherstatus — gewünscht auf schreibgeschützt eingestellt ist, führen Sie die folgenden

Schritte aus:

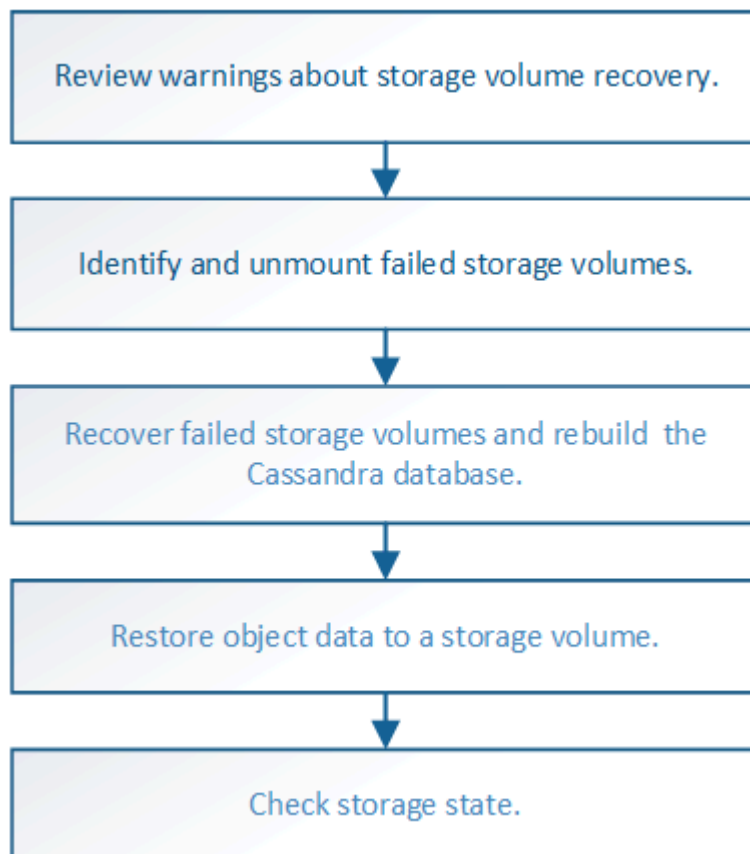
- a. Klicken Sie auf die Registerkarte **Konfiguration**.
- b. Wählen Sie aus der Dropdown-Liste **Storage State — gewünschte** die Option **Online** aus.
- c. Klicken Sie Auf **Änderungen Übernehmen**.
- d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

Wiederherstellung nach einem Storage-Volume-Ausfall bei intaktem Systemlaufwerk

Sie müssen eine Reihe von Aufgaben durchführen, um einen softwarebasierten Storage Node wiederherzustellen, bei dem ein oder mehrere Storage-Volumes auf dem Storage-Node ausgefallen sind, das Systemlaufwerk jedoch intakt ist. Wenn nur Speichervolumen ausgefallen sind, steht der Speicherknoten dem StorageGRID-System weiterhin zur Verfügung.

Über diese Aufgabe

Dieses Wiederherstellungsverfahren gilt nur für softwarebasierte Speicherknoten. Falls Storage-Volumes auf einem Appliance-Storage-Node ausgefallen sind, verwenden Sie das Verfahren für „Appliance Storage Node wiederherstellen“.



Verwandte Informationen

[Appliance Storage Node wiederherstellen](#)

Prüfen Sie Warnungen zur Wiederherstellung des Speichervolumens

Bevor Sie fehlgeschlagene Speicher-Volumes für einen Speicherknoten wiederherstellen, müssen Sie die folgenden Warnungen überprüfen.

Die Storage-Volumes (oder Rangedbs) in einem Storage-Node werden durch eine hexadezimale Zahl identifiziert, die als Volume-ID bezeichnet wird. Zum Beispiel ist 0000 das erste Volumen und 000F das sechzehnte Volumen. Der erste Objektspeicher (Volume 0) auf jedem Storage-Node belegt bis zu 4 TB Speicherplatz für Objekt-Metadaten und Cassandra-Datenbankvorgänge. Für Objektdaten werden der verbleibende Speicherplatz auf diesem Volume verwendet. Alle anderen Storage Volumes werden ausschließlich für Objektdaten verwendet.

Falls Volume 0 ausfällt und wiederhergestellt werden muss, kann die Cassandra-Datenbank im Rahmen des Volume-Recovery-Verfahrens neu erstellt werden. Cassandra kann unter folgenden Umständen auch wieder aufgebaut werden:

- Ein Storage-Node wird nach mehr als 15 Tagen offline wieder online geschaltet.
- Das Systemlaufwerk und ein oder mehrere Storage-Volumes ausfallen und werden wiederhergestellt.

Nach dem Rebuilt von Cassandra verwendet das System Informationen von anderen Speicherknoten. Wenn zu viele Storage-Nodes offline sind, sind einige Cassandra-Daten möglicherweise nicht verfügbar. Falls Cassandra vor Kurzem neu aufgebaut wurde, sind Cassandra-Daten möglicherweise noch nicht konsistent im gesamten Grid. Datenverluste können auftreten, wenn Cassandra neu aufgebaut wird, wenn zu viele Storage-Nodes offline sind oder wenn zwei oder mehr Storage-Nodes innerhalb von 15 Tagen neu erstellt werden.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie den folgenden Wiederherstellungsvorgang nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen kann zu Datenverlust führen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Wenden Sie sich an den technischen Support.

Durchführen der Standortwiederherstellung durch den technischen Support



Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und sich die Kopie auf einem ausgefallenen Storage Volume befindet, können Sie das Objekt nicht wiederherstellen.



Wenn während der Wiederherstellung ein Alarm „Service: Status – Cassandra (SVST)“ (Service: Status – Cassandra) ausgegeben wird, lesen Sie die Überwachungs- und Fehlerbehebungsanweisungen zur Wiederherstellung des Alarms durch Neuaufbau von Cassandra. Nach dem Wiederaufbau von Cassandra sollten die Alarme gelöscht werden. Wenn die Alarme nicht gelöscht werden, wenden Sie sich an den technischen Support.

Verwandte Informationen

Ermitteln und Aufheben fehlgeschlagener Storage Volumes

Bei der Wiederherstellung eines Storage-Nodes mit ausgefallenen Storage-Volumes müssen Sie die ausgefallenen Volumes identifizieren und deren Bereitstellung aufheben. Sie müssen überprüfen, ob nur die fehlgeschlagenen Speicher-Volumes im Rahmen der Wiederherstellungsverfahren neu formatiert werden.

Was Sie benötigen

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

Über diese Aufgabe

Sie sollten ausgefallene Storage Volumes so bald wie möglich wiederherstellen.

Der erste Schritt des Wiederherstellungsprozesses besteht darin, Volumes zu erkennen, die entfernt wurden, abgehängt werden müssen oder I/O-Fehler haben. Wenn weiterhin fehlgeschlagene Volumes angehängt sind, aber ein zufällig beschädigtes Dateisystem vorhanden ist, erkennt das System möglicherweise keine Beschädigung in nicht verwendeten oder nicht zugewiesenen Teilen der Festplatte.



Sie müssen dieses Verfahren abschließen, bevor Sie manuelle Schritte zur Wiederherstellung von Volumes durchführen, z. B. das Hinzufügen oder erneutes Anschließen von Festplatten, das Anhalten des Node, Starten des Node oder Neustarten. Andernfalls, wenn Sie den ausführen `reformat_storage_block_devices.rb` Skript, möglicherweise tritt ein Dateisystemfehler auf, der zum Aufhängen oder Fehlschlagen des Skripts führt.



Reparieren Sie die Hardware und schließen Sie die Festplatten ordnungsgemäß an, bevor Sie den ausführen `reboot` Befehl.

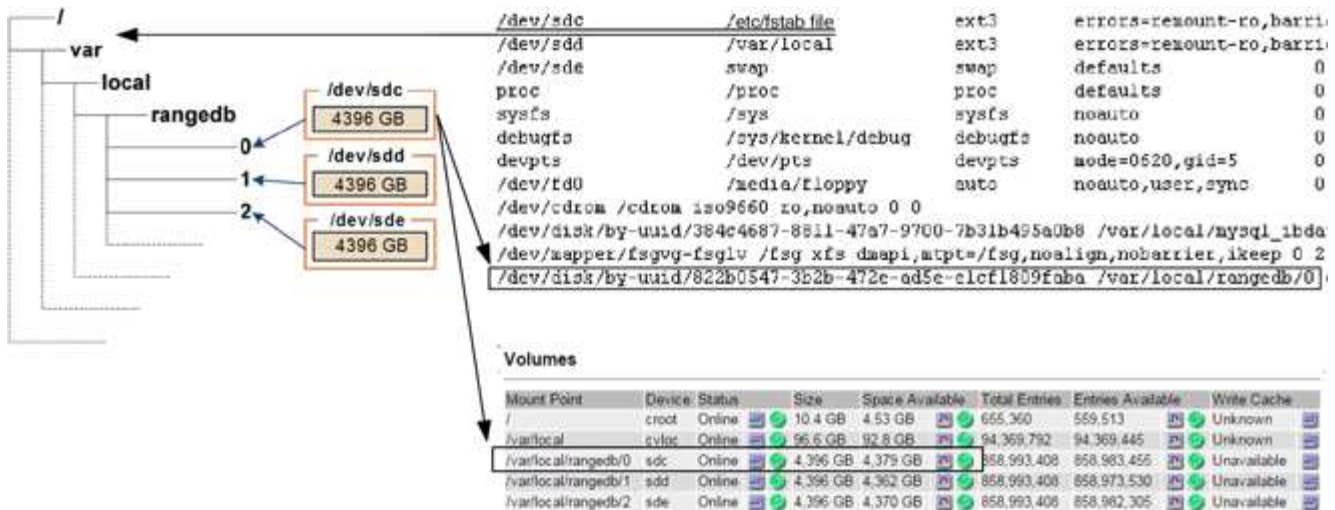


Fehlerhafte Storage-Volumes sorgfältig ermitteln Anhand dieser Informationen können Sie überprüfen, welche Volumes neu formatiert werden müssen. Sobald ein Volume neu formatiert wurde, können die Daten auf dem Volume nicht mehr wiederhergestellt werden.

Um fehlgeschlagene Speicher-Volumes korrekt wiederherzustellen, müssen Sie sowohl die Gerätenamen der ausgefallenen Speicher-Volumes als auch die zugehörigen Volume-IDs kennen.

Bei der Installation wird jedem Storage-Gerät eine UUID (Universal Unique Identifier) des Filesystems zugewiesen und über die zugewiesene Filesystem-UUID in ein `rangedb`-Verzeichnis auf dem Storage Node gemountet. Die UUID des Dateisystems und das Verzeichnis „`rangedb`“ sind im aufgeführt `/etc/fstab` Datei: Der Gerätename, das `rankgedb`-Verzeichnis und die Größe des gemounteten Volumes werden im Grid Manager angezeigt.

Im folgenden Beispiel ist das Gerät `/dev/sdc` Hat eine Volume-Größe von 4 TB, wird angehängt auf `/var/local/rangedb/0`, Verwenden des Gerätenamens `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` Im `/etc/fstab` Datei:



Schritte

- Führen Sie die folgenden Schritte durch, um die fehlgeschlagenen Speicher-Volumes und deren Gerätenamen aufzunehmen:
 - Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - Wählen Sie **Standort > fehlgeschlagener Speicherknoten > LDR > Storage > Übersicht > Haupt**, und suchen Sie nach Objektspeichern mit Alarmen.

Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

- Wählen Sie **Standort > fehlgeschlagener Speicherknoten > SSM > Ressourcen > Übersicht > Haupt**. Ermitteln Sie den Mount-Punkt und die Volume-Größe jedes im vorherigen Schritt identifizierten ausgefallenen Storage-Volumes.

Objektspeichern werden in Hex-Notation nummeriert. Zum Beispiel ist 0000 das erste Volumen und 000F das sechzehnte Volumen. Im Beispiel entspricht der Objektspeicher mit der ID 0000 `/var/local/rangedb/0` mit dem Gerätenamen `sdc` und einer Größe von 107 GB.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
<code>/</code>	<code>croot</code>	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
<code>/var/local</code>	<code>cvloc</code>	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
<code>/var/local/rangedb/0</code>	<code>sdc</code>	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
<code>/var/local/rangedb/1</code>	<code>sdd</code>	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
<code>/var/local/rangedb/2</code>	<code>sde</code>	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

- Melden Sie sich beim fehlgeschlagenen Speicherknoten an:
 - 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. Führen Sie das folgende Skript aus, um die Speicherdienste zu stoppen und die Bereitstellung eines fehlerhaften Speicher-Volumes aufzuheben:

```
sn-unmount-volume object_store_ID
```

Der `object_store_ID` ist die ID des ausgefallenen Speicher-Volumes. Geben Sie beispielsweise an 0. Im Befehl für einen Objektspeicher mit der ID 0000.

4. Wenn Sie dazu aufgefordert werden, drücken Sie **y**, um die Speicherdienste auf dem Speicherknoten zu stoppen.



Wenn die Storage-Services bereits angehalten wurden, werden Sie nicht aufgefordert. Der Cassandra-Service wird nur für Volume 0 angehalten.

```
root@Storage-180:~ # sn-unmount-volume 0
Storage services (ldr, chunk, dds, cassandra) are not down.
Storage services must be stopped before running this script.
Stop storage services [y/N]? y
Shutting down storage services.
Storage services stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

In wenigen Sekunden werden die Speicherservices angehalten und das Volume wird abgehängt. Die Meldungen werden angezeigt, die jeden Schritt des Prozesses angeben. Die letzte Meldung gibt an, dass das Volume abgehängt wurde.

Recovery ausgefallener Storage-Volumes und Wiederherstellung der Cassandra-Datenbank

Sie müssen ein Skript ausführen, das den Speicher auf ausgefallenen Storage-Volumes neu formatiert und neu einbindet, und die Cassandra-Datenbank auf dem Storage-Node neu erstellen, falls das System den Bedarf ermittelt.

- Sie müssen die haben `Passwords.txt` Datei:
- Die Systemlaufwerke auf dem Server müssen intakt sein.
- Die Fehlerursache muss ermittelt worden sein und bei Bedarf muss bereits Ersatz-Storage-Hardware angeschafft worden sein.
- Die Gesamtgröße des Ersatzspeichers muss mit dem Original übereinstimmen.
- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang

zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Dekommission.**)

- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Erweiterung.**)
- Das ist schon [Die Warnungen zur Wiederherstellung des Speichervolumens wurden überprüft.](#)
 - a. Ersetzen Sie bei Bedarf den fehlerhaften physischen oder virtuellen Speicher, der mit den fehlerhaften Speicher-Volumes verbunden ist, die Sie zuvor ermittelt und abgehängt haben.

Stellen Sie nach dem Ersetzen des Speichers sicher, dass Sie ihn erneut scannen oder neu booten, um sicherzustellen, dass er vom Betriebssystem erkannt wird, die Volumes jedoch nicht neu mounten. Der Speicher wird neu eingebunden und hinzugefügt `/etc/fstab` In einem späteren Schritt.

- b. Melden Sie sich beim fehlgeschlagenen Speicherknoten 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 `#`.

- c. Verwenden Sie einen Texteditor (`vi` oder `vim`), um fehlgeschlagene Volumes aus dem zu löschen `/etc/fstab` Datei und dann speichern Sie die Datei.



Kommentieren eines ausgefallenen Volumes in `/etc/fstab` Datei reicht nicht aus. Das Volume muss aus gelöscht werden `fstab` Während der Wiederherstellungsvorgang überprüft, ob alle Leitungen im vorhanden sind `fstab` Die Datei stimmt mit den gemounteten Dateisystemen überein.

- d. Formatieren Sie alle ausgefallenen Storage-Volumes neu und stellen Sie ggf. die Cassandra-Datenbank wieder her. Geben Sie Ein: `reformat_storage_block_devices.rb`
 - Wenn Speicherservices ausgeführt werden, werden Sie aufgefordert, diese zu beenden. Geben Sie ein: **Y**
 - Sie werden aufgefordert, die Cassandra-Datenbank bei Bedarf neu aufzubauen.
 - Überprüfen Sie die Warnungen. Falls keines dieser Beispiele zutreffend ist, bauen Sie die Cassandra-Datenbank neu aus. Geben Sie ein: **Y**
 - Wenn mehr als ein Speicherknoten offline ist oder wenn ein anderer Speicherknoten in den letzten 15 Tagen wieder aufgebaut wurde. Geben Sie: **N** ein

Das Skript wird beendet, ohne dass Cassandra neu aufgebaut werden muss. Wenden Sie sich an den technischen Support.

- Wenn Sie nach jedem Rangedb-Laufwerk auf dem Storage-Node gefragt werden: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, Geben Sie eine der folgenden Antworten ein:
 - **Y** um ein Laufwerk neu zu formatieren, das Fehler hatte. Dadurch wird das Speichervolumen neu formatiert und das neu formatierte Speichervolume wird hinzugefügt `/etc/fstab` Datei:

- **N** wenn das Laufwerk keine Fehler enthält und Sie es nicht neu formatieren wollen.



Durch Auswahl von **n** wird das Skript beendet. Entweder montieren Sie das Laufwerk (wenn Sie denken, dass die Daten auf dem Laufwerk beibehalten werden sollten und das Laufwerk fehlerhaft abgehängt wurde) oder entfernen Sie das Laufwerk. Führen Sie dann die aus `reformat_storage_block_devices.rb` Befehl erneut.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptausgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

Im folgenden Beispiel wird das Laufwerk ausgegeben `/dev/sdf` Muss neu formatiert werden, und Cassandra musste nicht neu aufgebaut werden:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done. Now do manual steps to
restore copies of data.
```

Wiederherstellung von Objektdaten auf dem Storage Volume, auf dem das Systemlaufwerk intakt ist

Nach der Wiederherstellung eines Storage-Volumes auf einem Storage-Node, auf dem das Systemlaufwerk intakt ist, können Sie die Objektdaten wiederherstellen, die bei einem Ausfall des Storage-Volume verloren gegangen sind.

Was Sie benötigen

- Sie müssen bestätigt haben, dass der wiederhergestellte Speicherknoten einen Verbindungsstatus von **verbunden** hat  Auf der Registerkarte **NODES Übersicht** im Grid Manager.

Über diese Aufgabe

Objektdaten können von anderen Storage-Nodes, einem Archiv-Node oder einem Cloud Storage-Pool wiederhergestellt werden, wenn die ILM-Regeln des Grid so konfiguriert wurden, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Recovery-Zeitrahmens und der damit verbundenen Kosten zu erhalten.
- Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden Objektdaten vom Archiv-Node abgerufen. Das Wiederherstellen von Objektdaten auf einem Storage-Node aus einem Archiv-Node dauert länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes, da die Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen zu einer Verzögerung führt.

Informationen zum `repair-data` Skript

Zum Wiederherstellen von Objektdaten führen Sie den aus `repair-data` Skript: Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans zusammen, um sicherzustellen, dass ILM-Regeln eingehalten werden.

Wählen Sie unten **replizierte Daten** oder **Erasure-codierte (EC) Daten** aus, um die verschiedenen Optionen für das zu erfahren `repair-data` Skript erstellen, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding-Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssets ausführen.



Weitere Informationen zum `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile des primären Admin-Knotens.

Replizierte Daten

Zwei Befehle sind zum Wiederherstellen replizierter Daten verfügbar, unabhängig davon, ob Sie den gesamten Node oder nur bestimmte Volumes auf dem Node reparieren müssen:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Sie können Reparaturen replizierter Daten mit diesem Befehl verfolgen:

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

Zwei Befehle sind zum Wiederherstellen von Erasure-codierten Daten verfügbar. Dabei basiert es darauf, ob Sie den gesamten Node reparieren müssen oder nur bestimmte Volumes auf dem Node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Sie können Reparaturen von Daten, die auf Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```



Der EC-Reparaturauftrag reserviert vorübergehend eine große Menge an Lagerung. Storage-Warnmeldungen können zwar ausgelöst werden, werden aber nach Abschluss der Reparatur behoben. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturauftrag abgeschlossen wurde, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Suchen Sie nach Hostnamen für Speicherknoten

1. Melden Sie sich beim primären Admin-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:
- 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 `#`.

2. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die wiederhergestellten Speicher-Volumes zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`.

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn nur einige Volumes gescheitert sind, gehen Sie zu [wenn nur einige Volumes ausgefallen sind](#).



Sie können nicht ausgeführt werden `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

Replizierte Daten

Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die replizierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Siehe [Monitoring und Fehlerbehebung](#).

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die Erasure-codierte Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zu [wenn alle Volumes ausgefallen sind](#).

Geben Sie die Volume-IDs in hexadezimal ein. Beispiel: 0000 Ist der erste Band und 000F Ist der sechzehnte Band. Sie können ein Volume, einen Bereich von Volumes oder mehrere Volumes angeben, die sich nicht in einer Sequenz befinden.

Alle Volumes müssen sich auf demselben Speicherknoten befinden. Wenn Sie Volumes für mehr als einen Speicherknoten wiederherstellen müssen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Grid replizierte Daten enthält, verwenden Sie das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf das Volume wieder her 0002 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf alle Volumes im Bereich wieder her 0003 Bis 0009 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Mehrere Volumes nicht in einer Sequenz: Dieser Befehl stellt replizierte Daten in Volumes wieder her 0001, 0005, und 0008 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt die mit dem Löschen kodierte Daten auf das Volume wieder her 0007 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt Daten mit Löschungscode auf alle Volumes im Bereich wieder her 0004 Bis 0006 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Mehrere Volumes nicht in einer Sequenz: Dieser Befehl stellt Erasure-codierte Daten auf Volumes wieder her 000A, 000C, und 000E Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies

`repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Überwachen Sie Reparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beides verwenden.

Replizierte Daten

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES Storage Node wird repariert ILM** aus.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid Speicherknoten, der repariert wird LDR Datenspeicher** aus.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA):** Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM):** Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.
- Wenn Sie optional einen geschätzten Fertigstellungsgrad für die replizierte Reparatur erhalten möchten, fügen Sie den hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:

- Wählen Sie **SUPPORT Tools Kennzahlen** aus, um die voraussichtliche Zeit bis zur Fertigstellung und den Prozentsatz für den Abschluss des aktuellen Jobs anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
- Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data` Betriebliche Gründe:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

```
repair-data show-ec-repair-status
```

Die Ausgabe enthält Informationen, einschließlich `repair ID`, Für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung von Storage Volumes

Nach der Wiederherstellung von Speichervolumes müssen Sie überprüfen, ob der gewünschte Status des Speicherknoten auf „Online“ gesetzt ist, und sicherstellen, dass der Status beim Neustart des Speicherknotenservers standardmäßig online ist.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten > LDR > Storage > Speicherzustand — gewünscht** und **Speicherstatus — Strom**.

Der Wert beider Attribute sollte Online sein.

3. Wenn der Speicherstatus — gewünscht auf schreibgeschützt eingestellt ist, führen Sie die folgenden Schritte aus:

- a. Klicken Sie auf die Registerkarte **Konfiguration**.
- b. Wählen Sie aus der Dropdown-Liste **Storage State — gewünschte** die Option **Online** aus.
- c. Klicken Sie Auf **Änderungen Übernehmen**.
- d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

Wiederherstellung nach einem Laufwerksausfall

Wenn das Systemlaufwerk auf einem softwarebasierten Speicherknoten ausgefallen ist, steht der Speicherknoten dem StorageGRID-System nicht zur Verfügung. Sie müssen einen bestimmten Satz von Aufgaben zur Wiederherstellung nach einem Systemausfall ausführen.

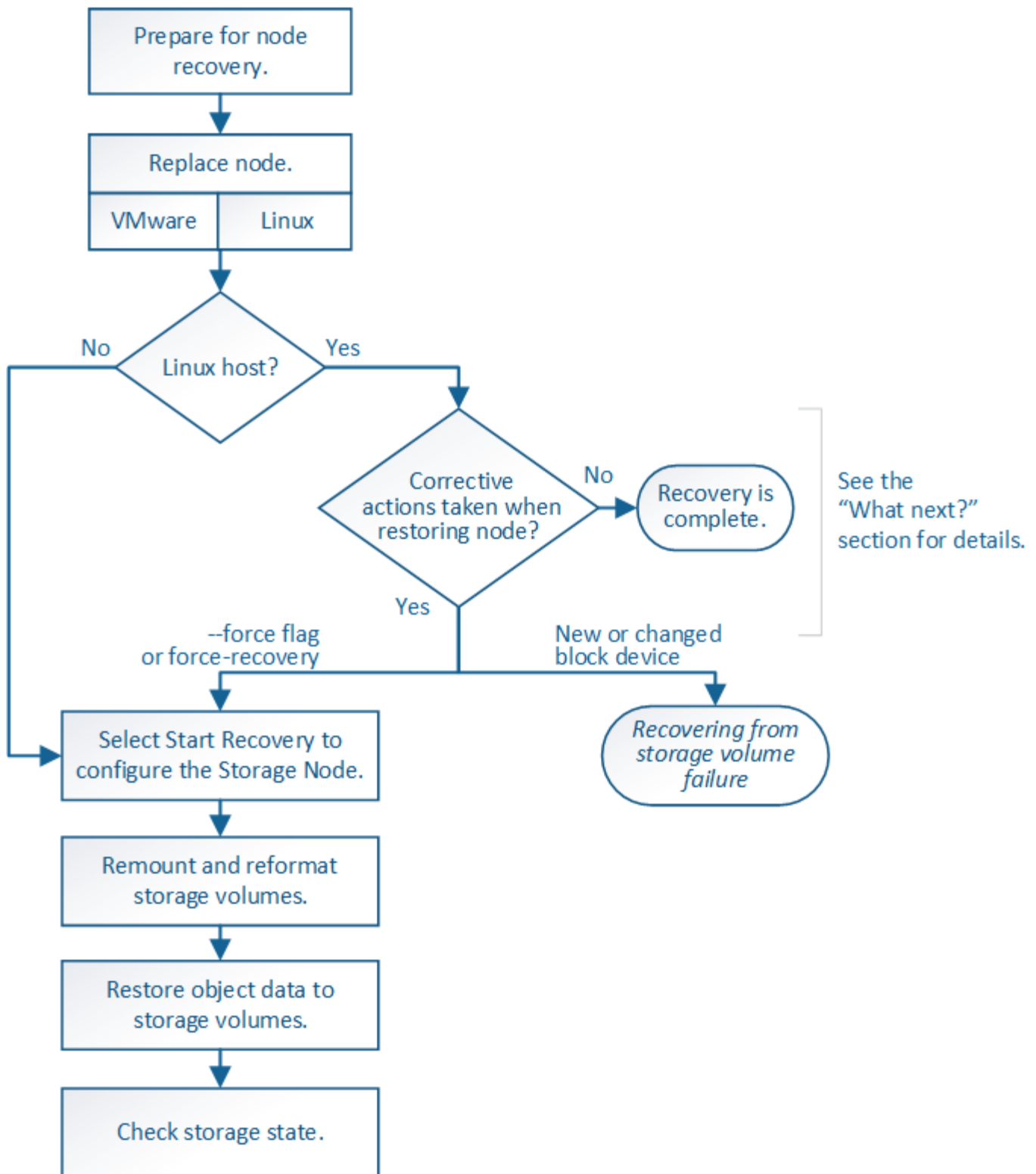
Über diese Aufgabe

Gehen Sie folgendermaßen vor, um nach einem Systemlaufwerksausfall auf einem softwarebasierten Speicherknoten wiederherzustellen. Dieses Verfahren umfasst die folgenden Schritte, wenn auch Storage-Volumes ausgefallen sind oder nicht neu eingebunden werden können.



Dieses Verfahren gilt nur für softwarebasierte Speicherknoten. Sie müssen ein anderes Verfahren befolgen, um einen Appliance-Speicherknoten wiederherzustellen.

[Appliance Storage Node wiederherstellen](#)



Prüfen Sie die Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken

Bevor Sie ein ausgefallenes Systemlaufwerk eines Speicherknoten wiederherstellen, müssen Sie die folgenden Warnungen überprüfen.

Storage-Nodes verfügen über eine Cassandra Datenbank mit Objekt-Metadaten. Unter folgenden Umständen kann die Cassandra-Datenbank neu erstellt werden:

- Ein Storage-Node wird nach mehr als 15 Tagen offline wieder online geschaltet.
- Ein Speichervolume ist ausgefallen und wurde wiederhergestellt.
- Das Systemlaufwerk und ein oder mehrere Storage-Volumes ausfallen und werden wiederhergestellt.

Nach dem Rebuild von Cassandra verwendet das System Informationen von anderen Speicherknoten. Wenn zu viele Storage-Nodes offline sind, sind einige Cassandra-Daten möglicherweise nicht verfügbar. Falls Cassandra vor Kurzem neu aufgebaut wurde, sind Cassandra-Daten möglicherweise noch nicht konsistent im gesamten Grid. Datenverluste können auftreten, wenn Cassandra neu aufgebaut wird, wenn zu viele Storage-Nodes offline sind oder wenn zwei oder mehr Storage-Nodes innerhalb von 15 Tagen neu erstellt werden.



Wenn mehrere Speicherknoten ausgefallen sind (oder offline ist), wenden Sie sich an den technischen Support. Führen Sie den folgenden Wiederherstellungsvorgang nicht durch. Es kann zu Datenverlusten kommen.



Falls dies der zweite Ausfall des Storage-Nodes in weniger als 15 Tagen nach Ausfall oder Wiederherstellung eines Storage-Nodes ist, wenden Sie sich an den technischen Support. Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen kann zu Datenverlust führen.



Wenn mehr als ein Speicherknoten an einem Standort ausgefallen ist, ist möglicherweise ein Verfahren zur Standortwiederherstellung erforderlich. Wenden Sie sich an den technischen Support.

Durchführen der Standortwiederherstellung durch den technischen Support



Wenn sich dieser Speicherknoten im schreibgeschützten Wartungsmodus befindet, um das Abrufen von Objekten durch einen anderen Speicherknoten mit ausgefallenen Speichervolumes zu ermöglichen, stellen Sie Volumes auf dem Speicherknoten mit fehlerhaften Speichervolumes wieder her, bevor Sie diesen fehlgeschlagenen Speicherknoten wiederherstellen. Beachten Sie die Anweisungen für die Wiederherstellung nach einem Verlust von Storage-Volumes, bei denen das Systemlaufwerk intakt ist.



Wenn ILM-Regeln so konfiguriert sind, dass nur eine replizierte Kopie gespeichert wird und sich die Kopie auf einem ausgefallenen Storage Volume befindet, können Sie das Objekt nicht wiederherstellen.



Wenn während der Wiederherstellung ein Alarm „Service: Status – Cassandra (SVST)“ (Service: Status – Cassandra) ausgegeben wird, lesen Sie die Überwachungs- und Fehlerbehebungsanweisungen zur Wiederherstellung des Alarms durch Neuaufbau von Cassandra. Nach dem Wiederaufbau von Cassandra sollten die Alarme gelöscht werden. Wenn die Alarme nicht gelöscht werden, wenden Sie sich an den technischen Support.

Verwandte Informationen

[Monitoring und Fehlerbehebung](#)

[Warnungen und Überlegungen für die Wiederherstellung von Grid Nodes](#)

[Wiederherstellung nach einem Storage-Volume-Ausfall bei intaktem Systemlaufwerk](#)

Ersetzen Sie den Speicherknoten

Wenn das Systemlaufwerk ausgefallen ist, müssen Sie zuerst den Speicherknoten ersetzen.

Sie müssen das Verfahren zum Ersetzen des Node für Ihre Plattform auswählen. Die Schritte zum Ersetzen eines Node sind für alle Typen von Grid-Nodes identisch.



Dieses Verfahren gilt nur für softwarebasierte Speicherknoten. Sie müssen ein anderes Verfahren befolgen, um einen Appliance-Speicherknoten wiederherzustellen.

Appliance Storage Node wiederherstellen

Linux: Wenn Sie sich nicht sicher sind, ob Ihr Systemlaufwerk ausgefallen ist, befolgen Sie die Anweisungen, um den Knoten zu ersetzen, um festzustellen, welche Wiederherstellungsschritte erforderlich sind.

Plattform	Verfahren
VMware	Einen VMware-Knoten ersetzen
Linux	Ersetzen Sie einen Linux-Knoten
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um Speicherknoten zu konfigurieren

Nachdem Sie einen Speicherknoten ersetzt haben, müssen Sie im Grid Manager die Option Wiederherstellung starten auswählen, um den neuen Knoten als Ersatz für den ausgefallenen Knoten zu konfigurieren.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.
- Sie müssen das Startdatum aller Reparaturaufträge für Daten mit Löschungscode kennen.
- Sie müssen überprüft haben, dass der Speicherknoten innerhalb der letzten 15 Tage nicht neu aufgebaut wurde.

Über diese Aufgabe

Wenn der Storage-Node als Container auf einem Linux-Host installiert ist, müssen Sie diesen Schritt nur ausführen, wenn einer dieser Schritte zutrifft:

- Man musste das benutzen `--force` Flag, um den Knoten zu importieren, oder Sie haben ausgegeben `storagegrid node force-recovery node-name`
- Sie mussten eine vollständige Neuinstallation des Knotens durchführen oder `/var/local` wiederherstellen.

Schritte

1. Wählen Sie im Grid Manager die Option **WARTUNG Tasks Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search 				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:
`storagegrid node force-recovery node-name`

6. Wenn der Speicherknoten die Stufe „Warten auf manuelle Schritte“ erreicht hat, gehen Sie zur nächsten Aufgabe im Wiederherstellungsverfahren, um Speicher-Volumes neu zu mounten und neu zu formatieren.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset

Verwandte Informationen

[Appliance für die Neuinstallation vorbereiten \(nur Plattformaustausch\)](#)

Speicher-Volumes neu einbinden und neu formatieren („Manuelle Schritte“)

Sie müssen zwei Skripte manuell ausführen, um die erhaltenen Storage Volumes neu einzubinden und ausgefallene Storage Volumes neu zu formatieren. Das erste Skript bindet Volumes wieder ein, die ordnungsgemäß als StorageGRID-Storage-Volumes formatiert sind. Das zweite Skript formatiert alle nicht abgehängt Volumes neu, stellt Cassandra bei Bedarf wieder her und startet Services.

Was Sie benötigen

- Sie haben bereits die Hardware für alle ausgefallenen Storage Volumes ausgetauscht, die ausgetauscht

werden müssen.

Ausführen des `sn-remount-volumes` Skript kann Ihnen helfen, zusätzliche ausgefallene Storage-Volumes zu identifizieren.

- Sie haben überprüft, dass keine Ausmusterung von Storage-Nodes ausgeführt wird oder Sie den Vorgang zur Deaktivierung eines Node angehalten haben. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Dekommission.**)
- Sie haben überprüft, dass keine Erweiterung ausgeführt wird. (Wählen Sie im Grid Manager die Option **WARTUNG Aufgaben Erweiterung.**)
- Das ist schon [Überprüfen Sie die Warnungen für die Wiederherstellung des Speicherknoten-Systemlaufwerks.](#)



Wenden Sie sich an den technischen Support, wenn mehr als ein Speicherknoten offline ist oder wenn ein Speicherknoten in diesem Grid in den letzten 15 Tagen neu aufgebaut wurde. Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript: Die Neuerstellung von Cassandra auf zwei oder mehr Storage-Nodes innerhalb von 15 Tagen voneinander kann zu Datenverlust führen.

Über diese Aufgabe

Zum Abschluss dieses Vorgangs führen Sie die folgenden grundlegenden Aufgaben aus:

- Melden Sie sich beim wiederhergestellten Speicherknoten an.
- Führen Sie die aus `sn-remount-volumes` Skript zum Neumounten ordnungsgemäß formatierter Speicher-Volumes. Wenn dieses Skript ausgeführt wird, führt es Folgendes aus:
 - Hängt jedes Storage-Volume an und ab, um das XFS-Journal wiederzugeben.
 - Führt eine Konsistenzprüfung der XFS-Datei durch.
 - Wenn das Dateisystem konsistent ist, bestimmt, ob das Storage Volume ein ordnungsgemäß formatiertes StorageGRID Storage Volume ist.
 - Wenn das Storage Volume ordnungsgemäß formatiert ist, wird das Storage-Volume wieder gemountet. Alle bestehenden Daten auf dem Volume bleiben erhalten.
- Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.
- Führen Sie die aus `sn-recovery-postinstall.sh` Skript: Wenn dieses Skript ausgeführt wird, führt es Folgendes aus.



Starten Sie einen Speicherknoten während der Wiederherstellung nicht neu, bevor Sie ausführen `sn-recovery-postinstall.sh` Formatieren ausgefallener Storage-Volumes und Wiederherstellen von Objekt-Metadaten Vor dem Neubooten des Speicherknoten `sn-recovery-postinstall.sh` Durch das Abschließen werden Fehler bei Diensten verursacht, die zu starten versuchen, und die Knoten der StorageGRID-Appliance den Wartungsmodus beenden. Siehe den Schritt für [Skript nach der Installation.](#)

- Umformatiert alle Storage-Volumes, die von der `sn-remount-volumes` Das Skript konnte nicht gemountet werden oder es wurde festgestellt, dass es nicht ordnungsgemäß formatiert wurde.



Wenn ein Speicher-Volume neu formatiert wird, gehen alle Daten auf diesem Volume verloren. Sie müssen ein zusätzliches Verfahren durchführen, um Objektdaten von anderen Standorten im Grid wiederherzustellen, vorausgesetzt, dass ILM-Regeln für die Speicherung von mehr als einer Objektkopie konfiguriert wurden.

- Stellt die Cassandra-Datenbank bei Bedarf auf dem Node wieder her.
- Startet die Dienste auf dem Speicherknoten.

Schritte

1. Melden Sie sich beim wiederhergestellten Speicherknoten an:

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

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

2. Führen Sie das erste Skript aus, um alle ordnungsgemäß formatierten Speicher-Volumes neu zu mounten.



Wenn alle Speicher-Volumes neu sind und formatiert werden müssen, oder wenn alle Speicher-Volumes ausgefallen sind, können Sie diesen Schritt überspringen und das zweite Skript ausführen, um alle nicht abgehängt Speicher-Volumes neu zu formatieren.

- Führen Sie das Skript aus: `sn-remount-volumes`

Dieses Skript kann Stunden dauern, bis es auf Storage-Volumes ausgeführt wird, die Daten enthalten.

- Überprüfen Sie die Ausgabe, während das Skript ausgeführt wird, und beantworten Sie alle Eingabeaufforderungen.



Nach Bedarf können Sie die verwenden `tail -f` Befehl zum Überwachen des Inhalts der Protokolldatei des Skripts (`/var/local/log/sn-remount-volumes.log`). Die Protokolldatei enthält ausführlichere Informationen als die Befehlsausgabe der Befehlszeile.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
```

Device /dev/sdb remounted successfully

===== Device /dev/sdc =====

Mount and unmount device /dev/sdc and checking file system consistency:

Error: File system consistency check retry failed on device /dev/sdc. You can see the diagnosis information in the /var/local/log/sn-remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-postinstall.sh, this volume and any data on this volume will be deleted. If you only had two copies of object data, you will temporarily have only a single copy. StorageGRID Webscale will attempt to restore data redundancy by making additional replicated copies or EC fragments, according to the rules in the active ILM policy.

Do not continue to the next step if you believe that the data remaining on this volume cannot be rebuilt from elsewhere in the grid (for example, if your ILM policy uses a rule that makes only one copy or if volumes have failed on multiple nodes). Instead, contact support to determine how to recover your data.

===== Device /dev/sdd =====

Mount and unmount device /dev/sdd and checking file system consistency:

Failed to mount device /dev/sdd

This device could be an uninitialized disk or has corrupted superblock.

File system check might take a long time. Do you want to continue? (y or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd. You can see the diagnosis information in the /var/local/log/sn-remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-postinstall.sh, this volume and any data on this volume will be deleted. If you only

had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

===== Device /dev/sde =====

Mount and unmount device /dev/sde and checking file system

consistency:

The device is consistent.

Check rangedb structure on device /dev/sde:

Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options

This device has all rangedb directories.

Found LDR node id 12000078, volume number 9 in the volID file

Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

In der Beispielausgabe wurde ein Storage-Volume erfolgreich neu eingebunden und drei Storage-Volumes wiesen Fehler auf.

- /dev/sdb Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und hatte eine gültige Volume-Struktur, so dass es erfolgreich neu eingebunden wurde. Daten auf Geräten, die vom Skript neu eingebunden werden, bleiben erhalten.
- /dev/sdc Die Konsistenzprüfung des XFS-Dateisystems ist fehlgeschlagen, da das Speichervolume neu oder beschädigt war.
- /dev/sdd Konnte nicht gemountet werden, da die Festplatte nicht initialisiert wurde oder der Superblock der Festplatte beschädigt war. Wenn das Skript kein Speicher-Volume mounten kann, wird gefragt, ob Sie die Konsistenzprüfung des Dateisystems ausführen möchten.
 - Wenn das Speichervolumen an eine neue Festplatte angeschlossen ist, beantworten Sie **N** mit der Eingabeaufforderung. Sie müssen das Dateisystem auf einer neuen Festplatte nicht überprüfen.
 - Wenn das Speichervolumen an eine vorhandene Festplatte angeschlossen ist, beantworten Sie **Y** mit der Eingabeaufforderung. Sie können die Ergebnisse der Dateisystemüberprüfung verwenden, um die Quelle der Beschädigung zu bestimmen. Die Ergebnisse werden im gespeichert /var/local/log/sn-remount-volumes.log Protokolldatei.

- `/dev/sde` Die Konsistenzprüfung des XFS-Dateisystems wurde bestanden und eine gültige Volume-Struktur hatte. Die LDR-Knoten-ID in der `volID`-Datei stimmt jedoch nicht mit der ID für diesen Storage-Node überein (die `configured LDR noid` Oben angezeigt). Diese Meldung gibt an, dass dieses Volume zu einem anderen Speicherknoten gehört.

3. Prüfen Sie die Skriptausgabe und beheben Sie etwaige Probleme.



Wenn ein Speichervolume die Konsistenzprüfung des XFS-Dateisystems fehlgeschlagen ist oder nicht gemountet werden konnte, überprüfen Sie sorgfältig die Fehlermeldungen in der Ausgabe. Sie müssen die Auswirkungen der Ausführung des `sn-recovery-postinstall.sh` Skript auf diesen Volumen.

- Überprüfen Sie, ob die Ergebnisse einen Eintrag für alle Volumes enthalten, die Sie erwartet haben. Wenn keine Volumes aufgeführt sind, führen Sie das Skript erneut aus.
- Überprüfen Sie die Meldungen für alle angeschlossenen Geräte. Stellen Sie sicher, dass keine Fehler vorliegen, die darauf hinweisen, dass ein Speichervolume nicht zu diesem Speicherknoten gehört.

Im Beispiel die Ausgabe für `/dev/sde` Enthält die folgende Fehlermeldung:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Wenn ein Storage-Volume gemeldet wird, das zu einem anderen Storage Node gehört, wenden Sie sich an den technischen Support. Wenn Sie den ausführen `sn-recovery-postinstall.sh` Skript: Das Speichervolumen wird neu formatiert, was zu Datenverlust führen kann.

- Wenn keine Speichergeräte montiert werden konnten, notieren Sie sich den Gerätenamen und reparieren oder ersetzen Sie das Gerät.



Sie müssen Speichergeräte reparieren oder ersetzen, die nicht montiert werden können.

Sie verwenden den Gerätenamen, um die Volume-ID zu suchen. Dies ist erforderlich, wenn Sie den ausführen `repair-data` Skript zum Wiederherstellen von Objektdaten auf dem Volume (beim nächsten Verfahren).

- Führen Sie nach der Reparatur oder dem Austausch aller nicht montierbaren Geräte den aus `sn-remount-volumes` Skript erneut, um zu bestätigen, dass alle Speicher-Volumes, die neu gemountet werden können, neu eingebunden wurden.



Wenn ein Speicher-Volume nicht angehängt oder nicht ordnungsgemäß formatiert werden kann, und Sie mit dem nächsten Schritt fortfahren, werden das Volume und alle Daten auf dem Volume gelöscht. Falls Sie zwei Kopien von Objektdaten hatten, ist nur eine einzige Kopie verfügbar, bis Sie das nächste Verfahren (Wiederherstellen von Objektdaten) abgeschlossen haben.



Führen Sie das nicht aus `sn-recovery-postinstall.sh` Skript, wenn Sie der Meinung sind, dass die in einem ausgefallenen Storage Volume verbliebenen Daten nicht von einer anderen Stelle im Grid wiederhergestellt werden können (falls Ihre ILM-Richtlinie eine Regel verwendet, die nur eine Kopie macht, oder falls Volumes auf mehreren Nodes ausgefallen sind). Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, wie Sie Ihre Daten wiederherstellen können.

4. Führen Sie die aus `sn-recovery-postinstall.sh` Skript: `sn-recovery-postinstall.sh`

Dieses Skript formatiert alle Storage-Volumes, die nicht gemountet werden konnten oder die sich als falsch formatiert herausfanden. Darüber hinaus wird die Cassandra-Datenbank bei Bedarf auf dem Node wiederhergestellt und die Services auf dem Storage-Node gestartet.

Beachten Sie Folgendes:

- Das Skript kann Stunden in Anspruch nehmen.
- Im Allgemeinen sollten Sie die SSH-Sitzung allein lassen, während das Skript ausgeführt wird.
- Drücken Sie nicht **Strg+C**, wenn die SSH-Sitzung aktiv ist.
- Das Skript wird im Hintergrund ausgeführt, wenn eine Netzwerkunterbrechung auftritt und die SSH-Sitzung beendet wird. Sie können jedoch den Fortschritt auf der Seite Wiederherstellung anzeigen.
- Wenn der Storage-Node den RSM-Service verwendet, wird das Skript möglicherweise 5 Minuten lang blockiert, während die Node-Services neu gestartet werden. Diese 5-minütige Verzögerung wird erwartet, wenn der RSM-Dienst zum ersten Mal startet.



Der RSM-Dienst ist auf Speicherknoten vorhanden, die den ADC-Service enthalten.



Einige StorageGRID-Wiederherstellungsverfahren verwenden Reaper für die Bearbeitung von Cassandra-Reparaturen. Reparaturen werden automatisch ausgeführt, sobald die entsprechenden oder erforderlichen Services gestartet wurden. Sie können die Skriptaussgabe bemerken, die "reaper" oder "Cassandra Reparatur erwähnt." Wenn eine Fehlermeldung angezeigt wird, dass die Reparatur fehlgeschlagen ist, führen Sie den in der Fehlermeldung angegebenen Befehl aus.

5. als `sn-recovery-postinstall.sh` Skript wird ausgeführt, überwachen Sie die Wiederherstellungsseite im Grid Manager.

Die Fortschrittsanzeige und die Spalte Phase auf der Seite Wiederherstellung geben einen allgemeinen Status des an `sn-recovery-postinstall.sh` Skript:

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

Nach dem `sn-recovery-postinstall.sh` Skript hat Dienste auf dem Knoten gestartet. Sie können Objektdaten auf allen Speicher-Volumes wiederherstellen, die durch das Skript formatiert wurden, wie in diesem Verfahren beschrieben.

Verwandte Informationen

[Prüfen Sie die Warnungen für die Wiederherstellung von Speicherknoten-Laufwerken](#)

[Wiederherstellen von Objektdaten im Storage Volume, falls erforderlich](#)

Wiederherstellen von Objektdaten im Storage Volume, falls erforderlich

Wenn der `sn-recovery-postinstall.sh` Skript ist erforderlich, um ein oder mehrere fehlgeschlagene Speicher-Volumes neu zu formatieren, müssen Sie Objektdaten auf dem neu formatierten Speicher-Volume von anderen Speicherknoten und Archiv-Nodes wiederherstellen. Diese Schritte sind erst dann erforderlich, wenn ein oder mehrere Storage Volumes neu formatiert wurden.

Was Sie benötigen

- Sie müssen bestätigt haben, dass der wiederhergestellte Speicherknoten einen Verbindungsstatus von **verbunden** hat  Auf der Registerkarte **NODES Übersicht** im Grid Manager.

Über diese Aufgabe

Objektdaten können von anderen Storage-Nodes, einem Archiv-Node oder einem Cloud Storage-Pool wiederhergestellt werden, wenn die ILM-Regeln des Grid so konfiguriert wurden, dass Objektkopien verfügbar sind.

Beachten Sie Folgendes:

- Wenn eine ILM-Regel so konfiguriert wurde, dass nur eine replizierte Kopie gespeichert wird und sich diese Kopie auf einem ausgefallenen Storage Volume befand, können Sie das Objekt nicht wiederherstellen.
- Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, muss StorageGRID mehrere Anfragen an den Cloud Storage Pool Endpunkt stellen, um Objektdaten wiederherzustellen. Bevor Sie dieses Verfahren durchführen, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Recovery-Zeitrahmens und der damit verbundenen Kosten zu

erhalten.

- Wenn sich die einzige verbleibende Kopie eines Objekts auf einem Archiv-Node befindet, werden Objektdaten vom Archiv-Node abgerufen. Das Wiederherstellen von Objektdaten auf einem Storage-Node aus einem Archiv-Node dauert länger als die Wiederherstellung von Kopien aus anderen Storage-Nodes, da die Latenz beim Abrufen von Daten aus externen Archiv-Storage-Systemen zu einer Verzögerung führt.

Informationen zum `repair-data` Skript

Zum Wiederherstellen von Objektdaten führen Sie den `repair-data` Skript: Dieses Skript startet den Prozess der Wiederherstellung von Objektdaten und arbeitet mit ILM-Scans zusammen, um sicherzustellen, dass ILM-Regeln eingehalten werden.

Wählen Sie unten **replizierte Daten** oder **Erasure-codierte (EC) Daten** aus, um die verschiedenen Optionen für das `repair-data` Skript erstellen, unabhängig davon, ob Sie replizierte Daten oder Erasure Coding-Daten wiederherstellen. Wenn Sie beide Datentypen wiederherstellen müssen, müssen Sie beide Befehlssets ausführen.



Weitere Informationen zum `repair-data` Skript, geben Sie ein `repair-data --help` Über die Befehlszeile des primären Admin-Knotens.

Replizierte Daten

Zwei Befehle sind zum Wiederherstellen replizierter Daten verfügbar, unabhängig davon, ob Sie den gesamten Node oder nur bestimmte Volumes auf dem Node reparieren müssen:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Sie können Reparaturen replizierter Daten mit diesem Befehl verfolgen:

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

Zwei Befehle sind zum Wiederherstellen von Erasure-codierten Daten verfügbar. Dabei basiert es darauf, ob Sie den gesamten Node reparieren müssen oder nur bestimmte Volumes auf dem Node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Sie können Reparaturen von Daten, die auf Erasure-Coding-Verfahren codiert wurden, mit diesem Befehl verfolgen:

```
repair-data show-ec-repair-status
```



Der EC-Reparaturauftrag reserviert vorübergehend eine große Menge an Lagerung. Storage-Warnmeldungen können zwar ausgelöst werden, werden aber nach Abschluss der Reparatur behoben. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt der EC-Reparaturauftrag fehl. Speicherreservierungen werden freigegeben, wenn der EC-Reparaturauftrag abgeschlossen wurde, unabhängig davon, ob der Job fehlgeschlagen oder erfolgreich war.

Suchen Sie nach Hostnamen für Speicherknoten

1. Melden Sie sich beim primären Admin-Node an:

- Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:
- 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 `#`.

2. Verwenden Sie die `/etc/hosts` Datei, um den Hostnamen des Speicher-Knotens für die wiederhergestellten Speicher-Volumes zu finden. Um eine Liste aller Nodes im Raster anzuzeigen, geben Sie Folgendes ein: `cat /etc/hosts`.

Reparieren Sie Daten, wenn alle Volumes ausgefallen sind

Wenn alle Storage-Volumes ausgefallen sind, reparieren Sie den gesamten Node. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn nur einige Volumes gescheitert sind, gehen Sie zu [wenn nur einige Volumes ausgefallen sind](#).



Sie können nicht ausgeführt werden `repair-data` Betrieb für mehr als einen Node gleichzeitig. Wenden Sie sich an den technischen Support, um mehrere Nodes wiederherzustellen.

Replizierte Daten

Wenn in Ihrem Grid replizierte Daten enthalten sind, verwenden Sie das `repair-data start-replicated-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die replizierten Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Siehe [Monitoring und Fehlerbehebung](#).

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `repair-data start-ec-node-repair` Befehl mit dem `--nodes` Option zum Reparieren des gesamten Speicherknoten.

Mit diesem Befehl werden die Erasure-codierte Daten auf einem Storage-Node mit dem Namen SG-DC-SN3 repariert:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies `repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Reparieren Sie Daten, wenn nur einige Volumes ausgefallen sind

Wenn nur einige Volumes ausgefallen sind, die betroffenen Volumes reparieren. Befolgen Sie die Anweisungen für **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beide, je nachdem, ob Sie replizierte Daten, Erasure-codierte (EC) Daten oder beide verwenden.

Wenn alle Volumes ausgefallen sind, gehen Sie zu [wenn alle Volumes ausgefallen sind](#).

Geben Sie die Volume-IDs in hexadezimal ein. Beispiel: `0000` Ist der erste Band und `000F` Ist der sechzehnte Band. Sie können ein Volume, einen Bereich von Volumes oder mehrere Volumes angeben, die sich nicht in einer Sequenz befinden.

Alle Volumes müssen sich auf demselben Speicherknoten befinden. Wenn Sie Volumes für mehr als einen Speicherknoten wiederherstellen müssen, wenden Sie sich an den technischen Support.

Replizierte Daten

Wenn Ihr Grid replizierte Daten enthält, verwenden Sie das `start-replicated-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt replizierte Daten auf das Volume wieder her 0002 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Bereich von Volumes: Dieser Befehl stellt replizierte Daten auf alle Volumes im Bereich wieder her 0003 Bis 0009 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Mehrere Volumes nicht in einer Sequenz: Dieser Befehl stellt replizierte Daten in Volumes wieder her 0001, 0005, und 0008 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Während Objektdaten wiederhergestellt werden, wird die Warnmeldung **Objekte verloren** ausgelöst, wenn das StorageGRID System replizierte Objektdaten nicht finden kann. Auf Storage-Nodes im gesamten System können Warnmeldungen ausgelöst werden. Sie sollten die Ursache des Schadens bestimmen und feststellen, ob eine Wiederherstellung möglich ist. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.

EC-Daten (Erasure Coding)

Wenn in Ihrem Grid Daten zur Einhaltung von Datenkonsistenz (Erasure Coding) enthalten sind, verwenden Sie den `start-ec-volume-repair` Befehl mit dem `--nodes` Option zum Identifizieren des Knotens. Fügen Sie dann entweder die hinzu `--volumes` Oder `--volume-range` Option, wie in den folgenden Beispielen dargestellt.

Einzelnes Volume: Dieser Befehl stellt die mit dem Löschen kodierte Daten auf das Volume wieder her 0007 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Bereich von Volumes: Dieser Befehl stellt Daten mit Löschungscode auf alle Volumes im Bereich wieder her 0004 Bis 0006 Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Mehrere Volumes nicht in einer Sequenz: Dieser Befehl stellt Erasure-codierte Daten auf Volumes wieder her 000A, 000C, und 000E Auf einem Storage-Node mit dem Namen SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Der `repair-data` Der Vorgang gibt einen eindeutigen zurück `repair ID` Das identifiziert dies

`repair_data` Betrieb. Verwenden Sie diese Option `repair ID` Den Fortschritt und das Ergebnis des verfolgen `repair_data` Betrieb. Beim Abschluss des Wiederherstellungsprozesses wird kein weiteres Feedback zurückgegeben.



Reparaturen von Daten, die auf Löschung codiert wurden, können beginnen, während einige Storage-Nodes offline sind. Die Reparatur ist abgeschlossen, wenn alle Nodes verfügbar sind.

Überwachen Sie Reparaturen

Überwachen Sie den Status der Reparaturaufträge, je nachdem, ob Sie **replizierte Daten**, **Erasure-codierte (EC) Daten** oder beides verwenden.

Replizierte Daten

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES Storage Node wird repariert ILM** aus.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid Speicherknoten, der repariert wird LDR Datenspeicher** aus.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA):** Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM):** Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.
- Wenn Sie optional einen geschätzten Fertigstellungsgrad für die replizierte Reparatur erhalten möchten, fügen Sie den hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:

- Wählen Sie **SUPPORT Tools Kennzahlen** aus, um die voraussichtliche Zeit bis zur Fertigstellung und den Prozentsatz für den Abschluss des aktuellen Jobs anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
- Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data` Betriebliche Gründe:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

```
repair-data show-ec-repair-status
```

Die Ausgabe enthält Informationen, einschließlich `repair ID`, Für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Überprüfen Sie den Speicherstatus nach der Wiederherstellung des Speicherknoten-Systemlaufwerks

Nach der Wiederherstellung des Systemlaufwerks für einen Speicherknoten müssen Sie überprüfen, ob der gewünschte Status des Speicherknoten auf Online gesetzt ist, und vergewissern Sie sich, dass der Status beim Neustart des Speicherknotenservers standardmäßig online ist.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Der Speicherknoten wurde wiederhergestellt und die Datenwiederherstellung ist abgeschlossen.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Überprüfen Sie die Werte von **wiederhergestellten Speicherknoten > LDR > Storage > Speicherzustand — gewünscht** und **Speicherstatus — Strom**.

Der Wert beider Attribute sollte Online sein.

3. Wenn der Speicherstatus — gewünscht auf schreibgeschützt eingestellt ist, führen Sie die folgenden

Schritte aus:

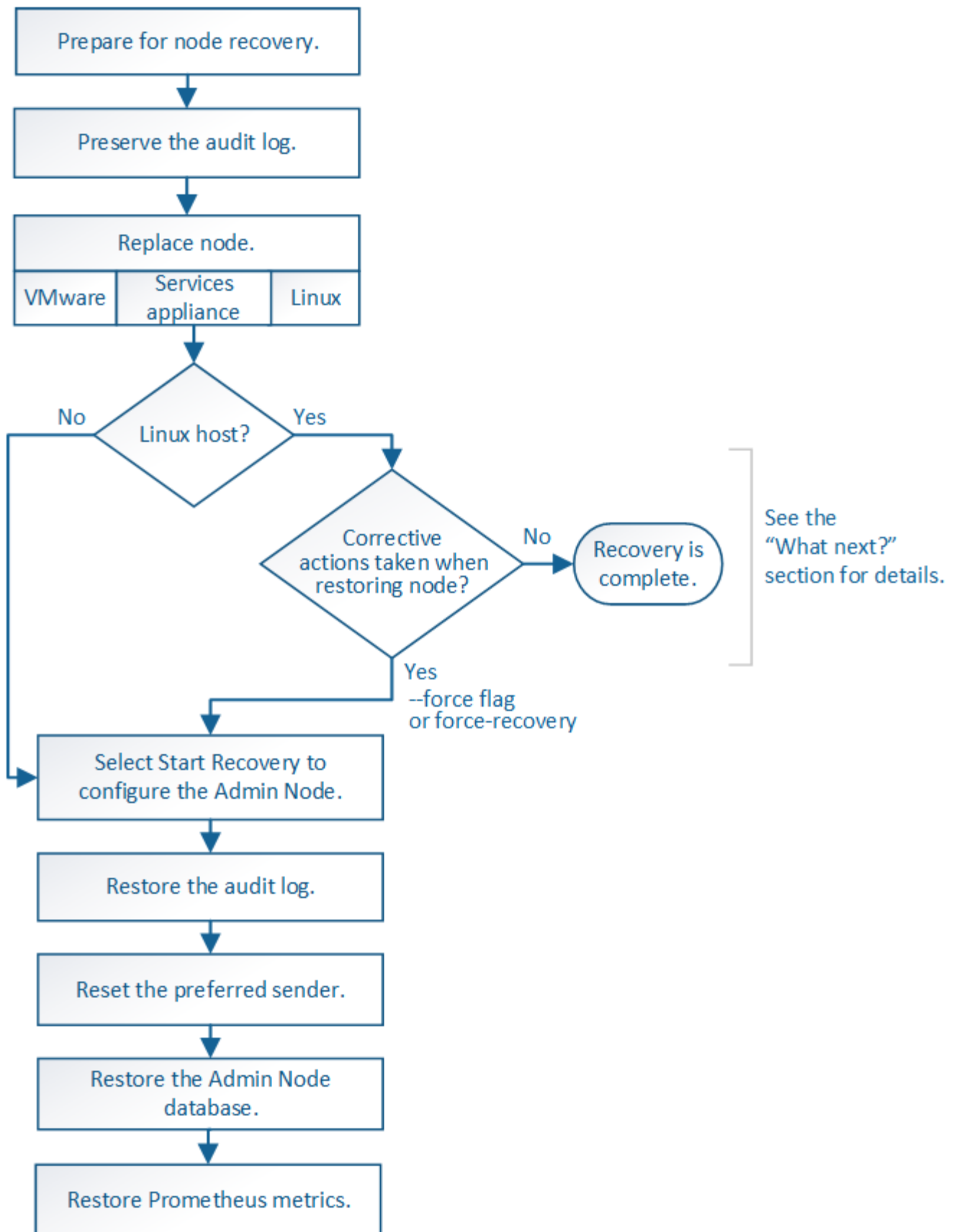
- a. Klicken Sie auf die Registerkarte **Konfiguration**.
- b. Wählen Sie aus der Dropdown-Liste **Storage State — gewünschte** die Option **Online** aus.
- c. Klicken Sie Auf **Änderungen Übernehmen**.
- d. Klicken Sie auf die Registerkarte **Übersicht** und bestätigen Sie, dass die Werte von **Speicherzustand — gewünscht** und **Speicherzustand — Aktuell** auf Online aktualisiert werden.

Wiederherstellung bei Ausfällen des Admin-Nodes

Der Wiederherstellungsprozess für einen Admin-Knoten hängt davon ab, ob es sich um den primären Admin-Knoten oder einen nicht-primären Admin-Knoten handelt.

Über diese Aufgabe

Die Schritte für die Wiederherstellung eines primären oder nicht primären Admin-Knotens auf hoher Ebene sind identisch, wobei sich die Details der einzelnen Schritte unterscheiden.



Befolgen Sie immer den richtigen Wiederherstellungsvorgang für den Admin-Knoten, den Sie wiederherstellen. Die Verfahren sehen auf hohem Niveau gleich aus, unterscheiden sich aber in den Details.

Verwandte Informationen

Wahlmöglichkeiten

- [Wiederherstellung nach Ausfällen des primären Admin-Nodes](#)
- [Wiederherstellung nach Ausfällen von Admin-Nodes außerhalb des primären Standorts](#)

Wiederherstellung nach Ausfällen des primären Admin-Nodes

Sie müssen einen bestimmten Satz von Aufgaben ausführen, um nach einem Ausfall eines primären Admin-Knotens wiederherstellen zu können. Der primäre Admin-Node hostet den Configuration Management Node (CMN)-Service für das Grid.

Über diese Aufgabe

Ein fehlgeschlagener primärer Admin-Node sollte umgehend ersetzt werden. Der Configuration Management Node (CMN)-Dienst auf dem primären Admin-Node ist für die Ausgabe von Objektkennungen für das Grid verantwortlich. Diese Kennungen werden Objekten bei ihrer Aufnahme zugewiesen. Neue Objekte können erst dann aufgenommen werden, wenn Identifikatoren verfügbar sind. Die Objektaufnahme kann fortgesetzt werden, während das CMN nicht verfügbar ist, da die Identifikatoren ungefähr einen Monat im Grid zwischengespeichert werden. Nachdem jedoch die gecachten Kennungen erschöpft sind, können keine neuen Objekte hinzugefügt werden.



Sie müssen einen fehlerhaften primären Administrator-Node innerhalb von etwa einem Monat reparieren oder ersetzen. Andernfalls kann das Grid die Aufnahme neuer Objekte verlieren. Der genaue Zeitraum hängt von der Geschwindigkeit der Objekterfassung ab: Wenn Sie eine genauere Bewertung des Zeitrahmens für Ihr Grid benötigen, wenden Sie sich an den technischen Support.

Prüfprotokolle vom fehlgeschlagenen primären Admin-Node kopieren

Wenn Sie Audit-Protokolle vom fehlgeschlagenen primären Admin-Node kopieren können, sollten Sie diese beibehalten, um den Datensatz der Systemaktivität und -Nutzung des Rasters beizubehalten. Sie können die erhaltenen Audit-Protokolle nach dem wiederhergestellten primären Admin-Knoten wiederherstellen, nachdem er in Betrieb ist.

Mit diesem Verfahren werden die Audit-Log-Dateien vom fehlgeschlagenen Admin-Node in einen temporären Speicherort auf einem separaten Grid-Node kopiert. Diese erhaltenen Audit-Protokolle können dann in den Ersatz-Admin-Node kopiert werden. Audit-Protokolle werden nicht automatisch auf den neuen Admin-Node kopiert.

Je nach Art des Fehlers können Sie unter Umständen keine Prüfprotokolle von einem fehlgeschlagenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Node verfügt, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen zum Audit-Protokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Node enthält, können Sie die Audit-Protokolle von einem anderen Admin-Node wiederherstellen.



Wenn jetzt auf dem fehlgeschlagenen Admin-Node die Überwachungsprotokolle nicht mehr zugegriffen werden kann, können Sie später, z. B. nach der Hostwiederherstellung, darauf zugreifen.

1. Melden Sie sich nach Möglichkeit beim fehlgeschlagenen Admin-Knoten an. Melden Sie sich andernfalls

beim primären Admin-Node oder einem anderen Admin-Node an, falls verfügbar.

- 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 `#`.

- 2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Protokolldatei erstellt wird:`service ams stop`
- 3. Benennen Sie die Datei `audit.log` um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

Benennen Sie `audit.log` in einen eindeutigen nummerierten Dateinamen um, z. B. `yyyy-mm-dd.txt.1`.
Beispielsweise können Sie die Datei `audit.log` in `2015-10-25.txt.1` umbenennen`cd /var/local/audit/export/`

- 4. AMS-Dienst neu starten: `service ams start`
- 5. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien in einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

- 6. Alle Audit-Log-Dateien kopieren: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

- 7. Melden Sie sich als Root an: `exit`

Primären Admin-Node ersetzen

Um einen primären Admin-Node wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen fehlgeschlagenen primären Admin-Node durch einen primären Admin-Node ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen primären Admin-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen primären Admin-Node ersetzen, der auf einer Services-Appliance gehostet wird.

Verwenden Sie das Verfahren, das der für den Node ausgewählten Ersatzplattform entspricht. Nachdem Sie den Knotenaustausch abgeschlossen haben (der für alle Node-Typen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die primäre Admin-Knoten-Wiederherstellung geleitet.

Austauschplattform	Verfahren
VMware	Einen VMware-Knoten ersetzen

Austauschplattform	Verfahren
Linux	Ersetzen Sie einen Linux-Knoten
SG100- und SG1000-Services-Appliances	Ersetzen Sie eine Service Appliance
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Primären Ersatzadministrator-Knoten konfigurieren

Der Ersatzknoten muss als primärer Admin-Node für Ihr StorageGRID System konfiguriert sein.

Was Sie benötigen

- Für primäre Admin-Knoten, die auf virtuellen Maschinen gehostet werden, muss die virtuelle Maschine bereitgestellt, eingeschaltet und initialisiert werden.
- Für primäre Admin-Nodes, die auf einer Services-Appliance gehostet werden, haben Sie die Appliance ersetzt und die installierte Software installiert. Informationen zum Gerät finden Sie im Installationshandbuch.

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

- Sie müssen über die neueste Sicherung der Wiederherstellungspaket-Datei verfügen (`sgws-recovery-package-id-revision.zip`).
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Schritte

1. Öffnen Sie Ihren Webbrowser, und navigieren Sie zu https://primary_admin_node_ip.

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



Install a StorageGRID system



Recover a failed primary Admin
Node

2. Klicken Sie auf **Wiederherstellen eines fehlgeschlagenen primären Admin-Knotens**.
3. Laden Sie das aktuellste Backup des Wiederherstellungspakets hoch:
 - a. Klicken Sie Auf **Durchsuchen**.
 - b. Suchen Sie die aktuellste Wiederherstellungspakedatei für Ihr StorageGRID-System und klicken Sie auf **Öffnen**.
4. Geben Sie die Provisionierungs-Passphrase ein.
5. Klicken Sie Auf **Wiederherstellung Starten**.

Der Wiederherstellungsprozess beginnt. Der Grid Manager ist möglicherweise einige Minuten lang nicht mehr verfügbar, wenn die erforderlichen Dienste gestartet werden. Wenn die Wiederherstellung abgeschlossen ist, wird die Anmeldeseite angezeigt.

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Zertifikat der Standardverwaltungsoberfläche konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Node auf die Vertrauensbasis in Active Directory Federation Services (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.



Informationen zum Konfigurieren eines Vertrauensverhältnisses mit einer vertrauenswürdigen Partei finden Sie in den Anweisungen zur Verwaltung von StorageGRID. Melden Sie sich zum Zugriff auf das Standard-Serverzertifikat bei der Eingabeaufforderung des Admin-Knotens an. Wechseln Sie zum `/var/local/mgmt-api` Und wählen Sie das aus `server.crt` Datei:

7. Bestimmen Sie, ob Sie einen Hotfix anwenden müssen.

- a. Melden Sie sich mit einem bei Grid Manager an [Unterstützter Webbrowser](#).
- b. Wählen Sie **KNOTEN**.
- c. Wählen Sie in der Liste links den primären Admin-Node aus.
- d. Notieren Sie sich auf der Registerkarte Übersicht die Version, die im Feld **Softwareversion** angezeigt wird.
- e. Wählen Sie einen beliebigen anderen Grid-Knoten aus.
- f. Notieren Sie sich auf der Registerkarte Übersicht die Version, die im Feld **Softwareversion** angezeigt wird.
 - Wenn die in den Feldern **Software Version** angezeigten Versionen identisch sind, müssen Sie keinen Hotfix anwenden.
 - Wenn die in den Feldern **Softwareversion** angezeigten Versionen anders sind, müssen Sie einen Hotfix anwenden, um den wiederhergestellten primären Admin-Knoten auf dieselbe Version zu aktualisieren.

Verwandte Informationen

[StorageGRID verwalten](#)

[StorageGRID Hotfix Verfahren](#)

Prüfprotokoll auf wiederhergestellten primären Admin-Knoten wiederherstellen

Wenn Sie das Revisionsprotokoll vom fehlgeschlagenen primären Admin-Knoten erhalten konnten, können Sie es in den primären Admin-Knoten kopieren, den Sie wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Nachdem der ursprüngliche Admin-Node fehlgeschlagen ist, müssen Sie die Prüfprotokolle an einen anderen Speicherort kopiert haben.

Wenn ein Admin-Knoten ausfällt, gehen in diesem Admin-Knoten gespeicherte Prüfprotokolle möglicherweise verloren. Es könnte möglich sein, Daten vor Verlust durch Kopieren von Prüfprotokollen aus dem fehlgeschlagenen Admin-Knoten und dann die Wiederherstellung dieser Prüfprotokolle auf den wiederhergestellten Admin-Knoten. Je nach Ausfall ist es möglicherweise nicht möglich, Prüfprotokolle vom fehlgeschlagenen Admin-Node zu kopieren. Wenn die Bereitstellung mehr als einen Admin-Node hat, können Sie in diesem Fall Audit-Protokolle von einem anderen Admin-Node wiederherstellen, da Audit-Protokolle auf allen Admin-Nodes repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Audit-Protokoll nicht vom fehlgeschlagenen Knoten kopiert werden kann, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen in das Auditprotokoll, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.

Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:



- Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.

Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#) Entsprechende Details.

Schritte

1. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@recovery_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:

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

2. Prüfen Sie, welche Audit-Dateien erhalten wurden: `cd /var/local/audit/export`

3. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.
5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten: `chown ams-user:bycast *`
6. Melden Sie sich als Root an: `exit`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

[StorageGRID verwalten](#)

Bevorzugter Absender auf wiederhergestellten primären Admin-Knoten zurücksetzen

Wenn der primäre Admin-Knoten, den Sie wiederherstellen, derzeit als bevorzugter Absender von Warnmeldungen, Alarmanmeldungen und AutoSupport-Meldungen eingestellt ist, müssen Sie diese Einstellung neu konfigurieren.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.

Schritte

1. Wählen Sie **KONFIGURATION System Anzeigeoptionen**.
2. Wählen Sie den wiederhergestellten Admin-Knoten aus der Dropdown-Liste **bevorzugter Absender** aus.
3. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

[StorageGRID verwalten](#)

Stellen Sie die Admin-Knoten-Datenbank wieder her, wenn Sie den primären Admin-Knoten wiederherstellen

Wenn Sie die historischen Informationen über Attribute, Alarme und Alarme auf einem primären Admin-Node, der ausgefallen ist, behalten möchten, können Sie die Admin-Node-Datenbank wiederherstellen. Sie können diese Datenbank nur wiederherstellen, wenn Ihr StorageGRID-System einen anderen Admin-Knoten enthält.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält folgende Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT Tools Grid Topology** verfügbar sind.

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen für Server und Services, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID-System einen anderen Admin-Knoten hat, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Knoten-Datenbank von einem nicht-primären Admin-Knoten (der `_Quell-Admin-Knoten_`) auf den wiederhergestellten primären Admin-Knoten kopieren. Wenn Ihr System nur einen primären Admin-Knoten hat, können Sie die Admin-Knoten-Datenbank nicht wiederherstellen.



Das Kopieren der Admin-Node-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

1. Melden Sie sich beim Quell-Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführten 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:
2. Beenden Sie den MI-Dienst vom Quell-Admin-Node: `service mi stop`
3. Beenden Sie vom Quell-Admin-Node den Management Application Program Interface (Management-API)-Service: `service mgmt-api stop`
4. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
 - a. Melden Sie sich beim wiederhergestellten Admin-Knoten 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:
 - b. Beenden SIE DEN MI-Dienst: `service mi stop`
 - c. Beenden Sie den Management API-Service: `service mgmt-api stop`
 - d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
 - f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem wiederhergestellten Admin-Knoten überschreiben möchten.

Die Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten.
 - h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein: `ssh-add -D`
5. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Stellen Sie bei der Wiederherstellung des primären Admin-Knotens Prometheus-Kennzahlen wieder her

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem primären Admin-Node gewartet wurden, der ausgefallen ist. Die Prometheus Kennzahlen können nur wiederhergestellt werden, wenn Ihr StorageGRID System einen anderen Admin-Knoten enthält.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten gepflegten Kennzahlen verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Node gestartet wurde, zeichnet er die Metriken auf, als ob Sie eine neue Installation des StorageGRID-Systems durchgeführt hatten.

Wenn Sie einen primären Admin-Knoten wiederhergestellt haben und Ihr StorageGRID-System einen anderen Admin-Knoten hat, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank von einem nicht-primären Admin-Knoten (den *Source Admin-Knoten*) auf den wiederhergestellten primären Admin-Knoten kopieren. Wenn Ihr System nur einen primären Admin-Knoten hat, können Sie die Prometheus-Datenbank nicht wiederherstellen.



Das Kopieren der Prometheus-Datenbank dauert möglicherweise eine Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

1. Melden Sie sich beim Quell-Admin-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:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
 - a. Melden Sie sich beim wiederhergestellten Admin-Knoten 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:
 - b. Stoppen Sie den Prometheus Service: `service prometheus stop`
 - c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
 - e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
 - f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem wiederhergestellten Admin-Knoten zerstören möchten.

Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten. Der folgende Status wird angezeigt:

Datenbank geklont, Dienste starten

- a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein: `ssh-add -D`
4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu: `service prometheus start`

Wiederherstellung nach Ausfällen von Admin-Nodes außerhalb des primären Standorts

Sie müssen die folgenden Aufgaben durchführen, um nach einem Ausfall eines nicht

primären Admin-Knotens wiederherzustellen. Ein Admin-Node hostet den Configuration Management Node (CMN)-Service und ist als primärer Admin-Node bekannt. Obwohl Sie mehrere Admin-Nodes haben können, enthält jedes StorageGRID-System nur einen primären Admin-Node. Alle anderen Admin-Nodes sind nicht primäre Admin-Nodes.

Verwandte Informationen

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

Prüfprotokolle vom fehlgeschlagenen Admin-Knoten kopieren

Wenn Sie in der Lage sind, Audit-Protokolle vom fehlgeschlagenen Admin-Node zu kopieren, sollten Sie diese beibehalten, um die Aufzeichnung der Systemaktivität und -Nutzung des Rasters beizubehalten. Sie können die erhaltenen Audit-Protokolle nach dem Wiederherstellen des nicht-primären Admin-Knotens wiederherstellen, nachdem er ausgeführt wurde.

Mit diesem Verfahren werden die Audit-Log-Dateien vom fehlgeschlagenen Admin-Node in einen temporären Speicherort auf einem separaten Grid-Node kopiert. Diese erhaltenen Audit-Protokolle können dann in den Ersatz-Admin-Node kopiert werden. Audit-Protokolle werden nicht automatisch auf den neuen Admin-Node kopiert.

Je nach Art des Fehlers können Sie unter Umständen keine Prüfprotokolle von einem fehlgeschlagenen Admin-Knoten kopieren. Wenn die Bereitstellung nur über einen Admin-Node verfügt, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen zum Audit-Protokoll in einer neuen leeren Datei und zuvor aufgezeichnete Daten gehen verloren. Wenn die Bereitstellung mehr als einen Admin-Node enthält, können Sie die Audit-Protokolle von einem anderen Admin-Node wiederherstellen.



Wenn jetzt auf dem fehlgeschlagenen Admin-Node die Überwachungsprotokolle nicht mehr zugegriffen werden kann, können Sie später, z. B. nach der Hostwiederherstellung, darauf zugreifen.

1. Melden Sie sich nach Möglichkeit beim fehlgeschlagenen Admin-Knoten an. Melden Sie sich andernfalls beim primären Admin-Node oder einem anderen Admin-Node an, falls verfügbar.
 - 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 `#`.

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Protokolldatei erstellt wird:

```
service oms
stop
```
3. Benennen Sie die Datei `audit.log` um, damit sie die vorhandene Datei nicht überschreiben kann, wenn Sie sie in den wiederhergestellten Admin-Node kopieren.

Benennen Sie `audit.log` in einen eindeutigen nummerierten Dateinamen um, z. B. `yyyy-mm-dd.txt`.
Beispielsweise können Sie die Datei `audit.log` in `2015-10-25.txt` umbenennen:
`cd /var/local/audit/export/`

4. AMS-Dienst neu starten: `service ams start`

5. Erstellen Sie das Verzeichnis, um alle Audit-Log-Dateien in einen temporären Speicherort auf einem separaten Grid-Knoten zu kopieren: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

6. Alle Audit-Log-Dateien kopieren: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

7. Melden Sie sich als Root an: `exit`

Nicht-primärer Admin-Node ersetzen

Um einen nicht-primären Admin-Node wiederherzustellen, müssen Sie zuerst die physische oder virtuelle Hardware ersetzen.

Sie können einen nicht primären Admin-Node durch einen nicht-primären Admin-Node ersetzen, der auf derselben Plattform ausgeführt wird, oder Sie können einen nicht-primären Admin-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen nicht-primären Admin-Node ersetzen, der auf einer Services Appliance gehostet wird.

Verwenden Sie das Verfahren, das der für den Node ausgewählten Ersatzplattform entspricht. Nachdem Sie den Knotenaustausch abgeschlossen haben (der für alle Node-Typen geeignet ist), werden Sie durch dieses Verfahren zum nächsten Schritt für die Wiederherstellung eines nicht-primären Admin-Knotens geleitet.

Austauschplattform	Verfahren
VMware	Einen VMware-Knoten ersetzen
Linux	Ersetzen Sie einen Linux-Knoten
SG100- und SG1000-Services-Appliances	Ersetzen Sie eine Service Appliance
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren

Nach dem Ersetzen eines nicht-primären Admin-Knotens müssen Sie im Grid-Manager die Option Wiederherstellung starten wählen, um den neuen Knoten als Ersatz für den fehlgeschlagenen Knoten zu konfigurieren.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **WARTUNG Tasks Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:
`storagegrid node force-recovery node-name`
- **Appliance:** Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Geräteknoten durch Ausführen in einen vorinstallierten Zustand wiederherstellen `sgareinstall` Auf dem Node.

6. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist und das Vertrauen der Vertrauensstelle für den wiederhergestellten Admin-Knoten für das Zertifikat der Standardverwaltungsoberfläche konfiguriert wurde, aktualisieren (oder löschen und neu erstellen) das Vertrauen des Node auf die Vertrauensbasis in Active Directory Federation Services (AD FS). Verwenden Sie das neue Standard-Serverzertifikat, das während der Wiederherstellung des Admin-Knotens generiert wurde.



Informationen zum Konfigurieren eines Vertrauensverhältnisses mit einer vertrauenswürdigen Partei finden Sie in den Anweisungen zur Verwaltung von StorageGRID. Melden Sie sich zum Zugriff auf das Standard-Serverzertifikat bei der Eingabeaufforderung des Admin-Knotens an. Wechseln Sie zum `/var/local/mgmt-api` Und wählen Sie das aus `server.crt` Datei:

Verwandte Informationen

[StorageGRID verwalten](#)

[Appliance für die Neuinstallation vorbereiten \(nur Plattformaustausch\)](#)

Stellen Sie das Prüfprotokoll auf dem wiederhergestellten Admin-Node, der nicht dem primären Administrator gehört, wieder her

Wenn Sie das Audit-Protokoll vom fehlgeschlagenen nicht-primären Admin-Node erhalten konnten, damit die Informationen des historischen Audit-Protokolls beibehalten werden,

können Sie es in den nicht-primären Admin-Node kopieren, den Sie wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Nachdem der ursprüngliche Admin-Node fehlgeschlagen ist, müssen Sie die Prüfprotokolle an einen anderen Speicherort kopiert haben.

Wenn ein Admin-Knoten ausfällt, gehen in diesem Admin-Knoten gespeicherte Prüfprotokolle möglicherweise verloren. Es könnte möglich sein, Daten vor Verlust durch Kopieren von Prüfprotokollen aus dem fehlgeschlagenen Admin-Knoten und dann die Wiederherstellung dieser Prüfprotokolle auf den wiederhergestellten Admin-Knoten. Je nach Ausfall ist es möglicherweise nicht möglich, Prüfprotokolle vom fehlgeschlagenen Admin-Node zu kopieren. Wenn die Bereitstellung mehr als einen Admin-Node hat, können Sie in diesem Fall Audit-Protokolle von einem anderen Admin-Node wiederherstellen, da Audit-Protokolle auf allen Admin-Nodes repliziert werden.

Wenn nur ein Admin-Knoten vorhanden ist und das Audit-Protokoll nicht vom fehlgeschlagenen Knoten kopiert werden kann, startet der wiederhergestellte Admin-Knoten die Aufzeichnung von Ereignissen in das Auditprotokoll, als ob die Installation neu ist.

Sie müssen einen Admin-Knoten so schnell wie möglich wiederherstellen, um die Protokollierungsfunktion wiederherzustellen.



Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:

- Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
- Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.

Siehe [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#) Entsprechende Details.

Schritte

1. Melden Sie sich beim wiederhergestellten Admin-Knoten an:

a. Geben Sie den folgenden Befehl ein:

```
ssh admin@recovery_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:

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

2. Prüfen Sie, welche Audit-Dateien erhalten wurden:

```
cd /var/local/audit/export
```

3. Kopieren Sie die erhaltenen Audit-Log-Dateien auf den wiederhergestellten Admin-Knoten:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Geben Sie bei der entsprechenden Eingabeaufforderung das Passwort für den Administrator ein.

4. Löschen Sie aus Sicherheitsgründen die Prüfprotokolle vom fehlgeschlagenen Grid-Knoten, nachdem Sie überprüft haben, ob sie erfolgreich auf den wiederhergestellten Admin-Node kopiert wurden.
5. Aktualisieren Sie die Benutzer- und Gruppeneinstellungen der Audit-Log-Dateien auf dem wiederhergestellten Admin-Knoten:

```
chown ams-user:bycast *
```

6. Melden Sie sich als Root an: `exit`

Sie müssen auch alle bereits vorhandenen Clientzugriffe auf die Revisionsfreigabe wiederherstellen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

[StorageGRID verwalten](#)

Setzen Sie den bevorzugten Absender auf den wiederhergestellten Admin-Node, der nicht primär ist, zurück

Wenn der nicht-primäre Admin-Node, den Sie wiederherstellen, derzeit als bevorzugter Absender von Warnmeldungen, Alarmbenachrichtigungen und AutoSupport-Meldungen eingestellt ist, müssen Sie diese Einstellung im StorageGRID-System neu konfigurieren.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.

Schritte

1. Wählen Sie **KONFIGURATION System Anzeigeoptionen**.
2. Wählen Sie den wiederhergestellten Admin-Knoten aus der Dropdown-Liste **bevorzugter Absender** aus.
3. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

[StorageGRID verwalten](#)

Stellen Sie die Admin-Node-Datenbank wieder her, wenn Sie einen nicht-primären Admin-Node wiederherstellen

Wenn Sie die historischen Informationen zu Attributen, Alarmen und Warnmeldungen bei einem nicht primären Admin-Node behalten möchten, der ausgefallen ist, können Sie die Admin-Knoten-Datenbank vom primären Admin-Node wiederherstellen.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in seiner Admin-Knoten-Datenbank gespeicherten historischen Informationen verloren. Diese Datenbank enthält folgende Informationen:

- Meldungsverlauf
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT Tools Grid Topology** verfügbar sind.

Wenn Sie einen Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine leere Admin-Knoten-Datenbank auf dem wiederhergestellten Knoten. Die neue Datenbank enthält jedoch nur Informationen für Server und Services, die derzeit Teil des Systems sind oder später hinzugefügt werden.

Wenn Sie einen nicht-primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Informationen wiederherstellen, indem Sie die Admin-Node-Datenbank vom primären Admin-Knoten (den_Quell-Admin-Node_) auf den wiederhergestellten Knoten kopieren.



Das Kopieren der Admin-Node-Datenbank kann mehrere Stunden dauern. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quellknoten angehalten werden.

1. Melden Sie sich beim Quell-Admin-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:
2. Führen Sie den folgenden Befehl vom Quell-Admin-Knoten aus. Geben Sie dann die Provisionierungs-Passphrase ein, wenn Sie dazu aufgefordert werden. `recover-access-points`
3. Beenden Sie den MI-Dienst vom Quell-Admin-Node: `service mi stop`
4. Beenden Sie vom Quell-Admin-Node den Management Application Program Interface (Management-API)-Service: `service mgmt-api stop`
5. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
 - a. Melden Sie sich beim wiederhergestellten Admin-Knoten 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:
 - b. Beenden SIE DEN MI-Dienst: `service mi stop`
 - c. Beenden Sie den Management API-Service: `service mgmt-api stop`
 - d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
 - f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem wiederhergestellten Admin-Knoten überschreiben möchten.

Die Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten.

- h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie `ssh-add -D`

6. Starten Sie die Dienste auf dem Quell-Admin-Node neu: `service servermanager start`

Stellen Sie Prometheus-Kennzahlen wieder her, wenn Sie einen nicht-primären Admin-Node wiederherstellen

Optional können Sie die historischen Metriken aufbewahren, die von Prometheus auf einem nicht primären Admin-Node gewartet wurden, der ausgefallen ist.

- Der wiederhergestellte Admin-Node muss installiert und ausgeführt werden.
- Das StorageGRID System muss mindestens zwei Admin-Nodes enthalten.
- Sie müssen die `Passwords.txt` Datei:
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Wenn ein Admin-Knoten ausfällt, gehen die in der Prometheus-Datenbank auf dem Admin-Knoten gepflegten Kennzahlen verloren. Wenn Sie den Admin-Knoten wiederherstellen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Nachdem der wiederhergestellte Admin-Node gestartet wurde, zeichnet er die Metriken auf, als ob Sie eine neue Installation des StorageGRID-Systems durchgeführt hatten.

Wenn Sie einen nicht-primären Admin-Knoten wiederhergestellt haben, können Sie die historischen Metriken wiederherstellen, indem Sie die Prometheus-Datenbank vom primären Admin-Knoten (den `_Source Admin-Node_`) auf den wiederhergestellten Admin-Knoten kopieren.



Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

1. Melden Sie sich beim Quell-Admin-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:
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie die folgenden Schritte auf dem wiederhergestellten Admin-Knoten aus:
 - a. Melden Sie sich beim wiederhergestellten Admin-Knoten 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:
 - b. Stoppen Sie den Prometheus Service: `service prometheus stop`

- c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
- d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
- e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Knoten auf den wiederhergestellten Admin-Knoten: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem wiederhergestellten Admin-Knoten zerstören möchten.

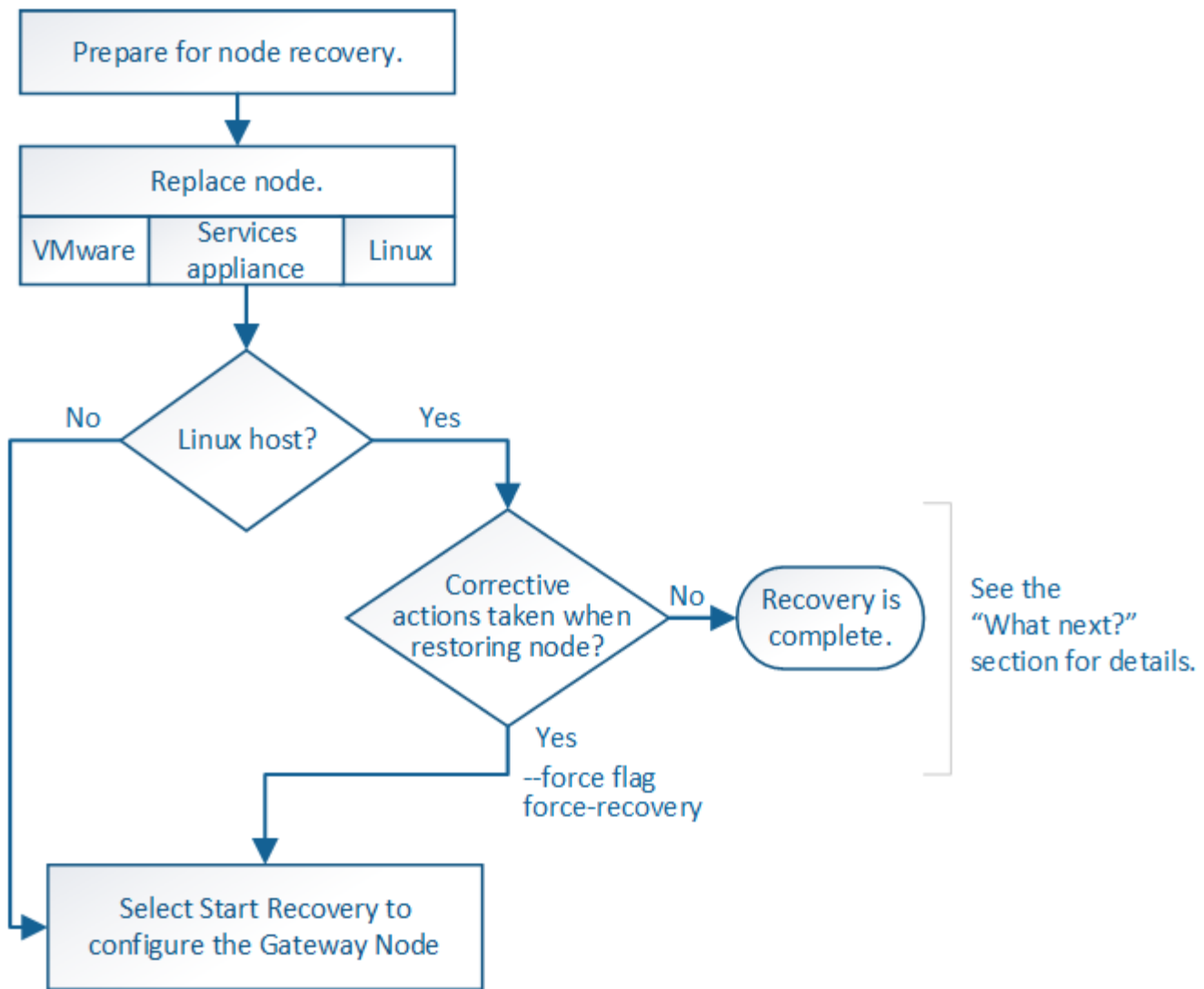
Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den wiederhergestellten Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den wiederhergestellten Admin-Knoten. Der folgende Status wird angezeigt:

Datenbank geklont, Dienste starten

- a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:`ssh-add -D`
4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node `neu.service prometheus start`

Wiederherstellung nach Gateway-Node-Ausfällen

Sie müssen eine Reihe von Aufgaben genau durchführen, um nach einem Gateway Node-Ausfall wiederherstellen zu können.



Verwandte Informationen

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

Gateway-Node Ersetzen

Sie können einen fehlgeschlagenen Gateway-Node durch einen Gateway-Node ersetzen, der auf derselben physischen oder virtuellen Hardware ausgeführt wird, oder Sie können einen Gateway-Node, der auf VMware oder einem Linux-Host ausgeführt wird, durch einen Gateway-Node ersetzen, der auf einer Services-Appliance gehostet wird.

Das Verfahren zum Austausch des Nodes, das Sie befolgen müssen, hängt davon ab, welche Plattform vom Austausch-Node verwendet wird. Nach Abschluss des Austauschverfahrens für den Node (geeignet für alle Node-Typen) werden Sie durch dieses Verfahren zum nächsten Schritt für die Gateway Node Recovery geleitet.

Austauschplattform	Verfahren
VMware	Einen VMware-Knoten ersetzen
Linux	Ersetzen Sie einen Linux-Knoten

Austauschplattform	Verfahren
SG100- und SG1000-Services-Appliances	Ersetzen Sie eine Service Appliance
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren

Nachdem Sie einen Gateway-Node ersetzt haben, müssen Sie im Grid Manager Recovery starten auswählen, um den neuen Node als Ersatz für den ausgefallenen Node zu konfigurieren.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **WARTUNG Tasks Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

- Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknotten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:
`storagegrid node force-recovery node-name`
- **Appliance:** Wenn Sie die Wiederherstellung nach dem Zurücksetzen des Vorgangs erneut versuchen möchten, müssen Sie den Geräteknoten durch Ausführen in einen vorinstallierten Zustand

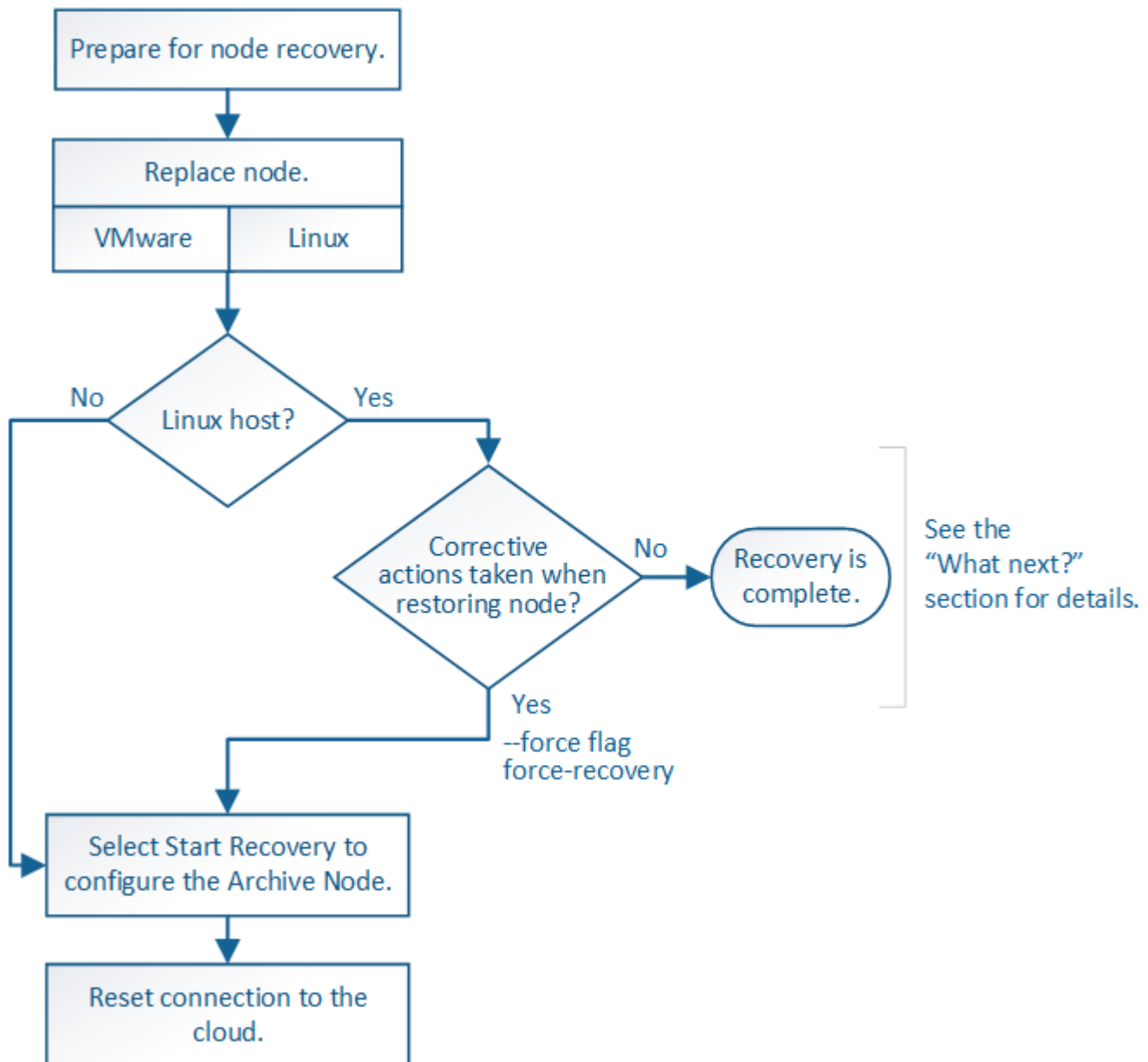
wiederherstellen `sgareinstall` Auf dem Node.

Verwandte Informationen

[Appliance für die Neuinstallation vorbereiten \(nur Plattformaustausch\)](#)

Wiederherstellung nach Ausfällen des Archivierungs-Nodes

Sie müssen eine Reihe von Aufgaben genau durchführen, um nach einem Ausfall des Archivierungs-Knotens wiederherstellen zu können.



Über diese Aufgabe

Die Wiederherstellung von Archivknoten ist von den folgenden Problemen betroffen:

- Wenn die ILM-Richtlinie für die Replizierung einer einzelnen Kopie konfiguriert ist

In einem StorageGRID-System, das für eine einzelne Objektkopie konfiguriert ist, kann ein Ausfall des Archiv-Nodes zu einem nicht wiederherstellbaren Verlust von Daten führen. Wenn ein Fehler auftritt, gehen

alle diese Objekte verloren. Sie müssen jedoch weiterhin Wiederherstellungsverfahren durchführen, um Ihr StorageGRID-System zu „bereinigen“ und verlorene Objektinformationen aus der Datenbank zu löschen.

- Wenn während der Wiederherstellung des Speicherknotens ein Ausfall des Archivknotens auftritt.

Wenn der Archivknoten bei der Verarbeitung der Massenabrufe im Rahmen einer Speicherknotenwiederherstellung ausfällt, Sie müssen das Verfahren wiederholen, um Kopien von Objektdaten auf den Storage-Node von Anfang an wiederherzustellen, um sicherzustellen, dass alle vom Archiv-Node abgerufenen Objektdaten auf dem Storage-Node wiederhergestellt werden.

Archivknoten Ersetzen

Um einen Archiv-Knoten wiederherzustellen, müssen Sie zuerst den Knoten ersetzen.

Sie müssen das Verfahren zum Ersetzen des Node für Ihre Plattform auswählen. Die Schritte zum Ersetzen eines Node sind für alle Typen von Grid-Nodes identisch.

Plattform	Verfahren
VMware	Einen VMware-Knoten ersetzen
Linux	Ersetzen Sie einen Linux-Knoten
OpenStack	Die von NetApp bereitgestellten Festplattendateien und Skripte für Virtual Machines von OpenStack werden für Recovery-Vorgänge nicht mehr unterstützt. Wenn Sie einen Knoten wiederherstellen müssen, der in einer OpenStack-Implementierung ausgeführt wird, laden Sie die Dateien für Ihr Linux-Betriebssystem herunter. Befolgen Sie dann das Verfahren zum Ersetzen eines Linux-Knotens.

Wählen Sie Wiederherstellung starten, um den Knoten Archiv zu konfigurieren

Nachdem Sie einen Archivknoten ersetzt haben, müssen Sie im Grid Manager die Option Wiederherstellung starten auswählen, um den neuen Knoten als Ersatz für den fehlgeschlagenen Knoten zu konfigurieren.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Der Ersatz-Node muss bereitgestellt und konfiguriert sein.

Schritte

1. Wählen Sie im Grid Manager die Option **WARTUNG Tasks Recovery**.
2. Wählen Sie in der Liste Ausstehende Knoten den Rasterknoten aus, den Sie wiederherstellen möchten.

Nodes werden nach ihrem Ausfall in der Liste angezeigt. Sie können jedoch keinen Node auswählen, bis er neu installiert wurde und zur Wiederherstellung bereit ist.

3. Geben Sie die **Provisioning-Passphrase** ein.
4. Klicken Sie Auf **Wiederherstellung Starten**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search Q				
Name	IPv4 Address	State	Recoverable	
104-217-S1	10.96.104.217	Unknown	✓	

Passphrase

Provisioning Passphrase

Start Recovery

5. Überwachen Sie den Fortschritt der Wiederherstellung in der Tabelle „Netzknoten wiederherstellen“.



Während der Wiederherstellungsvorgang läuft, können Sie auf **Zurücksetzen** klicken, um eine neue Wiederherstellung zu starten. Ein Info-Dialogfeld wird angezeigt, das angibt, dass der Knoten bei einem Zurücksetzen des Vorgangs in einen unbestimmten Zustand zurückgelassen wird.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Wenn Sie die Recovery nach dem Zurücksetzen der Prozedur erneut versuchen möchten, müssen Sie den Node in einen vorinstallierten Status wiederherstellen:

- **VMware:** Den bereitgestellten virtuellen Grid-Knoten löschen. Wenn Sie bereit sind, die Recovery neu zu starten, implementieren Sie den Node erneut.
- **Linux:** Starten Sie den Knoten neu, indem Sie diesen Befehl auf dem Linux-Host ausführen:

```
storagegrid node force-recovery node-name
```

Die Verbindung mit dem Archivierungs-Node zur Cloud wird zurückgesetzt

Nachdem Sie einen Archiv-Node wiederhergestellt haben, der die Cloud über die S3-API anzieht, müssen Sie die Konfigurationseinstellungen ändern, um Verbindungen zurückzusetzen. Ein ORSU-Alarm (Outbound Replication Status) wird ausgelöst, wenn der Archivknoten keine Objektdaten abrufen kann.



Wenn der Archivknoten über die TSM Middleware mit externem Storage verbunden ist, wird der Node automatisch zurückgesetzt und Sie müssen es nicht neu konfigurieren.

Was Sie benötigen

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

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten > ARC > Ziel**.
3. Bearbeiten Sie das Feld **Zugriffsschlüssel**, indem Sie einen falschen Wert eingeben und auf **Änderungen anwenden** klicken.
4. Bearbeiten Sie das Feld **Zugriffsschlüssel**, indem Sie den richtigen Wert eingeben und auf **Änderungen anwenden** klicken.

Alle Grid-Node-Typen: VMware Node ersetzen

Wenn Sie einen ausgefallenen StorageGRID-Node wiederherstellen, der auf VMware gehostet wurde, müssen Sie den ausgefallenen Node entfernen und einen Recovery-Node implementieren.

Was Sie benötigen

Sie müssen festgestellt haben, dass die virtuelle Maschine nicht wiederhergestellt werden kann und ersetzt werden muss.

Über diese Aufgabe

Sie verwenden den VMware vSphere Web Client, um zuerst die dem ausgefallenen Grid-Node zugeordnete virtuelle Maschine zu entfernen. Anschließend können Sie eine neue Virtual Machine implementieren.

Dieses Verfahren ist nur ein Schritt im Recovery-Prozess des Grid Node. Das Verfahren zum Entfernen und Implementieren eines Node ist für alle VMware Nodes identisch, einschließlich Admin-Nodes, Storage-Nodes, Gateway-Nodes und Archiv-Nodes.

Schritte

1. Melden Sie sich beim VMware vSphere Web Client an.
2. Navigieren Sie zu der ausgefallenen virtuellen Maschine des Grid-Node.
3. Notieren Sie sich alle Informationen, die zur Implementierung des Recovery-Nodes erforderlich sind.
 - a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie die Registerkarte **Einstellungen bearbeiten** aus, und notieren Sie die verwendeten Einstellungen.
 - b. Wählen Sie die Registerkarte **vApp Options** aus, um die Netzwerkeinstellungen des Grid Node

anzuzeigen und aufzuzeichnen.

4. Wenn der fehlgeschlagene Grid-Node ein Storage-Node ist, ermitteln Sie, ob eine der virtuellen Festplatten, die für die Datenspeicherung verwendet werden, unbeschädigt sind, und bewahren Sie sie für die erneute Verbindung mit dem wiederhergestellten Grid-Node auf.
5. Schalten Sie die virtuelle Maschine aus.
6. Wählen Sie **Aktionen Alle vCenter-Aktionen Löschen von Disk**, um die virtuelle Maschine zu löschen.
7. Implementieren Sie eine neue Virtual Machine als Ersatz-Node und verbinden Sie sie mit einem oder mehreren StorageGRID Netzwerken.

Bei der Implementierung des Node können Sie optional Node-Ports neu zuordnen oder CPU- oder Speichereinstellungen erhöhen.



Nach der Bereitstellung des neuen Knotens können Sie entsprechend Ihren Speicheranforderungen neue virtuelle Festplatten hinzufügen, alle virtuellen Festplatten, die vom zuvor entfernten ausgefallenen Grid-Knoten oder beiden beibehalten werden, neu anbinden.

Weitere Informationen:

[VMware installieren](#) StorageGRID-Knoten als virtuelle Maschine implementieren

8. Führen Sie das Recovery-Verfahren für den Node anhand des Node aus, den Sie wiederherstellen.

Node-Typ	Gehen Sie zu
Primärer Admin-Node	Primären Ersatzadministrator-Knoten konfigurieren
Nicht primärer Admin-Node	Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren
Gateway-Node	Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren
Storage-Node	Wählen Sie Wiederherstellung starten, um Speicherknoten zu konfigurieren
Archiv-Node	Wählen Sie Wiederherstellung starten, um den Knoten Archiv zu konfigurieren

Alle Grid-Node-Typen: Ersetzen Sie den Linux-Node

Wenn ein Ausfall erfordert, dass Sie einen oder mehrere neue physische oder virtuelle Hosts bereitstellen oder Linux auf einem vorhandenen Host neu installieren, müssen Sie den Ersatz-Host implementieren und konfigurieren, bevor Sie den Grid-Node wiederherstellen können. Dieses Verfahren ist ein Schritt der Wiederherstellung des Grid-Nodes für alle Arten von Grid-Nodes.

„Linux“ bezieht sich auf eine Red hat® Enterprise Linux®, Ubuntu®, CentOS- oder Debian®-Bereitstellung.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Dieses Verfahren wird nur als ein Schritt bei der Wiederherstellung von softwarebasierten Speicherknoten, primären oder nicht primären Admin-Nodes, Gateway-Nodes oder Archiv-Nodes durchgeführt. Die Schritte sind unabhängig vom Typ des wiederherenden Grid-Node identisch.

Wenn mehr als ein Grid-Node auf einem physischen oder virtuellen Linux-Host gehostet wird, können Sie die Grid-Nodes in beliebiger Reihenfolge wiederherstellen. Die Wiederherstellung eines primären Admin-Knotens zuerst verhindert jedoch, falls vorhanden, dass die Wiederherstellung anderer Grid-Knoten abstuckt, während sie versuchen, den primären Admin-Knoten zu kontaktieren, um sich für die Wiederherstellung zu registrieren.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Implementieren Sie neue Linux-Hosts

Bis auf ein paar Ausnahmen bereiten Sie die neuen Hosts wie während der Erstinstallation vor.

Um neue oder neu installierte physische oder virtuelle Linux-Hosts bereitzustellen, befolgen Sie das Verfahren zur Vorbereitung der Hosts in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

Dieses Verfahren umfasst Schritte zur Durchführung folgender Aufgaben:

1. Installieren Sie Linux.
2. Konfigurieren Sie das Hostnetzwerk.
3. Hostspeicher konfigurieren.
4. Die Container-Engine einbauen.
5. Installieren Sie den StorageGRID Host Service.



Beenden Sie den Vorgang „StorageGRID Host Service installieren“ in den Installationsanweisungen. Starten Sie nicht die Aufgabe „DBereitstellung von Grid-Nodes“.

Beachten Sie bei der Durchführung dieser Schritte die folgenden wichtigen Richtlinien:

- Verwenden Sie die gleichen Hostnamen, die Sie auf dem ursprünglichen Host verwendet haben.
- Wenn Sie Shared Storage zur Unterstützung Ihrer StorageGRID Nodes verwenden oder einige oder alle Festplatten oder SSDs von den ausgefallenen auf die Ersatz-Nodes verschoben haben, müssen Sie die gleichen Storage-Zuordnungen wiederherstellen, die auf dem ursprünglichen Host vorhanden waren. Wenn Sie beispielsweise WWIDs und Aliase in verwendet haben `/etc/multipath.conf` Wie in der Installationsanleitung empfohlen, verwenden Sie die gleichen Alias-/WWID-Paare in `/etc/multipath.conf` Auf dem Ersatzhost.
- Wenn der StorageGRID-Node Storage verwendet, der einem NetApp ONTAP System zugewiesen ist, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

Verwandte Informationen

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

Stellen Sie die Grid-Nodes für den Host wieder her

Um einen fehlgeschlagenen Grid-Node auf einem neuen Linux-Host wiederherzustellen, stellen Sie die Node-Konfigurationsdatei mit den entsprechenden Befehlen wieder her.

Bei einer Neuinstallation erstellen Sie für jeden Grid-Node, der auf einem Host installiert werden soll, eine Node-Konfigurationsdatei. Beim Wiederherstellen eines Grid-Node auf einem Ersatzhost stellen Sie die Node-Konfigurationsdatei für ausgefallene Grid-Nodes wieder her oder ersetzen sie.

Falls alle Block-Storage-Volumes vom vorherigen Host erhalten würden, müssen möglicherweise weitere Recovery-Verfahren durchgeführt werden. Mit den Befehlen in diesem Abschnitt können Sie ermitteln, welche zusätzlichen Verfahren erforderlich sind.

Schritte

- [Wiederherstellung und Validierung der Grid Nodes](#)
- [Starten Sie den StorageGRID Host Service](#)
- [Wiederherstellung von Nodes, die nicht ordnungsgemäß gestartet werden können](#)

Wiederherstellung und Validierung der Grid Nodes

Sie müssen die Grid-Konfigurationsdateien für alle ausgefallenen Grid-Nodes wiederherstellen, dann die Grid-Konfigurationsdateien validieren und Fehler beheben.

Über diese Aufgabe

Sie können jeden Grid-Node importieren, der auf dem Host vorhanden sein soll, solange er vorhanden ist `/var/local` Das Volume ging aufgrund des Ausfalls des vorherigen Hosts nicht verloren. Beispiel: Der `/var/local` Möglicherweise ist das Volume immer noch vorhanden, wenn Sie gemeinsam genutzten Storage für Daten-Volumes von StorageGRID Systemen verwendet haben, wie in der StorageGRID Installationsanleitung für Ihr Linux Betriebssystem beschrieben. Durch das Importieren des Knotens wird seine Knotenkonfigurationsdatei auf den Host wiederhergestellt.

Wenn fehlende Knoten nicht importiert werden können, müssen Sie ihre Grid-Konfigurationsdateien neu erstellen.

Sie müssen dann die Grid-Konfigurationsdatei validieren und alle Netzwerk- oder Storage-Probleme beheben, bevor Sie StorageGRID neu starten. Wenn Sie die Konfigurationsdatei für einen Node neu erstellen, müssen Sie denselben Namen für den Austausch-Node verwenden, der für den wiederherzuenden Node verwendet wurde.

Weitere Informationen zum Standort des finden Sie in den Installationsanweisungen `/var/local` Volume für einen Node:

Schritte

1. Führen Sie in der Befehlszeile des wiederhergestellten Hosts alle derzeit konfigurierten StorageGRID-Grid-Knoten auf:`sudo storagegrid node list`

Wenn keine Grid-Nodes konfiguriert sind, wird keine Ausgabe ausgegeben. Wenn einige Grid-Nodes konfiguriert sind, erwarten Sie die Ausgabe im folgenden Format:

Name	Metadata-Volume
dc1-adm1	/dev/mapper/sgws-adm1-var-local
dc1-gw1	/dev/mapper/sgws-gw1-var-local
dc1-sn1	/dev/mapper/sgws-sn1-var-local
dc1-arc1	/dev/mapper/sgws-arc1-var-local

Wenn einige oder alle Grid-Nodes, die auf dem Host konfiguriert werden sollen, nicht aufgeführt sind, müssen Sie die fehlenden Grid-Nodes wiederherstellen.

2. So importieren Sie Grid-Knoten mit einem `/var/local` Lautstärke:

- a. Führen Sie für jeden Knoten, den Sie importieren möchten, den folgenden Befehl aus:`sudo storagegrid node import node-var-local-volume-path`

Der `storagegrid node import` Befehl ist nur erfolgreich, wenn der Ziel-Node sauber heruntergefahren wurde auf dem Host, auf dem er zuletzt ausgeführt wurde. Wenn dies nicht der Fall ist, beobachten Sie einen Fehler, der dem folgenden ähnlich ist:

```
This node (node-name) appears to be owned by another host (UUID host-uuid).
```

Use the `--force` flag if you are sure import is safe.

- a. Wenn der Fehler angezeigt wird, dass der Node, der einem anderen Host gehört, ausgeführt wird, führen Sie den Befehl erneut mit dem aus `--force` Flag, um den Import abzuschließen:`sudo storagegrid --force node import node-var-local-volume-path`



Alle mit dem importierten Knoten `--force` Flag erfordert weitere Wiederherstellungsschritte, bevor sie das Raster erneut verbinden können, wie unter beschrieben [Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen](#).

3. Für Grid-Nodes, die keinen über einen verfügen `/var/local` Volume: Erstellen Sie die Konfigurationsdatei des Node neu, um sie auf dem Host wiederherzustellen.

Befolgen Sie die Richtlinien unter „Create Node Configuration files“ in den Installationsanweisungen.



Wenn Sie die Konfigurationsdatei für einen Node neu erstellen, müssen Sie denselben Namen für den Austausch-Node verwenden, der für den wiederherzuenden Node verwendet wurde. Stellen Sie bei Linux-Bereitstellungen sicher, dass der Name der Konfigurationsdatei den Node-Namen enthält. Sie sollten, wenn möglich, dieselben Netzwerkschnittstellen, Gerätezuordnungen blockieren und IP-Adressen verwenden. Dieses Verfahren minimiert die Datenmenge, die während des Recovery auf den Node kopiert werden muss. Dadurch kann die Recovery erheblich schneller (in manchen Fällen nur Minuten statt Wochen) erfolgen.



Wenn Sie neue Blockgeräte (Geräte, die zuvor vom StorageGRID-Knoten nicht genutzt wurden) als Werte für eine der mit zu startenden Konfigurationsvariablen verwenden `BLOCK_DEVICE_` Wenn Sie die Konfigurationsdatei für einen Knoten neu erstellen, befolgen Sie unbedingt alle Richtlinien in [Beheben Sie fehlende Blockgerätfehler](#).

4. Führen Sie den folgenden Befehl auf dem wiederhergestellten Host aus, um alle StorageGRID Knoten aufzulisten.

```
sudo storagegrid node list
```

5. Überprüfen Sie die Node-Konfigurationsdatei für jeden Grid-Node, dessen Name in der Ausgabe der StorageGRID-Node-Liste angezeigt wurde:

```
sudo storagegrid node validate node-name
```

Sie müssen alle Fehler oder Warnungen beheben, bevor Sie den StorageGRID-Hostdienst starten. In den folgenden Abschnitten werden Fehler näher erläutert, die bei der Wiederherstellung möglicherweise eine besondere Bedeutung haben.

Verwandte Informationen

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

[Beheben Sie fehlende Fehler an der Netzwerkschnittstelle](#)

Beheben Sie fehlende Fehler an der Netzwerkschnittstelle

Wenn das Hostnetzwerk nicht richtig konfiguriert ist oder ein Name falsch geschrieben wird, tritt ein Fehler auf, wenn StorageGRID die in angegebene Zuordnung überprüft `/etc/storagegrid/nodes/node-name.conf` Datei:

Möglicherweise wird ein Fehler oder eine Warnung angezeigt, die diesem Muster entspricht:

```
Checking configuration file `/etc/storagegrid/nodes/node-name.conf' Für Node_Node-Name_...`ERROR: node-name: GRID_NETWORK_TARGET = host-interface-name` Node-Name: Schnittstelle 'Host-Interface-Name' existiert nicht`
```

Der Fehler konnte für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk gemeldet werden. Dieser Fehler bedeutet, dass der `/etc/storagegrid/nodes/node-name.conf` Datei ordnet das angezeigte StorageGRID-Netzwerk der Host-Schnittstelle namens zu `host-interface-name`, Aber es gibt keine Schnittstelle mit diesem Namen auf dem aktuellen Host.

Wenn Sie diesen Fehler erhalten, überprüfen Sie, ob Sie die Schritte unter ausgeführt haben [Implementieren](#)

[Sie neue Linux-Hosts](#). Verwenden Sie dieselben Namen für alle Host-Schnittstellen, die auf dem ursprünglichen Host verwendet wurden.

Wenn Sie die Host-Schnittstellen nicht benennen können, die mit der Node-Konfigurationsdatei übereinstimmen, können Sie die Node-Konfigurationsdatei bearbeiten und den Wert des GRID_NETWORK_TARGET, DES ADMIN_NETWORK_TARGET oder DES CLIENT_NETWORK_TARGET ändern, um einer vorhandenen Hostschnittstelle zu entsprechen.

Stellen Sie sicher, dass die Host-Schnittstelle Zugriff auf den entsprechenden physischen Netzwerk-Port oder VLAN bietet und dass die Schnittstelle keinen direkten Bezug auf ein Bond- oder Bridge-Gerät hat. Sie müssen entweder ein VLAN (oder eine andere virtuelle Schnittstelle) auf dem Bond-Gerät auf dem Host konfigurieren oder ein Bridge- und virtuelles Ethernet-Paar (veth) verwenden.

Beheben Sie fehlende Blockgerätfehler

Das System überprüft, ob jeder wiederhergestellte Knoten einer gültigen Blockgerätespezialldatei oder einem gültigen Softlink zu einer speziellen Blockgerätedatei zugeordnet wird. Wenn StorageGRID eine ungültige Zuordnung im findet `/etc/storagegrid/nodes/node-name.conf` Datei: Es wird ein Fehler des Blockgerätes angezeigt.

Wenn Sie einen Fehler beobachten, der diesem Muster entspricht:

```
Checking configuration file /etc/storagegrid/nodes/node-name.conf for node node-  
name... ERROR: node-name: BLOCK_DEVICE_PURPOSE = path-name` Node-Name: Path-Name existiert  
nicht`
```

Es bedeutet das `/etc/storagegrid/nodes/node-name.conf` Ordnet das von *Node-Name* verwendete Blockgerät dem angegebenen Pfad-Namen im Linux-Dateisystem zu, aber an diesem Speicherort gibt es keine gültige Sonderdatei für Blockgeräte oder keinen Softlink zu einer Sonderdatei für Blockgeräte.

Stellen Sie sicher, dass Sie die Schritte in abgeschlossen haben [Implementieren Sie neue Linux-Hosts](#). Verwenden Sie für alle Blockgeräte dieselben persistenten Gerätenamen, die auf dem ursprünglichen Host verwendet wurden.

Wenn Sie die fehlende Sonderdatei für Blockgeräte nicht wiederherstellen oder neu erstellen können, können Sie ein neues Blockgerät mit der entsprechenden Größe und Speicherkategorie zuweisen und die Knotenkonfigurationsdatei bearbeiten, um den Wert VON BLOCK_DEVICE_PURPOSE zu ändern, um auf die neue Sonderdatei für Blockgeräte zu verweisen.

Bestimmen Sie die geeignete Größe und Speicherkategorie aus den Tabellen im Abschnitt „Storage Requirements“ der Installationsanleitung für Ihr Linux-Betriebssystem. Lesen Sie die Empfehlungen unter „Hostspeicher konfigurieren“, bevor Sie mit dem Austausch von Blockgeräten fortfahren.



Wenn Sie ein neues Blockspeichergerät für eine der Konfigurationsdateivariablen angeben müssen, die mit `BLOCK_DEVICE_` beginnen. Da das ursprüngliche Blockgerät mit dem ausgefallenen Host verloren gegangen ist, stellen Sie sicher, dass das neue Blockgerät nicht formatiert ist, bevor Sie weitere Wiederherstellungsverfahren durchführen. Das neue Blockgerät wird unformatiert, wenn Sie gemeinsam genutzten Speicher verwenden und ein neues Volume erstellt haben. Wenn Sie sich nicht sicher sind, führen Sie den folgenden Befehl gegen neue Spezialdateien für das Blockspeichergerät aus.

ACHTUNG:

Führen Sie den folgenden Befehl nur für neue Block Storage-Geräte aus. Führen Sie diesen Befehl nicht aus, wenn Sie glauben, dass der Block Storage noch gültige Daten für den wiederherzustellenden Node enthält, da alle Daten auf dem Gerät verloren gehen.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Verwandte Informationen

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

Starten Sie den StorageGRID Host Service

Um die StorageGRID Nodes zu starten und sicherzustellen, dass sie nach einem Neustart des Hosts neu gestartet werden, müssen Sie den StorageGRID Host Service aktivieren und starten.

1. Führen Sie auf jedem Host folgende Befehle aus:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Bereitstellung fortgesetzt wird:

```
sudo storagegrid node status node-name
```

Führen Sie für jeden Node, der den Status „nicht ausgeführt“ oder „angehalten“ zurückgibt, den folgenden Befehl aus:

```
sudo storagegrid node start node-name
```

3. Wenn Sie zuvor den StorageGRID-Hostdienst aktiviert und gestartet haben (oder wenn Sie sich nicht sicher sind, ob der Dienst aktiviert und gestartet wurde), führen Sie auch den folgenden Befehl aus:

```
sudo systemctl reload-or-restart storagegrid
```

Wiederherstellung von Nodes, die nicht ordnungsgemäß gestartet werden können

Wenn ein StorageGRID Node nicht ordnungsgemäß wieder in das Grid kommt und nicht als wiederherstellbar angezeigt wird, kann er beschädigt werden. Sie können den Node in den Recovery-Modus erzwingen.

So erzwingen Sie den Knoten in den Wiederherstellungsmodus:

```
sudo storagegrid node force-recovery node-name
```



Bestätigen Sie vor Ausgabe dieses Befehls, dass die Netzwerkkonfiguration des Node korrekt ist. Möglicherweise ist es aufgrund falscher Netzwerkschnittstellenzuordnungen oder einer falschen Grid-Netzwerk-IP-Adresse oder eines falschen Gateways fehlgeschlagen, das Grid-Netzwerk erneut anzuschließen.



Nach Ausstellung des `storagegrid node force-recovery node-name` Befehl, Sie müssen zusätzliche Recovery-Schritte für *Node-Name* durchführen.

Verwandte Informationen

[Nächste Schritte: Falls erforderlich, zusätzliche Recovery-Schritte durchführen](#)

Was ist weiter: Führen Sie zusätzliche Recovery-Schritte, wenn erforderlich

Abhängig von den spezifischen Aktionen, die Sie unternommen haben, um die StorageGRID Nodes auf dem Ersatzhost auszuführen, müssen Sie möglicherweise zusätzliche Recovery-Schritte für jeden Node durchführen.

Die Node-Recovery ist abgeschlossen, wenn Sie keine Korrekturmaßnahmen vornehmen müssen, während Sie den Linux Host ersetzt oder den ausgefallenen Grid Node auf dem neuen Host wiederhergestellt haben.

Korrekturmaßnahmen und nächste Schritte

Beim Austausch eines Node sind möglicherweise folgende Korrekturmaßnahmen erforderlich:

- Man musste das benutzen `--force` Flag zum Importieren des Knotens.
- Für alle `<PURPOSE>`, Der Wert des `BLOCK_DEVICE_<PURPOSE>` Die Variable der Konfigurationsdatei bezieht sich auf ein Blockgerät, das nicht die gleichen Daten enthält, die es vor dem Ausfall des Hosts gemacht hat.
- Sie sind ausgestellt `storagegrid node force-recovery node-name` Für den Node.
- Sie haben ein neues Blockgerät hinzugefügt.

Wenn Sie **eine** dieser Korrekturmaßnahmen ergriffen haben, müssen Sie zusätzliche Wiederherstellungsschritte durchführen.

Art der Wiederherstellung	Nächster Schritt
Primärer Admin-Node	Primären Ersatzadministrator-Knoten konfigurieren
Nicht primärer Admin-Node	Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren
Gateway-Node	Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren
Archiv-Node	Wählen Sie Wiederherstellung starten, um den Knoten Archiv zu konfigurieren

Art der Wiederherstellung	Nächster Schritt
Storage-Node (softwarebasiert): • Wenn man das benutzen musste <code>--force</code> Flag, um den Knoten zu importieren, oder Sie haben ausgegeben <code>storagegrid node force-recovery node-name</code> • Wenn Sie eine vollständige Neuinstallation des Knotens durchführen mussten, oder Sie müssen <code>/var/local</code> wiederherstellen	Wählen Sie Wiederherstellung starten, um Speicherknoten zu konfigurieren
Storage-Node (softwarebasiert): • Wenn Sie ein neues Blockgerät hinzugefügt haben. • Wenn, für alle <code><PURPOSE></code>, Der Wert des <code>BLOCK_DEVICE_<PURPOSE></code> Die Variable der Konfigurationsdatei bezieht sich auf ein Blockgerät, das nicht die gleichen Daten enthält, die es vor dem Ausfall des Hosts gemacht hat.	Wiederherstellung nach einem Storage-Volume-Ausfall bei intaktem Systemlaufwerk

Austausch eines fehlerhaften Node durch Services Appliance

Sie können eine SG100- oder SG1000-Services-Appliance verwenden, um einen fehlgeschlagenen Gateway-Node, einen ausgefallenen nicht-primären Admin-Node oder einen ausgefallenen primären Admin-Node wiederherzustellen, der auf VMware, einem Linux-Host oder einer Services Appliance gehostet wurde. Dieses Verfahren ist ein Schritt der Wiederherstellung des Grid-Nodes.

Was Sie benötigen

- Sie müssen festgestellt haben, dass eine der folgenden Situationen zutrifft:
 - Die virtuelle Maschine, die den Node hostet, kann nicht wiederhergestellt werden.
 - Der physische oder virtuelle Linux-Host für den Grid-Node ist ausgefallen und muss ersetzt werden.
 - Die Services-Appliance, die den Grid-Node hostet, muss ersetzt werden.
- Sie müssen sicherstellen, dass die Installationsversion von StorageGRID Appliance auf der Services Appliance mit der Softwareversion des StorageGRID Systems übereinstimmt. Diese wird in der Hardwareinstallation und -Wartung für die Überprüfung und das Upgrade der Installationsversion von StorageGRID Appliance beschrieben.

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



Stellen Sie keine SG100- und SG1000-Service-Appliance am selben Standort bereit. Das kann zu einer unvorhersehbaren Performance führen.

Über diese Aufgabe

In den folgenden Fällen können Sie eine SG100- oder SG1000-Services-Appliance verwenden, um einen

fehlgeschlagenen Grid-Node wiederherzustellen:

- Der ausgefallene Node wurde auf VMware oder Linux gehostet (Plattformänderung)
- Der ausgefallene Node wurde auf einer Service Appliance gehostet (Plattformaustausch).

Installation der Services Appliance (nur Plattformänderung)

Wenn Sie einen fehlgeschlagenen Grid-Node wiederherstellen, der auf VMware oder einem Linux-Host gehostet wurde und eine SG100- oder SG1000-Services-Appliance für den Ersatzknoten verwenden, müssen Sie zuerst die neue Appliance-Hardware mit dem gleichen Node-Namen wie der ausgefallene Node installieren.

Sie müssen über die folgenden Informationen zum ausgefallenen Node verfügen:

- **Knotenname:** Sie müssen die Services-Appliance mit dem gleichen Knotennamen wie der ausgefallene Knoten installieren.
- **IP-Adressen:** Sie können dem Services-Gerät dieselben IP-Adressen zuweisen wie dem ausgefallenen Knoten, was die bevorzugte Option ist, oder Sie können eine neue ungenutzte IP-Adresse in jedem Netzwerk auswählen.

Führen Sie diese Vorgehensweise nur aus, wenn Sie einen ausgefallenen Node, der auf VMware oder Linux gehostet wurde, wiederherstellen und diesen durch einen Node ersetzen, der auf einer Services Appliance gehostet wird.

1. Befolgen Sie die Anweisungen zum Installieren einer neuen SG100- oder SG1000-Services-Appliance.
2. Verwenden Sie bei der Aufforderung zu einem Node-Namen den Node-Namen des ausgefallenen Node.

Verwandte Informationen

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

Appliance für die erneute Installation vorbereiten (nur Plattformaustausch)

Bei der Wiederherstellung eines Grid-Node, der auf einer Services Appliance gehostet wurde, müssen Sie zuerst die Appliance für die Neuinstallation der StorageGRID Software vorbereiten.

Führen Sie diese Schritte nur aus, wenn Sie einen ausgefallenen Node ersetzen, der auf einer Services Appliance gehostet wurde. Führen Sie diese Schritte nicht aus, wenn der ausgefallene Node ursprünglich auf VMware oder einem Linux-Host gehostet wurde.

1. Loggen Sie sich beim fehlgeschlagenen Grid-Node ein:
 - 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 `#`.

2. Bereiten Sie die Appliance auf die Installation der StorageGRID Software vor. Geben Sie Ein:

sgareinstall

3. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie Folgendes ein: *y*

Die Appliance wird neu gestartet, und Ihre SSH-Sitzung wird beendet. In der Regel dauert es etwa 5 Minuten, bis das Installationsprogramm für StorageGRID-Appliances verfügbar ist, obwohl in einigen Fällen Sie möglicherweise bis zu 30 Minuten warten müssen.

Die Services-Appliance wird zurückgesetzt und die Daten auf dem Grid-Node sind nicht mehr verfügbar. Die während der ursprünglichen Installation konfigurierten IP-Adressen sollten intakt bleiben. Nach Abschluss des Vorgangs wird jedoch empfohlen, dies zu bestätigen.

Nach Ausführung des `sgareinstall` Der Befehl entfernt alle über StorageGRID bereitgestellten Konten, Passwörter und SSH-Schlüssel und generiert neue Host-Schlüssel.

Starten der Softwareinstallation auf der Services-Appliance

Um einen Gateway-Node oder Admin-Node auf einer SG100- oder SG1000-Service-Appliance zu installieren, verwenden Sie das Installationsprogramm der StorageGRID-Appliance, das auf der Appliance enthalten ist.

Was Sie benötigen

- Die Appliance muss in einem Rack installiert, mit dem Netzwerk verbunden und eingeschaltet sein.
- Netzwerkverbindungen und IP-Adressen müssen für die Appliance mithilfe des StorageGRID Appliance Installer konfiguriert werden.
- Wenn Sie einen Gateway-Node oder einen nicht-primären Admin-Node installieren, kennen Sie die IP-Adresse des primären Admin-Nodes für das StorageGRID-Grid.
- Alle Grid-Subnetze, die auf der Seite IP-Konfiguration des Installationsprogramms für StorageGRID-Geräte aufgeführt sind, müssen in der Netznetzwerksubnetz-Liste auf dem primären Admin-Node definiert sein.

Anweisungen zum Abschließen dieser Vorraussaufgaben finden Sie in der Installations- und Wartungsanleitung für eine SG100- oder SG1000-Service-Appliance.

- Sie müssen ein verwenden [Unterstützter Webbrowser](#).
- Sie müssen eine der IP-Adressen kennen, die der Appliance zugewiesen sind. Sie können die IP-Adresse für das Admin-Netzwerk, das Grid-Netzwerk oder das Client-Netzwerk verwenden.
- Wenn Sie einen primären Admin-Knoten installieren, haben Sie die Ubuntu- oder Debian-Installationsdateien für diese Version von StorageGRID zur Verfügung.



Eine aktuelle Version der StorageGRID-Software wird während der Fertigung vorinstalliert auf die Services-Appliance geladen. Wenn die vorinstallierte Version der Software mit der in der StorageGRID-Bereitstellung verwendeten Version übereinstimmt, benötigen Sie die Installationsdateien nicht.

Über diese Aufgabe

So installieren Sie die StorageGRID-Software auf einer SG100- oder SG1000-Services-Appliance:

- Für einen primären Admin-Node geben Sie den Namen des Knotens an und laden dann die entsprechenden Softwarepakete hoch (falls erforderlich).
- Für einen nicht-primären Admin-Node oder einen Gateway-Node geben Sie die IP-Adresse des primären

Admin-Node und den Namen des Node an oder bestätigen Sie diese.

- Sie starten die Installation und warten, bis Volumes konfiguriert und die Software installiert ist.
- Durch den Prozess partway, die Installation pausiert. Um die Installation fortzusetzen, müssen Sie sich beim Grid Manager anmelden und den ausstehenden Node als Ersatz für den ausgefallenen Node konfigurieren.
- Nachdem Sie den Node konfiguriert haben, wird die Installation der Appliance abgeschlossen und die Appliance wird neu gestartet.

Schritte

1. Öffnen Sie einen Browser, und geben Sie eine der IP-Adressen für die SG100- oder SG1000-Services-Appliance ein.

`https://Controller_IP:8443`

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

The screenshot shows the 'NetApp® StorageGRID® Appliance Installer' web interface. At the top is a blue header with the title and a 'Help' link. Below the header is a navigation bar with tabs: 'Home', 'Configure Networking', 'Configure Hardware', 'Monitor Installation', and 'Advanced'. The 'Home' tab is selected. The main content area is titled 'Home' and contains three sections: 'This Node', 'Primary Admin Node connection', and 'Installation'. In the 'This Node' section, 'Node type' is set to 'Gateway' and 'Node name' is 'NetApp-SGA'. There are 'Cancel' and 'Save' buttons. The 'Primary Admin Node connection' section shows 'Enable Admin Node discovery' checked, with a message 'Admin Node discovery is in progress'. It also has 'Cancel' and 'Save' buttons. The 'Installation' section shows the 'Current state' as 'Unable to start installation. The Admin Node connection is not ready.' with a 'Start installation' button.

NetApp® StorageGRID® Appliance Installer		Help ▾			
Home	Configure Networking ▾	Configure Hardware ▾	Monitor Installation	Advanced ▾	
Home					
This Node					
Node type	Gateway ▾				
Node name	NetApp-SGA				
	Cancel				
	Save				
Primary Admin Node connection					
Enable Admin Node discovery	☒ Uncheck to manually enter the Primary Admin Node IP				
Connection state	Admin Node discovery is in progress				
	Cancel				
	Save				
Installation					
Current state	Unable to start installation. The Admin Node connection is not ready.				
	Start installation				

2. So installieren Sie einen primären Admin-Knoten:

- a. Wählen Sie im Abschnitt This Node für **Node Type** die Option **Primary Admin** aus.
- b. Geben Sie im Feld **Knotenname** den gleichen Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.
- c. Überprüfen Sie im Abschnitt Installation die unter Aktueller Status aufgeführte Softwareversion

Wenn die Version der zu installierenden Software richtig ist, fahren sie mit fort [Installationsschritt](#).

- d. Wenn Sie eine andere Version der Software hochladen möchten, wählen Sie im Menü * Erweitert* die Option **StorageGRID-Software hochladen**.

Die Seite StorageGRID-Software hochladen wird angezeigt.

- a. Klicken Sie auf **Durchsuchen**, um das **Softwarepaket** und die Checksum-Datei* für die StorageGRID-Software hochzuladen.

Die Dateien werden nach der Auswahl automatisch hochgeladen.

- b. Klicken Sie auf **Startseite**, um zur Startseite des StorageGRID-Appliance-Installationsprogramms zurückzukehren.

3. So installieren Sie einen Gateway-Node oder einen nicht-primären Admin-Node:

- a. Wählen Sie im Abschnitt This Node für **Node Type** die Option **Gateway** oder **Non-Primary Admin** aus, je nach Typ des wiederherzustellenden Knotens.
- b. Geben Sie im Feld **Knotenname** den gleichen Namen ein, der für den Knoten verwendet wurde, den Sie wiederherstellen, und klicken Sie auf **Speichern**.
- c. Legen Sie im Abschnitt primäre Administratorknoten-Verbindung fest, ob Sie die IP-Adresse für den primären Admin-Node angeben müssen.

Das Installationsprogramm der StorageGRID-Appliance kann diese IP-Adresse automatisch erkennen, wenn der primäre Admin-Node oder mindestens ein anderer Grid-Node mit Admin_IP konfiguriert ist, sich im selben Subnetz befindet.

- d. Wenn diese IP-Adresse nicht angezeigt wird oder Sie sie ändern müssen, geben Sie die Adresse an:

Option	Beschreibung
Manuelle IP-Eingabe	a. Deaktivieren Sie das Kontrollkästchen Admin Node Discovery aktivieren. b. Geben Sie die IP-Adresse manuell ein. c. Klicken Sie Auf Speichern. d. Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.

Option	Beschreibung
Automatische Erkennung aller verbundenen primären Admin-Nodes	- Aktivieren Sie das Kontrollkästchen Admin Node Discovery aktivieren. - Wählen Sie aus der Liste der ermittelten IP-Adressen den primären Admin-Node für das Grid aus, in dem diese Service-Appliance bereitgestellt wird. - Klicken Sie Auf Speichern. - Warten Sie, während der Verbindungsstatus für die neue IP-Adresse in „ready.“ lautet.

- im Abschnitt Installation müssen Sie bestätigen, dass der aktuelle Status bereit ist, die Installation des Knotennamens zu starten, und dass die Schaltfläche **Installation starten** aktiviert ist.

Wenn die Schaltfläche **Installation starten** nicht aktiviert ist, müssen Sie möglicherweise die Netzwerkkonfiguration oder die Porteinstellungen ändern. Anweisungen hierzu finden Sie in der Installations- und Wartungsanleitung für Ihr Gerät.

- Klicken Sie auf der Startseite des StorageGRID-Appliance-Installationsprogramms auf **Installation starten**.

Der aktuelle Status ändert sich in „Installation is in progress,“ und die Seite Monitor Installation wird angezeigt.



Wenn Sie manuell auf die Seite Monitor-Installation zugreifen müssen, klicken Sie in der Menüleiste auf **Monitor-Installation**.

Verwandte Informationen

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

Überwachen Sie die Installation der Services Appliance

Das Installationsprogramm der StorageGRID Appliance stellt den Status bereit, bis die Installation abgeschlossen ist. Nach Abschluss der Softwareinstallation wird die Appliance neu gestartet.

- Um den Installationsfortschritt zu überwachen, klicken Sie in der Menüleiste auf **Installation überwachen**.

Auf der Seite Monitor-Installation wird der Installationsfortschritt angezeigt.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

Die blaue Statusleiste zeigt an, welche Aufgabe zurzeit ausgeführt wird. Grüne Statusleisten zeigen Aufgaben an, die erfolgreich abgeschlossen wurden.



Das Installationsprogramm stellt sicher, dass Aufgaben, die in einer früheren Installation ausgeführt wurden, nicht erneut ausgeführt werden. Wenn Sie eine Installation erneut ausführen, werden alle Aufgaben, die nicht erneut ausgeführt werden müssen, mit einer grünen Statusleiste und dem Status „Skipped.“ angezeigt.

2. Überprüfen Sie den Fortschritt der ersten beiden Installationsphasen.

◦ 1. Speicher konfigurieren

In dieser Phase löscht das Installationsprogramm alle vorhandenen Konfigurationen von den Laufwerken und konfiguriert die Hosteinstellungen.

◦ 2. Installieren Sie das Betriebssystem

Während dieser Phase kopiert das Installationsprogramm das Betriebssystem-Image für StorageGRID vom primären Admin-Node auf die Appliance oder installiert das Betriebssystem aus dem Installationspaket für den primären Admin-Node.

3. Überwachen Sie den Installationsfortschritt, bis einer der folgenden Schritte eintritt:

- Bei Appliance-Gateway-Knoten oder nicht-primären Appliance-Admin-Knoten wird die Phase **Install StorageGRID** angehalten. Auf der eingebetteten Konsole wird eine Meldung angezeigt, die Sie dazu auffordert, diesen Knoten auf dem Admin-Knoten mithilfe des Grid-Managers zu genehmigen.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type=: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Für primäre Administrator-Knoten der Appliance wird eine fünfte Phase (Installationsprogramm für StorageGRID laden) angezeigt. Wenn die fünfte Phase länger als 10 Minuten in Bearbeitung ist, aktualisieren Sie die Seite manuell.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Fahren Sie mit dem nächsten Schritt des Recovery-Prozesses für den Typ des Appliance-Grid-Node fort, den Sie wiederherstellen.

Art der Wiederherstellung	Referenz
Gateway-Node	Wählen Sie Wiederherstellung starten, um Gateway-Node zu konfigurieren
Nicht primärer Admin-Node	Wählen Sie Wiederherstellung starten, um einen nicht-primären Admin-Node zu konfigurieren
Primärer Admin-Node	Primären Ersatzadministrator-Knoten konfigurieren

Durchführen der Standortwiederherstellung durch den technischen Support

Falls eine gesamte StorageGRID Site ausfällt oder mehrere Storage Nodes ausfallen, müssen Sie sich an den technischen Support wenden. Der technische Support analysiert das Unternehmen, entwickelt einen Recovery-Plan und stellt die ausgefallenen Nodes oder Standorte dann auf eine Art und Weise wieder her, die Ihre Geschäftsziele erfüllt. Die Recovery-Zeit wird optimiert und unnötige Datenverluste werden vermieden.



Das Standort-Recovery kann nur durch den technischen Support durchgeführt werden.

StorageGRID Systeme sind für die unterschiedlichsten Fehler anfällig und viele Recovery- und Wartungsvorgänge können problemlos selbst durchgeführt werden. Es ist jedoch schwierig, ein einfaches, generalisiertes Standortwiederherstellungsverfahren zu erstellen, da die detaillierten Schritte von Faktoren abhängen, die spezifisch für Ihre Situation sind. Beispiel:

- **Ihre Geschäftsziele:** Nach dem vollständigen Verlust einer StorageGRID-Website sollten Sie bewerten, wie Sie Ihre Geschäftsziele am besten erreichen können. Möchten Sie beispielsweise den verlorenen Standort neu aufbauen? Möchten Sie die verlorene StorageGRID Site an einem neuen Standort ersetzen? Jede Kundensituation ist anders, und Ihr Recovery-Plan muss Ihre Prioritäten berücksichtigen.
- **Exakte Art des Ausfalls:** Vor Beginn der Standortwiederherstellung ist es wichtig festzustellen, ob alle Knoten am ausgefallenen Standort intakt sind oder ob Speicherknoten wiederherstellbare Objekte

enthalten. Wenn Sie Nodes oder Storage Volumes neu erstellen, die gültige Daten enthalten, kann es zu unnötigen Datenverlusten kommen.

- **Aktive ILM-Richtlinie:** Die Anzahl, Art und der Speicherort von Objektkopien in Ihrem Grid wird durch Ihre aktive ILM-Richtlinie gesteuert. Die Besonderheiten Ihrer ILM-Richtlinie können sich auf die Menge der wiederherstellbaren Daten sowie auf die spezifischen für die Recovery erforderlichen Techniken auswirken.



Wenn ein Standort die einzige Kopie eines Objekts enthält und der Standort verloren geht, geht das Objekt verloren.

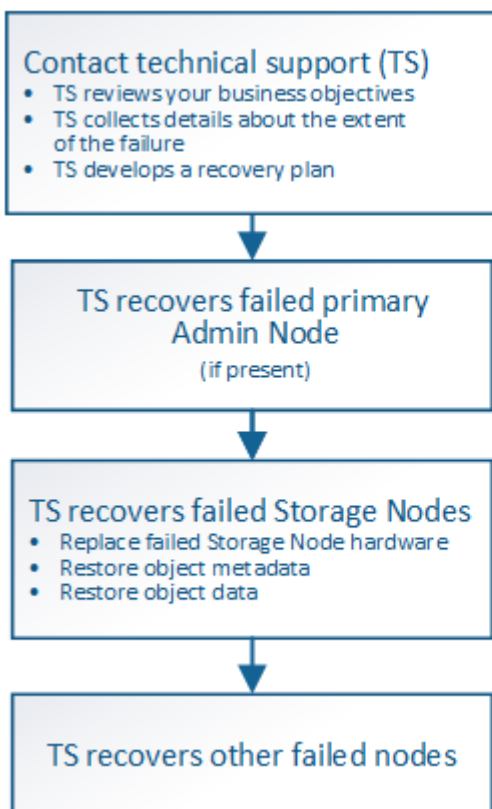
- **Bucket (oder Container) Konsistenz:** Die auf einen Bucket (oder Container) angewendete Konsistenzstufe wirkt sich darauf aus, ob StorageGRID die Objektmetadaten vollständig auf alle Nodes und Standorte repliziert, bevor einem Client mitgeteilt wird, dass die Objektaufnahme erfolgreich war. Wenn die Konsistenzstufe für eventuelle Konsistenz sorgt, sind einige Objektmetadaten bei einem Standortausfall verloren gegangen. Dies kann sich auf die Menge der wiederherstellbaren Daten und möglicherweise auf die Details des Recovery-Verfahrens auswirken.
- **Historie der neuesten Änderungen:** Die Details Ihres Wiederherstellungsverfahrens können davon beeinflusst werden, ob zum Zeitpunkt des Ausfalls Wartungsarbeiten durchgeführt wurden oder ob kürzlich Änderungen an Ihrer ILM-Richtlinie vorgenommen wurden. Der technische Support muss den aktuellen Verlauf des Grid sowie dessen aktuelle Situation vor Beginn einer Wiederherstellung des Standorts beurteilen.

Überblick über die Standortwiederherstellung

Dies ist eine allgemeine Übersicht über das Verfahren, das der technische Support zur Wiederherstellung eines ausgefallenen Standorts verwendet.



Das Standort-Recovery kann nur durch den technischen Support durchgeführt werden.



Caution: Do not use the recovery procedures designed for a single failed Storage Node. Data loss will occur.

1. Wenden Sie sich an den technischen Support.

Der technische Support führt eine detaillierte Bewertung der Fehler durch und prüft gemeinsam mit Ihnen Ihre Geschäftsziele. Auf der Grundlage dieser Informationen entwickelt der technische Support einen Recovery-Plan, der auf Ihre Situation zugeschnitten ist.

2. Der technische Support stellt den primären Admin-Knoten wieder her, wenn er ausgefallen ist.

3. Der technische Support stellt alle Storage-Knoten wieder her, folgt dieser Beschreibung:

- a. Ersetzen Sie bei Bedarf Storage Node Hardware oder Virtual Machines.
- b. Wiederherstellung von Objektmetadaten am ausgefallenen Standort
- c. Wiederherstellung von Objektdaten auf den wiederhergestellten Storage-Nodes



Wenn die Wiederherstellungsverfahren für einen einzelnen ausgefallenen Speicherknoten verwendet werden, kann es zu Datenverlusten kommen.



Wenn ein kompletter Standort ausfällt, sind spezielle Befehle erforderlich, um Objekte und Objektmetadaten erfolgreich wiederherzustellen.

4. Der technische Support stellt andere ausgefallene Nodes wieder her.

Nach der Wiederherstellung von Objektmetadaten und -Daten können fehlerhafte Gateway-Nodes, nicht primäre Admin-Nodes oder Archiv-Nodes anhand von Standardverfahren wiederhergestellt werden.

Verwandte Informationen

[Deaktivierung der Website](#)

Verfahren zur Deaktivierung

Sie können einen Außerbetriebnahme durchführen, um Grid-Nodes oder eine ganze Website dauerhaft vom StorageGRID System zu entfernen.

Um einen Grid-Node oder einen Standort zu entfernen, führen Sie einen der folgenden Verfahren zur Deaktivierung durch:

- Führen Sie einen **Knoten außer Betrieb** aus, um einen oder mehrere Knoten zu entfernen, die sich an einem oder mehreren Standorten befinden können. Die entfernenden Nodes können online und mit dem StorageGRID System verbunden sein oder offline bzw. getrennt sein.
- Führen Sie eine Deaktivierung einer Site mit * Connected Site durch, um eine Site zu entfernen, auf der alle Nodes mit StorageGRID verbunden sind.
- Führen Sie eine Deaktivierung der Site durch **getrennt**, um eine Site zu entfernen, in der alle Nodes von StorageGRID getrennt sind.



Bevor Sie eine Website außer Betrieb nehmen, müssen Sie sich an Ihren NetApp Ansprechpartner wenden. NetApp überprüft Ihre Anforderungen, bevor Sie alle Schritte im Decommission Site Wizard aktivieren. Sie sollten keinen Versuch Unternehmen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie der Meinung sind, dass eine Wiederherstellung der Site oder die Wiederherstellung von Objektdaten von der Site möglich wäre.

Wenn ein Standort eine Mischung aus verbundenen (✔) Und nicht verbundene Knoten (☾ Oder ⚙), Sie müssen alle Offline-Knoten wieder online bringen.



Wenn Sie eine zweite Wartung durchführen müssen, können Sie [Unterbrechen Sie die Deaktivierung, während die Speicherknoten entfernt werden](#). Die Schaltfläche **Pause** ist nur aktiviert, wenn die ILM-Bewertung oder die mit Erasure Coding versehenen Phasen der Datenauswertung erreicht sind. Die ILM-Evaluierung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt. Nach Abschluss des zweiten Wartungsverfahrens können Sie die Außerbetriebnahme fortsetzen.

Verwandte Informationen

[Der Grid-Node wird deaktiviert](#)

[Deaktivierung der Website](#)

Der Grid-Node wird deaktiviert

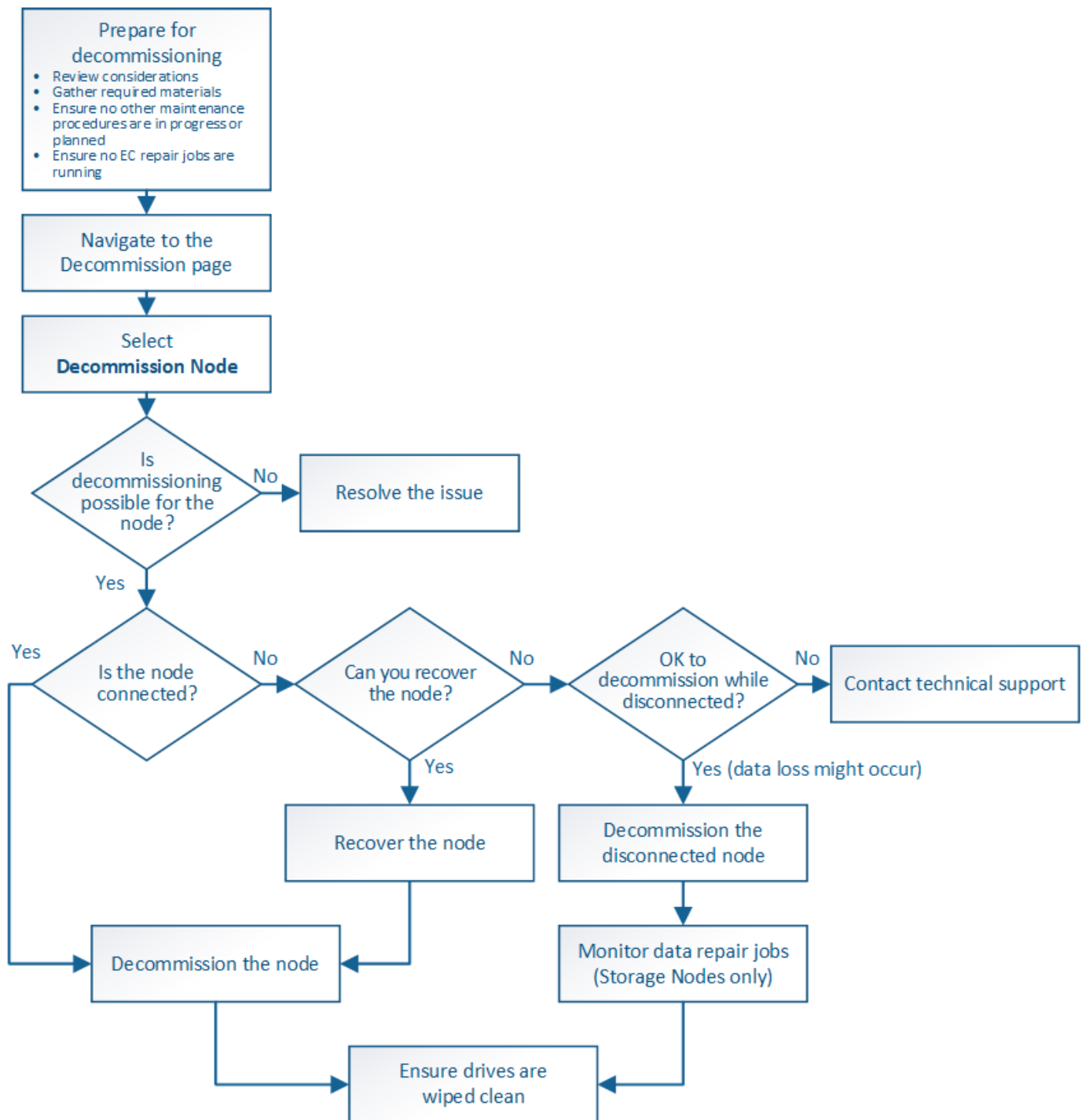
Sie können den Node Decounter-Vorgang verwenden, um einen oder mehrere Storage-Nodes, Gateway-Nodes oder nicht-primäre Admin-Nodes an einem oder mehreren Standorten zu entfernen. Sie können den primären Admin-Node oder einen Archiv-Node nicht stilllegen.

Im Allgemeinen sollten die Grid-Knoten nur dann außer Betrieb gesetzt werden, wenn sie mit dem StorageGRID-System verbunden sind und alle Knoten im normalen Zustand sind (mit grünen Symbolen auf den **NODES**-Seiten und auf der Seite **Decommission-Knoten**). Bei Bedarf können Sie jedoch einen nicht verbundenen Grid-Node außer Betrieb nehmen. Bevor Sie einen getrennten Knoten entfernen, stellen Sie sicher, dass Sie die Auswirkungen und Einschränkungen dieses Prozesses verstehen.

Wenn einer der folgenden Optionen zutrifft, wird das Verfahren zur Deaktivierung des Nodes ausgeführt:

- Sie haben dem System einen größeren Speicherknoten hinzugefügt, und Sie möchten einen oder mehrere kleinere Speicherknoten entfernen, während gleichzeitig Objekte erhalten bleiben.
- Sie benötigen weniger Storage insgesamt.
- Sie benötigen keinen Gateway-Node mehr.
- Sie benötigen keinen nicht mehr primären Admin-Node.
- Das Grid enthält einen getrennten Node, den Sie nicht wiederherstellen können oder wieder online schalten können.

Das Flussdiagramm zeigt die grundlegenden Schritte zur Deaktivierung von Grid-Nodes.



Grid-Nodes vorbereiten, um sie stillzulegen

Sie müssen die Überlegungen zum Entfernen von Grid-Nodes prüfen und bestätigen, dass keine Reparaturaufträge für Daten mit Erasure-Coding-Verfahren aktiv sind.

Überlegungen zur Deaktivierung des Grid Node

Bevor Sie dieses Verfahren zur Deaktivierung von einem oder mehreren Nodes starten, müssen Sie die Auswirkungen des Entferns der einzelnen Node verstehen. Bei der erfolgreichen Ausmusterung eines Node werden seine Services deaktiviert und der Node wird automatisch heruntergefahren.

Wenn Sie einen Node jedoch nicht stilllegen, wird StorageGRID dadurch in einem ungültigen Status belassen. Folgende Regeln werden durchgesetzt:

- Sie können den primären Admin-Node nicht stilllegen.
- Sie können Archiv-Knoten nicht stilllegen.
- Sie können einen Admin-Node oder einen Gateway-Node nicht stilllegen, wenn eine seiner Netzwerkschnittstellen Teil einer HA-Gruppe (High Availability, Hochverfügbarkeit) ist.
- Sie können einen Speicherknoten nicht stilllegen, wenn sich dessen Entfernung auf das ADC-Quorum auswirkt.
- Sie können einen Storage-Node nicht stilllegen, wenn er für die aktive ILM-Richtlinie erforderlich ist.
- Sie sollten nicht mehr als 10 Storage-Nodes in einem einzigen Decommission-Node-Verfahren außer Betrieb nehmen.
- Sie können einen verbundenen Knoten nicht stilllegen, wenn in Ihrem Grid keine getrennten Knoten enthalten sind (Knoten, deren Zustand unbekannt oder administrativ ausgefallen ist). Sie müssen zunächst die getrennten Nodes außer Betrieb nehmen oder wiederherstellen.
- Wenn Ihr Grid mehrere getrennte Knoten enthält, muss die Software gleichzeitig ausmustern, wodurch das Potenzial für unerwartete Ergebnisse erhöht wird.
- Wenn ein nicht getrennter Knoten nicht entfernt werden kann (z. B. ein Speicherknoten, der für das ADC-Quorum benötigt wird), kann kein anderer nicht getrennter Knoten entfernt werden.
- Wenn Sie ein älteres Gerät durch ein neueres Gerät ersetzen möchten, sollten Sie dies in Betracht ziehen [Klonen des Appliance-Node](#) Statt den alten Node außer Betrieb zu setzen und den neuen Node in einer Erweiterung hinzuzufügen.



Entfernen Sie die virtuelle Maschine oder andere Ressourcen eines Grid-Node erst, wenn Sie dazu aufgefordert werden, dies in Stilllegen-Verfahren zu tun.

Überlegungen zur Deaktivierung von Admin Node oder Gateway Node

Prüfen Sie die folgenden Überlegungen, bevor Sie einen Admin-Node oder einen Gateway-Node außer Betrieb setzen.

- Für das Verfahren zur Deaktivierung ist ein exklusiver Zugriff auf einige Systemressourcen erforderlich. Sie müssen also bestätigen, dass keine weiteren Wartungsverfahren ausgeführt werden.
- Sie können den primären Admin-Node nicht stilllegen.
- Sie können einen Admin-Node oder einen Gateway-Node nicht stilllegen, wenn eine seiner Netzwerkschnittstellen Teil einer HA-Gruppe (High Availability, Hochverfügbarkeit) ist. Sie müssen zuerst die Netzwerkschnittstellen aus der HA-Gruppe entfernen. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.
- Bei Bedarf können Sie die ILM-Richtlinie sicher ändern und gleichzeitig einen Gateway-Node oder einen Admin-Node außer Betrieb nehmen.
- Wenn Sie einen Admin-Node deaktivieren und Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, müssen Sie daran denken, das Vertrauen des Knotens zu entfernen, das auf die Grundlage von Active Directory Federation Services (AD FS) basiert.

Verwandte Informationen

[StorageGRID verwalten](#)

Überlegungen zur Deaktivierung von Storage Node

Wenn Sie einen Storage Node außer Betrieb nehmen möchten, müssen Sie wissen, wie StorageGRID die Objektdaten und Metadaten dieses Node managt.

Bei der Ausmusterung von Storage-Nodes gelten die folgenden Überlegungen und Einschränkungen:

- Das System muss zu jeder Zeit genügend Storage Nodes enthalten, um den betrieblichen Anforderungen gerecht zu werden, einschließlich des ADC-Quorums und der aktiven ILM-Richtlinie. Um diese Einschränkung zu erfüllen, müssen Sie möglicherweise einen neuen Storage-Node zu einem Erweiterungsvorgang hinzufügen, bevor Sie einen vorhandenen Storage-Node stilllegen können.
- Wenn der Storage-Node getrennt wird, wenn Sie ihn ausmustern, muss das System die Daten mithilfe der Daten der verbundenen Storage-Nodes rekonstruieren. Dies kann zu Datenverlusten führen.
- Wenn Sie einen Storage-Node entfernen, müssen große Mengen von Objektdaten über das Netzwerk übertragen werden. Obwohl diese Transfers den normalen Systembetrieb nicht beeinträchtigen sollten, können sie sich auf die gesamte vom StorageGRID System benötigte Netzwerkbandbreite auswirken.
- Aufgaben für die Deaktivierung von Storage-Nodes haben eine niedrigere Priorität als Aufgaben, die mit normalen Systemvorgängen verbunden sind. Dadurch wird die Ausmusterung normale StorageGRID Systemvorgänge nicht beeinträchtigt und es muss keine Zeit für die Inaktivität des Systems eingeplant werden. Da die Ausmusterung im Hintergrund erfolgt, ist es schwierig zu schätzen, wie lange der Vorgang dauert. Im Allgemeinen erfolgt die Ausmusterung von Storage-Nodes schneller, wenn das System still ist oder nur ein Storage-Node gleichzeitig entfernt wird.
- Es kann Tage oder Wochen dauern, bis ein Storage-Node außer Betrieb gesetzt wurde. Planen Sie dieses Verfahren entsprechend. Der Prozess zur Deaktivierung sorgt zwar dafür, dass der Betrieb des Systems nicht beeinträchtigt wird, aber weitere Verfahren werden möglicherweise eingeschränkt. Im Allgemeinen sollten geplante System-Upgrades oder -Erweiterungen durchgeführt werden, bevor Grid-Nodes entfernt werden.
- Während bestimmter Phasen können Verfahren zur Deaktivierung von Speicherknoten angehalten werden, damit andere Wartungsvorgänge bei Bedarf ausgeführt und nach Abschluss wieder aufgenommen werden können.
- Wenn eine Aufgabe zur Ausmusterung ausgeführt wird, können auf keinem Grid-Node Reparaturvorgänge ausgeführt werden.
- Während der Deaktivierung eines Storage Node sollten Sie keine Änderungen an der ILM-Richtlinie vornehmen.
- Wenn Sie einen Storage-Node entfernen, werden die Daten des Node zu anderen Grid-Nodes migriert. Diese Daten werden jedoch nicht vollständig aus dem ausgemusterten Grid-Node entfernt. Zum endgültigen und sicheren Entfernen von Daten müssen die Laufwerke des ausgemusterten Grid-Nodes nach Abschluss des Stilllegen-Vorgangs gelöscht werden.
- Wenn Sie einen Storage-Node außer Betrieb nehmen, werden möglicherweise die folgenden Warnmeldungen und Alarmer ausgelöst. Darüber hinaus erhalten Sie möglicherweise entsprechende E-Mail- und SNMP-Benachrichtigungen:
 - **Kommunikation mit Knoten** Warnung nicht möglich. Diese Warnmeldung wird ausgelöst, wenn Sie einen Speicherknoten außer Betrieb setzen, der den ADC-Dienst enthält. Die Meldung wird nach Abschluss des Stilllegen-Vorgangs behoben.
 - **VSTU-Alarm (Object Verification Status)**. Dieser Alarm auf Benachrichtigungsebene zeigt an, dass der Speicherknoten während der Stilllegung in den Wartungsmodus wechselt.
 - **CASA (Data Store Status) Alarm**. Dieser Großalarm zeigt an, dass die Cassandra-Datenbank ausfällt, da die Dienste angehalten wurden.

Verwandte Informationen

[Wiederherstellen von Objektdaten im Storage Volume, falls erforderlich](#)

Das ADC-Quorum verstehen

Bestimmte Storage-Nodes können an einem Datacenter-Standort möglicherweise nicht außer Betrieb gesetzt werden, falls nach der Ausmusterung zu wenige Dienste des Administrative Domain Controller (ADC) verbleiben würden. Dieser Service, der auf einigen Storage-Nodes enthalten ist, pflegt Grid-Topologiedaten und stellt Konfigurationsdienste für das Grid bereit. Das StorageGRID System erfordert, dass an jedem Standort und zu jeder Zeit ein Quorum von ADC-Services verfügbar ist.

Ein Speicherknoten kann nicht stillgelegt werden, wenn das Entfernen des Knotens dazu führt, dass das ADC-Quorum nicht mehr erfüllt wird. Um das ADC-Quorum während eines Stilllegungsvorgangs zu erfüllen, muss an jedem Datacenter mindestens drei Storage-Nodes über den ADC-Service verfügen. Bei mehr als drei Storage-Nodes an einem Datacenter mit dem ADC-Service muss ein einfacher Großteil dieser Nodes nach der Ausmusterung verfügbar sein $((0.5 * \text{Storage Nodes with ADC}) + 1)$.

Nehmen Sie beispielsweise an, ein Datacenter-Standort umfasst derzeit sechs Storage-Nodes mit ADC-Services, und Sie möchten drei Storage-Nodes außer Betrieb nehmen. Aufgrund der Quorum-Anforderung des ADC müssen Sie zwei Verfahren zur Deaktivierung durchführen:

- Beim ersten Stilllegen müssen Sie sicherstellen, dass vier Speicherknoten mit ADC-Diensten verfügbar bleiben $((0.5 * 6) + 1)$. Das bedeutet, dass Sie zunächst nur zwei Storage-Nodes außer Betrieb nehmen können.
- Im zweiten Verfahren können Sie den dritten Speicherknoten entfernen, da das ADC-Quorum jetzt nur noch drei ADC-Dienste benötigt $((0.5 * 4) + 1)$.

Wenn ein Speicherknoten außer Betrieb gesetzt werden muss, aber aufgrund der ADC-Quorum-Anforderung nicht in der Lage ist, müssen Sie einen neuen Speicherknoten in einer Erweiterung hinzufügen und angeben, dass er über einen ADC-Dienst verfügen soll. Anschließend können Sie den vorhandenen Storage-Node ausmustern.

Verwandte Informationen

[Erweitern Sie Ihr Raster](#)

Prüfen der ILM-Richtlinie und Storage-Konfiguration

Wenn Sie einen Storage-Node außer Betrieb nehmen möchten, sollten Sie die ILM-Richtlinie Ihres StorageGRID Systems überprüfen, bevor Sie den Ausmusterungsprozess starten.

Bei der Ausmusterung werden alle Objektdaten vom ausgemusterten Storage Node zu anderen Storage-Nodes migriert.



Die ILM-Richtlinie, die Sie während der Stilllegung haben, wird *nach* der Deaktivierung verwendet. Sie müssen sicherstellen, dass diese Richtlinie sowohl vor Beginn der Stilllegung als auch nach Abschluss der Stilllegung Ihre Daten erfüllt.

Sie sollten die Regeln in der aktiven ILM-Richtlinie überprüfen, um sicherzustellen, dass das StorageGRID System weiterhin über ausreichende Kapazität des richtigen Typs und an den richtigen Standorten verfügt, um

die Ausmusterung eines Storage-Nodes bewältigen zu können.

Bedenken Sie Folgendes:

- Werden ILM-Evaluierungsservices möglich sein, Objektdaten so zu kopieren, dass ILM-Regeln erfüllt sind?
- Was passiert, wenn ein Standort während der Stilllegung vorübergehend nicht mehr verfügbar ist? Können zusätzliche Kopien an einem alternativen Speicherort erstellt werden?
- Wie wird sich der Ausmusterungsprozess auf die finale Verteilung der Inhalte auswirken? Wie in beschrieben [Storage-Nodes Konsolidieren](#), Sie sollten neue Storage-Nodes hinzufügen, bevor Sie alte stilllegen. Wenn Sie nach der Stilllegung eines kleineren Storage-Nodes einen größeren Ersatz-Storage-Node hinzufügen, könnten die alten Storage-Nodes nahezu an Kapazität arbeiten und der neue Storage-Node könnte fast keinen Inhalt haben. Die meisten Schreibvorgänge für neue Objektdaten würden dann auf den neuen Storage-Node geleitet, wodurch die allgemeine Effizienz der Systemvorgänge verringert wird.
- Wird das System jederzeit genügend Storage-Nodes enthalten, um die aktive ILM-Richtlinie zu erfüllen?



Eine ILM-Richtlinie, die nicht zufriedenstellend ist, führt zu Rückprotokollen und Alarmen und kann den Betrieb des StorageGRID Systems unterbrechen.

Überprüfen Sie, ob die vorgeschlagene Topologie, die sich aus dem Stilllegungsvorgang ergibt, die ILM-Richtlinie erfüllt, indem Sie die in der Tabelle aufgeführten Faktoren bewerten.

Einzuschätzen	Hinweise
Verfügbare Kapazität	Werden genügend Storage-Kapazitäten für alle im StorageGRID System gespeicherten Objektdaten vorhanden sein, Sollen die permanenten Kopien der aktuell auf dem Storage Node gespeicherten Objektdaten stillgelegt werden?gibt es genügend Kapazität, um das erwartete Wachstum gespeicherter Objektdaten für ein vernünftiges Zeitintervall nach der Stilllegung zu verarbeiten?
Speicherort	Wenn genügend Kapazität im gesamten StorageGRID System verbleibt, sind die Kapazitäten an den richtigen Standorten, um den Geschäftsregeln des StorageGRID Systems gerecht zu werden?
Storage-Typ	Wird es genügend Storage des entsprechenden Typs geben, nachdem die Ausmusterung abgeschlossen ist? So kann es beispielsweise aufgrund von ILM-Regeln geben, dass Inhalte je nach Alter von einem Storage-Typ auf einen anderen verschoben werden. Wenn dies der Fall ist, müssen Sie sicherstellen, dass in der endgültigen Konfiguration des StorageGRID Systems genügend Storage des entsprechenden Typs verfügbar ist.

Verwandte Informationen

[Objektmanagement mit ILM](#)

[Erweitern Sie Ihr Raster](#)

Trennen Sie nicht verbundene Storage-Nodes außer Betrieb

Sie müssen wissen, was passieren kann, wenn Sie einen Storage-Knoten außer Betrieb setzen, während er nicht verbunden ist (Zustand ist unbekannt oder administrativ ausgefallen).

Wenn Sie einen Storage-Node, der vom Raster getrennt wird, außer Betrieb nehmen, verwendet StorageGRID Daten von anderen Storage-Nodes, um die Objektdaten und Metadaten des getrennten Node zu rekonstruieren. Dazu werden am Ende des Stilllegungsvorgangs automatisch Datenreparaturaufgaben gestartet.

Bevor Sie einen getrennten Storage-Node stilllegen, müssen Sie Folgendes beachten:

- Ein getrennter Node sollte niemals außer Betrieb genommen werden, es sei denn, Sie können ihn nicht online oder wiederhergestellt werden.



Führen Sie dieses Verfahren nicht aus, wenn Sie glauben, dass möglicherweise Objektdaten vom Node wiederhergestellt werden können. Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, ob das Recovery von Nodes möglich ist.

- Wenn ein getrennter Storage-Node die einzige Kopie eines Objekts enthält, geht dieses Objekt verloren, wenn Sie den Node ausmustern. Die Datenrekonstruktionsaufgaben können Objekte nur rekonstruieren und wiederherstellen, wenn mindestens eine replizierte Kopie oder genug Fragmente mit Lösungscode auf aktuell verbundenen Storage-Nodes vorhanden sind.
- Wenn Sie einen getrennten Storage-Node ausmustern, wird der Vorgang der Ausmusterung relativ schnell abgeschlossen. Die Ausführung der Reparatur von Daten kann jedoch Tage oder Wochen dauern und wird nicht durch den Außerbetriebnahme überwacht. Sie müssen diese Jobs manuell überwachen und nach Bedarf neu starten. Siehe [Prüfen Sie die Reparatur von Daten](#).
- Wenn Sie mehrere getrennte Storage-Nodes gleichzeitig außer Betrieb nehmen, kann es zu Datenverlusten kommen. Das System ist möglicherweise nicht in der Lage, Daten zu rekonstruieren, wenn zu wenige Kopien von Objektdaten, Metadaten oder Erasure-Coding-Fragmenten verfügbar sind.



Wenn mehr als ein getrennter Speicherknoten vorhanden ist, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

Storage-Nodes Konsolidieren

Sie können Storage-Nodes konsolidieren, um die Anzahl der Storage-Nodes für einen Standort oder eine Bereitstellung zu verringern und gleichzeitig die Storage-Kapazität zu erhöhen.

Wenn Sie Storage-Nodes konsolidieren, erweitern Sie das StorageGRID System, um neue Storage-Nodes mit größerer Kapazität hinzuzufügen, und Mustern die alten Storage-Nodes mit geringerer Kapazität aus. Während der Deaktivierung werden Objekte von den alten Storage Nodes zu den neuen Storage Nodes migriert.



Wenn Sie ältere und kleinere Appliances mit neuen Modellen oder Appliances mit höherer Kapazität konsolidieren, nutzen Sie viele die Klon-Funktion des Nodes oder das Verfahren des Node-Klonens und Mustern die Ausmusterung, wenn Sie keinen Einzelaustausch durchführen.

Beispielsweise können Sie zwei neue Storage-Nodes mit größerer Kapazität hinzufügen, um drei ältere

Storage-Nodes zu ersetzen. Sie würden zuerst das Erweiterungsverfahren verwenden, um die beiden neuen, größeren Storage-Nodes hinzuzufügen, und anschließend die drei alten Storage-Nodes mit geringerer Kapazität entfernen.

Durch Hinzufügen neuer Kapazität vor dem Entfernen vorhandener Storage-Nodes wird eine ausgewogenere Datenverteilung im gesamten StorageGRID System sichergestellt. Sie reduzieren auch die Möglichkeit, dass ein vorhandener Storage-Node über die Storage-Grenzmarke hinaus geschoben werden kann.

Verwandte Informationen

[Erweitern Sie Ihr Raster](#)

Ausmustern mehrerer Storage-Nodes

Wenn mehr als ein Storage-Node entfernt werden muss, können Sie sie nacheinander oder parallel absetzen.

- Wenn Sie Storage-Nodes nacheinander ausmustern, müssen Sie warten, bis der erste Storage-Node heruntergefahren wurde, bevor Sie den nächsten Storage-Node außer Betrieb nehmen.
- Wenn Sie Storage-Nodes parallel ausmustern, verarbeiten die Storage-Nodes zugleich Aufgaben zur Deaktivierung aller Storage-Nodes. Dies kann dazu führen, dass alle permanenten Kopien einer Datei als "read-only," markiert werden, wenn das Löschen in Gittern, in denen diese Funktion aktiviert ist, vorübergehend deaktiviert wird.

Prüfen Sie die Reparatur von Daten

Bevor Sie einen Grid-Node außer Betrieb nehmen, müssen Sie bestätigen, dass keine Datenreparatur-Jobs aktiv sind. Wenn Reparaturen fehlgeschlagen sind, müssen Sie sie neu starten und vor der Außerbetriebnahme abschließen lassen.

Wenn Sie einen getrennten Speicherknoten stilllegen müssen, führen Sie diese Schritte auch aus, nachdem der Vorgang abgeschlossen wurde, um sicherzustellen, dass der Reparaturauftrag erfolgreich abgeschlossen wurde. Sie müssen sicherstellen, dass alle Fragmente, die mit Erasure-Coding-Verfahren codiert wurden, die sich auf dem entfernten Node befanden, erfolgreich wiederhergestellt wurden.

Die Schritte gelten nur für Systeme mit Erasure-Coding-Objekten.

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

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

- 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:

2. Auf laufende Reparaturen prüfen: `repair-data show-ec-repair-status`

- Wenn Sie noch nie einen Datenreparaturauftrag ausgeführt haben, wird die Ausgabe angezeigt `No job found`. Sie müssen keine Reparaturaufträge neu starten.
- Wenn der Datenreparaturauftrag zuvor ausgeführt wurde oder derzeit ausgeführt wird, listet die Ausgabe Informationen für die Reparatur auf. Jede Reparatur hat eine eindeutige Reparatur-ID.

Fahren Sie mit dem nächsten Schritt fort.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
=====
=====
949283 DC1-S-99-10 (Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10 (Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10 (Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10 (Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. Wenn der Zustand für alle Reparaturen ist `Success`, Sie müssen keine Reparaturaufträge neu starten.
4. Wenn der Status für eine Reparatur ist `Failure`, Sie müssen diese Reparatur neu starten.
 - a. Beziehen Sie die Reparatur-ID für die fehlerhafte Reparatur von der Ausgabe.
 - b. Führen Sie die aus `repair-data start-ec-node-repair` Befehl.

Verwenden Sie die `--repair-id` Option zum Festlegen der Reparatur-ID. Wenn Sie beispielsweise eine Reparatur mit der Reparatur-ID 949292 erneut versuchen möchten, führen Sie den folgenden Befehl aus: `repair-data start-ec-node-repair --repair-id 949292`
 - c. Verfolgen Sie den Status der EC-Datenreparaturen weiter, bis der Zustand für alle Reparaturen vorliegt `Success`.

Sammeln Sie die erforderlichen Materialien

Bevor Sie einen Grid-Node außer Betrieb nehmen, müssen Sie die folgenden Informationen erhalten.

Element	Hinweise
Wiederherstellungspaket .zip Datei	Unbedingt Laden Sie das neueste Wiederherstellungspaket herunter .zip Datei (<code>sgws-recovery-package-id-revision.zip</code>). Sie können die Recovery Package-Datei verwenden, um das System wiederherzustellen, wenn ein Fehler auftritt.
Passwords.txt Datei	Diese Datei enthält die Passwörter, die für den Zugriff auf Grid-Knoten in der Befehlszeile erforderlich sind und im Wiederherstellungspaket enthalten sind.

Element	Hinweise
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im <code>Passwords.txt</code> Datei:
Beschreibung der Topologie des StorageGRID Systems vor der Stilllegung	Falls verfügbar, finden Sie eine Dokumentation, die die aktuelle Topologie des Systems beschreibt.

Verwandte Informationen

[Anforderungen an einen Webbrowser](#)

Öffnen Sie die Seite Decommission Nodes

Wenn Sie im Grid Manager auf die Seite Decommission Nodes zugreifen, sehen Sie auf einen Blick, welche Knoten deaktiviert werden können.

Was Sie benötigen

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

Schritte

1. Wählen Sie **WARTUNG Aufgaben Dekommission**.
2. Wählen Sie **Decommission Nodes**.

Die Seite Decommission Nodes wird angezeigt. Auf dieser Seite können Sie:

- Legen Sie fest, welche Grid-Nodes derzeit deaktiviert werden können.
- Den Systemzustand aller Grid-Nodes anzeigen
- Sortieren Sie die Liste in aufsteigender oder absteigender Reihenfolge nach **Name**, **Standort**, **Typ** oder **hat ADC**.
- Geben Sie Suchbegriffe ein, um bestimmte Nodes schnell zu finden. Beispielsweise werden auf dieser Seite die Grid-Nodes in zwei Datacentern angezeigt. Die Spalte Decommission Mögliche gibt an, dass Sie den Gateway-Node, einen der fünf Storage-Nodes und den nicht primären Admin-Node außer Betrieb nehmen können.

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

Search Q								
Name	Site	Type	Has ADC	Health	Decommission Possible			
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, primary Admin Node decommissioning is not supported.			
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, Archive Nodes decommissioning is not supported.			
☐ DC1-G1	Data Center 1	API Gateway Node	-	✓	✓			
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.			
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.			
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.			
☐ DC1-S4	Data Center 1	Storage Node	No	✓	✓			
☐ DC2-ADM1	Data Center 2	Admin Node	-	✓	✓			
DC2-S1	Data Center 2	Storage Node	Yes	✓	No, site Data Center 2 requires a minimum of 3 Storage Nodes with ADC services.			

3. Überprüfen Sie die Spalte **Decommission möglich** für jeden Knoten, den Sie stilllegen möchten.

Wenn ein Grid-Node deaktiviert werden kann, enthält diese Spalte ein grünes Häkchen, und in der Spalte links ist das Kontrollkästchen enthalten. Wenn ein Node nicht außer Betrieb genommen werden kann, wird in dieser Spalte das Problem beschrieben. Wenn ein Node nicht mehr außer einem Grund außer Betrieb genommen werden kann, wird der kritischste Grund angezeigt.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, die Ausmusterung von Node-Typen wird nicht unterstützt.	Sie können den primären Admin-Node oder einen Archiv-Node nicht stilllegen.	Keine.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, mindestens ein Grid-Node ist getrennt. Hinweis: Diese Meldung wird nur für verbundene Grid-Knoten angezeigt.	Sie können einen verbundenen Grid-Node nicht stilllegen, wenn ein Grid-Node getrennt ist. Die Spalte Health enthält eines der folgenden Symbole für getrennte Grid-Knoten: •  (Grau): Administrativ nach unten •  (Blau): Unbekannt	Wechseln Sie zum Schritt, in dem die Optionen für das Stilllegen aufgeführt sind.
Nein, ein oder mehrere erforderliche Nodes sind derzeit getrennt und müssen wiederhergestellt werden. Hinweis: Diese Meldung wird nur für getrennte Gitterknoten angezeigt.	Ein nicht getrennter Grid-Node kann nicht stillgelegt werden, wenn auch ein oder mehrere erforderliche Nodes getrennt sind (z. B. ein Storage-Node, der für das ADC-Quorum erforderlich ist).	- Überprüfen Sie die möglichen Meldungen zur Dekommission für alle nicht verbundenen Knoten. - Legen Sie fest, welche Nodes nicht außer Betrieb genommen werden können, da sie erforderlich sind. - Wenn der Status eines erforderlichen Knotens „Administrativ ausgefallen“ ist, stellen Sie den Knoten wieder in den Online-Modus. - Wenn der Systemzustand eines erforderlichen Node Unbekannt ist, führen Sie einen Wiederherstellungsvorgang für den Node durch, um den erforderlichen Node wiederherzustellen.
Nein, Mitglied der HA-Gruppe(n): X. Bevor Sie diesen Node außer Betrieb nehmen können, müssen Sie ihn aus allen HA-Gruppen entfernen.	Sie können einen Admin-Node oder einen Gateway-Node nicht außer Betrieb nehmen, wenn eine Node-Schnittstelle einer HA-Gruppe (High Availability, Hochverfügbarkeit) angehört.	Bearbeiten Sie die HA-Gruppe, um die Schnittstelle des Node zu entfernen, oder entfernen Sie die gesamte HA-Gruppe. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Möglichen Grund einer Deaktivierung	Beschreibung	Schritte zur Lösung
Nein, Standort x erfordert mindestens n Storage Nodes mit ADC-Services.	Nur Speicherknoten. ein Speicherknoten kann nicht stillgelegt werden, wenn nicht genügend Knoten am Standort verbleiben würden, um ADC-Quorum-Anforderungen zu unterstützen.	Eine Erweiterung durchführen. Fügen Sie dem Standort einen neuen Speicherknoten hinzu, und geben Sie an, dass ein ADC-Dienst vorhanden sein soll. Siehe Informationen über das ADC-Quorum.
Nein, mindestens ein Erasure Coding-Profil benötigt mindestens n Storage-Nodes. Wenn das Profil in einer ILM-Regel nicht verwendet wird, können Sie es deaktivieren.	Nur Speicherknoten. Sie können einen Speicherknoten nicht stilllegen, es sei denn, es würden genügend Knoten für die vorhandenen Erasure Coding Profile übrig bleiben. Wenn beispielsweise ein Erasure Coding-Profil für das Erasure Coding-Verfahren von 4+2 vorhanden ist, müssen mindestens 6 Storage-Nodes verbleiben.	Führen Sie für jedes betroffene Erasure Coding-Profil einen der folgenden Schritte aus, je nachdem, wie das Profil verwendet wird: • In der aktiven ILM-Richtlinie verwendet: Eine Erweiterung durchführen. Fügen Sie genügend neue Storage-Nodes hinzu, um das Erasure Coding-Verfahren fortzusetzen. Weitere Informationen finden Sie in den Anweisungen zum erweitern von StorageGRID. • Wird in einer ILM-Regel verwendet, aber nicht in der aktiven ILM-Richtlinie: Bearbeiten oder löschen Sie die Regel und deaktivieren Sie dann das Erasure Coding-Profil. • Nicht in einer ILM-Regel verwendet: Deaktivieren Sie das Erasure Coding-Profil. Hinweis: eine Fehlermeldung erscheint, wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren und Objektdaten weiterhin mit dem Profil verknüpft sind. Sie müssen möglicherweise mehrere Wochen warten, bevor Sie den Deaktivierungsprozess erneut versuchen. Erfahren Sie mehr über die Deaktivierung eines Erasure Coding-Profils in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

4. Falls für den Knoten ein Stilllegen möglich ist, bestimmen Sie, welche Prozedur Sie durchführen müssen:

Wenn Ihr Grid Folgendes enthält:	Gehe zu...
Alle getrennten Grid-Nodes	Die getrennten Grid-Nodes werden deaktiviert
Nur verbundene Grid-Nodes	Verbundene Grid-Nodes ausmustern

Verwandte Informationen

[Prüfen Sie die Reparatur von Daten](#)

[Das ADC-Quorum verstehen](#)

[Objektmanagement mit ILM](#)

[Erweitern Sie Ihr Raster](#)

[StorageGRID verwalten](#)

Die getrennten Grid-Nodes werden deaktiviert

Möglicherweise müssen Sie einen Knoten außer Betrieb setzen, der derzeit nicht mit dem Grid verbunden ist (einen Node, dessen Status unbekannt oder administrativ ausgefallen ist).

Was Sie benötigen

- Sie verstehen die Anforderungen und [Überlegungen für die Deaktivierung von Grid-Nodes](#).
- Sie haben alle erforderlichen Elemente erhalten.
- Sie haben sichergestellt, dass keine Datenreparaturjobs aktiv sind. Siehe [Prüfen Sie die Reparatur von Daten](#).
- Sie haben bestätigt, dass die Wiederherstellung von Storage-Nodes an keiner Stelle im Grid ausgeführt wird. In diesem Fall müssen Sie warten, bis alle Cassandra-Rebuilds im Rahmen der Recovery abgeschlossen sind. Anschließend können Sie mit der Stilllegung fortfahren.
- Sie haben sichergestellt, dass andere Wartungsvorgänge während der Deaktivierung des Nodes nicht ausgeführt werden, es sei denn, der Vorgang zur Deaktivierung des Nodes wurde angehalten.
- Die Spalte **Decommission möglich** für den Knoten oder Knoten, die Sie außer Betrieb nehmen möchten, enthält ein grünes Häkchen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Über diese Aufgabe

Sie können nicht verbundene Knoten identifizieren, indem Sie in der Spalte **Health** nach Unbekannt (blau) oder Administrativ Down (grau)-Symbolen suchen. Im Beispiel ist der Speicherknoten DC1-S4 getrennt; alle anderen Knoten sind verbunden.

Beachten Sie vor dem Stilllegen getrennter Nodes Folgendes:

- Dieses Verfahren dient in erster Linie zum Entfernen eines einzelnen nicht verbundenen Knotens. Wenn Ihr Grid mehrere getrennte Knoten enthält, muss die Software gleichzeitig ausmustern, wodurch das Potenzial für unerwartete Ergebnisse erhöht wird.



Gehen Sie sehr vorsichtig vor, wenn Sie mehrere getrennte Grid-Nodes gleichzeitig außer Betrieb nehmen. Dies gilt insbesondere dann, wenn Sie mehrere getrennte Storage-Nodes auswählen.

- Wenn ein nicht getrennter Knoten nicht entfernt werden kann (z. B. ein Speicherknoten, der für das ADC-Quorum benötigt wird), kann kein anderer nicht getrennter Knoten entfernt werden.

Beachten Sie vor dem Stilllegen eines nicht verbundenen **Storage Node** Folgendes

- Sie sollten niemals einen getrennten Storage-Knoten außer Betrieb nehmen, wenn Sie sicher sind, dass er nicht online oder wiederhergestellt werden kann.



Wenn Sie glauben, dass Objektdaten weiterhin über den Node wiederhergestellt werden können, führen Sie dieses Verfahren nicht aus. Wenden Sie sich stattdessen an den technischen Support, um zu ermitteln, ob das Recovery von Nodes möglich ist.

- Wenn Sie mehrere getrennte Storage-Nodes außer Betrieb nehmen, kann es zu Datenverlusten kommen. Das System ist möglicherweise nicht in der Lage, Daten zu rekonstruieren, wenn nicht genügend Objektkopien, Fragmente mit Erasure-Coding-Verfahren oder Objekt-Metadaten verfügbar sind.



Wenn mehr als ein getrennter Speicherknoten vorhanden ist, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

- Wenn Sie einen getrennten Storage-Node außer Betrieb nehmen, startet StorageGRID am Ende des Stilllegungsvorgangs die Reparatur der Daten. Diese Jobs versuchen, die Objektdaten und Metadaten, die auf dem getrennten Node gespeichert waren, zu rekonstruieren.
- Wenn Sie einen getrennten Storage-Node ausmustern, wird der Vorgang der Ausmusterung relativ schnell abgeschlossen. Die Ausführung der Reparatur von Daten kann jedoch Tage oder Wochen dauern und wird nicht durch den Außerbetriebnahme überwacht. Sie müssen diese Jobs manuell überwachen und nach Bedarf neu starten. Siehe [Prüfen Sie die Reparatur von Daten](#).
- Wenn Sie einen getrennten Storage-Node stilllegen, der die einzige Kopie eines Objekts enthält, geht das Objekt verloren. Die Datenrekonstruktionsaufgaben können Objekte nur rekonstruieren und wiederherstellen, wenn mindestens eine replizierte Kopie oder genug Fragmente mit Lösungscode auf aktuell verbundenen Storage-Nodes vorhanden sind.

Beachten Sie vor dem Stilllegen eines nicht verbundenen **Admin-Node** oder **Gateway-Node** Folgendes:

- Wenn Sie einen getrennten Admin-Node stilllegen, verlieren Sie die Audit-Protokolle von diesem Node. Diese Protokolle sollten jedoch auch im primären Admin-Node vorhanden sein.
- Sie können einen Gateway-Node sicher außer Betrieb setzen, während er getrennt ist.

Schritte

1. Versuchen Sie, getrennte Grid-Nodes wieder online zu bringen oder sie wiederherzustellen.

Anweisungen hierzu finden Sie in den Wiederherstellungsverfahren.

2. Wenn Sie einen getrennten Grid-Node nicht wiederherstellen können und ihn während der Trennung außer Betrieb setzen möchten, aktivieren Sie das Kontrollkästchen für diesen Node.



Wenn Ihr Grid mehrere getrennte Knoten enthält, muss die Software gleichzeitig ausmustern, wodurch das Potenzial für unerwartete Ergebnisse erhöht wird.



Gehen Sie sehr vorsichtig vor, wenn Sie mehrere getrennte Grid-Nodes gleichzeitig außer Betrieb nehmen möchten, insbesondere wenn Sie mehrere getrennte Storage-Nodes auswählen. Wenn mehr als ein getrennter Speicherknoten vorhanden ist, den Sie nicht wiederherstellen können, wenden Sie sich an den technischen Support, um die beste Vorgehensweise zu ermitteln.

3. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start Decommission** ist aktiviert.

4. Klicken Sie Auf **Start Decommission**.

Es wird eine Warnung angezeigt, die angibt, dass Sie einen nicht verbundenen Knoten ausgewählt haben und dass Objektdaten verloren gehen, wenn der Knoten die einzige Kopie eines Objekts hat.

 Warning

The selected nodes are disconnected (health is Unknown or Administratively Down). If you continue and the node has the only copy of an object, the object will be lost when the node is removed.

The following grid nodes have been selected for decommissioning and will be permanently removed from the StorageGRID Webscale system.

DC1-S4

Do you want to continue?

Cancel

OK

5. Überprüfen Sie die Liste der Knoten, und klicken Sie auf **OK**.

Der Vorgang zur Deaktivierung wird gestartet und für jeden Node wird der Fortschritt angezeigt. Während des Verfahrens wird ein neues Wiederherstellungspaket mit der Änderung der Grid-Konfiguration generiert.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package page](#) to download it.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Search				
Name	Type	Progress	Stage	
DC1-S4	Storage Node		Prepare Task	

Pause Resume

6. Sobald das neue Wiederherstellungspaket verfügbar ist, klicken Sie auf den Link oder wählen Sie **WARTUNG System Wiederherstellungspaket**, um die Seite des Wiederherstellungspakets aufzurufen. Laden Sie anschließend die herunter .zip Datei:

Siehe Anweisungen für [Herunterladen des Wiederherstellungspakets](#).



Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Grid wiederherstellen können, wenn während des Stillfalls etwas schief geht.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

7. Überwachen Sie die Seite Dekommission regelmäßig, um sicherzustellen, dass alle ausgewählten Knoten erfolgreich außer Betrieb gesetzt werden.

Storage-Nodes können Tage oder Wochen ausmustern. Wenn alle Aufgaben abgeschlossen sind, wird die Liste der Knotenauswahl mit einer Erfolgsmeldung erneut angezeigt. Wenn Sie einen getrennten Speicherknoten außer Betrieb genommen haben, zeigt eine Informationsmeldung an, dass die Reparaturaufträge gestartet wurden.

8. Nachdem die Nodes im Rahmen der Stilllegung automatisch heruntergefahren wurden, entfernen Sie alle verbleibenden Virtual Machines oder anderen Ressourcen, die dem ausgemusterten Node zugeordnet sind.



Führen Sie diesen Schritt erst aus, wenn die Nodes automatisch heruntergefahren wurden.

9. Wenn Sie einen Storage Node außer Betrieb nehmen, überwachen Sie den Status der Reparatur-Jobs mit **replizierten Daten** und **Erasure-codierten (EC) Daten**, die während des Stilllegungsprozesses automatisch gestartet werden.

Replizierte Daten

- So stellen Sie fest, ob Reparaturen abgeschlossen sind:
 - a. Wählen Sie **NODES Storage Node wird repariert ILM** aus.
 - b. Prüfen Sie die Attribute im Abschnitt Bewertung. Wenn die Reparaturen abgeschlossen sind, weist das Attribut **wartet - Alle** 0 Objekte an.
- So überwachen Sie die Reparatur genauer:
 - a. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
 - b. Wählen Sie **Grid Speicherknoten, der repariert wird LDR Datenspeicher** aus.
 - c. Verwenden Sie eine Kombination der folgenden Attribute, um festzustellen, ob replizierte Reparaturen abgeschlossen sind.



Cassandra ist möglicherweise Inkonsistenzen vorhanden und fehlgeschlagene Reparaturen werden nicht nachverfolgt.

- **Reported (XRPA):** Verwenden Sie dieses Attribut, um den Fortschritt der replizierten Reparaturen zu verfolgen. Dieses Attribut erhöht sich jedes Mal, wenn ein Storage-Node versucht, ein risikoreicheres Objekt zu reparieren. Wenn dieses Attribut für einen Zeitraum nicht länger als die aktuelle Scan-Periode (vorgesehen durch das Attribut **Scan Period — Estimated**) steigt, bedeutet dies, dass ILM-Scans keine hoch riskant Objekte gefunden haben, die auf allen Knoten repariert werden müssen.



Objekte mit hohem Risiko sind Objekte, die Gefahr laufen, völlig verloren zu sein. Dies umfasst keine Objekte, die ihre ILM-Konfiguration nicht erfüllen.

- **Scan Period — Estimated (XSCM):** Verwenden Sie dieses Attribut, um zu schätzen, wann eine Richtlinienänderung auf zuvor aufgenommene Objekte angewendet wird. Wenn sich das Attribut **Repairs versuchte** über einen Zeitraum nicht länger als der aktuelle Scanzeitraum erhöht, ist es wahrscheinlich, dass replizierte Reparaturen durchgeführt werden. Beachten Sie, dass sich der Scanzeitraum ändern kann. Das Attribut **Scan Period — Estimated (XSCM)** gilt für das gesamte Raster und ist die maximale Anzahl aller Knoten Scan Perioden. Sie können den Attributverlauf des Attributs **Scanperiode — Estimated** für das Raster abfragen, um einen geeigneten Zeitrahmen zu ermitteln.
- Wenn Sie optional einen geschätzten Fertigstellungsgrad für die replizierte Reparatur erhalten möchten, fügen Sie den hinzu `show-replicated-repair-status` Option zum Befehl `Repair-Data`.

```
repair-data show-replicated-repair-status
```



Der `show-replicated-repair-status` Die Option ist für die technische Vorschau in StorageGRID 11.6 verfügbar. Diese Funktion ist in der Entwicklung, und der zurückgegebene Wert kann falsch oder verzögert sein. Um festzustellen, ob eine Reparatur abgeschlossen ist, verwenden Sie **Anstehend – Alle, Reparaturen versucht (XRPA)** und **Scanzeitraum — Estimated (XSCM)** wie in beschrieben [Überwachen Sie Reparaturen](#).

EC-Daten (Erasure Coding)

So überwachen Sie die Reparatur von Daten mit Verfahren zur Einhaltung von Datenkonsistenz und versuchen Sie es erneut, eventuell fehlgeschlagene Anfragen zu senden:

1. Status von Datenreparaturen mit Lösungscode ermitteln:

- Wählen Sie **SUPPORT Tools Kennzahlen** aus, um die voraussichtliche Zeit bis zur Fertigstellung und den Prozentsatz für den Abschluss des aktuellen Jobs anzuzeigen. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.
- Verwenden Sie diesen Befehl, um den Status eines bestimmten anzuzeigen `repair-data` Betriebliche Gründe:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Verwenden Sie diesen Befehl, um alle Reparaturen aufzulisten:

```
repair-data show-ec-repair-status
```

Die Ausgabe enthält Informationen, einschließlich `repair ID`, Für alle zuvor und derzeit laufenden Reparaturen.

2. Wenn in der Ausgabe angezeigt wird, dass der Reparaturvorgang fehlgeschlagen ist, verwenden Sie den `--repair-id` Option, um die Reparatur erneut zu versuchen.

Mit diesem Befehl wird eine fehlerhafte Node-Reparatur mithilfe der Reparatur-ID 6949309319275667690 erneut versucht:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Mit diesem Befehl wird eine fehlerhafte Volume-Reparatur mithilfe der Reparatur-ID 6949309319275667690 wiederholt:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Nachdem Sie fertig sind

Sobald die getrennten Nodes außer Betrieb genommen und alle Reparatur-Jobs abgeschlossen sind, können Sie alle verbundenen Grid-Nodes je nach Bedarf ausmustern.

Führen Sie anschließend die folgenden Schritte aus, nachdem Sie den Vorgang zur Deaktivierung abgeschlossen haben:

- Stellen Sie sicher, dass die Laufwerke des ausgemusterten Grid-Node sauber gelöscht werden. Verwenden Sie ein handelsübliches Datenwischwerkzeug oder einen Dienst, um die Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn Sie einen Appliance-Node deaktiviert haben und die Daten auf der Appliance mithilfe der Node-Verschlüsselung geschützt wurden, löschen Sie die Konfiguration des Verschlüsselungsmanagement-Servers (Clear KMS) mithilfe des StorageGRID Appliance Installer. Wenn Sie die Appliance einem anderen Grid hinzufügen möchten, müssen Sie die KMS-Konfiguration löschen.
 - [SG100- und SG1000-Services-Appliances](#)
 - [SG5600 Storage Appliances](#)
 - [SG5700 Storage-Appliances](#)
 - [SG6000 Storage-Appliances](#)

Verwandte Informationen

Verfahren zur Recovery von Grid-Nodes

Verbundene Grid-Nodes ausmustern

Sie können Nodes, die mit dem Grid verbunden sind, außer Betrieb nehmen und dauerhaft entfernen.

- Sie müssen die Anforderungen und verstehen [Überlegungen für die Deaktivierung von Grid-Nodes](#).
- Sie müssen alle erforderlichen Materialien gesammelt haben.
- Sie müssen sicherstellen, dass keine Datenreparaturjobs aktiv sind.
- Sie müssen bestätigen, dass die Wiederherstellung von Storage-Nodes an keiner Stelle im Grid ausgeführt wird. In diesem Fall müssen Sie warten, bis alle Cassandra-Rebuilds im Rahmen der Recovery abgeschlossen sind. Anschließend können Sie mit der Stilllegung fortfahren.
- Sie müssen sicherstellen, dass andere Wartungsvorgänge während der Deaktivierung des Nodes nicht ausgeführt werden, es sei denn, der Vorgang zur Deaktivierung des Nodes wurde angehalten.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Die Grid-Nodes sind verbunden.
- Die Spalte **Decommission möglich** für den Knoten oder Knoten, die deaktiviert werden sollen, muss ein grünes Häkchen enthalten.
- Alle Grid-Nodes müssen den normalen Zustand (grün) aufweisen . Wenn eines dieser Symbole in der Spalte **Gesundheit** angezeigt wird, müssen Sie versuchen, das Problem zu lösen:

Symbol	Farbe	Schweregrad
	Gelb	Hinweis
	Hellorange	Gering
	Dunkelorange	Major
	Rot	Kritisch

- Wenn Sie zuvor einen getrennten Speicherknoten außer Betrieb genommen haben, wurden die Reparaturaufträge erfolgreich abgeschlossen. Siehe [Prüfen Sie die Reparatur von Daten](#).



Entfernen Sie die virtuelle Maschine oder andere Ressourcen eines Grid-Node erst, wenn Sie dazu in diesem Verfahren aufgefordert werden.

1. Aktivieren Sie auf der Seite Decommission Nodes das Kontrollkästchen für jeden Grid-Knoten, den Sie stilllegen möchten.
2. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start Decommission** ist aktiviert.

3. Klicken Sie Auf **Start Decommission**.

Ein Bestätigungsdialogfeld wird angezeigt.

 **Info**

The following grid nodes have been selected for decommissioning and will be permanently removed from the StorageGRID Webscale system.

DC1-S5

Do you want to continue?

Cancel OK

4. Überprüfen Sie die Liste der ausgewählten Knoten, und klicken Sie auf **OK**.

Daraufhin wird der Vorgang zum Stilllegen des Node gestartet, und der Fortschritt wird für jeden Node angezeigt. Während des Verfahrens wird ein neues Wiederherstellungspaket generiert, um die Änderung der Grid-Konfiguration anzuzeigen.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package page](#) to download it.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Name	Type	Progress	Stage
DC1-S5	Storage Node		Prepare Task

Pause Resume



Nehmen Sie einen Storage Node nicht in den Offline-Modus, nachdem der Vorgang zur Deaktivierung gestartet wurde. Wenn Sie den Status ändern, werden einige Inhalte möglicherweise nicht an andere Orte kopiert.

5. Sobald das neue Wiederherstellungspaket verfügbar ist, klicken Sie auf den Link oder wählen Sie **WARTUNG System Wiederherstellungspaket**, um die Seite des Wiederherstellungspakets aufzurufen. Laden Sie anschließend die herunter .zip Datei:

Siehe Anweisungen für [Herunterladen des Wiederherstellungspakets](#).



Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Grid wiederherstellen können, wenn während des Stillfalls etwas schief geht.

6. Überwachen Sie die Seite Decommission Nodes regelmäßig, um sicherzustellen, dass alle ausgewählten

Knoten erfolgreich deaktiviert wurden.

Storage-Nodes können Tage oder Wochen ausmustern. Wenn alle Aufgaben abgeschlossen sind, wird die Liste der Knotenauswahl mit einer Erfolgsmeldung erneut angezeigt.

7. Befolgen Sie den entsprechenden Schritt für Ihre Plattform. Beispiel:

- **Linux:** Möglicherweise möchten Sie die Volumes trennen und die Knoten-Konfigurationsdateien löschen, die Sie während der Installation erstellt haben.
- **VMware:** Sie können die vCenter “Delete from Disk” Option verwenden, um die virtuelle Maschine zu löschen. Möglicherweise müssen Sie auch alle Datenfestplatten löschen, die unabhängig von der virtuellen Maschine sind.
- **StorageGRID-Appliance:** Der Appliance-Knoten wird automatisch in einen nicht bereitgestellten Zustand zurückgesetzt, in dem Sie auf das Installationsprogramm der StorageGRID-Appliance zugreifen können. Sie können das Gerät ausschalten oder es einem anderen StorageGRID-System hinzufügen.

Führen Sie die folgenden Schritte aus, nachdem Sie den Vorgang zur Deaktivierung des Node abgeschlossen haben:

- Stellen Sie sicher, dass die Laufwerke des ausgemusterten Grid-Node sauber gelöscht werden. Verwenden Sie ein handelsübliches Datenwischwerkzeug oder einen Dienst, um die Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn Sie einen Appliance-Node deaktiviert haben und die Daten auf der Appliance mithilfe der Node-Verschlüsselung geschützt wurden, löschen Sie die Konfiguration des Verschlüsselungsmanagement-Servers (Clear KMS) mithilfe des StorageGRID Appliance Installer. Wenn Sie die Appliance in einem anderen Raster verwenden möchten, müssen Sie die KMS-Konfiguration löschen.

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

[SG5600 Storage Appliances](#)

[SG5700 Storage-Appliances](#)

[SG6000 Storage-Appliances](#)

Verwandte Informationen

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

Anhalten und Fortsetzen des Stilllegen-Prozesses für Storage-Nodes

Wenn Sie einen zweiten Wartungsvorgang durchführen müssen, können Sie das Verfahren zur Deaktivierung eines Storage Nodes während bestimmter Phasen unterbrechen. Nachdem das andere Verfahren abgeschlossen ist, können Sie die Stilllegung fortsetzen.



Die Schaltfläche **Pause** ist nur aktiviert, wenn die ILM-Bewertung oder die mit Erasure Coding versehenen Phasen der Datenauswertung erreicht sind. Die ILM-Evaluierung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt.

Was Sie benötigen

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

Schritte

1. Wählen Sie **WARTUNG Aufgaben Dekommission**.

Die Seite Decommission wird angezeigt.

2. Wählen Sie **Decommission Nodes**.

Die Seite Decommission Nodes wird angezeigt. Wenn die Deaktivierung eine der folgenden Stufen erreicht, ist die Schaltfläche **Pause** aktiviert.

- ILM-Evaluierung
- Erasure-codierte Daten werden stillgelegt

3. Wählen Sie **Pause**, um den Vorgang zu unterbrechen.

Die aktuelle Phase wird angehalten, und die Schaltfläche **Fortsetzen** ist aktiviert.

Decommission Nodes

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

 Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Search Q				
Name	Type	Progress	Stage	
DC1-S5	Storage Node		Evaluating ILM	

Pause

Resume

4. Nachdem der andere Wartungsvorgang abgeschlossen ist, wählen Sie **Fortsetzen** aus, um mit der Stilllegung fortzufahren.

Fehlerbehebung bei der Ausmusterung von Nodes

Wenn der Node aufgrund eines Fehlers deaktiviert wird, können Sie spezifische Schritte zum Beheben des Problems durchführen.

Was Sie benötigen

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

Über diese Aufgabe

Wenn Sie den stillgelegten Grid-Node herunterfahren, wird die Aufgabe angehalten, bis der Grid-Node neu gestartet wird. Der Grid-Node muss sich online sein.

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Erweitern Sie in der Struktur Grid Topology jeden Storage Node-Eintrag und überprüfen Sie, ob die DDS- und LDR-Dienste online sind.

Um eine Ausmusterung von Storage-Nodes durchzuführen, müssen alle Nodes und alle Services zu Beginn der Deaktivierung eines Online-Nodes/Standorts in einem ordnungsgemäßen Zustand sein.

3. Um die aktiven Grid-Aufgaben anzuzeigen, wählen Sie **Primary Admin Node CMN Grid Tasks Übersicht**.
4. Überprüfen Sie den Status der Task „Stilllegen“.
 - a. Wenn der Status des DeaktivierungsGrid-Tasks ein Problem beim Speichern von Grid Task Bundles anzeigt, wählen Sie **Primary Admin Node CMN Events Übersicht** aus
 - b. Prüfen Sie die Anzahl der verfügbaren Audit-Relais.

Wenn das Attribut Available Audit Relay ein oder größer ist, ist der CMN-Dienst mit mindestens einem ADC-Dienst verbunden. ADC-Dienste fungieren als Überwachungsrelais.

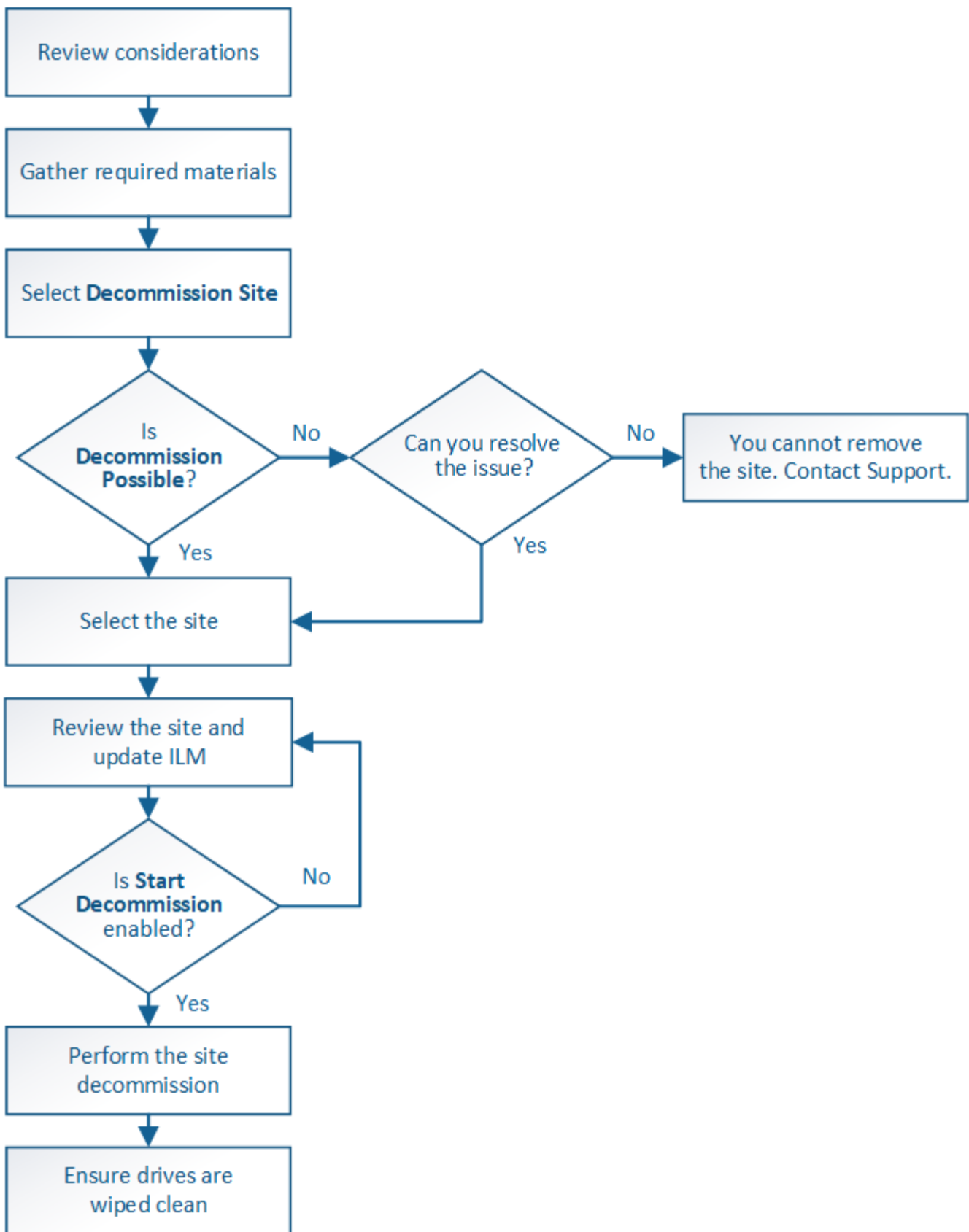
Der CMN-Dienst muss mit mindestens einem ADC-Dienst verbunden sein, und eine Mehrheit (50 Prozent plus einer) der ADC-Dienste des StorageGRID-Systems muss verfügbar sein, damit eine Grid-Aufgabe von einer Phase der Stilllegung in eine andere und zum Abschluss verschoben werden kann.

- a. Wenn der CMN-Dienst nicht mit genügend ADC-Diensten verbunden ist, stellen Sie sicher, dass Storage-Nodes online sind, und überprüfen Sie die Netzwerkverbindung zwischen dem primären Admin-Node und Storage-Nodes.

Deaktivierung der Website

Möglicherweise müssen Sie einen Datacenter-Standort aus dem StorageGRID System entfernen. Um eine Website zu entfernen, müssen Sie sie ausmustern.

Das Flussdiagramm zeigt die Schritte für die Außerbetriebnahme eines Standorts auf hoher Ebene.



Überlegungen zum Entfernen eines Standorts

Bevor Sie die Website wieder entfernen, müssen Sie zunächst die entsprechenden Überlegungen überprüfen.

Was geschieht, wenn Sie eine Website ausmustern

Durch die Stilllegung einer Website StorageGRID werden alle Nodes an der Website und der Standort selbst endgültig vom StorageGRID System entfernt.

Nach Abschluss der Deaktivierung der Website:

- StorageGRID kann nicht mehr zum Anzeigen und Zugreifen auf den Standort oder auf einen der Nodes am Standort verwendet werden.
- Sie können keine Storage-Pools oder Erasure Coding-Profil mehr verwenden, die auf den Standort verwiesen wurden. Wenn StorageGRID einen Standort dekomprimiert, werden diese Storage-Pools automatisch entfernt und diese Erasure Coding-Profil deaktiviert.

Unterschiede zwischen dem angeschlossenen Standort und dem Verfahren zur Deaktivierung des Standorts

Im Rahmen der Deaktivierung einer Website können Sie eine Site entfernen, in der alle Nodes mit StorageGRID verbunden sind (die als Deaktivierung verbundenen Site bezeichnet wird), oder eine Site entfernen, in der alle Nodes von StorageGRID getrennt sind (die so genannte Deaktivierung einer getrennten Site wird als deaktiviert). Bevor Sie beginnen, müssen Sie die Unterschiede zwischen diesen Verfahren verstehen.



Wenn ein Standort eine Mischung aus verbundenen (✓) Und nicht verbundene Knoten (☾) Oder (⚙️), Sie müssen alle Offline-Knoten wieder online bringen.

- Durch eine Deaktivierung einer verbundenen Website können Sie einen betrieblichen Standort aus dem StorageGRID System entfernen. Beispielsweise können Sie eine verbundene Website ausmustern, um eine funktionierende, aber nicht mehr benötigte Website zu entfernen.
- Wenn StorageGRID einen verbundenen Standort entfernt, wird ILM für das Management der Objektdaten am Standort verwendet. Bevor Sie eine verbundene Site außer Betrieb nehmen können, müssen Sie die Site von allen ILM-Regeln entfernen und eine neue ILM-Richtlinie aktivieren. Die ILM-Prozesse zur Migration von Objektdaten und die internen Prozesse zur Entfernung eines Standorts können gleichzeitig durchgeführt werden. Es empfiehlt sich jedoch, die ILM-Schritte zu schließen, bevor Sie den tatsächlichen Außerbetriebnahme starten.
- Bei einer getrennten Deaktivierung der Website können Sie fehlerhafte Standorte aus dem StorageGRID System entfernen. So können Sie beispielsweise eine abgelöste Außerbetriebnahme des Standorts durchführen, um einen Standort zu entfernen, der durch einen Brand oder eine Überschwemmung zerstört wurde.

Wenn StorageGRID eine getrennte Site entfernt, werden alle Nodes als nicht wiederherstellbar erachtet und nicht versucht, Daten zu erhalten. Bevor Sie eine getrennte Site jedoch außer Betrieb nehmen können, müssen Sie die Website jedoch von allen ILM-Regeln entfernen und eine neue ILM-Richtlinie aktivieren.



Bevor Sie eine Deaktivierung des Standorts durchführen, müssen Sie sich an Ihren NetApp Ansprechpartner wenden. NetApp überprüft Ihre Anforderungen, bevor Sie alle Schritte im Decommission Site Wizard aktivieren. Sie sollten keinen Versuch Unternehmen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie der Meinung sind, dass eine Wiederherstellung der Site oder die Wiederherstellung von Objektdaten von der Site möglich wäre.

Allgemeine Anforderungen für das Entfernen eines verbundenen oder getrennten Standorts

Bevor Sie einen angeschlossenen oder getrennten Standort entfernen, müssen Sie die folgenden Anforderungen erfüllen:

- Sie können keinen Standort außer Betrieb nehmen, der den primären Admin-Node enthält.
- Sie können keine Site außer Betrieb setzen, die einen Archiv-Node enthält.
- Sie können einen Standort nicht stilllegen, wenn einer der Nodes über eine Schnittstelle verfügt, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehört. Sie müssen entweder die HA-Gruppe bearbeiten, um die Schnittstelle des Node zu entfernen, oder die gesamte HA-Gruppe entfernen.
- Sie können eine Site nicht stilllegen, wenn sie eine Mischung aus verbundener ( Oder ) Knoten.  Und getrennt ( Oder ).
- Sie können einen Standort nicht stilllegen, wenn ein Node an einem anderen Standort getrennt ist ( Oder ).
- Sie können den Vorgang zur Deaktivierung des Standorts nicht starten, wenn derzeit ein ec-Node-Reparaturvorgang ausgeführt wird. Siehe [Prüfen Sie die Reparatur von Daten](#) Zur Nachverfolgung von Reparaturen mit Erasure-Coding-Daten.
- Während die Deaktivierung der Website läuft:
 - Sie können keine ILM-Regeln erstellen, die sich auf die auszugemusterte Site beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf die Site zu verweisen.
 - Sie können keine anderen Wartungsvorgänge wie z. B. Erweiterung oder Upgrade durchführen.



Wenn Sie während der Stilllegung einer verbundenen Website einen weiteren Wartungsvorgang durchführen müssen, können Sie dies auch tun [Halten Sie das Verfahren an, während die Speicherknoten entfernt werden](#). Die Schaltfläche **Pause** ist nur aktiviert, wenn die ILM-Bewertung oder die mit Erasure Coding versehenen Phasen der Datenauswertung erreicht sind. Die ILM-Evaluierung (Datenmigration) wird jedoch weiterhin im Hintergrund ausgeführt. Nach Abschluss des zweiten Wartungsverfahrens können Sie die Außerbetriebnahme fortsetzen.

- Falls Nodes nach dem Starten der Deaktivierung der Website wiederhergestellt werden müssen, müssen Sie den Support kontaktieren.
- Sie können nicht mehrere Standorte gleichzeitig außer Betrieb nehmen.
- Wenn die Site einen oder mehrere Admin-Nodes enthält und Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, müssen Sie alle Vertrauensstellen der Vertrauensstelle für die Site von Active Directory Federation Services (AD FS) entfernen.

Anforderungen für Information Lifecycle Management (ILM)

Beim Entfernen eines Standorts müssen Sie Ihre ILM-Konfiguration aktualisieren. Der Assistent für die Decommission Site führt Sie durch eine Reihe von erforderlichen Schritten, um Folgendes sicherzustellen:

- Die ILM-Richtlinie für den Standort wird nicht genutzt. In diesem Fall müssen Sie eine neue ILM-Richtlinie mit neuen ILM-Regeln erstellen und aktivieren.
- Es gibt keine vorgeschlagene ILM-Richtlinie. Wenn Sie über eine vorgeschlagene Richtlinie verfügen, müssen Sie diese löschen.

- Keine ILM-Regeln beziehen sich auf die Site, auch wenn diese Regeln nicht in der aktiven oder vorgeschlagenen Richtlinie verwendet werden. Sie müssen alle Regeln, die sich auf die Website beziehen, löschen oder bearbeiten.

Wenn StorageGRID den Standort dekomprimiert, werden automatisch alle nicht verwendeten Erasure Coding-Profilen deaktiviert, die auf den Standort verweisen. Außerdem werden alle nicht verwendeten Speicherpools, die sich auf den Standort beziehen, automatisch gelöscht. Der standardmäßige Speicherpool Alle Speicherknoten wird entfernt, da er alle Standorte verwendet.



Bevor Sie einen Standort entfernen können, müssen Sie möglicherweise neue ILM-Regeln erstellen und eine neue ILM-Richtlinie aktivieren. Diese Anweisungen setzen voraus, dass Sie alle Kenntnisse über die Funktionsweise von ILM haben und dass Sie mit der Erstellung von Storage-Pools, Erasure Coding-Profilen, ILM-Regeln sowie der Simulation und Aktivierung einer ILM-Richtlinie vertraut sind. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Objektmanagement mit ILM

Überlegungen zu den Objektdaten an einem angeschlossenen Standort

Wenn Sie eine verbundene Site außer Betrieb nehmen, müssen Sie beim Erstellen neuer ILM-Regeln und einer neuen ILM-Richtlinie festlegen, welche Daten an der Website gespeichert werden. Sie können entweder oder beide der folgenden Aktionen ausführen:

- Verschieben Sie Objektdaten vom ausgewählten Standort zu einem oder mehreren anderen Standorten in der Tabelle.

Beispiel für das Verschieben von Daten: Angenommen, Sie möchten eine Website in Raleigh ausmustern, weil Sie eine neue Website in Sunnyvale hinzugefügt haben. In diesem Beispiel möchten Sie alle Objektdaten vom alten Standort auf den neuen Standort verschieben. Bevor Sie Ihre ILM-Regeln und ILM-Richtlinie aktualisieren, müssen Sie die Kapazität an beiden Standorten prüfen. Sie müssen sicherstellen, dass der Standort in Sunnyvale über genügend Kapazität für die Objektdaten vom Standort Raleigh verfügt und dass im Rahmen eines zukünftigen Wachstums in Sunnyvale ausreichend Kapazität zur Verfügung steht.



Um sicherzustellen, dass ausreichend Kapazität verfügbar ist, müssen Sie möglicherweise einem vorhandenen Standort Storage-Volumes oder Speicherknoten hinzufügen oder einen neuen Standort hinzufügen, bevor Sie diesen Vorgang ausführen. Anweisungen zum Erweitern eines StorageGRID-Systems finden Sie in den Anweisungen.

- Löschen von Objektkopien vom ausgewählten Standort.

Beispiel für das Löschen von Daten: Angenommen, Sie verwenden derzeit eine ILM-Regel mit 3 Kopien, um Objektdaten auf drei Standorten zu replizieren. Bevor Sie einen Standort außer Betrieb nehmen, können Sie eine äquivalente ILM-Regel mit zwei Kopien erstellen, um Daten an nur zwei Standorten zu speichern. Wenn Sie eine neue ILM-Richtlinie aktivieren, die die Regel mit zwei Kopien verwendet, löscht StorageGRID die Kopien vom dritten Standort, da diese die ILM-Anforderungen nicht mehr erfüllen. Die Objektdaten werden jedoch weiterhin gesichert und die Kapazität der beiden verbleibenden Standorte bleibt gleich.



Erstellen Sie niemals eine ILM-Regel für eine einzelne Kopie, um die Entfernung eines Standorts aufzunehmen. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Zusätzliche Anforderungen für die Deaktivierung einer verbundenen Website

Bevor StorageGRID einen verbundenen Standort entfernen kann, müssen Sie Folgendes sicherstellen:

- Alle Knoten in Ihrem StorageGRID-System müssen über einen Verbindungsstatus von **Connected** (verfügen); die Knoten können jedoch aktive Warnmeldungen haben.



Wenn ein oder mehrere Knoten getrennt werden, können Sie die Schritte 1-4 des Assistenten zum Decommission Site ausführen. Sie können jedoch Schritt 5 des Assistenten nicht abschließen, der den Stilllegen-Prozess startet, es sei denn, alle Knoten sind verbunden.

- Wenn der Standort, den Sie entfernen möchten, einen Gateway-Node oder einen Admin-Node enthält, der zum Load Balancing verwendet wird, müssen Sie möglicherweise ein Erweiterungsverfahren durchführen, um einen entsprechenden neuen Node an einem anderen Standort hinzuzufügen. Es muss sichergestellt sein, dass Clients eine Verbindung zum Ersatz-Node herstellen können, bevor der Standort ausmustern wird.
- Wenn der Standort, den Sie entfernen möchten, einen Gateway-Node oder Admin-Knoten enthält, die sich in einer HA-Gruppe befinden, können Sie die Schritte 1-4 des Assistenten zur Decommission Site ausführen. Sie können jedoch Schritt 5 des Assistenten nicht abschließen. Dieser startet den Ausmustern-Prozess, bis Sie diese Nodes aus allen HA-Gruppen entfernen. Wenn bestehende Clients mit einer HA-Gruppe verbunden sind, die die Nodes vom Standort enthält, müssen Sie sicherstellen, dass nach dem Entfernen des Standorts die Verbindung zu StorageGRID fortgesetzt werden kann.
- Wenn Clients direkt mit Storage Nodes an dem Standort verbunden sind, den Sie entfernen möchten, müssen Sie sicherstellen, dass sie eine Verbindung zu Storage Nodes an anderen Standorten herstellen können, bevor Sie den Vorgang zur Deaktivierung des Standorts starten.
- Sie müssen auf den übrigen Standorten ausreichend Speicherplatz für alle Objektdaten bereitstellen, die aufgrund von Änderungen an der aktiven ILM-Richtlinie verschoben werden. In einigen Fällen müssen Sie Ihr StorageGRID System möglicherweise um Storage Nodes, Storage Volumes oder neue Standorte erweitern, bevor Sie eine angeschlossene Website ausmustern.
- Sie müssen genügend Zeit haben, bis der Stilllegen abgeschlossen ist. Die ILM-Prozesse von StorageGRID dauern möglicherweise Tage, Wochen oder sogar Monate, um Objektdaten vom Standort zu verschieben oder zu löschen, bevor der Standort stillgelegt werden kann.



Das Verschieben oder Löschen von Objektdaten von einem Standort kann Tage, Wochen oder sogar Monate dauern, abhängig von der Datenmenge am Standort, der Systemlast, den Netzwerklatenzen und der Art der erforderlichen ILM-Änderungen.

- Wenn möglich, sollten Sie die Schritte 1-4 des Decommission Site-Assistenten so früh wie möglich abschließen. Die Deaktivierung erfolgt schneller und mit weniger Unterbrechungen und Leistungseinflüssen, wenn Sie zulassen, dass Daten von der Website verschoben werden, bevor Sie die tatsächliche Deaktivierung starten (indem Sie in Schritt 5 des Assistenten **Start Decommission** wählen).

Zusätzliche Anforderungen für die Deaktivierung eines getrennten Standorts

Bevor StorageGRID eine getrennte Site entfernen kann, müssen Sie Folgendes sicherstellen:

- Sie haben sich an Ihren NetApp Ansprechpartner wenden. NetApp überprüft Ihre Anforderungen, bevor Sie alle Schritte im Decommission Site Wizard aktivieren.



Sie sollten keinen Versuch Unternehmen, eine getrennte Site außer Betrieb zu nehmen, wenn Sie der Meinung sind, dass eine Wiederherstellung der Site oder die Wiederherstellung von Objektdaten von der Site möglich wäre.

- Alle Nodes am Standort müssen einen Verbindungsstatus von einer der folgenden aufweisen:
 - * Unbekannt* (): Der Knoten ist aus einem unbekannten Grund nicht mit dem Raster verbunden. Beispielsweise wurde die Netzwerkverbindung zwischen den Knoten unterbrochen oder der Strom ist ausgefallen.
 - **Administrativ Down** (): Der Knoten ist aus einem erwarteten Grund nicht mit dem Raster verbunden. Beispielsweise wurde der Node oder die Services auf dem Node ordnungsgemäß heruntergefahren.
- Alle Knoten an allen anderen Standorten müssen über einen Verbindungsstatus von **Connected** (); aber diese anderen Knoten können aktive Warnmeldungen haben.
- Sie müssen wissen, dass Sie mit StorageGRID keine Objektdaten mehr anzeigen oder abrufen können, die auf der Site gespeichert wurden. Wenn StorageGRID dieses Verfahren durchführt, wird nicht versucht, Daten vom getrennten Standort zu bewahren.



Wenn Ihre ILM-Regeln und -Richtlinien zum Schutz vor dem Verlust eines einzelnen Standorts ausgelegt wurden, sind noch Kopien der Objekte auf den übrigen Standorten vorhanden.

- Sie müssen verstehen, dass das Objekt verloren geht, wenn die Site die einzige Kopie eines Objekts enthielt und nicht abgerufen werden kann.

Überlegungen zu Konsistenzkontrollen beim Entfernen eines Standorts

Die Konsistenzstufe für einen S3-Bucket oder Swift-Container bestimmt, ob StorageGRID Objektmetadaten vollständig auf alle Nodes und Standorte repliziert, bevor einem Client mitgeteilt wird, dass die Objektaufnahme erfolgreich war. Konsistenzkontrollen bieten ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg.

Wenn StorageGRID einen Standort entfernt, muss es sicherstellen, dass keine Daten auf den entfernten Standort geschrieben werden. Daher wird das Konsistenzlevel vorübergehend für jeden Bucket oder Container überschrieben. Nach dem Starten der Website-Außerbetriebnahme verwendet StorageGRID vorübergehend eine hohe Standort-Konsistenz, um zu verhindern, dass Objekt-Metadaten auf die Website geschrieben werden.

Aufgrund dieser vorübergehenden Überschreibung ist es nicht bekannt, dass alle während der Außerbetriebnahme eines Standorts laufenden Client-Schreibvorgänge, Updates und Löschvorgänge fehlschlagen können, wenn auf den verbleibenden Standorten nicht mehr mehrere Nodes verfügbar sind.

Verwandte Informationen

[Durchführen der Standortwiederherstellung durch den technischen Support](#)

Sammeln Sie die erforderlichen Materialien

Bevor Sie eine Website ausmustern, sind die folgenden Unterlagen erforderlich.

Element	Hinweise
Wiederherstellungspaket .zip Datei	Sie müssen das neueste Wiederherstellungspaket herunterladen .zip Datei (sgws-recovery-package-id-revision.zip). Sie können die Recovery Package-Datei verwenden, um das System wiederherzustellen, wenn ein Fehler auftritt.
Passwords.txt Datei	Diese Datei enthält die Passwörter, die für den Zugriff auf Grid-Knoten in der Befehlszeile erforderlich sind und im Wiederherstellungspaket enthalten sind.
Provisioning-Passphrase	Die Passphrase wird erstellt und dokumentiert, wenn das StorageGRID-System zum ersten Mal installiert wird. Die Provisionierungs-Passphrase befindet sich nicht im Passwords.txt Datei:
Beschreibung der Topologie des StorageGRID Systems vor der Stilllegung	Falls verfügbar, finden Sie eine Dokumentation, die die aktuelle Topologie des Systems beschreibt.

Verwandte Informationen

[Anforderungen an einen Webbrowser](#)

[Laden Sie das Recovery Package herunter](#)

Schritt 1: Standort Auswählen

Um zu bestimmen, ob eine Site deaktiviert werden kann, öffnen Sie zunächst den Assistenten zur Deaktivierung der Site.

Was Sie benötigen

- Sie müssen alle erforderlichen Materialien erhalten haben.
- Sie müssen die Überlegungen zum Entfernen eines Standorts geprüft haben.
- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Stammzugriff oder die Wartungs- und ILM-Berechtigungen verfügen.

Schritte

1. Wählen Sie **WARTUNG Aufgaben Dekommission**.
2. Wählen Sie **Dekommission Site**.

Schritt 1 (Standort auswählen) des Assistenten für die Dekommission-Site wird angezeigt. Dieser Schritt

enthält eine alphabetische Liste der Sites in Ihrem StorageGRID-System.

Decommission Site

1

Select Site

2

View Details

3

Revise ILM Policy

4

Remove ILM References

5

Resolve Node Conflicts

6

Monitor Decommission

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
☐	Raleigh	3.93 MB	✓
☐	Sunnyvale	3.97 MB	✓
	Vancouver	3.90 MB	No. This site contains the primary Admin Node.

Next

3. Zeigen Sie die Werte in der Spalte **verwendete Storage-Kapazität** an, um festzustellen, wie viel Storage derzeit für Objektdaten an den einzelnen Standorten verwendet wird.

Die genutzte Storage-Kapazität ist eine Schätzung. Wenn Knoten offline sind, ist die verwendete Speicherkapazität der letzte bekannte Wert für den Standort.

- Um eine zusammenhängende Website außer Betrieb zu nehmen, gibt dieser Wert an, wie viele Objektdaten zu anderen Standorten verschoben oder durch ILM gelöscht werden müssen, bevor Sie diese Website zur sicheren Deaktivierung verwenden können.
- Im Falle einer Deaktivierung einer Website stellt dieser Wert dar, auf welchen Anteil der Datenspeicher Ihres Systems beim Deaktivierung dieser Website nicht mehr zugegriffen werden kann.



Falls Ihre ILM-Richtlinie zum Schutz vor dem Verlust eines einzelnen Standorts ausgelegt wurde, sollten weiterhin Kopien der Objektdaten auf den übrigen Standorten vorhanden sein.

4. Prüfen Sie die Gründe in der Spalte **Dekommission möglich**, um festzustellen, welche Standorte derzeit außer Betrieb genommen werden können.



Gibt es mehr als einen Grund, warum ein Standort nicht stillgelegt werden kann, wird der kritischste Grund angezeigt.

Möglichen Grund einer Deaktivierung	Beschreibung	Nächster Schritt
Grünes Häkchen (✓)	Sie können diese Website außer Betrieb nehmen.	Gehen Sie zu Im nächsten Schritt .
Nein Dieser Standort enthält den primären Admin-Knoten.	Sie können keine Site außer Betrieb nehmen, die den primären Admin-Node enthält.	Keine. Sie können dieses Verfahren nicht durchführen.
Nein Diese Site enthält mindestens einen Archiv-Knoten.	Sie können keine Site außer Betrieb setzen, die einen Archiv-Node enthält.	Keine. Sie können dieses Verfahren nicht durchführen.
Nein Alle Knoten an diesem Standort werden getrennt. Wenden Sie sich an Ihren NetApp Account-Ansprechpartner.	Sie können eine Deaktivierung einer verbundenen Site nur dann ausführen, wenn jeder Node auf der Site verbunden ist (✓).	Um eine getrennte Website außer Betrieb zu nehmen, müssen Sie sich an Ihren NetApp Ansprechpartner wenden. Dieser überprüft Ihre Anforderungen und aktiviert den Rest des Assistenten zur Decommission Site. WICHTIG: Nehmen Sie niemals Online-Knoten offline, so dass Sie eine Seite entfernen können. Sie verlieren Daten.

Das Beispiel zeigt ein StorageGRID System mit drei Standorten. Das grüne Häkchen (✓) Für die Raleigh und Sunnyvale Seiten bedeutet, dass Sie diese Websites außer Betrieb nehmen können. Sie können den Standort in Vancouver jedoch nicht stilllegen, da er den primären Admin-Node enthält.

1. Wenn eine Deaktivierung möglich ist, aktivieren Sie das Optionsfeld für die Website.

Die Schaltfläche **Weiter** ist aktiviert.

2. Wählen Sie **Weiter**.

Schritt 2 (Details anzeigen) wird angezeigt.

Schritt 2: Details Anzeigen

Ab Schritt 2 (Details anzeigen) des Assistenten für die Decommission-Site können Sie überprüfen, welche Knoten auf der Site enthalten sind, sehen, wie viel Speicherplatz auf den einzelnen Speicherknoten verwendet wurde, und bewerten, wie viel freier Speicherplatz auf den anderen Standorten in Ihrem Raster verfügbar ist.

Was Sie benötigen

Bevor Sie einen Standort außer Betrieb nehmen, müssen Sie überprüfen, wie viele Objektdaten am Standort vorhanden sind.

- Wenn Sie eine verbundene Website ausmustern, müssen Sie vor der Aktualisierung des ILM die derzeit vorhandene Objektdaten an der Website kennen. Basierend auf den Kapazitäten des Standorts und den Datensicherungsanforderungen können Sie neue ILM-Regeln erstellen, um Daten an andere Standorte zu verschieben oder Objektdaten vom Standort zu löschen.
- Führen Sie ggf. erforderliche Erweiterungen für Storage-Nodes durch, bevor Sie den Vorgang zur Deaktivierung nach Möglichkeit starten.
- Wenn Sie eine nicht verbundene Website deaktivieren, müssen Sie verstehen, wie viele Objektdaten dauerhaft zugänglich werden, wenn Sie die Website entfernen.

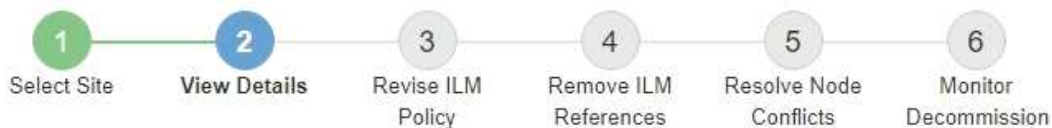


Wenn Sie eine getrennte Site außer Betrieb nehmen, kann ILM keine Objektdaten verschieben oder löschen. Alle Daten, die am Standort verbleiben, gehen verloren. Wenn Ihre ILM-Richtlinie jedoch zum Schutz vor dem Verlust eines einzelnen Standorts konzipiert wurde, sind Kopien der Objektdaten weiterhin auf den übrigen Standorten vorhanden.

Schritte

1. Überprüfen Sie ab Schritt 2 (Details anzeigen) alle Warnungen im Zusammenhang mit dem zu entfernenden Standort.

Decommission Site



Data Center 2 Details

⚠ This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

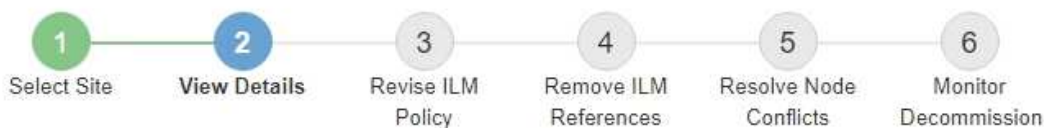
⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

In diesen Fällen wird eine Warnung angezeigt:

- Der Standort enthält einen Gateway-Node. Wenn S3- und Swift-Clients derzeit eine Verbindung zu diesem Node herstellen, müssen Sie an einem anderen Standort einen entsprechenden Node konfigurieren. Vergewissern Sie sich, dass Clients eine Verbindung zum Ersatz-Node herstellen können, bevor Sie die Deaktivierung durchführen.
- Der Standort enthält eine Mischung aus verbundenen (✅) Und nicht verbundene Knoten (🌙 Oder 🔄). Bevor Sie diesen Standort entfernen können, müssen Sie alle Offline-Nodes wieder in den Online-Modus versetzen.

2. Überprüfen Sie die Details der zu entfernenden Site.

Decommission Site



Raleigh Details

Number of Nodes: 3 Free Space: 475.38 GB
Used Space: 3.93 MB Site Capacity: 475.38 GB

Node Name	Node Type	Connection State	Details
RAL-S1-101-196	Storage Node	✓	1.30 MB used space
RAL-S2-101-197	Storage Node	✓	1.30 MB used space
RAL-S3-101-198	Storage Node	✓	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

[Previous](#)[Next](#)

Für den ausgewählten Standort sind folgende Informationen enthalten:

- Anzahl der Nodes
- Der insgesamt verwendete Speicherplatz, der freie Speicherplatz und die Kapazität aller Speicherknoten am Standort.
 - Für die Stilllegung einer verbundenen Site gibt der Wert **verwendeter Speicherplatz** an, wie viele Objektdaten auf andere Standorte verschoben oder mit ILM gelöscht werden müssen.
 - Bei einer nicht verbundenen Deaktivierung des Standorts gibt der Wert **verwendeter Speicherplatz** an, auf welche Objektdaten beim Entfernen der Website nicht mehr zugegriffen werden kann.
- Node-Namen, -Typen und -Verbindungsstatus:
 -  (Verbunden)
 -  (Administrativ Nach Unten)
 -  (Unbekannt)
- Details zu jedem Node:

- Für jeden Storage-Node die Menge an Speicherplatz, die für Objektdaten verwendet wurde.
- Gibt an, ob der Node derzeit in einer HA-Gruppe (Hochverfügbarkeit) verwendet wird, für Admin-Nodes und Gateway-Nodes. Sie können einen Admin-Node oder einen Gateway-Node, der in einer HA-Gruppe verwendet wird, nicht stilllegen. Bevor Sie die Ausmusterung beginnen, müssen Sie HA-Gruppen bearbeiten, um alle Nodes am Standort zu entfernen. Oder Sie können die HA-Gruppe entfernen, wenn sie nur Nodes von diesem Standort enthält.

StorageGRID verwalten

3. Bewerten Sie im Abschnitt Details für andere Standorte auf der Seite, wie viel Platz auf den anderen Standorten in Ihrem Raster verfügbar ist.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Wenn Sie eine verbundene Website ausmustern und mithilfe von ILM Objektdaten von der ausgewählten Site verschieben (statt sie zu löschen), müssen Sie sicherstellen, dass die anderen Standorte über genügend Kapazität für die verschobenen Daten verfügen und dass genügend Kapazität für zukünftiges Wachstum verfügbar ist.



Eine Warnung wird angezeigt, wenn der **verwendete Platz** für die zu entfernende Website größer als der **gesamte freie Speicherplatz für andere Standorte** ist. Bevor Sie diesen Vorgang durchführen, müssen Sie sicherstellen, dass nach dem Entfernen des Standorts ausreichend Speicherkapazität verfügbar ist.

4. Wählen Sie **Weiter**.

Schritt 3 (ILM-Richtlinie überarbeiten) wird angezeigt.

Verwandte Informationen

[Objektmanagement mit ILM](#)

Schritt 3: ILM-Richtlinie überarbeiten

Ab Schritt 3 (ILM-Richtlinie überarbeiten) des Assistenten für die Dekommission-Site können Sie feststellen, ob die Site von der aktiven ILM-Richtlinie angesprochen wird.

Was Sie benötigen

Sie wissen gut, wie ILM funktioniert und kennen die Erstellung von Storage-Pools, Erasure Coding-Profilen, ILM-Regeln und die Simulation und Aktivierung einer ILM-Richtlinie bereits.

[Objektmanagement mit ILM](#)

Über diese Aufgabe

StorageGRID kann einen Standort nicht stilllegen, wenn auf diesen Standort durch eine ILM-Regel in der aktiven ILM-Richtlinie verwiesen wird.

Wenn sich Ihre aktuelle ILM-Richtlinie auf die Site bezieht, die Sie entfernen möchten, müssen Sie eine neue ILM-Richtlinie aktivieren, die bestimmte Anforderungen erfüllt. Insbesondere die neue ILM-Richtlinie:

- Es kann kein Speicherpool verwendet werden, der sich auf den Standort bezieht.
- Ein Erasure-Coding-Profil, das sich auf den Standort bezieht, kann nicht verwendet werden.
- Der Standard * Alle Speicherknoten* oder der Standard **Alle Standorte**-Standort kann nicht verwendet werden.
- Kann den Bestand nicht verwenden **Regel 2 Kopien erstellen**.
- Muss auf einen vollständigen Schutz aller Objektdaten ausgelegt sein.



Erstellen Sie niemals eine ILM-Regel für eine einzelne Kopie, um die Entfernung eines Standorts aufzunehmen. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Wenn Sie eine „*connected Site*“-*Ausmusterung* durchführen, müssen Sie bedenken, wie StorageGRID die Objektdaten, die sich derzeit an der zu entfernenden Site befinden, verwalten sollte. Je nach Datensicherungsanforderungen können vorhandene Objektdaten nach den neuen Regeln auf verschiedene Standorte verschoben oder zusätzliche Objektkopien gelöscht werden, die nicht mehr benötigt werden.

Wenden Sie sich an den technischen Support, wenn Sie Hilfe beim Entwerfen der neuen Richtlinie benötigen.

Schritte

1. Stellen Sie ab Schritt 3 (ILM-Richtlinie überarbeiten) fest, ob ILM-Regeln der aktiven ILM-Richtlinie auf den Standort verweisen, den Sie entfernen möchten.
2. Wenn keine Regeln aufgeführt sind, wählen Sie **Weiter** aus, um zu Schritt 4 zu wechseln (ILM-Referenzen entfernen)

Schritt 4: Entfernen Sie ILM-Referenzen

3. Wenn eine oder mehrere ILM-Regeln in der Tabelle aufgeführt sind, wählen Sie den Link neben **Active Policy Name** aus.

Die Seite ILM-Richtlinien wird auf einer neuen Registerkarte „Browser“ angezeigt. Auf dieser Registerkarte können Sie ILM aktualisieren. Die Seite „Decommission Site“ bleibt auf der anderen Registerkarte geöffnet.

- a. Wählen Sie bei Bedarf **ILM Speicherpools** aus, um einen oder mehrere Speicherpools zu erstellen, die sich nicht auf den Standort beziehen.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- b. Wenn Sie Erasure Coding verwenden möchten, wählen Sie **ILM Erasure Coding** aus, um ein oder mehrere Erasure Coding-Profil zu erstellen.

Sie müssen Speicherpools auswählen, die sich nicht auf den Standort beziehen.



Verwenden Sie nicht den Speicherpool **All Storage Nodes** in den Erasure Coding-Profilen.

4. Wählen Sie **ILM Regeln** aus und klonen Sie jede der Regeln, die in der Tabelle für Schritt 3 aufgeführt sind (ILM-Richtlinie überarbeiten).



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- a. Verwenden Sie Namen, die die Auswahl dieser Regeln in einer neuen Richtlinie erleichtern.
- b. Aktualisieren Sie die Anweisungen für die Platzierung.

Entfernen Sie alle Storage-Pools oder Erasure Coding-Profile, die auf den Standort verweisen, und ersetzen Sie sie durch neue Speicherpools oder Erasure Coding-Profile.



Verwenden Sie den **Alle Speicherknoten** nicht in den neuen Regeln.

5. Wählen Sie **ILM Richtlinien** und erstellen Sie eine neue Richtlinie, die die neuen Regeln verwendet.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- a. Wählen Sie die aktive Richtlinie aus, und wählen Sie **Clone**.
- b. Geben Sie einen Richtliniennamen und einen Grund für die Änderung an.
- c. Wählen Sie Regeln für die geklonte Richtlinie aus.
 - Deaktivieren Sie alle Regeln, die für Schritt 3 (ILM-Richtlinie überarbeiten) auf der Seite „Dekommission Site“ aufgeführt sind.
 - Wählen Sie eine Standardregel aus, die sich nicht auf die Site bezieht.



Wählen Sie nicht die Regel **2 Kopien** aus, da diese Regel den **Alle Speicherknoten**-Speicherpool verwendet, der nicht erlaubt ist.

- Wählen Sie die anderen Ersatzregeln aus, die Sie erstellt haben. Diese Regeln sollten sich nicht auf die Website beziehen.

Select Rules for Policy

Select Default Rule

This list shows the rules that do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last. The default rule should retain objects forever.

Rule Name
☒ 2 copies at Sunnyvale and Vancouver for smaller objects
☐ 2 copy 2 sites for smaller objects
☐ Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

Rule Name	Tenant Account
☐ 3 copies for S3 tenant	S3 (61659555232085399385)
☐ EC for larger objects	—
☒ 1-site EC for larger objects	—
☒ 2 copies for S3 tenant	S3 (61659555232085399385)

Cancel

Apply

d. Wählen Sie **Anwenden**.

e. Ziehen Sie die Zeilen per Drag-and-Drop, um die Regeln in der Richtlinie neu anzuordnen.

Sie können die Standardregel nicht verschieben.



Sie müssen sich vergewissern, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen.

a. Speichern Sie die vorgeschlagene Richtlinie.

6. Nehmen Sie Testobjekte auf und simulieren Sie die vorgeschlagene Richtlinie, um sicherzustellen, dass die richtigen Regeln angewendet werden.



Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.



Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

7. Aktivieren Sie die neue Richtlinie.

Wenn Sie eine verbundene Website ausmustern, beginnt StorageGRID, Objektdaten von der ausgewählten Site zu entfernen, sobald Sie die neue ILM-Richtlinie aktivieren. Das Verschieben oder

Löschen aller Objektkopien kann Wochen in Anspruch nehmen. Sie können zwar eine Deaktivierung einer Website sicher starten, während noch Objektdaten am Standort vorhanden sind, aber die Deaktivierung erfolgt schneller und mit weniger Unterbrechungen und Performance-Beeinträchtigungen, wenn Daten vom Standort verschoben werden können, bevor Sie mit der tatsächlichen Außerbetriebnahme beginnen (Durch Auswahl von **Start Decommission** in Schritt 5 des Assistenten).

8. Zurück zu **Schritt 3 (ILM-Richtlinie überarbeiten)** um sicherzustellen, dass in der neuen aktiven Richtlinie keine ILM-Regeln auf der Site angegeben sind und die Schaltfläche **Weiter** aktiviert ist.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: [Data Protection for Two Sites](#) 

No ILM rules in the active ILM policy refer to Raleigh.

Previous

Next



Wenn Regeln aufgeführt sind, müssen Sie eine neue ILM-Richtlinie erstellen und aktivieren, bevor Sie fortfahren können.

9. Wenn keine Regeln aufgeführt sind, wählen Sie **Weiter**.

Schritt 4 (ILM-Referenzen entfernen) wird angezeigt.

Schritt 4: Entfernen Sie ILM-Referenzen

Ab Schritt 4 (Entfernen von ILM-Referenzen) des Decommission Site Wizard können Sie die vorgeschlagene Richtlinie entfernen, wenn diese vorhanden ist, und alle nicht verwendeten ILM-Regeln löschen oder bearbeiten, die sich noch auf die Site beziehen.

Über diese Aufgabe

In den folgenden Fällen können Sie den Ablauf zur Deaktivierung der Website nicht starten:

- Es gibt eine vorgeschlagene ILM-Richtlinie. Wenn Sie über eine vorgeschlagene Richtlinie verfügen, müssen Sie diese löschen.
- Jede ILM-Regel bezieht sich auf den Standort, selbst wenn diese Regel in keiner ILM-Richtlinie verwendet wird. Sie müssen alle Regeln, die sich auf die Website beziehen, löschen oder bearbeiten.

Schritte

1. Wenn eine vorgeschlagene Richtlinie aufgeführt ist, entfernen Sie sie.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

Proposed policy exists ^

You must delete the proposed policy before you can start the site decommission procedure.

Policy name: [Data Protection for Two Sites \(v2\)](#)  [Delete Proposed Policy](#)

4 ILM rules refer to Raleigh v

1 **Erasure Coding profile** will be deactivated v

3 **storage pools** will be deleted v

[Previous](#)[Next](#)

- a. Wählen Sie **Vorgeschlagene Richtlinie Löschen**.
 - b. Wählen Sie im Bestätigungsdiaologfeld * OK* aus.
2. Stellen Sie fest, ob sich ungenutzte ILM-Regeln auf den Standort beziehen.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

4 ILM rules refer to Data Center 3

This table lists the unused ILM rules that still refer to the site. For each rule listed, you must do one of the following:

- Edit the rule to remove the Erasure Coding profile or storage pool from the placement instructions.
- Delete the rule.

[Go to the ILM Rules page](#)

Name	EC Profiles	Storage Pools	Delete
Make 2 Copies	—	All Storage Nodes	
3 copies for S3 tenant	—	Raleigh storage pool	
2 copies 2 sites for smaller objects	—	Raleigh storage pool	
EC larger objects	three site EC profile	All 3 Sites	

1 Erasure Coding profile will be deactivated

3 storage pools will be deleted

ILM-Regeln, die aufgeführt sind, beziehen sich immer noch auf die Site, werden aber in keinen Richtlinien verwendet. Im Beispiel:

- Die Stock **make 2 Kopien** Regel verwendet den Systemstandard **Alle Speicherknoten** Speicherpool, der die Site Alle Sites verwendet.
- Die ungenutzte **3 Kopien für S3-Mandanten**-Regel bezieht sich auf den **Raleigh**-Speicherpool.
- Die ungenutzte **2 Copy 2-Seiten für kleinere Objekte**-Regel bezieht sich auf den **Raleigh**-Speicherpool.
- Die ungenutzten **EC-Regeln für größere Objekte** verwenden die Raleigh-Site im Profil **Alle 3 Sites** Erasure Coding.
- Wenn keine ILM-Regeln aufgeführt sind, wählen Sie **Weiter** aus, um zu **Schritt 5 (Node-Konflikte auflösen)** zu wechseln.

[Schritt 5: Auflösen von Knotenkonflikten \(und Start der Stilllegung\)](#)



Wenn StorageGRID den Standort dekomprimiert, werden automatisch alle nicht verwendeten Erasure Coding-Profil deaktiviert, die auf den Standort verweisen. Außerdem werden alle nicht verwendeten Speicherpools, die sich auf den Standort beziehen, automatisch gelöscht. Der standardmäßige Speicherpool Alle Speicherknoten wird entfernt, da er den Standort Alle Standorte verwendet.

- Wenn eine oder mehrere ILM-Regeln aufgeführt sind, fahren Sie mit dem nächsten Schritt fort.

3. Bearbeiten oder Löschen jeder nicht verwendeten Regel:

- Um eine Regel zu bearbeiten, gehen Sie auf der Seite ILM-Regeln und aktualisieren Sie alle Platzierungen, die ein Erasure Coding-Profil oder einen Speicherpool verwenden, der sich auf den Standort bezieht. Kehren Sie dann zu **Schritt 4 (ILM-Referenzen entfernen)** zurück.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

- Um eine Regel zu löschen, wählen Sie das Papierkorb-Symbol aus Und wählen Sie **OK**.



Sie müssen die Regel für Lagerbestand **Erstellen von 2 Kopien** löschen, bevor Sie eine Website stilllegen können.

4. Vergewissern Sie sich, dass keine vorgeschlagene ILM-Richtlinie vorhanden ist, keine ungenutzten ILM-Regeln auf die Site verweisen und die Schaltfläche **Weiter** ist aktiviert.

Decommission Site



Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

No ILM rules refer to Raleigh

1 Erasure Coding profile will be deactivated



3 storage pools will be deleted



Previous

Next

5. Wählen Sie **Weiter**.



Alle verbleibenden Speicherpools und Erasure Coding-Profile, die sich auf den Standort beziehen, werden ungültig, wenn der Standort entfernt wird. Wenn StorageGRID den Standort dekomprimiert, werden automatisch alle nicht verwendeten Erasure Coding-Profile deaktiviert, die auf den Standort verweisen. Außerdem werden alle nicht verwendeten Speicherpools, die sich auf den Standort beziehen, automatisch gelöscht. Der standardmäßige Speicherpool Alle Speicherknoten wird entfernt, da er den Standort Alle Standorte verwendet.

Schritt 5 (Auflösen von Knotenkonflikten) wird angezeigt.

Schritt 5: Auflösen von Knotenkonflikten (und Start der Stilllegung)

Ab Schritt 5 (Auflösen von Knotenkonflikten) des Assistenten für die Dekommission-Website können Sie feststellen, ob Knoten in Ihrem StorageGRID-System getrennt sind oder ob Knoten am ausgewählten Standort zu einer HA-Gruppe gehören. Nachdem Konflikte mit Knoten behoben wurden, starten Sie den Vorgang zur Deaktivierung auf dieser Seite.

Sie müssen sicherstellen, dass alle Nodes in Ihrem StorageGRID System den richtigen Status aufweisen, wie folgt:

- Alle Knoten im StorageGRID-System müssen verbunden sein (✓).



Wenn Sie eine getrennte Site außer Betrieb nehmen, müssen alle Nodes an der entfernenden Site getrennt sein. Alle Nodes an allen anderen Standorten müssen verbunden sein.

- Kein Node an dem gerade entfernenden Standort kann eine Schnittstelle besitzen, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehört.

Wenn ein Knoten für Schritt 5 (Auflösen von Knotenkonflikten) aufgeführt ist, müssen Sie das Problem beheben, bevor Sie den Stilllegen starten können.

Prüfen Sie vor dem Starten des Verfahrens zur Deaktivierung der Website auf dieser Seite die folgenden Aspekte:

- Sie müssen genügend Zeit haben, bis der Stilllegen abgeschlossen ist.



Das Verschieben oder Löschen von Objektdaten von einem Standort kann Tage, Wochen oder sogar Monate dauern, abhängig von der Datenmenge am Standort, der Systemlast, den Netzwerklatenzen und der Art der erforderlichen ILM-Änderungen.

- Während die Deaktivierung der Website läuft:
 - Sie können keine ILM-Regeln erstellen, die sich auf die auszugemusterte Site beziehen. Sie können auch keine vorhandene ILM-Regel bearbeiten, um auf die Site zu verweisen.
 - Sie können keine anderen Wartungsvorgänge wie z. B. Erweiterung oder Upgrade durchführen.



Wenn Sie während der Stilllegung einer verbundenen Site einen weiteren Wartungsvorgang durchführen müssen, können Sie den Vorgang unterbrechen, während die Storage-Nodes entfernt werden. Die Schaltfläche **Pause** ist während der Phase „DEcommissioning Replicated and Erasure coded Data“ aktiviert.

- Falls Nodes nach dem Starten der Deaktivierung der Website wiederhergestellt werden müssen, müssen Sie den Support kontaktieren.

Schritte

1. Überprüfen Sie den Abschnitt „nicht verbundene Knoten“ von Schritt 5 (Auflösen von Knotenkonflikten), um festzustellen, ob Knoten in Ihrem StorageGRID-System einen Verbindungsstatus von Unbekannt () Oder Administrativ Down ().

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193 	 Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group

Passphrase

Provisioning Passphrase 

Previous

Start Decommission

2. Wenn Knoten getrennt werden, bringen Sie sie wieder in den Online-Modus.

Anweisungen zum Monitoring und zur Fehlerbehebung für StorageGRID und die Verfahren für den Grid-Node finden Sie in den Anweisungen. Wenden Sie sich an den technischen Support, wenn Sie Hilfe

benötigen.

3. Wenn alle getrennten Nodes wieder in den Online-Modus versetzt wurden, überprüfen Sie den Abschnitt HA-Gruppen in Schritt 5 (Auflösen von Node-Konflikten).

In dieser Tabelle werden alle Nodes am ausgewählten Standort aufgelistet, die zu einer HA-Gruppe (High Availability, Hochverfügbarkeit) gehören.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

1 node in the selected site belongs to an HA group

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#)

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase ?

Previous

Start Decommission

4. Wenn alle Knoten aufgelistet sind, führen Sie einen der folgenden Schritte aus:

- Bearbeiten Sie jede betroffene HA-Gruppe, um die Node-Schnittstelle zu entfernen.
- Entfernen Sie eine HA-Gruppe, die nur Nodes aus diesem Standort enthält. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Wenn alle Nodes verbunden sind und keine Nodes am ausgewählten Standort in einer HA-Gruppe verwendet werden, ist das Feld **Provisioning-Passphrase** aktiviert.

5. Geben Sie die Provisionierungs-Passphrase ein.

Die Schaltfläche **Start Decommission** wird aktiviert.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase ?

.....

Previous

Start Decommission

6. Wenn Sie bereit sind, den Vorgang zur Deaktivierung der Website zu starten, wählen Sie **Start Decommission**.

Eine Warnung zeigt den Standort und die Knoten, die entfernt werden. Sie werden daran erinnert, dass es Tage, Wochen oder sogar Monate dauern kann, die Website vollständig zu entfernen.

Warning

The following site and its nodes have been selected for decommissioning and will be permanently removed from the StorageGRID system:

Data Center 3

- DC3-S1
- DC3-S2
- DC3-S3

When StorageGRID removes a site, it temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed. Client write and delete operations can fail if multiple nodes become unavailable at the remaining sites.

This procedure might take days, weeks, or even months to complete. Select **Maintenance > Decommission** to monitor the decommission progress.

Do you want to continue?

Cancel

OK

7. Überprüfen Sie die Warnung. Wenn Sie bereit sind, zu beginnen, wählen Sie **OK**.

Beim Generieren der neuen Grid-Konfiguration wird eine Meldung angezeigt. Dieser Prozess kann je nach Typ und Anzahl der nicht mehr verwendeten Grid-Nodes einige Zeit in Anspruch nehmen.

Passphrase

Provisioning Passphrase 

 Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission 

Wenn die neue Grid-Konfiguration generiert wurde, wird Schritt 6 (Monitor Decommission) angezeigt.



Die Schaltfläche * Previous* bleibt deaktiviert, bis die Stilllegung abgeschlossen ist.

Verwandte Informationen

[Monitoring und Fehlerbehebung](#)

[Verfahren für den Grid-Node](#)

[StorageGRID verwalten](#)

Schritt 6: Überwachung Der Dekommission

Ab Schritt 6 (Überwachung der Dekommission) des Seitenassistenten der Decommission-Website können Sie den Fortschritt überwachen, während die Site entfernt wird.

Über diese Aufgabe

Wenn StorageGRID einen verbundenen Standort entfernt, werden Nodes in dieser Reihenfolge entfernt:

1. Gateway-Nodes
2. Admin-Nodes
3. Storage-Nodes

Wenn StorageGRID einen getrennten Standort entfernt, werden Nodes in dieser Reihenfolge entfernt:

1. Gateway-Nodes
2. Storage-Nodes
3. Admin-Nodes

Jeder Gateway-Node oder Admin-Node kann möglicherweise nur ein paar Minuten oder eine Stunde entfernt werden. Storage-Nodes können jedoch Tage oder Wochen in Anspruch nehmen.

Schritte

1. Sobald ein neues Wiederherstellungspaket erstellt wurde, laden Sie die Datei herunter.

Decommission Site



i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.



Laden Sie das Wiederherstellungspaket so schnell wie möglich herunter, um sicherzustellen, dass Sie Ihr Grid wiederherstellen können, wenn während des Stillfalls etwas schief geht.

- a. Wählen Sie den Link in der Nachricht, oder wählen Sie **WARTUNG System Wiederherstellungspaket**.
- b. Laden Sie die herunter .zip Datei:

Siehe Anweisungen für [Herunterladen des Wiederherstellungspakets](#).

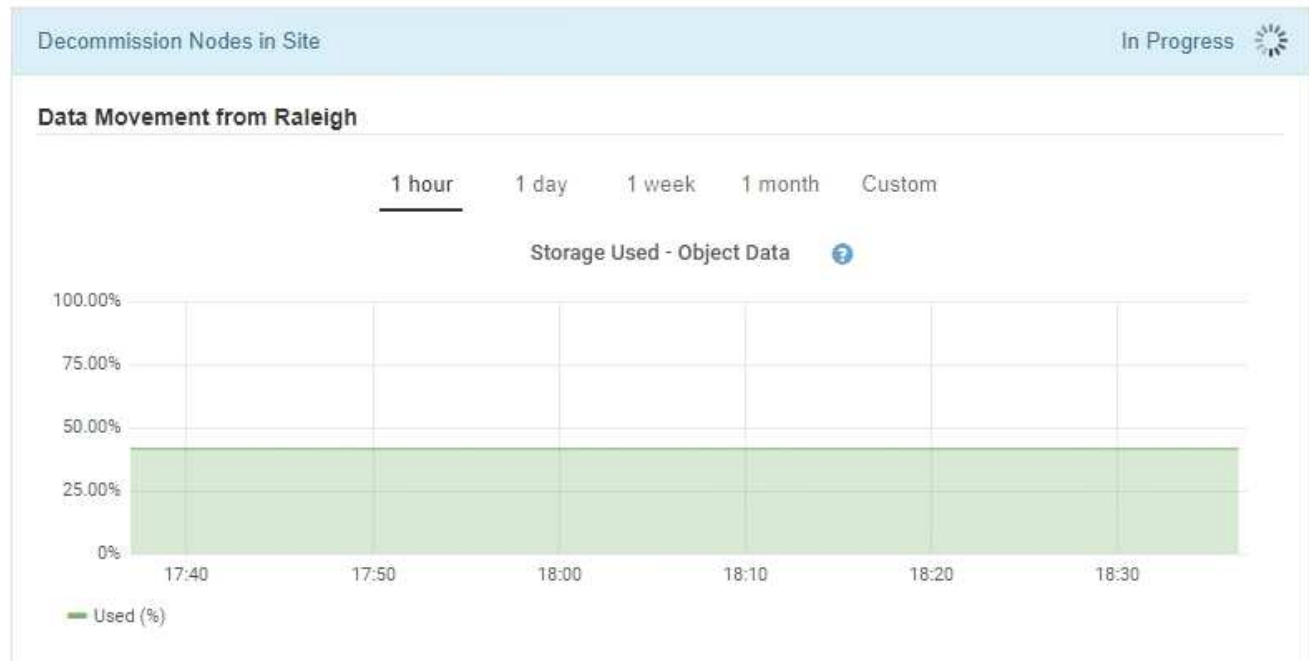


Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

- Überwachen Sie mithilfe des Diagramms für die Datenverschiebung das Verschieben von Objektdaten von dieser Seite zu anderen Standorten.

Datenverschiebung gestartet, als Sie die neue ILM-Richtlinie in Schritt 3 aktiviert haben (ILM-Richtlinie überarbeiten). Die Datenverschiebung findet während der gesamten Außerbetriebnahme statt.

Decommission Site Progress



- Überwachen Sie im Abschnitt Status des Knotens der Seite den Fortschritt des Stillstandsvorgangs, wenn Nodes entfernt werden.

Wenn ein Speicherknoten entfernt wird, durchläuft jeder Knoten eine Reihe von Phasen. Obwohl die meisten dieser Phasen schnell oder sogar unmerklich auftreten, müssen Sie möglicherweise Tage oder sogar Wochen warten, bis andere Phasen abgeschlossen sind, je nachdem, wie viele Daten verschoben werden müssen. Zur Verwaltung von Daten, die mit Erasure Coding versehen sind, und zur Neubewertung von ILM-Verfahren ist zusätzlicher Zeit erforderlich.

Node Progress

i Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).

Pause

Resume

Search				
Name	Type	Progress	Stage	
RAL-S1-101-196	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S2-101-197	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S3-101-198	Storage Node		Decommissioning Replicated and Erasure Coded Data	

Wenn Sie den Fortschritt der Deaktivierung einer verbundenen Site überwachen, lesen Sie diese Tabelle, um die Phasen zur Ausmusterung eines Storage Node zu verstehen:

Stufe	Geschätzte Dauer
Ausstehend	Minuten oder weniger
Warten Sie auf Sperren	Minuten
Aufgabe Vorbereiten	Minuten oder weniger
Markieren von LDR deaktiviert	Minuten
Stilllegung replizierter und Erasure Coding von Daten	Stunden, Tage oder Wochen, basierend auf der Datenmenge Hinweis: Wenn Sie weitere Wartungsarbeiten durchführen müssen, können Sie die Deaktivierung der Website während dieser Phase unterbrechen.
LDR-Status gesetzt	Minuten
Audit-Warteschlangen Leeren	Minuten bis Stunden, basierend auf der Anzahl der Nachrichten und der Netzwerklatenz.
Vollständig	Minuten

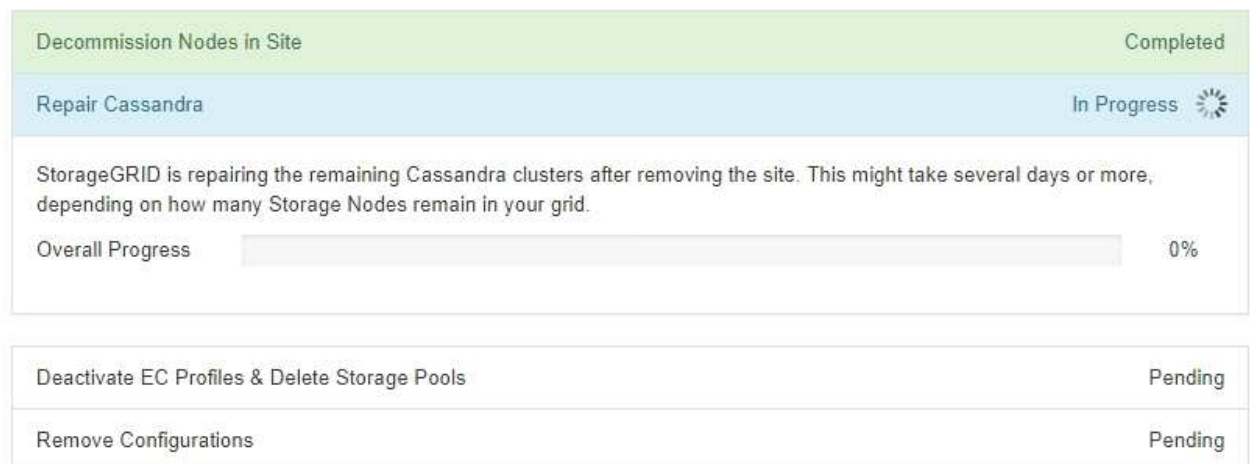
Wenn Sie den Fortschritt der Deaktivierung einer getrennten Site überwachen, lesen Sie diese Tabelle, um

weitere Informationen zur Ausmusterung von Storage Nodes zu erhalten:

Stufe	Geschätzte Dauer
Ausstehend	Minuten oder weniger
Warten Sie auf Sperren	Minuten
Aufgabe Vorbereiten	Minuten oder weniger
Externe Dienste Deaktivieren	Minuten
Widerruf Des Zertifikats	Minuten
Knoten Nicht Registrieren	Minuten
Storage-Klasse Nicht Registrieren	Minuten
Entfernung Von Speichergruppen	Minuten
Entfernen Der Einheit	Minuten
Vollständig	Minuten

4. Sobald alle Nodes abgeschlossen sind, warten Sie, bis der restliche Standort außer Betrieb ist.
- Im Schritt **Cassandra reparieren** führt StorageGRID alle erforderlichen Reparaturen an den Cassandra-Clustern durch, die in Ihrem Grid verbleiben. Je nachdem, wie viele Speicherknoten im Raster verbleiben, kann diese Reparaturen mehrere Tage oder länger dauern.

Decommission Site Progress



- Während des Schritts **EC-Profil löschen Speicherpools** werden folgende ILM-Änderungen vorgenommen:
 - Alle auf den Standort verwiesenen Erasure Coding-Profiles werden deaktiviert.

- Alle Speicherpools, die auf den Standort verwiesen werden gelöscht.



Der systemstandardmäßige Speicherpool „Alle Speicherknoten“ wird ebenfalls entfernt, da er den Standort „Alle Standorte“ verwendet.

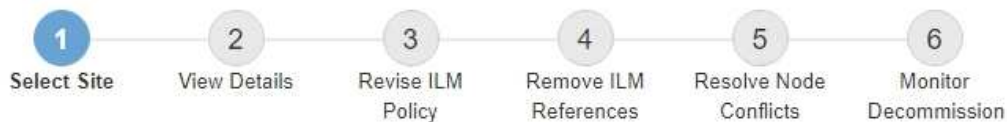
- Schließlich werden im Schritt **Konfiguration entfernen** alle verbleibenden Verweise auf die Site und ihre Knoten aus dem Rest des Rasters entfernt.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress
StorageGRID is removing the site and node configurations from the rest of the grid.	

5. Nach Abschluss des Stilllegen-Verfahrens wird auf der Seite Decommission Site eine Meldung angezeigt, die den entfernten Standort nicht mehr anzeigt.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity	Decommission Possible
☐	Sunnyvale	4.79 MB	
☐	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Nachdem Sie fertig sind

Führen Sie diese Aufgaben nach Abschluss des Verfahrens zur Deaktivierung der Website durch:

- Stellen Sie sicher, dass die Laufwerke aller Storage-Nodes am ausgemusterten Standort sauber gelöscht werden. Verwenden Sie ein handelsübliches Datenwischwerkzeug oder einen Dienst, um die Daten dauerhaft und sicher von den Laufwerken zu entfernen.
- Wenn die Site einen oder mehrere Admin-Nodes enthält und Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, entfernen Sie alle Vertrauensstellen für die Site aus Active Directory Federation Services (AD FS).
- Nachdem die Knoten im Rahmen der Deaktivierung des angeschlossenen Standorts automatisch ausgeschaltet wurden, entfernen Sie die zugehörigen virtuellen Maschinen.

Netzwerkwartungsverfahren

Subnetze für Grid Network aktualisieren

StorageGRID pflegt eine Liste der für die Kommunikation zwischen den Grid-Nodes im Grid-Netzwerk (eth0) verwendeten Subnetze. Zu diesen Einträgen gehören die Subnetze, die von jedem Standort im StorageGRID-System für das Grid-Netzwerk verwendet werden, sowie alle Subnetze, die für NTP, DNS, LDAP oder andere externe Server verwendet werden, auf die über das Grid-Netzwerk-Gateway zugegriffen wird. Wenn Sie Grid-Nodes oder einen neuen Standort in einer Erweiterung hinzufügen, müssen Sie möglicherweise Subnetze zum Grid-Netzwerk aktualisieren oder hinzufügen.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen die Netzwerkadressen in CIDR-Notation der Subnetze haben, die Sie konfigurieren möchten.

Über diese Aufgabe

Wenn Sie eine Erweiterungsaktivität durchführen, die das Hinzufügen eines neuen Subnetzes beinhaltet, müssen Sie das neue Grid-Subnetz hinzufügen, bevor Sie den Erweiterungsvorgang starten.

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > Grid-Netzwerk**.

Grid Network

Configure the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network (eth0) for each site in your StorageGRID system as well as any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnets

Subnet 1



Passphrase

Provisioning
Passphrase

Save

2. Klicken Sie in der Liste Subnetze auf das Pluszeichen, um ein neues Subnetz in CIDR-Notation hinzuzufügen.

Geben Sie beispielsweise ein 10.96.104.0/22.

3. Geben Sie die Provisionierungs-Passphrase ein, und klicken Sie auf **Speichern**.

Die angegebenen Subnetze werden automatisch für Ihr StorageGRID System konfiguriert.

4. Laden Sie ein neues Wiederherstellungspaket aus dem Grid Manager herunter.
 - a. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
 - b. Geben Sie die Provisionierungs-Passphrase ein.

Konfigurieren Sie IP-Adressen

Sie können eine Netzwerkkonfiguration durchführen, indem Sie IP-Adressen für Grid-Nodes mithilfe des Tools IP ändern konfigurieren.

Sie müssen das Change IP-Tool verwenden, um die meisten Änderungen an der Netzwerkkonfiguration vorzunehmen, die ursprünglich während der Grid-Implementierung festgelegt wurde. Manuelle Änderungen unter Verwendung von standardmäßigen Linux-Netzwerkbefehlen und Dateien werden möglicherweise nicht an allen StorageGRID-Diensten weitergegeben. Dabei bleiben Upgrades, Neustarts oder Recovery-Verfahren für Knoten nicht erhalten.



Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Raster ändern möchten, verwenden Sie den [Sondervorgang für netzweite Änderungen](#).



Wenn Sie nur Änderungen an der Netznetzwerksubnetz-Liste vornehmen, verwenden Sie den Grid-Manager, um die Netzwerkkonfiguration hinzuzufügen oder zu ändern. Verwenden Sie andernfalls das Change IP-Tool, wenn der Grid Manager aufgrund eines Netzwerkkonfigurationsproblem nicht erreichbar ist, oder Sie führen gleichzeitig eine Änderung des Grid Network Routing und andere Netzwerkänderungen durch.



Das IP-Änderungsverfahren kann eine Unterbrechungsmaßnahme sein. Teile des Rasters sind möglicherweise erst verfügbar, wenn die neue Konfiguration angewendet wird.

- Ethernet-Schnittstellen*

Die eth0 zugewiesene IP-Adresse ist immer die Grid-Netzwerk-IP-Adresse des Grid-Node. Die eth1 zugewiesene IP-Adresse ist immer die Admin-Netzwerk-IP-Adresse des Grid-Node. Die eth2 zugewiesene IP-Adresse ist immer die Client-Netzwerk-IP-Adresse des Grid-Node.

Beachten Sie, dass auf einigen Plattformen, z. B. StorageGRID Appliances, eth0, eth1 und eth2, aggregierte Schnittstellen bestehen, die aus untergeordneten Bridges oder Bindungen von physischen oder VLAN-Schnittstellen bestehen. Auf diesen Plattformen wird auf der Registerkarte **SSM Ressourcen** die Grid-, Admin- und Client-Netzwerk-IP-Adresse angezeigt, die anderen Schnittstellen zusätzlich zu eth0, eth1 oder eth2 zugewiesen ist.

DHCP

Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten. Sie müssen die Änderungsverfahren für die IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Wenn Sie das Tool IP ändern verwenden, werden DHCP-Adressen statisch.

Hochverfügbarkeitsgruppen

- Wenn eine Client-Netzwerkschnittstelle in einer HA-Gruppe enthalten ist, können Sie die Client-Netzwerk-IP-Adresse für diese Schnittstelle nicht in eine Adresse ändern, die sich außerhalb des für die HA-Gruppe konfigurierten Subnetzes befindet.
- Sie können die Client-Netzwerk-IP-Adresse nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die einer HA-Gruppe zugewiesen ist, die in der Client-Netzwerkschnittstelle konfiguriert ist.
- Wenn eine Grid-Netzwerkschnittstelle in einer HA-Gruppe enthalten ist, können Sie die Grid-Netzwerk-IP-Adresse für diese Schnittstelle nicht in eine Adresse ändern, die sich außerhalb des für die HA-Gruppe konfigurierten Subnetzes befindet.
- Sie können die Grid-Netzwerk-IP-Adresse nicht in den Wert einer vorhandenen virtuellen IP-Adresse ändern, die einer auf der Grid-Netzwerkschnittstelle konfigurierten HA-Gruppe zugewiesen ist.

Ändern der Node-Netzwerkkonfiguration

Mit dem Change IP-Tool können Sie die Netzwerkkonfiguration für einen oder mehrere Knoten ändern. Sie können die Konfiguration des Grid-Netzwerks ändern oder den Administrator- oder Client-Netzwerk hinzufügen, ändern oder entfernen.

Was Sie benötigen

Sie müssen die `Passwords.txt` Datei:

Über diese Aufgabe

Linux: Wenn Sie zum ersten Mal einen Grid-Knoten zum Admin-Netzwerk oder Client-Netzwerk hinzufügen und SIE IN der Node-Konfigurationsdatei NOCH nicht `ADMIN_NETWORK_TARGET` oder `CLIENT_NETWORK_TARGET` konfiguriert haben, müssen Sie dies jetzt tun.

Weitere Informationen finden Sie in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

Appliances: bei StorageGRID-Geräten, wenn das Client- oder Admin-Netzwerk während der Erstinstallation

nicht im StorageGRID Appliance Installer konfiguriert wurde, kann das Netzwerk nicht mit dem Change IP-Tool hinzugefügt werden. Zunächst müssen Sie [Stellen Sie das Gerät in den Wartungsmodus](#), Konfigurieren Sie die Links, stellen Sie die Appliance in den normalen Betriebsmodus zurück, und verwenden Sie dann das Change IP-Tool, um die Netzwerkkonfiguration zu ändern. Informationen zum Konfigurieren von Netzwerkverbindungen finden Sie in der Installations- und Wartungsanleitung für Ihre Appliance.

Sie können die IP-Adresse, die Subnetzmaske, das Gateway oder den MTU-Wert für einen oder mehrere Knoten in einem Netzwerk ändern.

Sie können auch einen Knoten aus einem Client-Netzwerk oder aus einem Admin-Netzwerk hinzufügen oder entfernen:

- Sie können einem Client-Netzwerk oder einem Admin-Netzwerk einen Knoten hinzufügen, indem Sie dem Knoten eine IP-Adresse/Subnetzmaske hinzufügen.
- Sie können einen Knoten aus einem Client-Netzwerk oder aus einem Admin-Netzwerk entfernen, indem Sie die IP-Adresse/Subnetzmaske für den Knoten in diesem Netzwerk löschen.

Knoten können nicht aus dem Grid-Netzwerk entfernt werden.



IP-Adressenschwalben sind nicht zulässig. Wenn Sie IP-Adressen zwischen Grid-Nodes austauschen müssen, müssen Sie eine temporäre IP-Adresse verwenden.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist und Sie die IP-Adresse eines Admin-Knotens ändern, ist zu beachten, dass jedes Vertrauen, das mit der IP-Adresse des Admin-Knotens konfiguriert wurde (anstelle des vollständig qualifizierten Domännennamens, wie empfohlen), ungültig wird. Sie können sich nicht mehr bei dem Node anmelden. Unmittelbar nach dem Ändern der IP-Adresse müssen Sie das Vertrauen des Knotens in Active Directory Federation Services (AD FS) mit der neuen IP-Adresse aktualisieren oder neu konfigurieren. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.



Alle Änderungen, die Sie mit dem Change IP-Tool an das Netzwerk vornehmen, werden an die Installer-Firmware für die StorageGRID-Appliances übertragen. Auf diese Weise wird bei einer erneuten Installation der StorageGRID Software auf einer Appliance oder beim Einsatz einer Appliance in den Wartungsmodus die Netzwerkkonfiguration korrekt ausgeführt.

Schritte

1. Melden Sie sich beim primären Admin-Node an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
- 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 #.

2. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`

3. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase ein.

Das Hauptmenü wird angezeigt.


```

Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █

```

4. Wählen Sie optional **1** aus, um die zu aktualisierenden Knoten auszuwählen. Wählen Sie dann eine der folgenden Optionen aus:

- **1:** Einzelner Knoten — nach Namen auswählen
- **2:** Single Node — Wählen Sie nach Standort, dann nach Name
- **3:** Single Node — Wählen Sie nach aktueller IP
- **4:** Alle Knoten an einem Standort
- **5:** Alle Knoten im Raster

Hinweis: Wenn Sie alle Knoten aktualisieren möchten, lassen Sie "alle" ausgewählt bleiben.

Nachdem Sie Ihre Auswahl getroffen haben, wird das Hauptmenü angezeigt, wobei das Feld **Ausgewählte Knoten** aktualisiert wird, um Ihre Auswahl zu berücksichtigen. Alle nachfolgenden Aktionen werden nur auf den angezeigten Nodes ausgeführt.

5. Wählen Sie im Hauptmenü die Option **2**, um IP/Maske, Gateway und MTU-Informationen für die ausgewählten Knoten zu bearbeiten.

a. Wählen Sie das Netzwerk aus, in dem Sie Änderungen vornehmen möchten:

- **1:** Netznetz
- **2:** Admin-Netzwerk
- **3:** Client-Netzwerk
- **4:** Alle Netzwerke nach der Auswahl zeigt die Eingabeaufforderung den Knotennamen, den Netzwerknamen (Grid, Admin oder Client), den Datentyp (IP/Maske, Gateway oder MTU) und aktueller Wert.

Wenn Sie die IP-Adresse, die Präfixlänge, das Gateway oder die MTU einer DHCP-konfigurierten Schnittstelle bearbeiten, wird die Schnittstelle zu statisch geändert. Wenn Sie eine durch DHCP konfigurierte Schnittstelle ändern möchten, wird eine Warnung angezeigt, die Sie darüber informiert, dass sich die Schnittstelle in statisch ändert.

Als konfigurierte Schnittstellen `fixed` Kann nicht bearbeitet werden.

- b. Um einen neuen Wert festzulegen, geben Sie ihn in das für den aktuellen Wert angezeigte Format ein.
- c. Um den aktuellen Wert unverändert zu lassen, drücken Sie **Enter**.
- d. Wenn der Datentyp ist `IP/mask`, Sie können das Admin- oder Client-Netzwerk vom Knoten löschen,

indem Sie **d** oder **0.0.0.0/0** eingeben.

- e. Nachdem Sie alle Knoten bearbeitet haben, die Sie ändern möchten, geben Sie **q** ein, um zum Hauptmenü zurückzukehren.

Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.

6. Überprüfen Sie Ihre Änderungen, indem Sie eine der folgenden Optionen auswählen:

- **5:** Zeigt Edits in der Ausgabe an, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe dargestellt:
- **6:** Zeigt Änderungen in der Ausgabe an, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert.



Bestimmte Befehlszeilenschnittstellen zeigen möglicherweise Ergänzungen und Löschungen mithilfe von durchgestrichter Formatierung. Die richtige Anzeige hängt von Ihrem Terminalclient ab, der die erforderlichen VT100-Escape-Sequenzen unterstützt.

7. Wählen Sie Option **7**, um alle Änderungen zu validieren.

Durch diese Validierung wird sichergestellt, dass die Regeln für Grid-, Admin- und Client-Netzwerke, z. B. die Verwendung überlappender Subnetze, nicht verletzt werden.

In diesem Beispiel ergab die Validierung Fehler.

In diesem Beispiel wurde die Validierung erfolgreich bestanden.

8. Wenn die Validierung erfolgreich abgeschlossen ist, wählen Sie eine der folgenden Optionen:

- **8:** Speichern Sie nicht angewendete Änderungen.

Mit dieser Option können Sie das Tool IP ändern beenden und es später erneut starten, ohne dabei unangewendete Änderungen zu verlieren.

- **10:** Die neue Netzwerkkonfiguration anwenden.

9. Wenn Sie die Option **10** ausgewählt haben, wählen Sie eine der folgenden Optionen:

- **Apply:** Die Änderungen sofort anwenden und bei Bedarf automatisch jeden Knoten neu starten.

Wenn für die neue Netzwerkkonfiguration keine Änderungen am physischen Netzwerk erforderlich sind, können Sie **Apply** auswählen, um die Änderungen sofort anzuwenden. Nodes werden bei Bedarf automatisch neu gestartet. Knoten, die neu gestartet werden müssen, werden angezeigt.

- **Stufe:** Beim nächsten manuellen Neustart der Knoten die Änderungen anwenden.

Wenn Sie Änderungen an der physischen oder virtuellen Netzwerkkonfiguration vornehmen müssen, damit die neue Netzwerkkonfiguration funktioniert, müssen Sie die Option **Stage** verwenden, die betroffenen Knoten herunterfahren, die erforderlichen Änderungen am physischen Netzwerk vornehmen und die betroffenen Knoten neu starten. Wenn Sie **Apply** wählen, ohne zuvor diese Netzwerkänderungen vornehmen zu müssen, schlagen die Änderungen normalerweise fehl.



Wenn Sie die Option **Stage** verwenden, müssen Sie den Knoten nach der Staging so schnell wie möglich neu starten, um Störungen zu minimieren.

- **Abbrechen:** Nehmen Sie keine Netzwerkänderungen vor.

Wenn Sie nicht wissen, dass für die vorgeschlagenen Änderungen ein Neustart von Nodes erforderlich ist, können Sie die Änderungen verschieben, um die Auswirkungen für den Benutzer zu minimieren. Mit der Option **Cancel** gelangen Sie zurück zum Hauptmenü und erhalten Ihre Änderungen, damit Sie sie später anwenden können.

Wenn Sie **Apply** oder **Stage** auswählen, wird eine neue Netzwerkkonfigurationsdatei generiert, die Bereitstellung durchgeführt und Knoten mit neuen Arbeitsinformationen aktualisiert.

Während der Bereitstellung wird der Status bei der Anwendung von Aktualisierungen angezeigt.

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

Nach dem Anwenden oder Staging von Änderungen wird ein neues Wiederherstellungspaket als Ergebnis der Änderung der Grid-Konfiguration generiert.

10. Wenn Sie **Phase** ausgewählt haben, führen Sie nach Abschluss der Bereitstellung folgende Schritte aus:

- a. Nehmen Sie die erforderlichen Änderungen am physischen oder virtuellen Netzwerk vor.

Physische Netzwerkänderungen: Nehmen Sie die erforderlichen Änderungen an der physischen Netzwerkumgebung vor, und fahren Sie den Knoten bei Bedarf sicher herunter.

Linux: Wenn Sie den Knoten zum ersten Mal zu einem Admin-Netzwerk oder Client-Netzwerk hinzufügen, stellen Sie sicher, dass Sie die Schnittstelle wie unter „Hinzufügen von Schnittstellen zu einem vorhandenen Knoten“ hinzugefügt haben.

- a. Starten Sie die betroffenen Knoten neu.

11. Wählen Sie **0** aus, um das Change IP-Tool nach Abschluss der Änderungen zu beenden.

12. Laden Sie ein neues Wiederherstellungspaket aus dem Grid Manager herunter.

- a. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
- b. Geben Sie die Provisionierungs-Passphrase ein.

Verwandte Informationen

[Linux: Hinzufügen von Schnittstellen zu vorhandenem Node](#)

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

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

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

[StorageGRID verwalten](#)

[Konfigurieren Sie IP-Adressen](#)

Fügen Sie zu Subnetzlisten im Admin-Netzwerk hinzu oder ändern Sie diese

Sie können die Subnetze in der Subnetz-Liste Admin-Netzwerk eines oder mehrerer Nodes hinzufügen, löschen oder ändern.

Was Sie benötigen

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

Sie können Subnetze zu allen Nodes in der Subnetz-Liste des Admin-Netzwerks hinzufügen, löschen oder ändern.

Schritte

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

2. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`
3. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase ein.

Das Hauptmenü wird angezeigt.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. Optional können Sie auch die Netzwerke/Nodes begrenzen, auf denen Vorgänge ausgeführt werden. Folgenden Optionen wählbar:
 - Wählen Sie die Knoten aus, die Sie bearbeiten möchten, indem Sie **1** wählen, wenn Sie bestimmte

Knoten filtern möchten, auf denen der Vorgang ausgeführt werden soll. Wählen Sie eine der folgenden Optionen:

- **1:** Einzelner Knoten (nach Namen auswählen)
- **2:** Einzelner Knoten (nach Standort auswählen, dann nach Name)
- **3:** Einzelner Knoten (nach aktueller IP auswählen)
- **4:** Alle Knoten an einem Standort
- **5:** Alle Knoten im Raster
- **0:** Zurück

- Die Option „all“ bleibt aktiviert. Nach der Auswahl wird der Hauptmenü-Bildschirm angezeigt. Das Feld „Ausgewählte Knoten“ gibt Ihre neue Auswahl wieder. Nun werden alle ausgewählten Vorgänge nur für dieses Element ausgeführt.

5. Wählen Sie im Hauptmenü die Option zum Bearbeiten von Subnetzen für das Admin-Netzwerk (Option **3**).

6. Folgenden Optionen wählbar:

- Fügen Sie ein Subnetz hinzu, indem Sie diesen Befehl eingeben: `add CIDR`
- Löschen Sie ein Subnetz, indem Sie diesen Befehl eingeben: `del CIDR`
- Legen Sie die Liste der Subnetze fest, indem Sie diesen Befehl eingeben: `set CIDR`



Für alle Befehle können Sie mit diesem Format mehrere Adressen eingeben: `add CIDR, CIDR`

Beispiel: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Sie können den erforderlichen Tippaufwand reduzieren, indem Sie „Pfeil nach oben“ verwenden, um zuvor eingegebene Werte an die aktuelle Eingabeaufforderung abzurufen und diese gegebenenfalls zu bearbeiten.

Im folgenden Beispiel werden Subnetze zur Subnetz-Liste des Admin-Netzwerks hinzugefügt:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
 10.0.0.0/8
 172.19.0.0/16
 172.21.0.0/16
 172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. Wenn Sie bereit sind, geben Sie **q** ein, um zum Hauptmenü-Bildschirm zurückzukehren. Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.



Wenn Sie in Schritt 2 einen der „alle“ Knotenauswahlmodi ausgewählt haben, müssen Sie **Enter** (ohne **q**) drücken, um zum nächsten Knoten in der Liste zu gelangen.

8. Folgenden Optionen wählbar:

- Wählen Sie die Option **5**, um Änderungen in der Ausgabe anzuzeigen, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Zusätze) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe unten gezeigt:
- Wählen Sie die Option **6**, um Änderungen in der Ausgabe anzuzeigen, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert. **Hinweis:** bestimmte Terminalemulatoren könnten Ergänzungen und Löschungen mit durchgestrichter Formatierung anzeigen.

Wenn Sie versuchen, die Subnetz-Liste zu ändern, wird die folgende Meldung angezeigt:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

Wenn Sie die NTP- und DNS-Servernetze nicht speziell einem Netzwerk zugewiesen haben, erstellt StorageGRID automatisch eine Host-Route (/32) für die Verbindung. Wenn Sie beispielsweise eine /16- oder /24-Route für eine ausgehende Verbindung zu einem DNS- oder NTP-Server verwenden möchten, sollten Sie die automatisch erstellte /32-Route löschen und die gewünschten Routen hinzufügen. Wenn Sie die automatisch erstellte Host-Route nicht löschen, wird sie beibehalten, nachdem Sie Änderungen an der Subnetz-Liste vorgenommen haben.



Sie können diese automatisch erkannten Host-Routen verwenden, aber im Allgemeinen sollten Sie die DNS- und NTP-Routen manuell konfigurieren, um die Konnektivität zu gewährleisten.

9. Wählen Sie Option **7**, um alle stufenweisen Änderungen zu validieren.

Diese Validierung stellt sicher, dass die Regeln für Grid, Admin und Client-Netzwerke befolgt werden, z. B. die Verwendung überlappender Subnetze.

10. Wählen Sie optional die Option **8**, um alle Änderungen in der Stufendschicht zu speichern und später zurückzukehren, um die Änderungen fortzusetzen.

Mit dieser Option können Sie das Tool IP ändern beenden und es später erneut starten, ohne dabei unangewendete Änderungen zu verlieren.

11. Führen Sie einen der folgenden Schritte aus:

- Wählen Sie Option **9**, wenn Sie alle Änderungen löschen möchten, ohne die neue Netzwerkkonfiguration zu speichern oder anzuwenden.
- Wählen Sie Option **10**, wenn Sie bereit sind, Änderungen anzuwenden und die neue Netzwerkkonfiguration bereitzustellen. Während des Provisioning wird der Status als Aktualisierung angezeigt, wie in der folgenden Beispielausgabe dargestellt:

Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name

12. Laden Sie ein neues Wiederherstellungspaket aus dem Grid Manager herunter.

- Wählen Sie **WARTUNG** > **System** > **Wiederherstellungspaket**.
- Geben Sie die Provisionierungs-Passphrase ein.

Verwandte Informationen

Konfigurieren Sie IP-Adressen

Fügen Sie zu Subnetzlisten im Grid-Netzwerk hinzu oder ändern Sie diese

Mithilfe des Tools IP ändern können Sie Subnetze im Grid Network hinzufügen oder ändern.

Was Sie benötigen

- Sie müssen die haben Passwords.txt Datei:

[illegible]

Wenn Sie nur Änderungen an der Netznetzwerksubnetz-Liste vornehmen, verwenden Sie den Grid-Manager, um die Netzwerkkonfiguration hinzuzufügen oder zu ändern. Verwenden Sie andernfalls das Change IP-Tool, wenn der Grid Manager aufgrund eines Netzwerkkonfigurationsproblem nicht erreichbar ist, oder Sie führen gleichzeitig eine Änderung des Grid Network Routing und andere Netzwerkkänderungen durch.

Schritte

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

2. Starten Sie das Change IP-Tool mit folgendem Befehl: `change-ip`
3. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase ein.

Das Hauptmenü wird angezeigt.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. Wählen Sie im Hauptmenü die Option zum Bearbeiten von Subnetzen für das Grid-Netzwerk (Option 4).



Änderungen an der Netznetzwerksubnetz-Liste sind im gesamten Grid verfügbar.

5. Folgenden Optionen wählbar:

- Fügen Sie ein Subnetz hinzu, indem Sie diesen Befehl eingeben: `add CIDR`
- Löschen Sie ein Subnetz, indem Sie diesen Befehl eingeben: `del CIDR`
- Legen Sie die Liste der Subnetze fest, indem Sie diesen Befehl eingeben: `set CIDR`



Für alle Befehle können Sie mit diesem Format mehrere Adressen eingeben: `add CIDR, CIDR`

Beispiel: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Sie können den erforderlichen Tippaufwand reduzieren, indem Sie „Pfeil nach oben“ verwenden, um zuvor eingegebene Werte an die aktuelle Eingabeaufforderung abzurufen und diese gegebenenfalls zu bearbeiten.

Die unten stehende Beispieleingabe zeigt das Festlegen von Subnetzen für die Netzsubnetz-Liste:

6. Wenn Sie bereit sind, geben Sie `q` ein, um zum Hauptmenü-Bildschirm zurückzukehren. Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.

7. Folgenden Optionen wählbar:

- Wählen Sie die Option 5, um Änderungen in der Ausgabe anzuzeigen, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Zusätze) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe unten gezeigt:
- Wählen Sie die Option 6, um Änderungen in der Ausgabe anzuzeigen, die die vollständige

Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert.



Bestimmte Befehlszeilenschnittstellen zeigen möglicherweise Ergänzungen und Löschungen mithilfe von durchgestrichter Formatierung.

8. Wählen Sie Option **7**, um alle stufenweisen Änderungen zu validieren.

Diese Validierung stellt sicher, dass die Regeln für Grid, Admin und Client-Netzwerke befolgt werden, z. B. die Verwendung überlappender Subnetze.

9. Wählen Sie optional die Option **8**, um alle Änderungen in der Stufendschicht zu speichern und später zurückzukehren, um die Änderungen fortzusetzen.

Mit dieser Option können Sie das Tool IP ändern beenden und es später erneut starten, ohne dabei unangewendete Änderungen zu verlieren.

10. Führen Sie einen der folgenden Schritte aus:

- Wählen Sie Option **9**, wenn Sie alle Änderungen löschen möchten, ohne die neue Netzwerkkonfiguration zu speichern oder anzuwenden.
- Wählen Sie Option **10**, wenn Sie bereit sind, Änderungen anzuwenden und die neue Netzwerkkonfiguration bereitzustellen. Während des Provisioning wird der Status als Aktualisierung angezeigt, wie in der folgenden Beispielausgabe dargestellt:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

11. Wenn Sie beim Ändern des Grid-Netzwerks die Option **10** ausgewählt haben, wählen Sie eine der folgenden Optionen aus:

- **Apply:** Die Änderungen sofort anwenden und bei Bedarf automatisch jeden Knoten neu starten.

Wenn die neue Netzwerkkonfiguration ohne externe Änderungen gleichzeitig mit der alten Netzwerkkonfiguration funktioniert, können Sie die Option **Apply** für eine vollautomatische Konfigurationsänderung verwenden.

- **Stufe:** Beim nächsten Neustart der Knoten die Änderungen anwenden.

Wenn Sie Änderungen an der physischen oder virtuellen Netzwerkkonfiguration vornehmen müssen, damit die neue Netzwerkkonfiguration funktioniert, müssen Sie die Option **Stage** verwenden, die betroffenen Knoten herunterfahren, die erforderlichen Änderungen am physischen Netzwerk vornehmen und die betroffenen Knoten neu starten.



Wenn Sie die Option **Stage** verwenden, müssen Sie den Knoten nach der Staging so schnell wie möglich neu starten, um Störungen zu minimieren.

- **Abbrechen:** Nehmen Sie keine Netzwerkänderungen vor.

Wenn Sie nicht wissen, dass für die vorgeschlagenen Änderungen ein Neustart von Nodes erforderlich

ist, können Sie die Änderungen verschieben, um die Auswirkungen für den Benutzer zu minimieren. Mit der Option **Cancel** gelangen Sie zurück zum Hauptmenü und erhalten Ihre Änderungen, damit Sie sie später anwenden können.

Nach dem Anwenden oder Staging von Änderungen wird ein neues Wiederherstellungspaket als Ergebnis der Änderung der Grid-Konfiguration generiert.

12. Wenn die Konfiguration aufgrund von Fehlern angehalten wird, stehen folgende Optionen zur Verfügung:

- Um den IP-Änderungsvorgang abubrechen und zum Hauptmenü zurückzukehren, geben Sie **A** ein.
- Um den fehlgeschlagenen Vorgang erneut zu versuchen, geben Sie **r** ein.
- Um mit der nächsten Operation fortzufahren, geben Sie **c** ein.

Der fehlgeschlagene Vorgang kann später erneut versucht werden, indem Sie im Hauptmenü die Option **10** (Änderungen übernehmen) wählen. Das IP-Änderungsverfahren wird erst abgeschlossen, wenn alle Vorgänge erfolgreich abgeschlossen wurden.

- Wenn Sie manuell eingreifen mussten (zum Beispiel um einen Knoten neu zu starten) und sich sicher sind, dass die Aktion, die das Tool für erfolgreich hält, tatsächlich erfolgreich abgeschlossen wurde, geben Sie **f** ein, um sie als erfolgreich zu markieren und zum nächsten Vorgang zu wechseln.

13. Laden Sie ein neues Wiederherstellungspaket aus dem Grid Manager herunter.

- Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
- Geben Sie die Provisionierungs-Passphrase ein.



Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

Verwandte Informationen

[Konfigurieren Sie IP-Adressen](#)

Ändern Sie die IP-Adressen für alle Nodes im Grid

Wenn Sie die Grid-Netzwerk-IP-Adresse für alle Knoten im Raster ändern müssen, müssen Sie dieses spezielle Verfahren befolgen. Sie können eine Grid-Netzwerk-IP-Änderung nicht unter Verwendung des Verfahrens zum Ändern einzelner Knoten vornehmen.

Was Sie benötigen

- Sie müssen die `Passwords.txt` Datei:

Um sicherzustellen, dass das Raster erfolgreich gestartet wird, müssen Sie alle Änderungen gleichzeitig vornehmen.



Dieses Verfahren gilt nur für das Grid-Netzwerk. Mit diesem Verfahren können Sie keine IP-Adressen in Admin- oder Client-Netzwerken ändern.

Wenn Sie die IP-Adressen und die MTU nur für die Nodes an einem Standort ändern möchten, folgen Sie den [Ändern der Node-Netzwerkconfiguration](#) Anweisungen.

Schritte

1. Planen Sie im Voraus, wenn Änderungen außerhalb des Tools zur Änderung der IP vorgenommen werden müssen, z. B. Änderungen an DNS oder NTP oder Änderungen an der SSO-Konfiguration (Single Sign On).



Wenn auf den neuen IP-Adressen nicht auf die vorhandenen NTP-Server für das Grid zugegriffen werden kann, fügen Sie die neuen NTP-Server hinzu, bevor Sie das Change-ip-Verfahren durchführen.



Wenn auf den neuen IP-Adressen nicht auf die vorhandenen DNS-Server für das Grid zugegriffen werden kann, fügen Sie die neuen DNS-Server hinzu, bevor Sie das Change-ip-Verfahren durchführen.



Wenn SSO für Ihr StorageGRID-System aktiviert ist und alle Vertrauensstellen, die sich auf Administratorknoten-IP-Adressen befinden, konfiguriert wurden (anstelle von vollständig qualifizierten Domännennamen, wie empfohlen), müssen Sie diese Vertrauensstellungen der betreffenden Partei in Active Directory Federation Services (AD FS) aktualisieren oder neu konfigurieren. Unmittelbar nach dem Ändern der IP-Adressen. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.



Fügen Sie bei Bedarf das neue Subnetz für die neuen IP-Adressen hinzu.

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 das Change IP-Tool mit folgendem Befehl: `change-ip`
4. Geben Sie an der Eingabeaufforderung die Provisionierungs-Passphrase ein.

Das Hauptmenü wird angezeigt. Standardmäßig wird der verwendet `Selected nodes` Feld ist auf festgelegt `all`.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

5. Wählen Sie im Hauptmenü **2** aus, um IP/Subnetzmaske, Gateway und MTU-Informationen für alle Knoten zu bearbeiten.

a. Wählen Sie **1**, um Änderungen am Grid-Netzwerk vorzunehmen.

Nach der Auswahl werden in der Eingabeaufforderung die Node-Namen, Grid Network Name, Datentyp (IP/Maske, Gateway oder MTU) angezeigt. Und aktuellen Werten.

Wenn Sie die IP-Adresse, die Präfixlänge, das Gateway oder die MTU einer DHCP-konfigurierten Schnittstelle bearbeiten, wird die Schnittstelle zu statisch geändert. Vor jeder über DHCP konfigurierten Schnittstelle wird eine Warnung angezeigt.

Als konfigurierte Schnittstellen `fixed` Kann nicht bearbeitet werden.

a. Um einen neuen Wert festzulegen, geben Sie ihn in das für den aktuellen Wert angezeigte Format ein.

b. Nachdem Sie alle Knoten bearbeitet haben, die Sie ändern möchten, geben Sie **q** ein, um zum Hauptmenü zurückzukehren.

Ihre Änderungen werden so lange gespeichert, bis sie gelöscht oder angewendet wurden.

6. Überprüfen Sie Ihre Änderungen, indem Sie eine der folgenden Optionen auswählen:

- **5**: Zeigt Edits in der Ausgabe an, die isoliert sind, um nur das geänderte Element anzuzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) hervorgehoben, wie in der Beispielausgabe dargestellt:

- **6**: Zeigt Änderungen in der Ausgabe an, die die vollständige Konfiguration anzeigen. Änderungen werden grün (Ergänzungen) oder rot (Löschungen) markiert.



Bestimmte Befehlszeilenschnittstellen zeigen möglicherweise Ergänzungen und Löschungen mithilfe von durchgestrichter Formatierung. Die richtige Anzeige hängt von Ihrem Terminalclient ab, der die erforderlichen VT100-Escape-Sequenzen unterstützt.

7. Wählen Sie Option **7**, um alle Änderungen zu validieren.

Diese Validierung stellt sicher, dass die Regeln für das Grid-Netzwerk, wie z. B. die Verwendung überlappender Subnetze, nicht verletzt werden.

In diesem Beispiel ergab die Validierung Fehler.

In diesem Beispiel wurde die Validierung erfolgreich bestanden.

8. Wenn die Validierung erfolgreich abgeschlossen ist, wählen Sie **10** aus, um die neue Netzwerkkonfiguration anzuwenden.

9. Wählen Sie **Stufe**, um die Änderungen beim nächsten Neustart der Knoten anzuwenden.



Sie müssen **Stufe** wählen. Führen Sie keinen Rolling-Neustart durch, entweder manuell oder durch Auswahl von **Apply** statt **Stage**; das Raster wird nicht erfolgreich gestartet.

10. Wenn die Änderungen abgeschlossen sind, wählen Sie **0** aus, um das Change IP-Tool zu verlassen.

11. Fahren Sie alle Nodes gleichzeitig herunter.



Das gesamte Grid muss gleichzeitig heruntergefahren werden, um alle Nodes gleichzeitig ausgefallen zu sein.

12. Nehmen Sie die erforderlichen Änderungen am physischen oder virtuellen Netzwerk vor.

13. Vergewissern Sie sich, dass alle Grid-Nodes ausgefallen sind.

14. Schalten Sie alle Knoten ein.

15. Sobald das Raster erfolgreich gestartet wurde:

- a. Wenn Sie neue NTP-Server hinzugefügt haben, löschen Sie die alten NTP-Serverwerte.
- b. Wenn Sie neue DNS-Server hinzugefügt haben, löschen Sie die alten DNS-Serverwerte.

16. Laden Sie das neue Wiederherstellungspaket aus dem Grid Manager herunter.

- a. Wählen Sie **WARTUNG > System > Wiederherstellungspaket**.
- b. Geben Sie die Provisionierungs-Passphrase ein.

Verwandte Informationen

[StorageGRID verwalten](#)

[Fügen Sie zu Subnetzlisten im Grid-Netzwerk hinzu oder ändern Sie diese](#)

[Fahren Sie den Grid-Node herunter](#)

Fügen Sie Schnittstellen zum vorhandenen Node hinzu

Linux: Hinzufügen von Admin- oder Client-Schnittstellen zu einem bestehenden Knoten

Führen Sie diese Schritte aus, um einen Linux-Knoten nach der Installation eine Schnittstelle im Admin-Netzwerk oder im Client-Netzwerk hinzuzufügen.

Wenn SIE WÄHREND der Installation IN der Node-Konfigurationsdatei auf dem Linux-Host NICHT ADMIN_NETWORK_TARGET oder CLIENT_NETWORK_TARGET konfiguriert haben, verwenden Sie dieses Verfahren, um die Schnittstelle hinzuzufügen. Weitere Informationen zur Node-Konfigurationsdatei finden Sie in den Anweisungen für Ihr Linux-Betriebssystem:

- [Installieren Sie Red hat Enterprise Linux oder CentOS](#)
- [Installieren Sie Ubuntu oder Debian](#)

Sie führen diese Schritte auf dem Linux-Server durch, der den Node hostet, der die neue Netzwerkzuweisung benötigt, nicht innerhalb des Nodes. Bei diesem Vorgang wird die Schnittstelle nur dem Knoten hinzugefügt. Ein Validierungsfehler tritt auf, wenn Sie versuchen, andere Netzwerkparameter anzugeben.

Um Adressinformationen bereitzustellen, müssen Sie das Werkzeug IP ändern verwenden. Siehe [Ändern der Node-Netzwerkkonfiguration](#).

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Node gehostet wird.
2. Bearbeiten Sie die Konfigurationsdatei des Knotens: `/etc/storagegrid/nodes/node-name.conf`.



Geben Sie keine anderen Netzwerkparameter an, oder ein Validierungsfehler führt zu einem Ergebnis.

- a. Fügen Sie einen Eintrag für das neue Netzwerkziel hinzu. Beispiel:

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Optional: Fügen Sie einen Eintrag für die MAC-Adresse hinzu. Beispiel:

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Führen Sie den Node-Validier-Befehl aus:

```
sudo storagegrid node validate node-name
```

4. Beheben Sie alle Validierungsfehler.

5. Führen Sie den Befehl zum erneuten Laden des Node aus:

```
sudo storagegrid node reload node-name
```

Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Nach der Installation können Sie einem Linux-Knoten zusätzliche Trunk- oder Zugangsschnittstellen hinzufügen. Die fügen Sie Schnittstellen hinzu, werden auf der Seite VLAN-Schnittstellen und auf der Seite HA-Gruppen angezeigt.

Was Sie benötigen

- Sie haben Zugriff auf die Anweisungen für die Installation von StorageGRID auf Ihrer Linux-Plattform.
 - [Installieren Sie Red hat Enterprise Linux oder CentOS](#)
 - [Installieren Sie Ubuntu oder Debian](#)
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, einem Node Schnittstellen hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Verwenden Sie diese Schritte, um einem Linux-Knoten eine oder mehrere zusätzliche Schnittstellen hinzuzufügen, nachdem der Knoten installiert wurde. Beispielsweise möchten Sie einem Admin oder Gateway Node eine Trunk-Schnittstelle hinzufügen, sodass Sie den Datenverkehr zwischen verschiedenen Applikationen oder Mandanten über VLAN-Schnittstellen trennen können. Oder auch, wenn Sie eine Access-Schnittstelle hinzufügen möchten, um sie in einer HA-Gruppe (High Availability, Hochverfügbarkeit) zu verwenden.

Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsoberfläche hinzufügen, können Sie die Schnittstelle direkt einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.

Der Node ist für kurze Zeit nicht verfügbar, wenn Sie Schnittstellen hinzufügen. Sie sollten dieses Verfahren

auf jeweils einem Knoten durchführen.

Schritte

1. Melden Sie sich beim Linux-Server an, auf dem der Node gehostet wird.
2. Bearbeiten Sie mit einem Texteditor wie vim oder pico die Konfigurationsdatei des Knotens:

```
/etc/storagegrid/nodes/node-name.conf
```

3. Fügen Sie der Datei einen Eintrag hinzu, um den Namen und optional die Beschreibung jeder zusätzlichen Schnittstelle anzugeben, die Sie dem Node hinzufügen möchten. Verwenden Sie dieses Format.

```
INTERFACES_TARGET_nnnn=value
```

Geben Sie für *nnnn* eine eindeutige Zahl für jede ein `INTERFACES_TARGET` Eintrag, den Sie hinzufügen.

Geben Sie unter *value* den Namen der physischen Schnittstelle auf dem Bare-Metal-Host an. Fügen Sie dann optional ein Komma hinzu und geben Sie eine Beschreibung der Schnittstelle an, die auf der Seite VLAN-Schnittstellen und der Seite HA-Gruppen angezeigt wird.

Beispiel:

```
INTERFACES_TARGET_01=ens256, Trunk
```



Geben Sie keine anderen Netzwerkparameter an, oder ein Validierungsfehler führt zu einem Ergebnis.

4. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Node-Konfigurationsdatei zu validieren:

```
sudo storagegrid node validate node-name
```

Beheben Sie Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

5. Führen Sie den folgenden Befehl aus, um die Konfiguration des Node zu aktualisieren:

```
sudo storagegrid node reload node-name
```

Nachdem Sie fertig sind

- Wenn Sie eine oder mehrere Trunk-Schnittstellen hinzugefügt haben, gehen Sie zu [Konfigurieren Sie die VLAN-Schnittstellen](#) So konfigurieren Sie eine oder mehrere VLAN-Schnittstellen für jede neue übergeordnete Schnittstelle:
- Wenn Sie eine oder mehrere Access Interfaces hinzugefügt haben, gehen Sie zu [Konfigurieren Sie Hochverfügbarkeitsgruppen](#) Um die neuen Schnittstellen direkt zu HA-Gruppen hinzuzufügen.

VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Nach der Installation des Node können Sie einem VM-Node eine Trunk- oder Zugriffsschnittstelle hinzufügen. Die fügen Sie Schnittstellen hinzu, werden auf der Seite VLAN-Schnittstellen und auf der Seite HA-Gruppen angezeigt.

Was Sie benötigen

- Sie haben Zugriff auf die Anweisungen zum Installieren von StorageGRID auf Ihrer VMware Plattform.

VMware installieren

- Sie haben StorageGRID 11.6 konfiguriert.
- Sie haben virtuelle Admin-Node- und Gateway-Node-VMware-Maschinen.
- Sie haben ein Netzwerk-Subnetz, das nicht als Grid-, Admin- oder Client-Netzwerk verwendet wird.
- Sie haben die `Passwords.txt` Datei:
- Sie haben spezifische Zugriffsberechtigungen.



Versuchen Sie nicht, einem Node Schnittstellen hinzuzufügen, während ein Software-Upgrade, ein Wiederherstellungsverfahren oder ein Erweiterungsvorgang aktiv ist.

Über diese Aufgabe

Verwenden Sie diese Schritte, um einem VMware Node nach der Installation des Node mindestens eine zusätzliche Schnittstelle hinzuzufügen. Beispielsweise möchten Sie einem Admin oder Gateway Node eine Trunk-Schnittstelle hinzufügen, sodass Sie den Datenverkehr zwischen verschiedenen Applikationen oder Mandanten über VLAN-Schnittstellen trennen können. Oder Sie möchten vielleicht eine Zugriffsoberfläche hinzufügen, die in einer HA-Gruppe (High Availability, Hochverfügbarkeit) verwendet werden soll.

Wenn Sie eine Trunk-Schnittstelle hinzufügen, müssen Sie eine VLAN-Schnittstelle in StorageGRID konfigurieren. Wenn Sie eine Zugriffsoberfläche hinzufügen, können Sie die Schnittstelle direkt einer HA-Gruppe hinzufügen. Sie müssen keine VLAN-Schnittstelle konfigurieren.

Der Node ist möglicherweise für einen kurzen Zeitraum nicht verfügbar, wenn Sie Schnittstellen hinzufügen.

Schritte

1. Fügen Sie in vCenter einen neuen Netzwerkadapter (Typ VMXNET3) zu einer Admin-Node- und Gateway-Node-VM hinzu. Aktivieren Sie die Kontrollkästchen **verbunden** und **bei Einschalten verbinden**.

Network adapter 4 *	CLIENT683_old_vlan	Connected
Status	Connect At Power On	
Adapter Type	VMXNET 3	
DirectPath I/O	Enable	

2. Verwenden Sie SSH, um sich beim Admin-Node oder Gateway-Node anzumelden.
3. Nutzung `ip link show` Um zu überprüfen, ob die neue Netzwerkschnittstelle `ens256` erkannt wurde.


```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Nachdem Sie fertig sind

- Wenn Sie eine oder mehrere Trunk-Schnittstellen hinzugefügt haben, gehen Sie zu [Konfigurieren Sie die VLAN-Schnittstellen](#) So konfigurieren Sie eine oder mehrere VLAN-Schnittstellen für jede neue übergeordnete Schnittstelle:
- Wenn Sie eine oder mehrere Access Interfaces hinzugefügt haben, gehen Sie zu [Konfigurieren Sie Hochverfügbarkeitsgruppen](#) Um die neuen Schnittstellen direkt zu HA-Gruppen hinzuzufügen.

Konfigurieren Sie DNS-Server

Sie können DNS-Server (Domain Name System) hinzufügen, entfernen und aktualisieren, sodass Sie vollständig qualifizierte Domain Name (FQDN) Hostnamen anstelle von IP-Adressen verwenden können.

Was Sie benötigen

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

Wenn Sie DNS-Serverinformationen angeben, können Sie vollständig qualifizierte Domännennamen (FQDN)-Hostnamen anstelle von IP-Adressen für E-Mail- oder SNMP-Benachrichtigungen und AutoSupport verwenden. Es wird empfohlen, mindestens zwei DNS-Server anzugeben.



Geben Sie zwei bis sechs IP-Adressen für DNS-Server ein. Im Allgemeinen wählen Sie DNS-Server aus, auf die jeder Standort im Falle einer Netzwerkislanding lokal zugreifen kann. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie dies ausführen [Passen Sie die DNS-Serverliste für jeden Knoten weiter an](#).

Wenn die DNS-Serverinformationen nicht angegeben oder falsch konfiguriert sind, wird ein DNST-Alarm für den SSM-Service jedes Grid-Knotens ausgelöst. Der Alarm wird gelöscht, wenn DNS richtig konfiguriert ist und

die neuen Serverinformationen alle Grid-Knoten erreicht haben.

Schritte

1. Wählen Sie **WARTUNG > Netzwerk > DNS-Server**.
2. Fügen Sie im Abschnitt „Server“ nach Bedarf Aktualisierungen hinzu oder entfernen Sie DNS-Servereinträge.

Als Best Practice empfehlen wir, mindestens zwei DNS-Server pro Standort anzugeben. Sie können bis zu sechs DNS-Server angeben.

3. Klicken Sie Auf **Speichern**.

Ändern der DNS-Konfiguration für einen einzelnen Grid-Node

Anstatt das Domain Name System (DNS) global für die gesamte Bereitstellung zu konfigurieren, können Sie ein Skript ausführen, um DNS für jeden Grid-Knoten unterschiedlich zu konfigurieren.

Im Allgemeinen sollten Sie die Option **WARTUNG Netzwerk DNS Server** im Grid Manager verwenden, um DNS-Server zu konfigurieren. Verwenden Sie das folgende Skript nur, wenn Sie unterschiedliche DNS-Server für unterschiedliche Grid-Nodes verwenden müssen.

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

- e. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein: `ssh-add`
 - f. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:
2. Melden Sie sich beim Knoten an, den Sie mit einer benutzerdefinierten DNS-Konfiguration aktualisieren möchten: `ssh node_IP_address`
 3. Führen Sie das DNS-Setup-Skript aus: `setup_resolv.rb`.

Das Skript antwortet mit der Liste der unterstützten Befehle.

Tool to modify external name servers

available commands:

```
add search <domain>
    add a specified domain to search list
    e.g.> add search netapp.com
remove search <domain>
    remove a specified domain from list
    e.g.> remove search netapp.com
add nameserver <ip>
    add a specified IP address to the name server list
    e.g.> add nameserver 192.0.2.65
remove nameserver <ip>
    remove a specified IP address from list
    e.g.> remove nameserver 192.0.2.65
remove nameserver all
    remove all nameservers from list
save
    write configuration to disk and quit
abort
    quit without saving changes
help
    display this help message
```

Current list of name servers:

192.0.2.64

Name servers inherited from global DNS configuration:

192.0.2.126

192.0.2.127

Current list of search entries:

netapp.com

Enter command [``add search <domain>|remove search <domain>|add nameserver <ip>``]

[``remove nameserver <ip>|remove nameserver all|save|abort|help``]

4. Fügen Sie die IPv4-Adresse eines Servers hinzu, der einen Domännennamendienst für Ihr Netzwerk bereitstellt: `add <nameserver IP_address>`
5. Wiederholen Sie den `add nameserver` Befehl zum Hinzufügen von Nameserver.
6. Befolgen Sie die Anweisungen, wenn Sie dazu aufgefordert werden, weitere Befehle einzugeben.
7. Speichern Sie Ihre Änderungen und beenden Sie die Anwendung: `save`
8. Schließen Sie die Befehlsshell auf dem Server: `exit`
9. Wiederholen Sie für jeden Grid-Node die Schritte von [Anmeldung beim Node](#) Bis [Schließen der Befehlsshell](#).

10. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein: `ssh-add -D`

Konfigurieren Sie NTP-Server

Sie können NTP-Server (Network Time Protocol) hinzufügen, aktualisieren oder entfernen, um sicherzustellen, dass die Daten zwischen den Grid-Nodes in Ihrem StorageGRID-System korrekt synchronisiert werden.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen über die Berechtigung Wartung oder Stammzugriff verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.
- Sie müssen die IPv4-Adressen der NTP-Server konfigurieren.

Über diese Aufgabe

Das StorageGRID-System verwendet das Network Time Protocol (NTP) zur Synchronisierung der Zeit zwischen allen Grid-Nodes im Grid.

Jedem Standort werden mindestens zwei Nodes im StorageGRID-System die primäre NTP-Rolle zugewiesen. Sie synchronisieren sich mit einem vorgeschlagenen Minimum von vier und maximal sechs externen Zeitquellen und miteinander. Jeder Node im StorageGRID System, der kein primärer NTP-Node ist, fungiert als NTP-Client und synchronisiert mit diesen primären NTP-Nodes.

Die externen NTP-Server stellen eine Verbindung zu den Nodes her, denen Sie zuvor primäre NTP-Rollen zugewiesen haben. Aus diesem Grund wird die Angabe von mindestens zwei Nodes mit primären NTP-Rollen empfohlen.



Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

Die angegebenen externen NTP-Server müssen das NTP-Protokoll verwenden. Sie müssen NTP-Serverreferenzen von Stratum 3 oder besser angeben, um Probleme mit Zeitdrift zu vermeiden.



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.

["Begrenzung des Supports, um Windows Time Service für hochpräzise Umgebungen zu konfigurieren"](#)

Wenn Probleme mit der Stabilität oder Verfügbarkeit der NTP-Server auftreten, die ursprünglich während der Installation angegeben wurden, können Sie die Liste der externen NTP-Quellen, die das StorageGRID-System verwendet, aktualisieren oder entfernen Sie vorhandene Server.

Schritte

1. Wählen Sie **WARTUNG Netzwerk NTP-Server**.

2. Fügen Sie im Abschnitt „Server“ bei Bedarf Update hinzu oder entfernen Sie NTP-Servereinträge.

Sie sollten mindestens 4 NTP-Server enthalten, und Sie können bis zu 6 Server angeben.

3. Geben Sie im Textfeld **Provisioning Passphrase** die Provisioning-Passphrase für Ihr StorageGRID-System ein und klicken Sie auf **Speichern**.

Der Status des Verfahrens wird oben auf der Seite angezeigt. Die Seite wird deaktiviert, bis die Konfigurationsaktualisierungen abgeschlossen sind.



Wenn alle NTP-Server den Verbindungstest nicht ausführen, nachdem Sie die neuen NTP-Server gespeichert haben, fahren Sie nicht fort. Wenden Sie sich an den technischen Support.

Stellt die Netzwerkverbindung für isolierte Knoten wieder her

Unter bestimmten Umständen, z. B. Änderungen an der IP-Adresse für Standort oder das gesamte Grid, kann sich eine oder mehrere Node-Gruppen möglicherweise nicht an den Rest des Grid wenden.

Im Grid Manager (**SUPPORT Tools Grid Topology**), wenn ein Knoten grau ist oder wenn ein Knoten blau ist, wobei viele seiner Dienste einen anderen Status als laufen aufweisen, sollten Sie auf Knotenisolierung prüfen.

The screenshot displays the Grid Manager interface. On the left, the 'Grid Topology' panel shows a hierarchical view of the grid structure, including 'Grid1', 'Site1', and various nodes like 'abrian-adm1', 'abrian-g1', 'SSM', 'Services', 'Events', 'Resources', 'Timing', 'CLB', 'abrian-s1', 'abrian-s2', and 'abrian-s3'. The main panel shows the 'Overview' tab for 'SSM (abrian-g1) - Services'. It includes a gear icon, the title 'Overview: SSM (abrian-g1) - Services', and a timestamp 'Updated: 2018-01-23 15:03:45 MST'. Below this, the 'Operating System' is listed as 'Linux 4.9.0-3-amd64'. The 'Services' section contains a table with columns: Service, Version, Status, Threads, Load, and Memory. The 'Packages' section contains a table with columns: Package, Installed, and Version.

Service	Version	Status	Threads	Load	Memory
ADE Exporter Service	11.1.0-20171214.1441.c29e2f8	Running	11	0.011 %	7.87 MB
Connection Load Balancer (CLB)	11.1.0-20180120.0111.02137fe	Running	61	0.07 %	39.3 MB
Dynamic IP Service	11.1.0-20180123.1919.deeeba7.abrian	Not Running	0	0 %	0 B
Nginx Service	1.10.3-1+deb9u1	Running	5	0.002 %	20 MB
Node Exporter Service	0.13.0+ds-1+b2	Running	5	0 %	8.58 MB
Persistence Service	11.1.0-20180123.1919.deeeba7.abrian	Running	6	0.064 %	17.1 MB
Server Manager	11.1.0-20171214.1441.c29e2f8	Running	4	2.116 %	18.7 MB
Server Status Monitor (SSM)	11.1.0-20180120.0111.02137fe	Running	61	0.288 %	45.8 MB
System Logging	3.8.1-10	Running	3	0.006 %	8.27 MB
Time Synchronization	1:4.2.8p10+dfsg-3+deb9u1	Running	2	0.007 %	4.54 MB

Package	Installed	Version
storage-grid-release	Installed	11.1.0-20180123.1919.deeeba7.abrian

Isolierte Nodes haben einige der Folgen:

- Wenn mehrere Knoten isoliert sind, können Sie sich möglicherweise nicht bei Grid Manager anmelden oder auf diesen zugreifen.
- Wenn mehrere Nodes isoliert sind, sind die im Dashboard für den Mandanten-Manager angezeigten Werte für Storage-Auslastung und Kontingente möglicherweise nicht mehr aktuell. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

Um das Isolationsproblem zu lösen, führen Sie auf jedem isolierten Knoten oder auf einem Knoten in einer Gruppe (alle Knoten in einem Subnetz, das nicht den primären Admin-Node enthält) ein Befehlszeilen-Dienstprogramm aus, das vom Raster isoliert ist. Das Dienstprogramm stellt den Knoten die IP-Adresse eines nicht isolierten Knotens im Raster zur Verfügung, sodass der isolierte Knoten oder die Gruppe der Knoten das gesamte Raster erneut kontaktieren kann.



Wenn das Multicast Domain Name System (mDNS) in den Netzwerken deaktiviert ist, muss möglicherweise auf jedem isolierten Knoten das Befehlszeilendienstprogramm ausgeführt werden.

1. Auf den Knoten zugreifen und überprüfen `/var/local/log/dynip.log` Für Isolationsmeldungen.

Beispiel:

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action may be required.
```

Wenn Sie die VMware Konsole verwenden, enthält sie eine Meldung, dass der Node möglicherweise isoliert ist.

Bei Linux-Bereitstellungen werden in Isolationsmeldungen angezeigt
`/var/log/storagegrid/node/<nodename>.log` Dateien:

2. Wenn die Isolationsmeldungen immer wieder und dauerhaft sind, führen Sie den folgenden Befehl aus:

```
add_node_ip.py <address>
```

Wo `<address>` Ist die IP-Adresse eines Remote-Node, der mit dem Grid verbunden ist.

```
# /usr/sbin/add_node_ip.py 10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. Überprüfen Sie Folgendes für jeden zuvor isolierten Node:

- Die Services des Knotens wurden gestartet.
- Der Status des dynamischen IP-Dienstes lautet „Running“, nachdem Sie den ausgeführt haben `storagegrid-status` Befehl.
- In der Struktur Grid Topology erscheint der Knoten nicht mehr vom Rest des Rasters getrennt.



Wenn Sie den ausführen `add_node_ip.py` Der Befehl löst das Problem nicht, es können weitere Netzwerkprobleme auftreten, die gelöst werden müssen.

Verfahren auf Host-Ebene und Middleware

Einige Wartungsverfahren sind für Linux oder VMware Implementierungen von StorageGRID oder speziell für andere Komponenten der StorageGRID Lösung entwickelt.

Linux: Migrieren des Grid-Node zu neuem Host

Sie können StorageGRID Nodes von einem Linux-Host auf einen anderen migrieren, um Host-Wartungsarbeiten (wie BS-Patches und Neustart) durchzuführen, ohne die Funktionalität oder Verfügbarkeit Ihres Grid zu beeinträchtigen.

Sie migrieren einen oder mehrere Knoten von einem Linux-Host (der „source Host“) zu einem anderen Linux-Host (der „target-Host“). Der Zielhost muss bereits für die Verwendung mit StorageGRID vorbereitet sein.



Sie können diese Prozedur nur verwenden, wenn Sie die StorageGRID-Bereitstellung mit Migrationssupport geplant haben.

Um einen Grid-Node auf einen neuen Host zu migrieren, müssen beide der folgenden Bedingungen erfüllt sein:

- Shared Storage wird für alle Storage Volumes pro Node verwendet
- Netzwerkschnittstellen haben zwischen Hosts einheitliche Namen



Führen Sie in einer Produktionsimplementierung nicht mehr als einen Speicherknoten auf einem einzelnen Host aus. Die Verwendung eines dedizierten Hosts für jeden Speicherknoten stellt eine isolierte Ausfalldomäne zur Verfügung.

Andere Node-Typen, wie beispielsweise Admin-Nodes oder Gateway-Nodes, können auf demselben Host implementiert werden. Wenn Sie jedoch mehrere Nodes desselben Typs haben (z. B. zwei Gateway-Nodes), installieren Sie nicht alle Instanzen auf demselben Host.

Weitere Informationen finden Sie unter „Node Migration Requirements“ in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

Verwandte Informationen

[Implementieren Sie neue Linux-Hosts](#)

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

Linux: Export Node vom Quell-Host

Fahren Sie den Grid-Node herunter, und exportieren Sie ihn vom Linux-Quell-Host.

Führen Sie den folgenden Befehl auf dem Linux-Quell-Host aus.

1. Abrufen des Status aller derzeit auf dem Quell-Host ausgeführten Nodes

```
sudo storagegrid node status all
```

```
Name Config-State Run-State
```

```
DC1-ADM1 Configured Running
```

```
DC1-ARC1 Configured Running
```

```
DC1-GW1 Configured Running
```

```
DC1-S1 Configured Running
```

```
DC1-S2 Configured Running
```

```
DC1-S3 Configured Running
```

2. Geben Sie den Namen des Node an, den Sie migrieren möchten, und beenden Sie ihn, wenn dessen Ausführungszustand lautet Running.

```
sudo storagegrid node stop DC1-S3
```

```
Stopping node DC1-S3
```

```
Waiting up to 630 seconds for node shutdown
```

3. Exportieren Sie den Knoten vom Quell-Host.

```
sudo storagegrid node export DC1-S3
```

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
```

```
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you  
want to import it again.
```

4. Beachten Sie die import command suggested in the output of the `export Befehl.

Im nächsten Schritt führen Sie diesen Befehl auf dem Zielhost aus.

Linux: Importknoten auf Zielhost

Nachdem Sie den Knoten vom Quell-Host exportiert haben, importieren und validieren Sie den Knoten auf dem Ziel-Linux-Host. Die Validierung bestätigt, dass der Knoten Zugriff auf denselben Block-Speicher und Netzwerkschnittstellengeräte hat, wie er auf dem Quell-Host hatte.

Führen Sie den folgenden Befehl auf dem Ziel-Linux-Host aus.

1. Importieren Sie den Knoten auf dem Zielhost.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.

You should run 'storagegrid node validate DC1-S3'

2. Validieren der Node-Konfiguration auf dem neuen Host

```
sudo storagegrid node validate DC1-S3
```

Confirming existence of node DC1-S3... PASSED

Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node DC1-S3... PASSED

Checking for duplication of unique values... PASSED

3. Wenn Validierungsfehler auftreten, beheben Sie diese, bevor Sie den migrierten Knoten starten.

Informationen zur Fehlerbehebung finden Sie in der StorageGRID-Installationsanleitung für Ihr Linux-Betriebssystem.

Verwandte Informationen

[Installieren Sie Red hat Enterprise Linux oder CentOS](#)

[Installieren Sie Ubuntu oder Debian](#)

Linux: Migrierenden Knoten starten

Nachdem Sie den migrierten Node validiert haben, starten Sie den Node durch Ausführen eines Befehls auf dem Linux-Zielhost.

Schritte

1. Starten Sie den Knoten auf dem neuen Host.

```
sudo storagegrid node start DC1-S3  
Starting node DC1-S3
```

2. Überprüfen Sie im Grid Manager, ob der Status des Knotens grün ist und keine Alarme dagegen ausgelöst werden.



Überprüfen, ob der Status des Node grün lautet, stellt sicher, dass der migrierte Node vollständig neu gestartet und wieder dem Grid beigetreten ist. Wenn der Status nicht grün lautet, migrieren Sie keine zusätzlichen Nodes, damit nicht mehr als ein Node außer Betrieb ist.

Wenn Sie nicht auf den Grid Manager zugreifen können, warten Sie 10 Minuten, und führen Sie den folgenden Befehl aus:

```
sudo storagegrid node status node-name
```

Vergewissern Sie sich, dass der migrierte Knoten einen Run-State von `Running` hat.

Wartung von Archivierungs-Nodes für TSM Middleware

Archive Nodes sind möglicherweise für Tapes über einen TSM Middleware-Server oder die Cloud über die S3-API konfiguriert. Nach der Konfiguration kann das Ziel eines Archivierungs-Knotens nicht mehr geändert werden.

Wenn der Server, der den Archivknoten hostet, ausfällt, ersetzen Sie den Server, und befolgen Sie den entsprechenden Wiederherstellungsvorgang.

Fehler bei Archivgeräten

Wenn Sie feststellen, dass ein Fehler beim Archivspeichergerät vorliegt, auf das der Archivknoten über Tivoli Storage Manager (TSM) zugreift, schalten Sie den Archivknoten offline, um die Anzahl der im StorageGRID-System angezeigten Alarme zu begrenzen. Anschließend können Sie das Problem mit den administrativen Tools des TSM-Servers, des Speichergeräts oder beidem weiter diagnostizieren und lösen.

Versetzen Sie die Zielkomponente in den Offline-Modus

Bevor Sie eine Wartung des TSM Middleware-Servers durchführen, der dazu führen kann, dass der Knoten „Archiv“ nicht mehr verfügbar ist, nehmen Sie die Zielkomponente offline, um die Anzahl der Alarme zu begrenzen, die ausgelöst werden, wenn der TSM Middleware-Server nicht mehr verfügbar ist.

Was Sie benötigen

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

Schritte

1. Wählen Sie **SUPPORT > Tools > Grid-Topologie** aus.
2. Wählen Sie **Archivknoten ARC Ziel Konfiguration Main**.
3. Ändern Sie den Wert für Tivoli Storage Manager Status in **Offline** und klicken Sie auf **Änderungen anwenden**.
4. Nachdem die Wartung abgeschlossen ist, ändern Sie den Wert des Tivoli Storage Manager-Status in **Online** und klicken Sie auf **Änderungen übernehmen**.

Administrative Tools für Tivoli Storage Manager

Das `dsmadm`-Tool ist die Administrationskonsole für den TSM Middleware-Server, der auf dem Archiv-Knoten installiert ist. Sie können auf das Tool zugreifen, indem Sie eingeben `dsmadm` In der Befehlszeile des Servers. Melden Sie sich an der Verwaltungskonsole mit demselben administrativen Benutzernamen und Kennwort an, das für den ARC-Dienst konfiguriert ist.

Der `tsmquery.rb` Skript wurde erstellt, um Statusinformationen aus `dsmadm` in lesbarer Form zu generieren. Sie können dieses Skript ausführen, indem Sie den folgenden Befehl in der Befehlszeile des Archiv-Knotens eingeben: `/usr/local/arc/tsmquery.rb status`

Weitere Informationen zur TSM Administrationskonsole dsmadm finden Sie im *Tivoli Storage Manager für Linux: Administrator's Reference*.

Objekt dauerhaft nicht verfügbar

Wenn der Archivknoten ein Objekt vom Tivoli Storage Manager (TSM)-Server anfordert und der Abruf fehlschlägt, versucht der Archivknoten die Anforderung nach einem Intervall von 10 Sekunden erneut. Wenn das Objekt dauerhaft nicht verfügbar ist (z. B. weil das Objekt auf Band beschädigt ist), kann die TSM-API dies nicht auf den Archiv-Node hinweisen, sodass der Archivknoten die Anforderung weiterhin erneut versucht.

Wenn diese Situation eintritt, wird ein Alarm ausgelöst, und der Wert steigt weiter. Um den Alarm anzuzeigen, wählen Sie **SUPPORT Tools Grid-Topologie**. Wählen Sie dann **Archiv-Knoten ARC Abrufen Fehler anfordern**.

Wenn das Objekt dauerhaft nicht verfügbar ist, müssen Sie das Objekt identifizieren und die Anfrage des Archivierungs-Nodes manuell abbrechen, wie in der Prozedur beschrieben. [Bestimmen, ob Objekte dauerhaft nicht verfügbar sind](#).

Ein Abruf kann auch fehlschlagen, wenn das Objekt vorübergehend nicht verfügbar ist. In diesem Fall sollten nachfolgende Abrufanfragen erfolgreich sein.

Wenn das StorageGRID System so konfiguriert ist, dass eine ILM-Regel verwendet wird, die eine einzelne Objektkopie erstellt und die Kopie nicht abgerufen werden kann, geht das Objekt verloren und kann nicht wiederhergestellt werden. Sie müssen jedoch weiterhin das Verfahren befolgen, um festzustellen, ob das Objekt zum Entfernen von`` zum StorageGRID-System dauerhaft nicht verfügbar ist, zum Abbrechen der Anfrage des Archivknotens und zum Löschen von Metadaten für das verlorene Objekt.

Bestimmen, ob Objekte dauerhaft nicht verfügbar sind

Sie können feststellen, ob Objekte dauerhaft nicht verfügbar sind, indem Sie eine Anforderung über die TSM-Administrationskonsole erstellen.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Über diese Aufgabe

Dieses Beispiel dient nur zu Ihren Informationen. Dieses Verfahren kann Ihnen nicht dabei helfen, alle Ausfallbedingungen zu identifizieren, die zu nicht verfügbaren Objekten oder Bandvolumes führen können. Informationen zur TSM-Administration finden Sie in der TSM-Server-Dokumentation.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Identifizieren Sie das Objekt oder die Objekte, die nicht vom Archiv-Node abgerufen werden konnten:
 - a. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält: `cd /var/local/audit/export`

Die aktive Audit-Log-Datei heißt `Audit.log`. Einmal am Tag, die aktive `audit.log` Die Datei wird gespeichert und eine neue `audit.log` Datei wird gestartet. Der Name der gespeicherten Datei gibt

an, wann sie gespeichert wurde, im Format `yyyy-mm-dd.txt`. Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, Die das ursprüngliche Datum bewahrt.

- b. Durchsuchen Sie die entsprechende Audit-Log-Datei nach Meldungen, die darauf hinweisen, dass ein archiviertes Objekt nicht abgerufen werden konnte. Geben Sie beispielsweise Folgendes ein: `grep ARCE audit.log | less -n`

Wenn ein Objekt nicht von einem Archiv-Node abgerufen werden kann, zeigt die ARCE-Überwachungsmeldung (Archivobjekt Retrieve End) IM Ergebnisfeld ARUN (nicht verfügbare Archiv-Middleware) oder GERR (allgemeiner Fehler) an. Die folgende Beispielzeile aus dem Audit-Protokoll zeigt, dass die ARCE-Meldung mit dem Ergebnis ARUN für CBID 498D8A1F681F05B3 beendet wurde.

```
[AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):20091127][RSLT(FC32):ARUN][AVER(UI32):7]
[ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][AMID(FC32):ARCI]
[ATID(UI64):4560349751312520631]]
```

Weitere Informationen finden Sie in den Anweisungen zum Verständnis von Überwachungsmeldungen.

- c. Notieren Sie die CBID jedes Objekts, bei dem ein Anforderungsfehler auftritt.

Möglicherweise möchten Sie auch die folgenden zusätzlichen Informationen aufzeichnen, die vom TSM zur Identifizierung von Objekten verwendet werden, die vom Archiv-Node gespeichert wurden:

- **Dateiplatzname:** Entspricht der Archiv-Knoten-ID. Um die Archiv-Knoten-ID zu finden, wählen Sie **SUPPORT Tools Grid-Topologie**. Wählen Sie dann **Archiv-Node ARC Ziel Übersicht**.
- **Hoher Level Name:** Entspricht der Volume-ID, die dem Objekt durch den Archiv-Node zugewiesen wurde. Die Volume-ID hat die Form eines Datums (z. B. 20091127), und wird als VLID des Objekts in Archiv-Audit-Nachrichten aufgezeichnet.
- **Name der unteren Ebene:** Entspricht der CBID, die einem Objekt vom StorageGRID-System zugewiesen wurde.

- d. Melden Sie sich aus der Befehlsshell ab: `exit`

3. Überprüfen Sie den TSM-Server, ob die in Schritt 2 identifizierten Objekte dauerhaft nicht verfügbar sind:

- a. Melden Sie sich bei der Administrationskonsole des TSM-Servers an: `dsmadm`

Verwenden Sie den für den ARC-Dienst konfigurierten administrativen Benutzernamen und das für den ARC-Dienst konfigurierte Passwort. Geben Sie den Benutzernamen und das Kennwort in den Grid Manager ein. (Um den Benutzernamen anzuzeigen, wählen Sie **SUPPORT Tools Grid-Topologie**. Wählen Sie dann **Archiv-Node ARC Ziel Konfiguration**.)

- b. Stellen Sie fest, ob das Objekt dauerhaft nicht verfügbar ist.

Beispielsweise können Sie im TSM-Aktivitätsprotokoll nach einem Datenintegritätsfehler für das Objekt suchen. Das folgende Beispiel zeigt eine Suche des Aktivitätsprotokolls für den letzten Tag nach einem Objekt mit CBID 498D8A1F681F05B3.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

Je nach Art des Fehlers kann die CBID nicht im TSM-Aktivitätsprotokoll aufgezeichnet werden. Zum Zeitpunkt des Fehlers der Anforderung müssen Sie möglicherweise das Protokoll nach anderen TSM-Fehlern durchsuchen.

- c. Wenn ein ganzes Band dauerhaft nicht verfügbar ist, identifizieren Sie die CBIDs für alle Objekte, die auf diesem Volume gespeichert sind: `query content TSM_Volume_Name`

Wo `TSM_Volume_Name` ist der TSM-Name für das nicht verfügbare Band. Im Folgenden finden Sie ein Beispiel für die Ausgabe dieses Befehls:

```
> query content TSM-Volume-Name
Node Name      Type Filespace  FSID Client's Name for File Name
-----
DEV-ARC-20     Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20     Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

Der Client's Name for File Name Entspricht der Archiv-Node-Volume-ID (oder TSM „High-Level Name“), gefolgt von der CBID des Objekts (oder TSM „Low-Level-Name“). Das ist, das Client's Name for File Name Nimmt das Formular an /Archive Node volume ID /CBID. In der ersten Zeile der Beispielausgabe wird der angezeigt Client's Name for File Name ist /20081201/ C1D172940E6C7E12.

Erinnern Sie sich auch daran, dass die Filespace ist die Knoten-ID des Archiv-Knotens.

Sie benötigen die CBID jedes auf dem Volume gespeicherten Objekts und die Node-ID des Archiv-Node, um die Anforderung zum Abrufen abzubrechen.

4. Brechen Sie bei jedem Objekt, das dauerhaft nicht verfügbar ist, die Abfrage ab, und geben Sie einen Befehl ein, um das StorageGRID System über den Verlust der Objektkopie zu informieren:



Verwenden Sie die ADE-Konsole vorsichtig. Wenn die Konsole nicht ordnungsgemäß verwendet wird, können Systemvorgänge und beschädigte Daten unterbrochen werden. Geben Sie Befehle sorgfältig ein, und verwenden Sie nur die in diesem Verfahren dokumentierten Befehle.

- a. Wenn Sie nicht bereits beim Archiv-Node angemeldet sind, melden Sie sich wie folgt 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:
- b. Zugriff auf die ADE-Konsole des ARC-Dienstes: `telnet localhost 1409`
- c. Abbrechen der Anfrage für das Objekt: `/proc/BRTR/cancel -c CBID`

Wo `CBID` Ist die Kennung des Objekts, das nicht vom TSM abgerufen werden kann.

Wenn sich die einzigen Kopien des Objekts auf Band befinden, wird die Anforderung „Bulk refrain“ mit einer Nachricht abgebrochen, „1 Requests stornierte“. Wenn Kopien des Objekts an anderer Stelle im System vorhanden sind, wird der Objektabruf durch ein anderes Modul verarbeitet, sodass die Antwort auf die Nachricht „0 Requests stornierte“ lautet.

- d. Geben Sie einen Befehl ein, um das StorageGRID System darüber zu informieren, dass eine Objektkopie verloren gegangen ist und dass weitere Kopien erstellt werden müssen:
`/proc/CMSI/Object_Lost CBID node_ID`

Wo `CBID` Ist die Kennung des Objekts, das nicht vom TSM-Server abgerufen werden kann, und `node_ID` Ist die Knoten-ID des Archiv-Knotens, bei dem der Abruf fehlgeschlagen ist.

Sie müssen einen separaten Befehl für jede verlorene Objektkopie eingeben: Die Eingabe eines Bereichs von CBIDs wird nicht unterstützt.

In den meisten Fällen erstellt das StorageGRID System sofort zusätzliche Kopien von Objektdaten, um sicherzustellen, dass die ILM-Richtlinie des Systems befolgt wird.

Wenn jedoch die ILM-Regel für das Objekt angegeben hat, dass nur eine Kopie erstellt wurde und nun verloren gegangen ist, kann das Objekt nicht wiederhergestellt werden. In diesem Fall die ausführen `Object_Lost` Der Befehl bereinigt die Metadaten des verlorenen Objekts aus dem StorageGRID System.

Wenn der `Object_Lost` Befehl wurde erfolgreich abgeschlossen, die folgende Meldung wird zurückgegeben:

```
CLOC_LOST_ANS returned result 'SUCS'
```

+



Der `/proc/CMSI/Object_Lost` Der Befehl ist nur für verlorene Objekte gültig, die auf Archiv-Knoten gespeichert sind.

- a. Verlassen Sie die ADE-Konsole: `exit`
 - b. Melden Sie sich vom Archiv-Knoten ab: `exit`
5. Zurücksetzen des Werts von Anfragefehlern im StorageGRID System:
- a. Gehen Sie zu **Archivknoten ARC Abruf Konfiguration**, und wählen Sie **Fehleranzahl der Anforderung zurücksetzen**.
 - b. Klicken Sie Auf **Änderungen Übernehmen**.

Verwandte Informationen

VMware: Virtuelle Maschine für automatischen Neustart konfigurieren

Wenn die virtuelle Maschine nach dem Neustart des VMware vSphere-Hypervisors nicht neu gestartet wird, müssen Sie die virtuelle Maschine möglicherweise für den automatischen Neustart konfigurieren.

Führen Sie diese Schritte aus, wenn Sie bemerken, dass eine virtuelle Maschine nicht neu gestartet wird, während Sie einen Grid-Knoten wiederherstellen oder einen anderen Wartungsvorgang ausführen.

Schritte

1. Wählen Sie in der VMware vSphere Client-Struktur die virtuelle Maschine aus, die nicht gestartet wurde.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, und wählen Sie **Einschalten**.
3. Konfigurieren Sie den VMware vSphere Hypervisor, um die virtuelle Maschine in Zukunft automatisch neu zu starten.

Verfahren für den Grid-Node

Möglicherweise müssen Sie auf einem bestimmten Grid-Node Verfahren durchführen. Sie können zwar einige dieser Verfahren im Grid Manager ausführen, jedoch müssen Sie bei den meisten Verfahren von der Befehlszeile des Knotens aus auf Server Manager zugreifen.

Server Manager wird auf jedem Grid-Knoten ausgeführt, um das Starten und Beenden von Diensten zu überwachen und sicherzustellen, dass Dienste problemlos dem StorageGRID-System beitreten und das System verlassen. Server Manager überwacht auch die Dienste auf jedem Grid-Knoten und versucht automatisch, alle Services, die Fehler melden, neu zu starten.



Sie sollten auf Server Manager zugreifen, wenn Sie von technischem Support dazu aufgefordert wurden.



Sie müssen die aktuelle Shell-Sitzung des Befehls schließen und sich ausloggen, nachdem Sie mit Server Manager fertig sind. Geben Sie Ein: `exit`

Zeigen Sie den Status und die Version von Server Manager an

Für jeden Grid-Node können Sie den aktuellen Status und die Version des auf diesem Grid-Node ausgeführten Server Managers anzeigen. Zudem erhalten Sie den aktuellen Status aller auf diesem Grid-Node ausgeführten Services.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. 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 `#`.

2. Anzeigen des aktuellen Status von Server Manager, der auf dem Grid-Node ausgeführt wird: **`service servermanager status`**

Der aktuelle Status von Server Manager, der auf dem Grid-Knoten ausgeführt wird, wird gemeldet (wird ausgeführt oder nicht). Wenn der Status von Server Manager lautet `running`, Die Zeit, die es seit dem letzten Start läuft, ist aufgelistet. Beispiel:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Zeigen Sie die aktuelle Version von Server Manager an, der auf einem Grid-Node ausgeführt wird: **`service servermanager version`**

Die aktuelle Version wird aufgelistet. Beispiel:

```
11.1.0-20180425.1905.39c9493
```

4. Melden Sie sich aus der Befehlsshell ab: **`exit`**

Den aktuellen Status aller Dienste anzeigen

Sie können jederzeit den aktuellen Status aller auf einem Grid-Node ausgeführten Services anzeigen.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. 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 `#`.

2. Status aller auf dem Grid-Node ausgeführten Services anzeigen: `storagegrid-status`

Beispielsweise zeigt die Ausgabe für den primären Admin-Node den aktuellen Status der AMS-, CMN- und

NMS-Dienste als ausgeführt an. Diese Ausgabe wird sofort aktualisiert, wenn sich der Status eines Dienstes ändert.

Host Name	190-ADM1	
IP Address		
Operating System Kernel	4.9.0	Verified
Operating System Environment	Debian 9.4	Verified
StorageGRID Webscale Release	11.1.0	Verified
Networking		Verified
Storage Subsystem		Verified
Database Engine	5.5.9999+default	Running
Network Monitoring	11.1.0	Running
Time Synchronization	1:4.2.8p10+dfsg	Running
ams	11.1.0	Running
cmn	11.1.0	Running
nms	11.1.0	Running
ssm	11.1.0	Running
mi	11.1.0	Running
dynip	11.1.0	Running
nginx	1.10.3	Running
tomcat	8.5.14	Running
grafana	4.2.0	Running
mgmt api	11.1.0	Running
prometheus	1.5.2+ds	Running
persistence	11.1.0	Running
ade exporter	11.1.0	Running
attrDownPurge	11.1.0	Running
attrDownSampl	11.1.0	Running
attrDownSamp2	11.1.0	Running
node exporter	0.13.0+ds	Running

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Optional können Sie einen statischen Bericht für alle Dienste anzeigen, die auf dem Grid-Node ausgeführt werden: `/usr/local/servermanager/reader.rb`

Dieser Bericht enthält dieselben Informationen wie der ständig aktualisierte Bericht, wird jedoch nicht aktualisiert, wenn sich der Status eines Dienstes ändert.

5. Melden Sie sich aus der Befehlsshell ab: `exit`

Starten Sie Server Manager und alle Dienste

Möglicherweise müssen Sie Server Manager starten, der auch alle Dienste auf dem Grid-Knoten startet.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Der Start von Server Manager auf einem Grid-Knoten, auf dem er bereits ausgeführt wird, führt zu einem Neustart des Server-Managers und aller Dienste auf dem Grid-Knoten.

Schritte

1. 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 `#`.

2. Server Manager Starten: `service servermanager start`

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Starten Sie Server Manager und alle Services neu

Möglicherweise müssen Sie den Server-Manager und alle Dienste, die auf einem Grid-Knoten ausgeführt werden, neu starten.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. 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 `#`.

2. Starten Sie Server Manager und alle Services auf dem Grid-Knoten neu: `service servermanager restart`

Server Manager und alle Dienste auf dem Grid-Knoten werden angehalten und dann neu gestartet.



Verwenden der `restart` Der Befehl ist der gleiche wie mit dem `stop` Befehl gefolgt vom `start` Befehl.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Beenden Sie Server Manager und alle Dienste

Server Manager ist dafür gedacht, immer ausgeführt zu werden, aber möglicherweise müssen Sie Server Manager und alle Dienste, die auf einem Grid-Knoten ausgeführt werden, anhalten.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. 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 `#`.

2. Stoppen Sie Server Manager und alle Services, die auf dem Grid-Knoten ausgeführt werden: `service servermanager stop`

Server Manager und alle auf dem Grid-Knoten ausgeführten Dienste werden ordnungsgemäß beendet. Das Herunterfahren des Services kann bis zu 15 Minuten dauern.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Zeigt den aktuellen Servicestatus an

Sie können jederzeit den aktuellen Status einer auf einem Grid-Node ausgeführten Services anzeigen.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. 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 `#`.

2. Den aktuellen Status eines Dienstes anzeigen, der auf einem Grid-Knoten ausgeführt wird:
Service_servicename_ Status der aktuelle Status des angeforderten Dienstes, der auf dem Grid-Knoten ausgeführt wird, wird gemeldet (wird ausgeführt oder nicht). Beispiel:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Melden Sie sich aus der Befehlsshell ab: **exit**

Dienst stoppen

Einige Wartungsvorgänge erfordern, dass Sie einen einzelnen Service beenden und gleichzeitig andere Services auf dem Grid-Node ausgeführt werden. Stoppen Sie nur einzelne Dienste, wenn Sie dazu durch ein Wartungsverfahren angewiesen werden.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Wenn Sie mit diesen Schritten einen Dienst „administrativ stoppen“ beenden, startet der Server Manager den Dienst nicht automatisch neu. Sie müssen entweder den einzelnen Dienst manuell starten oder Server Manager neu starten.

Wenn Sie den LDR-Dienst auf einem Speicherknoten anhalten müssen, beachten Sie, dass es möglicherweise eine Weile dauern kann, bis der Dienst beendet wird, wenn aktive Verbindungen vorhanden sind.

Schritte

1. Melden Sie sich beim Grid-Node an:

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

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

2. Beenden eines einzelnen Dienstes: `service servicename stop`

Beispiel:

```
service ldr stop
```



Der Service kann bis zu 11 Minuten dauern.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

[Dienst zum Beenden erzwingen](#)

Stellen Sie das Gerät in den Wartungsmodus

Sie müssen das Gerät in den Wartungsmodus versetzen, bevor Sie bestimmte Wartungsarbeiten durchführen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Berechtigung Wartung oder Stammzugriff. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Über diese Aufgabe

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.



Das Passwort des Admin-Kontos und die SSH-Host-Schlüssel für eine StorageGRID-Appliance im Wartungsmodus bleiben identisch mit dem Kennwort, das zum Zeitpunkt der Wartung der Appliance vorhanden war.

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Strukturansicht der Seite Knoten den Appliance Storage Node aus.
3. Wählen Sie **Aufgaben**.

Overview Hardware Network Storage Objects ILM **Tasks**

Reboot

Reboots the node. [Reboot](#)

Maintenance mode

Places the appliance's compute controller into maintenance mode. [Maintenance mode](#)

4. Wählen Sie **Wartungsmodus**.

Ein Bestätigungsdialogfeld wird angezeigt.

⚠ **Enter maintenance mode on S2-10-224-2-24** ✕

You must place the appliance's compute controller into maintenance mode to perform certain maintenance procedures on the appliance.

Attention: All StorageGRID services on this node will be shut down. Wait a few minutes for the node to reboot into maintenance mode.

If you are ready to start, enter the provisioning passphrase and select OK.

Provisioning passphrase

.....

[Cancel](#) [OK](#)

5. Geben Sie die Provisionierungs-Passphrase ein, und wählen Sie **OK**.

Eine Fortschrittsleiste und eine Reihe von Meldungen, darunter „Anfrage gesendet“, „StorageGRID stoppen“ und „neu booten“, geben an, dass die Appliance die Schritte zum Eintritt in den Wartungsmodus abschließt.

S2-10-224-2-24 (Storage Node)

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

Reboot

Reboots the node.

Reboot

Maintenance mode

Places the appliance's compute controller into maintenance mode.

Maintenance mode

 **Attention**

Your request has been sent, but the appliance might take 10-15 minutes to enter maintenance mode. **Do not perform maintenance procedures until this tab indicates maintenance mode is ready, or data could become corrupted.**

  Rebooting...

Wenn sich die Appliance im Wartungsmodus befindet, wird in einer Bestätigungsmeldung die URLs aufgeführt, mit denen Sie auf das Installationsprogramm der StorageGRID-Appliance zugreifen können.

S2-10-224-2-24 (Storage Node)

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

Reboot

Reboots the node.

Reboot

Maintenance mode

Places the appliance's compute controller into maintenance mode.

Maintenance mode

 This node is currently in maintenance mode. Navigate to one of the URLs listed below and perform any necessary maintenance procedures.

- <https://172.16.2.24:8443>
- <https://10.224.2.24:8443>

When you are done with any required maintenance procedures, you must exit maintenance mode by selecting Reboot Controller from the StorageGRID Appliance Installer.

- Um auf das Installationsprogramm der StorageGRID-Appliance zuzugreifen, navigieren Sie zu einer beliebigen der angezeigten URLs.

Verwenden Sie nach Möglichkeit die URL, die die IP-Adresse des Admin Network-Ports der Appliance enthält.

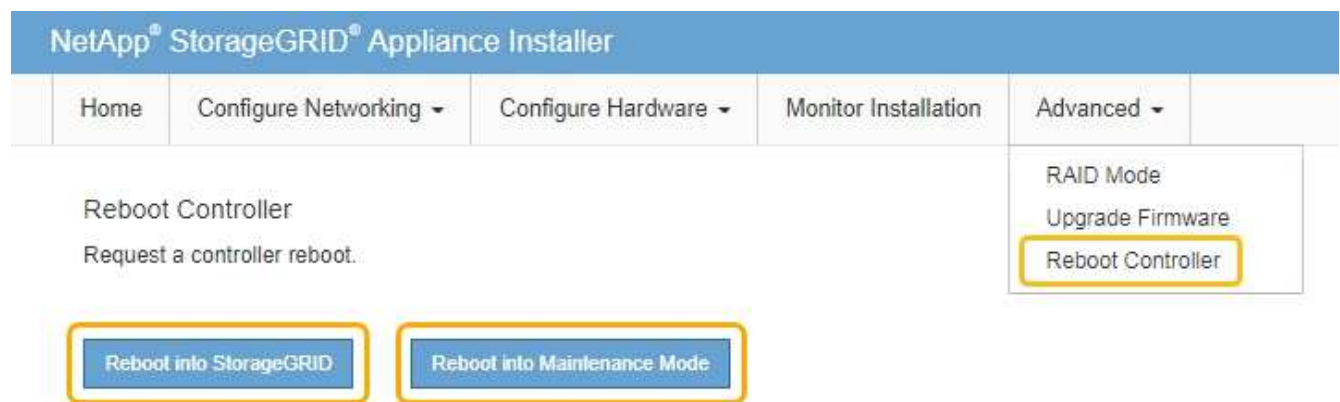


Zugriff Auf <https://169.254.0.1:8443> Erfordert eine direkte Verbindung zum lokalen Management-Port.

7. Vergewissern Sie sich beim Installationsprogramm der StorageGRID Appliance, dass sich die Appliance im Wartungsmodus befindet.

This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to [reboot](#) the controller.

8. Führen Sie alle erforderlichen Wartungsaufgaben durch.
9. Beenden Sie nach Abschluss der Wartungsaufgaben den Wartungsmodus und fahren Sie den normalen Node-Betrieb fort. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Erweitert Controller neu starten** und wählen Sie dann **Neustart in StorageGRID** aus.



Die Appliance kann bis zu 20 Minuten dauern, bis sie neu gestartet und wieder in das Grid eingesetzt wird. Um zu überprüfen, ob das Neubooten abgeschlossen ist und dass der Node wieder dem Grid beigetreten ist, gehen Sie zurück zum Grid Manager. Die Seite **Nodes** sollte einen normalen Status (keine Symbole links neben dem Knotennamen) für den Appliance-Knoten anzeigen, der angibt, dass keine Warnmeldungen aktiv sind und der Knoten mit dem Raster verbunden ist.

Nodes

View the list and status of sites and grid nodes.

Search... Q Total node count: 14

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	—	—	2%
DC1-G1	Gateway Node	—	—	2%
DC1-S1	Storage Node	0%	0%	12%
DC1-S2	Storage Node	0%	0%	11%
DC1-S3	Storage Node	0%	0%	11%

Dienst zum Beenden erzwingen

Wenn Sie einen Dienst sofort beenden müssen, können Sie den verwenden `force-stop` Befehl.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

- Melden Sie sich beim Grid-Node an:
 - Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

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

- Erzwingen Sie den Dienst manuell zum Beenden: `service servicename force-stop`

Beispiel:

```
service ldr force-stop
```


Das System wartet 30 Sekunden, bevor der Dienst beendet wird.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Dienst starten oder neu starten

Möglicherweise müssen Sie einen Dienst starten, der angehalten wurde, oder Sie müssen einen Dienst anhalten und neu starten.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

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

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

2. Entscheiden Sie, welcher Befehl das Problem verursacht, basierend darauf, ob der Service derzeit ausgeführt oder angehalten ist.

- Wenn der Dienst derzeit angehalten ist, verwenden Sie das `start` Befehl zum manuellen Starten des Dienstes: `service servicename start`

Beispiel:

```
service ldr start
```

- Wenn der Dienst derzeit ausgeführt wird, verwenden Sie das `restart` Befehl, um den Dienst zu beenden und ihn dann neu zu starten: `service servicename restart`

Beispiel:

```
service ldr restart
```

+



Verwenden der `restart` Der Befehl ist der gleiche wie mit dem `stop` Befehl gefolgt vom `start` Befehl. Sie können ein Problem lösen `restart` Selbst wenn der Dienst derzeit angehalten ist.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Entfernen Sie die Port-Remaps

Wenn Sie einen Endpunkt für den Load Balancer-Dienst konfigurieren möchten und einen Port verwenden möchten, der bereits als Port mit dem Port einer Port-Remap konfiguriert wurde, müssen Sie zunächst die vorhandene Port-Remap entfernen, oder der Endpunkt ist nicht wirksam. Sie müssen auf jedem Admin-Node und Gateway-Node ein Skript ausführen, das über widersprüchliche neu zugeordnete Ports verfügt, um alle Port-Remaps des Node zu entfernen.



Über diese Aufgabe

Durch dieses Verfahren werden alle Port-Remaps entfernt. Wenden Sie sich an den technischen Support, wenn Sie einige der Rückpläne aufbewahren müssen.

Informationen über das Konfigurieren von Endpunkten für den Load Balancer finden Sie in den Anweisungen zur Verwaltung von StorageGRID.



Wenn die Port-Remap Client-Zugriff bietet, sollte der Client neu konfiguriert werden, um einen anderen Port zu verwenden, der, wenn möglich, als Load Balancer-Endpunkt konfiguriert ist, um einen Serviceverlust zu vermeiden, andernfalls führt das Entfernen der Port-Zuordnung zu einem Verlust des Client-Zugriffs und sollte entsprechend geplant werden.



Dieses Verfahren ist bei einem StorageGRID System, das als Container auf Bare-Metal-Hosts bereitgestellt wird, nicht möglich. Siehe Anweisungen für [Entfernen von Port-Remaps auf Bare-Metal-Hosts](#).

Schritte

1. Melden Sie sich bei dem Node an.

a. Geben Sie den folgenden Befehl ein: `ssh -p 8022 admin@node_IP`

Port 8022 ist der SSH-Port des Basis-OS, während Port 22 der SSH-Port der Container-Engine ist, auf der StorageGRID ausgeführt wird.

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 `#`.

2. Führen Sie das folgende Skript aus: `remove-port-remap.sh`

3. Booten Sie den Node neu.

Befolgen Sie die Anweisungen für [Neubooten eines Grid-Node](#).

4. Wiederholen Sie diese Schritte auf jedem Admin-Node und Gateway-Node mit gegensätzlichen neu zugeordneten Ports.

Verwandte Informationen

[StorageGRID verwalten](#)

Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts

Wenn Sie einen Endpunkt für den Load Balancer-Dienst konfigurieren möchten und einen Port verwenden möchten, der bereits als Port mit dem Port einer Port-Remap konfiguriert wurde, müssen Sie zunächst die vorhandene Port-Remap entfernen, oder der Endpunkt ist nicht wirksam. Wenn Sie StorageGRID auf Bare-Metal-Hosts ausführen, führen Sie dieses Verfahren anstelle des allgemeinen Verfahrens zum Entfernen von Port-Remaps durch. Sie müssen die Node-Konfigurationsdatei für jeden Admin-Node und Gateway-Node bearbeiten, der über widersprüchliche neu zugeordnete Ports verfügt, um alle Port-Neuzuordnungen des Node zu entfernen und den Node neu zu starten.



Über diese Aufgabe

Durch dieses Verfahren werden alle Port-Remaps entfernt. Wenden Sie sich an den technischen Support, wenn Sie einige der Rückpläne aufbewahren müssen.

Informationen über das Konfigurieren von Endpunkten für den Load Balancer finden Sie in den Anweisungen zur Verwaltung von StorageGRID.



Dieses Verfahren kann zu einem vorübergehenden Serviceverlust führen, wenn Knoten neu gestartet werden.

Schritte

1. Melden Sie sich bei dem Host an, der den Node unterstützt. Melden Sie sich als root oder mit einem Konto an, das über sudo-Berechtigung verfügt.
2. Führen Sie den folgenden Befehl aus, um den Node vorübergehend zu deaktivieren: `sudo storagegrid node stop node-name`
3. Bearbeiten Sie mithilfe eines Texteditors wie vim oder pico die Konfigurationsdatei des Knotens für den Knoten.

Die Konfigurationsdatei des Knotens ist unter zu finden `/etc/storagegrid/nodes/node-name.conf`.

4. Suchen Sie den Abschnitt der Node-Konfigurationsdatei, die die Port-Zuordnungen enthält.

Siehe die letzten beiden Zeilen im folgenden Beispiel.

```

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443

```

5. BEARBEITEN Sie DIE Einträge PORT_REMAP und PORT_REMAP_INBOUND, um Port-Remaps zu entfernen.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Führen Sie den folgenden Befehl aus, um Ihre Änderungen an der Node-Konfigurationsdatei für den Node zu validieren: `sudo storagegrid node validate node-name`

Beheben Sie Fehler oder Warnungen, bevor Sie mit dem nächsten Schritt fortfahren.

7. Führen Sie den folgenden Befehl aus, um den Node ohne Port-Zuordnungen neu zu starten: `sudo storagegrid node start node-name`
8. Loggen Sie sich als Administrator beim Node mit dem im angegebenen Passwort ein `Passwords.txt` Datei:
9. Überprüfen Sie, ob die Dienste richtig starten.
 - a. Anzeigen einer Liste der Status aller Dienste auf dem Server: `sudo storagegrid-status`

Der Status wird automatisch aktualisiert.

b. Warten Sie, bis alle Dienste den Status „wird ausgeführt“ oder „verifiziert“ aufweisen.

c. Statusbildschirm verlassen:Ctrl+C

10. Wiederholen Sie diese Schritte auf jedem Admin-Node und Gateway-Node mit gegensätzlichen neu zugeordneten Ports.

Grid-Node neu booten

Sie können einen Grid-Node aus dem Grid Manager oder aus der Befehlshaber des Node neu booten.

Über diese Aufgabe

Beim Neubooten eines Grid-Node wird der Node heruntergefahren und neu gestartet. Alle Dienste werden automatisch neu gestartet.

Wenn Sie Storage-Nodes neu starten 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.

Verwandte Informationen

[StorageGRID verwalten](#)

Grid-Node aus Grid Manager neu booten

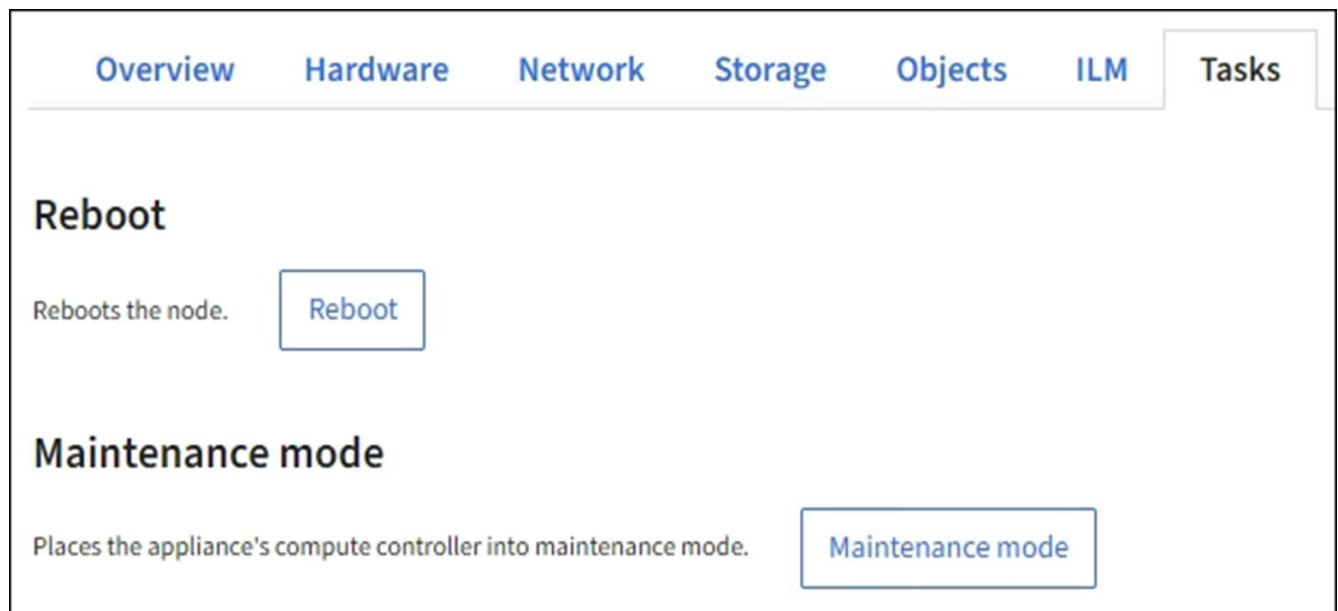
Beim Neubooten eines Grid-Node aus dem Grid Manager wird der Probleme auftreten `reboot` Befehl auf dem Ziel-Node.

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.

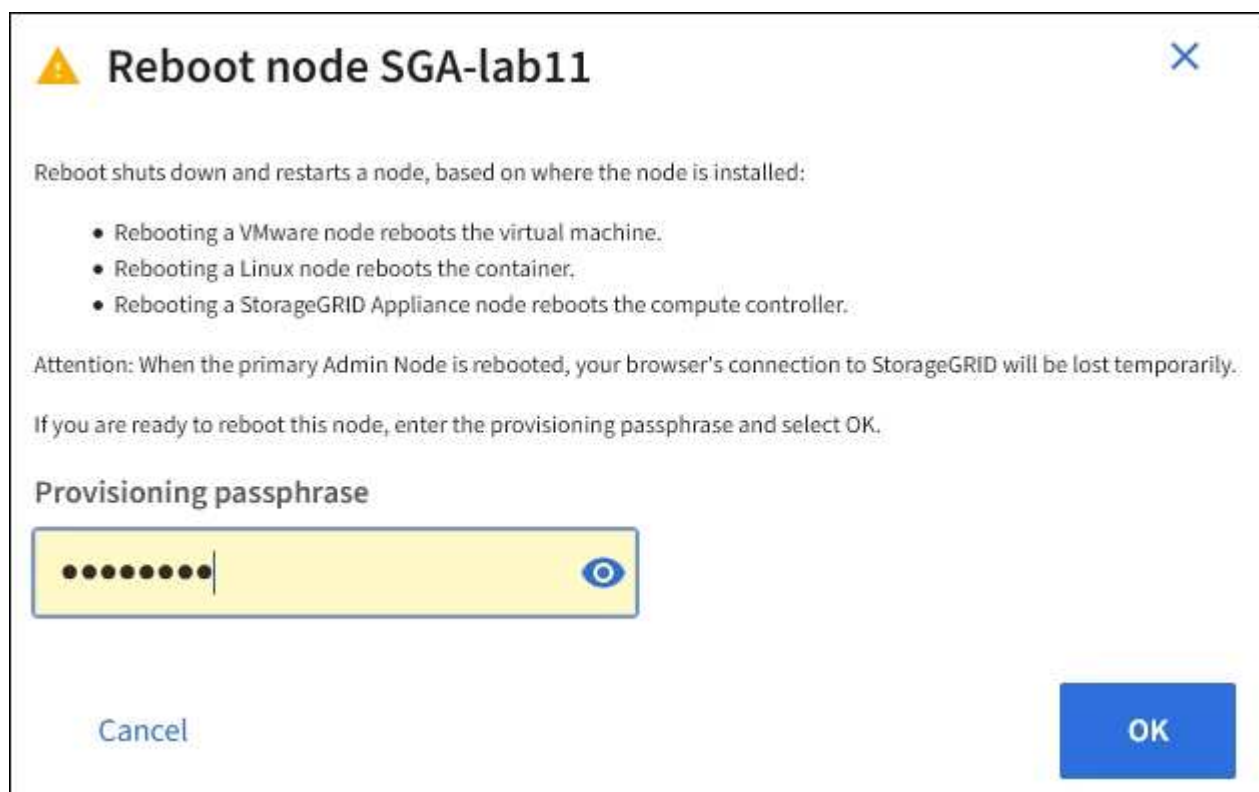
Schritte

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



4. Wählen Sie **Neustart**.

Ein Bestätigungsdialogfeld wird angezeigt.



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

5. Geben Sie die Provisionierungs-Passphrase ein, und klicken Sie auf **OK**.

6. Warten Sie, bis der Node neu gebootet wird.

Es kann einige Zeit dauern, bis Dienste heruntergefahren werden.

Wenn der Knoten neu gestartet wird, wird das graue Symbol (Administrativ Down) auf der linken Seite der Seite **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.

Grid-Node aus der Eingabeaufforderung neu booten

Wenn Sie den Neustart genauer überwachen müssen oder nicht auf den Grid Manager zugreifen können, können Sie sich beim Grid-Node anmelden und den Befehl `Server Manager reboot` über die Befehlszeile ausführen.

Sie müssen die haben `Passwords.txt` Datei:

1. 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 `#`.

2. Optional Dienste beenden: `service servermanager stop`

Das Beenden von Diensten ist ein optionaler, aber empfohlener Schritt. Die Services können bis zu 15 Minuten zum Herunterfahren dauern. Möglicherweise möchten Sie sich beim System per Remote-Zugriff anmelden, um den Shutdown-Prozess zu überwachen, bevor Sie im nächsten Schritt den Node neu booten.

3. Booten Sie den Grid-Node neu: `reboot`
4. Melden Sie sich aus der Befehlsshell ab: `exit`

Fahren Sie den Grid-Node herunter

Sie können einen Grid-Node über die Befehlshaber des Node herunterfahren.

Was Sie benötigen

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

Über diese Aufgabe

Bevor Sie dieses Verfahren durchführen, sollten Sie folgende Punkte beachten:

- Im Allgemeinen sollten Sie nicht mehr als einen Node gleichzeitig herunterfahren, um Unterbrechungen zu vermeiden.
- Schalten Sie einen Node während eines Wartungsvorgangs nicht herunter, es sei denn, er wird ausdrücklich von der Dokumentation oder vom technischen Support dazu aufgefordert.

- Das Herunterfahren basiert auf dem Installationsort des Node, wie folgt:
 - Durch das Herunterfahren eines VMware-Knotens wird die virtuelle Maschine heruntergefahren.
 - Durch das Herunterfahren eines Linux-Node wird der Container heruntergefahren.
 - Durch das Herunterfahren eines StorageGRID-Appliance-Node wird der Computing-Controller heruntergefahren.
- Wenn Sie planen, mehr als einen Storage-Node an einem Standort herunterzufahren, beenden Sie die Aufnahme von Objekten an diesem Standort ca. eine Stunde lang, bevor Sie die Nodes herunterfahren.

Wenn eine ILM-Regel die **Dual Commit**-Aufnahmeoption verwendet (oder wenn eine Regel die Option **symmetrisch** verwendet und alle erforderlichen Kopien nicht sofort erstellt werden können), setzt StorageGRID alle neu aufgenommenen Objekte sofort auf zwei Storage-Nodes an demselben Standort und wertet ILM später aus. Wenn mehr als ein Storage-Node an einem Standort heruntergefahren wird, sind Sie möglicherweise während des Herunterfahrens nicht in der Lage, auf neu aufgenommene Objekte zuzugreifen. Schreibvorgänge können auch fehlschlagen, wenn am Standort zu wenige Speicherknoten verfügbar bleiben.

Schritte

1. 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 `#`.

2. Beenden Sie alle Dienste: `service servermanager stop`

Die Dienste können bis zu 15 Minuten zum Herunterfahren dauern. Außerdem können Sie sich möglicherweise per Remote-Zugriff beim System anmelden, um den Shutdown-Prozess zu überwachen.

3. Wenn der Node auf einer virtuellen VMware-Maschine ausgeführt wird oder er ein Appliance-Node ist, geben Sie den Befehl zum Herunterfahren aus: `shutdown -h now`

Führen Sie diesen Schritt unabhängig vom Ergebnis des aus `service servermanager stop` Befehl.



Nachdem Sie das ausstellen `shutdown -h now` Befehl auf einem Appliance-Node müssen Sie die Appliance aus- und wieder einschalten, um den Node neu zu starten.

Bei diesem Befehl wird der Controller heruntergefahren, das Gerät ist jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

4. Wenn Sie einen Appliance-Node herunterfahren:
 - Für die SG100- oder SG1000-Services-Appliance
 - i. Schalten Sie das Gerät aus.
 - ii. Warten Sie, bis die blaue Betriebs-LED erlischt.
 - Für das SG6000-Gerät

- i. Warten Sie, bis die grüne LED Cache Active auf der Rückseite der Storage Controller ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- ii. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.

- Für die SG5700 Appliance

- i. Warten Sie, bis die grüne LED Cache Active auf der Rückseite des Storage Controllers ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- ii. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.

Verwandte Informationen

[StorageGRID verwalten](#)

Schalten Sie den Host aus

Bevor Sie einen Host herunterfahren, müssen Sie Dienste auf allen Grid-Nodes auf diesem Host anhalten.

Schritte

1. 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 `#`.

2. Beenden Sie alle auf dem Knoten ausgeführten Services: `service servermanager stop`

Die Dienste können bis zu 15 Minuten zum Herunterfahren dauern. Außerdem können Sie sich möglicherweise per Remote-Zugriff beim System anmelden, um den Shutdown-Prozess zu überwachen.

3. Wiederholen Sie die Schritte 1 und 2 für jeden Knoten auf dem Host.

4. Wenn Sie einen Linux-Host haben:

- a. Melden Sie sich beim Host-Betriebssystem an.
- b. Stoppen Sie den Knoten: `storagegrid node stop`
- c. Fahren Sie das Host-Betriebssystem herunter.

5. Wenn der Node auf einer virtuellen VMware-Maschine ausgeführt wird oder er ein Appliance-Node ist, geben Sie den Befehl zum Herunterfahren aus: `shutdown -h now`

Führen Sie diesen Schritt unabhängig vom Ergebnis des `service servermanager stop` Befehl.



Nachdem Sie das ausstellen `shutdown -h now` Befehl auf einem Appliance-Node müssen Sie die Appliance aus- und wieder einschalten, um den Node neu zu starten.

Bei diesem Befehl wird der Controller heruntergefahren, das Gerät ist jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

6. Wenn Sie einen Appliance-Node herunterfahren:

- Für die SG100- oder SG1000-Services-Appliance
 - i. Schalten Sie das Gerät aus.
 - ii. Warten Sie, bis die blaue Betriebs-LED erlischt.
- Für das SG6000-Gerät
 - i. Warten Sie, bis die grüne LED Cache Active auf der Rückseite der Storage Controller ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- ii. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.
- Für die SG5700 Appliance
 - i. Warten Sie, bis die grüne LED Cache Active auf der Rückseite des Storage Controllers ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- ii. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.

7. Melden Sie sich aus der Befehlsshell ab: `exit`

Verwandte Informationen

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

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

Schalten Sie alle Knoten im Grid aus und wieder ein

Möglicherweise müssen Sie Ihr gesamtes StorageGRID System herunterfahren, wenn Sie ein Datacenter verschieben. Diese Schritte bieten einen allgemeinen Überblick über die empfohlene Sequenz für ein kontrolliertes Herunterfahren und Starten.

Wenn Sie alle Nodes an einem Standort oder Grid ausschalten, können Sie nicht auf aufgenommene Objekte zugreifen, während die Storage-Nodes offline sind.

Stoppen Sie Services und fahren Sie die Grid-Nodes herunter

Bevor Sie ein StorageGRID System ausschalten können, müssen Sie alle Services, die auf jedem Grid-Node ausgeführt werden, anhalten und anschließend alle VMware Virtual

Machines, Container-Engines und StorageGRID Appliances herunterfahren.

Über diese Aufgabe

Stoppen Sie zuerst die Dienste auf Admin-Nodes und API-Gateway-Knoten, und stoppen Sie dann die Dienste auf Storage-Nodes.

Dieser Ansatz ermöglicht Ihnen, den primären Admin-Knoten so lange wie möglich zu verwenden, um den Status der anderen Grid-Knoten zu überwachen.



Wenn ein einzelner Host mehr als einen Grid-Node enthält, fahren Sie den Host erst herunter, wenn Sie alle Nodes auf diesem Host angehalten haben. Wenn der Host den primären Admin-Node enthält, fahren Sie diesen Host zuletzt herunter.



Bei Bedarf können Sie dies tun [Migrieren Sie Nodes von einem Linux-Host zu einem anderen](#) Hostwartung ohne Auswirkungen auf die Funktionalität oder Verfügbarkeit des Grids durchführen.

Schritte

1. Beenden Sie alle Client-Applikationen vom Zugriff auf das Grid.
2. Melden Sie sich bei jedem Gateway-Knoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
 - b. Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführten Passwort ein `Passwords.txt` Datei:

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

3. Beenden Sie alle Dienste, die auf dem Knoten ausgeführt werden: `service servermanager stop`

Die Dienste können bis zu 15 Minuten zum Herunterfahren dauern. Außerdem können Sie sich möglicherweise per Remote-Zugriff beim System anmelden, um den Shutdown-Prozess zu überwachen.

4. Wiederholen Sie die beiden vorherigen Schritte, um die Dienste auf allen Speicherknoten, den Knoten Archiv und nicht-primären Admin-Knoten anzuhalten.

Sie können die Dienste auf diesen Knoten in beliebiger Reihenfolge anhalten.



Wenn Sie das ausgegeben `service servermanager stop` Befehl zum Beenden der Dienste auf einem Appliance-Speicherknoten müssen Sie die Appliance aus- und wieder einschalten, um den Node neu zu starten.

5. Wiederholen Sie für den primären Admin-Knoten die Schritte für [Anmeldung beim Node](#) Und [Anhalten aller Dienste auf dem Knoten](#).
6. Für Knoten, die auf Linux-Hosts ausgeführt werden:
 - a. Melden Sie sich beim Host-Betriebssystem an.
 - b. Stoppen Sie den Knoten: `storagegrid node stop`
 - c. Fahren Sie das Host-Betriebssystem herunter.

7. Geben Sie für Knoten, die auf VMware Virtual Machines und für Appliance Storage Nodes ausgeführt werden, den Befehl shutdown aus: `shutdown -h now`

Führen Sie diesen Schritt unabhängig vom Ergebnis des `service servermanager stop` Befehl.

Bei diesem Befehl wird der Compute-Controller heruntergefahren, das Gerät ist jedoch weiterhin eingeschaltet. Sie müssen den nächsten Schritt abschließen.

8. Wenn Sie Appliance-Nodes haben:

- Für die SG100- oder SG1000-Services-Appliance
 - i. Schalten Sie das Gerät aus.
 - ii. Warten Sie, bis die blaue Betriebs-LED erlischt.
- Für das SG6000-Gerät
 - i. Warten Sie, bis die grüne LED Cache Active auf der Rückseite der Storage Controller ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- ii. Schalten Sie das Gerät aus und warten Sie, bis die blaue Strom-LED ausgeschaltet ist.
- Für die SG5700 Appliance
 - i. Warten Sie, bis die grüne LED Cache Active auf der Rückseite des Storage Controllers ausgeschaltet ist.

Diese LED leuchtet, wenn zwischengespeicherte Daten auf die Laufwerke geschrieben werden müssen. Sie müssen warten, bis diese LED ausgeschaltet ist, bevor Sie den Strom ausschalten.

- ii. Schalten Sie das Gerät aus und warten Sie, bis alle LED- und siebensegmentreichen Anzeigeaktivitäten angehalten sind.

9. Melden Sie sich bei Bedarf von der Eingabeaufforderung ab: `exit`

Das StorageGRID-Grid wurde jetzt heruntergefahren.

Verwandte Informationen

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

[SG6000 Storage-Appliances](#)

[SG5700 Storage-Appliances](#)

Grid-Nodes starten

Folgen Sie dieser Sequenz, um die Grid-Knoten nach einem vollständigen Herunterfahren zu starten.



Was Sie und#8217;ll benötigen

Wenn das gesamte Grid seit mehr als 15 Tagen heruntergefahren wurde, müssen Sie sich an den technischen Support wenden, bevor Sie die Grid-Nodes starten. Versuchen Sie nicht, die Wiederherstellungsverfahren für die Wiederherstellung von Cassandra-Daten zu verwenden. Dies kann zu Datenverlust führen.

Über diese Aufgabe

Wenn möglich, sollten Sie die Netzknoten in dieser Reihenfolge einschalten:

- Zuerst die Administratorknoten mit Strom versorgen.
- Strom auf Gateway-Knoten zuletzt anwenden.



Wenn ein Host mehrere Grid-Nodes enthält, werden die Nodes automatisch wieder online geschaltet, wenn Sie den Host einschalten.

Schritte

1. Schalten Sie die Hosts für den primären Admin-Node und alle nicht-primären Admin-Nodes ein.



Sie können sich erst bei den Admin-Knoten anmelden, wenn die Speicherknoten neu gestartet wurden.

2. Schalten Sie die Hosts für alle Archiv-Nodes und Speicherknoten ein.

Sie können diese Knoten in beliebiger Reihenfolge einschalten.

3. Schalten Sie die Hosts für alle Gateway-Nodes ein.
4. Melden Sie sich beim Grid Manager an.
5. Wählen Sie **NODES** aus, und überwachen Sie den Status der Grid-Knoten. Vergewissern Sie sich, dass neben den Node-Namen keine Warnsymbole vorhanden sind.

Nodes

View the list and status of sites and grid nodes.

Search...					Total node count: 14
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	—	—	2%	
DC1-G1	Gateway Node	—	—	2%	
DC1-S1	Storage Node	0%	0%	12%	
DC1-S2	Storage Node	0%	0%	11%	
DC1-S3	Storage Node	0%	0%	11%	

Verwenden Sie eine DoNotStart-Datei

Wenn Sie unter Anleitung des technischen Supports verschiedene Wartungs- oder Konfigurationsverfahren ausführen, werden Sie möglicherweise aufgefordert, eine DoNotStart-Datei zu verwenden, um zu verhindern, dass Dienste beim Starten von Server Manager gestartet oder neu gestartet werden.



Sie sollten eine DoNotStart-Datei nur hinzufügen oder entfernen, wenn Sie vom technischen Support dazu aufgefordert wurden.

Um den Start eines Dienstes zu verhindern, legen Sie eine DoNotStart-Datei in das Verzeichnis des Dienstes, den Sie verhindern möchten, dass dieser gestartet wird. Beim Start sucht der Server Manager nach der DoNotStart-Datei. Wenn die Datei vorhanden ist, wird der Dienst (und alle Services, die davon abhängig sind) nicht gestartet. Wenn die DoNotStart-Datei entfernt wird, wird der zuvor angefangene Dienst beim nächsten Start oder Neustart von Server Manager gestartet. Dienste werden beim Entfernen der DoNotStart-Datei nicht automatisch gestartet.

Der effizienteste Weg, um einen Neustart aller Dienste zu verhindern, ist, dass der NTP-Dienst nicht gestartet wird. Alle Dienste sind vom NTP-Dienst abhängig und können nicht ausgeführt werden, wenn der NTP-Dienst nicht ausgeführt wird.

Fügen Sie die DoNotStart-Datei für den Dienst hinzu

Sie können verhindern, dass ein einzelner Dienst gestartet wird, indem Sie dem Verzeichnis dieses Dienstes auf einem Grid-Node eine DoNotStart-Datei hinzufügen.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

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

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

2. Fügen Sie eine `DoNotStart`-Datei hinzu: `touch /etc/sv/service/DoNotStart`

Wo `service` Ist der Name des Dienstes, der verhindert werden soll, dass der Dienst gestartet wird.
Beispiel:

```
touch /etc/sv/ldr/DoNotStart
```

Eine `DoNotStart`-Datei wird erstellt. Es werden keine Dateiinhalte benötigt.

Wenn Server Manager oder der Grid-Node neu gestartet wird, wird der Server Manager neu gestartet, der Service jedoch nicht.

3. Melden Sie sich aus der Befehlsshell ab: `exit`

Entfernen Sie `DoNotStart`-Datei für den Dienst

Wenn Sie eine `DoNotStart`-Datei entfernen, die den Start eines Dienstes verhindert, müssen Sie diesen Dienst starten.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Schritte

1. Melden Sie sich beim Grid-Node an:

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

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

2. Entfernen Sie die `DoNotStart`-Datei aus dem Service-Verzeichnis: `rm /etc/sv/service/DoNotStart`

Wo `service` Ist der Name des Service. Beispiel:

```
rm /etc/sv/ldr/DoNotStart
```

3. Starten Sie den Service: `service servicename start`
4. Melden Sie sich aus der Befehlsshell ab: `exit`

Fehlerbehebung Für Server Manager

Rufen Sie die Protokolldatei von Server Manager auf

Wenn bei der Verwendung von Server Manager ein Problem auftritt, überprüfen Sie dessen Protokolldatei.

Fehlermeldungen im Zusammenhang mit Server Manager werden in der Server Manager-Protokolldatei erfasst, die sich unter befindet: `/var/local/log/servermanager.log`

Prüfen Sie diese Datei auf Fehlermeldungen zu Fehlern. Eskalieren des Problems gegebenenfalls an den technischen Support. Möglicherweise werden Sie aufgefordert, Protokolldateien an den technischen Support weiterzuleiten.

Dienst mit Fehlerstatus

Wenn Sie feststellen, dass ein Dienst einen Fehlerstatus eingegeben hat, versuchen Sie, den Dienst neu zu starten.

Was Sie benötigen

Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

Server Manager überwacht Dienste und startet alle, die unerwartet angehalten haben. Wenn ein Dienst ausfällt, versucht der Server Manager, ihn neu zu starten. Wenn drei fehlgeschlagene Versuche bestehen, einen Dienst innerhalb von fünf Minuten zu starten, wechselt der Dienst in einen Fehlerzustand. Server Manager versucht keinen anderen Neustart.

Schritte

1. 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 `#`.

2. Bestätigen Sie den Fehlerstatus des Dienstes: `service servicename status`

Beispiel:


```
service ldr status
```

Wenn sich der Dienst in einem Fehlerzustand befindet, wird die folgende Meldung zurückgegeben:
servicename in error state. Beispiel:

```
ldr in error state
```



Wenn der Servicestatus lautet `disabled`, Siehe die Anweisungen für [Entfernen einer DoNotStart-Datei für einen Dienst](#).

3. Versuchen Sie, den Fehlerstatus durch Neustart des Dienstes zu entfernen: `service servicename restart`

Wenn der Service nicht neu gestartet werden kann, wenden Sie sich an den technischen Support.

4. Melden Sie sich aus der Befehlsshell ab: `exit`

Klonen von Appliance-Nodes

Sie können einen Appliance-Node in StorageGRID klonen, um eine Appliance mit neuerem Design oder höheren Funktionen zu verwenden. Durch das Klonen werden alle Informationen des vorhandenen Nodes an die neue Appliance übertragen, ein Hardware-Upgrade-Prozess ist einfach durchzuführen und eine Alternative zur Ausmusterung und Erweiterung beim Austausch von Appliances zu bieten.

Funktionsweise des Appliance-Node-Klonens

Mit dem Appliance-Node-Klonen können Sie einen vorhandenen Appliance-Node (Quelle) im Grid ganz einfach durch eine kompatible Appliance (Ziel) ersetzen, die Teil desselben logischen StorageGRID-Standorts ist. Dabei werden alle Daten auf die neue Appliance übertragen, die Appliance wird in Betrieb versetzt, um den alten Appliance-Node zu ersetzen und die alte Appliance im Installationszustand zu lassen.

Warum einen Appliance-Node klonen?

Sie können einen Appliance-Node klonen, wenn Sie Folgendes benötigen:

- Ersetzen Sie Appliances, die sich dem Ende ihrer Lebensdauer nähert.
- Aktualisieren Sie vorhandene Nodes, um von der verbesserten Appliance-Technologie zu profitieren.
- Erhöhen Sie die Grid-Storage-Kapazität, ohne die Anzahl der Storage-Nodes in Ihrem StorageGRID System zu ändern.
- Verbessern Sie die Storage-Effizienz, z. B. durch Ändern des RAID-Modus von DDP-8 auf DDP-16 oder auf RAID-6.
- Node-Verschlüsselung wird effizient implementiert, sodass die externen Verschlüsselungsmanagement-Server (KMS) verwendet werden können.

Welches StorageGRID Netzwerk wird verwendet?

Durch das Klonen werden Daten vom Quell-Node über ein beliebiges StorageGRID-Netzwerk direkt an die Ziel-Appliance übertragen. Das Grid-Netzwerk wird normalerweise verwendet, Sie können aber auch das Admin-Netzwerk oder das Client-Netzwerk verwenden, wenn die Quell-Appliance mit diesen Netzwerken verbunden ist. Wählen Sie das Netzwerk für den Klon-Traffic aus, das die beste Performance bei der Datenübertragung bietet, ohne die Leistung des StorageGRID-Netzwerks oder die Datenverfügbarkeit zu beeinträchtigen.

Bei der Installation der Ersatzanwendung müssen Sie temporäre IP-Adressen für StorageGRID-Verbindung und Datentransfer angeben. Da die Ersatz-Appliance Teil derselben Netzwerke ist wie der von ihr ersetzte Appliance-Node, müssen Sie für jedes dieser Netzwerke auf der Ersatzanwendung temporäre IP-Adressen angeben.

Kompatibilität der Ziel-Appliance

Ersatz-Appliances müssen vom gleichen Typ sein wie der Quell-Node, den sie ersetzen, und beide müssen Teil desselben logischen StorageGRID-Standorts sein.

- Eine Ersatz-Services-Appliance kann sich von dem Admin-Node oder dem Gateway-Node unterscheiden, den er ersetzt.
 - Sie können eine SG100-Quell-Node-Appliance zu einer SG1000-Services-Ziel-Appliance klonen, um dem Admin-Node oder Gateway-Node eine höhere Funktion zuzuweisen.
 - Sie können eine SG1000-Quell-Node-Appliance in einer SG100-Services-Ziel-Appliance klonen, um die SG1000 für eine anspruchsvollere Applikation neu zu implementieren.

Beispiel: Wenn eine SG1000-Quell-Node-Appliance als Admin-Node verwendet wird und Sie sie als dedizierten Load-Balancing-Node verwenden möchten.

- Durch den Austausch einer SG1000-Quell-Node-Appliance durch eine SG100-Services-Ziel-Appliance wird die maximale Geschwindigkeit der Netzwerkports von 100 GbE auf 25 GbE verringert.
- Die SG100- und SG1000-Appliances verfügen über unterschiedliche Netzwerkverbindungen. Wenn Sie den Gerätetyp ändern, müssen möglicherweise die Kabel oder SFP-Module ersetzt werden.
- Eine Ersatz-Speicher-Appliance muss die gleiche oder höhere Kapazität aufweisen als der Speicherknoten, den sie ersetzt.
 - Wenn die Ziel-Storage-Appliance über dieselbe Anzahl von Laufwerken wie der Quell-Node verfügt, müssen die Laufwerke in der Ziel-Appliance über eine größere Kapazität (in TB) verfügen.
 - Wenn Sie planen, denselben RAID-Modus auf dem Ziel-Node zu verwenden, der auf dem Quell-Node verwendet wurde, Oder einen weniger Storage-effizienten RAID-Modus (beispielsweise beim Wechsel von RAID 6 zu DDP) müssen die Laufwerke in der Ziel-Appliance größer sein (in TB) als die Laufwerke in der Quell-Appliance.
 - Wenn die Anzahl der Standardlaufwerke, die in einer Ziel-Storage Appliance installiert sind, kleiner als die Anzahl der Laufwerke im Quell-Node ist, da Solid State Drives (SSDs) installiert sind, wird die gesamte Storage-Kapazität der Standardlaufwerke in der Ziel-Appliance (in TB) Die Gesamtkapazität aller Laufwerke im Quell-Storage-Node muss erreicht oder überschritten werden.

Wenn beispielsweise eine SG5660 Quell-Storage-Node-Appliance mit 60 Laufwerken auf eine SG6060- oder SG6060X-Zielapplikation mit 58 Standardlaufwerken geklont wird, sollten größere Laufwerke in der SG6060 oder SG6060X Ziellanwendung installiert werden, bevor das Klonen die Storage-Kapazität erhalten. (Die zwei Laufwerksschächte mit SSDs in der Ziel-Appliance sind nicht in der gesamten Appliance-Storage-Kapazität enthalten.)

Wenn jedoch eine SG5660 Quell-Node-Appliance mit 60 Laufwerken mit SANtricity Dynamic Disk Pools DDP-8 konfiguriert ist, kann die SG6060 oder SG6060X Zielapplikation mit DDP-16 für 58 Laufwerke aus der SG6060 oder SG6060X Appliance aufgrund der verbesserten Storage-Effizienz ein gültiges Klonziel machen.

Auf der Seite **NODES** im Grid Manager können Sie Informationen zum aktuellen RAID-Modus des Quell-Appliance-Knotens anzeigen. Wählen Sie die Registerkarte * Storage* für das Gerät aus.

Welche Informationen sind nicht geklont?

Die folgenden Appliance-Konfigurationen werden während des Klonens nicht auf die Ersatz-Appliance übertragen. Sie müssen sie während der Ersteinrichtung des Ersatzgeräts konfigurieren.

- BMC Schnittstelle
- Netzwerkverbindungen
- Verschlüsselungsstatus der Nodes
- SANtricity System Manager (für Storage-Nodes)
- RAID-Modus (für Storage-Nodes)

Welche Probleme verhindern das Klonen?

Wenn beim Klonen eines der folgenden Probleme auftreten, stoppt der Klonprozess und eine Fehlermeldung wird erzeugt:

- Falsche Netzwerkkonfiguration
- Fehlende Konnektivität zwischen Quell- und Ziel-Appliances
- Nicht kompatibel mit Quell- und Ziel-Appliance
- Bei Storage-Nodes eine Ersatz-Appliance mit unzureichender Kapazität

Sie müssen jedes Problem lösen, damit das Klonen fortgesetzt werden kann.

Überlegungen und Anforderungen zum Klonen von Appliance-Nodes

Vor dem Klonen eines Appliance-Nodes müssen Sie die Überlegungen und Anforderungen verstehen.

Hardwareanforderungen für die Ersatz-Appliance

Stellen Sie sicher, dass das Ersatzgerät die folgenden Kriterien erfüllt:

- Der Quell-Node (eine Appliance, die ersetzt wird) und das Ziel-Appliance müssen denselben Appliance-Typ sein:
 - Sie können eine Admin-Node-Appliance oder eine Gateway-Node-Appliance nur auf einer neuen Services-Appliance klonen.
 - Sie können eine Storage-Node-Appliance nur auf einer neuen Storage Appliance klonen.
- Bei Admin-Node- oder Gateway-Node-Appliances müssen die Quell-Node-Appliance und die Ziel-Appliance nicht vom gleichen Appliance-Typ sein. Bei Änderungen des Appliance-Typs müssen jedoch möglicherweise die Kabel oder SFP-Module ausgetauscht werden.

Sie können beispielsweise eine SG1000-Node-Appliance durch ein SG100 ersetzen oder eine SG100-

Appliance durch eine SG1000-Appliance ersetzen.

- Bei Storage Node Appliances müssen die Quell-Node-Appliance und die Ziel-Appliance nicht denselben Appliance-Typ sein. Die Ziel-Appliance muss jedoch über eine größere Storage-Kapazität verfügen als die Quell-Appliance.

So können Sie beispielsweise eine SG5600 Node-Appliance durch eine SG5700 oder SG6000 Appliance ersetzen.

Wenden Sie sich an Ihren StorageGRID Vertriebsmitarbeiter, wenn Sie Unterstützung bei der Auswahl kompatibler Ersatzgeräte benötigen, um bestimmte Appliance-Nodes in Ihrer StorageGRID Installation zu klonen.

Das Klonen eines Appliance-Nodes wird vorbereitet

Vor dem Klonen eines Appliance-Node müssen Sie folgende Informationen haben:

- Beziehen Sie eine temporäre IP-Adresse für das Grid-Netzwerk von Ihrem Netzwerkadministrator zur Verwendung mit der Ziel-Appliance während der ersten Installation. Wenn der Quellknoten zu einem Admin-Netzwerk oder Client-Netzwerk gehört, erhalten Sie temporäre IP-Adressen für diese Netzwerke.

Temporäre IP-Adressen befinden sich normalerweise im selben Subnetz wie die zu klonenden Quell-Node-Appliance und werden nach Abschluss des Klonens nicht benötigt. Die Quell- und Ziel-Appliances müssen eine Verbindung zu dem primären Admin-Node Ihrer StorageGRID herstellen, um eine Klonverbindung herzustellen.

- Bestimmung des Netzwerks zum Klonen von Datenübertragungsdaten, das die beste Performance bei der Datenübertragung bietet, ohne die Leistung des StorageGRID-Netzwerks oder die Datenverfügbarkeit zu beeinträchtigen



Die Verwendung des 1-GbE-Admin-Netzwerks für die Übertragung von Klondaten führt zu langsamerem Klonen.

- Ermitteln, ob die Node-Verschlüsselung mithilfe eines Verschlüsselungsmanagement-Servers (KMS) auf der Ziel-Appliance verwendet wird, damit die Node-Verschlüsselung während der Erstinstallation der Ziel-Appliance vor dem Klonen aktiviert werden kann. Sie können überprüfen, ob die Node-Verschlüsselung auf dem Quell-Appliance-Node aktiviert ist, wie in der Appliance-Installation beschrieben.

Der Quell- und die Ziel-Appliance können unterschiedliche Node-Verschlüsselungseinstellungen aufweisen. Die Entschlüsselung und Verschlüsselung der Daten erfolgt automatisch während des Datentransfers und beim Neustart des Ziel-Nodes und Beitritt zum Grid.

- [SG100- und SG1000-Services-Appliances](#)
- [SG5600 Storage Appliances](#)
- [SG5700 Storage-Appliances](#)
- [SG6000 Storage-Appliances](#)

- Ermitteln Sie, ob der RAID-Modus auf der Ziel-Appliance von der Standardeinstellung geändert werden soll, damit Sie diese Informationen bei der Erstinstallation der Ziel-Appliance vor dem Klonen angeben können. Auf der Seite **NODES** im Grid Manager können Sie Informationen zum aktuellen RAID-Modus des Quell-Appliance-Knotens anzeigen. Wählen Sie die Registerkarte * Storage* für das Gerät aus.

Der Quell- und die Ziel-Appliance können unterschiedliche RAID-Einstellungen aufweisen.

- Planen Sie ausreichend Zeit, um den Node-Klonprozess abzuschließen. Für den Datentransfer von einem betrieblichen Storage Node zu einer Ziel-Appliance sind möglicherweise mehrere Tage erforderlich. Planen Sie das Klonen zu einer Zeit, die die Auswirkungen auf Ihr Geschäft minimiert.
- Sie sollten jeweils nur einen Appliance-Node klonen. Durch Klonen wird verhindert, dass Sie weitere StorageGRID-Wartungsarbeiten gleichzeitig ausführen.
- Nachdem Sie einen Appliance-Node geklont haben, können Sie die Quell-Appliance verwenden, die zu einem Installationszustand zurückgeschickt wurde, als Ziel, eine weitere kompatible Node-Appliance zu klonen.

Klon-Appliance-Node

Der Klonprozess kann mehrere Tage dauern, bis die Daten zwischen dem Quell-Node (Appliance, die ersetzt wird) und der Ziel-Appliance übertragen werden.

Was Sie benötigen

- Sie haben das kompatible Zielgerät in einem Schrank oder Rack installiert, alle Kabel angeschlossen und mit Strom versorgt.
- Sie haben überprüft, ob die Installationsversion für die StorageGRID Appliance auf der Ersatzanwendung mit der Softwareversion des StorageGRID-Systems übereinstimmt. Dabei müssen Sie ggf. die StorageGRID Appliance Installer-Firmware aktualisieren.
- Sie haben die Ziel-Appliance konfiguriert, einschließlich der Konfiguration von StorageGRID-Verbindungen, SANtricity System Manager (nur Storage Appliances) und der BMC-Schnittstelle.
 - Verwenden Sie beim Konfigurieren von StorageGRID-Verbindungen die temporären IP-Adressen.
 - Verwenden Sie bei der Konfiguration von Netzwerkverbindungen die abschließende Link-Konfiguration.



Lassen Sie das Installationsprogramm der StorageGRID Appliance nach Abschluss der Erstkonfiguration der Ziel-Appliance offen. Nach dem Start des Node-Klonprozesses kehren Sie zur Installationsseite der Zielanwendung zurück.

- Optional ist die Node-Verschlüsselung für die Ziel-Appliance aktiviert.
- Sie haben optional den RAID-Modus für die Ziel-Appliance eingestellt (nur Storage Appliances).
- [Überlegungen und Anforderungen zum Klonen von Appliance-Nodes](#)

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

[SG5600 Storage Appliances](#)

[SG5700 Storage-Appliances](#)

[SG6000 Storage-Appliances](#)

Sie sollten jeweils nur einen Appliance-Node klonen, um die Netzwerk-Performance und Datenverfügbarkeit von StorageGRID zu erhalten.

Schritte

1. [Platzieren Sie den Quellknoten, den Sie klonen, in den Wartungsmodus.](#)
2. Wählen Sie im StorageGRID-Appliance-Installationsprogramm auf dem Quellknoten im Abschnitt Installation der Startseite die Option **Klonen aktivieren** aus.

NetApp® StorageGRID® Appliance Installer

Help

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to [reboot](#) the controller.

This Node

Node type

Storage ▾

Node name

hrmny2-1-254-sn

Cancel

Save

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.0.62

Connection state

Connection to 172.16.0.62 ready.

Cancel

Save

Installation

Current state

Maintenance mode. [Reboot](#) the node to resume normal operation.

Start Expansion

Enable Cloning

Der Abschnitt primäre Admin-Node-Verbindung wird durch den Abschnitt „Verbindung zum Ziel-Node klonen“ ersetzt.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to [reboot](#) the controller.

This Node

Node type
Storage
Node name
hrmny2-1-254-sn
Cancel
Save

Clone target node connection

Clone target node IP
0.0.0.0
Connection state
No connection information available.
Cancel
Save

Installation

Current state
Waiting for configuration and validation of clone target.
Start Cloning
Disable Cloning

- Geben Sie für **Zielknoten-IP** die temporäre IP-Adresse ein, die dem Zielknoten zugewiesen ist, das Netzwerk für den Datenverkehr der Klondatenübertragung verwenden soll, und wählen Sie dann **Speichern** aus.

Normalerweise geben Sie die IP-Adresse für das Grid-Netzwerk ein. Wenn Sie jedoch ein anderes Netzwerk für den Datenverkehr von Klondaten verwenden müssen, geben Sie die IP-Adresse des Zielknoten in diesem Netzwerk ein.



Die Verwendung des 1-GbE-Admin-Netzwerks für die Übertragung von Klondaten führt zu langsamerem Klonen.

Nachdem die Zielanwendung konfiguriert und validiert wurde, ist im Abschnitt Installation **Klonen starten** auf dem Quellknoten aktiviert.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking ▾
Configure Hardware ▾
Monitor Installation
Advanced ▾

Home

⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

ℹ The cloning process is ready to be started. Select **Start Cloning** when you are ready. To terminate cloning before it completes and return this node to service, trigger a reboot.

This Node

Node type
Storage ▾

Node name
hrmny2-1-254-sn

Cancel
Save

Clone target node connection

Clone target node IP
10.224.1.253

Connection state
Connection to 10.224.1.253 ready.

Cancel
Save

Installation

Current state
Ready to start cloning all data from this node to the clone target node using the Admin Network connection.
⚠ Attention: the Admin Network typically has less bandwidth than the Grid or Client Networks. Use the Grid or Client IP of the target node for faster cloning.

Start Cloning
Disable Cloning

Wenn Probleme bestehen, die das Klonen verhindern, ist **Klonen starten** nicht aktiviert und Probleme, die Sie lösen müssen, werden als **Verbindungsstatus** aufgeführt. Diese Probleme sind auf der Startseite des StorageGRID-Appliance-Installationsprogramms sowohl des Quell-Knotens als auch der Ziel-Appliance aufgeführt. Es wird immer nur ein Problem angezeigt, und der Status wird automatisch aktualisiert, wenn sich die Bedingungen ändern. Lösen Sie alle Klonprobleme, um **Klonen starten** zu aktivieren.

Wenn **Klonen starten** aktiviert ist, zeigt der **Aktueller Status** das zum Klonen des Datenverkehrs ausgewählte StorageGRID-Netzwerk sowie Informationen über die Verwendung dieser Netzwerkverbindung an.

Überlegungen und Anforderungen zum Klonen von Appliance-Nodes

- Wählen Sie **Klonen starten** auf dem Quellknoten aus.
- Überwachen Sie den Klonfortschritt mit dem Installationsprogramm von StorageGRID Appliance auf dem Quell- oder Zielknoten.

Das Installationsprogramm der StorageGRID Appliance auf den Quell- und den Ziel-Nodes weist denselben Status auf.

NetApp® StorageGRID® Appliance Installer

Help

Home

Configure Networking

Configure Hardware

Monitor Installation

Advanced

Monitor Cloning

1. Establish clone peering relationship

Complete

2. Clone another node from this node

Running

Step	Progress	Status
Send data to clone target node		Sending data, 0% complete, 8.99 GB transferred

3. Activate cloned node and leave this one offline

Pending

Die Seite Klonen überwachen bietet detaillierte Fortschritte für jede Phase des Klonprozesses:

- **Aufbau einer Klon-Peering-Beziehung** zeigt den Fortschritt der Klonerstellung und -Konfiguration.
- **Ein weiterer Knoten von diesem Knoten klonen** zeigt den Fortschritt der Datenübertragung an. (Dieser Teil des Klonprozesses kann mehrere Tage dauern.)
- **Geklonter Knoten aktivieren und diesen offline lassen** zeigt den Fortschritt der Übertragung der Steuerung auf den Zielknoten und der Platzierung des Quellknoten in einen Pre-install Zustand, nachdem die Datenübertragung abgeschlossen ist.

6. Wenn Sie den Klonprozess beenden und den Quellknoten vor dem Abschluss des Klonens in den Dienst zurücksenden müssen, wechseln Sie auf dem Quellknoten zur Startseite des StorageGRID Appliance Installer und wählen Sie **Erweitert Controller neu starten** aus und wählen dann **Neustart in StorageGRID** aus.

Wenn der Klonprozess beendet wird:

- Der Quell-Node beendet den Wartungsmodus und verbindet sich neu zu StorageGRID.
- Der Ziel-Node bleibt im Installationszustand. Um das Klonen des Quellknoten neu zu starten, starten Sie den Klonprozess erneut von Schritt 1.

Wenn das Klonen erfolgreich abgeschlossen wurde:

- Die Quell- und Ziel-Knoten tauschen IP-Adressen aus:
 - Der Zielknoten verwendet nun die IP-Adressen, die ursprünglich dem Quellknoten für Grid-, Admin- und Client-Netzwerke zugewiesen wurden.
 - Der Quellknoten verwendet jetzt die temporäre IP-Adresse, die dem Zielknoten ursprünglich zugewiesen wurde.
- Der Ziel-Node beendet den Wartungsmodus und tritt dem StorageGRID bei und ersetzt den Quell-Node.
- Die Quell-Appliance befindet sich in einem vorinstallierten Zustand, so als ob Sie es hätten [Es für die Neuinstallation vorbereitet](#).



Wenn das Gerät nicht wieder in das Raster integriert wird, wechseln Sie zur Startseite des StorageGRID-Appliance-Installationsprogramms für den Quellknoten, wählen Sie **Erweitert Controller neu starten** und wählen Sie dann **Neustart im Wartungsmodus** aus. Nachdem der Quell-Node im Wartungsmodus neu gebootet wurde, wiederholen Sie den Vorgang des Node-Klonens.

Benutzerdaten auf der Quell-Appliance bleiben als Wiederherstellungsoption, wenn bei dem Ziel-Node ein unerwartetes Problem auftritt. Nachdem der Ziel-Node der StorageGRID erneut beigetreten ist, sind die Benutzerdaten auf der Quell-Appliance veraltet und werden nicht mehr benötigt. Bitten Sie den StorageGRID-Support bei Bedarf, die Quell-Appliance zu löschen, damit diese Daten zerstört werden können.

Ihre Vorteile:

- Verwenden Sie die Quell-Appliance als Ziel für weitere Klonvorgänge: Es ist keine zusätzliche Konfiguration erforderlich. Dieser Appliance wurde bereits die temporäre IP-Adresse zugewiesen, die ursprünglich für das erste Klonziel angegeben wurde.
- Installieren und richten Sie die Quell-Appliance als neuen Appliance-Node ein.
- Entsorgen Sie die Quell-Appliance, wenn sie nicht mehr mit StorageGRID verwendet wird.

Prüfung von Audit-Protokollen

Audit-Protokolle: Übersicht

Diese Anweisungen enthalten Informationen zur Struktur und zum Inhalt der StorageGRID-Prüfmeldungen und Prüfprotokolle. Sie können diese Informationen zum Lesen und Analysieren des Prüfprotokolls der Systemaktivität verwenden.

Diese Anweisungen richten sich an Administratoren, die für die Erstellung von Berichten zu Systemaktivitäten und -Nutzung verantwortlich sind, für die eine Analyse der Audit-Meldungen des StorageGRID Systems erforderlich ist.

Um die Text-Log-Datei verwenden zu können, müssen Sie auf die konfigurierte Revisionsfreigabe im Admin-Knoten zugreifen können.

Informationen zur Konfiguration von Meldungsebenen und zur Verwendung eines externen Syslog-Servers finden Sie unter [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#).

Verwandte Informationen

- [StorageGRID verwalten](#)

Meldungsfluss und -Aufbewahrung von Audits

Alle StorageGRID-Services generieren während des normalen Systembetriebs Audit-Meldungen. Sie sollten verstehen, wie diese Audit-Meldungen über das StorageGRID-System in das übertragen werden `audit.log` Datei:

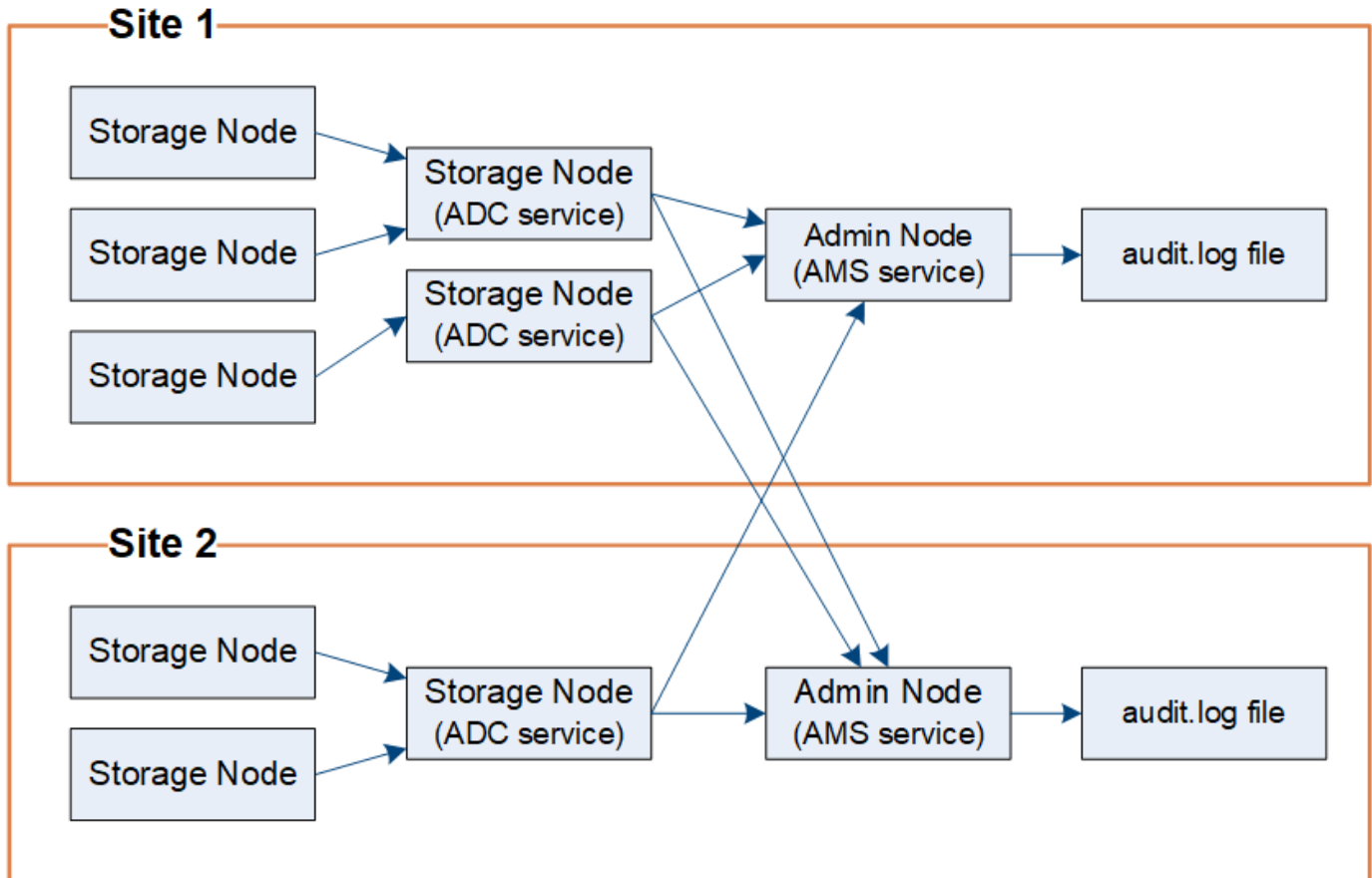
Audit-Nachrichtenfluss

Überwachungsmeldungen werden von Admin-Nodes und Storage-Nodes verarbeitet, die über einen ADC-Dienst (Administrative Domain Controller) verfügen.

Wie im Überwachungsmeldung-Flow-Diagramm dargestellt, sendet jeder StorageGRID Node seine Audit-Meldungen an einen der ADC-Services am Datacenter-Standort. Der ADC-Dienst wird automatisch für die ersten drei Speicherknoten aktiviert, die an jedem Standort installiert sind.

Jeder ADC-Dienst fungiert wiederum als Relais und sendet seine Sammlung von Audit-Meldungen an jeden Admin-Knoten im StorageGRID-System, wodurch jeder Admin-Knoten einen vollständigen Datensatz der Systemaktivität erhält.

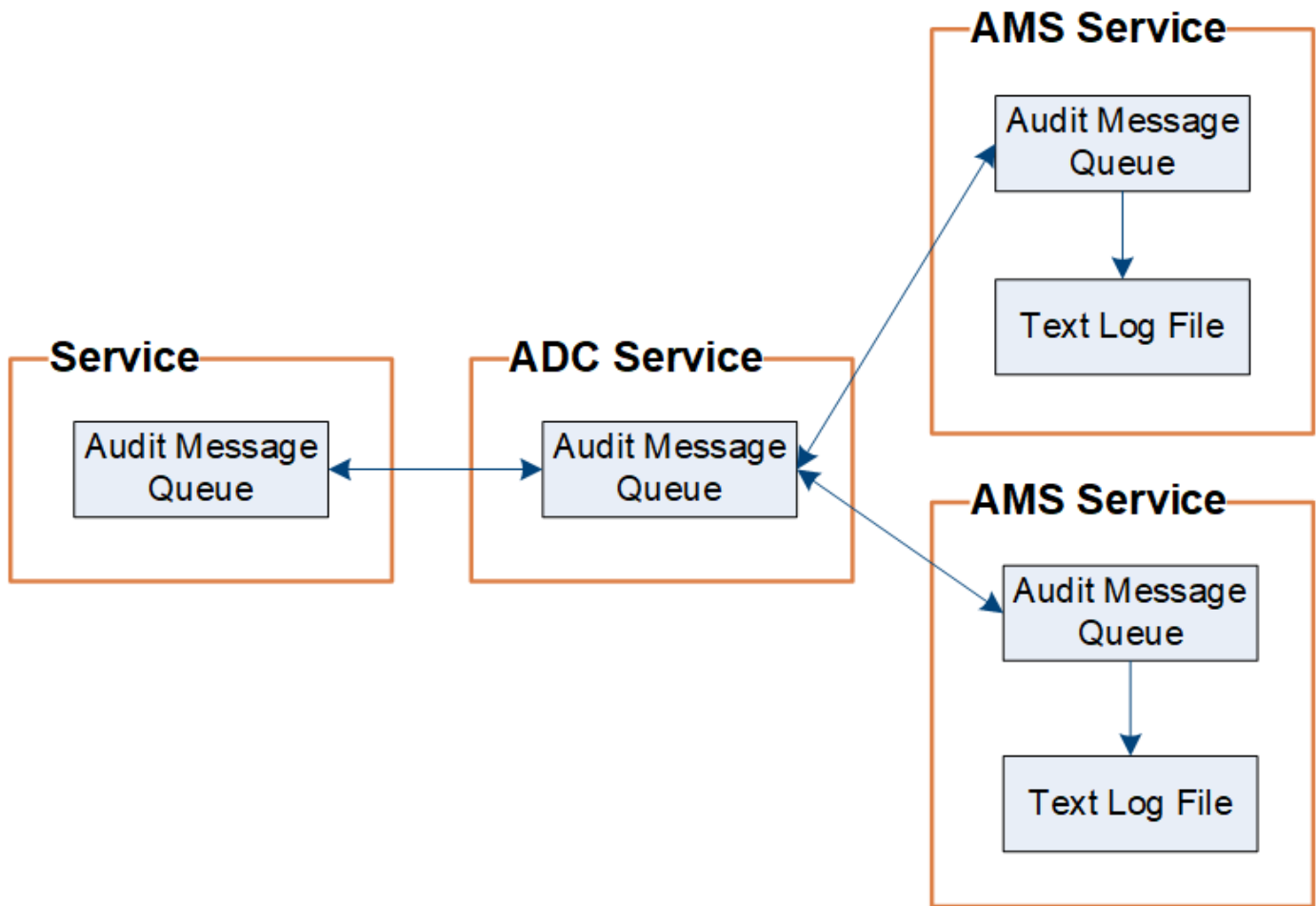
Jeder Admin-Knoten speichert Audit-Meldungen in Text-Log-Dateien; die aktive Protokolldatei wird benannt `audit.log`.



Aufbewahrung von Überwachungsnachrichten

StorageGRID verwendet einen Kopier- und Löschmod, um sicherzustellen, dass keine Audit-Meldungen verloren gehen, bevor sie in das Audit-Protokoll geschrieben werden.

Wenn ein Knoten eine Überwachungsmeldung generiert oder sendet, wird die Meldung in einer Meldungswarteschlange auf der Systemfestplatte des Grid-Node gespeichert. Eine Kopie der Nachricht wird immer in einer Warteschlange mit Überwachungsmeldung gespeichert, bis die Nachricht in die Audit-Log-Datei des Admin-Knotens geschrieben wird `/var/local/audit/export` Verzeichnis. Dadurch wird der Verlust einer Prüfmeldung während des Transports verhindert.



Die Warteschlange für Überwachungsnachrichten kann aufgrund von Problemen mit der Netzwerkverbindung oder aufgrund unzureichender Audit-Kapazität vorübergehend erhöht werden. Wenn die Warteschlangen steigen, verbrauchen sie mehr des verfügbaren Speicherplatzes in den einzelnen Nodes `/var/local/` Verzeichnis. Wenn das Problem weiterhin besteht und das Verzeichnis der Überwachungsmeldungen eines Knotens zu voll ist, werden die einzelnen Knoten die Verarbeitung ihres Rückstands priorisieren und für neue Meldungen vorübergehend nicht verfügbar sein.

Sie können insbesondere folgende Verhaltensweisen erkennen:

- Wenn der `/var/local/audit/export` Verzeichnis, das von einem Admin-Knoten verwendet wird, wird voll, der Admin-Knoten wird als nicht verfügbar für neue Audit-Meldungen markiert, bis das Verzeichnis nicht mehr voll ist. S3- und Swift-Client-Anforderungen sind nicht betroffen. Der Alarm XAMS (Unreachable Audit Repositories) wird ausgelöst, wenn ein Audit-Repository nicht erreichbar ist.
- Wenn der `/var/local/` Das von einem Speicherknoten mit dem ADC-Dienst verwendete Verzeichnis wird zu 92 % voll, der Knoten wird als nicht verfügbar markiert, um Meldungen zu prüfen, bis das Verzeichnis nur zu 87 % voll ist. S3- und Swift-Client-Anfragen zu anderen Nodes sind nicht betroffen. Der Alarm NRLY (Available Audit Relays) wird ausgelöst, wenn Audit-Relais nicht erreichbar sind.



Wenn keine Speicherknoten mit dem ADC-Dienst verfügbar sind, speichern die Speicherknoten die Überwachungsmeldungen lokal im `/var/local/log/localaudit.log` Datei:

- Wenn der `/var/local/` Das von einem Storage-Node verwendete Verzeichnis ist zu 85 % voll, wobei der Node die S3- und Swift-Client-Anforderungen ablehnen wird 503 Service Unavailable.

Die folgenden Arten von Problemen können dazu führen, dass die Warteschlangen für Überwachungsnachrichten sehr groß werden:

- Der Ausfall eines Admin-Knotens oder Speicherknoten mit dem ADC-Dienst. Wenn einer der Systemknoten ausgefallen ist, werden die übrigen Knoten möglicherweise rückgemeldet.
- Eine nachhaltige Aktivitätsrate, die die Audit-Kapazität des Systems übersteigt.
- Der `/var/local/` Speicherplatz auf einem ADC-Speicherknoten wird aus Gründen voll, die nicht mit Audit-Meldungen zusammenhängen. In diesem Fall hört der Knoten auf, neue Überwachungsmeldungen zu akzeptieren und priorisiert seinen aktuellen Rückstand, was zu Backlogs auf anderen Knoten führen kann.

Großer Alarm für Überwachungswarteschlangen und Überwachungsmeldungen in Queued (AMQS)

Um Ihnen dabei zu helfen, die Größe der Überwachungsmeldungswarteschlangen im Laufe der Zeit zu überwachen, werden die Warnung **große Prüfwarteschlange** und der ältere AMQS-Alarm ausgelöst, wenn die Anzahl der Nachrichten in einer Speicherknotenwarteschlange oder Admin-Knoten-Warteschlange bestimmte Schwellenwerte erreicht.

Wenn der Alarm `* Large Audit queue*` oder der alte AMQS-Alarm ausgelöst wird, prüfen Sie zunächst die Auslastung des Systems – wenn eine beträchtliche Anzahl aktueller Transaktionen vorliegt, sollten sich die Warnung und der Alarm im Laufe der Zeit lösen und können ignoriert werden.

Wenn die Warnung oder der Alarm weiterhin besteht und die Schwere erhöht wird, zeigen Sie ein Diagramm der Warteschlangengröße an. Wenn die Zahl über Stunden oder Tage stetig zunimmt, hat die Audit-Last wahrscheinlich die Audit-Kapazität des Systems überschritten. Verringern Sie die Betriebsrate des Clients, oder verringern Sie die Anzahl der protokollierten Audit-Meldungen, indem Sie das Audit-Level für Client-Schreibvorgänge und Client-Lesevorgänge auf Fehler oder aus ändern. Siehe „[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#).“

Duplizieren von Nachrichten

Bei einem Netzwerk- oder Node-Ausfall ist das StorageGRID System konservativ. Aus diesem Grund können doppelte Nachrichten im Audit-Protokoll vorhanden sein.

Zugriff auf die Audit-Log-Datei

Die Revisionsfreigabe enthält die aktive `audit.log` Datei und alle komprimierten Audit-Log-Dateien. Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, können Sie den Client-Zugriff auf Audit-Shares sowohl für NFS als auch für CIFS (CIFS ist veraltet) konfigurieren. Sie können auch direkt über die Befehlszeile des Admin-Knotens auf Audit-Protokolldateien zugreifen.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die `Passwords.txt` Datei:
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:

- a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`

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

2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:

```
cd /var/local/audit/export
```

3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

Verwandte Informationen

[StorageGRID verwalten](#)

Drehung der Audit-Log-Dateien

Audit-Log-Dateien werden auf einem Admin-Node gespeichert

`/var/local/audit/export` Verzeichnis. Die aktiven Audit-Log-Dateien werden benannt `audit.log`.



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](#).

Einmal am Tag, die aktive `audit.log` Die Datei wird gespeichert und eine neue `audit.log` Datei wird gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format `yyyy-mm-dd.txt`. Wenn an einem Tag mehrere Auditprotokolle erstellt werden, verwenden die Dateinamen das Datum, an dem die Datei im Format gespeichert wurde `yyyy-mm-dd.txt.n`. Beispiel: `2018-04-15.txt` Und `2018-04-15.txt.1` Sind die ersten und zweiten Log-Dateien, die am 15. April 2018 erstellt und gespeichert wurden.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, Die das ursprüngliche Datum bewahrt. Im Lauf der Zeit führt dies zu einem Verbrauch von für Prüfprotokolle auf dem Admin-Node zugewiesenem Storage. Ein Skript überwacht den Verbrauch von Speicherplatz im Überwachungsprotokoll und löscht die Protokolldateien nach Bedarf, um Speicherplatz im freizugeben `/var/local/audit/export` Verzeichnis. Audit-Protokolle werden nach dem Erstellungsdatum der Prüfprotokolle gelöscht, wobei der älteste zuerst gelöscht wird. Sie können die Aktionen des Skripts in der folgenden Datei überwachen: `/var/local/log/manage-audit.log`.

Dieses Beispiel zeigt die aktive `audit.log` Datei, Datei des Vortags (`2018-04-15.txt`), und die komprimierte Datei für den Vortag (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Audit-Log-Datei und Nachrichtenformate

Mit Audit-Protokollen können Informationen zu Ihrem System erfasst und Probleme behoben werden. Sie sollten das Format der Audit-Log-Datei und das allgemeine Format für Audit-Meldungen verstehen.

Format der Auditprotokolldatei

Die Audit-Log-Dateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Nachrichten.

Jede Überwachungsmeldung enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Meldung (ATIM) im ISO 8601-Format auslöste, gefolgt von einem Leerzeichen:

YYYY-MM-DDTHH:MM:SS.UUUUUU, Wo *UUUUUU* Nur Mikrosekunden.

- Die Meldung selbst, die in eckigen Klammern eingeschlossen ist und mit beginnt AUDT.

Das folgende Beispiel zeigt drei Audit-Nachrichten in einer Audit-Log-Datei (Zeilenumbrüche zur Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, wenn ein Mandant einen S3-Bucket erstellt und diesem Bucket zwei Objekte hinzugefügt hat.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):13489590586043706682]]
```

In ihrem Standardformat sind die Audit-Meldungen in den Audit-Log-Dateien nicht einfach zu lesen oder zu interpretieren. Sie können das verwenden `audit-explain` Tool zum Abrufen vereinfachter Zusammenfassungen der Audit-Meldungen im Audit-Protokoll. Sie können das verwenden `audit-sum` Tool zum Zusammenfassen, wie viele Schreibvorgänge, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

Verwandte Informationen

[Verwenden Sie das Audit-Erklären-Tool](#)

Verwenden Sie das Audit-Sum-Tool

Verwenden Sie das Audit-Erklären-Tool

Sie können das `audit-explain` Tool zum Übersetzen der Audit-Meldungen im Audit-Protokoll in ein einfach zu lesendes Format.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die `Passwords.txt` Datei:
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

Der `audit-explain` Das auf dem primären Admin-Knoten verfügbare Tool bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Audit-Protokoll.



Der `audit-explain` Das Tool ist hauptsächlich für den technischen Support bei der Fehlerbehebung vorgesehen. Wird `audit-explain` Abfragen können eine große Menge an CPU-Energie verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt die typische Ausgabe von der `audit-explain` Werkzeug. Diese vier SPUT-Audit-Nachrichten wurden generiert, als der S3-Mandant mit Konto-ID 92484777680322627870 S3-PUT-Anforderungen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und diesem Bucket drei Objekte hinzuzufügen.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Der `audit-explain` Das Tool kann einfache oder komprimierte Prüfprotokolle verarbeiten. Beispiel:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

Der `audit-explain` Das Tool kann auch mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Schließlich das `audit-explain` Das Tool kann Eingaben aus einer Leitung annehmen, sodass Sie die Eingabe mit dem `filtern` und `vorverarbeiten` können `grep` Befehl oder andere Mittel. Beispiel:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Da Audit-Protokolle sehr groß und langsam zu analysieren sein können, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen und ausführen möchten `audit-explain` Auf die Teile, statt der gesamten Datei.



Der `audit-explain` Das Werkzeug akzeptiert keine komprimierten Dateien als `Piper`-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente an, oder verwenden Sie das `zcat` Werkzeug, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
zcat audit.log.gz | audit-explain
```

Verwenden Sie die `help` (`-h`) Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-explain -h
```

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` Gibt den Namen und den Speicherort der zu analysierenden Datei oder der zu analysierenden Dateien an:

```
$ audit-explain /var/local/audit/export/audit.log
```

Der `audit-explain` Werkzeug druckt menschliche Interpretationen aller Nachrichten in der angegebenen Datei oder Datei.



Um die Zeilenlänge zu verringern und die Lesbarkeit zu erleichtern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel anzeigen möchten, verwenden Sie den Zeitstempel (`-t`) Option.

Verwandte Informationen

[SPUT: S3 PUT](#)

Verwenden Sie das Audit-Sum-Tool

Sie können das verwenden `audit-sum` Tool zum Zählen der Schreib-, Lese-, Kopf- und Löschmeldungen und zum Anzeigen der minimalen, maximalen und durchschnittlichen Zeit (oder Größe) für jeden Operationstyp.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

Über diese Aufgabe

Der `audit-sum` Tool, das auf dem primären Admin-Knoten verfügbar ist, fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.



Der `audit-sum` Das Tool ist hauptsächlich für den technischen Support bei der Fehlerbehebung vorgesehen. Wird Verarbeitet `audit-sum` Abfragen können eine große Menge an CPU-Energie verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt die typische Ausgabe von der `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

```
message group          count      min(sec)      max(sec)
average(sec)
=====
=====
IDEL                   274
SDEL                  213371      0.004         20.934
0.352
SGET                  201906      0.010         1740.290
1.132
SHEA                   22716      0.005          2.349
0.272
SPUT                  1771398     0.011         1770.563
0.487
```

Der `audit-sum` Das Tool bietet Zählung und Zeiten für die folgenden S3, Swift und ILM-Audit-Meldungen in einem Prüfprotokoll:

Codieren	Beschreibung	Siehe
ARCT	Archivieren von Cloud-Tier	ARCT: Archiv Abrufen aus Cloud-Tier
ASCT	Archivspeicher Cloud-Tier	ASCT: Archivspeicher Cloud-Tier

Codieren	Beschreibung	Siehe
IDEL	ILM initiated Delete: Protokolliert, wenn ILM den Prozess des Löschens eines Objekts startet.	IDEL: ILM gestartet Löschen
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	SDEL: S3 LÖSCHEN
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten.	SGET S3 ABRUFEN
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	SHEA: S3 KOPF
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen.	SPUT: S3 PUT
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	WDEL: Swift LÖSCHEN
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten.	WGET: Schneller ERHALTEN
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.	WHEA: Schneller KOPF
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.	WPUT: Schnell AUSGEDRÜCKT

Der `audit-sum` Das Tool kann einfache oder komprimierte Prüfprotokolle verarbeiten. Beispiel:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

Der `audit-sum` Das Tool kann auch mehrere Dateien gleichzeitig verarbeiten. Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Schließlich das `audit-sum` Das Tool kann auch Eingaben aus einer Leitung annehmen, sodass Sie die Eingabe mit dem `filtern` und `vorverarbeiten` können `grep` Befehl oder andere Mittel. Beispiel:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Dieses Tool akzeptiert keine komprimierten Dateien als `Piper` Input. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente an, oder verwenden Sie das `zcat` Werkzeug, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Mit Befehlszeilenoptionen können Operationen für Buckets separat von Operationen für Objekte zusammengefasst oder Nachrichtenübersichten nach Bucket-Namen, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden in den Zusammenfassungen die minimale, maximale und durchschnittliche Betriebszeit angezeigt, Sie können jedoch die verwenden `size` (`-s`) Option, stattdessen die Objektgröße zu betrachten.

Verwenden Sie die `help` (`-h`) Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

```
$ audit-sum -h
```

Schritte

1. Melden Sie sich beim primären Admin-Node an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Wenn Sie alle Nachrichten analysieren möchten, die mit Schreibvorgängen, Lese-, Kopf- und Löschvorgängen zusammenhängen, führen Sie die folgenden Schritte aus:

- a. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` Gibt den Namen und den Speicherort der zu analysierenden Datei oder der zu analysierenden Dateien an:

```
$ audit-sum /var/local/audit/export/audit.log
```

Dieses Beispiel zeigt die typische Ausgabe von der `audit-sum` Werkzeug. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

In diesem Beispiel sind SGET (S3 GET) Vorgänge im Durchschnitt mit 1.13 Sekunden die langsamsten. SGET und SPUT (S3 PUT) Vorgänge weisen jedoch lange Schlimmstfallszeiten von etwa 1,770 Sekunden auf.

- b. Um die langsamsten 10 Abruffunktionen anzuzeigen, wählen Sie mit dem `grep`-Befehl nur SGET-Nachrichten aus und fügen Sie die Long-Output-Option hinzu (`-l`) So fügen Sie Objektpfade ein: `grep SGET audit.log | audit-sum -l`

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, mit dem Sie das Audit-Protokoll für andere Meldungen zu diesen speziellen Objekten `grep` erstellen können.

```

Total:          201906 operations
Slowest:        1740.290 sec
Average:        1.132 sec
Fastest:        0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====
      1740289662      10.96.101.125      object      5663711385
backup/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r90l0aQ8JB-1566861764-4518.iso
      70839      10.96.101.125      object      28338
bucket3/dat.1566861764-6619
      68487      10.96.101.125      object      27890
bucket3/dat.1566861764-6615
      67798      10.96.101.125      object      27671
bucket5/dat.1566861764-6617
      67027      10.96.101.125      object      27230
bucket5/dat.1566861764-4517
      60922      10.96.101.125      object      26118
bucket3/dat.1566861764-4520
      35588      10.96.101.125      object      11311
bucket3/dat.1566861764-6616
      23897      10.96.101.125      object      10692
bucket3/dat.1566861764-4516

```

+ Aus diesem Beispielausgang sehen Sie, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von ca. 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe berücksichtigt die langsamen Abrufzeiten im schlimmsten Fall.

3. Wenn Sie feststellen möchten, welche Größe von Objekten in Ihr Raster aufgenommen und aus diesem abgerufen werden soll, verwenden Sie die Option „Größe“ (-s):

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

In diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2.5 MB, die durchschnittliche Größe für SGET ist jedoch deutlich größer. Die Anzahl der SPUT-Meldungen ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hinweist, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufvorgänge gestern langsam waren:
 - a. Geben Sie den Befehl für das entsprechende Prüfprotokoll ein und verwenden Sie die Option „Gruppe für Zeit“ (-gt), gefolgt von dem Zeitraum (z. B. 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```


message group average(sec) =====	count =====	min(sec) =====	max(sec) =====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Diese Ergebnisse zeigen, dass S3 VERKEHR zwischen 06:00 und 07:00 Spikes. Auch die max- und Durchschnittszeiten sind zu diesen Zeiten deutlich höher, und sie stiegen nicht schrittweise auf, wenn die Zahl erhöht wurde. Dies deutet darauf hin, dass die Kapazität irgendwo überschritten wurde, vielleicht im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

- b. Um zu bestimmen, welche Objekte in der Größe gestern jede Stunde abgerufen wurden, fügen Sie die Option Größe hinzu (-s) Zum Befehl:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Diese Ergebnisse zeigen, dass einige sehr große Rückrufe auftraten, als der gesamte Abrufverkehr seinen maximalen Wert hatte.

- c. Verwenden Sie zum Anzeigen weiterer Details die `audit-explain` Tool zur Überprüfung aller SGET-Vorgänge während dieser Stunde:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Wenn die Ausgabe des `grep`-Befehls viele Zeilen sein soll, fügen Sie den hinzu `less` Befehl zum Anzeigen des Inhalts der Audit-Log-Datei eine Seite (ein Bildschirm) gleichzeitig.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen auf Buckets langsamer sind als SPUT-Vorgänge für Objekte:

- a. Verwenden Sie als erstes die `-go` Bei dieser Option werden Meldungen für Objekt- und Bucket-Vorgänge getrennt gruppiert:

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets unterschiedliche Leistungseigenschaften haben als SPUT-Operationen für Objekte.

- b. Um festzustellen, welche Buckets die langsamsten SPUT-Operationen haben, verwenden Sie den `-gb` Option, die Meldungen nach Bucket gruppiert:

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ldt002 0.361	1564563	0.011	51.569

- c. Um zu bestimmen, welche Buckets die größte SPUT-Objektgröße haben, verwenden Sie beide `-gb` Und das `-s` Optionen:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

Verwandte Informationen

[Verwenden Sie das Audit-Erklären-Tool](#)

Überwachungsmeldungsformat

Im StorageGRID-System ausgetauschte Audit-Meldungen enthalten Standardinformationen, die für alle Meldungen und spezifische Inhalte zur Beschreibung des Ereignisses oder der Aktivität üblich sind.

Wenn die von bereitgestellten Zusammenfassungsdaten angezeigt werden `audit-explain` Und `audit-sum` Tools reichen nicht aus. Lesen Sie in diesem Abschnitt, um das allgemeine Format aller Audit-Meldungen zu verstehen.

Im Folgenden finden Sie eine Beispielmeldung, wie sie in der Audit-Log-Datei angezeigt werden kann:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

Jede Überwachungsmeldung enthält eine Zeichenfolge von Attributelementen. Der gesamte String ist in Klammern eingeschlossen ([]), und jedes Attributelement in der Zeichenfolge weist folgende Merkmale auf:

- In Halterungen eingeschlossen []
- Eingeführt durch den String `AUDT`, Das eine Audit-Nachricht anzeigt
- Ohne Trennzeichen (keine Kommata oder Leerzeichen) vor oder nach
- Wird durch ein Zeilenvorschub-Zeichen beendet `\n`

Jedes Element umfasst einen Attributcode, einen Datentyp und einen Wert, der in diesem Format angegeben wird:

```
[ATTR(type):value] [ATTR(type):value] ...  
[ATTR(type):value]\n
```

Die Anzahl der Attributelemente in der Nachricht hängt vom Ereignistyp der Nachricht ab. Die Attributelemente werden in keiner bestimmten Reihenfolge aufgeführt.

In der folgenden Liste werden die Attributelemente beschrieben:

- `ATTR` Ist ein 4-Zeichen-Code für das Attribut, das gemeldet wird. Es gibt einige Attribute, die für alle Audit-Meldungen und andere, die ereignisspezifisch sind, gelten.
- `type` Ist eine 4-Zeichen-Kennung des Programmierdatentyps des Wertes, wie UI64, FC32 usw. Der Typ ist in Klammern eingeschlossen ().
- `value` Ist der Inhalt des Attributs, in der Regel ein numerischer Wert oder Textwert. Werte folgen immer einem Doppelpunkt (:). Werte des Datentyps CSTR werden von doppelten Anführungszeichen umgeben " ".

Verwandte Informationen

[Verwenden Sie das Audit-Erklären-Tool](#)

[Verwenden Sie das Audit-Sum-Tool](#)

[Audit-Meldungen](#)

[Gemeinsame Elemente in Audit-Meldungen](#)

[Datentypen](#)

[Beispiele für Überwachungsnachrichten](#)

Datentypen

Verschiedene Datentypen werden zur Speicherung von Informationen in Audit-Meldungen verwendet.

Typ	Beschreibung
UI32	Unsigned long integer (32 Bit); es kann die Zahlen 0 bis 4,294,967,295 speichern.
UI64	Unsigned double long integer (64 Bit); es kann die Zahlen 0 bis 18,446,744,073,709,551,615 speichern.
FC32	Vierklarlige Konstante; ein 32-Bit unsigned integer Wert, der als vier ASCII-Zeichen wie "ABCD" dargestellt wird.
IPAD	Wird für IP-Adressen verwendet.

Codieren	Typ	Beschreibung
INMITTEN	FC32	Modul-ID: Eine vier-Zeichen-ID der Modul-ID, die die Nachricht generiert hat. Dies gibt das Codesegment an, in dem die Überwachungsmeldung generiert wurde.
ANID	UI32	Node-ID: Die Grid-Node-ID, die dem Service zugewiesen wurde, der die Meldung generiert hat. Jedem Service wird bei Konfiguration und Installation des StorageGRID-Systems eine eindeutige Kennung zugewiesen. Diese ID kann nicht geändert werden.
ASES	UI64	Kennung der Auditsitzung: In vorherigen Releases gab dieses Element die Zeit an, zu der das Audit-System nach dem Start des Dienstes initialisiert wurde. Dieser Zeitwert wurde in Mikrosekunden seit der Betriebssystemepoche gemessen (00:00:00 UTC am 1. Januar 1970). Hinweis: Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ASQN	UI64	Sequenzanzahl: In vorherigen Releases wurde dieser Zähler für jede erzeugte Überwachungsmeldung auf dem Grid-Node (ANID) erhöht und beim Neustart des Dienstes auf Null zurückgesetzt. Hinweis: Dieses Element ist veraltet und wird nicht mehr in Audit-Nachrichten angezeigt.
ATID	UI64	Trace-ID: Eine Kennung, die von den Nachrichten, die von einem einzelnen Ereignis ausgelöst wurden, gemeinsam genutzt wird.
ATIM	UI64	Zeitstempel: Die Zeit, zu der das Ereignis generiert wurde, das die Audit-Nachricht auslöste, gemessen in Mikrosekunden seit der Betriebssystemepoche (00:00:00 UTC am 1. Januar, 1970). Beachten Sie, dass die meisten verfügbaren Tools zum Konvertieren des Zeitstempels in lokales Datum und Uhrzeit auf Millisekunden basieren. Möglicherweise ist ein Aufrundung oder Verkürzung des protokollierten Zeitstempels erforderlich. Die lesbare Zeit des Menschen, die zu Beginn der Überwachungsmeldung angezeigt wird <code>audit.log</code> Die Datei ist das ATIM-Attribut im ISO 8601-Format. Das Datum und die Uhrzeit werden als dargestellt <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, Wo der T Ist ein Literalzeichenzeichen, das den Beginn des Zeitsegments des Datums angibt. <code>UUUUUU</code> Nur Mikrosekunden.
ATYP	FC32	Ereignistyp: Eine 4-Zeichen-Kennung des zu protokollierenden Ereignisses. Dies regelt den "Nutzlastinhalt" der Nachricht: Die Attribute, die enthalten sind.
AVER	UI32	Version: Die Version der Audit-Nachricht. Wenn die StorageGRID Software weiterentwickelt wird, können neue Serviceversionen neue Funktionen in die Audit-Berichte integrieren. Dieses Feld ermöglicht die Abwärtskompatibilität im AMS-Dienst zur Verarbeitung von Meldungen aus älteren Serviceversionen.

Codieren	Typ	Beschreibung
RSLT	FC32	Ergebnis: Das Ergebnis von Ereignis, Prozess oder Transaktion. Wenn für eine Nachricht nicht relevant ist, WIRD KEINE verwendet, sondern SUCS, damit die Nachricht nicht versehentlich gefiltert wird.

Beispiele für Überwachungsnachrichten

Detaillierte Informationen finden Sie in jeder Audit-Nachricht. Alle Überwachungsmeldungen verwenden das gleiche Format.

Im Folgenden finden Sie eine Beispielmeldung für Audits, wie sie im angezeigt werden kann `audit.log` Datei:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPUT
] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):1579224144
102530435]]
```

Die Überwachungsmeldung enthält Informationen über das zu protokollierte Ereignis sowie Informationen über die Meldung selbst.

Um festzustellen, welches Ereignis durch die Überwachungsmeldung aufgezeichnet wird, suchen Sie nach dem ATYP-Attribut (unten hervorgehoben):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP\ (FC32\):SP
UT] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):1579224
144102530435]]
```

Der Wert des ATYP-Attributs ist SPUT. SPUT stellt eine S3-PUT-Transaktion dar, die die Aufnahme eines Objekts in einen Bucket protokolliert.

Die folgende Meldung des Audits zeigt auch den Bucket an, dem das Objekt zugeordnet ist:


```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3
KY(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):
0] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPU
T] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):157922414
4102530435]]
```

Um zu ermitteln, wann das PUT-Ereignis aufgetreten ist, notieren Sie den UTC-Zeitstempel (Universal Coordinated Time, Universal Coordinated Time, koordinierte Zeit) zu Beginn der Überwachungsmeldung. Dieser Wert ist eine menschliche-lesbare Version des ATIM-Attributs der Prüfmeldung selbst:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SP
UT] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):15792241
44102530435]]
```

ATIM zeichnet die Zeit in Mikrosekunden, seit Beginn der UNIX-Epoche. Im Beispiel der Wert 1405631878959669 Übersetzt bis Donnerstag, 17. Juli 2014 21:17:59 UTC.

Verwandte Informationen

[SPUT: S3 PUT](#)

[Gemeinsame Elemente in Audit-Meldungen](#)

Überwachungsmeldungen und der Lebenszyklus von Objekten

Audit-Nachrichten werden bei jeder Aufnahme, jedem Abruf oder jedem Löschen eines Objekts generiert. Sie können diese Transaktionen im Audit-Protokoll identifizieren, indem Sie API-spezifische (S3 oder Swift) Audit-Nachrichten suchen.

Überwachungsmeldungen werden durch Kennungen verknüpft, die für jedes Protokoll spezifisch sind.

Protokoll	Codieren
Verknüpfen von S3-Vorgängen	S3BK (S3-Bucket) und/oder S3KY (S3-Schlüssel)
Swift-Vorgänge verknüpfen	WCON (Swift-Container) und/oder WOBJ (Swift-Objekt)

Protokoll	Codieren
Verknüpfen interner Vorgänge	CBID (interne Kennung des Objekts)

Timing von Audit-Meldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Nodes, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der durch die verschiedenen Services erzeugten Audit-Meldungen von den Beispielen in diesem Abschnitt abweichen.

Konfiguration der Richtlinien für das Informationslebenszyklus-Management

Bei der ILM-Standardrichtlinie (Baseline 2 Copy) werden Objektdaten einmal für insgesamt zwei Kopien kopiert. Wenn die ILM-Richtlinie mehr als zwei Kopien erfordert, gibt es für jede zusätzliche Kopie einen zusätzlichen Satz von CBRE-, CBSE- und SCMT-Meldungen. Weitere Informationen zu ILM-Richtlinien finden Sie unter Informationen zum Managen von Objekten mit Information Lifecycle Management.

Archiv-Nodes

Die Reihe von Meldungen, die beim Senden von Objektdaten an ein externes Archiv-Speichersystem generiert werden, ist ähnlich wie bei Storage-Nodes, es sei denn, es gibt keine SCMT-Meldung (Store Object Commit). Und die ATCE (Archive Object Store Begin) und ASCE (Archive Object Store End) Nachrichten werden für jede archivierte Kopie von Objektdaten generiert.

Die Reihe von Audit-Meldungen, die beim Abrufen von Objektdaten aus einem externen Archiv-Storage-System generiert werden, ähnelt der für Storage-Nodes, jedoch werden für jede abgerufene Kopie von Objektdaten ARCB (Archivobjekt Retrieve Begin) und ARCE (Archive Object Retrieve End) Nachrichten generiert.

Die beim Löschen von Objektdaten aus einem externen Archivspeichersystem generierte Reihe von Überwachungsmeldungen ähnelt der für Speicherknoten, es sei denn, ES gibt keine SREM (Object Store Remove)-Nachricht und für jede Löschanforderung gibt es eine AREM-Nachricht (Archive Object Remove).

Verwandte Informationen

[Objektmanagement mit ILM](#)

Objektaufnahme von Transaktionen

Sie können Transaktionen zur Client-Aufnahme im Prüfprotokoll identifizieren, indem API-spezifische (S3 oder Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Aufnahmetransaktion generierten Audit-Meldungen aufgeführt. Es sind nur die Nachrichten enthalten, die für die Aufzeichnung der Transaktion erforderlich sind.

S3 Aufnahme von Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3-PUT-Aufnahmerate wurde erfolgreich abgeschlossen.	CBID, S3BK, S3KY	SPUT: S3 PUT

Codieren	Name	Beschreibung	Verfolgen	Siehe
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	ORLM: Objektregeln erfüllt

Swift Ingest-Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
WPUT	Swift PUT-Transaktion	EINE Swift PUT-Aufnahme-Transaktion wurde erfolgreich abgeschlossen.	CBID, WCON, WOBJ	WPUT: Schnell AUSGEDRÜCKT
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	ORLM: Objektregeln erfüllt

Beispiel: S3-Objektaufnahme

Die folgende Serie von Audit-Meldungen ist ein Beispiel für die im Revisionsprotokoll generierten und gespeicherten Audit-Meldungen, wenn ein S3-Client ein Objekt in einen Storage-Node (LDR-Service) einspeist.

In diesem Beispiel umfasst die aktive ILM-Richtlinie die ILM-Regel für das Lager, erstellen Sie 2 Kopien.



Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Audit-Meldungen aufgeführt. Es werden nur solche aufgeführt, die sich auf die S3-Aufnahmetransaktion (SPUT) beziehen.

In diesem Beispiel wird vorausgesetzt, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Meldung gibt an, dass eine S3-PUT-Transaktion ausgegeben wurde, um ein Objekt in einem bestimmten Bucket zu erstellen.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Objektregeln erfüllt

Die ORLM-Meldung gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Meldung enthält die CBID des Objekts und den Namen der verwendeten ILM-Regel.

Bei replizierten Objekten umfasst das Feld LOCS die LDR-Node-ID und Volume-ID der Objektstandorte.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\ (UI64\):0x50C4F7AC2BC8EDF7] [RULE (CSTR): "Make
2 Copies"] [STAT (FC32): DONE] [CSIZ (UI64): 0] [UUID (CSTR): "0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"] [LOCS (CSTR): "CLDI 12828634 2148730112, CLDI 12745543
2147552014"] [RSLT (FC32): SUCS] [AVER (UI32): 10] [ATYP\ (FC32\): ORLM] [ATIM (UI64)
: 1563398230669] [ATID (UI64): 15494889725796157557] [ANID (UI32): 13100453] [AMID
(FC32): BCMS]]
```

Bei Objekten mit Erasure Coding enthält das Feld LOCS die Profile-ID für Erasure Coding und die Gruppen-ID für Erasure Coding

```
2019-02-23T01:52:54.647537
[AUDT:[CBID (UI64): 0xFA8ABE5B5001F7E2] [RULE (CSTR): "EC_2_plus_1"] [STAT (FC32)
: DONE] [CSIZ (UI64): 10000] [UUID (CSTR): "E291E456-D11A-4701-8F51-
D2F7CC9AFECA"] [LOCS (CSTR): "CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"] [RSLT (FC32): SUCS] [AVER (UI32): 10] [ATIM (UI64): 1550929974537]\ [
ATYP\ (FC32\): ORLM\] [ANID (UI32): 12355278] [AMID (FC32): ILMX] [ATID (UI64): 41685
59046473725560]]
```

Das PFADFELD umfasst S3-Bucket und wichtige Informationen sowie Swift-Container- und Objektinformationen, je nachdem, welche API verwendet wurde.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID (UI64): 0x82704DFA4C9674F4] [RULE (CSTR): "Make 2
Copies"] [STAT (FC32): DONE] [CSIZ (UI64): 3145729] [UUID (CSTR): "8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"] [PATH (CSTR): "frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"] [LOCS (CSTR): "CLDI 12525468, CLDI
12222978"] [RSLT (FC32): SUCS] [AVER (UI32): 10] [ATIM (UI64): 1568555574559] [ATYP (
FC32): ORLM] [ANID (UI32): 12525468] [AMID (FC32): OBDI] [ATID (UI64): 3448338865383
69336]]
```

Löschen von Objekttransaktionen

Sie können Transaktionen zum Löschen von Objekten im Prüfprotokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Meldungen angezeigt werden.

In den folgenden Tabellen sind nicht alle während einer Löschtransaktion generierten

Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die zum Verfolgen der Löschransaktion erforderlich sind.

S3-Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Anforderung zum Löschen des Objekts aus einem Bucket gemacht.	CBID, S3KY	SDEL: S3 LÖSCHEN

Swift Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WDEL	Swift Löschen	Anforderung gemacht, das Objekt aus einem Container oder Container zu löschen.	CBID, WOBJ	WDEL: Swift LÖSCHEN

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt aus einem Storage-Node (LDR-Service) löscht, wird eine Überwachungsmeldung generiert und im Revisionsprotokoll gespeichert.



Im folgenden Beispiel sind nicht alle während einer Löschransaktion generierten Audit-Meldungen aufgeführt. Es werden nur diejenigen aufgelistet, die mit der S3-Löschransaktion (SDEL) in Verbindung stehen.

SDEL: S3 Löschen

Die Objektlöschung beginnt, wenn der Client eine LÖSCHANFORDERUNG an einen LDR-Dienst sendet. Die Meldung enthält den Bucket, aus dem das Objekt gelöscht werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\ (CSTR\):"example"\]\[S3KY\ (CSTR\):"testobject-0-
7"\][CBID\ (UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\ (FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Abrufen von Objekttransaktionen

Sie können Transaktionen zum Abrufen von Objekten im Audit-Protokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Abruftransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die für die Rückrufs-Transaktion erforderlich sind.

S3-Abruf von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 ABRUFEN	Anforderung zum Abrufen eines Objekts aus einem Bucket	CBID, S3BK, S3KY	SGET S3 ABRUFEN

Schnelles Abrufen von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WGET	Swift GET	Anforderung gemacht, ein Objekt aus einem Container abzurufen.	CBID, WCON, WOBJ	WGET: Schneller ERHALTEN

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Storage-Node (LDR-Service) abruft, wird eine Audit-Meldung erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET S3 ABRUFEN

Der Objektabruf beginnt, wenn der Client eine GET Object-Anforderung an einen LDR-Service sendet. Die Meldung enthält den Bucket, aus dem das Objekt abgerufen werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEW=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\CSTR\):"bucket-
anonymous"\]\[S3KY\CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\) :SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Wenn die Bucket-Richtlinie ermöglicht, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört. Die Überwachungsmeldung enthält Informationen über das Mandantenkonto des Bucket-Inhabers, sodass Sie diese anonymen und Cross-Account-Anforderungen verfolgen können.

In der folgenden Beispielmeldung sendet der Client eine GET Object-Anforderung für ein in einem Bucket gespeichertes Objekt, das ihnen nicht gehört. Die Werte für SBAI und SBAC zeichnen die Konto-ID und den Namen des Mandanten des Bucket-Besitzers auf. Diese Werte unterscheiden sich von der Konto-ID und dem Namen des in S3AI und SACC aufgezeichneten Clients.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\[CSTR\):"17915054115450519830"\]\[SACC\[CSTR\):"s3-account-
b"\]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="\][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\[CSTR\):"4397929817
8977966408"\]\[SBAC\[CSTR\):"s3-account-a"\]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02]\[CSIZ(UI
64):12]\[AVER(UI32):10]\[ATIM(UI64):1505947995876415]\[ATYP(FC32):SGET]\[ANID(
UI32):12272050]\[AMID(FC32):S3RQ]\[ATID(UI64):6888780247515624902]]
```

Beispiel: S3 Select auf einem Objekt

Wenn ein S3-Client eine S3-Select-Abfrage für ein Objekt ausgibt, werden Audit-Meldungen erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3 Select-Transaktion (SelectObjectContent) beziehen.

Bei jeder Abfrage werden zwei Audit-Meldungen ausgegeben: Eine, die die Autorisierung der S3 Select-Anfrage (das S3SR-Feld ist auf „SELECT“ gesetzt) und ein nachfolgender Standard-GET-Vorgang, der die Daten während der Verarbeitung aus dem Speicher abruft.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"]\[S3AI(CSTR):"63147909414576125820"]\[SACC(CSTR):"Ten
ant1636027116"]\[S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"]\[SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"]\[SBAI(CSTR):"63147909414576125820"]\[SBA
C(CSTR):"Tenant1636027116"]\[S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"]\[S3KY(CSTR):"SUB-
EST2020_ALL.csv"]\[CBID(UI64):0x0496F0408A721171]\[UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"]\[CSIZ(UI64):0]\[S3SR(CSTR):"select"]\[AVER(UI32):10]\[ATIM(UI64
):1636385730750038]\[ATYP(FC32):SPOS]\[ANID(UI32):12601166]\[AMID(FC32):S3RQ]
\[ATID(UI64):1363009709396895985]]
```

```

2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\": \"unix:\"}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant16
36027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CST
R):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"] [S3KY(CSTR):"SUB-
EST2020_ALL.csv"] [CBID(UI64):0x0496F0408A721171] [UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"] [CSIZ(UI64):10185581] [MTME(UI64):1636380348695262] [AVER(UI32
):10] [ATIM(UI64):1636385732604886] [ATYP(FC32):SGET] [ANID(UI32):12733063] [A
MID(FC32):S3RQ] [ATID(UI64):16562288121152341130]]

```

Nachrichten zum Metadatenupdate

Audit-Meldungen werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zu S3-Metadaten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten wurden aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	SUPD: S3-Metadaten wurden aktualisiert

Beispiel: S3-Metadatenaktualisierung

Das Beispiel zeigt eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadatenaktualisierung

Der S3-Client fordert eine SUPD (SUPD) auf, die angegebenen Metadaten zu aktualisieren (`x-amz-meta-*`) Für das S3-Objekt (S3KY). In diesem Beispiel sind Anforderungsheader im Feld HTRH enthalten, da sie als Audit-Protokoll-Header konfiguriert wurde (**KONFIGURATION Monitoring Audit- und Syslog-Server**).


```

2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\", \"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\", \"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\", \"x-amz-metadata-
directive\":\"REPLACE\", \"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]

```

Verwandte Informationen

[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)

Audit-Meldungen

Detaillierte Beschreibungen der vom System zurückgegebenen Audit-Meldungen finden Sie in den folgenden Abschnitten. Jede Überwachungsmeldung wird zuerst in einer Tabelle aufgeführt, in der verwandte Nachrichten nach der Aktivitätsklasse gruppiert werden, für die die Meldung steht. Diese Gruppierungen sind sowohl für das Verständnis der Arten von Aktivitäten, die geprüft werden, als auch für die Auswahl der gewünschten Art der Filterung von Überwachungsnachrichten nützlich.

Die Überwachungsmeldungen werden auch alphabetisch nach ihren vier-Zeichen-Codes aufgelistet. Mit dieser alphabetischen Auflistung können Sie Informationen zu bestimmten Nachrichten suchen.

Die in diesem Kapitel verwendeten 4-Zeichen-Codes sind die ATYP-Werte, die in den Audit-Meldungen gefunden werden, wie in der folgenden Beispielmeldung dargestellt:

```

2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]

```

Informationen zum Festlegen von Meldungsebenen, zum Ändern von Protokollzielen und zur Verwendung

eines externen Syslog-Servers für Ihre Audit-Informationen finden Sie unter [Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)

Kategorien von Überwachungsnachrichten

Sie sollten mit den verschiedenen Kategorien vertraut sein, in denen Audit-Meldungen gruppiert werden. Diese Gruppen sind auf der Grundlage der Aktivitätsklasse organisiert, für die die Nachricht steht.

Systemaudits Meldungen

Sie sollten mit Audit-Meldungen vertraut sein, die zur Systemaudit-Kategorie gehören. Dies sind Ereignisse in Bezug auf das Auditing von Systemen selbst, den Status von Grid-Nodes, systemweite Task-Aktivitäten (Grid-Aufgaben) und Service-Backup-Vorgänge, sodass Sie potenzielle Probleme beheben können.

Codieren	Titel und Beschreibung der Nachricht	Siehe
ECMC	Datenfragment mit Löschmoder fehlt: Zeigt an, dass ein fehlendes Datenfragment mit Löschmoder erkannt wurde.	ECMC: Fehlendes Erasure coded Data Fragment
ECOC	Beschädigte Datenfragment mit Erasure-Code: Zeigt an, dass ein korruptes Datenfragment mit Löschmoder erkannt wurde.	ECOC: Korrupte, mit Erasure codierte Datenfragment
ETAF	Sicherheitsauthentifizierung fehlgeschlagen: Verbindungsversuch mit TLS (Transport Layer Security) fehlgeschlagen.	ETAF: Sicherheitsauthentifizierung fehlgeschlagen
GNRG	GNDS Registrierung: Ein Dienst aktualisiert oder registriert Informationen über sich selbst im StorageGRID-System.	GNRG: GNDS Registrierung
GNUR	GNDS Unregistrierung: Ein Dienst hat sich vom StorageGRID-System nicht registriert.	GNUR: GNDS Registrierung aufheben
GTED	Grid Task beendet: Der CMN-Dienst hat die Verarbeitung der Grid-Aufgabe abgeschlossen.	GTED: Grid Task beendet

Codieren	Titel und Beschreibung der Nachricht	Siehe
GTST	Grid Task gestartet: Der CMN-Dienst hat mit der Verarbeitung der Grid-Aufgabe begonnen.	GTST: Grid Task gestartet
GSU	Grid Task übermittelt: Eine Grid-Aufgabe wurde an den CMN-Dienst übermittelt.	GTSU: Grid Task übermittelt
IDEL	ILM-Initiated Delete: Diese Audit-Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.	IDEL: ILM gestartet Löschen
LKCU	Bereinigung Des Objekts Überschrieben. Diese Überwachungsmeldung wird erzeugt, wenn ein überschriebtes Objekt automatisch entfernt wird, um Speicherplatz freizugeben.	LKCU: Objektbereinigung überschrieben
LLST	Standort verloren: Diese Überwachungsmeldung wird generiert, wenn ein Standort verloren geht.	LLST: Standort verloren
OLST	Objekt verloren: Ein angeforderter Gegenstand kann nicht innerhalb des StorageGRID Systems gefunden werden.	OLST: System hat Lost Object erkannt
ORLM	Objektregeln erfüllt: Objektdaten werden gemäß den ILM-Regeln gespeichert.	ORLM: Objektregeln erfüllt
SADD	Sicherheitsüberprüfung deaktivieren: Die Protokollierung von Überwachungsnachrichten wurde deaktiviert.	SADD: Security Audit deaktiviert
SADE	Sicherheitsüberprüfung aktivieren: Die Protokollierung von Prüfnachrichten wurde wiederhergestellt.	SADE: Sicherheits-Audit aktivieren
SVRF	Objektspeicherüberprüfung fehlgeschlagen: Überprüfung durch einen Inhaltsblock fehlgeschlagen.	SVRF: Objektspeicherüberprüfung fehlgeschlagen

Codieren	Titel und Beschreibung der Nachricht	Siehe
SVRU	Objektspeicher Verify Unbekannt: Unerwartete Objektdaten im Objektspeicher erkannt.	SVRU: Objektspeicher überprüfen Unbekannt
SYSD	Knotenstopp: Es wurde ein Herunterfahren angefordert.	SYSD: Knoten stoppen
SYST	Knoten stoppen: Ein Dienst hat einen graziösen Stopp initiiert.	SYST: Knoten wird angehalten
SYSU	Node Start: Ein Dienst gestartet. In der Meldung wird der Charakter des vorherigen Herunterfahrens angezeigt.	SYSU: Knoten Start
VLST	Vom Benutzer Initiiertes Volume Verloren: Das <code>/proc/CMSI/Volume_Lost</code> Befehl wurde ausgeführt.	VLST: Vom Benutzer initiiertes Volumen verloren

Verwandte Informationen

[LKCU: Objektbereinigung überschrieben](#)

Audit-Meldungen zu Objekt-Storage

Sie sollten mit Audit-Meldungen vertraut sein, die zur Objektspeicheraudits-Kategorie gehören. Dies sind Ereignisse, die mit der Speicherung und dem Management von Objekten innerhalb des StorageGRID Systems zusammenhängen. Dazu zählen Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Verifizierungen.

Codieren	Beschreibung	Siehe
APCT	Archiv aus Cloud-Tier: Archivierte Objektdaten werden aus einem externen Archiv-Storage-System gelöscht, das über die S3-API eine Verbindung zur StorageGRID herstellt.	APCT: Löschen von Archiven aus der Cloud-Ebene
ARCB	Archiv Objekt abrufen Begin: Der ARC-Dienst beginnt den Abruf von Objektdaten aus dem externen Archivspeichersystem.	ARCB: Archiv Objekt abrufen beginnen

Codieren	Beschreibung	Siehe
ARCE	Archivobjekt Retrieve End: Objektdaten wurden von einem externen Archivspeichersystem abgerufen, und der ARC-Dienst meldet den Status des Abruffvorgangs.	ARCE: Archiv Objekt abrufen Ende
ARCT	Archive Retrieve von Cloud-Tier: Archivierte Objektdaten werden von einem externen Archiv-Storage-System abgerufen, das über die S3-API eine Verbindung zur StorageGRID herstellt.	ARCT: Archiv Abrufen aus Cloud-Tier
AREM	Archiv Objekt entfernen: Ein Inhaltsblock wurde erfolgreich oder erfolglos aus dem externen Archiv-Speichersystem gelöscht.	ARM: Archivobjekt Entfernen
ASCE	Archiv Objekt Store Ende: Ein Inhaltsblock wurde auf das externe Archivspeichersystem geschrieben und der ARC-Dienst meldet den Status des Schreibvorgangs.	ASCE: Archiv-Objektspeicher Ende
ASCT	Archivspeicher Cloud-Tier: Objektdaten werden in einem externen Archiv-Storage-System gespeichert, das über die S3-API eine Verbindung zur StorageGRID herstellt.	ASCT: Archivspeicher Cloud-Tier
ATCE	Archive Object Store Begin: Das Schreiben eines Inhaltsblocks in einen externen Archiv-Speicher hat begonnen.	ATCE: Archiv-Objektspeicher beginnen
AVCC	Archiv Validierung der Cloud-Tier-Konfiguration: Die angegebenen Account- und Bucket-Einstellungen wurden erfolgreich oder nicht erfolgreich validiert.	AVCC: Archiv Validierung der Cloud-Tier-Konfiguration
CBSES	Objekt Send End: Die Quelleinheit hat einen Grid-Node zum Grid-Node-Datentransfer abgeschlossen.	CBSE: Objekt Senden Ende

Codieren	Beschreibung	Siehe
CBRE	Empfang des Objekts: Die Zieleinheit hat einen Grid-Node zum Datentransfer des Grid-Node abgeschlossen.	CBRE: Das Objekt erhält das Ende
SCMT	Object Store Commit: Ein Inhaltsblock wurde vollständig gespeichert und verifiziert und kann nun angefordert werden.	SCMT: Objekt Store Commit
SREM	Objektspeicher Remove: Ein Inhaltsblock wurde von einem Grid-Knoten gelöscht und kann nicht mehr direkt angefordert werden.	SREM: Objektspeicher Entfernen

Client liest Audit-Meldungen

Client-Read-Audit-Meldungen werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Abrufen eines Objekts vorgibt.

Codieren	Beschreibung	Verwendet von	Siehe
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	SGET S3 ABRUFEN
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.	S3-Client	SHEA: S3 KOPF
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten.	Swift Client	WGET: Schneller ERHALTEN

Codieren	Beschreibung	Verwendet von	Siehe
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.	Swift Client	WHEA: Schneller KOPF

Audit-Meldungen des Clients schreiben

Audit-Meldungen zu Clientschreibmeldungen werden protokolliert, wenn eine S3- oder Swift-Client-Applikation eine Anforderung zum Erstellen oder Ändern eines Objekts macht.

Codieren	Beschreibung	Verwendet von	Siehe
OVWR	Objekt-Überschreiben: Protokolliert eine Transaktion, um ein Objekt mit einem anderen Objekt zu überschreiben.	S3-Clients Swift Clients	OVWR: Objektüberschreibung
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	SDEL: S3 LÖSCHEN
SPOS	S3 POST: Protokolliert eine erfolgreiche Transaktion zur Wiederherstellung eines Objekts aus AWS Glacier Storage in einem Cloud Storage Pool.	S3-Client	SPOS: S3-BEITRAG

Codieren	Beschreibung	Verwendet von	Siehe
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen. Hinweis: Wenn die Transaktion auf einer Unterressource ausgeführt wird, enthält die Audit-Nachricht das Feld S3SR.	S3-Client	SPUT: S3 PUT
SUPD	Aktualisierte S3 Metadaten: Protokolliert eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes Objekt oder Bucket.	S3-Client	SUPD: S3-Metadaten wurden aktualisiert
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	Swift Client	WDEL: Swift LÖSCHEN
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.	Swift Client	WPUT: Schnell AUSGEDRÜCKT

Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API.

Codieren	Titel und Beschreibung der Nachricht	Siehe
MGAU	Management-API-Audit-Nachricht: Ein Protokoll von Benutzeranfragen.	MGAU: Management-Audit-Nachricht

Referenz für Überwachungsmeldung

APCT: Löschen von Archiven aus der Cloud-Ebene

Diese Meldung wird erzeugt, wenn archivierte Objektdaten aus einem externen Storage-System gelöscht werden, das eine Verbindung zur StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den gelöschten Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte. Gibt immer 0 zurück.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Eindeutige Kennung (UUID) des Cloud-Tiers, aus dem das Objekt gelöscht wurde.

ARCB: Archiv Objekt abrufen beginnen

Diese Meldung wird erzeugt, wenn eine Anfrage zum Abrufen der archivierten Objektdaten gestellt wird und der Abrufvorgang beginnt. Abrufanfragen werden sofort bearbeitet, können jedoch neu geordnet werden, um die Effizienz des Abrufs von linearen Medien wie z. B. Bandmedien zu verbessern.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivspeichersystem abgerufen werden soll.
RSLT	Ergebnis	Zeigt das Ergebnis des Speicherabrufs an. Aktuell definierter Wert ist:SUCS: Die Inhaltsanforderung wurde empfangen und zum Abruf in die Warteschlange gestellt.

Diese Überwachungsmeldung markiert den Zeitpunkt eines Archivabrufs. Damit können Sie die Nachricht mit einer entsprechenden ARCE-End-Nachricht abgleichen, um die Dauer des Archivabrufs zu bestimmen und ob der Vorgang erfolgreich war.

ARCE: Archiv Objekt abrufen Ende

Diese Meldung wird erzeugt, wenn ein Versuch des Archiv-Knotens, Objektdaten von

einem externen Archivspeichersystem abzurufen, abgeschlossen wird. Wenn die Meldung erfolgreich ist, zeigt die Meldung an, dass die angeforderten Objektdaten vollständig aus dem Archivverzeichnis gelesen und erfolgreich verifiziert wurden. Nachdem die Objektdaten abgerufen und verifiziert wurden, werden sie an den anfragenden Service geliefert.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivspeichersystem abgerufen werden soll.
VLID	Volume-Kennung	Die Kennung des Volumes, auf dem die Daten archiviert wurden. Wenn kein Archivverzeichnis für den Inhalt gefunden wird, wird eine Volume-ID von 0 zurückgegeben.
RSLT	Abrufergebnis	Der Abschlussstatus des Archivabrufs: • ERFOLGREICH • VRFL: Fehlgeschlagen (Objektverifizierung fehlgeschlagen) • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • STORNO: Fehlgeschlagen (Abrufvorgang abgebrochen) • GERR: Fehlgeschlagen (allgemeiner Fehler)

Wenn Sie diese Nachricht mit der entsprechenden ARCB-Nachricht abstimmen, können Sie die Zeit angeben, die für den Archivabruf benötigt wurde. Diese Meldung gibt an, ob der Abruf erfolgreich war, und im Falle eines Fehlers die Ursache für das Abrufen des Inhaltsblocks.

ARCT: Archiv Abrufen aus Cloud-Tier

Diese Meldung wird generiert, wenn archivierte Objektdaten von einem externen Archiv-Storage-System abgerufen werden, das eine Verbindung mit der StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den abgerufenen Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte. Der Wert ist nur für erfolgreiche Abrufen genau.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Unique Identifier (UUID) des externen Archivspeichersystems.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

ARM: Archivobjekt Entfernen

Die Meldung „Archiv Objekt entfernen“ zeigt an, dass ein Inhaltsblock erfolgreich oder nicht erfolgreich von einem Archiv-Knoten gelöscht wurde. Wenn das Ergebnis erfolgreich ist, hat der Archivknoten das externe Archivspeichersystem erfolgreich darüber informiert, dass StorageGRID einen Objektspeicherort freigegeben hat. Ob das Objekt aus dem externen Archivspeichersystem entfernt wird, hängt vom Systemtyp und dessen Konfiguration ab.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des Inhaltsblocks, der vom externen Archivmediensystem abgerufen werden soll.
VLID	Volume-Kennung	Die Kennung des Volumes, auf dem die Objektdaten archiviert wurden.
RSLT	Ergebnis	Der Abschlussstatus des Löschvorgangs für das Archiv: • ERFOLGREICH • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • GERR: Fehlgeschlagen (allgemeiner Fehler)

Diese Meldung zeigt an, dass das Schreiben eines Inhaltsblocks in ein externes Archiv-Speichersystem beendet ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die Kennung des Inhaltsblocks, der auf dem externen Archivspeichersystem gespeichert ist.
VLID	Volume-Kennung	Die eindeutige Kennung des Archiv-Volume, auf das die Objektdaten geschrieben werden.
VREN	Überprüfung Aktiviert	Zeigt an, ob eine Überprüfung für Inhaltsblöcke durchgeführt wird. Aktuell definierte Werte sind: • VENA: Die Überprüfung ist aktiviert • VDSA: Die Überprüfung ist deaktiviert
MCLS	Management-Klasse	Eine Zeichenfolge, die die TSM-Managementklasse identifiziert, der der Inhaltsblock zugeordnet ist, falls zutreffend.
RSLT	Ergebnis	Zeigt das Ergebnis des Archivierungsvorgangs an. Aktuell definierte Werte sind: • ERFOLGREICH (Archivierungsprozess erfolgreich) • OFFL: Fehlgeschlagen (Archivierung ist offline) • VRFL: Fehlgeschlagen (Objektüberprüfung fehlgeschlagen) • ARUN: Fehlgeschlagen (externes Archiv-Storage-System nicht verfügbar) • GERR: Fehlgeschlagen (allgemeiner Fehler)

Diese Überwachungsmeldung bedeutet, dass der angegebene Inhaltsblock auf das externe Archivspeichersystem geschrieben wurde. Wenn der Schreibvorgang fehlschlägt, liefert das Ergebnis

grundlegende Informationen zur Fehlerbehebung über den Fehlerort. Ausführlichere Informationen zu Archivfehlern finden Sie unter Untersuchung der Attribute von Archivierungs-Knoten im StorageGRID System.

ASCT: Archivspeicher Cloud-Tier

Diese Meldung wird generiert, wenn archivierte Objektdaten in einem externen Storage-System gespeichert werden, das eine Verbindung mit StorageGRID über die S3-API herstellt.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung für den abgerufenen Inhaltsblock.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	Unique Identifier (UUID) des Cloud-Tiers, in dem der Inhalt gespeichert wurde.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

ATCE: Archiv-Objektspeicher beginnen

Diese Meldung weist darauf hin, dass das Schreiben eines Inhaltsblocks in einen externen Archivspeicher gestartet wurde.

Codieren	Feld	Beschreibung
CBID	Inhaltsblock-ID	Die eindeutige Kennung des zu archivierenden Inhaltsblocks.
VLID	Volume-Kennung	Die eindeutige Kennung des Volumes, auf das der Inhaltsblock geschrieben wird. Wenn der Vorgang fehlschlägt, wird eine Volume-ID von 0 zurückgegeben.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Gibt das Ergebnis der Übertragung des Inhaltsblocks an. Aktuell definierte Werte sind: • ERFOLGREICH (Inhaltsblock erfolgreich gespeichert) • EXIS: Ignoriert (Inhaltsblock wurde bereits gespeichert) • ISFD: Fehlgeschlagen (nicht genügend Speicherplatz) • STER: Fehlgeschlagen (Fehler beim Speichern der CBID) • OFFL: Fehlgeschlagen (Archivierung ist offline) • GERR: Fehlgeschlagen (allgemeiner Fehler)

AVCC: Archiv Validierung der Cloud-Tier-Konfiguration

Diese Meldung wird generiert, wenn die Konfigurationseinstellungen für einen Cloud Tiering – Simple Storage Service (S3)-Zieltyp validiert werden.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.
SUID	Eindeutige Kennung Für Speicher	UUID, die dem validierten externen Archivspeichersystem zugeordnet ist.

CBRB: Objekt empfangen beginnen

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn der Transfer eines Inhaltsblocks von einem Node zum anderen initiiert wird, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBRE: Das Objekt erhält das Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen

abgeschlossen ist, wird diese Meldung von der Zieleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.

Codieren	Feld	Beschreibung
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung endete aufgrund des Empfangs von beschädigten oder ungültigen Daten (kann auf Manipulation hinweisen)

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

CBSB: Objektsendebeginn

Während des normalen Systembetriebs werden Content-Blöcke kontinuierlich zwischen verschiedenen Nodes übertragen, wenn auf die Daten zugegriffen wird, repliziert und aufbewahrt werden. Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen initiiert wird, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.

Codieren	Feld	Beschreibung
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Zeigt die erste angeforderte Sequenzanzahl an. Wenn der Transfer erfolgreich war, beginnt die Anzahl dieser Sequenz.
CES	Erwartete Anzahl Der Endsequenzen	Zeigt die letzte angeforderte Sequenzanzahl an. Wenn die Übertragung erfolgreich war, gilt sie als abgeschlossen, wenn diese Sequenzzahl empfangen wurde.
RSLT	Startstatus Übertragen	Status zum Zeitpunkt des Startes der Übertragung: SUCS: Übertragung erfolgreich gestartet.

Diese Überwachungsmeldung bedeutet, dass ein Vorgang der Datenübertragung zwischen Knoten und Knoten auf einem einzelnen Inhaltselement initiiert wurde, wie er durch seine Content Block Identifier identifiziert wurde. Der Vorgang fordert Daten von „Startreihenanzahl“ bis „erwartete Ende-Sequenz-Anzahl“ an. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können zur Nachverfolgung des Systemdatenflusses und in Kombination mit Storage-Audit-Meldungen zur Überprüfung der Replikatanzahl verwendet werden.

CBSE: Objekt Senden Ende

Wenn die Übertragung eines Inhaltsblocks von einem Node auf einen anderen abgeschlossen ist, wird diese Meldung von der Quelleinheit ausgegeben.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Kennung der Node-to-Node-Sitzung/-Verbindung.
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des zu übertragenden Inhaltsblocks.
CTDR	Übertragungsrichtung	Gibt an, ob die CBID-Übertragung Push-Initiierung oder Pull-Initiierung war: PUSH: Der Übertragungsvorgang wurde von der sendenden Einheit angefordert. PULL: Der Transfer-Vorgang wurde von der empfangenden Einheit angefordert.
CTSR	Quelleinheit	Die Knoten-ID der Quelle (Absender) der CBID-Übertragung.
CTDS	Zieleinheit	Die Knoten-ID des Ziels (Empfänger) der CBID-Übertragung.
CTSS	Startreihenanzahl	Gibt die Anzahl der Sequenzen an, auf denen die Übertragung gestartet wurde.
CTAS	Tatsächliche Endsequenz Anzahl	Zeigt die letzte erfolgreich übertragene Sequenzzahl an. Wenn die Anzahl der tatsächlichen Endsequenzen mit der Anzahl der Startsequenzen identisch ist und das Ergebnis der Übertragung nicht erfolgreich war, wurden keine Daten ausgetauscht.

Codieren	Feld	Beschreibung
RSLT	Übertragungsergebnis	Das Ergebnis der Übertragungsoperation (aus der Perspektive der sendenden Einheit): SUCS: Übertragung erfolgreich abgeschlossen; alle angeforderten Sequenzzählungen wurden gesendet. CONL: Verbindung während der Übertragung unterbrochen CTMO: Zeitüberschreitung der Verbindung während der Einrichtung oder Übertragung UNRE: Ziel-Node-ID nicht erreichbar CRPT: Übertragung endete aufgrund des Empfangs von beschädigten oder ungültigen Daten (kann auf Manipulation hinweisen)

Diese Meldung bedeutet, dass der Datentransfer zwischen Nodes abgeschlossen wurde. Wenn das Ergebnis der Übertragung erfolgreich war, übermittelte der Vorgang Daten von „Startreihenanzahl“ in „tatsächliche Endsequenzanzahl“. Sendende und empfangende Nodes werden durch ihre Node-IDs identifiziert. Diese Informationen können verwendet werden, um den Datenfluss des Systems zu verfolgen und Fehler zu lokalisieren, zu tabulieren und zu analysieren. In Kombination mit Storage-Audit-Meldungen kann sie auch zur Überprüfung der Replikatanzahl verwendet werden.

ECMC: Fehlendes Erasure coded Data Fragment

Diese Meldung zeigt an, dass das System ein fehlendes Datenfragment mit Löschungscode erkannt hat.

Codieren	Feld	Beschreibung
VCMC	VCS-ID	Der Name des VCS, der den fehlenden Teil enthält.
MCID	Block-ID	Der Bezeichner des fehlenden Fragments mit Löschungscode.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ECOC: Korrupte, mit Erasure codierte Datenfragment

Diese Meldung zeigt an, dass das System ein korruptes Datenfragment mit Lösungscode erkannt hat.

Codieren	Feld	Beschreibung
VCCO	VCS-ID	Der Name des VCS, der den beschädigten Teil enthält.
VLID	Volume-ID	Das RangeDB-Volume, das das korrupte Fragment mit Lösungscode enthält.
CCID	Block-ID	Der Identifier des beschädigten Fragments zur Löschung.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein obligatorisches Nachrichtenfeld, ist aber für diese bestimmte Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

ETAF: Sicherheitsauthentifizierung fehlgeschlagen

Diese Meldung wird erzeugt, wenn ein Verbindungsversuch mit Transport Layer Security (TLS) fehlgeschlagen ist.

Codieren	Feld	Beschreibung
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung, über die die Authentifizierung fehlgeschlagen ist.

Codieren	Feld	Beschreibung
RUID	Benutzeridentität	Eine dienstabhängige Kennung, die die Identität des Remote-Benutzers darstellt.
RSLT	Ursachencode	Der Grund für den Fehler: SCNI: Sichere Verbindungseinrichtung fehlgeschlagen. CERM: Zertifikat fehlt. Zertifikat: Zertifikat war ungültig. CERE: Das Zertifikat ist abgelaufen. CERR: Zertifikat wurde widerrufen. CSGN: Die Zertifikatsignatur war ungültig. CSGU: Zertifikatssignator war unbekannt. UCRM: Benutzerkennungen fehlten. UCRI: Die Benutzeranmeldeinformationen waren ungültig. UCRU: Benutzeranmeldeinformationen wurden nicht zulässig. TOUT: Zeitüberschreitung bei der Authentifizierung.

Wenn eine Verbindung zu einem sicheren Service hergestellt wird, der TLS verwendet, werden die Anmeldeinformationen der Remote-Einheit mithilfe des TLS-Profiles und der zusätzlichen Logik, die in den Service integriert ist, überprüft. Wenn diese Authentifizierung aufgrund ungültiger, unerwarteter oder unzulässiger Zertifikate oder Anmeldeinformationen fehlschlägt, wird eine Überwachungsmeldung protokolliert. Dies ermöglicht Abfragen für nicht autorisierte Zugriffsversuche und andere sicherheitsrelevante Verbindungsprobleme.

Die Meldung kann dazu führen, dass eine Remoteeinheit eine falsche Konfiguration hat oder dass versucht wird, ungültige oder unzulässige Anmeldedaten für das System vorzulegen. Diese Überwachungsmeldung sollte überwacht werden, um Versuche zu erkennen, unbefugten Zugriff auf das System zu erlangen.

GNRG: GNDS Registrierung

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst Informationen über sich selbst im StorageGRID-System aktualisiert oder registriert hat.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.
GNTTP	Gerätetyp	Der Gerätetyp des Grid-Knotens (z. B. BLDR für einen LDR-Dienst).
GNDV	Modellversion des Geräts	Der String, der die Gerätemodellversion des Grid-Knotens im DMDL-Bundle identifiziert.
GNGP	Gruppieren	Die Gruppe, zu der der Grid-Knoten gehört (im Zusammenhang mit Verbindungskosten und Service-Query-Ranking).
GNIA	IP-Adresse	Die IP-Adresse des Grid-Node.

Diese Meldung wird generiert, wenn ein Grid-Knoten seinen Eintrag im Grid-Knoten-Paket aktualisiert.

GNUR: GNDS Registrierung aufheben

Der CMN-Dienst generiert diese Prüfmeldung, wenn ein Dienst nicht registrierte Informationen über sich selbst vom StorageGRID-System enthält.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis der Aktualisierungsanfrage: • ERFOLGREICH • SUNV: Dienst nicht verfügbar • GERR: Anderer Fehler

Codieren	Feld	Beschreibung
GNID	Node-ID	Die Node-ID des Service, der die Update-Anforderung initiiert hat.

GTED: Grid Task beendet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst die Verarbeitung der angegebenen Rasteraufgabe abgeschlossen hat und die Aufgabe in die Tabelle „Historisch“ verschoben hat. Wenn es sich um SUCS, ABRT oder ROLF handelt, wird eine entsprechende Überwachungsmeldung für die mit Grid Task gestartete Aufgabe angezeigt. Die anderen Ergebnisse zeigen, dass die Verarbeitung dieser Grid-Aufgabe nie gestartet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Grid-Aufgabe über den gesamten Lebenszyklus. Hinweis: die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das endgültige Statusergebnis der Grid-Aufgabe: • SUCS: Die Grid-Aufgabe wurde erfolgreich abgeschlossen. • ABRT: Die Grid-Aufgabe wurde ohne einen Rollback-Fehler abgebrochen. • ROLF: Die Grid-Aufgabe wurde abgebrochen und konnte den Rollback-Vorgang nicht abschließen. • STORNO: Die Grid-Aufgabe wurde vom Benutzer vor dem Start abgebrochen. • EXPR: Der Grid-Task ist vor dem Start abgelaufen. • IVLD: Die Grid-Aufgabe war ungültig. • AUTH: Die Grid-Aufgabe war nicht zulässig. • DUPL: Die Grid-Aufgabe wurde als Duplikat abgelehnt.

GTST: Grid Task gestartet

Diese Überwachungsmeldung zeigt an, dass der CMN-Dienst mit der Verarbeitung der angegebenen Grid-Aufgabe begonnen hat. Die Meldung „Audit“ folgt unmittelbar der Nachricht „Grid Task Submission Submitted“ für Grid-Aufgaben, die vom internen Grid Task Submission Service initiiert und für die automatische Aktivierung ausgewählt wurde. Für Grid-Aufgaben, die in die Tabelle „Ausstehend“ eingereicht werden, wird diese Meldung generiert, wenn der Benutzer die Grid-Aufgabe startet.

Codieren	Feld	Beschreibung
TSID	Task-ID	Dieses Feld identifiziert eine generierte Grid-Aufgabe eindeutig und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. Hinweis: die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.
RSLT	Ergebnis	Das Ergebnis. Dieses Feld hat nur einen Wert: • SUCS: Die Grid-Aufgabe wurde erfolgreich gestartet.

GTSU: Grid Task übermittelt

Diese Überwachungsmeldung zeigt an, dass eine Grid-Aufgabe an den CMN-Dienst gesendet wurde.

Codieren	Feld	Beschreibung
TSID	Task-ID	Identifiziert eindeutig eine generierte Grid-Aufgabe und ermöglicht die Verwaltung der Aufgabe über den gesamten Lebenszyklus. Hinweis: die Task-ID wird zum Zeitpunkt der Erstellung einer Grid-Aufgabe zugewiesen, nicht zum Zeitpunkt der Einreichung. Es ist möglich, dass eine bestimmte Grid-Aufgabe mehrfach eingereicht wird. In diesem Fall reicht das Feld Task-ID nicht aus, um die übermittelten, gestarteten und beendeten Audit-Meldungen eindeutig zu verknüpfen.

Codieren	Feld	Beschreibung
TTYP	Aufgabentyp	Der Typ der Rasteraufgabe.
TVER	Aufgabenversion	Eine Zahl, die die Version der Grid-Aufgabe angibt.
TDSC	Aufgabenbeschreibung	Eine vom Menschen lesbare Beschreibung der Grid-Aufgabe.
VATS	Gültig Nach Zeitstempel	Die früheste Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX-Zeit), zu der die Grid-Aufgabe gültig ist.
VBTS	Gültig Vor Zeitstempel	Die letzte Zeit (UINT64 Mikrosekunden ab 1. Januar 1970 - UNIX Zeit), zu der die Grid-Aufgabe gültig ist.
TSRC	Quelle	Die Quelle der Aufgabe: • TXTB: Die Grid-Aufgabe wurde über das StorageGRID-System als signierter Textblock gesendet. • GRID: Die Grid-Aufgabe wurde über den internen Grid Task Submit Service übermittelt.
ACTV	Aktivierungstyp	Die Art der Aktivierung: • AUTO: Die Grid-Aufgabe wurde zur automatischen Aktivierung eingereicht. • PEND: Die Grid-Aufgabe wurde in die ausstehende Tabelle übermittelt. Dies ist die einzige Möglichkeit für die TXTB-Quelle.
RSLT	Ergebnis	Das Ergebnis der Einreichung: • SUCS: Die Grid-Aufgabe wurde erfolgreich übermittelt. • FAIL: Die Aufgabe wurde direkt in die historische Tabelle verschoben.

Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet.

Die IDEL-Nachricht wird in einer der folgenden Situationen erzeugt:

- **Für Objekte in konformen S3-Buckets:** Diese Meldung wird generiert, wenn ILM den Prozess des automatischen Löschens eines Objekts startet, da der Aufbewahrungszeitraum abgelaufen ist (vorausgesetzt, die Einstellung zum automatischen Löschen ist aktiviert und die Legal Hold ist deaktiviert).
- **Für Objekte in nicht konformen S3 Buckets oder Swift Containern.** Diese Meldung wird generiert, wenn ILM den Prozess zum Löschen eines Objekts startet, da derzeit keine Platzierungsanweisungen in der aktiven ILM-Richtlinie für das Objekt gelten.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CMPA	Compliance: Automatisches Löschen	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true) geben an, ob ein konformes Objekt automatisch gelöscht werden soll, wenn der Aufbewahrungszeitraum endet, es sei denn, der Bucket befindet sich unter einer gesetzlichen Aufbewahrungspflichten.
CMPL	Einhaltung: Gesetzliche Aufbewahrungspflichten	Nur für Objekte in S3-konformen Buckets. 0 (false) oder 1 (true), die angeben, ob der Bucket derzeit unter einer gesetzlichen Aufbewahrungspflichten steht.
CMPR	Compliance: Aufbewahrungszeitraum	Nur für Objekte in S3-konformen Buckets. Die Länge der Aufbewahrungsdauer des Objekts in Minuten.
CTME	Compliance: Aufnahmezeit	Nur für Objekte in S3-konformen Buckets. Die Aufnahmezeit des Objekts. Sie können den Aufbewahrungszeitraum in Minuten zu diesem Wert hinzufügen, um zu bestimmen, wann das Objekt aus dem Bucket gelöscht werden kann.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.

Codieren	Feld	Beschreibung
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte mit Erasure-Coding-Verfahren, die Profil-ID für das Erasure-Coding-Verfahren und die Gruppen-ID für das Erasure-Coding-Verfahren, die auf die Daten des Objekts angewendet werden. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	• Wenn ein Objekt in einem konformen S3-Bucket automatisch gelöscht wird, weil der Aufbewahrungszeitraum abgelaufen ist, ist dieses Feld leer. • Wenn das Objekt gelöscht wird, da derzeit keine Anweisungen zur Platzierung für das Objekt vorhanden sind, zeigt dieses Feld den vom Menschen lesbaren Namen der letzten ILM-Regel an, die auf das Objekt angewendet wurde.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

LKCU: Objektbereinigung überschrieben

Diese Meldung wird generiert, wenn StorageGRID ein überschriebenes Objekt entfernt, das zuvor zur Freigabe von Speicherplatz erforderlich war. Ein Objekt wird überschrieben, wenn ein S3- oder Swift-Client ein Objekt in einen Pfad schreibt, der bereits ein Objekt enthält. Die Entfernung erfolgt automatisch und im Hintergrund.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
LTyp	Art der Bereinigung	<i>Nur zur internen Verwendung.</i>
LUID	Objekt-UUID entfernt	Die Kennung des entfernten Objekts.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
UUID	Universell Eindeutige Kennung	Die Kennung des noch vorhandenen Objekts. Dieser Wert ist nur verfügbar, wenn das Objekt nicht gelöscht wurde.

LLST: Standort verloren

Diese Meldung wird immer dann erzeugt, wenn ein Speicherort für eine Objektkopie (repliziert oder Erasure Coding) nicht gefunden werden kann.

Codieren	Feld	Beschreibung
CBIL	CBID	Die betroffene CBID.
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
UUID	Universally Unique ID	Die Kennung des betroffenen Objekts im StorageGRID-System.
ECPR	Verfahren Zur Einhaltung Von Datenkonsistenz	Für Erasure-Coding-Objektdaten. Die ID des verwendeten Erasure Coding-Profiles.

Codieren	Feld	Beschreibung
LTYP	Positionstyp	CLDI (Online): Für replizierte Objektdaten CLEC (Online): Für Erasure-codierte Objektdaten CLNL (Nearline): Für archivierte replizierte Objektdaten
PCLD	Pfad zu repliziertem Objekt	Der vollständige Pfad zum Speicherort der verlorenen Objektdaten. Wird nur zurückgegeben, wenn LTYP einen Wert von CLDI (d.h. für replizierte Objekte) hat. Nimmt das Formular an <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Ergebnis	Immer KEINE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.
TSRC	Auslösequelle	BENUTZER: Benutzer ausgelöst SYST: System ausgelöst

MGAU: Management-Audit-Nachricht

Die Kategorie Management protokolliert Benutzeranfragen an die Management-API. Jede Anfrage, die keine GET- oder HEAD-Anforderung an die API ist, protokolliert eine Antwort mit dem Benutzernamen, der IP und der Art der Anfrage an die API.

Codieren	Feld	Beschreibung
MDIP	Ziel-IP-Adresse	Die IP-Adresse des Servers (Ziel).
MDNA	Domain-Name	Der Host-Domain-Name.
MPAT	AnfraPfad	Der Anfraspfad.
MPQP	Abfrageparameter anfordern	Die Abfrageparameter für die Anforderung.

Codieren	Feld	Beschreibung
MRBD	Text anfordern	Der Inhalt des Anforderungsinstanz. Während der Antwortkörper standardmäßig protokolliert wird, wird der Anforderungskörper in bestimmten Fällen protokolliert, wenn der Antwortkörper leer ist. Da die folgenden Informationen im Antwortkörper nicht verfügbar sind, werden sie von der Anforderungsstelle für die folgenden POST-Methoden übernommen: • Benutzername und Konto-ID in POST authorize • Neue Subnetze-Konfiguration in POST /Grid/Grid-Networks/Update • Neue NTP-Server in POST /grid/ntp-Servers/Update • Ausgemusterte Server-IDs in POST /Grid/Servers/Decommission Hinweis: sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MRMD	Anforderungsmethode	Die HTTP-Anforderungsmethode: • POST • PUT • Löschen • PATCH
MRSC	Antwortcode	Der Antwortcode.

Codieren	Feld	Beschreibung
MRSP	Antwortkörper	Der Inhalt der Antwort (der Antwortkörper) wird standardmäßig protokolliert. Hinweis: sensible Daten werden entweder gelöscht (z. B. ein S3-Zugriffsschlüssel) oder mit Sternchen (z. B. ein Passwort) maskiert.
MSIP	Quell-IP-Adresse	Die Client (Quell-) IP-Adresse.
MUUN	User-URN	Der URN (einheitlicher Ressourcename) des Benutzers, der die Anforderung gesendet hat.
RSLT	Ergebnis	Gibt erfolgreich (SUCS) oder den Fehler zurück, der vom Backend gemeldet wurde.

OLST: System hat Lost Object erkannt

Diese Meldung wird erzeugt, wenn der DDS-Dienst keine Kopien eines Objekts im StorageGRID-System finden kann.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die CBID des verlorenen Objekts.
NID	Node-ID	Falls verfügbar, der letzte bekannte direkte oder Nearline-Speicherort des verlorenen Objekts. Es ist möglich, nur die Knoten-ID ohne eine Volume-ID zu haben, wenn die Volume-Informationen nicht verfügbar sind.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Falls verfügbar: Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Codieren	Feld	Beschreibung
UUID	Universally Unique ID	Die Kennung des verlorenen Objekts im StorageGRID System.
VOLI	Volume-ID	Falls verfügbar, die Volume-ID des Speicherknoten oder Archiv-Knotens für den letzten bekannten Speicherort des verlorenen Objekts.

ORLM: Objektregeln erfüllt

Diese Meldung wird generiert, wenn das Objekt erfolgreich gespeichert und wie durch die ILM-Regeln festgelegt kopiert wird.



Die ORLM-Meldung wird nicht generiert, wenn ein Objekt erfolgreich mit der Regel 2 Kopien erstellen gespeichert wird, wenn eine andere Regel in der Richtlinie den erweiterten Filter Objektgröße verwendet.

Codieren	Feld	Beschreibung
BUID	Bucket-Header	Bucket-ID-Feld Wird für interne Vorgänge verwendet. Wird nur angezeigt, wenn STAT PRGD ist.
CBID	Kennung Für Inhaltsblock	Die CBID des Objekts.
CSIZ	Inhaltsgröße	Die Größe des Objekts in Byte.
STANDORT	Standorte	Der Speicherort von Objektdaten im StorageGRID System. Der Wert für GEBIETSSCHEMA lautet „“, wenn das Objekt keine Speicherorte hat (zum Beispiel wurde es gelöscht). CLEC: Für Objekte mit Erasure-Coding-Verfahren, die Profil-ID für das Erasure-Coding-Verfahren und die Gruppen-ID für das Erasure-Coding-Verfahren, die auf die Daten des Objekts angewendet werden. CLDI: Für replizierte Objekte, die LDR-Node-ID und die Volume-ID des Objektstandorts. CLNL: LICHTBOGENKNOTEN-ID des Objektes, wenn die Objektdaten archiviert werden.
PFAD	S3 Bucket/Key oder Swift Container/Objekt-ID	Der S3-Bucket-Name und der S3-Schlüsselname oder der Swift-Container-Name und die Swift-Objektkennung.

Codieren	Feld	Beschreibung
RSLT	Ergebnis	Das Ergebnis des ILM-Vorgangs. SUCS: Der ILM-Vorgang war erfolgreich.
REGEL	Regelbezeichnung	Das von Menschen lesbare Etikett, das der ILM-Regel gegeben wurde, die auf dieses Objekt angewendet wurde.
SEGC	Container-UUID	UUID des Containers für das segmentierte Objekt. Dieser Wert ist nur verfügbar, wenn das Objekt segmentiert ist.
SGCB	Container-CBID	CBID des Containers für das segmentierte Objekt. Dieser Wert ist nur für segmentierte und mehrteilige Objekte verfügbar.
STAT	Status	Der Status des ILM-Betriebs. FERTIG: ILM-Vorgänge für das Objekt wurden abgeschlossen. DFER: Das Objekt wurde für zukünftige ILM-Neuevaluierungen markiert. PRGD: Das Objekt wurde aus dem StorageGRID-System gelöscht. NLOC: Die Objektdaten können nicht mehr im StorageGRID-System gefunden werden. Dieser Status kann darauf hinweisen, dass alle Kopien von Objektdaten fehlen oder beschädigt sind.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.

Die ORLM-Überwachungsmeldung kann für ein einzelnes Objekt mehrmals ausgegeben werden. Sie wird beispielsweise ausgegeben, wenn eines der folgenden Ereignisse stattfindet:

- ILM-Regeln für das Objekt sind dauerhaft erfüllt.
- ILM-Regeln für das Objekt werden für diese Epoche erfüllt.
- Das Objekt wurde durch ILM-Regeln gelöscht.
- Bei der Hintergrundüberprüfung wird erkannt, dass eine Kopie replizierter Objektdaten beschädigt ist. Das StorageGRID System führt eine ILM-Bewertung durch, um das beschädigte Objekt zu ersetzen.

Verwandte Informationen

- [Objektaufnahme von Transaktionen](#)
- [Löschen von Objekttransaktionen](#)

OVWR: Objektüberschreibung

Diese Meldung wird erzeugt, wenn ein externer (Client-angeforderter) Vorgang ein Objekt durch ein anderes Objekt überschrieben.

Codieren	Feld	Beschreibung
CBID	Kennung für Inhaltsblock (neu)	Die CBID für das neue Objekt.
CSIZ	Vorherige Objektgröße	Die Größe des Objekts in Byte, das überschrieben wird.
OCBD	Kennung für Inhaltsblock (vorherige)	Die CBID für das vorherige Objekt.
UUID	Universally Unique ID (neu)	Die Kennung des neuen Objekts im StorageGRID System.
OID	Universally Unique ID (vorherige)	Die Kennung für das vorherige Objekt innerhalb des StorageGRID-Systems.
PFAD	S3 oder Swift Objektpfad	Der S3- oder Swift-Objektpfad wird sowohl für das vorherige als auch für das neue Objekt verwendet
RSLT	Ergebniscode	Ergebnis der Transaktion Objekt überschreiben. Das Ergebnis ist immer: ERFOLGREICH
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das überschreibende Objekt am angegebenen Standort gelöscht, was nicht der Standort ist, an dem das überschreibende Objekt aufgenommen wurde.

SADD: Security Audit deaktiviert

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung der Überwachungsmeldungen deaktiviert hat; Audit-Meldungen werden nicht mehr erfasst oder geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, mit der das Audit deaktiviert wird.

Codieren	Feld	Beschreibung
AEUN	Benutzername	Der Benutzername, der den Befehl zum Deaktivieren der Revisionsprotokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Meldung besagt, dass die Protokollierung zuvor aktiviert, aber jetzt deaktiviert wurde. Dies wird normalerweise nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt (SADE) und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SADE: Sicherheits-Audit aktivieren

Diese Meldung gibt an, dass der ursprüngliche Dienst (Node-ID) die Protokollierung von Überwachungsmeldungen wiederhergestellt hat; Audit-Meldungen werden erneut erfasst und geliefert.

Codieren	Feld	Beschreibung
AETM	Methode Aktivieren	Die Methode, die zum Aktivieren des Audits verwendet wird.
AEUN	Benutzername	Der Benutzername, der den Befehl zum Aktivieren der Audit-Protokollierung ausgeführt hat.
RSLT	Ergebnis	Dieses Feld hat den Wert NONE. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. KEINE wird verwendet, anstatt SUCS, damit diese Meldung nicht gefiltert wird.

Die Nachricht bedeutet, dass die Protokollierung vorher deaktiviert (SADD) war, aber jetzt wiederhergestellt wurde. Dies wird in der Regel nur während der Massenaufnahme verwendet, um die Systemperformance zu verbessern. Nach der Massenaktivität ist das Auditing wiederhergestellt und die Möglichkeit, das Auditing zu deaktivieren, wird dann dauerhaft gesperrt.

SCMT: Objekt Store Commit

Grid-Inhalte werden erst dann zur Verfügung gestellt oder als gespeichert erkannt, wenn sie bereitgestellt wurden (was bedeutet, dass sie dauerhaft gespeichert wurden).

Dauerhaft gespeicherte Inhalte wurden vollständig auf Festplatte geschrieben und haben entsprechende Integritätsprüfungen bestanden. Diese Meldung wird ausgegeben, wenn ein Inhaltsblock auf den Speicher gesetzt wird.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der zu permanentem Speicher verpflichtet ist.
RSLT	Ergebniscode	Status zum Zeitpunkt, zu dem das Objekt auf Festplatte gespeichert wurde: SUCS: Objekt erfolgreich gespeichert.

Diese Meldung bedeutet, dass ein bestimmter Inhaltsblock vollständig gespeichert und überprüft wurde und nun angefordert werden kann. Er kann zur Nachverfolgung des Datenflusses im System eingesetzt werden.

SDEL: S3 LÖSCHEN

Wenn ein S3-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anfrage gestellt, um das angegebene Objekt oder den angegebenen Bucket zu entfernen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungs-kennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
DMRK	Löschen der Marker-Version-ID	Version-ID des Löschmarker, der beim Löschen eines Objekts aus einem versionierten Bucket erstellt wurde. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkonto name (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkonto name (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.

Codieren	Feld	Beschreibung
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <code>urn:sgws:identity::03393893651506583485:root</code> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das gelöscht wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SGET S3 ABRUFEN

Wenn ein S3-Client eine GET-Transaktion ausgibt, wird eine Anfrage gestellt, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
KLINGELTE	Bereichsleser	Nur für Bereichslesevorgänge. Gibt den Bereich der Bytes an, die von dieser Anforderung gelesen wurden. Der Wert nach dem Schrägstrich (/) zeigt die Größe des gesamten Objekts an.
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.

Codieren	Feld	Beschreibung
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: <pre>urn:sgws:identity::03393893651506583485:root</pre> Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

Codieren	Feld	Beschreibung
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SHEA: S3 KOPF

Wenn ein S3-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, ob es sich um ein Objekt oder einen Bucket handelt und die Metadaten zu einem Objekt abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des überprüften Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: urn:sgws:identity::03393893651506583485:root Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SPOS: S3-BEITRAG

Wenn ein S3-Client eine POST Object-Anforderung ausgibt, wird diese Meldung vom Server ausgegeben, wenn die Transaktion erfolgreich durchgeführt wurde.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der Anforderung ZUR Wiederherstellung DES POSTOBJEKTS. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name

Codieren	Feld	Beschreibung
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend Für einen S3-Select-Vorgang auf „select“ setzen.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Stellen Sie Informationen wieder her.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: urn:sgws:identity::03393893651506583485:root Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.

Codieren	Feld	Beschreibung
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Version-ID der spezifischen Version eines Objekts, das angefordert wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SPUT: S3 PUT

Wenn ein S3-Client eine PUT-Transaktion ausgibt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Buckets gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CMPS	Compliance-Einstellungen	Die beim Erstellen des Buckets verwendeten Compliance-Einstellungen, sofern diese in der PUT Bucket-Anforderung vorhanden sind (gekürzt auf die ersten 1024 Zeichen)
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert der Kopfzeile der Consistency-Control HTTP-Anfrage, wenn diese in der Anforderung vorhanden ist.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.

Codieren	Feld	Beschreibung
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
LKEN	Objektsperre Aktiviert	Der Wert der Anfrageüberschrift x-amz-bucket-object-lock-enabled, Wenn vorhanden in DER PUT Bucket Anforderung.
LKLH	Gesetzliche Sperren Für Objekte	Der Wert der Anfrageüberschrift x-amz-object-lock-legal-hold, Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKMD	Aufbewahrungsmodus Für Objektsperre	Der Wert der Anfrageüberschrift x-amz-object-lock-mode, Wenn vorhanden in DER PUT-Objekt-Anforderung.
LKRU	Objektsperre Bis Datum Beibehalten	Der Wert der Anfrageüberschrift x-amz-object-lock-retain-until-date, Wenn vorhanden in DER PUT-Objekt-Anforderung.
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH

Codieren	Feld	Beschreibung
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3KY	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
S3SR	S3-Unterressource	Der Bucket oder die Objektunterressource, an der sie betrieben wird, falls zutreffend
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SRCF	Konfiguration Von Unterressourcen	Die neue Subressourcenkonfiguration (auf die ersten 1024 Zeichen gekürzt).

Codieren	Feld	Beschreibung
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: urn:sgws:identity::03393893651506583485:root Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
ULID	Upload-ID	Nur in SPUT-Nachrichten für komplette mehrteilige Uploadvorgänge enthalten. Zeigt an, dass alle Teile hochgeladen und zusammengesetzt wurden.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Versionsnummer eines neuen Objekts, das in einem versionierten Bucket erstellt wurde. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.
VSST	Status Der Versionierung	Der neue Versionierungs-Status eines Buckets. Es werden zwei Zustände verwendet: "Aktiviert" oder "ausgesetzt". Operationen für Objekte enthalten dieses Feld nicht.

SREM: Objektspeicher Entfernen

Diese Meldung wird ausgegeben, wenn Inhalte aus einem persistenten Storage entfernt werden und nicht mehr über regelmäßige APIs zugänglich sind.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, der aus dem permanenten Speicher gelöscht wurde.
RSLT	Ergebniscode	Gibt das Ergebnis der Aktionen zum Entfernen von Inhalten an. Der einzige definierte Wert ist: SUCS: Inhalt aus persistentem Storage entfernt

Diese Überwachungsmeldung bedeutet, dass ein bestimmter Inhaltsblock von einem Knoten gelöscht wurde und nicht mehr direkt angefordert werden kann. Die Nachricht kann verwendet werden, um den Fluss gelöschter Inhalte innerhalb des Systems zu verfolgen.

SUPD: S3-Metadaten wurden aktualisiert

Diese Nachricht wird von der S3-API generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert. Die Meldung wird vom Server ausgegeben, wenn die Metadatenaktualisierung erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht in Operationen in Buckets enthalten.
CNCH.	Kopfzeile Der Konsistenzgruppe	Der Wert des HTTP-Anfrageheaders Consistency-Control, falls in der Anfrage vorhanden, beim Aktualisieren der Compliance-Einstellungen eines Buckets.
CNID	Verbindungskennung	Die eindeutige Systemkennung für die TCP/IP-Verbindung.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht in Operationen in Buckets enthalten.

Codieren	Feld	Beschreibung
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
S3AI	S3-Mandantenkonto-ID (Absender anfordern)	Die Mandanten-Konto-ID des Benutzers, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3AK	S3 Access Key ID (Absender anfordern)	Die gehashte S3-Zugriffsschlüssel-ID für den Benutzer, der die Anforderung gesendet hat. Ein leerer Wert zeigt anonymen Zugriff an.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Dieses Feld ist nicht in Operationen in Buckets enthalten.
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SAIP	IP-Adresse (Absender anfordern)	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.

Codieren	Feld	Beschreibung
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SBAI	S3-Mandantenkonto-ID (Bucket-Eigentümer)	Die Mandanten-Account-ID des Eigentümers des Ziel-Buckets. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
SUSR	S3-Benutzer-URN (Absender anfordern)	Die Mandanten-Account-ID und der Benutzername des Benutzers, der die Anforderung macht. Der Benutzer kann entweder ein lokaler Benutzer oder ein LDAP-Benutzer sein. Beispiel: urn:sgws:identity::03393893651506583485:root Für anonyme Anfragen leer.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
VSID	Version-ID	Die Versionsnummer der spezifischen Version eines Objekts, dessen Metadaten aktualisiert wurden. Dieses Feld wird nicht von Vorgängen in Buckets und Objekten in nicht versionierten Buckets erfasst.

SVRF: Objektspeicherüberprüfung fehlgeschlagen

Diese Meldung wird ausgegeben, wenn ein Inhaltsblock den Verifizierungsprozess nicht erfolgreich durchführt. Jedes Mal, wenn replizierte Objektdaten von der Festplatte gelesen oder auf die Festplatte geschrieben werden, werden verschiedene Verifizierungsprüfungen durchgeführt, um sicherzustellen, dass die an den anfordernden Benutzer gesendeten Daten mit den ursprünglich im System aufgenommenen Daten

identisch sind. Wenn eine dieser Prüfungen fehlschlägt, werden die beschädigten replizierten Objektdaten vom System automatisch gesperrt, um ein erneuten Abruf der Daten zu verhindern.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des Inhaltsblocks, bei der die Überprüfung fehlgeschlagen ist.
RSLT	Ergebniscode	Fehlertyp Verifikation: CRCF: Zyklische Redundanzprüfung (CRC) fehlgeschlagen. HMAC: Prüfung des Hashbasierten Nachrichtenauthentifizierungscode s (HMAC) fehlgeschlagen. EHSB: Unerwarteter verschlüsselter Content-Hash. PHSH: Unerwarteter Originalinhalt Hash. SEQC: Falsche Datensequenz auf der Festplatte. PERR: Ungültige Struktur der Festplattendatei. DERR: Festplattenfehler. FNAM: Ungültiger Dateiname.

Hinweis: Diese Nachricht sollte genau überwacht werden. Fehler bei der Inhaltsprüfung können auf Manipulationen an Inhalten oder drohende Hardwareausfälle hinweisen.

Um zu bestimmen, welcher Vorgang die Meldung ausgelöst hat, lesen Sie den Wert des FELDS AMID (Modul-ID). Beispielsweise gibt ein SVFY-Wert an, dass die Meldung vom Storage Verifier-Modul generiert wurde, d. h. eine Hintergrundüberprüfung und STOR zeigt an, dass die Meldung durch den Abruf von Inhalten ausgelöst wurde.

SVRU: Objektspeicher überprüfen Unbekannt

Die Storage-Komponente des LDR-Service scannt kontinuierlich alle Kopien replizierter Objektdaten im Objektspeicher. Diese Meldung wird ausgegeben, wenn eine unbekannte oder unerwartete Kopie replizierter Objektdaten im Objektspeicher erkannt und in das Quarantäneverzeichnis verschoben wird.

Codieren	Feld	Beschreibung
FPTH	Dateipfad	Dateipfad der unerwarteten Objektkopie.
RSLT	Ergebnis	Dieses Feld hat den Wert 'NEIN'. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

Hinweis: die SVRU: Objektspeicher überprüfen Unbekannte Überwachungsmeldung sollte genau überwacht werden. Es bedeutet, dass im Objektspeicher unerwartete Kopien von Objektdaten erkannt wurden. Diese Situation sollte sofort untersucht werden, um festzustellen, wie diese Kopien erstellt wurden, da sie auf den Versuch hinweisen können, Inhalte zu manipulieren oder Hardware-Ausfälle anzufangen.

SYSD: Knoten stoppen

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde. Normalerweise wird diese Meldung erst nach einem späteren Neustart gesendet, da die Warteschlange für die Überwachungsmeldung vor dem Herunterfahren nicht gelöscht wird. Suchen Sie nach der SYST-Meldung, die zu Beginn der Abschaltsequenz gesendet wird, wenn der Dienst nicht neu gestartet wurde.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Das RSLT eines SYSD kann nicht auf ein „nicht ordnungsgemäßes“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYST: Knoten wird angehalten

Wenn ein Dienst ordnungsgemäß angehalten wird, wird diese Meldung generiert, um anzugeben, dass das Herunterfahren angefordert wurde und dass der Dienst seine Abschaltsequenz initiiert hat. SYST kann verwendet werden, um festzustellen, ob das Herunterfahren angefordert wurde, bevor der Dienst neu gestartet wird (im Gegensatz zu SYSD, das normalerweise nach dem Neustart des Dienstes gesendet wird).

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SAUCS: Das System wurde sauber abgeschaltet.

Die Meldung gibt nicht an, ob der Host-Server angehalten wird, sondern nur der Reporting-Service. Der RSLT-Code einer SYST-Meldung kann nicht auf ein „nicht ordnungsgemäßes“ Herunterfahren hinweisen, da die Meldung nur durch „sauberes“ Herunterfahren generiert wird.

SYSU: Knoten Start

Wenn ein Dienst neu gestartet wird, wird diese Meldung erzeugt, um anzugeben, ob die vorherige Abschaltung sauber (befehl) oder ungeordnet (unerwartet) war.

Codieren	Feld	Beschreibung
RSLT	Herunterfahren Reinigen	Die Art des Herunterfahrens: SUCS: Das System wurde sauber abgeschaltet. DSDN: Das System wurde nicht sauber heruntergefahren. VRGN: Das System wurde erstmals nach der Server-Installation (oder Neuinstallation) gestartet.

Die Meldung gibt nicht an, ob der Host-Server gestartet wurde, sondern nur der Reporting-Service. Diese Meldung kann verwendet werden, um:

- Diskontinuität im Prüfprotokoll erkennen.
- Ermitteln Sie, ob ein Service während des Betriebs ausfällt (da die verteilte Natur des StorageGRID Systems diese Fehler maskieren kann). Der Server Manager startet einen fehlgeschlagenen Dienst automatisch neu.

VLST: Vom Benutzer initiiertes Volumen verloren

Diese Meldung wird ausgegeben, wenn der `/proc/CMSI/Volume_Lost` Befehl wird ausgeführt.

Codieren	Feld	Beschreibung
VOLL	Volume Identifier Lower	Das untere Ende des betroffenen Volumenbereichs oder eines einzelnen Volumens.

Codieren	Feld	Beschreibung
VOLU	Volume Identifier Ober	Das obere Ende des betroffenen Volumenbereichs. Gleich VOLL wenn ein einzelnes Volume ist.
NID	Quell-Node-ID	Die Knoten-ID, auf der die Speicherorte verloren waren.
LTYP	Positionstyp	„CLDI“ (Online) oder „CLNL“ (Nearline). Wenn nicht angegeben, ist die Standardeinstellung „CLDI“.
RSLT	Ergebnis	Immer „KEINE“. RSLT ist ein Pflichtfeld, ist aber für diese Nachricht nicht relevant. „KEINE“ wird anstelle von „UCS“ verwendet, damit diese Meldung nicht gefiltert wird.

WDEL: Swift LÖSCHEN

Wenn ein Swift-Client eine LÖSCHTRANSAKTION ausgibt, wird eine Anfrage zum Entfernen des angegebenen Objekts oder Containers gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
CSIZ	Inhaltsgröße	Die Größe des gelöschten Objekts in Byte. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der LÖSCHAKTION. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
SGRP	Standort (Gruppe)	Wenn vorhanden, wurde das Objekt am angegebenen Standort gelöscht, nicht der Standort, an dem das Objekt aufgenommen wurde.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WGET: Schneller ERHALTEN

Wenn ein Swift-Client eine GET-Transaktion ausgibt, wird eine Anfrage gestellt, um ein Objekt abzurufen, die Objekte in einem Container aufzulisten oder die Container in einem Konto aufzulisten. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
RSLT	Ergebniscode	Ergebnis der GET-Transaktion. Das Ergebnis ist immer ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.

Codieren	Feld	Beschreibung
WOW	Swift Container	Der Swift-Containernamen. Dieses Feld wird nicht von Operationen für Accounts berücksichtigt.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WHEA: Schneller KOPF

Wenn ein Swift-Client eine HEAD-Transaktion ausgibt, wird eine Anfrage gestellt, ob ein Konto, Container oder Objekt vorhanden ist, und alle relevanten Metadaten abzurufen. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).

Codieren	Feld	Beschreibung
RSLT	Ergebniscode	Ergebnis der HAUPTTRANSAKTION. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client- Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer- IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername. Dieses Feld wird nicht von Operationen für Accounts berücksichtigt.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld ist nicht bei Operationen für Konten und Container enthalten.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

WPUT: Schnell AUSGEDRÜCKT

Wenn ein Swift-Client eine PUT-Transaktion ausgibt, wird eine Anfrage zum Erstellen eines neuen Objekts oder Containers gestellt. Diese Meldung wird vom Server ausgegeben, wenn die Transaktion erfolgreich ist.

Codieren	Feld	Beschreibung
CBID	Kennung Für Inhaltsblock	Die eindeutige Kennung des angeforderten Inhaltsblocks. Wenn die CBID unbekannt ist, ist dieses Feld auf 0 gesetzt. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
CSIZ	Inhaltsgröße	Die Größe des abgerufenen Objekts in Byte. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
HTRH	HTTP-Anforderungskopf	Liste der während der Konfiguration ausgewählten Namen und Werte für protokollierte HTTP-Anfragen. Hinweis: X-Forwarded-For Wird automatisch einbezogen, wenn sie in der Anfrage vorhanden ist und wenn der X-Forwarded-For Der Wert unterscheidet sich von der IP-Adresse des Anforderungssenders (Feld SAIP-Audit).
MTME	Uhrzeit Der Letzten Änderung	Der Unix-Zeitstempel in Mikrosekunden, der angibt, wann das Objekt zuletzt geändert wurde.
RSLT	Ergebniscode	Ergebnis der PUT-Transaktion. Das Ergebnis ist immer: ERFOLGREICH
SAIP	IP-Adresse des anfragenden Clients	Die IP-Adresse der Client-Anwendung, die die Anforderung gestellt hat.
ZEIT	Zeit	Gesamtbearbeitungszeit für die Anfrage in Mikrosekunden.
TLIP	Vertrauenswürdige Load Balancer-IP-Adresse	Wenn die Anforderung von einem vertrauenswürdigen Layer 7 Load Balancer weitergeleitet wurde, ist die IP-Adresse des Load Balancer.
UUID	Universell Eindeutige Kennung	Die Kennung des Objekts im StorageGRID System.

Codieren	Feld	Beschreibung
WACC	Swift Konto-ID	Die eindeutige Konto-ID, die vom StorageGRID System festgelegt wurde.
WOW	Swift Container	Der Swift-Containername.
WOBJ	Swift Objekt	Die Swift Objekt-ID. Dieses Feld wird nicht von den Operationen in Containern berücksichtigt.
WUSR	Swift-Account-Benutzer	Der Swift-Account-Benutzername, der den Client, der die Transaktion ausführt, eindeutig identifiziert.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN 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.