监控和维护 StorageGRID

StorageGRID

NetApp
June 14, 2023

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-116/monitor/index.html on June 14, 2023. Always check docs.netapp.com for the latest.

目录

监控和维护 StorageGRID . . . 1
监控和故障排除 . . . 1
扩展网格 . . . 310
恢复和维护 . . . 358
查看审核日志 . . . 583

监控和维护 StorageGRID

监控和故障排除

监控和故障排除：概述

按照以下说明监控 StorageGRID 系统，并评估和解决可能发生的问题。

关于这些说明

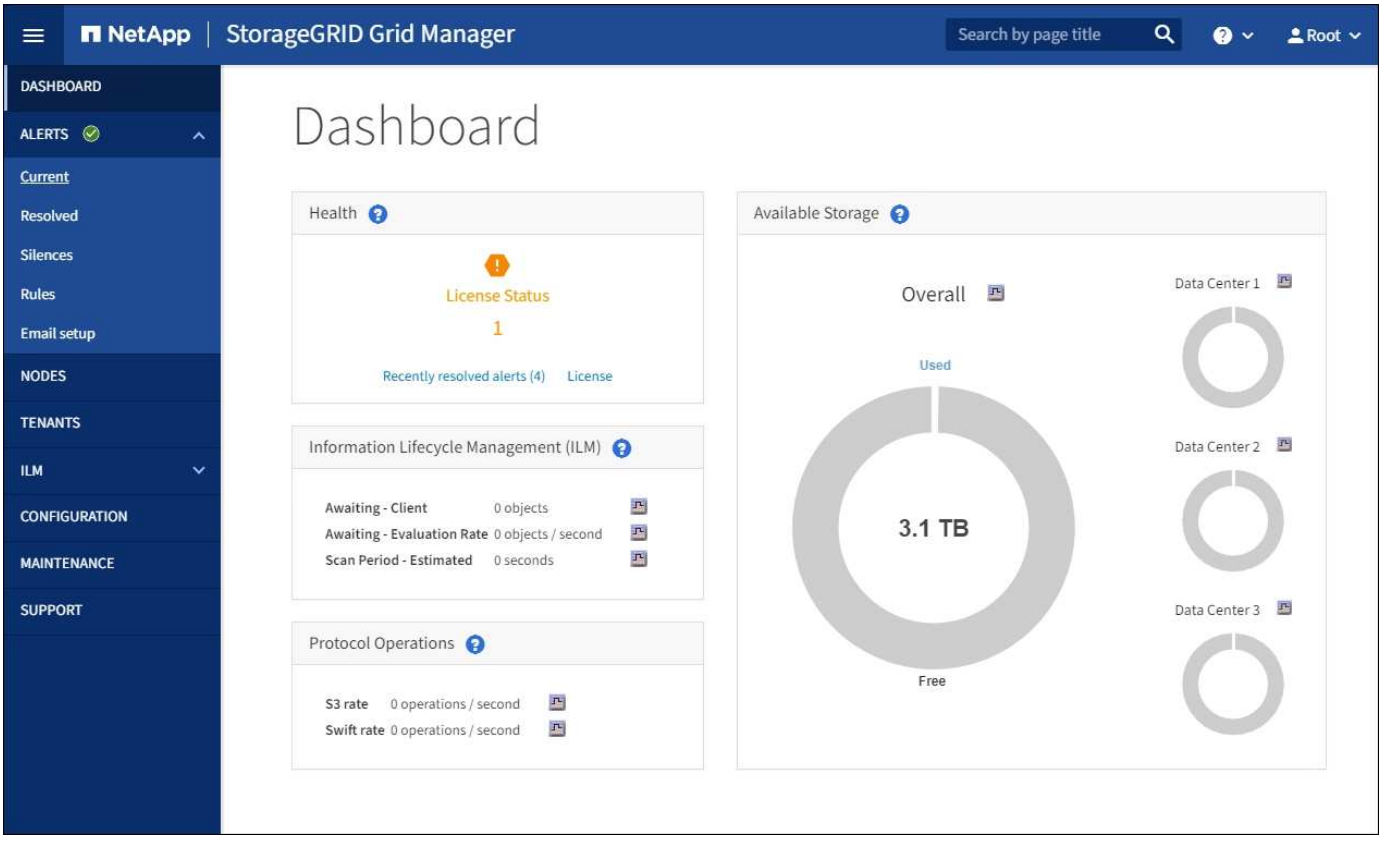
以下说明介绍如何使用网格管理器监控 StorageGRID 系统。您将了解应定期监控哪些信息，如何管理警报和旧警报，如何使用 SNMP 进行监控以及如何获取其他 StorageGRID 数据，包括指标和诊断。

这些说明还介绍如何对 StorageGRID 系统进行故障排除，并介绍所有系统警报，旧警报和日志文件。

如果要在安装 StorageGRID 系统后对其进行监控和支持，请按照以下说明进行操作。

查看信息板

首次登录到网格管理器时，您可以使用信息板一目了然地监控系统活动。信息板包含有关系统运行状况，使用情况指标以及操作趋势和图表的信息。



搜索字段

通过标题栏中的 * 搜索 * 字段，您可以快速导航到网格管理器中的特定页面或边栏条目。例如，您可以输入 * 密

钥 * 以访问密钥管理服务器页面。

运行状况面板

Description	查看其他详细信息	了解更多信息。
汇总了系统的运行状况。绿色复选标记表示当前没有警报，并且所有网格节点均已连接。任何其他图标表示至少存在一个当前警报或已断开连接的节点。	您可能会看到以下一个或多个链接： • * 网格详细信息 * ： 如果任何节点断开连接（连接状态为未知或管理员关闭），则显示此消息。单击链接或单击蓝色或灰色图标以确定受影响的节点。 • * 当前警报 * ： 如果任何警报当前处于活动状态，则显示此消息。单击链接，或单击 * 严重 * ， * 主要 * 或 * 次要 * 以查看 * 警报 * > * 当前 * 页面上的详细信息。 • * 最近解决的警报 * ： 如果过去一周触发的任何警报现已解决，则显示此消息。单击此链接可在 * 警报 * > * 已解决 * 页面上查看详细信息。 • * 旧警报 * ： 如果任何警报（旧系统）当前处于活动状态，则显示此消息。单击此链接可在 * 支持 * > * 警报（传统） * > * 当前警报 * 页面上查看详细信息。 • * 许可证 * ： 如果存在具有此 StorageGRID 系统软件许可证的问题描述 ，则显示此。单击此链接可在 * 维护 * > * 系统 * > * 许可证 * 页面上查看详细信息。	• 监控节点连接状态 • 查看当前警报 • 查看已解决的警报 • 查看旧警报 • 管理 StorageGRID

可用存储面板

Description	查看其他详细信息	了解更多信息。
显示整个网格中的可用存储容量和已用存储容量，不包括归档介质。 " 整体 " 图表显示了网格范围内的总计。如果这是一个多站点网格，则会为每个数据中心站点显示其他图表。 您可以使用此信息将已用存储与可用存储进行比较。如果您使用的是多站点网格，则可以确定哪个站点占用的存储更多。	• 要查看容量，请将光标置于图表的 " 可用容量 " 和 " 已用容量 " 部分上方。 • 要查看某个日期范围内的容量趋势，请单击图表图标 对于整个网格或数据中心站点。 • 要查看详细信息，请选择 * 节点 * 。然后，查看整个网格，整个站点或单个存储节点的存储选项卡。	• 查看存储选项卡 • 监控存储容量

信息生命周期管理（ **ILM** ）面板

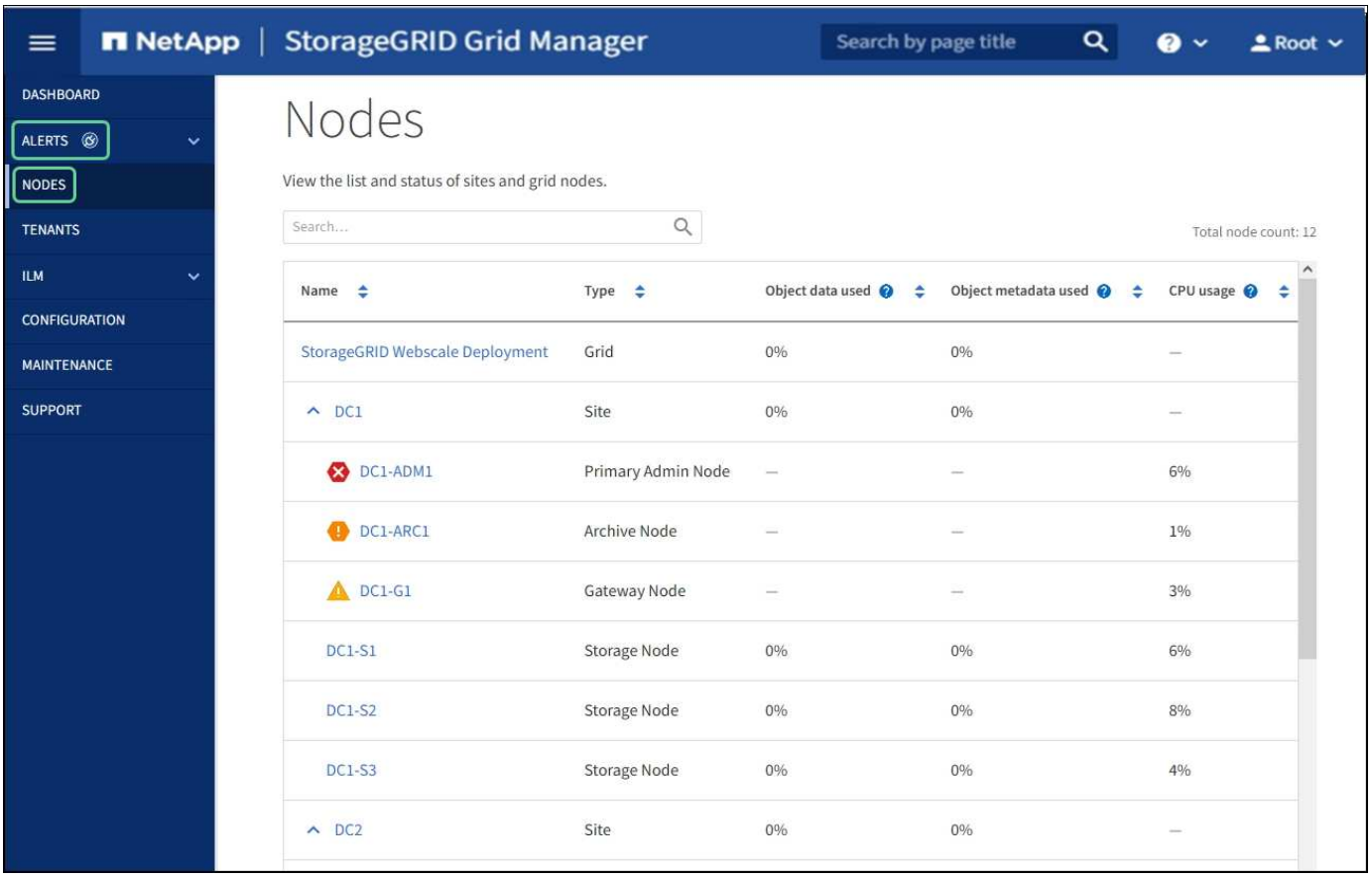
Description	查看其他详细信息	了解更多信息。
显示系统的当前 ILM 操作和 ILM 队列。您可以使用此信息监控系统的工作负载。 • * 正在等待 - 客户端 * ： 等待通过客户端操作（例如载入）进行 ILM 评估的对象总数。 • * 等待 - 评估速率 * ： 根据网格中的 ILM 策略评估对象的当前速率。 • * 扫描期间 - 估计 * ： 完成对所有对象的完整 ILM 扫描的估计时间。* 注意： * 完全扫描并不能保证 ILM 已应用于所有对象。	• 要查看详细信息，请选择 * 节点 * 。然后，查看整个网格，整个站点或单个存储节点的 ILM 选项卡。 • 要查看现有 ILM 规则，请选择 * 。 ILM > * 规则 * 。 • 要查看现有 ILM 策略，请选择 * 。 ILM > * 策略 * 。	• 查看 ILM 选项卡 • 管理 StorageGRID。

协议操作面板

Description	查看其他详细信息	了解更多信息。
显示系统执行的特定于协议的操作（ S3 和 Swift ）的数量。 您可以使用此信息监控系统的工作负载和效率。协议速率是过去两分钟的平均值。	• 要查看详细信息，请选择 * 节点 * 。然后，查看整个网格，整个站点或单个存储节点的对象选项卡。 • 要查看某个日期范围内的趋势，请单击图表图标 S3 或 Swift 协议速率右侧。	• 查看对象选项卡 • 使用 S3 • 使用 Swift

查看节点页面

如果您需要比信息板提供的信息更详细的 StorageGRID 系统信息，则可以使用节点页面查看整个网格，网格中的每个站点以及站点上的每个节点的指标。



节点表列出了 StorageGRID 系统中的所有站点和节点。系统将显示每个节点的摘要信息。如果节点具有活动警报，则节点名称旁边会显示一个图标。如果节点已连接且没有活动警报，则不会显示任何图标。

连接状态图标

- * 未连接 - 未知 * ：节点未连接到网格，原因未知。例如，节点之间的网络连接已断开或电源已关闭。此外，可能还会触发 * 无法与节点 * 通信 " 警报。其他警报可能也处于活动状态。这种情况需要立即引起关注。

  在受管关闭操作期间，节点可能会显示为未知。在这些情况下，您可以忽略未知状态。

- * 未连接 - 已管理员关闭 * ：由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。一个或多个警报可能也处于活动状态。

如果节点与网格断开连接，则可能存在底层警报，但仅会显示 "`Not connected` " 图标。要查看节点的活动警报，请选择节点。

警报图标

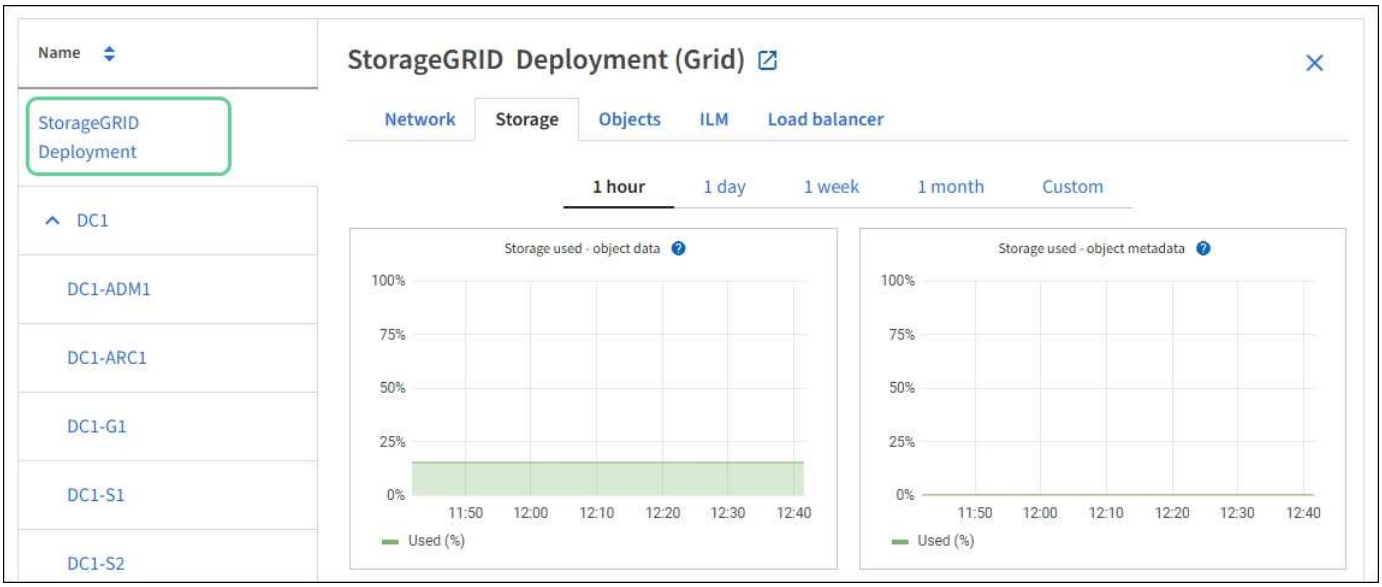
如果节点存在活动警报，则节点名称旁边会显示以下图标之一：

- * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。
- * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。
- * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。

查看系统，站点或节点的详细信息

要查看可用信息，请按如下所示选择网格，站点或节点的名称：

- 选择网格名称可查看整个 StorageGRID 系统统计信息的聚合摘要。
- 选择一个特定的数据中心站点，以查看该站点上所有节点的统计信息的聚合摘要。
- 选择一个特定节点以查看该节点的详细信息。



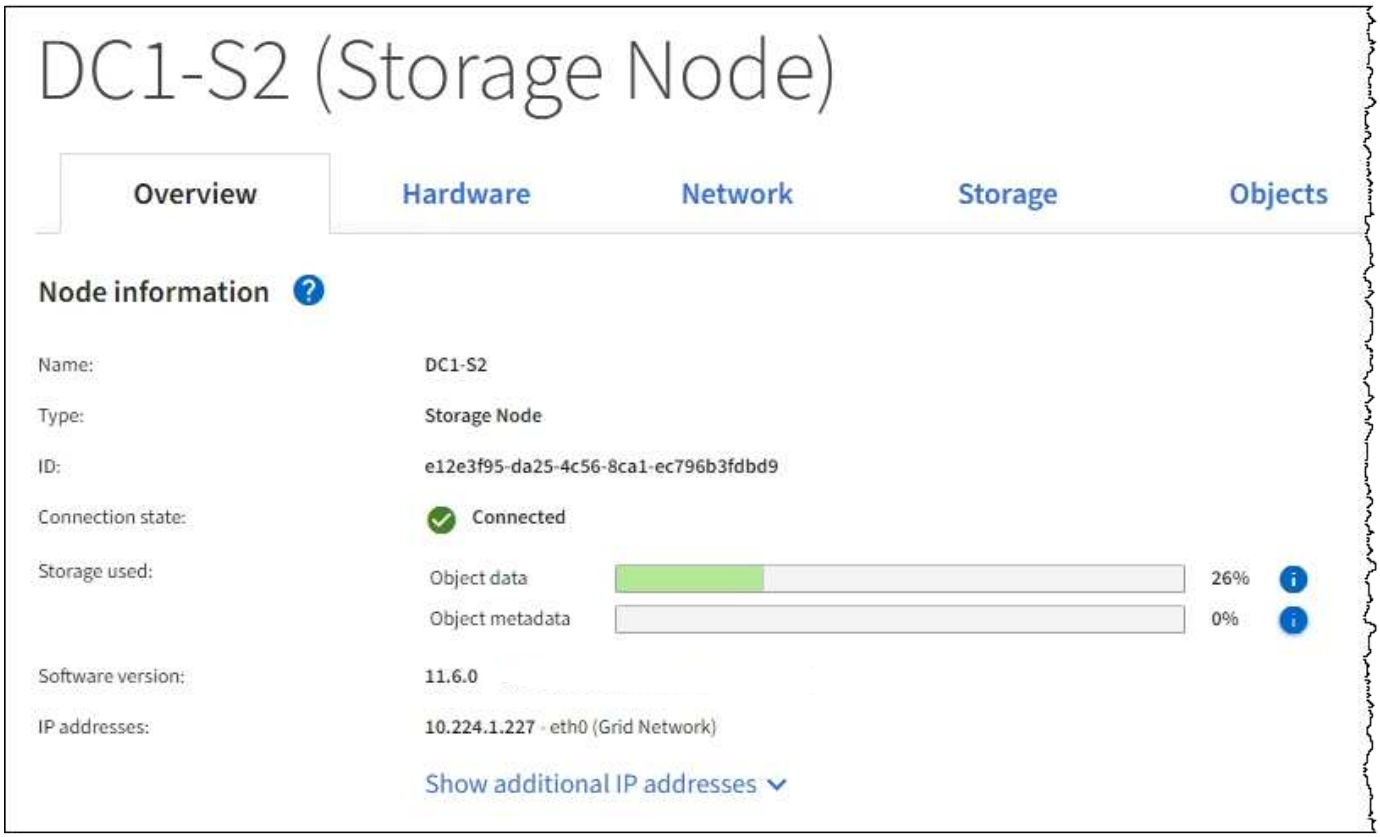
查看概述选项卡

概述选项卡提供了有关每个节点的基本信息。此外，它还会显示当前影响节点的任何警报。

此时将显示所有节点的概述选项卡。

节点信息

概述选项卡的节点信息部分列出了有关网格节点的基本信息。



节点的概述信息包括：

- * 名称 * ： 分配给节点并显示在网格管理器中的主机名。
- * 类型 * ： 节点的类型—管理节点，主管理节点，存储节点，网关节点或归档节点。
- * ID * ： 节点的唯一标识符，也称为 UUID 。
- * 连接状态 * ： 三种状态之一。此时将显示最严重状态的图标。
  - * 未知 * ： 节点未连接到网格，原因未知。例如，节点之间的网络连接已断开或电源已关闭。此外，可能还会触发 * 无法与节点 * 通信 " 警报。其他警报可能也处于活动状态。这种情况需要立即引起关注。

    在受管关闭操作期间，节点可能会显示为未知。在这些情况下，您可以忽略未知状态。

  - * 已管理员关闭 * ： 由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。一个或多个警报可能也处于活动状态。
  - * 已连接 * ： 节点已连接到网格。
- * 已用存储 * ： 仅适用于存储节点。
  - * 对象数据 * ： 存储节点上已使用的对象数据总可用空间的百分比。
  - * 对象元数据 * ： 存储节点上已使用的对象元数据的总允许空间百分比。
- * 软件版本 * ： 节点上安装的 StorageGRID 版本。
- * HA 组 * ： 仅适用于管理节点和网关节点。如果节点上的网络接口包含在高可用性组中，并且该接口是否为主接口，则显示此信息。

- * IP 地址 * ： 节点的 IP 地址。单击 * 显示其他 IP 地址 * 以查看节点的 IPv4 和 IPv6 地址以及接口映射。

警报

" 概述 " 选项卡的 " 警报 " 部分列出了当前影响此节点且尚未静音的所有警报。单击警报名称可查看其他详细信息和建议的操作。



相关信息

监控节点连接状态

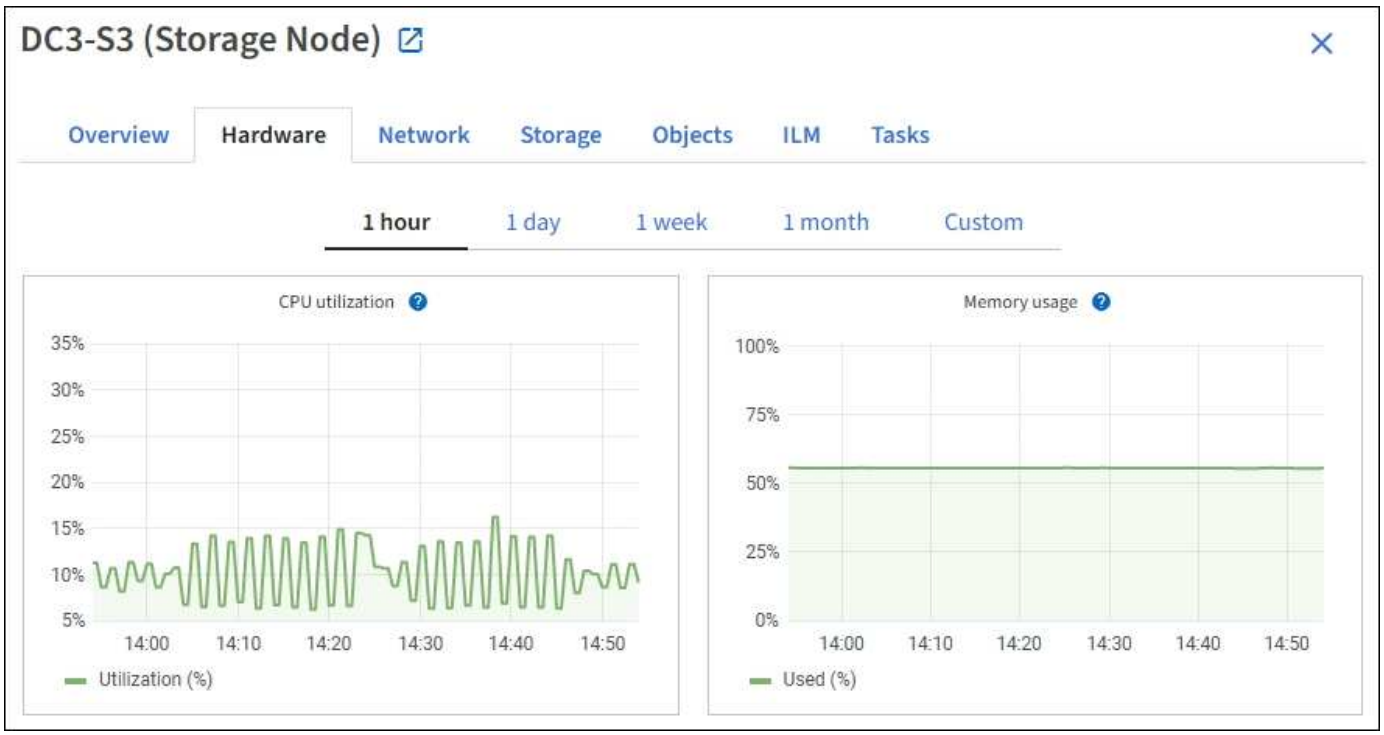
查看当前警报

查看特定警报

查看硬件选项卡

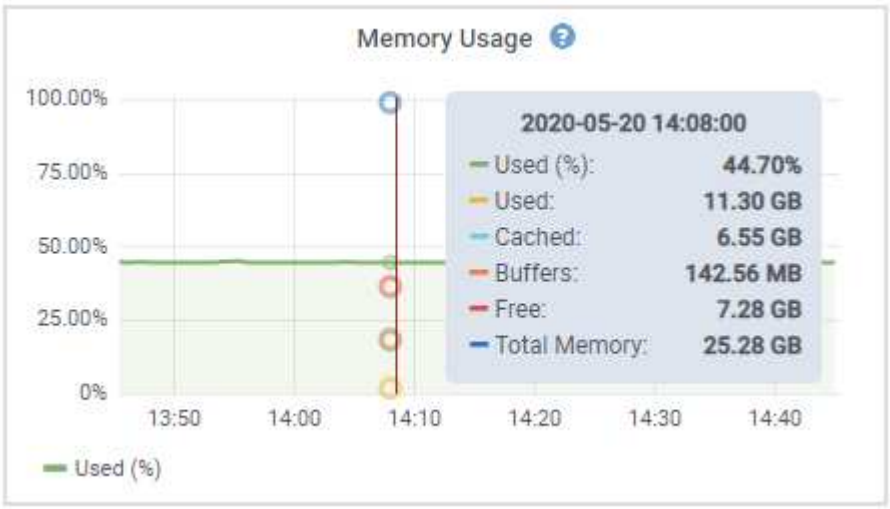
硬件选项卡可显示每个节点的 CPU 利用率和内存使用情况，以及有关设备的其他硬件信息。

此时将显示所有节点的硬件选项卡。



要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。

要查看有关 CPU 利用率和内存使用情况的详细信息，请将光标悬停在每个图形上。



如果节点是设备节点，则此选项卡还会包含一个部分，其中包含有关设备硬件的详细信息。

查看有关设备存储节点的信息

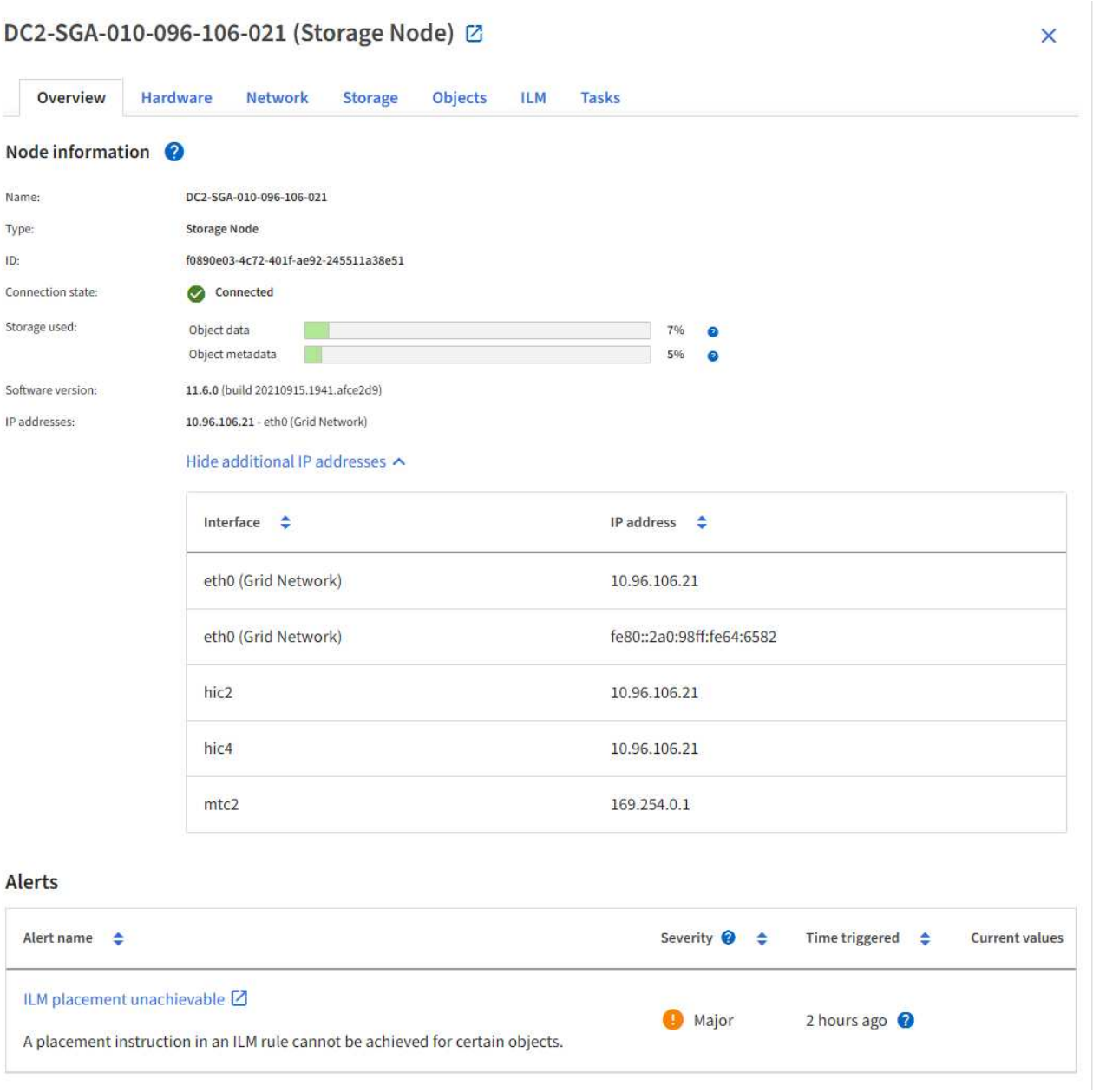
节点页面列出了有关每个设备存储节点的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，控制器固件版本，网络资源，网络接口， 网络地址以及接收和传输数据。

步骤

1. 从节点页面中，选择设备存储节点。
2. 选择 * 概述 * 。

   " 概述 " 选项卡的 " 节点信息 " 部分显示节点的摘要信息，例如节点的名称，类型， ID 和连接状态。IP 地址列表包括每个地址的接口名称，如下所示：

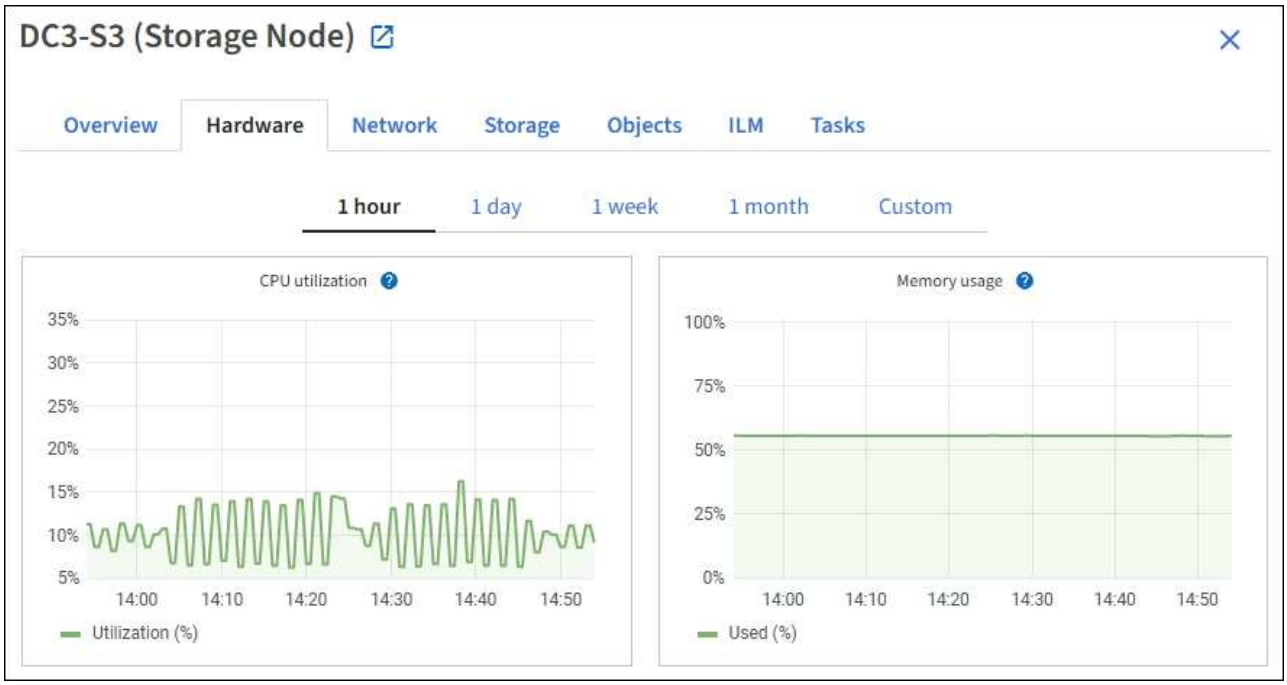
   - * eth * ： 网格网络，管理网络或客户端网络。
   - * hic* ： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
   - * MTC* ： 设备上的一个物理 1 GbE 端口。一个或多个 MTC 接口已绑定，以构成 StorageGRID 管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。



" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

3. 选择 * 硬件 * 可查看有关此设备的详细信息。

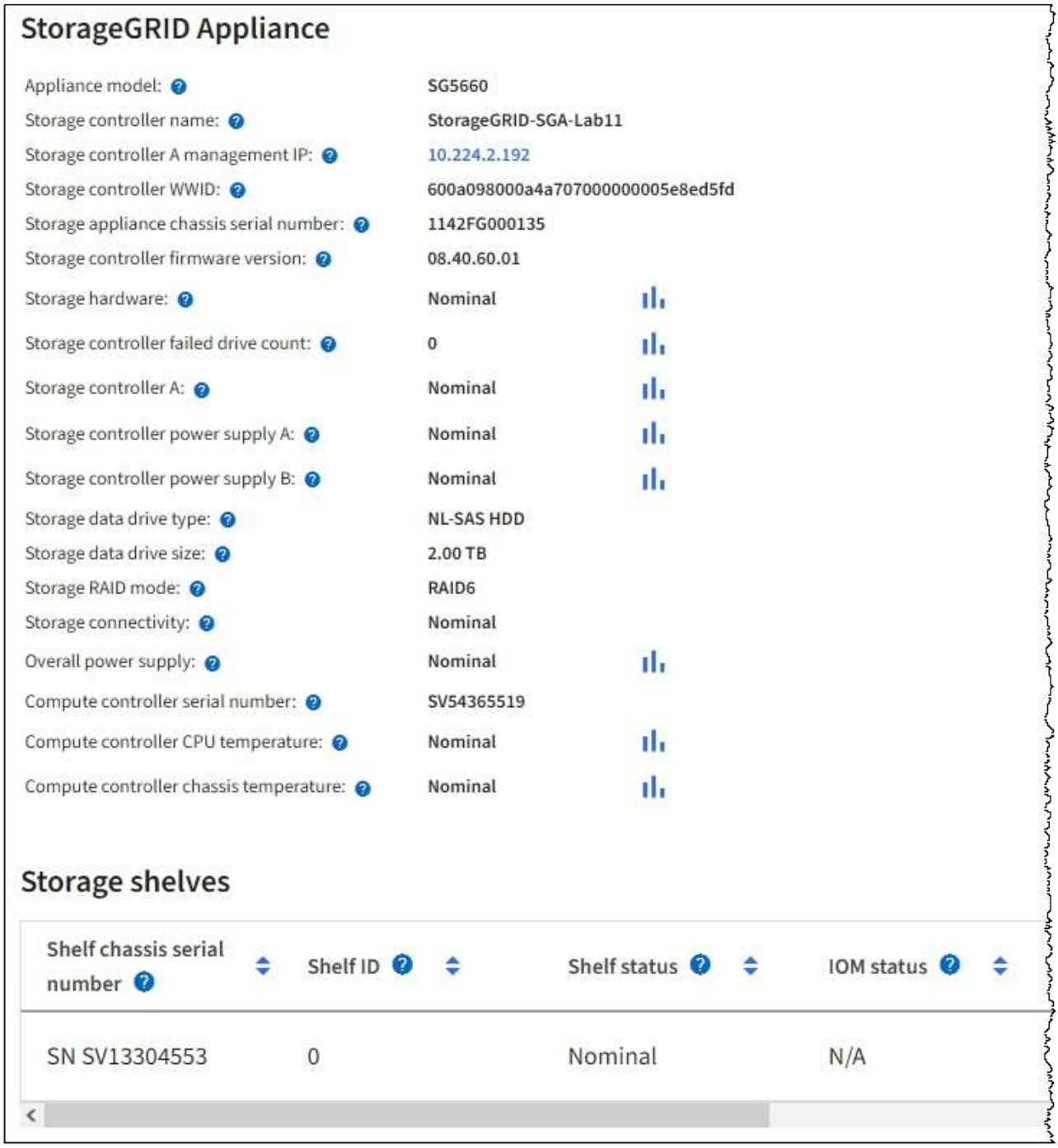
   a. 查看 CPU 利用率和内存图形，确定 CPU 和内存使用量随时间的变化所占百分比。要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。



b. 向下滚动以查看设备组件表。此表包含设备的型号名称，控制器名称，序列号和 IP 地址以及每个组件的状态等信息。

某些字段（例如计算控制器 BMC IP 和计算硬件）仅针对具有此功能的设备显示。

存储架和扩展架（如果是安装的一部分）的组件会显示在设备表下方的单独表中。



字段	Description
设备型号	SANtricity 软件中显示的此 StorageGRID 设备的型号。
存储控制器名称	SANtricity 软件中显示的此 StorageGRID 设备的名称。
存储控制器 A 管理 IP	存储控制器 A 上管理端口 1 的 IP 地址您可以使用此 IP 访问 SANtricity 软件来解决存储问题。

字段	Description
存储控制器 B 的管理 IP	存储控制器 B 上管理端口 1 的 IP 地址您可以使用此 IP 访问 SANtricity 软件来解决存储问题。 某些设备型号没有存储控制器 B
存储控制器 WWID	SANtricity 软件中显示的存储控制器的全球标识符。
存储设备机箱序列号	设备的机箱序列号。
存储控制器固件版本	此设备的存储控制器上的固件版本。
存储硬件	存储控制器硬件的整体状态。如果 SANtricity System Manager 报告存储硬件的状态为 "Needs Attention （需要注意） "，则 StorageGRID 系统也会报告此值。 如果状态为 "`needs attention，` "，请首先使用 SANtricity 软件检查存储控制器。然后，确保不存在适用于计算控制器的其他警报。
存储控制器故障驱动器计数	非最佳驱动器的数量。
存储控制器 A	存储控制器 A 的状态
存储控制器 B	存储控制器 B 的状态某些设备型号没有存储控制器 B
存储控制器电源 A	存储控制器的电源 A 的状态。
存储控制器电源 B	存储控制器的电源 B 的状态。
存储数据驱动器类型	设备中的驱动器类型，例如 HDD （硬盘驱动器）或 SSD （固态驱动器）。
存储数据驱动器大小	一个数据驱动器的有效大小。 • 注 * ： 对于具有扩展架的节点，请使用 每个磁盘架的数据驱动器大小 而是。有效驱动器大小可能因磁盘架而异。
存储 RAID 模式	为设备配置的 RAID 模式。
存储连接	存储连接状态。
整体电源	设备的所有电源的状态。

字段	Description
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller ， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含 BMC 的设备型号，不会显示此字段。
计算控制器序列号	计算控制器的序列号。
计算硬件	计算控制器硬件的状态。对于没有单独计算硬件和存储硬件的设备型号，不会显示此字段。
计算控制器 CPU 温度	计算控制器 CPU 的温度状态。
计算控制器机箱温度	计算控制器的温度状态。

+

存储架表中的列	Description
磁盘架机箱序列号	存储架机箱的序列号。
磁盘架 ID	存储架的数字标识符。 • 99 ： 存储控制器架 • 0 ： 第一个扩展架 • 1 ： 第二个扩展架 *注：*扩展架仅适用于SG6060和SG60X。
磁盘架状态	存储架的整体状态。
IOM 状态	任何扩展架中的输入 / 输出模块（ IOM ）的状态。不适用于扩展架。
电源状态	存储架电源的整体状态。
抽盒状态	存储架中抽盒的状态。不适用，如果磁盘架不包含抽盒。
风扇状态	存储架中的散热风扇的整体状态。
驱动器插槽	存储架中的驱动器插槽总数。
数据驱动器	存储架中用于数据存储的驱动器数量。

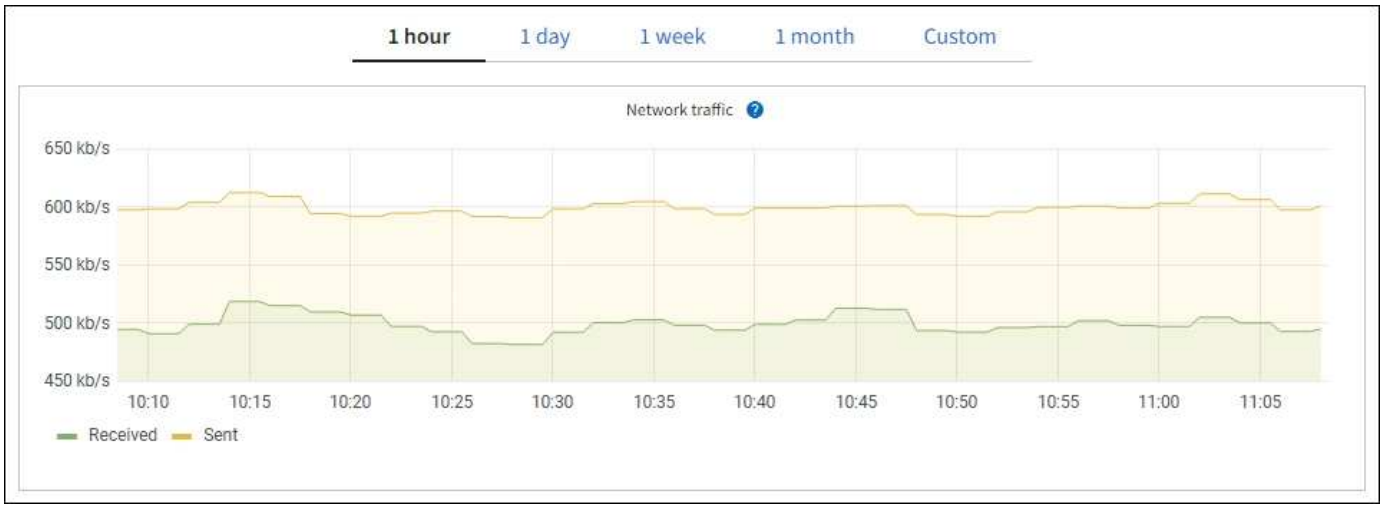
存储架表中的列	Description
【磁盘架数据驱动器大小】数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储架中用作缓存的驱动器数量。
缓存驱动器大小	存储架中最小缓存驱动器的大小。通常，缓存驱动器的大小相同。
配置状态	存储架的配置状态。

4. 确认所有状态均为 "`标称值。` "

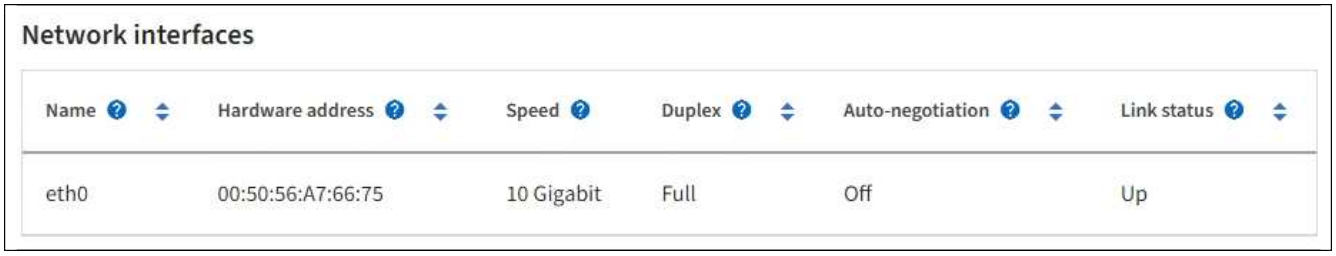
   如果状态不是 "`标称，` " ，请查看任何当前警报。您还可以使用 SANtricity 系统管理器详细了解其中一些硬件值。请参见有关安装和维护设备的说明。

5. 选择 * 网络 * 可查看每个网络的信息。

网络流量图提供了整体网络流量的摘要。



1. 查看网络接口部分。



使用下表以及网络接口表中 * 速度 * 列中的值确定设备上的 10/225-GbE 网络端口是配置为使用主动 / 备份模式还是 LACP 模式。

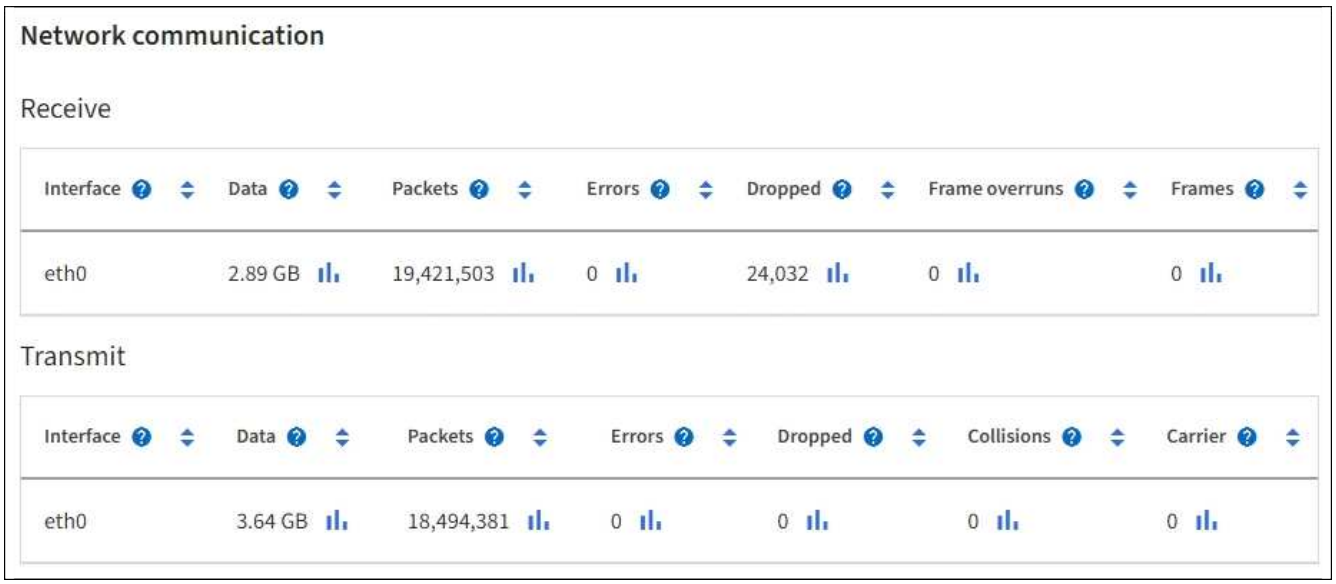
表中显示的值假定使用了所有四个链路。

链路模式	绑定模式	单个 **HIC** 链路速度（ **hic1** ， **hic2** ， **hic3** ， **hic4** ）	预期网格 **/** 客户端网络速度（ **eth0** ， **eth2** ）
聚合	LACP	25.	100
已修复	LACP	25.	50
已修复	主动 / 备份	25.	25.
聚合	LACP	10	40
已修复	LACP	10	20
已修复	主动 / 备份	10	10

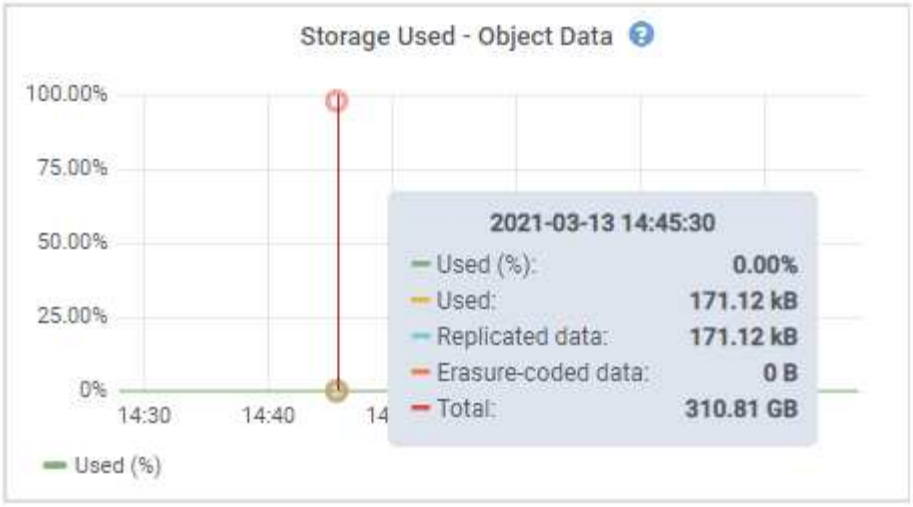
有关配置 10/225-GbE 端口的详细信息，请参见设备的安装和维护说明。

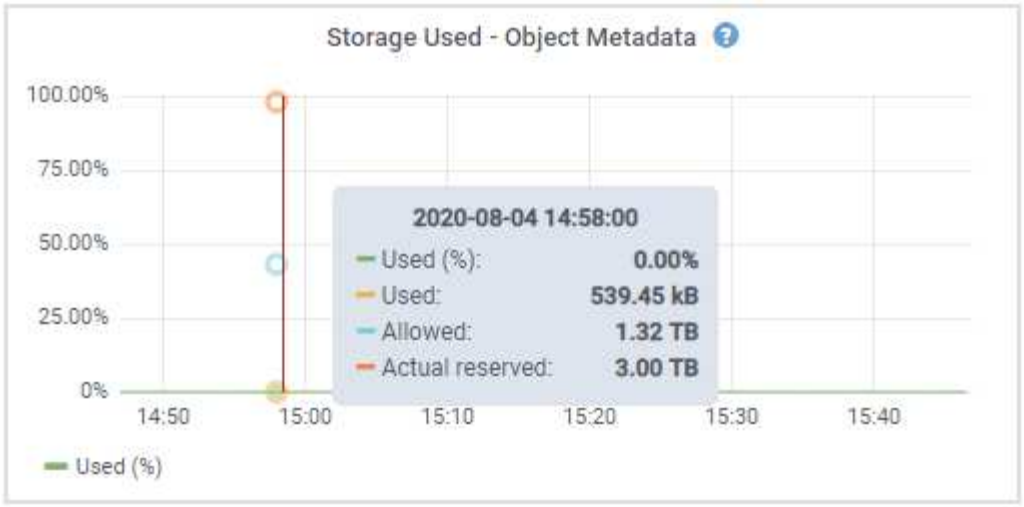
2. 查看网络通信部分。

接收和传输表显示了通过每个网络接收和发送的字节数和数据包数，以及其他接收和传输指标。



3. 选择 * 存储 * 可查看显示对象数据和对象元数据在一段时间内所用存储百分比的图形，以及有关磁盘设备，卷和对象存储的信息。

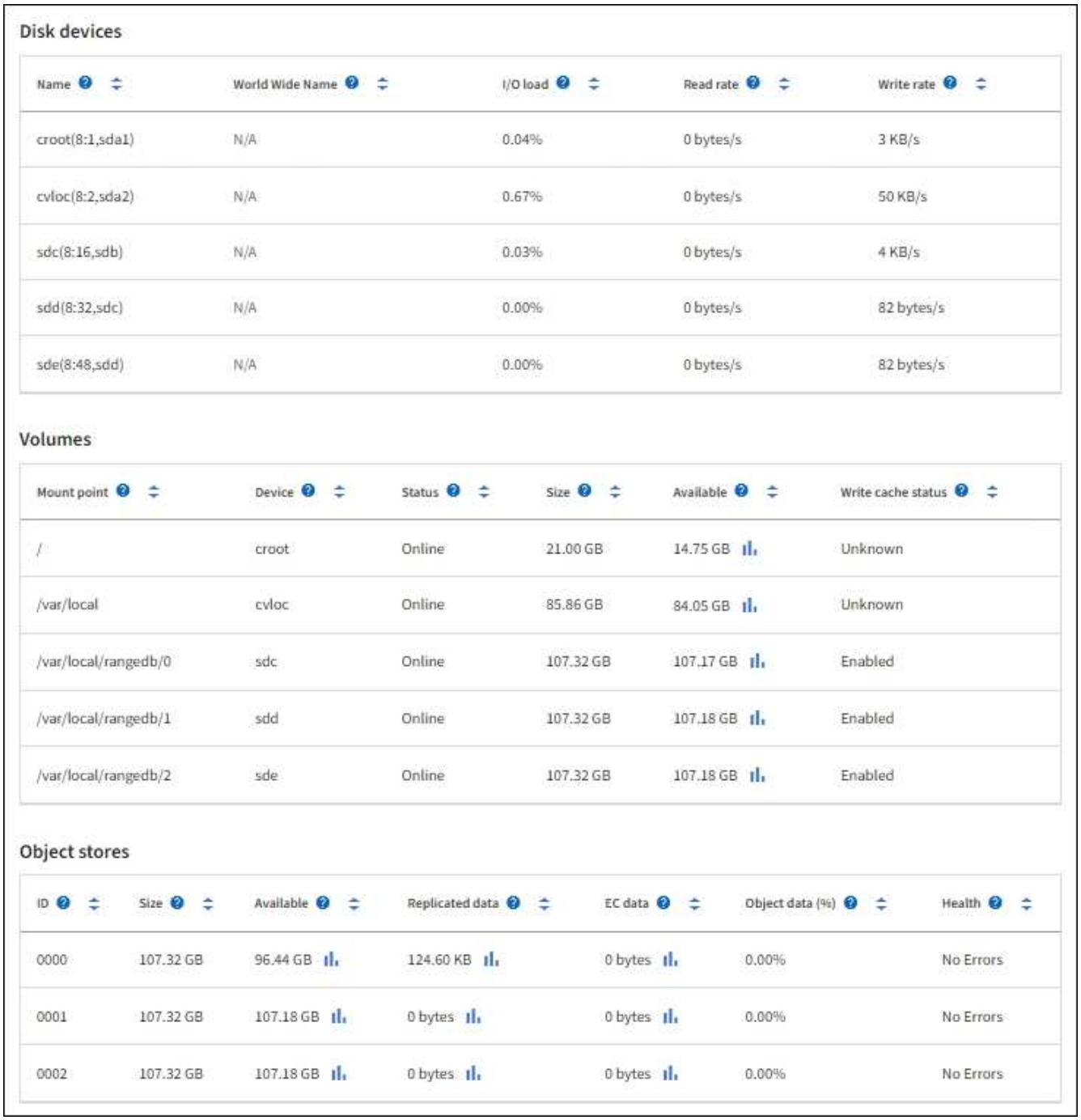




a. 向下滚动以查看每个卷和对象存储的可用存储容量。

   每个磁盘的全球通用名称都与在 SANtricity 软件（连接到设备存储控制器的管理软件）中查看标准卷属性时显示的卷全球通用标识符（ WWID ）匹配。

   为了帮助您解释与卷挂载点相关的磁盘读取和写入统计信息，磁盘设备表的 * 名称 * 列（即 *sdc* ， *sdd* ， *sde* 等）中显示的名称的第一部分与卷表的 * 设备 * 列中显示的值匹配。



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

相关信息

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

查看有关设备管理节点和网关节点的信息

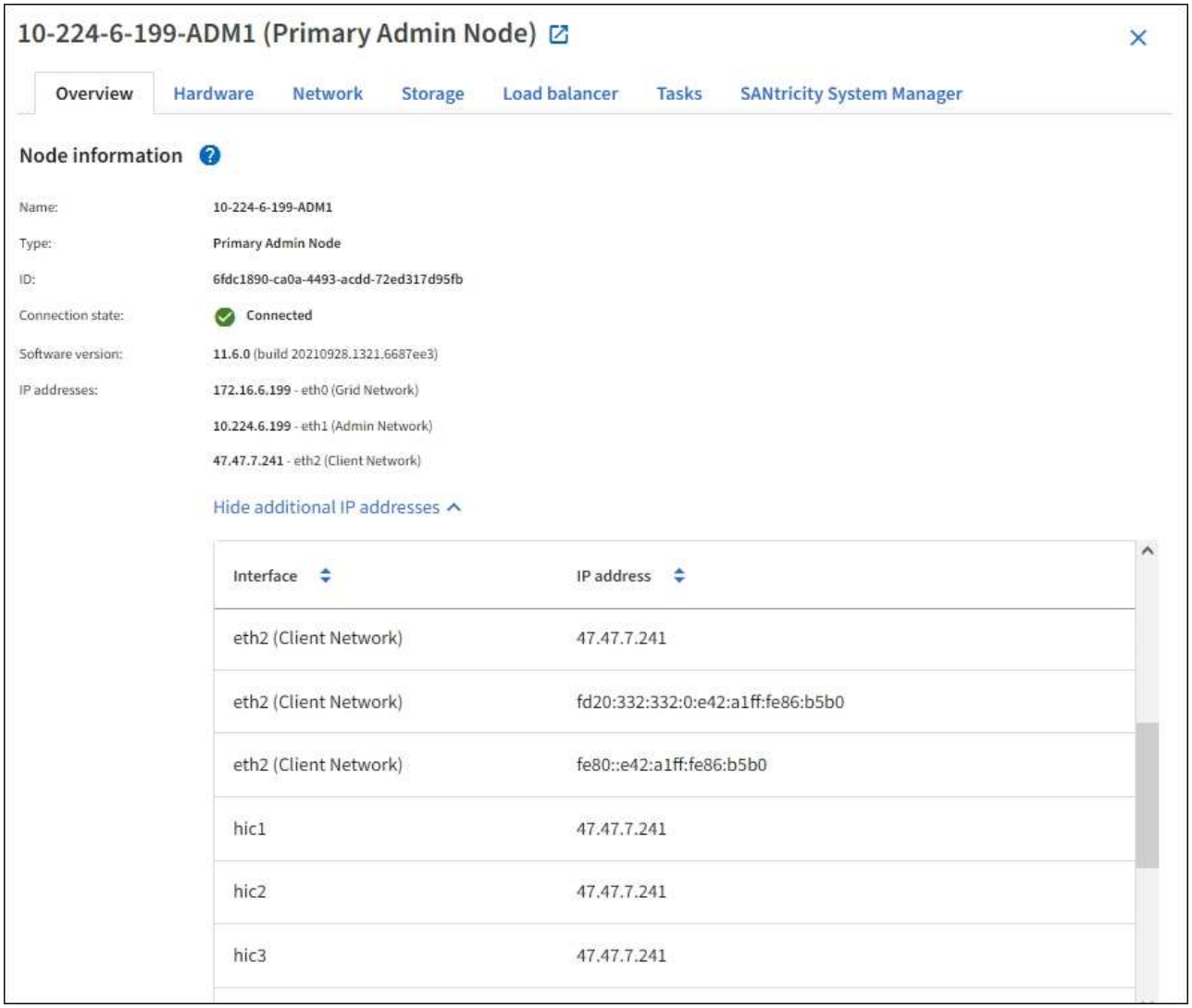
节点页面列出了有关用作管理节点或网关节点的每个服务设备的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，网络资源，网络接口，网络地址， 以及接收和传输数据。

步骤

1. 从节点页面中，选择设备管理节点或设备网关节点。
2. 选择 * 概述 * 。

   " 概述 " 选项卡的 " 节点信息 " 部分显示节点的摘要信息，例如节点的名称，类型， ID 和连接状态。IP 地址列表包括每个地址的接口名称，如下所示：

   - * adllb* 和 * adlli* ： 如果对管理网络接口使用主动 / 备份绑定，则显示此信息
   - * eth * ： 网格网络，管理网络或客户端网络。
   - * hic* ： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
   - * MTC* ： 设备上的一个物理 1-GbE 端口。一个或多个 MTC 接口已绑定，以构成管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。

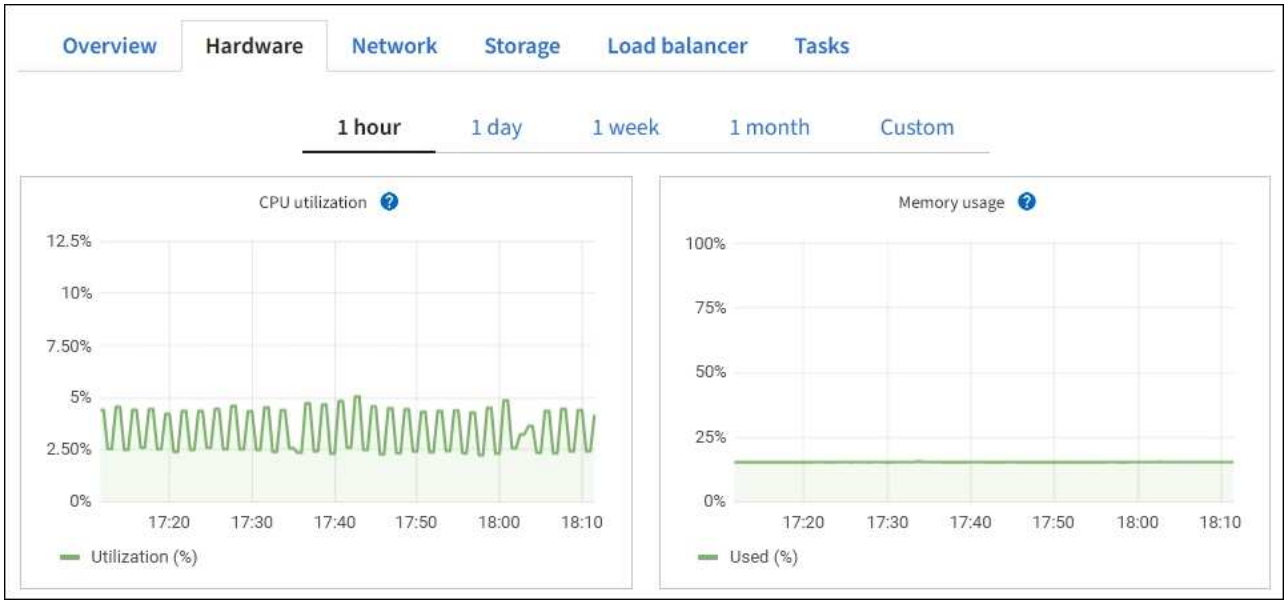


   " 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

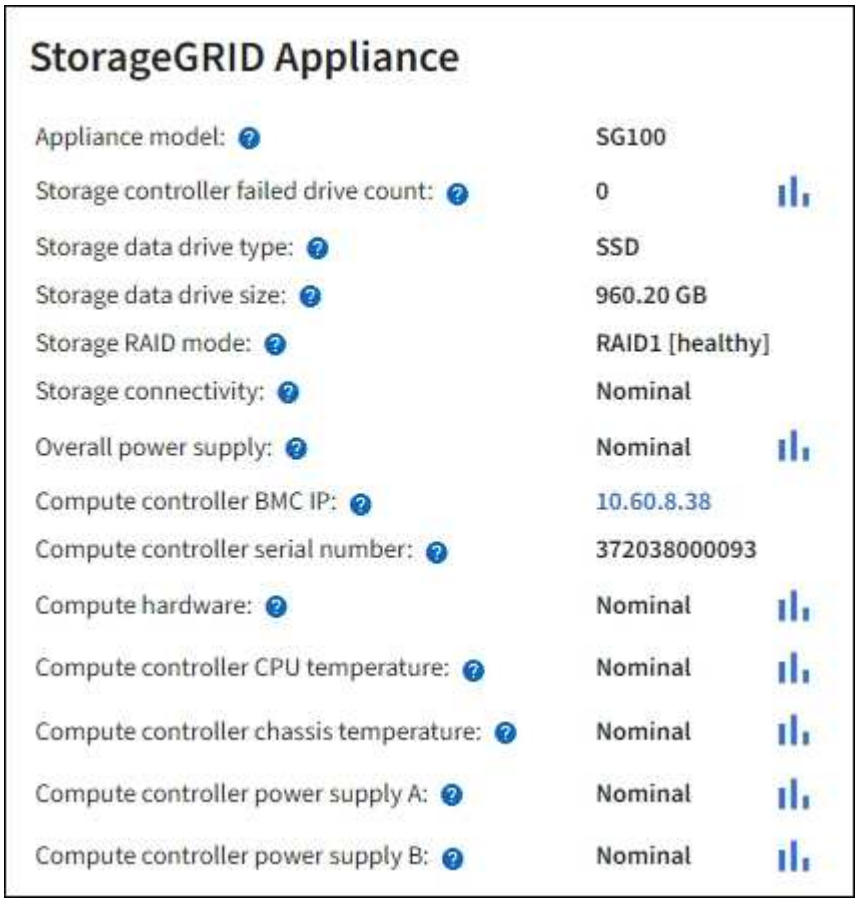
3. 选择 * 硬件 * 可查看有关此设备的详细信息。

   a. 查看 CPU 利用率和内存图形，确定 CPU 和内存使用量随时间的变化所占百分比。要显示不同的时间间

隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。



b. 向下滚动以查看设备组件表。此表包含型号名称，序列号，控制器固件版本以及每个组件的状态等信息。



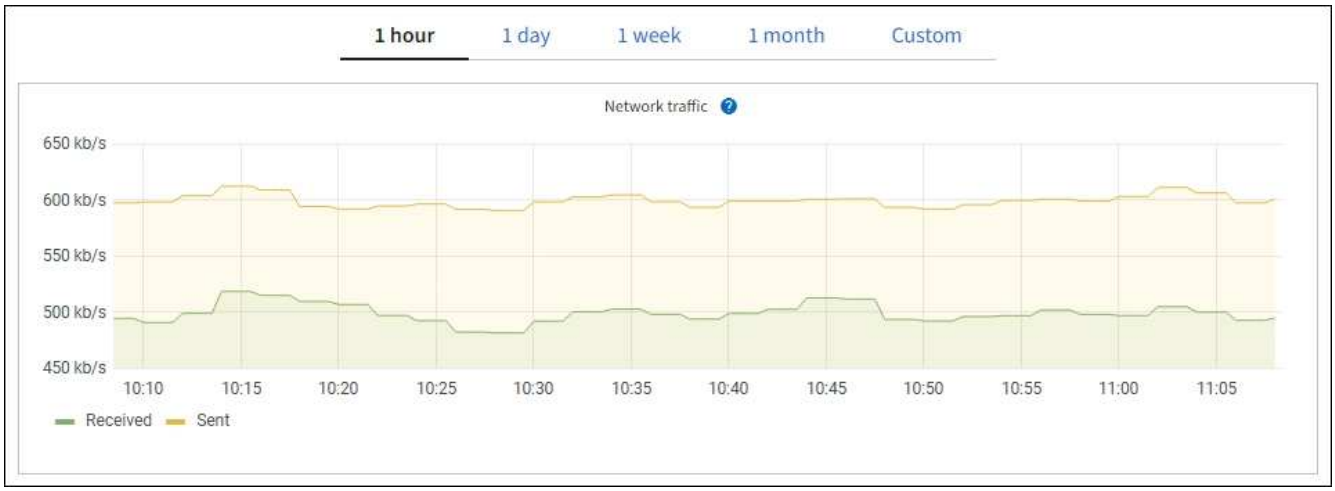
字段	Description
设备型号	此 StorageGRID 设备的型号。
存储控制器故障驱动器计数	非最佳驱动器的数量。
存储数据驱动器类型	设备中的驱动器类型，例如 HDD （硬盘驱动器）或 SSD （固态驱动器）。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller ， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含 BMC 的设备型号，不会显示此字段。
计算控制器序列号	计算控制器的序列号。
计算硬件	计算控制器硬件的状态。
计算控制器 CPU 温度	计算控制器 CPU 的温度状态。
计算控制器机箱温度	计算控制器的温度状态。

a. 确认所有状态均为 "`标称值。` "

如果状态不是 "`标称，` " ，请查看任何当前警报。

4. 选择 * 网络 * 可查看每个网络的信息。

网络流量图提供了整体网络流量的摘要。



a. 查看网络接口部分。

Network interfaces

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

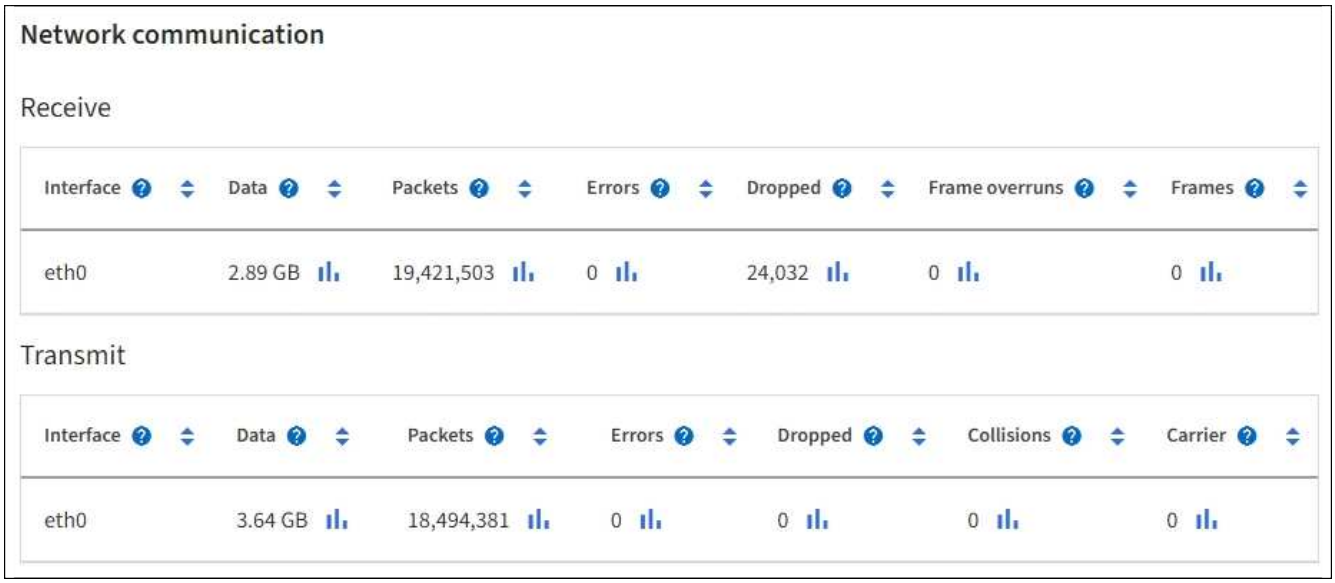
使用下表以及网络接口表中 * 速度 * 列中的值确定设备上的四个 40/100-GbE 网络端口是否配置为使用主动 / 备份模式或 LACP 模式。

表中显示的值假定使用了所有四个链路。

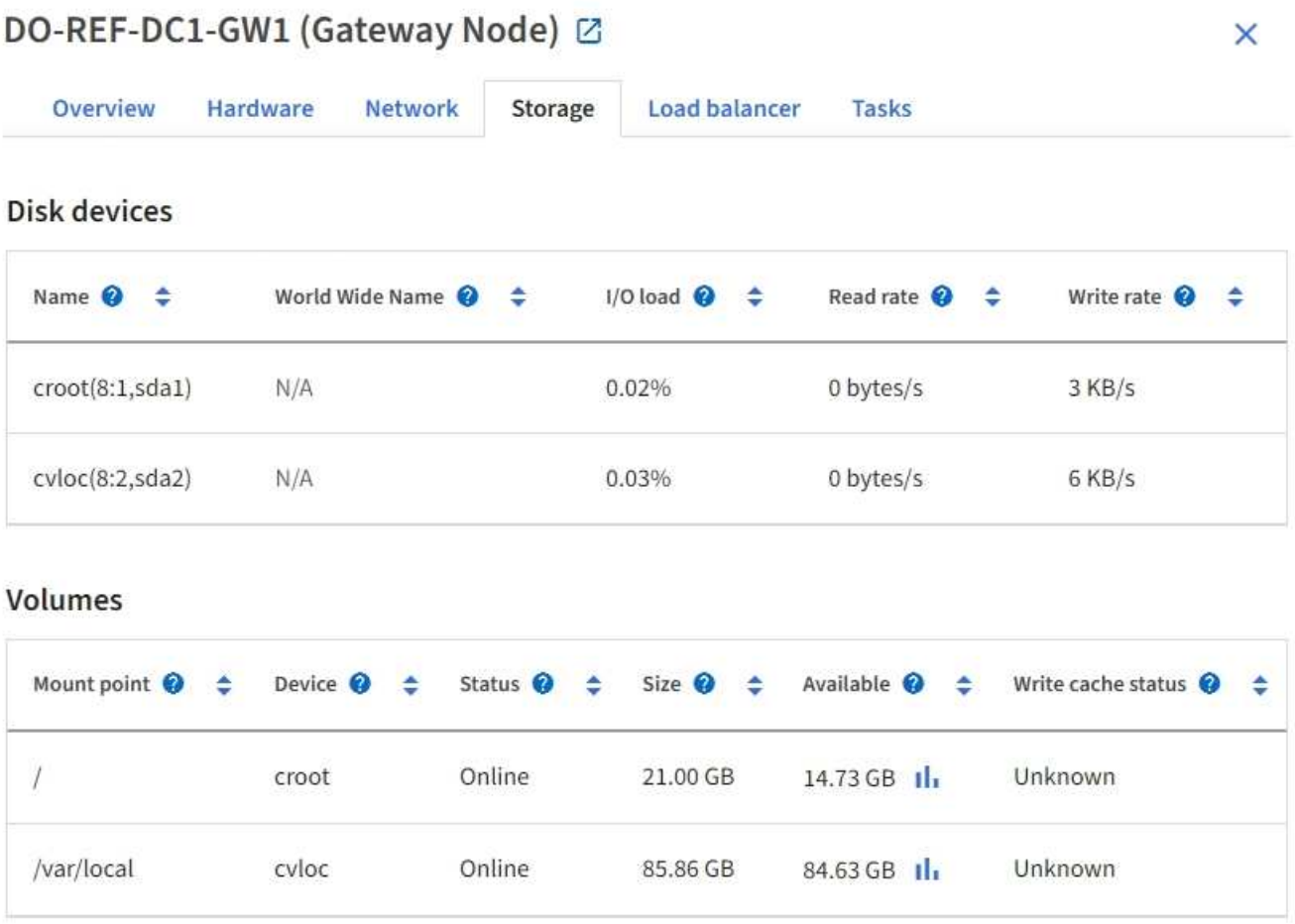
链路模式	绑定模式	单个 **HIC** 链路速度（ **hic1** ， **hic2** ， **hic3** ， **hic4** ）	预期网格 **/** 客户端网络速度（ **eth0** ， **eth2** ）
聚合	LACP	100	400
已修复	LACP	100	200
已修复	主动 / 备份	100	100
聚合	LACP	40	160
已修复	LACP	40	80
已修复	主动 / 备份	40	40

b. 查看网络通信部分。

接收和传输表显示了通过每个网络接收和发送的字节数和数据包数，以及其他接收和传输指标。



5. 选择 * 存储 * 可查看有关服务设备上的磁盘设备和卷的信息。



相关信息

SG100 和 SG1000 服务设备

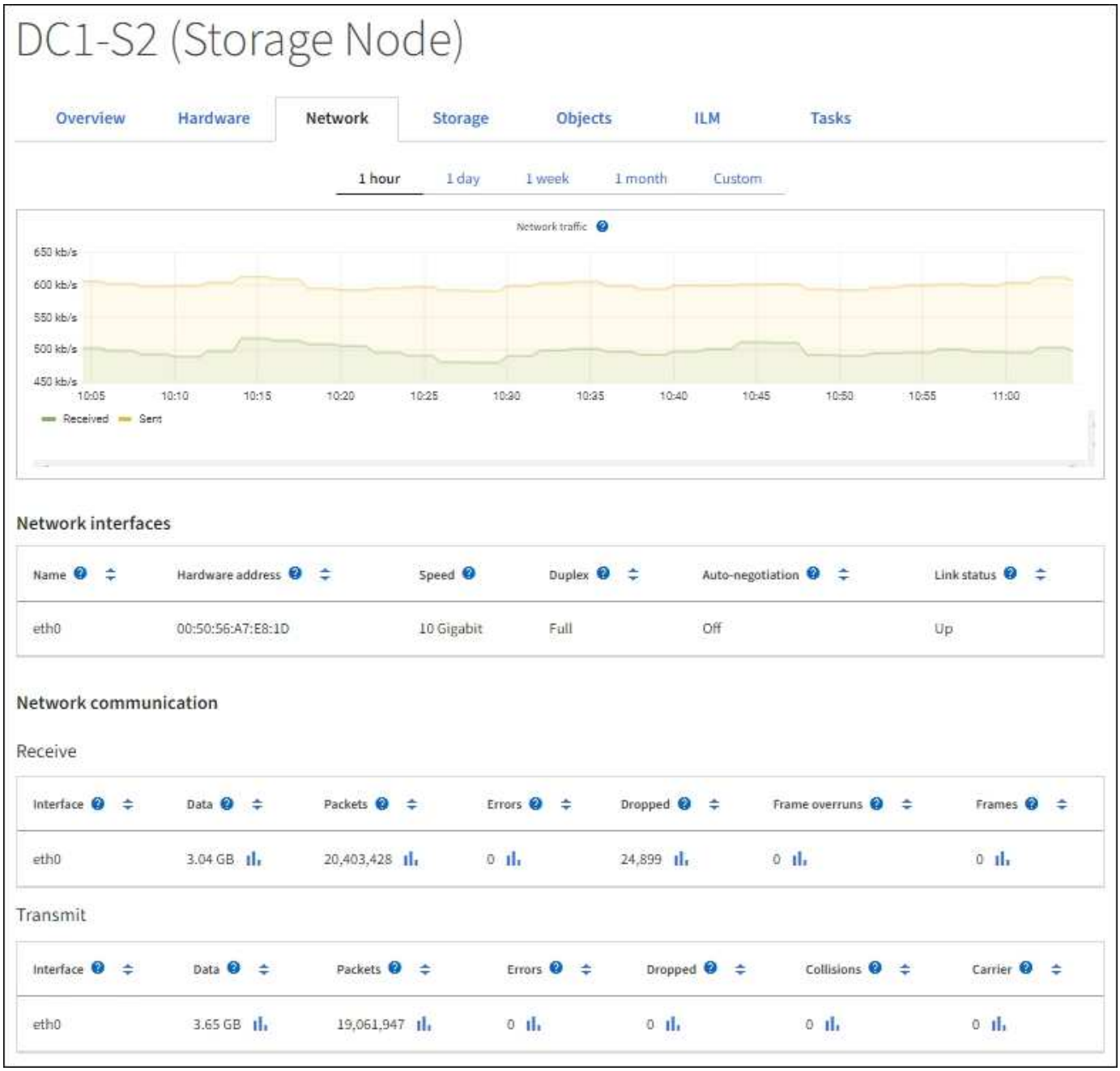
查看网络选项卡

网络选项卡显示一个图形，其中显示了通过节点，站点或网格上的所有网络接口接收和发送的网络流量。

此时将显示所有节点，每个站点和整个网格的网络选项卡。

要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。

对于节点，网络接口表提供了有关每个节点的物理网络端口的信息。网络通信表提供了有关每个节点的接收和传输操作以及任何驱动程序报告的故障计数器的详细信息。



相关信息

监控网络连接和性能

查看存储选项卡

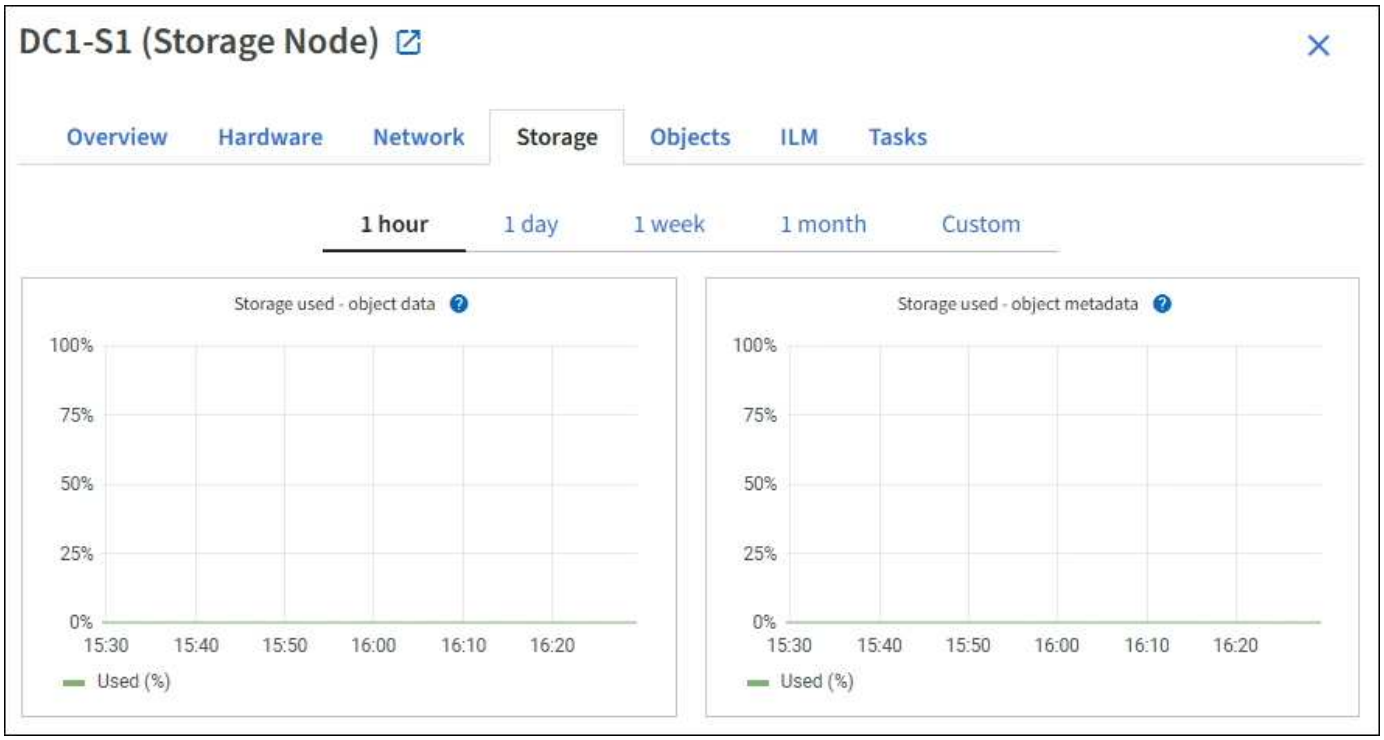
存储选项卡汇总了存储可用性和其他存储指标。

此时将显示所有节点，每个站点和整个网格的存储选项卡。

已用存储图

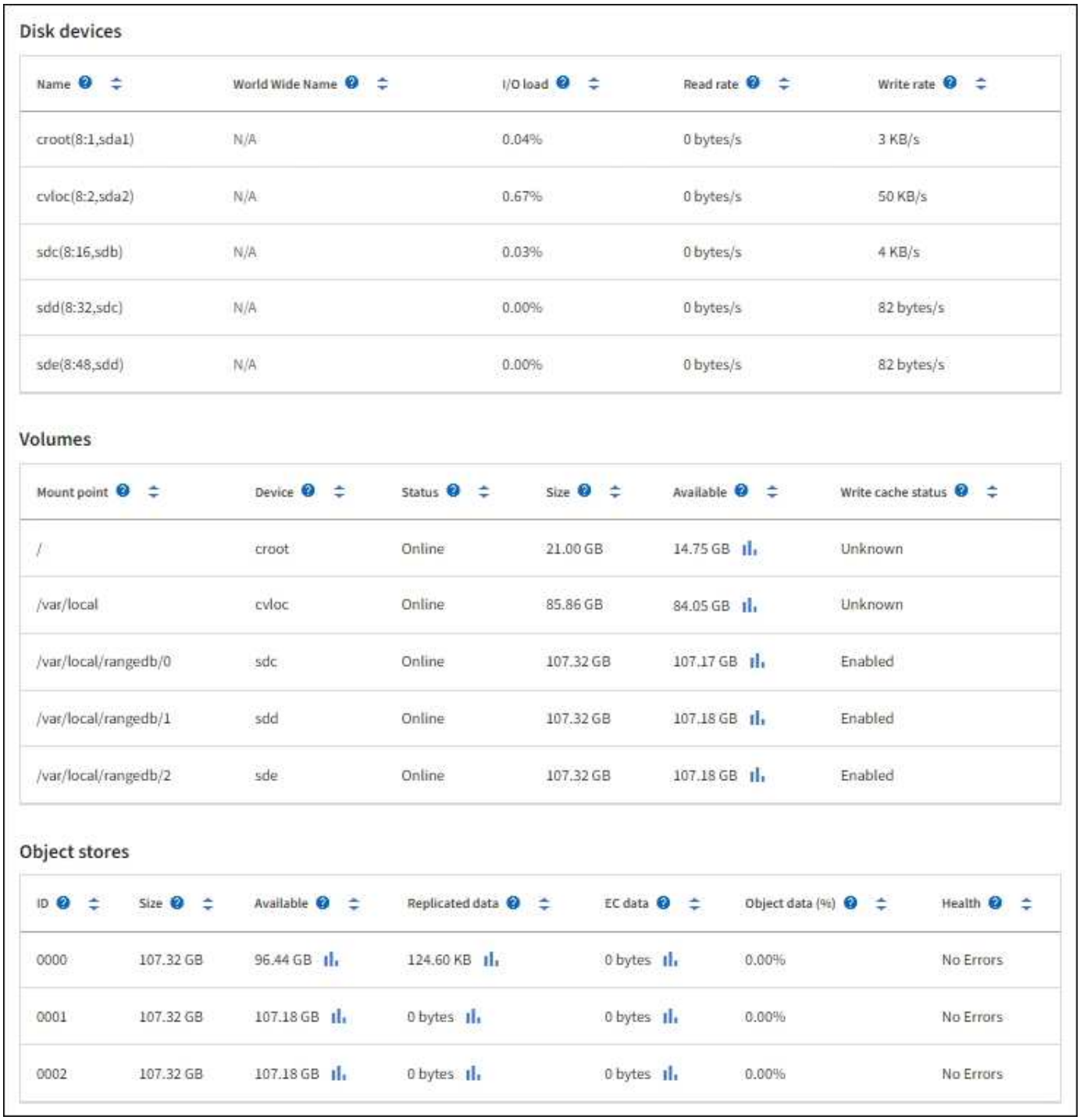
对于存储节点，每个站点和整个网格， " 存储 " 选项卡包含一些图形，用于显示对象数据和对象元数据在一段时间内使用了多少存储。

站点或网格的总值不包括至少在五分钟内未报告指标的节点，例如脱机节点。



磁盘设备，卷和对象存储表

对于所有节点，存储选项卡包含节点上磁盘设备和卷的详细信息。对于存储节点，对象存储表提供了有关每个存储卷的信息。



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

相关信息

监控存储容量

使用任务选项卡重新启动网格节点

通过任务选项卡，您可以重新启动选定节点。此时将显示所有节点的任务选项卡。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。

- 您具有配置密码短语。

关于此任务

您可以使用任务选项卡重新启动节点。对于设备节点，您还可以使用任务选项卡将设备置于维护模式。

- 从任务选项卡重新启动网格节点会在目标节点上发出 reboot 命令。重新启动节点时，该节点将关闭并重新启动。所有服务都会自动重新启动。

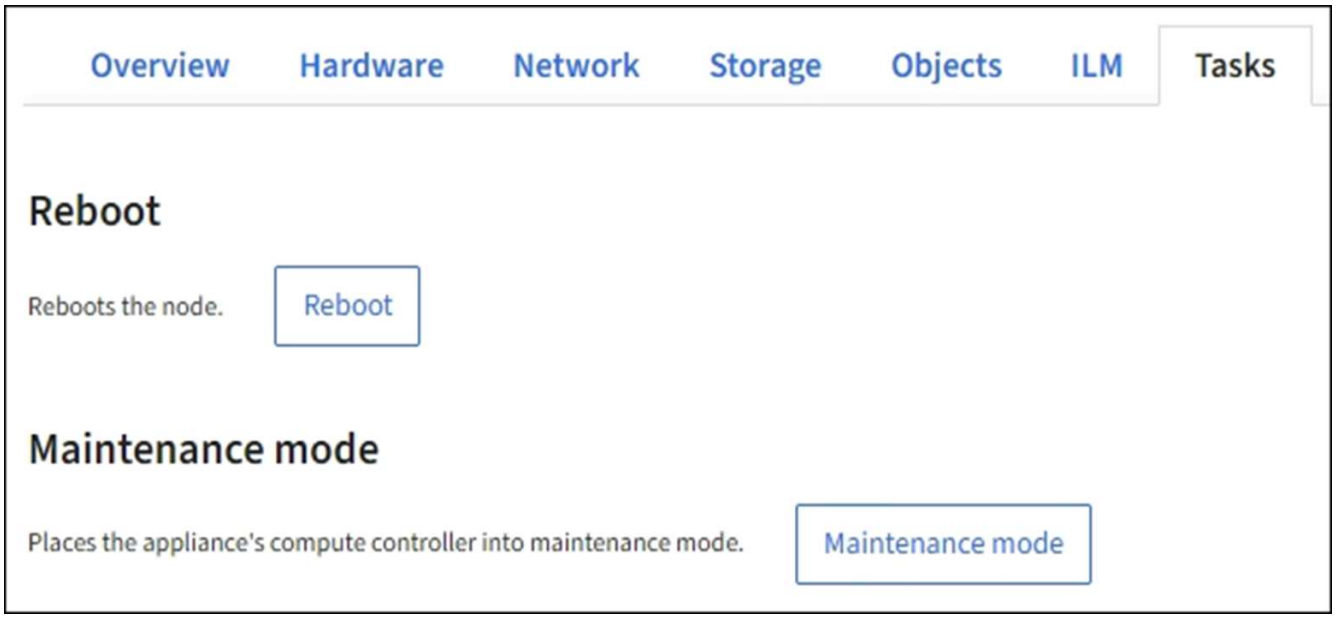
  如果您计划重新启动存储节点，请注意以下事项：

  - 如果 ILM 规则指定了 " 双提交 " 的载入行为或规则指定了 " 已平衡 " ，并且无法立即创建所有必需的副本，则 StorageGRID 会立即将任何新载入的对象提交到同一站点上的两个存储节点，并在稍后评估 ILM 。如果要重新启动给定站点上的两个或多个存储节点，则在重新启动期间可能无法访问这些对象。
  - 为了确保您可以在存储节点重新启动时访问所有对象，请在重新启动节点之前，停止在站点上载入对象大约一小时。
- 您可能需要将 StorageGRID 设备置于维护模式才能执行某些过程，例如更改链路配置或更换存储控制器。有关说明，请参见设备的硬件安装和维护说明。

  在极少数情况下，将 StorageGRID 设备置于维护模式可能会使该设备无法进行远程访问。

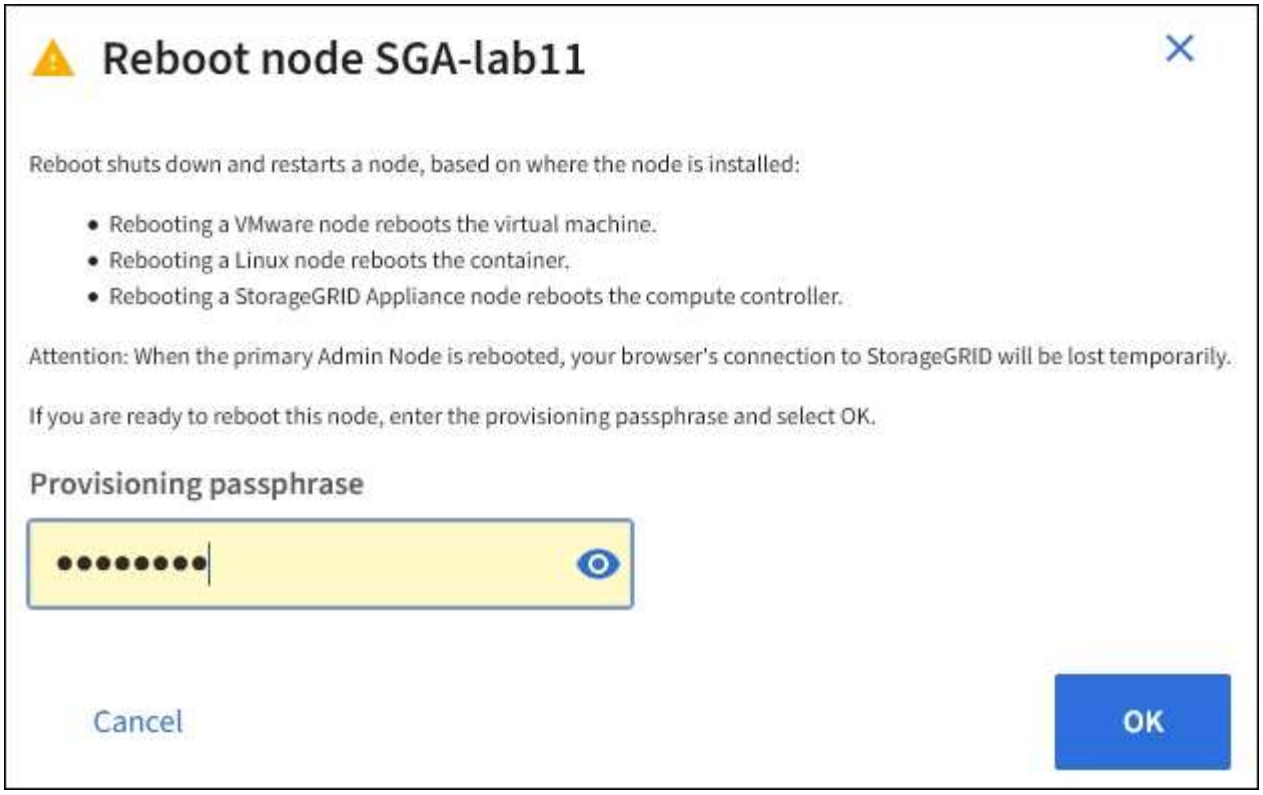
步骤

1. 选择 * 节点 * 。
2. 选择要重新启动的网格节点。
3. 选择 * 任务 * 选项卡。



4. 选择 * 重新启动 * 。

   此时将显示确认对话框。



如果要重新启动主管理节点，则确认对话框会提醒您，服务停止后，浏览器与网格管理器的连接将暂时断开。

5. 输入配置密码短语，然后单击 * 确定 * 。
6. 等待节点重新启动。

   关闭服务可能需要一些时间。

   节点重新启动时， * 节点 * 页面左侧会显示灰色图标（管理员关闭）。当所有服务重新启动且节点已成功连接到网格时， * 节点 * 页面应显示正常状态（节点名称左侧没有图标），表示没有活动警报且节点已连接到网格。

相关信息

SG6000 存储设备

SG5700 存储设备

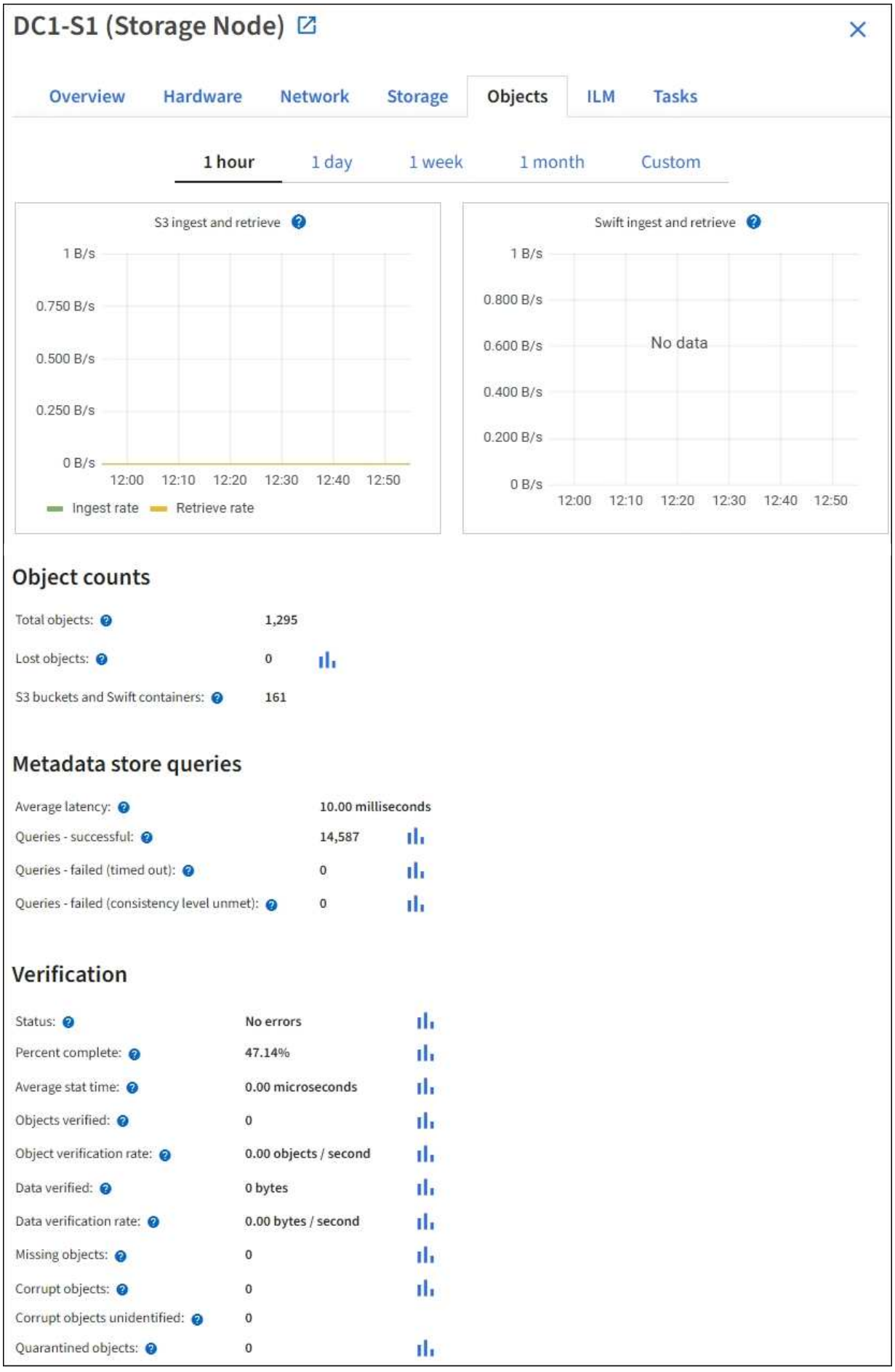
SG5600 存储设备

SG100 和 SG1000 服务设备

查看对象选项卡

对象选项卡提供了有关的信息 S3 和 Swift 载入和检索速率。

此时将显示每个存储节点，每个站点和整个网格的对象选项卡。对于存储节点，对象选项卡还提供对象计数以及有关元数据查询和后台验证的信息。

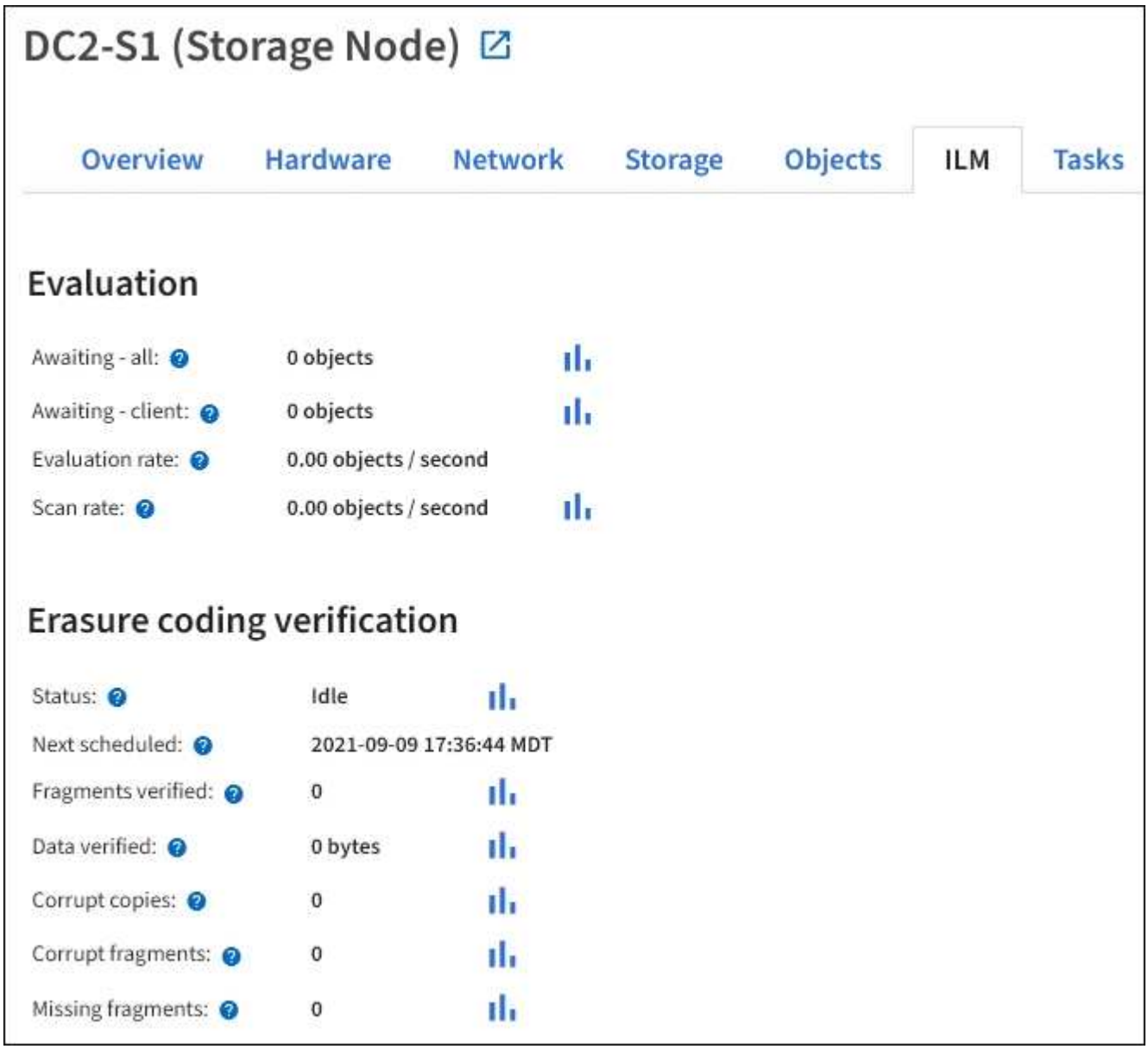

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

查看 **ILM** 选项卡

ILM 选项卡提供了有关信息生命周期管理（ ILM ）操作的信息。

此时将显示每个存储节点，每个站点和整个网格的 ILM 选项卡。对于每个站点和网格， "ILM " 选项卡会显示一个 ILM 队列随时间变化的图形。对于网格，此选项卡还提供完成对所有对象的完整 ILM 扫描的估计时间。

对于存储节点， "ILM " 选项卡提供有关纠删编码对象的 ILM 评估和后台验证的详细信息。



相关信息

监控信息生命周期管理

管理 StorageGRID

查看负载平衡器选项卡

" 负载平衡器 " 选项卡包含与负载平衡器服务的运行相关的性能和诊断图。

此时将为管理节点和网关节点，每个站点和整个网格显示负载平衡器选项卡。对于每个站点， " 负载平衡器 " 选项卡提供该站点所有节点的统计信息的聚合摘要。对于整个网格， " 负载平衡器 " 选项卡提供了所有站点统计信息的聚合摘要。

如果未通过负载平衡器服务运行任何 I/O ，或者未配置任何负载平衡器，则图形将显示 "`No data.` " 。



请求流量

此图提供了负载平衡器端点与发出请求的客户端之间传输的数据吞吐量的 3 分钟移动平均值，以每秒位数为单位。

此值将在每个请求完成时更新。因此，此值可能与请求率较低或请求寿命较长时的实时吞吐量不同。您可以查看 " 网络 " 选项卡，更真实地查看当前网络行为。

传入请求速率

此图按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分，提供每秒新请求数的 3 分钟移动平均值。验证新请求的标头后，此值将更新。

平均请求持续时间（非错误）

此图提供了按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分的 3 分钟移动平均请求持续时间。每个请求持续时间从负载平衡器服务解析请求标头时开始，到将完整的响应正文返回给客户端时结束。

错误响应率

此图提供了每秒返回给客户端的错误响应数的 3 分钟移动平均值，并按错误响应代码进行细分。

相关信息

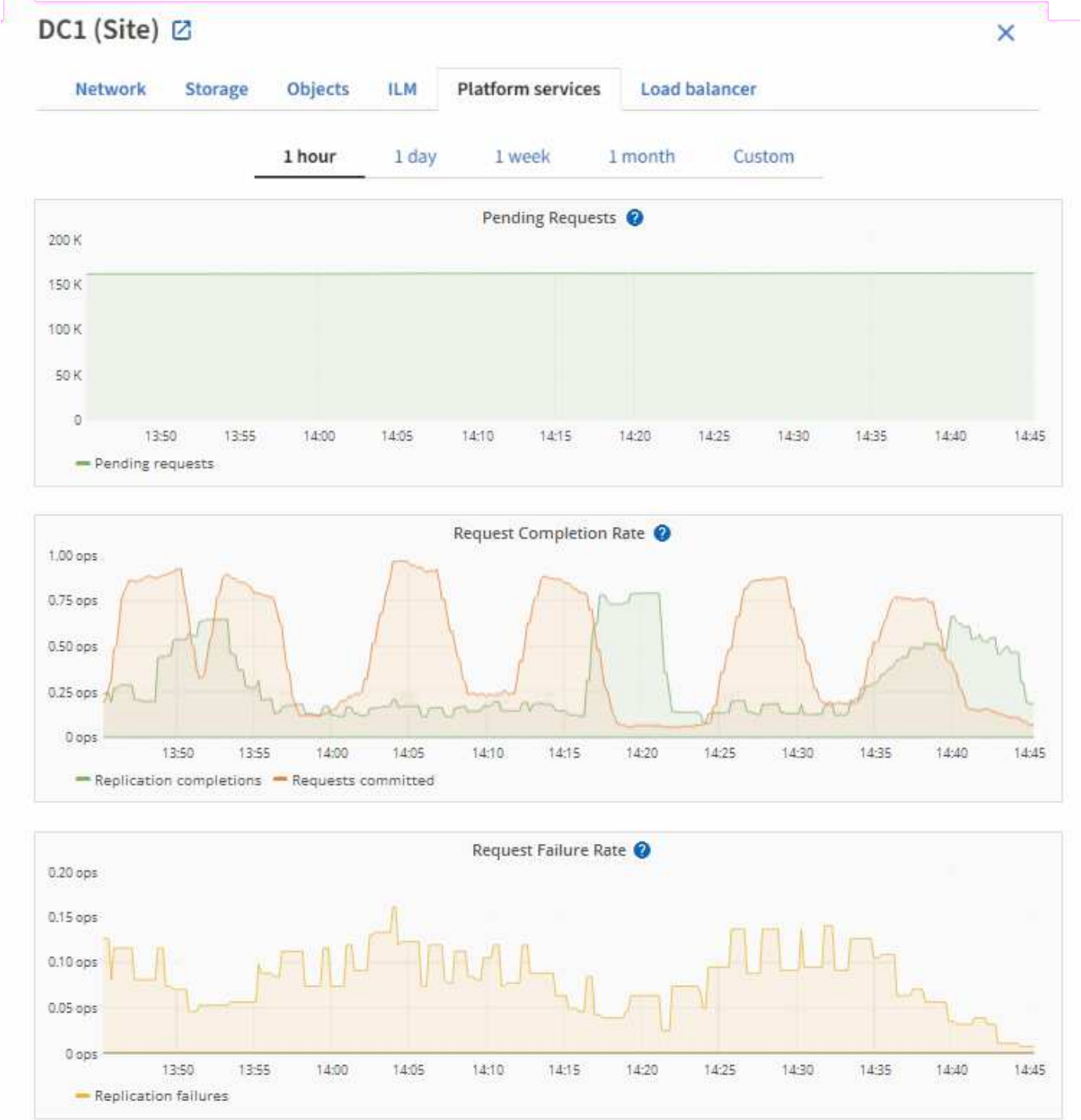
监控负载平衡操作

管理 StorageGRID

查看平台服务选项卡

平台服务选项卡提供了有关站点上任何 S3 平台服务操作的信息。

此时将显示每个站点的平台服务选项卡。此选项卡提供了有关 S3 平台服务的信息，例如 CloudMirror 复制和搜索集成服务。此选项卡上的图形显示了待处理请求数，请求完成率和请求失败率等指标。



有关 S3 平台服务的详细信息，包括故障排除详细信息，请参见 有关管理 StorageGRID 的说明。

查看 **SANtricity** 系统管理器选项卡

通过 SANtricity 系统管理器选项卡，您可以访问 SANtricity 系统管理器，而无需配置或连接存储设备的管理端口。您可以使用此选项卡查看硬件诊断和环境信息以及与驱动器相关的问题。

此时将为存储设备节点显示 SANtricity System Manager 选项卡。

使用 SANtricity System Manager ，您可以执行以下操作：

- 查看存储阵列级别性能， I/O 延迟，存储控制器 CPU 利用率和吞吐量等性能数据
- 检查硬件组件状态
- 执行支持功能，包括查看诊断数据和配置 E 系列 AutoSupport

要使用 SANtricity 系统管理器为 E 系列 AutoSupport 配置代理，请参见管理 StorageGRID 中的说明。

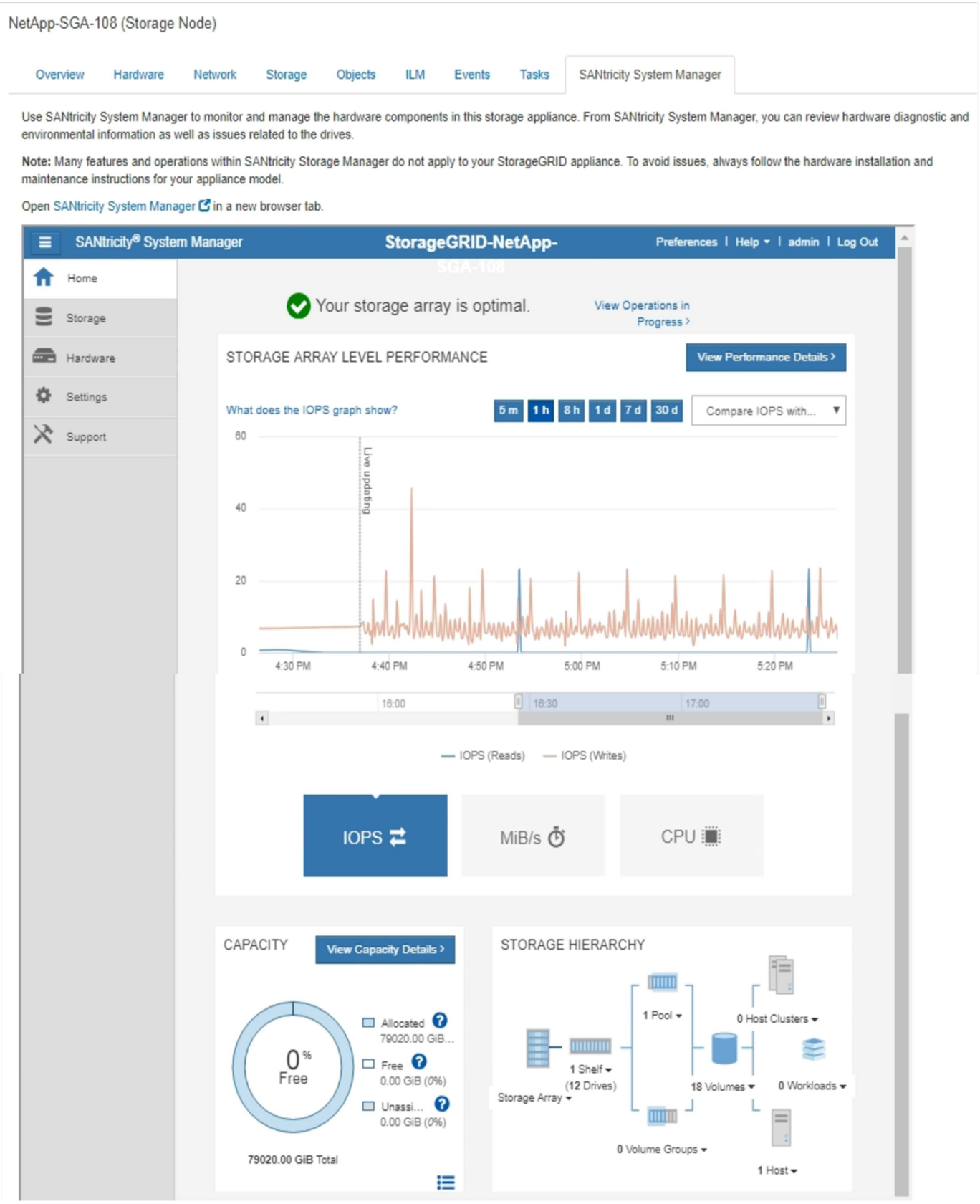
管理 StorageGRID

要通过网格管理器访问 SANtricity 系统管理器，您必须具有存储设备管理员权限或 root 访问权限。

要使用网格管理器访问SANtricity 系统管理器、您必须具有SANtricity 固件8.70 (11.70)或更高版本。

从网格管理器访问 SANtricity 系统管理器通常仅用于监控设备硬件和配置 E 系列 AutoSupport 。SANtricity System Manager 中的许多功能和操作（例如升级固件）不适用于监控 StorageGRID 设备。为避免出现问题，请始终按照适用于您的设备的硬件安装和维护说明进行操作。

此选项卡将显示 SANtricity 系统管理器的主页。



您可以使用 SANtricity 系统管理器链接在新浏览器窗口中打开 SANtricity 系统管理器，以便于查看。

要查看存储阵列级别性能和容量使用情况的详细信息，请将光标悬停在每个图形上。

有关查看可从 SANtricity 系统管理器选项卡访问的信息的详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

您应定期监控的信息

StorageGRID 是一种容错分布式存储系统，即使发生错误或节点或站点不可用，它也可以继续运行。您必须主动监控系统运行状况，工作负载和使用情况统计信息，以便在潜在问题影响网格的效率或可用性之前采取措施解决这些问题。

繁忙的系统会生成大量信息。本节提供了有关持续监控的最重要信息的指导。

要监控的内容	**Frequency**
。 系统运行状况数据 显示在网格管理器信息板上。记下是否与前一天发生了任何更改。	每天
速率 存储节点对象和元数据容量 正在使用	每周
信息生命周期管理操作	每周
网络连接和性能	每周
节点级资源	每周
租户活动	每周
外部归档存储系统的容量	每周
负载平衡操作	在初始配置之后以及任何配置更改之后
提供软件修补程序和软件升级	每月

监控系统运行状况

您应每天监控 StorageGRID 系统的整体运行状况。

关于此任务

StorageGRID 系统具有容错功能，即使网格的某些部分不可用，它也可以继续运行。StorageGRID 系统中可能出现的问题描述 的第一个迹象可能是警报或警报（传统系统），而不一定是具有系统操作的问题描述 。注意系统运行状况有助于您在小问题影响操作或网格效率之前检测到这些问题。

网格管理器信息板上的 " 运行状况 " 面板提供了可能影响系统的问题的摘要。您应调查信息板上显示的任何问题。

要在触发警报后立即收到警报通知，您可以为警报设置电子邮件通知或配置 SNMP 陷阱。

步骤

1. 登录到网格管理器以查看信息板。
2. 查看运行状况面板中的信息。



如果存在问题，则会显示一些链接，您可以通过这些链接查看其他详细信息：

链接。	表示
网格详细信息	如果任何节点已断开连接（连接状态为未知或管理员关闭），则显示此消息。单击链接或单击蓝色或灰色图标以确定受影响的节点。
当前警报	如果当前有任何警报处于活动状态，则显示此消息。单击链接，或单击 * 严重 * ， * 主要 * 或 * 次要 * 以查看 * 警报 * > * 当前 * 页面上的详细信息。
最近解决的警报	如果已解决过去一周触发的任何警报，则显示此消息。单击此链接可在 * 警报 * > * 已解决 * 页面上查看详细信息。
许可证	如果存在具有此 StorageGRID 系统软件许可证的问题描述 ，则显示此消息。单击此链接可在 * 维护 * > * 系统 * > * 许可证 * 页面上查看详细信息。

相关信息

- 管理 StorageGRID
- 为警报设置电子邮件通知
- 使用 SNMP 监控

监控节点连接状态

如果一个或多个节点与网格断开连接，则关键 StorageGRID 操作可能会受到影响。您必须监控节点连接状态并及时解决任何问题。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

节点可以具有以下三种连接状态之一：

- * 未连接 - 未知 * ：节点未连接到网格，原因未知。例如，节点之间的网络连接已断开或电源已关闭。此外，可能还会触发 * 无法与节点 * 通信 " 警报。其他警报可能也处于活动状态。这种情况需要立即引起关注。

  在受管关闭操作期间，节点可能会显示为未知。在这些情况下，您可以忽略未知状态。

- * 未连接 - 已管理员关闭 * ：由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。一个或多个警报可能也处于活动状态。

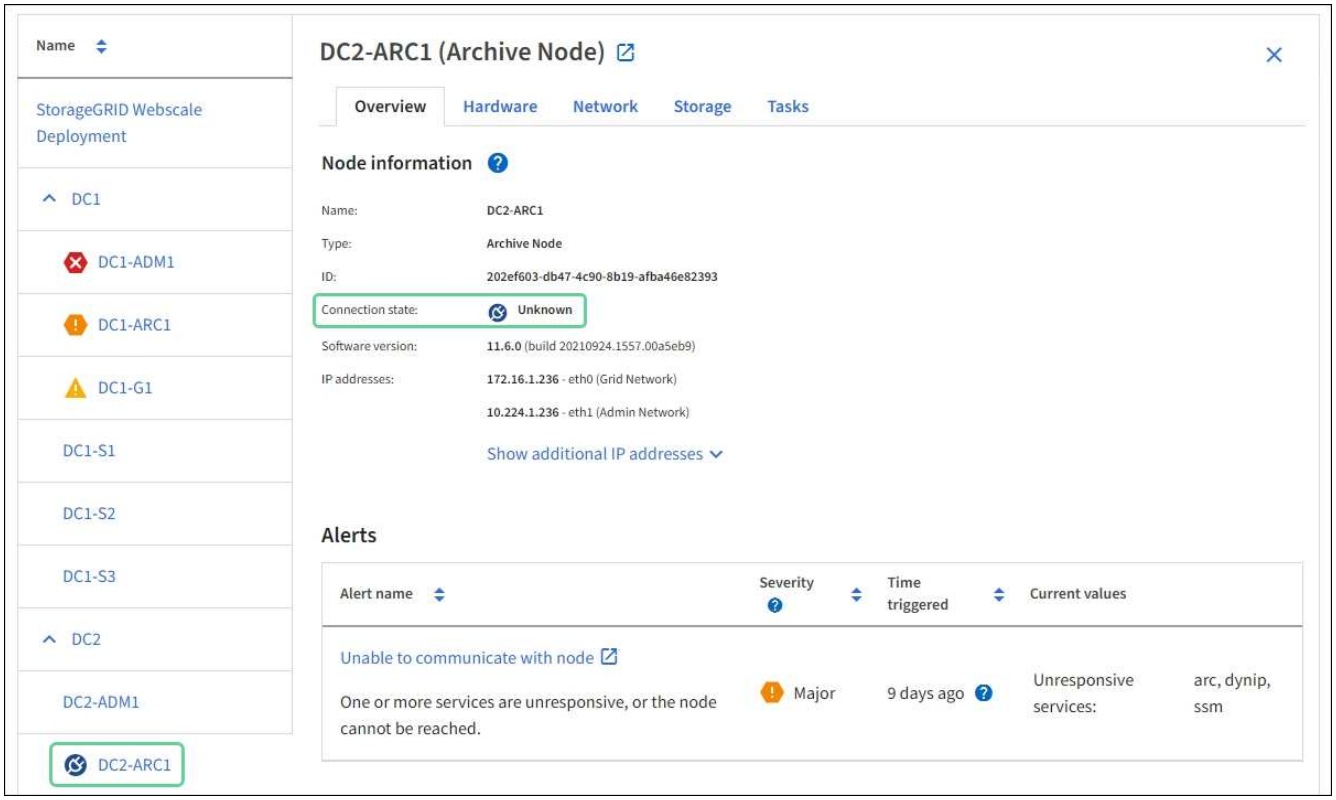
- * 已连接 * ：节点已连接到网格。

步骤

1. 如果信息板的 " 运行状况 " 面板上显示蓝色或灰色图标，请单击该图标或单击 * 网格详细信息 * 。（只有在至少有一个节点与网格断开连接时，才会显示蓝色或灰色图标以及 * 网格详细信息 * 链接。）

   此时将显示节点树中第一个蓝色节点的 "Overview" 页面。如果没有蓝色节点，则会显示树中第一个灰色节点的 " 概述 " 页面。

   在此示例中，名为 DC1-S3 的存储节点具有一个蓝色图标。节点信息面板上的 * 连接状态 * 为 * 未知 * ，并且 * 无法与节点 * 通信警报处于活动状态。此警报指示一个或多个服务无响应或无法访问节点。



2. 如果节点有蓝色图标，请按照以下步骤操作：

   a. 选择表中的每个警报，然后按照建议的操作进行操作。

例如，您可能需要重新启动已停止的服务或重新启动节点的主机。

b. 如果无法使节点恢复联机，请联系技术支持。

3. 如果节点有灰色图标，请执行以下步骤：

在维护过程中，灰色节点是预期的，并且可能与一个或多个警报关联。根据底层问题描述，这些 "`administratively down` " 节点通常会恢复联机，而无需任何干预。

a. 查看警报部分，并确定是否有任何警报影响此节点。

b. 如果一个或多个警报处于活动状态，请选择表中的每个警报，然后按照建议的操作进行操作。

c. 如果无法使节点恢复联机，请联系技术支持。

相关信息

警报参考

恢复和维护

查看当前警报

触发警报后，信息板上会显示一个警报图标。节点页面上还会显示节点的警报图标。除非警报已静音，否则也可能会发送电子邮件通知。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您也可以观看以下视频： "视频：警报概述"。



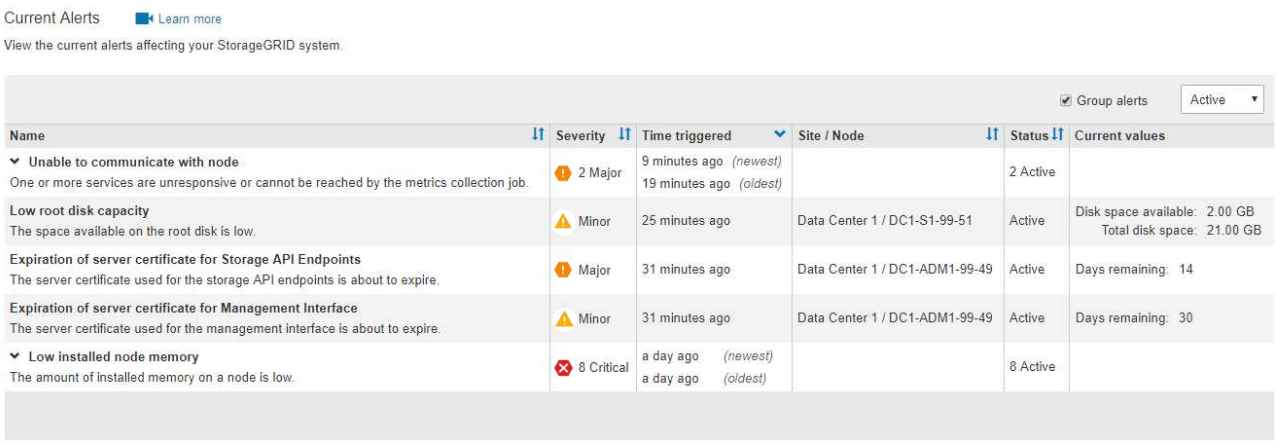
步骤

1. 如果一个或多个警报处于活动状态，请执行以下操作之一：

◦ 在信息板上的 " 运行状况 " 面板中，单击警报图标或单击 * 当前警报 * 。（只有当前至少有一个警报处于活动状态时，才会显示警报图标和 * 当前警报 * 链接。）

◦ 选择 * 警报 * > * 当前 * 。

此时将显示当前警报页面。它会列出当前影响 StorageGRID 系统的所有警报。



默认情况下，警报显示如下：

- 首先显示最近触发的警报。
- 同一类型的多个警报显示为一个组。
- 未显示已静音的警报。
- 对于特定节点上的特定警报，如果达到阈值的严重性超过一个，则仅显示最严重的警报。也就是说，如果达到次要，主要和严重严重性的警报阈值，则仅显示严重警报。

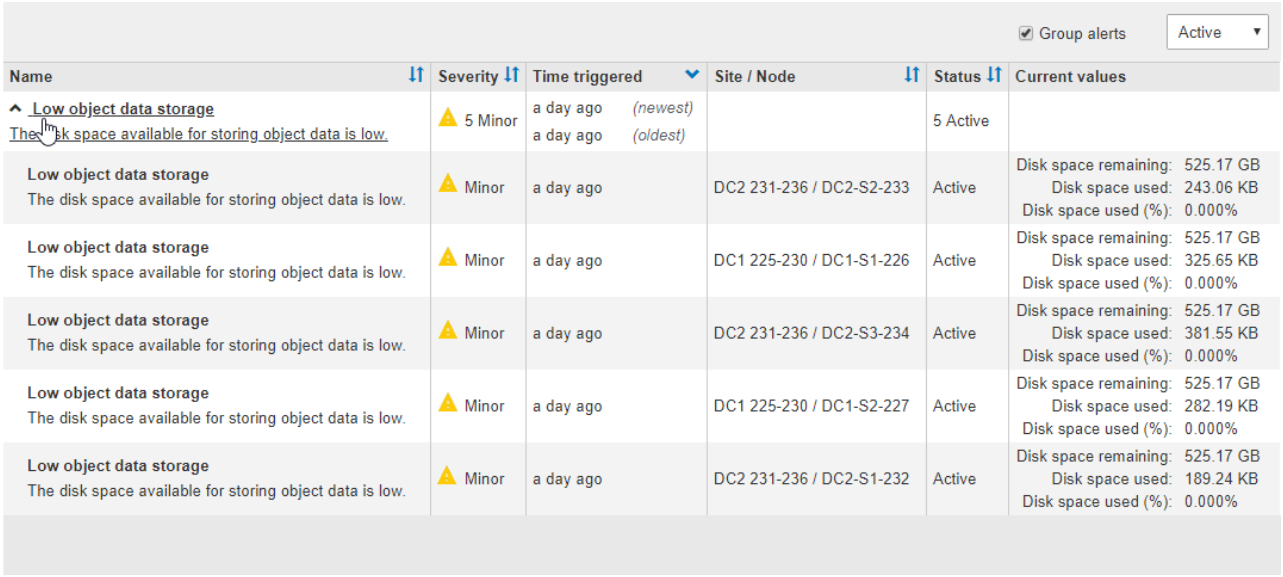
" 当前警报 " 页面每两分钟刷新一次。

2. 查看表中的信息。

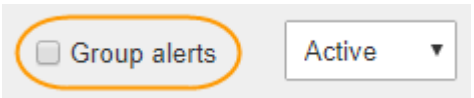
列标题	**Description**
Name	警报及其问题描述 的名称。
severity	警报的严重性。如果对多个警报进行了分组，则标题行将显示每个严重性发生的警报实例数。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 • * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。
时间已触发	触发警报多长时间前。如果对多个警报进行了分组，则标题行将显示警报的最新实例（ *lates* ）和最旧的警报实例（ *oldest* ）的时间。

列标题	Description
站点 / 节点	发生警报的站点和节点的名称。如果对多个警报进行分组，则站点和节点名称不会显示在标题行中。
Status	警报处于活动状态还是已静音。如果对多个警报进行分组，并在下拉列表中选择了 * 所有警报 * ，则标题行将显示该警报处于活动状态的实例数以及已静音的实例数。
当前值	导致触发警报的指标的当前值。对于某些警报，还会显示其他值，以帮助您了解和调查此警报。例如，为 "* 对象数据存储空间不足 * " 警报显示的值包括已用磁盘空间百分比，磁盘空间总量和已用磁盘空间量。 • 注： * 如果对多个警报进行分组，则当前值不会显示在标题行中。

3. 要扩展和折叠警报组，请执行以下操作：
   - 要显示组中的各个警报，请单击向下记号 ⌄ 或单击组的名称。
   - 要隐藏组中的各个警报，请单击 UP caret ⌃ 或单击组的名称。



4. 要显示单个警报而不是多组警报，请取消选中表顶部的 * 组警报 * 复选框。



5. 要对警报或警报组进行排序，请单击向上 / 向下箭头 ⇅ 在每个列标题中。
   - 如果选择 * 组警报 * ，则会对每个组中的警报组和各个警报进行排序。例如，您可能希望按 * 时间触发 * 对组中的警报进行排序，以查找特定警报的最新实例。
   - 取消选择 * 组警报 * 后，系统将对整个警报列表进行排序。例如，您可能希望按 * 节点 / 站点 * 对所有警报进行排序，以查看影响特定节点的所有警报。
6. 要按状态筛选警报，请使用表顶部的下拉菜单。



- 选择 * 所有警报 * 可查看所有当前警报（活动警报和静音警报）。
- 选择 * 活动 * 可仅查看当前处于活动状态的警报。
- 选择 * 已静音 * 可仅查看当前已静音的警报。请参见 静默警报通知。

7. 要查看特定警报的详细信息，请从表中选择该警报。

   此时将显示警报对话框。请参见 查看特定警报。

查看已解决的警报

您可以搜索和查看已解决的警报历史记录。

您需要的内容

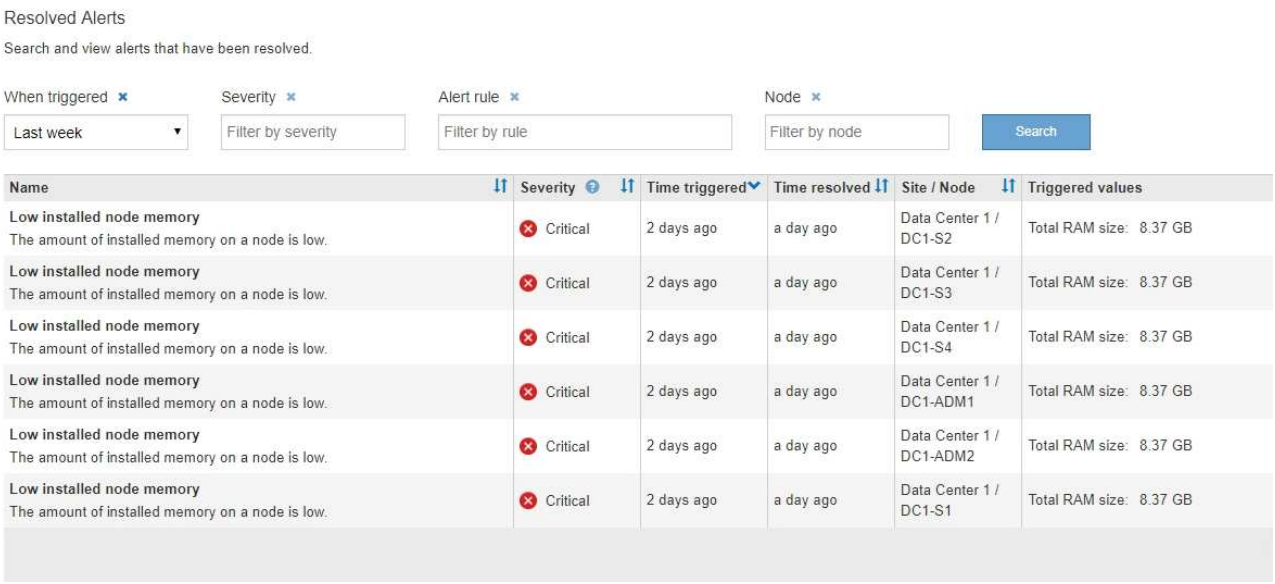
- 您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 要查看已解决的警报，请执行以下操作之一：
   - 从信息板上的 " 运行状况 " 面板中，单击 * 最近解决的警报 * 。

     只有在过去一周触发了一个或多个警报且这些警报现已解决时， * 最近解决的警报 * 链接才会显示。

   - 选择 * 警报 * > * 已解决 * 。此时将显示 "Resolved Alerts" 页面。默认情况下，将显示上周触发的已解决警报，而最近触发的警报将首先显示。此页面上的警报先前显示在 " 当前警报 " 页面或电子邮件通知中。



2. 查看表中的信息。

列标题	Description
Name	警报及其问题描述 的名称。
severity	警报的严重性。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 • * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。
时间已触发	触发警报多长时间前。
已解决时间	警报解决多长时间前。
站点 / 节点	发生警报的站点和节点的名称。
触发值	导致触发警报的度量值。对于某些警报，还会显示其他值，以帮助您了解和调查此警报。例如，为 "* 对象数据存储空间不足 * " 警报显示的值包括已用磁盘空间百分比，磁盘空间总量和已用磁盘空间量。

3. 要对已解决警报的整个列表进行排序，请单击向上 / 向下箭头 在每个列标题中。

   例如，您可能希望按 * 站点 / 节点 * 对已解决的警报进行排序，以查看影响特定节点的警报。

4. 或者，也可以使用表顶部的下拉菜单筛选已解决警报列表。
   a. 从 * 何时触发 * 下拉菜单中选择一个时间段，以根据触发警报的时间长度显示已解决的警报。

      您可以搜索在以下时间段内触发的警报：

      - 过去一小时
      - 最后一天
      - 上周（默认视图）
      - 上个月
      - 任何时间段

- 自定义（用于指定时间段的开始日期和结束日期）

b. 从 * 严重性 * 下拉菜单中选择一个或多个严重性，以筛选已解决的特定严重性警报。

c. 从 * 警报规则 * 下拉菜单中选择一个或多个默认或自定义警报规则，以筛选与特定警报规则相关的已解决警报。

d. 从 * 节点 * 下拉菜单中选择一个或多个节点，以筛选与特定节点相关的已解决警报。

e. 单击 * 搜索 * 。

5. 要查看特定已解决警报的详细信息，请从表中选择该警报。

此时将显示警报对话框。请参见 查看特定警报。

查看特定警报

您可以查看有关当前正在影响 StorageGRID 系统的警报或已解决的警报的详细信息。详细信息包括建议的更正操作，触发警报的时间以及与此警报相关的指标的当前值。

您也可以选择 静默当前警报 或 更新警报规则。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 根据您要查看当前警报还是已解决警报，执行以下操作之一：

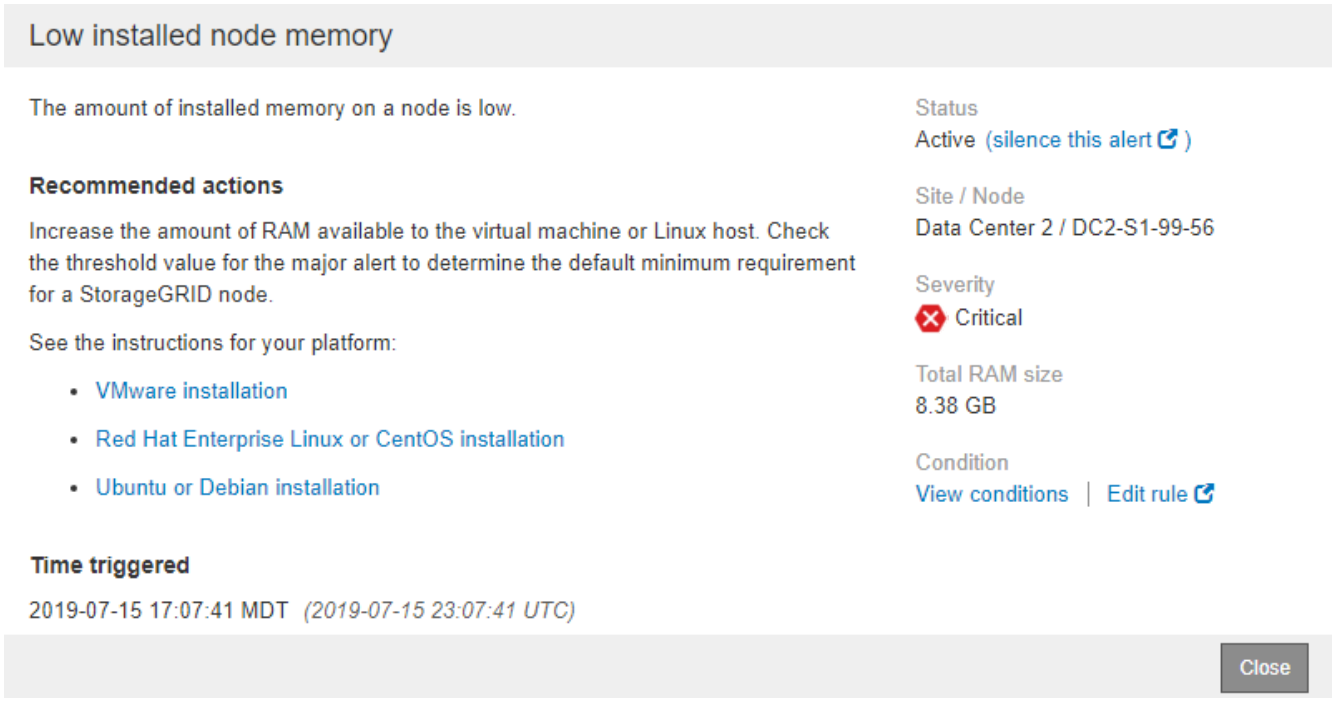
列标题	Description
当前警报	• 从信息板上的 " 运行状况 " 面板中，单击 * 当前警报 * 链接。只有当前至少有一个警报处于活动状态时，才会显示此链接。如果当前没有警报或当前所有警报均已静音，则此链接将隐藏。 • 选择 * 警报 * > * 当前 * 。 • 从 * 节点 * 页面中，为具有警报图标的节点选择 * 概述 * 选项卡。然后，在警报部分中，单击警报名称。
已解决警报	• 从信息板上的 " 运行状况 " 面板中，单击 * 最近解决的警报 * 链接。（只有在过去一周触发了一个或多个警报且现已解决时，才会显示此链接。如果上周未触发和解决任何警报，则此链接将隐藏。） • 选择 * 警报 * > * 已解决 * 。

2. 根据需要展开一组警报，然后选择要查看的警报。

选择警报，而不是一组警报的标题。



此时将显示一个对话框，其中提供了选定警报的详细信息。



3. 查看警报详细信息。

信息	Description
title	警报的名称。
第一段 _	警报的问题描述 。
建议的操作	此警报的建议操作。
时间已触发	在您当地时间和 UTC 时间触发警报的日期和时间。
已解决时间	仅对于已解决的警报，是指在您当地时间和 UTC 解决警报的日期和时间。
Status	警报的状态：活动，静音或已解决。
站点 / 节点	受警报影响的站点和节点的名称。

信息	Description
severity	警报的严重性。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 • * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。
数据值 _	此警报的指标的当前值。对于某些警报，还会显示其他值，以帮助您了解和调查此警报。例如，为 "* 低元数据存储 * " 警报显示的值包括已用磁盘空间百分比，磁盘空间总量和已用磁盘空间量。

4. 或者，也可以单击 * 静默此警报 * 以静默导致触发此警报的警报规则。

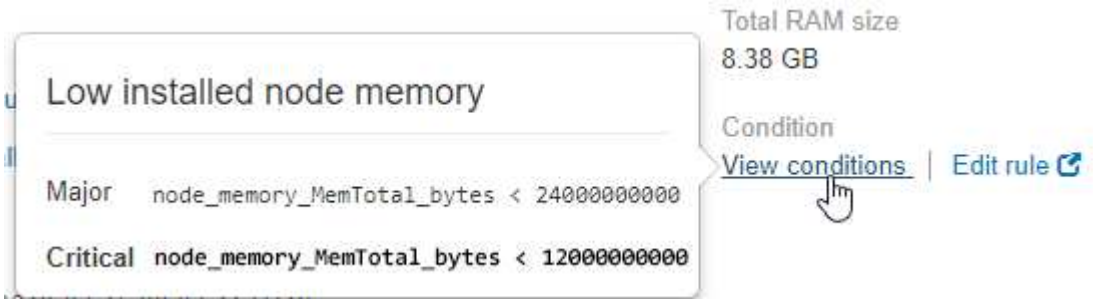
   要使警报规则静默，您必须具有管理警报或 root 访问权限。

   在决定静默警报规则时，请务必小心。如果某个警报规则已静音，则在阻止完成关键操作之前，您可能无法检测到潜在问题。

5. 要查看警报规则的当前条件，请执行以下操作：

   a. 在警报详细信息中，单击 * 查看条件 * 。

      此时将显示一个弹出窗口，其中列出了每个已定义严重性的 Prometheus 表达式。



   a. 要关闭此弹出窗口，请单击此弹出窗口以外的任意位置。

6. 或者，也可以单击 * 编辑规则 * 来编辑导致触发此警报的警报规则：

   要编辑警报规则，您必须具有管理警报或 root 访问权限。

   决定编辑警报规则时请务必小心。如果更改了触发值，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

7. 要关闭警报详细信息，请单击 * 关闭 * 。

查看旧警报

当系统属性达到警报阈值时，将触发警报（传统系统）。您可以从当前警报页面查看当前活动的警报。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。



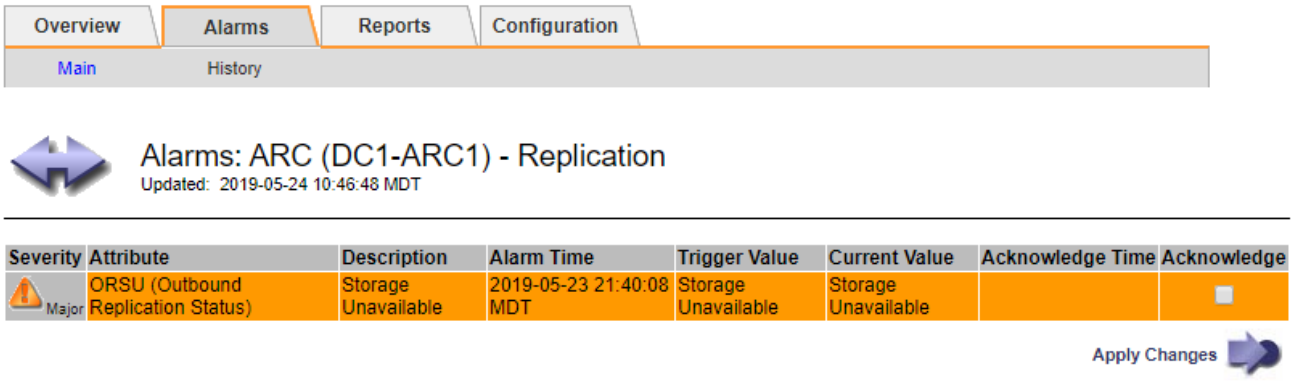
警报图标指示每个警报的严重性，如下所示：

图标。	颜色	警报严重性	含义
	黄色	通知	节点已连接到网格，但存在不影响正常操作的异常情况。
	浅橙色	次要	节点已连接到网格，但存在异常情况，可能会影响未来的运行。您应进行调查以防止上报。
	深橙色	major	节点已连接到网格，但存在当前影响操作的异常情况。这需要立即引起注意，以防止升级。
	红色	严重	节点已连接到网格，但存在已停止正常操作的异常情况。您应立即解决此问题描述 。

2. 要了解触发警报的属性，请右键单击表中的属性名称。
3. 要查看有关警报的其他详细信息，请单击表中的服务名称。

   此时将显示选定服务的警报选项卡（ * 支持 * > * 工具 * > * 网格拓扑 * > * 网格节点 _* > * 服务 _* > * 警报 *

）。



4. 如果要清除当前警报计数，您可以选择执行以下操作：
   - 确认警报。已确认的警报将不再包含在原有警报计数中，除非它在下一严重性级别触发，或者已解决并再次发生。
   - 为整个系统禁用特定的默认警报或全局自定义警报，以防止再次触发该警报。

相关信息

警报参考（旧系统）

确认当前警报（旧系统）

禁用警报（旧系统）

监控存储容量

监控可用总空间，以确保 StorageGRID 系统不会用尽对象或对象元数据的存储空间。

StorageGRID 会分别存储对象数据和对象元数据，并为包含对象元数据的分布式 Cassandra 数据库预留特定空间量。监控对象和对象元数据的已用空间总量，以及每个对象的已用空间量趋势。这样，您可以提前计划添加节点，并避免任何服务中断。

您可以 查看存储容量信息 适用于整个网格，每个站点以及 StorageGRID 系统中的每个存储节点。

监控整个网格的存储容量

您必须监控网格的整体存储容量，以确保为对象数据和对象元数据保留足够的可用空间。了解存储容量如何随时间变化有助于您计划在占用网格的可用存储容量之前添加存储节点或存储卷。

您需要的内容

您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

通过网格管理器中的信息板，您可以快速评估整个网格和每个数据中心的可用存储容量。节点页面提供了对象数据和对象元数据的更详细值。

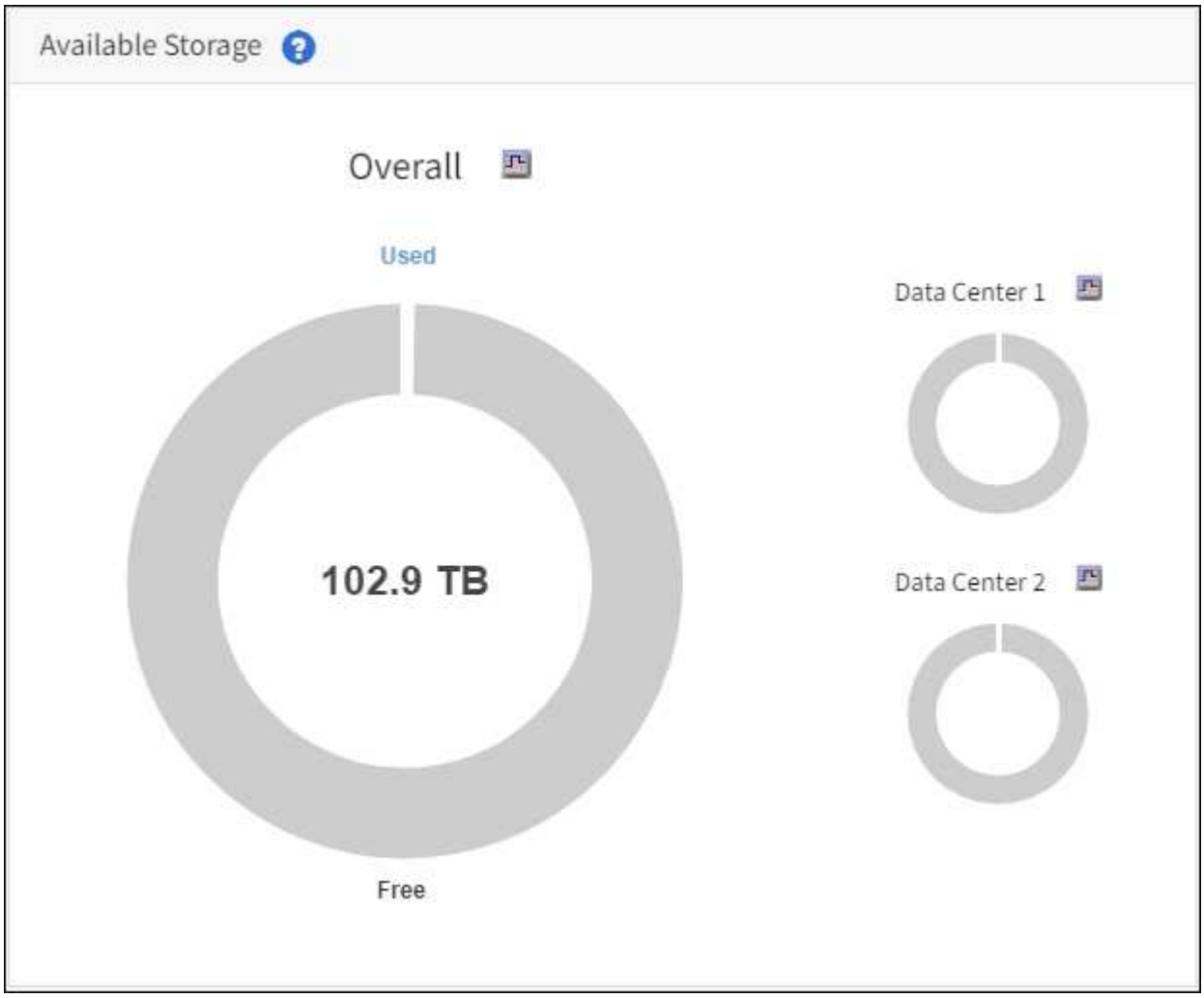
步骤

1. 评估可用于整个网格和每个数据中心的存储量。

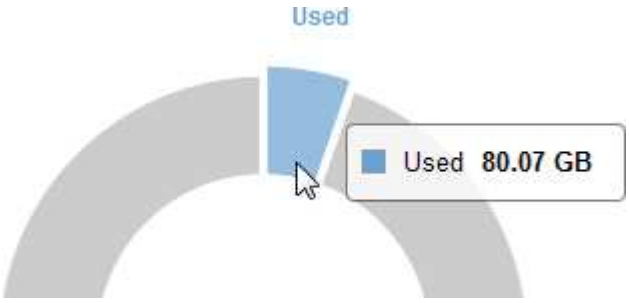
a. 选择 * 信息板 * 。

b. 在可用存储面板中，记下可用存储容量和已用存储容量的总体摘要。

此摘要不包括归档介质。



a. 将光标置于图表的 " 可用容量 " 或 " 已用容量 " 部分上方，可准确查看可用空间量或已用空间量。

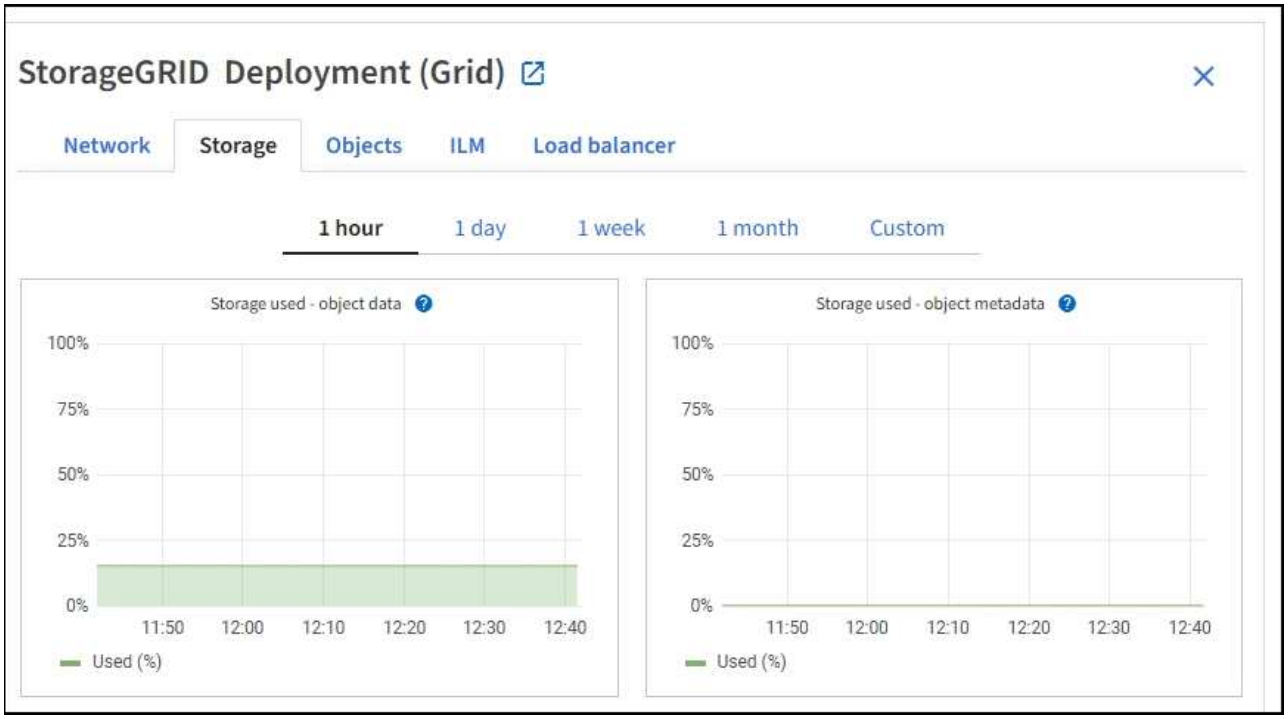


b. 对于多站点网格，请查看每个数据中心的图表。

c. 单击图表图标 用于查看整体图表或单个数据中心的图形，以显示一段时间内的容量使用情况。

显示已用存储容量百分比（ % ）与的图形此时将显示时间。

2. 确定已使用的存储容量以及仍可用于对象数据和对象元数据的存储容量。
   a. 选择 * 节点 * 。
   b. 选择 * ； grid_* > * 存储 * 。



   c. 将光标悬停在 * 已用存储 - 对象数据 * 和 * 已用存储 - 对象元数据 * 图表上，可查看整个网格可使用的对象存储和对象元数据存储容量以及已使用的容量。

> 站点或网格的总值不包括至少在五分钟内未报告指标的节点，例如脱机节点。

3. 计划执行扩展，以便在占用网格的可用存储容量之前添加存储节点或存储卷。

   在规划扩展时间时，请考虑购买和安装额外存储需要多长时间。

> 如果您的 ILM 策略使用纠删编码，则您可能希望在现有存储节点已满大约 70% 时进行扩展，以减少必须添加的节点数量。

   有关规划存储扩展的详细信息，请参见 扩展 StorageGRID 的说明。

监控每个存储节点的存储容量

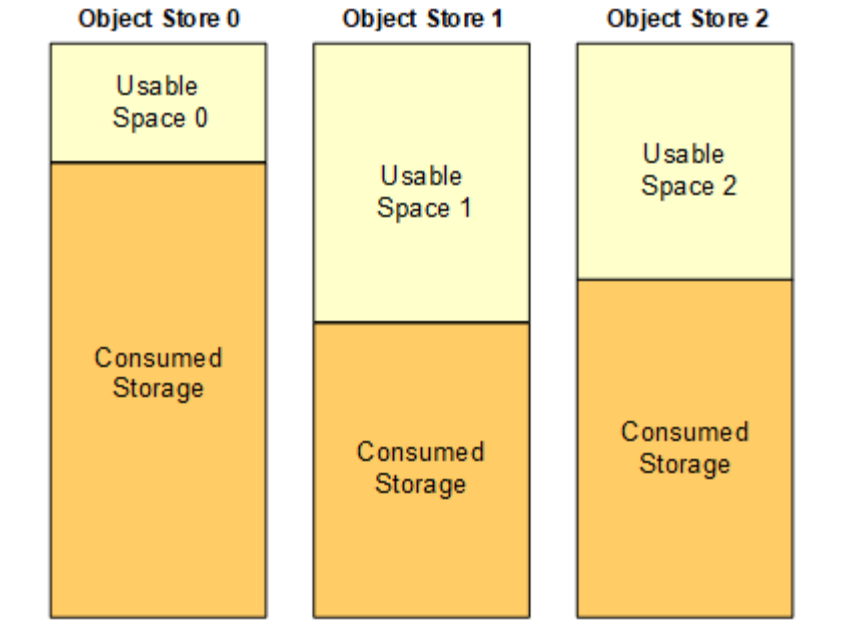
监控每个存储节点的总可用空间，以确保该节点具有足够的空间来容纳新对象数据。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

可用空间是指可用于存储对象的存储空间量。存储节点的总可用空间是通过将节点中所有对象存储上的可用空间相加来计算得出的。



步骤

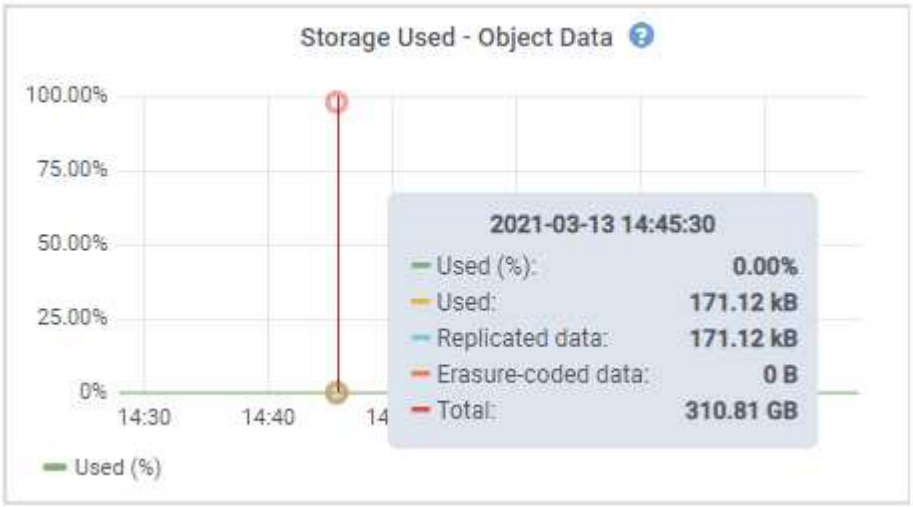
1. 选择 * 节点 * > * 存储节点 _* > * 存储 * 。

   此时将显示节点的图形和表。

2. 将光标悬停在已用存储 - 对象数据图上。

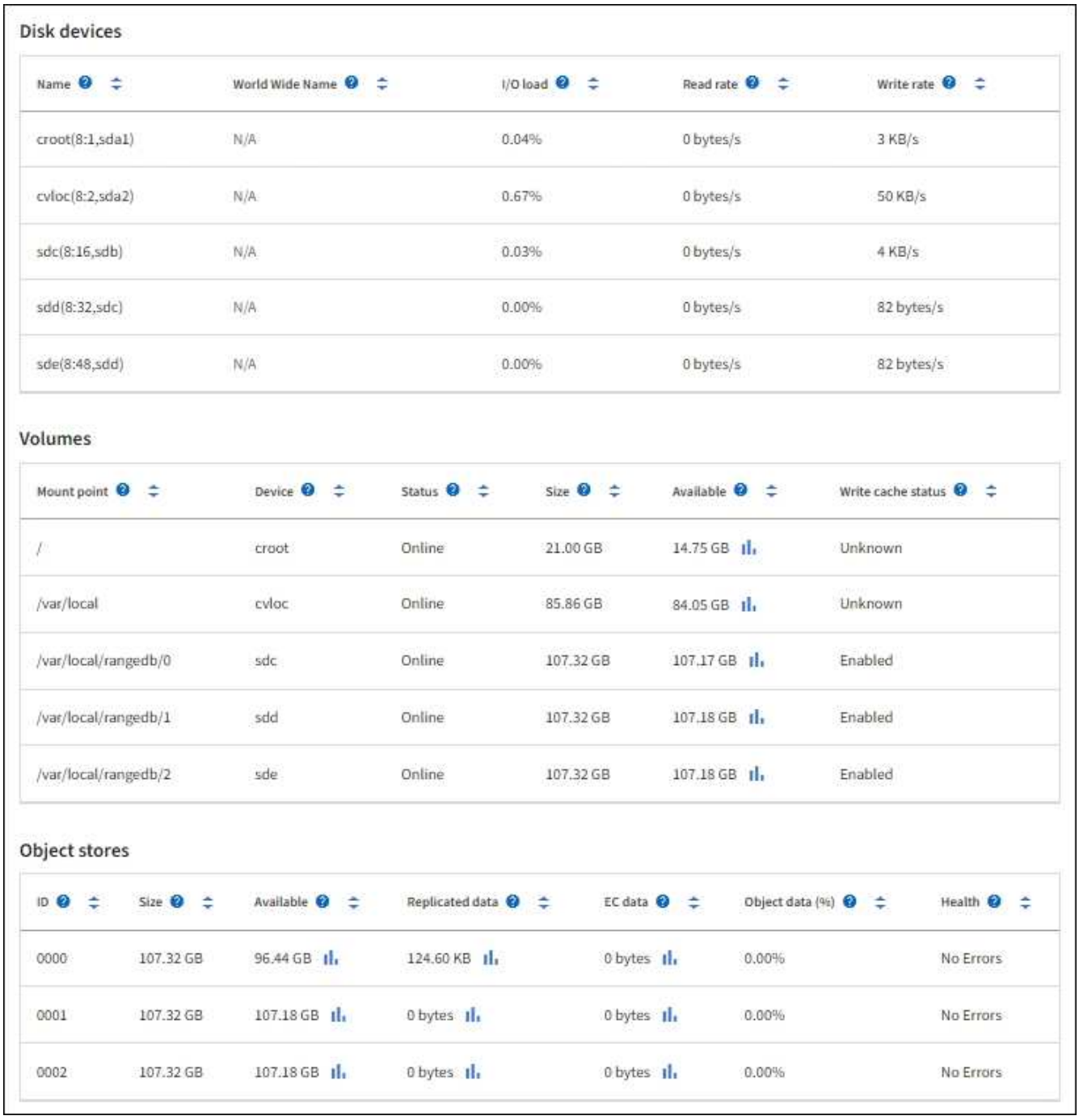
   此时将显示以下值：

   - * 已用（ % ） * ： 已用于对象数据的总可用空间的百分比。
   - * 已用 * ： 已用于对象数据的总可用空间量。
   - * 复制数据 * ： 此节点，站点或网格上复制的对象数据量的估计值。
   - * 擦除编码数据 * ： 此节点，站点或网格上经过擦除编码的对象数据量的估计值。
   - * 总计 * ： 此节点，站点或网格上的可用空间总量。使用的值是 `storagegRid_storage_utilization _data_bytes` 指标。



3. 查看图形下方的卷和对象存储表中的可用值。

   要查看这些值的图形，请单击图表图标 在可用列中。



Disk devices

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

Volumes

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

Object stores

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

4. 监控值随时间变化，以估计可用存储空间的消耗速率。
5. 要保持系统正常运行，请在使用可用空间之前添加存储节点，添加存储卷或归档对象数据。

   在规划扩展时间时，请考虑购买和安装额外存储需要多长时间。

   如果您的 ILM 策略使用纠删编码，则您可能希望在现有存储节点已满大约 70% 时进行扩展，以减少必须添加的节点数量。

有关规划存储扩展的详细信息，请参见 扩展 StorageGRID 的说明。

。 * 对象数据存储空间不足 * 如果在存储节点上存储对象数据的空间不足，则会触发警报。

监控每个存储节点的对象元数据容量

监控每个存储节点的元数据使用情况，以确保为基本数据库操作保留足够的可用空间。在对象元数据超过允许的元数据空间的 100% 之前，您必须在每个站点添加新的存储节点。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

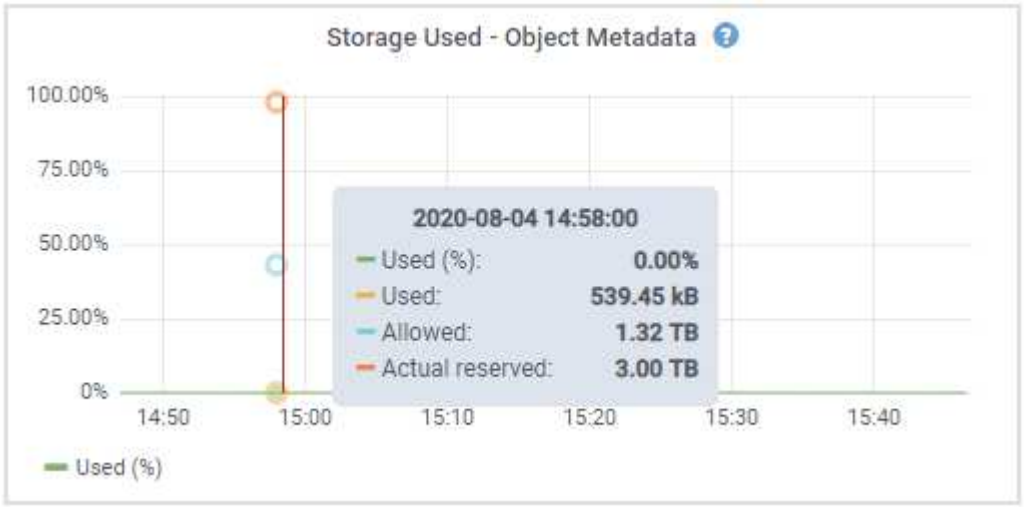
StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并防止对象元数据丢失。这三个副本会使用每个存储节点的存储卷 0 上为元数据预留的空间均匀分布在每个站点的所有存储节点上。

在某些情况下，网格的对象元数据容量消耗速度可能比其对象存储容量更快。例如，如果您通常要载入大量小对象，则可能需要添加存储节点以增加元数据容量，即使仍有足够的对象存储容量。

可能增加元数据使用量的一些因素包括用户元数据和标记的大小和数量，多部分上传中的部件总数以及 ILM 存储位置的更改频率。

步骤

1. 选择 * 节点 * > * 存储节点 _* > * 存储 * 。
2. 将光标悬停在已用存储 - 对象元数据图上可查看特定时间的值。



价值	Description	Prometheus 指标
已用（%）	此存储节点上已使用的允许元数据空间的百分比。	`storagegRid_storage_utilization metadata_bytes/ storagegRid_storage_utilization _metadata_allowed_bytes`

价值	Description	Prometheus 指标
已用	此存储节点上已使用的允许元数据空间的字节数。	`storagegRid_storage_utilization metadata_bytes`
允许	此存储节点上的对象元数据允许的空间。要了解如何为每个存储节点确定此值，请参见 有关管理 StorageGRID 的说明。	`storagegRid_storage_utilization metadata_allowed_bytes`
实际预留	为此存储节点上的元数据预留的实际空间。包括基本元数据操作所需的允许空间和空间。要了解如何为每个存储节点计算此值，请参见 有关管理 StorageGRID 的说明。	_Metric 将在未来版本中添加。 _

站点或网格的总值不包括至少在五分钟内未报告指标的节点，例如脱机节点。

3. 如果 * 已用（ % ） * 值为 70% 或更高，请通过向每个站点添加存储节点来扩展 StorageGRID 系统。

当 * 已用（ % ） * 值达到特定阈值时，将触发 * 元数据存储不足 * 警报。如果对象元数据使用的空间超过允许的 100% ，则可能会出现不希望出现的结果。

添加新节点时，系统会自动在站点内的所有存储节点之间重新平衡对象元数据。请参见 有关扩展 StorageGRID 系统的说明。

监控信息生命周期管理

信息生命周期管理（ ILM ）系统可为网格中存储的所有对象提供数据管理。您必须监控 ILM 操作，以了解网格是否可以处理当前负载，或者是否需要更多资源。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

StorageGRID 系统通过应用活动 ILM 策略来管理对象。ILM 策略和关联的 ILM 规则可确定创建的副本数，创建的副本类型，副本放置位置以及每个副本的保留时间长度。

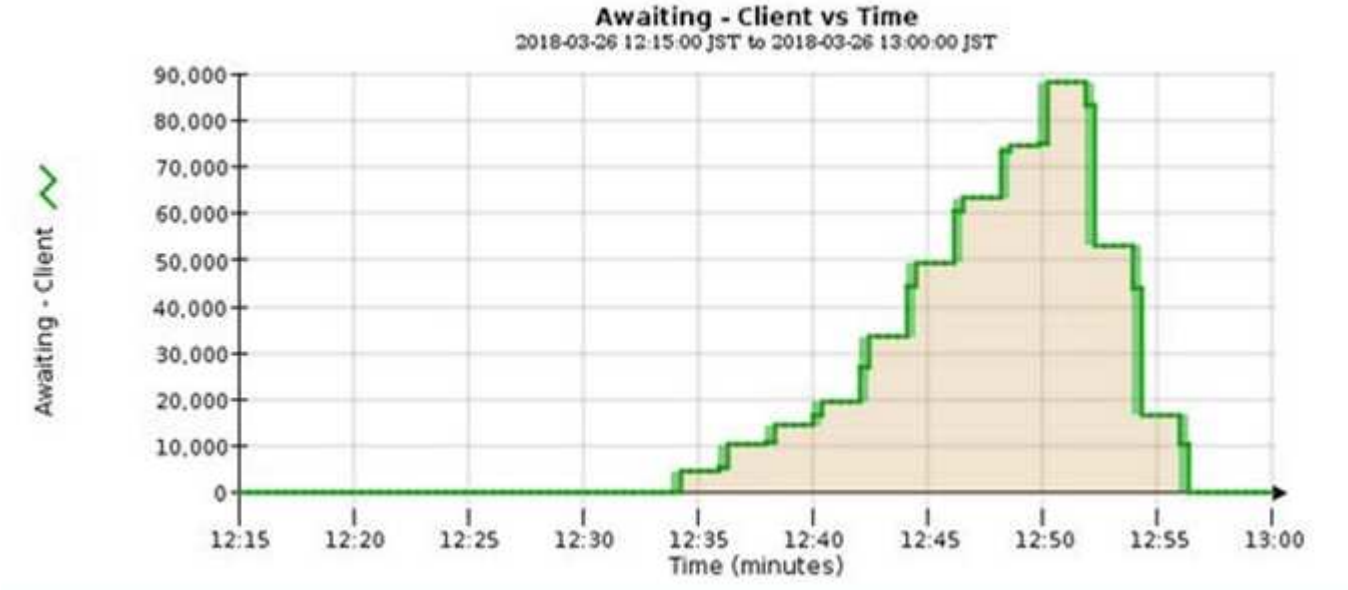
对象载入和其他与对象相关的活动可能会超过 StorageGRID 评估 ILM 的速率，从而导致系统对无法近乎实时地执行 ILM 放置指令的对象进行排队。您可以通过绘制 waiting - Client 属性来监控 StorageGRID 是否与客户端操作保持一致。

要对此属性进行绘制，请执行以下操作：

1. 登录到网格管理器。
2. 在信息板中，在信息生命周期管理（ ILM ）面板中找到 * 正在等待 - 客户端 * 条目。
3. 单击图表图标 。

此示例图表显示了以下情形：等待 ILM 评估的对象数量以不可持续的方式临时增加，然后最终减少。这种趋势

表明， ILM 暂时未近乎实时地完成。



等待 - 客户端图表中的临时峰值是预期的。但是，如果图表上显示的值持续增加且从不下降，则网格需要更多资源来高效运行：存储节点更多，或者如果 ILM 策略将对象放置在远程位置，则网络带宽更多。

您可以使用 * 节点 * 页面进一步调查 ILM 队列。

步骤

1. 选择 * 节点 * 。
2. 选择 * 网格名称 _* > * ILM * 。
3. 将光标悬停在 ILM 队列图上，可查看给定时间点以下属性的值：
   - * 已排队的对象（来自客户端操作） * ： 由于客户端操作（例如载入）而等待 ILM 评估的对象总数。
   - * 已排队的对象（从所有操作） * ： 等待 ILM 评估的对象总数。
   - * 扫描速率（对象 / 秒） * ： 为 ILM 扫描网格中的对象并使其排队的速率。
   - * 评估速率（对象 / 秒） * ： 根据网格中的 ILM 策略评估对象的当前速率。
4. 在 "ILM Queue" 部分中，查看以下属性。

   "ILM Queue" 部分仅适用于网格。此信息不会显示在站点或存储节点的 "ILM " 选项卡上。

   - * 扫描期间 - 估计 * ： 完成对所有对象的完整 ILM 扫描的估计时间。

     完全扫描并不能保证 ILM 已应用于所有对象。

   - * 已尝试修复 * ： 已尝试对复制数据执行的对象修复操作总数。每当存储节点尝试修复高风险对象时，此计数都会递增。如果网格繁忙，高风险 ILM 修复会优先处理。

     如果修复后复制失败，则同一对象修复可能会再次增加。

在监控存储节点卷恢复的进度时，这些属性可能会很有用。如果尝试的修复次数停止增加，并且已完成完整

扫描，则修复可能已完成。

监控网络连接和性能

网格节点必须能够彼此通信，才能使网格正常运行。节点和站点之间的网络完整性以及站点之间的网络带宽对于高效运行至关重要。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

如果您的信息生命周期管理（ ILM ）策略使用提供站点丢失保护的方案在站点之间复制复制复制的对象或存储经过纠删编码的对象，则网络连接和带宽尤其重要。如果站点之间的网络不可用，网络延迟过高或网络带宽不足，则某些 ILM 规则可能无法将对象放置在预期位置。这可能导致载入失败（为 ILM 规则选择了严格载入选项时），或者仅仅导致载入性能和 ILM 积压。

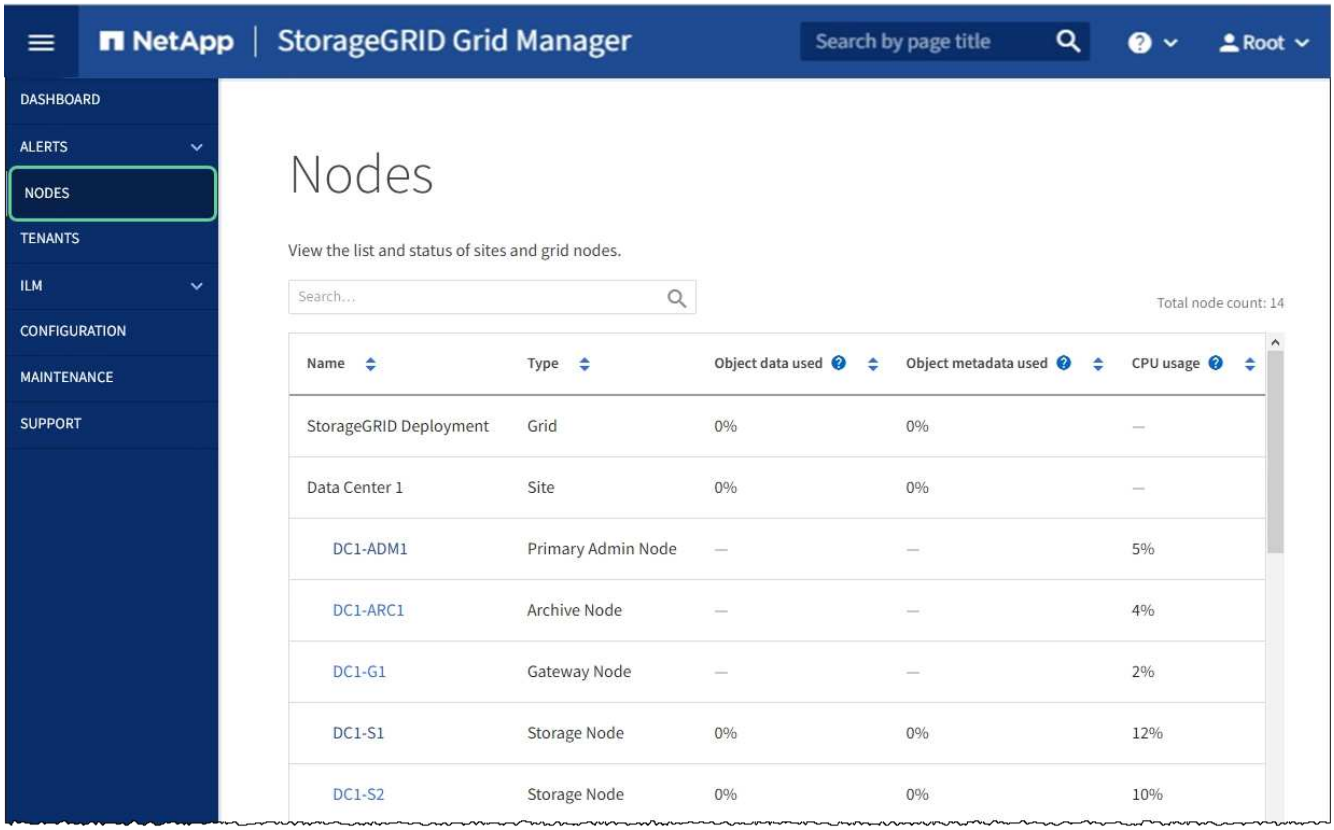
您可以使用网格管理器监控连接和网络性能，以便及时解决任何问题。

此外，还应考虑创建网络流量分类策略，以便监控和限制与特定租户，分段，子网或负载平衡器端点相关的流量。请参见 有关管理 StorageGRID 的说明。

步骤

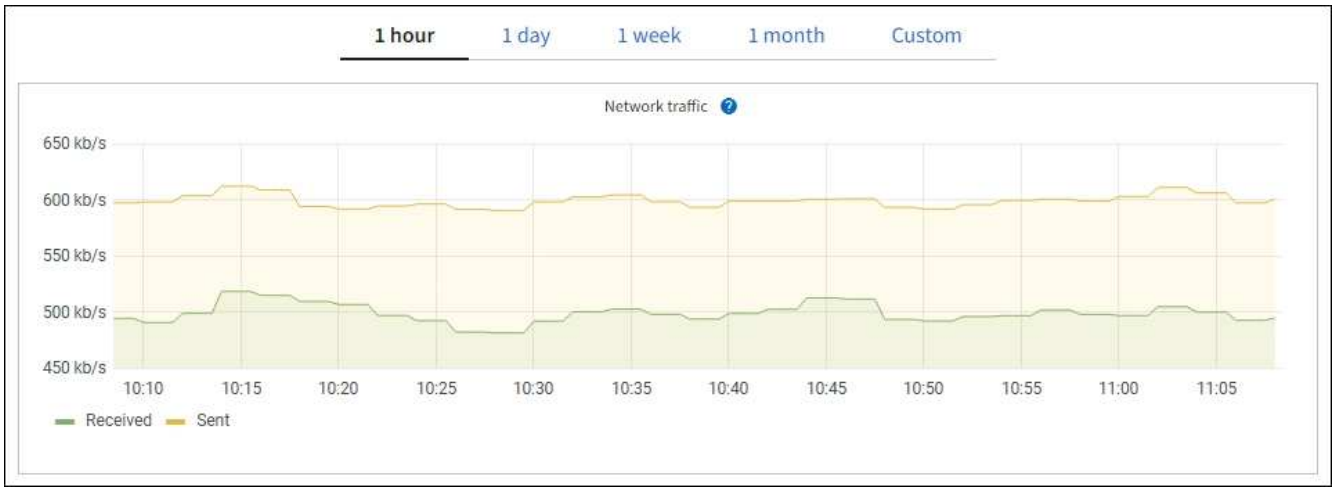
1. 选择 * 节点 * 。

   此时将显示节点页面。网格中的每个节点均以表格式列出。

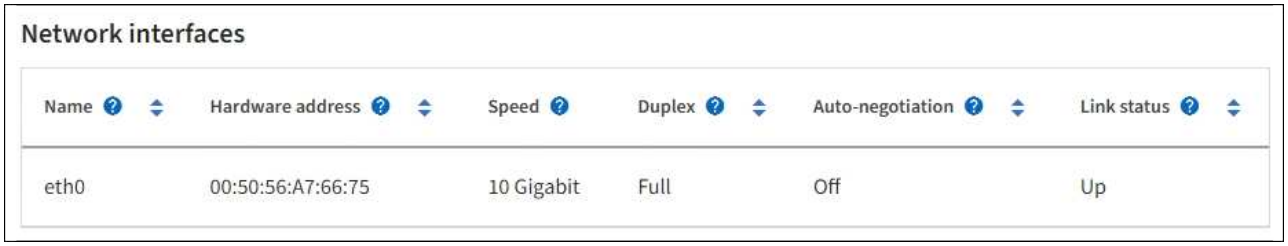


2. 选择网格名称，特定数据中心站点或网格节点，然后选择 * 网络 * 选项卡。

   网络流量图提供了整个网格，数据中心站点或节点的整体网络流量摘要。



   a. 如果选择了网格节点，请向下滚动以查看页面的 * 网络接口 * 部分。

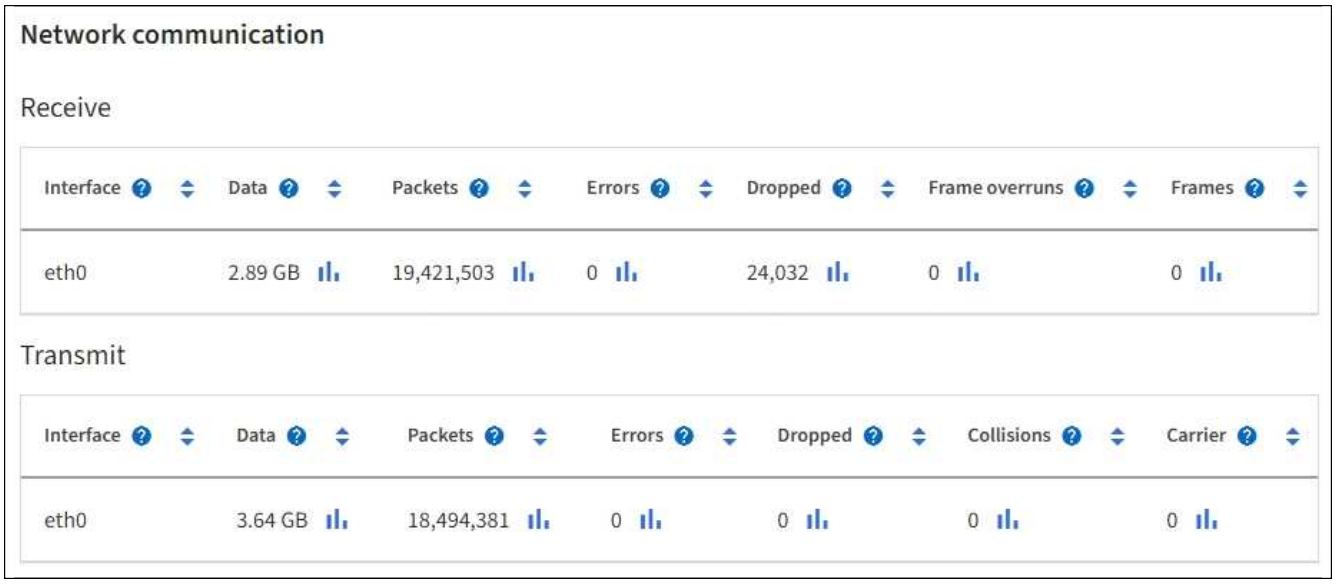


Network interfaces

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

   b. 对于网格节点，向下滚动以查看页面的 * 网络通信 * 部分。

      接收和传输表显示了通过每个网络接收和发送的字节数和数据包数，以及其他接收和传输指标。



Network communication

Receive

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

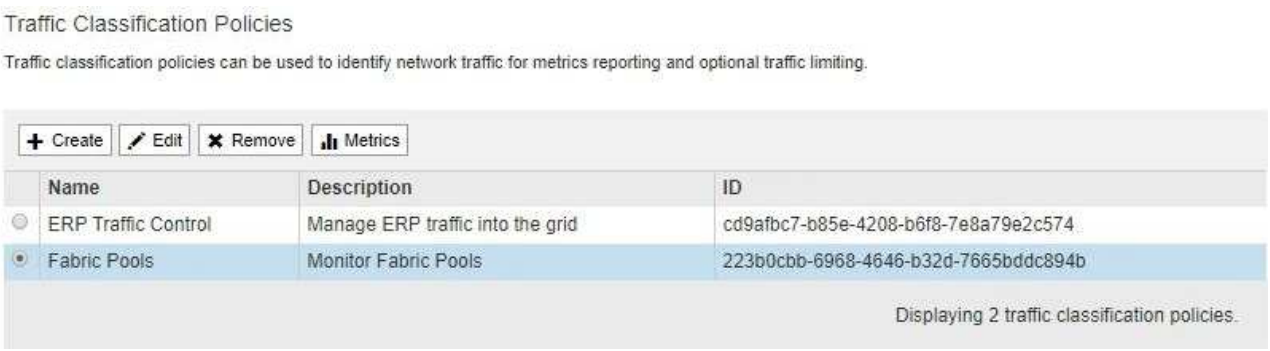
Transmit

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

3. 使用与流量分类策略关联的指标监控网络流量。

   a. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



b. 要查看显示与策略关联的网络指标的图形，请选择策略左侧的单选按钮，然后单击 * 指标 * 。

c. 查看图形以了解与策略关联的网络流量。

   如果流量分类策略旨在限制网络流量，请分析流量限制的频率，并确定该策略是否仍能满足您的需求。根据需要不时调整每个流量分类策略。

要创建，编辑或删除流量分类策略，请参见 有关管理 StorageGRID 的说明。

相关信息

查看网络选项卡

监控节点连接状态

监控节点级资源

您应监控各个网格节点以检查其资源利用率级别。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

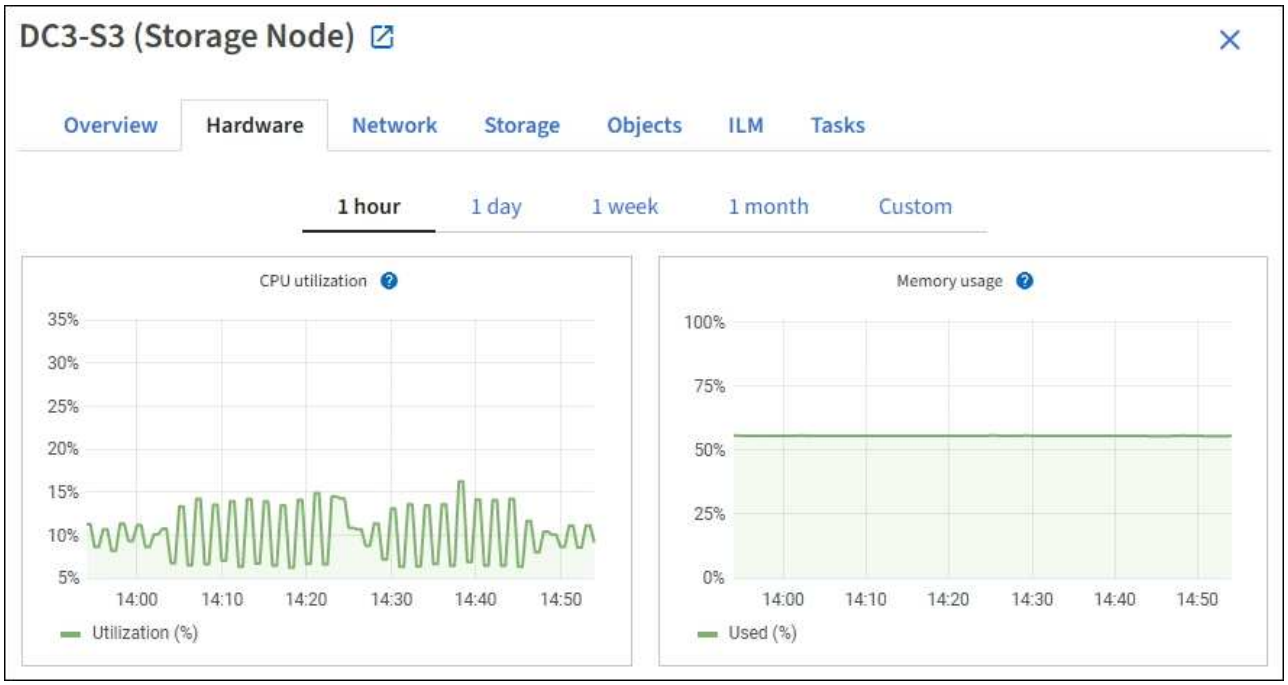
如果节点始终过载，则可能需要更多节点才能高效运行。

步骤

1. 要查看有关网格节点硬件利用率的信息，请执行以下操作：

   a. 从 * 节点 * 页面中，选择节点。

   b. 选择 * 硬件 * 选项卡以显示 CPU 利用率和内存使用情况的图形。



c. 要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。

d. 如果节点托管在存储设备或服务设备上，请向下滚动以查看组件表。所有组件的状态均应为 "`标称值。` " 调查具有任何其他状态的组件。

相关信息

查看有关设备存储节点的信息

查看有关设备管理节点和网关节点的信息

监控租户活动

所有客户端活动都与租户帐户相关联。您可以使用网格管理器监控租户的存储使用情况或网络流量，也可以使用审核日志或 Grafana 信息板收集有关租户如何使用 StorageGRID 的更多详细信息。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限或管理员权限。

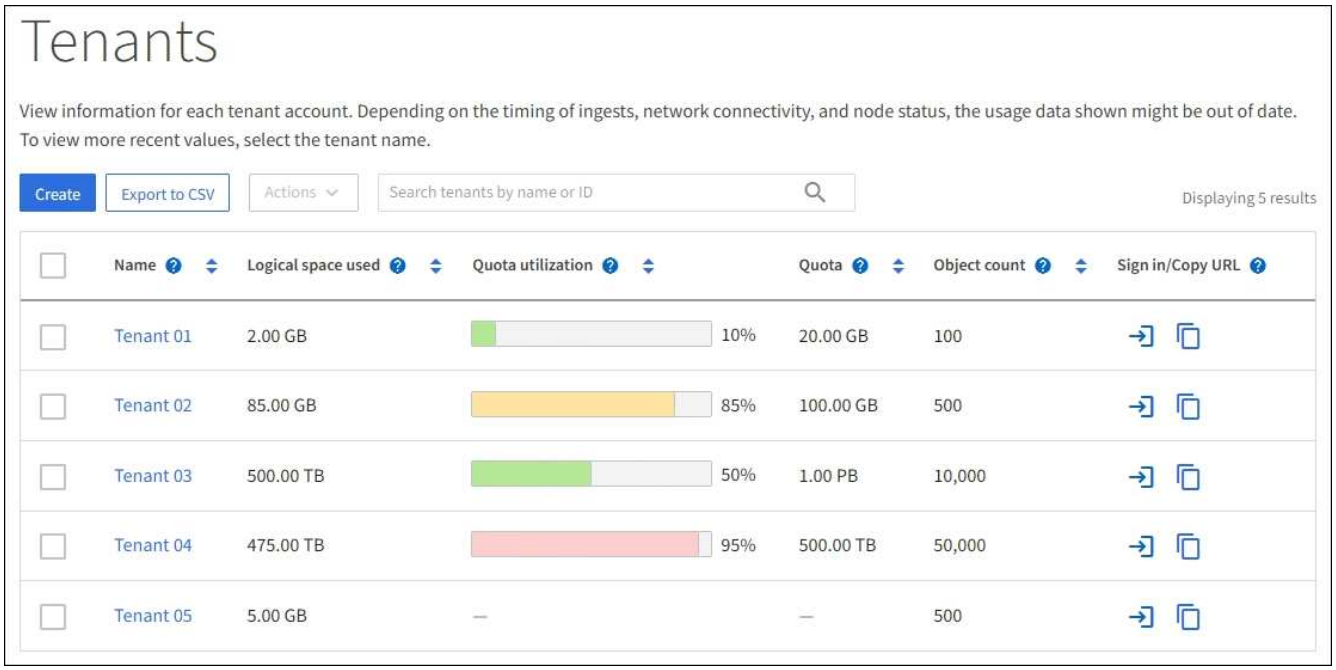
关于此任务

已用空间值是估计值。这些估计值受载入时间，网络连接和节点状态的影响。

步骤

1. 选择 * 租户 * 可查看所有租户使用的存储量。

   系统会为每个租户列出已用逻辑空间，配额利用率，配额和对象计数。如果未为租户设置配额，则配额利用率和配额字段包含一个短划线（ &#8212 ； ）。



您可以通过选择登录链接登录到租户帐户 在表的 * 登录 / 复制 URL* 列中。

您可以通过选择复制 URL 链接来复制租户登录页面的 URL 在表的 * 登录 / 复制 URL* 列中。

2. 或者，选择 * 导出到 CSV* 以查看和导出包含所有租户的使用量值的 .csv 文件。

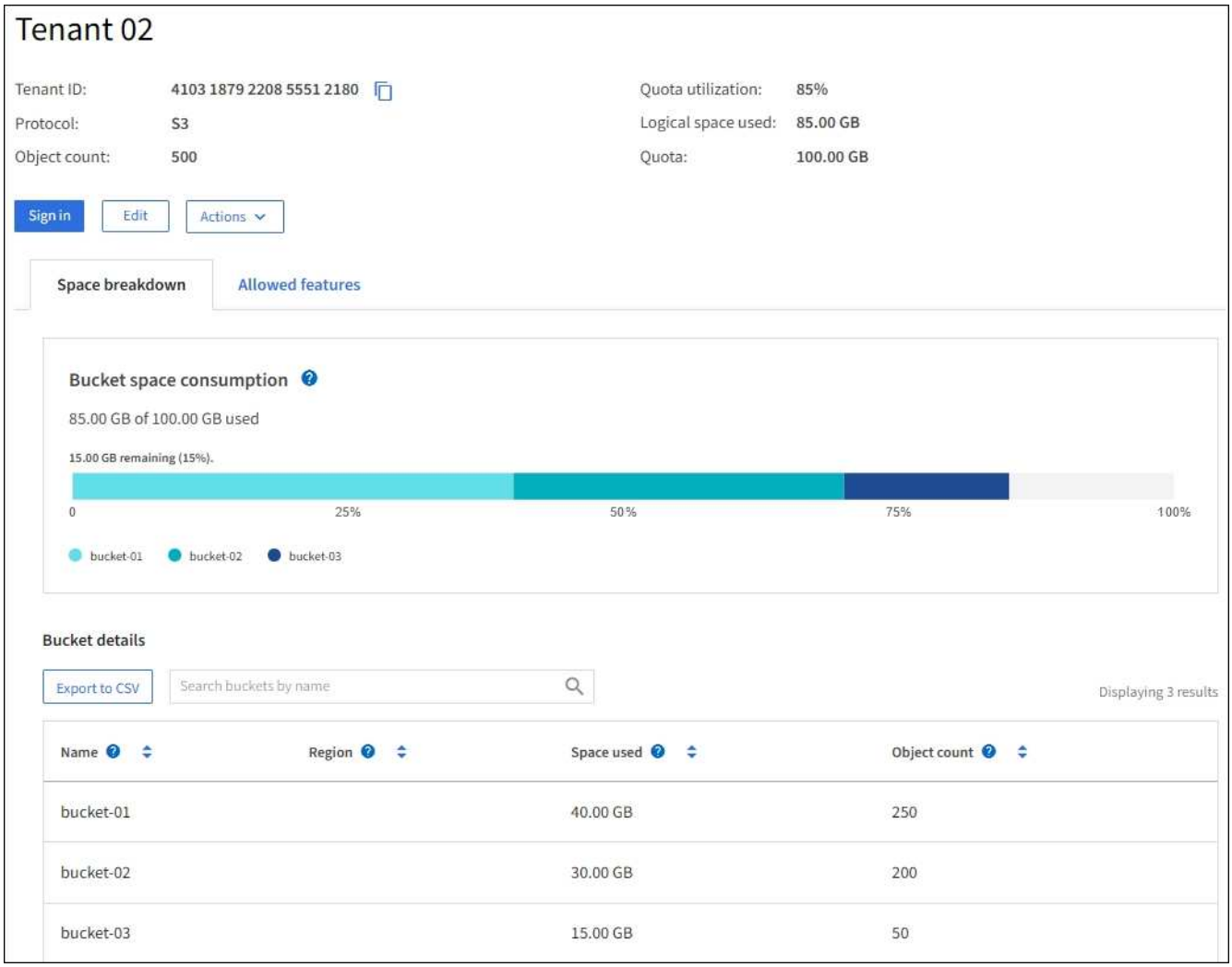
   系统会提示您打开或保存 ` .csv` 文件。

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

图 **1. csv** 文件的内容如下所示：

您可以在电子表格应用程序中打开 .csv 文件，也可以在自动化环境中使用该文件。

3. 要查看特定租户的详细信息，包括使用情况图表，请从租户页面中选择租户帐户名称。



◦ * 租户概述 *

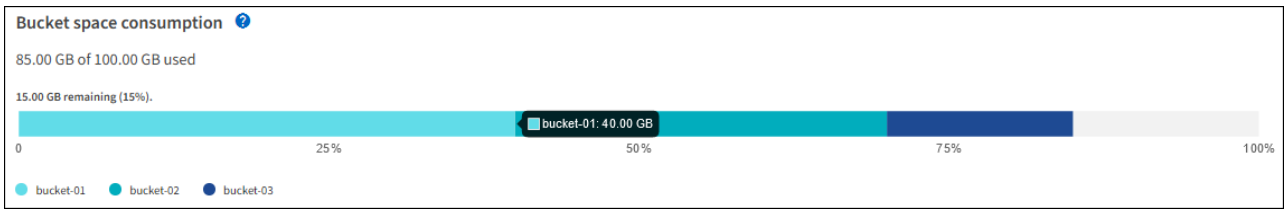
租户的概述区域包含对象计数，配额利用率，已用逻辑空间和配额设置的值。

◦ * 空间细分 - 空间消耗 *

" 空间细分 " 选项卡包含分段（ S3 ）或容器（ Swift ）总空间消耗值以及每个分段或容器的已用空间和对象计数。

如果为此租户设置了配额，则已用配额量和剩余配额量将以文本形式显示（例如， `85.00 GB of 100 GB used` ）。如果未设置配额，则租户的配额为无限制，并且文本仅包含已用空间量（例如， `85.00 GB used` ）。条形图显示每个分段或容器中的配额百分比。如果租户超过存储配额 1% 以上且至少超过 1 GB ，则此图表将显示总配额和超额量。

您可以将光标置于条形图上方，以查看每个分段或容器使用的存储。您可以将光标置于可用空间段上方以查看剩余存储配额量。



配额利用率基于内部估计值，在某些情况下可能会超出此值。例如，当租户开始上传对象时， StorageGRID 会检查配额，如果租户超过配额，则会拒绝新的载入。但是，在确定是否超过配额时， StorageGRID 不会考虑当前上传的大小。如果删除对象，则可能会暂时阻止租户上传新对象，直到重新计算配额利用率为止。配额利用率计算可能需要 10 分钟或更长时间。

租户的配额利用率表示租户已上传到 StorageGRID 的对象数据总量（逻辑大小）。配额利用率并不表示用于存储这些对象及其元数据副本的空间（物理大小）。

您可以启用 * 租户配额使用量高 * 警报，以确定租户是否正在使用其配额。如果启用，则在租户已使用其配额的 90% 时触发此警报。有关详细信息，请参见警报参考。

- * 空间细分 - 分段或容器详细信息 *
  - 分段详细信息 * （ S3 ）或 * 容器详细信息 * （ Swift ）表列出了租户的分段或容器。已用空间是指存储分段或容器中的对象数据总量。此值不表示 ILM 副本和对象元数据所需的存储空间。

4. 或者，也可以选择 * 导出到 CSV* 以查看和导出包含每个分段或容器的使用量值的 .csv 文件。

   单个 S3 租户的 .csv 文件的内容如下所示：

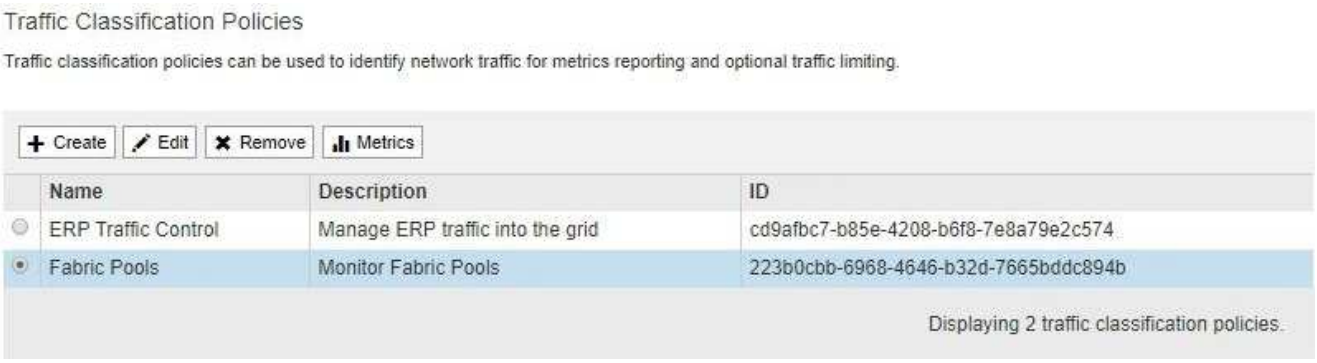
Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   您可以在电子表格应用程序中打开 .csv 文件，也可以在自动化环境中使用该文件。

5. 如果某个租户已设置流量分类策略，请查看该租户的网络流量。

   a. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

      此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



   a. 查看策略列表以确定适用于特定租户的策略。

   b. 要查看与策略关联的指标，请选择策略左侧的单选按钮，然后单击 * 指标 * 。

   c. 分析图形以确定策略限制流量的频率以及是否需要调整策略。

      要创建，编辑或删除流量分类策略，请参见有关管理 StorageGRID 的说明。

6. 或者，也可以使用审核日志更精细地监控租户的活动。

   例如，您可以监控以下类型的信息：

   - 特定客户端操作，例如 PUT ， GET 或 DELETE
   - 对象大小
   - 应用于对象的 ILM 规则
   - 客户端请求的源 IP

     审核日志会写入文本文件，您可以使用所选的日志分析工具进行分析。这样，您可以更好地了解客户活动，或者实施复杂的成本分摊和计费模式。

   有关详细信息，请参见了解审核消息的说明。

7. 或者，也可以使用 Prometheus 指标报告租户活动：
   - 在网格管理器中，选择 * 支持 * > * 工具 * > * 指标 * 。您可以使用现有信息板（如 S3 概述）查看客户端活动。

     > 指标页面上提供的工具主要供技术支持使用。这些工具中的某些功能和菜单项会有意失效。

   - 从网格管理器的顶部，选择帮助图标并选择 * API Documentation" 。您可以使用网格管理 API 的 " 指标 " 部分中的指标为租户活动创建自定义警报规则和信息板。

相关信息

警报参考

查看审核日志

管理 StorageGRID

查看支持指标

监控归档容量

您不能通过 StorageGRID 系统直接监控外部归档存储系统的容量。但是，您可以监控归档节点是否仍可将对象数据发送到归档目标，这可能表示需要扩展归档介质。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

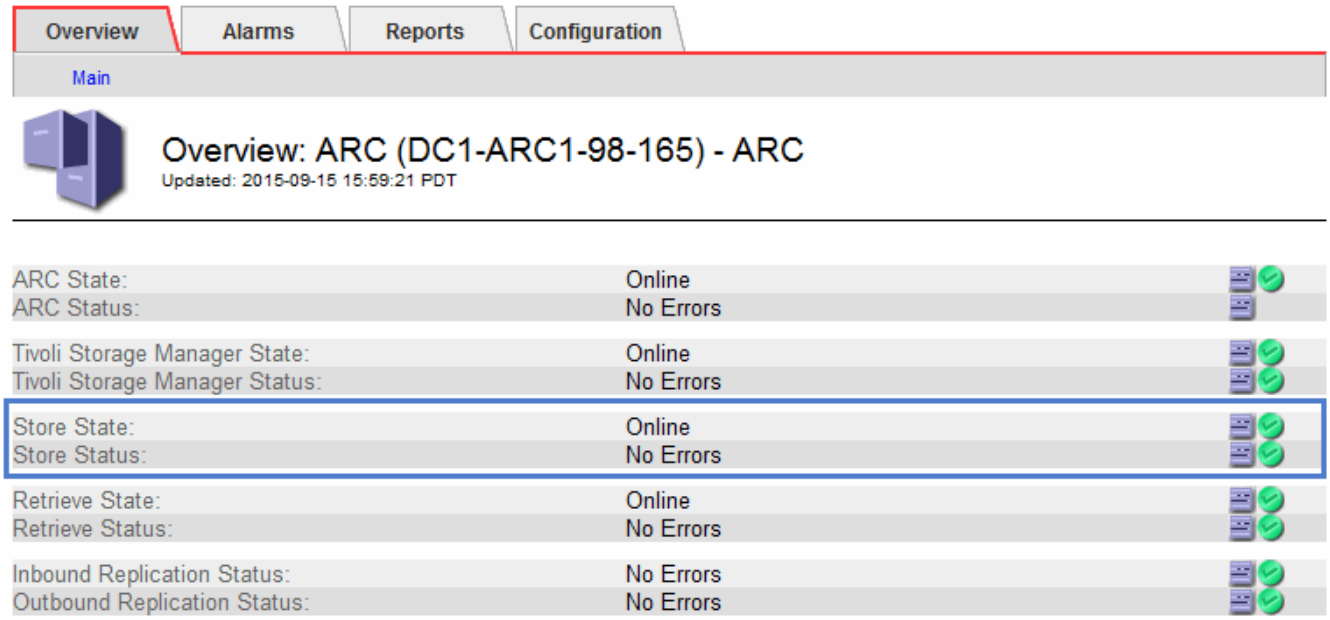
关于此任务

您可以监控存储组件以检查归档节点是否仍可将对象数据发送到目标归档存储系统。存储故障（ ARVF ）警报还可能指示目标归档存储系统已达到容量，无法再接受对象数据。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

2. 选择 * ： 归档节点 _* > * 。 ARR>> 概述 >> 主系统 * 。
3. 检查存储状态和存储状态属性以确认存储组件处于联机状态且无错误。



脱机存储组件或存在错误的组件可能指示目标归档存储系统无法再接受对象数据，因为它已达到容量。

监控负载平衡操作

如果您使用负载平衡器管理客户端与 StorageGRID 的连接，则应在最初配置系统之后以及在进行任何配置更改或执行扩展之后监控负载平衡操作。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

您可以使用管理节点或网关节点上的负载平衡器服务，外部第三方负载平衡器或网关节点上的 CLB 服务在多个存储节点上分发客户端请求。

CLB 服务已弃用。

配置负载平衡后，您应确认对象载入和检索操作在存储节点之间均匀分布。均匀分布的请求可确保 StorageGRID 始终响应负载下的客户端请求，并有助于保持客户端性能。

如果您在主动备份模式下为网关节点或管理节点配置了一个高可用性（ HA ）组，则该组中只有一个节点会主动分发客户端请求。

请参见有关管理 StorageGRID 的说明中有关配置客户端连接的章节。

步骤

1. 如果 S3 或 Swift 客户端使用负载平衡器服务进行连接，请检查管理节点或网关节点是否按预期主动分布流量：

a. 选择 * 节点 * 。
b. 选择网关节点或管理节点。
c. 在 * 概述 * 选项卡上，检查节点接口是否位于 HA 组中，以及节点接口是否具有主接口角色。

   具有主节点角色的节点以及不在 HA 组中的节点应主动向客户端分发请求。

d. 对于应主动分发客户端请求的每个节点，选择 * 负载平衡器 * 选项卡。
e. 查看上一周的负载平衡器请求流量图表，以确保节点一直在主动分发请求。

   主动备份 HA 组中的节点可能会不时承担备份角色。在此期间，节点不会分发客户端请求。

f. 查看上周的负载平衡器传入请求速率图表，查看节点的对象吞吐量。
g. 对 StorageGRID 系统中的每个管理节点或网关节点重复上述步骤。
h. 或者，也可以使用流量分类策略来查看负载平衡器服务所提供流量的更详细细分。

2. 如果 S3 或 Swift 客户端使用 CLB 服务进行连接（已弃用），请执行以下检查：
   a. 选择 * 节点 * 。
   b. 选择一个网关节点。
   c. 在 * 概述 * 选项卡上，检查节点接口是否位于 HA 组中，以及节点接口是否具有主接口角色。

      具有主节点角色的节点以及不在 HA 组中的节点应主动向客户端分发请求。

   d. 对于应主动分发客户端请求的每个网关节点，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   e. 选择 * 网关节点 _* > * CLB* > * http * > * 概述 * > * 主 * 。
   f. 查看 * 传入会话数 - 已建立 * 以验证网关节点是否一直在主动处理请求。
3. 验证这些请求是否均匀分布到存储节点。
   a. 选择 * 存储节点 _* > * LDR* > * HTTP * 。
   b. 查看 * 当前已建立的传入会话 * 的数量。
   c. 对网格中的每个存储节点重复上述步骤。

      所有存储节点的会话数应大致相等。

相关信息

管理 StorageGRID

查看负载平衡器选项卡

如有必要，应用修补程序或升级软件

如果提供了修补程序或新版本的 StorageGRID 软件，您应评估此更新是否适合您的系统，并在需要时进行安装。

关于此任务

StorageGRID 修补程序包含在功能或修补程序版本之外进行的软件更改。未来版本也会进行同样的更改。

步骤

1. 转到 StorageGRID 的 "NetApp 下载 " 页面。

   "NetApp 下载： StorageGRID"

2. 选择 * 类型 / 选择版本 * 字段的向下箭头可查看可供下载的更新列表：
   - * StorageGRID 软件版本 *： 11.*x.y*
   - * StorageGRID 修补程序 *： 11.*x.y.z*
3. 查看更新中包含的更改：
   a. 从下拉菜单中选择版本，然后单击 * 执行 * 。
   b. 使用您的 NetApp 帐户的用户名和密码登录。
   c. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。

      此时将显示选定版本的下载页面。
4. 了解软件版本或修补程序中包含的更改。
   - 有关新的软件版本，请参见 StorageGRID 升级说明中的 "`新增功能` " 主题。
   - 对于热修补程序，请下载 README 文件以获取热修补程序中所做更改的摘要。
5. 如果您确定需要软件更新，请在继续操作之前找到相关说明。
   - 对于新的软件版本，请仔细按照说明升级 StorageGRID 。
   - 有关热修补程序，请在恢复和维护说明中找到热修补程序操作步骤

     ▪ 相关信息 *

升级软件

恢复和维护

管理警报和警报

管理警报和警报：概述

StorageGRID 警报系统旨在通知您需要关注的操作问题。旧警报系统已弃用。

警报系统

警报系统是用于监控 StorageGRID 系统中可能发生的任何问题的主要工具。警报系统提供了一个易于使用的界面，用于检测，评估和解决问题。

当警报规则条件评估为 true 时，系统将在特定严重性级别触发警报。触发警报后，将执行以下操作：

- 网格管理器的信息板上会显示一个警报严重性图标，当前警报计数将递增。
- 警报显示在 * 节点 * 摘要页面和 * 节点 * > * 节点 _* > * 概述 * 选项卡上。
- 假定您已配置 SMTP 服务器并为收件人提供了电子邮件地址，则会发送电子邮件通知。

- 假定您已配置 StorageGRID SNMP 代理，则会发送简单网络管理协议（ SNMP ）通知。

传统警报系统

与警报一样，当属性达到定义的阈值时，也会在特定严重性级别触发警报。但是，与警报不同的是，对于可以安全忽略的事件，系统会触发许多警报，这可能会导致电子邮件或 SNMP 通知过多。

> 警报系统已弃用，将在未来版本中删除。如果您仍在使用传统警报，则应尽快完全过渡到警报系统。

触发警报后，将执行以下操作：

- 警报将显示在 * 支持 * > * 警报（原有） * > * 当前警报 * 页面上。
- 假定您已配置 SMTP 服务器并配置了一个或多个邮件列表，则会发送电子邮件通知。
- 假设您已配置 StorageGRID SNMP 代理，则可能会发送 SNMP 通知。（并非针对所有警报或警报严重性发送 SNMP 通知。）

比较警报和警报

警报系统与传统警报系统之间存在许多相似之处，但警报系统具有显著优势，并且更易于使用。

请参见下表，了解如何执行类似操作。

	警报	警报（旧系统）
如何查看哪些警报处于活动状态？	• 选择信息板上的 * 当前警报 * 链接。 • 在 * 节点 * > * 概述 * 页面上选择警报。 • 选择 * 警报 * > * 当前 * 。 查看当前警报	选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。 管理警报（旧系统）
触发警报或警报的原因是什么？	如果警报规则中的 Prometheus 表达式在特定触发条件和持续时间下评估为 true ，则会触发警报。 查看警报规则	当 StorageGRID 属性达到阈值时，将触发警报。 管理警报（旧系统）
如果触发警报或警报，如何解决根本问题？	电子邮件通知中包含警报的建议操作，您可以从网格管理器的警报页面中获取这些操作。 StorageGRID 文档会根据需要提供追加信息 。 警报参考	您可以通过选择属性名称来了解警报，也可以在 StorageGRID 文档中搜索警报代码。 警报参考（旧系统）

	警报	警报（旧系统）
在哪里可以看到已解决的警报或警报列表？	选择 * 警报 * > * 已解决 * 。 查看已解决的警报	选择 * 支持 * > * 警报（原有） * > * 历史警报 * 。 管理警报（旧系统）
在何处管理设置？	选择 * 警报 * > * 规则 * 。 管理警报	选择 * 支持 * 。然后，使用菜单 * 警报（原有） * 部分中的选项。 管理警报（旧系统）
我需要哪些用户组权限？	• 可以登录到网格管理器的任何人都可以查看当前警报和已解决警报。 • 您必须具有管理警报权限才能管理静音，警报通知和警报规则。 管理 StorageGRID	• 可以登录到网格管理器的任何人都可以查看旧警报。 • 您必须具有确认警报权限才能确认警报。 • 要管理全局警报和电子邮件通知，您必须同时具有网格拓扑页面配置和其他网格配置权限。 管理 StorageGRID
如何管理电子邮件通知？	选择 * 警报 * > * 电子邮件设置 * 。 • 注意： * 由于警报和警报是独立的系统，因此用于警报和 AutoSupport 通知的电子邮件设置不用于警报通知。但是，您可以对所有通知使用同一邮件服务器。 为警报设置电子邮件通知	选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。 管理警报（旧系统）
如何管理 SNMP 通知？	选择 * 配置 * > * 监控 * > * SNMP 代理 * 。 使用 SNMP 监控	选择 * 配置 * > * 监控 * > * SNMP 代理 * 。 使用 SNMP 监控 • 注 * ：不会针对每个警报或警报严重性发送 SNMP 通知。 生成 SNMP 通知的警报（旧系统）

	警报	警报（旧系统）
如何控制谁接收通知？	1. 选择 * 警报 * > * 电子邮件设置 * 。 2. 在 * 收件人 * 部分中，为每个电子邮件列表或发生警报时应接收电子邮件的人员输入一个电子邮件地址。 为警报设置电子邮件通知	1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。 2. 创建邮件列表。 3. 选择 * 通知 * 。 4. 选择邮件列表。 管理警报（旧系统）
哪些管理节点会发送通知？	一个管理节点（ "`preferred sender"` ）。 管理 StorageGRID	一个管理节点（ "`preferred sender"` ）。 管理 StorageGRID
如何禁止某些通知？	1. 选择 * 警报 * > * 静音 * 。 2. 选择要静默的警报规则。 3. 指定静默的持续时间。 4. 选择要静默的警报的严重性。 5. 选择可对整个网格，单个站点或单个节点应用静默。 ◦ 注 * ： 如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。 静默警报通知	1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。 2. 选择 * 通知 * 。 3. 选择一个邮件列表，然后选择 * 禁止 * 。 管理警报（旧系统）
如何禁止所有通知？	选择 * 警报 * > * 静音 * 。然后选择 * 所有规则 * 。 • 注 * ： 如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。 静默警报通知	1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。 2. 选中 * 通知禁止全部 * 复选框。 ◦ 注 * ： 在系统范围内禁止电子邮件通知还会禁止事件触发的 AutoSupport 电子邮件。 管理警报（旧系统）
如何自定义条件和触发器？	1. 选择 * 警报 * > * 规则 * 。 2. 选择要编辑的默认规则，或者选择 * 创建自定义规则 * 。 编辑警报规则 创建自定义警报规则	1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。 2. 创建全局自定义警报以覆盖默认警报或监控没有默认警报的属性。 管理警报（旧系统）

	警报	警报（旧系统）
如何禁用单个警报？	1. 选择 * 警报 * > * 规则 * 。 2. 选择规则，然后选择 * 编辑规则 * 。 3. 取消选中 * 已启用 * 复选框。 禁用警报规则	1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。 2. 选择规则，然后选择编辑图标。 3. 取消选中 * 已启用 * 复选框。 管理警报（旧系统）

管理警报

管理警报：概述

通过警报，您可以监控 StorageGRID 系统中的各种事件和状况。您可以通过创建自定义警报，编辑或禁用默认警报，设置警报电子邮件通知以及使警报通知静音来管理警报。

关于 **StorageGRID** 警报

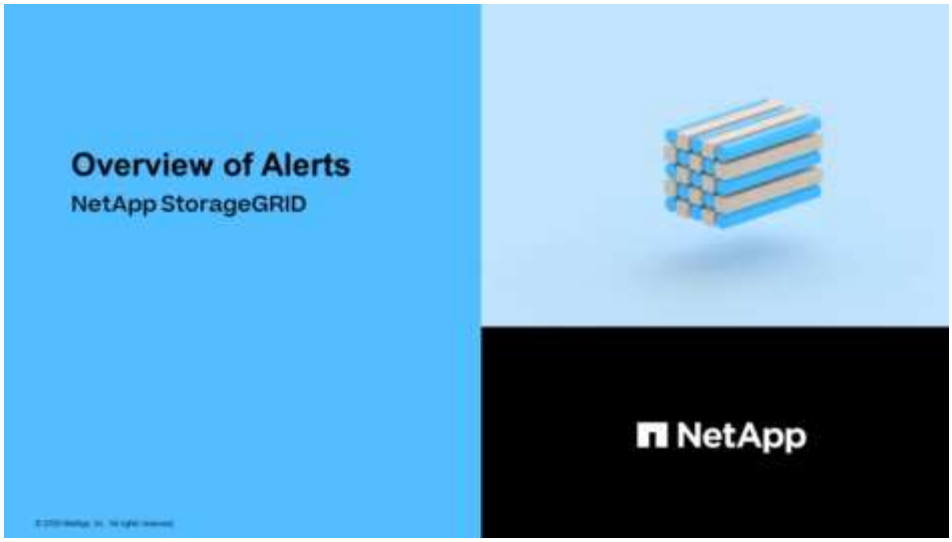
警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

- 警报系统侧重于系统中可操作的问题。对于需要您立即关注的事件，系统会触发警报，而对于可以安全忽略的事件，则不会触发警报。
- " 当前警报 " 页面提供了一个便于用户查看当前问题的界面。您可以按各个警报和警报组对列表进行排序。例如，您可能希望按节点 / 站点对所有警报进行排序，以查看哪些警报正在影响特定节点。或者，您可能希望按触发时间对组中的警报进行排序，以查找特定警报的最新实例。
- " 已解决警报 " 页面提供的信息与 " 当前警报 " 页面上的信息类似，但您可以搜索和查看已解决警报的历史记录，包括警报触发时间和解决时间。
- 同一类型的多个警报会分组到一个电子邮件中，以减少通知数量。此外，同一类型的多个警报将在警报页面上显示为一个组。您可以展开和折叠警报组以显示或隐藏各个警报。例如，如果多个节点报告 "* 无法与节点 * 通信 " 警报大致同时出现，则只会发送一封电子邮件，并且警报会在警报页面上显示为一个组。
- 警报使用直观的名称和说明来帮助您快速了解问题。警报通知包括有关受影响节点和站点的详细信息，警报严重性，触发警报规则的时间以及与警报相关的指标的当前值。
- 警报电子邮件通知以及 " 当前警报 " 和 " 已解决警报 " 页面上的警报列表提供了解决警报的建议操作。这些建议操作通常包括直接链接到 StorageGRID 文档中心，以便于查找和访问更详细的故障排除过程。
- 如果需要在一个或多个严重性级别临时禁止警报通知，您可以轻松地在指定持续时间内对整个网格，单个站点或单个节点静默特定警报规则。您还可以将所有警报规则静默，例如，在软件升级等计划内维护操作步骤期间。
- 您可以根据需要编辑默认警报规则。您可以完全禁用警报规则，也可以更改其触发条件和持续时间。
- 您可以创建自定义警报规则，以确定与您的情况相关的特定条件，并提供您自己的建议操作。要定义自定义警报的条件，请使用网格管理 API 的 " 指标 " 部分提供的 Prometheus 指标创建表达式。

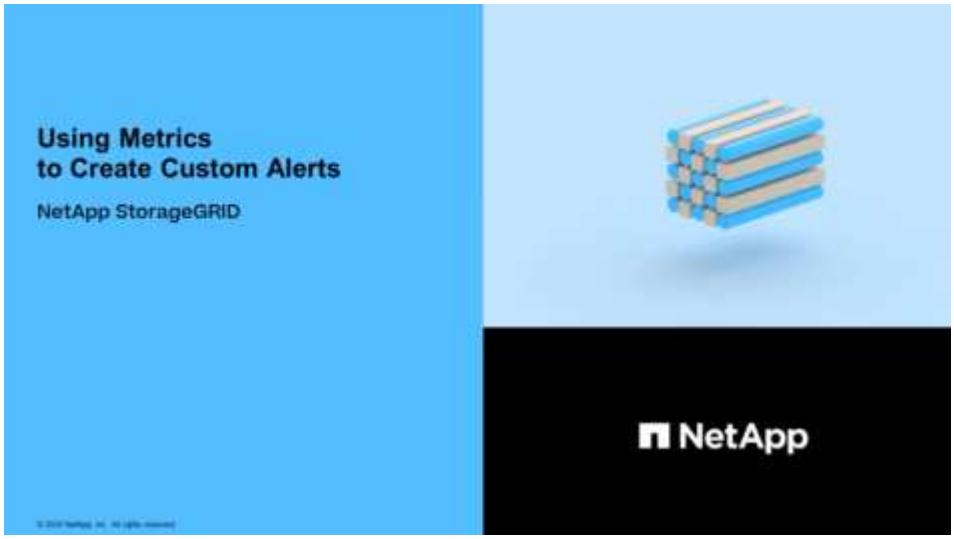
了解更多信息。

要了解更多信息，请查看以下视频：

- "视频：警报概述"



- "视频：使用指标创建自定义警报"



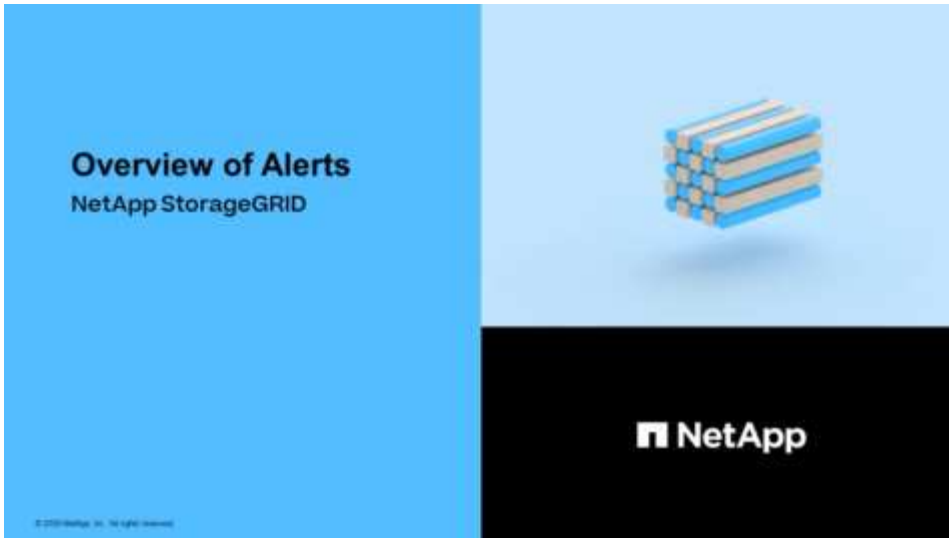
查看警报规则

警报规则用于定义触发的条件 特定警报。StorageGRID 包含一组默认警报规则，您可以按原定义使用或修改这些规则，也可以创建自定义警报规则。

您可以查看所有默认和自定义警报规则的列表，以了解将触发每个警报的条件以及是否已禁用任何警报。

您需要的内容

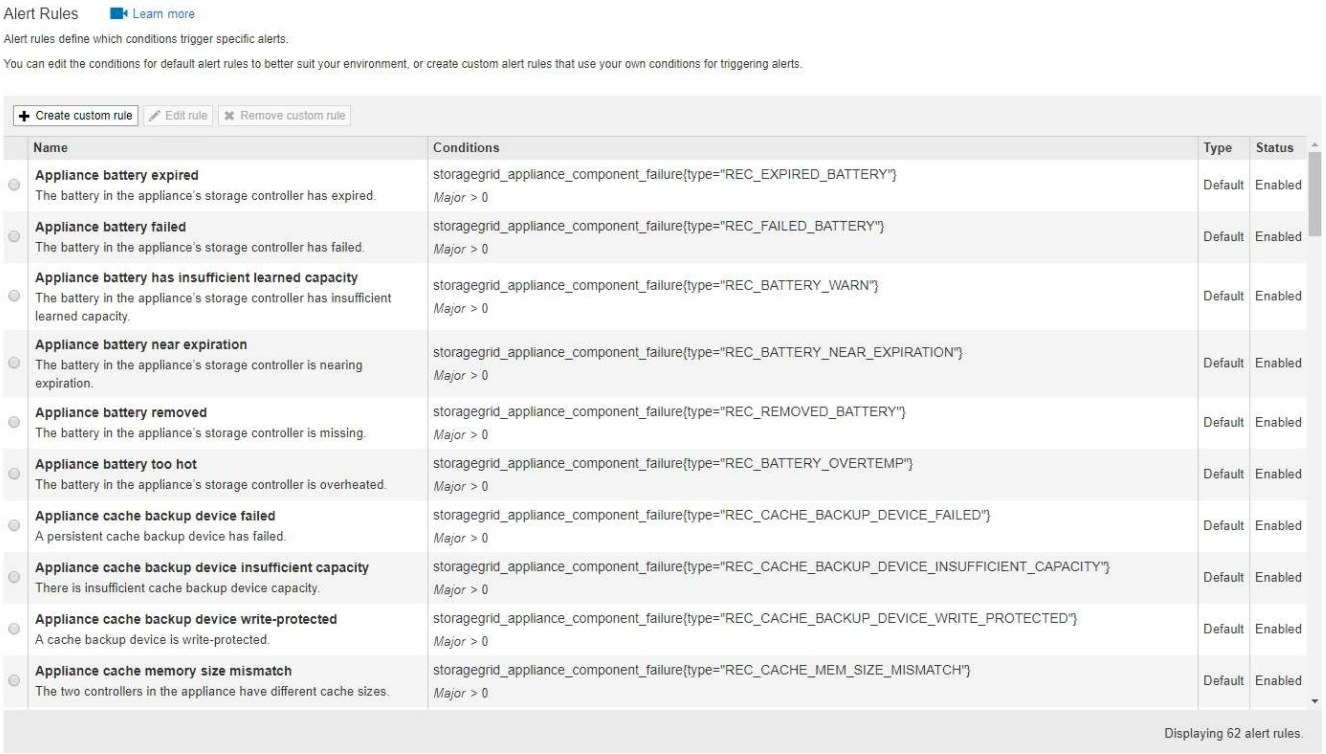
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。
- 您也可以观看以下视频： "视频：警报概述"



步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。



2. 查看警报规则表中的信息：

列标题	**Description**
Name	警报规则的唯一名称和问题描述 。首先列出自定义警报规则，然后列出默认警报规则。警报规则名称是电子邮件通知的主题。

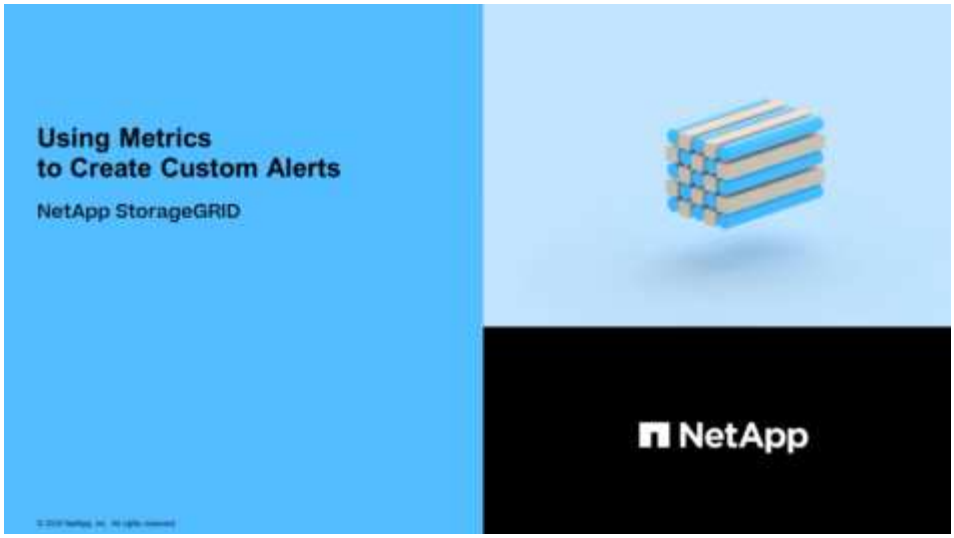
列标题	Description
条件	用于确定何时触发此警报的 Prometheus 表达式。可以在以下一个或多个严重性级别触发警报，但不需要为每个严重性设置一个条件。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 • * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。
Type	警报规则的类型： • * 默认 * ：随系统提供的警报规则。您可以禁用默认警报规则或编辑默认警报规则的条件和持续时间。您不能删除默认警报规则。 • * 默认值 * ：包含已编辑条件或持续时间的默认警报规则。根据需要，您可以轻松地将修改后的条件还原回原始默认值。 • * 自定义 * ：创建的警报规则。您可以禁用，编辑和删除自定义警报规则。
Status	当前是否已启用此警报规则。不会评估已禁用警报规则的条件，因此不会触发任何警报。

创建自定义警报规则

您可以创建自定义警报规则来定义自己触发警报的条件。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器
- 您具有 " 管理警报 " 或 " 根访问 " 权限
- 您熟悉 常用的 Prometheus 指标
- 您了解 "Prometheus 查询的语法"
- 您也可以观看以下视频： "视频：使用指标创建自定义警报"



关于此任务

StorageGRID 不会验证自定义警报。如果您决定创建自定义警报规则，请遵循以下一般准则：

- 查看默认警报规则的条件，并将其用作自定义警报规则的示例。
- 如果为警报规则定义了多个条件，请对所有条件使用相同的表达式。然后，更改每个条件的阈值。
- 仔细检查每个条件是否存在拼写错误和逻辑错误。
- 请仅使用网格管理 API 中列出的指标。
- 在使用网格管理 API 测试表达式时，请注意 " `s`成功 " 响应可能只是空响应正文（未触发警报）。要查看警报是否实际触发，您可以临时将阈值设置为您希望当前为 true 的值。

  例如，要测试表达式 `node_memory_MemTotal_bytes < 240000000` ，请先执行 `node_memory_MemTotal_bytes >= 0` 并确保获得预期结果（所有节点均返回一个值）。然后，将运算符和阈值改回预期值并重新执行。无结果表明此表达式当前没有警报。

- 除非您验证警报是在预期时间触发的，否则请勿假定自定义警报正在运行。

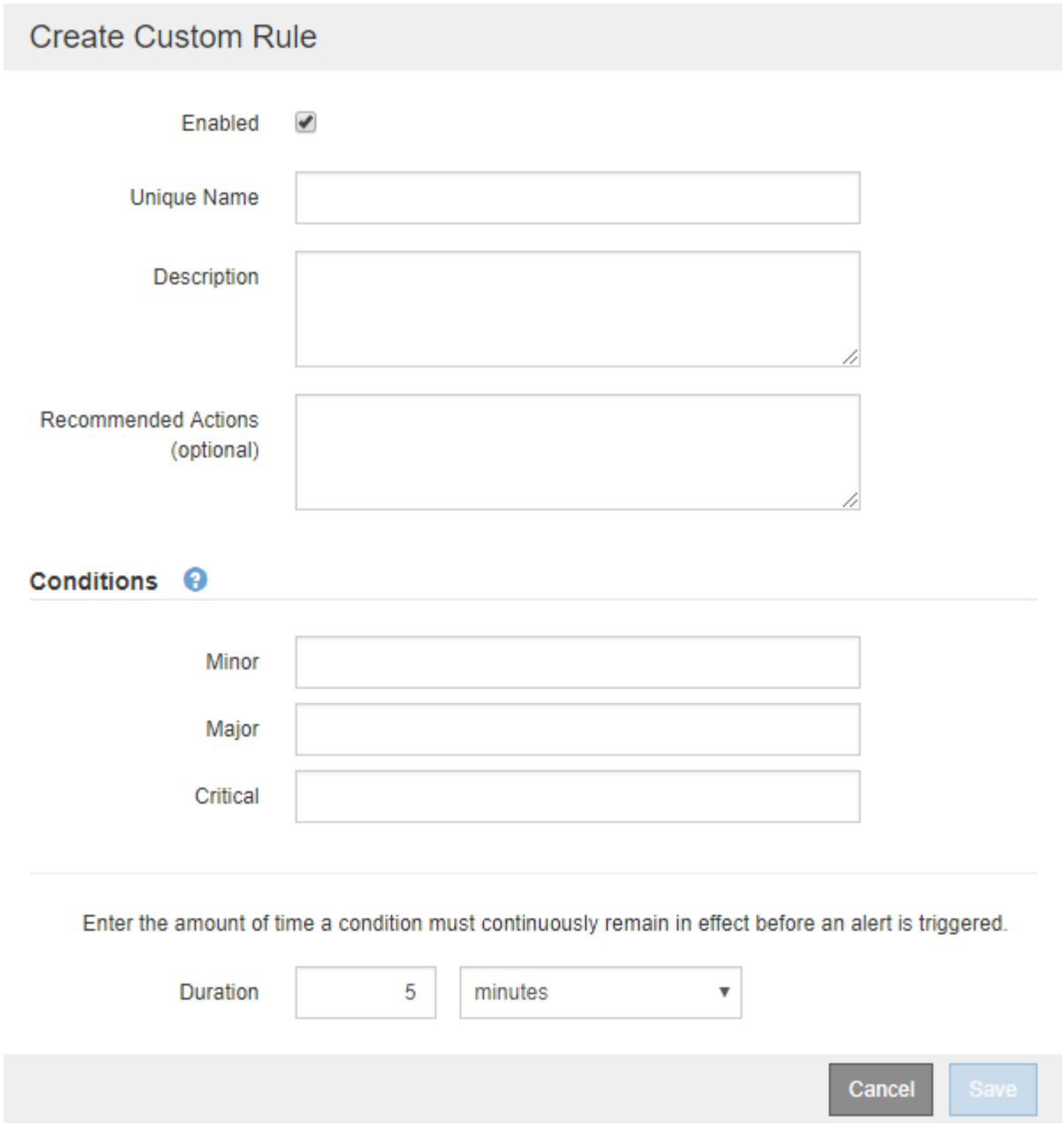
步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

2. 选择 * 创建自定义规则 * 。

   此时将显示创建自定义规则对话框。



3. 选中或取消选中 * 已启用 * 复选框以确定当前是否已启用此警报规则。

   如果禁用了警报规则，则不会评估其表达式，也不会触发任何警报。

4. 输入以下信息：

字段	Description
唯一名称	此规则的唯一名称。警报规则名称显示在警报页面上，也是电子邮件通知的主题。警报规则的名称可以介于 1 到 64 个字符之间。
Description	所发生问题的问题描述 。问题描述 是警报页面和电子邮件通知中显示的警报消息。警报规则的说明可以介于 1 到 128 个字符之间。

字段	Description
建议的操作	也可以选择触发此警报时建议采取的操作。以纯文本格式输入建议的操作（无格式化代码）。警报规则的建议操作可以介于 0 到 1 ， 024 个字符之间。

5. 在条件部分中，为一个或多个警报严重性级别输入一个 Prometheus 表达式。

   基本表达式通常采用以下形式：

   `，指标，运算符，值，`

   表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

   如果节点的已安装 RAM 量小于 24 ， 000 ， 000 ， 000 字节（ 24 GB ），则此表达式会触发警报。

   ```
   node_memory_MemTotal_bytes < 240000000
   ```

   要查看可用指标并测试 Prometheus 表达式，请选择帮助图标 并单击网格管理 API 中的指标部分链接。

6. 在 * 持续时间 * 字段中，输入在触发警报之前条件必须持续保持有效的时间量，然后选择一个时间单位。

   要在条件变为 true 时立即触发警报，请输入 * 。增加此值可防止临时条件触发警报。

   默认值为 5 分钟。

7. 选择 * 保存 * 。

   此时，对话框将关闭，新的自定义警报规则将显示在 "Alert Rules" 表中。

编辑警报规则

您可以编辑警报规则以更改触发条件，对于自定义警报规则，您还可以更新规则名称，问题描述 和建议的操作。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。

关于此任务

编辑默认警报规则时，您可以更改次要警报，主要警报和严重警报的条件以及持续时间。编辑自定义警报规则时，您还可以编辑规则的名称，问题描述 和建议的操作。

> 决定编辑警报规则时请务必小心。如果更改了触发值，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

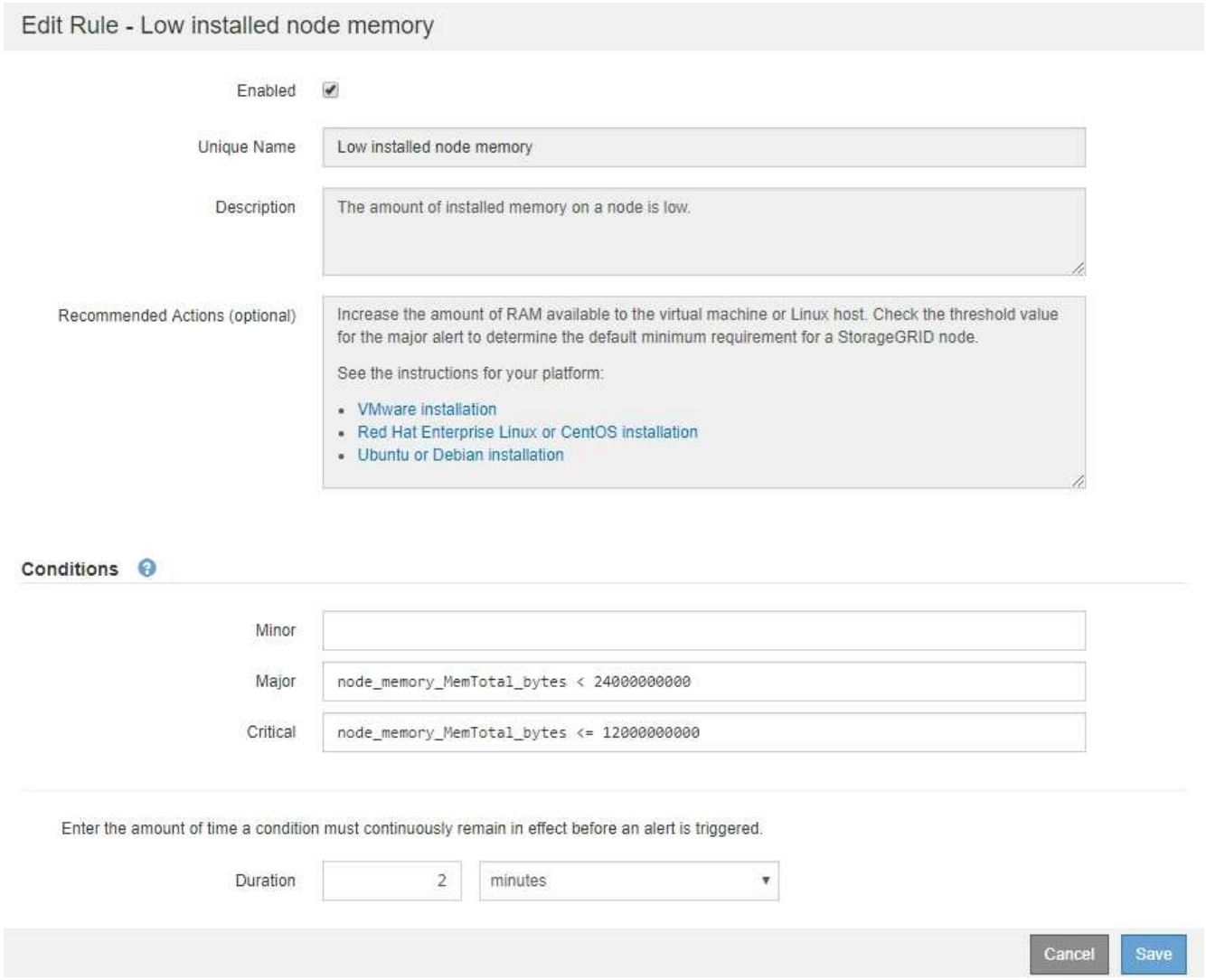
步骤

1. 选择 * 警报 * > * 规则 * 。

此时将显示 "Alert Rules" 页面。

2. 选择要编辑的警报规则对应的单选按钮。
3. 选择 * 编辑规则 * 。

   此时将显示编辑规则对话框。此示例显示了一个默认警报规则— Unique Name ，问题描述 和 Recommended Actions 字段已禁用，无法编辑。



4. 选中或取消选中 * 已启用 * 复选框以确定当前是否已启用此警报规则。

   如果禁用了警报规则，则不会评估其表达式，也不会触发任何警报。

   如果您对当前警报禁用警报规则，则必须等待几分钟，使警报不再显示为活动警报。

   通常，不建议禁用默认警报规则。如果禁用了警报规则，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

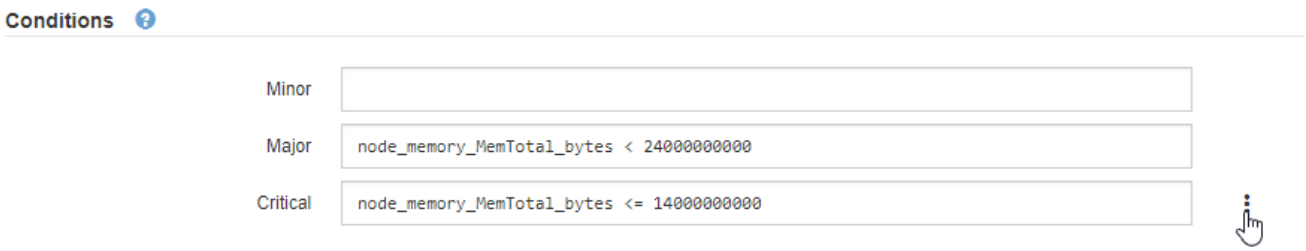
5. 对于自定义警报规则，请根据需要更新以下信息。

您不能为默认警报规则编辑此信息。

字段	Description
唯一名称	此规则的唯一名称。警报规则名称显示在警报页面上，也是电子邮件通知的主题。警报规则的名称可以介于 1 到 64 个字符之间。
Description	所发生问题的问题描述 。问题描述 是警报页面和电子邮件通知中显示的警报消息。警报规则的说明可以介于 1 到 128 个字符之间。
建议的操作	也可以选择触发此警报时建议采取的操作。以纯文本格式输入建议的操作（无格式化代码）。警报规则的建议操作可以介于 0 到 1 ， 024 个字符之间。

6. 在条件部分中，输入或更新一个或多个警报严重性级别的 Prometheus 表达式。

如果要将已编辑默认警报规则的条件还原为其原始值，请选择已修改条件右侧的三个点。



如果您更新了当前警报的条件，则在解决上一条件之前，可能无法实施您所做的更改。下次满足规则的其中一个条件时，警报将反映更新后的值。

基本表达式通常采用以下形式：

`，指标，运算符，值，`

表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

如果节点的已安装 RAM 量小于 24 ， 000 ， 000 ， 000 字节（ 24 GB ），则此表达式会触发警报。

```
node_memory_MemTotal_bytes < 240000000
```

7. 在 * 持续时间 * 字段中，输入在触发警报之前条件必须持续保持有效的时间量，然后选择时间单位。

要在条件变为 true 时立即触发警报，请输入 * 。增加此值可防止临时条件触发警报。

默认值为 5 分钟。

8. 选择 * 保存 * 。

如果您编辑了默认警报规则，则 "Type" 列中将显示 "* 默认值 " 。如果禁用了默认或自定义警报规则， * 状态 * 列中将显示 * 已禁用 * 。

禁用警报规则

您可以更改默认或自定义警报规则的启用 / 禁用状态。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。

关于此任务

禁用警报规则后，不会评估其表达式，也不会触发任何警报。

> 通常，不建议禁用默认警报规则。如果禁用了警报规则，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

2. 选择要禁用或启用的警报规则对应的单选按钮。
3. 选择 * 编辑规则 * 。

   此时将显示编辑规则对话框。

4. 选中或取消选中 * 已启用 * 复选框以确定当前是否已启用此警报规则。

   如果禁用了警报规则，则不会评估其表达式，也不会触发任何警报。

   > 如果您对当前警报禁用警报规则，则必须等待几分钟，以使警报不再显示为活动警报。

5. 选择 * 保存 * 。
   - 已禁用 * 显示在 * 状态 * 列中。

删除自定义警报规则

如果您不想再使用自定义警报规则，可以将其删除。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。

步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

2. 选择要删除的自定义警报规则对应的单选按钮。

您不能删除默认警报规则。

3. 选择 * 删除自定义规则 * 。

   此时将显示确认对话框。

4. 选择 * 确定 * 以删除警报规则。

   任何处于活动状态的警报实例将在 10 分钟内得到解决。

管理警报通知

为警报设置 **SNMP** 通知

如果您希望 StorageGRID 在发生警报时发送 SNMP 通知，则必须启用 StorageGRID SNMP 代理并配置一个或多个陷阱目标。

您可以使用网格管理器中的 * 配置 * > * 监控 * > * SNMP 代理 * 选项或网格管理 API 的 SNMP 端点来启用和配置 StorageGRID SNMP 代理。SNMP 代理支持所有三个版本的 SNMP 协议。

要了解如何配置 SNMP 代理，请参见 使用 SNMP 监控。

配置 StorageGRID SNMP 代理后，可以发送两种类型的事件驱动型通知：

- 陷阱是指 SNMP 代理发送的通知，不需要管理系统确认。陷阱用于通知管理系统 StorageGRID 中发生了某种情况，例如触发警报。所有三个版本的 SNMP 均支持陷阱。
- 通知与陷阱类似，但需要管理系统确认。如果 SNMP 代理未在特定时间内收到确认，则会重新发送通知，直到收到确认或达到最大重试值为止。SNMPv2c 和 SNMPv3 支持 INFORM 。

在任何严重性级别触发默认或自定义警报时，系统都会发送陷阱和通知通知通知。要禁止警报的 SNMP 通知，您必须为此警报配置静默。请参见 静默警报通知。

警报通知由配置为首选发送方的任何管理节点发送。默认情况下，会选择主管理节点。请参见 有关管理 StorageGRID 的说明。

> 在指定严重性级别或更高级别触发某些警报（传统系统）时，也会发送陷阱和通知通知通知；但是，不会针对每个警报或每个警报严重性发送 SNMP 通知。请参见 生成 SNMP 通知的警报（旧系统）。

为警报设置电子邮件通知

如果您希望在出现警报时发送电子邮件通知，则必须提供有关 SMTP 服务器的信息。您还必须输入警报通知收件人的电子邮件地址。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。

关于此任务

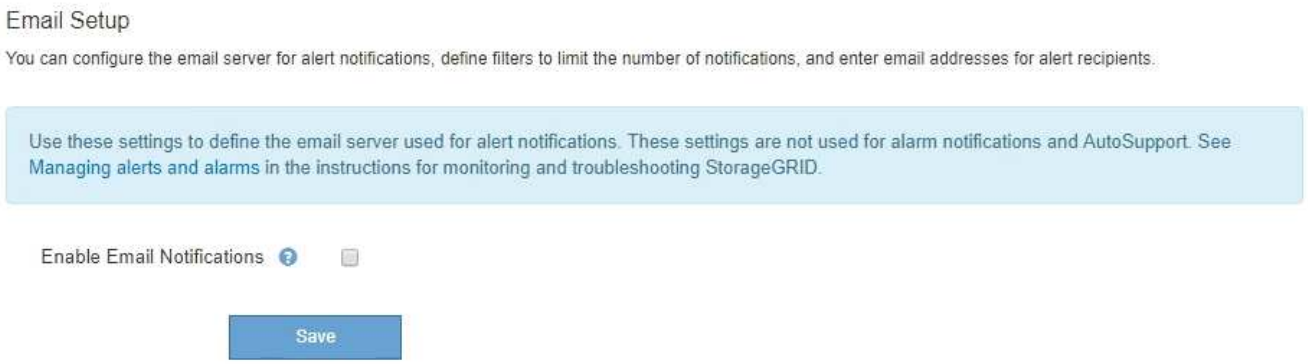
由于警报和警报是独立的系统，因此用于警报通知的电子邮件设置不会用于警报通知和 AutoSupport 消息。但是，您可以对所有通知使用同一个电子邮件服务器。

如果您的 StorageGRID 部署包含多个管理节点，则可以选择哪个管理节点应是警报通知的首选发送方。警报通知和 AutoSupport 消息也会使用相同的 "`首选发件人` " 。默认情况下，会选择主管理节点。有关详细信息，请参见 有关管理 StorageGRID 的说明。

步骤

1. 选择 * 警报 * > * 电子邮件设置 * 。

   此时将显示电子邮件设置页面。



2. 选中 * 启用电子邮件通知 * 复选框，以指示您希望在警报达到配置的阈值时发送通知电子邮件。

   此时将显示电子邮件（ SMTP ）服务器，传输层安全（ TLS ），电子邮件地址和筛选器部分。

3. 在电子邮件（ SMTP ）服务器部分中，输入 StorageGRID 访问 SMTP 服务器所需的信息。

   如果 SMTP 服务器需要身份验证，则必须同时提供用户名和密码。

字段	输入 ...
邮件服务器	SMTP 服务器的完全限定域名（ FQDN ）或 IP 地址。
Port	用于访问 SMTP 服务器的端口。必须介于 1 到 65535 之间。
用户名（可选）	如果 SMTP 服务器需要身份验证，请输入要进行身份验证的用户名。
密码（可选）	如果 SMTP 服务器需要身份验证，请输入用于进行身份验证的密码。



4. 在电子邮件地址部分中，输入发件人和每个收件人的电子邮件地址。

   a. 对于 * 发件人电子邮件地址 * ，请指定一个有效的电子邮件地址，用作警报通知的发件人地址。

      例如： `storagegrid-alerts@example.com`

   b. 在收件人部分中，为每个电子邮件列表或发生警报时应接收电子邮件的人员输入电子邮件地址。

      选择加号图标 ✚ 以添加收件人。



5. 如果要与 SMTP 服务器进行通信，需要使用传输层安全（ TLS ），请在传输层安全（ TLS ）部分中选择 * 需要 TLS* 。

   a. 在 * CA 证书 * 字段中，提供用于验证 SMTP 服务器标识的 CA 证书。

      您可以将内容复制并粘贴到此字段中，或者选择 * 浏览 * 并选择文件。

      您必须提供一个文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

   b. 如果 SMTP 电子邮件服务器要求电子邮件发件人提供用于身份验证的客户端证书，请选中 * 发送客户端证书 * 复选框。

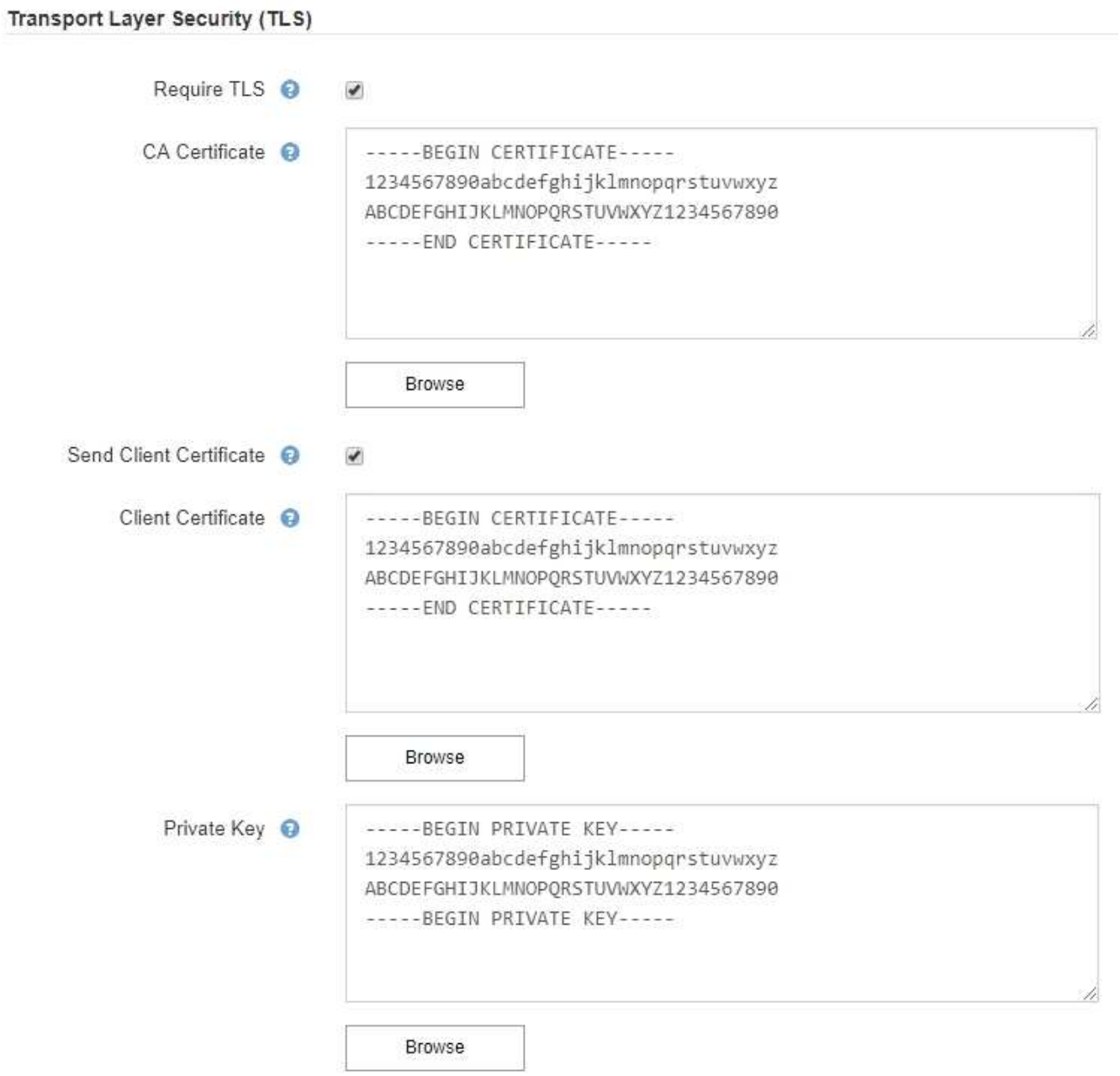
   c. 在 * 客户端证书 * 字段中，提供 PEM 编码的客户端证书以发送到 SMTP 服务器。

      您可以将内容复制并粘贴到此字段中，或者选择 * 浏览 * 并选择文件。

   d. 在 * 专用密钥 * 字段中，输入未加密 PEM 编码的客户端证书的专用密钥。

      您可以将内容复制并粘贴到此字段中，或者选择 * 浏览 * 并选择文件。

      如果需要编辑电子邮件设置，请选择铅笔图标以更新此字段。



6. 在筛选器部分中，选择应导致电子邮件通知的警报严重性级别，除非特定警报的规则已被静音。

severity	Description
次要，重大，严重	满足警报规则的次要，主要或严重条件时，系统会发送电子邮件通知。
主要，关键	当满足警报规则的主要或关键条件时，系统会发送电子邮件通知。不会针对次要警报发送通知。
仅严重	只有在满足警报规则的严重条件时，才会发送电子邮件通知。对于次要或主要警报，不会发送通知。



7. 准备好测试电子邮件设置后，请执行以下步骤：

   a. 选择 * 发送测试电子邮件 * 。

      此时将显示一条确认消息，指示已发送测试电子邮件。

   b. 检查所有电子邮件收件人的收件箱，确认已收到测试电子邮件。

      如果在几分钟内未收到电子邮件，或者触发了 * 电子邮件通知失败 * 警报，请检查您的设置并重试。

   c. 登录到任何其他管理节点并发送测试电子邮件以验证所有站点的连接。

      在测试警报通知时，您必须登录到每个管理节点以验证连接。这与测试警报通知和 AutoSupport 消息不同，所有管理节点都会发送测试电子邮件。

8. 选择 * 保存 * 。

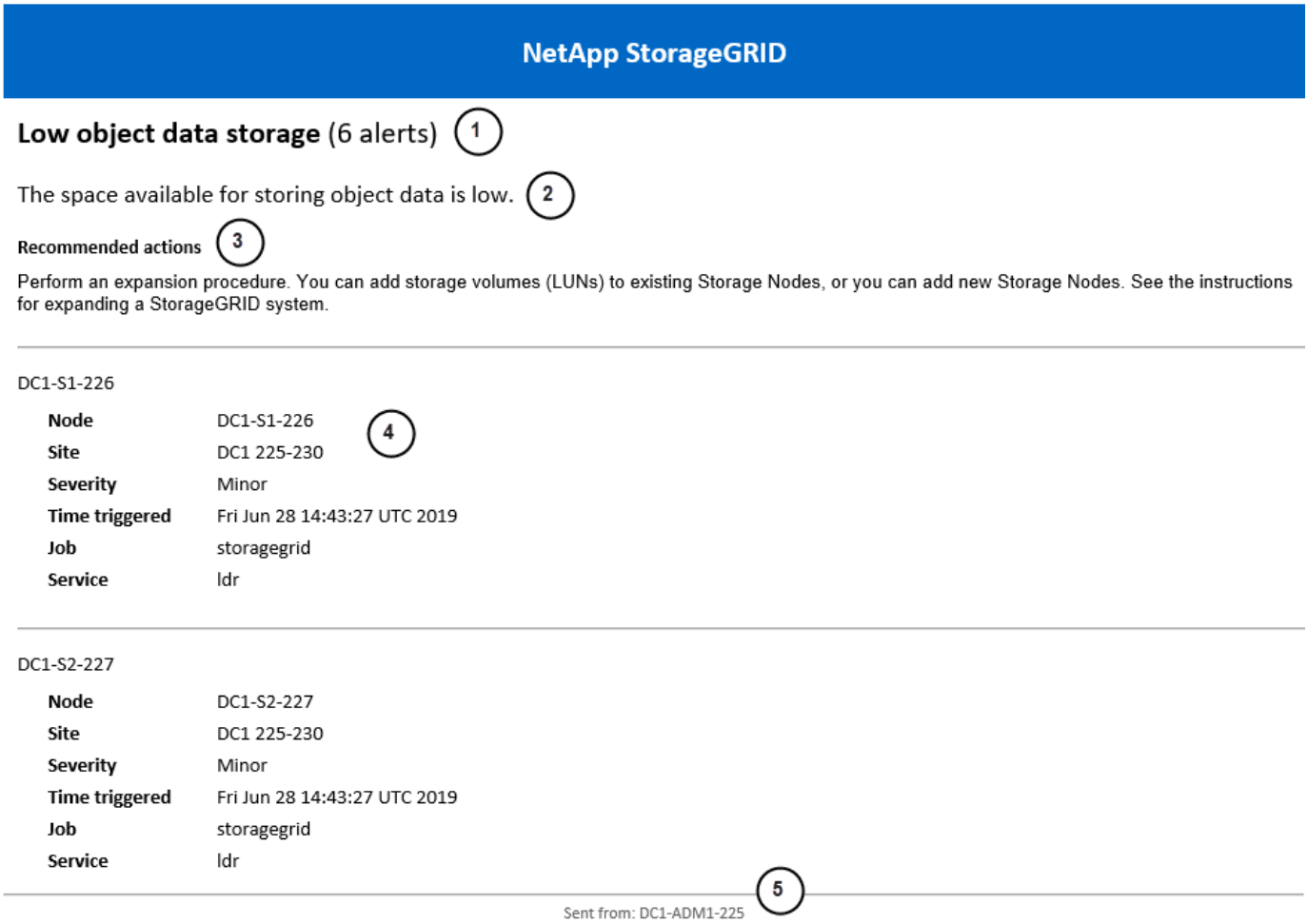
   发送测试电子邮件不会保存您的设置。您必须选择 * 保存 * 。

   此时将保存电子邮件设置。

警报电子邮件通知中包含的信息

配置 SMTP 电子邮件服务器后，在触发警报时，系统会向指定的收件人发送电子邮件通知，除非警报规则被静默禁止。请参见 静默警报通知。

电子邮件通知包括以下信息：



Callout	Description
1.	警报名称，后跟此警报的活动实例数。
2.	警报的问题描述 。
3.	为警报建议的任何操作。
4.	有关警报的每个活动实例的详细信息，包括受影响的节点和站点，警报严重性，触发警报规则的 UTC 时间以及受影响作业和服务的名称。
5.	发送通知的管理节点的主机名。

如何对警报进行分组

为了防止在触发警报时发送过多的电子邮件通知， StorageGRID 会尝试在同一通知中对多个警报进行分组。

有关 StorageGRID 如何在电子邮件通知中对多个警报进行分组的示例，请参见下表。

行为	示例
每个警报通知仅适用于同名警报。如果同时触发两个名称不同的警报，则会发送两封电子邮件通知。	• 警报 A 会同时在两个节点上触发。仅发送一个通知。 • 节点 1 上触发警报 A ，节点 2 上同时触发警报 B 。系统会发送两个通知—每个警报一个。
对于特定节点上的特定警报，如果达到阈值的严重性超过一个，则仅针对最严重警报发送通知。	• 此时将触发警报 A ，并达到次要，主要和严重警报阈值。系统会为严重警报发送一条通知。
首次触发警报时， StorageGRID 会等待 2 分钟，然后再发送通知。如果在此期间触发了其他同名警报，则 StorageGRID 会在初始通知中对所有警报进行分组。	1. 节点 1 上的警报 A 在 08： 00 触发。不会发送任何通知。 2. 节点 2 上的警报 A 在 08： 01 触发。不会发送任何通知。 3. 8： 02 发送通知以报告两个警报实例。
如果触发另一个同名警报， StorageGRID 将等待 10 分钟，然后再发送新通知。新通知会报告所有活动警报（当前未静音的警报），即使先前已报告这些警报也是如此。	1. 节点 1 上的警报 A 在 08： 00 触发。通知在 08： 02 发送。 2. 节点 2 上的警报 A 在 08： 05 触发。第二个通知将在 8： 15 （ 10 分钟后）发送。此时将报告这两个节点。
如果当前存在多个同名警报且其中一个警报已解决，则在已解决警报的节点上重新出现此警报时，不会发送新通知。	1. 已针对节点 1 触发警报 A 。此时将发送通知。 2. 已针对节点 2 触发警报 A 。此时将发送第二个通知。 3. 已解决节点 2 的警报 A ，但此警报对于节点 1 仍处于活动状态。 4. 此时将再次触发节点 2 的警报 A 。不会发送任何新通知，因为此警报对于节点 1 仍处于活动状态。
StorageGRID 会继续每 7 天发送一次电子邮件通知，直到所有警报实例均已解决或警报规则已静音为止。	1. 3 月 8 日为节点 1 触发警报 A 。此时将发送通知。 2. 警报 A 未解决或静音。其他通知将于 3 月 15 日， 3 月 22 日， 3 月 29 日等时间发送。

对警报电子邮件通知进行故障排除

如果触发了 * 电子邮件通知失败 * 警报，或者您无法收到测试警报电子邮件通知，请按照以下步骤解决问题描述。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。

步骤

1. 验证设置。
   a. 选择 * 警报 * > * 电子邮件设置 * 。
   b. 验证电子邮件（ SMTP ）服务器设置是否正确。
   c. 验证您是否为收件人指定了有效的电子邮件地址。
2. 检查垃圾邮件筛选器，确保电子邮件未发送到垃圾文件夹。
3. 请您的电子邮件管理员确认不会阻止来自发件人地址的电子邮件。
4. 收集管理节点的日志文件，然后联系技术支持。

   技术支持可以使用日志中的信息帮助确定出现问题的原因。例如， prometheus.log 文件在连接到您指定的服务器时可能会显示错误。

   请参见 收集日志文件和系统数据。

静默警报通知

或者，您也可以配置静音以临时禁止警报通知。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。

关于此任务

您可以对整个网格，单个站点或单个节点以及一个或多个严重性静默警报规则。每次静默都将禁止针对单个警报规则或所有警报规则发出所有通知。

如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。

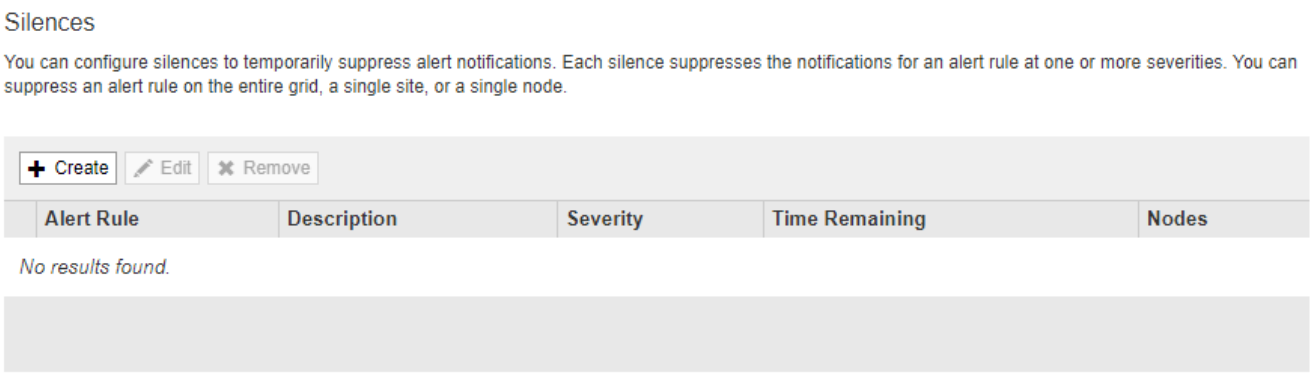
> 在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

> 由于警报和警报是独立的系统，因此不能使用此功能禁止警报通知。

步骤

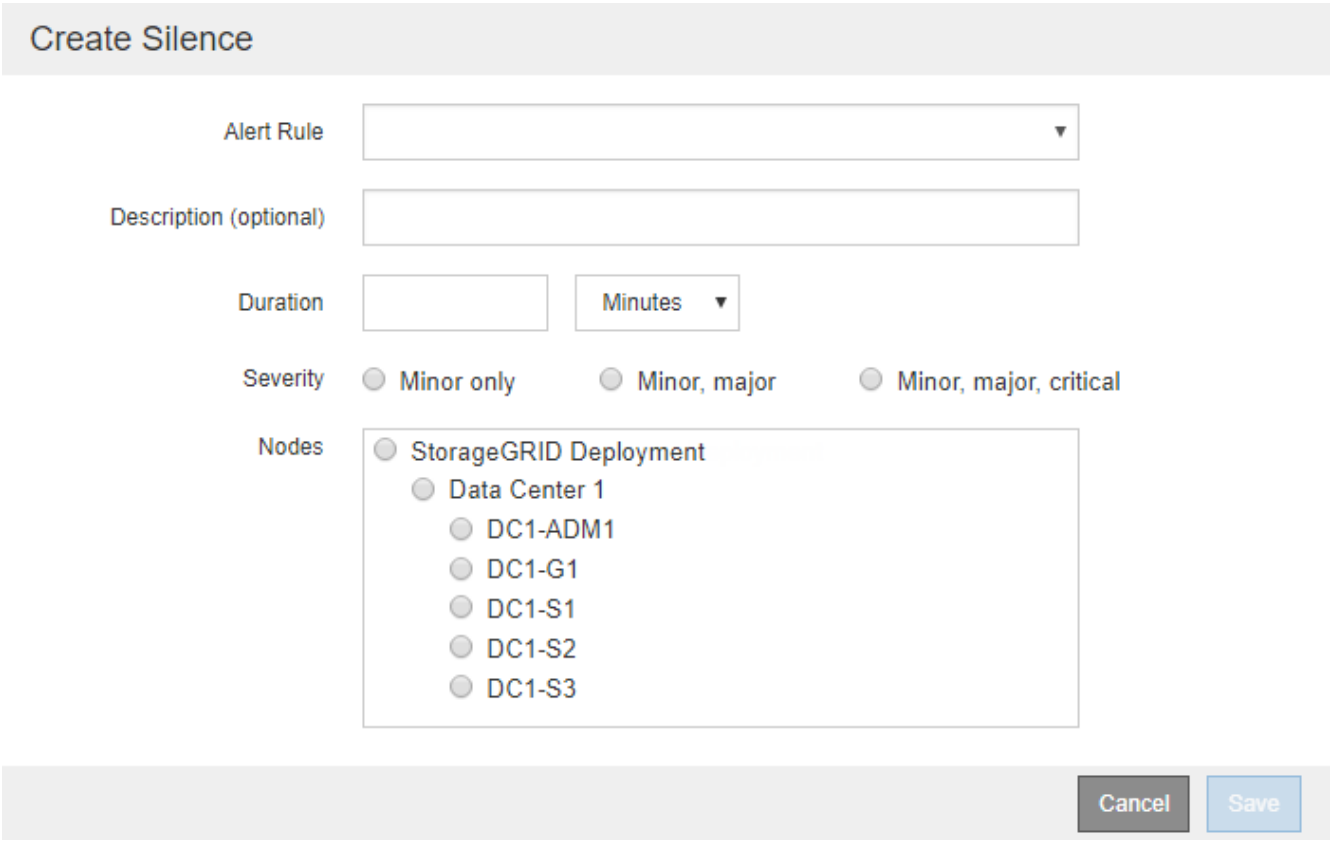
1. 选择 * 警报 * > * 静音 * 。

   此时将显示 Silences 页面。



2. 选择 * 创建 * 。

   此时将显示创建静默对话框。



3. 选择或输入以下信息：

字段	Description
警报规则	要静默的警报规则的名称。您可以选择任何默认或自定义警报规则，即使警报规则已禁用也是如此。 • 注： * 如果要使用此对话框中指定的标准将所有警报规则静默，请选择 * 所有规则 * 。
Description	也可以选择静默问题描述 。例如，请描述此静默的目的。

字段	Description
Duration	希望此静默保持有效的时间，以分钟，小时或天为单位。静默时间为 5 分钟到 1 ， 825 天（ 5 年）。 • 注意： * 不应将警报规则静默较长时间。如果某个警报规则已静音，则在阻止完成关键操作之前，您可能无法检测到潜在问题。但是，如果警报是由特定的有意配置触发的，则可能需要使用长时间静默，例如， "* 服务设备链路已关闭 " 警报和 "* 存储设备链路已关闭 " 警报可能会出现这种情况。
severity	应将哪个警报严重性或严重性静音。如果在选定严重性之一触发警报，则不会发送任何通知。
节点	您希望此静默应用于哪个或哪些节点。您可以禁止整个网格，单个站点或单个节点上的警报规则或所有规则。如果选择整个网格，则会将适用场景 静默所有站点和所有节点。如果选择站点，则此静默状态仅适用于该站点上的节点。 • 注意： * 每次静默不能选择多个节点或多个站点。如果要同时在多个节点或多个站点上禁止相同的警报规则，则必须创建其他静音。

4. 选择 * 保存 * 。
5. 如果要在静默过期之前修改或结束静默，可以对其进行编辑或删除。

选项	Description
编辑静默	a. 选择 * 警报 * > * 静音 * 。 b. 从表中，选择要编辑的静默设置对应的单选按钮。 c. 选择 * 编辑 * 。 d. 更改问题描述 ，剩余时间，选定严重性或受影响的节点。 e. 选择 * 保存 * 。
取消静默	a. 选择 * 警报 * > * 静音 * 。 b. 从表中，选择要删除的静默设置对应的单选按钮。 c. 选择 * 删除 * 。 d. 选择 * 确定 * 确认要删除此静默状态。 ◦ 注意 * ：现在，在触发此警报时，系统将发送通知（除非被另一个静默禁止）。如果当前触发此警报，则发送电子邮件或 SNMP 通知以及更新警报页面可能需要几分钟的时间。

相关信息

- 配置 SNMP 代理

StorageGRID 警报系统是一种传统系统，用于识别正常运行期间有时会出现的故障点。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

警报类（旧系统）

旧警报可以属于两个相互排斥的警报类之一。

- 每个 StorageGRID 系统都提供默认警报，无法修改。但是，您可以禁用默认警报或通过定义全局自定义警报来覆盖这些警报。
- 全局自定义警报可监控 StorageGRID 系统中给定类型的所有服务的状态。您可以创建全局自定义警报以覆盖默认警报。您还可以创建新的全局自定义警报。这对于监控 StorageGRID 系统的任何自定义条件非常有用。

警报触发逻辑（旧系统）

当 StorageGRID 属性达到阈值时，系统将触发传统警报，该阈值将根据警报类（默认或全局自定义）和警报严重性级别的组合计算为 true 。

图标。	颜色	警报严重性	含义
	黄色	通知	节点已连接到网格，但存在不影响正常操作的异常情况。
	浅橙色	次要	节点已连接到网格，但存在异常情况，可能会影响未来的运行。您应进行调查以防止上报。
	深橙色	major	节点已连接到网格，但存在当前影响操作的异常情况。这需要立即引起注意，以防止升级。
	红色	严重	节点已连接到网格，但存在已停止正常操作的异常情况。您应立即解决此问题描述 。

可以为每个数字属性设置警报严重性和相应的阈值。每个管理节点上的 NMS 服务会根据已配置的阈值持续监控当前属性值。触发警报后，系统会向所有指定人员发送通知。

请注意，严重性级别为 " 正常 " 不会触发警报。

将根据为属性定义的已启用警报列表评估属性值。系统将按以下顺序检查警报列表，以查找第一个警报类，该警报类已为属性定义并启用警报：

1. 全局自定义警报，其警报严重性从严重到通知不等。
2. 警报严重性从严重到通知的默认警报。

在较高的警报类中找到已启用的属性警报后， NMS 服务仅会在该类中进行评估。NMS 服务不会根据其他低优先级类进行评估。也就是说，如果某个属性启用了全局自定义警报，则 NMS 服务仅根据全局自定义警报评估属性值。不评估默认警报。因此，为某个属性启用的默认警报可以满足触发警报所需的条件，但由于为同一属性启

用了全局自定义警报（不符合指定的标准），因此不会触发此警报。不会触发任何警报，也不会发送任何通知。

警报触发示例

您可以使用此示例了解如何触发全局自定义警报和默认警报。

对于以下示例，属性定义并启用了全局自定义警报和默认警报，如下表所示。

	全局自定义警报阈值（已启用）	默认警报阈值（已启用）
通知	>= 1500	>= 1000
次要	>= 15 ， 000	>= 1000
major	>=150 ， 000	>= 250 ， 000

如果在该属性的值为 1000 时对其进行评估，则不会触发任何警报，也不会发送任何通知。

全局自定义警报优先于默认警报。值 1000 不会达到全局自定义警报的任何严重性级别的阈值。因此，警报级别将评估为正常。

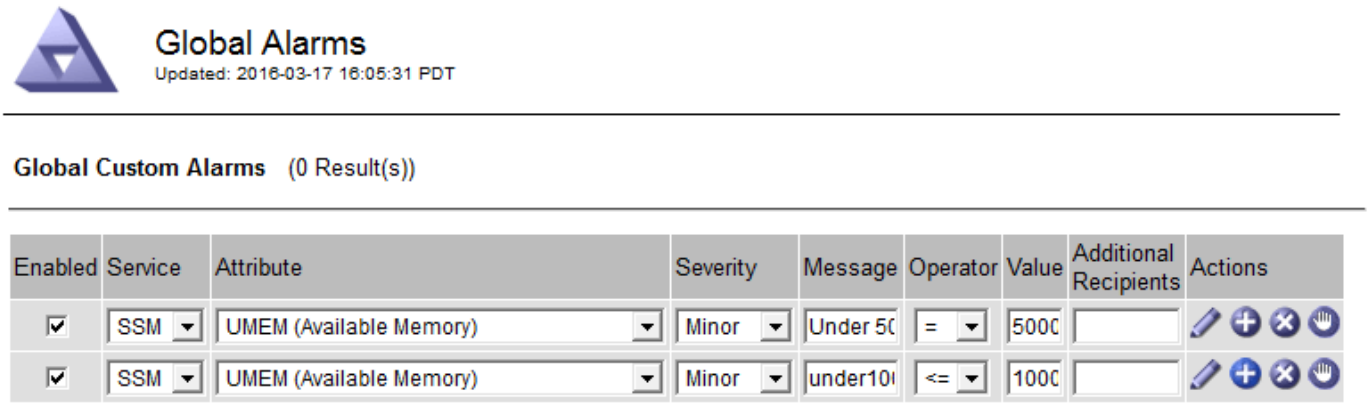
在上述情形之后，如果禁用了全局自定义警报，则不会发生任何更改。在触发新的警报级别之前，必须重新评估属性值。

在禁用全局自定义警报的情况下，重新评估属性值时，系统会根据默认警报的阈值评估属性值。警报级别将触发通知级别警报，并向指定人员发送电子邮件通知。

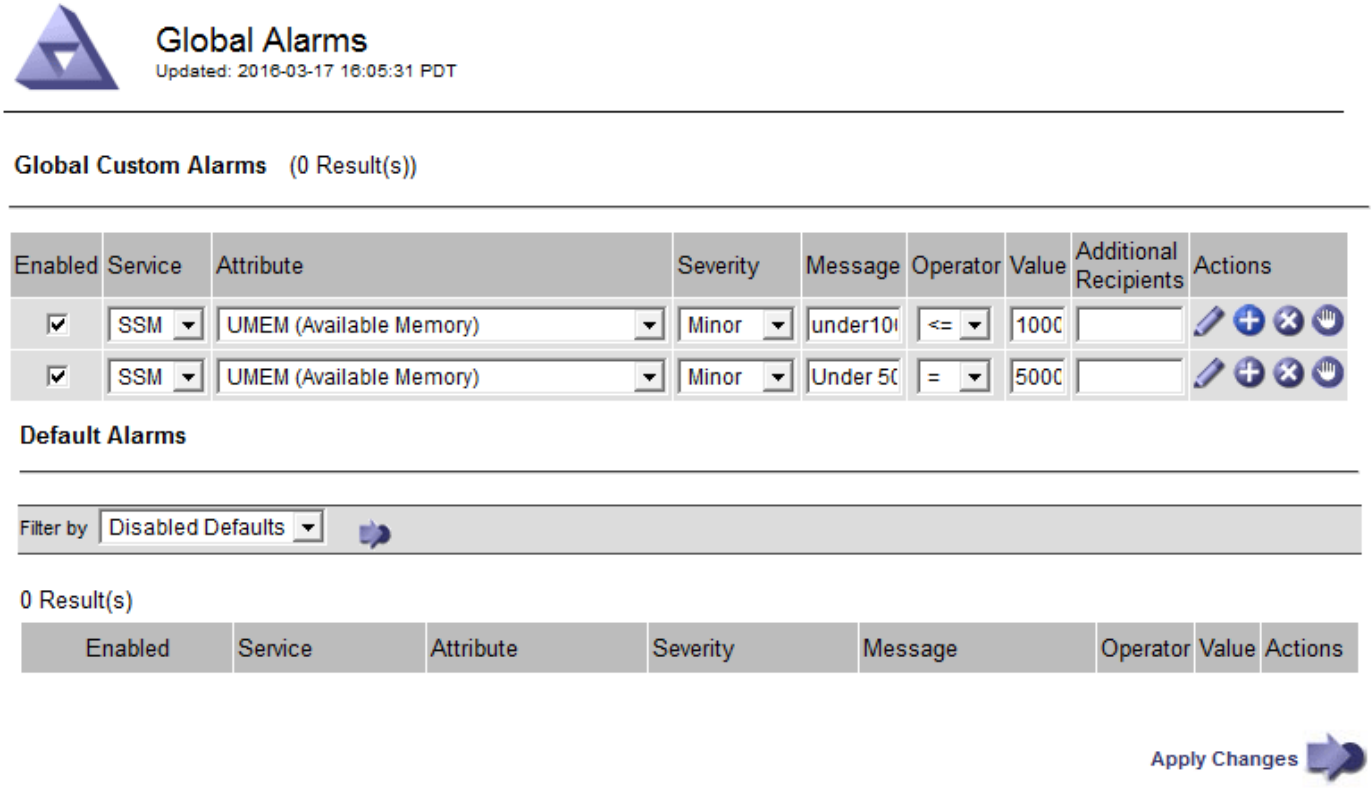
严重性相同的警报

如果同一属性的两个全局自定义警报的严重性相同，则会使用 "`top down` " 优先级对警报进行评估。

例如，如果 UMEM 降至 50 MB ，则会触发第一个警报（ = 50000 ），但不会触发其下一个警报（ <=100000000 ）。



如果顺序相反，则在 UMEM 降至 100 MB 时，将触发第一个警报（ <=100000000 ），但不会触发其下一个警报（ = 50000000 ）。



通知

通知用于报告警报发生情况或服务状态发生变化。可以通过电子邮件或 SNMP 发送警报通知。

为了避免在达到警报阈值时发送多个警报和通知，系统会根据属性的当前警报严重性检查警报严重性。如果没有更改，则不会采取进一步操作。这意味着，随着 NMS 服务继续监控系统，它只会在首次发现某个属性的警报条件时发出警报并发送通知。如果达到并检测到属性的新值阈值，则警报严重性会发生变化，并会发送新通知。当条件恢复到正常水平时，警报将被清除。

警报状态通知中显示的触发值将四舍五入为小数点后三位。因此，属性值 1.9999 将触发阈值小于（ < ） 2.0 的警报，但警报通知会将触发值显示为 2.0 。

新服务

随着通过添加新网格节点或站点来添加新服务，这些服务将继承默认警报和全局自定义警报。

警报和表

表中显示的警报属性可以在系统级别禁用。不能为表中的各个行禁用警报。

例如，下表显示了两个严重条目可用（ VMFI ）警报。（选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 存储节点 _* > * SSM* > * 资源 * 。）

您可以禁用 VMFI 警报，以便不触发严重级别的 VMFI 警报（当前严重警报均会在表中显示为绿色）； 但是，您不能在表行中禁用单个警报，以便一个 VMFI 警报显示为严重级别警报，而另一个警报保持绿色。

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

确认当前警报（旧系统）

当系统属性达到警报阈值时，系统会触发原有警报。或者，如果要减少或清除旧警报列表，您也可以确认这些警报。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有确认警报权限。

关于此任务

由于传统警报系统仍受支持，因此每当发生新警报时，" 当前警报 " 页面上的原有警报列表都会增加。您通常可以忽略警报（因为警报可提供更好的系统视图），也可以确认警报。

或者，在完全过渡到警报系统后，您可以禁用每个旧警报，以防止其被触发并添加到旧警报计数中。

确认警报后，它将不再列在网格管理器的 " 当前警报 " 页面上，除非警报在下一个严重性级别触发，或者已解决并再次发生。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

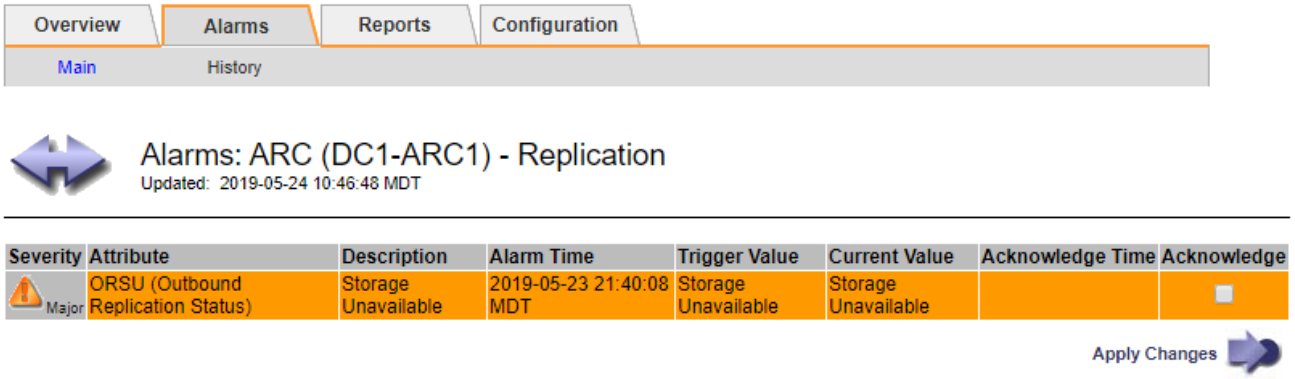
步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。



2. 在表中选择服务名称。

此时将显示选定服务的警报选项卡（ * 支持 * > * 工具 * > * 网格拓扑 * > * 网格节点 _* > * 服务 _* > * 警报 * ）。



3. 选中警报的 * 确认 * 复选框，然后单击 * 应用更改 * 。

   警报不再显示在信息板或当前警报页面上。

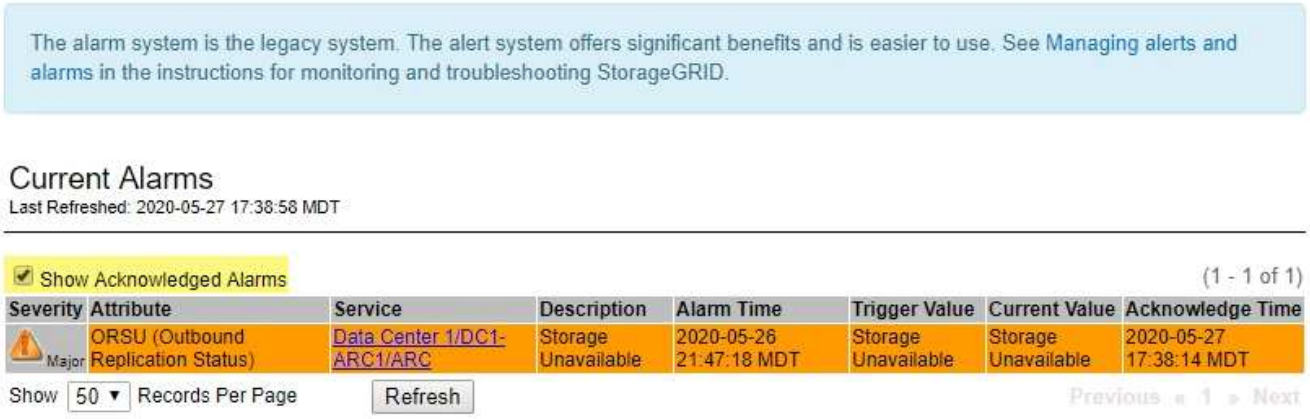
   确认警报后，确认不会复制到其他管理节点。因此，如果您从另一个管理节点查看信息板，则可能仍会看到活动警报。

4. 根据需要查看已确认的警报。

   a. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。

   b. 选择 * 显示已确认警报 * 。

      此时将显示任何已确认的警报。



查看默认警报（旧系统）

您可以查看所有默认旧警报的列表。

您需要的内容

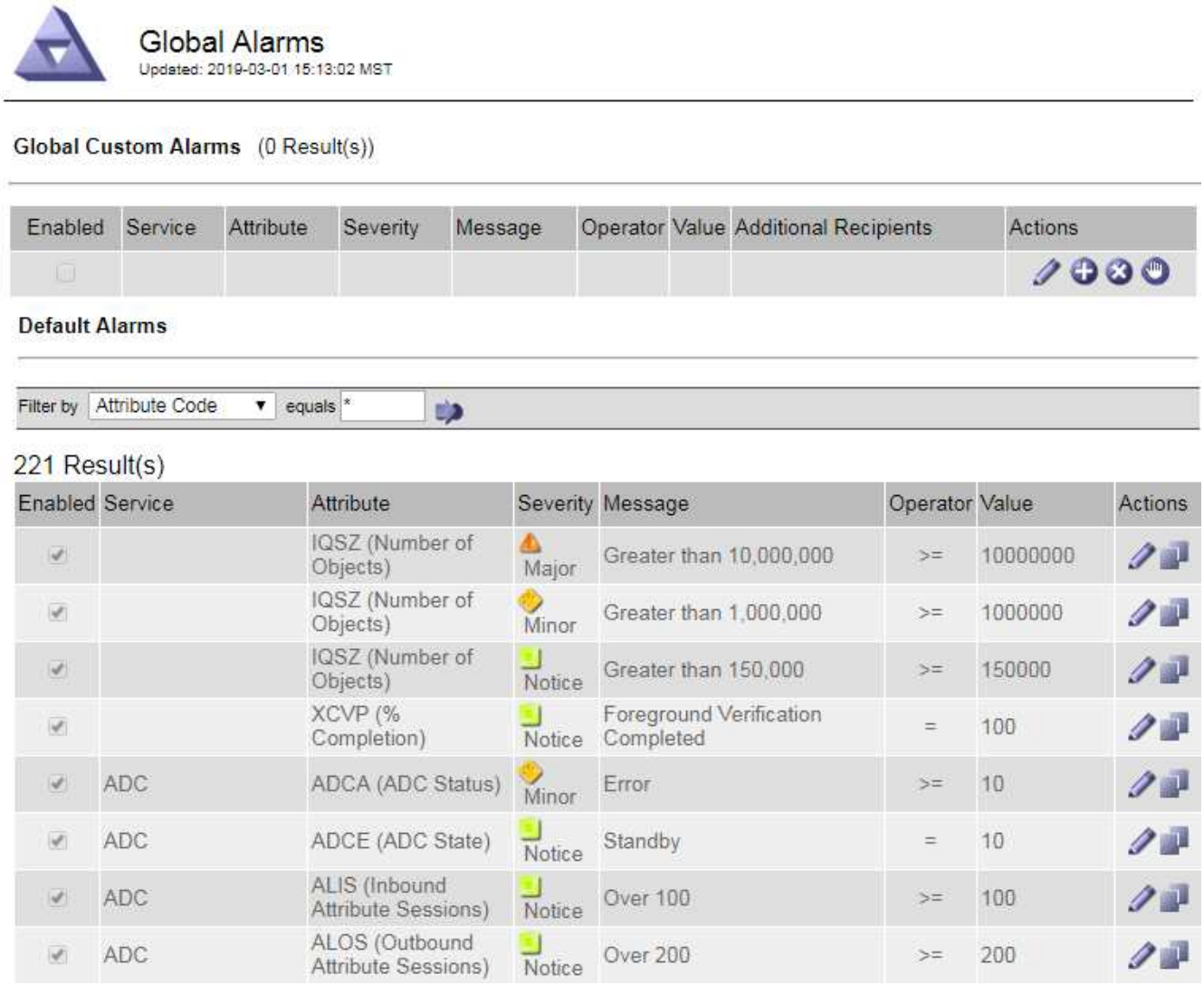
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 对于 Filter by ，选择 * 属性代码 * 或 * 属性名称 * 。
3. 对于等于，输入星号： `*`
4. 单击箭头 或按 * 输入 * 。

   此时将列出所有默认警报。



查看历史警报和警报频率（传统系统）

对问题描述 进行故障排除时，您可以查看过去触发传统警报的频率。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 按照以下步骤获取一段时间内触发的所有警报的列表。
   a. 选择 * 支持 * > * 警报（原有） * > * 历史警报 * 。
   b. 执行以下操作之一：
      - 单击一个时间段。
      - 输入自定义范围，然后单击 * 自定义查询 * 。
2. 按照以下步骤了解针对特定属性触发警报的频率。
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 ***GRID NODE*** > * 服务或组件 _* > * 警报 * > * 历史记录 * 。
   c. 从列表中选择属性。
   d. 执行以下操作之一：
      - 单击一个时间段。
      - 输入自定义范围，然后单击 * 自定义查询 * 。

      警报按时间倒序列出。
   e. 要返回到警报历史记录请求表单，请单击 * 历史记录 * 。

创建全局自定义警报（旧系统）

您可能已对旧系统使用全局自定义警报来满足特定监控要求。全局自定义警报可能具有覆盖默认警报的警报级别，或者它们可能会监控没有默认警报的属性。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

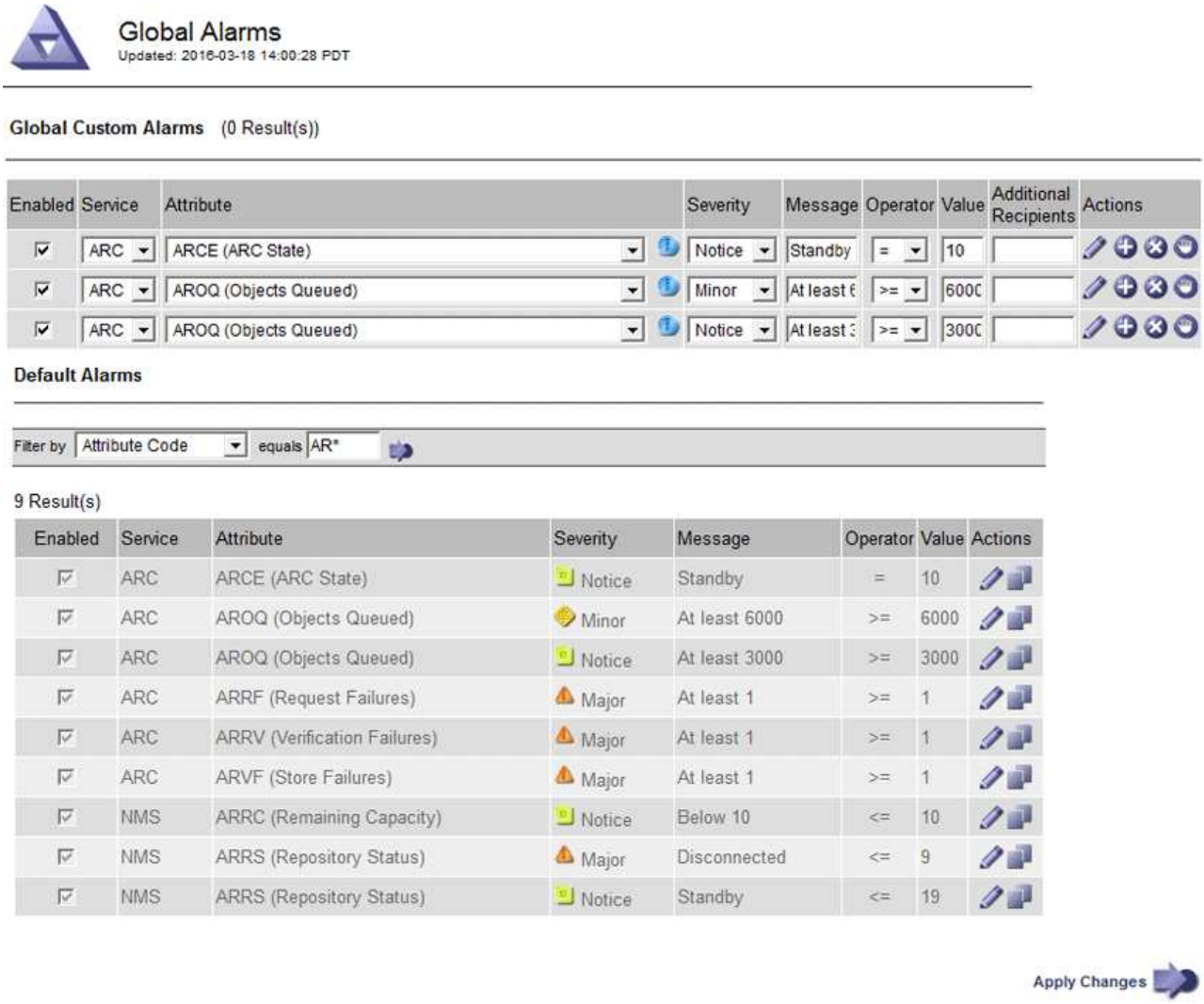
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

全局自定义警报会覆盖默认警报。除非绝对必要，否则不应更改默认警报值。通过更改默认警报，您将面临隐藏可能触发警报的问题的风险。

如果更改警报设置，请务必小心。例如，如果您增加警报的阈值，则可能无法检测到潜在问题。在更改警报设置之前，请与技术支持讨论您建议的更改。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 向全局自定义警报表添加新行：
   - 要添加新警报，请单击 * 编辑 * （如果这是第一个条目）或 * 插入 * 。



- 要修改默认警报，请搜索默认警报。
  i. 在 Filter by 下，选择 * 属性代码 * 或 * 属性名称 * 。
  ii. 键入搜索字符串。

  指定四个字符或使用通配符（例如， a？？？？？ 或 AB* ）。星号（ * ）表示多个字符，问号（？ ） 表示单个字符。

  iii. 单击箭头，或按 * 输入 * 。
  iv. 在结果列表中，单击 * 复制 * 要修改的警报旁边。

  默认警报将复制到全局自定义警报表。

3. 对全局自定义警报设置进行任何必要的更改：

标题	Description
enabled	选中或取消选中此复选框可启用或禁用警报。

标题	Description
属性	从适用于选定服务或组件的所有属性列表中选择要监控的属性的名称和代码。要显示有关属性的信息，请单击 * 信息 * 属性名称旁边。
severity	指示警报级别的图标和文本。
message	警报的原因（连接丢失，存储空间低于 10% 等）。
运算符	用于根据值阈值测试当前属性值的运算符： • = 等于 • > 大于 • 小于 • >= 大于或等于 • <= 小于或等于 • ≠不等于
价值	用于使用运算符根据属性的实际值测试的警报阈值。此条目可以是单个数字，使用冒号（ 1 ： 3 ）指定的数字范围，也可以是以逗号分隔的数字和范围列表。
其他收件人	触发警报时要通知的电子邮件地址的补充列表。这是对 * 警报 * > * 电子邮件设置 * 页面上配置的邮件列表的补充。列表以逗号分隔。 • 注： * 邮件列表需要设置 SMTP 服务器才能运行。在添加邮件列表之前，请确认已配置 SMTP 。自定义警报通知可以覆盖全局自定义或默认警报的通知。
操作	控制按钮用于： 编辑行 + 插入一行 + 删除行 + 上下拖放一行 + 复制行

4. 单击 * 应用更改 * 。

禁用警报（旧系统）

默认情况下，原有警报系统中的警报处于启用状态，但您可以禁用不需要的警报。您还可以在完全过渡到新警报系统后禁用原有警报。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

禁用默认警报（传统系统）

您可以为整个系统禁用一个原有的默认警报。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

如果为当前已触发警报的属性禁用警报，则不会清除当前警报。下次属性超过警报阈值时，警报将被禁用，您也可以清除触发的警报。

在完全过渡到新警报系统之前，请勿禁用任何原有警报。否则，在无法完成关键操作之前，您可能无法检测到底层问题。

步骤

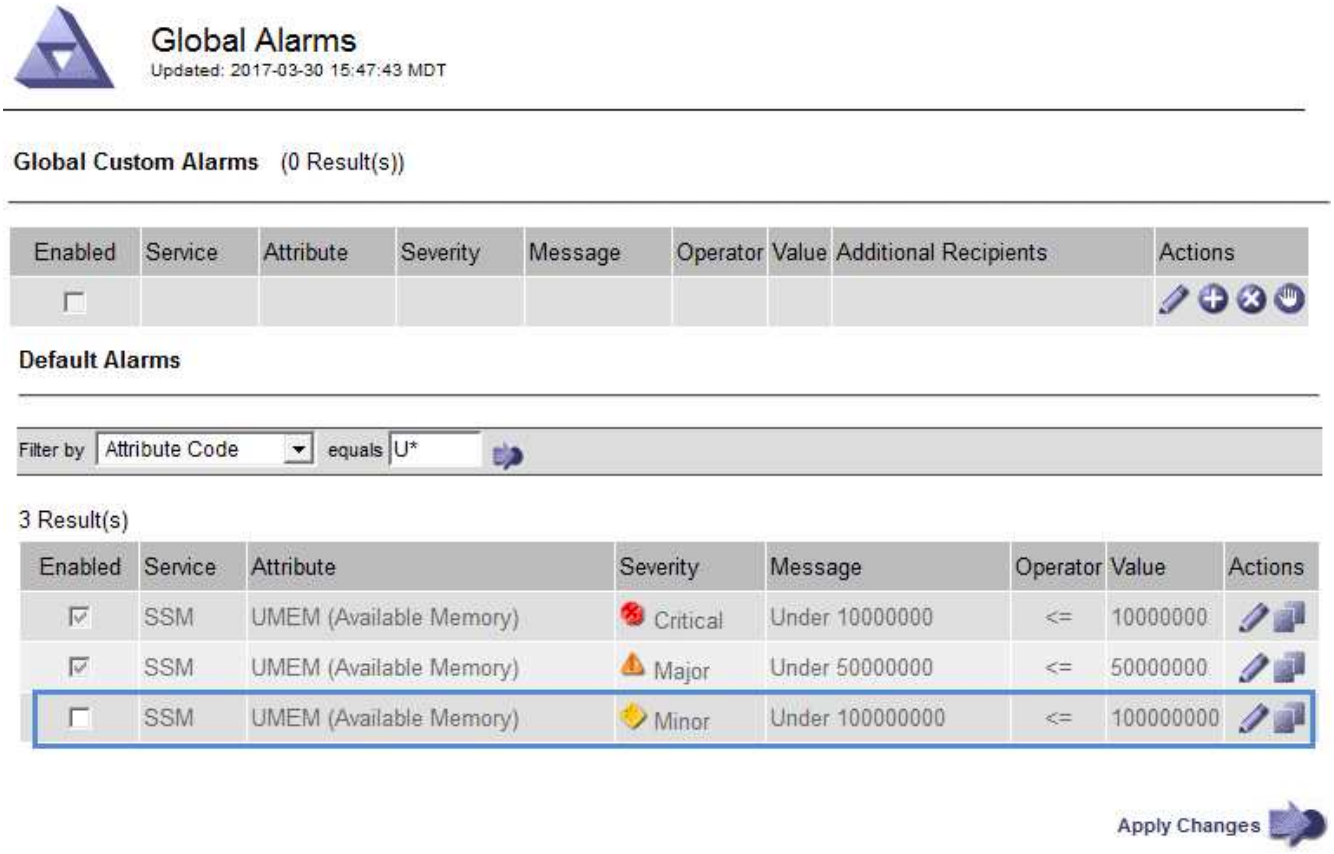
1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 搜索要禁用的默认警报。
   a. 在默认警报部分中，选择 * 筛选依据 * > * 属性代码 * 或 * 属性名称 * 。
   b. 键入搜索字符串。

      指定四个字符或使用通配符（例如， a？？？？？ 或 AB* ）。星号（ * ）表示多个字符，问号（？） 表示单个字符。

   c. 单击箭头 ，或按 * 输入 * 。

      选择 * 已禁用默认值 * 将显示当前已禁用的所有默认警报的列表。

3. 在搜索结果表中，单击编辑图标  要禁用的警报。



选定警报的 * 已启用 * 复选框将变为活动状态。

4. 取消选中 * 已启用 * 复选框。
5. 单击 * 应用更改 * 。

   默认警报已禁用。

禁用全局自定义警报（旧系统）

您可以为整个系统禁用旧版全局自定义警报。

您需要的内容

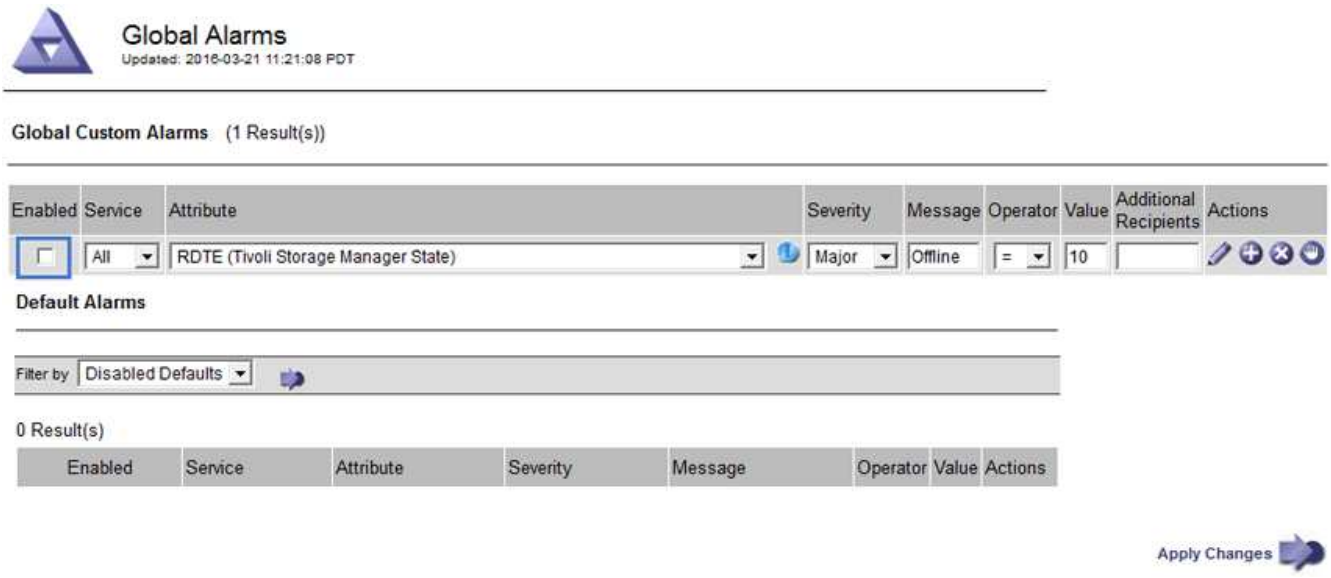
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

如果为当前已触发警报的属性禁用警报，则不会清除当前警报。下次属性超过警报阈值时，警报将被禁用，您也可以清除触发的警报。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 在全局自定义警报表中，单击 * 编辑 * 要禁用的警报旁边。
3. 取消选中 * 已启用 * 复选框。



4. 单击 * 应用更改 * 。

   已禁用全局自定义警报。

清除触发的警报（旧系统）

如果触发了旧警报，您可以清除它，而不是确认它。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

如果为当前已触发警报的属性禁用警报，则不会清除此警报。下次更改属性时，此警报将被禁用。您可以确认警报，或者，如果您希望立即清除警报，而不是等待属性值发生更改（从而导致警报状态发生更改），则可以清除触发的警报。如果您希望立即针对某个属性清除警报，而该属性的值不会经常更改（例如，状态属性），则此功能可能会很有用。

1. 禁用警报。
2. 登录到主管理节点：
   a. 输入以下命令： ` *ssh admin@primary_Admin_Node_IP*`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
3. 重新启动 NMS 服务： `sservice nms restart`
4. 从管理节点中注销： `exit`

   警报已清除。

StorageGRID 系统可以自动发送电子邮件和 SNMP 通知 触发警报或服务状态发生变化时。

默认情况下，不会发送警报电子邮件通知。对于电子邮件通知，您必须配置电子邮件服务器并指定电子邮件收件人。对于 SNMP 通知，您必须配置 SNMP 代理。

警报通知类型（旧系统）

触发传统警报时， StorageGRID 系统会发送两种类型的警报通知：严重性级别和服务状态。

严重性级别通知

在选定严重性级别触发旧警报时，系统会发送警报电子邮件通知：

- 通知
- 次要
- major
- 严重

邮件列表将接收与选定严重性的警报相关的所有通知。当警报离开警报级别时，也会发送通知—解决或输入其他警报严重性级别。

服务状态通知

服务（例如 LDR 服务或 NMS 服务）进入选定服务状态以及离开选定服务状态时，系统会发送服务状态通知。服务状态通知在服务进入或离开以下服务状态之一时发送：

- 未知
- 已管理员关闭

邮件列表将接收与选定状态下的更改相关的所有通知。

为警报配置电子邮件服务器设置（旧系统）

如果您希望 StorageGRID 在触发旧警报时发送电子邮件通知，则必须指定 SMTP 邮件服务器设置。StorageGRID 系统仅发送电子邮件，无法接收电子邮件。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

使用这些设置可以定义用于传统警报电子邮件通知和 AutoSupport 电子邮件消息的 SMTP 服务器。这些设置不用于警报通知。

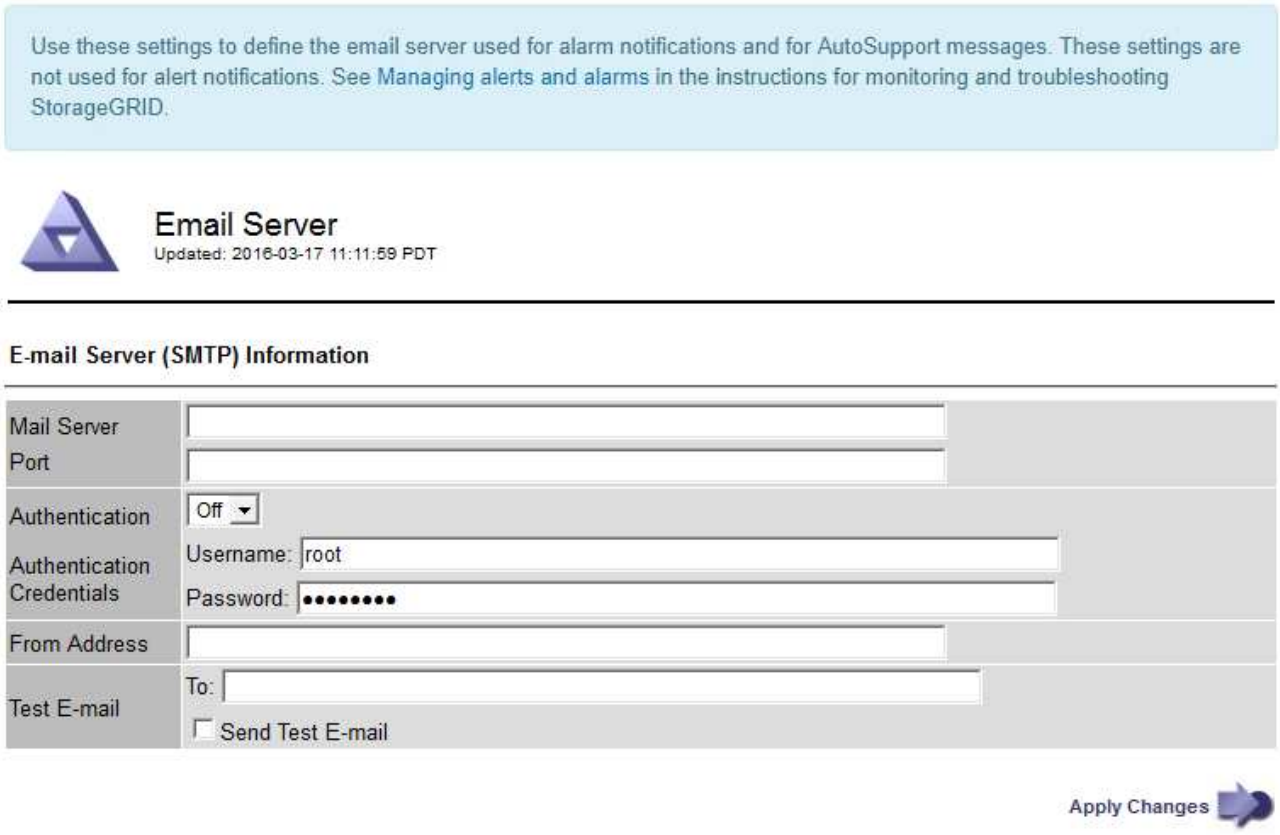
> 如果使用 SMTP 作为 AutoSupport 消息的协议，则可能已配置 SMTP 邮件服务器。同一个 SMTP 服务器用于警报电子邮件通知，因此您可以跳过此操作步骤 。请参见 有关管理 StorageGRID 的说明。

SMTP 是唯一支持发送电子邮件的协议。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。
2. 从电子邮件菜单中，选择 * 服务器 * 。

   此时将显示电子邮件服务器页面。此页面还用于为 AutoSupport 消息配置电子邮件服务器。



3. 添加以下 SMTP 邮件服务器设置：

项目	Description
邮件服务器	SMTP 邮件服务器的 IP 地址。如果先前已在管理节点上配置了 DNS 设置，则可以输入主机名而不是 IP 地址。
Port	用于访问 SMTP 邮件服务器的端口号。
身份验证	允许对 SMTP 邮件服务器进行身份验证。默认情况下，身份验证处于关闭状态。
身份验证凭据	SMTP 邮件服务器的用户名和密码。如果身份验证设置为 on ，则必须提供用于访问 SMTP 邮件服务器的用户名和密码。

4. 在 * 发件人地址 * 下，输入 SMTP 服务器将识别为发送电子邮件地址的有效电子邮件地址。这是用于发送电子邮件的官方电子邮件地址。

5. （可选）发送测试电子邮件以确认 SMTP 邮件服务器设置正确无误。

   a. 在 * 测试电子邮件 * > * 至 * 框中，添加一个或多个可访问的地址。

      您可以输入一个电子邮件地址或一个逗号分隔的电子邮件地址列表。由于 NMS 服务在发送测试电子邮件时不会确认成功或失败，因此您必须能够检查测试收件人的收件箱。

   b. 选择 * 发送测试电子邮件 * 。

6. 单击 * 应用更改 * 。

   此时将保存 SMTP 邮件服务器设置。如果您为测试电子邮件输入了信息，则会发送该电子邮件。测试电子邮件会立即发送到邮件服务器，而不会通过通知队列发送。在具有多个管理节点的系统中，每个管理节点都会发送一封电子邮件。收到测试电子邮件将确认 SMTP 邮件服务器设置正确，并且 NMS 服务已成功连接到邮件服务器。NMS 服务和邮件服务器之间的连接问题会在次要严重性级别触发旧的分钟（ NMS 通知状态）警报。

创建警报电子邮件模板（旧系统）

通过电子邮件模板，您可以自定义旧警报电子邮件通知的页眉，页脚和主题行。您可以使用电子邮件模板向不同的邮件列表发送包含相同正文的唯一通知。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

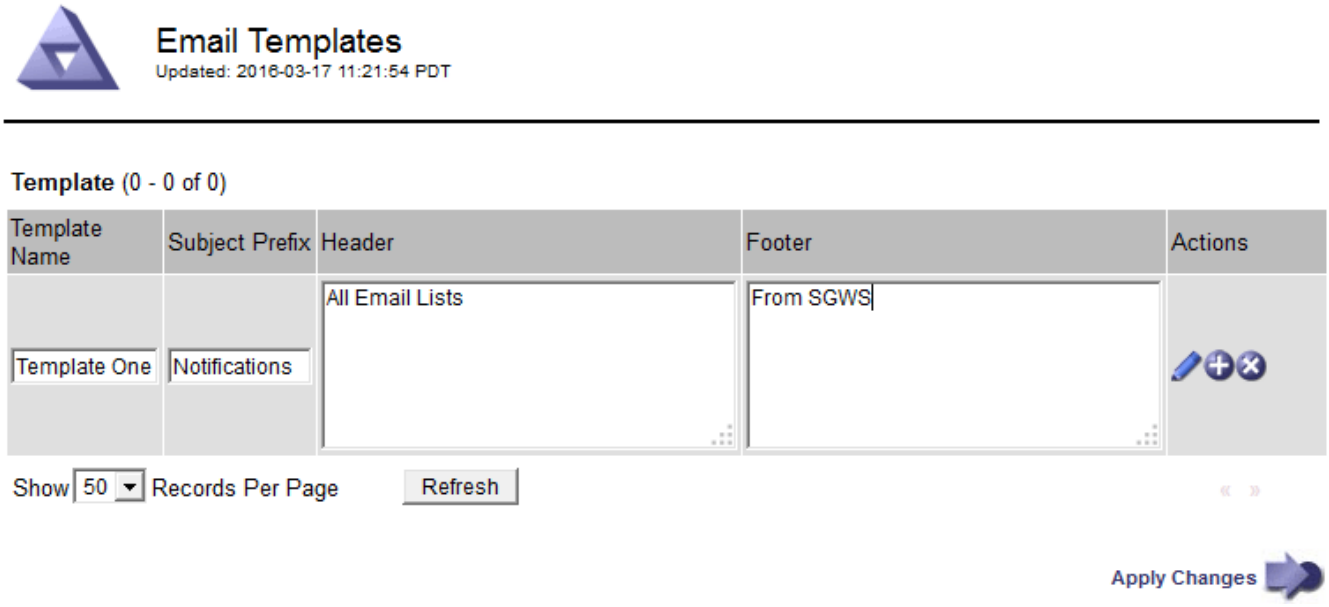
关于此任务

使用这些设置可以定义用于旧警报通知的电子邮件模板。这些设置不用于警报通知。

不同的邮件列表可能需要不同的联系信息。模板不包含电子邮件的正文。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。
2. 从电子邮件菜单中，选择 * 模板 * 。
3. 单击 * 编辑 * 。  （或 * 插入 *  如果这不是第一个模板）。



4. 在新行中添加以下内容：

项目	Description
模板名称	用于标识模板的唯一名称。模板名称不能重复。
主题前缀	可选。将显示在电子邮件主题行开头的前缀。前缀可用于轻松配置电子邮件筛选器和组织通知。
标题	可选。显示在电子邮件正文开头的标题文本。可以使用标题文本在电子邮件内容的前面添加公司名称和地址等信息。
页脚	可选。显示在电子邮件正文末尾的页脚文本。可以使用页脚文本关闭包含提醒信息的电子邮件，例如联系人电话号码或网站链接。

5. 单击 * 应用更改 * 。

   此时将为通知添加一个新模板。

为警报通知创建邮件列表（旧系统）

通过邮件列表，您可以在触发旧警报或服务状态发生变化时通知收件人。您必须至少创建一个邮件列表，然后才能发送任何警报电子邮件通知。要向单个收件人发送通知，请使用一个电子邮件地址创建一个邮件列表。

您需要的内容

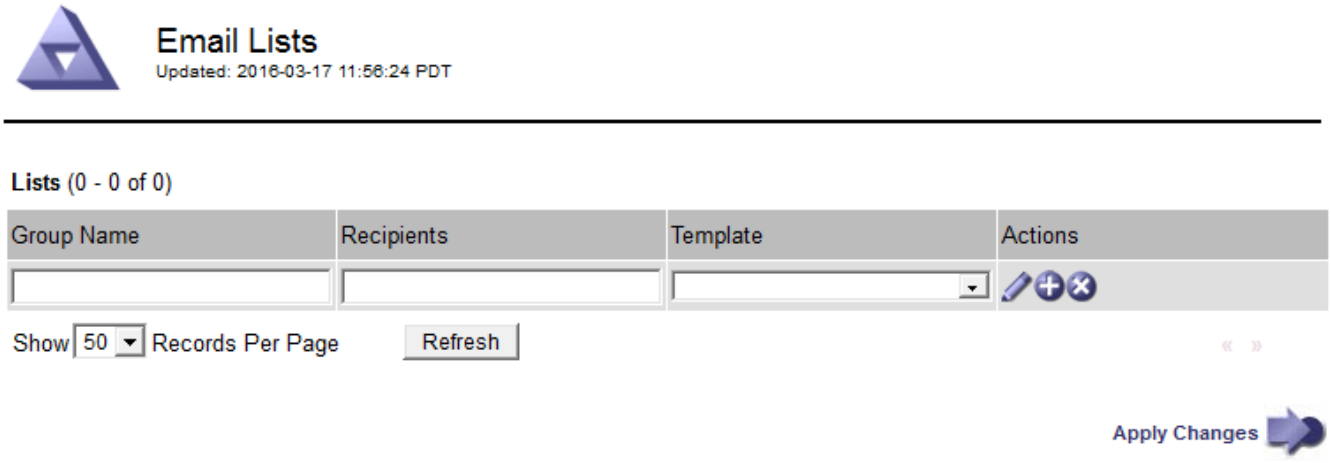
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 如果要为邮件列表指定电子邮件模板（自定义页眉，页脚和主题行），则必须已创建此模板。

关于此任务

使用这些设置可以定义用于旧警报电子邮件通知的邮件列表。这些设置不用于警报通知。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。
2. 从电子邮件菜单中，选择 * 列表 * 。
3. 单击 * 编辑 * 。 （或 * 插入 * 如果这不是第一个邮件列表）。



4. 在新行中，添加以下内容：

项目	Description
组名称	用于标识邮件列表的唯一名称。邮件列表名称不能重复。 • 注意： * 如果更改了邮件列表的名称，则此更改不会传播到使用邮件列表名称的其他位置。您必须手动更新所有已配置的通知，才能使用新的邮件列表名称。
收件人	单个电子邮件地址，先前配置的邮件列表或将通知发送到的电子邮件地址和邮件列表的逗号分隔列表。 • 注意： * 如果电子邮件地址属于多个邮件列表，则在发生通知触发事件时仅发送一封电子邮件通知。
模板	或者，也可以选择一个电子邮件模板，以便向发送给此邮件列表的所有收件人的通知添加唯一的页眉，页脚和主题行。

5. 单击 * 应用更改 * 。

   此时将创建一个新的邮件列表。

配置警报电子邮件通知（旧系统）

要接收旧警报系统的电子邮件通知，收件人必须是邮件列表的成员，并且必须将该列表添加到通知页面。通知配置为仅在触发具有指定严重性级别的警报或服务状态发生更改时才向收件人发送电子邮件。因此，收件人只会收到需要接收的通知。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须已配置电子邮件列表。

关于此任务

使用这些设置为旧警报配置通知。这些设置不用于警报通知。

如果某个电子邮件地址（或列表）属于多个邮件列表，则在发生通知触发事件时仅会发送一封电子邮件通知。例如，可以将组织中的一组管理员配置为接收所有警报的通知，而不管严重性如何。另一个组可能只需要针对严重性为 " 严重 " 的警报发出通知。您可以同时属于这两个列表。如果触发严重警报，您只会收到一条通知。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。
2. 从电子邮件菜单中，选择 * 通知 * 。
3. 单击 * 编辑 * 。 （或 * 插入 * 如果这不是第一个通知）。
4. 在电子邮件列表下，选择邮件列表。
5. 选择一个或多个警报严重性级别和服务状态。
6. 单击 * 应用更改 * 。

   触发或更改具有选定警报严重性级别或服务状态的警报时，系统会向邮件列表发送通知。

禁止发送邮件列表的警报通知（旧系统）

如果您不再希望邮件列表接收有关警报的通知，则可以禁止此邮件列表的警报通知。例如，在过渡到使用警报电子邮件通知后，您可能希望禁止有关旧警报的通知。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

使用这些设置可禁止向原有警报系统发送电子邮件通知。这些设置不适用于警报电子邮件通知。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。
2. 从电子邮件菜单中，选择 * 通知 * 。
3. 单击 * 编辑 * 。 要禁止其通知的邮件列表旁边。
4. 在禁止下，选中要禁止的邮件列表旁边的复选框，或者选择列顶部的 * 禁止 * 以禁止所有邮件列表。
5. 单击 * 应用更改 * 。

   选定邮件列表将禁止使用旧警报通知。

在系统范围内禁止电子邮件通知

您可以阻止 StorageGRID 系统针对旧警报和事件触发的 AutoSupport 消息发送电子邮件通知。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

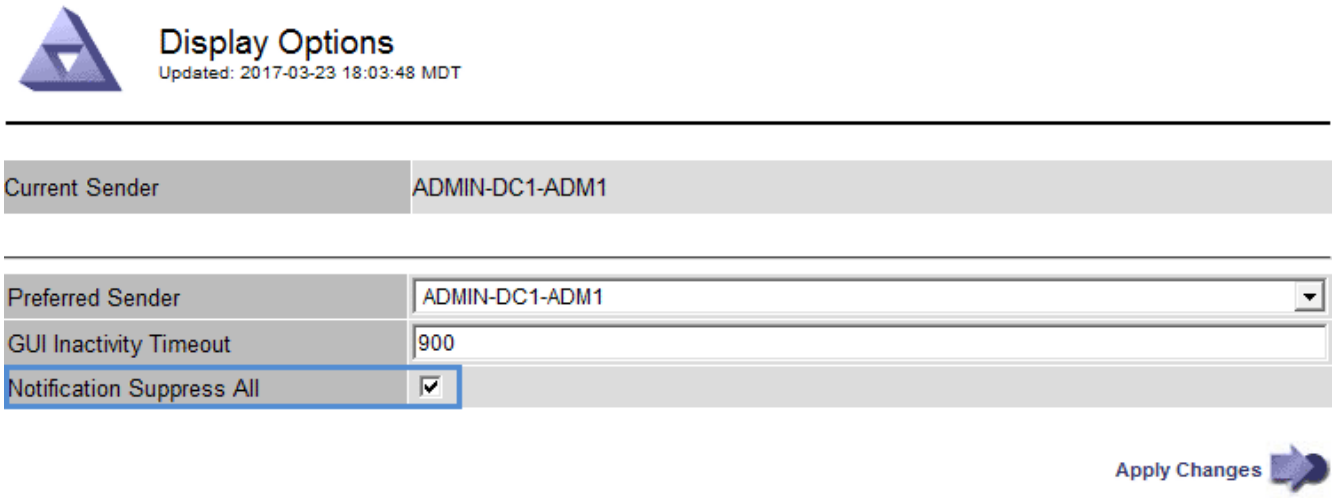
关于此任务

使用此选项可禁止对原有警报和事件触发的 AutoSupport 消息发送电子邮件通知。

此选项不会禁止警报电子邮件通知。它也不会禁止每周或用户触发的 AutoSupport 消息。

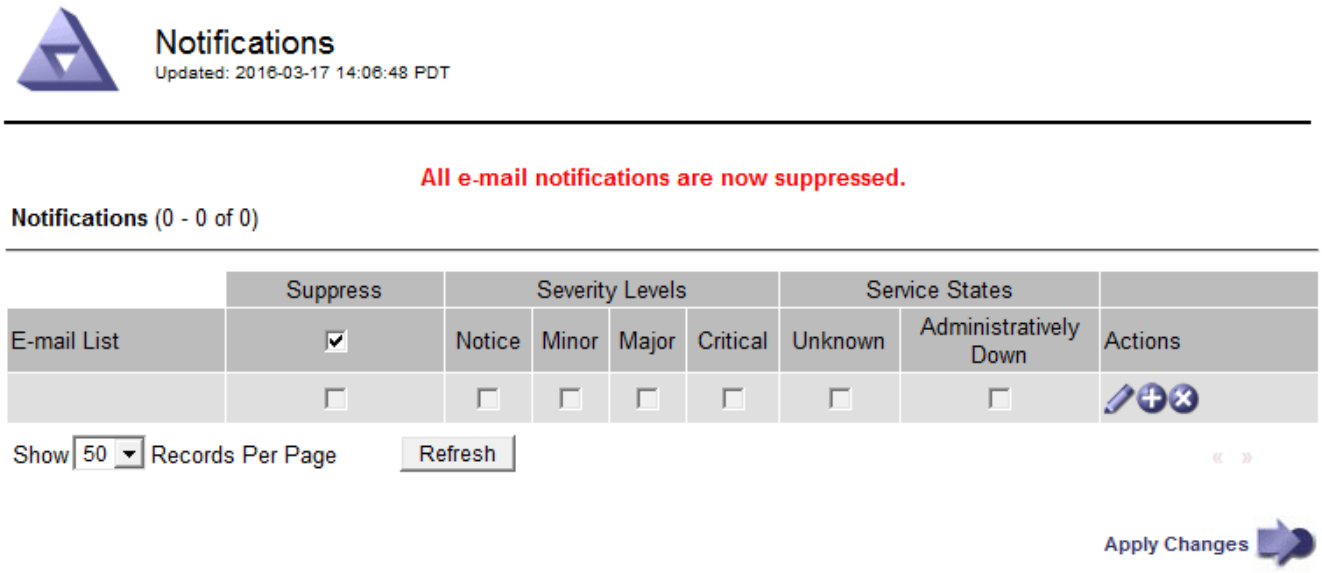
步骤

1. 选择 * 配置 * > * 系统设置 * > * 显示选项 * 。
2. 从显示选项菜单中，选择 * 选项 * 。
3. 选择 * 通知禁止全部 * 。



4. 单击 * 应用更改 * 。

通知页面（ * 配置 * > * 通知 * ）显示以下消息：



配置审核消息和日志目标

审核消息和日志可记录系统活动和安全事件，是监控和故障排除的重要工具。您可以调整审核级别以增加或减少记录的审核消息的类型和数量。您也可以定义要包含在客户端读取和写入审核消息中的任何 HTTP 请求标头。您还可以配置外部系统日志服务器并更改审核信息的目标。

有关审核消息的详细信息，请参见 查看审核日志。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。

关于此任务

所有 StorageGRID 节点都会生成审核消息和日志，以跟踪系统活动和事件。默认情况下，审核信息会发送到管理节点上的审核日志。您可以调整审核级别以增加或减少审核日志中记录的审核消息的类型和数量。您也可以将审核信息配置为发送到远程系统日志服务器或临时存储在源节点上以手动收集。

更改审核日志中的审核消息级别

您可以为审核日志中的以下每种消息设置不同的审核级别：

审核类别	**Description**
系统	默认情况下，此级别设置为 " 正常 " 。请参见 系统审核消息。
存储	默认情况下，此级别设置为 Error 。请参见 对象存储审核消息。
管理	默认情况下，此级别设置为 " 正常 " 。请参见 管理审核消息。
客户端读取	默认情况下，此级别设置为 " 正常 " 。请参见 客户端读取审核消息。

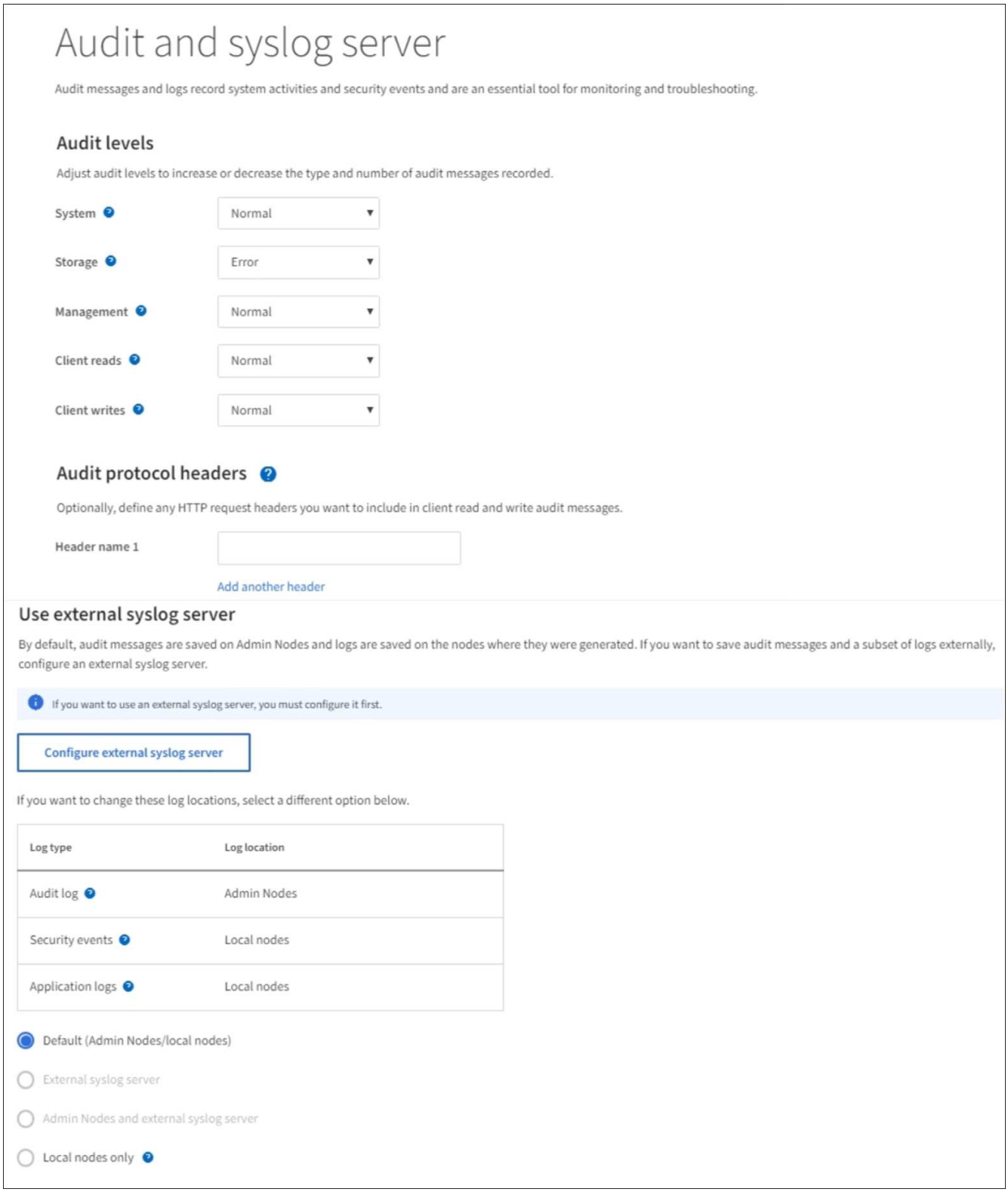
审核类别	Description
客户端写入	默认情况下，此级别设置为 " 正常 " 。请参见 客户端写入审核消息。

如果您最初使用 10.3 或更高版本安装 StorageGRID ，则这些默认设置适用。如果您已从早期版本的 StorageGRID 升级，则所有类别的默认值均设置为正常。

升级期间，审核级别配置不会立即生效。

步骤

1. 选择 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。



2. 对于每个审核消息类别，从下拉列表中选择一个审核级别：

审核级别	Description
关闭	不会记录此类别中的任何审核消息。

审核级别	Description
error	仅会记录错误消息—审核结果代码不是 " 成功 " （ SUC ）的消息。
正常	系统会记录标准事务处理消息，即这些说明中针对此类别列出的消息。
调试	已弃用。此级别的行为与正常审核级别相同。

对于任何特定级别，包含的消息都包括那些将在较高级别记录的消息。例如，正常级别包括所有错误消息。

3. 或者，在 * 审核协议标头 * 下，定义要包含在客户端读取和写入审核消息中的任何 HTTP 请求标头。使用星号（ * ）作为通配符，以匹配零个或多个字符。使用转义序列（ * ）匹配文字星号。

   审核协议标头仅适用于 S3 和 Swift 请求。

4. 如果需要，选择 * 添加另一个标题 * 以创建其他标题。

   在请求中找到 HTTP 标头后，它们将包含在审核消息中的字段 HTRH 下。

   只有当 * 客户端读取 * 或 * 客户端写入 * 的审核级别不是 * 关闭 * 时，才会记录审核协议请求标头。

5. 选择 * 保存 *

   此时将显示一个绿色横幅，指示您的配置已成功保存。

使用外部系统日志服务器

如果要远程保存审核信息，可以配置外部系统日志服务器。

- 如果要将审核信息保存到外部系统日志服务器，请转至 配置外部系统日志服务器。
- 如果您不使用外部系统日志服务器，请转至 选择审核信息目标。

选择审核信息目标

您可以指定将审核日志，安全事件日志和应用程序日志发送到何处。

只有在使用外部系统日志服务器时，某些目标才可用。请参见 配置外部系统日志服务器 配置外部系统日志服务器。

有关 StorageGRID 软件日志的详细信息，请参见 StorageGRID 软件日志。

1. 在 Audit and syslog server 页面上，从列出的选项中选择审核信息的目标：

选项	Description
默认（管理节点 / 本地节点）	审核消息会发送到管理节点上的审核日志（`audit.log`），而安全事件日志和应用程序日志会存储在生成它们的节点（也称为 " 本地节点 " ）上。
外部系统日志服务器	审核信息将发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。
管理节点和外部系统日志服务器	审核消息会发送到管理节点上的审核日志（`audit.log`），审核信息会发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。
仅限本地节点	不会向管理节点或远程系统日志服务器发送任何审核信息。审核信息仅保存在生成该信息的节点上。 • 注 * ： StorageGRID 会定期轮换删除这些本地日志以释放空间。当节点的日志文件达到 1 GB 时，系统将保存现有文件并启动新的日志文件。日志的轮换限制为 21 个文件。创建日志文件的第 22 版时，将删除最早的日志文件。每个节点平均存储约 20 GB 的日志数据。

在每个本地节点上生成的审核信息存储在 ` /var/local/log/localaudit.log` 中

1. 选择 * 保存 * 。

此时将显示一条警告消息：

是否更改日志目标?

1. 选择 * 确定 * 以确认要更改审核信息的目标。

   此时将显示一个绿色横幅，通知您已成功保存审核配置。

   新日志将发送到选定的目标。现有日志将保留在其当前位置。

相关信息

外部系统日志服务器的注意事项

管理 StorageGRID

对外部系统日志服务器进行故障排除

使用外部系统日志服务器

外部系统日志服务器的注意事项

请按照以下准则估算所需外部系统日志服务器的大小。

什么是外部系统日志服务器?

外部系统日志服务器是 StorageGRID 外部的服务器，您可以使用它在一个位置收集系统审核信息。通过使用外部系统日志服务器，您可以配置审核信息的目标，以便减少管理节点上的网络流量并更高效地管理信息。可以发送到外部系统日志服务器的审核信息类型包括：

- 包含在正常系统操作期间生成的审核消息的审核日志
- 与安全相关的事件，例如登录和上报给 root
- 如果需要创建支持案例以对遇到的问题描述 进行故障排除，则可能需要请求的应用程序日志

如何估算外部系统日志服务器的大小

通常，您的网格会进行规模估算，以达到所需的吞吐量，该吞吐量是按每秒 S3 操作数或每秒字节数定义的。例如，您可能要求网格每秒处理 1 ， 000 次 S3 操作，或者每秒处理 2 ， 000 MB 的对象载入和检索。您应根据网格的数据要求调整外部系统日志服务器的大小。

本节提供了一些启发式公式，可帮助您估算外部系统日志服务器需要能够处理的各种类型的日志消息的速率和平均大小，这些消息以网格的已知或所需性能特征（每秒 S3 操作数）表示。

在估计公式中使用每秒 **S3** 操作数

如果网格的大小以每秒字节为单位表示，则必须将此规模估算转换为每秒 S3 操作，才能使用估算公式。要转换网格吞吐量，您必须先确定平均对象大小，您可以使用现有审核日志和指标（如果有）中的信息或根据您对将使用 StorageGRID 的应用程序的了解来确定平均对象大小。例如，如果您的网格大小调整为可实现 2 ， 000 MB/秒的吞吐量，而您的平均对象大小为 2 MB ，则您的网格大小将调整为能够每秒处理 1 ， 000 次 S3 操作（ 2 ， 000 MB/ 2 MB ）。

> 以下各节中用于估算外部系统日志服务器规模的公式提供了常见案例估算（而不是最坏案例估算）。根据您的配置和工作负载，您可能会发现系统日志消息或系统日志数据卷的速率高于或低于公式的预测。这些公式仅供参考。

审核日志的估计公式

如果除了网格应支持的每秒 S3 操作数之外，您没有其他有关 S3 工作负载的信息，则可以使用以下公式估算外部系统日志服务器需要处理的审核日志卷， 假设您将审核级别设置为默认值（所有类别均设置为正常，但存储设置为错误除外）：

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

例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，则外部系统日志服务器的大小应为每秒支持 2 ， 000 条系统日志消息，并且应能够以每秒 1.6 MB 的速率接收（并且通常存储）审核日志数据。

如果您对工作负载有更多了解，可以进行更准确的估计。对于审核日志，最重要的附加变量是放置的 S3 操作的百分比（与获取）以及以下 S3 字段的平均大小（以字节为单位）（表中使用的 4 个字符缩写为审核日志字段名

称）：

代码	字段	Description
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。

让我们使用 P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

我们使用 K 表示 S3 帐户名称， S3 Bucket 和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。然后， K 值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器需要处理的审核日志卷，前提是您将审核级别设置为默认值（除存储外的所有类别均设置为正常）。 设置为 Error ）：

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

例如，如果您的网格大小为每秒 1 ， 000 次 S3 操作，则工作负载将占 50% ， S3 帐户名称，存储分段名称，对象名称平均为 90 字节，您的外部系统日志服务器应调整大小以支持每秒 1 ， 500 条系统日志消息，并且应能够以大约每秒 1 MB 的速率接收（并且通常存储）审核日志数据。

非默认审核级别的估计公式

为审核日志提供的公式假定使用默认审核级别设置（所有类别均设置为 " 正常 " ，但存储设置为 " 错误 " 除外）。无法使用详细的公式来估算非默认审核级别设置的审核消息的速率和平均大小。但是，可以使用下表粗略估算此速率； 您可以使用为审核日志提供的平均大小公式，但请注意，这可能会导致过度估计，因为 " 额外 " 审核消息平均小于默认审核消息。

条件	公式
Replication： Audit Levels all set to Debug or Normal	审核日志速率 = 8 x S3 操作速率
纠删编码：审核级别均设置为 " 调试 " 或 " 正常 "	使用与默认设置相同的公式

安全事件的估计公式

安全事件与 S3 操作无关，通常会生成可忽略不计的日志和数据卷。出于这些原因，不提供任何估计公式。

应用程序日志的估计公式

如果除了网格预期支持的每秒 S3 操作数之外，您没有其他有关 S3 工作负载的信息，则可以使用以下公式估算外部系统日志服务器需要处理的应用程序日志卷：

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

因此，例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，则外部系统日志服务器的大小应为每秒支持 3 ，300 个应用程序日志，并且能够以大约每秒 1.2 MB 的速率接收（和存储）应用程序日志数据。

如果您对工作负载有更多了解，可以进行更准确的估计。对于应用程序日志，最重要的附加变量是数据保护策略（复制与纠删编码），所执行 S3 操作的百分比（与GES/OTHER其他 ）以及以下 S3 字段的平均大小（以字节为单位）（表中使用的 4 个字符缩写是审核日志字段名称）：

代码	字段	**Description**
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。

规模估算示例

本节介绍了如何使用网格估算公式和以下数据保护方法的示例案例：

- Replication
- 纠删编码

如果使用复制来保护数据

Let P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

让 K 表示 S3 帐户名称， S3 Bucket 和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。K 的值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器必须能够处理的应用程序日志卷。

```
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
```

因此，例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，工作负载占用率为 50% ， S3 帐户名称，存储分段名称和对象名称平均为 90 字节，则外部系统日志服务器的大小应为每秒支持 1800 个应用程序日志。 并且将以每秒 0.5 MB 的速率接收（并通常存储）应用程序数据。

如果您使用纠删编码进行数据保护

Let P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

让 K 表示 S3 帐户名称， S3 Bucket 和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。K 的值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器必须能够处理的应用程序日志卷。

```
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
```

因此，例如，如果您的网格大小为每秒 1 ， 000 次 S3 操作，则您的工作负载为 50% ， S3 帐户名称，存储分段名称， 对象名称平均为 90 字节，您的外部系统日志服务器应调整大小以支持每秒 2 ， 250 个应用程序日志，并且应能够以每秒 0.6 MB 的速率接收并将其存储。

有关配置审核消息级别和外部系统日志服务器的详细信息，请参见以下内容：

- 配置外部系统日志服务器
- 配置审核消息和日志目标

配置外部系统日志服务器

如果要将审核日志，应用程序日志和安全事件日志保存到网格外部的位置，请使用此操作步骤 配置外部系统日志服务器。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您有一个能够接收和存储日志文件的系统日志服务器。有关详细信息，请参见 外部系统日志服务器的注意事项。
- 如果您计划使用 TLS 或 ROLP/TLS ，则您拥有正确的服务器和客户端认证。

关于此任务

如果要将审核信息发送到外部系统日志服务器，则必须先配置外部服务器。

通过将审核信息发送到外部系统日志服务器，您可以：

- 更高效地收集和管理审核信息，例如审核消息，应用程序日志和安全事件
- 减少管理节点上的网络流量，因为审核信息直接从各种存储节点传输到外部系统日志服务器，而无需通过管理节点

> 将日志发送到外部系统日志服务器时，超过 8192 字节的单个日志会在消息末尾截断，以符合外部系统日志服务器实施中的常见限制。

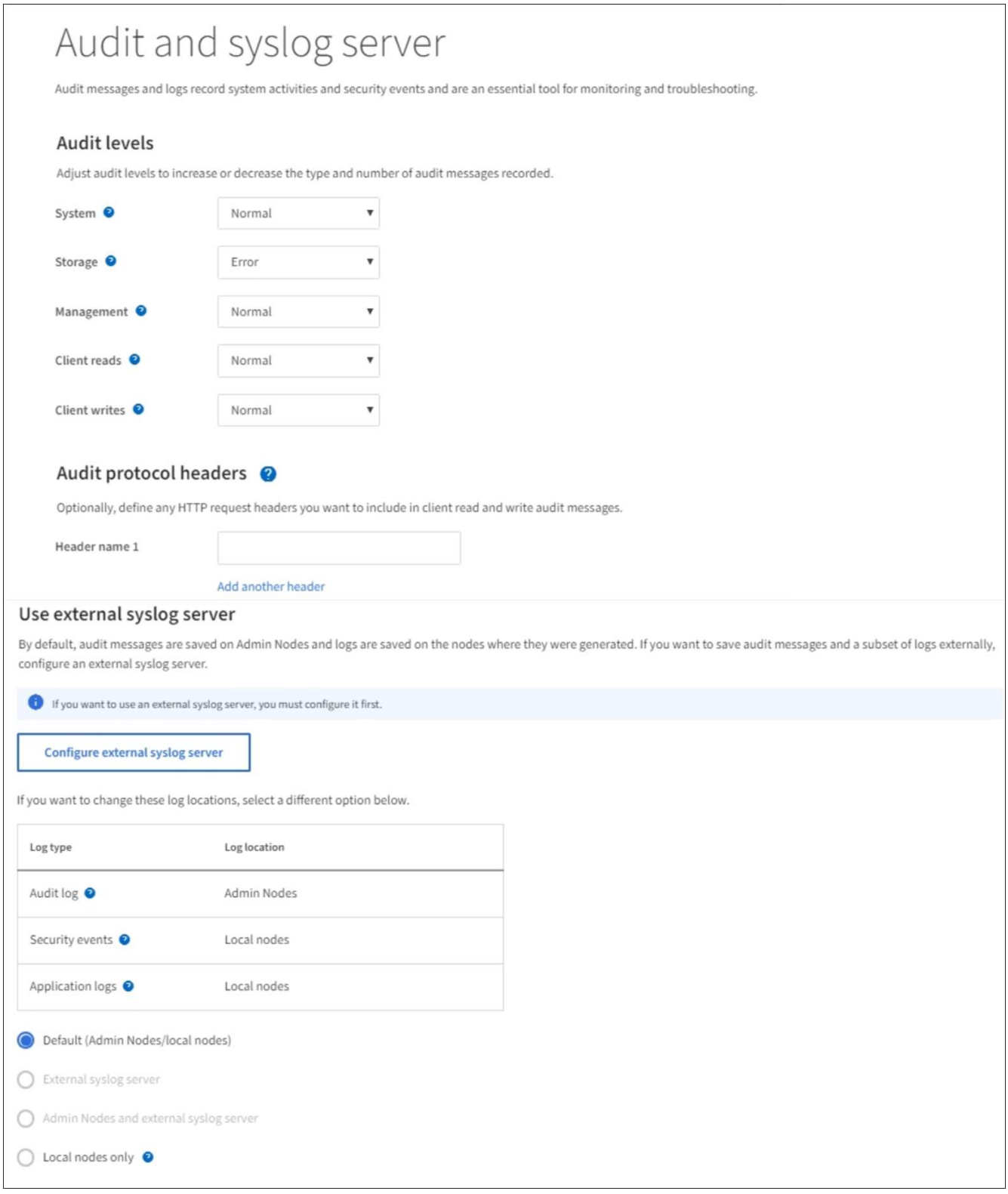
> 为了在外部系统日志服务器发生故障时最大程度地提高完整数据恢复的选项，每个节点上最多会保留 20 GB 的本地审核记录日志（ localaudit.log ）。

> 如果此操作步骤 中提供的配置选项不够灵活，无法满足您的要求，则可以使用专用 API `audit-destinations` 端点应用其他配置选项。例如，可以对不同的节点组使用不同的系统日志服务器。

访问系统日志服务器配置向导

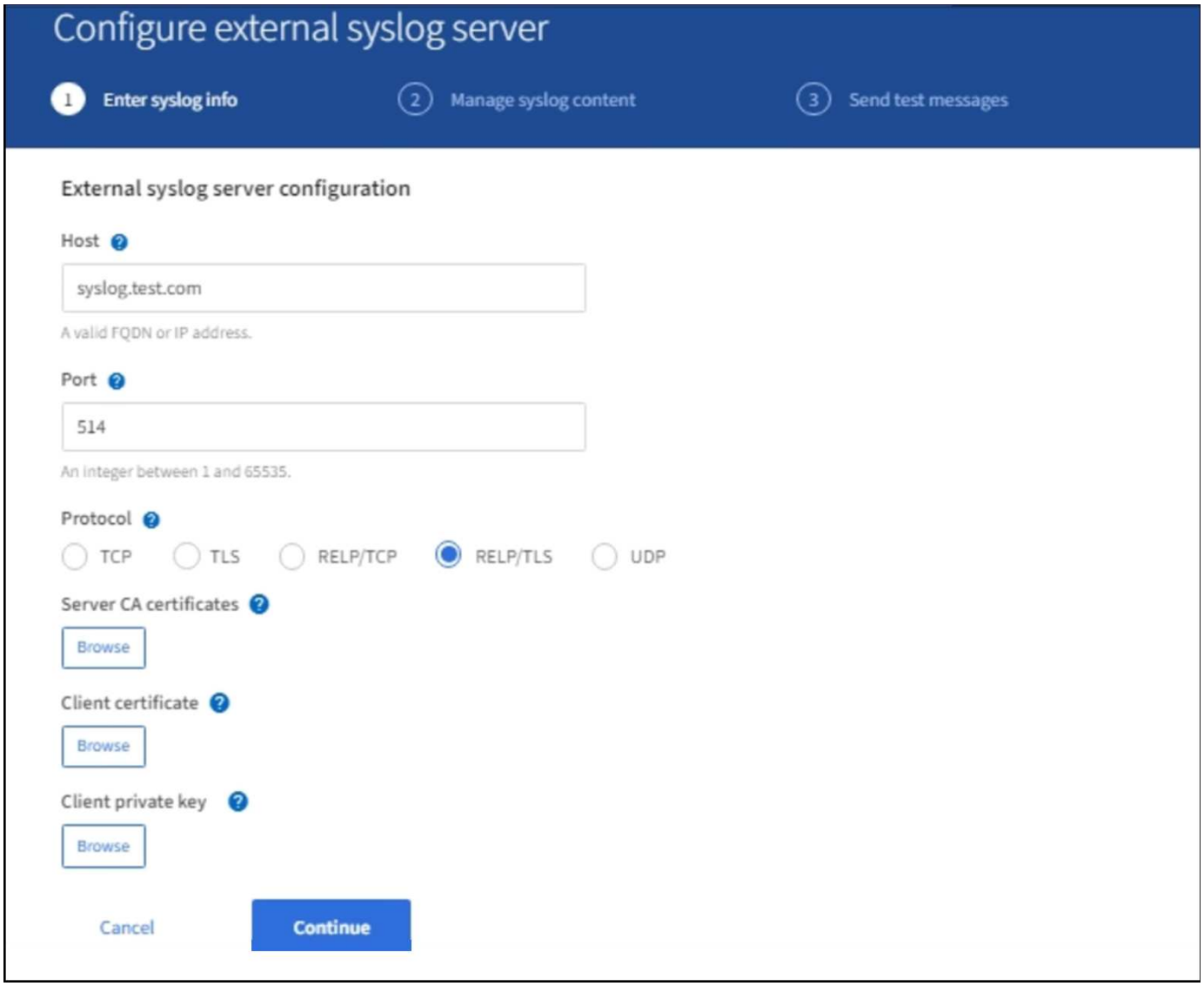
步骤

1. 选择 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。



2. 从 Audit and syslog server 页面中，选择 * 配置外部系统日志服务器 * 。如果先前已配置外部系统日志服务器，请选择 * 编辑外部系统日志服务器 * 。

输入系统日志信息



1. 在 * 主机 * 字段中输入外部系统日志服务器的有效完全限定域名或 IPv4 或 IPv6 地址。
2. 输入外部系统日志服务器上的目标端口（必须是介于 1 到 65535 之间的整数）。默认端口为 514 。
3. 选择用于向外部系统日志服务器发送审核信息的协议。

   建议使用 TLS 或 RELP/TLS 。您必须上传服务器证书才能使用其中任一选项。

   使用证书有助于确保网格与外部系统日志服务器之间的连接安全。有关详细信息，请参见 使用 StorageGRID 安全证书。

   所有协议选项都需要外部系统日志服务器的支持和配置。您必须选择与外部系统日志服务器兼容的选项。

   > 可靠事件日志记录协议（ Relp ）扩展了系统日志协议的功能，可提供可靠的事件消息传送。如果外部系统日志服务器必须重新启动，则使用 RELP 有助于防止审核信息丢失。

4. 选择 * 继续 * 。
5. 【附加证书】如果您选择了 * TLS * 或 * ROLP/TLS* ，请上传以下证书：

   ◦ * 服务器 CA 证书 * ：一个或多个用于验证外部系统日志服务器的可信 CA 证书（采用 PEM 编码）。如

果省略此参数，则会使用默认网格 CA 证书。您在此上传的文件可能是 CA 捆绑包。

- * 客户端证书 * ： 用于向外部系统日志服务器进行身份验证的客户端证书（采用 PEM 编码）。
- * 客户端专用密钥 * ： 客户端证书的专用密钥（采用 PEM 编码）。

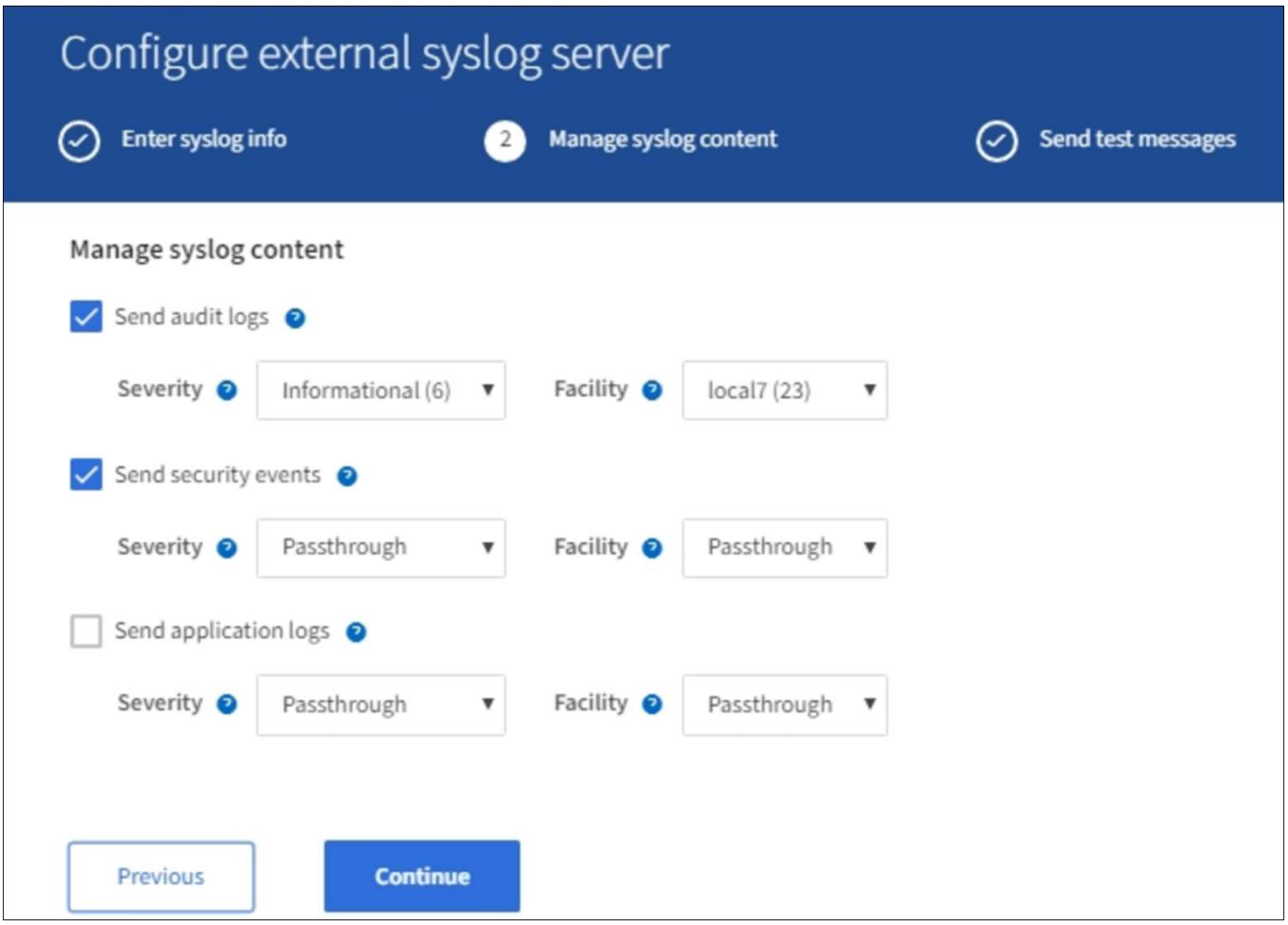
> 如果使用客户端证书，则还必须使用客户端专用密钥。如果您提供加密的私钥，则还必须提供密码短语。使用加密的私钥不会带来显著的安全优势，因为必须存储密钥和密码短语；为了简化操作，建议使用未加密的私钥（如果可用）。

i. 为要使用的证书或密钥选择 * 浏览 * 。
ii. 选择证书文件或密钥文件。
iii. 选择 * 打开 * 上传文件。

证书或密钥文件名称旁边会显示一个绿色复选框，通知您已成功上传此证书或密钥文件。

6. 选择 * 继续 * 。

管理系统日志内容



1. 选择要发送到外部系统日志服务器的每种审核信息。
   - * 发送审核日志 * ： StorageGRID 事件和系统活动
   - * 发送安全事件 * ： 安全事件，例如，未经授权的用户尝试登录或用户以 root 身份登录时

- * 发送应用程序日志 * ： 日志文件可用于故障排除，其中包括：
  - bycast-err.log
  - bycast.log
  - jaeger.log
  - nms.log （仅限管理节点）
  - prometheus.log
  - raft.log
  - hagroups.log

2. 使用下拉菜单为要发送的审核信息类别选择严重性和工具（消息类型）。

   如果为严重性和设备选择 * 直通 * ，则发送到远程系统日志服务器的信息将获得与本地登录到节点时相同的严重性和设备。设置工具和严重性可以帮助您以可自定义的方式聚合日志，以便于分析。

   有关 StorageGRID 软件日志的详细信息，请参见 StorageGRID 软件日志。

   a. 对于 * 严重性 * ，如果希望发送到外部系统日志的每个消息的严重性值与本地系统日志中的严重性值相同，请选择 * 直通 * 。

      对于审核日志，如果选择 * 直通 * ，则严重性为 "info" 。

      对于安全事件，如果选择 * 直通 * ，则严重性值由节点上的 Linux 分发版生成。

      对于应用程序日志，如果选择 * 直通 * ，则 " 信息 " 和 " 通知 " 之间的严重性会有所不同，具体取决于问题描述 的含义。例如，添加 NTP 服务器并配置 HA 组会提供一个值 "info" ，而有意停止 SSM 或 RSM 服务则会提供一个值 "notice" 。

   b. 如果不想使用直通值，请选择一个介于 0 到 7 之间的严重性值。

      选定值将应用于此类型的所有消息。如果选择使用固定值覆盖严重性，则有关不同严重性的信息将丢失。

severity	Description
0	紧急：系统不可用
1.	alert ： 必须立即执行操作
2.	严重：严重情况
3.	错误：错误情况
4.	警告：警告条件
5.	注意：正常但重要的情况

severity	Description
6.	Informational ： 信息性消息
7.	debug ： 调试级别的消息

c. 对于 * 设备 * ，如果希望发送到外部系统日志的每个消息都与本地系统日志中的设备值相同，请选择 * 直通 * 。

对于审核日志，如果选择 * 直通 * ，则发送到外部系统日志服务器的工具为 "local7" 。

对于安全事件，如果选择 * 直通 * ，则设备值由节点上的 Linux 分发版生成。

对于应用程序日志，如果选择 * 直通 * ，则发送到外部系统日志服务器的应用程序日志具有以下设施值：

应用程序日志	直通值
bycast.log	用户或守护进程
bycast-err.log	用户，守护进程， local3 或 local4
jaeger.log	本地 2.
nms.log	本地 3.
prometheus.log	本地 4.
raft.log	本地 5.
hagroups.log	本地 6.

d. 如果不想使用直通值，请选择 0 到 23 之间的设施值。

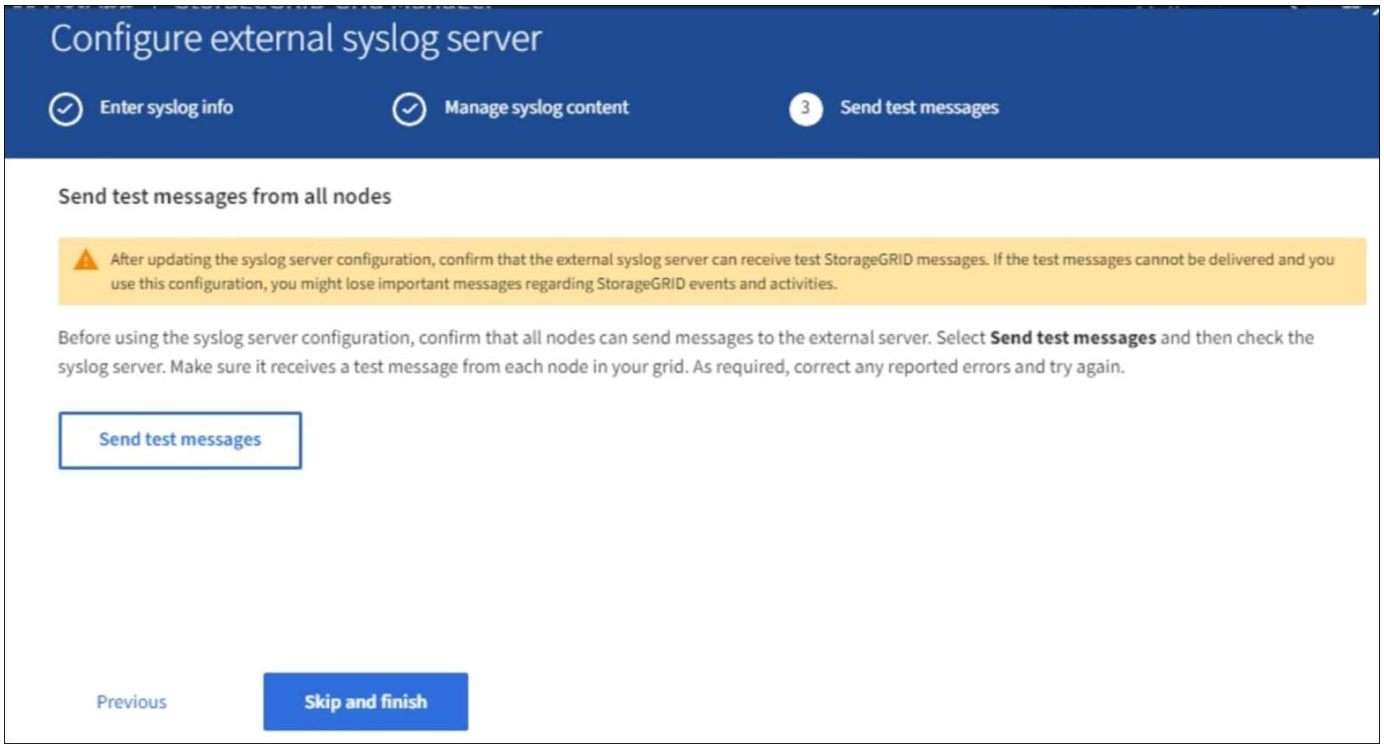
选定值将应用于此类型的所有消息。如果您选择使用固定值覆盖设施，则有关不同设施的信息将丢失。

设施	Description
0	KERN （内核消息）
1.	用户（用户级消息）
2.	邮件
3.	守护进程（系统守护进程）

设施	Description
4.	auth （安全 / 授权消息）
5.	系统日志（由 syslogd 在内部生成的消息）
6.	LPR （行式打印机子系统）
7.	新闻（网络新闻子系统）
8.	uucp
9	cron （时钟守护进程）
10	安全性（安全性 / 授权消息）
11.	FTP
12	NTP
13	日志审核（日志审核）
14	日志警报（日志警报）
15	时钟（时钟守护进程）
16.	本地 0
17	本地 1
18	本地 2.
19	本地 3.
20	本地 4.
21	本地 5.
22.	本地 6.
23	本地 7.

3. 选择 * 继续 * 。

发送测试消息



在开始使用外部系统日志服务器之前，您应请求网格中的所有节点向外部系统日志服务器发送测试消息。在提交向外部系统日志服务器发送数据之前，您应使用这些测试消息来帮助验证整个日志收集基础架构。

在确认外部系统日志服务器从网格中的每个节点收到测试消息且消息已按预期进行处理之前，请勿使用外部系统日志服务器配置。

1. 如果您不希望发送测试消息，并且您确定外部系统日志服务器配置正确，并且可以从网格中的所有节点接收审核信息，请选择 * 跳过并完成 * 。

   此时将显示一个绿色横幅，指示您的配置已成功保存。

2. 否则，请选择 * 发送测试消息 * 。

   测试结果会持续显示在页面上，直到您停止测试为止。测试期间，审核消息会继续发送到先前配置的目标。

3. 如果收到任何错误，请更正这些错误，然后再次选择 * 发送测试消息 * 。请参见 对外部系统日志服务器进行故障排除 以帮助您解决任何错误。
4. 请等待，直到看到一个绿色横幅，指示所有节点均已通过测试。
5. 检查系统日志服务器以确定是否按预期接收和处理了测试消息。

   如果使用的是 UDP ，请检查整个日志收集基础架构。UDP 协议不允许像其他协议那样严格地检测错误。

6. 选择 * 停止并完成 * 。

   此时将返回到 * 审核和系统日志服务器 * 页面。此时将显示一个绿色横幅，通知您已成功保存系统日志服务器配置。

除非选择包含外部系统日志服务器的目标，否则不会将 StorageGRID 审核信息发送到外部系统日志服务器。

选择审核信息目标

您可以指定将安全事件日志，应用程序日志和审核消息日志发送到何处。

有关 StorageGRID 软件日志的详细信息，请参见 StorageGRID 软件日志。

1. 在 Audit and syslog server 页面上，从列出的选项中选择审核信息的目标：

选项	Description
默认（管理节点 / 本地节点）	审核消息会发送到管理节点上的审核日志（`audit.log`），而安全事件日志和应用程序日志会存储在生成它们的节点（也称为 " 本地节点 " ）上。
外部系统日志服务器	审核信息将发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。
管理节点和外部系统日志服务器	审核消息会发送到管理节点上的审核日志（`audit.log`），审核信息会发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。
仅限本地节点	不会向管理节点或远程系统日志服务器发送任何审核信息。审核信息仅保存在生成该信息的节点上。 • 注 * ： StorageGRID 会定期轮换删除这些本地日志以释放空间。当节点的日志文件达到 1 GB 时，系统将保存现有文件并启动新的日志文件。日志的轮换限制为 21 个文件。创建日志文件的第 22 版时，将删除最早的日志文件。每个节点平均存储约 20 GB 的日志数据。

在每个本地节点上生成的审核信息存储在 ` /var/local/log/localaudit.log` 中

1. 选择 * 保存 * 。然后，选择确定以接受对日志目标所做的更改。
2. 如果选择 * 外部系统日志服务器 * 或 * 管理节点和外部系统日志服务器 * 作为审核信息的目标，则会显示一条附加警告。查看警告文本。

您必须确认外部系统日志服务器可以接收测试 StorageGRID 消息。

1. 选择 * 确定 * 以确认要更改审核信息的目标。

   此时将显示一个绿色横幅，通知您已成功保存审核配置。

新日志将发送到选定的目标。现有日志将保留在其当前位置。

相关信息

审核消息概述

配置审核消息和日志目标

系统审核消息

对象存储审核消息

管理审核消息

客户端读取审核消息

管理 StorageGRID

使用 **SNMP** 监控

如果要使用简单网络管理协议（ Simple Network Management Protocol ， SNMP ）监控 StorageGRID ，则必须配置 StorageGRID 附带的 SNMP 代理。

- 配置 SNMP 代理
- 更新 SNMP 代理

功能

每个 StorageGRID 节点都运行一个 SNMP 代理或守护进程，该代理或守护进程可提供一个管理信息库（ Management Information Base ， MIB ）。StorageGRID MIB 包含警报和警报的表和通知定义。MIB 还包含系统问题描述 信息，例如每个节点的平台和型号。每个 StorageGRID 节点还支持一组 MIB-II 对象。

最初，所有节点上都会禁用 SNMP 。配置 SNMP 代理时，所有 StorageGRID 节点都会收到相同的配置。

StorageGRID SNMP 代理支持所有三个版本的 SNMP 协议。它为查询提供只读 MIB 访问权限，并可向管理系统发送两种类型的事件驱动型通知：

- * 陷阱 * 是 SNMP 代理发送的通知，不需要管理系统确认。陷阱用于通知管理系统 StorageGRID 中发生了某种情况，例如触发警报。

  所有三个版本的 SNMP 均支持陷阱。

- * 通知 * 与陷阱类似，但它们需要管理系统确认。如果 SNMP 代理未在特定时间内收到确认，则会重新发送通知，直到收到确认或达到最大重试值为止。

  SNMPv2c 和 SNMPv3 支持 INFORM 。

在以下情况下会发送陷阱和通知通知通知：

- 默认或自定义警报将在任何严重性级别触发。要禁止警报的 SNMP 通知，您必须为此警报配置静默。警报通知由配置为首选发送方的任何管理节点发送。

每个警报都会根据警报的严重性级别映射到以下三种陷阱类型之一： activeMinorAlert ， activeMajorAlert 和 activeCriticalAlert 。有关可能触发这些陷阱的警报的说明，请参见 警报参考。

- 某些警报（旧系统）会在指定的严重性级别或更高级别触发。

> 不会针对每个警报或每个警报严重性发送 SNMP 通知。

SNMP 版本支持

下表简要总结了每个 SNMP 版本支持的功能。

	SNMPv1	**SNMPv2c**	**SNMPv3**
查询	只读 MIB 查询	只读 MIB 查询	只读 MIB 查询
查询身份验证	社区字符串	社区字符串	基于用户的安全模型（ USM ）用户
通知	仅陷阱	陷阱和通知	陷阱和通知
通知身份验证	每个陷阱目标的默认陷阱社区或自定义社区字符串	每个陷阱目标的默认陷阱社区或自定义社区字符串	每个陷阱目标的 USM 用户

限制

- StorageGRID 支持只读 MIB 访问。不支持读写访问。
- 网格中的所有节点都接收相同的配置。
- SNMPv3： StorageGRID 不支持传输支持模式（ TSM ）。
- SNMPv3： 支持的唯一身份验证协议是 SHA （ HMAC-SHA-96 ）。
- SNMPv3： 支持的唯一隐私协议是 AES 。

访问 **MIB**

您可以在任何 StorageGRID 节点上的以下位置访问 MIB 定义文件：

` /usr/share/snmp/MIBS/NetApp-STORAGEGRID-MIB.txt`

相关信息

- 警报参考
- 警报参考（旧系统）
- 生成 SNMP 通知的警报（旧系统）
- 静默警报通知

如果要使用第三方 SNMP 管理系统进行只读 MIB 访问和通知，则可以配置 StorageGRID SNMP 代理。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。

关于此任务

StorageGRID SNMP 代理支持所有三个版本的 SNMP 协议。您可以为代理配置一个或多个版本。

步骤

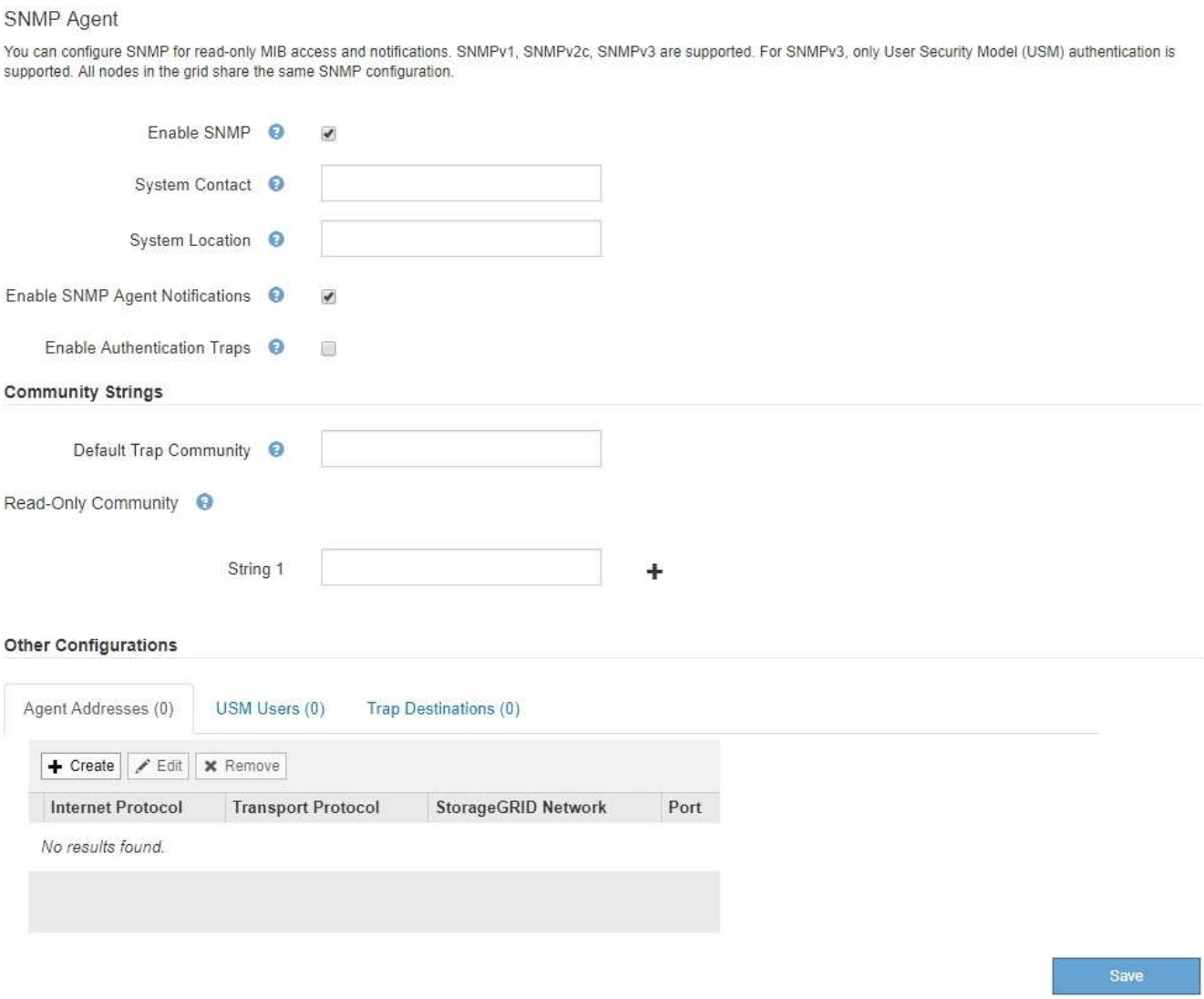
1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

   此时将显示 SNMP 代理页面。



2. 要在所有网格节点上启用 SNMP 代理，请选中 * 启用 SNMP* 复选框。

   此时将显示用于配置 SNMP 代理的字段。



3. 在 * 系统联系人 * 字段中，输入希望 StorageGRID 在 sysContact 的 SNMP 消息中提供的值。

   系统联系人通常是电子邮件地址。您为 StorageGRID 系统中的所有节点提供的适用场景 值。* 系统联系人 * 最多可以包含 255 个字符。

4. 在 * 系统位置 * 字段中，输入希望 StorageGRID 在 "SNMP messages"sysLocation" 中提供的值。

   系统位置可以是有助于确定 StorageGRID 系统位置的任何信息。例如，您可以使用设施的街道地址。您为 StorageGRID 系统中的所有节点提供的适用场景 值。* 系统位置 * 最多可以包含 255 个字符。

5. 如果希望 StorageGRID SNMP 代理发送陷阱并通知通知，请保持选中 * 启用 SNMP 代理通知 * 复选框。

   如果未选中此复选框，则 SNMP 代理支持只读 MIB 访问，但不会发送任何 SNMP 通知。

6. 如果希望 StorageGRID SNMP 代理在收到身份验证不当的协议消息时发送身份验证陷阱，请选中 * 启用身份验证陷阱 * 复选框。
7. 如果使用 SNMPv1 或 SNMPv2c ，请完成社区字符串部分。

   本节中的字段用于 SNMPv1 或 SNMPv2c 中基于社区的身份验证。这些字段不适用于 SNMPv3 。

a. 在 * 默认陷阱社区 * 字段中，也可以输入要用于陷阱目标的默认社区字符串。

   您可以根据需要提供其他（ "`custom` " ）社区字符串 定义特定陷阱目标。

   - 默认陷阱社区 * 最多可以包含 32 个字符，并且不能包含空格字符。

b. 对于 * 只读社区 * ，输入一个或多个社区字符串以允许对 IPv4 和 IPv6 代理地址进行只读 MIB 访问。单击加号 ✚ 添加多个字符串。

   当管理系统查询 StorageGRID MIB 时，它会发送一个社区字符串。如果社区字符串与此处指定的值之一匹配，则 SNMP 代理会向管理系统发送响应。

   每个社区字符串最多可以包含 32 个字符，并且不能包含空格字符。最多允许五个字符串。

   为确保 StorageGRID 系统的安全性，请勿使用 "`公有` " 作为社区字符串。如果不输入社区字符串， SNMP 代理将使用 StorageGRID 系统的网格 ID 作为社区字符串。

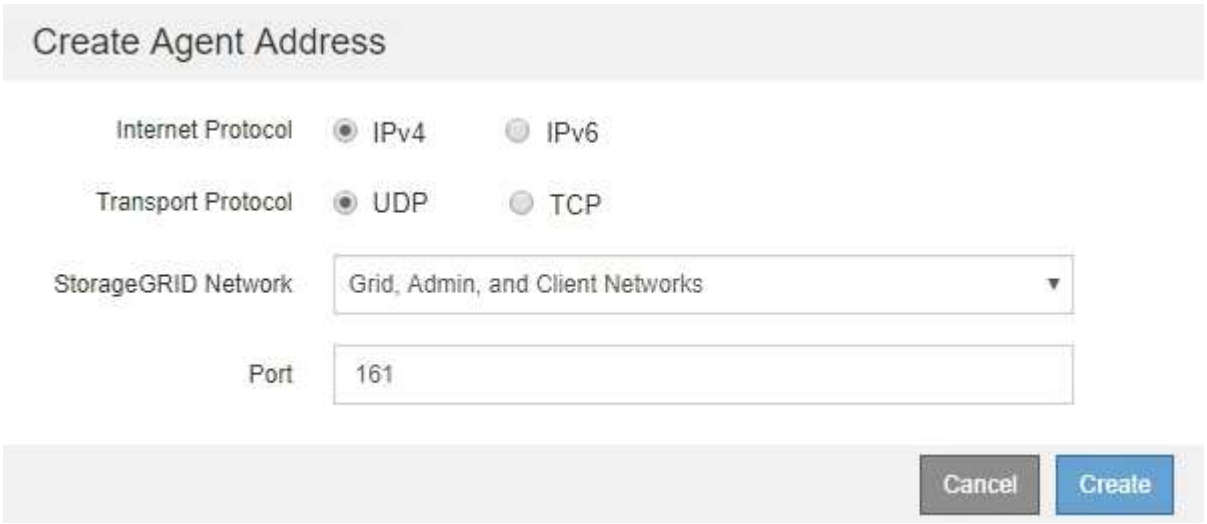
8. 也可以选择其他配置部分中的代理地址选项卡。

使用此选项卡指定一个或多个 "`侦听地址。` " 这些是 SNMP 代理可以接收查询的 StorageGRID 地址。每个代理地址都包括一个 Internet 协议，一个传输协议，一个 StorageGRID 网络以及一个端口（可选）。

如果不配置代理地址，则所有 StorageGRID 网络上的默认侦听地址均为 UDP 端口 161 。

a. 单击 * 创建 * 。

   此时将显示创建代理地址对话框。



b. 对于 * 互联网协议 * ，选择此地址是使用 IPv4 还是 IPv6 。

   默认情况下， SNMP 使用 IPv4 。

c. 对于 * 传输协议 * ，选择此地址是使用 UDP 还是 TCP 。

   默认情况下， SNMP 使用 UDP 。

d. 在 * StorageGRID Network* 字段中，选择要接收查询的 StorageGRID 网络。

- 网格，管理和客户端网络： StorageGRID 应侦听所有三个网络上的 SNMP 查询。
- 网格网络
- 管理网络
- 客户端网络

> 要确保客户端与 StorageGRID 的通信保持安全，不应为此客户端网络创建代理地址。

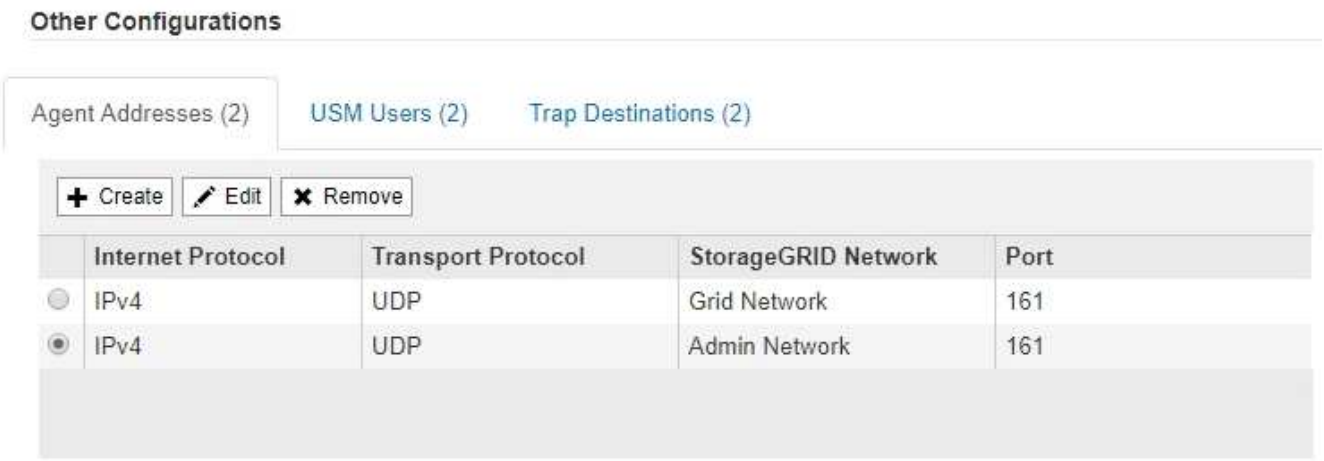
e. 在 * 端口 * 字段中，也可以输入 SNMP 代理应侦听的端口号。

SNMP 代理的默认 UDP 端口为 161 ，但您可以输入任何未使用的端口号。

> 保存 SNMP 代理时， StorageGRID 会自动打开内部防火墙上的代理地址端口。您必须确保任何外部防火墙允许访问这些端口。

f. 单击 * 创建 * 。

此时将创建代理地址并将其添加到表中。



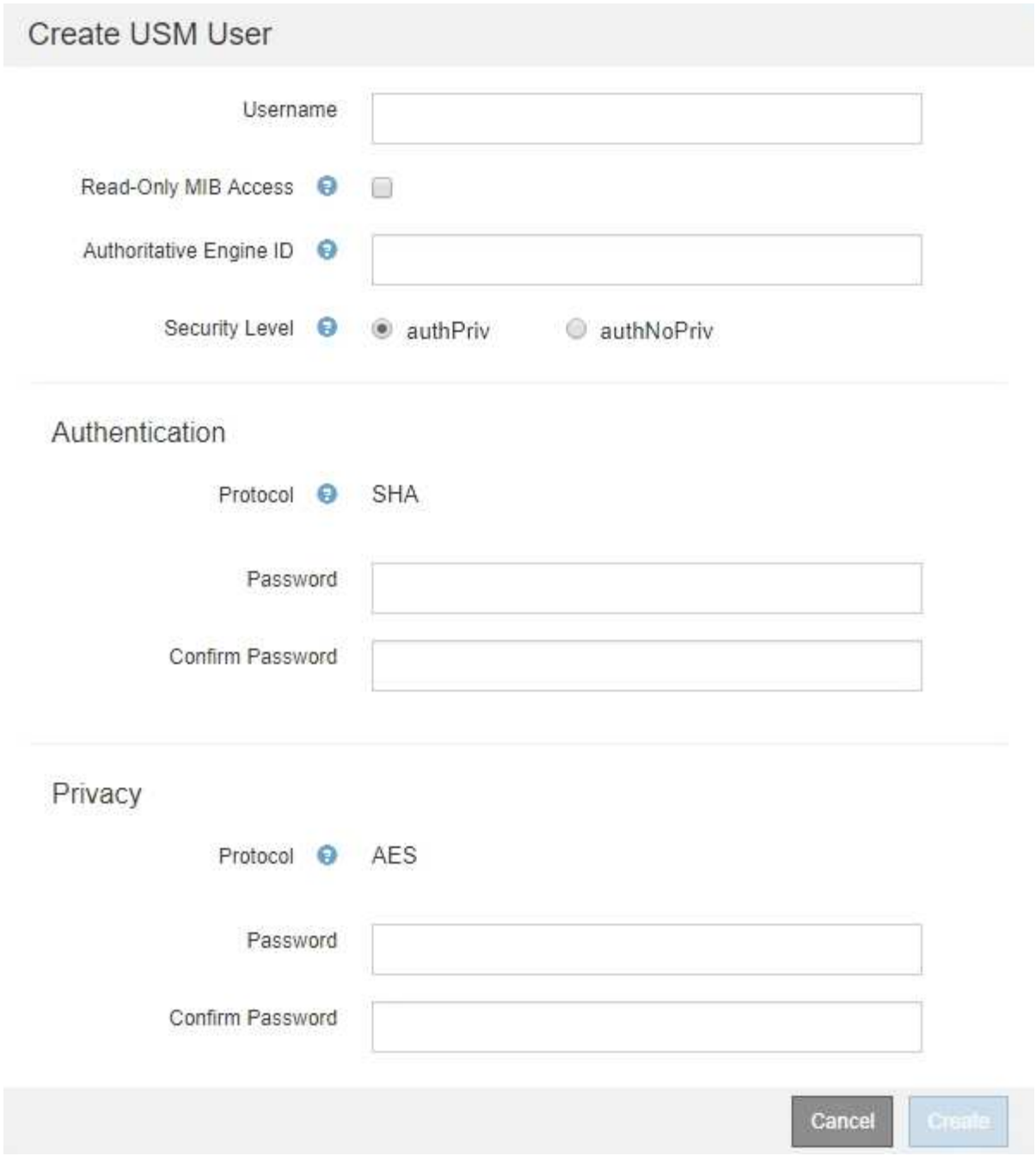
9. 如果您使用的是 SNMPv3 ，请在其他配置部分中选择 USM 用户选项卡。

使用此选项卡可定义有权查询 MIB 或接收陷阱并通知的 USM 用户。

> 如果您仅使用 SNMPv1 或 SNMPv2c ，则此步骤不适用。

a. 单击 * 创建 * 。

此时将显示创建 USM 用户对话框。



b. 为此 USM 用户输入唯一的 * 用户名 * 。

用户名最多包含 32 个字符，不能包含空格字符。创建用户后，无法更改此用户名。

c. 如果此用户应对 MIB 具有只读访问权限，请选中 * 只读 MIB 访问 * 复选框。

如果选择 * 只读 MIB 访问 * ，则会禁用 * 权威引擎 ID* 字段。

具有只读 MIB 访问权限的 USM 用户不能具有引擎 ID 。

d. 如果要在通知目标中使用此用户，请为此用户输入 * 权威引擎 ID* 。

SNMPv3 INFORM 目标必须具有具有引擎 ID 的用户。SNMPv3 陷阱目标不能包含具有引擎 ID 的用户。

权威引擎 ID 可以是 5 到 32 字节，以十六进制表示。

e. 为 USM 用户选择一个安全级别。

- * authPriv* ： 此用户与身份验证和隐私（加密）通信。您必须指定身份验证协议和密码以及隐私协议和密码。
- * authNoPriv* ： 此用户使用身份验证进行通信，并且没有隐私（无加密）。您必须指定身份验证协议和密码。

f. 输入并确认此用户将用于身份验证的密码。

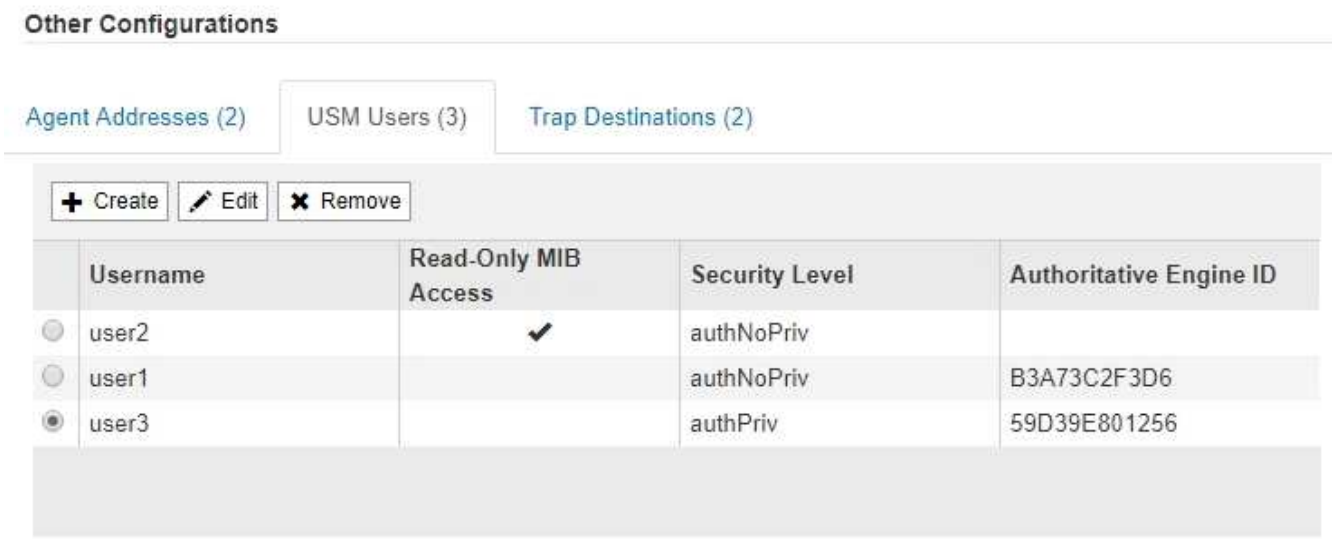
唯一支持的身份验证协议是 SHA （ HMAC-SHA-96 ）。

g. 如果您选择了 * 身份验证基础 * ，请输入并确认此用户将用于隐私保护的密码。

唯一支持的隐私协议是 AES 。

h. 单击 * 创建 * 。

此时将创建 USM 用户并将其添加到表中。

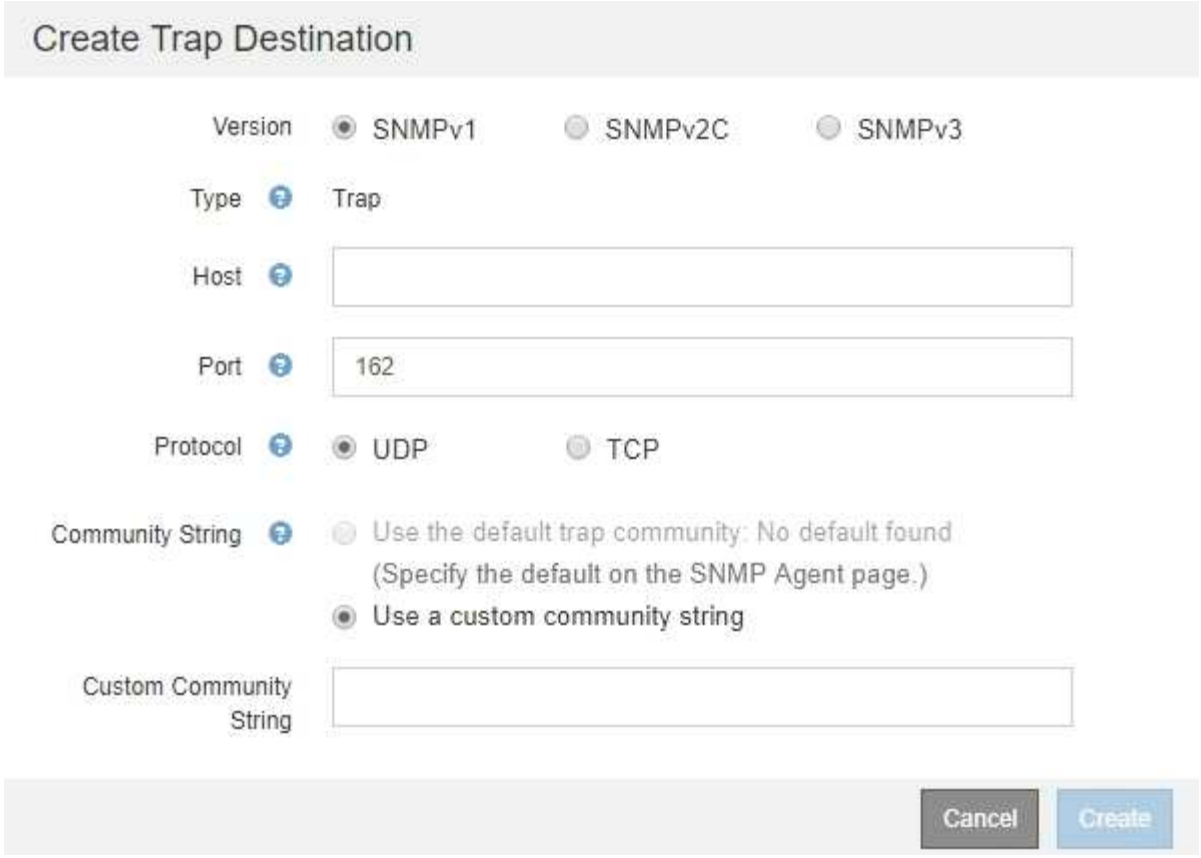


10. 在其他配置部分中，选择陷阱目标选项卡。

通过陷阱目标选项卡，您可以为 StorageGRID 陷阱或通知通知定义一个或多个目标。启用 SNMP 代理并单击 * 保存 * 后， StorageGRID 将开始向每个定义的目标发送通知。触发警报和警报时会发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

a. 单击 * 创建 * 。

此时将显示创建陷阱目标对话框。



b. 在 * 版本 * 字段中，选择要用于此通知的 SNMP 版本。

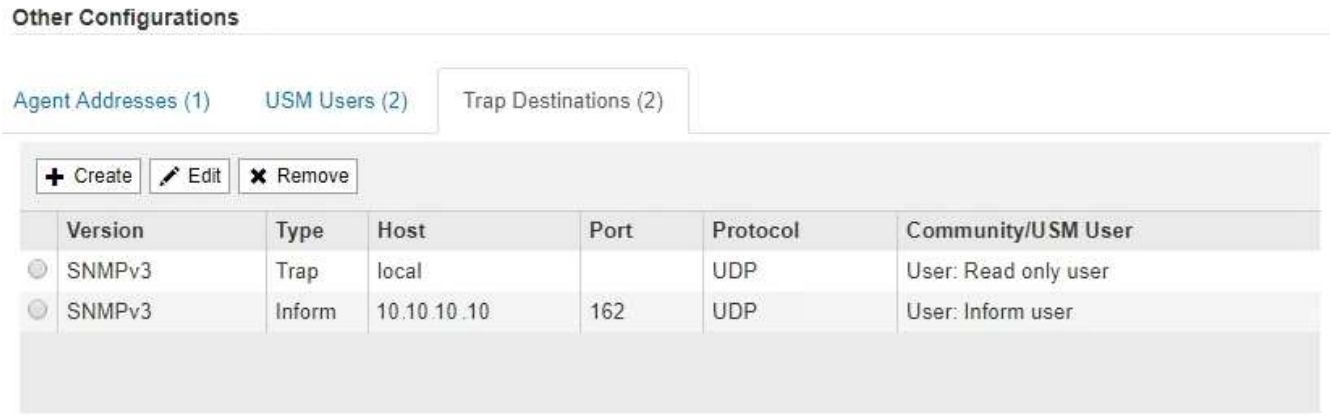
c. 根据您选择的版本填写此表单

version	指定此信息
SNMPv1	• 注： * 对于 SNMPv1 ， SNMP 代理只能发送陷阱。不支持 INFORM 。 i. 在 * 主机 * 字段中，输入要接收陷阱的 IPv4 或 IPv6 地址（或 FQDN ）。 ii. 对于 * 端口 * ，请使用默认值（ 162 ），除非必须使用其他值。（ 162 是 SNMP 陷阱的标准端口。） iii. 对于 * 协议 * ，请使用默认值（ UDP ）。此外，还支持 TCP 。（ UDP 是标准 SNMP 陷阱协议。） iv. 如果在 SNMP 代理页面上指定了一个陷阱团体，请使用默认陷阱团体，或者为此陷阱目标输入自定义社区字符串。 自定义社区字符串最多可以包含 32 个字符，并且不能包含空格。

version	指定此信息
SNMPv2c	i. 选择目标是用于陷阱还是用于通知。 ii. 在 * 主机 * 字段中，输入要接收陷阱的 IPv4 或 IPv6 地址（或 FQDN ）。 iii. 对于 * 端口 * ，请使用默认值（ 162 ），除非必须使用其他值。（ 162 是 SNMP 陷阱的标准端口。） iv. 对于 * 协议 * ，请使用默认值（ UDP ）。此外，还支持 TCP 。（ UDP 是标准 SNMP 陷阱协议。） v. 如果在 SNMP 代理页面上指定了一个陷阱团体，请使用默认陷阱团体，或者为此陷阱目标输入自定义社区字符串。 自定义社区字符串最多可以包含 32 个字符，并且不能包含空格。
SNMPv3	i. 选择目标是用于陷阱还是用于通知。 ii. 在 * 主机 * 字段中，输入要接收陷阱的 IPv4 或 IPv6 地址（或 FQDN ）。 iii. 对于 * 端口 * ，请使用默认值（ 162 ），除非必须使用其他值。（ 162 是 SNMP 陷阱的标准端口。） iv. 对于 * 协议 * ，请使用默认值（ UDP ）。此外，还支持 TCP 。（ UDP 是标准 SNMP 陷阱协议。） v. 选择要用于身份验证的 USM 用户。 ◦ 如果选择了 * 陷阱 * ，则仅显示不具有权威引擎 ID 的 USM 用户。 ◦ 如果选择 * 通知 * ，则仅显示具有权威引擎 ID 的 USM 用户。

d. 单击 * 创建 * 。

此时将创建陷阱目标并将其添加到表中。



11. 完成 SNMP 代理配置后，单击 * 保存 *

    新的 SNMP 代理配置将变为活动状态。

相关信息

静默警报通知

更新 **SNMP** 代理

您可能需要禁用 SNMP 通知，更新社区字符串，或者添加或删除代理地址， USM 用户和陷阱目标。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有 root 访问权限。

关于此任务

更新时 SNMP 代理配置，请注意，您必须单击 SNMP 代理页面底部的 * 保存 * 以提交对每个选项卡所做的任何更改。

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

   此时将显示 SNMP 代理页面。

2. 如果要在所有网格节点上禁用 SNMP 代理，请取消选中 * 启用 SNMP* 复选框，然后单击 * 保存 * 。

   已对所有网格节点禁用 SNMP 代理。如果稍后重新启用代理，则会保留先前的任何 SNMP 配置设置。

3. 或者，更新您为 * 系统联系人 * 和 * 系统位置 * 输入的值。
4. 如果您不再希望 StorageGRID SNMP 代理发送陷阱并通知通知，也可以取消选中 * 启用 SNMP 代理通知 * 复选框。

   取消选中此复选框后， SNMP 代理支持只读 MIB 访问，但不会发送任何 SNMP 通知。

5. 或者，如果您不再希望 StorageGRID SNMP 代理在收到未经正确身份验证的协议消息时发送身份验证陷阱，请取消选中 * 启用身份验证陷阱 * 复选框。

6. 如果您使用 SNMPv1 或 SNMPv2c ，也可以更新社区字符串部分。

   本节中的字段用于 SNMPv1 或 SNMPv2c 中基于社区的身份验证。这些字段不适用于 SNMPv3 。

   如果要删除默认社区字符串，必须首先确保所有陷阱目标都使用自定义社区字符串。

7. 如果要更新代理地址，请选择其他配置部分中的代理地址选项卡。



   使用此选项卡指定一个或多个 "`侦听地址。` " 这些是 SNMP 代理可以接收查询的 StorageGRID 地址。每个代理地址都包括一个 Internet 协议，一个传输协议，一个 StorageGRID 网络和一个端口。

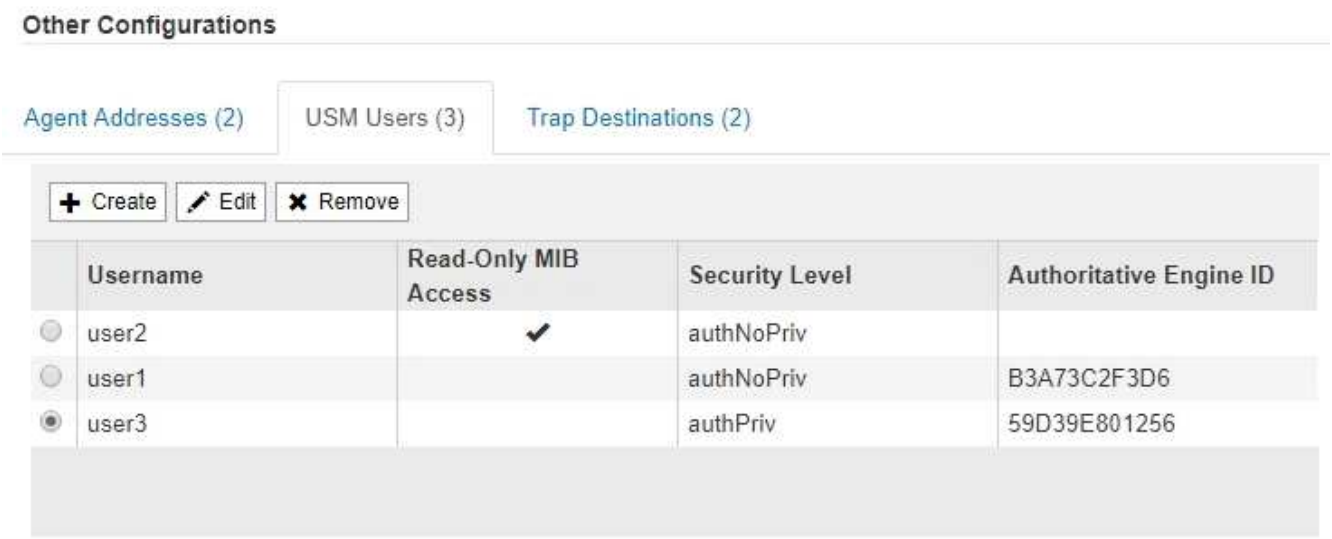
   a. 要添加代理地址，请单击 * 创建 * 。然后，请参见有关配置 SNMP 代理的说明中的代理地址步骤。

   b. 要编辑代理地址，请选择该地址的单选按钮，然后单击 * 编辑 * 。然后，请参见有关配置 SNMP 代理的说明中的代理地址步骤。

   c. 要删除代理地址，请选择该地址的单选按钮，然后单击 * 删除 * 。然后，单击 * 确定 * 以确认要删除此地址。

   d. 要提交更改，请单击 SNMP 代理页面底部的 * 保存 * 。

8. 如果要更新 USM 用户，请在其他配置部分中选择 USM 用户选项卡。



   使用此选项卡可定义有权查询 MIB 或接收陷阱并通知的 USM 用户。

a. 要添加 USM 用户，请单击 * 创建 * 。然后，请参见配置 SNMP 代理的说明中适用于 USM 用户的步骤。

b. 要编辑 USM 用户，请选择该用户的单选按钮，然后单击 * 编辑 * 。然后，请参见配置 SNMP 代理的说明中适用于 USM 用户的步骤。

无法更改现有 USM 用户的用户名。如果需要更改用户名，必须删除此用户并创建新用户名。

> 如果您添加或删除用户的权威引擎 ID ，并且当前已选择该用户作为目标，则必须按照步骤中所述编辑或删除该目标 SNMP 陷阱目标。否则，在保存 SNMP 代理配置时会发生验证错误。

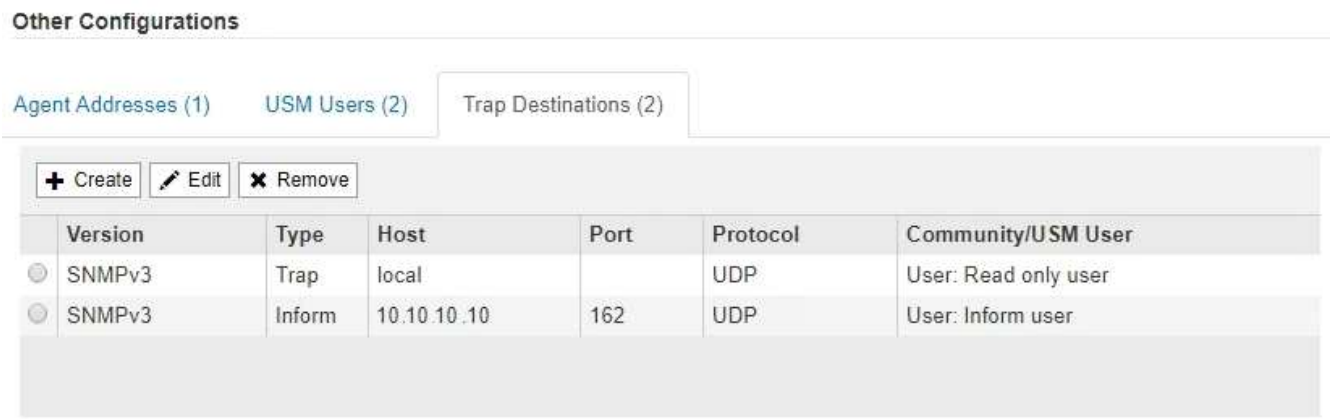
c. 要删除 USM 用户，请选择该用户的单选按钮，然后单击 * 删除 * 。然后，单击 * 确定 * 以确认要删除此用户。

> 如果当前已为陷阱目标选择删除的用户，则必须按照步骤中所述编辑或删除此目标 SNMP 陷阱目标。否则，在保存 SNMP 代理配置时会发生验证错误。



a. 要提交更改，请单击 SNMP 代理页面底部的 * 保存 * 。

9. 【 SNMP 陷阱目标， start=9]] 如果要更新陷阱目标，请选择其他配置部分中的陷阱目标选项卡。



通过陷阱目标选项卡，您可以为 StorageGRID 陷阱或通知通知定义一个或多个目标。启用 SNMP 代理并单击 * 保存 * 后， StorageGRID 将开始向每个定义的目标发送通知。触发警报和警报时会发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

a. 要添加陷阱目标，请单击 * 创建 * 。然后，请参见配置 SNMP 代理的说明中有关陷阱目标的步骤。

b. 要编辑陷阱目标，请选择用户的单选按钮，然后单击 * 编辑 * 。然后，请参见配置 SNMP 代理的说明中有关陷阱目标的步骤。

c. 要删除陷阱目标，请选择目标的单选按钮，然后单击 * 删除 * 。然后，单击 * 确定 * 以确认要删除此目标。

d. 要提交更改，请单击 SNMP 代理页面底部的 * 保存 * 。

10. 更新 SNMP 代理配置后，单击 * 保存 * 。

收集其他 **StorageGRID** 数据

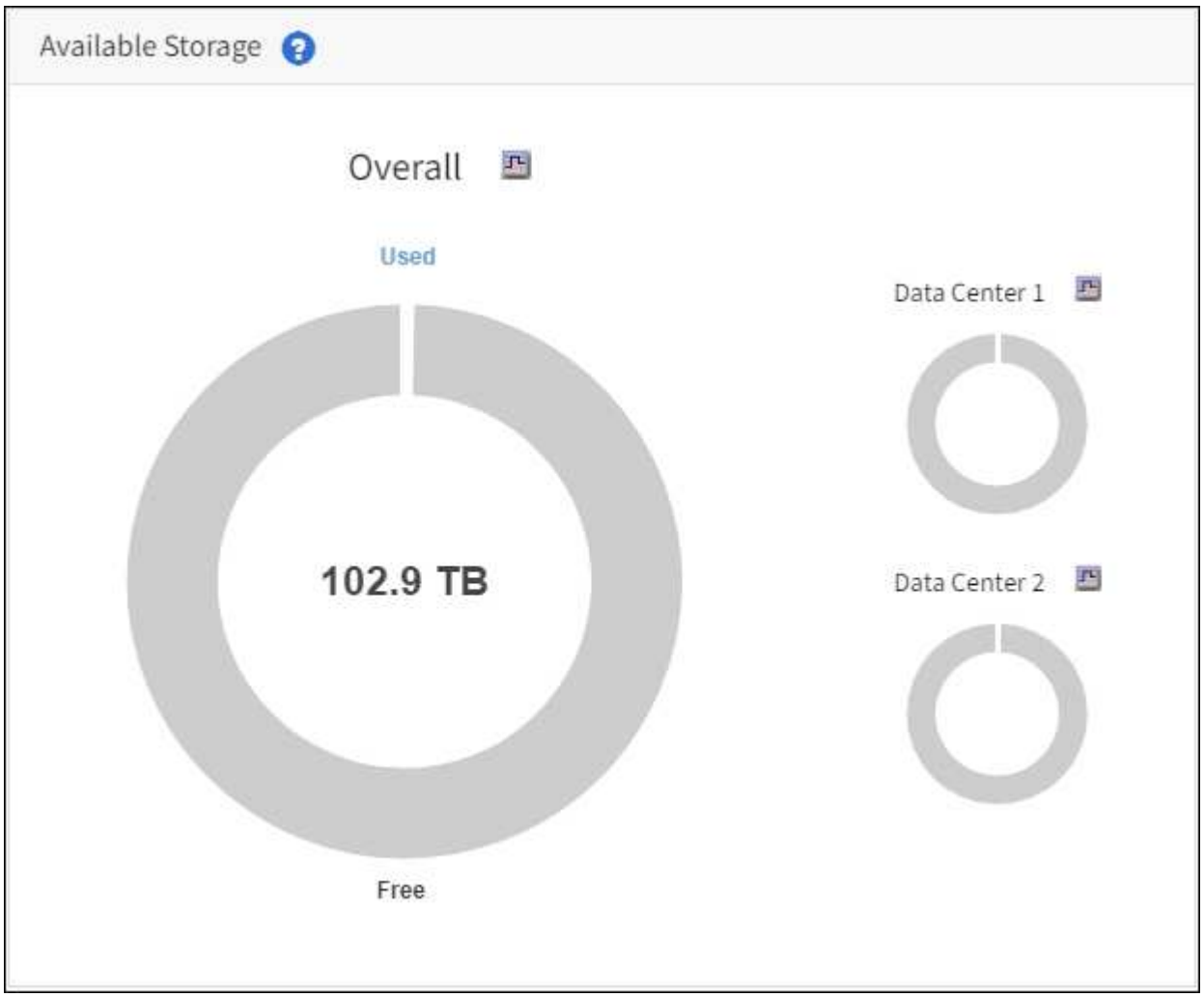
使用图表和图形

您可以使用图表和报告监控 StorageGRID 系统的状态并对问题进行故障排除。网格管理器中提供的图表和报告类型包括圆环图（仅在信息板上），图形和文本报告。

图表类型

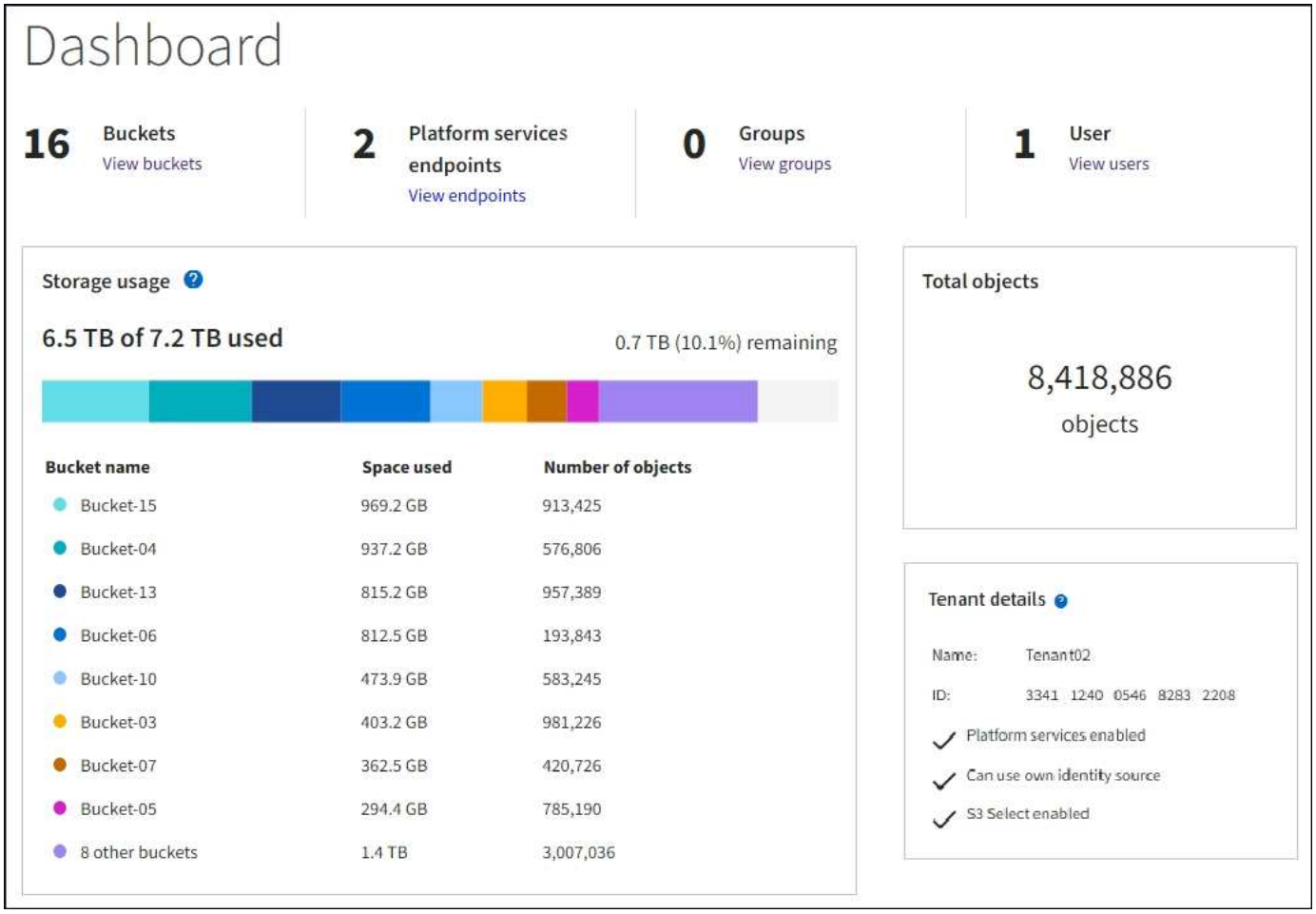
图表和图形汇总了特定 StorageGRID 指标和属性的值。

网格管理器信息板包含圆环图表，用于汇总网格和每个站点的可用存储。



租户管理器信息板上的存储使用情况面板显示以下内容：

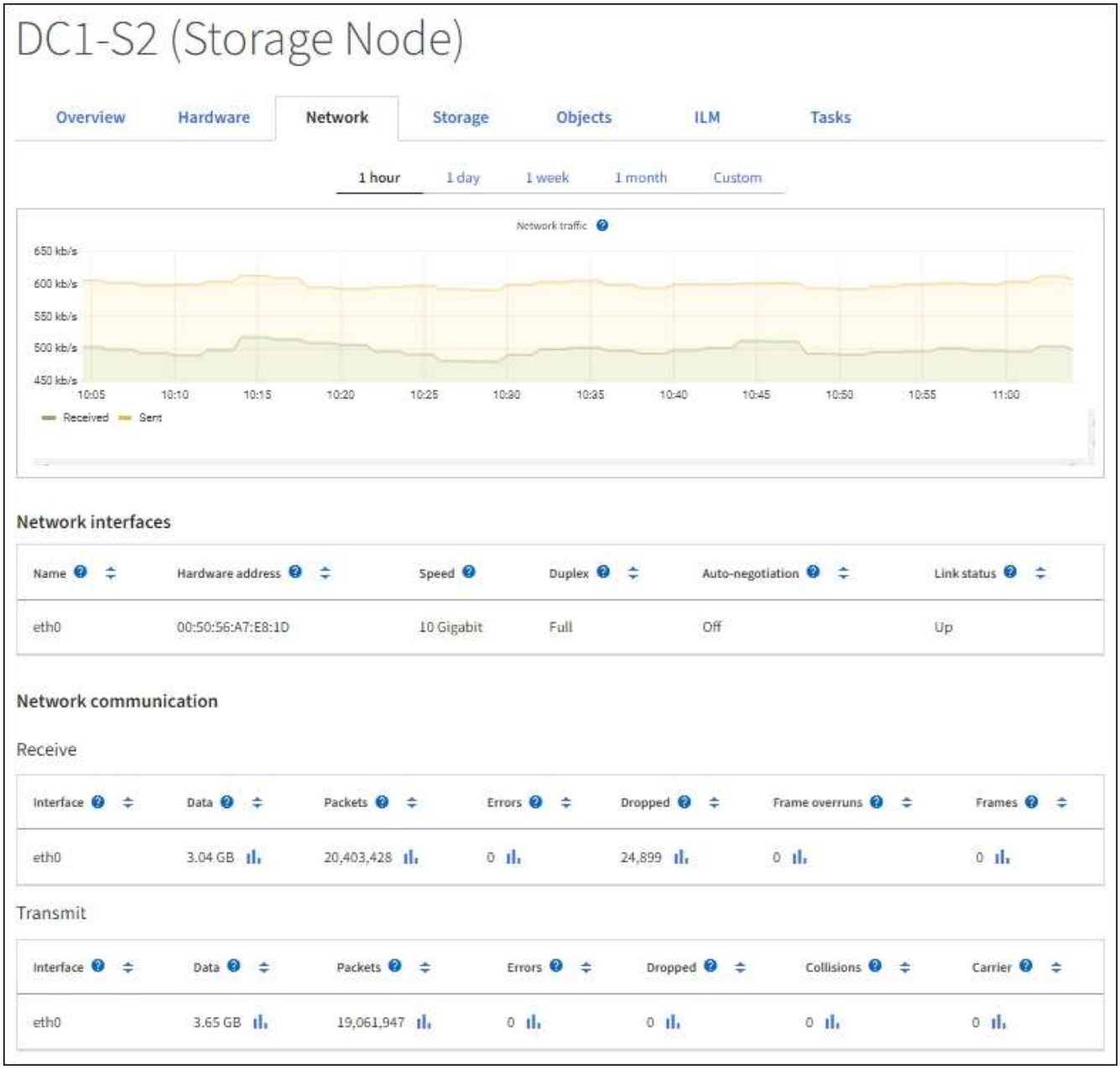
- 租户最大的分段（ S3 ）或容器（ Swift ）列表
- 一个条形图，表示最大分段或容器的相对大小
- 已用总空间量，如果设置了配额，则还会显示剩余空间量和百分比



此外，还可以从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面查看显示 StorageGRID 指标和属性随时间变化的图形。

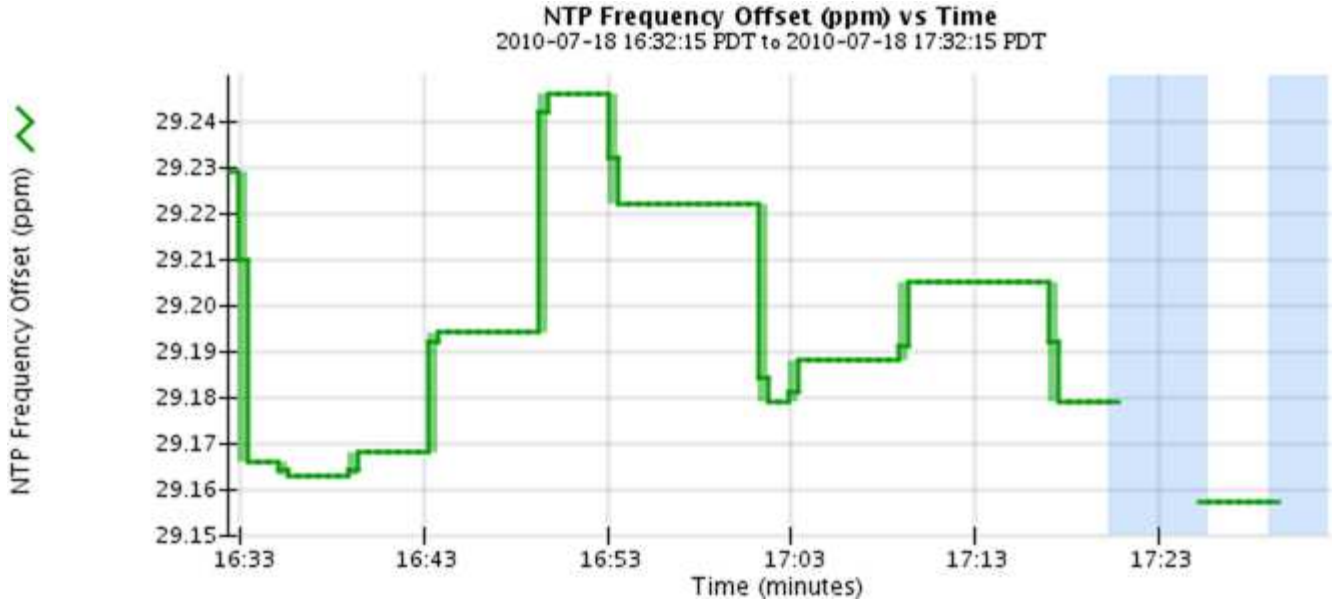
图形有四种类型：

- * 格拉法纳图表 * ：如节点页面上所示，格拉法纳图表用于绘制一段时间内的 Prometheus 指标值。例如，存储节点的 * 节点 * > * 网络 * 选项卡包含网络流量的 Grafana 图表。

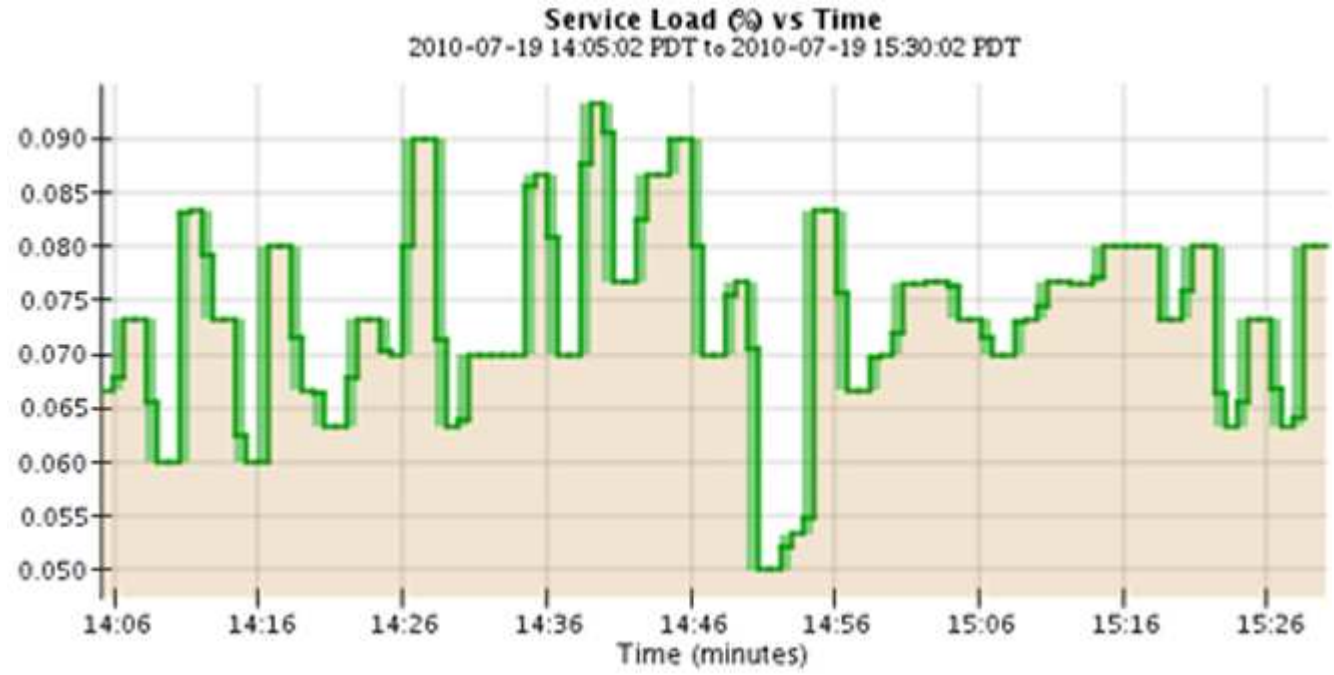


Grafana 图表也包含在预构建的信息板中，这些信息板可从 * 支持 * > * 工具 * > * 指标 * 页面获得。

- * 折线图 * ： 可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用折线图绘制具有单位值（例如 NTP 频率偏移，以 PPM 为单位）的 StorageGRID 属性值。值的更改会按定期数据间隔（箱）绘制。



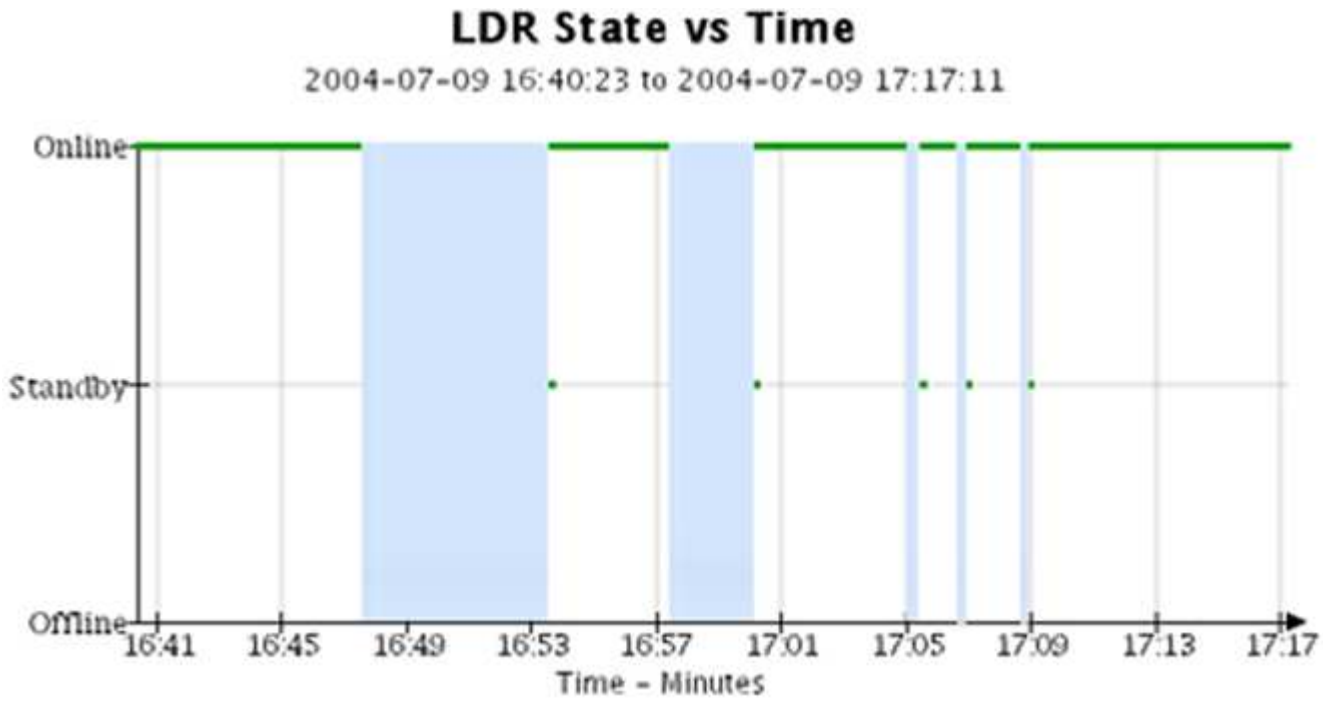
- * 区域图形 * ： 可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用分区图绘制容量属性数量，例如对象计数或服务负载值。区域图形与折线图类似，但在折线下方会显示浅棕色阴影。值的更改会按定期数据间隔（箱）绘制。



- 某些图形使用不同类型的图表图标表示 格式不同：



- * 状态图 * ： 可从 * 支持 * > * 工具 * > * 网格拓扑 * 页面访问（选择图表图标 在数据值之后，状态图用于绘制表示不同状态的属性值，例如服务状态可以是联机，备用或脱机。状态图与折线图类似，但过渡不连续，即值从一个状态值跳到另一个状态值。



相关信息

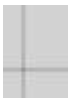
查看节点页面

查看网格拓扑树

查看支持指标

图表图例

用于绘制图表的线条和颜色具有特定的含义。

示例	含义
	报告的属性值使用深绿色线绘制。
	暗绿线周围的浅绿色阴影表示该时间范围内的实际值各不相同，并且已 "`绑定` " 以加快绘制速度。暗线表示加权平均值。绿色的范围表示箱内的最大值和最小值。区域图使用浅棕色阴影来指示容量数据。
	空白区域（未绘制任何数据）表示属性值不可用。背景可以是蓝色，灰色或灰色和蓝色混合，具体取决于报告属性的服务的状态。
	浅蓝色阴影表示当时的部分或全部属性值不确定；属性未报告值，因为服务处于未知状态。
	灰色阴影表示当时部分或全部属性值未知，因为报告属性的服务已被管理员关闭。
	灰色和蓝色阴影混合表示当时的某些属性值不确定（因为服务处于未知状态），而其他属性值则未知，因为报告属性的服务已被管理员关闭。

显示图表和图形

节点页面包含您应定期访问的图表和图形，用于监控存储容量和吞吐量等属性。在某些情况下，尤其是在与技术支持人员合作时，您可以使用 * 支持 * > * 工具 * > * 网格拓扑 * 页面访问其他图表。

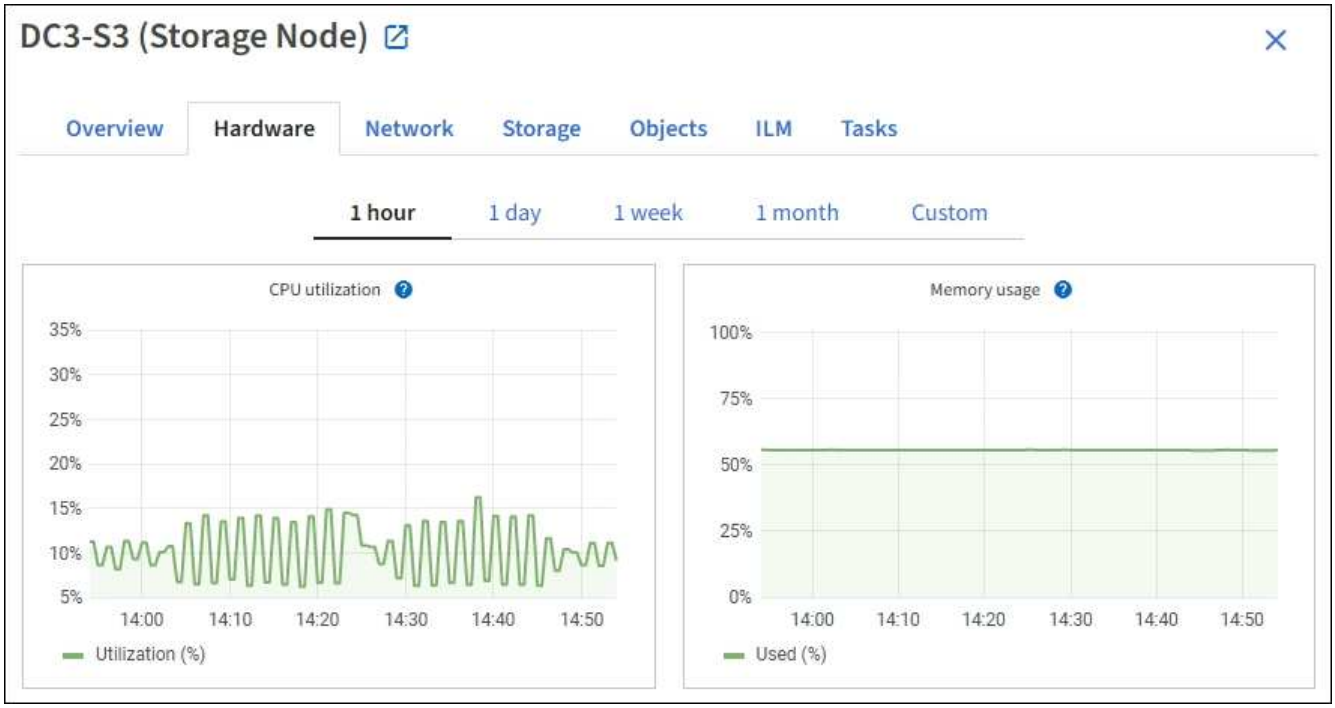
您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

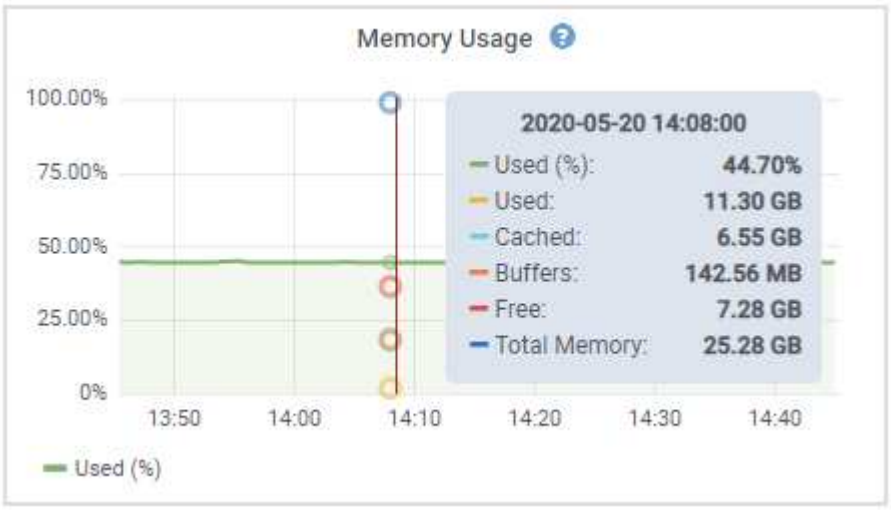
步骤

1. 选择 * 节点 * 。然后，选择节点，站点或整个网格。
2. 选择要查看其信息的选项卡。

   某些选项卡包含一个或多个 Grafana 图表，用于绘制一段时间内 Prometheus 指标的值。例如，节点的 * 节点 * > * 硬件 * 选项卡包含两个 Grafana 图表。



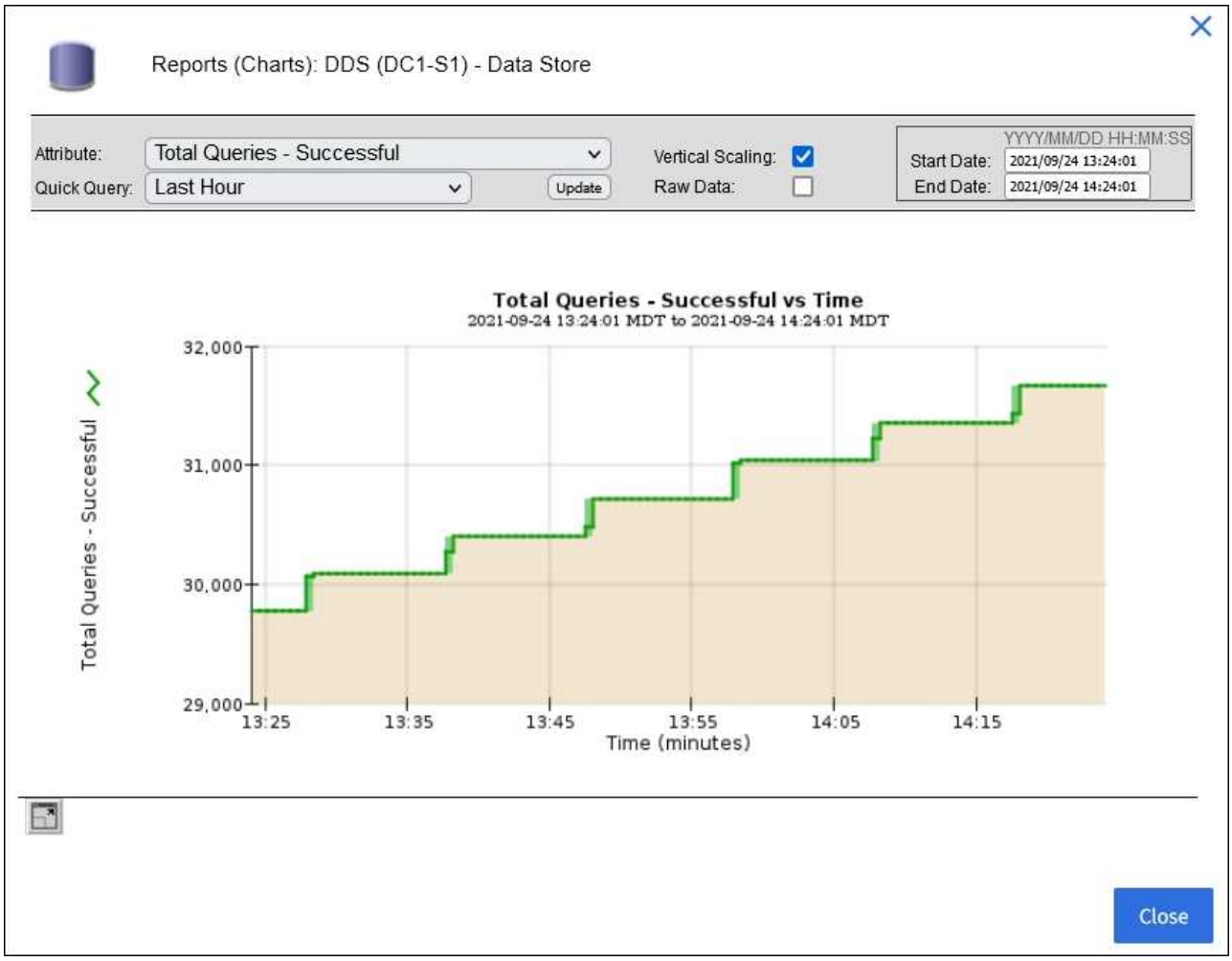
3. 或者，将光标悬停在图表上方可查看特定时间点的更详细值。

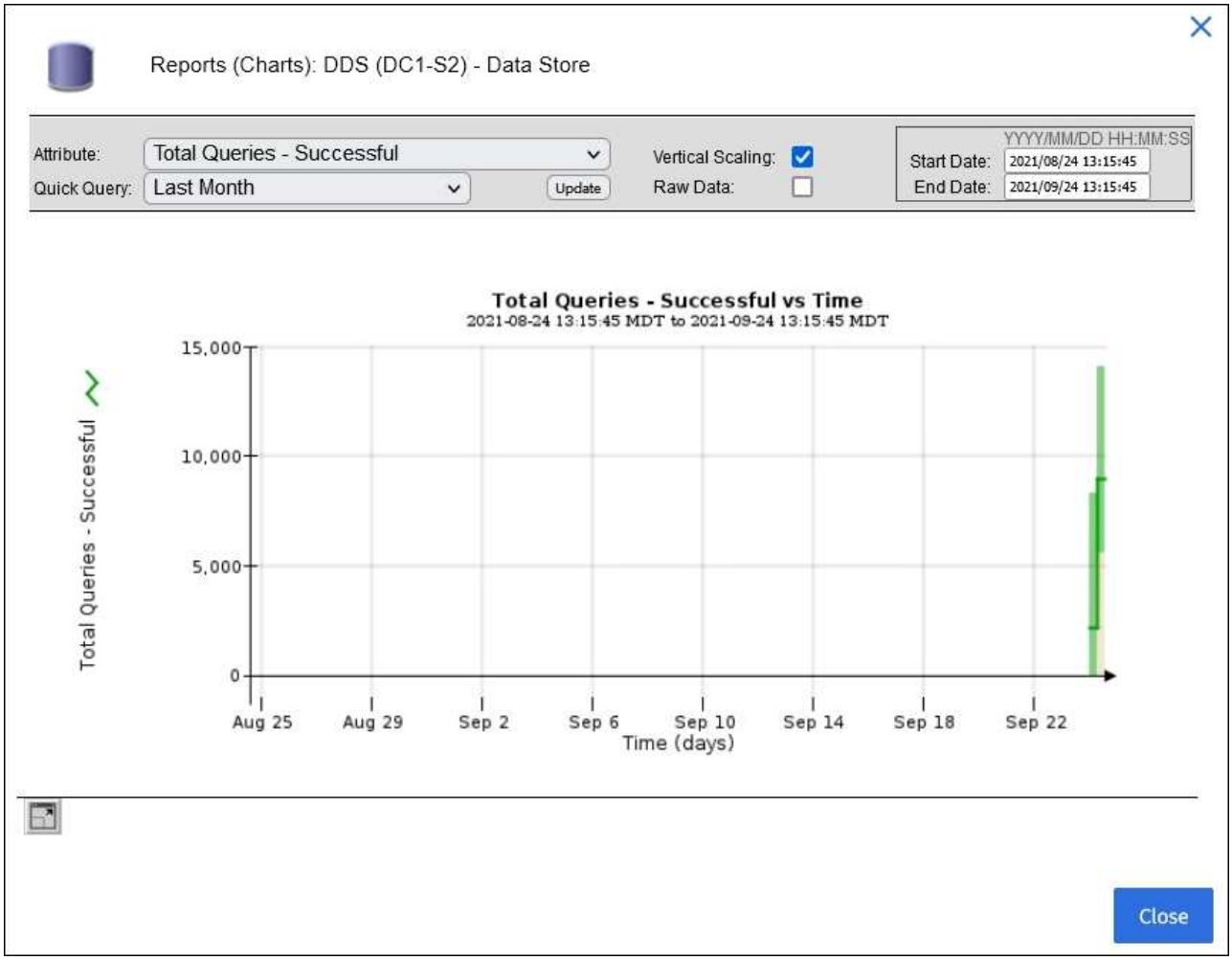


4. 您通常可以根据需要显示特定属性或指标的图表。从节点页面上的表中，选择图表图标 属性名称右侧。

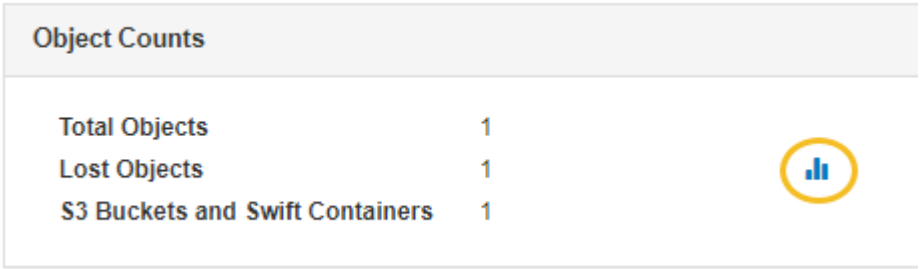
   并非所有指标和属性都有图表。

   - 示例 1*：从存储节点的对象选项卡中，您可以选择图表图标 可查看存储节点的成功元数据存储查询总数。


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

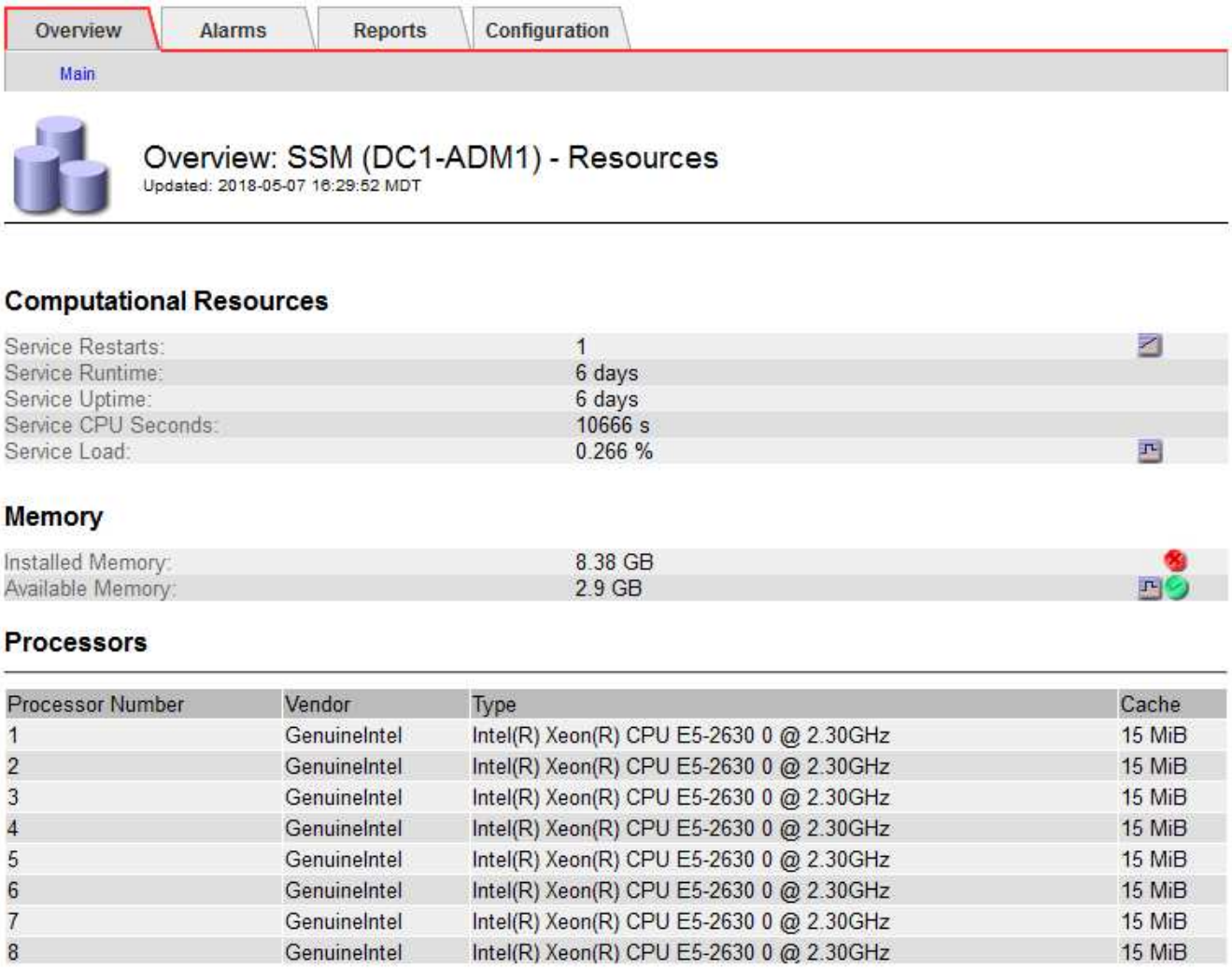


◦ 示例 2*： 从存储节点的对象选项卡中，您可以选择图表图标 可查看随时间检测到的丢失对象计数的 Grafana 图形。





5. 要显示节点页面未显示的属性的图表，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
6. 选择 ***GRID NODE*** > * 组件或 service_* > * 概述 * > * 主要 * 。



7. 选择图表图标 属性旁边。

   显示内容将自动更改为 "* 报告 * > * 图表 * " 页面。此图表显示属性在过去一天的数据。

生成图表

图表以图形方式显示属性数据值。您可以报告数据中心站点，网格节点，组件或服务。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 ***GRID NODE*** > * 组件或 service_* > * 报告 * > * 图表 * 。
3. 从 * 属性 * 下拉列表中选择要报告的属性。
4. 要强制 Y 轴从零开始，请取消选中 * 垂直扩展 * 复选框。
5. 要以完全精确度显示值，请选中 * 原始数据 * 复选框，或者要将值舍入为最多三位小数（例如，对于以百分比形式报告的属性），请取消选中 * 原始数据 * 复选框。

6. 从 * 快速查询 * 下拉列表中选择要报告的时间段。

   选择自定义查询选项以选择特定的时间范围。

   稍后，图表将显示。请留出几分钟时间，以表格形式列出较长的时间范围。

7. 如果选择了自定义查询，请输入 * 开始日期 * 和 * 结束日期 * 自定义图表的时间段。

   在当地时间使用格式 ` YYYY/MM/DDHH： MM： SS_` 。要与格式匹配，必须使用前导零。例如，2017/4/6 7： 30： 00 验证失败。正确格式为 2017 年 4 月 06 日 07： 30： 00 。

8. 选择 * 更新 * 。

   几秒钟后会生成一个图表。请留出几分钟时间，以表格形式列出较长的时间范围。根据为查询设置的时间长度，将显示原始文本报告或聚合文本报告。

使用文本报告

文本报告以文本形式显示 NMS 服务已处理的属性数据值。根据您报告的时间段，会生成两种类型的报告：一周以下时段的原始文本报告和一周以上时段的聚合文本报告。

原始文本报告

原始文本报告显示有关选定属性的详细信息：

- Time Received： NMS 服务处理属性数据样本值的本地日期和时间。
- 采样时间：在源上采样或更改属性值的本地日期和时间。
- value ： 样本时间的属性值。

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 %

聚合文本报告

聚合文本报告显示的数据比原始文本报告显示的时间更长（通常为一周）。每个条目都是由 NMS 服务在一段时间内将多个属性值（属性值的聚合）汇总到一个条目中的结果，其中包含从聚合派生的平均值，最大值和最小值。

每个条目都会显示以下信息：

- 聚合时间： NMS 服务聚合（收集）一组更改属性值的最后本地日期和时间。
- Average value ： 属性值在聚合时间段内的平均值。
- 最小值：聚合时间段内的最小值。
- 最大值：聚合时间段内的最大值。

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

生成文本报告

文本报告以文本形式显示 NMS 服务已处理的属性数据值。您可以报告数据中心站点，网格节点，组件或服务。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

对于预期会持续更改的属性数据， NMS 服务（在源上）会定期对这些属性数据进行采样。对于不经常更改的属性数据（例如，基于状态或状态更改等事件的数据），当属性值发生更改时，会将该属性值发送到 NMS 服务。

显示的报告类型取决于配置的时间段。默认情况下，系统会为超过一周的时间段生成聚合文本报告。

灰色文本表示服务在取样期间被管理员关闭。蓝色文本表示服务处于未知状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 ***GRID NODE*** > * 组件或 service_* > * 报告 * > * 文本 * 。
3. 从 * 属性 * 下拉列表中选择要报告的属性。
4. 从 * 每页结果 * 下拉列表中选择每页结果数。
5. 要将值舍入为最多三位小数（例如，对于以百分比形式报告的属性），请取消选中 * 原始数据 * 复选框。
6. 从 * 快速查询 * 下拉列表中选择要报告的时间段。

   选择自定义查询选项以选择特定的时间范围。

   此报告将在片刻后显示。请留出几分钟时间，以表格形式列出较长的时间范围。

7. 如果选择了自定义查询，则需要输入 * 开始日期 * 和 * 结束日期 * 来自定义要报告的时间段。

   在当地时间使用格式 `YYYY/MM/DDHH ： MM ： SS` 。要与格式匹配，必须使用前导零。例如， 2017/4/6

7： 30： 00 验证失败。正确格式为 2017 年 4 月 06 日 07： 30： 00 。

8. 单击 * 更新 * 。

   稍后将生成一个文本报告。请留出几分钟时间，以表格形式列出较长的时间范围。根据为查询设置的时间长度，将显示原始文本报告或聚合文本报告。

导出文本报告

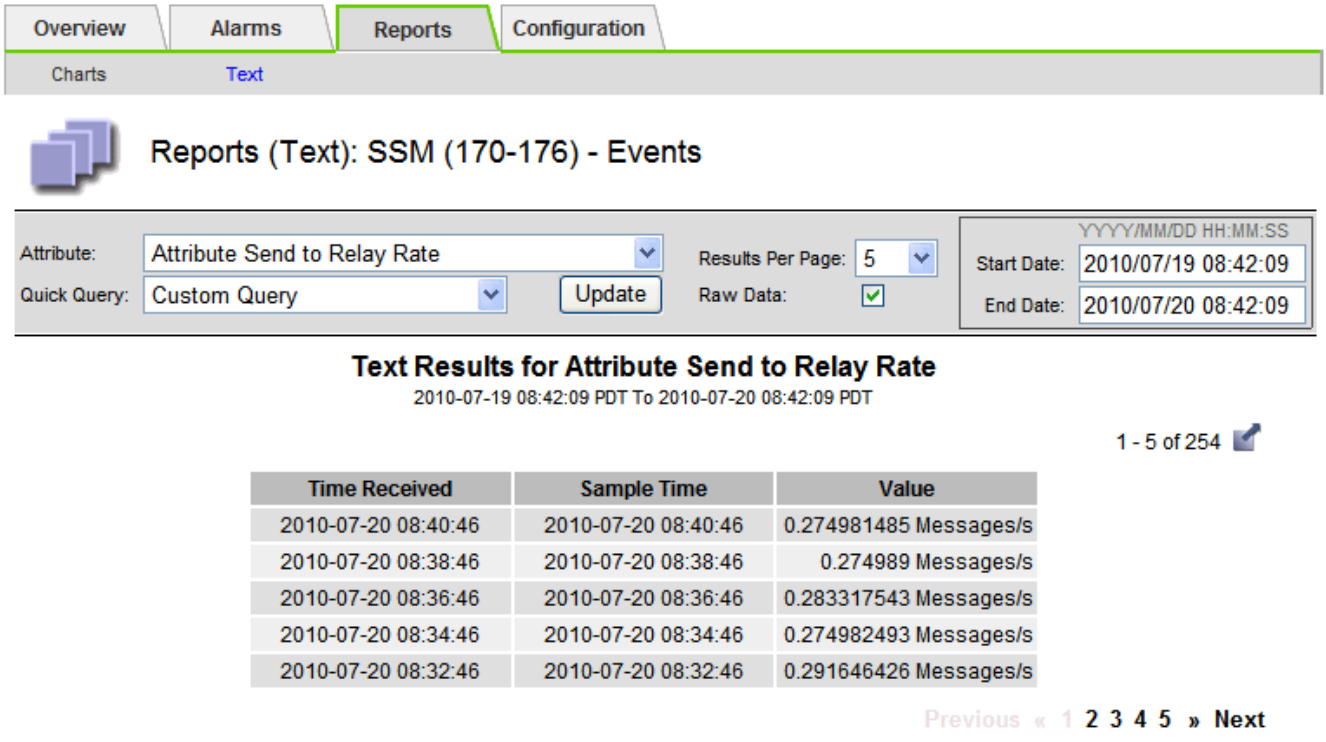
导出的文本报告将打开一个新的浏览器选项卡，在此可以选择和复制数据。

关于此任务

然后，可以将复制的数据保存到新文档（例如电子表格）中，并用于分析 StorageGRID 系统的性能。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 创建文本报告。
3. 单击 * 导出 * 。



   此时将打开导出文本报告窗口，其中显示了此报告。

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. 选择并复制导出文本报告窗口的内容。

   现在，可以将此数据粘贴到电子表格等第三方文档中。

监控 **PUT** 和 **GET** 性能

您可以监控某些操作的性能，例如对象存储和检索，以帮助确定可能需要进一步调查的更改。

关于此任务

要监控 PUT 和 GET 性能，您可以直接从工作站或使用开源 S3tester 应用程序运行 S3 和 Swift 命令。使用这些方法可以独立于 StorageGRID 外部因素（例如客户端应用程序问题或外部网络问题）评估性能。

对 PUT 和 GET 操作执行测试时，请遵循以下准则：

- 使用与通常载入到网格中的对象相当的对象大小。
- 对本地站点和远程站点执行操作。

中的消息 审核日志 指示运行某些操作所需的总时间。例如，要确定 S3 GET 请求的总处理时间，您可以查看 SGET 审核消息中的时间属性值。您还可以在以下操作的审核消息中找到时间属性：

- * S3： delete， get， head， Metadata updated， post， PUT
- * Swift*： delete， get， head， put

在分析结果时，请查看满足请求所需的平均时间以及可以实现的总吞吐量。定期重复相同的测试并记录结果，以便确定可能需要调查的趋势。

- 您可以 "从 GitHub 下载 S3tester"。

StorageGRID 系统可以验证存储节点上对象数据的完整性，并检查是否存在损坏和缺失的对象。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。

关于此任务

两个 验证过程 协同工作以确保数据完整性：

- * 后台验证 * 会自动运行，并持续检查对象数据的正确性。

  后台验证会自动持续检查所有存储节点，以确定复制的和经过纠删编码的对象数据是否存在损坏的副本。如果发现问题， StorageGRID 系统会自动尝试替换存储在系统其他位置的副本中损坏的对象数据。后台验证不会在归档节点或云存储池中的对象上运行。

  如果系统检测到无法自动更正的损坏对象，则会触发 * 检测到未标识的损坏对象 * 警报。

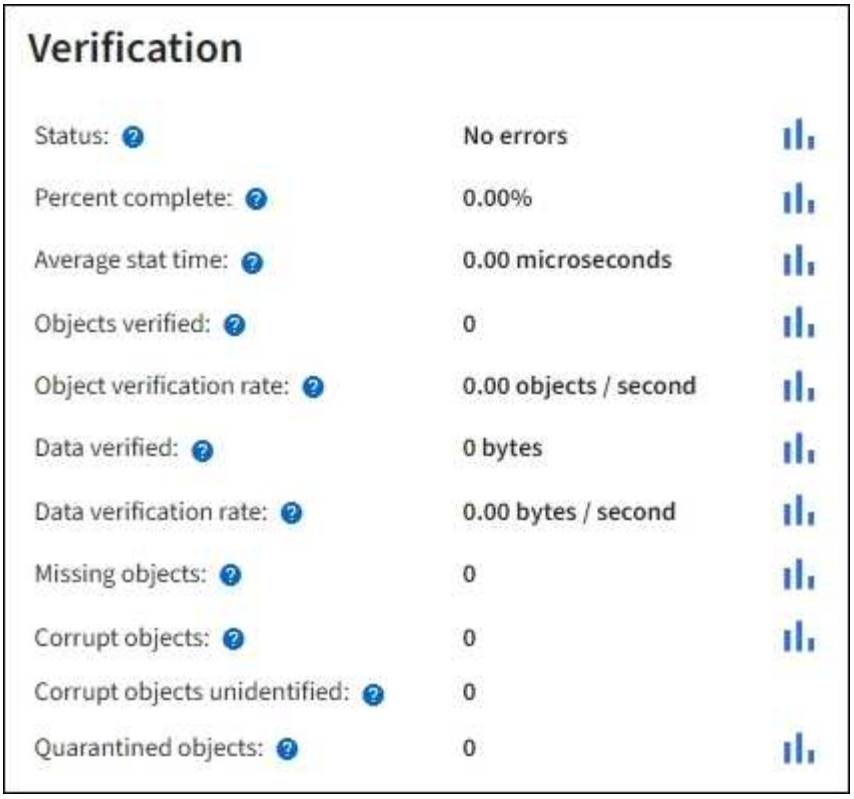
- 用户可以触发 * 对象存在检查 * ，以便更快速地验证对象数据是否存在（尽管不是正确）。

  对象存在检查可验证存储节点上是否存在所有预期复制的对象副本以及经过纠删编码的片段。对象存在检查提供了一种验证存储设备完整性的方法，尤其是在最新的硬件问题描述 可能会影响数据完整性的情况下。

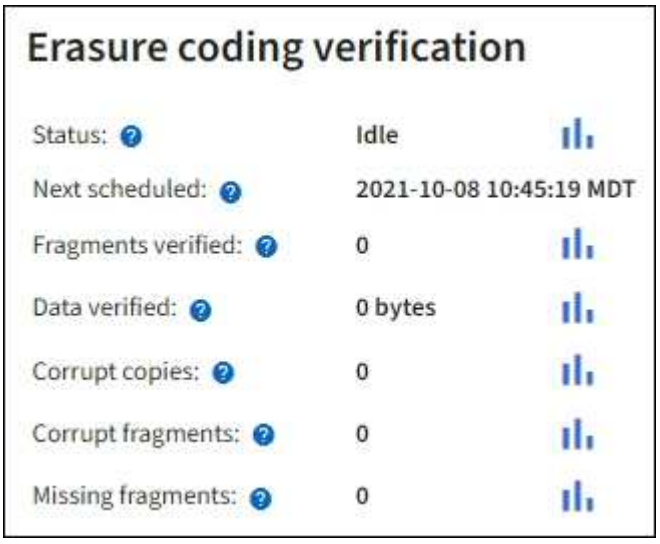
您应定期查看后台验证和对象存在检查的结果。立即调查任何对象数据损坏或丢失的实例，以确定根发生原因。

步骤

1. 查看后台验证的结果：
   a. 选择 * 节点 * > * 存储节点 _* > * 对象 * 。
   b. 检查验证结果：
      - 要检查复制的对象数据验证，请查看验证部分中的属性。

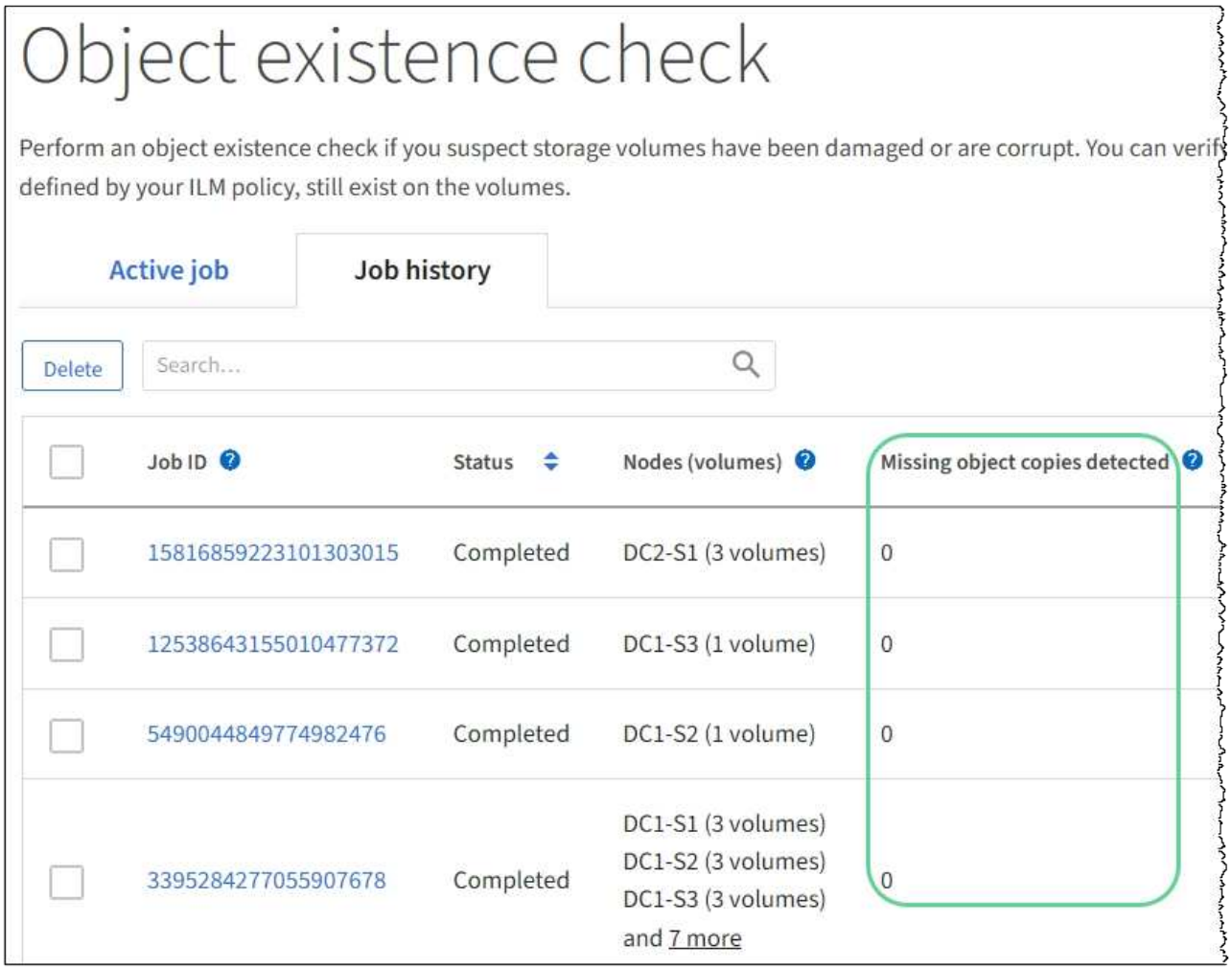


- 要检查擦除编码的片段验证，请选择 * 存储节点 _* > * ILM * ，然后查看擦除编码验证部分中的属性。



选择问号 在属性名称旁边显示帮助文本。

2. 查看对象存在检查作业的结果：
   a. 选择 * 维护 * > * 对象存在检查 * > * 作业历史记录 * 。
   b. 扫描检测到的缺少对象副本列。如果任何作业导致缺少 100 个或更多对象副本和 对象丢失警报 已触发，请联系技术支持。



监控事件

您可以监控网格节点检测到的事件，包括您为跟踪记录到系统日志服务器的事件而创建的自定义事件。网格管理器中显示的最后一个事件消息提供了有关最新事件的详细信息。

事件消息也会列在 ` /var/local/log/byncast-err.log` 日志文件中。请参见 日志文件参考。

网络问题，断电或升级等问题可能会重复触发 SMTT" （事件总数） " 警报。本节介绍了有关调查事件的信息，以便您更好地了解发生这些警报的原因。如果由于已知问题描述 而发生事件，则可以安全地重置事件计数器。

步骤

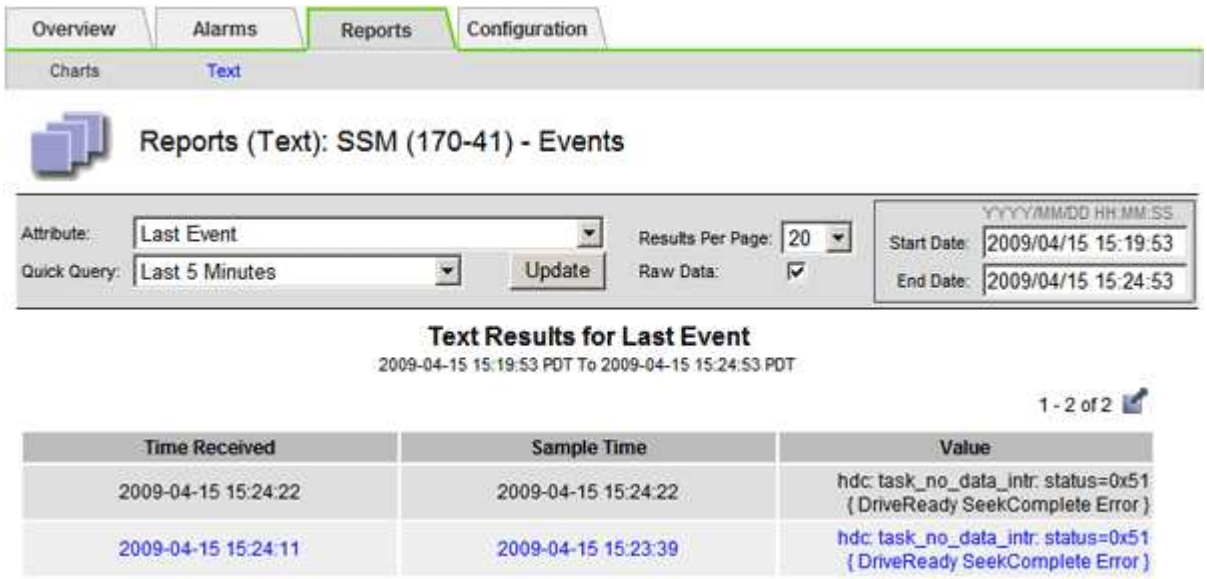
1. 查看每个网格节点的系统事件：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 概述 * > * 主 * 。
2. 生成先前事件消息的列表，以帮助隔离过去发生的问题：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 报告 * 。
   c. 选择 * 文本 * 。

中未显示 * 最后一个事件 * 属性 图表视图。要查看它，请执行以下操作：

d. 将 * 属性 * 更改为 * 最后一个事件 * 。

e. 也可以选择 * 快速查询 * 的时间段。

f. 选择 * 更新 * 。



创建自定义系统日志事件

通过自定义事件，您可以跟踪记录到系统日志服务器的所有内核，守护进程，错误和严重级别的用户事件。自定义事件可用于监控系统日志消息的发生情况（进而监控网络安全事件和硬件故障）。

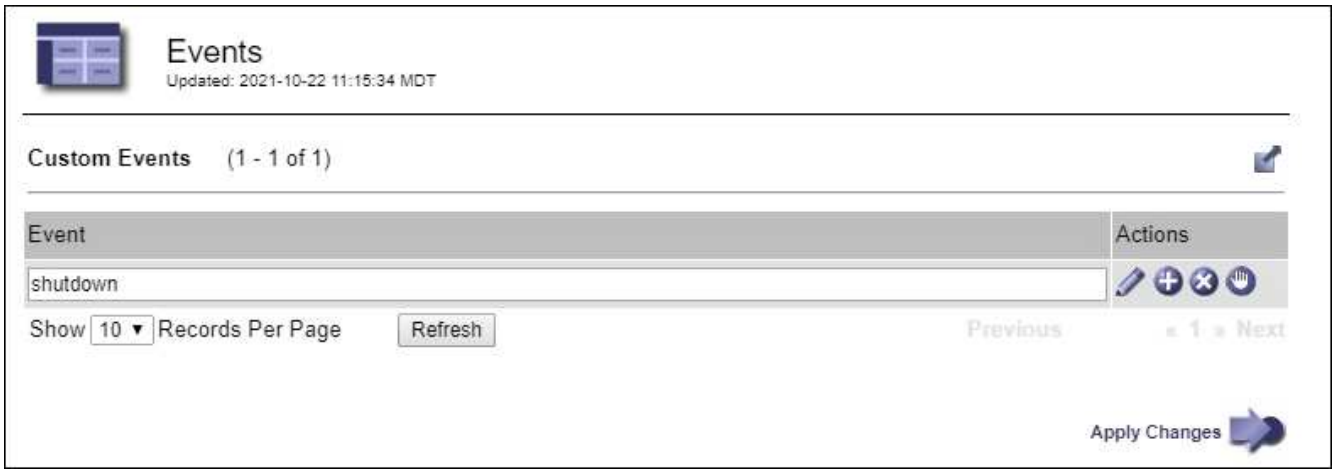
关于此任务

请考虑创建自定义事件以监控重复出现的问题。以下注意事项适用于自定义事件。

- 创建自定义事件后，系统会监控其每次发生情况。
- 要基于 ` /var/local/log/messages` 文件中的关键字创建自定义事件，这些文件中的日志必须为：
  - 由内核生成
  - 由守护进程或用户程序在错误或严重级别生成
- 注： * ` /var/local/log/messages` 文件中的所有条目不会匹配，除非它们满足上述要求。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 自定义事件 * 。
2. 单击 * 编辑 * 。 （或 * 插入 * 如果这不是第一个事件）。
3. 输入自定义事件字符串，例如 shutdown



4. 选择 * 应用更改 * 。
5. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
6. 选择 ***GRID NODE*** > * 。 ssm * > * 事件 * 。
7. 在事件表中找到自定义事件条目，并监控 * 计数 * 的值。

   如果计数增加，则会在该网格节点上触发您正在监控的自定义事件。

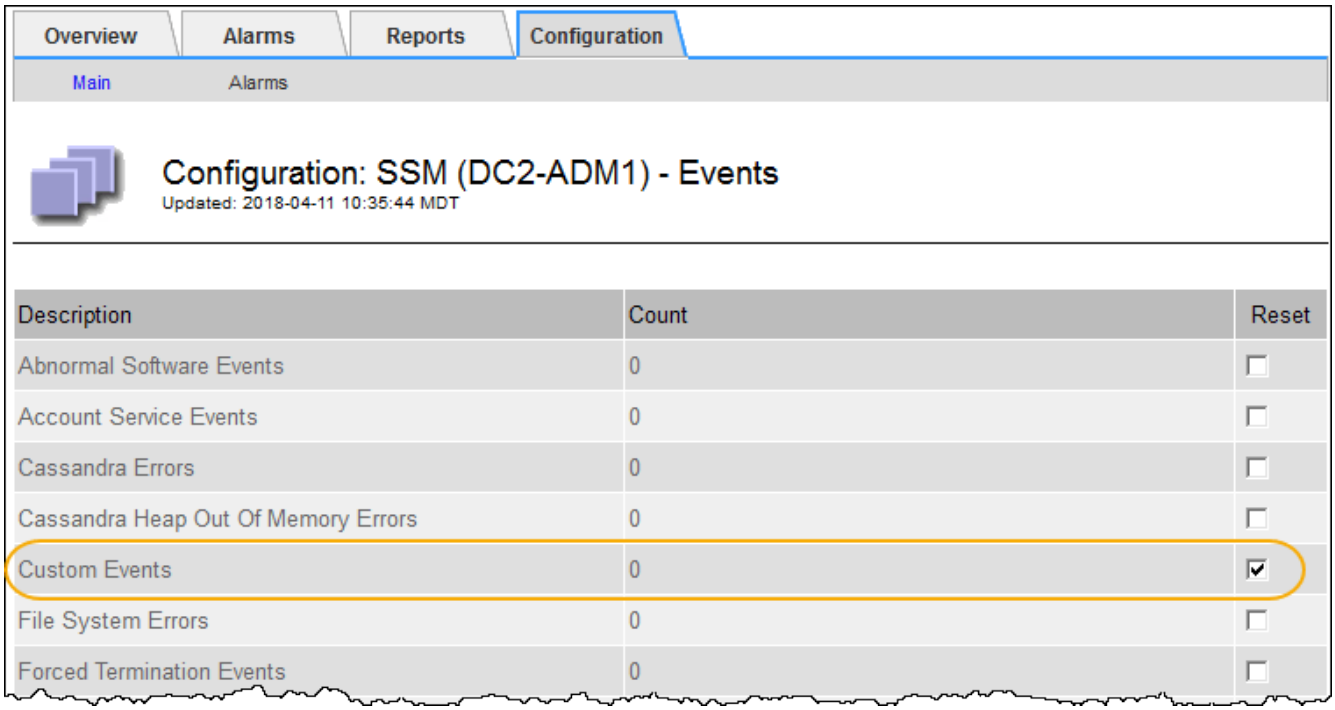
将自定义事件计数重置为零

如果只想重置自定义事件的计数器，则必须使用支持菜单中的网格拓扑页面。

关于此任务

重置计数器会导致下一个事件触发警报。相反，确认警报时，只有在达到下一阈值级别时才会重新触发该警报。

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 ***GRID NODE*** > * SSM* > * 事件 * > * 配置 * > * 主 * 。
3. 选中自定义事件的 * 重置 * 复选框。



4. 选择 * 应用更改 * 。

查看审核消息

审核消息可帮助您更好地了解 StorageGRID 系统的详细操作。您可以使用审核日志对问题进行故障排除并评估性能。

在系统正常运行期间，所有 StorageGRID 服务都会生成审核消息，如下所示：

- 系统审核消息与审核系统本身，网格节点状态，系统范围的任务活动和服务备份操作相关。
- 对象存储审核消息与 StorageGRID 中对象的存储和管理相关，包括对象存储和检索，网格节点到网格节点的传输以及验证。
- 当 S3 或 Swift 客户端应用程序请求创建，修改或检索对象时，系统会记录客户端读写审核消息。
- 管理审核消息会将用户请求记录到管理 API 。

每个管理节点都会将审核消息存储在文本文件中。审核共享包含活动文件（ audit.log ）以及前几天压缩的审核日志。网格中的每个节点还会存储在该节点上生成的审核信息的副本。

为了便于访问审核日志，您可以为 NFS 和 CIFS 配置客户端对审核共享的访问权限（ CIFS 已弃用）。您也可以直接从管理节点的命令行访问审核日志文件。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

有关审核日志文件的详细信息，审核消息的格式，审核消息的类型以及可用于分析审核消息的工具，请参见审核消息的说明。要了解如何配置审核客户端访问，请参见有关管理 StorageGRID 的说明。

相关信息

查看审核日志

收集日志文件和系统数据

您可以使用网格管理器检索 StorageGRID 系统的日志文件和系统数据（包括配置数据）。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须具有配置密码短语。

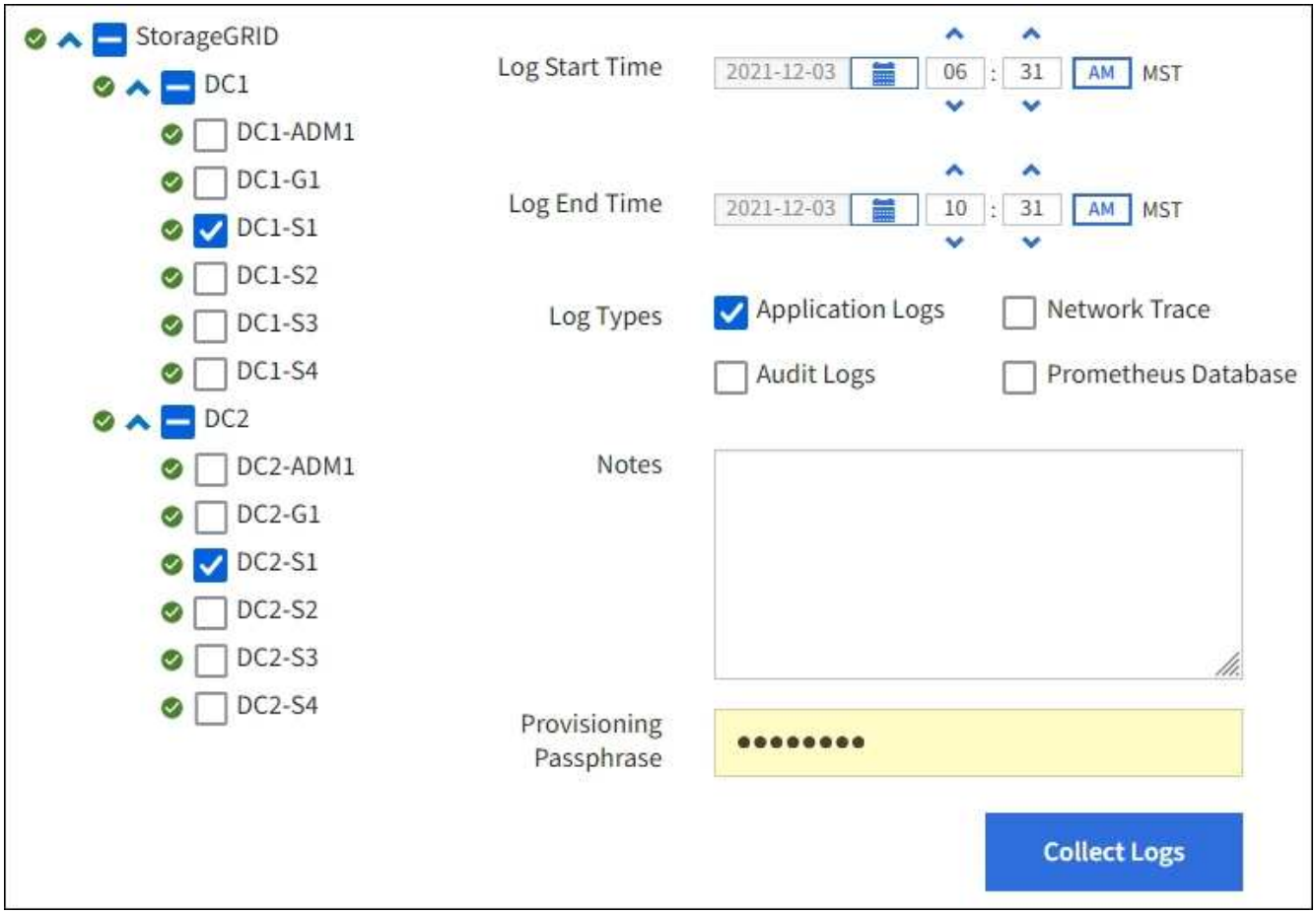
关于此任务

您可以使用网格管理器收集 日志文件选定时间段内任何网格节点的系统数据和配置数据。数据会收集并归档在 .tar.gz 文件中，然后可下载到本地计算机。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

步骤

1. 选择 * 支持 * > * 工具 * > * 日志 * 。



2. 选择要收集日志文件的网格节点。

   您可以根据需要收集整个网格或整个数据中心站点的日志文件。

3. 选择 * 开始时间 * 和 * 结束时间 * 以设置要包含在日志文件中的数据的时间范围。

   如果选择很长的时间段或从大型网格中的所有节点收集日志，则日志归档可能会变得过大，无法存储在节点上，或者可能会变得过大，无法收集到主管理节点以供下载。如果发生这种情况，您必须使用一组较小的数据重新启动日志收集。

4. 选择要收集的日志类型。
   - * 应用程序日志 * ： 技术支持最常用于故障排除的应用程序特定日志。收集的日志是可用应用程序日志的一部分。
   - * 审核日志 * ： 包含在正常系统操作期间生成的审核消息的日志。
   - * 网络跟踪 * ： 用于网络调试的日志。
   - * Prometheus Database* ： 所有节点上的服务的时间序列指标。
5. 或者，也可以在 * 注释 * 文本框中输入有关要收集的日志文件的注释。

   您可以使用这些注释提供有关提示您收集日志文件的问题的技术支持信息。您的注释以及有关日志文件收集的其他信息将添加到名为 `info.txt` 的文件中。`info.txt` 文件保存在日志文件归档包中。

6. 在 * 配置密码短语 * 文本框中输入 StorageGRID 系统的配置密码短语。
7. 选择 * 收集日志 * 。

   提交新请求时，系统将删除先前收集的日志文件。

   您可以使用日志页面监控每个网格节点的日志文件收集进度。

   如果您收到有关日志大小的错误消息，请尝试收集较短时间段或较少节点的日志。

8. 日志文件收集完成后，选择 * 下载 * 。

   .tar.gz 文件包含成功收集日志的所有网格节点中的所有日志文件。在组合的 *.tar.gz* 文件中，每个网格节点有一个日志文件归档。

完成后

如果需要，您可以稍后重新下载日志文件归档包。

您也可以选择 * 删除 * 以删除日志文件归档软件包并释放磁盘空间。下次收集日志文件时，系统会自动删除当前日志文件归档包。

手动触发 **AutoSupport** 消息

为了帮助技术支持解决 StorageGRID 系统的问题，您可以手动触发要发送的 AutoSupport 消息。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

2. 选择 * 发送用户触发的 AutoSupport * 。

   StorageGRID 尝试向技术支持发送 AutoSupport 消息。如果尝试成功，则会更新 * 结果 * 选项卡上的 * 最新结果 * 和 * 最后成功时间 * 值。如果出现问题， * 最新结果 * 值将更新为 " 失败 " ， StorageGRID 不会再尝试发送 AutoSupport 消息。

   发送用户触发的 AutoSupport 消息后，请在 1 分钟后刷新浏览器中的 AutoSupport 页面以访问最新结果。

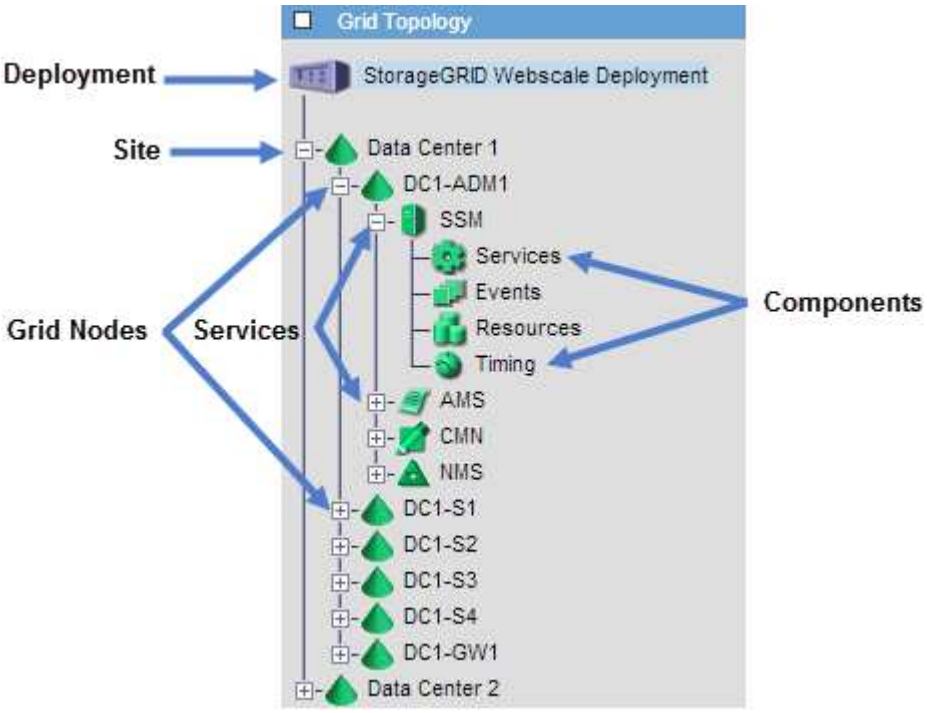
相关信息

为警报配置电子邮件服务器设置（旧系统）

查看网格拓扑树

通过网格拓扑树，您可以访问有关 StorageGRID 系统元素的详细信息，包括站点，网格节点，服务和组件。在大多数情况下，只有在文档中说明或与技术支持合作时，您才需要访问网格拓扑树。

要访问网格拓扑树，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。



要展开或折叠网格拓扑树，请单击 ⊞ 或 ⊟ 在站点，节点或服务级别。要展开或折叠整个站点或每个节点中的所有项，请按住 * 键 * 并单击。

查看支持指标

对问题描述 进行故障排除时，您可以与技术支持人员一起查看 StorageGRID 系统的详细

指标和图表。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

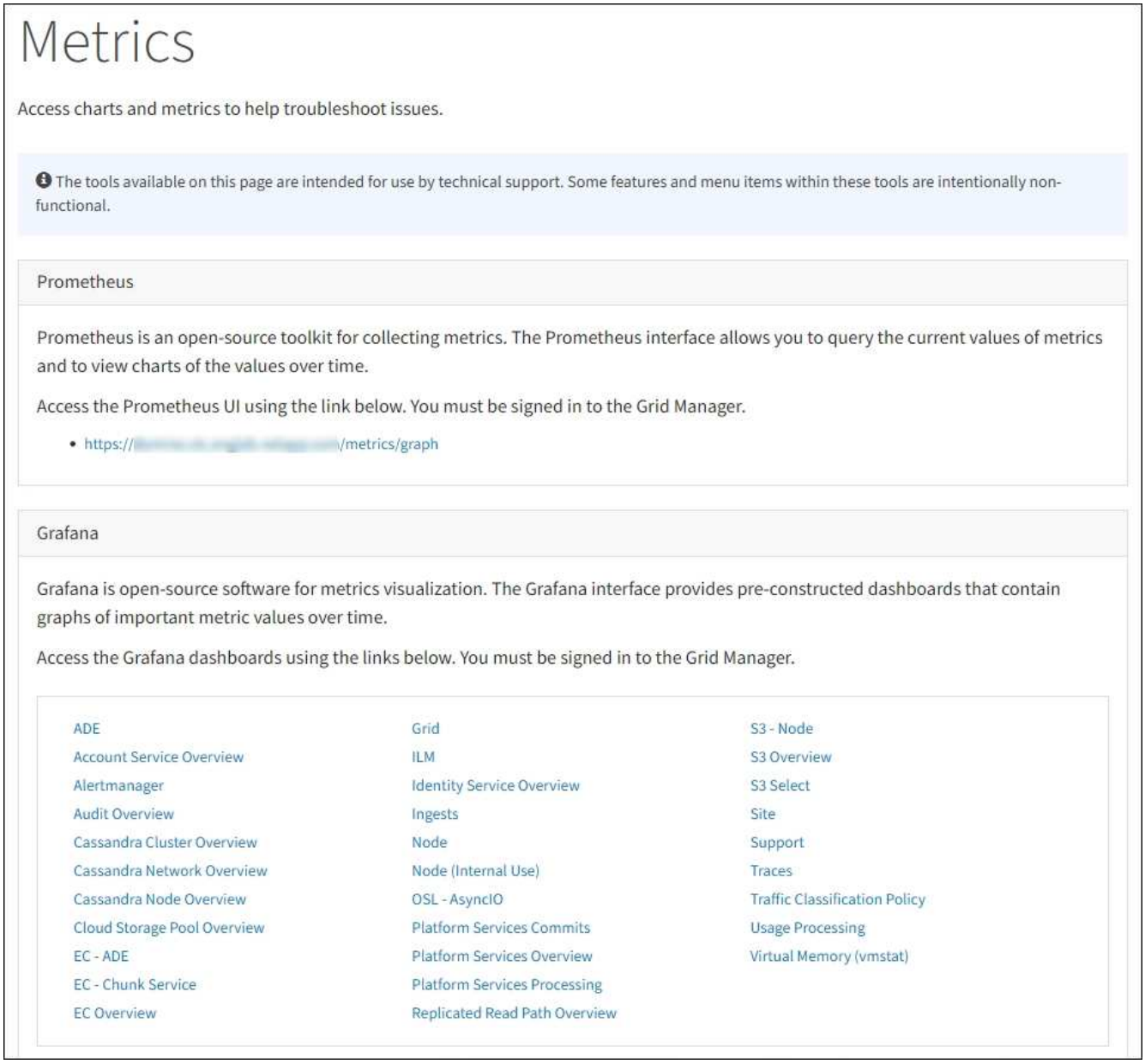
您可以通过指标页面访问 Prometheus 和 Grafana 用户界面。Prometheus 是用于收集指标的开源软件。Grafana 是用于可视化指标的开源软件。

> 指标页面上提供的工具供技术支持使用。这些工具中的某些功能和菜单项有意不起作用，可能会发生更改。请参见列表 常用的 Prometheus 指标。

步骤

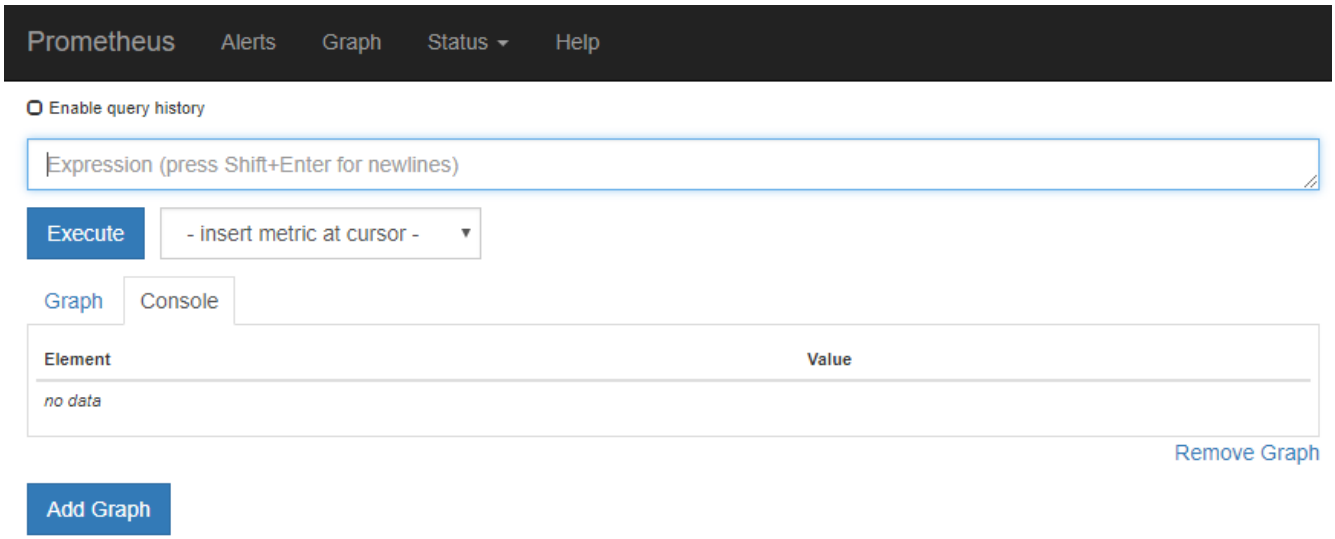
1. 根据技术支持的指示，选择 * 支持 * > * 工具 * > * 指标 * 。

   下面显示了 " 指标 " 页面的一个示例：



2. 要查询 StorageGRID 指标的当前值并查看随时间变化的值图形，请单击 Prometheus 部分中的链接。

   此时将显示 Prometheus 界面。您可以使用此界面对可用的 StorageGRID 指标执行查询，并绘制一段时间内的 StorageGRID 指标图。



名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间可能会发生更改，恕不另行通知。

3. 要访问包含一段时间内 StorageGRID 指标图的预构建信息板，请单击 Grafana 部分中的链接。

   此时将显示选定链接的 Grafana 界面。



Run diagnostics

在对问题描述 进行故障排除时，您可以与技术支持一起在 StorageGRID 系统上运行诊断并查看结果。

- 查看支持指标
- 常用的 Prometheus 指标

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。

关于此任务

" 诊断 " 页面会对网格的当前状态执行一组诊断检查。每个诊断检查可以具有以下三种状态之一：

-

* 正常 * ：所有值均在正常范围内。

- * 注意 * ：一个或多个值超出正常范围。
- * 小心 * ：一个或多个值明显超出正常范围。

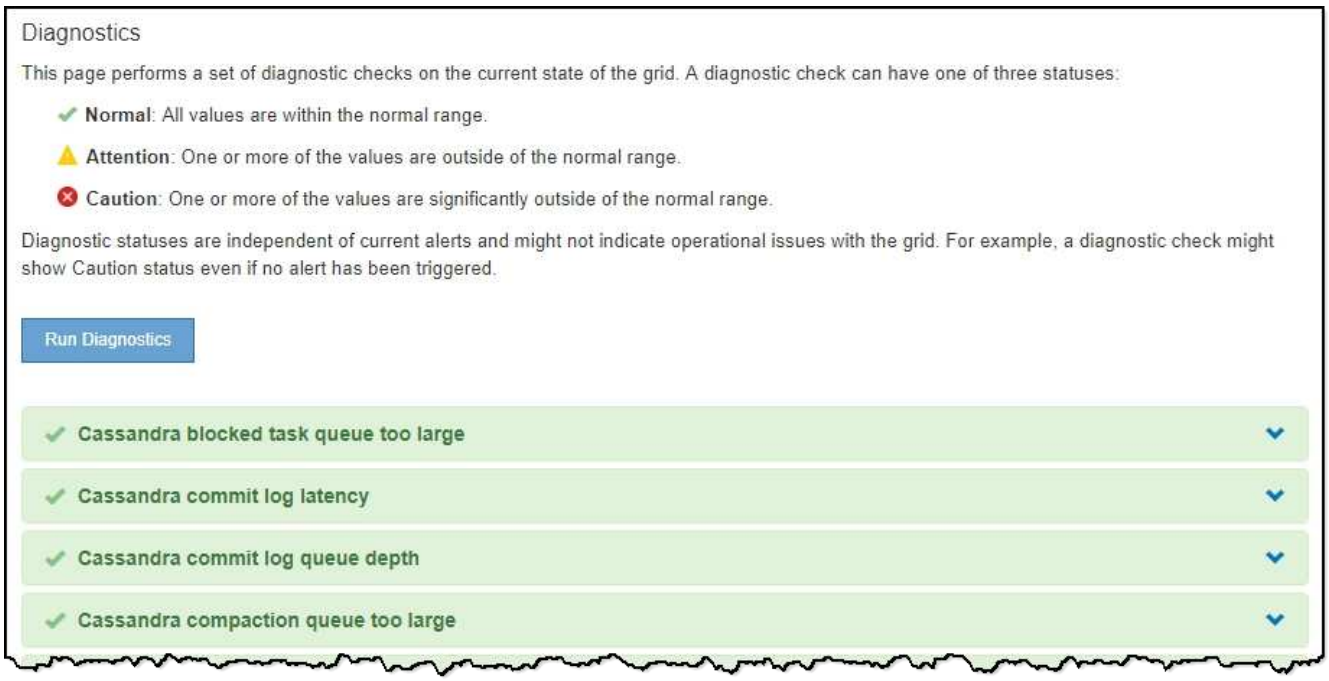
诊断状态与当前警报无关，可能并不表示网格存在操作问题。例如，即使未触发任何警报，诊断检查也可能会显示 " 小心 " 状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 诊断 * 。

   此时将显示 "Diagnostics " 页面，其中列出了每个诊断检查的结果。结果将按严重性（ " 小心 " ， " 注意 " 和 " 正常 " ）进行排序。在每个严重性范围内，结果按字母顺序排序。

   在此示例中，所有诊断均处于正常状态。



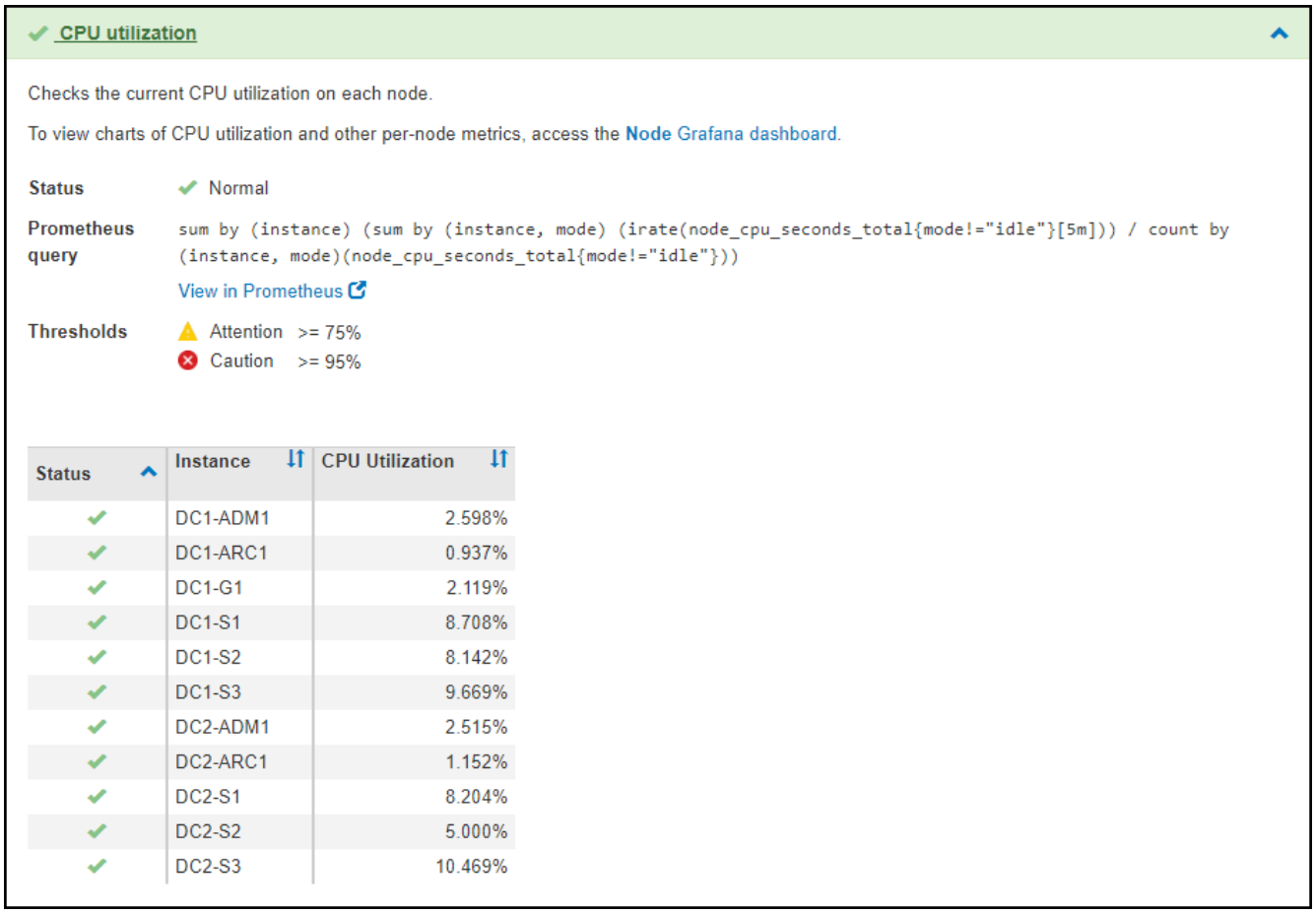
2. 要了解有关特定诊断的详细信息，请单击行中的任意位置。

   此时将显示有关此诊断及其当前结果的详细信息。此时将列出以下详细信息：

   - * 状态 * ：此诊断的当前状态：正常，注意或小心。
   - * 项目查询 * ：如果用于诊断，则为用于生成状态值的 Prometheus 表达式。（并非所有诊断都使用 Prometheus 表达式。）
   - * 阈值 * ：如果可用于诊断，则为每个异常诊断状态提供系统定义的阈值。（并非所有诊断都使用阈值。）

     您不能更改这些阈值。

   - * 状态值 * ：显示整个 StorageGRID 系统中诊断的状态和值的表。在此示例中，显示了 StorageGRID 系统中每个节点的当前 CPU 利用率。所有节点值均低于警示和警示阈值，因此诊断的整体状态为正常。



3. * 可选 * ： 要查看与此诊断相关的 Grafana 图表，请单击 * Grafana dashboard* 链接。

   并非所有诊断都显示此链接。

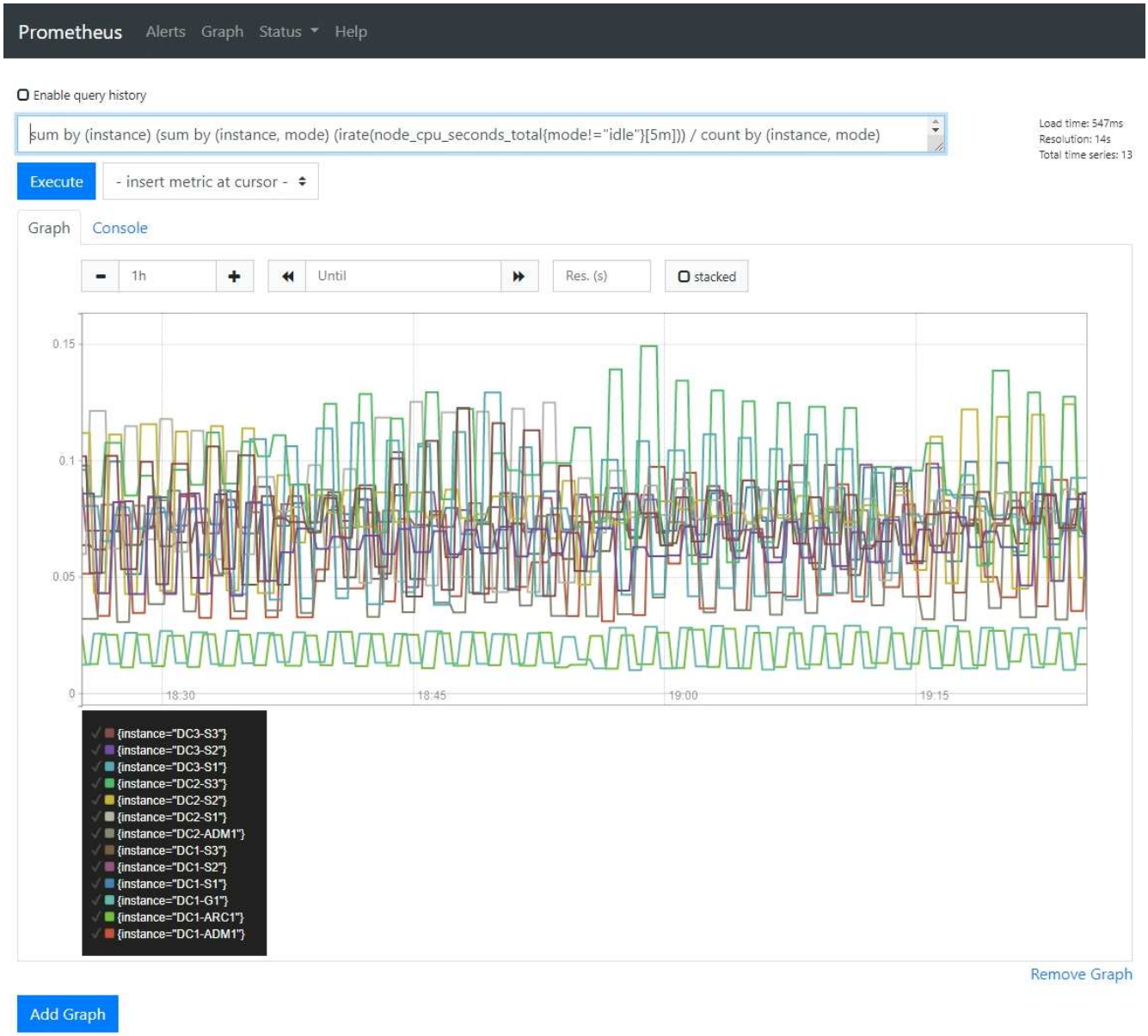
   此时将显示相关的 Grafana 信息板。在此示例中，将显示节点信息板，其中显示了此节点的 CPU 利用率随时间变化以及此节点的其他 Grafana 图表。

   > 您也可以从 * 支持 * > * 工具 * > * 指标 * 页面的 Grafana 部分访问预构建的 Grafana 信息板。



4. * 可选 * ： 要查看一段时间内的 Prometheus 表达式图表，请单击 * 在 Prometheus* 中查看。

   此时将显示诊断中使用的表达式的 Prometheus 图形。



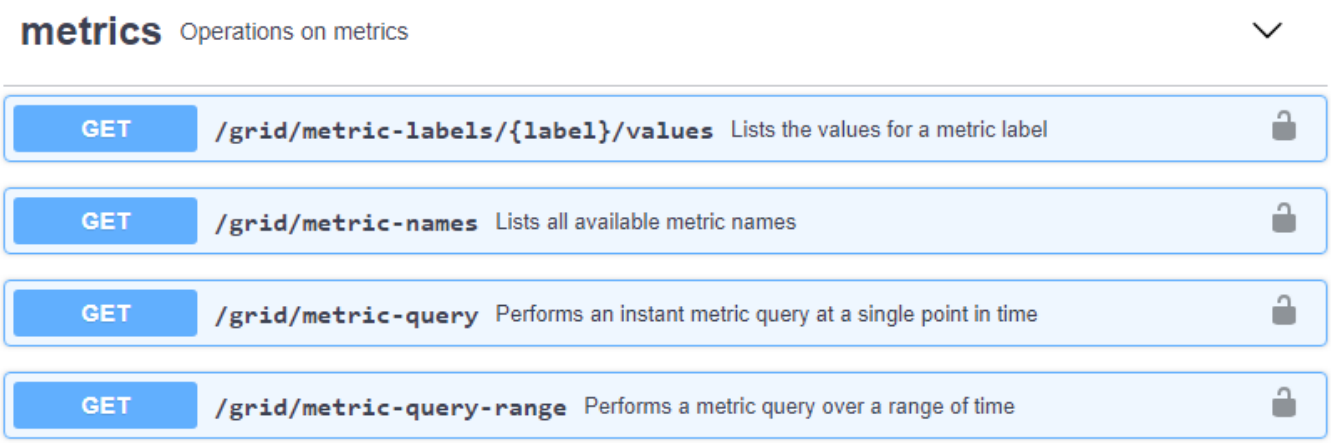
创建自定义监控应用程序

您可以使用网格管理 API 提供的 StorageGRID 指标构建自定义监控应用程序和信息板。

如果要监控网格管理器的现有页面上未显示的指标，或者要为 StorageGRID 创建自定义信息板，则可以使用网格管理 API 查询 StorageGRID 指标。

您还可以直接使用外部监控工具（例如 Grafana ）访问 Prometheus 指标。使用外部工具时，您需要上传或生成管理客户端证书，以使 StorageGRID 能够对该工具进行身份验证以确保安全性。请参见 有关管理 StorageGRID 的说明。

要查看指标 API 操作，包括可用指标的完整列表，请转到网格管理器。从页面顶部，选择帮助图标并选择 * API Documentation* > * 指标 * 。



本文档不会详细介绍如何实施自定义监控应用程序。

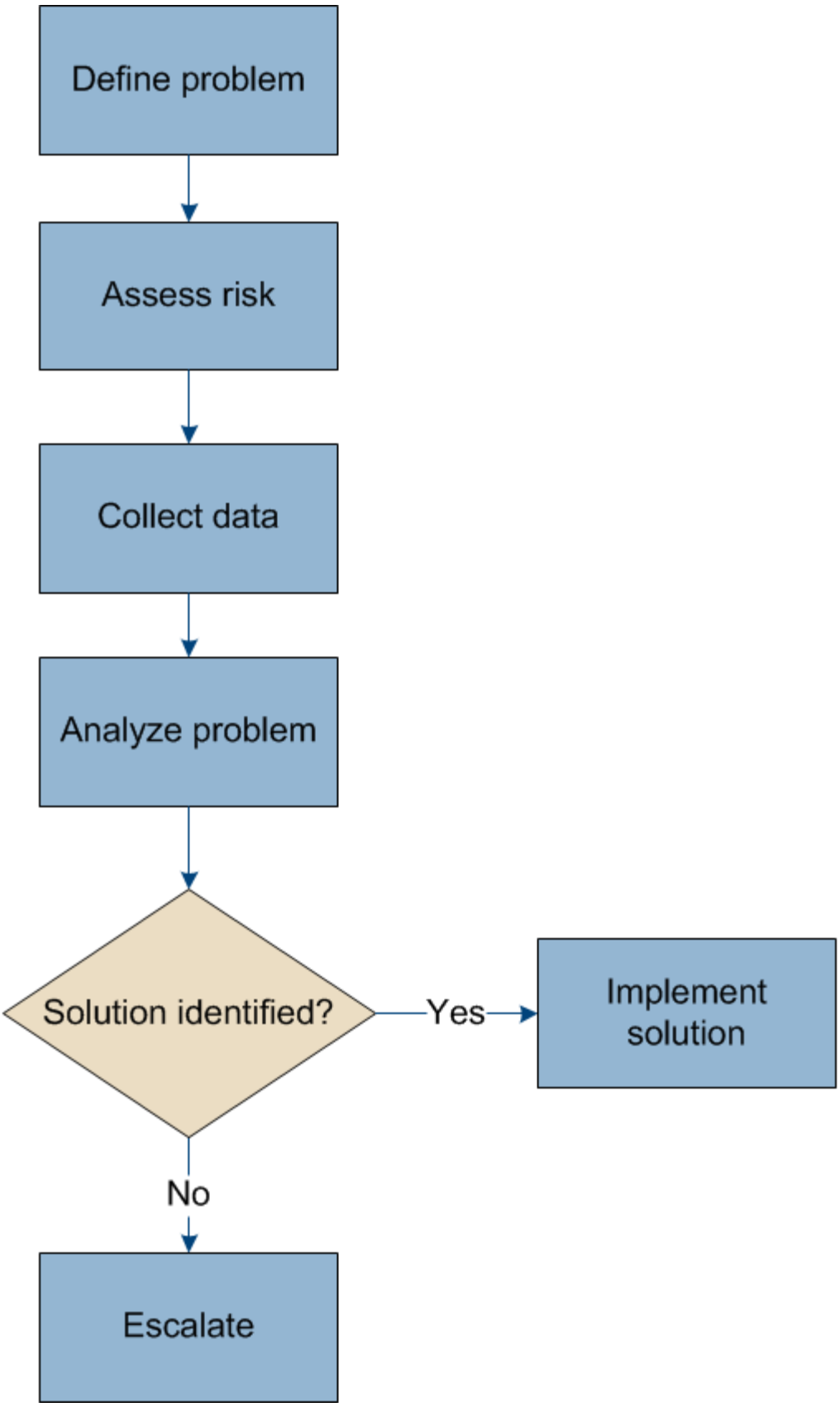
对 StorageGRID 系统进行故障排除

对 **StorageGRID** 系统进行故障排除

如果在使用 StorageGRID 系统时遇到问题，请参阅本节中的提示和准则，以帮助确定和解决问题描述 。

问题确定概述

如果遇到问题，请执行此操作 管理 StorageGRID 系统，您可以使用此图中概述的过程来识别和分析问题描述 。在许多情况下，您可以自行解决问题；但是，您可能需要将某些问题上报给技术支持。



定义问题

解决问题的第一步是明确定义问题。

下表提供了定义问题时可能收集的信息类型示例：

问题	响应示例
StorageGRID 系统正在执行什么操作或不执行什么操作？其症状是什么？	客户端应用程序报告无法将对象载入 StorageGRID 。
问题是从何时开始的？	对象载入于 2020 年 1 月 8 日 14： 50 时被首次拒绝。
您是如何首次注意到该问题的？	客户端应用程序已通知。同时还收到警报电子邮件通知。
问题是持续发生还是仅偶尔发生？	问题仍在继续。
如果此问题经常发生，则说明发生发生原因 的步骤是什么	每次客户端尝试载入对象时都会发生问题。
如果此问题间歇性发生，何时发生？记录您所知的每个意外事件的时间。	问题不是间歇性的。
您以前是否遇到过此问题？您过去遇到此问题的频率如何？	这是我第一次看到此问题描述 。

评估风险和对系统的影响

定义问题后，请评估其对 StorageGRID 系统的风险和影响。例如，存在严重警报并不一定意味着系统不提供核心服务。

下表总结了示例问题对系统操作的影响：

问题	响应示例
StorageGRID 系统是否可以载入内容？	否
客户端应用程序是否可以检索内容？	可以检索某些对象，而不能检索其他对象。
数据是否存在风险？	否
开展业务的能力是否受到严重影响？	可以，因为客户端应用程序无法将对象存储到 StorageGRID 系统，并且无法一致地检索数据。

收集数据

定义问题并评估其风险和影响后，收集数据以供分析。最有用的数据类型取决于问题的性质。

要收集的数据类型	为什么收集此数据	说明
创建最近更改的时间线	对 StorageGRID 系统，其配置或环境进行更改可以发生原因 新行为。	• 创建最近更改的时间线
查看警报和警报	警报和警报可通过提供有关可能导致问题的根本问题的重要线索，帮助您快速确定问题的根本发生原因 。 查看当前警报和警报列表，查看 StorageGRID 是否已确定问题的根发生原因 。 查看过去触发的警报和警报，以获得更多见解。	• 查看当前警报 • 查看旧警报 • 查看已解决的警报 • 查看历史警报和警报频率（传统系统）
监控事件	事件包括节点的任何系统错误或故障事件，包括网络错误等错误。监控事件以了解有关问题的更多信息或帮助进行故障排除。	• 监控事件
使用图表和文本报告确定趋势	趋势可以提供有关问题首次出现的宝贵线索，并有助于您了解事情发生的速度。	• 使用图表和图形 • 使用文本报告
建立基线	收集有关各种运行值的正常级别的信息。这些基线值以及与这些基线的偏差可以提供有价值的线索。	• 建立基线
执行载入和检索测试	要解决载入和检索的性能问题，请使用工作站存储和检索对象。将结果与使用客户端应用程序时看到的结果进行比较。	• 监控 PUT 和 GET 性能
查看审核消息	查看审核消息以详细了解 StorageGRID 操作。审核消息中的详细信息对于排除包括性能问题在内的多种类型的问题非常有用。	• 查看审核消息
检查对象位置和存储完整性	如果存在存储问题，请验证对象是否已放置在预期位置。检查存储节点上对象数据的完整性。	• 监控对象验证操作 • 确认对象数据位置 • 验证对象完整性
为技术支持收集数据	技术支持可能会要求您收集数据或查看特定信息，以帮助您解决问题。	• 收集日志文件和系统数据 • 手动触发 AutoSupport 消息 • 查看支持指标

【create_timeline】创建最近更改的时间线

出现问题时，您应考虑最近发生了哪些更改以及何时发生了这些更改。

- 对 StorageGRID 系统，其配置或环境进行更改可以发生原因 新行为。

- 更改时间线可以帮助您确定哪些更改可能会对问题描述 造成影响，以及每个更改可能会对其开发产生何种影响。

创建一个系统近期更改的表，其中包含有关每次更改发生时间的信息以及有关更改的任何相关详细信息，以及有关更改进行期间发生的其他情况的信息：

更改时间	更改类型	详细信息
例如： • 您何时开始节点恢复？ • 软件升级何时完成？ • 您是否中断了此过程？	发生什么事了？您做了什么？	记录有关变更的任何相关详细信息。例如： • 网络更改的详细信息。 • 安装了哪个修补程序。 • 客户端工作负载如何更改。 请务必注意，如果同时发生多个更改。例如，是否在升级过程中进行了此更改？

近期重大变更的示例

以下是一些可能会发生重大变化的示例：

- StorageGRID 系统是最近安装，扩展还是恢复的？
- 系统近期是否已升级？是否应用了修补程序？
- 最近是否修复或更改过任何硬件？
- 是否已更新 ILM 策略？
- 客户端工作负载是否已更改？
- 客户端应用程序或其行为是否发生变化？
- 您是否更改了负载平衡器，添加或删除了管理节点或网关节点的高可用性组？
- 是否已启动可能需要很长时间才能完成的任务？示例包括：
  - 恢复发生故障的存储节点
  - 存储节点停用
- 是否对用户身份验证进行了任何更改，例如添加租户或更改 LDAP 配置？
- 是否正在进行数据迁移？
- 最近是否启用或更改了平台服务？
- 最近是否启用了合规性？
- 是否已添加或删除云存储池？
- 是否对存储压缩或加密进行了任何更改？
- 网络基础架构是否有任何变化？例如， VLAN ，路由器或 DNS 。
- 是否对 NTP 源进行了任何更改？

- 是否对网格，管理员或客户端网络接口进行了任何更改？
- 是否对归档节点进行了任何配置更改？
- 是否对 StorageGRID 系统或其环境进行了任何其他更改？

【建立基线】建立基线

您可以通过记录各种运行值的正常级别来为系统建立基线。将来，您可以将当前值与这些基线进行比较，以帮助检测和解决异常值。

属性	价值	如何获取
平均存储消耗	GB 已用 / 天 每日消耗百分比	转到网格管理器。在节点页面上，选择整个网格或站点，然后转到存储选项卡。 在 " 已用存储 - 对象数据 " 图表上，找到一个线相当稳定的句点。将光标悬停在图表上方可估计每天占用的存储空间量 您可以收集整个系统或特定数据中心的此信息。
平均元数据消耗	GB 已用 / 天 每日消耗百分比	转到网格管理器。在节点页面上，选择整个网格或站点，然后转到存储选项卡。 在 " 已用存储 - 对象元数据 " 图表上，找到一个线相当稳定的句点。将光标悬停在图表上方，可估算每天占用的元数据存储量 您可以收集整个系统或特定数据中心的此信息。
S3/Swift 操作速率	操作数 / 秒	转到网格管理器中的信息板。在协议操作部分中，查看 S3 速率和 Swift 速率的值。 要查看特定站点或节点的载入率和检索率以及计数，请选择 * 节点 * > * 站点或存储节点 _* > * 对象 * 。将光标悬停在 Insest and retrieve 图表上，查看 S3 或 Swift 的图表。
S3/Swift 操作失败	操作	选择 * 支持 * > * 工具 * > * 网格拓扑 * 。在 API Operations 部分的 Overview 选项卡上，查看 S3 Operations - Failed 或 Swift Operations - Failed 的值。

属性	价值	如何获取
ILM 评估率	对象 / 秒	从节点页面中，选择 * ； grid_* > * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标悬停在图表上方可估算系统的 * 评估速率 * 基线值。
ILM 扫描速率	对象 / 秒	选择 * 节点 * > * 网格 _* > * ILM * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标悬停在图表上方可估算系统的 * 扫描速率 * 基线值。
从客户端操作排队的对象	对象 / 秒	选择 * 节点 * > * 网格 _* > * ILM * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标悬停在图表上方，可估算系统中 * 已排队（从客户端操作） * 的对象的基线值。
平均查询延迟	毫秒	选择 * 节点 * > * 存储节点 _* > * 对象 * 。在查询表中，查看平均延迟的值。

分析数据

使用您收集的信息确定问题的发生原因 以及可能的解决方案。

分析与问题 - 相关，但一般而言：

- 使用警报查找故障点和瓶颈。
- 使用警报历史记录和图表重建问题历史记录。
- 使用图表查找异常并将问题情况与正常运行进行比较。

上报信息检查清单

如果您无法自行解决此问题，请联系技术支持。在联系技术支持之前，请收集下表中列出的信息，以便于解决问题。

✔	项目	注释：
	问题陈述	问题症状是什么？问题是从何时开始的？是否持续或间歇性发生？如果间歇性发生，发生过什么时间？ 定义问题
	影响评估	问题的严重性是什么？对客户端应用程序有何影响？ • 客户端以前是否已成功连接？ • 客户端是否可以载入，检索和删除数据？
	StorageGRID 系统 ID	选择 * 维护 * > * 系统 * > * 许可证 * 。StorageGRID 系统 ID 显示为当前许可证的一部分。
	软件版本	从网格管理器顶部，选择帮助图标并选择 * 关于 * 以查看 StorageGRID 版本。
	自定义	总结 StorageGRID 系统的配置方式。例如，列出以下内容： • 网格是否使用存储压缩，存储加密或合规性？ • ILM 是否会创建复制或擦除编码对象？ILM 是否可确保站点冗余？ILM 规则是否使用严格，平衡或双重提交载入行为？
	日志文件和系统数据	收集系统的日志文件和系统数据。选择 * 支持 * > * 工具 * > * 日志 * 。 您可以收集整个网格或选定节点的日志。 如果仅收集选定节点的日志，请确保至少包含一个具有此 ADA 服务的存储节点。（一个站点的前三个存储节点包含此 ADC-Service 。） 收集日志文件和系统数据
	基线信息	收集有关载入操作，检索操作和存储消耗的基线信息。 建立基线
	最近更改的时间线	创建一个时间线，用于汇总系统或其环境的所有近期更改。 创建最近更改的时间线

✔	项目	注释：
	诊断问题描述 的工作历史记录	如果您已自行采取步骤对问题描述 进行诊断或故障排除，请务必记录所采取的步骤和结果。

对对象和存储问题进行故障排除

确认对象数据位置

根据问题，您可能需要确认对象数据的存储位置。例如，您可能需要验证 ILM 策略是否按预期执行，以及对象数据是否按预期存储。

您需要的内容

- 您必须具有一个对象标识符，该标识符可以是以下项之一：
  - * UUID * ： 对象的通用唯一标识符。以全大写形式输入 UUID 。
  - * CBID* ： StorageGRID 中对象的唯一标识符。您可以从审核日志中获取对象的 CBID 。输入全部大写的 CBID 。
  - * S3 存储分段和对象密钥 * ： 通过 S3 接口载入对象时，客户端应用程序使用存储和标识对象的分段和对象密钥组合。
  - * Swift 容器和对象名称 * ： 通过 Swift 界面输入对象时，客户端应用程序将使用容器和对象名称组合来存储和标识对象。

步骤

1. 选择 * ILM * > * 对象元数据查找 * 。
2. 在 * 标识符 * 字段中键入对象的标识符。

   您可以输入 UUID ， CBID ， S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称。

3. 如果要查找对象的特定版本，请输入版本 ID （可选）。



4. 选择 * 查找 * 。

此时将显示对象元数据查找结果。此页面列出了以下类型的信息：

- 系统元数据，包括对象 ID （ UUID ），版本 ID （可选），对象名称，容器名称，租户帐户名称或 ID ，对象的逻辑大小，首次创建对象的日期和时间以及上次修改对象的日期和时间。
- 与对象关联的任何自定义用户元数据键值对。
- 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
- 对于复制的对象副本，为每个副本提供当前存储位置。
- 对于经过擦除编码的对象副本，为每个片段的当前存储位置。
- 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。
- 对于分段对象和多部分对象，包含分段标识符和数据大小的对象分段列表。对于包含 100 个以上区块的对象，仅显示前 100 个区块。
- 所有对象元数据均采用未处理的内部存储格式。此原始元数据包括内部系统元数据，不能保证这些元数据在版本之间持续存在。

  以下示例显示了存储为两个复制副本的 S3 测试对象的对象元数据查找结果。

System Metadata

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

Replicated Copies

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

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


相关信息

使用 ILM 管理对象

使用 S3

使用 Swift

对象存储（存储卷）故障

存储节点上的底层存储分为多个对象存储。对象存储也称为存储卷。

您可以查看每个存储节点的对象存储信息。对象存储显示在 * 节点 * > * 存储节点 _* > * 存储 * 页面的底部。

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

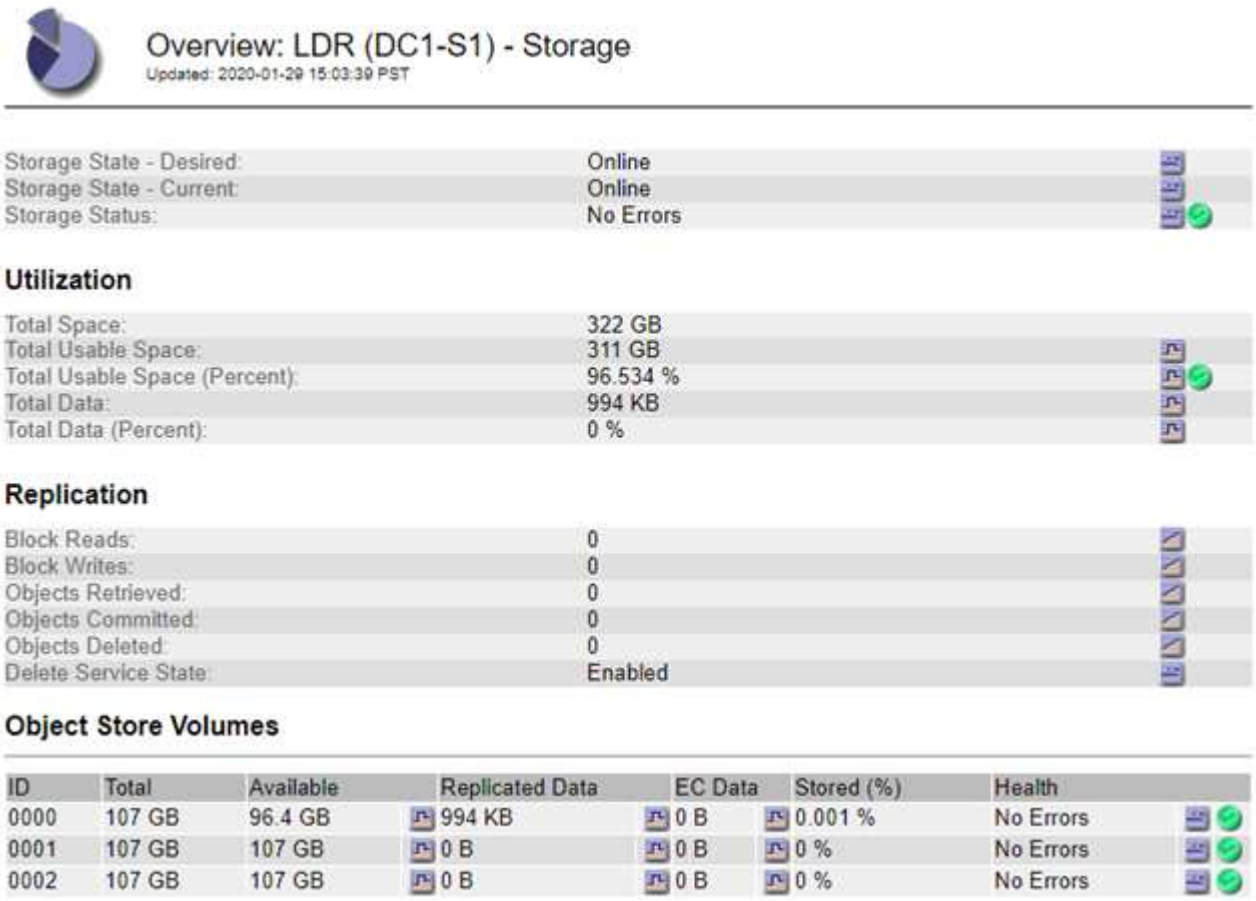
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	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

要查看有关每个存储节点的更多详细信息，请执行以下步骤：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 存储 * > * 概述 * > * 主 * 。



根据故障的性质，存储卷的故障可能会反映在有关存储状态或对象存储运行状况的警报中。如果存储卷发生故障，您应尽快修复故障存储卷，以将存储节点还原到完整功能。如有必要，您可以转到 * 配置 * 选项卡并将存储节点置于只读 - 状态，以便 StorageGRID 系统可以在准备服务器完全恢复时使用它进行数据检索。

相关信息

恢复和维护

验证对象完整性

StorageGRID 系统会验证存储节点上对象数据的完整性，并检查是否存在损坏和缺失的对象。

验证过程有两个：后台验证和对象存在检查（以前称为前台验证）。它们协同工作，确保数据完整性。后台验证会自动运行，并持续检查对象数据的正确性。用户可以触发对象存在检查，以便更快速地验证对象是否存在（尽管不是正确）。

什么是后台验证？

后台验证过程会自动持续检查存储节点中是否存在损坏的对象数据副本，并自动尝试修复发现的任何问题。

后台验证将检查复制对象和经过纠删编码的对象的完整性，如下所示：

- * 复制对象 * ：如果后台验证过程发现复制的对象已损坏，则损坏的副本将从其位置中删除，并隔离到存储节点上的其他位置。然后，系统将生成一个未损坏的新副本并放置该副本以满足活动 ILM 策略的要求。新副本可能不会放置在用于原始副本的存储节点上。

> 损坏的对象数据将被隔离而不是从系统中删除，以便仍可访问。有关访问隔离对象数据的详细信息，请联系技术支持。

- * 擦除编码对象 * ：如果后台验证过程检测到擦除编码对象的片段已损坏，则 StorageGRID 会自动尝试使用剩余的数据和奇偶校验片段在同一个存储节点上原位重建缺失的片段。如果损坏的片段无法重建，则会尝试检索对象的另一个副本。如果检索成功，则会执行 ILM 评估以创建经过纠删编码的对象的替代副本。

  后台验证过程仅检查存储节点上的对象。它不会检查归档节点或云存储池中的对象。对象必须超过四天，才能进行后台验证。

后台验证以连续速率运行，不会干扰普通系统活动。无法停止后台验证。但是，如果您怀疑存在问题，则可以提高后台验证率，以便更快地验证存储节点的内容。

与后台验证相关的警报和警报（传统）

如果系统检测到某个损坏的对象，而该对象无法自动更正（因为该损坏会阻止识别该对象），则会触发 * 检测到未标识的损坏对象 * 警报。

如果后台验证无法替换损坏的对象，因为它找不到其他副本，则会触发 * 对象丢失 * 警报。

更改后台验证速率

如果您担心数据完整性，可以更改后台验证检查存储节点上复制的对象数据的速率。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

您可以更改存储节点上用于后台验证的验证速率：

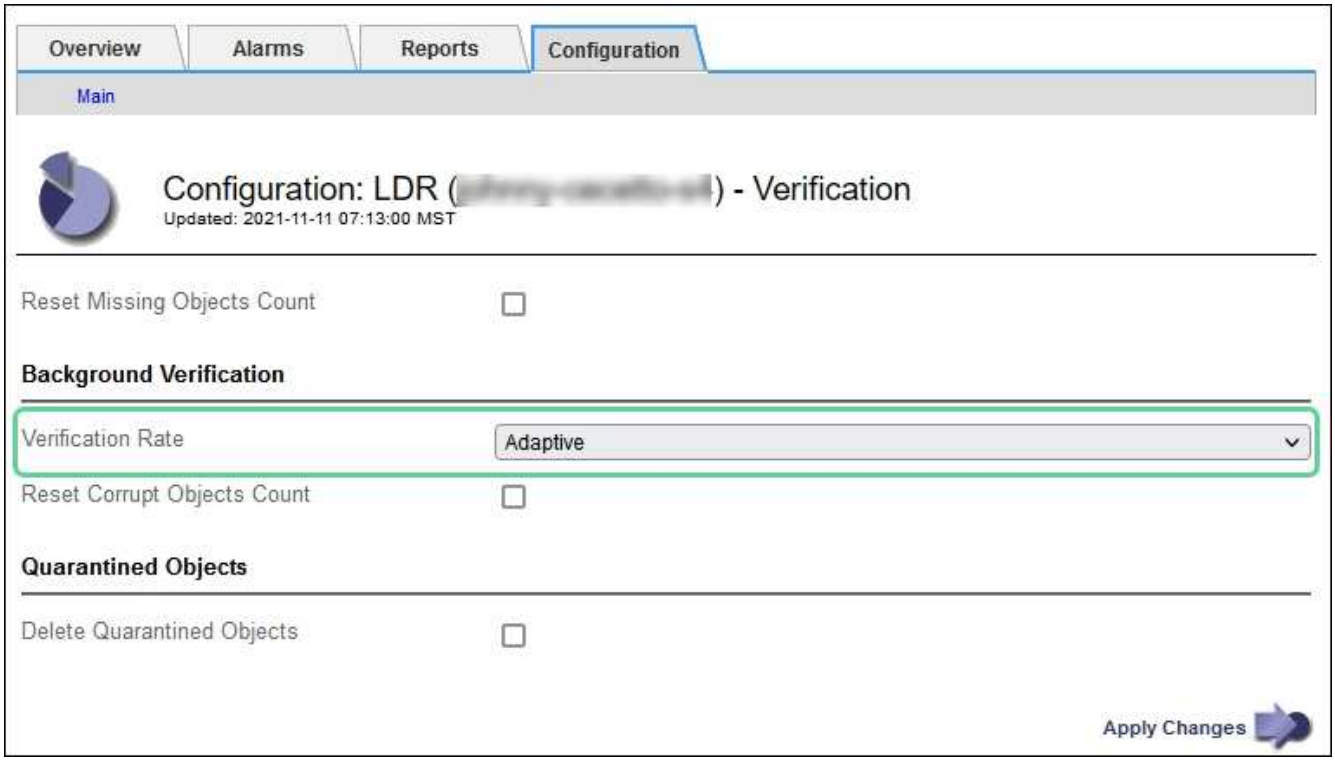
- Adaptive ： 默认设置。此任务用于验证速度最多为 4 MB/ 秒或 10 个对象 / 秒（以先超过者为准）。
- high ： 存储验证进展迅速，速度可能会减慢常规系统活动。

只有当您怀疑硬件或软件故障可能包含损坏的对象数据时，才使用 " 高 " 验证率。高优先级后台验证完成后，验证率将自动重置为自适应。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 存储节点 _* > * LDR* > * 验证 * 。
3. 选择 * 配置 * > * 主 * 。
4. 转至 * LDR* > * 验证 * > * 配置 * > * 主 * 。

5. 在后台验证下，选择 * 验证速率 * > * 高 * 或 * 验证速率 * > * 自适应 * 。



将验证速率设置为高会在通知级别触发 VPRi （验证速率）传统警报。

6. 单击 * 应用更改 * 。
7. 监控复制对象的后台验证结果。
   a. 转至 * 节点 * > * 存储节点 _* > * 对象 * 。
   b. 在验证部分中，监控 * 损坏对象 * 和 * 未标识的损坏对象 * 的值。

      如果后台验证发现复制的对象数据损坏，则 * 损坏的对象 * 指标将递增， StorageGRID 将尝试从数据中提取对象标识符，如下所示：

      - 如果可以提取对象标识符， StorageGRID 会自动为对象数据创建一个新副本。可以在 StorageGRID 系统中满足活动 ILM 策略的任何位置创建新副本。
      - 如果无法提取对象标识符（因为它已损坏），则会增加 "Corrupt Objects Unidentifited" 指标，并触发 "* Unidentified Corrupt object detected* " 警报。

   c. 如果发现复制的对象数据损坏，请联系技术支持以确定损坏的根发生原因 。
8. 监控纠删编码对象的后台验证结果。

   如果后台验证发现擦除编码对象数据的损坏片段，则检测到的损坏片段属性将递增。StorageGRID 通过在同一存储节点上原位重建损坏的片段来恢复。

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 存储节点 _* > * LDR* > * 擦除编码 * 。
   c. 在验证结果表中，监控已检测到损坏的碎片 （ ECCD ） 属性。

9. 在 StorageGRID 系统自动还原损坏的对象后，重置损坏的对象计数。
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 存储节点 _* > * LDR* > * 验证 * > * 配置 * 。
   c. 选择 * 重置损坏的对象计数 * 。
   d. 单击 * 应用更改 * 。
10. 如果您确信不需要隔离对象，可以将其删除。

> 如果触发了 * 对象丢失 * 警报或丢失（对象丢失）旧警报，技术支持可能希望访问隔离的对象以帮助调试底层问题描述 或尝试数据恢复。

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 存储节点 _* > * LDR* > * 验证 * > * 配置 * 。
   c. 选择 * 删除隔离的对象 * 。
   d. 选择 * 应用更改 * 。

什么是对象存在检查?

对象存在检查可验证存储节点上是否存在所有预期复制的对象副本以及经过纠删编码的片段。对象存在检查不会验证对象数据本身（后台验证会验证）；相反，它可以提供一种验证存储设备完整性的方法，尤其是在最新的硬件问题描述 可能会影响数据完整性的情况下。

与自动执行的后台验证不同，您必须手动启动对象存在检查作业。

对象存在检查会读取存储在 StorageGRID 中的每个对象的元数据，并验证是否存在复制的对象副本和经过纠删编码的对象片段。任何缺失的数据将按以下方式处理：

- * 复制的副本 * ： 如果缺少已复制对象数据的副本， StorageGRID 会自动尝试替换存储在系统其他位置的副本中的副本。存储节点通过 ILM 评估运行现有副本，该评估将确定此对象不再符合当前 ILM 策略，因为缺少另一个副本。系统会生成并放置一个新副本以满足系统的活动 ILM 策略。此新副本可能不会放置在存储缺失副本的同一位置。
- * 擦除编码片段 * ： 如果缺少擦除编码对象的片段， StorageGRID 会自动尝试使用剩余片段在同一存储节点上原位重建缺失的片段。如果无法重建缺少的片段（因为丢失了太多的片段）， ILM 将尝试查找对象的另一个副本，以便生成经过纠删编码的新片段。

运行对象存在检查

一次创建并运行一个对象存在检查作业。创建作业时，您可以选择要验证的存储节点和卷。您还可以为作业选择一致性控制。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或根访问权限。
- 您已确保要检查的存储节点处于联机状态。选择 * 节点 * 以查看节点表。确保要检查的节点的节点名称旁边未显示任何警报图标。
- 您已确保要检查的节点上 * 未 * 运行以下过程：

- 网格扩展以添加存储节点
- 存储节点停用
- 恢复发生故障的存储卷
- 恢复系统驱动器出现故障的存储节点
- EC 重新平衡
- 设备节点克隆

在这些过程中，对象存在检查不会提供有用的信息。

关于此任务

根据网格中的对象数量，选定存储节点和卷以及选定一致性控制，完成对象存在检查作业可能需要数天或数周时间。一次只能运行一个作业，但可以同时选择多个存储节点和卷。

步骤

1. 选择 * 维护 * > * 任务 * > * 对象存在检查 * 。
2. 选择 * 创建作业 * 。此时将显示创建对象存在检查作业向导。
3. 选择包含要验证的卷的节点。要选择所有联机节点，请选中列标题中的 * 节点名称 * 复选框。

   您可以按节点名称或站点进行搜索。

   您不能选择未连接到网格的节点。

4. 选择 * 继续 * 。
5. 为列表中的每个节点选择一个或多个卷。您可以使用存储卷编号或节点名称搜索卷。

   要为选定的每个节点选择所有卷，请选中列标题中的 * 存储卷 * 复选框。

6. 选择 * 继续 * 。
7. 选择作业的一致性控制。

   一致性控制用于确定对象存在检查所使用的对象元数据副本数。

   - * 强站点 * ： 在一个站点上创建两个元数据副本。
   - * 强 - 全局 * ： 每个站点上有两个元数据副本。
   - * 全部 * （默认）： 每个站点上的所有三个元数据副本。

     有关一致性控制的详细信息，请参见向导中的说明。

8. 选择 * 继续 * 。
9. 查看并验证您的选择。您可以选择 * 上一步 * 以转到向导中的上一步以更新所做的选择。

   此时将生成并运行对象存在检查作业，直到出现以下情况之一：

   - 作业完成。
   - 暂停或取消作业。您可以恢复已暂停的作业，但无法恢复已取消的作业。

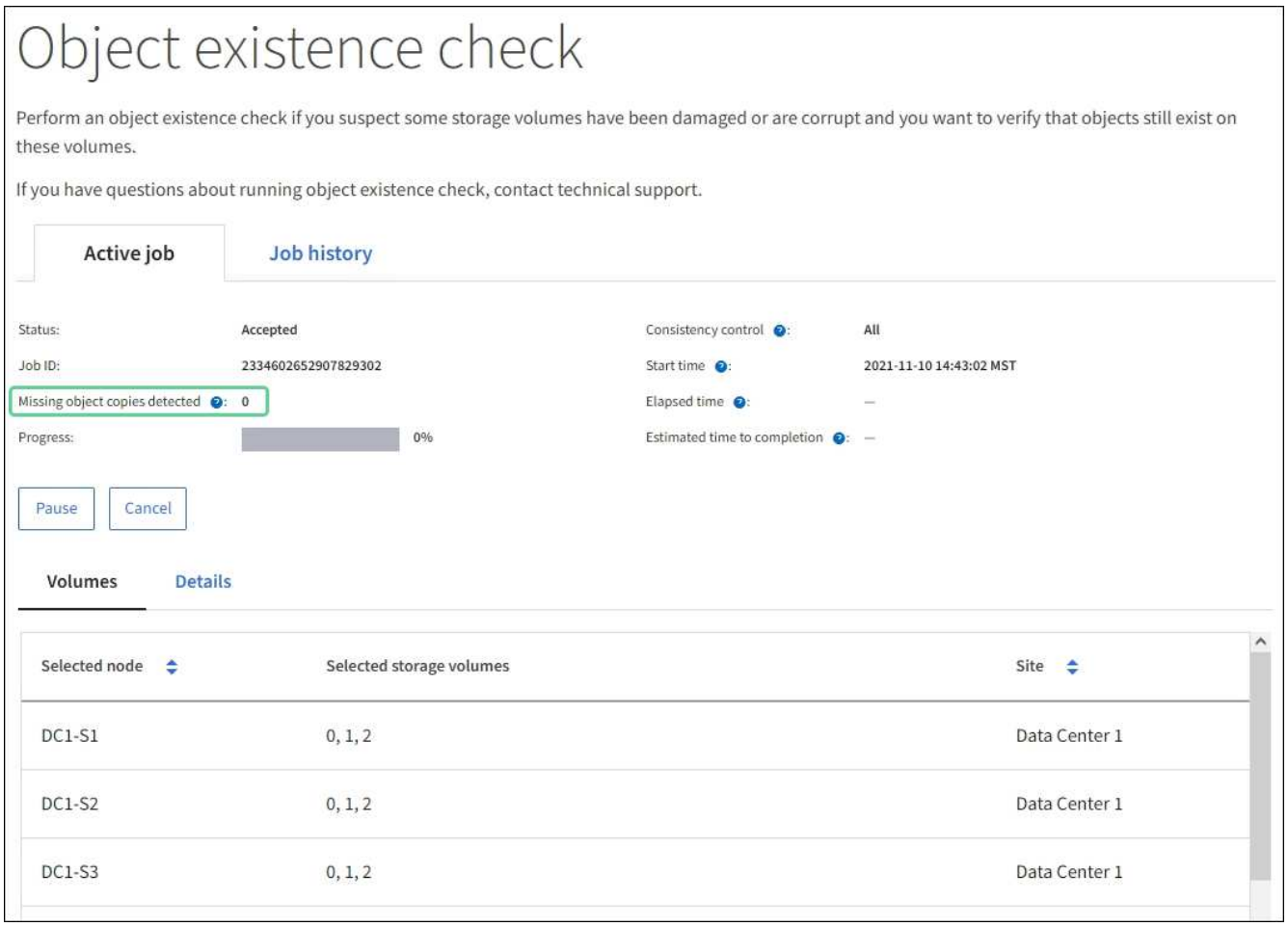
- 作业停止。此时将触发 * 对象存在检查已停止 * 警报。按照为警报指定的更正操作进行操作。
- 作业失败。触发 * 对象存在检查失败 * 警报。按照为警报指定的更正操作进行操作。
- 此时将显示 " 服务不可用` " 或 "`内部服务器错误 `S` " 消息。一分钟后，刷新页面以继续监控作业。

> 您可以根据需要离开对象存在检查页面并返回以继续监控作业。

10. 在作业运行时，查看 * 活动作业 * 选项卡，并记下检测到的缺少对象副本的值。

    此值表示缺少一个或多个片段的复制对象和经过纠删编码的对象的副本总数。

    如果检测到的缺少对象副本数大于 100 ，则可能存在存储节点存储的问题描述 。



11. 作业完成后，执行任何其他所需操作：
    - 如果检测到缺少对象副本为零，则未发现任何问题。无需执行任何操作。
    - 如果检测到缺少对象副本大于零，并且未触发 * 对象丢失 * 警报，则系统会修复所有缺少的副本。验证是否已更正任何硬件问题，以防止将来对对象副本造成损坏。
    - 如果检测到缺少对象副本大于零，并且已触发 * 对象丢失 * 警报，则数据完整性可能会受到影响。请联系技术支持。
    - 您可以使用 grep 提取 LLST 审核消息来调查丢失的对象副本： `grep LLST audit_file_name` 。

      此操作步骤 类似于的 调查丢失的对象，尽管对于对象副本，您搜索的是 `LLST` 而不是 `OLST` 。

12. 如果您为作业选择了强站点一致性或强全局一致性控制，请等待大约三周以保持元数据一致性，然后在相同卷上重新运行此作业。

    如果 StorageGRID 有时间为作业中包含的节点和卷实现元数据一致发生原因 性，则重新运行作业可能会错误地清除报告的缺失对象副本，或者如果未选中其他对象副本，则重新运行作业可能会清除这些副本。

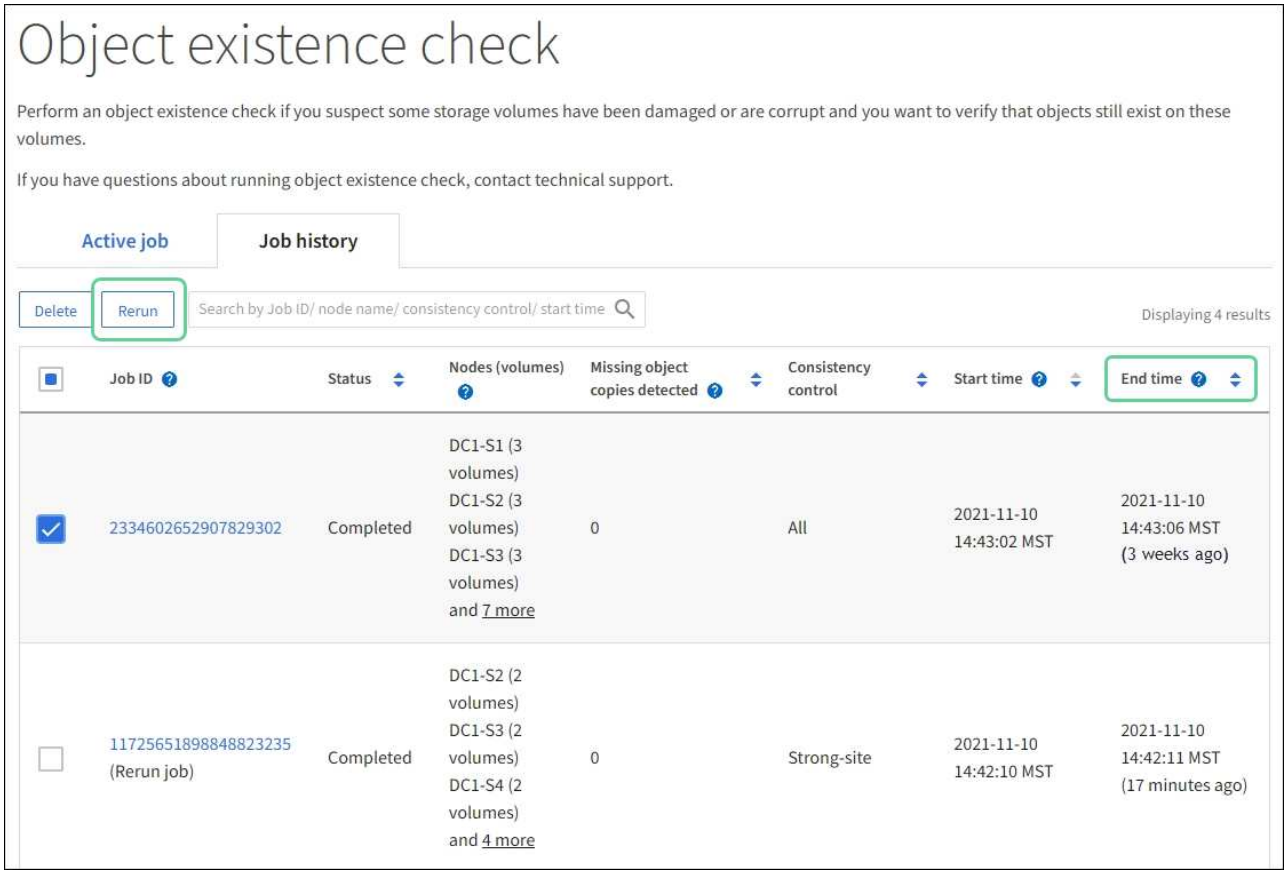
    a. 选择 * 维护 * > * 对象存在检查 * > * 作业历史记录 * 。

    b. 确定哪些作业已准备好重新运行：

        i. 查看 * 结束时间 * 列，确定三周前运行的作业。

        ii. 对于这些作业，请扫描一致性控制列中的强站点或强全局。

    c. 选中要重新运行的每个作业对应的复选框，然后选择 * 重新运行 * 。



    d. 在重新运行作业向导中，查看选定节点和卷以及一致性控制。

    e. 准备好重新运行作业后，请选择 * 重新运行 * 。

此时将显示活动作业选项卡。您选择的所有作业都将在强站点的一致性控制下作为一个作业重新运行。详细信息部分中的 * 相关作业 * 字段列出了原始作业的作业 ID 。

完成后

如果您仍对数据完整性有顾虑，请转到 * 支持 * > * 工具 * > * 网格拓扑 * > * 站点 _ * > * 存储节点 _ * > * LDR* > * 验证 * > * 配置 * > * 主 * 并提高验证后台速率。后台验证会检查所有已存储对象数据的准确性，并修复发现的任何问题。尽快发现并修复潜在问题可降低数据丢失的风险。

可以出于多种原因检索对象，包括从客户端应用程序读取请求，对复制的对象数据进行后台验证， ILM 重新评估以及在存储节点恢复期间还原对象数据。

StorageGRID 系统使用对象元数据中的位置信息来确定从哪个位置检索对象。如果在预期位置未找到对象的副本，则系统会尝试从系统中的其他位置检索该对象的另一个副本，前提是 ILM 策略包含一条规则，用于为该对象创建两个或更多副本。

如果此检索成功， StorageGRID 系统将替换缺少的对象副本。否则，系统将触发 * 对象丢失 * 警报，如下所示：

- 对于复制的副本，如果无法检索到另一个副本，则会将对象视为丢失，并触发警报。
- 对于经过擦除编码的副本，如果无法从预期位置检索到副本，则在尝试从其他位置检索副本之前，检测到的损坏副本（ DECOR ）属性会递增 1 。如果未找到其他副本，则会触发警报。

您应立即调查所有 * 对象丢失 * 警报，以确定丢失的根发生原因 ，并确定对象是否仍位于脱机存储节点或归档节点中，或者当前是否不可用。

如果没有副本的对象数据丢失，则不存在恢复解决方案 。但是，您必须重置丢失对象计数器，以防止已知丢失的对象屏蔽任何新的丢失对象。

相关信息

调查丢失的对象

重置丢失和缺失的对象计数

调查丢失的对象

触发 * 对象丢失 * 警报时，您必须立即进行调查。收集有关受影响对象的信息并联系技术支持。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。

关于此任务

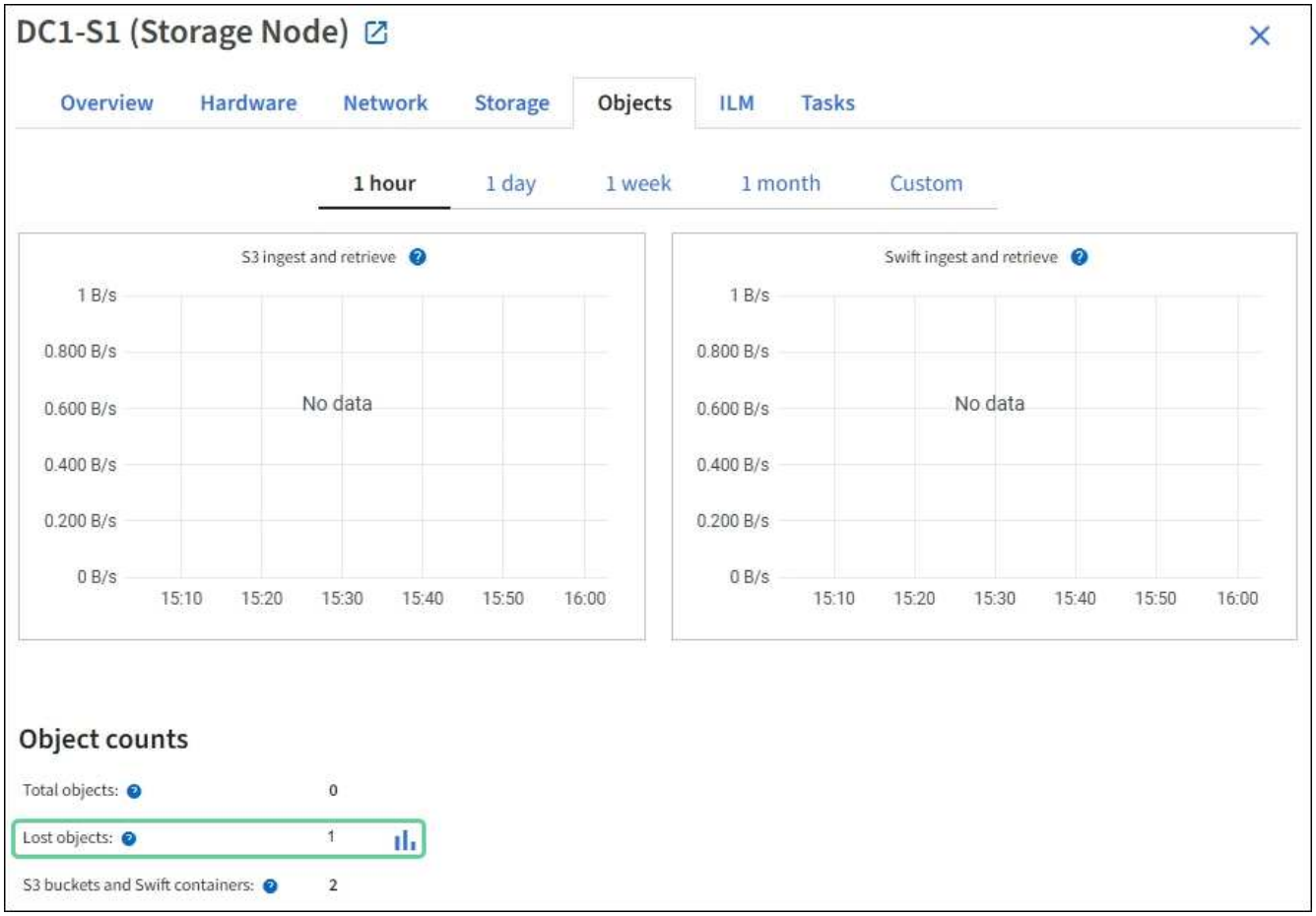
"* 对象丢失 * " 警报表示 StorageGRID 认为网格中没有对象副本。数据可能已永久丢失。

立即调查丢失的对象警报。您可能需要采取措施以防止进一步数据丢失。在某些情况下，如果您立即采取措施，则可能能够还原丢失的对象。

步骤

1. 选择 * 节点 * 。
2. 选择 * 存储节点 _* > * 对象 * 。
3. 查看对象计数表中显示的丢失对象的数量。

此数字表示此网格节点在整个 StorageGRID 系统中检测到缺少的对象总数。该值是 LDR 和 DDS 服务中数据存储组件的丢失对象计数器之和。



4. 从管理节点访问审核日志，以确定触发 * 对象丢失 * 警报的对象的唯一标识符（ UUID ）：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 更改为审核日志所在的目录。输入： `cd /var/local/audit/export/`
   c. 使用 grep 提取对象丢失（ OLST ）审核消息。输入： `grep OLST audit_file_name`
   d. 记下消息中包含的 UUID 值。

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. 使用 `ObjectByUUID` 命令按对象标识符（ UUID ）查找对象，然后确定数据是否存在风险。

   a. Telnet 到 localhost 1402 以访问 LDR 控制台。

   b. 输入：` /proc/obrp/ObjectByUUID UID_Value`

      在第一个示例中， `UUID` 为 `926026C4-00A4-449B-AC72-BCCA72DD1311` 的对象列出了两个位置。

```
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"
        }
    ]
}
```

在第二个示例中， `UUID` 为 `926026C4-00A4-449B-AC72-BCCA72DD1311` 的对象没有列出任何位置。

```
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. 查看 /proc/obrp/ObjectByUUID 的输出，并采取相应的操作：

元数据	结论
未找到对象（ "error" ： "" ）	如果未找到对象，则返回消息 "error" ： "" 。 如果未找到此对象，您可以重置 * 丢失的对象 * 计数以清除警报。缺少对象表示该对象已被有意删除。
位置 > 0	如果输出中列出了一些位置，则 * 对象丢失 * 警报可能为误报。 确认对象存在。使用输出中列出的节点 ID 和文件路径确认对象文件位于列出的位置。 （的操作步骤 正在搜索可能丢失的对象 介绍如何使用节点 ID 查找正确的存储节点。） 如果对象存在，您可以重置 * 丢失的对象 * 计数以清除警报。
位置 = 0	如果输出中未列出任何位置，则此对象可能会丢失。您可以尝试 搜索并还原对象 您也可以联系技术支持。 技术支持可能会要求您确定是否正在进行存储恢复操作步骤 。也就是说，是否已在任何存储节点上发出 *repair-data* 命令，并且恢复是否仍在进行中？请参见有关的信息 将对象数据还原到存储卷。

相关信息

查看审核日志

搜索并还原可能丢失的对象

可能会找到并还原已触发 " 对象丢失（丢失） " 警报和 " 对象丢失 * " 警报且您已确定可能丢失的对象。

您需要的内容

- 您必须具有 "`调查丢失的对象 " 中标识的任何丢失对象的 UUID 。`
- 您必须具有 `passwords.txt` 文件。

关于此任务

您可以按照此操作步骤 在网格中其他位置查找丢失对象的复制副本。在大多数情况下，找不到丢失的对象。但是，在某些情况下，如果您立即采取措施，则可能能够找到并还原丢失的复制对象。

请联系技术支持以获得有关此操作步骤 的帮助。

步骤

1. 在管理节点中，搜索审核日志以查找可能的对象位置：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 `$` 更改为 `#` 。

b. 更改为审核日志所在的目录： `cd /var/local/audit/export/`

c. 使用 grep 提取与可能丢失的对象关联的审核消息并将其发送到输出文件。输入： `grep uuid-valueaudit_file_name > output_file_name`

例如：

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

d. 使用 grep 从此输出文件中提取丢失位置（ LLLST ）审核消息。输入： `grep LLST output_file_name`

例如：

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

LLST 审核消息类似于此示例消息。

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. 在 LLST 消息中找到 PCLD 字段和 NOID 字段。

如果存在，则 PCLD 的值为磁盘上缺少复制对象副本的完整路径。NOID 的值是可能找到对象副本的 LDR 的节点 ID 。

如果找到对象位置，您可能能够还原该对象。

f. 找到此 LDR 节点 ID 的存储节点。

使用节点 ID 查找存储节点的方法有两种：

- 在网格管理器中，选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 。 Data Center_* > * 。 Storage Node_* > * 。LDR 节点 ID 位于 Node Information 表中。查看每个存储节点的信息，直到找到托管此 LDR 的存储节点为止。

- 下载并解压缩网格的恢复软件包。该软件包中有一个 *\docs* 目录。如果打开 index.html 文件， " 服务器摘要 " 将显示所有网格节点的所有节点 ID 。

2. 确定对象是否位于审核消息中指示的存储节点上：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

1. 确定对象的文件路径是否存在。

对于对象的文件路径，请使用 LLST 审核消息中的 PCLD 值。

例如，输入：

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

- 注 * ：在命令中，始终用单引号将对象文件路径括起来，以转义任何特殊字符。
- 如果未找到对象路径，则此对象将丢失，无法使用此操作步骤 进行还原。请联系技术支持。
- 如果找到对象路径，请继续执行步骤 将对象还原到 StorageGRID。您可以尝试将找到的对象还原回 StorageGRID 。
   a. 【还原对象到 StorageGRID ， start=3]] 如果找到对象路径，请尝试将对象还原到 StorageGRID ：
      i. 从同一个存储节点中，更改对象文件的所有权，以便可通过 StorageGRID 进行管理。输入： `chown LDR 用户： byncast 'file_path_of_object'`
      ii. Telnet 到 localhost 1402 以访问 LDR 控制台。输入： `telnet 0 1402`
      iii. 输入： `cd /proc/stor`
      iv. 输入： `object_found 'file_path_of_object"`

      例如，输入：

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      + 发出 `objection\_found` 命令，向网格通知对象的位置。它还会触发活动的 ILM 策略，该策略会根据策略中的指定创建其他副本。

- 注 * ：如果发现对象所在的存储节点脱机，则可以将该对象复制到任何联机存储节点。将对象放置在联机存储节点的任何 /var/local/rangedb 目录中。然后，使用该对象的文件路径问题描述 `Object\\_found` 命令。
   ◦ 如果无法还原此对象，则 `Object\\_found` 命令将失败。请联系技术支持。

◦ 如果对象已成功还原到 StorageGRID ，则会显示一条成功消息。例如：

```
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'
```

继续执行步骤 验证是否已创建新位置

i. 如果对象已成功还原到 StorageGRID ，请验证是否已创建新位置。

A. 输入： `cd /proc/obRP`

B. 输入： `ObjectByUUID UID_Value`

以下示例显示 UUID 为 926026C4-00A4-449B-AC72-BCCA72DD1311 的对象有两个位置。

```
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. 从 LDR 控制台注销。输入： `exit`
   a. 在管理节点中，搜索此对象的 ORLM 审核消息的审核日志，以确认信息生命周期管理（ ILM ）已根据需要放置副本。
2. 登录到网格节点：
   a. 输入以下命令： `ssh admin@grid_node_ip`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
3. 更改为审核日志所在的目录： `cd /var/local/audit/export/`
4. 使用 grep 将与对象关联的审核消息提取到输出文件中。输入： `grep uuid-valueaudit_file_name > output_file_name`

   例如：

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

5. 使用 grep 从此输出文件中提取对象规则已满足（ ORLM ）审核消息。输入： `grep ORLM output_file_name`

   例如：

   ```
   Admin: # grep ORLM messages_about_restored_object.txt
   ```

   ORLM 审核消息类似于此示例消息。

   ```
   [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. 在审核消息中找到 LOC 字段。

   如果存在，则在 LOM 中的 CLDI 值为节点 ID 和创建对象副本的卷 ID 。此消息显示已应用 ILM ，并且已在网格中的两个位置创建两个对象副本。。在网格管理器中重置丢失对象的计数。

相关信息

调查丢失的对象

重置丢失和缺失的对象计数

查看审核日志

重置丢失和缺失的对象计数

在调查 StorageGRID 系统并验证所有记录的丢失对象是否永久丢失或是否为虚假警报之后，您可以将丢失对象属性的值重置为零。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

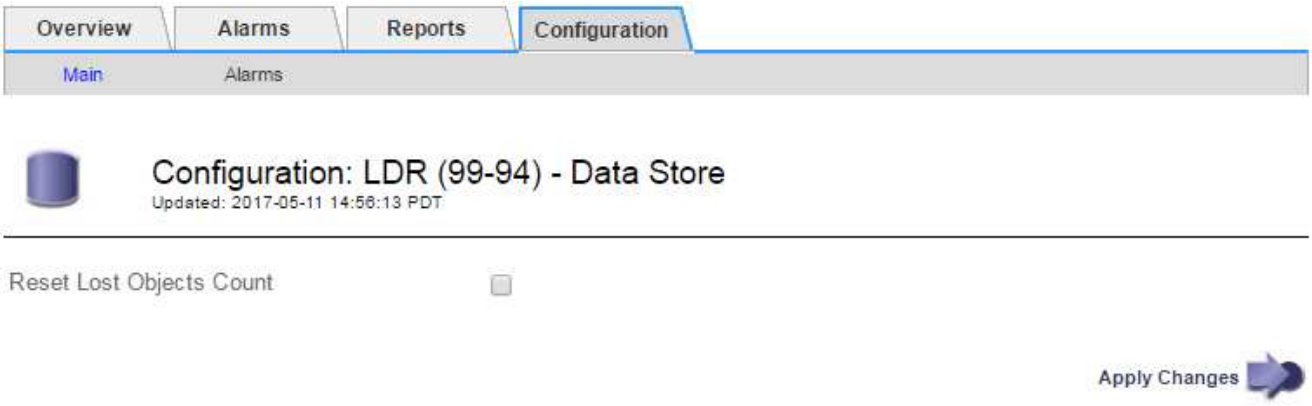
您可以从以下任一页面重置丢失的对象计数器：

- * 支持 * > * 工具 * > * 网格拓扑 * > * 站点 _* > * 存储节点 _* > * LDR* > * 数据存储 * > * 概述 * > * 主 *
- * 支持 * > * 工具 * > * 网格拓扑 * > * 站点 _* > * 存储节点 _* > * DDS* > * 数据存储 * > * 概述 * > * 主 *

以下说明显示了如何从 * LDR* > * 数据存储 * 页面重置计数器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 对于出现 "* 对象丢失 " 警报或 " 丢失 " 警报的存储节点，选择 * 站点 _* > * 存储节点 _* > * * 存储节点 * > * 数据存储 * > * 配置 * 。
3. 选择 * 重置丢失的对象计数 * 。



4. 单击 * 应用更改 * 。

   丢失的对象属性将重置为 0 ，并且 * 对象丢失 * 警报和丢失警报将清除，这可能需要几分钟的时间。

5. 或者，也可以重置在识别丢失的对象过程中可能会递增的其他相关属性值。

   a. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 擦除编码 * > * 配置 * 。
   b. 选择 * 重置读取失败计数 * 和 * 重置检测到的损坏副本计数 * 。
   c. 单击 * 应用更改 * 。
   d. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 验证 * > * 配置 * 。
   e. 选择 * 重置缺少的对象计数 * 和 * 重置损坏的对象计数 * 。
   f. 如果您确信不需要隔离对象，则可以选择 * 删除隔离对象 * 。

      在后台验证发现复制的对象副本损坏时，将创建隔离的对象。在大多数情况下， StorageGRID 会自动替换损坏的对象，并且可以安全地删除隔离的对象。但是，如果触发 * 对象丢失 * 警报或丢失警报，技术支持可能需要访问隔离的对象。

   g. 单击 * 应用更改 * 。

   单击 * 应用更改 * 后，可能需要几分钟时间才能重置属性。

对对象数据存储不足警报进行故障排除

对象数据存储空间 * 不足警报可监控每个存储节点上可用于存储对象数据的空间量。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

如果存储节点上复制和擦除编码的对象数据总量满足警报规则中配置的条件之一，则会触发 * 对象数据存储空间不足 * 警报。

默认情况下，如果此情况评估为 true ，则会触发重大警报：

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

在这种情况下：

- `storagegRid_storage_utilization_data_bytes` 是对存储节点的已复制和擦除编码对象数据总大小的估计值。
- `storagegRid_storage_utilization_usable_space_bytes` 是存储节点剩余的对象存储空间总量。

如果触发主要或次要的 * 对象数据存储空间不足 * 警报，则应尽快执行扩展操作步骤 。

步骤

1. 选择 * 警报 * > * 当前 * 。

   此时将显示警报页面。

2. 如果需要，从警报表中展开 * 对象数据存储空间不足 * 警报组，然后选择要查看的警报。

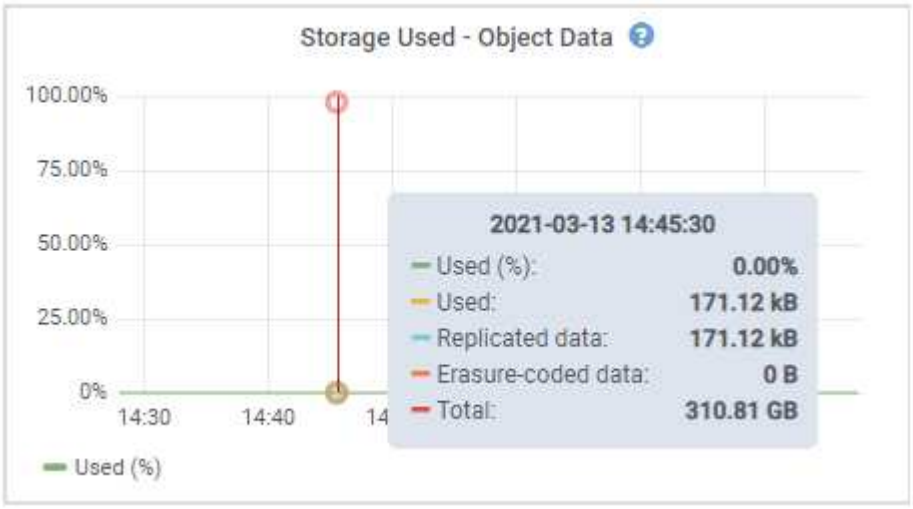
   选择警报，而不是一组警报的标题。

3. 查看对话框中的详细信息，并注意以下事项：
   - 时间已触发
   - 站点和节点的名称
   - 此警报的指标的当前值
4. 选择 * 节点 * > * 存储节点或站点 _* > * 存储 * 。
5. 将光标悬停在 "Storage Used - Object Data" 图上。

   此时将显示以下值：

   - * 已用（ % ） * ： 已用于对象数据的总可用空间的百分比。
   - * 已用 * ： 已用于对象数据的总可用空间量。
   - * 复制数据 * ： 此节点，站点或网格上复制的对象数据量的估计值。
   - * 擦除编码数据 * ： 此节点，站点或网格上经过擦除编码的对象数据量的估计值。

◦ * 总计 * ： 此节点，站点或网格上的可用空间总量。使用的值是 `storagegRid_storage_utilization _data_bytes` 指标。



6. 选择图形上方的时间控件可查看不同时间段的存储使用情况。

   查看一段时间内的存储使用量有助于您了解触发警报前后的存储使用量，并有助于您估计节点的剩余空间可能需要多长时间才能达到全满状态。

7. 请尽快执行扩展操作步骤 以添加存储容量。

   您可以向现有存储节点添加存储卷（ LUN ），也可以添加新的存储节点。

   要管理完整的存储节点，请参见有关管理 StorageGRID 的说明。

相关信息

对存储状态（ SSTS ）警报进行故障排除

扩展网格

管理 StorageGRID

对低只读水印覆盖警报进行故障排除

如果对存储卷水印使用自定义值，则可能需要解决 * 低只读水印覆盖 * 警报。如果可能，您应更新系统以开始使用优化值。

在先前版本中，这三个 存储卷水印 为全局设置 &#8212 ； 应用于每个存储节点上的每个存储卷的值相同。从 StorageGRID 11.6 开始，软件可以根据存储节点的大小和卷的相对容量为每个存储卷优化这些水印。

升级到 StorageGRID 11.6 时，经过优化的只读和读写水印会自动应用于所有存储卷，除非满足以下条件之一：

- 您的系统容量已接近，如果应用了优化的水印，则无法接受新数据。在这种情况下， StorageGRID 不会更改水印设置。
- 您先前已将任何存储卷水印设置为自定义值。StorageGRID 不会使用优化值覆盖自定义水印设置。但是，如果您对存储卷软只读水印的自定义值太小，则 StorageGRID 可能会触发 * 低只读水印覆盖 * 警报。

了解警报

如果对存储卷水印使用自定义值，则可能会为一个或多个存储节点触发 * 低只读水印覆盖 * 警报。

每个警报实例都指示 * 存储卷软只读水印 * 的自定义值小于该存储节点的最小优化值。如果您继续使用自定义设置，则存储节点可能会在空间严重不足的情况下运行，然后才能安全地过渡到只读状态。当节点达到容量时，某些存储卷可能无法访问（自动卸载）。

例如，假设您先前已将 * 存储卷软只读水印 * 设置为 5 GB 。现在，假设 StorageGRID 已为存储节点 A 中的四个存储卷计算出以下优化值：

卷 0	12 GB
卷 1	12 GB
第 2 卷	11 GB
第 3 卷	15 GB

为存储节点 A 触发 * 低只读水印覆盖 * 警报，因为您的自定义水印（ 5 GB ）小于该节点中所有卷的最小优化值（ 11 GB ）。如果继续使用自定义设置，则节点可能会在空间严重不足的情况下运行，然后才能安全过渡到只读状态。

解决警报

如果触发了一个或多个 * 低只读水印覆盖 * 警报，请执行以下步骤。如果您当前正在使用自定义水印设置，并且希望开始使用优化设置，即使未触发任何警报，也可以使用这些说明。

您需要的内容

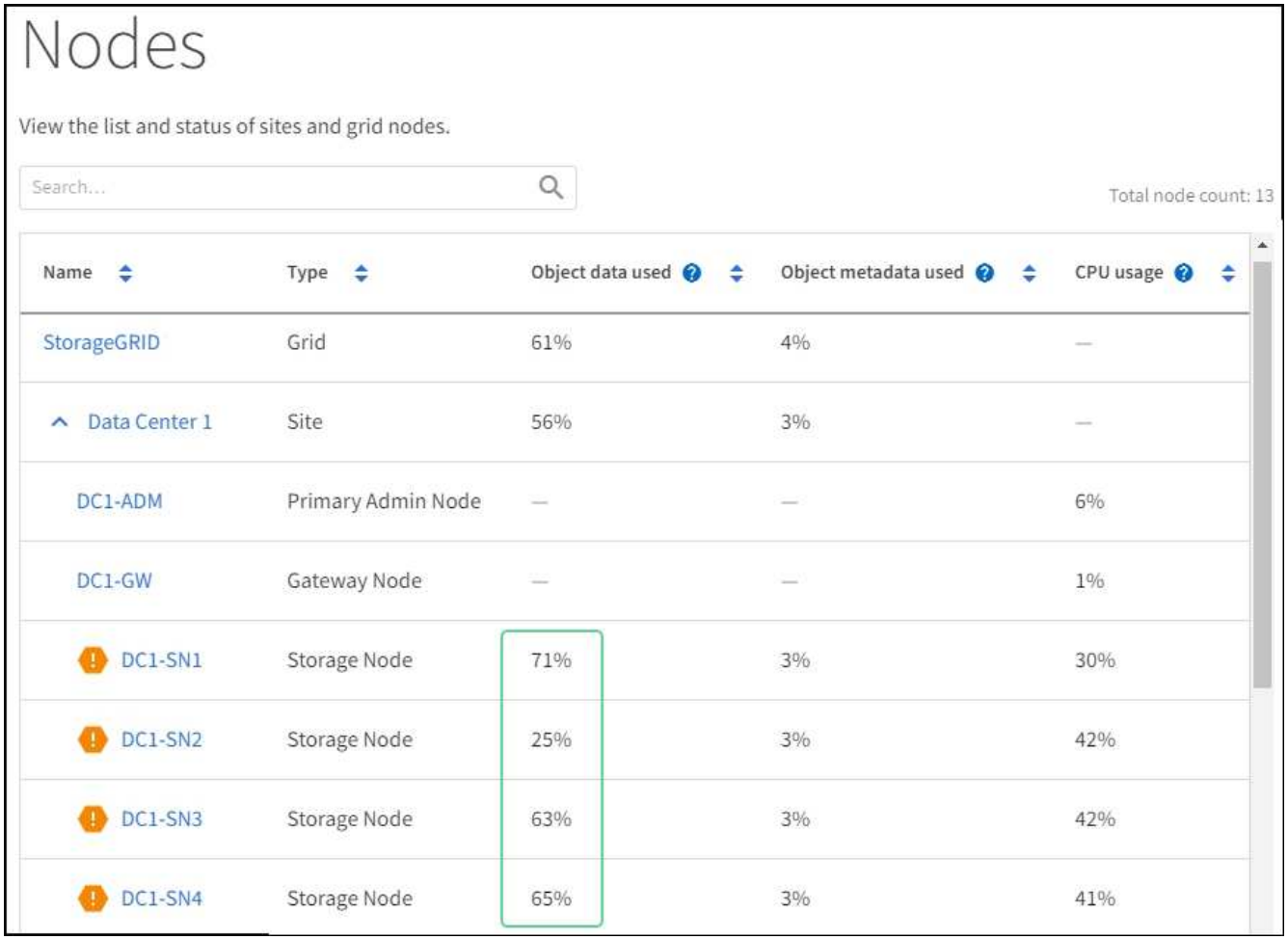
- 您已完成 StorageGRID 11.6 的升级。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。

关于此任务

您可以通过将自定义水印设置更新为新的水印覆盖来解决 * 低只读水印覆盖 * 警报。但是，如果一个或多个存储节点接近全满或您有特殊的 ILM 要求，则应首先查看优化的存储水印并确定使用它们是否安全。

评估整个网格的对象数据使用情况

1. 选择 * 节点 * 。
2. 对于网格中的每个站点，展开节点列表。
3. 查看每个站点的每个存储节点的 * 对象数据已用 * 列中显示的百分比值。



4. 如果所有存储节点均未接近全满（例如，所有 * 已使用的对象数据 * 值均小于 80% ），则可以开始使用覆盖设置。转至 [使用优化的水印]。

> 此一般规则存在一些例外情况。例如，如果 ILM 规则使用严格的载入行为或特定存储池接近全满，则应首先执行中的步骤 [查看优化的存储水印] 和 [确定是否可以使用优化的水印]。

5. 如果还有一个存储节点接近全满，请执行中的步骤 [查看优化的存储水印] 和 [确定是否可以使用优化的水印]。

查看优化的存储水印

StorageGRID 使用两个 Prometheus 指标来显示它为 * 存储卷软只读水印 * 计算的优化值。您可以查看网格中每个存储节点的最小和最大优化值。

1. 选择 * 支持 * > * 工具 * > * 指标 * 。
2. 在 Prometheus 部分中，选择用于访问 Prometheus 用户界面的链接。
3. 要查看建议的最小软只读水印，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegRid_storage_volume_minimum_optimized_soft_readonly_slogm
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最小优化值。如果此值大于 * 存储卷软只读水印 * 的自定义设置，则会为存储节点触发 * 低只读水印覆盖 * 警报。

4. 要查看建议的最大软只读水印数，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegRid_storage_volume_max_optimized_soft_readonly_slogm
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

5. 【最大优化值】记下每个存储节点的最大优化值。

确定是否可以使用优化的水印

1. 选择 * 节点 * 。
2. 对每个联机存储节点重复上述步骤：
   a. 选择 * 存储节点 _* > * 存储 * 。
   b. 向下滚动到对象存储表。
   c. 将每个对象存储（卷）的 * 可用 * 值与您为该存储节点记下的最大优化水印进行比较。
3. 如果每个联机存储节点上至少有一个卷的可用空间超过该节点的最大优化水印容量，请转至 [使用优化的水印] 开始使用经过优化的水印。

   否则， 扩展网格 请尽快。向现有节点添加存储卷或添加新的存储节点。然后，转到 [使用优化的水印] 更新水印设置。

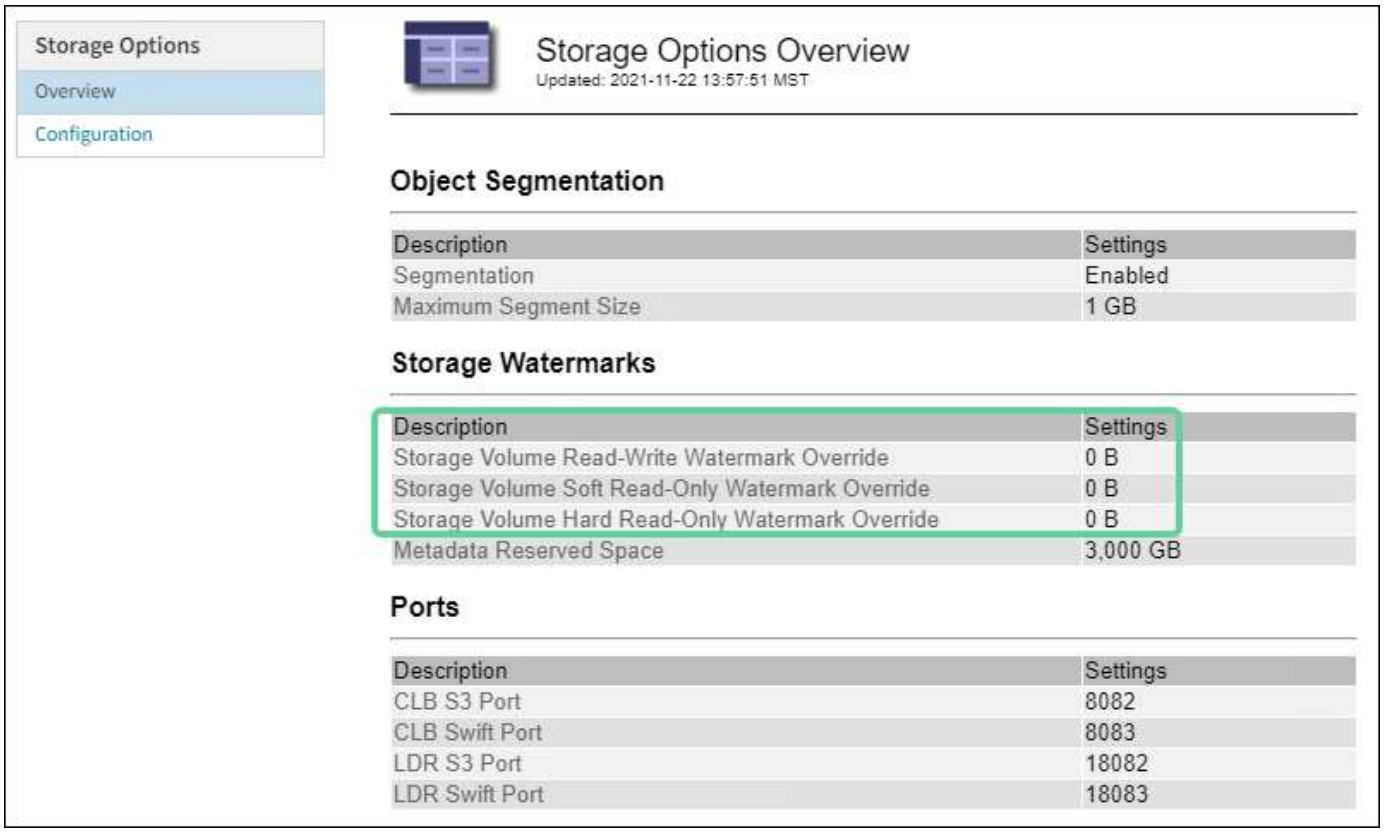
4. 如果需要继续对存储卷水印使用自定义值， 静默 或 -disable * 低只读水印覆盖 * 警报。

   相同的自定义水印值将应用于每个存储节点上的每个存储卷。对存储卷水印使用小于建议值可能发生原因 会导致某些存储卷在节点达到容量时无法访问（自动卸载）。

使用优化的水印

1. 转至 * 配置 * > * 系统 * > * 存储选项 * 。
2. 从存储选项菜单中选择 * 配置 * 。
3. 将所有三个 " 水印覆盖 " 更改为 0 。
4. 选择 * 应用更改 * 。

现在，根据存储节点的大小和卷的相对容量，优化的存储卷水印设置将对每个存储卷生效。



对存储状态（ **SSTS** ）警报进行故障排除

如果存储节点的对象存储剩余可用空间不足，则会触发存储状态（ SSTS ）警报。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

当存储节点中每个卷上的可用空间量降至存储卷软只读水印（ * 配置 * > * 系统 * > * 存储选项 * ）的值以下时，SSTS （存储状态）警报将在通知级别触发。

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

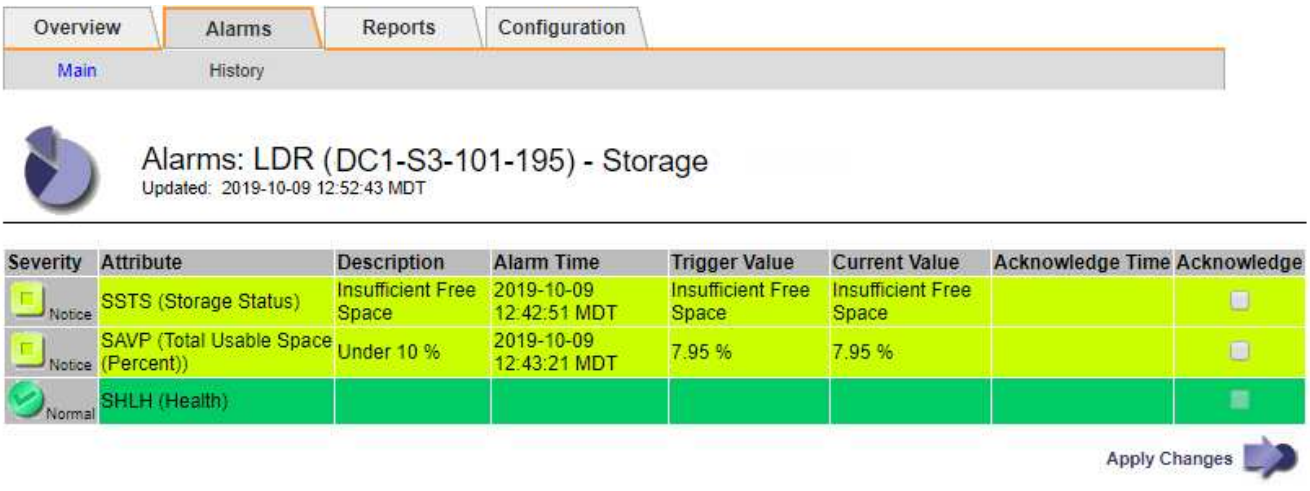
例如，假设存储卷软只读水印设置为 10 GB ，这是其默认值。如果存储节点中的每个存储卷上的可用空间不足 10 GB ，则会触发 SSTS 警报。如果任何卷具有 10 GB 或更大的可用空间，则不会触发警报。

如果已触发 SSTS 警报，您可以按照以下步骤更好地了解问题描述 。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。
2. 从服务列中，选择与 SSTS 警报关联的数据中心，节点和服务。

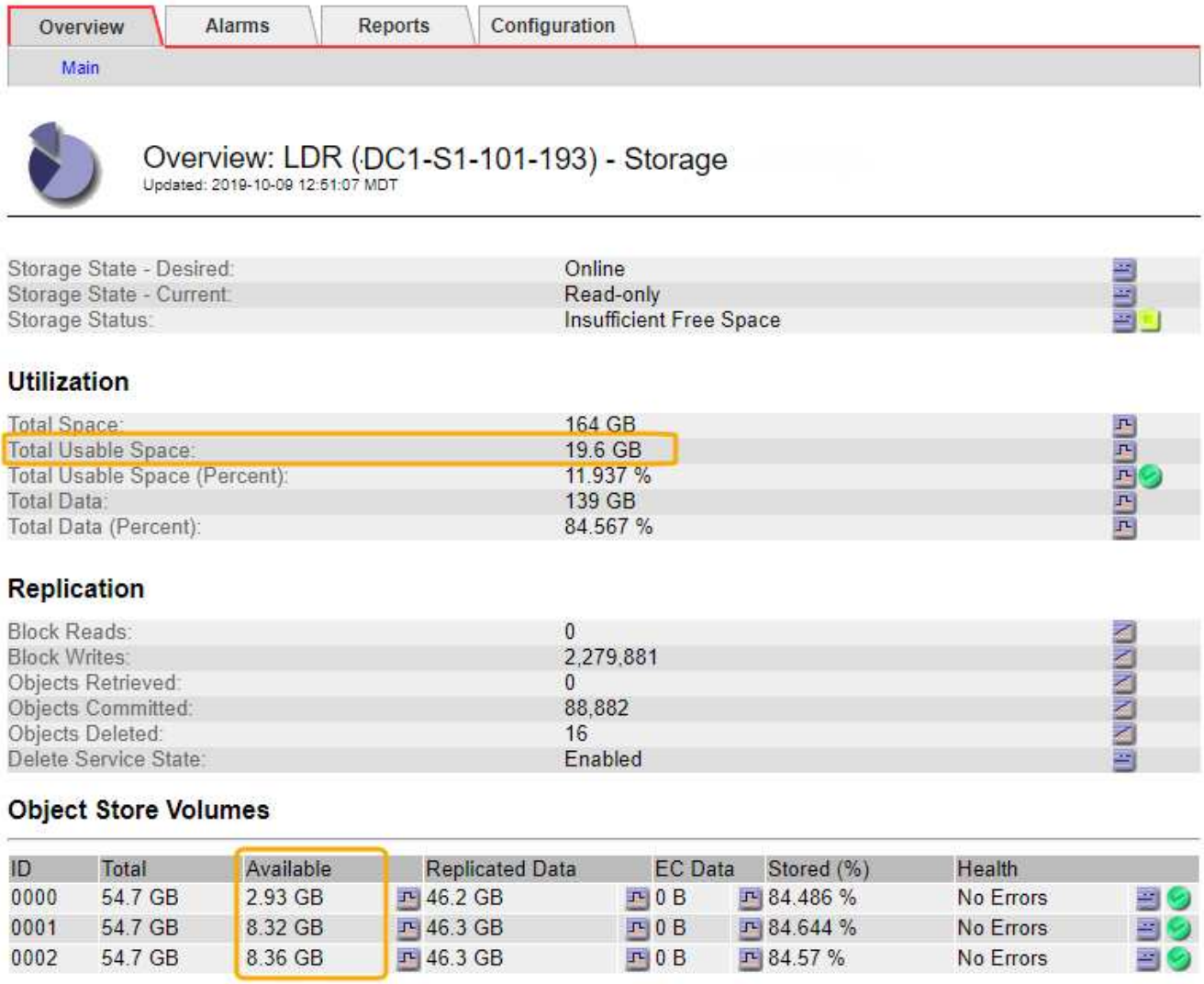
   此时将显示网格拓扑页面。警报选项卡显示选定节点和服务的活动警报。



   在此示例中，已在通知级别触发 SSTS （存储状态）和 SAVP （总可用空间（百分比））警报。

   通常， SSTS 警报和 SAVP 警报会同时触发；但是，是否同时触发这两个警报取决于以 GB 为单位的水印设置和以百分比表示的 SAVP 警报设置。

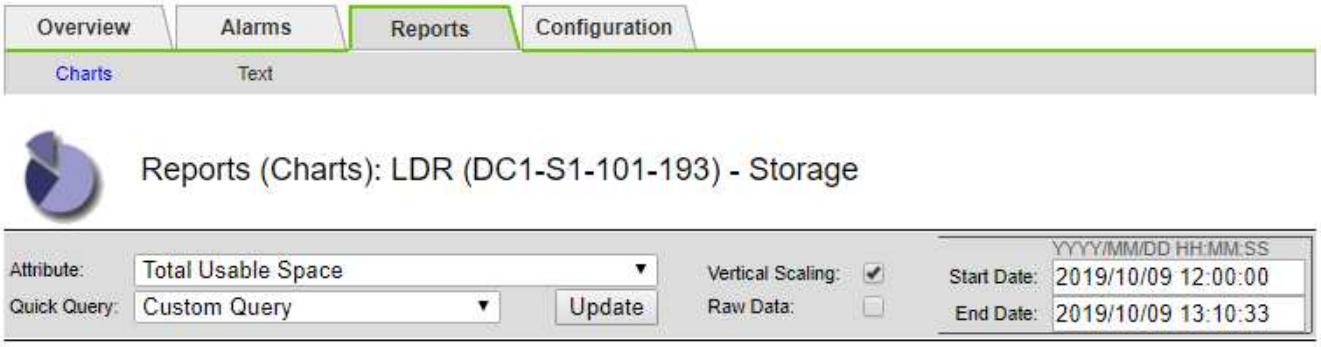
3. 要确定实际可用空间量，请选择 * LDR* > * 存储 * > * 概述 * ，然后找到总可用空间（ STAMP ）属性。

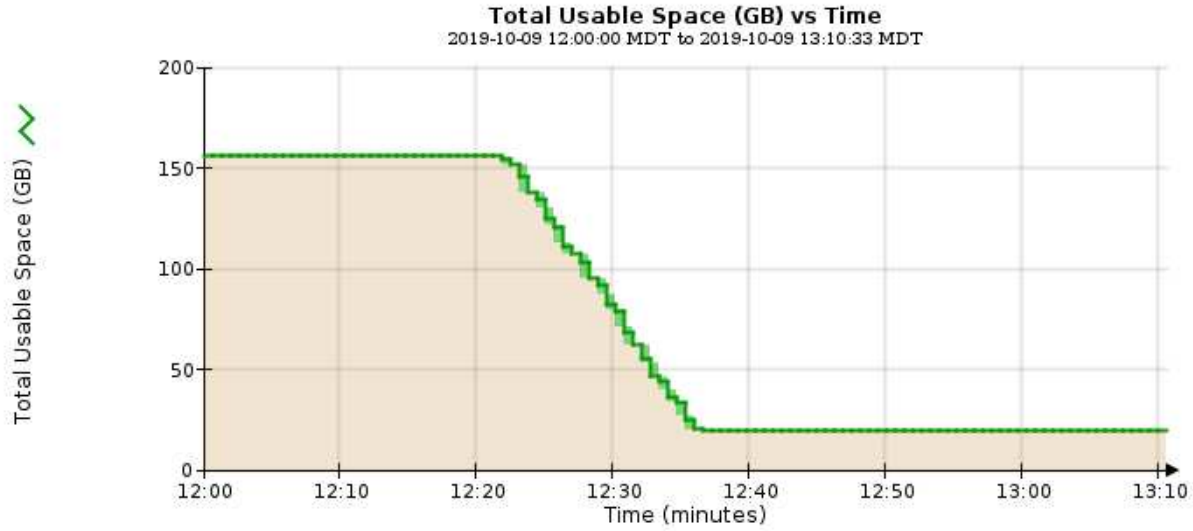


在此示例中，此存储节点上 164 GB 空间中只有 19.6 GB 可用。请注意，总计值是三个对象存储卷的 * 可用 * 值之和。之所以触发 SSTS 警报，是因为这三个存储卷中的每个卷的可用空间均小于 10 GB 。

4. 要了解存储在一段时间内的使用情况，请选择 * 报告 * 选项卡，然后绘制过去几小时的总可用空间。

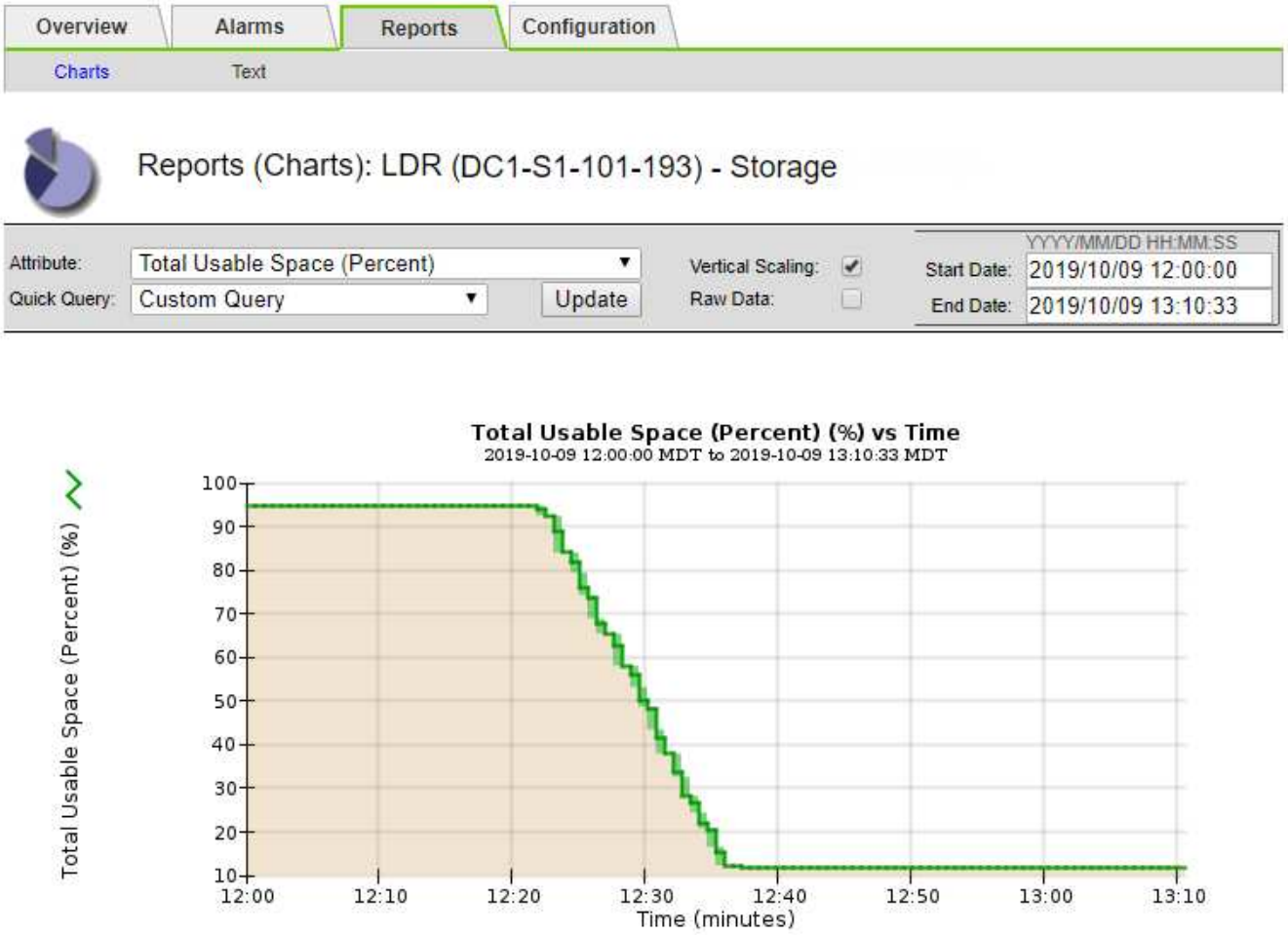
   在此示例中，总可用空间从 12： 00 处的大约 155 GB 降至 12： 35 处的 20 GB ，这与触发 SSTS 警报的时间相对应。





5. 要了解存储的使用情况占总空间的百分比，请绘制过去几小时的总可用空间（百分比）。

   在此示例中，总可用空间大约同时从 95% 下降到 10% 以上。



6. 根据需要添加存储容量 扩展 StorageGRID 系统。

   有关如何管理完整存储节点的过程，请参见 有关管理 StorageGRID 的说明。

对平台服务消息的传送进行故障排除（ **SMTTT** 警报）

如果平台服务消息传送到无法接受数据的目标，则会在网格管理器中触发总事件（ SMT ）警报。

关于此任务

例如，即使无法将关联的复制或通知消息传送到已配置的端点， S3 多部分上传也可以成功。或者，如果元数据过长，则可能无法传送有关 CloudMirror 复制的消息。

SMT 警报包含最后一条事件消息，其中显示： `failed to publish notifications for bucket-name object key` for the last object whose notification failed.

事件消息也会列在 ` /var/local/log/byncast-err.log` 日志文件中。请参见 日志文件参考。

有关追加信息 对平台服务进行故障排除的信息，请参见 有关管理 StorageGRID 的说明。您可能需要 从租户管理器访问租户 调试平台服务错误。

步骤

1. 要查看警报，请选择 * 节点 * > * 站点 _* > * 网格节点 _* > * 事件 * 。

2. 在表顶部查看上次事件。

   事件消息也会在 ` /var/local/log/byncast-err.log` 中列出。

3. 按照 SMT 警报内容中提供的指导更正问题描述 。
4. 选择 * 重置事件计数 * 。
5. 将尚未传送平台服务消息的对象通知租户。
6. 指示租户通过更新对象的元数据或标记来触发失败的复制或通知。

对元数据问题进行故障排除

您可以执行多项任务来帮助确定元数据问题的根源。

对 " 低元数据存储 " 警报进行故障排除

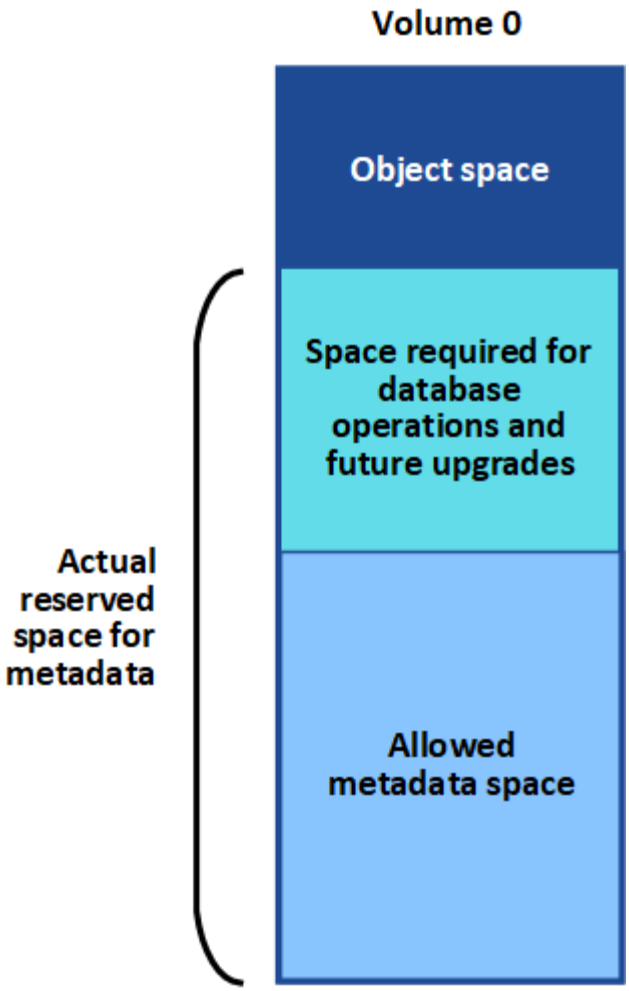
如果触发 * 低元数据存储 * 警报，则必须添加新的存储节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

StorageGRID 会在每个存储节点的卷 0 上为对象元数据预留一定数量的空间。此空间称为实际预留空间，并细分为对象元数据允许的空间（允许的元数据空间）以及数据缩减和修复等基本数据库操作所需的空间。允许的元数据空间用于控制整体对象容量。



如果对象元数据占用的空间超过元数据允许的 100% ，则数据库操作将无法高效运行，并会发生错误。

您可以 监控每个存储节点的对象元数据容量 帮助您预测错误并在发生错误之前予以更正。

StorageGRID 使用以下 Prometheus 指标来衡量允许的元数据空间的容量：

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

当此 Prometheus 表达式达到特定阈值时，将触发 * 低元数据存储 * 警报。

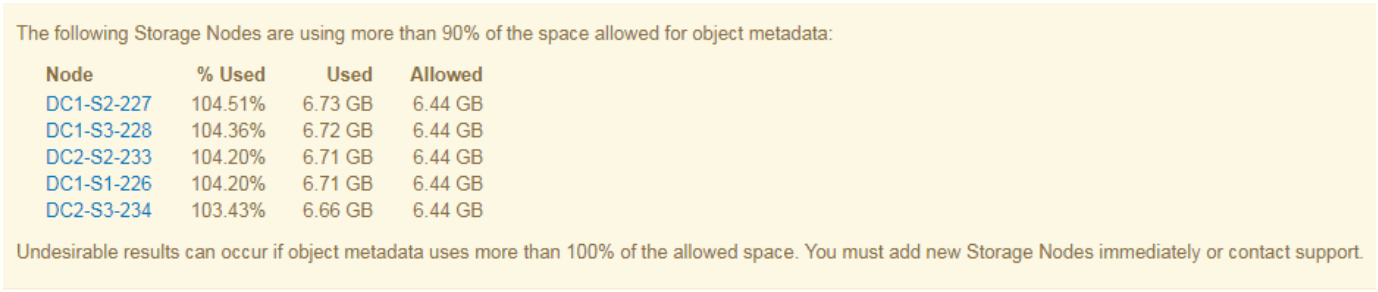
- * 次要 * ： 对象元数据正在使用允许的元数据空间的 70% 或更多。您应尽快添加新的存储节点。
- * 主要 * ： 对象元数据正在使用允许的元数据空间的 90% 或更多。您必须立即添加新的存储节点。

> 当对象元数据使用 90% 或更多的允许元数据空间时，信息板上会显示一条警告。如果显示此警告，则必须立即添加新的存储节点。绝不能允许对象元数据使用超过允许空间的 100% 。

- * 严重 * ： 对象元数据正在使用 100% 或更多的允许元数据空间，并且开始占用基本数据库操作所需的空间。您必须停止载入新对象，并且必须立即添加新的存储节点。

在以下示例中，对象元数据使用的元数据空间超过允许的 100% 。这是一种严重情况，会导致数据库运行效率

低下和出现错误。



如果卷 0 的大小小于元数据预留空间存储选项（例如，在非生产环境中），则计算 * 低元数据存储 * 警报可能不准确。

步骤

1. 选择 * 警报 * > * 当前 * 。
2. 如果需要，从警报表中展开 * 低元数据存储 * 警报组，然后选择要查看的特定警报。
3. 查看警报对话框中的详细信息。
4. 如果触发了主要或关键的 * 低元数据存储 * 警报，请执行扩展以立即添加存储节点。

由于 StorageGRID 会在每个站点保留所有对象元数据的完整副本，因此整个网格的元数据容量受最小站点的元数据容量限制。如果需要向一个站点添加元数据容量，则还应添加元数据容量 扩展任何其他站点 相同数量的存储节点。

执行扩展后， StorageGRID 会将现有对象元数据重新分发到新节点，从而增加网格的整体元数据容量。无需用户操作。已清除 * 低元数据存储 * 警报。

对服务进行故障排除：状态 - **Cassandra** （ **SVST** ）警报进行故障排除

服务：状态 - Cassandra （ SVST ）警报指示您可能需要为存储节点重建 Cassandra 数据库。Cassandra 用作 StorageGRID 的元数据存储。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。

关于此任务

如果 Cassandra 停止超过 15 天（例如，存储节点已关闭），则在节点恢复联机后， Cassandra 将无法启动。您必须为受影响的 DDS 服务重建 Cassandra 数据库。

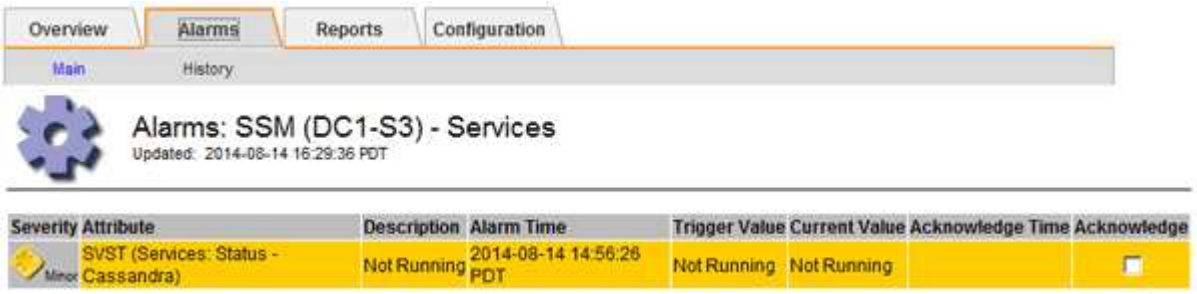
您可以 运行诊断 获取网格当前状态的追加信息 。

如果两个或多个 Cassandra 数据库服务关闭超过 15 天，请联系技术支持，不要继续执行以下步骤。

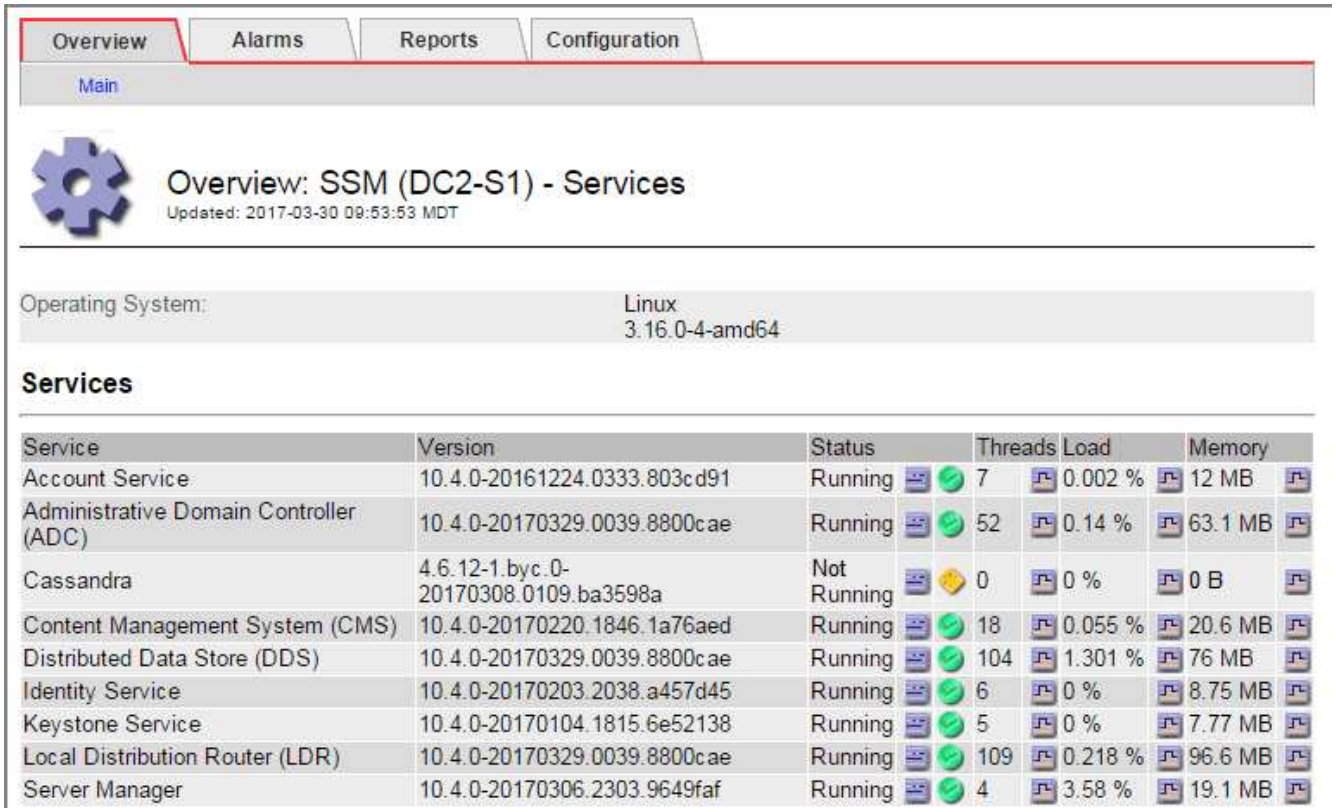
步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* > * SSM* > * 服务 * > * 警报 * > * 主 * 以显示警报。

   此示例显示已触发 SVST 警报。



   "SSM 服务主页 " 页面还指示 Cassandra 未运行。



3. 【重新启动 Cassandra_from_the_Storage_Node ， start=3]] 尝试从存储节点重新启动 Cassandra ：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root ： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 输入： ` /etc/init.d/Cassandra status`
   c. 如果 Cassandra 未运行，请重新启动它： ` /etc/init.d/Cassandra restart`

4. 如果 Cassandra 未重新启动，请确定 Cassandra 已关闭多长时间。如果 Cassandra 已关闭超过 15 天，则必须重建 Cassandra 数据库。

   如果两个或更多 Cassandra 数据库服务已关闭，请联系技术支持，不要继续执行以下步骤。

   您可以通过绘制 Cassandra 图表或查看 servermanager.log 文件来确定 Cassandra 已关闭多长时间。

5. 绘制 Cassandra 图表：

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 存储节点 _* > * SSM* > * 服务 * > * 报告 * > * 图表 * 。

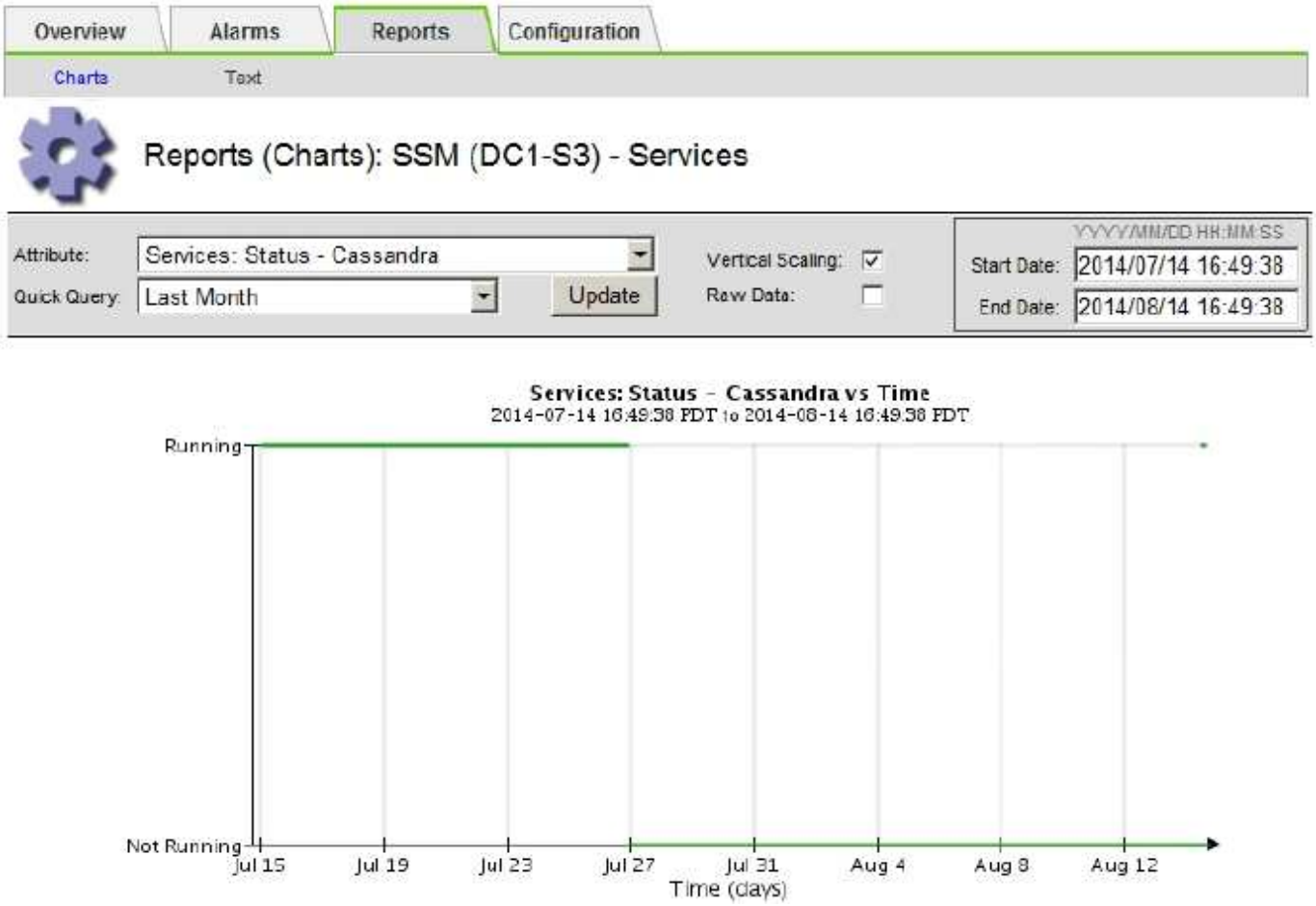
   b. 选择 * 属性 * > * 服务：状态 - Cassandra* 。

   c. 对于 * 开始日期 * ，请输入至少早于当前日期 16 天的日期。对于 * 结束日期 * ，输入当前日期。

   d. 单击 * 更新 * 。

   e. 如果图表显示 Cassandra 关闭超过 15 天，请重建 Cassandra 数据库。

以下图表示例显示 Cassandra 已关闭至少 17 天。



1. 查看存储节点上的 servermanager.log 文件：

   a. 登录到网格节点：

      i. 输入以下命令： `ssh admin@grid_node_ip`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

b. 输入： `cat /var/local/log/servermanager.log`

此时将显示 servermanager.log 文件的内容。

如果 Cassandra 已关闭超过 15 天，则 servermanager.log 文件中将显示以下消息：

```
"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. 确保此消息的时间戳是您按照步骤中的说明尝试重新启动 Cassandra 的时间 从存储节点重新启动 Cassandra。

Cassandra 可以有多个条目；您必须找到最新的条目。

b. 如果 Cassandra 已关闭超过 15 天，则必须重建 Cassandra 数据库。

有关说明，请参见 将存储节点恢复到关闭状态超过 15 天。

c. 如果重建 Cassandra 后无法清除警报，请联系技术支持。

对 **Cassandra** 内存不足错误（ **SMTTT** 警报）进行故障排除

如果 Cassandra 数据库出现内存不足错误，则会触发总计事件（ SMT ）警报。如果发生此错误，请联系技术支持以使用问题描述 。

关于此任务

如果 Cassandra 数据库发生内存不足错误，则会创建堆转储，触发总事件（ SMT ）警报， Cassandra 堆内存不足错误计数将增加 1 。

步骤

1. 要查看事件，请选择 * 支持 * > * 工具 * > * 网格拓扑 * > * 配置 * 。
2. 验证 Cassandra 堆内存不足错误计数是否为 1 或更高。

   您可以 运行诊断 获取网格当前状态的追加信息 。
3. 转至 ` /var/local/core/` ，压缩 `Cassandra.hprof` 文件，然后将其发送给技术支持。
4. 备份 `Cassandra.hprof` 文件，然后将其从 ` /var/local/core/ 目录` 中删除。

   此文件最大可达 24 GB ，因此您应将其删除以释放空间。
5. 解决问题描述 后，选中 Cassandra 堆内存不足错误计数的 * 重置 * 复选框。然后选择 * 应用更改 * 。

要重置事件计数，您必须具有网格拓扑页面配置权限。

对证书错误进行故障排除

如果您在尝试使用 Web 浏览器， S3 或 Swift 客户端或外部监控工具连接到 StorageGRID 时看到安全或证书问题描述 ，则应检查此证书。

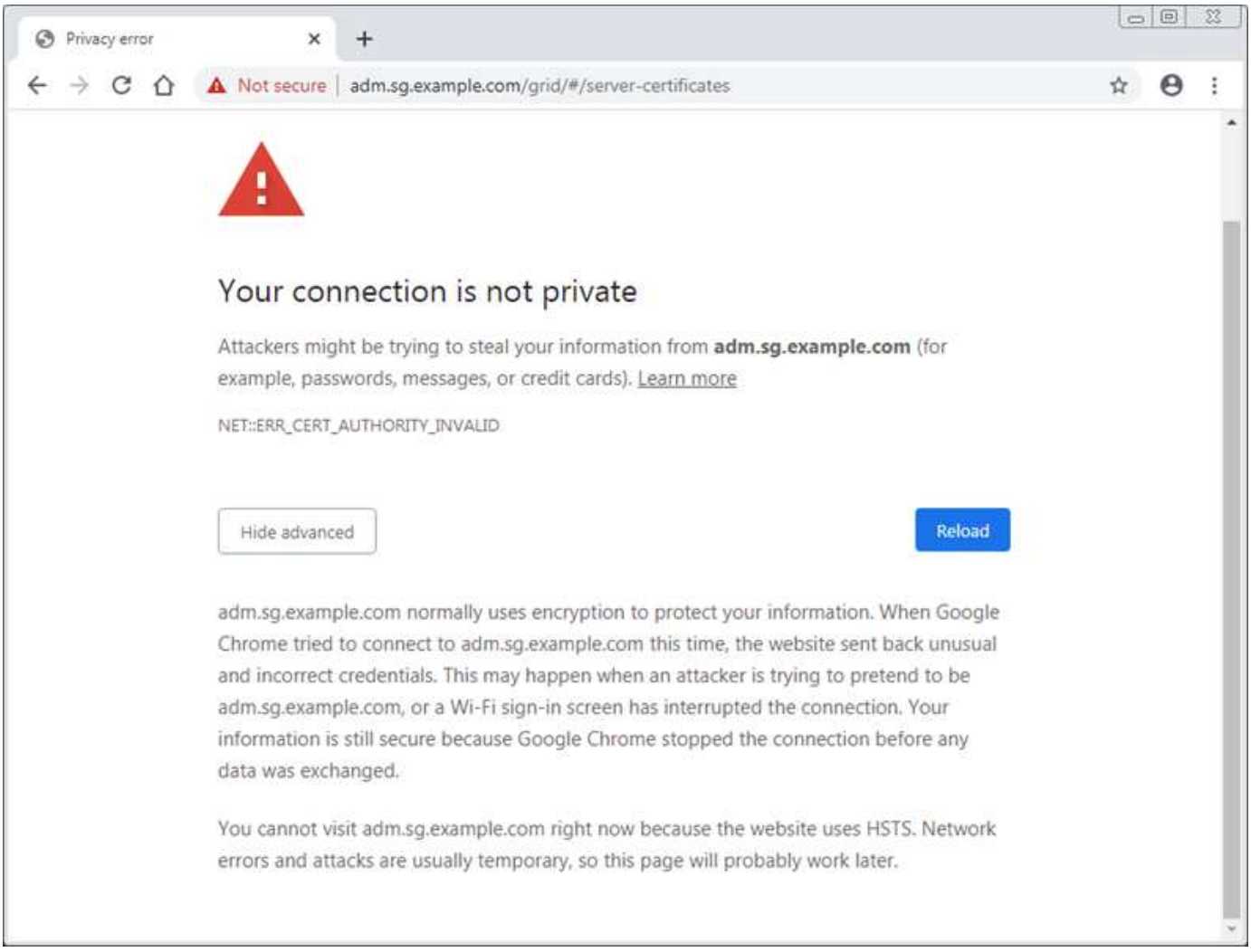
关于此任务

尝试使用网格管理器，网格管理 API ，租户管理器或租户管理 API 连接到 StorageGRID 时，证书错误可能会出现发生原因 问题。尝试连接到 S3 或 Swift 客户端或外部监控工具时，也可能发生证书错误。

如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：

- 您的自定义管理接口证书将过期。
- 您可以从自定义管理接口证书还原到默认服务器证书。

以下示例显示了自定义管理接口证书过期时的证书错误：



为了确保操作不会因服务器证书失败而中断，当服务器证书即将过期时，将触发 * 管理接口的服务器证书到期 *

警报。

在使用客户端证书进行外部 Prometheus 集成时，证书错误可能是由 StorageGRID 管理接口证书或客户端证书引起的。当客户端证书即将过期时，将触发 " 证书 " 页面上配置的 * 客户端证书到期 * 警报。

步骤

如果您收到有关证书已过期的警报通知，请访问证书详细信息：。选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 选择相应的证书选项卡。

1. 检查证书的有效期。+ 某些 Web 浏览器以及 S3 或 Swift 客户端不接受有效期超过 398 天的证书。
2. 如果证书已过期或即将过期，请上传或生成新证书。
   - 有关服务器证书，请参见的步骤 为网格管理器和租户管理器配置自定义服务器证书。
   - 有关客户端证书，请参见的步骤 配置客户端证书。
3. 对于服务器证书错误，请尝试以下任一或两个选项：
   - 确保已填充证书的使用者备用名称（ SAN ），并且 SAN 与要连接到的节点的 IP 地址或主机名匹配。
   - 如果您尝试使用域名连接到 StorageGRID ：
     i. 输入管理节点的 IP 地址，而不是域名，以绕过连接错误并访问网格管理器。
     ii. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 选择相应的证书选项卡 安装新的自定义证书或继续使用默认证书。
     iii. 在管理 StorageGRID 的说明中，请参见的步骤 为网格管理器和租户管理器配置自定义服务器证书。

对管理节点和用户界面问题进行故障排除

您可以执行多项任务来帮助确定与管理节点和 StorageGRID 用户界面相关的问题的根源。

对登录错误进行故障排除

如果您在登录到 StorageGRID 管理节点时遇到错误，则您的系统可能具有身份联合配置的问题描述 ，网络或硬件问题，具有管理节点服务的问题描述 或连接的存储节点上具有 Cassandra 数据库的问题描述 。

您需要的内容

- 您必须具有 `passwords.txt` 文件。
- 您必须具有特定的访问权限。

关于此任务

如果在尝试登录到管理节点时看到以下任何错误消息，请遵循以下故障排除准则：

- 您的此帐户凭据无效。请重试。
- 正在等待服务启动 ...
- 内部服务器错误。服务器遇到错误，无法完成您的请求。请重试。如果问题仍然存在，请联系技术支持。
- 无法与服务器通信。正在重新加载页面 ...

步骤

1. 等待 10 分钟，然后重新尝试登录。

如果此错误未自动解决，请转至下一步。

2. 如果您的 StorageGRID 系统具有多个管理节点，请尝试从另一个管理节点登录到网格管理器。
   - 如果您能够登录，则可以使用 * 信息板 * ， * 节点 * ， * 警报 * 和 * 支持 * 选项来帮助确定错误的发生原因 。
   - 如果只有一个管理节点，或者您仍然无法登录，请转至下一步。
3. 确定节点的硬件是否脱机。
4. 如果为 StorageGRID 系统启用了单点登录（ SSO ），请参见 StorageGRID 管理说明中的配置单点登录步骤。

   要解决任何问题，您可能需要暂时禁用并重新启用单个管理节点的 SSO 。

   > 如果启用了 SSO ，则无法使用受限端口登录。必须使用端口 443 。

5. 确定您正在使用的帐户是否属于联合用户。

   如果此联合用户帐户不起作用，请尝试以本地用户（例如 root ）身份登录到网格管理器。

   - 如果本地用户可以登录：
     i. 查看显示的任何警报。
     ii. 选择 * 配置 * > * 访问控制 * > * 身份联合 * 。
     iii. 单击 * 测试连接 * 以验证 LDAP 服务器的连接设置。
     iv. 如果测试失败，请解决任何配置错误。
   - 如果本地用户无法登录，并且您确信凭据正确无误，请转至下一步。
6. 使用安全 Shell （ ssh ）登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
7. 查看网格节点上运行的所有服务的状态： `storagegRid-status`

   确保 NMS ， Mi ， nginx 和 mgmt API 服务均已运行。

   如果服务状态发生变化，输出将立即更新。

```
$ 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. 确认 nginx gw 服务正在运行 ` # service nginx gw status`
9. 【使用 _lumberjack_to_collect_logs ， start=9]] 使用 lumberjack 收集日志： ` # /usr/local/sbin/lumberjack.rb`

   如果身份验证在过去失败，您可以使用 -start 和 -end Lumberjack 脚本选项指定适当的时间范围。有关这些选项的详细信息，请使用 lumberjack -h 。

   终端的输出指示日志归档的复制位置。

10. 【 review_logs ， start=10]] 查看以下日志：
    - ` /var/local/log/byncast.log`
    - ` /var/local/log/byncast-err.log`
    - ` /var/local/log/NMS.log`

◦ ` //* 命令 .txt`

11. 如果您无法确定管理节点存在任何问题问题描述，请执行以下任一命令来确定在您的站点上运行此 ADA 服务的三个存储节点的 IP 地址。通常，这些存储节点是站点上安装的前三个存储节点。

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

管理节点会在身份验证过程中使用此 ADC 服务。

12. 从管理节点中，使用您确定的 IP 地址登录到每个 ADC 存储节点。
    a. 输入以下命令： `ssh admin@grid_node_ip`
    b. 输入 `passwords.txt` 文件中列出的密码。
    c. 输入以下命令切换到 root： `su -`
    d. 输入 `passwords.txt` 文件中列出的密码。

    以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

13. 查看网格节点上运行的所有服务的状态： `storagegRid-status`

    确保 idnt ， Acct ， nginx 和 Cassandra 服务均已运行。

14. 重复步骤 使用 Lumberjack 收集日志 和 查看日志 查看存储节点上的日志。
15. If you are unable to resolve the issue, contact technical support.

    将收集的日志提供给技术支持。另请参见 日志文件参考。

对用户界面问题进行故障排除

升级到新版本的 StorageGRID 软件后，您可能会看到网格管理器或租户管理器出现问题。

Web 界面未按预期响应

升级 StorageGRID 软件后，网格管理器或租户管理器可能无法按预期做出响应。

如果您在使用 Web 界面时遇到问题：

- 确保您使用的是 支持的 Web 浏览器。

  StorageGRID 11.5 的浏览器支持已更改。确认您使用的是受支持的版本。

- 清除 Web 浏览器缓存。

  清除缓存将删除先前版本的 StorageGRID 软件所使用的过时资源，并允许用户界面再次正常运行。有关说明，请参见 Web 浏览器的文档。

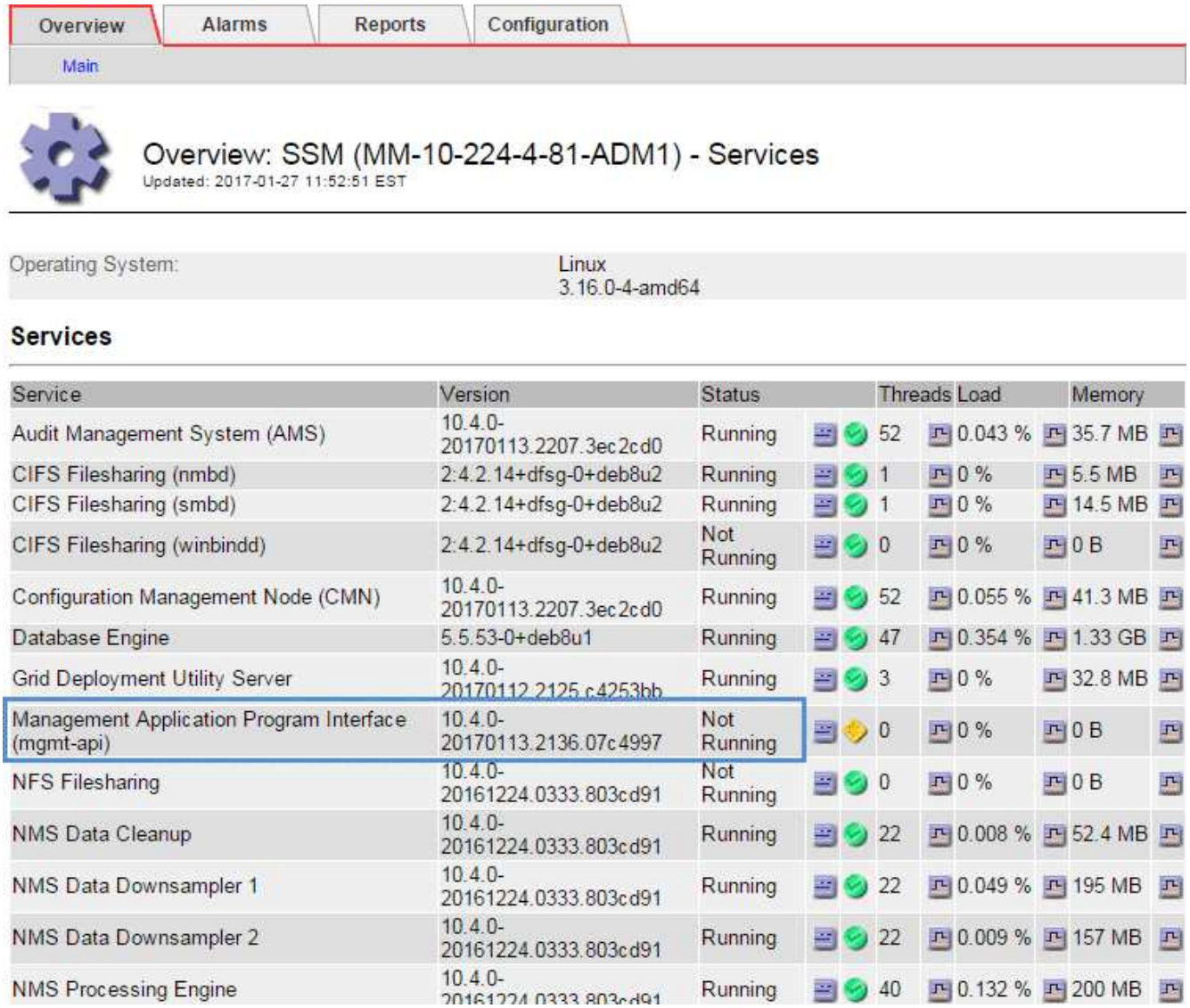
如果 StorageGRID 系统包含多个管理节点，则可以使用另一个管理节点检查不可用管理节点的状态。

您需要的内容

您必须具有特定的访问权限。

步骤

1. 从可用的管理节点中，使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
3. 选择 * 站点 * > * 不可用管理节点 _* > * SSM* > * 服务 * > * 概述 * > * 主 * 。
4. 查找状态为未运行且可能也显示为蓝色的服务。



5. 确定是否已触发警报。
6. 采取适当的操作解决问题描述 。

相关信息

对网络，硬件和平台问题进行故障排除

您可以执行多项任务来帮助确定与 StorageGRID 网络，硬件和平台问题相关的问题的根源。

对"`422：Unprocessable Entity`"错误进行故障排除

错误 422 ： 在许多情况下可能会出现 Unprocessable Entity 。检查错误消息以确定导致问题描述 的原因。

如果您看到列出的错误消息之一，请采取建议的操作。

错误消息	根发生原因 和更正操作

`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`
	如果在使用 Windows Active Directory （ AD ）配置身份联合时为传输层安全（ TLS ）选择 * 不使用 TLS* 选项，则可能会出现此消息。
	
	不支持对强制执行 LDAP 签名的 AD 服务器使用 * 不使用 TLS* 选项。您必须为 TLS 选择 * 使用 STARTTL* 选项或 * 使用 LDAPS* 选项。

错误消息	根发生原因 和更正操作

`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)`
	如果您尝试使用不受支持的密码从 StorageGRID 到用于标识联合或云存储池的外部系统建立传输层安全（ TLS ）连接，则会显示此消息。
	
	检查外部系统提供的密码。系统必须使用 StorageGRID 支持的其中一个密码进行传出 TLS 连接，如 StorageGRID 管理说明所示。

相关信息

管理 StorageGRID

【故障排除_MTU_ALERT]]对网格网络MTU不匹配警报进行故障排除

如果网格网络接口（ eth0 ）的最大传输单元（ MTU ）设置在网格中的各个节点之间差别很大，则会触发 * 网格网络 MTU 不匹配 * 警报。

关于此任务

MTU 设置的差异可能表明，某些（但并非所有） eth0 网络配置了巨型帧。如果 MTU 大小不匹配大于 1000 ，则可能会出现发生原因 网络性能问题。

步骤

1. 列出所有节点上 eth0 的 MTU 设置。
   - 使用网格管理器中提供的查询。
   - 导航到 ` 主管理节点 IP 地址 _/metrics/graph` 并输入以下查询： `node_network_mtu` 字节 `{interface="eth0' }`
2. 根据需要修改 MTU 设置，以确保所有节点上的网格网络接口（ eth0 ）设置相同。
   - 对于设备节点，请参见适用于您的设备的安装和维护说明。
   - 对于基于 Linux 和 VMware 的节点，请使用以下命令： ` +/usr/sbin/change-ip.py （ -h] （ -n 节点） MTU 网络（ network…） +`
     - 示例 * ： `change-ip.py -n node 1500 grid admin`
     - 注 * ： 在基于 Linux 的节点上，如果容器中网络所需的 MTU 值超过主机接口上已配置的值，则必须先将主机接口配置为具有所需的 MTU 值， 然后，使用 `change-ip.py` 脚本更改容器中网络的 MTU 值。

     使用以下参数修改基于 Linux 或 VMware 的节点上的 MTU 。

定位参数	Description
`mtu`	要设置的 MTU 。必须介于 1280 到 9216 之间。
网络	要应用 MTU 的网络。包括以下一种或多种网络类型： • 网格 • 管理员 • 客户端

+

可选参数	Description
` h ，–帮助`	显示帮助消息并退出。
` -n node ， -node node`	节点。默认值为本地节点。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

对网络接收错误（ **NRER** ）警报进行故障排除

StorageGRID 与网络硬件之间的连接问题可能会导致网络接收错误（ NRER ）警报。在某些情况下，无需手动干预即可清除 NRER 错误。如果未清除这些错误，请执行建议的操作。

关于此任务

与 StorageGRID 连接的网络硬件出现以下问题可能会导致 NRER 警报：

- 需要正向错误更正（ FEC ），但不在使用中
- 交换机端口和 NIC MTU 不匹配
- 链路错误率较高
- NIC 环缓冲区溢出

步骤

1. 根据您的网络配置，对 NRER 警报的所有潜在原因执行故障排除步骤。
    - 如果此错误是由 FEC 不匹配引起的，请执行以下步骤：

- 注 * ： 这些步骤仅适用于 StorageGRID 设备上 FEC 不匹配导致的 NRER 错误。

  i. 检查连接到 StorageGRID 设备的交换机中端口的 FEC 状态。

  ii. 检查从设备到交换机的缆线的物理完整性。

  iii. 如果要更改 FEC 设置以尝试解决 NRER 警报，请首先确保在 StorageGRID 设备安装程序的 " 链路配置 " 页面上将设备配置为 * 自动 * 模式（请参见适用于您设备的安装和维护说明）。然后，更改交换机端口上的 FEC 设置。如果可能， StorageGRID 设备端口会调整其 FEC 设置以匹配。

  （您不能在 StorageGRID 设备上配置 FEC 设置。相反，设备会尝试发现并镜像其所连接的交换机端口上的 FEC 设置。如果强制链路达到 25 GbE 或 100 GbE 网络速度，则交换机和 NIC 可能无法协商通用 FEC 设置。如果没有通用的 FEC 设置，网络将回退到 "`no-FEC` " 模式。如果未启用 FEC ，则连接更容易受到电气噪声引起的错误的影响。）

- 注 * ： StorageGRID 设备支持光纤节点（ FC ）和 Reed Solomon （ RS ） FEC ，并且不支持 FEC 。

◦ 如果此错误是由于交换机端口和 NIC MTU 不匹配导致的，请检查节点上配置的 MTU 大小是否与交换机端口的 MTU 设置相同。

节点上配置的 MTU 大小可能小于节点所连接的交换机端口上的设置。如果 StorageGRID 节点收到的以太网帧大于其 MTU ，则可能会报告 NRER 警报。如果您认为发生了这种情况，请根据端到端 MTU 目标或要求更改交换机端口的 MTU 以匹配 StorageGRID 网络接口 MTU ，或者更改 StorageGRID 网络接口的 MTU 以匹配交换机端口。

> 为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

> 要更改 MTU 设置，请参见适用于您的设备的安装和维护指南。

◦ 如果此错误是由高链路错误率引起的，请执行以下步骤：

  i. 启用 FEC （如果尚未启用）。

  ii. 确认网络布线质量良好，并且未损坏或连接不正确。

  iii. 如果电缆似乎不存在问题，请联系技术支持。

  > 在具有高电噪声的环境中，您可能会发现错误率较高。

◦ 如果错误是 NIC 环缓冲区溢出，请联系技术支持。

如果 StorageGRID 系统过载且无法及时处理网络事件，则环缓冲区可能会溢出。

2. 解决基本问题后，重置错误计数器。

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 资源 * > * 配置 * > * 主 * 。

   c. 选择 * 重置接收错误计数 * ，然后单击 * 应用更改 * 。

相关信息

对网格网络 MTU 不匹配警报进行故障排除

警报参考（旧系统）

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

SG100 和 SG1000 服务设备

对时间同步错误进行故障排除

您可能会在网格中看到时间同步问题。

如果遇到时间同步问题，请确认您至少指定了四个外部 NTP 源，每个源均提供 Stratum 3 或更好的参考，并且所有外部 NTP 源均正常运行且可由 StorageGRID 节点访问。

> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。

相关信息

恢复和维护

Linux： 网络连接问题

您可能会看到 Linux 主机上托管的 StorageGRID 网格节点的网络连接问题。

MAC 地址克隆

在某些情况下，可以使用 MAC 地址克隆来解决网络问题。如果使用的是虚拟主机，请在节点配置文件中将每个网络的 MAC 地址克隆密钥值设置为 "true" 。此设置会使 StorageGRID 容器的 MAC 地址使用主机的 MAC 地址。要创建节点配置文件，请参见适用于您的平台的安装指南中的说明。

> 创建单独的虚拟网络接口，以供 Linux 主机操作系统使用。如果发生原因 虚拟机管理程序未启用混杂模式，则对 Linux 主机操作系统和 StorageGRID 容器使用相同的网络接口可能会使主机操作系统无法访问。

有关启用 MAC 克隆的详细信息，请参见适用于您的平台的安装指南中的说明。

混杂模式

如果您不希望使用 MAC 地址克隆，而希望允许所有接口接收和传输非虚拟机管理程序分配的 MAC 地址的数据， 对于配置模式， MAC 地址更改和伪造传输，请确保虚拟交换机和端口组级别的安全属性设置为 * 接受 * 。虚拟交换机上设置的值可以被端口组级别的值覆盖，因此请确保这两个位置的设置相同。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

Linux：节点状态为"`孤立`"

处于孤立状态的 Linux 节点通常表示控制节点容器的 StorageGRID 服务或 StorageGRID 节点守护进程意外终止。

关于此任务

如果 Linux 节点报告其处于孤立状态，您应：

- 检查日志中的错误和消息。
- 尝试重新启动节点。
- 如有必要，请使用 container engine 命令停止现有节点容器。
- 重新启动节点。

步骤

1. 检查服务守护进程和孤立节点的日志，查看是否存在明显的错误或有关意外退出的消息。
2. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
3. 运行以下命令，尝试重新启动节点： ` $sudo StorageGRID node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   如果节点已孤立，则响应为

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. 在 Linux 中，停止容器引擎以及任何控制存储节点进程。例如：`sudo Docker stop -time secondscontainer-name`

   对于 `seconds` ，输入要等待容器停止的秒数（通常为 15 分钟或更短）。例如：

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. 重新启动节点： `StorageGRID node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

Linux： 对 IPv6 支持进行故障排除

如果您在 Linux 主机上安装了 StorageGRID 节点，并且注意到尚未按预期为节点容器分配 IPv6 地址，则可能需要在内核中启用 IPv6 支持。

关于此任务

您可以在网格管理器的以下位置查看已分配给网格节点的 IPv6 地址：

- 选择 * 节点 * ，然后选择节点。然后，在概述选项卡上选择 * IP 地址 * 旁边的 * 显示更多 * 。
- 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * ； node_* > * 。 ssm * > * 资源 * 。如果已分配 IPv6 地址，则此地址将列在 * 网络地址 * 部分的 IPv4 地址下方。

如果未显示 IPv6 地址且节点安装在 Linux 主机上，请按照以下步骤在内核中启用 IPv6 支持。

步骤

1. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
2. 运行以下命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

结果应为 0 。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

如果结果不是 0 ，请参见适用于您的操作系统的文档，了解如何更改 `sysctl` 设置。然后，将此值更改为 0 ，然后再继续。

3. 输入 StorageGRID 节点容器： `StorageGRID node enter node-name`
4. 运行以下命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

结果应为 1 。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

如果结果不是 1 ，则此操作步骤 不适用。请联系技术支持。

5. 退出容器： `exit`

```
root@DC1-S1:~ # exit
```

6. 以 root 用户身份编辑以下文件： ` /var/lib/storaggrid/settings/sysctl.d/net.conf` 。

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 找到以下两行并删除注释标记。然后，保存并关闭该文件。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 运行以下命令重新启动 StorageGRID 容器：

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

对外部系统日志服务器进行故障排除

下表介绍了外部系统日志服务器错误消息并列出了更正操作。

错误消息	问题描述 和建议的操作
无法解析主机名	您为系统日志服务器输入的 FQDN 无法解析为 IP 地址。 1. 检查输入的主机名。如果输入了 IP 地址，请确保其为 w.x.y.z （ " 点分十进制 " ）表示法中的有效 IP 地址。 2. 检查 DNS 服务器是否配置正确。 3. 确认每个节点均可访问 DNS 服务器的 IP 地址。
连接被拒绝	拒绝与系统日志服务器建立 TCP 或 TLS 连接。可能没有服务在侦听主机的 TCP 或 TLS 端口，或者防火墙可能正在阻止访问。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 2. 确认系统日志服务的主机正在运行侦听指定端口的系统日志守护进程。 3. 确认防火墙不会阻止从节点到系统日志服务器的 IP 和端口的 TCP/TLS 连接访问。

错误消息	问题描述 和建议的操作
无法访问网络	系统日志服务器不在直连子网上。路由器返回 ICMP 失败消息，指示它无法将测试消息从列出的节点转发到系统日志服务器。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 对于列出的每个节点，请检查网格网络子网列表，管理网络子网列表和客户端网络网关。确认这些配置已通过预期网络接口和网关（网格，管理员或客户端）将流量路由到系统日志服务器。
无法访问主机	系统日志服务器位于直连子网上（列出的节点用于其网格，管理员或客户端 IP 地址的子网）。节点尝试发送测试消息，但未收到对系统日志服务器 MAC 地址的 ARP 请求的响应。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 检查运行系统日志服务的主机是否已启动。
连接超时	已尝试进行 TCP/TLS 连接，但系统日志服务器长时间未收到任何响应。可能存在路由配置不当或防火墙在未发送任何响应的情况下丢弃流量（通用配置）。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 对于列出的每个节点，请检查网格网络子网列表，管理网络子网列表和客户端网络网关。确认已将这些配置为通过网络接口和网关（网格，管理员或客户端）将流量路由到系统日志服务器，而您希望通过该网关访问系统日志服务器。 3. 确认防火墙未阻止从列出的节点到系统日志服务器的 IP 和端口访问 TCP/TLS 连接。
配对节点已关闭连接	已成功建立与系统日志服务器的 TCP 连接，但稍后关闭。原因可能包括： • 系统日志服务器可能已重新启动或重新启动。 • 节点和系统日志服务器可能具有不同的 TCP/TLS 设置。 • 中间防火墙可能正在关闭闲置的 TCP 连接。 • 侦听系统日志服务器端口的非系统日志服务器可能已关闭连接。 a. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 b. 如果您使用的是 TLS ，请确认系统日志服务器也使用 TLS 。如果您使用的是 TCP ，请确认系统日志服务器也使用 TCP 。 c. 检查中间防火墙是否未配置为关闭空闲 TCP 连接。

错误消息	问题描述 和建议的操作
TLS 证书错误	从系统日志服务器收到的服务器证书与您提供的 CA 证书包和客户端证书不兼容。 1. 确认 CA 证书包和客户端证书（如果有）与系统日志服务器上的服务器证书兼容。 2. 确认系统日志服务器的服务器证书中的身份包含预期的 IP 或 FQDN 值。
转发已暂停	系统日志记录不再转发到系统日志服务器， StorageGRID 无法检测到原因。 查看随此错误提供的调试日志，尝试确定根发生原因 。
TLS 会话已终止	系统日志服务器已终止 TLS 会话， StorageGRID 无法检测到原因。 1. 查看随此错误提供的调试日志，尝试确定根发生原因 。 2. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 3. 如果您使用的是 TLS ，请确认系统日志服务器也使用 TLS 。如果您使用的是 TCP ，请确认系统日志服务器也使用 TCP 。 4. 确认 CA 证书包和客户端证书（如果有）与系统日志服务器的服务器证书兼容。 5. 确认系统日志服务器的服务器证书中的身份包含预期的 IP 或 FQDN 值。
结果查询失败	用于系统日志服务器配置和测试的管理节点无法从列出的节点请求测试结果。一个或多个节点可能已关闭。 1. 按照标准故障排除步骤操作，确保节点联机且所有预期服务均正在运行。 2. 在列出的节点上重新启动 miscd 服务。

警报参考

下表列出了所有默认 StorageGRID 警报。您可以根据需要创建自定义警报规则，以适合您的系统管理方法。

请参见有关的信息 常用的 Prometheus 指标 了解其中某些警报中使用的指标。

警报名称	问题描述 和建议的操作
设备电池已过期	设备存储控制器中的电池已过期。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池出现故障	设备存储控制器中的电池出现故障。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池的已学习容量不足	设备存储控制器中的电池已获取容量不足。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池即将过期	设备存储控制器中的电池即将过期。 1. 请尽快更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。

警报名称	问题描述 和建议的操作
已取出设备电池	设备存储控制器中的电池缺失。 1. 安装电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池过热	设备存储控制器中的电池过热。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 调查可能导致温度升高的原因，例如风扇或暖通空调出现故障。 3. 如果此警报仍然存在，请联系技术支持。
设备 BMC 通信错误	与基板管理控制器（ BMC ）的通信已丢失。 1. 确认 BMC 运行正常。选择 * 节点 * ，然后选择设备节点的 * 硬件 * 选项卡。找到 Compute Controller BMC IP 字段，然后浏览到此 IP 。 2. 尝试将节点置于维护模式，然后关闭并重新打开设备电源，以恢复 BMC 通信。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG6000 存储设备 3. 如果此警报仍然存在，请联系技术支持。
设备缓存备份设备失败	永久性缓存备份设备出现故障。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 请联系技术支持。
设备缓存备份设备容量不足	缓存备份设备容量不足。 请联系技术支持。
设备缓存备份设备已写保护	缓存备份设备受写保护。 请联系技术支持。

警报名称	问题描述 和建议的操作
设备缓存内存大小不匹配	设备中的两个控制器具有不同的缓存大小。 请联系技术支持。
设备计算控制器机箱温度过高	StorageGRID 设备中计算控制器的温度已超过额定阈值。 1. 检查硬件组件是否过热，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备计算控制器 CPU 温度过高	StorageGRID 设备中计算控制器的 CPU 温度已超过额定阈值。 1. 检查硬件组件是否过热，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备

警报名称	问题描述 和建议的操作
设备计算控制器需要引起注意	在 StorageGRID 设备的计算控制器中检测到硬件故障。 1. 检查硬件组件是否存在错误，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备
设备计算控制器电源 A 出现问题	计算控制器中的电源 A 存在问题。此警报可能指示电源出现故障或无法供电。 1. 检查硬件组件是否存在错误，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备

警报名称	问题描述 和建议的操作
设备计算控制器电源 B 出现问题	计算控制器中的电源 B 出现问题。 此警报可能指示电源出现故障或无法供电。 1. 检查硬件组件是否存在错误，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备
设备计算硬件监控服务已停止	监控存储硬件状态的服务已停止报告数据。 1. 在基础操作系统中检查 EOS 系统状态服务的状态。 2. 如果此服务处于 stopped 或 error 状态，请重新启动此服务。 3. 如果此警报仍然存在，请联系技术支持。
检测到设备光纤通道故障	检测到设备存储控制器和计算控制器之间存在光纤通道链路问题。 此警报可能指示设备中存储控制器和计算控制器之间的光纤通道连接出现问题。 1. 检查硬件组件是否存在错误（ * 节点 * > * 设备节点 _* > * 硬件 * ）。如果任何组件的状态不是 "`标称，` "，请执行以下操作： a. 验证控制器之间的光纤通道缆线是否已完全连接。 b. 确保光纤通道缆线没有过度弯曲。 c. 确认 SFP+ 模块已正确就位。 ▪ 注： * 如果此问题仍然存在，则 StorageGRID 系统可能会自动使有问题的连接脱机。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG5700 存储设备 ◦ SG6000 存储设备
设备光纤通道 HBA 端口故障	光纤通道 HBA 端口出现故障或出现故障。 请联系技术支持。

警报名称	问题描述 和建议的操作
设备闪存缓存驱动器非最佳	用于 SSD 缓存的驱动器并非最佳驱动器。 1. 更换 SSD 缓存驱动器。请参见适用于您的设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
已卸下设备互连 / 电池箱	互连 / 电池箱缺失。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明。 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
缺少设备 LACP 端口	StorageGRID 设备上的端口不参与 LACP 绑定。 1. 检查交换机的配置。确保接口配置在正确的链路聚合组中。 2. 如果此警报仍然存在，请联系技术支持。
设备整体电源性能下降	StorageGRID 设备的电源已偏离建议的工作电压。 1. 检查电源 A 和 B 的状态以确定哪个电源运行异常，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ SG100 和 SG1000 服务设备

警报名称	问题描述 和建议的操作
设备存储控制器 A 出现故障	StorageGRID 设备中的存储控制器 A 出现故障。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器 B 故障	StorageGRID 设备中的存储控制器 B 出现故障。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器驱动器故障	StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器硬件问题描述	SANtricity 软件报告 StorageGRID 设备中的某个组件 " 需要关注 " 。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备

警报名称	问题描述 和建议的操作
设备存储控制器电源 A 出现故障	StorageGRID 设备中的电源 A 与建议的工作电压不同。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器电源 B 故障	StorageGRID 设备中的电源 B 与建议的工作电压不同。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储硬件监控服务已停止	监控存储硬件状态的服务已停止报告数据。 1. 在基础操作系统中检查 EOS 系统状态服务的状态。 2. 如果此服务处于 stopped 或 error 状态，请重新启动此服务。 3. 如果此警报仍然存在，请联系技术支持。
设备存储架降级	存储设备存储架中某个组件的状态为已降级。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
已超过设备温度	已超过设备存储控制器的额定或最大温度。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 调查可能导致温度升高的原因，例如风扇或暖通空调出现故障。 3. 如果此警报仍然存在，请联系技术支持。

警报名称	问题描述 和建议的操作
已卸下设备温度传感器	已卸下温度传感器。请联系技术支持。
Cassandra auto-compactor 错误	Cassandra 自动 compactor 出现错误。 Cassandra 自动 compactor 位于所有存储节点上，用于管理 Cassandra 数据库的大小，以覆盖和删除繁重的工作负载。虽然此情况持续存在，但某些工作负载的元数据消耗量会异常高。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 请联系技术支持。
正在将审核日志添加到内存队列中	节点无法将日志发送到本地系统日志服务器，并且内存队列正在填满。 1. 确保 rsyslog 服务正在节点上运行。 2. 如有必要，请使用命令 `service rsyslog restart` 在节点上重新启动 rsyslog 服务。 3. 如果无法重新启动 rsyslog 服务，并且您未在管理节点上保存审核消息，请联系技术支持。如果不更正此情况，审核日志将丢失。
Cassandra 自动数据压缩器指标已过期	描述 Cassandra 自动数据压缩器的指标已过时。 Cassandra 自动 compactor 位于所有存储节点上，用于管理 Cassandra 数据库的大小，以覆盖和删除繁重的工作负载。尽管此警报持续存在，但某些工作负载的元数据消耗量会异常高。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 请联系技术支持。

警报名称	问题描述 和建议的操作
Cassandra 通信错误	运行 Cassandra 服务的节点无法彼此通信。 此警报表示存在干扰节点到节点通信的情况。一个或多个存储节点上可能存在网络问题描述 或 Cassandra 服务已关闭。 1. 确定是否存在其他影响一个或多个存储节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 检查是否存在可能影响一个或多个存储节点的网络问题描述 。 3. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 4. 对于系统中的每个存储节点，选择 * SSM* > * 服务 * 。确保 Cassandra 服务的状态为 "running" 。 5. 如果 Cassandra 未运行，请按照的步骤进行操作 启动或重新启动服务。 6. 如果 Cassandra 服务的所有实例现在都在运行，并且警报未得到解决，请联系技术支持。
Cassandra compActions 已过载	Cassandra 数据缩减过程过载。 如果数据缩减过程过载，读取性能可能会下降， RAM 可能会用尽。Cassandra 服务也可能无响应或崩溃。 1. 按照的步骤重新启动 Cassandra 服务 正在重新启动服务。 2. 如果此警报仍然存在，请联系技术支持。
Cassandra 修复指标已过期	描述 Cassandra 修复作业的指标已过时。如果此情况持续 48 小时以上，则存储分段列表等客户端查询可能会显示已删除的数据。 1. 重新启动节点。在网格管理器中，转到 * 节点 * ，选择节点，然后选择任务选项卡。 2. 如果此警报仍然存在，请联系技术支持。
Cassandra 修复进度缓慢	Cassandra 数据库修复进度缓慢。 当数据库修复速度较慢时， Cassandra 数据一致性操作会受到阻碍。如果此情况持续 48 小时以上，则存储分段列表等客户端查询可能会显示已删除的数据。 1. 确认所有存储节点均已联机，并且没有与网络相关的警报。 2. 监控此警报最多 2 天，查看问题描述 是否自行解决。 3. 如果数据库修复继续缓慢进行，请联系技术支持。

警报名称	问题描述 和建议的操作
Cassandra 修复服务不可用	Cassandra 修复服务不可用。 Cassandra 修复服务位于所有存储节点上，可为 Cassandra 数据库提供关键修复功能。如果此情况持续 48 小时以上，则存储分段列表等客户端查询可能会显示已删除的数据。 1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 2. 对于系统中的每个存储节点，选择 * SSM* > * 服务 * 。确保 Cassandra Reaper 服务的状态为 "running" 。 3. 如果 Cassandra Reaper 未运行，请按照中的步骤进行操作 启动或重新启动服务。 4. 如果 Cassandra Reaper 服务的所有实例现在都在运行，并且警报未得到解决，请联系技术支持。
Cassandra 表损坏	Cassandra 检测到表损坏。 如果 Cassandra 检测到表损坏，则它会自动重新启动。 请联系技术支持。
云存储池连接错误	云存储池的运行状况检查检测到一个或多个新错误。 1. 转到 " 存储池 " 页面的 " 云存储池 " 部分。 2. 查看 Last Error 列以确定哪个 Cloud Storage Pool 存在错误。 3. 请参见的说明 通过信息生命周期管理管理对象。
DHCP 租约已过期	网络接口上的 DHCP 租约已过期。如果 DHCP 租约已过期，请执行建议的操作： 1. 确保此节点与受影响接口上的 DHCP 服务器之间存在连接。 2. 确保 DHCP 服务器上的受影响子网中有可分配的 IP 地址。 3. 确保为 DHCP 服务器中配置的 IP 地址预留了永久空间。或者，使用 StorageGRID 更改 IP 工具在 DHCP 地址池之外分配静态 IP 地址。请参见 恢复和维护说明。

警报名称	问题描述 和建议的操作
DHCP 租约即将到期	网络接口上的 DHCP 租约即将到期。 要防止 DHCP 租约到期，请执行建议的操作： 1. 确保此节点与受影响接口上的 DHCP 服务器之间存在连接。 2. 确保 DHCP 服务器上的受影响子网中有可分配的 IP 地址。 3. 确保为 DHCP 服务器中配置的 IP 地址预留了永久空间。或者，使用 StorageGRID 更改 IP 工具在 DHCP 地址池之外分配静态 IP 地址。请参见 恢复和维护说明。
DHCP 服务器不可用	DHCP 服务器不可用。 StorageGRID 节点无法联系您的 DHCP 服务器。无法验证节点 IP 地址的 DHCP 租约。 1. 确保此节点与受影响接口上的 DHCP 服务器之间存在连接。 2. 确保 DHCP 服务器上的受影响子网中有可分配的 IP 地址。 3. 确保为 DHCP 服务器中配置的 IP 地址预留了永久空间。或者，使用 StorageGRID 更改 IP 工具在 DHCP 地址池之外分配静态 IP 地址。请参见 恢复和维护说明。
磁盘 I/O 速度非常慢	磁盘 I/O 非常慢可能会影响 StorageGRID 性能。 1. 如果问题描述 与存储设备节点相关，请使用 SANtricity 系统管理器检查是否存在故障驱动器，存在预测故障的驱动器或正在进行的驱动器修复。此外，还应检查设备计算控制器和存储控制器之间的光纤通道或 SAS 链路的状态，以查看是否有任何链路已关闭或显示的错误率过高。 2. 检查托管此节点的卷的存储系统，以确定并更正慢速 I/O 的根发生原因 3. 如果此警报仍然存在，请联系技术支持。 ◦ 注意： * 受影响的节点可能会禁用服务并自行重新启动，以避免影响整体网格性能。如果清除了底层条件，并且这些节点检测到正常 I/O 性能，则它们将自动恢复到完全服务状态。

警报名称	问题描述 和建议的操作

EC 重新平衡失败	在存储节点之间重新平衡擦除编码的数据的作业失败或已被用户暂停。
	
	1. 确保要重新平衡的站点上的所有存储节点均已联机且可用。
	2. 确保要重新平衡的站点上没有卷故障。如果存在，请终止 EC 重新平衡作业，以便您可以运行修复作业。
	
	`"rebalance-data terminate -job-id <ID>"`
	
	3. 确保要重新平衡的站点上没有服务故障。如果服务未运行，请按照恢复和维护说明中有关启动或重新启动服务的步骤进行操作。
	4. 解决任何问题后，请在主管理节点上运行以下命令以重新启动作业：
	
	`"rebalance-data start -job-id <ID>"`
	
	5. 如果无法解决此问题，请联系技术支持。

EC 修复失败	擦除编码数据的修复作业失败或已停止。 1. 确保有足够的可用存储节点或卷来替代发生故障的存储节点或卷。 2. 确保有足够的可用存储节点来满足活动 ILM 策略的要求。 3. 确保没有网络连接问题。 4. 解决任何问题后，请在主管理节点上运行以下命令以重新启动作业： `"repair-data start-EC-node-repair -repair-id <ID>"` 5. 如果无法解决此问题，请联系技术支持。
EC 修复已停止	擦除编码数据的修复作业已停止。 1. 确保有足够的可用存储节点或卷来替代发生故障的存储节点或卷。 2. 确保没有网络连接问题。 3. 解决任何问题后，请检查警报是否已解决。要查看有关修复进度的更详细报告，请在主管理节点上运行以下命令： `"repair-data show-EC-repair-status -repair-id <ID>"` 4. 如果无法解决此问题，请联系技术支持。

警报名称	问题描述 和建议的操作
电子邮件通知失败	无法发送警报电子邮件通知。 如果警报电子邮件通知失败或无法传送测试电子邮件（从 * 警报 * > * 电子邮件设置 * 页面发送），则会触发此警报。 1. 从警报的 * 站点 / 节点 * 列中列出的管理节点登录到网格管理器。 2. 转到 * 警报 * > * 电子邮件设置 * 页面，检查设置，并根据需要进行更改。 3. 单击 * 发送测试电子邮件 * ，然后检查测试收件人的收件箱中是否存在此电子邮件。如果无法发送测试电子邮件，则可能会触发此警报的新实例。 4. 如果无法发送测试电子邮件，请确认您的电子邮件服务器已联机。 5. 如果服务器正在运行，请选择 * 支持 * > * 工具 * > * 日志 * ，然后收集管理节点的日志。指定警报时间前后 15 分钟的时间段。 6. 提取下载的归档并查看 `Prometheus.log` （ _/GID<time_stamp>/<site_node>/<time_stamp>/metrics/Prometheus.log ）` 的内容。 7. 如果无法解决此问题，请联系技术支持。
在 " 证书 " 页面上配置的客户端证书到期	在 " 证书 " 页面上配置的一个或多个客户端证书即将过期。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。 2. 选择一个即将到期的证书。 3. 选择 * 附加新证书 * 上传或生成新证书。 4. 对即将过期的每个证书重复上述步骤。
负载平衡器端点证书到期	一个或多个负载平衡器端点证书即将过期。 1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。 2. 选择证书即将过期的端点。 3. 选择 * 编辑端点 * 可上传或生成新证书。 4. 对证书已过期或即将过期的每个端点重复上述步骤。 有关管理负载平衡器端点的详细信息，请参见 有关管理 StorageGRID 的说明。

警报名称	问题描述 和建议的操作
管理接口的服务器证书到期	用于管理接口的服务器证书即将过期。 1. 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。 3. 上传新的管理接口证书。
S3 和 Swift API 的全局服务器证书到期	用于访问存储 API 端点的服务器证书即将过期。 1. 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。 3. 上传新的 S3 和 Swift API 证书。
外部系统日志 CA 证书到期	用于签署外部系统日志服务器证书的证书颁发机构（ CA ）证书即将过期。 1. 更新外部系统日志服务器上的 CA 证书。 2. 获取更新后的 CA 证书的副本。 3. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 4. 选择 * 编辑外部系统日志服务器 * 。 5. 选择 * 浏览 * 以上传新证书。 6. 完成配置向导以保存新证书和密钥。
外部系统日志客户端证书到期	外部系统日志服务器的客户端证书即将过期。 1. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 2. 选择 * 编辑外部系统日志服务器 * 。 3. 选择 * 浏览 * 以上传新证书。 4. 选择 * 浏览 * 以上传新的私钥。 5. 完成配置向导以保存新证书和密钥。
外部系统日志服务器证书到期	外部系统日志服务器提供的服务器证书即将过期。 1. 更新外部系统日志服务器上的服务器证书。 2. 如果您之前使用网格管理器 API 提供用于证书验证的服务器证书，请使用 API 上传更新后的服务器证书。

警报名称	问题描述 和建议的操作
外部系统日志服务器转发错误	节点无法将日志转发到外部系统日志服务器。 1. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 2. 选择 * 编辑外部系统日志服务器 * 。 3. 继续执行配置向导，直到您能够选择 * 发送测试消息 * 。 4. 选择 * 发送测试消息 * 以确定无法将日志转发到外部系统日志服务器的原因。 5. 解决报告的任何问题。
网格网络 MTU 不匹配	网格网络接口（ eth0 ）的最大传输单元（ MTU ）设置在网格中的各个节点之间差别很大。 MTU 设置的差异可能表明，某些（但并非所有） eth0 网络配置了巨型帧。如果 MTU 大小不匹配大于 1000 ，则可能会出现发生原因 网络性能问题。 请参见中有关网格网络 MTU 不匹配警报的说明 对网络，硬件和平台问题进行故障排除。
Java 堆使用率较高	正在使用的 Java 堆空间百分比很高。 如果 Java 堆已满，则元数据服务可能不可用，客户端请求可能会失败。 1. 查看信息板上的 ILM 活动。当 ILM 工作负载减少时，此警报可能会自行解决。 2. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 3. 如果此警报仍然存在，请联系技术支持。
元数据查询延迟较长	Cassandra 元数据查询的平均时间过长。 查询延迟增加的原因可能包括硬件更改，例如更换磁盘，工作负载更改（例如载入量突然增加）或网络更改（例如节点和站点之间的通信问题）。 1. 确定查询延迟增加前后是否发生任何硬件，工作负载或网络更改。 2. 如果无法解决此问题，请联系技术支持。

警报名称	问题描述 和建议的操作
身份联合同步失败	无法从身份源同步联合组和用户。 1. 确认已配置的 LDAP 服务器已联机且可用。 2. 查看身份联合页面上的设置。确认所有值均为最新值。请参见 使用身份联合 在管理 StorageGRID 的说明中。 3. 单击 * 测试连接 * 以验证 LDAP 服务器的设置。 4. 如果无法解决此问题描述 ，请联系技术支持。
租户的身份联合同步失败	无法从租户配置的身份源同步联合组和用户。 1. 登录到租户管理器。 2. 确认租户配置的 LDAP 服务器已联机且可用。 3. 查看身份联合页面上的设置。确认所有值均为最新值。请参见 使用身份联合 在使用租户帐户的说明中。 4. 单击 * 测试连接 * 以验证 LDAP 服务器的设置。 5. 如果无法解决此问题描述 ，请联系技术支持。
无法实现 ILM 放置	无法为某些对象实现 ILM 规则中的放置指令。 此警报表示放置指令所需的节点不可用或 ILM 规则配置不当。例如，规则可能指定的复制副本数可能多于存储节点数。 1. 确保所有节点均已联机。 2. 如果所有节点均处于联机状态，请查看使用活动 ILM 策略的所有 ILM 规则中的放置说明。确认所有对象都有有效的说明。请参见 有关通过信息生命周期管理来管理对象的说明。 3. 根据需要更新规则设置并激活新策略。 ◦ 注意： * 清除警报可能需要长达 1 天的时间。 4. 如果问题仍然存在，请联系技术支持。 ◦ 注意： * 此警报可能会在升级期间出现，并且可能会在升级成功完成后持续 1 天。当此警报由升级触发时，它将自行清除。

警报名称	问题描述 和建议的操作
ILM 扫描周期过长	扫描，评估对象和应用 ILM 所需的时间过长。 如果完成对所有对象的完整 ILM 扫描的估计时间过长（请参见信息板上的 * 扫描时间段 - 估计值 * ），则活动 ILM 策略可能不会应用于新载入的对象。对 ILM 策略所做的更改可能不会应用于现有对象。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 确认所有存储节点均已联机。 3. 临时减少客户端流量。例如，在网格管理器中，选择 * 配置 * > * 网络 * > * 流量分类 * ，然后创建一个限制带宽或请求数量的策略。 4. 如果磁盘 I/O 或 CPU 过载，请尝试减少负载或增加资源。 5. 如有必要，请更新 ILM 规则以使用同步放置（对于在 StorageGRID 11.3 之后创建的规则，默认设置）。 6. 如果此警报仍然存在，请联系技术支持。 管理 StorageGRID
ILM 扫描速率低	ILM 扫描速率设置为每秒不到 100 个对象。 此警报表示有人已将系统的 ILM 扫描速率更改为每秒不到 100 个对象（默认值： 400 个对象 / 秒）。活动 ILM 策略可能不会应用于新载入的对象。此后对 ILM 策略所做的更改不会应用于现有对象。 1. 在持续支持调查中，确定是否临时更改了 ILM 扫描速率。 2. 请联系技术支持。 请勿在未联系技术支持的情况下更改 ILM 扫描速率。
Kms CA 证书到期	用于对密钥管理服务器（ KMS ）证书进行签名的证书颁发机构（ CA ）证书即将过期。 1. 使用 KMS 软件更新密钥管理服务器的 CA 证书。 2. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 3. 选择证书状态警告的 KMS 。 4. 选择 * 编辑 * 。 5. 选择 * 下一步 * 转到步骤 2 （上传服务器证书）。 6. 选择 * 浏览 * 以上传新证书。 7. 选择 * 保存 * 。 管理 StorageGRID

警报名称	问题描述 和建议的操作
Kms 客户端证书到期	密钥管理服务器的客户端证书即将过期。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 2. 选择证书状态警告的 KMS 。 3. 选择 * 编辑 * 。 4. 选择 * 下一步 * 转到步骤 3 （上传客户端证书）。 5. 选择 * 浏览 * 以上传新证书。 6. 选择 * 浏览 * 以上传新的私钥。 7. 选择 * 保存 * 。 管理 StorageGRID
无法加载 Kms 配置	密钥管理服务器的配置存在，但无法加载。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 如果此警报仍然存在，请联系技术支持。
Kms 连接错误	设备节点无法连接到其站点的密钥管理服务器。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 2. 确认端口和主机名条目正确无误。 3. 确认服务器证书，客户端证书和客户端证书专用密钥正确且未过期。 4. 确保防火墙设置允许设备节点与指定的 KMS 进行通信。 5. 更正任何网络或 DNS 问题。 6. 如果您需要帮助或此警报持续存在，请联系技术支持。
未找到 Kms 加密密钥名称	配置的密钥管理服务器没有与提供的名称匹配的加密密钥。 1. 确认分配给站点的 KMS 使用的加密密钥名称以及任何先前版本正确无误。 2. 如果您需要帮助或此警报持续存在，请联系技术支持。
Kms 加密密钥轮换失败	所有设备卷均已解密，但一个或多个卷无法轮换到最新密钥。请联系技术支持。

警报名称	问题描述 和建议的操作
未配置公里	此站点不存在密钥管理服务器。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 2. 为此站点添加 KMS 或添加默认 KMS 。 管理 StorageGRID
Kms 密钥无法对设备卷进行解密	无法使用当前 KMS 密钥对启用了节点加密的设备上的一个或多个卷进行解密。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 确保密钥管理服务器（ KMS ）已配置加密密钥以及任何先前的密钥版本。 3. 如果您需要帮助或此警报持续存在，请联系技术支持。
Kms 服务器证书到期	密钥管理服务器（ KMS ）使用的服务器证书即将过期。 1. 使用 KMS 软件更新密钥管理服务器的服务器证书。 2. 如果您需要帮助或此警报持续存在，请联系技术支持。 管理 StorageGRID
审核队列较大	审核消息的磁盘队列已满。 1. 检查系统上的负载—如果事务数量很多，则警报应逐渐自行解决，您可以忽略此警报。 2. 如果警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。 3. 通过将客户端写入和客户端读取的审核级别更改为 " 错误 " 或 " 关闭 "（ * 配置 * > * 监控 * > * 审核和系统日志服务器 * ），降低客户端操作速率或减少记录的审核消息数量。 查看审核日志

警报名称	问题描述 和建议的操作
检测到原有 CLB 负载平衡器活动	某些客户端可能正在使用默认 S3 和 Swift API 证书连接到已弃用的 CLB 负载平衡器服务。 1. 要简化未来升级，请在 * 证书 * 页面的 * 全局 * 选项卡上安装自定义 S3 和 Swift API 证书。然后，确保连接到原有 CLB 的所有 S3 或 Swift 客户端都具有新证书。 2. 创建一个或多个负载平衡器端点。然后，将所有现有 S3 和 Swift 客户端定向到这些端点。如果需要重新映射客户端端口，请联系技术支持。 其他活动可能会触发此警报，包括端口扫描。要确定当前是否正在使用已弃用的 CLB 服务，请查看 `storagegRid_private_clb_http_connection_established_successful` Prometheus 指标。 如果不再使用 CLB 服务，请根据需要静默或禁用此警报规则。
正在将日志添加到磁盘队列中	节点无法将日志转发到外部系统日志服务器，并且磁盘队列正在填满。 1. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 2. 选择 * 编辑外部系统日志服务器 * 。 3. 继续执行配置向导，直到您能够选择 * 发送测试消息 * 。 4. 选择 * 发送测试消息 * 以确定无法将日志转发到外部系统日志服务器的原因。 5. 解决报告的任何问题。
审核日志磁盘容量低	可用于审核日志的空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
可用节点内存不足	节点上的可用 RAM 量较低。 可用 RAM 不足可能表示工作负载发生变化或一个或多个节点发生内存泄漏。 1. 监控此警报以查看问题描述 是否自行解决。 2. 如果可用内存低于主要警报阈值，请联系技术支持。

警报名称	问题描述 和建议的操作
存储池可用空间不足	可用于在存储池中存储对象数据的空间量较低。 1. 选择 * ILM * > * 存储池 * 。 2. 选择警报中列出的存储池，然后选择 * 查看详细信息 * 。 3. 确定需要额外存储容量的位置。您可以向存储池中的每个站点添加存储节点，也可以向一个或多个现有存储节点添加存储卷（ LUN ）。 4. 执行扩展操作步骤 以增加存储容量。 扩展网格
节点内存不足	节点上安装的内存量不足。 增加虚拟机或 Linux 主机可用的 RAM 量。检查主要警报的阈值，以确定 StorageGRID 节点的默认最低要求。请参见适用于您的平台的安装说明： • 安装 Red Hat Enterprise Linux 或 CentOS • 安装 Ubuntu 或 Debian • 安装 VMware
元数据存储不足	可用于存储对象元数据的空间不足。 • 严重警报 * 1. 停止载入对象。 2. 立即在扩展操作步骤 中添加存储节点。 • 主要警报 * 立即在扩展操作步骤 中添加存储节点。 • 次要警报 * 1. 监控对象元数据空间的使用速率。选择 * 节点 * > * 存储节点 _* > * 存储 * ，然后查看已用存储 - 对象元数据图。 2. 在中添加存储节点 扩展操作步骤 请尽快。 添加新存储节点后，系统会自动在所有存储节点之间重新平衡对象元数据，并清除警报。 请参见中有关 " 低元数据存储 " 警报的说明 对元数据问题进行故障排除。
低指标磁盘容量	可用于指标数据库的空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。

警报名称	问题描述 和建议的操作
对象数据存储不足	可用于存储对象数据的空间不足。 执行扩展操作步骤 。您可以向现有存储节点添加存储卷（ LUN ），也可以添加新的存储节点。 对对象数据存储不足警报进行故障排除 扩展网格
低只读水印覆盖	存储卷软只读水印覆盖小于存储节点的最小优化水印。 要了解如何解决此警报，请转至 对低只读水印覆盖警报进行故障排除。
根磁盘容量低	根磁盘的可用空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
系统数据容量低	在 ` /var/local` 文件系统上可用于 StorageGRID 系统数据的空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
tmp 目录可用空间不足	/tmp 目录中的可用空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
节点网络连接错误	在节点之间传输数据时出错。 网络连接错误可能会在无需手动干预的情况下清除。如果错误无法清除，请联系技术支持。 请参见中的网络接收错误（ NRER ）警报说明 对网络，硬件和平台问题进行故障排除。
节点网络接收帧错误	节点收到的网络帧中有很高比例出现错误。 此警报可能指示硬件问题描述 ，例如以太网连接任一端的缆线损坏或收发器出现故障。 1. 如果您使用的是设备，请尝试更换每个 SFP+ 或 SFP28 收发器和缆线，一次更换一个，以查看警报是否清除。 2. 如果此警报仍然存在，请联系技术支持。

警报名称	问题描述 和建议的操作
节点与 NTP 服务器不同步	节点的时间与网络时间协议（ NTP ）服务器不同步。 1. 验证您是否已指定至少四个外部 NTP 服务器，每个服务器均提供 Stratum 3 或更好的参考。 2. 检查所有 NTP 服务器是否均正常运行。 3. 验证与 NTP 服务器的连接。确保它们未被防火墙阻止。
节点未使用 NTP 服务器锁定	节点未锁定到网络时间协议（ NTP ）服务器。 1. 验证您是否已指定至少四个外部 NTP 服务器，每个服务器均提供 Stratum 3 或更好的参考。 2. 检查所有 NTP 服务器是否均正常运行。 3. 验证与 NTP 服务器的连接。确保它们未被防火墙阻止。
非设备节点网络已关闭	一个或多个网络设备已关闭或断开连接。此警报表示无法访问虚拟机或 Linux 主机上安装的节点的网络接口（ eth ）。 请联系技术支持。
对象存在检查失败	对象存在检查作业失败。 1. 选择 * 维护 > 对象存在检查 * 。 2. 记下错误消息。执行相应的更正操作： ◦ 无法启动 * ， * 连接断开 * ， * 未知错误 * a. 确保作业中包含的存储节点和卷处于联机状态且可用。 b. 确保存储节点上没有服务或卷故障。如果某个服务未运行，请启动或重新启动该服务。请参见 恢复和维护说明。 c. 确保可以满足选定的一致性控制。 d. 解决任何问题后，选择 * 重试 * 。作业将从最后一个有效状态恢复。 卷中的 * 严重存储错误 * a. 恢复故障卷。请参见 恢复和维护说明。 b. 选择 * 重试 * 。 c. 作业完成后，为节点上的其余卷创建另一个作业，以检查是否存在其他错误。 3. 如果无法解决这些问题，请联系技术支持。

警报名称	问题描述 和建议的操作
对象存在检查已停止	对象存在检查作业已停止。 对象存在检查作业无法继续。作业中包含的一个或多个存储节点或卷脱机或无响应，或者由于节点过多或不可用，无法再满足选定一致性控制。 1. 确保所有要检查的存储节点和卷均处于联机状态且可用（选择 * 节点 * ）。 2. 确保有足够的存储节点处于联机状态且可用，以使当前协调者节点能够使用选定一致性控制读取对象元数据。如有必要，启动或重新启动服务。请参见 恢复和维护说明。 解决步骤 1 和 2 后，作业将自动从停止位置开始。 3. 如果无法满足选定的一致性控制，请取消作业并使用较低的一致性控制启动另一个作业。 4. 如果无法解决这些问题，请联系技术支持。
对象丢失	一个或多个对象已从网格中丢失。 此警报可能指示数据已永久丢失，无法检索。 1. 立即调查此警报。您可能需要采取措施以防止进一步数据丢失。如果您立即采取措施，则还可以还原丢失的对象。 对丢失和丢失的对象数据进行故障排除 2. 解决底层问题后，重置计数器： a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 b. 对于发出警报的存储节点，请选择 * ； site_* > * ； grid node_* > * LDR* > * 数据存储 * > * 配置 * > * 主 * 。 c. 选择 * 重置丢失的对象计数 * ，然后单击 * 应用更改 * 。
平台服务不可用	具有 RSM 服务的存储节点在站点上运行或可用的数量太少。 确保受影响站点上拥有 RSM 服务的大多数存储节点均处于运行状态且无错误状态。 请参见中的 "`解决平台服务问题` " 有关管理 StorageGRID 的说明。

警报名称	问题描述 和建议的操作
S3 PUT 对象大小太大	S3 客户端正在尝试执行超过 S3 大小限制的 PUT 对象操作。 1. 使用警报详细信息中显示的租户 ID 来标识租户帐户。 2. 转至 * 支持 * > * 工具 * > * 日志 * ，然后收集警报详细信息中显示的存储节点的应用程序日志。指定警报时间前后 15 分钟的时间段。 3. 提取下载的归档，然后导航到 `byncast.log` 的位置（` /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/byncast.log` ）。 4. 在 `byncast.log` 的内容中搜索 ` "method =pt"` ，并通过查看 `clientIP` 字段确定 S3 客户端的 IP 地址。 5. 通知所有客户端用户， PUT 对象大小上限为 5 GiB 。 6. 对大于 5 GiB 的对象使用多部分上传。
管理网络端口 1 上的服务设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。 1. 检查连接到管理网络端口 1 的缆线和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG100 和 SG1000 服务设备 ◦ 禁用警报规则
管理网络（或客户端网络）上的服务设备链接已关闭	管理网络（ eth1 ）或客户端网络（ eth2 ）的设备接口已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG100 和 SG1000 服务设备 ◦ 禁用警报规则

警报名称	问题描述 和建议的操作
网络端口 1 ， 2 ， 3 或 4 上的服务设备链路已关闭	设备上的网络端口 1 ， 2 ， 3 或 4 已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG100 和 SG1000 服务设备 ◦ 禁用警报规则
服务设备存储连接已降级	服务设备中的两个 SSD 之一出现故障或与另一个 SSD 不同步。 设备功能不受影响，但您应立即解决问题描述 。如果两个驱动器都发生故障，则设备将无法再正常运行。 1. 在网格管理器中，选择 * 节点 * > ***services appliage*** ，然后选择 " 硬件 " 选项卡。 2. 查看 * 存储 RAID 模式 * 字段中的消息。 3. 如果此消息显示重新同步操作的进度，请等待此操作完成，然后确认警报已解决。重新同步消息表示 SSD 最近已更换，或者由于其他原因正在重新同步。 4. 如果此消息指示其中一个 SSD 发生故障，请尽快更换发生故障的驱动器。 有关如何更换服务设备中的驱动器的说明，请参见 SG100 和 SG1000 设备安装和维护指南。 SG100 和 SG1000 服务设备
管理网络端口 1 上的存储设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。 1. 检查连接到管理网络端口 1 的缆线和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ 禁用警报规则

警报名称	问题描述 和建议的操作
管理网络（或客户端网络）上的存储设备链接已关闭	管理网络（ eth1 ）或客户端网络（ eth2 ）的设备接口已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ 禁用警报规则
网络端口 1 ， 2 ， 3 或 4 上的存储设备链路已关闭	设备上的网络端口 1 ， 2 ， 3 或 4 已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ 禁用警报规则
存储设备存储连接已降级	计算控制器和存储控制器之间的一个或多个连接出现问题。 1. 转至设备以检查端口指示灯。 2. 如果端口指示灯不亮，请确认缆线已正确连接。根据需要更换缆线。 3. 最多等待五分钟。 ◦ 注： * 如果需要更换另一根缆线，请至少拔下 5 分钟。否则，根卷可能会变为只读，这需要重新启动硬件。 4. 在网格管理器中，选择 * 节点 * 。然后，选择出现问题的节点的硬件选项卡。验证警报条件是否已解决。

警报名称	问题描述 和建议的操作
无法访问存储设备	无法访问存储设备。 此警报表示由于底层存储设备出现问题，无法挂载或访问卷。 1. 检查用于此节点的所有存储设备的状态： ◦ 如果节点安装在虚拟机或 Linux 主机上，请按照您的操作系统的说明运行硬件诊断或执行文件系统检查。 ▪ 安装 Red Hat Enterprise Linux 或 CentOS ▪ 安装 Ubuntu 或 Debian ▪ 安装 VMware ◦ 如果节点安装在 SG100 ， SG1000 或 SG6000 设备上，请使用 BMC 。 ◦ 如果此节点安装在 SG5600 或 SG5700 设备上，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
租户配额使用量高	正在使用的租户配额空间百分比很高。如果租户超过其配额，则新的载入将被拒绝。 • 注： * 默认情况下，此警报规则处于禁用状态，因为它可能会生成大量通知。 1. 在网格管理器中，选择 * 租户 * 。 2. 按 * 配额利用率 * 对表进行排序。 3. 选择配额利用率接近 100% 的租户。 4. 执行以下操作之一或同时执行这两项操作： ▪ 选择 * 编辑 * 以增加租户的存储配额。 ▪ 通知租户其配额利用率较高。

警报名称	问题描述 和建议的操作
无法与节点通信	一个或多个服务无响应，或者无法访问节点。 此警报表示节点已因未知原因断开连接。例如，节点上的服务可能已停止，或者节点可能已因电源故障或意外中断而丢失网络连接。 监控此警报以查看问题描述 是否自行解决。如果问题描述 仍然存在： 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 确认此节点上的所有服务均已运行。如果某个服务已停止，请尝试启动它。请参见 恢复和维护说明。 3. 确保节点的主机已启动。如果不是，请启动主机。 ◦ 注： * 如果关闭了多个主机，请参见 恢复和维护说明。 4. 确定此节点与管理节点之间是否存在网络连接问题描述 。 5. 如果无法解决此警报，请联系技术支持。
节点意外重新启动	节点在过去 24 小时内意外重新启动。 1. 监控此警报。此警报将在 24 小时后清除。但是，如果节点再次意外重新启动，则会再次触发此警报。 2. 如果无法解决此警报，则可能存在硬件故障。请联系技术支持。
检测到未标识的损坏对象	在复制的对象存储中找到无法标识为复制对象的文件。 1. 确定存储节点上的底层存储是否存在任何问题。例如，运行硬件诊断或执行文件系统检查。 2. 解决任何存储问题后， 运行对象存在检查 确定是否缺少 ILM 策略定义的任何复制副本。 3. 监控此警报。此警报将在 24 小时后清除，但如果问题描述 未修复，则会再次触发。 4. 如果无法解决此警报，请联系技术支持。

常用的 **Prometheus** 指标

管理节点上的 Prometheus 服务从所有节点上的服务收集时间序列指标。虽然 Prometheus 收集的指标超过 1000 个，但监控最关键的 StorageGRID 操作需要的指标相对较少。

指标会存储在每个管理节点上，直到为 Prometheus 数据预留的空间已满为止。当 ` /var/local/mysql_ibdata/` 卷达到容量时，首先删除最旧的指标。

要获取完整的指标列表，请使用网格管理 API 。

1. 从网格管理器的顶部，选择帮助图标并选择 * API Documentation" 。

2. 找到 * 指标 * 操作。
3. 执行 `GET /grid/metric-names` 操作。
4. 下载结果。

下表列出了最常用的 Prometheus 指标。您可以参考此列表来更好地了解默认警报规则中的条件，或者为自定义警报规则构建条件。

> 名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间可能会发生更改，恕不另行通知。

Prometheus 指标	**Description**
alertmanager_notifications _failed_total	失败警报通知的总数。
node_filesystem_avail_bytes	非 root 用户可用的文件系统空间量（以字节为单位）。
node_memory_MemAvailable_bytes	内存信息字段 MemAvailable_bytes 。
node_network_Carrier	/sys/class/net/<iface> 的托架值。
node_network_receive ； errs_total	网络设备统计信息 Receive _errs 。
node_network_transmit_errs_total	网络设备统计信息 transmit_errs 。
storaggrid_administratively 关闭	由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。
storagegrid_appliage_compute_controller_hardware_status	设备中计算控制器硬件的状态。
storagegrid_appliation_failed_disks	对于设备中的存储控制器，是指不是最佳的驱动器数量。
storagegrid_appliage_storage_controller_hardware_status	设备中存储控制器硬件的整体状态。
storagegrid_content_bages_and_containers	此存储节点已知的 S3 存储分段和 Swift 容器总数。
storaggrid_content_objects	此存储节点已知的 S3 和 Swift 数据对象总数。计数仅适用于通过 S3 或 Swift 与系统连接的客户端应用程序创建的数据对象。

Prometheus 指标	Description
storaggrid_content_objects_lost	此服务在 StorageGRID 系统中检测到缺失的对象总数。应采取措施确定丢失的发生原因 以及是否可以恢复。 对丢失和丢失的对象数据进行故障排除
storagegRid_http_sessions_incoming_attempted	尝试访问存储节点的 HTTP 会话总数。
storaggrid_http_sessions_incoming_currently 已建立	存储节点上当前处于活动状态（已打开）的 HTTP 会话数。
storagegRid_http_sessions_incoming_failed	由于 HTTP 请求格式错误或在处理操作时失败而无法成功完成的 HTTP 会话总数。
storagegRid_http_sessions_incoming_successful	已成功完成的 HTTP 会话总数。
storaggrid_ilm_awaiting 背景对象	此节点上等待通过扫描进行 ILM 评估的对象总数。
storaggrid_ilm_awaiting 客户端评估对象每秒对象数	根据此节点上的 ILM 策略评估对象的当前速率。
storaggrid_ilm_awaiting 客户端对象	此节点上等待通过客户端操作进行 ILM 评估的对象总数（例如，载入）。
storaggrid_ilm_awaing_total_objects	等待 ILM 评估的对象总数。
storagegrid_ilm_scanne_objects_per_second	此节点拥有的对象在 ILM 中进行扫描和排队的速率。
storaggrid_ilm_scann_period_estimated_minutes	在此节点上完成完整 ILM 扫描的估计时间。 • 注： * 完全扫描并不能保证 ILM 已应用于此节点拥有的所有对象。
storagegRid_load_Balancer_endpoint_ct_expiry_time	负载平衡器端点证书自 Epoch 以来的到期时间（以秒为单位）。
storaggrid_metadata_queries_average ； latency ；毫秒	通过此服务对元数据存储运行查询所需的平均时间。
storaggrid_network_received_bytes	自安装以来接收的总数据量。
storaggrid_network_transmated_bytes	自安装以来发送的总数据量。

Prometheus 指标	Description
storagegrid_node_cpu_utilization 百分比	此服务当前正在使用的可用 CPU 时间的百分比。指示服务的繁忙程度。可用 CPU 时间量取决于服务器的 CPU 数量。
storaggrid_ntp_chosed_time_source_offset_mms	选定时间源提供的系统时间偏移。如果到达某个时间源的延迟与该时间源到达 NTP 客户端所需的时间不相等，则会引入偏移。
storaggrid_ntp_locked	节点未锁定到网络时间协议（ NTP ）服务器。
storaggrid_s3_data_transfers_bytes_ingested	自上次重置属性以来从 S3 客户端载入到此存储节点的总数据量。
已检索 storagegRid_s3_data_transfers_bytes_reRetrieved	自上次重置属性以来 S3 客户端从此存储节点检索的总数据量。
storaggrid_s3_operations_failed	S3 操作失败的总数（ HTTP 状态代码 4xx 和 5xx ），不包括因 S3 授权失败而导致的操作。
storaggrid_s3_operations_successful	成功执行 S3 操作的总数（ HTTP 状态代码 2xx ）。
storaggrid_s3_operations_unauthorized	授权失败导致的 S3 操作失败的总数。
storagegRid_servercertificate_management_interface_cert_expiry_days	管理接口证书到期前的天数。
storagegRid_servercertificate_storage_api_Endpoints " 证书到期日 "	对象存储 API 证书到期前的天数。
storaggrid_service_cpu_seconds	自安装以来此服务使用 CPU 的累积时间。
storagegrid_service_memory_usage_bytes	此服务当前正在使用的内存量（ RAM ）。此值与 Linux 顶部实用程序显示的值相同，即 Res 。
storaggrid_service_network_received_bytes	自安装以来此服务收到的总数据量。
storaggrid_service_network_transmated_bytes	此服务发送的总数据量。
storagegrid_service_Restart	重新启动服务的总次数。
storaggrid_service_runtime_seconds	自安装以来服务一直运行的总时间量。
storaggrid_service_uptime_seconds	服务自上次重新启动以来的总运行时间。

Prometheus 指标	Description
storaggrid_storage_state_current	存储服务的当前状态。属性值为： • 10 = 脱机 • 15 = 维护 • 20 = 只读 • 30 = 联机
storagegrid_storage_status	存储服务的当前状态。属性值为： • 0 = 无错误 • 10 = 正在过渡 • 20 = 可用空间不足 • 30 = 卷不可用 • 40 = 错误
storaggrid_storage_utilization字节	存储节点上复制和擦除编码的对象数据的估计总大小。
storaggrid_storage_utilization metadata_allowed_bytes	每个存储节点的卷 0 上允许用于对象元数据的总空间。此值始终小于为节点上的元数据预留的实际空间，因为必要的数据库操作（如数据缩减和修复）以及未来的硬件和软件升级都需要预留部分空间。对象元数据允许的空间控制整体对象容量。
storaggrid_storage_utilization metadata_bytes	存储卷 0 上的对象元数据量，以字节为单位。
storaggrid_storage_utilization 总空间字节	分配给所有对象存储的存储空间总量。
storagegRid_storage_utilization_usable_space_bytes	剩余的对象存储空间总量。计算方法是将存储节点上所有对象存储的可用空间量相加。
storagegrid_swif_data_transfers_bytes_ingested	自上次重置属性以来从 Swift 客户端载入到此存储节点的总数据量。
已检索 storaggrid_swif_data_transfers_bytes_reRetrieved	自上次重置属性以来 Swift 客户端从此存储节点检索的总数据量。
storaggrid_swif_operations_failed	Swift 操作失败的总数（ HTTP 状态代码 4xx 和 5xx ），不包括因 Swift 授权失败而导致的操作。
storagegrid_swif_operations_successful	成功的 Swift 操作总数（ HTTP 状态代码 2xx ）。

Prometheus 指标	Description
storaggrid_swif_operations_unauthorized	授权失败导致的 Swift 操作失败的总数（ HTTP 状态代码 401 ， 403 ， 405 ）。
storagegrid_tenant_usage_data_bytes	租户的所有对象的逻辑大小。
storagegrid_tenant_usage_object_count	租户的对象数。
storagegRid_tenant_usage_quota_bytes	可用于租户对象的最大逻辑空间量。如果未提供配额指标，则可用空间量不受限制。

警报参考（旧系统）

下表列出了所有原有的默认警报。如果触发了警报，您可以在此表中查找警报代码以查找建议的操作。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

代码	Name	服务	建议的操作
ABRL	可用属性中继	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BSSM ， BDDS	尽快恢复与运行属性中继服务的服务（一种模数转换器服务）的连接。如果没有连接的属性中继，则网格节点无法向 NMS 服务报告属性值。因此， NMS 服务无法再监控服务的状态，也无法更新服务的属性。 如果问题仍然存在，请联系技术支持。
ACMS	可用元数据服务	BARR ， BLDR ， BCMN	如果 LDR 或 ARC-Service 与 DDS 服务断开连接，则会触发警报。如果发生这种情况，则无法处理载入或检索事务。如果 DDS 服务不可用只是一个短暂的瞬时问题描述 ，则事务可能会延迟。 检查并还原与 DDS 服务的连接，以清除此警报并使此服务恢复完整功能。
行为	云分层服务状态	圆弧	仅适用于目标类型为 Cloud Tiering 的归档节点 - 简单存储服务（ S3 ）。 如果归档节点的 "Acts " 属性设置为 "Read-Only Enabled" 或 "Read-Write Disabled" ，则必须将此属性设置为 "Read-Write Enabled" 。 如果因身份验证失败而触发重大警报，请验证与目标存储分段关联的凭据，并根据需要更新值。 如果因任何其他原因触发重大警报，请联系技术支持。

代码	**Name**	服务	建议的操作
ADCA	模数转换器状态	模数转换器	如果触发警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ADC* > * 概述 * > * 主要 * 和 * ADC* > * 警报 * > * 主要 * 来确定警报的发生原因 。 如果问题仍然存在，请联系技术支持。
ADCE	模数转换器状态	模数转换器	如果 "ADC-State" 的值为 "Standby" ，请继续监控此服务，如果问题仍然存在，请联系技术支持。 如果 "ADC" 状态的值为脱机，请重新启动此服务。如果问题仍然存在，请联系技术支持。
AITE	检索状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果检索状态值正在等待目标，请检查 TSM 中间件服务器并确保其正常运行。如果刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置归档节点与目标外部归档存储系统的连接。 如果 " 归档检索状态 " 的值为 " 脱机 " ，请尝试将此状态更新为 " 联机 " 。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主要 * ，选择 * 归档检索状态 * > * 联机 * ，然后单击 * 应用更改 * 。 如果问题仍然存在，请联系技术支持。
AITU-A	检索状态	BARC-B	如果检索状态的值为目标错误，请检查目标外部归档存储系统是否存在错误。 如果归档检索状态的值为会话丢失，请检查目标外部归档存储系统以确保其联机并正常运行。检查与目标的网络连接。 如果 " 归档检索状态 " 的值为未知错误，请联系技术支持。
Alis	入站属性会话	模数转换器	如果属性中继上的入站属性会话数增长得太大，则可能表示 StorageGRID 系统已变得不平衡。在正常情况下，属性会话应均匀分布在各个模块转换服务之间。不平衡可能导致性能问题。 如果问题仍然存在，请联系技术支持。
ALOS	出站属性会话	模数转换器	此 ADE 服务具有大量属性会话，并且正在过载。如果触发此警报，请联系技术支持。

代码	Name	服务	建议的操作
Alur	无法访问的属性存储库	模数转换器	检查与 NMS 服务的网络连接，以确保此服务可以与属性存储库联系。 如果触发此警报且网络连接良好，请联系技术支持。
AMQS	已排队的审核消息	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BDDS	如果无法将审核消息立即转发到审核中继或存储库，则这些消息将存储在磁盘队列中。如果磁盘队列已满，则可能发生中断。 为了及时做出响应以防止中断，当磁盘队列中的消息数量达到以下阈值时，系统将触发 AMQS 警报： • 注意：超过 100 ， 000 条消息 • 次要：至少 500 ， 000 条消息 • 主要：至少 2 ， 000 ， 000 条消息 • 严重：至少 5 ， 000 ， 000 条消息 如果触发了 AMQS 警报，请检查系统上的负载—如果存在大量事务，则该警报应随着时间的推移自行解决。在这种情况下，您可以忽略警报。 如果警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 配置审核消息和日志目标。
AOTE	存储状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果 "Store State" 的值为 Waiting for Target" ，请检查外部归档存储系统并确保其正常运行。如果刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置归档节点与目标外部归档存储系统的连接。 如果 " 存储状态 " 的值为 " 脱机 " ，请检查 " 存储状态 " 的值。在将存储状态移回联机之前更正所有问题。
AOTU	存储状态	BARC-B	如果 "Store Status" （存储状态）的值为 "Session lost" （会话丢失），请检查外部归档存储系统是否已连接并联机。 如果 "Target Error" 的值为，请检查外部归档存储系统是否存在错误。 如果 "Store Status" 的值为 "Unknown" 错误，请联系技术支持。

代码	**Name**	服务	建议的操作
APM	存储多路径连接	SSM	如果多路径状态警报显示为 `Degraded` （选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * ），请执行以下操作： 1. 插入或更换不显示任何指示灯的缆线。 2. 等待一到五分钟。 在插入另一根缆线至少五分钟后，再拔下另一根缆线。过早拔出可能会使根卷发生原因 变为只读，这要求重新启动硬件。 3. 返回到 * SSM* > * 资源 * 页面，并验证存储硬件部分中的 `Degraded` 多路径状态是否已更改为 "`nominal` " 。
Arce	弧状态	圆弧	在所有旋转组件（复制，存储，检索，目标）启动之前，此旋转式应用程序服务的状态均为 " 备用 " 。然后过渡到联机。 如果 "ARC-State" 值未从 " 备用 " 过渡到 " 联机 " ，请检查这些组件的状态。 如果 "ARC-State" 的值为 "Offlin" ，请重新启动此服务。如果问题仍然存在，请联系技术支持。
AROQ	已排队的对象	圆弧	如果可移动存储设备由于目标外部归档存储系统出现问题而运行缓慢，或者遇到多个读取错误，则可能会触发此警报。检查外部归档存储系统是否存在错误，并确保其正常运行。 在某些情况下，此错误可能是由于数据请求率较高而导致的。监控在系统活动减少时排队的对象数量。

代码	**Name**	服务	建议的操作
ARRF	请求失败	圆弧	如果从目标外部归档存储系统检索失败，则归档节点会重试检索，因为此失败可能是由于瞬时问题描述 造成的。但是，如果对象数据已损坏或已标记为永久不可用，则检索不会失败。相反，归档节点会持续重试检索，而请求失败的值会继续增加。 此警报可能指示保存所请求数据的存储介质已损坏。检查外部归档存储系统以进一步诊断此问题。 如果确定对象数据不再位于归档中，则必须从 StorageGRID 系统中删除该对象。有关详细信息，请联系技术支持。 触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主 * ，选择 * 重置请求失败计数 * 并单击 * 应用更改 * 。
ARRV	验证失败	圆弧	要诊断并更正此问题，请联系技术支持。 触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主 * ，选择 * 重置验证失败计数 * 并单击 * 应用更改 * 。
ARVF	存储故障	圆弧	如果目标外部归档存储系统出错，可能会出现此警报。检查外部归档存储系统是否存在错误，并确保其正常运行。 触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主 * ，选择 * 重置存储故障计数 * ，然后单击 * 应用更改 * 。
ASXP	审核共享	AMS	如果审核共享的值为未知，则会触发警报。此警报可能指示管理节点的安装或配置出现问题。 如果问题仍然存在，请联系技术支持。
AUMA	AMS 状态	AMS	如果 AMS Status 的值为 DB Connectivity Error ，请重新启动网格节点。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
AUME	AMS 状态	AMS	如果 AMS State 的值为 "Standby" ，请继续监控 StorageGRID 系统。如果问题仍然存在，请联系技术支持。 如果 AMS State 的值为 Offline ，请重新启动服务。如果问题仍然存在，请联系技术支持。
AUXS	审核导出状态	AMS	如果触发警报，请更正根本问题，然后重新启动 AMS 服务。 如果问题仍然存在，请联系技术支持。
badd	存储控制器故障驱动器计数	SSM	如果 StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器，则会触发此警报。根据需要更换驱动器。
BASF	可用对象标识符	CMN	配置 StorageGRID 系统后，系统会为 CMN 服务分配固定数量的对象标识符。当 StorageGRID 系统开始用尽其对象标识符时，会触发此警报。 要分配更多标识符，请联系技术支持。
重声	标识符块分配状态	CMN	默认情况下，如果无法分配对象标识符，因为无法达到模数转换仲裁，则会触发警报。 要在 CMN 服务上分配标识符块，需要使模拟学习中心服务达到联机和连接的仲裁（ 50% + 1 ）。如果仲裁不可用，则 CMN 服务将无法分配新的标识符块，直到重新建立了模板仲裁为止。如果丢失了模块转换仲裁，通常不会对 StorageGRID 系统产生任何即时影响（客户端仍可载入和检索内容），因为大约一个月的标识符会缓存在网格中的其他位置； 但是，如果此情况持续存在，则 StorageGRID 系统将无法载入新内容。 如果触发警报，请调查丢失 ADC 仲裁的原因（例如，可能是网络或存储节点故障）并采取更正措施。 如果问题仍然存在，请联系技术支持。
BRDT	计算控制器机箱温度	SSM	如果 StorageGRID 设备中计算控制器的温度超过额定阈值，则会触发警报。 检查硬件组件和环境问题是否过热。如有必要，请更换组件。

代码	**Name**	服务	建议的操作
BTOF	Offset	BADC ， BLDR ， BNMS ， BAMS ， BCLB ， BCMN ， BARC-A	如果服务时间（秒）与操作系统时间相差很大，则会触发警报。在正常情况下，服务应自行重新同步。如果服务时间偏离操作系统时间太远，则可能会影响系统操作。确认 StorageGRID 系统的时间源正确无误。 如果问题仍然存在，请联系技术支持。
BTSE	时钟状态	BADC ， BLDR ， BNMS ， BAMS ， BCLB ， BCMN ， BARC-A	如果服务的时间与操作系统跟踪的时间不同步，则会触发警报。在正常情况下，服务应自行重新同步。如果时间偏离操作系统时间太远，则可能会影响系统操作。确认 StorageGRID 系统的时间源正确无误。 如果问题仍然存在，请联系技术支持。
CAHP	Java 堆使用量百分比	DDS	如果 Java 无法以允许有足够堆空间使系统正常运行的速率执行垃圾收集，则会触发警报。警报可能指示用户工作负载超出整个系统可用于 DDS 元数据存储的资源。检查信息板中的 ILM 活动，或者选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * DDS * > * 资源 * > * 概述 * > * 主 * 。 如果问题仍然存在，请联系技术支持。
CAIH	可用的载入目标的数量	CLB	此警报已弃用。
CAQH	可用目标的数量	CLB	当可用 LDR 服务的基本问题得到更正时，此警报将清除。确保 LDR 服务的 HTTP 组件处于联机状态并正常运行。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
CASA	数据存储状态	DDS	如果 Cassandra 元数据存储不可用，则会发出警报。 检查 Cassandra 的状态： 1. 在存储节点上，使用 Passwords.txt 文件中列出的密码以 admin 和 `su` 登录到 root 。 2. 输入： `sservice Cassandra status` 3. 如果 Cassandra 未运行，请重新启动它： `sservice Cassandra restart` 此警报还可能指示存储节点的元数据存储（ Cassandra 数据库）需要重建。 请参见中有关对服务进行故障排除的信息：状态 - Cassandra （ SVST ）警报 对元数据问题进行故障排除。 如果问题仍然存在，请联系技术支持。
案例	数据存储状态	DDS	安装或扩展期间会触发此警报，以指示新的数据存储正在加入网格。
CCE	传入会话—已建立	CLB	如果网关节点上当前有 20 ， 000 个或更多 HTTP 会话处于活动状态（已打开），则会触发此警报。如果客户端的连接太多，您可能会看到连接失败。您应减少工作负载。
CCNA	计算硬件	SSM	如果需要注意 StorageGRID 设备中计算控制器硬件的状态，则会触发此警报。

代码	Name	服务	建议的操作
CDLP	元数据已用空间（百分比）	DDS	当元数据有效空间（ Metadata Effective Space ，CEMS ）达到 70% 全满（次要警报）， 90% 全满（主要警报）和 100% 全满（严重警报）时，将触发此警报。 如果此警报达到 90% 阈值，则网格管理器的信息板上将显示一条警告。要尽快添加新的存储节点，您必须执行扩展操作步骤 。请参见 扩展网格。 如果此警报达到 100% 阈值，则必须停止载入对象并立即添加存储节点。Cassandra 需要一定的空间来执行诸如压实和修复等基本操作。如果对象元数据使用的空间超过允许的 100% ，则这些操作将受到影响。可能会出现不希望的结果。 • 注 * ： 如果无法添加存储节点，请联系技术支持。 添加新存储节点后，系统会自动在所有存储节点之间重新平衡对象元数据，并清除警报。 另请参见中有关对 " 低元数据存储 " 警报进行故障排除的信息 对元数据问题进行故障排除。
CLBA	CLB 状态	CLB	如果触发警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * CLB* > * 概述 * > * 主 * 和 * CLB* > * 警报 * > * 主 * 以确定警报的发生原因 并解决问题。 如果问题仍然存在，请联系技术支持。
CLBE	CLB 状态	CLB	如果 CLB 状态的值为 " 备用 " ，请继续监控此情况，如果问题仍然存在，请联系技术支持。 如果此状态为脱机，并且没有已知的服务器硬件问题（例如，服务器已拔出）或计划的停机，请重新启动此服务。如果问题仍然存在，请联系技术支持。
CMNA	CMN 状态	CMN	如果 CMN Status 的值为 Error ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * CMN* > * 概述 * > * 主 * 和 * CMN* > * 警报 * > * 主 * 以确定错误的发生原因 并对问题进行故障排除。 切换 CMNS 后，在主管理节点硬件刷新期间会触发警报，并且 CMN 状态值为无联机 CMN （旧的 CMN 状态值为 " 备用 " ，新的 " 联机 " ）。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
CPRC	剩余容量	NMS	如果剩余容量（可打开到 NMS 数据库的可用连接数）降至配置的警报严重性以下，则会触发警报。 如果触发了警报，请联系技术支持。
CPSA	计算控制器电源 A	SSM	如果 StorageGRID 设备的计算控制器中存在电源为 A 的问题描述 ，则会触发警报。 如有必要，请更换组件。
cPSB	计算控制器电源 B	SSM	如果 StorageGRID 设备的计算控制器中存在电源为 B 的问题描述 ，则会触发警报。 如有必要，请更换组件。
CPUT	计算控制器 CPU 温度	SSM	如果 StorageGRID 设备中计算控制器中的 CPU 温度超过额定阈值，则会触发警报。 如果存储节点是 StorageGRID 设备，则 StorageGRID 系统指示需要关注控制器。 检查硬件组件和环境问题是否存在过热情况。如有必要，请更换组件。
DNST	DNS 状态	SSM	安装完成后，将在 SSM 服务中触发 DNST 警报。配置 DNS 并将新服务器信息访问到所有网格节点后，警报将被取消。
ECCD	检测到损坏的片段	LDR	当后台验证过程检测到损坏的纠删编码片段时，将触发警报。如果检测到损坏的片段，则会尝试重建该片段。重置检测到的损坏片段，并将丢失的属性复制到零，然后对其进行监控，以查看计数是否再次增加。如果计数增加，则存储节点的底层存储可能会出现问题。除非丢失或损坏的碎片数量违反纠删代码的容错能力，否则不会认为缺少纠删编码对象数据的副本；因此，可能存在损坏的碎片，并且仍能检索对象。 如果问题仍然存在，请联系技术支持。
ECST	验证状态	LDR	此警报指示此存储节点上经过纠删编码的对象数据的后台验证过程的当前状态。 如果后台验证过程出现错误，则会触发重大警报。

代码	**Name**	服务	建议的操作
FWPN	打开文件描述符	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BSSM ， BDDS	在活动高峰期间， FWPN 可能会变大。如果在活动缓慢期间不会减少，请联系技术支持。
HSTE	HTTP 状态	BLDR	请参见建议的 HSTU 操作。
HSTU	HTTP 状态	BLDR	HSTE 和 HSTU 与所有 LDR 流量的 HTTP 协议相关，包括 S3 ， Swift 和其他内部 StorageGRID 流量。警报表示已发生以下情况之一： • HTTP 协议已手动脱机。 • 已禁用自动启动 HTTP 属性。 • LDR 服务正在关闭。 默认情况下，自动启动 HTTP 属性处于启用状态。如果更改此设置， HTTP 可能会在重新启动后保持脱机状态。 如有必要，请等待 LDR 服务重新启动。 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 存储节点 _* > * LDR* > * 配置 * 。如果 HTTP 协议处于脱机状态，请将其置于联机状态。验证是否已启用自动启动 HTTP 属性。 如果 HTTP 协议仍处于脱机状态，请联系技术支持。
HTA	自动启动 HTTP	LDR	指定是否在启动时自动启动 HTTP 服务。这是用户指定的配置选项。
IRSU	入站复制状态	BLDR ， BARR	警报指示已禁用入站复制。确认配置设置：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 复制 * > * 配置 * > * 主 * 。

代码	Name	服务	建议的操作
延迟	平均延迟	NMS	检查连接问题。 检查系统活动以确认系统活动有所增加。系统活动增加将导致属性数据活动增加。这种增加的活动将导致属性数据处理延迟。这可以是正常的系统活动，也可以是次要活动。 检查是否存在多个警报。触发的警报数量过多可能表明平均延迟时间增加。 如果问题仍然存在，请联系技术支持。
LDRE	LDR 状态	LDR	如果 LDR 状态值为 " 备用 " ，请继续监控此情况，如果问题仍然存在，请联系技术支持。 如果 LDR 状态值为脱机，请重新启动服务。如果问题仍然存在，请联系技术支持。
已丢失	对象丢失	DDS ， LDR	当 StorageGRID 系统无法从系统中的任何位置检索所请求对象的副本时触发。在触发 " 丢失（丢失的对象） " 警报之前，系统会尝试从系统中的其他位置检索并更换缺失的对象。 对象丢失表示数据丢失。只要对象的位置数降至零，并且 DDS 服务未特意清除内容以满足 ILM 策略， " 丢失对象 " 属性就会递增。 立即调查丢失（对象丢失）警报。如果问题仍然存在，请联系技术支持。 对丢失和丢失的对象数据进行故障排除
MCEP	管理接口证书到期	CMN	用于访问管理接口的证书即将过期时触发。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。 3. 上传新的管理接口证书。
分钟	电子邮件通知已排队	NMS	检查托管 NMS 服务的服务器和外部邮件服务器的网络连接。另外，请确认电子邮件服务器配置正确。 为警报配置电子邮件服务器设置（旧系统）

代码	**Name**	服务	建议的操作
分钟	电子邮件通知状态	BNMS	如果 NMS 服务无法连接到邮件服务器，则会触发一个小警报。检查托管 NMS 服务的服务器和外部邮件服务器的网络连接。另外，请确认电子邮件服务器配置正确。 为警报配置电子邮件服务器设置（旧系统）
等	NMS 接口引擎状态	BNMS	如果管理节点上用于收集和生成接口内容的 NMS 接口引擎与系统断开连接，则会触发警报。检查服务器管理器以确定服务器单个应用程序是否已关闭。
Nang	网络自动协商设置	SSM	检查网络适配器配置。此设置必须与您的网络路由器和交换机的首选项匹配。 设置不正确可能会严重影响系统性能。
NDUP	网络双工设置	SSM	检查网络适配器配置。此设置必须与您的网络路由器和交换机的首选项匹配。 设置不正确可能会严重影响系统性能。
NLNK	网络链路检测	SSM	检查端口和交换机上的网络缆线连接。 检查网络路由器，交换机和适配器配置。 重新启动服务器。 如果问题仍然存在，请联系技术支持。
NRER	接收错误	SSM	以下可能是 NRER 警报的原因： • 正向错误更正（ FEC ）不匹配 • 交换机端口和 NIC MTU 不匹配 • 链路错误率较高 • NIC 环缓冲区溢出 请参见中有关对网络接收错误（ NRER ）警报进行故障排除的信息 对网络，硬件和平台问题进行故障排除。

代码	**Name**	服务	建议的操作
NRLY	可用的审核中继	BADC ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BDDS	如果审核中继未连接到 ADC- 服务，则无法报告审核事件。它们将排队，在连接恢复之前不可供用户使用。 请尽快恢复与模数转换器服务的连接。 如果问题仍然存在，请联系技术支持。
NSCA	NMS 状态	NMS	如果 NMS Status 的值为 DB Connectivity Error ，请重新启动此服务。如果问题仍然存在，请联系技术支持。
NSCE	NMS 状态	NMS	如果 NMS 状态的值为 " 备用 " ，请继续监控，如果问题仍然存在，请联系技术支持。 如果 NMS 状况的值为脱机，请重新启动服务。如果问题仍然存在，请联系技术支持。
NSPD	速度	SSM	这可能是由于网络连接或驱动程序兼容性问题造成的。如果问题仍然存在，请联系技术支持。
NBR	可用表空间	NMS	如果触发警报，请检查数据库使用量变化的速度。突然下降（而不是随着时间的推移逐渐变化）表示出现错误情况。如果问题仍然存在，请联系技术支持。 通过调整警报阈值，您可以主动管理何时需要分配更多存储。 如果可用空间达到较低阈值（请参见警报阈值），请联系技术支持以更改数据库分配。
NTER	传输错误	SSM	可以在不手动重置的情况下清除这些错误。如果未清除，请检查网络硬件。检查适配器硬件和驱动程序是否已正确安装并配置，以便与网络路由器和交换机配合使用。 解决底层问题后，重置计数器。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 资源 * > * 配置 * > * 主 * ，选择 * 重置传输错误计数 * ，然后单击 * 应用更改 * 。
NTFQ	NTP 频率偏移	SSM	如果频率偏移超过配置的阈值，则本地时钟可能存在硬件问题。如果问题仍然存在，请联系技术支持以安排更换。
NTLK	NTP 锁定	SSM	如果 NTP 守护进程未锁定到外部时间源，请检查与指定外部时间源的网络连接，这些时间源的可用性及其稳定性。

代码	**Name**	服务	建议的操作
NTOF	NTP 时间偏移	SSM	如果时间偏移超过配置的阈值，则本地时钟的振铃器可能存在硬件问题。如果问题仍然存在，请联系技术支持以安排更换。
NTSJ	选定时间源抖动	SSM	此值表示本地服务器上的 NTP 用作参考的时间源的可靠性和稳定性。 如果触发警报，则可能表示时间源的振荡器有缺陷，或者与时间源的 WAN 链路出现问题。
Ntlu	NTP 状态	SSM	如果 "NTP Status" 的值未运行，请联系技术支持。
OPST	整体电源状态	SSM	如果 StorageGRID 设备的电源与建议的工作电压不同，则会触发警报。 检查电源 A 或 B 的状态以确定哪个电源运行异常。 如有必要，请更换电源。
OQRT	已隔离对象	LDR	在 StorageGRID 系统自动还原对象后，可以从隔离目录中删除隔离的对象。 1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 2. 选择 * 站点 * > * 存储节点 * > * LDR* > * 验证 * > * 配置 * > * 主 * 。 3. 选择 * 删除隔离的对象 * 。 4. 单击 * 应用更改 * 。 隔离的对象将被删除，计数将重置为零。
ORSU	出站复制状态	BLDR ， BARR	警报指示无法进行出站复制：存储处于无法检索对象的状态。如果手动禁用了出站复制，则会触发警报。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 复制 * > * 配置 * 。 如果 LDR 服务不可用于复制，则会触发警报。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 存储 * 。
OSLF	磁盘架状态	SSM	如果存储设备存储架中某个组件的状态为已降级，则会触发警报。存储架组件包括 IOM ，风扇，电源和驱动器抽盒。如果触发此警报，请参见设备的维护说明。

代码	**Name**	服务	建议的操作
PMEM	服务内存使用量（百分比）	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BSSM ， BDDS	可以具有大于 Y% RAM 的值，其中 Y 表示服务器正在使用的内存百分比。 低于 80% 的数字是正常的。超过 90% 被视为问题。 如果一项服务的内存使用率较高，请监控情况并进行调查。 如果问题仍然存在，请联系技术支持。
PSAS	电源 A 状态	SSM	如果 StorageGRID 设备中的电源 A 与建议的工作电压不同，则会触发警报。 如有必要，请更换电源 A
PSB	电源 B 状态	SSM	如果 StorageGRID 设备中的电源 B 与建议的工作电压不同，则会触发警报。 如有必要，请更换电源 B
RTTE	Tivoli Storage Manager 状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果 Tivoli Storage Manager State 的值为脱机，请检查 Tivoli Storage Manager 状态并解决任何问题。 使组件重新联机。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 目标 * > * 配置 * > * 主要 * ，选择 * Tivoli Storage Manager State* > * 联机 * ，然后单击 * 应用更改 * 。

代码	**Name**	服务	建议的操作
RDTU	Tivoli Storage Manager 状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果 Tivoli Storage Manager 状态的值为配置错误，并且刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置 TSM 中间件服务器。 如果 Tivoli Storage Manager Status 的值为 Connection Failure 或 Connection Failure ，请重试，请检查 TSM 中间件服务器上的网络配置以及 TSM 中间件服务器和 StorageGRID 系统之间的网络连接。 如果 Tivoli Storage Manager 状态的值为身份验证失败或身份验证失败并重新连接，则 StorageGRID 系统可以连接到 TSM 中间件服务器，但无法对连接进行身份验证。检查 TSM 中间件服务器是否配置了正确的用户，密码和权限，然后重新启动服务。 如果 Tivoli Storage Manager Status 的值为 session failure ，则表示已建立的会话已意外丢失。检查 TSM 中间件服务器与 StorageGRID 系统之间的网络连接。检查中间件服务器是否存在错误。 如果 Tivoli Storage Manager Status 的值为未知错误，请联系技术支持。
RIRF	入站复制—失败	BLDR ， BARR	入站复制—在负载较高或网络临时中断期间，可能会发生故障警报。系统活动减少后，应清除此警报。如果失败的复制计数持续增加，请查找网络问题，并验证源和目标 LDR 以及 ARR 服务是否联机且可用。 要重置计数，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 复制 * > * 配置 * > * 主 * 。选择 * 重置入站复制失败计数 * ，然后单击 * 应用更改 * 。
RIRQ	入站复制—已排队	BLDR ， BARR	在高负载或临时网络中断期间，可能会发生警报。系统活动减少后，应清除此警报。如果排队复制的数量继续增加，请查找网络问题，并验证源和目标 LDR 以及 ARR 服务是否联机且可用。
RORQ	出站复制—已排队	BLDR ， BARR	出站复制队列包含要复制的对象数据，以满足客户端请求的 ILM 规则和对象。 系统过载可能会导致警报。等待系统活动下降时警报是否清除。如果警报再次出现，请通过添加存储节点来添加容量。

代码	**Name**	服务	建议的操作
SAVP	总可用空间（百分比）	LDR	如果可用空间达到较低阈值，则可选择扩展 StorageGRID 系统或通过归档节点将对象数据移动到归档。
SCA	Status	CMN	如果活动网格任务的状态值为错误，请查找网格任务消息。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * CMN* > * 网格任务 * > * 概述 * > * 主 * 。网格任务消息会显示有关此错误的信息（例如， "`check failed on node 12130011` " ）。 调查并更正问题后，重新启动网格任务。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * CMN* > * 网格任务 * > * 配置 * > * 主 * ，然后选择 * 操作 * > * 运行 * 。 如果要中止的网格任务的状态值为错误，请重试中止网格任务。 如果问题仍然存在，请联系技术支持。
SCEP	存储 API 服务端点证书过期	CMN	用于访问存储 API 端点的证书即将过期时触发。 1. 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。 3. 上传新的 S3 和 Swift API 证书。
SCHR	Status	CMN	如果历史网格任务的状态值已中止，请调查原因并在需要时再次运行此任务。 如果问题仍然存在，请联系技术支持。
SCSA	存储控制器 A	SSM	如果 StorageGRID 设备中存在存储控制器 A 的问题描述 ，则会触发警报。 如有必要，请更换组件。
SCSB	存储控制器 B	SSM	如果 StorageGRID 设备中存在存储控制器 B 的问题描述 ，则会触发警报。 如有必要，请更换组件。 某些设备型号没有存储控制器 B

代码	**Name**	服务	建议的操作
SHLH	运行状况	LDR	如果对象存储的 " 运行状况 " 值为 " 错误 " ，请检查并更正： • 正在挂载的卷出现问题 • 文件系统错误
SLSA	CPU 负载平均值	SSM	值越高，系统就越繁忙。 如果 CPU 负载平均值保持在较高的值，则应调查系统中的事务数，以确定这是否是由于当时的负载过重所致。查看 CPU 负载平均值图表：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 资源 * > * 报告 * > * 图表 * 。 如果系统上的负载不大，但问题仍然存在，请联系技术支持。
SMST	日志监控状态	SSM	如果日志监控状态值在一段时间内未连接，请联系技术支持。
SMTT	事件总数	SSM	如果总事件的值大于零，请检查是否存在已知事件（例如网络故障），这些事件可以是发生原因 。除非清除了这些错误（即，计数已重置为 0 ），否则可以触发事件总数警报。 解决问题描述 后，重置计数器以清除警报。选择 * 节点 * > * 站点 _* > * 网格节点 _* > * 事件 * > * 重置事件计数 * 。 要重置事件计数，您必须具有网格拓扑页面配置权限。 如果事件总数值为零，或者数量增加且问题仍然存在，请联系技术支持。
SNST	Status	CMN	警报表示存储网格任务包时出现问题。如果 " 状态 " 值为 " 检查点错误 " 或 " 未达到仲裁 " ，请确认大多数的 StorageGRID 服务已连接到系统（ 50% 加 1 ），然后等待几分钟。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
SOSS	存储操作系统状态	SSM	如果 SANtricity 软件指示 StorageGRID 设备中存在组件 "`Needs Attention` " 问题描述 ，则会触发警报。 选择 * 节点 * 。然后选择 * 设备存储节点 * > * 硬件 * 。向下滚动以查看每个组件的状态。在 SANtricity 软件中，检查其他设备组件以隔离问题描述 。
SSMA	SSM 状态	SSM	如果 SSM Status 的值为 Error ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 概述 * 和 * SSM* > * 概述 * > * 警报 * 以确定警报的发生原因 。 如果问题仍然存在，请联系技术支持。
SSME	SSM 状态	SSM	如果 "SSM State" 的值为 "Standby" ，请继续监控，如果问题仍然存在，请联系技术支持。 如果 "SSM State" 的值为 "Offlin" ，请重新启动此服务。如果问题仍然存在，请联系技术支持。
SST	存储状态	BLDR	如果 "Storage Status" 的值为 "Ininsufficient Available Space" ，则此存储节点上没有更多可用存储，并且数据载入将重定向到其他可用存储节点。可以继续从此网格节点传送检索请求。 应添加更多存储。它不会影响最终用户的功能，但警报会持续存在，直到添加更多存储为止。 如果 "Storage Status" （存储状态）的值为 "Volume Unavailage" （卷不可用），则表示部分存储不可用。无法从这些卷进行存储和检索。有关详细信息，请检查卷的运行状况：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 存储 * > * 概述 * > * 主 * 。卷的运行状况列在对象存储下。 如果 "Storage Status" 的值为 "Error" ，请联系技术支持。 对存储状态（ SSTS ）警报进行故障排除

代码	**Name**	服务	建议的操作
SVST	Status	SSM	解决与未运行的服务相关的其他警报后，此警报将清除。跟踪源服务警报以还原操作。 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 服务 * > * 概述 * > * 主 * 。如果某个服务的状态显示为未运行，则其状态为 administratively down 。此服务的状态可能会列为未运行，原因如下： • 已手动停止此服务（` /etc/init.d/<service\> stop` ）。 • 有一个包含 MySQL 数据库的问题描述 ，并且 Server Manager 会关闭 MI 服务。 • 已添加网格节点，但尚未启动。 • 在安装期间，网格节点尚未连接到管理节点。 如果某个服务列为未运行，请重新启动此服务（` /etc/init.d/<service\> restart` ）。 此警报还可能指示存储节点的元数据存储（ Cassandra 数据库）需要重建。 如果问题仍然存在，请联系技术支持。 对服务进行故障排除：状态 - Cassandra （ SVST ）警报进行故障排除
TMEM	已安装内存	SSM	如果节点运行的已安装内存小于 24 GiB ，则可能会导致性能问题和系统不稳定。系统上安装的内存量应至少增加到 24 GiB 。
TPOP	待定操作	模数转换器	消息队列可以指示此 ADA 服务过载。可以连接到 StorageGRID 系统的 ADC 服务太少。在大型部署中，可能需要添加计算资源，或者系统可能需要更多的模数转换服务。
UMEM	可用内存	SSM	如果可用 RAM 较低，请确定这是硬件问题描述 还是软件。如果不是硬件问题描述 ，或者可用内存降至 50 MB 以下（默认警报阈值），请联系技术支持。
VMFI	条目可用	SSM	这表示需要额外存储。请联系技术支持。
VMFR	可用空间	SSM	如果可用空间值过低（请参见警报阈值），则需要调查是否存在超出比例的日志文件，或者对象占用的磁盘空间过多（请参见警报阈值）需要减少或删除。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
VMST	Status	SSM	如果挂载的卷的状态值为未知，则会触发警报。如果值为未知或脱机，则表示由于底层存储设备出现问题，无法挂载或访问此卷。
VPRI.	验证优先级	BLDR ， BARR	默认情况下，验证优先级的值为自适应。如果验证优先级设置为高，则会触发警报，因为存储验证可能会减慢服务的正常运行速度。
VSTU	对象验证状态	BLDR	选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 存储 * > * 概述 * > * 主 * 。 检查操作系统是否存在任何块设备或文件系统错误的迹象。 如果对象验证状态的值为未知错误，则通常表示文件系统或硬件问题（ I/O 错误）级别较低，从而使存储验证任务无法访问存储的内容。请联系技术支持。
XAMS	无法访问审核存储库	BADC ， BARC ， BCLB ， BCMN ， BLDR ， BNMS	检查与托管管理节点的服务器的网络连接。 如果问题仍然存在，请联系技术支持。

生成 **SNMP** 通知的警报（旧系统）

下表列出了生成 SNMP 通知的原有警报。与警报不同，并非所有警报都会生成 SNMP 通知。只有列出的警报才会生成 SNMP 通知，并且严重性仅为指示值或更高。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

代码	**Name**	**severity**
ACMS	可用元数据服务	严重
AITE	检索状态	次要
AITU-A	检索状态	major
AMQS	已排队的审核消息	通知
AOTE	存储状态	次要
AOTU	存储状态	major

代码	Name	severity
AROQ	已排队的对象	次要
ARRF	请求失败	major
ARRV	验证失败	major
ARVF	存储故障	major
ASXP	审核共享	次要
AUMA	AMS 状态	次要
AUXS	审核导出状态	次要
BTOF	Offset	通知
CAHP	Java 堆使用量百分比	major
CAQH	可用目标的数量	通知
CASA	数据存储状态	major
CDLP	元数据已用空间（百分比）	major
CLBE	CLB 状态	严重
DNST	DNS 状态	严重
ECST	验证状态	major
HSTE	HTTP 状态	major
HTA	自动启动 HTTP	通知
已丢失	对象丢失	major
分钟	电子邮件通知已排队	通知
分钟	电子邮件通知状态	次要
Nang	网络自动协商设置	通知

代码	Name	severity
NDUP	网络双工设置	次要
NLNK	网络链路检测	次要
NRER	接收错误	通知
NSPD	速度	通知
NTER	传输错误	通知
NTFQ	NTP 频率偏移	次要
NTLK	NTP 锁定	次要
NTOF	NTP 时间偏移	次要
NTSJ	选定时间源抖动	次要
Ntlu	NTP 状态	major
OPST	整体电源状态	major
ORSU	出站复制状态	通知
PSAS	电源 A 状态	major
PSB	电源 B 状态	major
RTTE	Tivoli Storage Manager 状态	通知
RDTU	Tivoli Storage Manager 状态	major
SAVP	总可用空间（百分比）	通知
SHLH	运行状况	通知
SLSA	CPU 负载平均值	通知
SMTT	事件总数	通知
SNST	Status	

代码	Name	severity
SOSS	存储操作系统状态	通知
SST	存储状态	通知
SVST	Status	通知
TMEM	已安装内存	次要
UMEM	可用内存	次要
VMST	Status	次要
VPRI.	验证优先级	通知
VSTU	对象验证状态	通知

日志文件参考

StorageGRID 提供了用于捕获事件，诊断消息和错误情况的日志。系统可能会要求您收集日志文件并将其转发给技术支持以协助进行故障排除。

这些日志分为以下几类：

- StorageGRID 软件日志
- 部署和维护日志
- 第三方软件的日志
- 关于 bycast.log

> 为每种日志类型提供的详细信息仅供参考。这些日志可供技术支持进行高级故障排除。使用审核日志和应用程序日志文件重建问题历史记录的高级技术不在本说明的范围之内。

要访问日志，您可以将日志文件和系统数据作为一个日志文件归档（ * 支持 * > * 工具 * > * 日志 * ）从一个或多个节点收集。或者，如果主管理节点不可用或无法访问特定节点，您可以按如下所示访问每个网格节点的各个日志文件：

1. 输入以下命令： `ssh admin@grid_node_ip`
2. 输入 `passwords.txt` 文件中列出的密码。
3. 输入以下命令切换到 root： `su -`
4. 输入 `passwords.txt` 文件中列出的密码。

StorageGRID 日志文件归档包含为每个类别描述的日志以及包含指标和调试命令输出的其他文件。

归档位置	Description
审核	在正常系统操作期间生成的审核消息。
基础操作系统日志	基本操作系统信息，包括 StorageGRID 映像版本。
捆绑包	全局配置信息（捆绑包）。
Cassandra	Cassandra 数据库信息和 Reaper 修复日志。
EC	按配置文件 ID 显示有关当前节点和 EC 组的 vCSs 信息。
网格	常规网格日志，包括调试（`byncast.log`）和 `servermanager` 日志。
grid.xml	网格配置文件在所有节点之间共享。
hagroup	高可用性组指标和日志。
安装	`Gdu-server` 和安装日志。
lumberjack.log	与日志收集相关的调试消息。
lambda-arbitrator	与 S3 Select 代理请求相关的日志。
指标	Grafana ， Jaeger ，节点导出程序和 Prometheus 的服务日志。
错误	其他访问和错误日志。
MySQL	MariaDB 数据库配置和相关日志。
网络	网络相关脚本和动态 IP 服务生成的日志。
nginx	负载平衡器配置文件和日志。还包括 Grid Manager 和租户管理器流量日志。
nginx 网关	负载平衡器配置文件和日志。
NTP	NTP 配置文件和日志。
os	节点和网格状态文件，包括服务 `pid` 。
其他	` /var/local/log` 下未在其他文件夹中收集的日志文件。
性能	CPU ，网络和磁盘 I/O 的性能信息

归档位置	Description
Prometheus-data	当前 Prometheus 指标（如果日志收集包含 Prometheus 数据）。
配置	与网格配置过程相关的日志。
草稿	来自平台服务中使用的 raft 集群的日志。
SNMP	用于发送 SNMP 通知的 SNMP 代理配置和警报允许 / 拒绝列表。
套接字数据	用于网络调试的套接字数据。
system-commands.txt	StorageGRID 容器命令的输出。包含系统信息，例如网络连接和磁盘使用情况。

相关信息

收集日志文件和系统数据

StorageGRID 软件日志

您可以使用 StorageGRID 日志对问题进行故障排除。

如果要将日志发送到外部系统日志服务器或更改 `byncast.log` 和 `NMS.log` 等审核信息的目标，请参见 配置审核消息和日志目标。

常规 StorageGRID 日志

文件名	注释：	在上找到
` /var/local/log/byncast.log`	主 StorageGRID 故障排除文件。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。	所有节点
` /var/local/log/byncast-err.log`	包含一个子集 `byncast.log` （严重性错误和严重的消息）。系统中也会显示严重消息。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。	所有节点
` /var/local/core/`	包含在程序异常终止时创建的任何核心转储文件。可能的原因包括断言失败，违规或线程超时。 文件 ` /var/local/core/kexec_cmd` 通常位于设备节点上，并不表示存在错误。	所有节点

Server Manager 日志

文件名	注释：	在上找到
` /var/local/log/servermanager.log`	服务器上运行的 Server Manager 应用程序的日志文件。	所有节点
` /var/local/log/GridstatBackend.errlog`	Server Manager GUI 后端应用程序的日志文件。	所有节点
` /var/local/log/gridstat.errlog`	Server Manager 图形用户界面的日志文件。	所有节点

StorageGRID 服务的日志

文件名	注释：	在上找到
` /var/local/log/Acct.errlog`		运行此 ADC 服务的存储节点
` /var/local/log/ADC.errlog`	包含相应服务的标准错误（ stderr ）流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	运行此 ADC 服务的存储节点
` /var/local/log/AMS.errlog`		管理节点
` /var/local/log/arc.errlog`		归档节点
` /var/local/log/Cassandra/system.log`	元数据存储（ Cassandra 数据库）的信息，如果添加新存储节点时出现问题或节点池修复任务停止，则可以使用这些信息。	存储节点
` /var/local/log/Cassandra-reaper.log`	Cassandra Reaper 服务的信息，用于修复 Cassandra 数据库中的数据。	存储节点
` /var/local/log/Cassandra-reaper.errlog`	Cassandra Reaper 服务的错误信息。	存储节点
` /var/local/log/chun.errlog`		存储节点
` /var/local/log/CLB.errlog`	CLB 服务的错误信息。 • 注： * CLB 服务已弃用。	网关节点
` /var/local/log/CMN.errlog`		管理节点

文件名	注释：	在上找到
` /var/local/log/cms.errlog`	此日志文件可能存在于已从旧版 StorageGRID 升级的系统上。它包含旧信息。	存储节点
` /var/local/log/CTS.errlog`	只有当目标类型为 * 云分层 - 简单存储服务（ S3 ） * 时，才会创建此日志文件	归档节点
` /var/local/log/dds.errlog`		存储节点
` /var/local/log/DMV.errlog`		存储节点
` /var/local/log/dynip*`	包含与 dynip 服务相关的日志，该日志可监控网格中的动态 IP 更改并更新本地配置。	所有节点
` /var/local/log/grafana.log`	与 Grafana 服务关联的日志，用于在网格管理器中显示指标。	管理节点
` /var/local/log/hagroups.log`	与高可用性组关联的日志。	管理节点和网关节点
` /var/local/log/hagroup_events.log`	跟踪状态更改，例如从备份过渡到主节点或故障。	管理节点和网关节点
` /var/local/log/idnt.errlog`		运行此 ADC 服务的存储节点
` /var/local/log/jaeger.log`	与 jaeger 服务关联的日志，用于收集跟踪。	所有节点
` /var/local/log/kstn.errlog`		运行此 ADC 服务的存储节点
` /var/local/log/lambda/*`	包含 S3 Select 服务的日志。	管理节点和网关节点 只有某些管理节点和网关节点才包含此日志。请参见 S3 Select 管理节点和网关节点的要求和限制。
` /var/local/log/LDer.errlog`		存储节点

文件名	注释：	在上找到
` /var/local/log/miscd/* 。 log`	包含 MISCd 服务（信息服务控制守护进程）的日志，此服务提供一个界面，用于查询和管理其他节点上的服务以及管理节点上的环境配置，例如查询其他节点上运行的服务的状态。	所有节点
` /var/local/log/nginx/* 。 log`	包含 nginx 服务的日志，此服务可充当各种网格服务（例如 Prometheus 和动态 IP ）的身份验证和安全通信机制，以便能够通过 HTTPS API 与其他节点上的服务进行通信。	所有节点
` /var/local/log/nginx gw/* 。 log`	包含管理节点上受限管理端口和负载平衡器服务的日志，该服务可对从客户端到存储节点的 S3 和 Swift 流量进行负载平衡。	管理节点和网关节点
` /var/local/log/persistence *`	包含永久性服务的日志，该服务用于管理根磁盘上需要在重新启动后持续存在的文件。	所有节点
` /var/local/log/Prometheus.log`	对于所有节点，包含节点导出程序服务日志和 ade-exporter指标 服务日志。 对于管理节点，还包含 Prometheus 和警报管理器服务的日志。	所有节点
` /var/local/log/raf.log`	包含用于 raft 协议的 RSM 服务所使用的库的输出。	具有 RSM 服务的存储节点
` /var/local/log/rms.errlog`	包含用于 S3 平台服务的复制状态机服务（ RSM ）服务的日志。	具有 RSM 服务的存储节点
` /var/local/log/sSM.errlog`		所有节点
` /var/local/log/update-s3vs-domains.log`	包含与处理 S3 虚拟托管域名配置的更新相关的日志。请参见实施 S3 客户端应用程序的说明。	管理节点和网关节点
` /var/local/log/update-snmp-firewall.*`	包含与为 SNMP 管理的防火墙端口相关的日志。	所有节点
` /var/local/log/update-sysl.log`	包含与对系统系统系统日志配置所做更改相关的日志。	所有节点

文件名	注释：	在上找到
` /var/local/log/update-traffic 类 .log`	包含与流量分类器配置更改相关的日志。	管理节点和网关节点
` /var/local/log/update-utcn/log`	包含与此节点上的不可信客户端网络模式相关的日志。	所有节点

NMS 日志

文件名	注释：	在上找到
` /var/local/log/NMS.log`	• 从网格管理器和租户管理器捕获通知。 • 捕获与 NMS 服务运行相关的事件，例如警报处理，电子邮件通知和配置更改。 • 包含因系统中的配置更改而导致的 XML 包更新。 • 包含与每天执行一次的属性缩减采样相关的错误消息。 • 包含 Java Web 服务器错误消息，例如页面生成错误和 HTTP 状态 500 错误。	管理节点
` /var/local/log/NMS.errlog`	包含与 MySQL 数据库升级相关的错误消息。 包含相应服务的标准错误（ stderr ）流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	管理节点
` /var/local/log/nms.requestlog`	包含有关从管理 API 到内部 StorageGRID 服务的传出连接的信息。	管理节点

相关信息

关于 bycast.log

使用 S3

部署和维护日志

您可以使用部署和维护日志对问题进行故障排除。

文件名	注释：	在上找到
` /var/local/log/install.log`	在软件安装期间创建。包含安装事件的记录。	所有节点

文件名	注释：	在上找到
` /var/local/log/expand-progress.log`	在扩展操作期间创建。包含扩展事件的记录。	存储节点
` /var/local/log/gdu-server.log`	由 GDU 服务创建。包含与主管理节点管理的配置和维护过程相关的事件。	主管理节点
` /var/local/log/send_admin_hw.log`	在安装期间创建。包含与节点与主管理节点的通信相关的调试信息。	所有节点
` /var/local/log/upgrade.log`	在软件升级期间创建。包含软件更新事件的记录。	所有节点

第三方软件的日志

您可以使用第三方软件日志对问题进行故障排除。

类别	文件名	注释：	在上找到
归档	/var/local/log/dsierror.log	TSM 客户端 API 的错误信息。	归档节点
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	MySQL 生成的日志文件。 文件 `mysql.err` 可捕获数据库错误和事件，例如启动和关闭。 文件 `mysql-slow.log` （查询日志较慢）可捕获执行时间超过 10 秒的 SQL 语句。	管理节点
操作系统	/var/local/log/messages	此目录包含操作系统的日志文件。这些日志中包含的错误也会显示在网格管理器中。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 拓扑 * > * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。	所有节点
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntstats	` /var/local/log/ntp.log` 包含 NTP 错误消息的日志文件。 ` /var/lib/ntp/var/log/ntpstats /` 目录包含 NTP 时间统计信息。 `loopstats` 记录环路筛选器统计信息。 `peerstats` 记录对等统计信息。	所有节点

类别	文件名	注释：	在上找到
SAMBA	/var/local/log/samba/	Samba 日志目录包含每个 Samba 进程（ SMB， nmb 和 winbind ）以及每个客户端主机名 /IP 的日志文件。	已配置管理节点，用于通过 CIFS 导出审核共享

关于 bycast.log

文件 ` /var/local/log/byncast.log` 是 StorageGRID 软件的主要故障排除文件。每个网格节点都有一个 `byncast.log` 文件。该文件包含特定于该网格节点的消息。

文件 ` /var/local/log/byncast-err.log` 是 `byncast.log` 的子集。它包含严重性错误和严重的消息。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

bycast.log 的文件轮换

当 `byncast.log` 文件达到 1 GB 时，将保存现有文件并启动新的日志文件。

保存的文件将重命名为 `byncast.log.1` ，新文件名为 `byncast.log` 。当新的 `byncast.log` 达到 1 GB 时， `byncast.log.1` 将重命名并压缩为 `byncast.log.2.gz` ，而 `byncast.log` 将重命名为 `byncast.log.1` 。

`byncast.log` 的轮换限制为 21 个文件。创建 `byncast.log` 文件的第 22 个版本时，将删除最旧的文件。

`byncast-err.log` 的轮换限制为七个文件。

> 如果日志文件已被压缩，则不能将其解压缩到写入该文件的同一位置。将文件解压缩到同一位置可能会干扰日志轮换脚本。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

相关信息

收集日志文件和系统数据

bycast.log 中的消息

`byncast.log` 中的消息由 ADE （异步分布式环境）写入。ADE 是每个网格节点的服务所使用的运行时环境。

ADE 消息示例：

```
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 消息包含以下信息：

消息段	示例中的值
节点 ID	12455685
ADE 进程 ID	0357819531
模块名称	SVMR
消息标识符	EVHR
UTC 系统时间	2019-05-05T27T17： 10： 29.784677 （YYYY-MM-DDTHH： MM： SS.uuuuu ）
严重性级别	error
内部跟踪编号	0906
message	SVMR： 卷 3 的运行状况检查失败，原因为 "Tut"

bycast.log 中的消息严重性

已为 `byncast.log` 中的消息分配严重性级别。

例如：

- * 通知 * —发生了应记录的事件。大多数日志消息都处于此级别。
- * 警告 * - 发生意外情况。
- * 错误 * —发生了一个会影响操作的重大错误。
- * 严重 * —发生异常情况，导致正常操作停止。您应立即解决基本情况。网格管理器中也会显示严重消息。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 * > * 节点 * > * SSM* > * 事件 * 。

中的错误代码 `bycast.log`

`byncast.log` 中的大多数错误消息都包含错误代码。

下表列出了 `byncast.log` 中的常见非数字代码。非数字代码的确切含义取决于报告该代码的上下文。

错误代码	含义
SUC	无错误
GERR	未知

错误代码	含义
已完成	已取消
异常	已中止
输出	超时
调用	无效
NFND	未找到
服务器	version
配置	Configuration
失败	失败
ICPL	未完成
完成	完成
SUNV	服务不可用

下表列出了 `byncast.log` 中的数字错误代码。

错误编号	错误代码	含义
001	EPERM	不允许执行此操作
002	已执行	没有此类文件或目录
003	ESRCH	无此过程
004	EINTR	系统调用中断
005.	EIO	I/O 错误
006	ENXIO	没有此类设备或地址
007	E2BIG	参数列表太长
008	ENOExec	Exec 格式错误

错误编号	错误代码	含义
009.	EBADF	文件编号错误
010	ECHILD	无子进程
011	EAGAIN	请重试
012	ENOMEM	内存不足
013	EACCE	权限被拒绝
014	默认	地址错误
015	ENOTBLK	需要块设备
016	EBUSY	设备或资源繁忙
017	EEXIST	文件已存在
018	EXDEV	跨设备链路
019	ENODEV	没有此类设备
020	ENOTDIR	不是目录
21	EISDIR	是一个目录
0222	EINVAL	参数无效
023	ENFILE	文件表溢出
024	EMFILE	打开的文件过多
025	ENOTTY	不是一种打字机
026	ETXTBSY	文本文件繁忙
027	EFBIG	文件太大
028	ENOSPC	设备上没有剩余空间
029	ESPIPE	非法寻道

错误编号	错误代码	含义
030	EROFS	只读文件系统
0331	EMLINK	链路太多
032	EPIPE	管道已断开
033	以登	数学参数不在功能域中
034	电子书	数学结果不可代表
035	EDEADLK	可能会发生资源死锁
036	ENAMETOOLONG	文件名太长
037	ENOLCK	没有可用的记录锁定
038	ENOSYS	未实施功能
039	ENOTEMPTY	目录不为空
40	ELOOP	遇到的符号链接太多
041		
042	ENOMSG	没有所需类型的消息
043	EIDRM	已删除标识符
044	ECHRNG	通道编号超出范围
045	EL2NSync	2 级未同步
046	EL3HLT	3 级已暂停
047	EL3RST	3 级重置
048	ELNRNG	链路编号超出范围
049	EUNATCH	未连接协议驱动程序
050	ENOCSI	没有可用的 CSI 结构

错误编号	错误代码	含义
051	EL2HLT	级别 2 已暂停
052	EBADE	交换无效
053	EBADR	请求描述符无效
054	EXFULL	Exchange 已满
055	ENOANO	无阳极
056	EBADRQC	请求代码无效
057	EBADLT	插槽无效
058		
059	EBFNT	字体文件格式错误
060	ENOSTR	设备不是流
061	ENODATA	无可用数据
062	时间	计时器已过期
063	ENOSR	流资源不足
064	ENONET	计算机不在网络上
065	ENOPK	未安装软件包
066	EREMOTE	对象为远程对象
067	ENOLINK	链路已切断
068	EADV	公布错误
069	ESRMNT	Srmount 错误
070	eComm	发送时出现通信错误
071	EPROTO	协议错误

错误编号	错误代码	含义
072	EMULTIHOP	已尝试多跃点
073	EDOTDOT	RFS 专用错误
074	EBADMSG	不是数据消息
075	超越	对于定义的数据类型，值太大
076	ENOTUNIQ	名称在网络上不唯一
077	EBADFD	文件描述符处于错误状态
078	错误	已更改远程地址
079	EIBAcc	无法访问所需的共享库
080	EIBBAD	访问损坏的共享库
081	ELIBSCN	
082	ELIBMAX	正在尝试链接过多的共享库
083	ELIBExec	无法直接执行共享库
084	EILSEQ	字节序列非法
085	错误	应重新启动中断的系统调用
086	ESTRPIPE	流管道错误
087	EUSERs.	用户过多
088	ENOTSOCK	在非套接字上执行套接字操作
089	EDESTADDRREQ	目标地址为必填项
090	EMSSIZE	消息太长
091	EPROTOTYPE	套接字的协议类型错误
092	ENOPROTOOPT	协议不可用

错误编号	错误代码	含义
093	产品说明	不支持协议
094	ESOCKTNOSUPPORT	不支持套接字类型
095	EOPNOTSUPP	传输端点上不支持此操作
096	EPFNOSUPPORT	不支持协议系列
097	EAFNOSUPPORT	协议不支持地址系列
098	EADDRINUSE	地址已在使用中
099	EADDRNOTAVAIL	无法分配请求的地址
100	ENETDOWN	网络已关闭
101.	ENETUNREACH	无法访问网络
102.	ENETRESET	由于重置，网络已断开连接
103.	已完成	软件导致连接中止
104	ECONNRESET	对等方重置连接
105.	ENOBUFS	无可用缓冲区空间
106.	EISCONN	传输端点已连接
107.	ENOTCONN	传输端点未连接
108.	ESHUTDOWN	传输端点关闭后无法发送
109.	ETOOMANYREFS	引用过多：无法接合
110	ETIMEDOUT	连接超时
111.	ECONNREFUSED	连接被拒绝
112	EHOSTDOWN	主机已关闭
113	EHOSTUNREACH	没有到主机的路由

错误编号	错误代码	含义
114	EALREADY	操作已在进行中
115	EINPROGRESS	操作正在进行中
116		
117	EUC	结构需要清理
118	ENOTCAM	不是名为 type 的 Xenix 文件
119	ENAVAIL	没有可用的 Xenix 信号
120	EISNAM	是一个命名类型的文件
121.	EREMOTEIO	远程 I/O 错误
122.	EDQUOT	已超过配额
123.	ENOMINDIUM	未找到介质
124.	EMeduMTYPE	介质类型错误
125.	ECANCELED	操作已取消
126.	ENOKEY	所需密钥不可用
127.	EKEYEXPIRED	密钥已过期
128.	EKBREVOKED	密钥已撤销
129.	已完成	密钥已被服务拒绝
130	终止	对于稳定可靠的 mMutexes： owner died
131.	ENOTRECOVERABLE	对于强大的 mutexes：状态不可恢复

扩展网格

扩展网格：概述

按照以下说明扩展 StorageGRID 系统的容量或功能，而不会中断系统操作。

关于这些说明

以下说明介绍如何执行 StorageGRID 扩展，以便向存储节点，现有站点或整个新站点添加新网格节点。

本说明适用于安装 StorageGRID 系统后负责配置和支持该系统的技术人员。

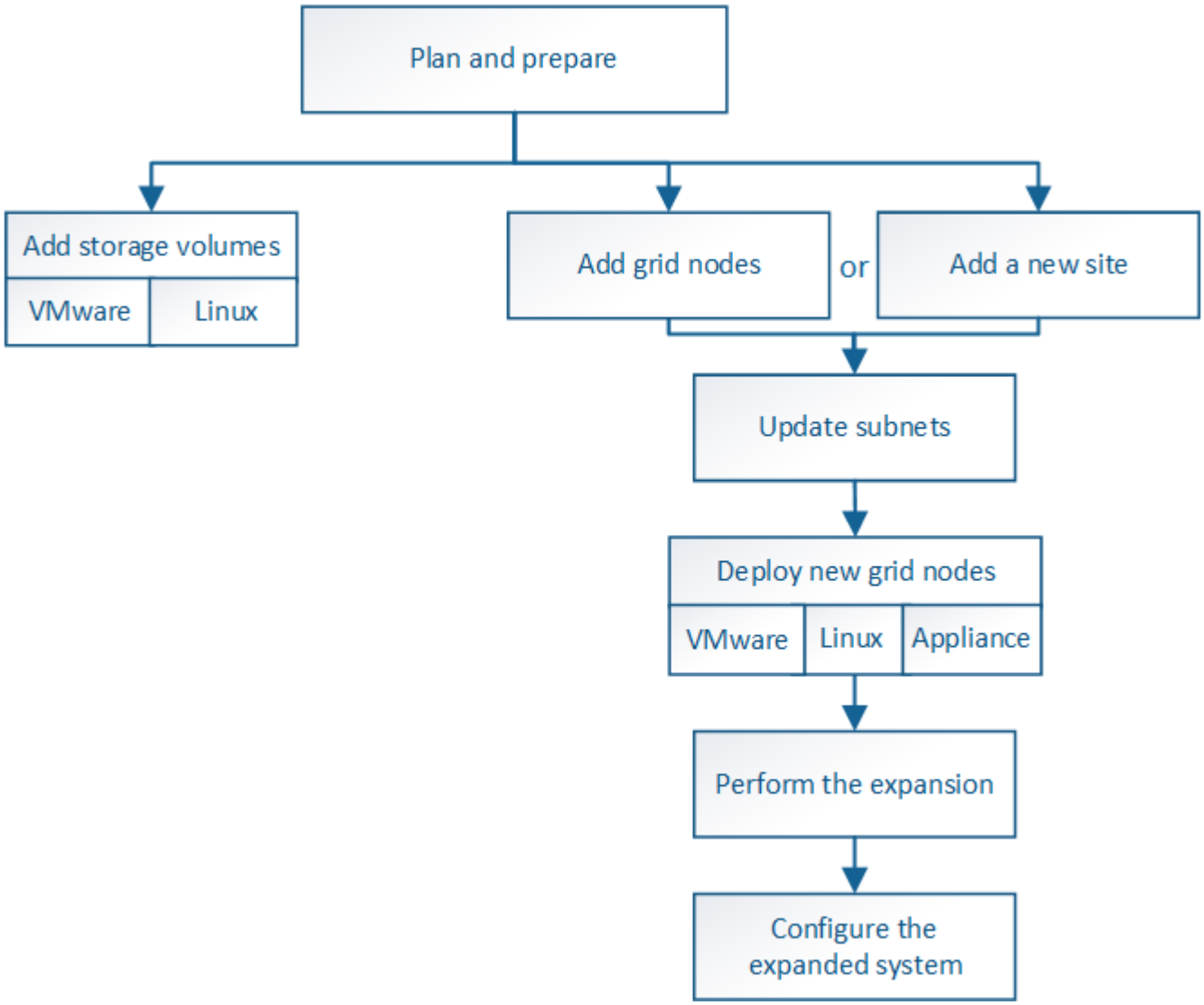
扩展操作步骤 概述

执行扩展的原因决定了您必须添加的每种类型的新节点数以及这些新节点的位置。例如，如果要执行扩展以增加存储容量，添加元数据容量或添加冗余或新功能，则节点要求会有所不同。

如工作流图所示，执行扩展的步骤取决于是向存储节点添加存储卷，向现有站点添加新节点还是添加新站点。无论哪种情况，您都可以在不中断当前系统运行的情况下执行扩展。

添加节点的步骤还取决于您是添加 StorageGRID 设备还是添加运行 VMware 或 Linux 的主机。

"`Linux`" 是指 Red Hat ® Enterprise Linux ® ， Ubuntu ® ， CentOS 或 Debian ® 部署。使用 "NetApp 互操作性表工具（ IMT ）" 以获取支持的版本列表。



规划 StorageGRID 扩展

添加存储容量

添加对象容量的准则

您可以通过向现有存储节点添加存储卷或向现有站点添加新存储节点来扩展 StorageGRID 系统的对象存储容量。添加存储容量时，必须满足信息生命周期管理（ ILM ）策略的要求。

添加存储卷的准则

在将存储卷添加到现有存储节点之前，请查看以下准则和限制：

- 您必须检查当前的 ILM 规则，以确定在何处以及何时添加存储卷以增加可用于复制或擦除编码对象的存储。请参见的说明 通过信息生命周期管理管理对象。
- 您不能通过添加存储卷来增加系统的元数据容量，因为对象元数据仅存储在卷 0 上。
- 每个基于软件的存储节点最多可支持 16 个存储卷。如果您需要添加的容量超出此范围，则必须添加新的存储节点。
- 您可以向每个SG6060或SG6060X设备添加一个或两个扩展架。每个扩展架可添加 16 个存储卷。如果安装了这两个扩展架、则SG6060和SG6060X每个扩展架总共可支持48个存储卷。
- 您不能将存储卷添加到任何其他存储设备。
- 您不能增加现有存储卷的大小。
- 您不能在执行系统升级，恢复操作或其他扩展的同时向存储节点添加存储卷。

在决定添加存储卷并确定必须扩展哪些存储节点以满足 ILM 策略后，请按照适用于您的存储节点类型的说明进行操作：

- 要向SG6060或SG60X存储设备添加一个或两个扩展架、请转至 将扩展架添加到已部署的SG6060或SG60X。
- 对于基于软件的节点，请按照的说明进行操作将存储卷添加到存储节点。

添加存储节点的准则

在将存储节点添加到现有站点之前，请查看以下准则和限制：

- 您必须检查当前的 ILM 规则，以确定在何处以及何时添加存储节点以增加可用于复制或擦除编码对象的存储。请参见的说明 通过信息生命周期管理管理对象。
- 在一个扩展操作步骤 中添加的存储节点不应超过 10 个。
- 您可以在一个扩展操作步骤 中将存储节点添加到多个站点。
- 您可以在一个扩展操作步骤 中添加存储节点和其他类型的节点。
- 在启动扩展操作步骤 之前，您必须确认在恢复过程中执行的所有数据修复操作均已完成。请参见 检查数据修复作业。
- 如果在执行扩展之前或之后需要删除存储节点，则在一个 " 停用节点 " 操作步骤 中停用的存储节点不应超过 10 个。

存储节点上的模块转换服务准则

配置扩展时，必须选择是否在每个新存储节点上包含管理域控制器（ADA）服务。此 ADA 服务可跟踪网格服务的位置和可用性。

- StorageGRID 系统需要 ADC 服务的仲裁 可在每个站点和任何时间使用。
- 每个站点至少有三个存储节点必须包含此 ADC-Service 。
- 不建议将此 ADA 服务添加到每个存储节点。包含过多的 ADC 服务可能会因节点间通信量增加而导致发生原因 速度变慢。
- 一个网格中包含的存储节点不应超过 48 个，而是使用了此 ADA 服务。这相当于 16 个站点，每个站点有三个模块转换服务。
- 通常，在为新节点选择 * 数字转换服务 * 设置时，应选择 * 自动 * 。仅当新节点将替换包含此 ADC-Service 的另一个存储节点时，才选择 * 是 * 。由于如果仍会保留的 ADD 服务太少，则无法停用存储节点，因此，这样可以确保在删除旧服务之前新的 ADD 服务可用。
- 在部署此节点后，您不能将此 ADC 服务添加到该节点中。

为复制的对象添加存储容量

如果您的部署的信息生命周期管理（ ILM ）策略包含一条规则，用于创建对象的复制副本，则必须考虑要添加的存储容量以及要添加新存储卷或存储节点的位置。

有关在何处添加额外存储的指导，请查看创建复制副本的 ILM 规则。如果 ILM 规则创建两个或更多对象副本，请计划在创建对象副本的每个位置添加存储。例如，如果您有一个双站点网格和一个 ILM 规则，在每个站点创建一个对象副本，则必须向每个站点添加存储，以增加网格的整体对象容量。请参见的说明 通过信息生命周期管理管理对象。

出于性能原因，您应尝试在各个站点之间保持存储容量和计算能力的平衡。因此，在此示例中，您应向每个站点添加相同数量的存储节点或在每个站点添加更多存储卷。

如果您的 ILM 策略更加复杂，其中包括根据存储分段名称等标准将对象放置在不同位置的规则，或者随着时间的推移更改对象位置的规则，则您对扩展所需存储位置的分析将类似，但更为复杂。

绘制整体存储容量的消耗速度图表有助于您了解要在扩展中添加多少存储以及何时需要额外存储空间。您可以使用网格管理器监控和绘制存储容量图表，如的说明所述 监控 StorageGRID 并对其进行故障排除。

在规划扩展的时间时，请务必考虑购买和安装额外存储可能需要多长时间。

为经过纠删编码的对象添加存储容量

如果 ILM 策略包含创建纠删编码副本的规则，则必须计划在何处添加新存储以及何时添加新存储。您添加的存储量和添加的时间可能会影响网格的可用存储容量。

规划存储扩展的第一步是，检查 ILM 策略中用于创建纠删编码对象的规则。由于 StorageGRID 会为每个纠删编码对象创建 *k+m_fragments* ，并将每个片段存储在不同的存储节点上，因此您必须确保在扩展后至少 *_k+m* 存储节点具有用于存储新纠删编码数据的空间。如果纠删编码配置文件提供站点丢失保护，则必须向每个站点添加存储。请参见 使用 ILM 管理对象。

您需要添加的节点数还取决于执行扩展时现有节点的容量。

有关为经过纠删编码的对象添加存储容量的一般建议

如果要避免详细计算，可以在现有存储节点容量达到 70% 时为每个站点添加两个存储节点。

对于单站点网格和纠删编码可提供站点丢失保护的网格，此一般建议可在多种纠删编码方案中提供合理的结果。

要更好地了解导致此建议的因素或为您的站点制定更精确的计划，请查看下一节。有关针对您的情况优化的自定义建议，请联系您的 NetApp 客户代表。

计算要为擦除编码对象添加的扩展存储节点数

要优化存储纠删编码对象的部署扩展方式，您必须考虑许多因素：

- 正在使用纠删编码方案
- 用于纠删编码的存储池的特征，包括每个站点上的节点数和每个节点上的可用空间量
- 网格之前是否已扩展（因为每个存储节点上的可用空间量可能并非所有节点上的大致相同）
- ILM 策略的确切性质，例如 ILM 规则是否同时创建复制的对象和经过纠删编码的对象

以下示例可帮助您了解纠删编码方案的影响，存储池中的节点数以及每个节点上的可用空间量。

类似的注意事项会影响存储复制数据和纠删编码数据的 ILM 策略的计算以及先前扩展的网格的计算。

> 本节中的示例介绍了向 StorageGRID 系统添加存储容量的最佳实践。如果无法添加建议的节点数，则可能需要运行 EC 重新平衡操作步骤 ，以便存储其他经过纠删编码的对象。请参见 重新平衡经过纠删编码的数据。

示例 **1** ： 扩展使用 **2+1** 纠删编码的单站点网格

此示例显示了如何扩展仅包含三个存储节点的简单网格。

> 为了简单起见，此示例仅使用三个存储节点。但是，不建议仅使用三个存储节点：实际生产网格应至少使用 *k*+*m* + 1 个存储节点来实现冗余，此值等于本示例中的四个存储节点（ 2+1+1 ）。

假设满足以下条件：

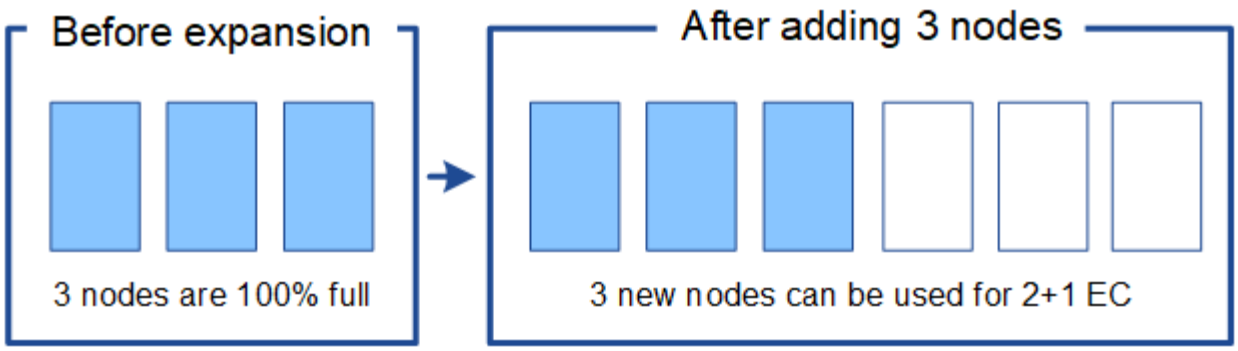
- 所有数据均使用 2+1 纠删编码方案进行存储。使用 2+1 纠删编码方案时，每个对象都存储为三个片段，每个片段保存在不同的存储节点上。
- 您有一个站点包含三个存储节点。每个存储节点的总容量为 100 TB 。
- 要通过添加新的 100 TB 存储节点进行扩展。
- 您希望最终在新旧节点之间平衡经过纠删编码的数据。

根据执行扩展时存储节点的容量，您可以选择多种方法。

- * 如果现有节点已满，请添加三个 100 TB 存储节点 *

  在此示例中，现有节点已满 100% 。由于没有可用容量，您必须立即添加三个节点以继续 2+1 纠删编码。

  扩展完成后，对对象进行纠删编码后，所有片段都将放置在新节点上。

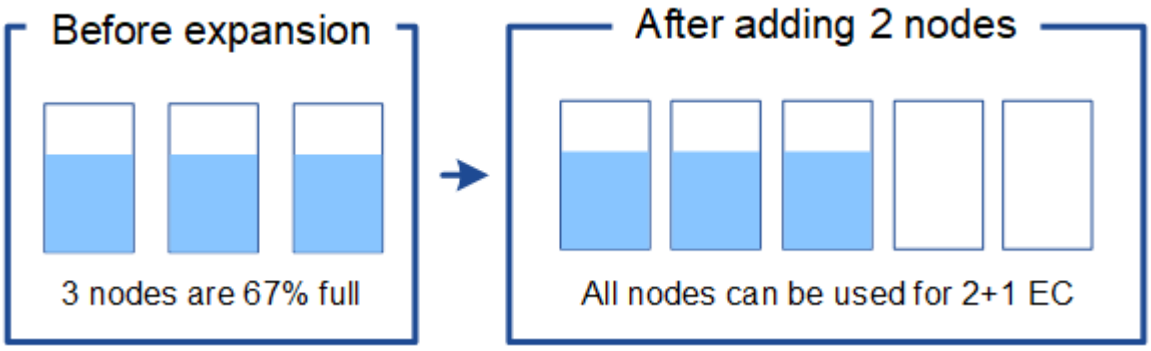


此扩展可添加 _k+m_nodes 。为实现冗余，建议添加四个节点。如果在现有节点已满 100% 时仅添加 _k+m_expansion Storage Node ，则所有新对象都会存储在扩展节点上。如果任何新节点变得不可用，即使是暂时不可用， StorageGRID 也无法满足 ILM 要求。

- * 如果现有存储节点已满 67% ，请添加两个 100 TB 存储节点 *

  在此示例中，现有节点已满 67% 。由于现有节点上有 100 TB 的可用容量（每个节点 33 TB ），因此，如果您现在执行扩展，则只需添加两个节点。

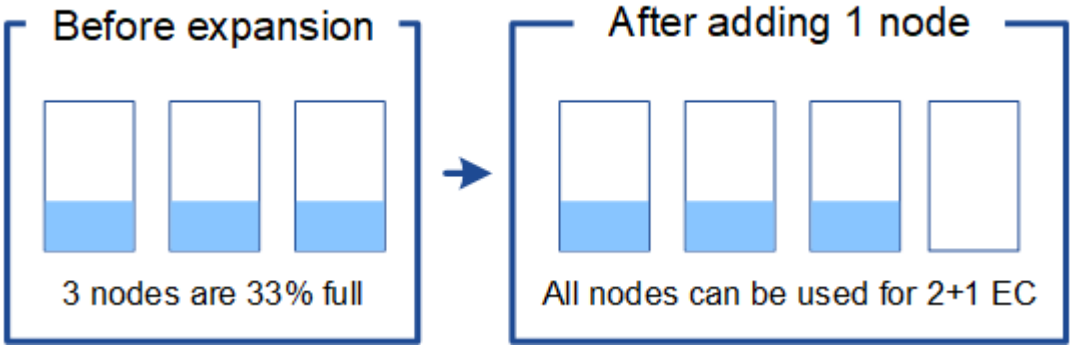
  添加 200 TB 的额外容量后，您可以继续 2+1 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。



- * 如果现有存储节点已满 33% ，请添加一个 100 TB 存储节点 *

  在此示例中，现有节点已满 33% 。由于现有节点上有 200 TB 的可用容量（每个节点 67 TB ），因此，如果您现在执行扩展，则只需要添加一个节点。

  添加 100 TB 的额外容量后，您可以继续 2+1 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。



示例 **2** ： 扩展使用 **6+3** 纠删编码的三站点网格

此示例显示了如何为多站点网格制定扩展计划，该网格采用的纠删编码方案包含更多片段。尽管这些示例之间存在差异，但建议的扩展计划非常相似。

假设满足以下条件：

- 所有数据均使用 6+3 纠删编码方案进行存储。使用 6+3 纠删编码方案时，每个对象将存储为 9 个片段，每个片段将保存到不同的存储节点。
- 您有三个站点，每个站点有四个存储节点（共 12 个节点）。每个节点的总容量为 100 TB 。
- 要通过添加新的 100 TB 存储节点进行扩展。
- 您希望最终在新旧节点之间平衡经过纠删编码的数据。

根据执行扩展时存储节点的容量，您可以选择多种方法。

- * 如果现有节点已满，请添加九个 100 TB 存储节点（每个站点三个） *

  在此示例中， 12 个现有节点已满。由于没有可用容量，您必须立即添加九个节点（ 900 TB 的额外容量），才能继续 6+3 纠删编码。

  扩展完成后，对对象进行纠删编码后，所有片段都将放置在新节点上。

  > 此扩展可添加 _k+m_nodes 。为了实现冗余，建议添加 12 个节点（每个站点四个）。如果在现有节点已满 100% 时仅添加 _k+m_expansion Storage Node ，则所有新对象都会存储在扩展节点上。如果任何新节点变得不可用，即使是暂时不可用， StorageGRID 也无法满足 ILM 要求。

- * 如果现有节点已满 75% ，请添加六个 100 TB 存储节点（每个站点两个） *

  在此示例中， 12 个现有节点已满 75% 。由于可用容量为 300 TB （每个节点 25 TB ），因此，如果您现在执行扩展，则只需添加六个节点。您应向这三个站点中的每个站点添加两个节点。

  添加 600 TB 的存储容量后，您可以继续 6+3 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。

- * 如果现有节点已满 50% ，请添加三个 100 TB 存储节点（每个站点一个） *

  在此示例中， 12 个现有节点已满 50% 。由于可用容量为 600 TB （每个节点 50 TB ），因此，如果您现在执行扩展，则只需添加三个节点。您应向这三个站点中的每个站点添加一个节点。

  添加 300 TB 的存储容量后，您可以继续 6+3 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。

重新平衡经过纠删编码的数据的注意事项

如果要执行扩展以添加存储节点，并且 ILM 策略包含一个或多个用于擦除代码数据的 ILM 规则，则可能需要在扩展完成后执行 EC 重新平衡操作步骤 。

例如，如果您无法为所使用的纠删编码方案添加建议数量的存储节点，则可能需要运行 EC 重新平衡操作步骤以存储其他经过纠删编码的对象。

查看这些注意事项后，请执行扩展，然后转到 添加存储节点后重新平衡经过纠删编码的数据 以运行操作步骤 。

什么是 **EC** 重新平衡?

EC 重新平衡是扩展存储节点后可能需要的 StorageGRID 操作步骤 。操作步骤 将作为主管理节点上的命令行脚本运行。运行 EC 重新平衡操作步骤 时， StorageGRID 会在站点的现有存储节点和新扩展的存储节点之间重新分布经过擦除编码的片段。

EC 重新平衡操作步骤 ：

- 仅移动经过纠删编码的对象数据。它不会移动复制的对象数据。
- 在站点内重新分布数据。它不会在站点之间移动数据。
- 在站点的所有存储节点之间重新分布数据。它不会在存储卷中重新分配数据。
- 在确定从何处移动经过纠删编码的数据时，不会考虑每个存储节点上的复制数据使用情况

完成 EC 重新平衡操作步骤 后：

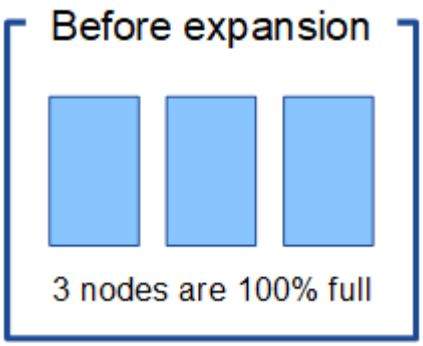
- 经过纠删编码的数据会从可用空间较少的存储节点移至可用空间较多的存储节点。
- 由于 EC 重新平衡操作步骤 不会移动复制的对象副本，因此存储节点之间的已用（ % ）值可能会保持不同。
- 擦除编码对象的数据保护将保持不变。

当 EC 重新平衡操作步骤 运行时， ILM 操作以及 S3 和 Swift 客户端操作的性能可能会受到影响。因此，您只能在有限情况下执行此操作步骤 。

何时不执行 **EC** 重新平衡

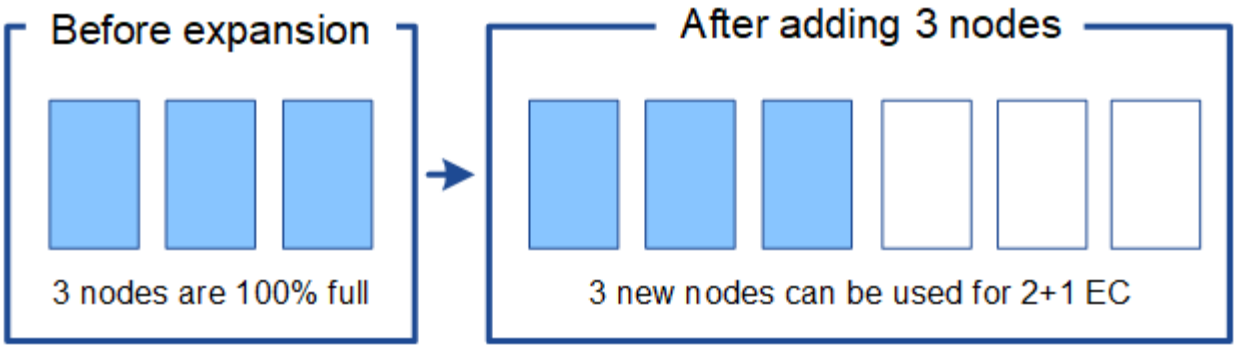
例如，当您不需要执行 EC 重新平衡时，请考虑以下几点：

- StorageGRID 正在一个站点上运行，该站点包含三个存储节点。
- ILM 策略对大于 1.0 MB 的所有对象使用 2+1 擦除编码规则，对较小的对象使用双副本复制规则。
- 所有存储节点均已完全满，并且已在主要严重性级别触发 * 对象存储空间不足 * 警报。建议执行扩展操作步骤 以添加存储节点。



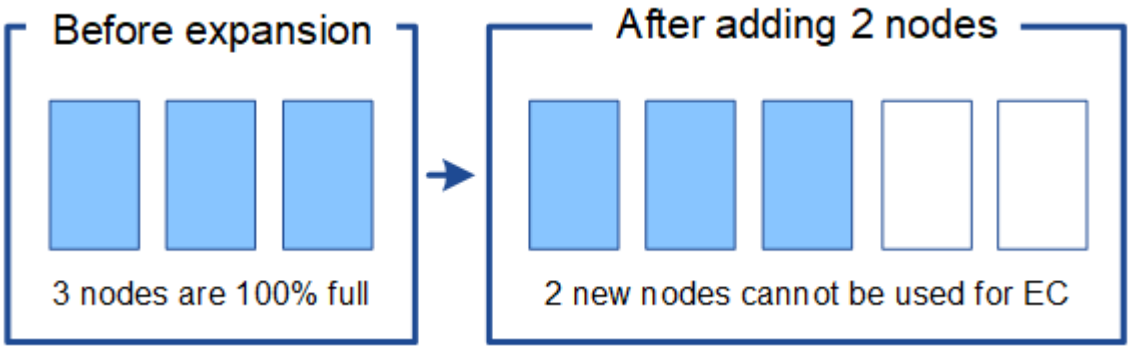
要在此示例中扩展站点，建议您添加三个或更多新的存储节点。StorageGRID 需要三个存储节点来执行 2+1 纠删编码，以便可以将两个数据片段和一个奇偶校验片段放置在不同的节点上。

添加三个存储节点后，原始存储节点将保持全满状态，但可以继续将对象载入新节点上的 2+1 纠删编码方案中。在这种情况下，不建议运行 EC 重新平衡操作步骤 ： 运行操作步骤 将暂时降低性能，这可能会影响客户端操作。

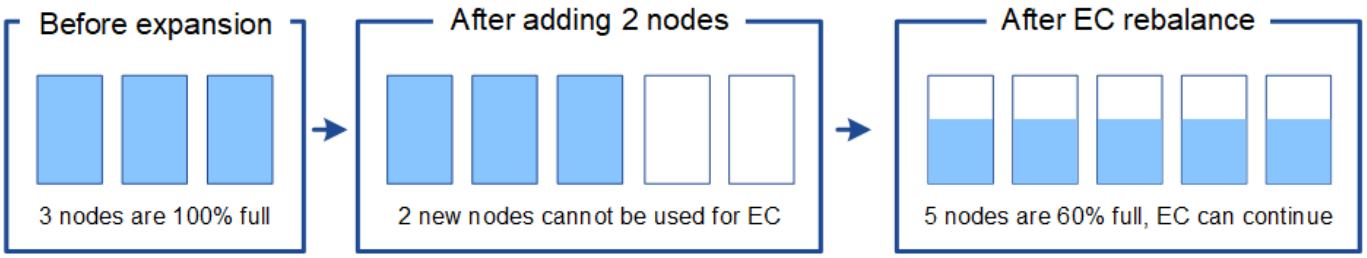


何时执行 **EC** 重新平衡

例如，您应在何时执行 EC 重新平衡操作步骤 ，请考虑相同的示例，但假定您只能添加两个存储节点。由于 2+1 纠删编码至少需要三个存储节点，因此新节点不能用于纠删编码的数据。



要解析此问题描述 并使用新的存储节点，您可以运行 EC 重新平衡操作步骤 。运行此操作步骤 时，StorageGRID 会在站点的所有存储节点之间重新分发经过纠删编码的数据和奇偶校验片段。在此示例中，当 EC 重新平衡操作步骤 完成后，所有五个节点的容量现在仅为 60% ，并且可以继续将对象载入所有存储节点上的 2+1 纠删编码方案。



EC 重新平衡的要求

通常，您只能在有限情况下运行 EC 重新平衡操作步骤 。具体而言，只有在以下所有陈述均正确的情况下，才应执行 EC 重新平衡：

- 您可以对对象数据使用纠删编码。
- 已针对站点上的一个或多个存储节点触发 * 对象存储空间不足 * 警报，表示这些节点已满 80% 或以上。
- 您无法为正在使用的纠删编码方案添加建议数量的新存储节点。请参见 为经过纠删编码的对象添加存储容量。
- 当 EC 重新平衡操作步骤 正在运行时， S3 和 Swift 客户端的写入和读取操作可以容忍较低的性能。

EC 重新平衡操作步骤 如何与其他维护任务进行交互

您不能在运行 EC 重新平衡操作步骤 的同时执行某些维护过程。

操作步骤	在 **EC** 重新平衡操作步骤 期间是否允许?
其他 EC 重新平衡过程	否 一次只能运行一个 EC 重新平衡操作步骤 。
停用操作步骤 EC 数据修复作业	否 • 在 EC 重新平衡操作步骤 运行期间，系统会阻止您启动停用操作步骤或 EC 数据修复。 • 在存储节点停用操作步骤 操作步骤 或 EC 数据修复正在运行时，系统会阻止您启动 EC 重新平衡。
扩展操作步骤	否 如果需要在扩展中添加新的存储节点，应等待运行 EC 重新平衡操作步骤，直到添加完所有新节点为止。如果在添加新存储节点时正在进行 EC 重新平衡操作步骤 ，则不会将数据移动到这些节点。
升级操作步骤	否 如果需要升级 StorageGRID 软件，应在运行 EC 重新平衡操作步骤 之前或之后执行升级操作步骤 。您可以根据需要终止 EC 重新平衡操作步骤以执行软件升级。
设备节点克隆操作步骤	否 如果需要克隆设备存储节点，应等待运行 EC 重新平衡操作步骤 ，直到添加新节点为止。如果在添加新存储节点时正在进行 EC 重新平衡操作步骤 ，则不会将数据移动到这些节点。
修补程序操作步骤	是的。 您可以在 EC 重新平衡操作步骤 运行期间应用 StorageGRID 修补程序。
其他维护过程	否 在运行其他维护过程之前，您必须终止 EC 重新平衡操作步骤 。

EC 重新平衡操作步骤 如何与 ILM 交互

在运行 EC 重新平衡操作步骤 时，请避免进行可能会更改现有纠删编码对象位置的 ILM 更改。例如，请勿开始使用具有不同擦除编码配置文件的 ILM 规则。如果需要进行此类 ILM 更改，应中止 EC 重新平衡操作步骤 。

要确保为对象元数据提供足够的可用空间，您可能需要执行扩展操作步骤 以在每个站点添加新的存储节点。

StorageGRID 会为每个存储节点的卷 0 上的对象元数据预留空间。每个站点维护三个所有对象元数据副本，这些副本均匀分布在所有存储节点上。

您可以使用网格管理器监控存储节点的元数据容量，并估计元数据容量的使用速度。此外，当已用元数据空间达到特定阈值时，系统会为存储节点触发 * 低元数据存储 * 警报。

请注意，根据网格的使用方式，网格的对象元数据容量消耗速度可能比其对象存储容量更快。例如，如果您通常要载入大量小对象或向对象添加大量用户元数据或标记，则即使仍有足够的对象存储容量，您可能需要添加存储节点以增加元数据容量。

有关详细信息，请参见以下内容：

- 管理对象元数据存储
- 监控每个存储节点的对象元数据容量

增加元数据容量的准则

在添加存储节点以增加元数据容量之前，请查看以下准则和限制：

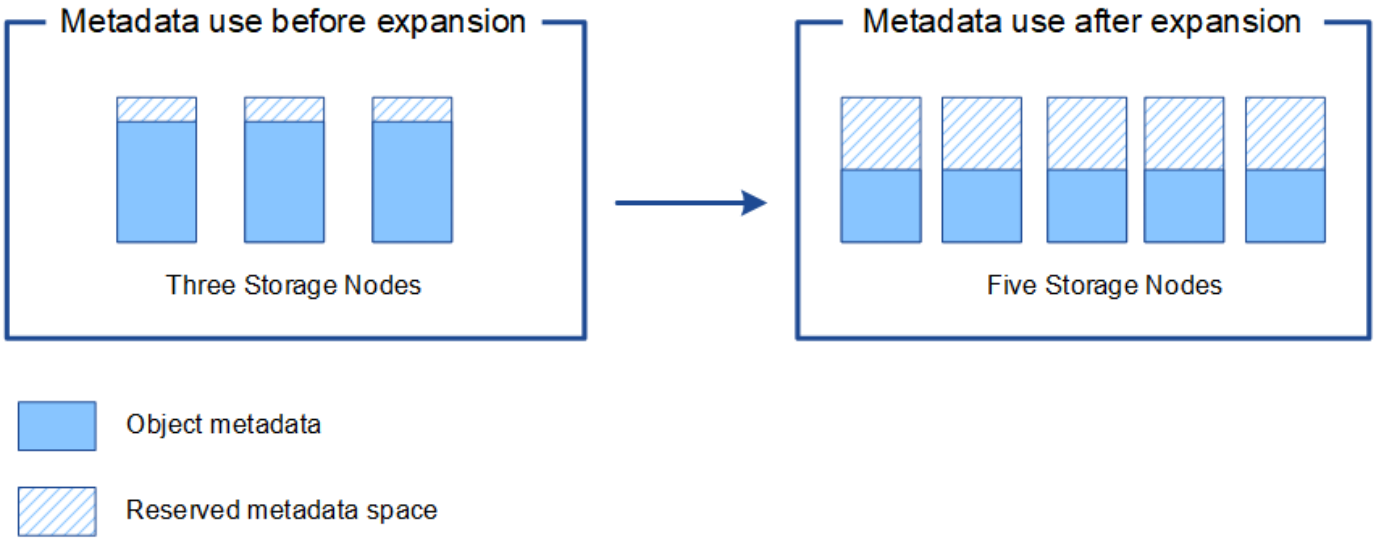
- 假设有足够的对象存储容量可用，则为对象元数据提供更多的可用空间将增加可存储在 StorageGRID 系统中的对象数量。
- 您可以通过向每个站点添加一个或多个存储节点来增加网格的元数据容量。
- 在任何给定存储节点上为对象元数据预留的实际空间取决于元数据预留空间存储选项（系统范围设置），分配给节点的 RAM 量以及节点卷 0 的大小。请参见的说明 管理 StorageGRID。
- 您不能通过向现有存储节点添加存储卷来增加元数据容量，因为元数据仅存储在卷 0 上。
- 您不能通过添加新站点来增加元数据容量。
- StorageGRID 会为每个站点上的所有对象元数据保留三个副本。因此，系统的元数据容量受最小站点的元数据容量限制。
- 在添加元数据容量时，应向每个站点添加相同数量的存储节点。

添加存储节点时如何重新分配元数据

在扩展中添加存储节点时， StorageGRID 会将现有对象元数据重新分发到每个站点的新节点，从而增加网格的整体元数据容量。无需用户操作。

下图显示了在扩展中添加存储节点时 StorageGRID 如何重新分发对象元数据。图的左侧表示扩展之前三个存储节点的卷 0 。元数据占用了每个节点可用元数据空间的相对较大部分，并且已触发 "* 低元数据存储 * " 警报。

图的右侧显示了在向站点添加两个存储节点后如何重新分配现有元数据。每个节点上的元数据数量已减少，不再触发 * 元数据存储不足 * 警报，并且可用于元数据的空间已增加。



添加网格节点以向系统添加功能

您可以通过向现有站点添加新的网格节点来为 StorageGRID 系统添加冗余或其他功能。

例如，您可以选择添加其他网关节点以支持创建网关节点的高可用性组，也可以在远程站点添加管理节点以允许使用本地节点进行监控。

您可以通过单个扩展操作向一个或多个现有站点添加以下一种或多种类型的节点：

- 非主管理节点
- 存储节点
- 网关节点
- 归档节点

准备添加网格节点时，请注意以下限制：

- 主管理节点会在初始安装期间部署。在扩展期间，不能添加主管理节点。
- 您可以在同一扩展中添加存储节点和其他类型的节点。
- 添加存储节点时，必须仔细规划新节点的数量和位置。请参见 添加对象容量的准则。
- 如果要添加归档节点，请注意，每个归档节点仅通过 Tivoli Storage Manager （ TSM ）中间件支持磁带。
- 如果在不可信客户端网络页面上将 * 新节点客户端网络默认 * 选项设置为 * 不可信 * ，则使用客户端网络连接到扩展节点的客户端应用程序必须使用负载平衡器端点端口（ * 配置 * > * 网络 * > * 不可信客户端网络 * ）进行连接。请参见的说明 管理 StorageGRID 更改新节点的设置并配置负载平衡器端点。

添加新站点

您可以通过添加新站点来扩展 StorageGRID 系统。

添加站点的准则

在添加站点之前，请查看以下要求和限制：

- 每个扩展操作只能添加一个站点。
- 不能在同一扩展中向现有站点添加网格节点。
- 所有站点必须至少包含三个存储节点。
- 添加新站点不会自动增加可存储的对象数量。网格的总对象容量取决于每个站点的可用存储容量， ILM 策略和元数据容量。
- 在估算新站点的规模时，您必须确保其包含足够的元数据容量。

  StorageGRID 会为每个站点上的所有对象元数据保留一份副本。添加新站点时，您必须确保它包含足够的元数据容量来容纳现有对象元数据，以及足够的元数据容量来支持增长。

  有关详细信息，请参见以下内容：

  - 管理对象元数据存储
  - 监控每个存储节点的对象元数据容量
- 您必须考虑站点之间的可用网络带宽以及网络延迟级别。元数据更新会在站点之间持续复制，即使所有对象都仅存储在要载入的站点上也是如此。
- 由于 StorageGRID 系统在扩展期间仍可正常运行，因此您必须在启动扩展操作步骤 之前查看 ILM 规则。您必须确保在扩展操作步骤 完成之前不会将对象副本存储到新站点。

  例如，在开始扩展之前，请确定是否有任何规则使用默认存储池（所有存储节点）。如果有，则必须创建一个包含现有存储节点的新存储池，并更新 ILM 规则以使用新存储池。否则，一旦新站点上的第一个节点变为活动状态，对象就会复制到该站点。

  有关在添加新站点时更改 ILM 的详细信息，请参见说明中的更改 ILM 策略示例 使用 ILM 管理对象。

收集所需材料

在执行扩展操作之前，请收集相关材料并安装和配置任何新的硬件和网络。

项目	注释：
StorageGRID 安装归档	如果要添加新的网格节点或新站点，则必须下载并提取 StorageGRID 安装归档。您必须使用网格上当前运行的相同版本。 有关详细信息，请参见的说明 下载并提取 StorageGRID 安装文件。 • 注意： * 如果要向现有存储节点添加新存储卷或安装新的 StorageGRID 设备，则不需要下载文件。
服务笔记本电脑	服务笔记本电脑具有以下功能： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器

项目	注释：
`passwords.txt` file	包含访问命令行上的网格节点所需的密码。包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
StorageGRID 文档	• 管理 StorageGRID • 发行说明 • 适用于您的平台的安装说明 ◦ 安装 Red Hat Enterprise Linux 或 CentOS ◦ 安装 Ubuntu 或 Debian ◦ 安装 VMware
适用于您的平台的最新文档	有关支持的版本，请参见 "互操作性表"。

下载并提取 **StorageGRID** 安装文件

【下载并提取安装文件】

在添加新网格节点或新站点之前，必须下载相应的 StorageGRID 安装归档并提取文件。

关于此任务

您必须使用网格上当前运行的 StorageGRID 版本执行扩展操作。

步骤

1. 转到 StorageGRID 的 "NetApp 下载 " 页面。

   "NetApp 下载： StorageGRID"

2. 选择网格上当前运行的 StorageGRID 版本。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。
5. 在下载页面的 * 安装 StorageGRID * 列中，为您的平台选择 ` .tgz` 或 ` .zip` 文件。

   安装归档文件中显示的版本必须与当前安装的软件版本匹配。

   如果您在服务笔记本电脑上运行 Windows ，请使用 ` .zip` 文件。

平台	安装归档
Red Hat Enterprise Linux 或 CentOS	`storageGRID-Webscale -version-RPM-uniqueID.zip` `StorageGRID-Webscale -version-RPM-uniqueID.tgz`

平台	安装归档
Ubuntu ， Debian 或设备	`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/ 其他虚拟机管理程序	要在 OpenStack 上扩展现有部署，您必须部署一个运行上述受支持 Linux 分发版本之一的虚拟机，并按照适用于 Linux 的相应说明进行操作。

6. 下载并提取归档文件。
7. 按照适用于您的平台的步骤，根据您的平台，计划的网格拓扑以及您将如何扩展 StorageGRID 系统来选择所需的文件。

   步骤中为每个平台列出的路径与归档文件安装的顶级目录相对。

8. 如果要扩展 Red Hat Enterprise Linux 或 CentOS 系统，请选择相应的文件。

路径和文件名	**Description**
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 节点映像。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 主机服务。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。

路径和文件名	Description
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 RHEL 或 CentOS 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要扩展 Ubuntu 或 Debian 系统，请选择相应的文件。

路径和文件名	Description
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。
	文件 ` /debs/storagegrid-webscale-images-version-SHA.deb` 的 MD5 校验和。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。

路径和文件名	Description
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要扩展 VMware 系统，请选择相应的文件。

路径和文件名	Description
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。
	用于部署主管理节点的开放式虚拟化格式模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署非主管理节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署归档节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署网关节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署基于虚拟机的存储节点的模板文件（`.OVF`）和清单文件（`.MF`）。
部署脚本工具	Description

路径和文件名	Description
	Bash shell 脚本，用于自动部署虚拟网格节点。
	与 `deept-vsphere-ovftool.sh` 脚本结合使用的示例配置文件。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	StorageGRID 的 API 架构。 • 注意 * ：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要扩展基于 StorageGRID 设备的系统，请选择相应的文件。

路径和文件名	Description
	用于在设备上安装 StorageGRID 节点映像的 Deb 软件包。
	StorageGRID 设备安装程序使用的 Deb 安装包的校验和，用于验证该软件包在上传后是否完好无损。

对于设备安装，只有在需要避免网络流量时，才需要这些文件。设备可以从主管理节点下载所需文件。

验证硬件和网络连接

开始扩展 StorageGRID 系统之前，请确保满足以下要求：

- 已安装并配置支持新网格节点或新站点所需的硬件。

- 所有新节点都具有指向所有现有节点和新节点的双向通信路径（网格网络的一项要求）。
- 主管理节点可以与用于托管 StorageGRID 系统的所有扩展服务器进行通信。
- 如果任何新节点的子网上有一个网格网络 IP 地址，而此地址以前未使用过，则表示您已使用 已添加新子网 到网格网络子网列表。否则，您必须取消扩展，添加新子网并重新启动操作步骤 。
- 您未在网格节点之间或 StorageGRID 站点之间的网格网络上使用网络地址转换（ Network Address Translation ， NAT ）。如果您对网格网络使用专用 IPv4 地址，则这些地址必须可从每个站点的每个网格节点直接路由。只有在使用对网格中的所有节点都透明的通道应用程序时，才支持使用 NAT 在公有 网段中桥接网格网络，这意味着网格节点不需要了解公有 IP 地址。

  此 NAT 限制特定于网格节点和网格网络。您可以根据需要在外部客户端和网格节点之间使用 NAT ，例如为网关节点提供公有 IP 地址。

添加存储卷

将存储卷添加到存储节点

您可以通过添加其他存储卷来扩展存储卷数量不超过 16 个的存储节点的存储容量。您可能需要将存储卷添加到多个存储节点，以满足对复制的或经过纠删编码的副本的 ILM 要求。

您需要的内容

在添加存储卷之前，请查看 添加对象容量的准则 确保您知道在何处添加卷以满足 ILM 策略的要求。

> 这些说明仅适用于基于软件的存储节点。请参见 将扩展架添加到已部署的SG6060或SG60X 了解如何通过安装扩展架将存储卷添加到SG6060或SG60X。无法扩展其他设备存储节点。

关于此任务

存储节点的底层存储分为多个存储卷。存储卷是基于块的存储设备，由 StorageGRID 系统格式化并挂载以存储对象。每个存储节点最多可支持 16 个存储卷，在网格管理器中称为 *object stores* 。

> 对象元数据始终存储在对象存储 0 中。

每个对象存储都挂载在与其 ID 对应的卷上。例如， ID 为 0000 的对象存储对应于 ` /var/local/rangedb/0` 挂载点。

在添加新存储卷之前，请使用网格管理器查看每个存储节点的当前对象存储以及相应的挂载点。您可以在添加存储卷时使用此信息。

步骤

1. 选择 * 节点 * > * 站点 _* > * 存储节点 _* > * 存储 * 。
2. 向下滚动以查看每个卷和对象存储的可用存储容量。

   对于设备存储节点，每个磁盘的全球通用名称与在 SANtricity 软件（连接到设备存储控制器的管理软件）中查看标准卷属性时显示的卷全球通用标识符（ WWID ）匹配。

   为了帮助您解释与卷挂载点相关的磁盘读取和写入统计信息，磁盘设备表的 * 名称 * 列（即 *sdc* ， *sdd* ， *sde* 等）中显示的名称的第一部分与卷表的 * 设备 * 列中显示的值匹配。

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. 按照适用于您的平台的说明向存储节点添加新存储卷。
   - VMware： 将存储卷添加到存储节点
   - Linux： 将直连卷或 SAN 卷添加到存储节点

VMware： 将存储卷添加到存储节点

如果某个存储节点包含的存储卷少于 16 个，则可以使用 VMware vSphere 添加卷来增加其容量。

您需要的内容

- 您可以访问有关安装适用于 VMware 的 StorageGRID 部署的说明。
  - 安装 VMware
- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

> 在软件升级，恢复操作步骤 或其他扩展操作步骤 处于活动状态时，请勿尝试向存储节点添加存储卷。

关于此任务

添加存储卷时，此存储节点将暂时不可用。您应一次在一个存储节点上执行此操作步骤 ，以避免影响面向客户端的网格服务。

步骤

1. 如有必要，请安装新的存储硬件并创建新的 VMware 数据存储库。
2. 向虚拟机添加一个或多个硬盘以用作存储（对象存储）。
   a. 打开 VMware vSphere Client 。
   b. 编辑虚拟机设置以添加一个或多个附加硬盘。

   硬盘通常配置为虚拟机磁盘（ Virtual Machine Disk ， VMDK ）。VMDK 的使用更广泛，管理更方便，而 RDM 则可以为使用较大对象大小（例如大于 100 MB ）的工作负载提供更好的性能。有关向虚拟机添加硬盘的详细信息，请参见 VMware vSphere 文档。
3. 使用 VMware vSphere Client 中的 * 重新启动子操作系统 * 选项或在与虚拟机的 ssh 会话中输入以下命令来重新启动虚拟机：`sudo reboot`

   > 请勿使用 * 关闭电源 * 或 * 重置 * 重新启动虚拟机。
4. 配置新存储以供存储节点使用：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

b. 配置新存储卷：

```
sudo add_rangedbs.rb
```

此脚本将查找任何新存储卷并提示您对其进行格式化。

a. 输入 * 。 * 接受格式化。

b. 如果先前已对任何卷进行格式化，请确定是否要重新格式化这些卷。

- 输入 * y * 重新格式化。
- 输入 * 。 n* 可跳过重新格式化。

c. 当系统询问时，输入 * 。 * 以停止存储服务。

存储服务将停止， `setup_rangedbs.sh` 脚本将自动运行。在卷准备好用作卷集之后，服务将重新启动。

5. 检查服务是否正确启动：

a. 查看服务器上所有服务的状态列表：

```
sUdo storagegRid-status
```

状态将自动更新。

a. 请等待所有服务均已运行或已验证。

b. 退出状态屏幕：

```
Ctrl+C
```

6. 验证存储节点是否联机：

a. 使用登录到网格管理器 支持的 Web 浏览器。

b. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

c. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 存储 * 。

d. 选择 * 配置 * 选项卡，然后选择 * 主 * 选项卡。

e. 如果 * 存储状态 - 所需 * 下拉列表设置为只读或脱机，请选择 * 联机 * 。

f. 选择 * 应用更改 * 。

7. 要查看新对象存储，请执行以下操作：

a. 选择 * 节点 * > * 站点 _* > * 存储节点 _* > * 存储 * 。

b. 在 * 对象存储 * 表中查看详细信息。

结果

您可以使用存储节点的扩展容量来保存对象数据。

Linux：将直连卷或 SAN 卷添加到存储节点

如果某个存储节点包含的存储卷少于 16 个，则可以通过添加新的块存储设备，使其对 Linux 主机可见，并将新的块设备映射添加到用于该存储节点的 StorageGRID 配置文件来增加其容量。

您需要的内容

- 您可以访问有关为 Linux 平台安装 StorageGRID 的说明。
  - 安装 Red Hat Enterprise Linux 或 CentOS
  - 安装 Ubuntu 或 Debian
- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

> 在软件升级，恢复操作步骤 或其他扩展操作步骤 处于活动状态时，请勿尝试向存储节点添加存储卷。

关于此任务

添加存储卷时，此存储节点将暂时不可用。您应一次在一个存储节点上执行此操作步骤 ，以避免影响面向客户端的网格服务。

步骤

1. 安装新的存储硬件。

   有关详细信息，请参见硬件供应商提供的文档。

2. 创建所需大小的新块存储卷。
   - 连接新磁盘驱动器并根据需要更新 RAID 控制器配置，或者在共享存储阵列上分配新的 SAN LUN 并允许 Linux 主机访问这些 LUN 。
   - 请使用与现有存储节点上的存储卷相同的永久性命名方案。
   - 如果使用 StorageGRID 节点迁移功能，请使作为此存储节点迁移目标的其他 Linux 主机可以看到新卷。有关详细信息，请参见有关为 Linux 平台安装 StorageGRID 的说明。
3. 以 root 身份或使用具有 sudo 权限的帐户登录到支持存储节点的 Linux 主机。
4. 确认新存储卷在 Linux 主机上可见。

   您可能需要重新扫描设备。

5. 运行以下命令以临时禁用存储节点：

   ```
   sUdo StorageGRID node stop <node-name>
   ```

6. 使用 vim 或 pico 等文本编辑器编辑存储节点的节点配置文件，该文件位于 ` /etc/storaggrid/nodes/<node-name>.conf` 中。
7. 找到节点配置文件中包含现有对象存储块设备映射的部分。

   在此示例中， `block_device_RANGEDB_00` 到 `block_device_RANGEDB_03` 是现有的对象存储块设备

映射。

```
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. 添加与为此存储节点添加的块存储卷对应的新对象存储块设备映射。

   请务必从下一个 `block_device_RANGEDB_nn` 开始。请勿留下空隙。

   - 基于以上示例，从 `block_device_RANGEDB_04` 开始。
   - 在以下示例中，向节点添加了四个新的块存储卷： `block_device_RANGEDB_04` to `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. 运行以下命令以验证对存储节点的节点配置文件所做的更改：

```
sUdo StorageGRID node validate <node-name>
```

解决所有错误或警告，然后再继续下一步。

如果您发现类似以下内容的错误，则表示节点配置文件正在尝试将 ` <node-name>` for ` <utility>` 使用的块设备映射到 Linux 文件系统中的给定 ` <path-name>` 。 但该位置没有有效的块设备专用文件（或指向块设备专用文件的软链接）。

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

验证您输入的 ` <path-name>` 是否正确。

10. 运行以下命令以重新启动具有新块设备映射的节点：

```
sUdo StorageGRID node start <node-name>
```

11. 使用 `passwords.txt` 文件中列出的密码以管理员身份登录到存储节点。
12. 检查服务是否正确启动：
    a. 查看服务器上所有服务的状态列表： + `sUdo storagegRid-status`

       状态将自动更新。

    b. 请等待所有服务均已运行或已验证。
    c. 退出状态屏幕：

       ```
       Ctrl+C
       ```

13. 配置新存储以供存储节点使用：
    a. 配置新存储卷：

       ```
       sudo add_rangedbs.rb
       ```

    此脚本将查找任何新存储卷并提示您对其进行格式化。

    a. 输入 * 。 * 格式化存储卷。
    b. 如果先前已对任何卷进行格式化，请确定是否要重新格式化这些卷。
       - 输入 * y * 重新格式化。
       - 输入 * 。 n* 可跳过重新格式化。
    c. 当系统询问时，输入 * 。 * 以停止存储服务。

       存储服务将停止， `setup_rangedbs.sh` 脚本将自动运行。在卷准备好用作卷集之后，服务将重新启动。

14. 检查服务是否正确启动：

a. 查看服务器上所有服务的状态列表：

```
sUdo storagegRid-status
```

状态将自动更新。

a. 请等待所有服务均已运行或已验证。

b. 退出状态屏幕：

```
Ctrl+C
```

15. 验证存储节点是否联机：

a. 使用登录到网格管理器 支持的 Web 浏览器。

b. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

c. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 存储 * 。

d. 选择 * 配置 * 选项卡，然后选择 * 主 * 选项卡。

e. 如果 * 存储状态 - 所需 * 下拉列表设置为只读或脱机，请选择 * 联机 * 。

f. 单击 * 应用更改 * 。

16. 要查看新对象存储，请执行以下操作：

a. 选择 * 节点 * > * 站点 _* > * 存储节点 _* > * 存储 * 。

b. 在 * 对象存储 * 表中查看详细信息。

结果

现在，您可以使用存储节点的扩展容量来保存对象数据。

添加网格节点或站点

向现有站点添加网格节点或添加新站点

您可以按照此操作步骤 向现有站点添加网格节点或添加新站点，但不能同时执行这两种类型的扩展。

您需要的内容

- 您具有 root 访问权限或维护权限。
- 网格中的所有现有节点在所有站点上均已启动且正在运行。
- 先前的任何扩展，升级，停用或恢复过程均已完成。

> 如果正在进行另一个扩展，升级，恢复或活动的停用操作步骤 ，则系统将阻止您启动扩展。但是，如有必要，您可以暂停已停用的操作步骤 以启动扩展。

步骤

1. 更新网格网络的子网。

2. 部署新的网格节点。
3. 执行扩展。

更新网格网络的子网

在扩展中添加网格节点或新站点时，您可能需要更新子网或向网格网络添加子网。

StorageGRID 会维护一个网络子网列表，用于在网格网络（ eth0 ）上的网格节点之间进行通信。这些条目包括 StorageGRID 系统中每个站点用于网格网络的子网，以及通过网格网络网关访问的 NTP ， DNS ， LDAP 或其他外部服务器所使用的任何子网。

您需要的内容

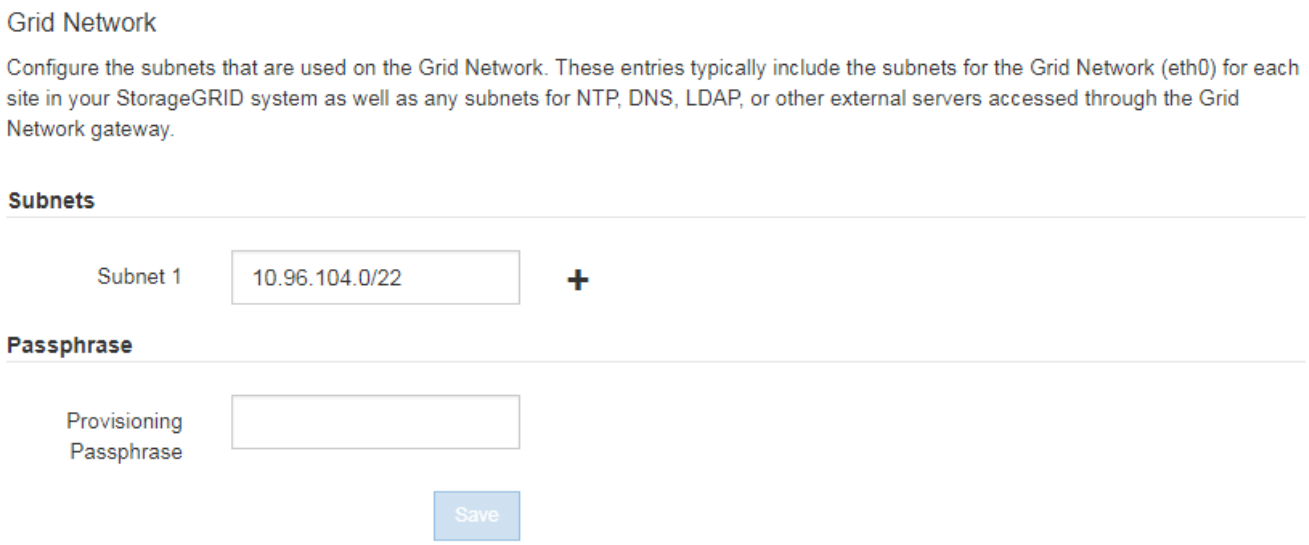
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有配置密码短语。
- 您已获得要配置的子网的网络地址，以 CIDR 表示法表示。

关于此任务

如果任何新节点的子网上有一个以前未使用的网格网络 IP 地址，则必须在开始扩展之前将此新子网添加到网格网络子网列表中。否则，您必须取消扩展，添加新子网并重新启动操作步骤 。

步骤

1. 选择 * 维护 * > * 网络 * > * 网格网络 * 。



2. 在子网列表中，选择加号以 CIDR 表示法添加新子网。

   例如，输入 10.96.104.0/22 。

3. 输入配置密码短语，然后选择 * 保存 * 。

   您指定的子网将自动为 StorageGRID 系统配置。

部署新的网格节点

在扩展中部署新网格节点的步骤与首次安装网格时使用的步骤相同。您必须先部署所有新的网格节点，然后才能执行扩展。

扩展网格时，您添加的节点不必与现有节点类型匹配。您可以添加 VMware 节点，基于 Linux 容器的节点或设备节点。

VMware： 部署网格节点

您必须在 VMware vSphere 中为要添加到扩展中的每个 VMware 节点部署一个虚拟机。

步骤

1. 将新节点部署为虚拟机 并将其连接到一个或多个 StorageGRID 网络。

   部署节点时，您可以选择重新映射节点端口或增加 CPU 或内存设置。

2. 部署所有新的 VMware 节点后， 执行扩展操作步骤。

Linux： 部署网格节点

您可以在新的 Linux 主机或现有的 Linux 主机上部署网格节点。如果您需要更多的 Linux 主机来满足要添加到网格中的 StorageGRID 节点的 CPU ， RAM 和存储要求，请按照首次安装主机时准备主机的方式对其进行准备。然后，按照安装期间部署网格节点的方式部署扩展节点。

您需要的内容

- 您已获得有关为您的 Linux 版本安装 StorageGRID 的说明，并已查看硬件和存储要求。
  - 安装 Red Hat Enterprise Linux 或 CentOS
  - 安装 Ubuntu 或 Debian
- 如果您计划在现有主机上部署新的网格节点，则已确认现有主机具有足够的 CPU ， RAM 和存储容量来容纳其他节点。
- 您计划最大限度地减少故障域。例如，不应将所有网关节点部署在一个物理主机上。

  在生产部署中，请勿在一个物理或虚拟主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

- 如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

步骤

1. 如果要添加新主机，请访问有关部署 StorageGRID 节点的安装说明。
2. 要部署新主机，请按照说明准备主机。
3. 要创建节点配置文件并验证 StorageGRID 配置，请按照有关部署网格节点的说明进行操作。
4. 如果要向新的 Linux 主机添加节点，请启动 StorageGRID 主机服务。
5. 如果要向现有 Linux 主机添加节点，请使用 StorageGRID 主机服务命令行界面启动新节点：`sUdo StorageGRID node start <<` 节点名称 `\>>`

完成后

部署所有新网格节点后，您可以 执行扩展。

设备：部署存储，网关或非主管理节点

要在设备节点上安装 StorageGRID 软件，请使用设备中提供的 StorageGRID 设备安装程序。在扩展中，每个存储设备都充当一个存储节点，而每个服务设备则充当一个网关节点或非主管理节点。任何设备都可以连接到网格网络，管理网络和客户端网络。

您需要的内容

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 您已使用 StorageGRID 设备安装程序完成设备安装和维护说明中的所有 "`configure hardware` " 步骤。
  - SG100 和 SG1000 服务设备
  - 配置硬件（ SG5600 ）
  - 配置硬件（ SG5700 ）
  - 配置硬件（ SG6000 ）

  配置设备硬件包括配置 StorageGRID 连接（网络链路和 IP 地址）所需的步骤，以及启用节点加密，更改 RAID 模式和重新映射网络端口的可选步骤。
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 替代设备上的 StorageGRID 设备安装程序固件与网格上当前运行的 StorageGRID 软件版本兼容。例如，StorageGRID 设备安装程序 3.6 版与 StorageGRID 11.6 版兼容。（如果版本不兼容，则必须升级 StorageGRID 设备安装程序固件。）
- 您的服务笔记本电脑具有 支持的 Web 浏览器。
- 您知道分配给设备计算控制器的一个 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。

关于此任务

在设备节点上安装 StorageGRID 的过程分为以下阶段：

- 您可以指定或确认主管理节点的 IP 地址以及设备节点的名称。
- 您开始安装，并等待卷配置完毕并安装软件。

  在执行设备安装任务时，安装将暂停。要恢复安装，请登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装过程。

> 如果您需要一次部署多个设备节点，则可以使用 `configure-sGa.py` 设备安装脚本自动执行安装过程。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

   `https://Controller_IP:8443`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在 * 主管理节点 * 连接部分中，确定是否需要指定主管理节点的 IP 地址。

   如果先前已在此数据中心中安装了其他节点，则 StorageGRID 设备安装程序可以自动发现此 IP 地址，前提是主管理节点或至少一个配置了 admin_IP 的其他网格节点位于同一子网上。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 等待连接状态，使新 IP 地址准备就绪。
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 等待显示发现的 IP 地址列表。 c. 为要部署此设备存储节点的网格选择主管理节点。 d. 单击 * 保存 * 。 e. 等待连接状态，使新 IP 地址准备就绪。

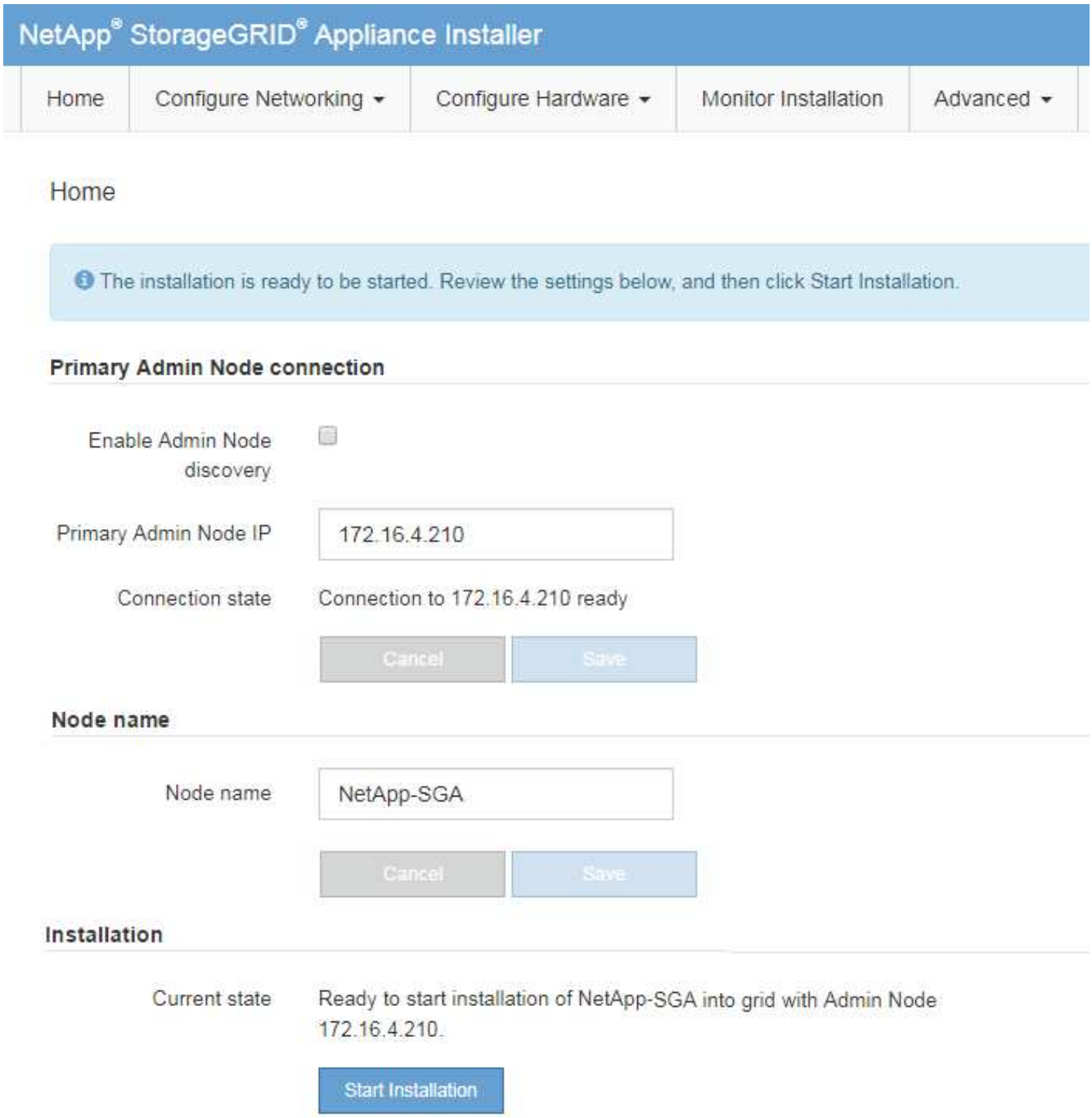
4. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后选择 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的节点页面（概述选项卡）上。如果需要，您可以在批准节点时更改名称。

5. 在 * 安装 * 部分中，确认当前状态为 "`Ready to start installation of *node name* into grid with primary Admin Node *admin_ip*` " ，并且 * 开始安装 * 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

6. 从 StorageGRID 设备安装程序主页中，选择 * 开始安装 * 。



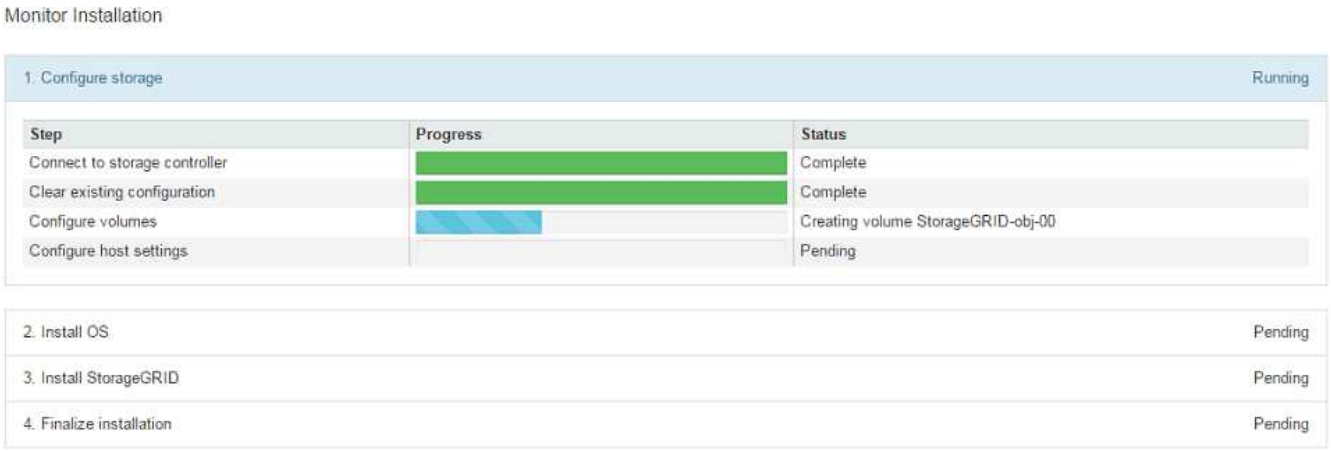
当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

7. 如果扩展包含多个设备节点，请对每个设备重复上述步骤。

   如果您需要一次部署多个设备存储节点，则可以使用 configure-sga.py 设备安装脚本自动执行安装过程。

8. 如果需要手动访问监控器安装页面，请从菜单栏中选择 * 监控器安装 * 。

   "Monitor Installation" 页面将显示安装进度。



蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

> 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

9. 查看前两个安装阶段的进度。

   ◦ 。配置设备 *

   在此阶段，将执行以下过程之一：

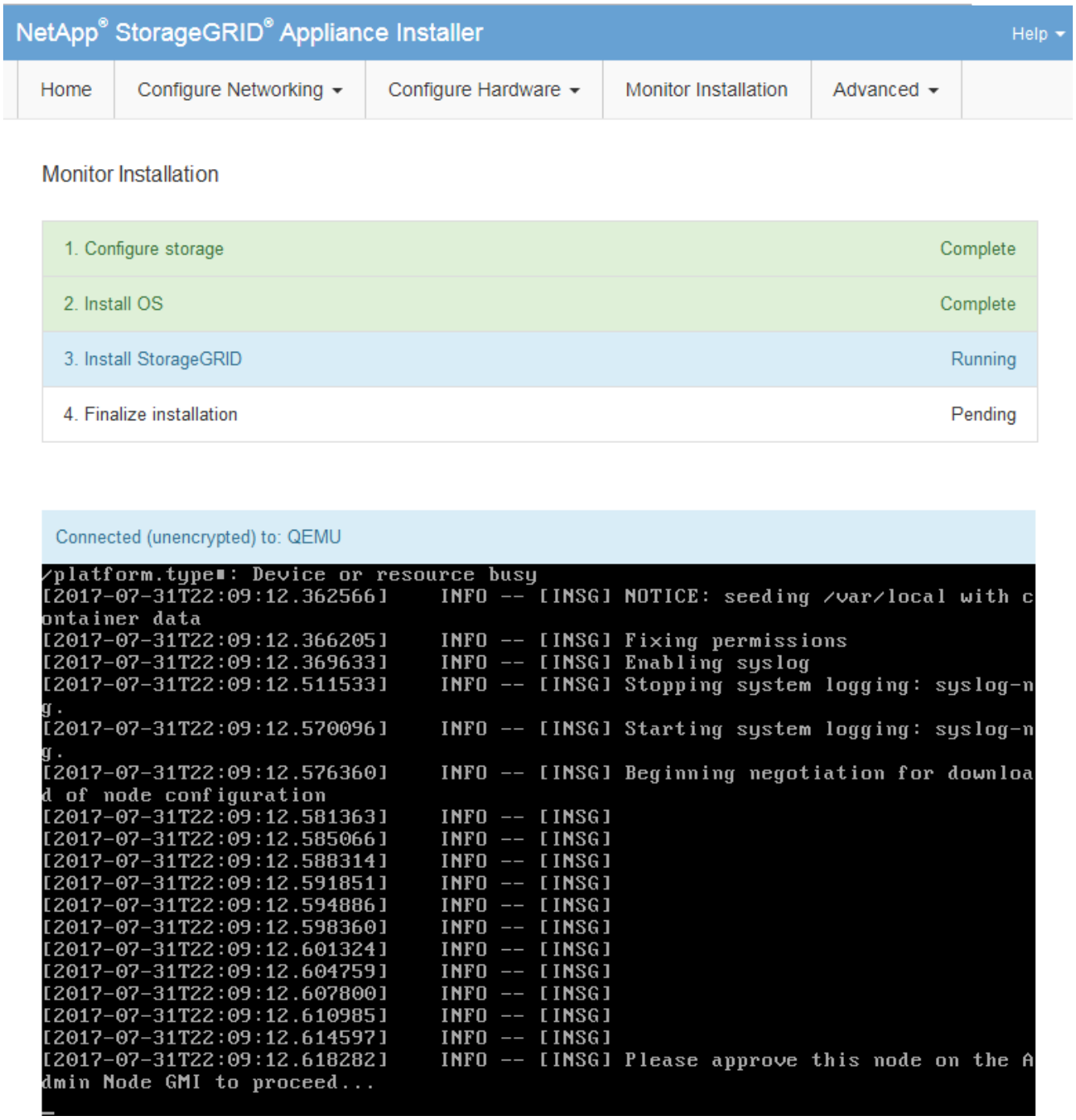
   - 对于存储设备，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。
   - 对于服务设备，安装程序将从计算控制器中的驱动器中清除任何现有配置，并配置主机设置。

   ◦ 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

10. 继续监控安装进度，直到控制台窗口显示一条消息，提示您使用网格管理器批准节点。

> 等待您在此扩展中添加的所有节点都准备好进行批准，然后再转到网格管理器来批准这些节点。



执行扩展

执行扩展时，新的网格节点将添加到现有 StorageGRID 部署中。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有配置密码短语。
- 您已部署要在此扩展中添加的所有网格节点。

- 如果您要添加存储节点，则已确认在恢复过程中执行的所有数据修复操作均已完成。请参见 检查数据修复作业。
- 如果要添加新站点，则必须在启动扩展操作步骤 之前查看和更新 ILM 规则，以确保在扩展完成之前不会将对象副本存储到新站点。例如，如果某个规则使用默认存储池（所有存储节点），则必须创建一个仅包含现有存储节点的新存储池，并更新 ILM 规则以使用新存储池。否则，一旦新站点上的第一个节点变为活动状态，对象就会复制到该站点。请参见的说明 使用 ILM 管理对象。

关于此任务

执行扩展包括以下阶段：

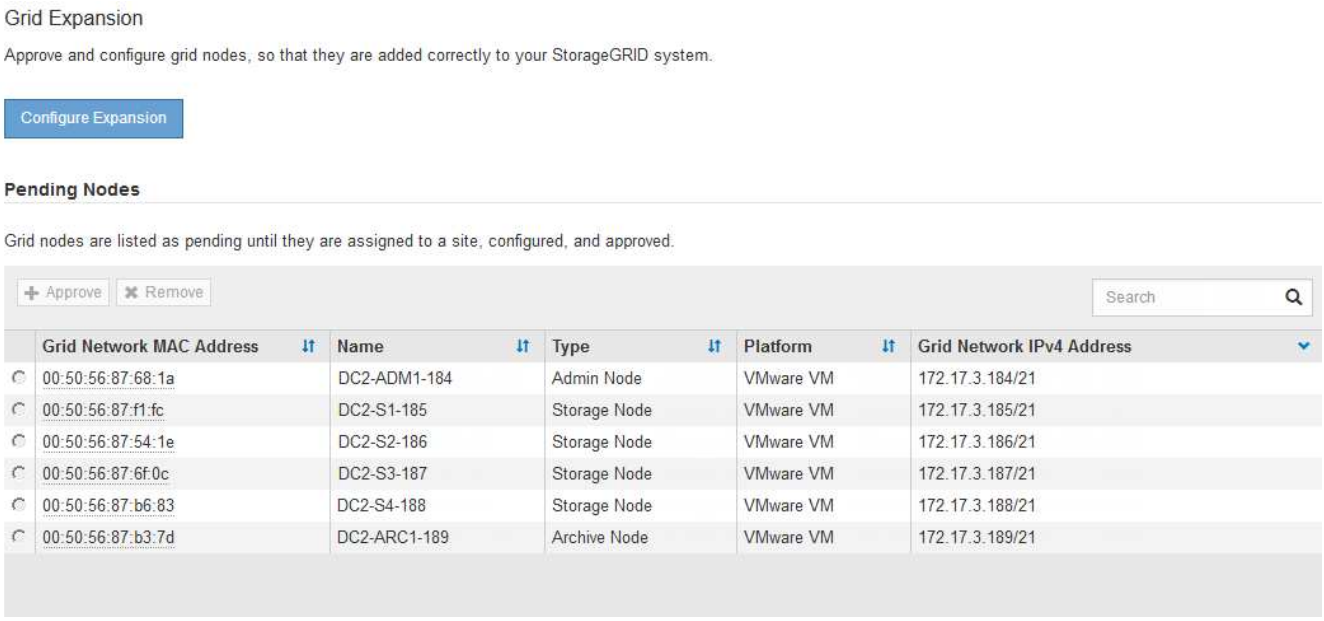
1. 您可以通过指定是添加新网格节点还是添加新站点并批准要添加的网格节点来配置扩展。
2. 开始扩展。
3. 在扩展过程运行期间，您会下载一个新的恢复软件包文件。
4. 您可以监控网格配置阶段的状态，这些配置阶段会自动运行。阶段集取决于要添加的网格节点类型以及是否要添加新站点。

> 在大型网格上运行某些阶段可能需要大量时间。例如，如果 Cassandra 数据库为空，则将 Cassandra 流式传输到新存储节点可能只需要几分钟的时间。但是，如果 Cassandra 数据库包含大量对象元数据，则此阶段可能需要数小时或更长时间。请勿在 " 扩展 Cassandra 集群 " 或 " 启动 Cassandra 和流式数据 " 阶段重新启动任何存储节点。

步骤

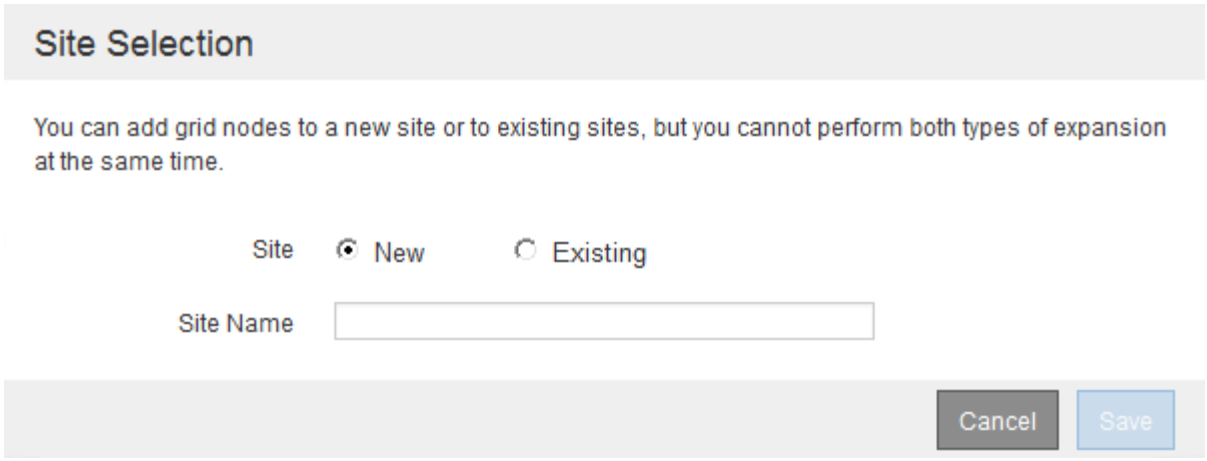
1. 选择 * 维护 * > * 任务 * > * 扩展 * 。

   此时将显示网格扩展页面。"Pending Nodes" 部分列出了准备添加的所有节点。



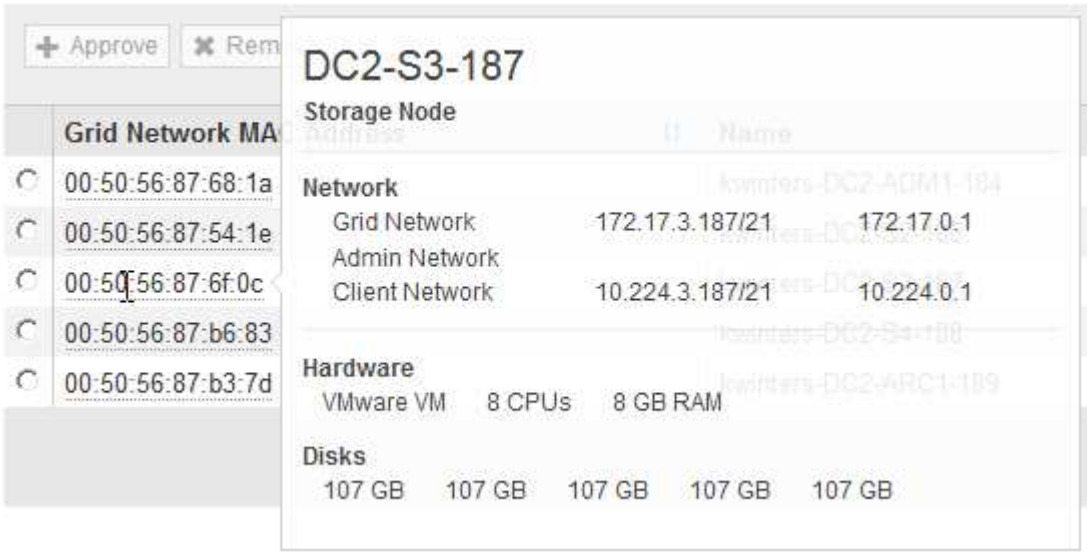
2. 选择 * 配置扩展 * 。

   此时将显示站点选择对话框。



3. 选择要启动的扩展类型：
   - 如果要添加新站点，请选择 * 新建 * ，然后输入新站点的名称。
   - 如果要向现有站点添加网格节点，请选择 * 现有 * 。
4. 选择 * 保存 * 。
5. 查看 * 待定节点 * 列表，并确认它显示了您部署的所有网格节点。

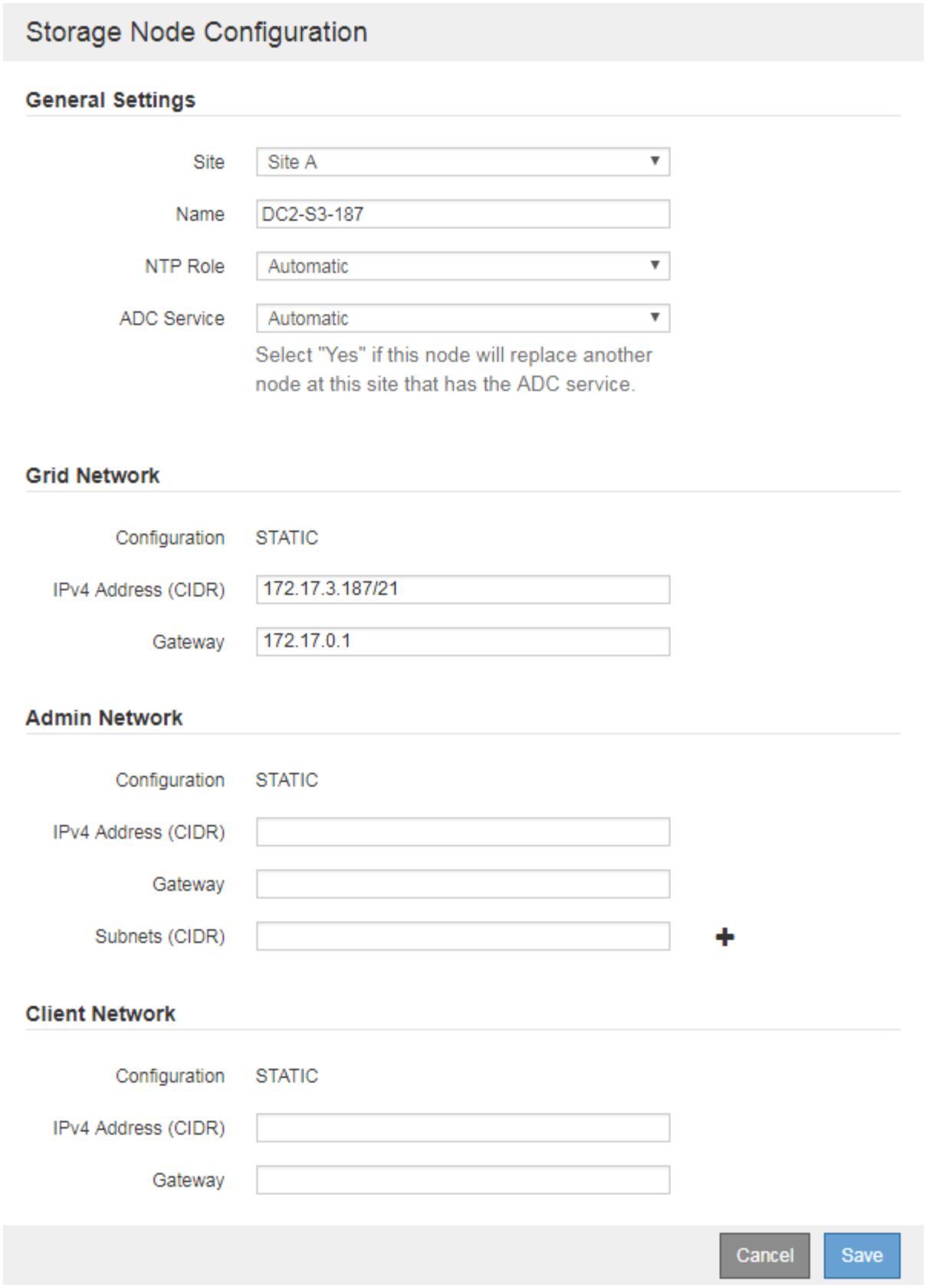
   根据需要，您可以将光标悬停在节点的 * 网格网络 MAC 地址 * 上以查看有关该节点的详细信息。



如果缺少网格节点，请确认已成功部署该节点。

6. 从待定节点列表中，批准此扩展的网格节点。
   a. 选择要批准的第一个待定网格节点旁边的单选按钮。
   b. 选择 * 批准 * 。

      此时将显示网格节点配置表单。



c. 根据需要修改常规设置：

- * 站点 * ：要与网格节点关联的站点的名称。如果要添加多个节点，请确保为每个节点选择正确的站点。如果要添加新站点，则所有节点都将添加到新站点。

- * 名称 * ：将分配给节点的主机名以及将在网格管理器中显示的名称。
- * NTP 角色 * ：网格节点的网络时间协议（ NTP ）角色。选项包括 * 自动 * ， * 主 * 和 * 客户端 * 。选择 * 自动 * 会将主角色分配给管理节点，具有模板转换服务的存储节点，网关节点以及具有非静态 IP 地址的任何网格节点。所有其他网格节点都分配有客户端角色。

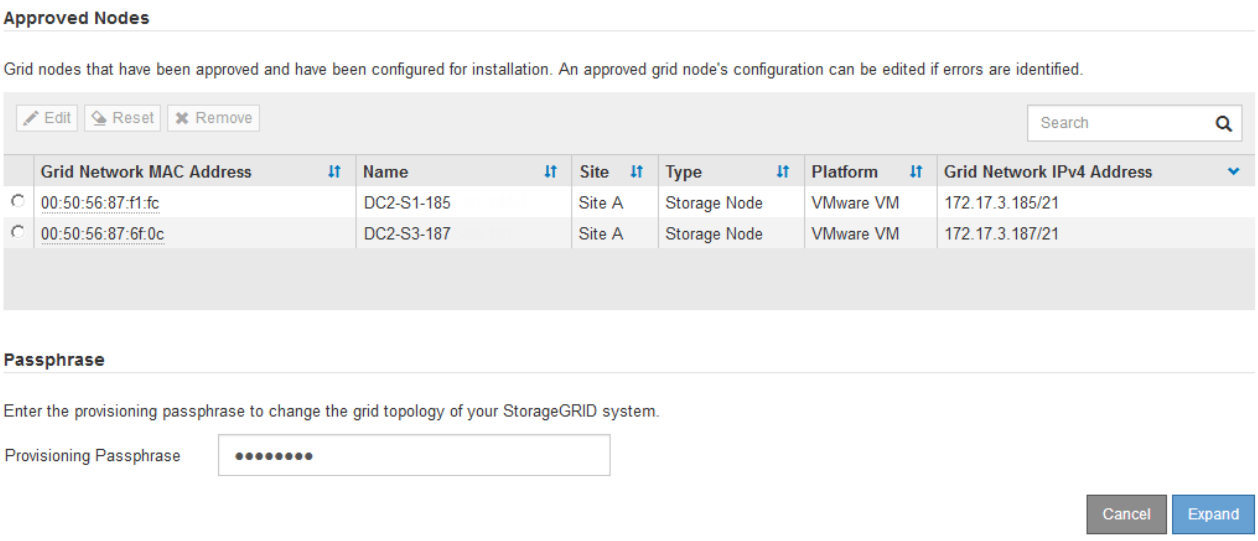
  > 将主 NTP 角色分配给每个站点上至少两个节点。这样，系统便可对外部计时源进行冗余访问。

- * ADC* 服务 * （仅限存储节点）：此存储节点是否将运行管理域控制器（ ADC-A ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。每个站点至少有三个存储节点必须包含此 ADC-Service 。在部署此节点后，您不能将此 ADC 服务添加到该节点中。
  - 如果要添加此节点以替换存储节点，请选择 * 是 * ，前提是要替换的节点包含此 ADA 服务。由于如果仍会保留的 ADD 服务太少，则无法停用存储节点，因此，这样可以确保在删除旧服务之前新的 ADD 服务可用。
  - 否则，请选择 * 自动 * 以让系统确定此节点是否需要使用此 ADC-Service 。了解有关模数转换器仲裁的信息 此处。

d. 根据需要修改网格网络，管理网络和客户端网络的设置。
   - * IPv4 地址（ CIDR ） * ：网络接口的 CIDR 网络地址。例如： 172.16.10.100/24
   - * 网关 * ：网格节点的默认网关。例如： 172.16.10.1
   - * 子网（ CIDR ） * ：管理网络的一个或多个子网。

e. 选择 * 保存 * 。

   批准的网格节点将移至批准的节点列表。



   - 要修改已批准的网格节点的属性，请选择其单选按钮，然后选择 * 编辑 * 。
   - 要将已批准的网格节点移回 "Pending Nodes" 列表，请选择其单选按钮，然后选择 * 重置 * 。
   - 要永久删除已批准的网格节点，请关闭此节点。然后，选择其单选按钮并选择 * 删除 * 。

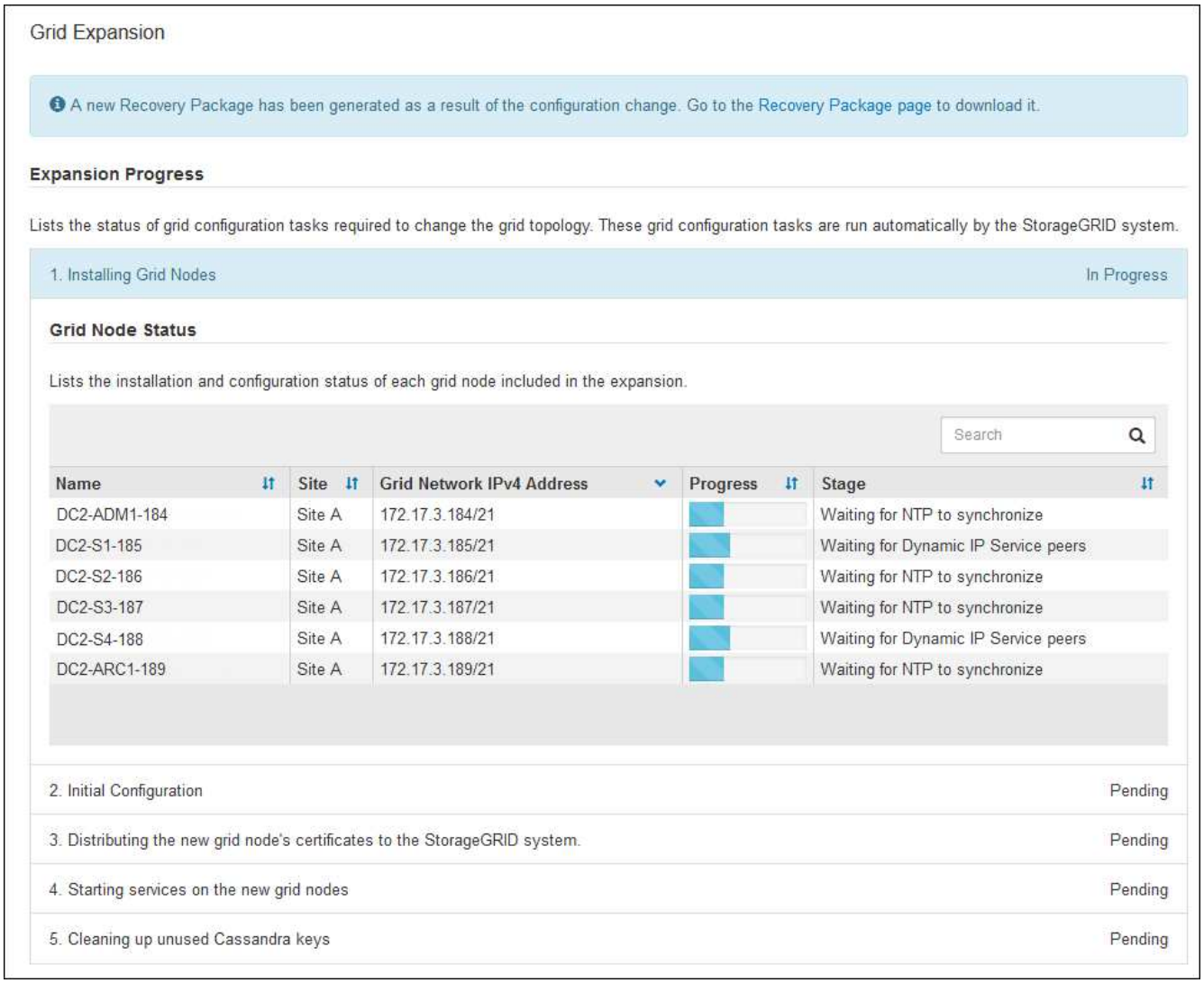
f. 对要批准的每个待定网格节点重复上述步骤。

如果可能，您应批准所有待定网格注释并执行一次扩展。如果执行多个小型扩展，则需要更多时间。

7. 批准所有网格节点后，输入 * 配置密码短语 * ，然后选择 * 扩展 * 。

几分钟后，此页面将更新以显示扩展操作步骤 的状态。如果正在执行影响单个网格节点的任务，则网格节点状态部分将列出每个网格节点的当前状态。

在此过程中，对于设备， StorageGRID 设备安装程序会显示安装从第 3 阶段移至第 4 阶段 " 完成安装 " 。阶段 4 完成后，控制器将重新启动。



站点扩展包括一项额外任务，用于为新站点配置 Cassandra 。

8. 显示 * 下载恢复包 * 链接后，立即下载恢复包文件。

在对 StorageGRID 系统进行网格拓扑更改后，您必须尽快下载恢复包文件的更新副本。通过恢复包文件，您可以在发生故障时还原系统。

a. 选择下载链接。

b. 输入配置密码短语，然后选择 * 开始下载 * 。

c. 下载完成后，打开 ` .zip` 文件并确认其中包含 `gpt 备份` 目录和 ` sed_said.zip` 文件。然后，提取 ` sa_sid.zip` 文件，转到 ` /GID* _REV*` 目录，确认您可以打开 `passwords.txt` 文件。

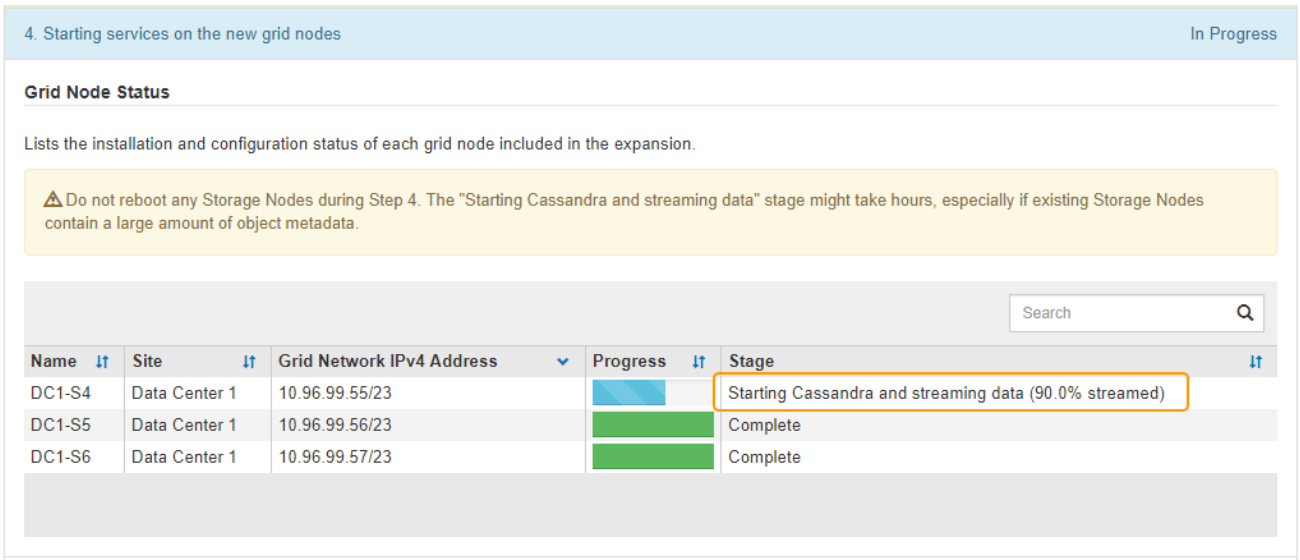
d. 将下载的恢复软件包文件（ .zip ）复制到两个安全的单独位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

9. 按照说明向现有站点添加存储节点或添加新站点。

将存储节点添加到现有站点

如果要向现有站点添加一个或多个存储节点，请查看状态消息中显示的百分比，以监控 " 启动 Cassandra 和流式传输数据 " 阶段的进度。



此百分比根据可用的 Cassandra 数据总量以及已写入新节点的数据量估计 Cassandra 流操作的完成程度。

> 请勿在 " 扩展 Cassandra 集群 " 或 " 启动 Cassandra 和流式数据 " 阶段重新启动任何存储节点。对于每个新存储节点，这些阶段可能需要花费数小时才能完成，尤其是在现有存储节点包含大量对象元数据的情况下。

添加新站点

如果要添加新站点，请使用 `nodetool status` 监控 Cassandra 流式传输的进度，并查看在 " 扩展 Cassandra 集群 " 阶段已向新站点复制多少元数据。新站点上的总数据负载应介于当前站点总负载的 20% 左右。

> 请勿在 " 扩展 Cassandra 集群 " 或 " 启动 Cassandra 和流式数据 " 阶段重新启动任何存储节点。对于每个新存储节点，这些阶段可能需要花费数小时才能完成，尤其是在现有存储节点包含大量对象元数据的情况下。

1. 继续监控扩展，直到所有任务均完成，并且 * 配置扩展 * 按钮再次出现。

完成后

根据您添加的网格节点类型，您必须执行其他集成和配置步骤。请参见 扩展后的配置步骤。

配置扩展系统

扩展后的配置步骤

完成扩展后，您必须执行其他集成和配置步骤。

关于此任务

您必须为要在扩展中添加的网格节点完成以下列出的配置任务。根据在安装和管理系统时选择的选项以及您希望如何配置在扩展期间添加的网格节点，某些任务可能是可选的。

步骤

1. 如果添加了存储节点，请完成以下配置任务：
   a. 查看 ILM 规则中使用的存储池，以确保使用新存储。请参见 使用 ILM 管理对象。
      - 如果您添加了站点，请为此站点创建一个存储池，并更新 ILM 规则以使用新的存储池。
      - 如果已将存储节点添加到现有站点，请确认新节点使用的存储级别正确。

      默认情况下，系统会将新的存储节点分配给所有存储节点存储级别，并将其添加到对站点使用该级别的存储池中。如果您希望新节点使用自定义存储级别，则必须手动将其分配给自定义级别（ * ILM * > * 存储级别 * ）。

   b. 验证存储节点是否正在载入对象。请参见 验证存储节点是否处于活动状态。
   c. 重新平衡擦除编码的数据（仅当无法添加建议数量的存储节点时）。请参见添加存储节点后重新平衡经过纠删编码的数据。
2. 如果添加了网关节点，请完成以下配置任务：
   - 如果将高可用性（ HA ）组用于客户端连接，则可以选择将网关节点添加到 HA 组。选择 * 配置 * > * 网络 * > * 高可用性组 * 以查看现有 HA 组列表并添加新节点。请参见 管理 StorageGRID。
3. 如果添加了管理节点，请完成以下配置任务：
   a. 如果为 StorageGRID 系统启用了单点登录（ Single Sign-On ， SSO ），请为新管理节点创建依赖方信任。创建此依赖方信任之前，您无法登录到此节点。请参见配置单点登录。
   b. 如果您计划在管理节点上使用负载平衡器服务、则可以选择将新的管理节点添加到HA组。选择*配置*网络高可用性组*以查看现有HA组列表并添加新节点。请参见 管理 StorageGRID。
   c. 如果要使每个管理节点上的属性和审核信息保持一致，也可以将管理节点数据库从主管理节点复制到扩展管理节点。请参见 复制管理节点数据库。
   d. 如果要使每个管理节点上的历史指标保持一致，也可以将 Prometheus 数据库从主管理节点复制到扩展管理节点。请参见 复制 Prometheus 指标。
   e. 如果要使每个管理节点上的历史日志信息保持一致，也可以将现有审核日志从主管理节点复制到扩展管理节点。请参见 复制审核日志。
   f. 或者，也可以通过 NFS 或 CIFS 文件共享配置对系统的访问以供审核。请参见 管理 StorageGRID。

      已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

g. 或者，也可以更改通知的首选发件人。您可以将扩展管理节点设置为首选发送器。否则，配置为首选发件人的现有管理节点将继续发送通知，包括 AutoSupport 消息， SNMP 通知，警报电子邮件和警报电子邮件（旧系统）。请参见 管理 StorageGRID。

4. 如果添加了归档节点，请完成以下配置任务。

   a. 配置归档节点与目标外部归档存储系统的连接。完成扩展后，归档节点将处于警报状态，直到您通过 * ARC/ * 目标 * 组件配置连接信息为止。请参见 管理 StorageGRID。

   b. 更新 ILM 策略以通过新的归档节点归档对象数据。请参见 使用 ILM 管理对象。

   c. 为用于监控从归档节点检索对象数据的速度和效率的属性配置自定义警报。请参见 管理 StorageGRID。

5. 要检查扩展节点是否是使用不可信客户端网络添加的，或者更改节点的客户端网络是不可信还是可信，请转到 * 配置 * > * 网络 * > * 不可信客户端网络 * 。

   如果扩展节点上的客户端网络不可信，则必须使用负载平衡器端点与客户端网络上的节点建立连接。请参见 管理 StorageGRID。

6. 配置域名系统（ DNS ）。

   如果您一直在为每个网格节点单独指定 DNS 设置，则必须为新节点添加自定义的每节点 DNS 设置。请参见 修改单网格节点的 DNS 配置。

   最佳做法是，网格范围的 DNS 服务器列表应包含一些可从每个站点本地访问的 DNS 服务器。如果您刚刚添加了一个新站点，请将该站点的新 DNS 服务器添加到网格范围的 DNS 配置中。

   > 为 DNS 服务器提供两到六个 IPv4 地址。您应选择 DNS 服务器，以便在网络隔离时每个站点都可以在本地访问这些服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以进一步自定义每个节点的 DNS 服务器列表。有关详细信息，请参见 修改单网格节点的 DNS 配置…

7. 如果添加了新站点，请确认网络时间协议（ NTP ）服务器可从该站点访问。请参见 配置 NTP 服务器。

   > 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

验证存储节点是否处于活动状态

添加新存储节点的扩展操作完成后， StorageGRID 系统应自动开始使用新存储节点。您必须使用 StorageGRID 系统验证新存储节点是否处于活动状态。

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 节点 * > * 扩展存储节点 _* > * 存储 * 。
3. 将光标悬停在 * 已用存储 - 对象数据 * 图上可查看 * 已用 * 的值，即已用于对象数据的总可用空间量。
4. 将光标移至图形右侧时，请验证 * 已用 * 的值是否正在增加。

复制管理节点数据库

通过扩展操作步骤 添加管理节点时，您可以选择将数据库从主管理节点复制到新的管理节点。通过复制数据库，您可以保留有关属性，警报和警报的历史信息。

您需要的内容

- 您已完成添加管理节点所需的扩展步骤。
- 您已有 `passwords.txt` 文件。
- 您具有配置密码短语。

关于此任务

StorageGRID 软件激活过程会在扩展管理节点上为 NMS 服务创建一个空数据库。当 NMS 服务在扩展管理节点上启动时，它会记录当前属于系统的服务器和服务的信息或稍后添加的服务器和服务的信息。此管理节点数据库包含以下信息：

- 警报历史记录
- 警报历史记录
- 历史属性数据，用于 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的图表和文本报告

为了确保管理节点数据库在节点之间保持一致，您可以将数据库从主管理节点复制到扩展管理节点。

> 将数据库从主管理节点（ _source 管理节点 _ ）复制到扩展管理节点可能需要数小时才能完成。在此期间，无法访问网格管理器。

在复制数据库之前，请按照以下步骤停止主管理节点和扩展管理节点上的 MI 服务和管理 API 服务。

步骤

1. 在主管理节点上完成以下步骤：
   a. 登录到管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 运行以下命令： `re封面访问点`
   c. 输入配置密码短语。
   d. 停止 MI 服务： `service mi stop`
   e. 停止管理应用程序接口（ mgmt-api ）服务： `service mgmt-api stop`
2. 在扩展管理节点上完成以下步骤：
   a. 登录到扩展管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。

b. 停止 MI 服务： `service mi stop`

c. 停止 mgmt-api 服务： `service mgmt-api stop`

d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

e. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

f. 将数据库从源管理节点复制到扩展管理节点： ` /usr/local/mi/bin/mi-clone-db.sh *Source_Admin_Node_IP*`

g. 出现提示时，确认要覆盖扩展管理节点上的 MI 数据库。

数据库及其历史数据将复制到扩展管理节点。完成复制操作后，此脚本将启动扩展管理节点。

h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

3. 在主管理节点上重新启动服务： `service servermanager start`

复制 **Prometheus** 指标

添加新的管理节点后，您可以选择将 Prometheus 维护的历史指标从主管理节点复制到新的管理节点。复制指标可确保管理节点之间的历史指标一致。

您需要的内容

- 新管理节点已安装并正在运行。
- 您已有 `passwords.txt` 文件。
- 您具有配置密码短语。

关于此任务

添加管理节点时，软件安装过程会创建一个新的 Prometheus 数据库。您可以通过将 Prometheus 数据库从主管理节点（ _source 管理节点 _ ）复制到新管理节点来保持节点之间的历史指标一致。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：

a. 输入以下命令： `ssh admin@ grid_node_ip_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

2. 从源管理节点中，停止 Prometheus 服务： `sservice Prometheus stop`

3. 在新管理节点上完成以下步骤：

a. 登录到新的管理节点：

   i. 输入以下命令： `ssh admin@ grid_node_ip_`

   ii. 输入 `passwords.txt` 文件中列出的密码。

   iii. 输入以下命令切换到 root： `su -`

   iv. 输入 `passwords.txt` 文件中列出的密码。

b. 停止 Prometheus 服务： `sservice Prometheus stop`

c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

d. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

e. 将 Prometheus 数据库从源管理节点复制到新的管理节点： ` /usr/local/Prometheus/bin/prometheus-clone-db.sh *Source_Admin_Node_IP*`

f. 出现提示时，按 * 输入 * 确认要销毁新管理节点上的新 Prometheus 数据库。

   原始 Prometheus 数据库及其历史数据将复制到新的管理节点。完成复制操作后，此脚本将启动新的管理节点。此时将显示以下状态：

`d`已克隆数据库，正在启动服务

a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入 …

   ```
   ssh-add -D
   ```

4. 在源管理节点上重新启动 Prometheus 服务。

   ```
   sService Prometheus start
   ```

复制审核日志

通过扩展操作步骤 添加新管理节点时，其 AMS 服务仅会记录在加入系统后发生的事件和操作。根据需要，您可以将审核日志从先前安装的管理节点复制到新的扩展管理节点，使其与 StorageGRID 系统的其余部分保持同步。

您需要的内容

- 您已完成添加管理节点所需的扩展步骤。
- 您已有 `passwords.txt` 文件。

关于此任务

要使历史审核消息在新管理节点上可用，必须手动将审核日志文件从现有管理节点复制到扩展管理节点。

默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：

- 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
- 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。

请参见 配置审核消息和日志目标 了解详细信息。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 停止 AMS 服务以防止其创建新文件： `sservice AMS stop`
3. 重命名 `audit.log` 文件，以确保它不会覆盖要将其复制到的扩展管理节点上的文件：

   `cd /var/local/audit/export + ls -l + mv audit.log new_name.txt`
4. 将所有审核日志文件复制到扩展管理节点：

   `scp -p * ip_address ： /var/local/audit/export`
5. 如果系统提示您输入 ` /root/.ssh/id_rsa` 的密码短语，请输入 `passwords.txt` 文件中列出的主管理节点的 SSH 访问密码。
6. 还原原始的 `audit.log` 文件：

   `mv new_name.txt audit.log`
7. 启动 AMS 服务：

   s服务 AMS 开始
8. 从服务器注销：

   退出
9. 登录到扩展管理节点：
   a. 输入以下命令： `ssh admin@ expansion Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

10. 更新审核日志文件的用户和组设置：

```
cd /var/local/audit/export + chown AMS-user ： byncast *
```

11. 从服务器注销：

    退出

添加存储节点后重新平衡经过纠删编码的数据

在某些情况下，您可能需要在添加新存储节点后重新平衡经过纠删编码的数据。

您需要的内容

- 您已完成添加新存储节点的扩展步骤。
- 您已查看 重新平衡经过纠删编码的数据的注意事项。

> 只有在为站点上的一个或多个存储节点触发了 * 对象存储空间不足 * 警报且您无法添加建议数量的新存储节点时，才能执行此操作步骤 。

- 您了解此操作步骤 不会移动复制的对象数据，并且在确定将纠删编码的数据移动到何处时， EC 重新平衡操作步骤 不会考虑每个存储节点上的复制数据使用情况。
- 您已有 `passwords.txt` 文件。

关于此任务

当 EC 重新平衡操作步骤 运行时， ILM 操作以及 S3 和 Swift 客户端操作的性能可能会受到影响。因此，您只能在有限情况下执行此操作步骤 。

> EC 重新平衡操作步骤 会临时预留大量存储。可能会触发存储警报，但会在重新平衡完成后解决。如果没有足够的存储空间用于预留， EC 重新平衡操作步骤 将失败。无论操作步骤 出现故障还是成功， EC 重新平衡操作步骤 完成后都会释放存储预留。

> 如果需要超过 24 小时才能完成 EC 重新平衡操作步骤 期间用于上传对象（或对象部件）的 S3 和 Swift API 操作可能会失败。如果适用的 ILM 规则在载入时使用严格或平衡的放置方式，则长时间的 PUT 操作将失败。此时将报告以下错误：
>
> `500` 内部服务器错误

步骤

1. 【 Review object_storage]] 查看计划重新平衡的站点的当前对象存储详细信息。
   a. 选择 * 节点 * 。
   b. 选择站点上的第一个存储节点。
   c. 选择 * 存储 * 选项卡。
   d. 将光标悬停在 " 已用存储 - 对象数据 " 图表上，可查看存储节点上当前复制的数据量以及经过纠删编码的数据。

e. 重复上述步骤以查看站点上的其他存储节点。

2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

3. 输入以下命令：

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

   对于 ` "site-name"` ，请指定添加新存储节点的第一个站点。请用引号将 `site-name` 括起来。

   此时将启动 EC 重新平衡操作步骤 ，并返回作业 ID 。

4. 复制作业 ID 。
5. 监控 EC 重新平衡操作步骤 的状态。
   - 要查看单个 EC 重新平衡操作步骤 的状态，请执行以下操作：

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

     对于 ` 作业 ID` ，指定启动操作步骤 时返回的 ID 。
   - 要查看当前 EC 重新平衡操作步骤 的状态以及先前完成的任何过程：

     ```
     rebalance-data status
     ```

     > 要获取有关 rebalance-data 命令的帮助，请执行以下操作：
     >
     > ```
     > rebalance-data — help
     > ```

   - 要查看当前作业的估计完成时间和完成百分比，请选择 * 支持 * > * 工具 * > * 指标 * 。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
6. 根据返回的状态执行其他步骤：
   - 如果状态为 `In progress` ，则 EC 重新平衡操作仍在运行。您应定期监控操作步骤 ，直到其完成。
   - 如果状态为 `failure` ，请执行 失败步骤。
   - 如果状态为 `Success` ，请执行 成功步骤。
7. 如果 EC 重新平衡操作步骤 生成的负载过多（例如，载入操作受到影响），请暂停操作步骤 。

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

8. 如果您需要终止 EC 重新平衡操作步骤 （例如，以便执行 StorageGRID 软件升级），请输入以下内容：

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

   > 终止 EC 重新平衡操作步骤 后，已移动的所有数据片段都将保留在新位置。数据不会移回原始位置。

9. 【 rebalance_fail 】如果 EC 重新平衡操作步骤 的状态为 `failure` ，请执行以下步骤：
   a. 确认站点上的所有存储节点均已连接到网格。
   b. 检查并解决可能影响这些存储节点的任何警报。

      有关特定警报的信息，请参见监控和故障排除说明。

   c. 重新启动 EC 重新平衡操作步骤： + `rebalance-data start – -job-id job-id`
   d. 如果 EC 重新平衡操作步骤 的状态仍为 `Failure` ，请联系技术支持。
10. `SEC` 重新平衡操作步骤 的状态为 " 无 `ccess` "（可选） 查看对象存储 以查看此站点的更新详细信息。

    现在，经过纠删编码的数据应在站点的存储节点之间更加平衡。

11. 如果要在多个站点上使用纠删编码，请对所有其他受影响站点运行此操作步骤 。

请联系技术支持

如果您在网格扩展过程中遇到无法解决的错误，或者网格任务失败，请联系技术支持。

关于此任务

联系技术支持时，您必须提供所需的日志文件，以帮助您解决遇到的错误。

步骤

1. 连接到发生故障的扩展节点：
   a. 输入以下命令：`ssh -p 8022 admin@ grid_node_ip_`

      > 端口 8022 是基础操作系统的 SSH 端口，而端口 22 是运行 StorageGRID 的容器引擎的 SSH 端口。

   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录后，提示符将从 ` $` 更改为 ` #` 。

2. 根据安装达到的阶段，检索网格节点上提供的以下任何日志：

平台	日志
VMware	• ` /var/log/daemon 。 log` • ` /var/log/storaggrid/daema.log` • ` /var/log/storaggrid/nodes/<node-name>.log`
Linux	• ` /var/log/storaggrid/daema.log` • ` /etc/storaggrid/nodes/<node-name>.conf` （对于每个故障节点） • ` /var/log/storaggrid/nodes/<node-name>.log` （对于每个故障节点，可能不存在）

恢复和维护

恢复和维护：概述

按照以下说明维护 StorageGRID 系统并从故障中恢复。

关于这些说明

这些说明介绍如何应用软件修补程序，恢复网格节点，恢复故障站点，停用网格节点或整个站点，执行网络维护，执行主机级别和中间件维护过程以及执行网格节点过程。

> 在这些说明中， "`Linux` " 是指 Red Hat ® Enterprise Linux ® ， Ubuntu ® ， CentOS 或 Debian ® 部署。使用 "NetApp 互操作性表工具" 以获取支持的版本列表。

开始之前

- 您对 StorageGRID 系统有着广泛的了解。
- 您已查看 StorageGRID 系统的拓扑并了解网格配置。
- 您知道必须严格按照所有说明进行操作，并注意所有警告。
- 您了解，不支持未介绍的维护过程或需要服务参与。

设备的维护过程

有关硬件过程，请参见 StorageGRID 设备的安装和维护说明。

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

下载恢复包

通过恢复包文件，您可以在发生故障时还原 StorageGRID 系统。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有配置密码短语。
- 您必须具有特定的访问权限。

在对 StorageGRID 系统进行网格拓扑更改之前或升级软件之前，请下载当前的恢复软件包文件。然后，在更改网格拓扑或升级软件后下载恢复包的新副本。

步骤

1. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
2. 输入配置密码短语，然后选择 * 开始下载 * 。

   下载将立即开始。

3. 下载完成后：
   a. 打开 ` .zip` 文件。
   b. 确认它包含 GPT-backup 目录和内部 ` .zip` 文件。
   c. 提取内部 ` .zip` 文件。
   d. 确认您可以打开 `passwords.txt` 文件。
4. 将下载的恢复软件包文件（` .zip` ）复制到两个安全的单独位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

相关信息

管理 StorageGRID

StorageGRID 热修补程序操作步骤

如果检测到软件问题并在功能版本之间得到解决，则可能需要将修补程序应用于 StorageGRID 系统。

StorageGRID 修补程序包含在功能或修补程序版本之外进行的软件更改。未来版本也会进行同样的更改。此外，每个热修补程序版本都包含此功能或修补程序版本中所有以前的修补程序的汇总。

应用修补程序的注意事项

应用修补程序时，系统会对 StorageGRID 系统中的节点应用累积系列软件更新。

当另一个维护操作步骤 正在运行时，您无法应用 StorageGRID 修补程序。例如，在停用，扩展或恢复操作步骤正在运行时，您无法应用修补程序。

如果节点或站点停用操作步骤 已暂停，您可以安全地应用修补程序。此外，您还可以在 StorageGRID 升级操作步骤 的最后阶段应用修补程序。有关详细信息，请参见有关升级 StorageGRID 软件的说明。

在网格管理器中上传此修补程序后，此修补程序将自动应用于主管理节点。然后，您可以批准将此修补程序应用于 StorageGRID 系统中的其余节点。

如果某个修补程序无法应用到一个或多个节点，则失败的原因将显示在该修补程序进度表的详细信息列中。您必须解决导致失败的任何问题，然后重试整个过程。先前已成功应用此修补程序的节点将在后续应用程序中跳过。您可以根据需要安全地重试此修复程序多次，直到所有节点均已更新为止。要使应用程序完成，必须在所有网格节点上成功安装此修补程序。

虽然网格节点会使用新的修补程序版本进行更新，但修补程序中的实际更改可能仅影响特定类型节点上的特定服务。例如，某个修补程序可能只会影响存储节点上的 LDR 服务。

如何应用修补程序进行恢复和扩展

在将修补程序应用到网格后，主管理节点会自动为通过恢复操作还原或添加到扩展中的任何节点安装相同的修补程序版本。

但是，如果需要恢复主管理节点，则必须手动安装正确的 StorageGRID 版本，然后应用此修补程序。主管理节点的最终 StorageGRID 版本必须与网格中其他节点的版本匹配。

以下示例说明了如何在恢复主管理节点时应用修补程序：

1. 假设网格运行的是具有最新修补程序的 StorageGRID 11.*A.B* 版本。"`网格版本` " 为 11.*A.B.y* 。
2. 主管理节点出现故障。
3. 您可以使用 StorageGRID 11.*A.B* 重新部署主管理节点，并执行恢复操作步骤 。

   根据需要，要与网格版本匹配，您可以在部署节点时使用次要版本；您无需先部署主要版本。

4. 然后，将修补程序 11.*A.B.y* 应用于主管理节点。

相关信息

配置替代主管理节点

规划并准备修补程序

您必须在应用修补程序之前进行规划，以确保 StorageGRID 系统的中断降至最低。

步骤

- 应用修补程序时对系统的影响
- 获取修补程序所需的材料
- 正在下载修补程序文件
- 在应用修补程序之前检查系统状况

应用修补程序时对系统的影响

您必须了解应用修补程序时 StorageGRID 系统将受到什么影响。

客户端应用程序可能会发生短期中断

StorageGRID 系统可以在整个修补程序过程中从客户端应用程序载入和检索数据；但是，如果修补程序需要在各个网关节点或存储节点上重新启动服务，则客户端与这些节点的连接可能会暂时中断。修复程序过程完成并在各个节点上恢复服务后，连接将恢复。

如果无法接受短时间内断开连接，您可能需要计划停机时间以应用修补程序。您可以使用选择性批准来计划某些节点的更新时间。

> 您可以使用多个网关和高可用性（ High Availability ， HA ）组在修复程序过程中提供自动故障转移。请参见的说明 配置高可用性组。

可能会触发警报和 **SNMP** 通知

当服务重新启动以及 StorageGRID 系统作为混合版本环境运行时（某些网格节点运行早期版本，而另一些网格节点已升级到更高版本），可能会触发警报和 SNMP 通知。通常，这些警报和通知将在修复程序完成时清除。

配置更改受限

将修补程序应用于 StorageGRID 时：

- 在对所有节点应用此修补程序之前，请勿进行任何网格配置更改（例如，指定网格网络子网或批准待定网格节点）。
- 在将此修补程序应用于所有节点之前，请勿更新 ILM 配置。

获取修复所需的材料

在应用修补程序之前，您必须获取所有必需的材料。

项目	注释：
StorageGRID 修补程序文件	您必须下载 StorageGRID 修补程序文件。
• 网络端口 • 支持的 Web 浏览器 • SSH 客户端（例如 PuTTY ）	
恢复软件包（` .zip` ）文件	应用修补程序之前， 下载最新的恢复软件包文件 如果在修复期间发生任何问题，请在应用此修复程序后下载恢复包文件的新副本并将其保存在安全位置。更新后的恢复包文件可用于在发生故障时还原系统。
Passwords.txt 文件	可选，只有在使用 SSH 客户端手动应用修补程序时才使用。`passwords.txt` 文件包含在该软件包中，该软件包是恢复软件包 ` .zip` 文件的一部分。

项目	注释：
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语未列在 `passwords.txt` 文件中。
相关文档	`reADME.txt` 此修补程序的文件。此文件包含在热修补程序下载页面中。在应用此修补程序之前，请务必仔细查看 `reADME` 文件。

相关信息

下载修补程序文件

下载修补程序文件

您必须先下载此修补程序文件，然后才能应用此修补程序。

步骤

1. 转到 StorageGRID 的 "NetApp 下载 " 页面。

   "NetApp 下载： StorageGRID"

2. 选择 * 可用软件 * 下的向下箭头可查看可供下载的修补程序列表。

   修补程序文件版本的格式为： 11.4_.x.y_ 。

3. 查看更新中包含的更改。

   如果您刚刚恢复了主管理节点，并且需要应用修补程序，请选择安装在其他网格节点上的相同修补程序版本。

   a. 选择要下载的热修补程序版本，然后选择 * 执行 * 。
   b. 使用您的 NetApp 帐户的用户名和密码登录。
   c. 阅读并接受最终用户许可协议。

      此时将显示选定版本的下载页面。

   d. 下载热修补程序 `reADME.txt` 文件以查看热修补程序中所含更改的摘要。

4. 选择此修补程序的下载按钮，然后保存此文件。

   请勿更改此文件的名称。

   如果您使用的是 macOS 设备，则此修补程序文件可能会自动保存为 ` .txt` 文件。如果是，则必须重命名此文件，而不使用 ` .txt` 扩展名。

5. 选择下载位置，然后选择 * 保存 * 。

相关信息

配置替代主管理节点

在应用修补程序之前，请检查系统的状况

您必须验证系统是否已准备好容纳此修补程序。

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 如果可能，请确保系统运行正常，并且所有网格节点均已连接到网格。

   已连接节点具有绿色复选标记  在节点页面上。

3. 如果可能，请检查并解决任何当前警报。

   有关特定警报的信息，请参见 StorageGRID 监控和故障排除说明。

4. 确保未执行任何其他维护过程，例如升级，恢复，扩展或停用操作步骤 。

   应用修补程序之前，您应等待所有活动的维护过程完成。

   当另一个维护操作步骤 正在运行时，您无法应用 StorageGRID 修补程序。例如，在停用，扩展或恢复操作步骤 正在运行时，您无法应用修补程序。

   如果节点或站点停用操作步骤 已暂停，您可以安全地应用修补程序。此外，您还可以在 StorageGRID 升级操作步骤 的最后阶段应用修补程序。有关详细信息，请参见有关升级 StorageGRID 软件的说明。

相关信息

监控和故障排除

暂停和恢复存储节点的停用过程

应用修补程序

此修补程序会首先自动应用于主管理节点。然后，您必须批准将此修补程序应用于其他网格节点，直到所有节点运行相同的软件版本为止。您可以通过选择批准单个网格节点，网格节点组或所有网格节点来自定义批准顺序。

您需要的内容

- 您已查看注意事项并完成中的步骤 规划并准备修补程序。
- 您具有配置密码短语。
- 您具有 root 访问权限或维护权限。

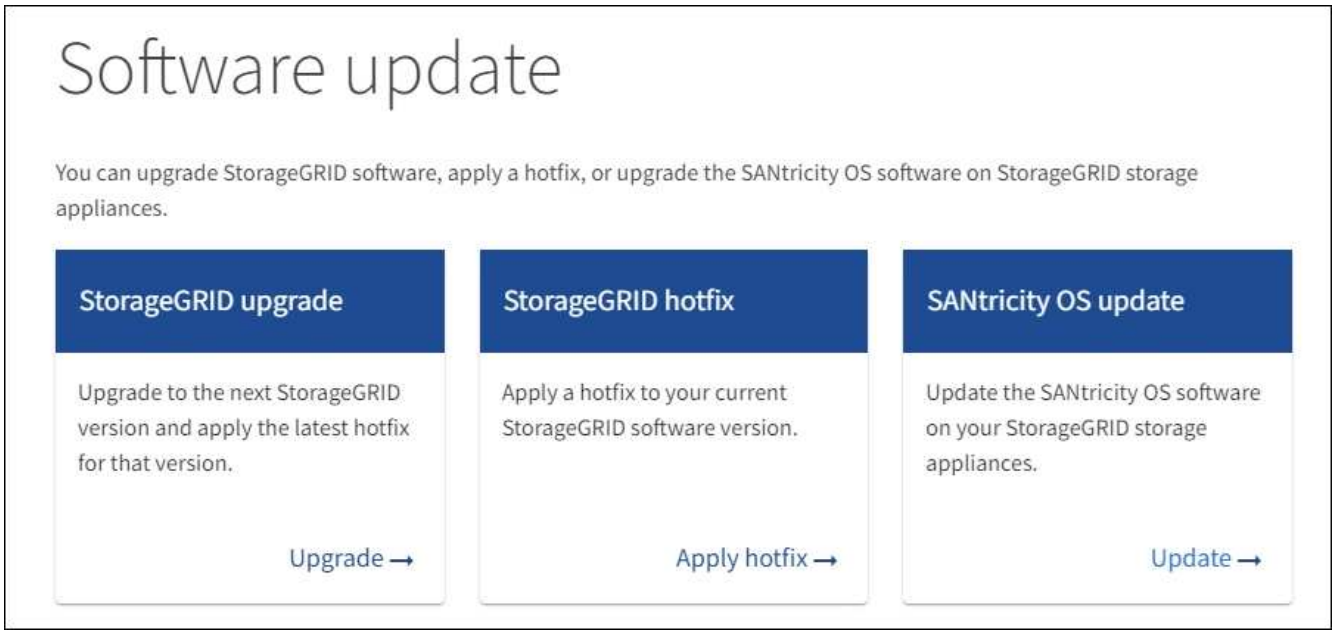
关于此任务

- 您可以延迟向节点应用修补程序，但只有在将修补程序应用到所有节点之后，此修补程序过程才会完成。
- 在完成修复程序过程之前，您无法执行 StorageGRID 软件升级或 SANtricity 操作系统升级。

步骤

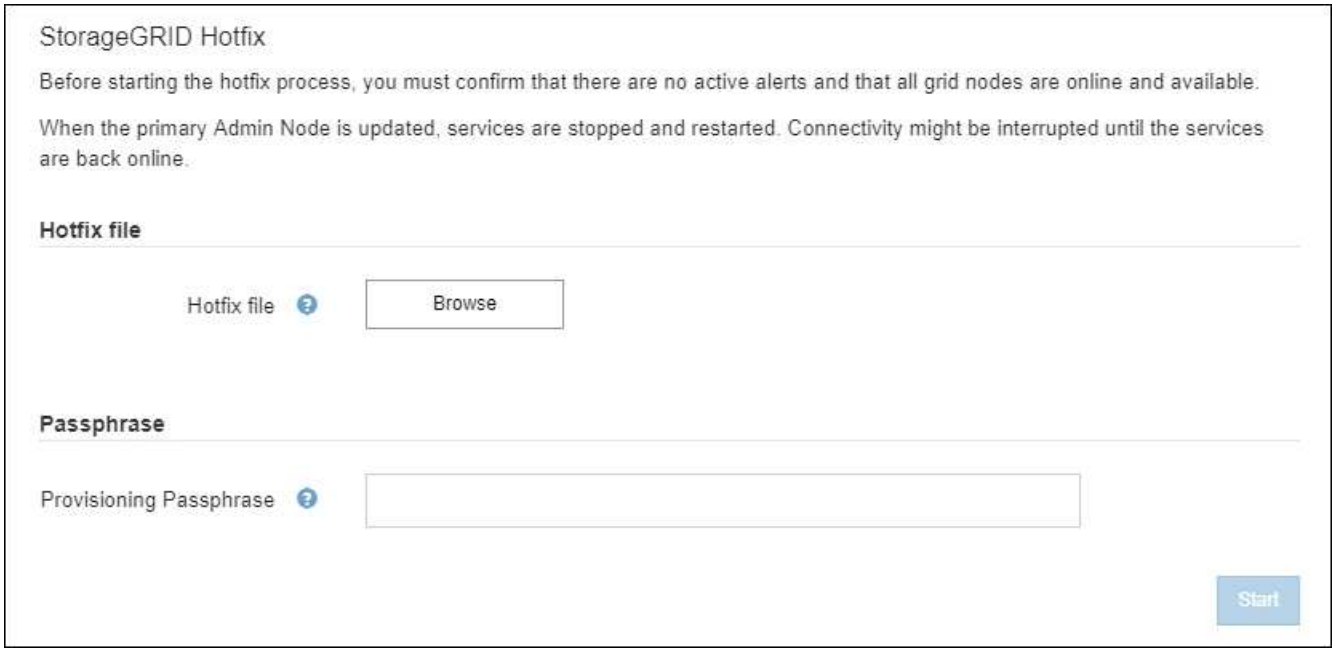
1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 维护 * > * 系统 * > * 软件更新 * 。

   此时将显示软件更新页面。



3. 选择 * 应用修补程序 * 。

   此时将显示 StorageGRID 热修补程序页面。



4. 选择从 NetApp 支持站点下载的修补程序文件。

   a. 选择 * 浏览 * 。

   b. 找到并选择文件。

`hotfix-install-version`

c. 选择 * 打开 * 。

已上传此文件。上传完成后，文件名将显示在详细信息字段中。

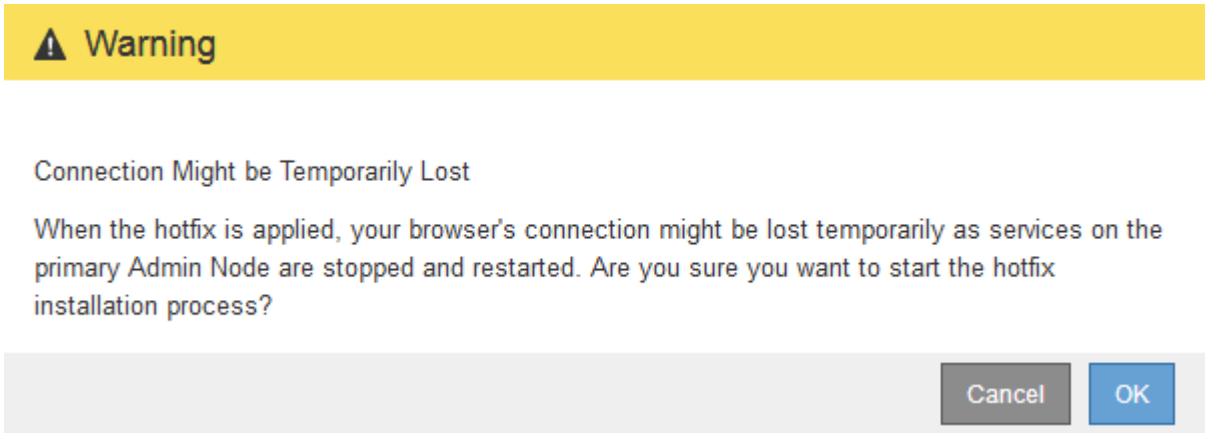
请勿更改文件名，因为它是验证过程的一部分。

5. 在文本框中输入配置密码短语。

此时将启用 * 开始 * 按钮。

6. 选择 * 开始 * 。

此时将显示一条警告，指出当主管理节点上的服务重新启动时，您的浏览器连接可能会暂时断开。



7. 选择 * 确定 * 开始将此修补程序应用于主管理节点。

当修复程序启动时：

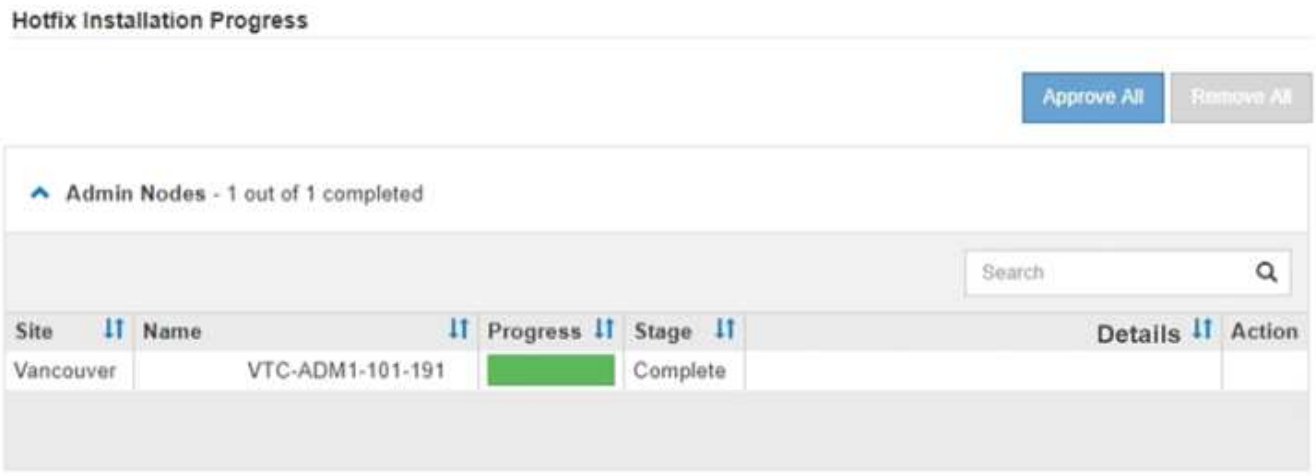
a. 此时将运行修补程序验证。

如果报告了任何错误，请予以解决，重新上传此修复程序文件，然后再次选择 * 启动 * 。

b. 此时将显示热修补程序安装进度表。此表显示了网格中的所有节点以及每个节点的修补程序安装的当前阶段。表中的节点按类型分组：

- 管理节点
- 网关节点
- 存储节点
- 归档节点

进度条将达到完成状态，然后会首先显示主管理节点，并显示阶段 "`complete" 。`



8. 或者，也可以按 * 站点 * ， * 名称 * ， * 进度 * ， * 阶段 * 或 * 详细信息 * 按升序或降序对每个分组中的节点列表进行排序。或者，在 * 搜索 * 框中输入一个术语以搜索特定节点。
9. 批准已准备好更新的网格节点。相同类型的已批准节点将一次升级一个。

   除非您确定节点已准备好进行更新，否则请勿批准节点的修补程序。将此修补程序应用于网格节点时，该节点上的某些服务可能会重新启动。对于与节点通信的客户端，这些操作可能会导致发生原因 服务中断。

   - 选择一个或多个 * 批准 * 按钮将一个或多个单独的节点添加到修补程序队列。
   - 在每个分组中选择 * 全部批准 * 按钮，将所有类型相同的节点添加到修补程序队列。如果您在 * 搜索 * 框中输入了搜索条件，则 * 全部批准 * 按钮将适用场景 所有搜索条件选择的节点。

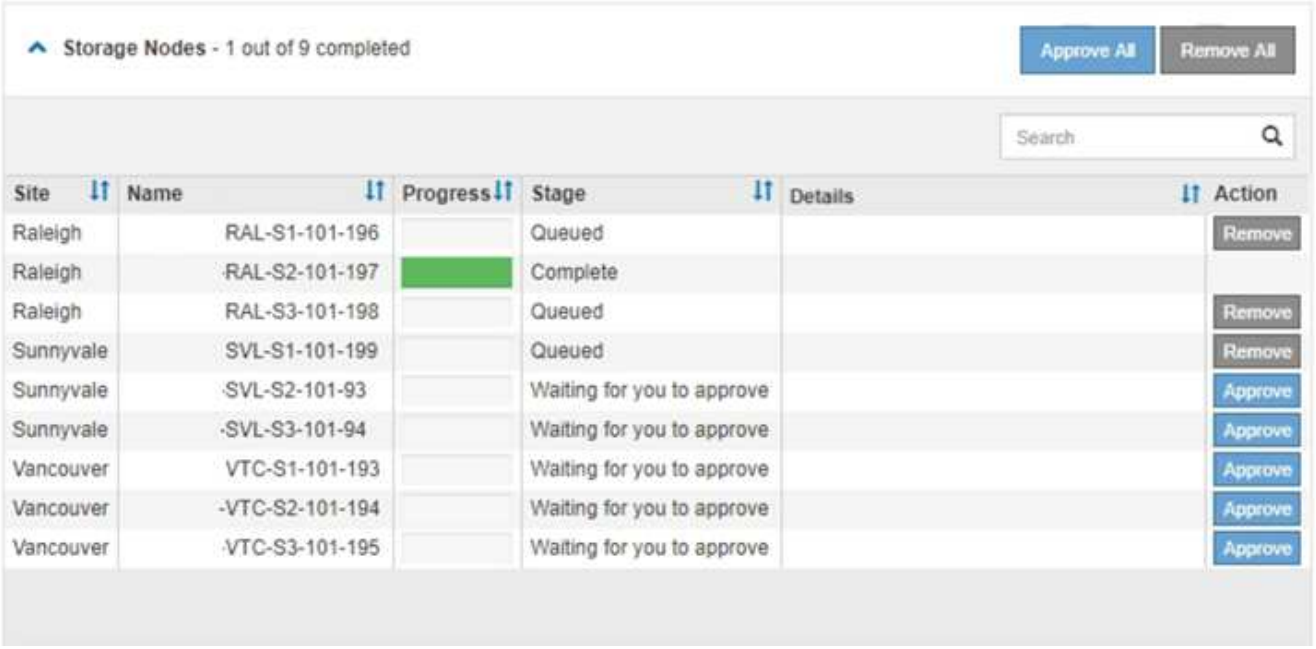
     页面顶部的 * 全部批准 * 按钮批准页面上列出的所有节点，而分组表顶部的 * 全部批准 * 按钮仅批准该组中的所有节点。如果节点升级顺序非常重要，请一次批准一个节点或一组节点，并等待每个节点完成升级，然后再批准下一个节点。

   - 选择页面顶部的顶级 * 全部批准 * 按钮，将网格中的所有节点添加到热修补程序队列。

     您必须先完成 StorageGRID 热修补程序，然后才能启动其他软件更新。如果无法完成此修补程序，请联系技术支持。

   - 选择 * 删除 * 或 * 全部删除 * 可从修补程序队列中删除一个节点或所有节点。

     当此阶段超过 "`Queued ，` " 时， * 删除 * 按钮将处于隐藏状态，您无法再从修补程序进程中删除此节点。



10. 请稍候，此修补程序将应用于每个已批准的网格节点。

    在所有节点上成功安装此修复程序后，热修复程序安装进度表将关闭。绿色横幅显示了完成修补程序的日期和时间。

11. 如果无法将此修补程序应用于任何节点，请查看每个节点的错误，解决问题描述 ，然后重复上述步骤。

    只有在将此修补程序成功应用于所有节点之后，操作步骤 才会完成。您可以根据需要安全地重试此修复程序多次，直到其完成为止。

相关信息

管理 StorageGRID

监控和故障排除

网格节点恢复过程

如果网格节点发生故障，您可以通过更换发生故障的物理或虚拟服务器，重新安装 StorageGRID 软件以及还原可恢复的数据来恢复该节点。

如果硬件，虚拟化，操作系统或软件故障导致节点无法运行或不可靠，则网格节点可能会发生故障。可能会发生多种类型的故障，从而需要恢复网格节点。

恢复网格节点的步骤因托管网格节点的平台和网格节点类型而异。每种类型的网格节点都有一个特定的恢复操作步骤 ，您必须严格遵循该恢复。

通常，您会尝试尽可能保留故障网格节点中的数据，修复或更换故障节点，使用网格管理器配置替代节点并还原节点的数据。

如果整个 StorageGRID 站点出现故障，请联系技术支持。技术支持将与您合作，制定和执行站点恢复计划，最大限度地提高已恢复的数据量，并满足您的业务目标。

相关信息

技术支持如何执行站点恢复

有关网格节点恢复的警告和注意事项

如果网格节点发生故障，您必须尽快恢复。开始之前，您必须查看节点恢复的所有警告和注意事项。

StorageGRID 是一个分布式系统，由多个节点组成，这些节点彼此协同工作。请勿使用磁盘快照还原网格节点。请参阅每种类型节点的恢复和维护过程。

尽快恢复出现故障的网格节点的一些原因包括：

- 出现故障的网格节点可以减少系统和对象数据的冗余，因此，如果另一个节点发生故障，您容易受到永久数据丢失的风险。
- 网格节点发生故障可能会影响 Day - 到 - Day 操作的效率。
- 出现故障的网格节点可能会降低您监控系统操作的能力。
- 如果存在严格的 ILM 规则，则出现故障的网格节点可能会发生原因 a 500 internal server error 。
- 如果未及时恢复网格节点，则恢复时间可能会增加。例如，可能会出现需要在恢复完成之前清除的队列。

对于要恢复的特定网格节点类型，请始终遵循恢复操作步骤 。恢复过程因主管理节点或非主管理节点，网关节点，归档节点，设备节点和存储节点而异。

恢复网格节点的前提条件

恢复网格节点时，系统会假设以下所有条件：

- 已更换并配置发生故障的物理或虚拟硬件。
- 替代设备上的 StorageGRID 设备安装程序版本与 StorageGRID 系统的软件版本匹配，如用于验证和升级 StorageGRID 设备安装程序版本的硬件安装和维护中所述。
  - SG100 和 SG1000 服务设备
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备
- 如果要恢复的网格节点不是主管理节点，则要恢复的网格节点与主管理节点之间会建立连接。

托管多个网格节点的服务器发生故障时的节点恢复顺序

如果托管多个网格节点的服务器发生故障，您可以按任意顺序恢复节点。但是，如果发生故障的服务器托管主管理节点，则必须先恢复该节点。首先恢复主管理节点可防止其他节点在等待与主管理节点联系时暂停恢复。

已恢复节点的 **IP** 地址

请勿尝试使用当前已分配给任何其他节点的 IP 地址恢复节点。部署新节点时，请使用故障节点的当前 IP 地址或未使用的 IP 地址。

如果您使用新 IP 地址部署新节点，然后恢复该节点，则新 IP 地址将继续用于已恢复的节点。如果要还原到原始 IP 地址，请在恢复完成后使用更改 IP 工具。

收集网格节点恢复所需的材料

在执行维护过程之前，您必须确保具有必要的材料来恢复出现故障的网格节点。

项目	注释：
StorageGRID 安装归档	如果需要恢复网格节点，则需要 下载 StorageGRID 安装文件 适用于您的平台。 • 注意： * 如果要恢复存储节点上的故障存储卷，则不需要下载文件。
服务笔记本电脑	服务笔记本电脑必须具有以下组件： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器
恢复软件包 ` .zip` 文件	获取最新恢复软件包 ` .zip` 文件的副本： `sGWS-recovery-package-id-revision.zip` 每次修改系统时，都会更新 ` .zip` 文件的内容。在进行此类更改后，系统会指示您将最新版本的恢复软件包存储在安全位置。使用最新副本从网格故障中恢复。 如果主管理节点运行正常，您可以从网格管理器下载恢复软件包。选择 * 维护 * > * 系统 * > * 恢复软件包 * 。 如果您无法访问网格管理器，则可以在包含此 ADC 服务的某些存储节点上找到恢复软件包的加密副本。在每个存储节点上，检查恢复软件包的位置： ` /var/local/install/sgws-recovery-package-*grid-revision*.zip 。 gpg` 使用修订版号最高的恢复软件包。
`passwords.txt` file	包含访问命令行上的网格节点所需的密码。包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
适用于您的平台的最新文档	请访问平台供应商的网站以获取相关文档。 有关您的平台当前支持的版本，请参见 "NetApp 互操作性表工具"。

下载并提取 **StorageGRID** 安装文件

下载软件并提取文件，除非您这样做 恢复存储节点上的故障存储卷。

您必须使用网格上当前运行的 StorageGRID 版本。

步骤

1. 确定当前安装的软件版本。从网格管理器顶部，选择帮助图标并选择 * 关于 * 。
2. 转至 "StorageGRID 的 "NetApp 下载 " 页面"。
3. 选择网格上当前运行的 StorageGRID 版本。

   StorageGRID 软件版本采用以下格式： `11.x.y` 。
4. 使用您的 NetApp 帐户的用户名和密码登录。
5. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。
6. 在下载页面的 * 安装 StorageGRID * 列中，为您的平台选择 ` .tgz` 或 ` .zip` 文件。

   安装归档文件中显示的版本必须与当前安装的软件版本匹配。

   如果您运行的是 Windows ，请使用 ` .zip` 文件。

平台	安装归档
Red Hat Enterprise Linux 或 CentOS	`storageGRID-Webscale -version-RPM-uniqueID.zip` `StorageGRID-Webscale -version-RPM-uniqueID.tgz`
Ubuntu ， Debian 或设备	`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. 下载并提取归档文件。
8. 根据您的平台以及需要恢复的网格节点，按照适用于您的平台的步骤选择所需的文件。

   步骤中为每个平台列出的路径与归档文件安装的顶级目录相对。
9. 如果要恢复 Red Hat Enterprise Linux 或 CentOS 系统下，选择相应的文件。

路径和文件名	Description
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 节点映像。

路径和文件名	Description
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 主机服务。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 RHEL 或 CentOS 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要恢复 Ubuntu 或 Debian 系统下，选择相应的文件。

路径和文件名	Description
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。

路径和文件名	Description
	文件 ` /debs/storagegrid-webscale-images-version-SHA.deb` 的 MD5 校验和。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 * ： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要恢复 VMware 系统下，选择相应的文件。

路径和文件名	Description
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。

路径和文件名	Description
	用于部署主管理节点的开放式虚拟化格式模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署非主管理节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署归档节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署网关节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署基于虚拟机的存储节点的模板文件（`.OVF`）和清单文件（`.MF`）。
部署脚本工具	Description
	Bash shell 脚本，用于自动部署虚拟网格节点。
	与 `deept-vsphere-ovftool.sh` 脚本结合使用的示例配置文件。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	StorageGRID 的 API 架构。 • 注意 *： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要恢复基于 StorageGRID 设备的系统，请选择相应的文件。

路径和文件名	Description
	用于在设备上安装 StorageGRID 节点映像的 Deb 软件包。
	StorageGRID 设备安装程序使用的 Deb 安装包的校验和，用于验证该软件包在上传后是否完好无损。

对于设备安装，只有在需要避免网络流量时，才需要这些文件。设备可以从主管理节点下载所需文件。

选择节点恢复操作步骤

您必须为出现故障的节点类型选择正确的恢复操作步骤 。

网格节点	恢复操作步骤
多个存储节点	请联系技术支持。如果多个存储节点出现故障，技术支持必须协助恢复，以防止数据库不一致导致数据丢失。可能需要站点恢复操作步骤 。 技术支持如何执行站点恢复
一个存储节点	存储节点恢复操作步骤 取决于故障的类型和持续时间。 从存储节点故障中恢复
管理节点	管理节点操作步骤 取决于您是需要恢复主管理节点还是非主管理节点。 从管理节点故障中恢复
网关节点	从网关节点故障中恢复。
归档节点	从归档节点故障中恢复。

如果托管多个网格节点的服务器发生故障，您可以按任意顺序恢复节点。但是，如果发生故障的服务器托管主管理节点，则必须先恢复该节点。首先恢复主管理节点可防止其他节点在等待与主管理节点联系时暂停恢复。

从存储节点故障中恢复

用于恢复故障存储节点的操作步骤 取决于故障类型和故障存储节点的类型。

使用此表为出现故障的存储节点选择恢复操作步骤 。

问题描述	Action	注释：
• 多个存储节点出现故障。 • 第二个存储节点在存储节点发生故障或恢复后不到 15 天出现故障。 这包括在恢复另一个存储节点期间存储节点出现故障的情况。	您必须联系技术支持。	如果所有故障存储节点都位于同一站点，则可能需要执行站点恢复操作步骤 。 技术支持将评估您的情况并制定恢复计划。 技术支持如何执行站点恢复 在 15 天内恢复多个存储节点（或多个存储节点）可能会影响 Cassandra 数据库的完整性，从而可能导致发生原因 数据丢失。 技术支持可以确定何时可以安全地开始恢复第二个存储节点。 • 注意 * ：如果某个站点上有多个包含此 ADA 服务的存储节点发生故障，则该站点的任何待定平台服务请求都将丢失。
存储节点已脱机超过 15 天。	将存储节点恢复到关闭状态超过 15 天	要确保 Cassandra 数据库的完整性，需要使用此操作步骤 。
设备存储节点出现故障。	恢复设备存储节点	对于所有故障，设备存储节点的恢复操作步骤 均相同。
一个或多个存储卷发生故障，但系统驱动器完好无损	从系统驱动器完好无损的存储卷故障中恢复	此操作步骤 用于基于软件的存储节点。
系统驱动器出现故障。	从系统驱动器故障中恢复	节点更换操作步骤 取决于部署平台以及是否有任何存储卷也出现故障。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

将存储节点恢复到关闭状态超过 **15** 天

如果一个存储节点脱机且未连接到其他存储节点超过 15 天，则必须在此节点上重建 Cassandra 。

您需要的内容

- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）

- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）

关于此任务

存储节点具有包含对象元数据的 Cassandra 数据库。如果某个存储节点无法与其他存储节点通信超过 15 天，则 StorageGRID 会假定该节点的 Cassandra 数据库已过时。在使用其他存储节点中的信息重建 Cassandra 之前，存储节点无法重新加入网格。

只有当一个存储节点关闭时，才可以使用此操作步骤 来重建 Cassandra 。如果其他存储节点已脱机或在过去 15 天内已在另一个存储节点上重建 Cassandra ，请联系技术支持；例如，在恢复故障存储卷或恢复故障存储节点的过程中， Cassandra 可能已重建。



如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。



如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。



如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

步骤

1. 如有必要，打开需要恢复的存储节点的电源。
2. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。



如果无法登录到网格节点，则系统磁盘可能不会损坏。转至的操作步骤 从系统驱动器故障中恢复。

1. 对存储节点执行以下检查：
   a. 问题描述 此命令： `nodetool status`

      输出应为 `Connection refused.`

   b. 在网格管理器中，选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   c. 选择 * 站点 _* > * 存储节点 * > * SSM* > * 服务 * 。验证 Cassandra 服务是否显示 `not running` 。
   d. 选择 * 存储节点 * > * SSM* > * 资源 * 。验证卷部分中是否没有错误状态。
   e. 问题描述 此命令： `grep -i Cassandra /var/local/log/servermanager.log`

您应在输出中看到以下消息：

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. 问题描述 此命令并监控脚本输出： `check-Cassandra-rebuild`
   - 如果存储服务正在运行，系统将提示您停止这些服务。输入： *
   - 查看脚本中的警告。如果不适用，请确认您要重建 Cassandra 。输入： *

> 某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

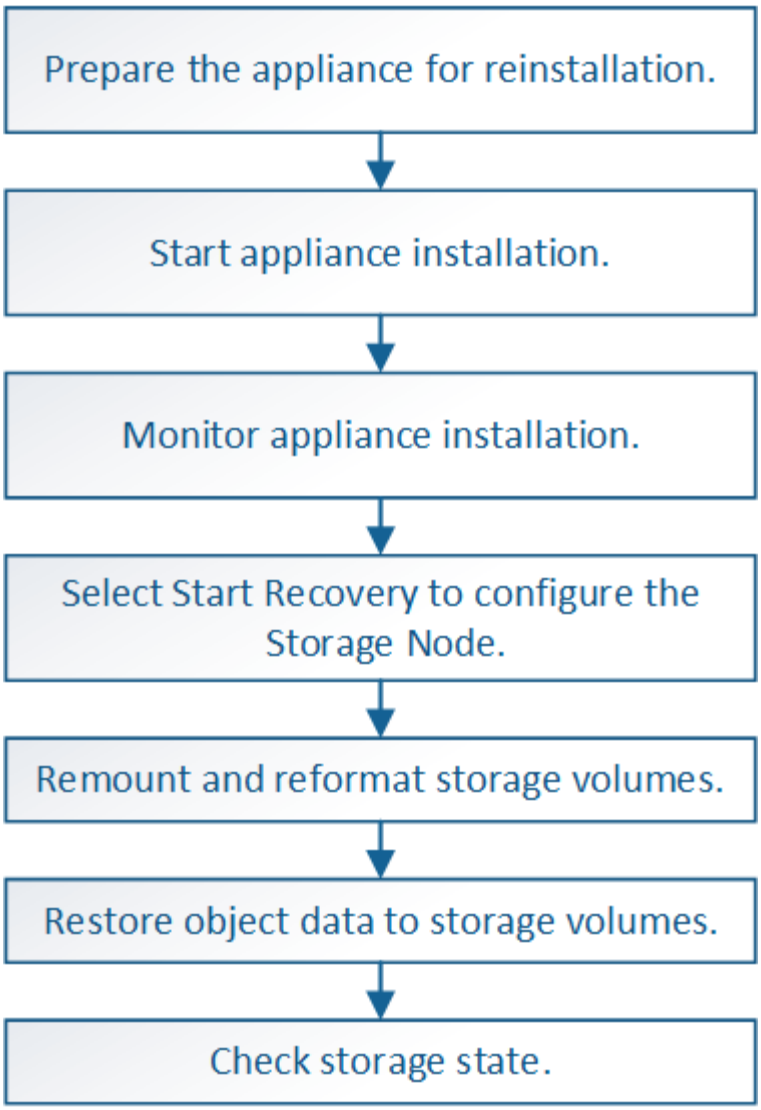
3. 重建完成后，请执行以下检查：
   a. 在网格管理器中，选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 已恢复存储节点 * > * SSM* > * 服务 * 。
   c. 确认所有服务均已运行。
   d. 选择 * DDS* > * 数据存储 * 。
   e. 确认 * 数据存储状态 * 为 "`up` " ， * 数据存储状态 * 为 "`Normal" 。`

恢复设备存储节点

无论您是从系统驱动器丢失还是仅从存储卷丢失中恢复，用于恢复出现故障的 StorageGRID 设备存储节点的操作步骤 都是相同的。

关于此任务

您必须准备设备并重新安装软件，配置节点以重新加入网格，重新格式化存储以及还原对象数据。



如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。在 15 天内在两个或多个存储节点上重建 Cassandra 可能会导致数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

如果在恢复期间遇到服务：状态 - Cassandra （ SVST ）警报，请参见有关通过重建 Cassandra 从警报中恢复的监控和故障排除说明。重建 Cassandra 后，应清除警报。如果未清除警报，请联系技术支持。

有关硬件维护过程，例如更换控制器或重新安装 SANtricity OS 的说明，请参见存储设备的安装和维护说明。

相关信息

监控和故障排除

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

准备要重新安装的设备存储节点

恢复设备存储节点时，必须先准备设备以重新安装 StorageGRID 软件。

1. 登录到发生故障的存储节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 准备设备存储节点以安装 StorageGRID 软件。`sgareinstall`
3. 当系统提示您继续时，输入： `y`

   设备将重新启动， SSH 会话将结束。StorageGRID 设备安装程序通常需要大约 5 分钟才能投入使用，但在某些情况下，您可能需要等待长达 30 分钟。

   StorageGRID 设备存储节点已重置，并且无法再访问存储节点上的数据。在初始安装过程中配置的 IP 地址应保持不变；但是，建议您在操作步骤 完成后进行确认。

   执行 `sgareinstall` 命令后，将删除所有 StorageGRID 配置的帐户，密码和 SSH 密钥，并生成新的主机密钥。

开始安装 **StorageGRID** 设备

要在设备存储节点上安装 StorageGRID ，请使用设备中提供的 StorageGRID 设备安装程序。

您需要的内容

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路和 IP 地址。
- 您知道 StorageGRID 网格的主管理节点的 IP 地址。

- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 您已按照存储设备的安装和维护说明完成以下前提条件任务：
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备
- 您正在使用 支持的 Web 浏览器。
- 您知道分配给设备中计算控制器的一个 IP 地址。您可以使用管理网络（控制器上的管理端口 1 ），网格网络或客户端网络的 IP 地址。

关于此任务

要在设备存储节点上安装 StorageGRID ，请执行以下操作：

- 您可以指定或确认主管理节点的 IP 地址和节点名称。
- 您开始安装，并等待卷配置完毕并安装软件。
- 在整个过程中，安装将暂停。要恢复安装，您必须登录到网格管理器，并将待定存储节点配置为故障节点的替代节点。
- 配置节点后，设备安装过程将完成，设备将重新启动。

步骤

1. 打开浏览器并输入设备中计算控制器的 IP 地址之一。

   ` + https://Controller_IP:8443+`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

   假设主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上， StorageGRID 设备安装程序可以自动发现此 IP 地址。

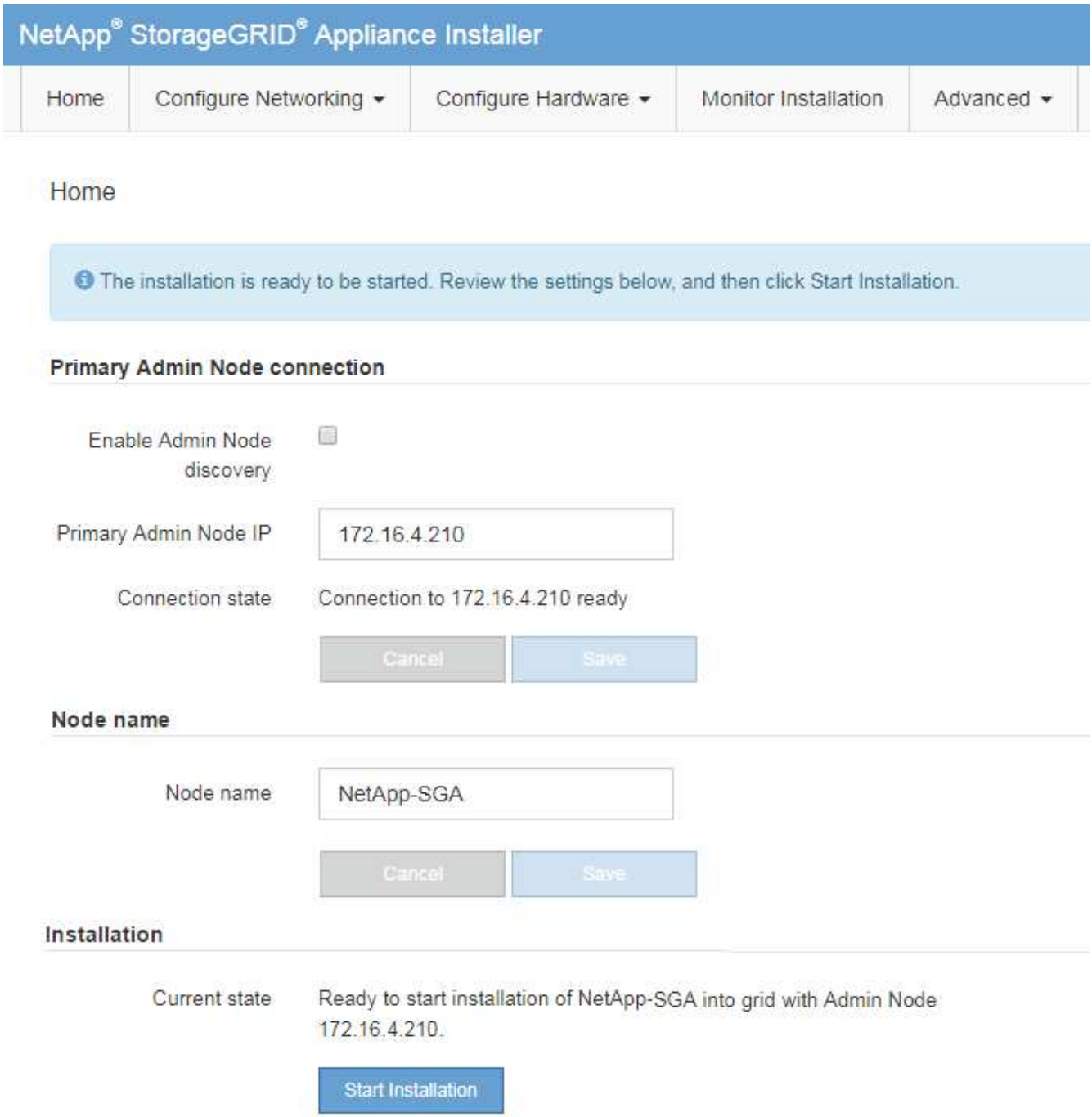
3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	步骤
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

选项	步骤
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 从已发现的 IP 地址列表中，选择要部署此设备存储节点的网格的主管理节点。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

4. 在 * 节点名称 * 字段中，输入与要恢复的节点相同的名称，然后单击 * 保存 * 。
5. 在安装部分中，确认当前状态为 "`Ready to start installation of node name into grid with Primary Admin Node admin_IP` " ，并且已启用 * 开始安装 * 按钮。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。
6. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。



当前状态将更改为 "`Installation is in progress，`"，此时将显示监控器安装页面。

如果需要手动访问监控器安装页面，请单击菜单栏中的 * 监控器安装 * 。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

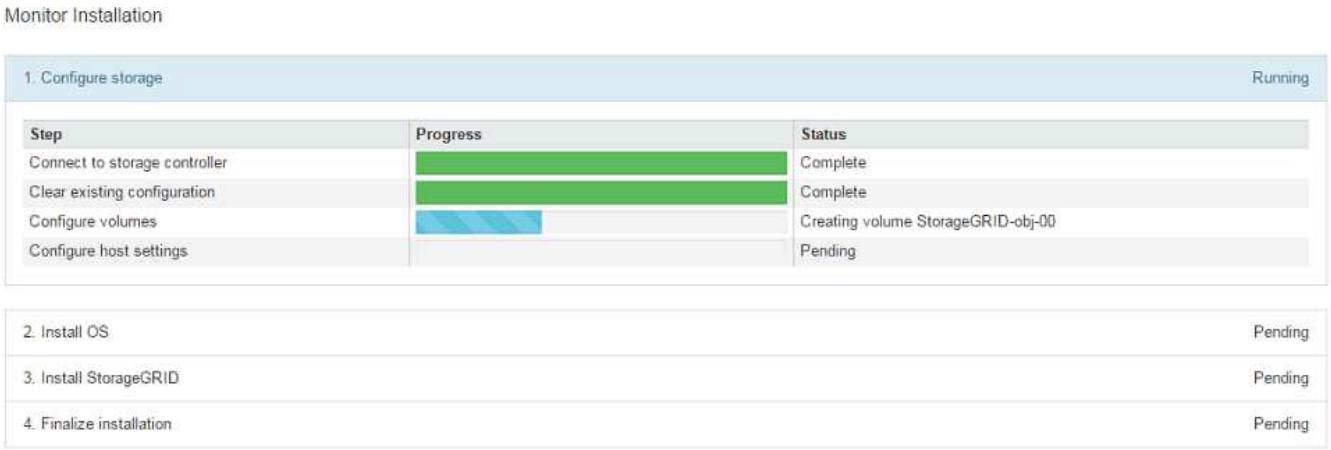
SG5700 存储设备

SG5600 存储设备

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

1. 要监控安装进度，请单击菜单栏中的 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

2. 查看前两个安装阶段的进度。

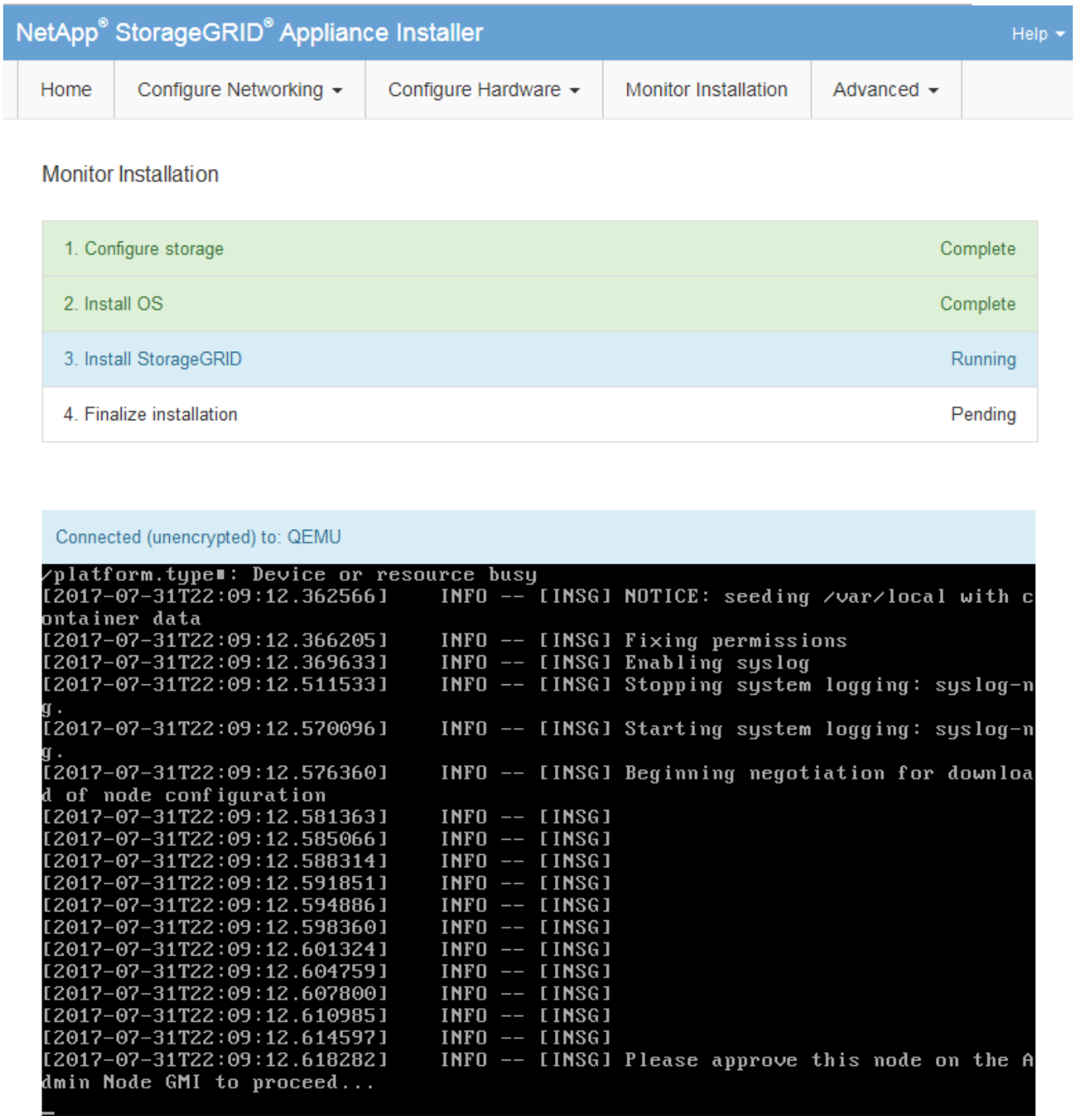
   ◦ * 。配置存储 *

   在此阶段，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。

   ◦ * 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

3. 继续监控安装进度，直到 * 安装 StorageGRID 网格管理器 * 阶段暂停，并且嵌入式控制台上显示一条消息，提示您使用网格管理器在管理节点上批准此节点。



4. 转至操作步骤 以配置设备存储节点。

选择 **Start Recovery** 以配置设备存储节点

您必须在网格管理器中选择启动恢复，才能将设备存储节点配置为故障节点的替代节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。

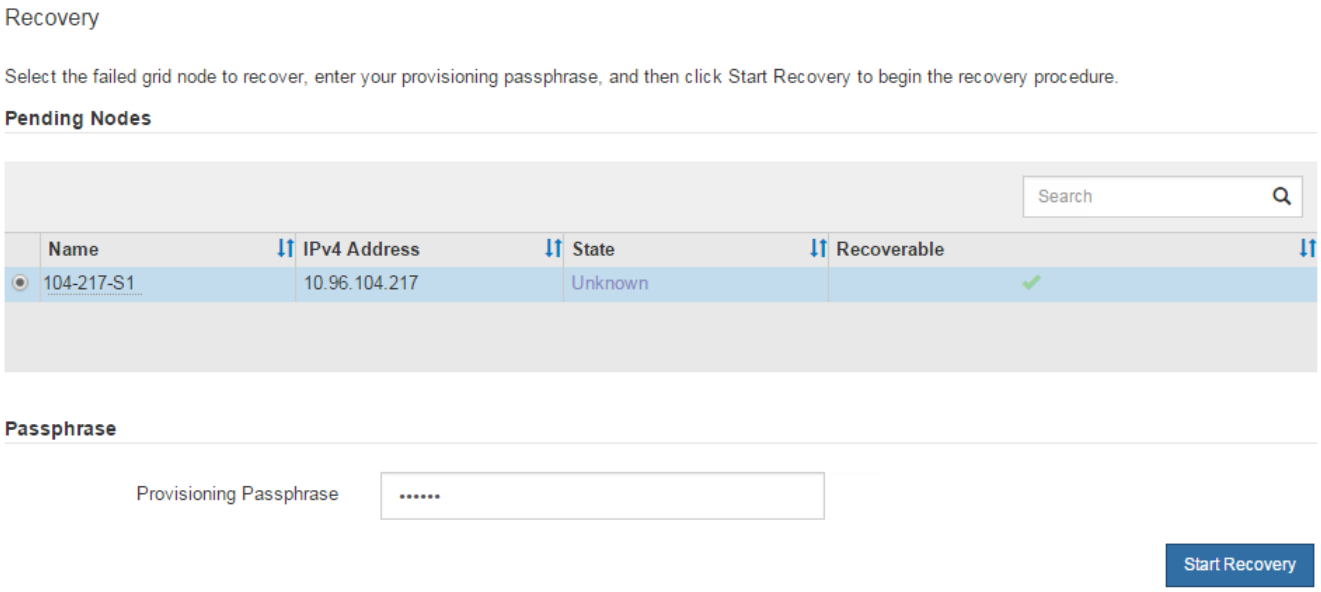
- 您必须已部署恢复设备存储节点。
- 您必须知道擦除编码数据的任何修复作业的开始日期。
- 您必须已确认过去 15 天内未重建此存储节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

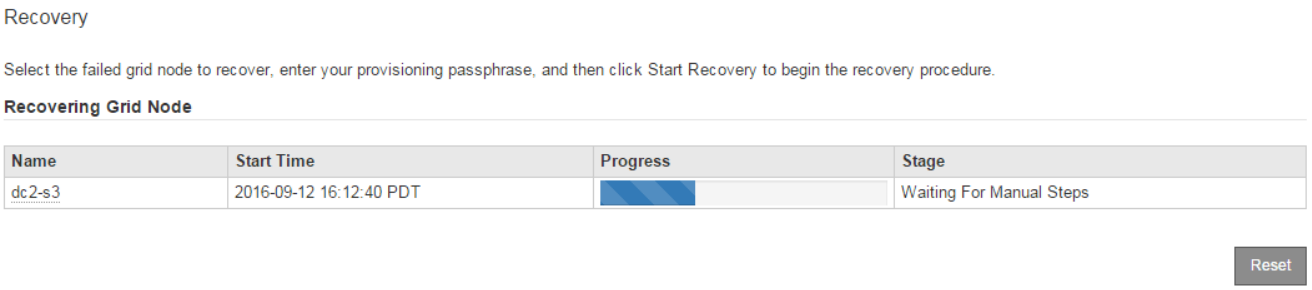
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。

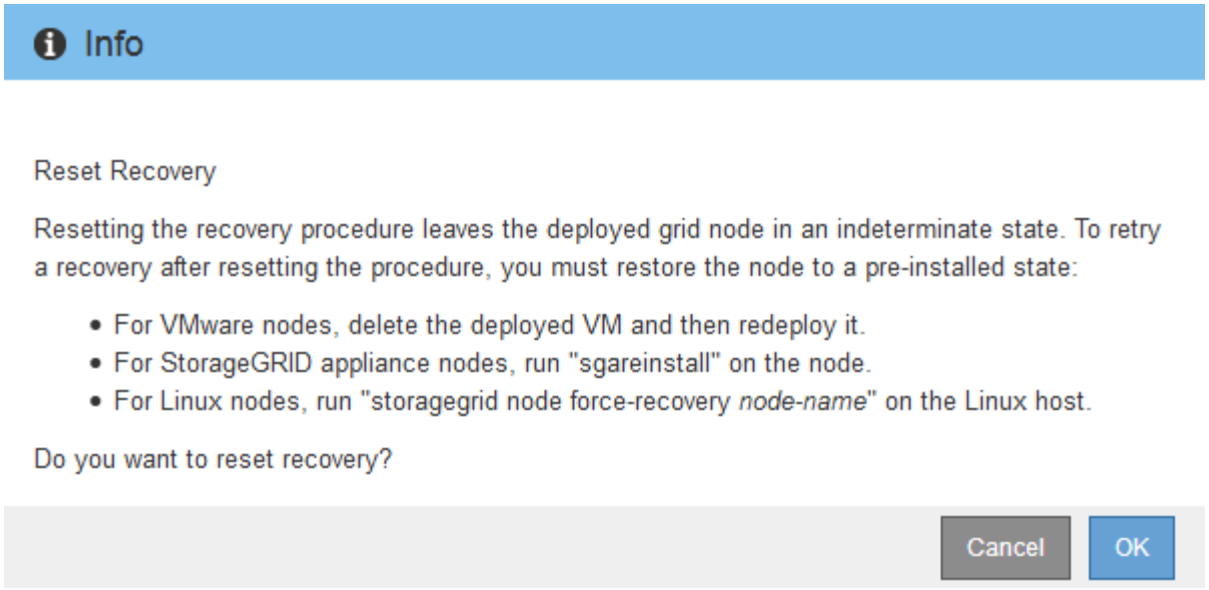


5. 在恢复网格节点表中监控恢复进度。

   当网格节点达到 "`Waiting for Manual steps` " 阶段时，转到下一主题并执行手动步骤以重新挂载和重新格式化设备存储卷。



> 在恢复期间的任何时刻，您都可以单击 * 重置 * 来启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，则必须通过在该节点上运行 `sgareinstall` 将设备节点还原到预安装状态。

重新挂载并重新格式化设备存储卷（ " 手动步骤 " ）

您必须手动运行两个脚本，才能重新挂载保留的存储卷并重新格式化任何发生故障的存储卷。第一个脚本将重新挂载格式正确的卷，使其格式化为 StorageGRID 存储卷。第二个脚本将重新格式化所有已卸载的卷，根据需要重新构建 Cassandra 数据库并启动服务。

您需要的内容

- 您已更换已知需要更换的任何故障存储卷的硬件。

  运行 `sn-remount-volumes` 脚本可能有助于您确定其他故障存储卷。

- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）
- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）

> 如果多个存储节点脱机或此网格中的存储节点在过去 15 天内已重建，请联系技术支持。请勿运行 `sn-recovery-postinstall.sh` 脚本。在两个或多个存储节点上相互重建 Cassandra 的 15 天内可能会导致数据丢失。

关于此任务

要完成此操作步骤 ，请执行以下高级任务：

- 登录到已恢复的存储节点。
- 运行 `sn-remount-volumes` 脚本重新挂载格式正确的存储卷。运行此脚本时，它将执行以下操作：
  - 挂载和卸载每个存储卷以重放 XFS 日志。
  - 执行 XFS 文件一致性检查。
  - 如果文件系统一致，则确定存储卷是否为格式正确的 StorageGRID 存储卷。

- 如果存储卷格式正确，请重新挂载该存储卷。卷上的所有现有数据保持不变。

- 查看脚本输出并解决任何问题。
- 运行 `sn-recovery-postinstall.sh` 脚本。运行此脚本时，它将执行以下操作。

> 在运行 `sn-recovery-postinstall.sh` （步骤 4 ）重新格式化故障存储卷并还原对象元数据之前，请勿在恢复期间重新启动存储节点。在 `sn-recovery-postinstall.sh` 完成之前重新启动存储节点会导致尝试启动的服务出错，并导致 StorageGRID 设备节点退出维护模式。

  - 重新格式化 `sn-remount-volumes` 脚本无法挂载或发现格式不正确的任何存储卷。

> 如果重新格式化某个存储卷，则该卷上的所有数据都将丢失。假设已将 ILM 规则配置为存储多个对象副本，则必须执行额外的操作步骤 以从网格中的其他位置还原对象数据。

  - 如果需要，在节点上重建 Cassandra 数据库。
  - 启动存储节点上的服务。

步骤

1. 登录到已恢复的存储节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 运行第一个脚本重新挂载任何格式正确的存储卷。

> 如果所有存储卷都是新的，需要进行格式化，或者所有存储卷都出现故障，您可以跳过此步骤并运行第二个脚本，重新格式化所有已卸载的存储卷。

   a. 运行以下脚本： `sn-remount-volumes`

   此脚本可能需要数小时才能在包含数据的存储卷上运行。

   b. 在脚本运行期间，查看输出并问题解答 任何提示。

> 根据需要，您可以使用 `tail -f` 命令监控脚本日志文件的内容（` /var/local/log/SN-remount-volumes.log` ）。日志文件包含比命令行输出更详细的信息。

```
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.
```

在示例输出中，一个存储卷已成功重新挂载，三个存储卷出现错误。

- ` /dev/sdb` 通过了 XFS 文件系统一致性检查，并具有有效的卷结构，因此已成功重新挂载。此脚本重新挂载的设备上的数据将保留下来。
- 由于存储卷是新的或已损坏， ` /dev/sdc` 未通过 XFS 文件系统一致性检查。
- 无法挂载 ` /dev/sdd` ，因为磁盘已取消初始化或磁盘的超级块已损坏。当脚本无法挂载存储卷时，它会询问您是否要运行文件系统一致性检查。
  - 如果存储卷已连接到新磁盘，请将 * N * 问题解答 到提示符处。您无需检查新磁盘上的文件系统。
  - 如果存储卷已连接到现有磁盘，问题解答 请将 * 。 *您可以使用文件系统检查的结果来确定损坏的来源。结果将保存在 ` /var/local/log/sn-remount-volumes.log` 日志文件中。
- ` dev/sde` 通过了 XFS 文件系统一致性检查，并且具有有效的卷结构；但是， `volID` 文件中的 LDR 节点 ID 与此存储节点的 ID 不匹配（顶部显示的 `configured LDR noid` ）。此消息表示此卷属于另一个存储节点。

3. 查看脚本输出并解决任何问题。

> 如果存储卷未通过 XFS 文件系统一致性检查或无法挂载，请仔细查看输出中的错误消息。您必须了解在这些卷上运行 `sn-recovery-postinstall.sh` 脚本的含义。

a. 检查以确保结果中包含所需所有卷的条目。如果未列出任何卷，请重新运行此脚本。

b. 查看所有已挂载设备的消息。确保没有指示存储卷不属于此存储节点的错误。

在此示例中， /dev/sde 的输出包含以下错误消息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 如果报告某个存储卷属于另一个存储节点，请联系技术支持。如果运行 `sn-recovery-postinstall.sh` 脚本，则存储卷将重新格式化，从而可能会丢失发生原因 数据。

c. 如果无法挂载任何存储设备，请记下此设备的名称，然后修复或更换此设备。

> 您必须修复或更换任何无法挂载的存储设备。

您将使用设备名称查找卷 ID ，在运行 `repair-data` 脚本将对象数据还原到卷（下一个操作步骤 ）时，需要输入此 ID 。

d. 修复或更换所有无法挂载的设备后，再次运行 `sn-remount-volumes` 脚本，以确认可以重新挂载的所有存储卷均已重新挂载。

> 如果无法挂载存储卷或存储卷格式不正确，而您继续执行下一步，则此卷以及此卷上的任何数据将被删除。如果对象数据有两个副本，则只有一个副本，直到完成下一个操作步骤（还原对象数据）为止。

> 如果您认为无法从网格中的其他位置重建故障存储卷上的剩余数据，请勿运行 `sn-recovery-postinstall.sh` 脚本（例如， ILM 策略使用的规则仅创建一个副本或卷在多个节点上发生故障）。请联系技术支持以确定如何恢复数据。

4. 运行 `sn-recovery-postinstall.sh` 脚本： `sn-recovery-postinstall.sh`

此脚本将重新格式化无法挂载或格式不正确的任何存储卷；根据需要在节点上重建 Cassandra 数据库；并启动存储节点上的服务。

请注意以下事项：

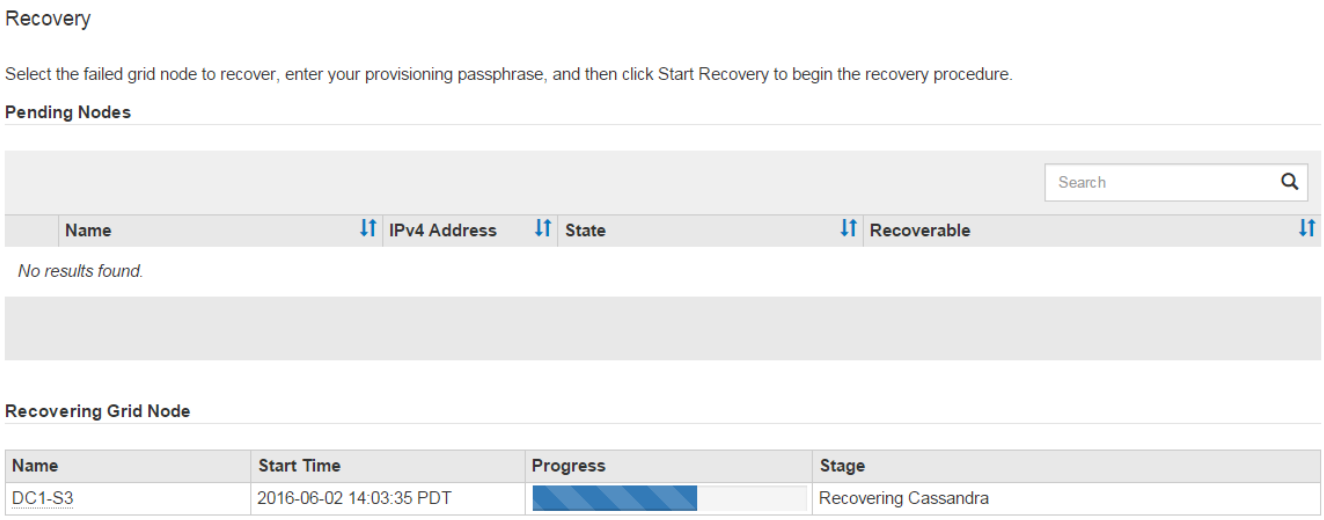
- 此脚本可能需要数小时才能运行。
- 通常，在脚本运行期间，您应单独保留 SSH 会话。
- SSH 会话处于活动状态时，请勿按 * 。 Ctrl+C* 。
- 如果发生网络中断并终止 SSH 会话，则此脚本将在后台运行，但您可以从 " 恢复 " 页面查看进度。
- 如果存储节点使用 RSM 服务，则随着节点服务重新启动，脚本可能会暂停 5 分钟。每当 RSM 服务首次启动时，预计会有 5 分钟的延迟。

> RSM 服务位于包含此 ADC 服务的存储节点上。

> 某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

5. 在 `sn-recovery-postinstall.sh` 脚本运行时，监控网格管理器中的恢复页面。

" 恢复 " 页面上的进度条和阶段列可提供 `sn-recovery-postinstall.sh` 脚本的高级状态。



在 `sn-recovery-postinstall.sh` 脚本启动节点上的服务后，您可以将对象数据还原到由该脚本格式化的任何存储卷，如下一个操作步骤 中所述。

相关信息

查看有关存储节点系统驱动器恢复的警告

将对象数据还原到设备的存储卷

将对象数据还原到设备的存储卷

恢复设备存储节点的存储卷后，您可以还原存储节点发生故障时丢失的对象数据。

您需要的内容

- 您必须确认已恢复的存储节点的连接状态为 * 已连接 * 在网格管理器的 * 节点 * > * 概述 * 选项卡上。

关于此任务

可以从其他存储节点，归档节点或云存储池还原对象数据，前提是已配置网格的 ILM 规则，以便可以使用对象副本。

请注意以下事项：

- 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于出现故障的存储卷上，则您将无法恢复对象。
- 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。在执行此操作步骤 之前，请联系技术支持以帮助估算恢复时间范围和相关成本。
- 如果对象的唯一剩余副本位于归档节点上，则会从归档节点检索对象数据。从归档节点将对象数据还原到存储节点比从其他存储节点还原副本所需时间更长，因为从外部归档存储系统检索数据会产生延迟。

关于 repair-data 脚本

要还原对象数据，请运行 repair-data 脚本。此脚本将开始还原对象数据的过程，并与 ILM 扫描配合使用以确保满足 ILM 规则。

选择下面的 * 复制数据 * 或 * 擦除编码（ Erasure-Coded ， EC ）数据 * ，根据您要还原的是复制的数据还是擦除编码的数据，了解 repair-data 脚本的不同选项。如果需要还原这两种类型的数据，则必须同时运行这两组命令。

有关 repair-data 脚本的详细信息，请在主管理节点的命令行中输入 repair-data -help 。

复制的数据

根据您是需要修复整个节点还是仅需要修复节点上的特定卷，可以使用两个命令还原复制的数据：

```
repair-data start-replicated -node-repair

repair-data start-replicated -volume-repair
```

您可以使用以下命令跟踪已复制数据的修复：

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 show -replicate-repair-status 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ Erasure Coded ， EC ）数据

根据您是需要修复整个节点还是仅修复节点上的特定卷，可以使用两个命令来还原经过擦除编码的数据：

```
repair-data start-EC-node-repair

repair-data start-EC-volume-repair
```

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

您可以使用以下命令跟踪纠删编码数据的修复情况：

```
repair-data show-EC-repair-status
```

EC 修复作业会临时预留大量存储。可能会触发存储警报，但会在修复完成后解决。如果没有足够的存储空间用于预留， EC 修复作业将失败。无论作业失败还是成功， EC 修复作业完成后都会释放存储预留。

查找存储节点的主机名

1. 登录到主管理节点：

a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 使用 ` /etc/hosts` 文件查找已还原存储卷的存储节点的主机名。要查看网格中所有节点的列表，请输入以下内容： `cat /etc/hosts` 。

如果所有卷都发生故障，请修复数据

如果所有存储卷都发生故障，请修复整个节点。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果只有部分卷发生故障，请转至 [如果只有部分卷出现故障，请修复数据]。

您不能同时对多个节点运行 `repair-data` 操作。要恢复多个节点，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `repair-data start-replicated -node-repair` 命令和 ` -nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上复制的数据：

```
repair-data start-replicated -node-repair -nodes sg-DC-SN3
```

还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见 监控和故障排除。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `repair-data start-EC-node-repair` 命令和 ` -nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上的擦除编码数据：

```
repair-data start-EC-node-repair -nodes sg-DC-SN3
```

此操作将返回唯一的 `repair ID` ，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

如果只有部分卷出现故障，请修复数据

如果只有部分卷出现故障，请修复受影响的卷。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果所有卷都发生故障，请转至 [如果所有卷都发生故障，请修复数据]。

以十六进制格式输入卷 ID 。例如， `0000` 是第一个卷， `000f` 是第 16 个卷。您可以指定一个卷，一个卷范围或多个不属于一个序列的卷。

所有卷必须位于同一个存储节点上。如果需要还原多个存储节点的卷，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `sSTART-replicated -volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0002`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0002
```

- 卷范围 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0003` 到 `0009` 范围内的所有卷：

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 不在序列中的多个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0001`，`0005` 和 `0008`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0001 ,
0005 ,  0008
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见有关 StorageGRID 监控和故障排除的说明。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `sSTART-EC-volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0007`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 0007
```

- 卷范围 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0004` 到 `0006` 范围内的所有卷：

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- 不在序列中的多个卷 *： 此命令会将经过纠删编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `000a`， `000c` 和 `000E`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 000a ,  000c ,
000E
```

`repair-data` 操作将返回唯一的 `repair ID`，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

监控修复情况

根据您是使用 * 复制数据 * ， * 纠删编码（ EC ）数据 * 还是同时使用这两者来监控修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

恢复设备存储节点后检查存储状态

恢复设备存储节点后，您必须验证设备存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 检查 * 已恢复存储节点 * > * LDR* > * 存储 * > * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值。

   这两个属性的值均应为联机。

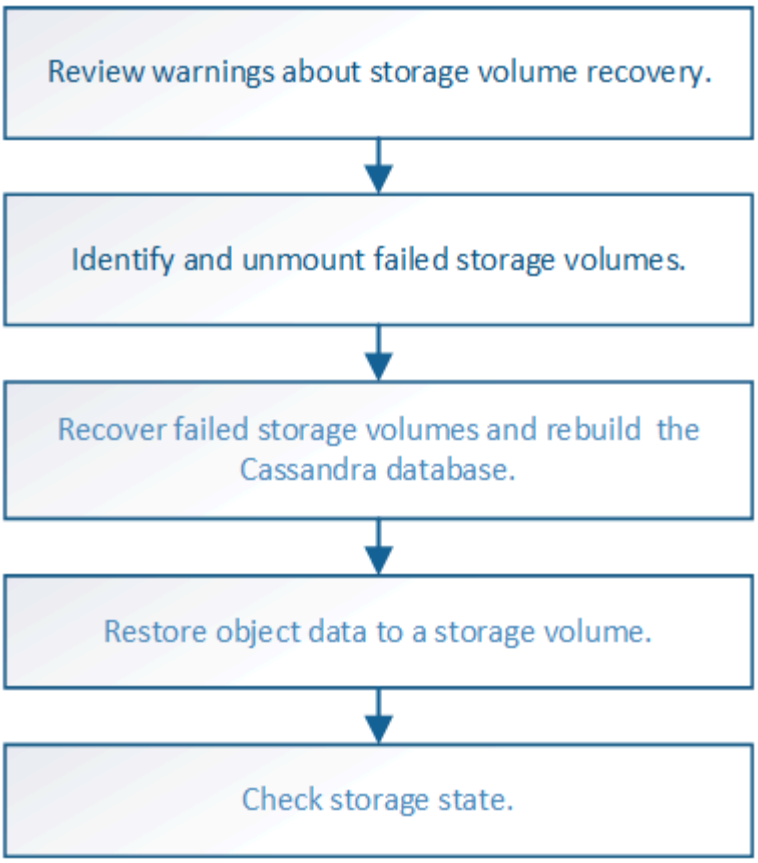
3. 如果 "Storage State" （存储状态）— "Desired " （所需）设置为只读，请完成以下步骤：
   a. 单击 * 配置 * 选项卡。
   b. 从 * 存储状态 - 所需 * 下拉列表中，选择 * 联机 * 。
   c. 单击 * 应用更改 * 。
   d. 单击 * 概述 * 选项卡并确认 * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值已更新为联机。

从系统驱动器完好无损的存储卷故障中恢复

您必须完成一系列任务，才能恢复基于软件的存储节点，如果此存储节点上的一个或多个存储卷发生故障，但系统驱动器完好无损。如果只有存储卷发生故障，则存储节点仍可供 StorageGRID 系统使用。

关于此任务

此恢复仅限基于 操作步骤 适用场景 软件的存储节点。如果设备存储节点上的存储卷发生故障，请使用操作步骤执行 "`Recover appliance Storage Node" 。`



相关信息

恢复设备存储节点

查看有关存储卷恢复的警告

在恢复存储节点的故障存储卷之前，您必须查看以下警告。

存储节点中的存储卷（或卷组）由十六进制数标识，该十六进制数称为卷 ID 。例如， 0000 是第一个卷， 000f 是第 16 个卷。每个存储节点上的第一个对象存储（卷 0 ）最多使用 4 TB 的空间来执行对象元数据和 Cassandra 数据库操作；该卷上的任何剩余空间都用于对象数据。所有其他存储卷专用于对象数据。

如果卷 0 发生故障并需要恢复，则 Cassandra 数据库可能会作为卷恢复操作步骤 的一部分进行重建。在以下情况下，还可以重建 Cassandra ：

- 存储节点脱机超过 15 天后将恢复联机。
- 系统驱动器和一个或多个存储卷发生故障并已恢复。

重建 Cassandra 后，系统将使用其他存储节点中的信息。如果脱机的存储节点过多，则某些 Cassandra 数据可能不可用。如果 Cassandra 最近已重建，则 Cassandra 数据可能尚未在网格中保持一致。如果在存储节点过多脱机时重建 Cassandra ，或者在彼此 15 天内重建两个或多个存储节点，则可能会发生数据丢失。

如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。在 15 天内在两个或多个存储节点上重建 Cassandra 可能会导致数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

如果在恢复期间遇到服务：状态 - Cassandra （ SVST ）警报，请参见有关通过重建 Cassandra 从警报中恢复的监控和故障排除说明。重建 Cassandra 后，应清除警报。如果未清除警报，请联系技术支持。

相关信息

监控和故障排除

有关网格节点恢复的警告和注意事项

确定并卸载故障存储卷

在恢复包含故障存储卷的存储节点时，您必须确定并卸载故障卷。您必须验证在恢复操作步骤 中仅重新格式化故障存储卷。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

您应尽快恢复发生故障的存储卷。

恢复过程的第一步是检测已断开连接，需要卸载或存在 I/O 错误的卷。如果故障卷仍然连接，但文件系统随机损坏，则系统可能无法检测到磁盘中未使用或未分配的部分有任何损坏。

您必须先完成此操作步骤 ，然后再执行手动步骤来恢复卷，例如添加或重新连接磁盘，停止节点，启动节点或重新启动。否则，在运行 `reformat_storage_block_devices.rb` 脚本时，可能会遇到文件系统错误，从而导致脚本挂起或失败。

在运行 `reboot` 命令之前，请修复硬件并正确连接磁盘。

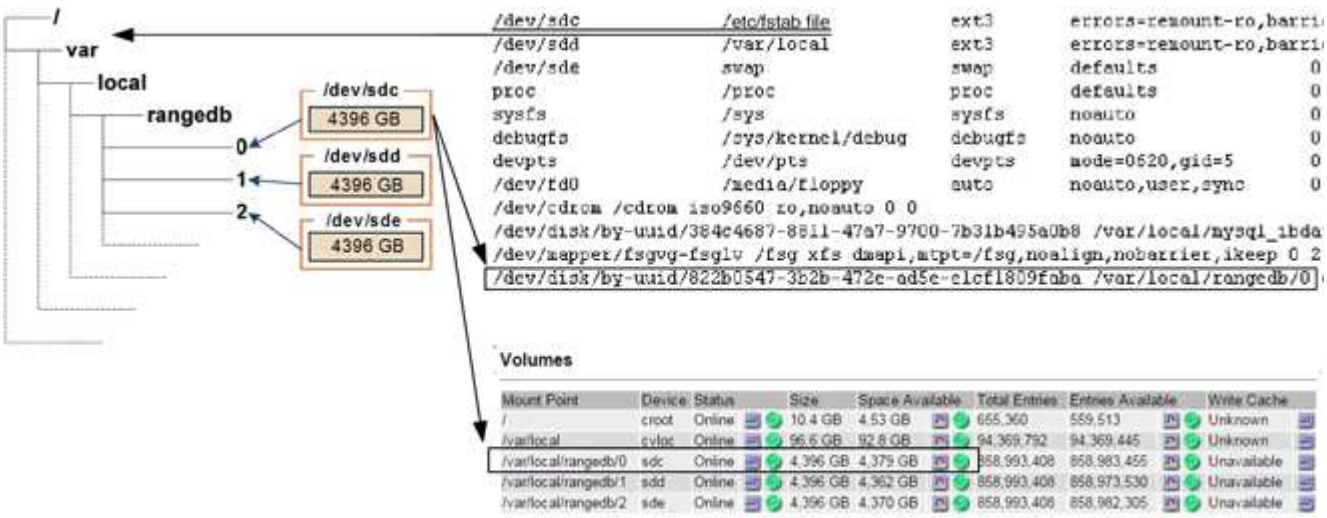
请仔细识别故障存储卷。您将使用此信息验证哪些卷必须重新格式化。重新格式化卷后，卷上的数据将无法恢复。

要正确恢复故障存储卷，您需要知道故障存储卷的设备名称及其卷 ID 。

在安装时，系统会为每个存储设备分配一个文件系统通用唯一标识符（ UUID ），并使用分配的文件系统 UUID 挂载到存储节点上的一个 rangedb 目录。文件系统 UUID 和 rangedb 目录将在 ` /etc/fstab` 文件中列出。网格管

理器中将显示设备名称，范围 b 目录以及已挂载卷的大小。

在以下示例中，设备 ` /dev/sdc` 的卷大小为 4 TB ，使用 `/etc/` 文件中的设备名称 ` /dev/disk/by-uid/822b0547-3b2E-472b-ad5e-e1cf1809faba` 挂载到 ` /var/local/rangedb/0` ：



步骤

1. 完成以下步骤以记录故障存储卷及其设备名称：

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

   b. 选择 * 站点 * > * 故障存储节点 * > * LDR* > * 存储 * > * 概述 * > * 主 * ，然后查找包含警报的对象存储。

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

   c. 选择 * 站点 * > * 故障存储节点 * > * SSM* > * 资源 * > * 概述 * > * 主 * 。确定上一步中确定的每个故障存储卷的挂载点和卷大小。

   对象存储以十六进制表示法进行编号。例如， 0000 是第一个卷， 000f 是第 16 个卷。在此示例中， ID 为 0000 的对象存储对应于设备名称为 sdc 且大小为 107 GB 的 ` /var/local/rangedb/0` 。

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. 登录到发生故障的存储节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

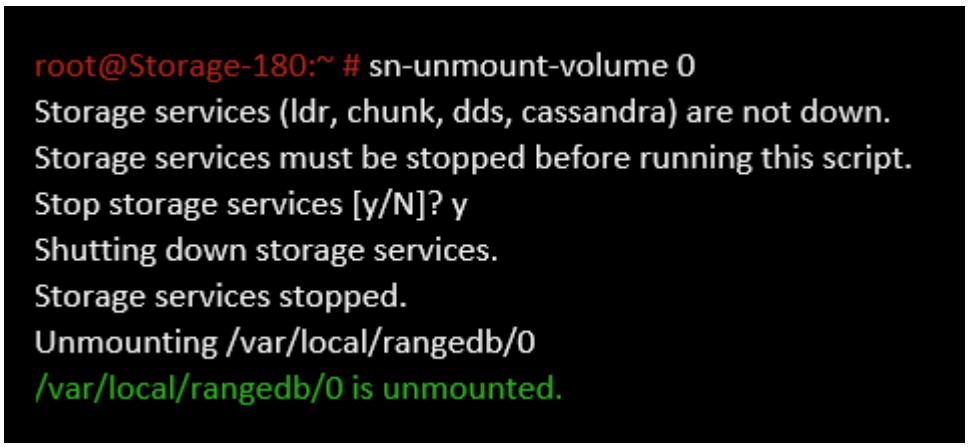
3. 运行以下脚本以停止存储服务并卸载故障存储卷：

   `sn-ununmount 卷 object_store_ID`

   `object_store_ID` 是故障存储卷的 ID 。例如，在命令中为 ID 为 0000 的对象存储指定 `0` 。

4. 如果出现提示，请按 * 。 * 停止存储节点上的存储服务。

   如果存储服务已停止，则不会提示您。仅对卷 0 停止 Cassandra 服务。

   几秒钟后，存储服务将停止，卷将卸载。此时将显示消息，指示此过程的每个步骤。最后一条消息指示卷已卸载。

恢复发生故障的存储卷并重建 **Cassandra** 数据库

您必须运行一个脚本来重新格式化和重新挂载故障存储卷上的存储，并在系统确定有必要时在存储节点上重建 Cassandra 数据库。

- 您必须具有 `passwords.txt` 文件。
- 服务器上的系统驱动器必须完好无损。
- 必须已确定故障的发生原因 ，必要时，必须已购买更换存储硬件。
- 替换存储的总大小必须与原始存储相同。
- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）

- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）
- 您已拥有 已查看有关存储卷恢复的警告。

a. 根据需要，更换与先前已确定并卸载的故障存储卷关联的故障物理或虚拟存储。

   更换存储后，请确保重新扫描或重新启动以确保操作系统能够识别该存储，但不要重新挂载卷。存储将重新挂载并在稍后的步骤中添加到 ` /etc/fstab` 中。

b. 登录到发生故障的存储节点：

   i. 输入以下命令： `ssh admin@ grid_node_ip_`

   ii. 输入 `passwords.txt` 文件中列出的密码。

   iii. 输入以下命令切换到 root： `su -`

   iv. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

c. 使用文本编辑器（ vi 或 vim ）从 ` /etc/fstab` 文件中删除故障卷，然后保存该文件。

   > 在 ` /etc/fstab` 文件中注释掉故障卷不足。必须从 `fstab` 中删除卷，因为恢复过程会验证 `fstab` 文件中的所有行是否与挂载的文件系统匹配。

d. 重新格式化任何发生故障的存储卷，并根据需要重建 Cassandra 数据库。输入： `reformat_storage_block_devices.rb`

   - 如果存储服务正在运行，系统将提示您停止这些服务。输入： *
   - 如果需要，系统将提示您重建 Cassandra 数据库。
     - 查看警告。如果其中任何一项都不适用，请重建 Cassandra 数据库。输入： *
     - 如果多个存储节点脱机或在过去 15 天内重建了另一个存储节点。输入： *

       该脚本将退出而不重建 Cassandra 。请联系技术支持。

   - 对于存储节点上的每个 rangedb 驱动器，当系统询问您以下问题时： **是否重新格式化 `rangedb` 驱动器 `<name>` （ `device` < 主要号码 >： < 次要号码 > ）？** `[Y/n]` **？** ，输入以下回答之一：

     - * y * 重新格式化出现错误的驱动器。这会重新格式化存储卷，并将重新格式化的存储卷添加到 ` /etc/fstab` 文件中。
     - 如果驱动器不包含任何错误，并且您不想重新格式化它，则为 * 否 * 。

       > 选择 * n * 将退出此脚本。挂载驱动器（如果您认为应保留驱动器上的数据且错误地卸载了驱动器）或删除驱动器。然后，再次运行 `reformat_storage_block_devices.rb` 命令。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

在以下示例输出中，必须重新格式化驱动器 ` /dev/sdf` ，而不需要重建 Cassandra ：

```
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.
```

将对象数据还原到系统驱动器完好无损的存储卷

在系统驱动器完好无损的存储节点上恢复存储卷后，您可以还原存储卷发生故障时丢失的对象数据。

您需要的内容

- 您必须确认已恢复的存储节点的连接状态为 * 已连接 * 在网格管理器的 * 节点 * > * 概述 * 选项卡上。

关于此任务

可以从其他存储节点，归档节点或云存储池还原对象数据，前提是已配置网格的 ILM 规则，以便可以使用对象副本。

请注意以下事项：

- 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于出现故障的存储卷上，则您将无法恢复对象。
- 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。在执行此操作步骤 之前，请联系技术支持以帮助估算恢复时间范围和相关成本。

- 如果对象的唯一剩余副本位于归档节点上，则会从归档节点检索对象数据。从归档节点将对象数据还原到存储节点比从其他存储节点还原副本所需时间更长，因为从外部归档存储系统检索数据会产生延迟。

关于 `repair-data` 脚本

要还原对象数据，请运行 `repair-data` 脚本。此脚本将开始还原对象数据的过程，并与 ILM 扫描配合使用以确保满足 ILM 规则。

选择下面的 * 复制数据 * 或 * 擦除编码（ Erasure-Coded ， EC ）数据 * ，根据您要还原的是复制的数据还是擦除编码的数据，了解 `repair-data` 脚本的不同选项。如果需要还原这两种类型的数据，则必须同时运行这两组命令。

有关 `repair-data` 脚本的详细信息，请在主管理节点的命令行中输入 `repair-data -help` 。

复制的数据

根据您是需要修复整个节点还是仅需要修复节点上的特定卷，可以使用两个命令还原复制的数据：

```
repair-data start-replicated -node-repair

repair-data start-replicated -volume-repair
```

您可以使用以下命令跟踪已复制数据的修复：

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

根据您是需要修复整个节点还是仅修复节点上的特定卷，可以使用两个命令来还原经过擦除编码的数据：

```
repair-data start-EC-node-repair

repair-data start-EC-volume-repair
```

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

您可以使用以下命令跟踪纠删编码数据的修复情况：

```
repair-data show-EC-repair-status
```

EC 修复作业会临时预留大量存储。可能会触发存储警报，但会在修复完成后解决。如果没有足够的存储空间用于预留， EC 修复作业将失败。无论作业失败还是成功， EC 修复作业完成后都会释放存储预留。

查找存储节点的主机名

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 使用 ` /etc/hosts` 文件查找已还原存储卷的存储节点的主机名。要查看网格中所有节点的列表，请输入以下内容： `cat /etc/hosts` 。

如果所有卷都发生故障，请修复数据

如果所有存储卷都发生故障，请修复整个节点。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果只有部分卷发生故障，请转至 [如果只有部分卷出现故障，请修复数据]。

> 您不能同时对多个节点运行 `repair-data` 操作。要恢复多个节点，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `repair-data start-replicated -node-repair` 命令和 `-nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上复制的数据：

```
repair-data start-replicated -node-repair -nodes sg-DC-SN3
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见 监控和故障排除。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `repair-data start-EC-node-repair` 命令和 `-nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上的擦除编码数据：

```
repair-data start-EC-node-repair -nodes sg-DC-SN3
```

此操作将返回唯一的 `repair ID` ，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

如果只有部分卷出现故障，请修复数据

如果只有部分卷出现故障，请修复受影响的卷。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果所有卷都发生故障，请转至 [如果所有卷都发生故障，请修复数据]。

以十六进制格式输入卷 ID 。例如， `0000` 是第一个卷， `000f` 是第 16 个卷。您可以指定一个卷，一个卷范围或多个不属于一个序列的卷。

所有卷必须位于同一个存储节点上。如果需要还原多个存储节点的卷，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `sSTART-replicated -volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0002`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0002
```

- 卷范围 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0003` 到 `0009` 范围内的所有卷：

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 不在序列中的多个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0001`，`0005` 和 `0008`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0001 ,
0005 ,  0008
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见有关 StorageGRID 监控和故障排除的说明。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `sSTART-EC-volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0007`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 0007
```

- 卷范围 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0004` 到 `0006` 范围内的所有卷：

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- 不在序列中的多个卷 *： 此命令会将经过纠删编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `000a`， `000c` 和 `000E`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 000a ,  000c ,
000E
```

`repair-data` 操作将返回唯一的 `repair ID`，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

监控修复情况

根据您是使用 * 复制数据 * ， * 纠删编码（ EC ）数据 * 还是同时使用这两者来监控修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

恢复存储卷后检查存储状态

恢复存储卷后，您必须验证存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 检查 * 已恢复存储节点 * > * LDR* > * 存储 * > * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值。

   这两个属性的值均应为联机。

3. 如果 "Storage State" （存储状态）— "Desired " （所需）设置为只读，请完成以下步骤：
   a. 单击 * 配置 * 选项卡。
   b. 从 * 存储状态 - 所需 * 下拉列表中，选择 * 联机 * 。
   c. 单击 * 应用更改 * 。
   d. 单击 * 概述 * 选项卡并确认 * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值已更新为联机。

从系统驱动器故障中恢复

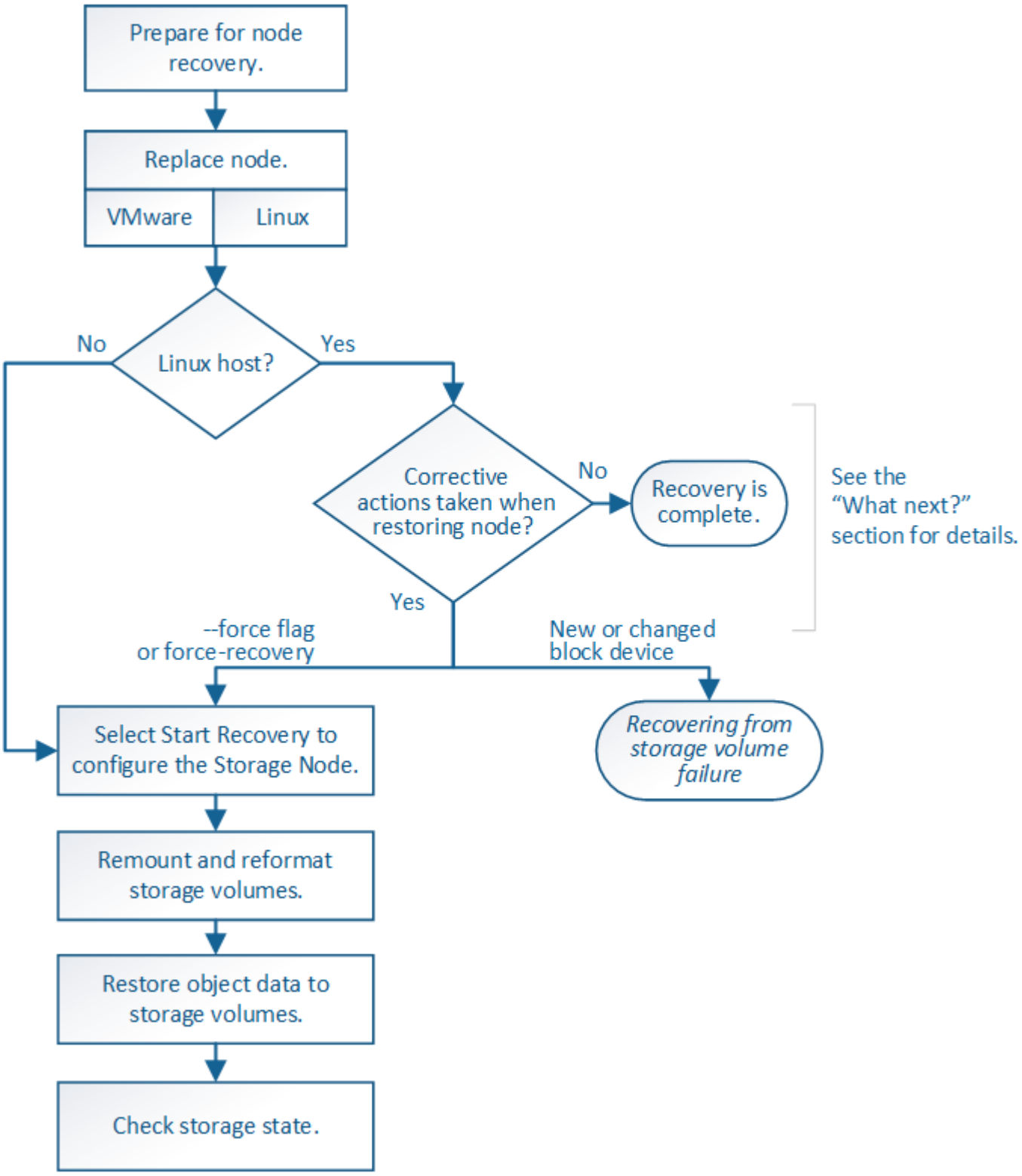
如果基于软件的存储节点上的系统驱动器发生故障，则此存储节点不可用于 StorageGRID 系统。您必须完成一组特定任务才能从系统驱动器故障中恢复。

关于此任务

使用此操作步骤 从基于软件的存储节点上的系统驱动器故障中恢复。此操作步骤 包括在任何存储卷同样出现故障或无法重新挂载时应遵循的步骤。

仅限此基于 操作步骤 适用场景 软件的存储节点。要恢复设备存储节点，您必须遵循其他操作步骤 。

恢复设备存储节点



查看有关存储节点系统驱动器恢复的警告

在恢复存储节点的故障系统驱动器之前，您必须查看以下警告。

存储节点具有包含对象元数据的 Cassandra 数据库。在以下情况下，可能会重建 Cassandra 数据库：

- 存储节点脱机超过 15 天后将恢复联机。
- 存储卷出现故障并已恢复。
- 系统驱动器和一个或多个存储卷发生故障并已恢复。

重建 Cassandra 后，系统将使用其他存储节点中的信息。如果脱机的存储节点过多，则某些 Cassandra 数据可能不可用。如果 Cassandra 最近已重建，则 Cassandra 数据可能尚未在网格中保持一致。如果在存储节点过多脱机时重建 Cassandra ，或者在彼此 15 天内重建两个或多个存储节点，则可能会发生数据丢失。

如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。在 15 天内在两个或多个存储节点上重建 Cassandra 可能会导致数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

如果此存储节点处于只读维护模式，以便允许存储卷出现故障的另一个存储节点检索对象，请先在存储卷出现故障的存储节点上恢复卷，然后再恢复此故障存储节点。请参见有关从系统驱动器完好无损的存储卷丢失中恢复的说明。

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

如果在恢复期间遇到服务：状态 - Cassandra （ SVST ）警报，请参见有关通过重建 Cassandra 从警报中恢复的监控和故障排除说明。重建 Cassandra 后，应清除警报。如果未清除警报，请联系技术支持。

相关信息

监控和故障排除

有关网格节点恢复的警告和注意事项

从系统驱动器完好无损的存储卷故障中恢复

更换存储节点

如果系统驱动器发生故障，您必须先更换存储节点。

您必须为您的平台选择节点替代操作步骤 。对于所有类型的网格节点，更换节点的步骤都相同。

仅限此基于 操作步骤 适用场景 软件的存储节点。要恢复设备存储节点，您必须遵循其他操作步骤 。

恢复设备存储节点

- Linux： * 如果您不确定系统驱动器是否出现故障，请按照说明更换节点以确定需要执行哪些恢复步骤。

平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

选择启动恢复以配置存储节点

更换存储节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。
- 您必须知道擦除编码数据的任何修复作业的开始日期。
- 您必须已确认过去 15 天内未重建此存储节点。

关于此任务

如果存储节点作为容器安装在 Linux 主机上，则只有在满足以下条件之一时，才必须执行此步骤：

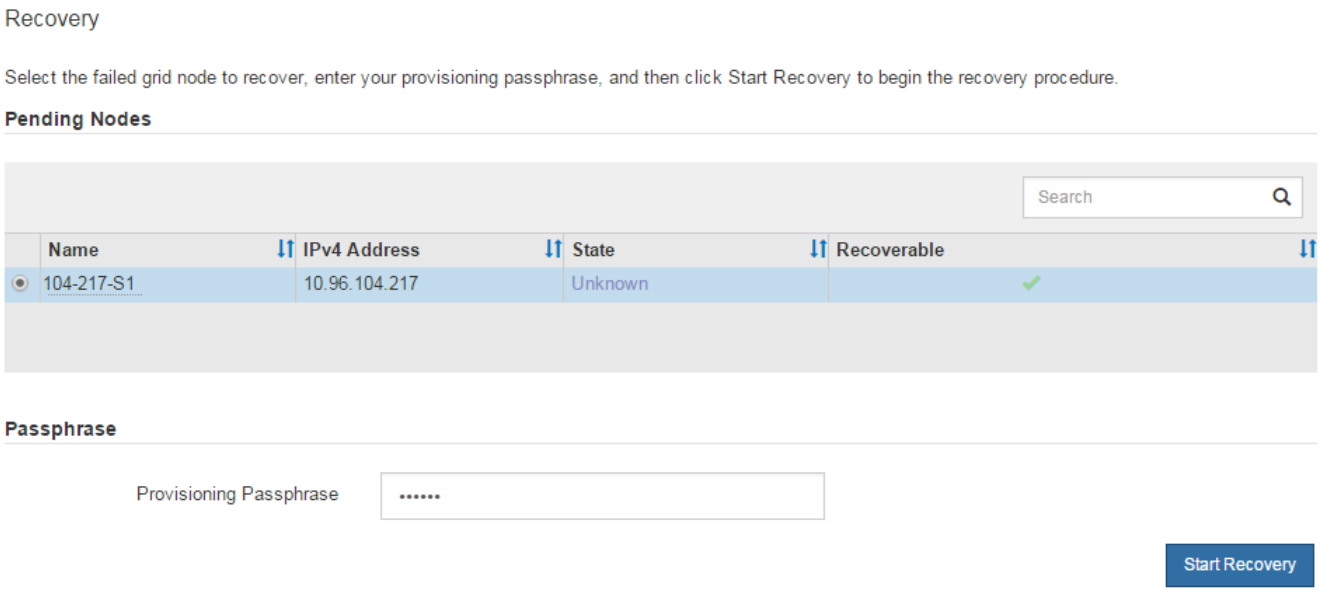
- 您必须使用 ` -force` 标志导入节点，或者发出 `StorageGRID node force-recovery node-name`
- 您必须执行完整节点重新安装，或者需要还原 /var/local 。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

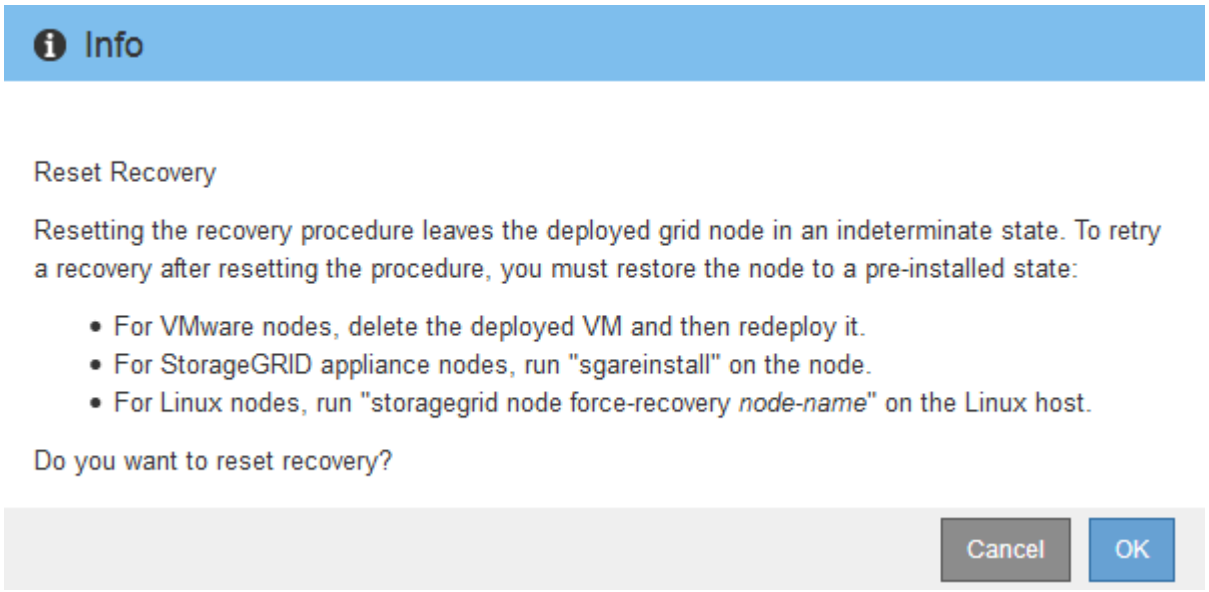
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

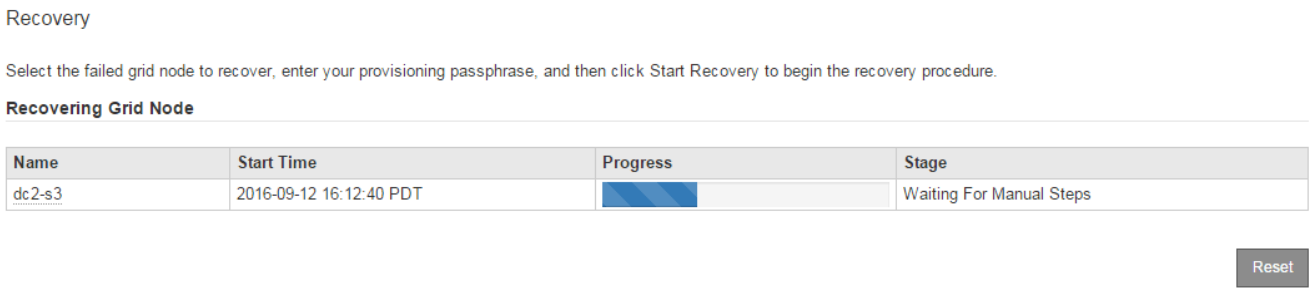
> 在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`

6. 当存储节点达到 "`Waiting for Manual steps` " 阶段时，请转至恢复操作步骤 中的下一个任务以重新挂载和重新格式化存储卷。



相关信息

准备要重新安装的设备（仅限平台更换）

重新挂载并重新格式化存储卷（ " 手动步骤 " ）

要重新挂载保留的存储卷并重新格式化任何故障存储卷，您必须手动运行两个脚本。第一个脚本将重新挂载格式正确的卷，使其格式化为 StorageGRID 存储卷。第二个脚本将重新格式化所有已卸载的卷，根据需要重新构建 Cassandra 并启动服务。

您需要的内容

- 您已更换已知需要更换的任何故障存储卷的硬件。

  运行 `sn-remount-volumes` 脚本可能有助于您确定其他故障存储卷。

- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）
- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）
- 您已拥有 已查看有关存储节点系统驱动器恢复的警告。

> 如果多个存储节点脱机或此网格中的存储节点在过去 15 天内已重建，请联系技术支持。请勿运行 `sn-recovery-postinstall.sh` 脚本。在两个或多个存储节点上相互重建 Cassandra 的 15 天内可能会导致数据丢失。

关于此任务

要完成此操作步骤 ，请执行以下高级任务：

- 登录到已恢复的存储节点。
- 运行 `sn-remount-volumes` 脚本重新挂载格式正确的存储卷。运行此脚本时，它将执行以下操作：
  - 挂载和卸载每个存储卷以重放 XFS 日志。
  - 执行 XFS 文件一致性检查。
  - 如果文件系统一致，则确定存储卷是否为格式正确的 StorageGRID 存储卷。
  - 如果存储卷格式正确，请重新挂载该存储卷。卷上的所有现有数据保持不变。
- 查看脚本输出并解决任何问题。
- 运行 `sn-recovery-postinstall.sh` 脚本。运行此脚本时，它将执行以下操作。

运行之前、请勿在恢复期间重新启动存储节点 `sn-recovery-postinstall.sh` 重新格式化故障存储卷并还原对象元数据。之前重新启动存储节点 `sn-recovery-postinstall.sh` 完成会导致尝试启动的服务出错、并导致StorageGRID 设备节点退出维护模式。请参见的步骤 安装后脚本。

- 重新格式化 `sn-remount-volumes` 脚本无法挂载或发现格式不正确的任何存储卷。

  如果重新格式化某个存储卷，则该卷上的所有数据都将丢失。假设已将 ILM 规则配置为存储多个对象副本，则必须执行额外的操作步骤 以从网格中的其他位置还原对象数据。

- 如果需要，在节点上重建 Cassandra 数据库。
- 启动存储节点上的服务。

步骤

1. 登录到已恢复的存储节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 运行第一个脚本重新挂载任何格式正确的存储卷。

   如果所有存储卷都是新的，需要进行格式化，或者所有存储卷都出现故障，您可以跳过此步骤并运行第二个脚本，重新格式化所有已卸载的存储卷。

   a. 运行以下脚本： `sn-remount-volumes`

   此脚本可能需要数小时才能在包含数据的存储卷上运行。

   b. 在脚本运行期间，查看输出并问题解答 任何提示。

   根据需要，您可以使用 `tail -f` 命令监控脚本日志文件的内容（` /var/local/log/SN-remount-volumes.log` ）。日志文件包含比命令行输出更详细的信息。

```
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.
```

在示例输出中，一个存储卷已成功重新挂载，三个存储卷出现错误。

- ` /dev/sdb` 通过了 XFS 文件系统一致性检查，并具有有效的卷结构，因此已成功重新挂载。此脚本重新挂载的设备上的数据将保留下来。
- 由于存储卷是新的或已损坏， ` /dev/sdc` 未通过 XFS 文件系统一致性检查。
- 无法挂载 ` /dev/sdd` ，因为磁盘已取消初始化或磁盘的超级块已损坏。当脚本无法挂载存储卷时，它会询问您是否要运行文件系统一致性检查。
  - 如果存储卷已连接到新磁盘，请将 * N * 问题解答 到提示符处。您无需检查新磁盘上的文件系统。
  - 如果存储卷已连接到现有磁盘，问题解答 请将 * 。 *您可以使用文件系统检查的结果来确定损坏的来源。结果将保存在 ` /var/local/log/sn-remount-volumes.log` 日志文件中。
- ` dev/sde` 已通过 XFS 文件系统一致性检查，并且卷结构有效；但是， volID 文件中的 LDR 节点 ID 与此存储节点的 ID 不匹配（顶部显示的 `configured LDR noid` ）。此消息表示此卷属于另一个

存储节点。

3. 查看脚本输出并解决任何问题。

> 如果存储卷未通过 XFS 文件系统一致性检查或无法挂载，请仔细查看输出中的错误消息。您必须了解在这些卷上运行 `sn-recovery-postinstall.sh` 脚本的含义。

a. 检查以确保结果中包含所需所有卷的条目。如果未列出任何卷，请重新运行此脚本。

b. 查看所有已挂载设备的消息。确保没有指示存储卷不属于此存储节点的错误。

在此示例中，` /dev/sde` 的输出包含以下错误消息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 如果报告某个存储卷属于另一个存储节点，请联系技术支持。如果运行 `sn-recovery-postinstall.sh` 脚本，则存储卷将重新格式化，从而可能会丢失发生原因 数据。

c. 如果无法挂载任何存储设备，请记下此设备的名称，然后修复或更换此设备。

> 您必须修复或更换任何无法挂载的存储设备。

您将使用设备名称查找卷 ID ，在运行 `repair-data` 脚本将对象数据还原到卷（下一个操作步骤 ）时，需要输入此 ID 。

d. 修复或更换所有无法挂载的设备后，再次运行 `sn-remount-volumes` 脚本，以确认可以重新挂载的所有存储卷均已重新挂载。

> 如果无法挂载存储卷或存储卷格式不正确，而您继续执行下一步，则此卷以及此卷上的任何数据将被删除。如果对象数据有两个副本，则只有一个副本，直到完成下一个操作步骤（还原对象数据）为止。

> 如果您认为无法从网格中的其他位置重建故障存储卷上的剩余数据，请勿运行 `sn-recovery-postinstall.sh` 脚本（例如， ILM 策略使用的规则仅创建一个副本或卷在多个节点上发生故障）。请联系技术支持以确定如何恢复数据。

4. 运行 `sn-recovery-postinstall.sh` 脚本： `sn-recovery-postinstall.sh`

此脚本将重新格式化无法挂载或格式不正确的任何存储卷；根据需要在节点上重建 Cassandra 数据库；并启动存储节点上的服务。

请注意以下事项：

- 此脚本可能需要数小时才能运行。
- 通常，在脚本运行期间，您应单独保留 SSH 会话。
- SSH 会话处于活动状态时，请勿按 * 。 Ctrl+C* 。

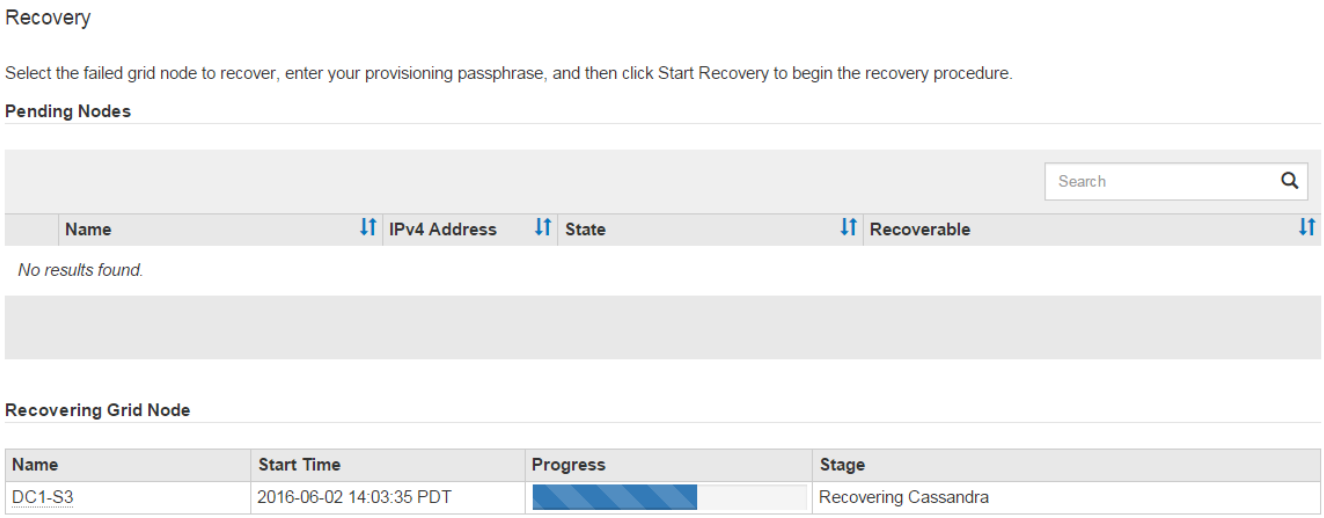
- 如果发生网络中断并终止 SSH 会话，则此脚本将在后台运行，但您可以从 " 恢复 " 页面查看进度。
- 如果存储节点使用 RSM 服务，则随着节点服务重新启动，脚本可能会暂停 5 分钟。每当 RSM 服务首次启动时，预计会有 5 分钟的延迟。

RSM 服务位于包含此 ADC 服务的存储节点上。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

5. [[post-install-script-step]]作为 `sn-recovery-postinstall.sh` 脚本运行时、监控网格管理器中的恢复页面。

" 恢复 " 页面上的进度条和阶段列可提供 `sn-recovery-postinstall.sh` 脚本的高级状态。



在 `sn-recovery-postinstall.sh` 脚本启动节点上的服务后，您可以将对象数据还原到该脚本格式化的任何存储卷，如该操作步骤 中所述。

相关信息

查看有关存储节点系统驱动器恢复的警告

根据需要将对象数据还原到存储卷

根据需要将对象数据还原到存储卷

如果需要使用 `sn-recovery-postinstall.sh` 脚本重新格式化一个或多个故障存储卷，则必须将对象数据从其他存储节点和归档节点还原到重新格式化的存储卷。除非重新格式化了一个或多个存储卷，否则不需要执行这些步骤。

您需要的内容

- 您必须确认已恢复的存储节点的连接状态为 * 已连接 * 在网格管理器的 * 节点 * > * 概述 * 选项卡上。

关于此任务

可以从其他存储节点，归档节点或云存储池还原对象数据，前提是已配置网格的 ILM 规则，以便可以使用对象副本。

请注意以下事项：

- 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于出现故障的存储卷上，则您将无法恢复对象。
- 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。在执行此操作步骤 之前，请联系技术支持以帮助估算恢复时间范围和相关成本。
- 如果对象的唯一剩余副本位于归档节点上，则会从归档节点检索对象数据。从归档节点将对象数据还原到存储节点比从其他存储节点还原副本所需时间更长，因为从外部归档存储系统检索数据会产生延迟。

关于 `repair-data` 脚本

要还原对象数据，请运行 `repair-data` 脚本。此脚本将开始还原对象数据的过程，并与 ILM 扫描配合使用以确保满足 ILM 规则。

选择下面的 * 复制数据 * 或 * 擦除编码（ Erasure-Coded ， EC ）数据 * ，根据您要还原的是复制的数据还是擦除编码的数据，了解 `repair-data` 脚本的不同选项。如果需要还原这两种类型的数据，则必须同时运行这两组命令。

> 有关 `repair-data` 脚本的详细信息，请在主管理节点的命令行中输入 `repair-data -help` 。

复制的数据

根据您是需要修复整个节点还是仅需要修复节点上的特定卷，可以使用两个命令还原复制的数据：

```
repair-data start-replicated -node-repair

repair-data start-replicated -volume-repair
```

您可以使用以下命令跟踪已复制数据的修复：

```
repair-data show-repliced-repair-status
```

> 在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

根据您是需要修复整个节点还是仅修复节点上的特定卷，可以使用两个命令来还原经过擦除编码的数据：

```
repair-data start-EC-node-repair

repair-data start-EC-volume-repair
```

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

您可以使用以下命令跟踪纠删编码数据的修复情况：

```
repair-data show-EC-repair-status
```

> EC 修复作业会临时预留大量存储。可能会触发存储警报，但会在修复完成后解决。如果没有足够的存储空间用于预留， EC 修复作业将失败。无论作业失败还是成功， EC 修复作业完成后都会释放存储预留。

查找存储节点的主机名

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 使用 ` /etc/hosts` 文件查找已还原存储卷的存储节点的主机名。要查看网格中所有节点的列表，请输入以下内容： `cat /etc/hosts` 。

如果所有卷都发生故障，请修复数据

如果所有存储卷都发生故障，请修复整个节点。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果只有部分卷发生故障，请转至 [如果只有部分卷出现故障，请修复数据]。

您不能同时对多个节点运行 `repair-data` 操作。要恢复多个节点，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `repair-data start-replicated -node-repair` 命令和 `-nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上复制的数据：

```
repair-data start-replicated -node-repair -nodes sg-DC-SN3
```

还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见 监控和故障排除。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `repair-data start-EC-node-repair` 命令和 `-nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上的擦除编码数据：

```
repair-data start-EC-node-repair -nodes sg-DC-SN3
```

此操作将返回唯一的 `repair ID` ，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

如果只有部分卷出现故障，请修复数据

如果只有部分卷出现故障，请修复受影响的卷。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果所有卷都发生故障，请转至 [如果所有卷都发生故障，请修复数据]。

以十六进制格式输入卷 ID 。例如， `0000` 是第一个卷， `000f` 是第 16 个卷。您可以指定一个卷，一个卷范围或多个不属于一个序列的卷。

所有卷必须位于同一个存储节点上。如果需要还原多个存储节点的卷，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `sSTART-replicated -volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0002`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0002
```

- 卷范围 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0003` 到 `0009` 范围内的所有卷：

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 不在序列中的多个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0001`，`0005` 和 `0008`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0001 ,
0005 ,  0008
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见有关 StorageGRID 监控和故障排除的说明。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `sSTART-EC-volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0007`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 0007
```

- 卷范围 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0004` 到 `0006` 范围内的所有卷：

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- 不在序列中的多个卷 *： 此命令会将经过纠删编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `000a`， `000c` 和 `000E`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 000a ,  000c ,
000E
```

`repair-data` 操作将返回唯一的 `repair ID`，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

监控修复情况

根据您是使用 * 复制数据 * ， * 纠删编码（ EC ）数据 * 还是同时使用这两者来监控修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

恢复存储节点系统驱动器后检查存储状态

恢复存储节点的系统驱动器后，您必须验证存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 检查 * 已恢复存储节点 * > * LDR* > * 存储 * > * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值。

   这两个属性的值均应为联机。

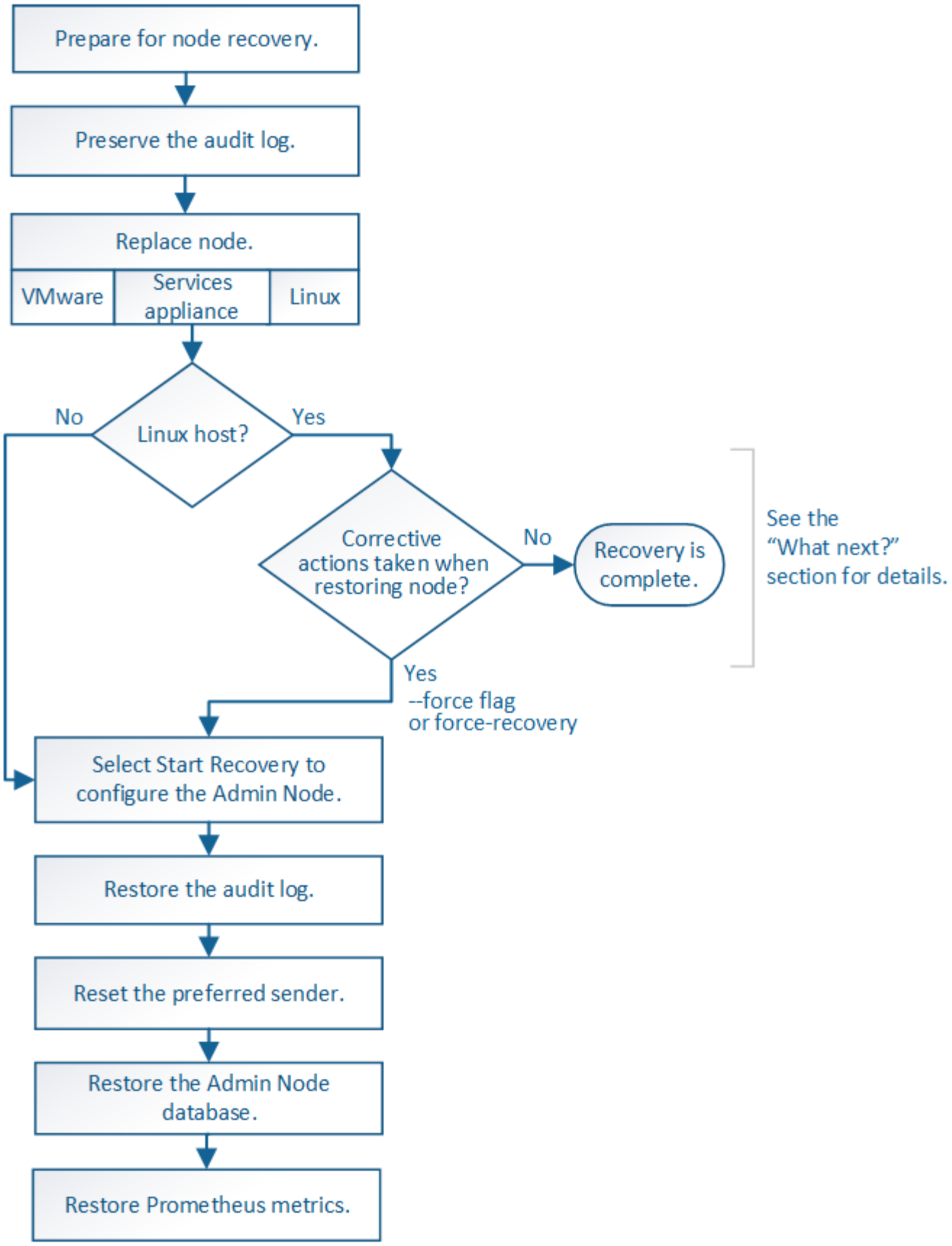
3. 如果 "Storage State" （存储状态）— "Desired " （所需）设置为只读，请完成以下步骤：
   a. 单击 * 配置 * 选项卡。
   b. 从 * 存储状态 - 所需 * 下拉列表中，选择 * 联机 * 。
   c. 单击 * 应用更改 * 。
   d. 单击 * 概述 * 选项卡并确认 * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值已更新为联机。

从管理节点故障中恢复

管理节点的恢复过程取决于它是主管理节点还是非主管理节点。

关于此任务

恢复主管理节点或非主管理节点的高级步骤相同，但具体步骤有所不同。



对于要恢复的管理节点，请始终遵循正确的恢复操作步骤 。这些过程从较高的层面来看是相同的，但细节却有所不同。

相关信息

SG100 和 SG1000 服务设备

选项

- 从主管理节点故障中恢复
- 从非主管理节点故障中恢复

从主管理节点故障中恢复

要从主管理节点故障中恢复，您必须完成一组特定的任务。主管理节点托管网格的配置管理节点（ CMN ）服务。

关于此任务

应立即更换发生故障的主管理节点。主管理节点上的配置管理节点（ CMN ）服务负责为网格发出对象标识符块。这些标识符将在载入对象时分配给对象。除非具有可用标识符，否则无法载入新对象。由于网格中缓存了大约一个月的标识符，因此在 CMN 不可用时，对象载入可以继续。但是，在缓存的标识符用尽后，无法添加任何新对象。

> 您必须在大约一个月内修复或更换发生故障的主管理节点，否则网格可能无法载入新对象。确切的时间段取决于对象载入率：如果您需要更准确地评估网格的时间范围，请联系技术支持。

从发生故障的主管理节点复制审核日志

如果您能够从出现故障的主管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的主管理节点启动并运行后将保留的审核日志还原到该节点。

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

> 如果现在无法在出现故障的管理节点上访问审核日志，您可以稍后访问这些日志，例如在主机恢复之后。

1. 如果可能，请登录到出现故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果有）。
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 停止 AMS 服务以防止其创建新的日志文件：`sservice AMS stop`
3. 重命名 audit.log 文件，使其在复制到已恢复的管理节点时不会覆盖现有文件。

将 audit.log 重命名为唯一编号的文件名，例如 yyyy-mm-dd.txt.1 。例如，您可以将 audit.log 文件重命名为 2015-10-25.txt 。 1cd /var/local/audit/exportls -l``mv audit.log 2015-10-25.1

4. 重新启动 AMS 服务： `sservice AMS start`
5. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@ grid_node_ip_ mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

6. 复制所有审核日志文件： `scp -p * admin@ grid_node_ip_ ： /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

7. 以 root 用户身份注销： `exit`

更换主管理节点

要恢复主管理节点，必须先更换物理或虚拟硬件。

您可以将出现故障的主管理节点替换为在同一平台上运行的主管理节点，也可以将在 VMware 或 Linux 主机上运行的主管理节点替换为服务设备上托管的主管理节点。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将引导您进入主管理节点恢复的下一步。

更换平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
SG100 和 SG1000 服务设备	更换服务设备
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

配置替代主管理节点

必须将替代节点配置为 StorageGRID 系统的主管理节点。

您需要的内容

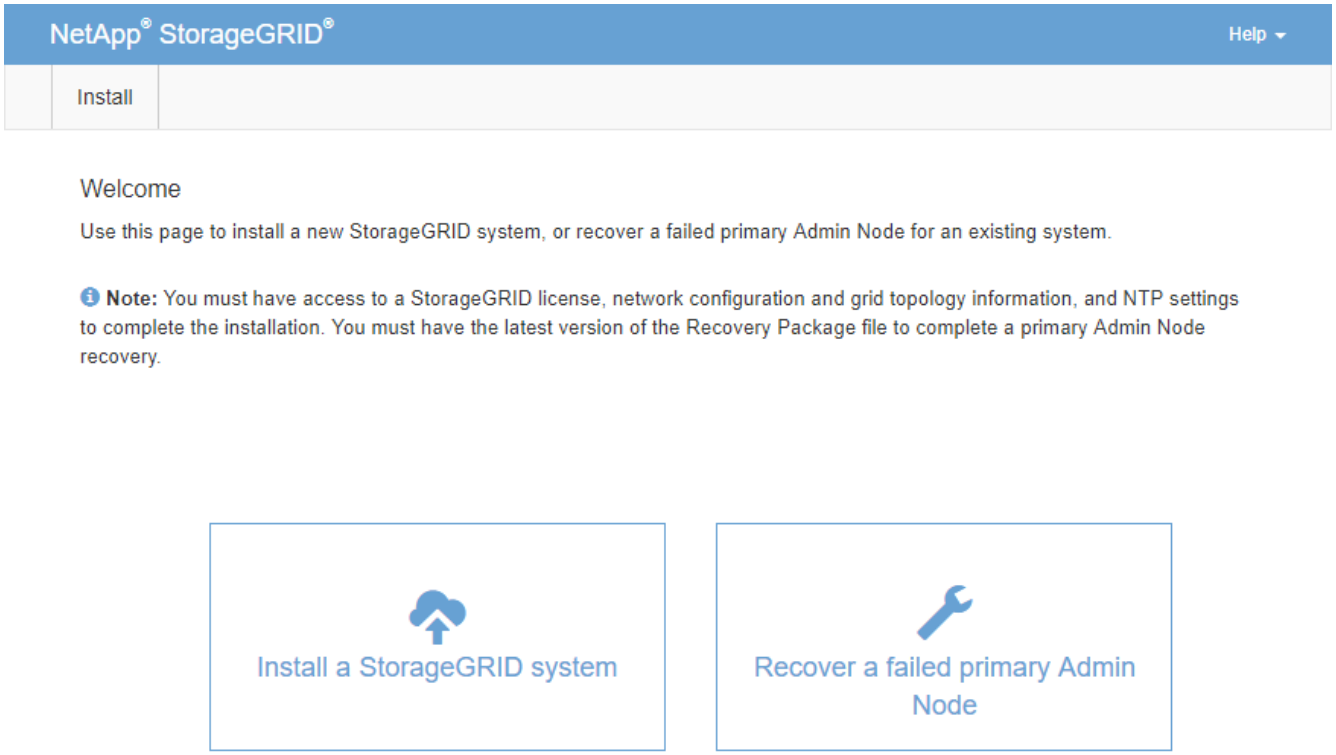
- 对于虚拟机上托管的主管理节点，必须部署，启动和初始化虚拟机。
- 对于服务设备上托管的主管理节点，您已更换此设备并安装了软件。请参见适用于您的设备的安装指南。

  SG100 和 SG1000 服务设备

- 您必须拥有恢复软件包文件的最新备份（ `sGWS-recovery-package-id-revision.zip` ）。
- 您必须具有配置密码短语。

步骤

1. 打开 Web 浏览器并导航到 `https://primary_admin_node_ip` 。



2. 单击 * 恢复发生故障的主管理节点 * 。
3. 上传恢复包的最新备份：
   a. 单击 * 浏览 * 。
   b. 找到 StorageGRID 系统的最新恢复软件包文件，然后单击 * 打开 * 。
4. 输入配置密码短语。
5. 单击 * 启动恢复 * 。

   恢复过程开始。随着所需服务的启动，网格管理器可能会在几分钟内不可用。恢复完成后，将显示登录页面。

6. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

   要配置依赖方信任，请参见有关管理 StorageGRID 的说明。要访问默认服务器证书，请登录到管理节点的命令 Shell 。转至 ` /var/local/mgmt-api` 目录，然后选择 `server.crt` 文件。

7. 确定是否需要应用修补程序。

a. 使用登录到网格管理器 支持的 Web 浏览器。

b. 选择 * 节点 * 。

c. 从左侧列表中，选择主管理节点。

d. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。

e. 选择任何其他网格节点。

f. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。

- 如果 * 软件版本 * 字段中显示的版本相同，则无需应用修补程序。
- 如果 * 软件版本 * 字段中显示的版本不同，则必须应用修补程序将恢复的主管理节点更新到相同版本。

相关信息

管理 StorageGRID

StorageGRID 热修补程序操作步骤

在已恢复的主管理节点上还原审核日志

如果能够保留故障主管理节点中的审核日志，则可以将其复制到要恢复的主管理节点。

- 必须安装并运行已恢复的管理节点。
- 在原始管理节点出现故障后，您必须已将审核日志复制到其他位置。

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点，并且无法从故障节点复制审核日志，则恢复的管理节点会开始将事件记录到审核日志中，就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：

- 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
- 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。

请参见 配置审核消息和日志目标 了解详细信息。

步骤

1. 登录到已恢复的管理节点：

a. 输入以下命令： `ssh admin@recovery_Admin_Node_IP`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录后，提示符将从 ` $` 更改为 ` #` 。

2. 检查已保留哪些审核文件： `cd /var/local/audit/export`
3. 将保留的审核日志文件复制到已恢复的管理节点： `scp admin@ grid_node_ip_ : /var/local/tmp/saved-audit-logs/yyy*` 。

   出现提示时，输入 admin 的密码。

4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复管理节点上审核日志文件的用户和组设置： `chown AMS-user : bycast *`
6. 以 root 用户身份注销： `exit`

您还必须还原对审核共享的任何已有客户端访问。有关详细信息，请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

重置已恢复的主管理节点上的首选发送器

如果您要恢复的主管理节点当前设置为警报通知，警报通知和 AutoSupport 消息的首选发送方，则必须重新配置此设置。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 必须安装并运行已恢复的管理节点。

步骤

1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。
2. 从 * 首选发件人 * 下拉列表中选择已恢复的管理节点。
3. 单击 * 应用更改 * 。

相关信息

管理 StorageGRID

恢复主管理节点时还原管理节点数据库

如果要在出现故障的主管理节点上保留有关属性，警报和警报的历史信息，则可以还原管理节点数据库。只有当 StorageGRID 系统包含另一个管理节点时，才能还原此数据库。

- 必须安装并运行已恢复的管理节点。

- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 警报历史记录
- 历史属性数据，用于 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的图表和文本报告。

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统一部分或稍后添加的服务器和服务的信息。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将管理节点数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史信息。如果您的系统只有主管理节点，则无法还原管理节点数据库。

> 复制管理节点数据库可能需要几小时的时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 从源管理节点中，停止 MI 服务： `service mi stop`
3. 从源管理节点中，停止管理应用程序接口（ Management Application Program Interface ， mgmt-API ）服务： `service mgmt-api stop`
4. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 停止 MI 服务： `service mi stop`
   c. 停止 mgmt-api 服务： `service mgmt-api stop`
   d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   e. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。
   f. 将数据库从源管理节点复制到已恢复的管理节点： ` /usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. 出现提示时，确认要覆盖已恢复的管理节点上的 MI 数据库。

数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。

h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

5. 在源管理节点上重新启动服务： `service servermanager start`

恢复主管理节点时还原 **Prometheus** 指标

或者，您也可以在出现故障的主管理节点上保留 Prometheus 维护的历史指标。只有当您的 StorageGRID 系统包含另一个管理节点时，才能还原 Prometheus 指标。

- 必须安装并运行已恢复的管理节点。
- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将 Prometheus 数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史指标。如果您的系统只有主管理节点，则无法还原 Prometheus 数据库。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 从源管理节点中，停止 Prometheus 服务： `sservice Prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 停止 Prometheus 服务： `sservice Prometheus stop`

c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

d. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

e. 将 Prometheus 数据库从源管理节点复制到已恢复的管理节点：` /usr/local/Prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

已克隆数据库，正在启动服务

a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

4. 在源管理节点上重新启动 Prometheus 服务。 `sservice Prometheus start`

从非主管理节点故障中恢复

要从非主管理节点故障中恢复，您必须完成以下任务。一个管理节点托管配置管理节点（ CMN ）服务，称为主管理节点。尽管可以有多个管理节点，但每个 StorageGRID 系统仅包含一个主管理节点。所有其他管理节点均为非主管理节点。

相关信息

SG100 和 SG1000 服务设备

从出现故障的非主管理节点复制审核日志

如果您能够从出现故障的管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的非主管理节点启动并运行后将保留的审核日志还原到该节点。

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

如果现在无法在出现故障的管理节点上访问审核日志，您可以稍后访问这些日志，例如在主机恢复之后。

1. 如果可能，请登录到出现故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果有）。

a. 输入以下命令： `ssh admin@grid_node_ip`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止 AMS 服务以防止其创建新的日志文件：`sservice AMS stop`
3. 重命名 audit.log 文件，使其在复制到已恢复的管理节点时不会覆盖现有文件。

   将 audit.log 重命名为唯一编号的文件名，例如 yyyy-mm-dd.txt.1 。例如，您可以将 audit.log 文件重命名为 2015-10-25.txt 。 `1cd /var/local/audit/exportls -l``mv audit.log 2015-10-25.1`
4. 重新启动 AMS 服务： `sservice AMS start`
5. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@grid_node_ip mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。
6. 复制所有审核日志文件： `scp -p * admin@grid_node_ip ： /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。
7. 以 root 用户身份注销： `exit`

更换非主管理节点

要恢复非主管理节点，必须首先更换物理或虚拟硬件。

您可以将出现故障的非主管理节点替换为在同一平台上运行的非主管理节点，也可以将 VMware 上运行的非主管理节点或 Linux 主机替换为服务设备上托管的非主管理节点。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将指导您执行非主管理节点恢复的下一步。

更换平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
SG100 和 SG1000 服务设备	更换服务设备
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

选择 **Start Recovery** 以配置非主管理节点

更换非主管理节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

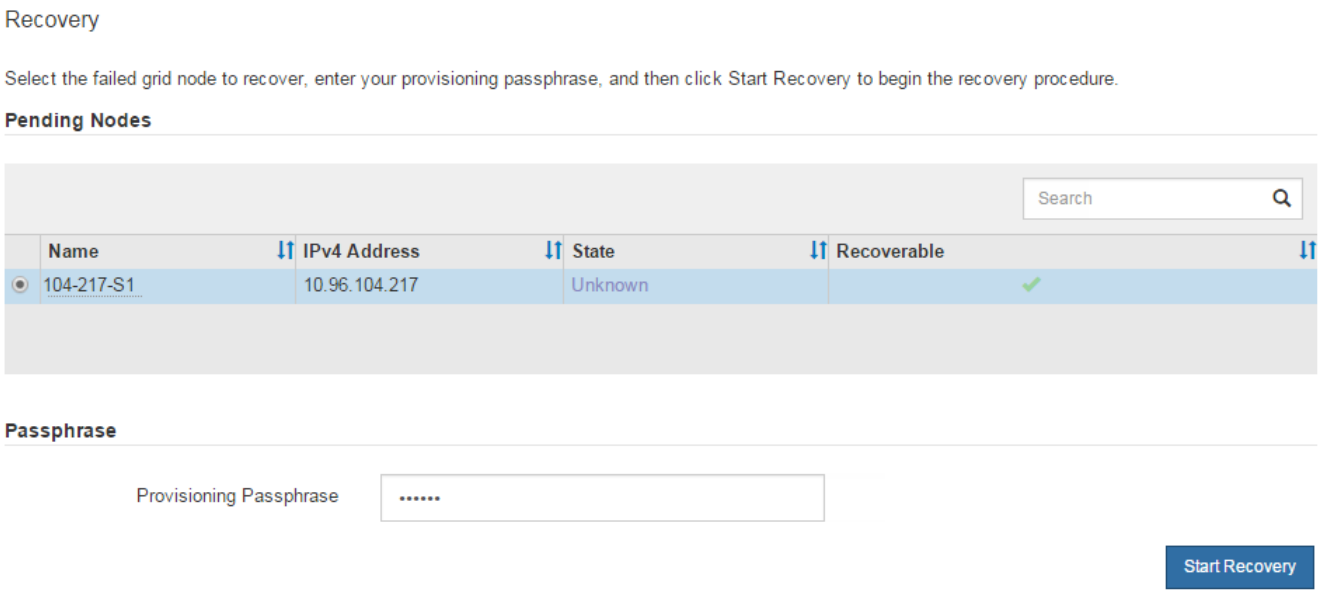
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

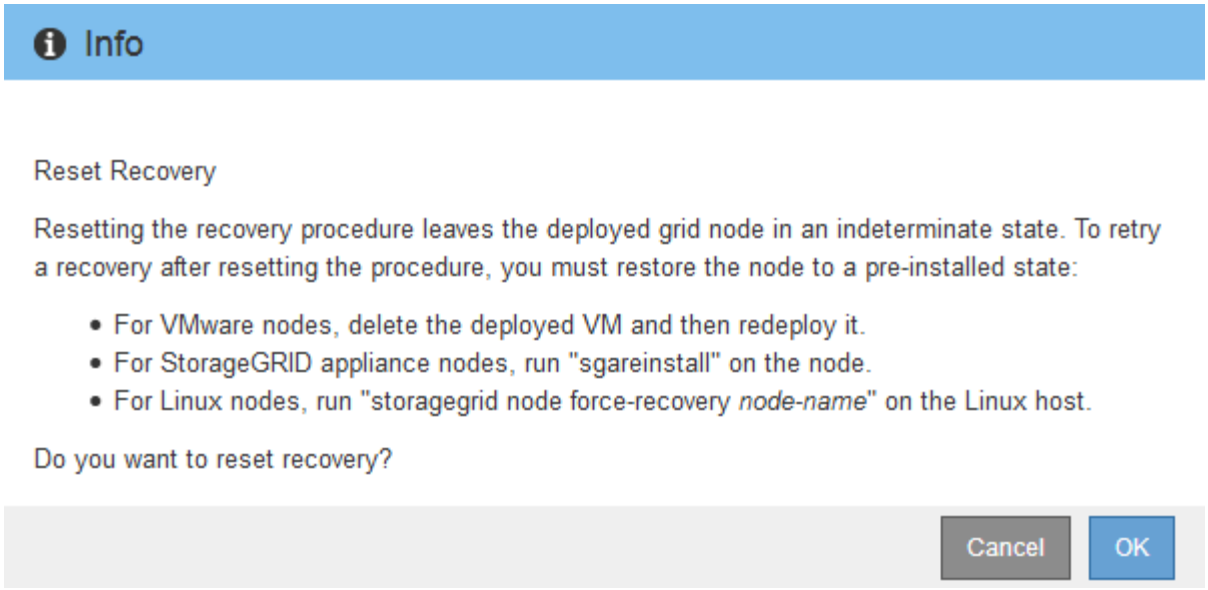
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

> 在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`
- * 设备 * ：如果要在重置操作步骤 后重试恢复，则必须通过在节点上运行 `sgareinstall` 将设备节点还原到预安装状态。

6. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

> 要配置依赖方信任，请参见有关管理 StorageGRID 的说明。要访问默认服务器证书，请登录到管理节点的命令 Shell 。转至 ` /var/local/mgmt-api` 目录，然后选择 `server.crt` 文件。

相关信息

管理 StorageGRID

准备要重新安装的设备（仅限平台更换）

在已恢复的非主管理节点上还原审核日志

如果您能够保留故障非主管理节点中的审核日志，以便保留历史审核日志信息，则可以将其复制到要恢复的非主管理节点。

- 必须安装并运行已恢复的管理节点。
- 在原始管理节点出现故障后，您必须已将审核日志复制到其他位置。

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点，并且无法从故障节点复制审核日志，则恢复的管理节点会开始将事件记录到审核日志中，就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

> 默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：
>
> - 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
> - 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。
>
> 请参见 配置审核消息和日志目标 了解详细信息。

步骤

1. 登录到已恢复的管理节点：
   a. 输入以下命令： + `ssh admin@recovery_Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录后，提示符将从 ` $` 更改为 ` #` 。
2. 检查已保留哪些审核文件：

   ```
   cd /var/local/audit/export
   ```
3. 将保留的审核日志文件复制到已恢复的管理节点：

   ```
   scp admin@grid_node_ip ： /var/local/tmp/saved-audit-logs/yyy*
   ```

   出现提示时，输入 admin 的密码。
4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复管理节点上审核日志文件的用户和组设置：

   ```
   chown AMS-user ： byncast *
   ```
6. 以 root 用户身份注销： `exit`

您还必须还原对审核共享的任何已有客户端访问。有关详细信息，请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

在已恢复的非主管理节点上重置首选发送器

如果您要恢复的非主管理节点当前设置为警报通知，警报通知和 AutoSupport 消息的首选发送方，则必须在 StorageGRID 系统中重新配置此设置。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 必须安装并运行已恢复的管理节点。

步骤

1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。
2. 从 * 首选发件人 * 下拉列表中选择已恢复的管理节点。
3. 单击 * 应用更改 * 。

相关信息

管理 StorageGRID

恢复非主管理节点时还原管理节点数据库

如果要在出现故障的非主管理节点上保留有关属性，警报和警报的历史信息，则可以从主管理节点还原管理节点数据库。

- 必须安装并运行已恢复的管理节点。
- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 警报历史记录
- 历史属性数据，用于 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的图表和文本报告。

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统一部分或稍后添加的服务器和服务的信息。

如果还原了非主管理节点，则可以通过将管理节点数据库从主管理节点（ *source Admin Node* ）复制到恢复的节点来还原历史信息。

> 复制管理节点数据库可能需要几小时的时间。在源节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

2. 从源管理节点运行以下命令。然后，根据提示输入配置密码短语。`re`覆盖访问点

3. 从源管理节点中，停止 MI 服务： `service mi stop`

4. 从源管理节点中，停止管理应用程序接口（ Management Application Program Interface ， mgmt-API ）服务： `service mgmt-api stop`

5. 在已恢复的管理节点上完成以下步骤：

a. 登录到已恢复的管理节点：

i. 输入以下命令： `ssh admin@ grid_node_ip_`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。

b. 停止 MI 服务： `service mi stop`

c. 停止 mgmt-api 服务： `service mgmt-api stop`

d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

e. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

f. 将数据库从源管理节点复制到已恢复的管理节点： ` /usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. 出现提示时，确认要覆盖已恢复的管理节点上的 MI 数据库。

数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。

h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

6. 在源管理节点上重新启动服务： `service servermanager start`

恢复非主管理节点时还原 **Prometheus** 指标

您也可以在出现故障的非主管理节点上保留 Prometheus 维护的历史指标。

- 必须安装并运行已恢复的管理节点。
- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果还原了非主管理节点，则可以通过将 Prometheus 数据库从主管理节点（ *source Admin Node* ）复制到恢

复的管理节点来还原历史指标。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 从源管理节点中，停止 Prometheus 服务： `sservice Prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 停止 Prometheus 服务： `sservice Prometheus stop`
   c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   d. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。
   e. 将 Prometheus 数据库从源管理节点复制到已恢复的管理节点： ` /usr/local/Prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

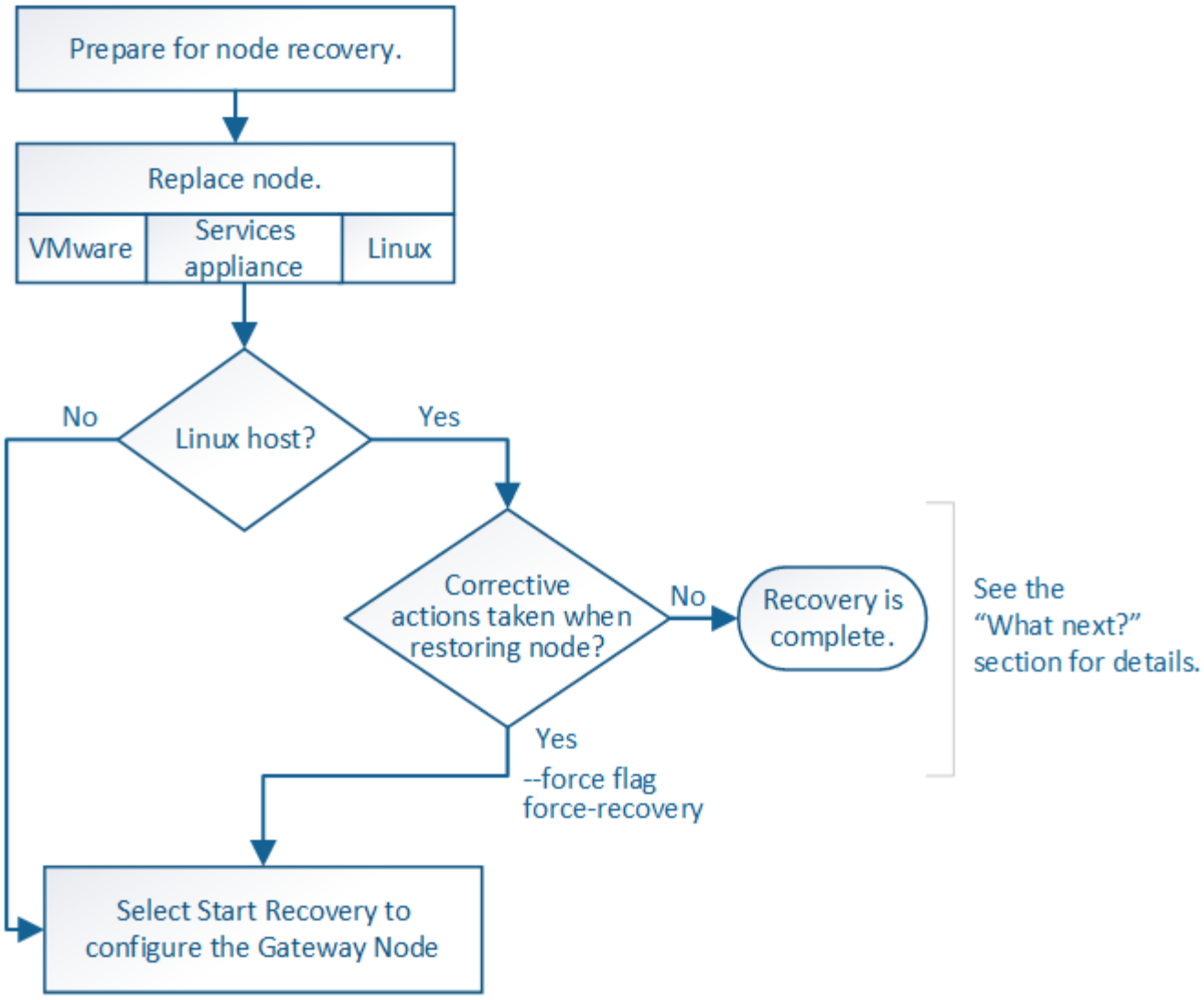
      原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

   已克隆数据库，正在启动服务

   a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`
4. 在源管理节点上重新启动 Prometheus 服务。 `sservice Prometheus start`

从网关节点故障中恢复

要从网关节点故障中恢复，您必须按确切顺序完成一系列任务。



相关信息

SG100 和 SG1000 服务设备

更换网关节点

您可以将出现故障的网关节点更换为运行在同一物理或虚拟硬件上的网关节点，也可以将运行在 VMware 或 Linux 主机上的网关节点更换为托管在服务设备上的网关节点。

您必须遵循的节点更换操作步骤 取决于更换节点将使用的平台。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将指导您执行网关节点恢复的下一步。

更换平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
SG100 和 SG1000 服务设备	更换服务设备

更换平台	操作步骤
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

选择 **Start Recovery** 以配置网关节点

更换网关节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

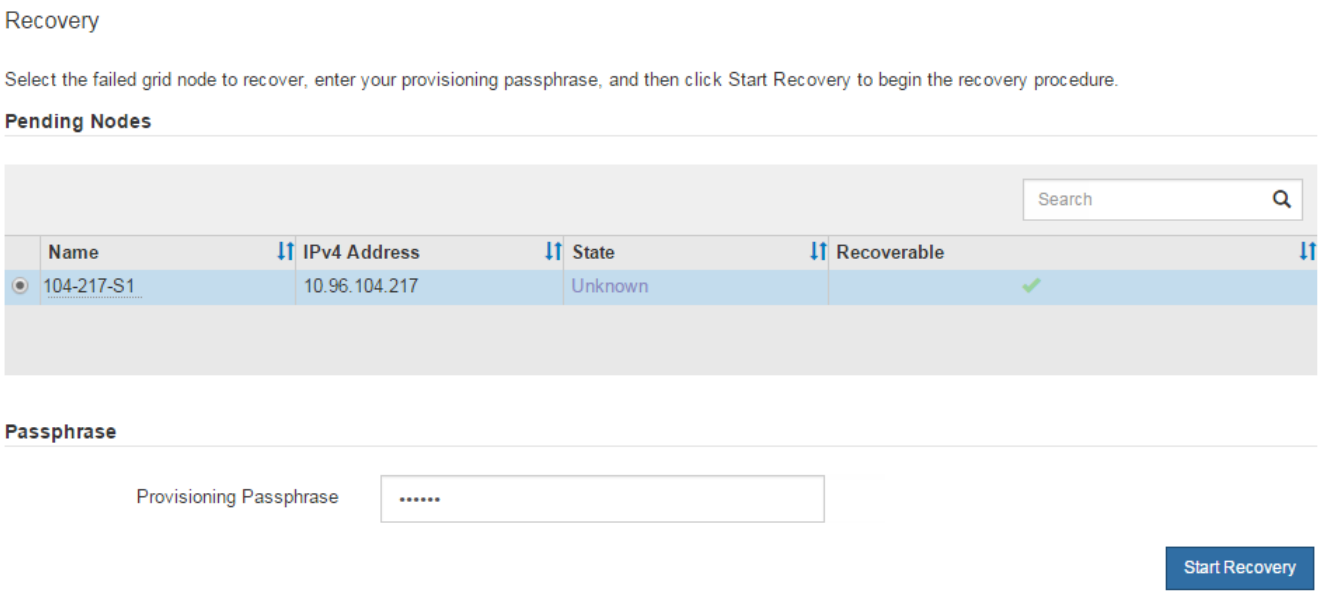
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

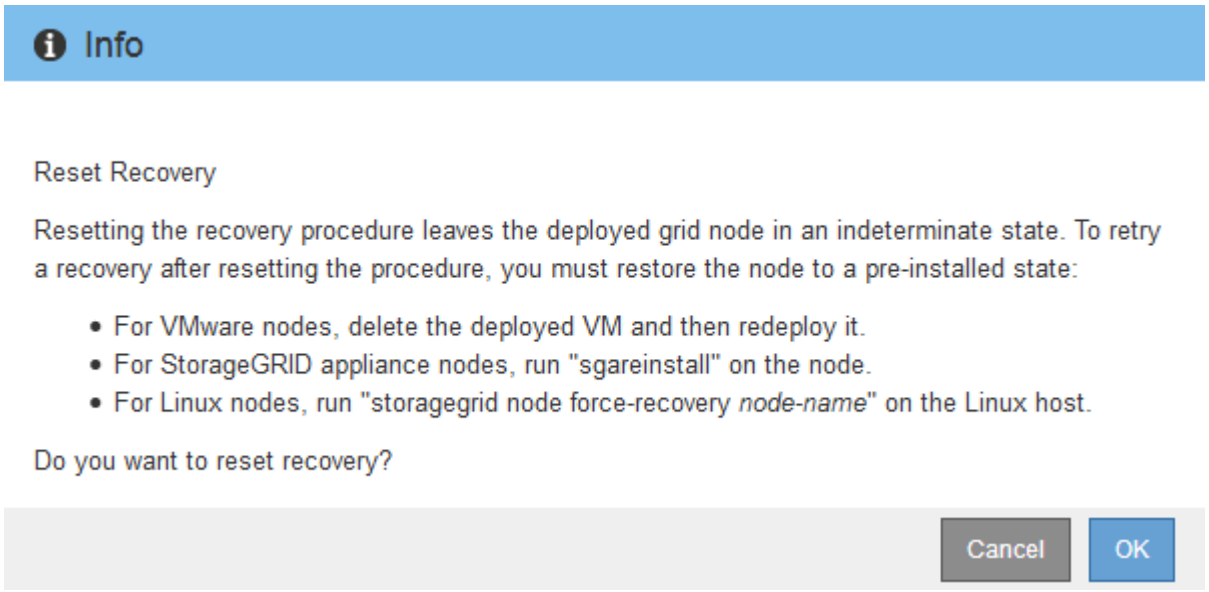
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

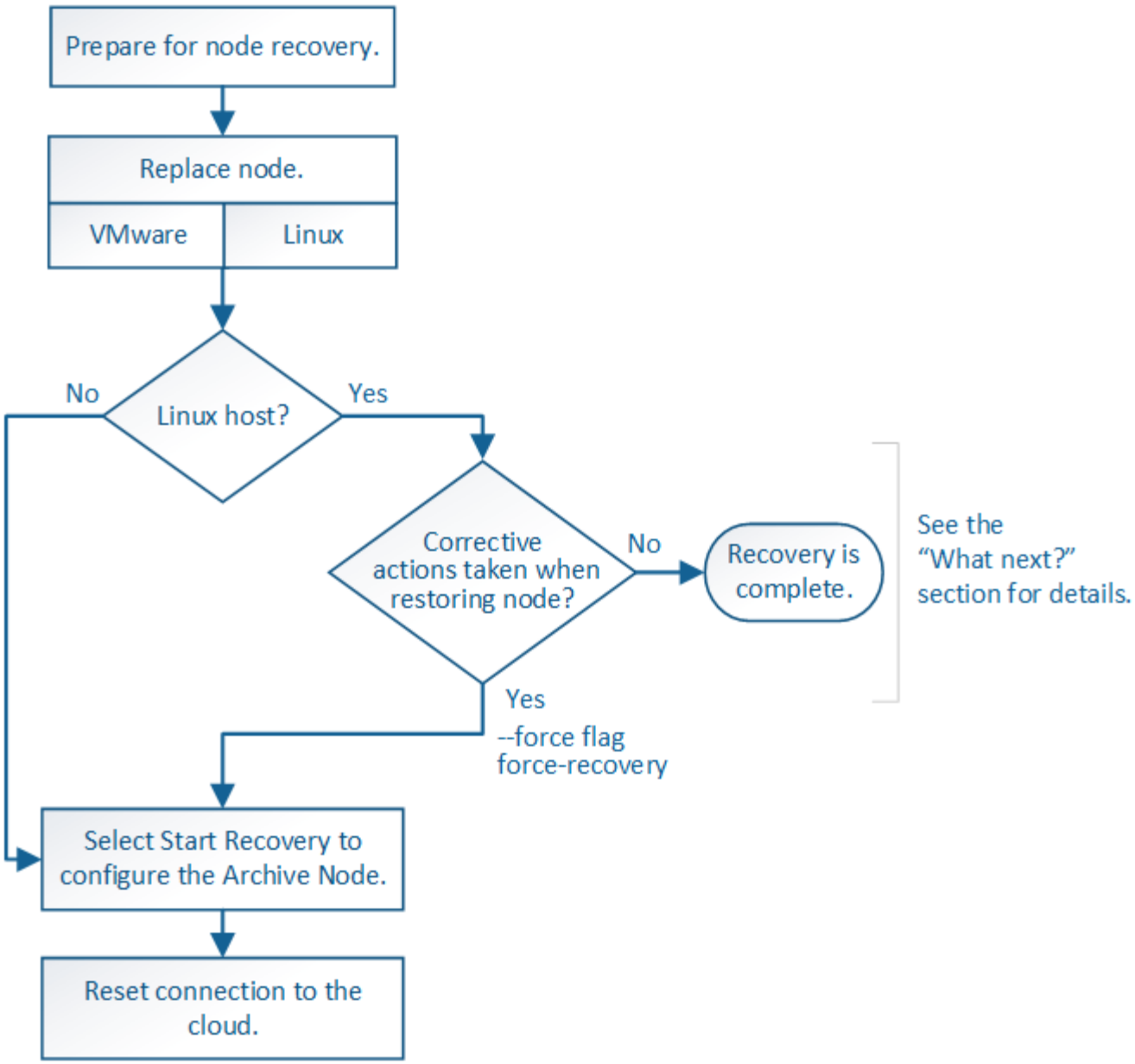
- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`
- * 设备 * ：如果要在重置操作步骤 后重试恢复，则必须通过在节点上运行 `sgareinstall` 将设备节点还原到预安装状态。

相关信息

准备要重新安装的设备（仅限平台更换）

从归档节点故障中恢复

要从归档节点故障中恢复，您必须按确切顺序完成一系列任务。



关于此任务

归档节点恢复受以下问题影响：

- 如果 ILM 策略配置为复制单个副本。

  在配置为创建一个对象副本的 StorageGRID 系统中，归档节点故障可能会导致无法恢复的数据丢失。如果发生故障，所有此类对象都将丢失；但是，您仍必须执行恢复过程 "`清理` " StorageGRID 系统并清除数据库中丢失的对象信息。

- 如果在存储节点恢复期间发生归档节点故障。

  如果在存储节点恢复过程中处理批量检索时归档节点出现故障， 您必须重复操作步骤 以从头开始将对象数据的副本恢复到存储节点，以确保从归档节点检索到的所有对象数据都还原到存储节点。

要恢复归档节点，必须先更换该节点。

您必须为您的平台选择节点替代操作步骤 。对于所有类型的网格节点，更换节点的步骤都相同。

平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

更换归档节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

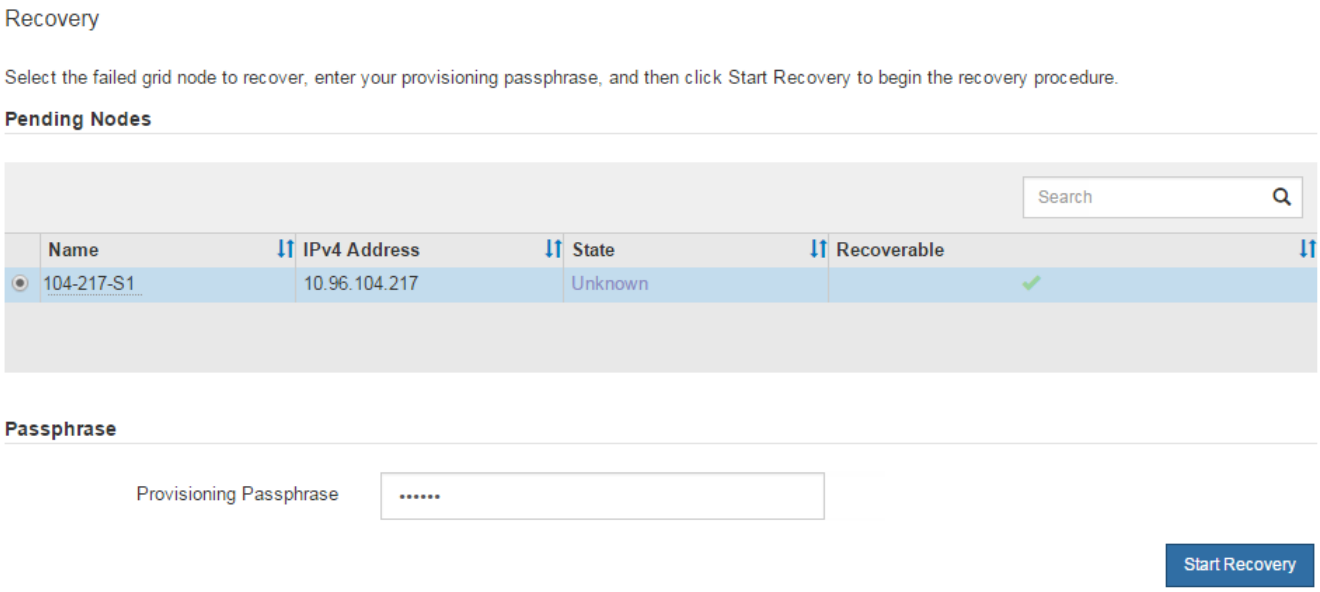
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

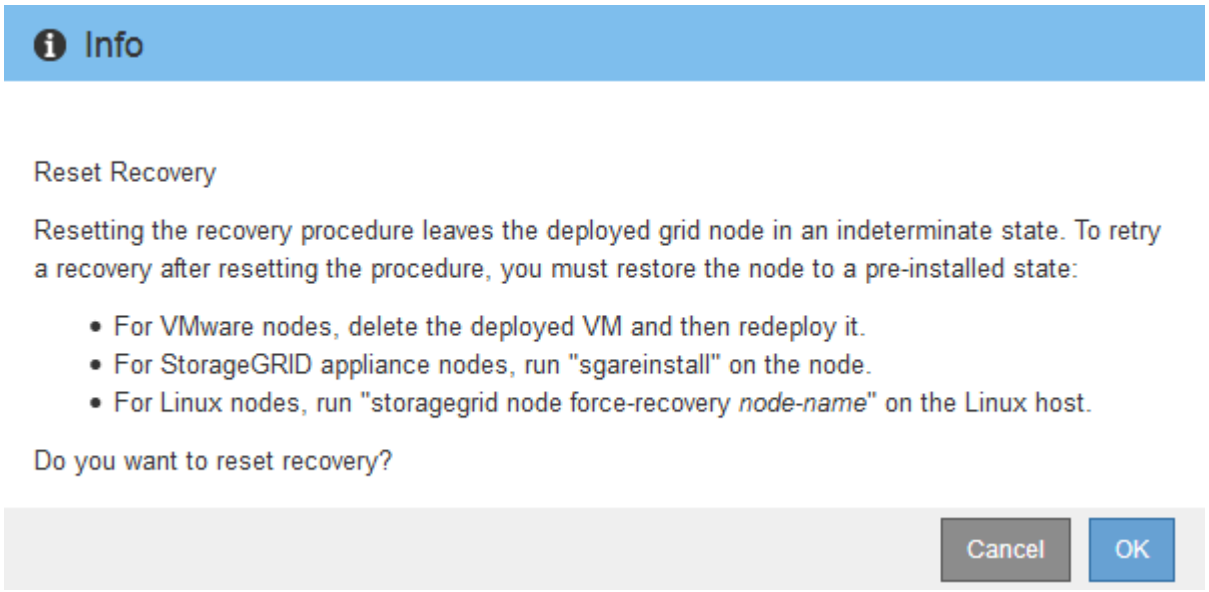
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

> 在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`

将归档节点连接重置为云

通过 S3 API 恢复以云为目标的归档节点后，您需要修改配置设置以重置连接。如果归档节点无法检索对象数据，则会触发出站复制状态（ ORSU ）警报。

如果归档节点通过 TSM 中间件连接到外部存储，则该节点将自动重置，您无需重新配置。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARE* > * 目标 * 。
3. 输入不正确的值以编辑 * 访问密钥 * 字段，然后单击 * 应用更改 * 。
4. 输入正确的值以编辑 * 访问密钥 * 字段，然后单击 * 应用更改 * 。

所有网格节点类型：更换 **VMware** 节点

在恢复 VMware 上托管的故障 StorageGRID 节点时，必须删除故障节点并部署恢复节点。

您需要的内容

您必须已确定虚拟机无法还原，并且必须更换。

关于此任务

您可以使用 VMware vSphere Web Client 首先删除与故障网格节点关联的虚拟机。然后，您可以部署新的虚拟机。

此操作步骤 只是网格节点恢复过程中的一个步骤。所有 VMware 节点的节点删除和部署操作步骤 均相同，包括管理节点，存储节点，网关节点和归档节点。

步骤

1. 登录到 VMware vSphere Web Client 。
2. 导航到出现故障的网格节点虚拟机。
3. 记下部署恢复节点所需的所有信息。
   a. 右键单击虚拟机，选择 * 编辑设置 * 选项卡，并记下正在使用的设置。
   b. 选择 * vApp 选项 * 选项卡以查看和记录网格节点网络设置。
4. 如果发生故障的网格节点是存储节点，请确定用于数据存储的任何虚拟硬盘是否完好无损，并保留这些虚拟硬盘以重新连接到已恢复的网格节点。
5. 关闭虚拟机。
6. 选择 * 操作 * > * 所有 vCenter 操作 * > * 从磁盘中删除 * 以删除虚拟机。
7. 将新虚拟机部署为替代节点，并将其连接到一个或多个 StorageGRID 网络。

   部署节点时，您可以选择重新映射节点端口或增加 CPU 或内存设置。

   部署新节点后，您可以根据存储要求添加新的虚拟磁盘，重新连接从先前删除的故障网格节点中保留的任何虚拟硬盘，或者同时添加这两者。

   有关说明：

安装 VMware > 将 StorageGRID 节点部署为虚拟机

8. 根据要恢复的节点类型完成节点恢复操作步骤 。

节点类型	转至
主管理节点	配置替代主管理节点
非主管理节点	选择 Start Recovery 以配置非主管理节点
网关节点	选择 Start Recovery 以配置网关节点
存储节点	选择启动恢复以配置存储节点
归档节点	选择启动恢复以配置归档节点

所有网格节点类型：替换 **Linux** 节点

如果发生故障时需要部署一个或多个新的物理或虚拟主机或在现有主机上重新安装 Linux ，则必须先部署和配置替代主机，然后才能恢复网格节点。对于所有类型的网格节点，此操作步骤 是网格节点恢复过程的一个步骤。

"`Linux` " 是指 Red Hat ® Enterprise Linux ® ， Ubuntu ® ， CentOS 或 Debian ® 部署。使用 NetApp 互操作性表工具可获取受支持版本的列表。

此操作步骤 仅在恢复基于软件的存储节点，主管理节点或非主管理节点，网关节点或归档节点的过程中执行一步。无论您要恢复的网格节点类型如何，这些步骤都是相同的。

如果物理或虚拟 Linux 主机上托管了多个网格节点，则可以按任意顺序恢复网格节点。但是，如果存在主管理节点，则首先恢复主管理节点会阻止其他网格节点在尝试联系主管理节点进行注册以进行恢复时停止恢复。

相关信息

"NetApp 互操作性表工具"

部署新的 **Linux** 主机

除了一些例外情况，您可以像在初始安装过程中一样准备新主机。

要部署新的或重新安装的物理或虚拟 Linux 主机，请按照适用于 Linux 操作系统的 StorageGRID 安装说明中的操作步骤 准备主机。

此操作步骤 包含用于完成以下任务的步骤：

1. 安装 Linux 。
2. 配置主机网络。
3. 配置主机存储。
4. 安装容器引擎。

5. 安装 StorageGRID 主机服务。

> 完成安装说明中的 "`安装 StorageGRID 主机服务` " 任务后停止。请勿启动 " D部署网格节点 " 任务。

执行这些步骤时，请注意以下重要准则：

- 请确保使用与原始主机上使用的主机接口名称相同的主机接口名称。
- 如果您使用共享存储来支持 StorageGRID 节点，或者已将部分或全部磁盘驱动器或 SSD 从故障节点移至替代节点，则必须重新建立原始主机上的相同存储映射。例如，如果按照安装说明中的建议在 ` /etc/multipath.conf` 中使用了 WWID 和别名，请务必在替代主机上的 ` /etc/multipath.conf` 中使用相同的别名 /WWID 对。
- 如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

将网格节点还原到主机

要将出现故障的网格节点还原到新的 Linux 主机，请使用相应的命令还原节点配置文件。

执行全新安装时，您需要为要安装在主机上的每个网格节点创建一个节点配置文件。将网格节点还原到替代主机时，您需要还原或替换任何出现故障的网格节点的节点配置文件。

如果从上一主机保留了任何块存储卷，则可能需要执行其他恢复过程。本节中的命令可帮助您确定需要执行的其他过程。

步骤

- 还原和验证网格节点
- 启动 StorageGRID 主机服务
- 恢复无法正常启动的节点

还原和验证网格节点

您必须还原任何出现故障的网格节点的网格配置文件，然后验证网格配置文件并解决任何错误。

关于此任务

您可以导入主机上应存在的任何网格节点，前提是其 ` 或 var/local` 卷未因上一主机故障而丢失。例如，如果您为 StorageGRID 系统数据卷使用共享存储，则 ` /var/local` 卷可能仍存在，如适用于 Linux 操作系统的 StorageGRID 安装说明中所述。导入节点会将其节点配置文件还原到主机。

如果无法导入缺少的节点，则必须重新创建其网格配置文件。

然后，您必须验证网格配置文件，并解决可能发生的任何网络或存储问题，然后再继续重新启动 StorageGRID 。重新创建节点的配置文件时，必须为要恢复的节点所使用的替代节点使用相同的名称。

有关节点的 ` /var/local` 卷位置的详细信息，请参见安装说明。

步骤

1. 在已恢复主机的命令行中，列出当前已配置的所有 StorageGRID 网格节点：`sUdo StorageGRID node list`

   如果未配置网格节点，则不会显示任何输出。如果配置了某些网格节点，则输出格式应为：

```
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
```

   如果未列出应在主机上配置的部分或全部网格节点，则需要还原缺少的网格节点。

2. 要导入具有 ` /var/local` 卷的网格节点，请执行以下操作：

   a. 对要导入的每个节点运行以下命令：`sUdo StorageGRID node import node-var-local-volume-path`

      只有当目标节点在上次运行的主机上完全关闭时， `StorageGRID node import` 命令才会成功。否则，您将看到类似以下内容的错误：

      此节点（ *node-name* ）似乎归另一主机所有（ `UUID host-uuid` ）。

   如果您确定导入安全，请使用 `-force` 标志。

   a. 如果您看到有关节点归另一主机所有的错误，请使用 ` -force` 标志再次运行命令以完成导入：`sUdo StorageGRID --force node import node-var-local-volume-path`

      使用 ` -force` 标志导入的任何节点都需要执行额外的恢复步骤，才能重新加入网格，如中所述 下一步操作：如果需要，执行其他恢复步骤。

3. 对于没有 ` /var/local` 卷的网格节点，请重新创建节点的配置文件以将其还原到主机。

   请按照安装说明中 "`Create node configuration files` " 中的准则进行操作。

   重新创建节点的配置文件时，必须为要恢复的节点所使用的替代节点使用相同的名称。对于 Linux 部署，请确保配置文件名称包含节点名称。应尽可能使用相同的网络接口，块设备映射和 IP 地址。这种做法可以最大限度地减少恢复期间需要复制到节点的数据量，从而可以显著加快恢复速度（在某些情况下，只需几分钟而不是几周）。

如果在为节点重新创建配置文件时使用任何新的块设备（ StorageGRID 节点先前未使用的设备）作为以 `block_device_` 开头的任何配置变量的值，请务必遵循中的所有准则 修复缺少的块设备错误。

4. 在已恢复的主机上运行以下命令以列出所有 StorageGRID 节点。

   `sUdo StorageGRID 节点列表`

5. 验证名称显示在 StorageGRID 节点列表输出中的每个网格节点的节点配置文件：

   `sUdo StorageGRID node validate node-name`

   在启动 StorageGRID 主机服务之前，您必须解决任何错误或警告。以下各节详细介绍了在恢复期间可能具有特殊意义的错误。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

修复缺少的网络接口错误

修复缺少的网络接口错误

如果主机网络配置不正确或名称拼写错误，则在 StorageGRID 检查 ` /etc/storaggrid/nodes/*node-name*.conf` 文件中指定的映射时会发生错误。

您可能会看到与此模式匹配的错误或警告：

正在检查节点 *node-name* **的配置文件** ` /etc/storaggrid/nodes/*node-name*.conf 。` **错误：** *node-name* ： `grid_network_target = *host-interface-name*` *node-name* ： interface '*host-interface-name*' does not exist`

可能会报告网格网络，管理网络或客户端网络的错误。此错误表示 ` /etc/storaggrid/nodes/*node-name*.conf` 文件会将指示的 StorageGRID 网络映射到名为 ` 主机接口名称 _` 的主机接口，但当前主机上没有具有此名称的接口。

如果收到此错误，请确认您已完成中的步骤 部署新的 Linux 主机。对所有主机接口使用与原始主机相同的名称。

如果您无法为主机接口命名以匹配节点配置文件，则可以编辑节点配置文件，并更改 grid_network_target ，admin_network_target 或 client_network_target 的值以匹配现有主机接口。

确保主机接口提供对相应物理网络端口或 VLAN 的访问，并且该接口不直接引用绑定或网桥设备。您必须在主机上的绑定设备上配置 VLAN （或其他虚拟接口），或者使用网桥和虚拟以太网（ veth ）对。

修复缺少的块设备错误

系统会检查每个已恢复的节点是否映射到有效的块设备专用文件或块设备专用文件的有效软链接。如果 StorageGRID 在 ` /etc/storaggrid/nodes/*node-name*.conf` 文件中发现映射

无效，则会显示缺少块设备错误。

如果您发现与此模式匹配的错误：

正在检查节点 *node-name* 的配置文件 `/etc/storaggrid/nodes/node-name.conf` … 错误： *node-name* ： `block_device_purpose = path-name` *node-name* ： *path-name* 不存在`

这意味着， `/etc/storagegRid/nodes/*node-name*.conf` 会将 *node-name* 用于目的的块设备映射到 Linux 文件系统中的给定路径名，但该位置没有有效的块设备专用文件或指向块设备专用文件的软链接。

确认您已完成中的步骤 部署新的 Linux 主机。对所有块设备使用与原始主机相同的永久性设备名称。

如果无法还原或重新创建缺少的块设备专用文件，您可以分配一个具有适当大小和存储类别的新块设备，并编辑节点配置文件以更改 block_device_purpose 的值以指向新的块设备专用文件。

从适用于您的 Linux 操作系统的安装说明的 s存储要求 一节中的表中确定适当的大小和存储类别。在继续更换块设备之前，请查看 "`配置主机存储` " 中的建议。

> 如果您必须为以 `block_device_` 开头的任何配置文件变量提供一个新的块存储设备，因为故障主机丢失了原始块设备，请在尝试执行进一步的恢复过程之前确保新块设备未格式化。如果您使用的是共享存储并已创建新卷，则新块设备将取消格式化。如果不确定，请对任何新的块存储设备特殊文件运行以下命令。

小心

仅对新块存储设备运行以下命令。如果您认为块存储仍包含要恢复的节点的有效数据，请勿运行此命令，因为设备上的任何数据都将丢失。

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

启动 **StorageGRID** 主机服务

要启动 StorageGRID 节点并确保它们在主机重新启动后重新启动，您必须启用并启动 StorageGRID 主机服务。

1. 在每个主机上运行以下命令：

   ```
   sudo systemctl enable storagegrid
   sudo systemctl start storagegrid
   ```

2. 运行以下命令以确保部署正在进行：

   ```
   sUdo StorageGRID node status node-name
   ```

对于返回未运行或已停止状态的任何节点，请运行以下命令：

`sUdo StorageGRID node start node-name`

3. 如果您先前已启用并启动 StorageGRID 主机服务（或者不确定此服务是否已启用和启动），请同时运行以下命令：

```
sudo systemctl reload-or-restart storagegrid
```

恢复无法正常启动的节点

如果 StorageGRID 节点未正常重新加入网格，并且无法显示为可恢复，则可能已损坏。您可以强制节点进入恢复模式。

要强制节点进入恢复模式，请执行以下操作：

`sUdo StorageGRID node force-recovery node-name`

发出此命令之前，请确认节点的网络配置正确无误；节点可能由于网络接口映射不正确或网格网络 IP 地址或网关不正确而无法重新加入网格。

发出 `StorageGRID node force-recovery node-name` 命令后，您必须对 *node-name* 执行其他恢复步骤。

相关信息

下一步操作：如果需要，执行其他恢复步骤

下一步操作：如果需要，执行其他恢复步骤

根据您为使 StorageGRID 节点在替代主机上运行而采取的特定操作，您可能需要对每个节点执行其他恢复步骤。

如果在更换 Linux 主机或将故障网格节点还原到新主机时不需要采取任何更正操作，则节点恢复已完成。

更正操作和后续步骤

在更换节点期间，您可能需要执行以下更正操作之一：

- 您必须使用 ` -force` 标志来导入节点。
- 对于任何 ` ， `block_device_<utility> 配置文件变量的值是指块设备，该块设备包含的数据与主机发生故障之前的数据不同。
- 您已为此节点发出 `StorageGRID node force-recovery node-name` 命令。
- 您添加了一个新的块设备。

如果您采取了上述 * 任何 * 更正操作，则必须执行其他恢复步骤。

恢复类型	下一步
主管理节点	配置替代主管理节点
非主管理节点	选择 Start Recovery 以配置非主管理节点
网关节点	选择 Start Recovery 以配置网关节点
归档节点	选择启动恢复以配置归档节点
存储节点（基于软件）： • 如果您必须使用 `-force` 标志导入节点，或者发出了 `StorageGRID node force-recovery node-name` • 如果您必须执行完整节点重新安装，或者需要还原 /var/local	选择启动恢复以配置存储节点
存储节点（基于软件）： • 添加新块设备时。 • 如果对于任何 `< 目的 >`， `block_device_< 目的 >` 配置文件变量的值是指块设备，而该块设备所包含的数据与主机发生故障之前的数据不同。	从系统驱动器完好无损的存储卷故障中恢复

将故障节点更换为服务设备

您可以使用 SG100 或 SG1000 服务设备恢复出现故障的网关节点，出现故障的非主管理节点或 VMware 上托管的主管理节点， Linux 主机或服务设备发生故障。此操作步骤 是网格节点恢复操作步骤 的一个步骤。

您需要的内容

- 您必须已确定以下情况之一是正确的：
  - 无法还原托管此节点的虚拟机。
  - 网格节点的物理或虚拟 Linux 主机出现故障，必须更换。
  - 必须更换托管网格节点的服务设备。
- 您必须确保服务设备上的 StorageGRID 设备安装程序版本与 StorageGRID 系统的软件版本匹配，如用于验证和升级 StorageGRID 设备安装程序版本的硬件安装和维护中所述。

  SG100 和 SG1000 服务设备

> 不要在同一站点同时部署 SG100 和 SG1000 服务设备。可能会导致性能不可预测。

关于此任务

在以下情况下，您可以使用 SG100 或 SG1000 服务设备恢复出现故障的网格节点：

- 故障节点托管在 VMware 或 Linux 上（平台更改）
- 故障节点托管在服务设备上（平台更换）

安装服务设备（仅限平台更改）

如果要恢复 VMware 或 Linux 主机上托管的故障网格节点，并且要使用 SG100 或 SG1000 服务设备作为替代节点，则必须先使用与故障节点相同的节点名称安装新设备硬件。

您必须具有有关故障节点的以下信息：

- * 节点名称 *：必须使用与故障节点相同的节点名称安装服务设备。
- * IP 地址 *：您可以为服务设备分配与故障节点相同的 IP 地址，这是首选选项，也可以在每个网络上选择新的未使用的 IP 地址。

只有在恢复 VMware 或 Linux 上托管的故障节点并将其替换为服务设备上托管的节点时，才执行此操作步骤 。

1. 按照说明安装新的 SG100 或 SG1000 服务设备。
2. 当系统提示您输入节点名称时，请使用故障节点的节点名称。

相关信息

SG100 和 SG1000 服务设备

准备要重新安装的设备（仅限平台更换）

在恢复服务设备上托管的网格节点时，您必须先准备该设备以重新安装 StorageGRID 软件。

只有在更换服务设备上托管的故障节点时，才执行此操作步骤 。如果故障节点最初托管在 VMware 或 Linux 主机上，请勿执行以下步骤。

1. 登录到出现故障的网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 准备用于安装 StorageGRID 软件的设备。输入： `sgareinstall`
3. 当系统提示您继续时，输入： `y`

   设备将重新启动， SSH 会话将结束。StorageGRID 设备安装程序通常需要大约 5 分钟才能投入使用，但在某些情况下，您可能需要等待长达 30 分钟。

服务设备将重置，并且网格节点上的数据将无法再访问。在初始安装过程中配置的 IP 地址应保持不变；但是，建议您在操作步骤 完成后进行确认。

执行 `sgareinstall` 命令后，将删除所有 StorageGRID 配置的帐户，密码和 SSH 密钥，并生成新的主机密钥。

开始在服务设备上安装软件

要在 SG100 或 SG1000 服务设备上安装网关节点或管理节点，请使用此设备上随附的 StorageGRID 设备安装程序。

您需要的内容

- 此设备必须安装在机架中，并连接到您的网络并已启动。
- 必须使用 StorageGRID 设备安装程序为此设备配置网络链路和 IP 地址。
- 如果要安装网关节点或非主管理节点，则您知道 StorageGRID 网格的主管理节点的 IP 地址。
- 必须在主管理节点上的网格网络子网列表中定义 StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网。

有关完成这些前提条件任务的说明，请参见 SG100 或 SG1000 服务设备的安装和维护说明。

- 您必须使用 支持的 Web 浏览器。
- 您必须知道分配给设备的 IP 地址之一。您可以使用管理网络，网格网络或客户端网络的 IP 地址。
- 如果您要安装主管理节点，则可以使用此版本 StorageGRID 的 Ubuntu 或 Debian 安装文件。

> 在制造过程中，服务设备会预加载最新版本的 StorageGRID 软件。如果预加载的软件版本与 StorageGRID 部署中使用的版本匹配，则不需要安装文件。

关于此任务

要在 SG100 或 SG1000 服务设备上安装 StorageGRID 软件，请执行以下操作：

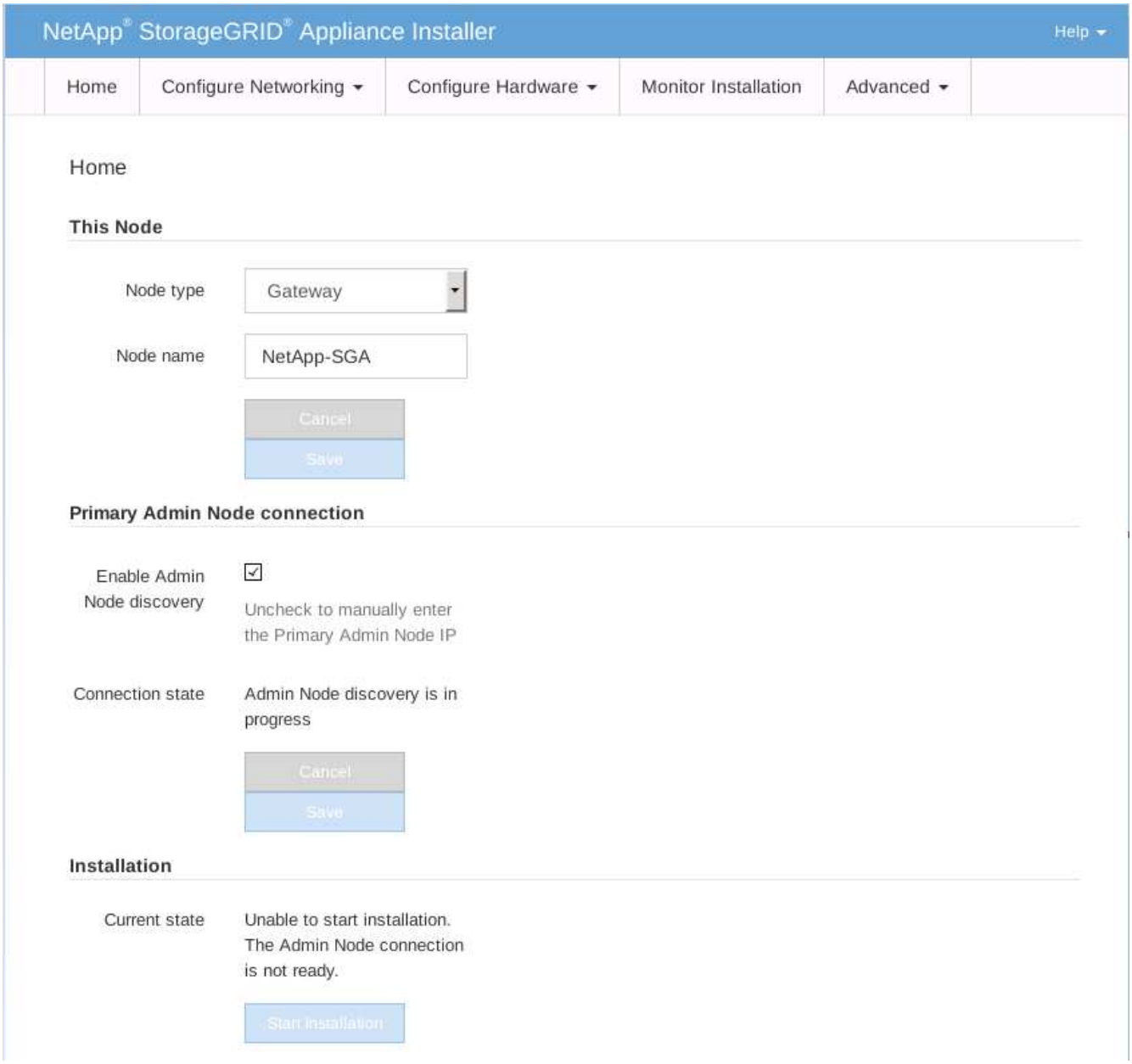
- 对于主管理节点，您可以指定节点的名称，然后上传相应的软件包（如果需要）。
- 对于非主管理节点或网关节点，您可以指定或确认主管理节点的 IP 地址以及节点的名称。
- 您开始安装，并等待卷配置完毕并安装软件。
- 在整个过程中，安装将暂停。要恢复安装，您必须登录到网格管理器并将待定节点配置为故障节点的替代节点。
- 配置节点后，设备安装过程将完成，设备将重新启动。

步骤

1. 打开浏览器并输入 SG100 或 SG1000 服务设备的 IP 地址之一。

   ` + https://Controller_IP:8443+`

   此时将显示 StorageGRID 设备安装程序主页页面。



2. 安装主管理节点：

   a. 在 "This Node" 部分中，对于 "* 节点类型 " ，选择 "* 主管理 * " 。

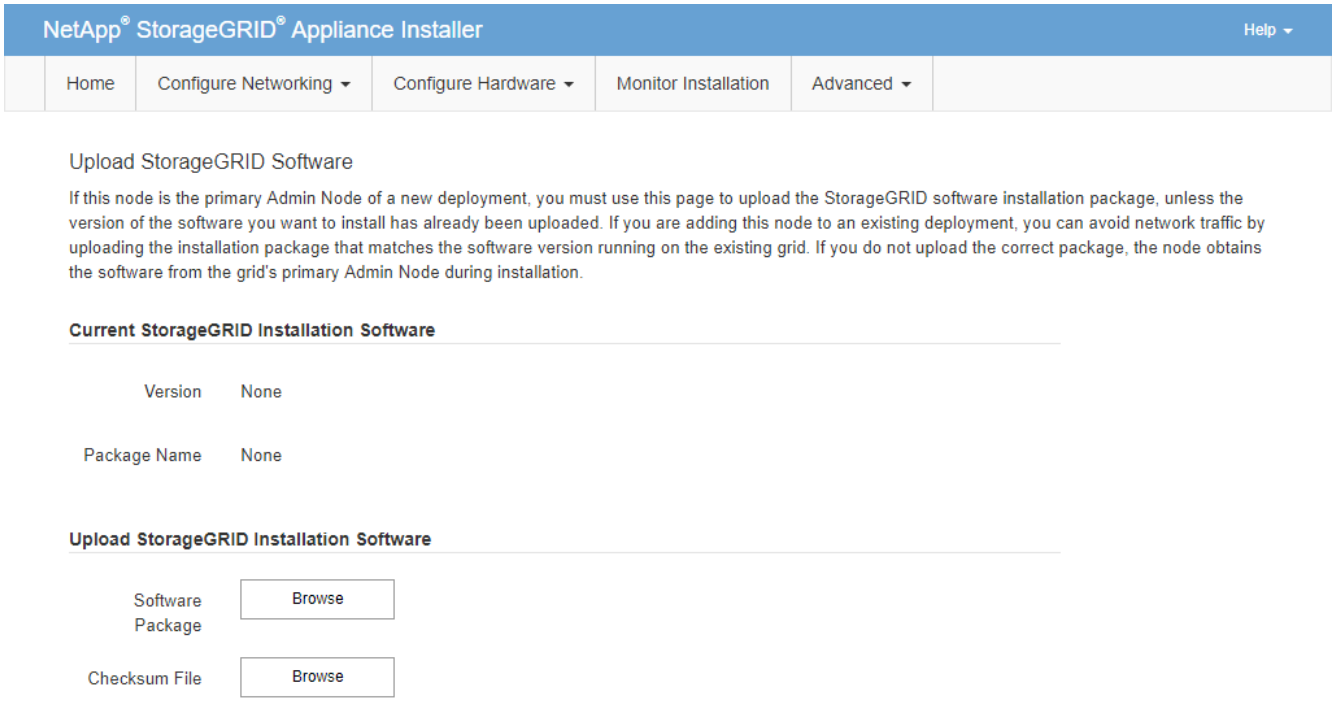
   b. 在 * 节点名称 * 字段中，输入与要恢复的节点相同的名称，然后单击 * 保存 * 。

   c. 在安装部分中，检查当前状态下列出的软件版本

      如果准备安装的软件版本正确，请跳至 安装步骤。

   d. 如果需要上传其他版本的软件，请在 * 高级 * 菜单下选择 * 上传 StorageGRID 软件 * 。

      此时将显示上传 StorageGRID 软件页面。



a. 单击 * 浏览 * 上传适用于 StorageGRID 软件的 * 软件包 * 和 * 校验和文件 * 。

选择这些文件后，这些文件将自动上传。

b. 单击 * 主页 * 返回到 StorageGRID 设备安装程序主页页面。

3. 安装网关节点或非主管理节点：

a. 在 "This Node" 部分中，对于 "* 节点类型 " ，根据要还原的节点类型选择 "* 网关 * " 或 "* 非主管理 * " 。

b. 在 * 节点名称 * 字段中，输入与要恢复的节点相同的名称，然后单击 * 保存 * 。

c. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

假设主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上， StorageGRID 设备安装程序可以自动发现此 IP 地址。

d. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

选项	Description
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 从已发现的 IP 地址列表中，选择要部署此服务设备的网格的主管理节点。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

4. 在 "Installation_section_steP]] 中，确认当前状态为 Ready to start installation of node name 且 * Start Installation* 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

5. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。

   当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

   如果需要手动访问监控器安装页面，请单击菜单栏中的 * 监控器安装 * 。

相关信息

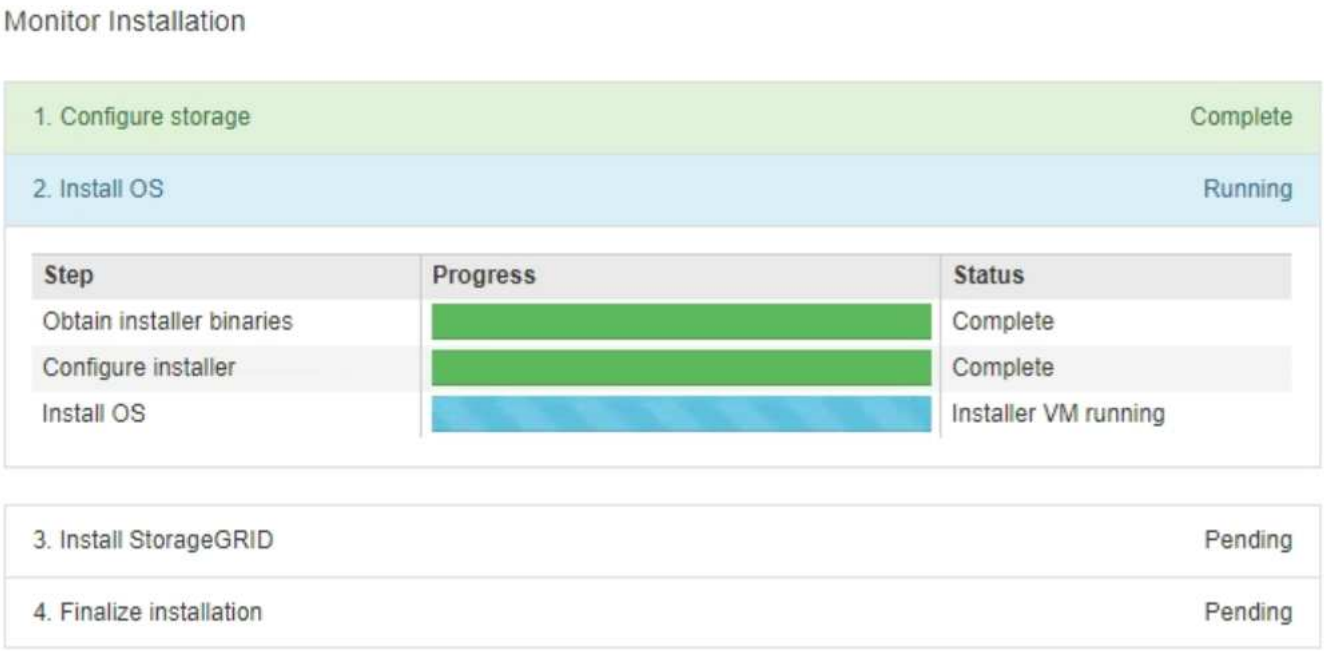
SG100 和 SG1000 服务设备

监控服务设备安装

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

1. 要监控安装进度，请单击菜单栏中的 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

> 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

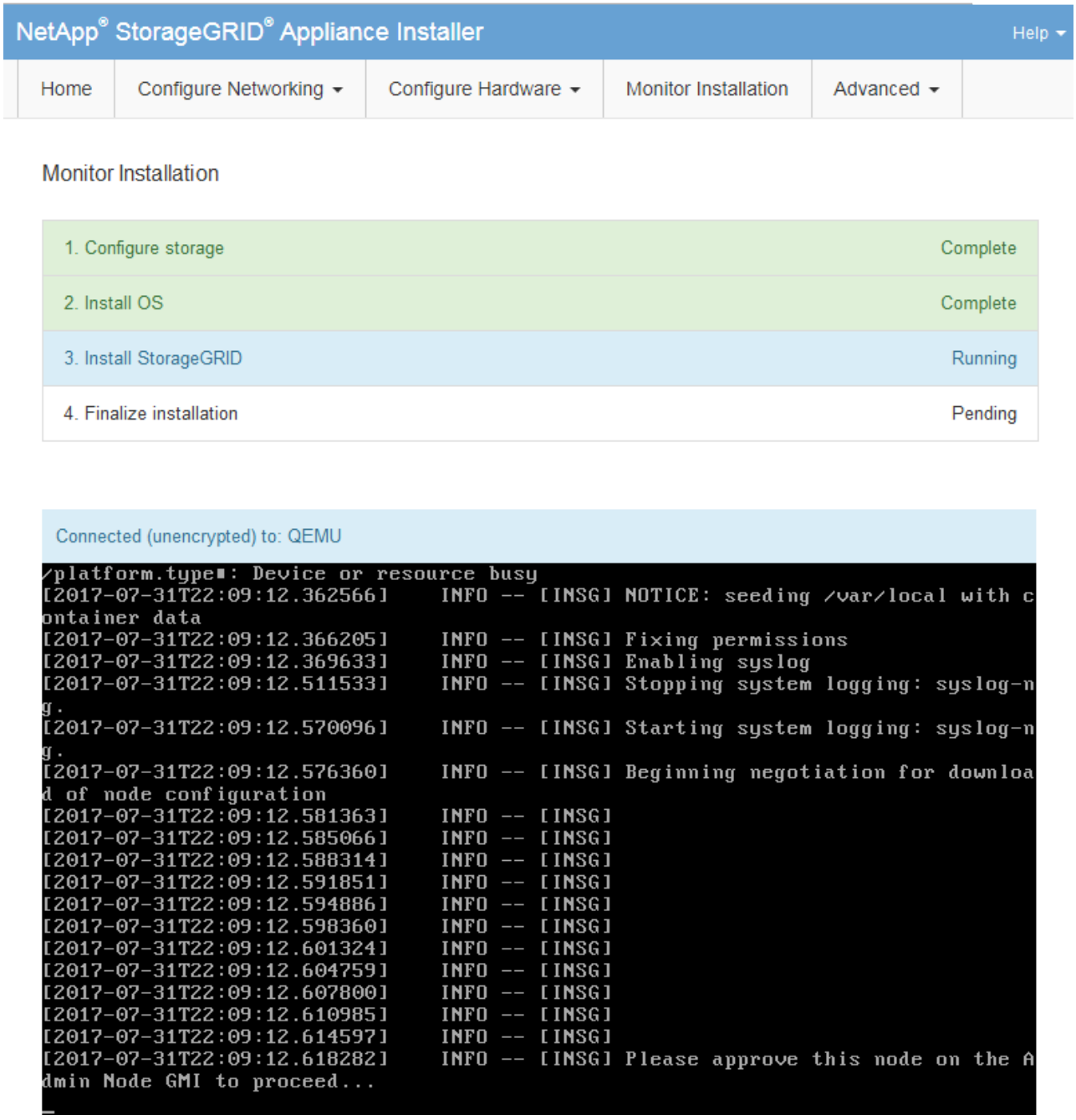
2. 查看前两个安装阶段的进度。
   - * 。配置存储 *

     在此阶段，安装程序将从驱动器中清除任何现有配置，并配置主机设置。

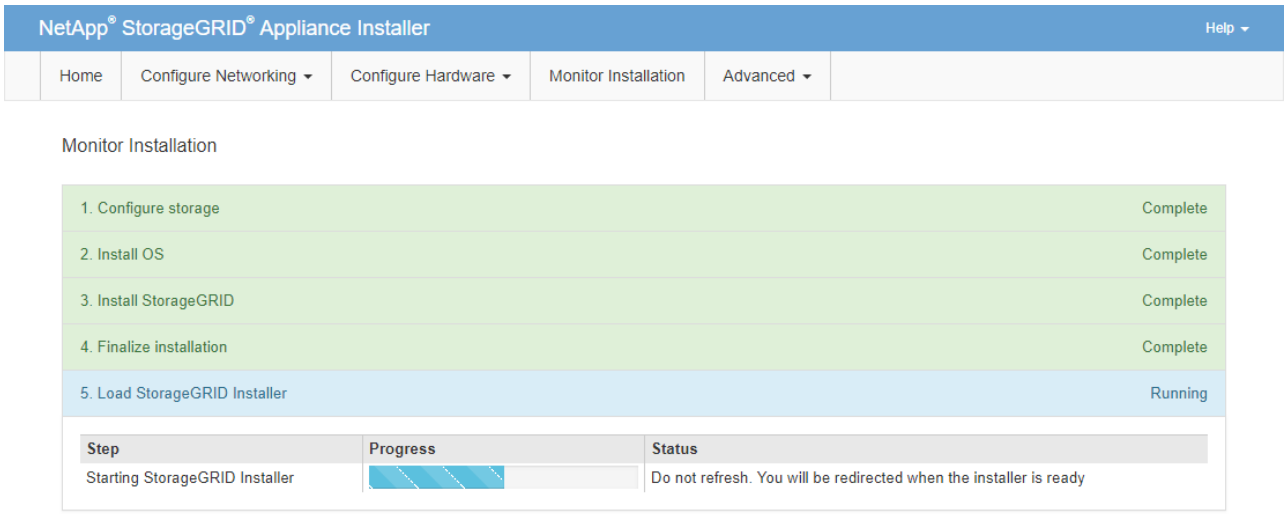
   - * 。安装 OS*

     在此阶段，安装程序会将 StorageGRID 的基本操作系统映像从主管理节点复制到设备，或者从主管理节点的安装包安装基本操作系统。

3. 继续监控安装进度，直到出现以下情况之一：
   - 对于设备网关节点或非主设备管理节点， * 安装 StorageGRID * 阶段将暂停，嵌入式控制台上会显示一条消息，提示您使用网格管理器在管理节点上批准此节点。



- 对于设备主管理节点，将显示第五阶段（ Load StorageGRID 安装程序）。如果第五阶段的进度超过 10 分钟，请手动刷新页面。



4. 对于要恢复的设备网格节点类型，请继续执行恢复过程的下一步。

恢复类型	参考
网关节点	选择 Start Recovery 以配置网关节点
非主管理节点	选择 Start Recovery 以配置非主管理节点
主管理节点	配置替代主管理节点

技术支持如何执行站点恢复

如果整个 StorageGRID 站点出现故障或多个存储节点出现故障，您必须联系技术支持。技术支持将评估您的情况，制定恢复计划，然后按照符合您业务目标的方式恢复故障节点或站点，优化恢复时间并防止不必要的数据丢失。

站点恢复只能由技术支持执行。

StorageGRID 系统可以对各种故障进行故障恢复，您可以自行成功执行许多恢复和维护过程。但是，创建一个简单的通用站点恢复操作步骤 很困难，因为详细步骤取决于您的具体情况。例如：

- * 您的业务目标 * ： 在完全丢失 StorageGRID 站点后，您应评估如何以最佳方式实现您的业务目标。例如，是否要原位重建丢失的站点？是否要在新位置更换丢失的 StorageGRID 站点？每个客户的情况都不同，您的恢复计划必须针对您的优先事项进行设计。
- * 故障的确切性质 * ： 在开始站点恢复之前，请务必确定故障站点上的任何节点是否完好无损，或者任何存储节点是否包含可恢复的对象。如果重建包含有效数据的节点或存储卷，可能会发生不必要的数据丢失。
- * 活动 ILM 策略 * ： 网格中对象副本的数量，类型和位置由活动 ILM 策略控制。ILM 策略的具体内容可能会影响可恢复的数据量以及恢复所需的特定技术。

  如果某个站点包含某个对象的唯一副本，而该站点丢失，则该对象将丢失。

- * 分段（或容器）一致性 * ： 应用于分段（或容器）的一致性级别会影响 StorageGRID 在通知客户端对象载

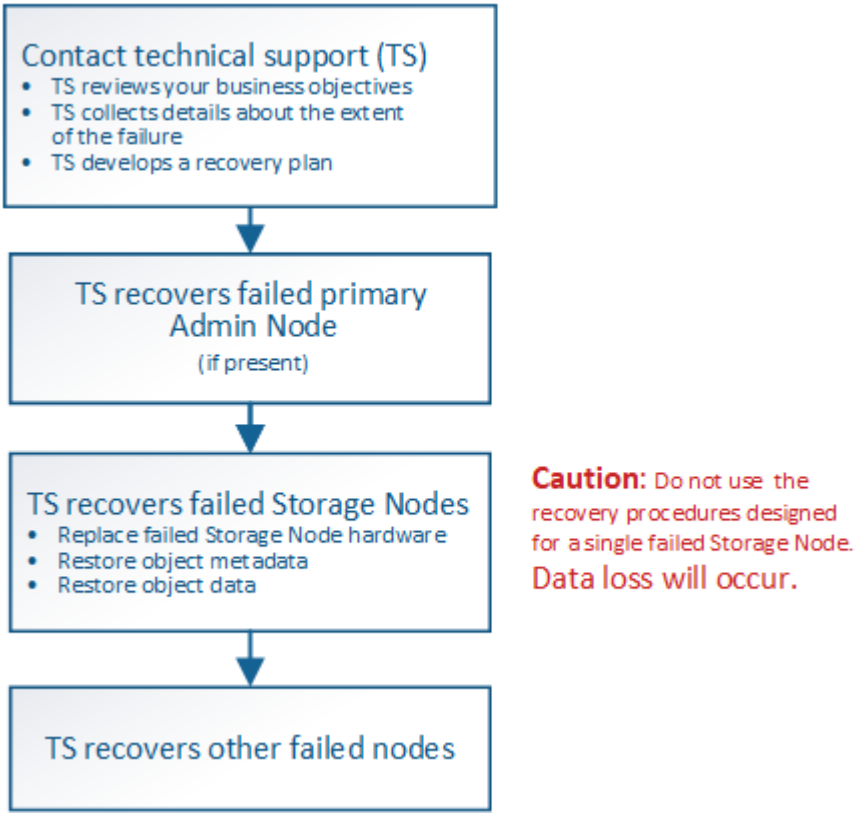
入成功之前是否将对象元数据完全复制到所有节点和站点。如果您的一致性级别允许最终保持一致性，则站点故障可能会丢失某些对象元数据。这可能会影响可恢复的数据量以及恢复操作步骤 的详细信息。

- * 近期更改历史记录 * ： 恢复操作步骤 的详细信息可能会受到故障发生时是否正在执行任何维护过程或是否最近对 ILM 策略进行了任何更改的影响。在开始站点恢复之前，技术支持必须评估网格的最新历史记录及其当前状况。

站点恢复概述

本文档概括介绍了技术支持用于恢复故障站点的过程。

站点恢复只能由技术支持执行。



1. 请联系技术支持。

   技术支持会对故障进行详细评估，并与您一起审核您的业务目标。根据这些信息，技术支持会根据您的具体情况制定一个恢复计划。

2. 如果主管理节点出现故障，技术支持将恢复该节点。
3. 技术支持将按照以下概述恢复所有存储节点：

   a. 根据需要更换 Storage Node 硬件或虚拟机。
   b. 将对象元数据还原到故障站点。
   c. 将对象数据还原到已恢复的存储节点。

   如果对单个故障存储节点执行恢复过程，则会发生数据丢失。

当整个站点出现故障时，需要使用专用命令来成功还原对象和对象元数据。

4. 技术支持可恢复其他故障节点。

恢复对象元数据和数据后，可以使用标准过程恢复出现故障的网关节点，非主管理节点或归档节点。

相关信息

站点停用

停用操作步骤

您可以执行停用操作步骤 ，以便从 StorageGRID 系统中永久删除网格节点或整个站点。

要删除网格节点或站点，请执行以下停用过程之一：

- 执行 * 节点停用 * 以删除一个或多个节点，这些节点可以位于一个或多个站点上。您删除的节点可以联机并连接到 StorageGRID 系统，也可以脱机并断开连接。
- 执行 * 已连接站点停用 * 以删除所有节点均已连接到 StorageGRID 的站点。
- 执行 * 已断开连接的站点停用 * 以删除所有节点均已从 StorageGRID 断开的站点。

在执行已断开连接的站点停用之前，您必须联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。如果您认为可以恢复站点或从站点恢复对象数据，则不应尝试执行已断开连接的站点停用。

如果站点包含混合的 Connected （ ）和已断开连接的节点（ 或 ），您必须使所有脱机节点重新联机。

如果需要执行第二个维护操作步骤 ，可以 在删除存储节点时暂停停用操作步骤。只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。第二个维护操作步骤 完成后，您可以恢复停用。

相关信息

网格节点停用

站点停用

网格节点停用

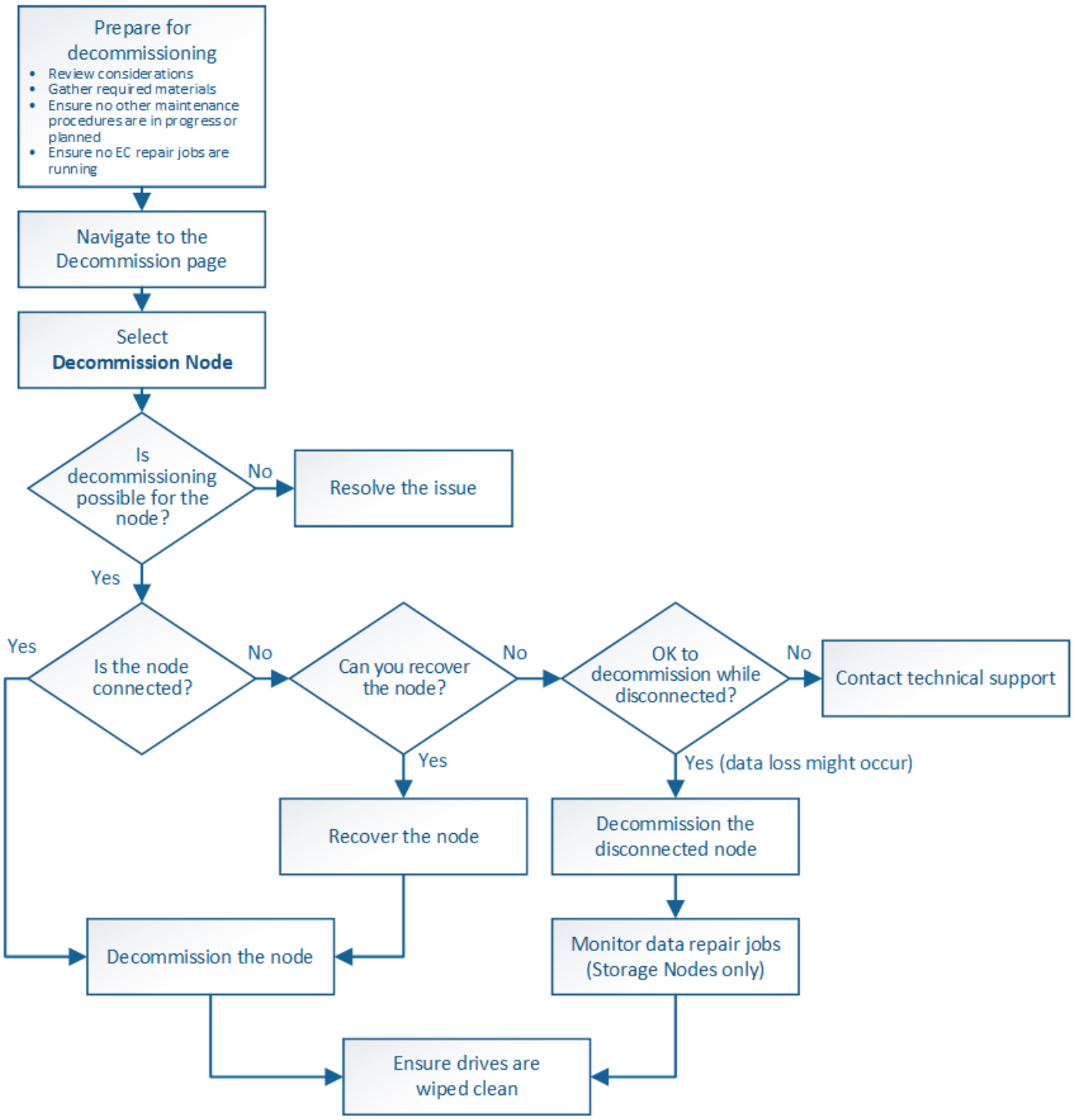
您可以使用节点停用操作步骤 删除一个或多个站点上的一个或多个存储节点，网关节点或非主管理节点。您不能停用主管理节点或归档节点。

通常，只有当网格节点已连接到 StorageGRID 系统且所有节点均处于正常运行状况时（在 * 节点 * 页面和 * 停用节点 * 页面上有绿色图标），才应停用这些节点。但是，如果需要，您可以停用已断开连接的网格节点。在删除已断开连接的节点之前，请确保您了解此过程的含义和限制。

如果满足以下任一条件，请使用节点停用操作步骤 ：

- 您已向系统中添加较大的存储节点，并希望删除一个或多个较小的存储节点，同时保留对象。
- 您所需的总存储较少。
- 您不再需要网关节点。
- 您不再需要非主管理节点。
- 您的网格包含一个断开连接的节点，您无法恢复此节点或使其恢复联机。

此流程图显示了停用网格节点的高级步骤。



您必须查看删除网格节点的注意事项，并确认擦除编码的数据没有处于活动状态的修复作业。

网格节点停用注意事项

在启动此操作步骤 以停用一个或多个节点之前，您必须了解删除每种类型的节点的含义。成功停用节点后，其服务将被禁用，并且节点将自动关闭。

如果停用某个节点会使 StorageGRID 处于无效状态，则无法停用此节点。将强制实施以下规则：

- 您不能停用主管理节点。
- 您不能停用归档节点。
- 如果管理节点或网关节点的某个网络接口属于高可用性（ HA ）组，则无法停用此节点。
- 如果删除存储节点会影响到模数转换器仲裁，则无法停用该存储节点。
- 如果活动 ILM 策略需要存储节点，则无法停用它。
- 在一个 " 停用节点 " 操作步骤 中停用的存储节点不应超过 10 个。
- 如果网格包含任何已断开连接的节点（运行状况为未知或管理员关闭的节点），则无法停用已连接节点。您必须先停用或恢复已断开连接的节点。
- 如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。
- 如果无法删除已断开连接的节点（例如，为实现模数转换器仲裁所需的存储节点），则不能删除任何其他已断开连接的节点。
- 如果要将旧设备更换为新设备，请考虑 正在克隆设备节点 而不是停用旧节点并在扩展中添加新节点。

> 在停用过程中指示删除网格节点的虚拟机或其他资源之前，请勿删除。

管理节点或网关节点停用的注意事项

停用管理节点或网关节点之前，请查看以下注意事项。

- 停用操作步骤 要求对某些系统资源具有独占访问权限，因此您必须确认未运行任何其他维护过程。
- 您不能停用主管理节点。
- 如果管理节点或网关节点的某个网络接口属于高可用性（ HA ）组，则无法停用此节点。您必须先从 HA 组中删除网络接口。请参见有关管理 StorageGRID 的说明。
- 您可以根据需要在停用网关节点或管理节点时安全地更改 ILM 策略。
- 如果停用管理节点并为 StorageGRID 系统启用了单点登录（ SSO ），则必须记住从 Active Directory 联合身份验证服务（ AD FS ）中删除该节点的依赖方信任。

相关信息

管理 StorageGRID

存储节点停用注意事项

如果您计划停用存储节点，则必须了解 StorageGRID 如何管理该节点上的对象数据和元数据。

停用存储节点时，应遵循以下注意事项和限制：

- 系统必须始终包含足够的存储节点以满足操作要求，包括模块数转换仲裁和活动 ILM 策略。要满足此限制，您可能需要在扩展操作中添加新的存储节点，然后才能停用现有存储节点。
- 如果在停用存储节点时断开了该存储节点的连接，则系统必须使用已连接存储节点中的数据重建数据，这可能会导致数据丢失。
- 删除存储节点时，必须通过网络传输大量对象数据。尽管这些传输不应影响正常系统操作，但它们可能会影响 StorageGRID 系统占用的网络带宽总量。
- 与正常系统操作相关的任务相比，与存储节点停用相关的任务的优先级更低。这意味着停用不会干扰 StorageGRID 系统的正常运行，也不需要计划系统在一段时间内处于非活动状态。由于停用是在后台执行的，因此很难估计完成此过程需要多长时间。通常，在系统处于静默状态或一次仅删除一个存储节点时，停用速度会更快。
- 停用存储节点可能需要数天或数周时间。相应地规划此操作步骤 。尽管停用过程不会影响系统运行，但它会限制其他过程。通常，在删除网格节点之前，您应执行任何计划内的系统升级或扩展。
- 涉及存储节点的停用过程可以在某些阶段暂停，以便在需要时运行其他维护过程，并在完成后继续执行。
- 当停用任务正在运行时，您不能在任何网格节点上运行数据修复操作。
- 在停用存储节点期间，不应对 ILM 策略进行任何更改。
- 删除存储节点时，节点上的数据将迁移到其他网格节点；但是，此数据不会从已停用的网格节点中完全删除。要永久安全地删除数据，必须在停用操作步骤 完成后擦除已停用网格节点的驱动器。
- 停用存储节点时，可能会发出以下警报，您可能会收到相关电子邮件和 SNMP 通知：
  - * 无法与节点 * 警报通信。停用包含此 ADC-Service 的存储节点时会触发此警报。停用操作完成后，此警报将得到解决。
  - VSTU （对象验证状态）警报。此通知级别的警报表示存储节点在停用过程中将进入维护模式。
  - CASA （数据存储状态）警报。此主要级别的警报表示 Cassandra 数据库正在关闭，因为服务已停止。

相关信息

根据需要将对象数据还原到存储卷

了解模数转换器仲裁

如果在停用后管理域控制器（ ADA ）服务仍会过多，您可能无法停用数据中心站点上的某些存储节点。此服务位于某些存储节点上，用于维护网格拓扑信息并为网格提供配置服务。StorageGRID 系统要求每个站点始终提供一定的数字转换服务仲裁。

如果删除某个存储节点将无法再满足发生原因 的仲裁，则无法停用此存储节点。要在停用期间满足模块转换仲裁要求，每个数据中心站点至少有三个存储节点必须具有模块转换服务。如果数据中心站点具有三个以上使用了 ADC 服务的存储节点，则在停用后，这些节点中的大多数节点必须保持可用（（ 0.5 * ` *Storage Nodes with ADC*` ） + 1 ）。

例如，假设一个数据中心站点当前包含六个具有模块化转换服务的存储节点，而您希望停用三个存储节点。由于

需要使用 ADC 仲裁，您必须完成两个停用过程，如下所示：

- 在第一个停用操作步骤 中，您必须确保具有 ADA 服务的四个存储节点仍然可用（（（ 0.5 * 6 ） +1 ）。这意味着最初只能停用两个存储节点。
- 在第二个停用操作步骤 中，您可以删除第三个存储节点，因为现在，由于仲裁只需要三个可用的 ADC 服务（（ 0.5 * 4 ） + 1 ）。

如果您需要停用某个存储节点，但由于要求使用的是 ADA 仲裁而无法停用，则必须在扩展中添加一个新的存储节点，并指定该存储节点应具有一个 ADA 服务。然后，您可以停用现有存储节点。

相关信息

扩展网格

查看 **ILM** 策略和存储配置

如果您计划停用存储节点，则应在开始停用过程之前查看 StorageGRID 系统的 ILM 策略。

在停用期间，所有对象数据都会从停用的存储节点迁移到其他存储节点。

停用期间使用的 ILM 策略将是停用后使用的策略。在开始停用之前和停用完成后，您必须确保此策略满足您的数据要求。

您应查看活动 ILM 策略中的规则，以确保 StorageGRID 系统将继续具有正确类型和位置的足够容量，以支持存储节点的停用。

请考虑以下几点：

- ILM 评估服务是否可以复制对象数据以满足 ILM 规则？
- 如果在停用过程中某个站点暂时不可用，会发生什么情况？是否可以在备用位置创建其他副本？
- 停用过程将如何影响内容的最终分发？如中所述 整合存储节点，您应先添加新的存储节点，然后再停用旧的存储节点。如果在停用较小的存储节点后添加较大的替代存储节点，则旧存储节点可能接近容量，新存储节点可能几乎没有任何内容。然后，新对象数据的大多数写入操作将定向到新存储节点，从而降低系统操作的整体效率。
- 系统是否会始终包含足够的存储节点来满足活动 ILM 策略？

无法满足的 ILM 策略将导致回退日志和警报，并可能会暂停 StorageGRID 系统的运行。

通过评估表中列出的因素，验证停用过程所产生的建议拓扑是否符合 ILM 策略。

要评估的区域	注释：
Available capacity	是否有足够的存储容量来容纳存储在 StorageGRID 系统中的所有对象数据？ 包括当前存储在要停用的存储节点上的对象数据的永久副本？在停用完成后，是否有足够的容量在合理的时间间隔内处理预期的存储对象数据增长？

要评估的区域	注释：
存储位置	如果整个 StorageGRID 系统中仍有足够的容量，则容量是否位于合适的位置以满足 StorageGRID 系统的业务规则？
Storage type	停用完成后，是否有足够的相应类型存储？例如， ILM 规则可能会规定在内容老化时将内容从一种存储类型移动到另一种存储类型。如果是，您必须确保在 StorageGRID 系统的最终配置中具有足够的相应类型的存储。

相关信息

使用 ILM 管理对象

扩展网格

停用已断开连接的存储节点

您必须了解在存储节点断开连接（运行状况为未知或管理员关闭）时停用存储节点可能会发生什么情况。

停用与网格断开的存储节点时， StorageGRID 会使用其他存储节点中的数据重建已断开连接的节点上的对象数据和元数据。为此，它会在停用过程结束时自动启动数据修复作业。

停用已断开连接的存储节点之前，请注意以下事项：

- 除非您确定已断开连接的节点无法联机或恢复，否则切勿停用此节点。

  如果您认为可以从节点恢复对象数据，请勿执行此操作步骤 。请联系技术支持以确定是否可以进行节点恢复。

- 如果断开连接的存储节点包含某个对象的唯一副本，则在停用此节点时，此对象将丢失。只有当当前连接的存储节点上至少存在一个复制副本或足够多的纠删编码片段时，数据修复作业才能重建和恢复对象。
- 停用已断开连接的存储节点时，停用操作步骤 的完成速度相对较快。但是，数据修复作业可能需要数天或数周才能运行，并且不受停用操作步骤 的监控。您必须手动监控这些作业并根据需要重新启动它们。请参见检查数据修复作业。
- 如果一次停用多个已断开连接的存储节点，则可能会发生数据丢失。如果对象数据，元数据或纠删编码片段的副本太少，则系统可能无法重建数据。

  如果有多个已断开连接的存储节点无法恢复，请联系技术支持以确定最佳操作方案。

整合存储节点

您可以整合存储节点以减少站点或部署的存储节点数，同时增加存储容量。

整合存储节点时，您可以扩展 StorageGRID 系统以添加容量更大的新存储节点，然后停用容量较小的旧存储节点。在停用操作步骤 期间，对象会从旧存储节点迁移到新存储节点。

如果您要将较旧的和较小的设备与新型号或容量较大的设备进行整合，则许多用户都使用节点克隆功能，或者如果不执行一对一更换，则使用节点克隆操作步骤 和停用操作步骤 。

例如，您可以添加两个容量更大的新存储节点来替换三个旧存储节点。您应首先使用扩展操作步骤 添加两个更大的新存储节点，然后使用停用操作步骤 删除三个容量较小的旧存储节点。

通过在删除现有存储节点之前添加新容量，您可以确保在 StorageGRID 系统中更平衡地分布数据。此外，还可以减少现有存储节点可能被推送到存储水印级别以外的可能性。

相关信息

扩展网格

停用多个存储节点

如果需要删除多个存储节点，可以按顺序或并行停用它们。

- 如果您按顺序停用存储节点，则必须等待第一个存储节点完成停用，然后再开始停用下一个存储节点。
- 如果您并行停用存储节点，则存储节点会同时处理要停用的所有存储节点的停用任务。这可能会导致文件的所有永久副本被标记为 `read-only` ， 在启用了此功能的网格中暂时禁用删除。

检查数据修复作业

停用网格节点之前，您必须确认没有处于活动状态的数据修复作业。如果任何修复失败，您必须重新启动修复并让其完成，然后再执行停用操作步骤 。

如果您需要停用已断开连接的存储节点，则还需要在停用操作步骤 完成后完成这些步骤，以确保数据修复作业已成功完成。您必须确保已成功还原已删除节点上的任何经过擦除编码的片段。

这些步骤仅适用于具有纠删编码对象的系统。

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 检查正在运行的修复： `repair-data show-EC-repair-status`
   - 如果您从未运行过数据修复作业，则输出为 `No job found` 。您无需重新启动任何修复作业。
   - 如果数据修复作业先前已运行或当前正在运行，则输出将列出要修复的信息。每个修复都有一个唯一的修复 ID 。继续执行下一步。

```
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. S所有修复的状态为 " 无 "，则无需重新启动任何修复作业。
4. 如果要进行任何修复的状态为 `failure`，则必须重新启动此修复。
   a. 从输出中获取失败修复的修复 ID 。
   b. 运行 `repair-data start-EC-node-repair` 命令。

      使用 ` -repair-id` 选项指定修复 ID 。例如，如果要重试修复 ID 为 949292 的修复，请运行以下命令：
      `repair-data start-EC-node-repair -repair-id 949292`

   c. S跟踪 `EC` 数据修复的状态，直到所有修复的状态为 " 无 " 。

收集所需材料

在执行网格节点停用之前，您必须获取以下信息。

项目	注释：
恢复软件包 ` .zip` 文件	您必须 下载最新的恢复软件包 ` .zip` file （ `sGWS-recovery-package-id-revision.zip` ）。如果发生故障，您可以使用恢复包文件还原系统。
`passwords.txt` file	此文件包含在命令行上访问网格节点所需的密码，并包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
停用前 StorageGRID 系统拓扑的问题描述	如果有，请获取描述系统当前拓扑的任何文档。

相关信息

访问 " 取消配置节点 " 页面

访问网格管理器中的 " 停用节点 " 页面时，您可以一目了然地看到哪些节点可以停用。

您需要的内容

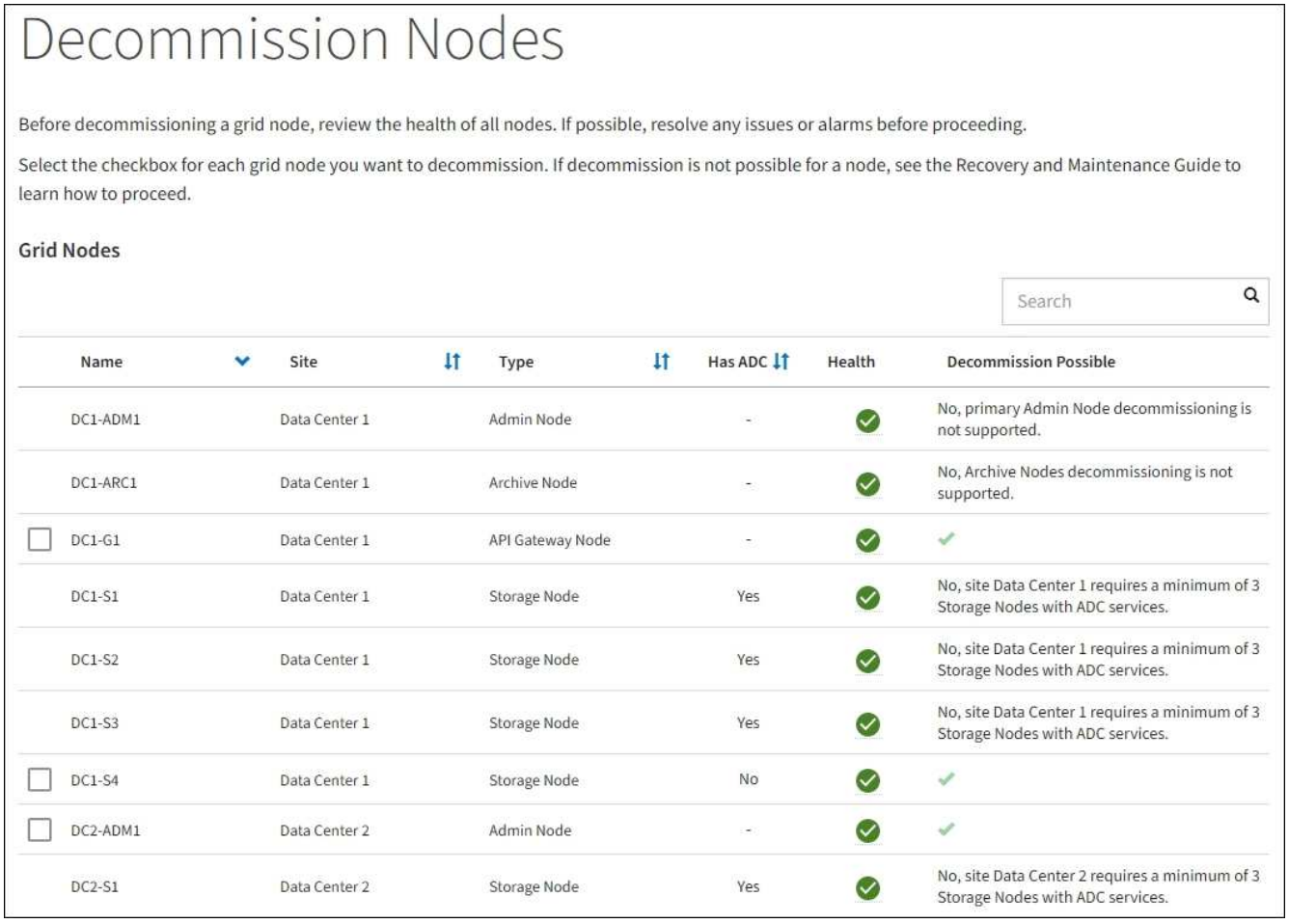
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。

步骤

1. 选择 * 维护 * > * 任务 * > * 取消配置 * 。
2. 选择 * 取消配置节点 * 。

   此时将显示 Decommission Nodes 页面。在此页面中，您可以：

   - 确定当前可以停用的网格节点。
   - 查看所有网格节点的运行状况
   - 按 * 名称 * ， * 站点 * ， * 类型 * 或 * 具有 ADC* 按升序或降序对列表进行排序。
   - 输入搜索词可快速查找特定节点。例如，此页面显示两个数据中心中的网格节点。Decommission possible 列指示您可以停用网关节点，五个存储节点之一和非主管理节点。



3. 查看要停用的每个节点的 * 可能停用 * 列。

   如果可以停用网格节点，则此列会显示一个绿色复选标记，最左侧的列会显示一个复选框。如果无法停用某个节点，此列将介绍问题描述 。如果无法停用某个节点的原因不止一个，则会显示最关键的原因。

停用可能的原因	Description	解决步骤
不支持，不支持节点类型停用。	您不能停用主管理节点或归档节点。	无
否，至少有一个网格节点已断开连接。 • 注： * 此消息仅针对已连接的网格节点显示。	如果任何网格节点已断开连接，则无法停用已连接的网格节点。 对于已断开连接的网格节点， * 运行状况 * 列包含以下图标之一： • （灰色）：已管理员关闭 • （蓝色）：未知	转至 列出停用操作步骤 选项的步骤。
否，一个或多个所需节点当前已断开连接，必须进行恢复。 • 注： * 此消息仅针对已断开连接的网格节点显示。	如果一个或多个所需节点也已断开连接，则您无法停用已断开连接的网格节点（例如，为实现 ADC 仲裁所需的存储节点）。	a. 查看所有已断开连接的节点的 " 取消配置 " 可能消息。 b. 确定哪些节点因需要而无法停用。 ◦ 如果所需节点的运行状况已被管理员关闭，请使此节点重新联机。 ◦ 如果所需节点的运行状况未知，请执行节点恢复操作步骤 以恢复所需节点。
否， HA 组的成员： *x* 。要停用此节点，必须先将其从所有 HA 组中删除。	如果某个节点接口属于高可用性（ HA ）组，则无法停用管理节点或网关节点。	编辑 HA 组以删除节点的接口或删除整个 HA 组。请参见有关管理 StorageGRID 的说明。
不可以，站点 *x* 至少需要具有模块化转换服务的 *n* 存储节点。	• 仅限存储节点。 * 如果站点上保留的节点不足以满足模块化转换仲裁要求，则无法停用存储节点。	执行扩展。向站点添加新的存储节点，并指定其应具有一个模块转换服务。请参见有关模数转换器仲裁的信息。

停用可能的原因	Description	解决步骤
不需要，一个或多个擦除编码配置文件至少需要 *n* 存储节点。如果在 ILM 规则中未使用此配置文件，您可以将其停用。	• 仅限存储节点。 * 除非为现有擦除编码配置文件保留足够的节点，否则无法停用存储节点。 例如，如果 4+2 纠删编码存在擦除编码配置文件，则必须至少保留 6 个存储节点。	对于每个受影响的擦除编码配置文件，根据配置文件的使用方式执行以下步骤之一： • * 用于活动 ILM 策略 * ：执行扩展。添加足够多的新存储节点，以便继续进行纠删编码。请参见有关扩展 StorageGRID 的说明。 • * 用于 ILM 规则，但不用于活动 ILM 策略 * ：编辑或删除规则，然后停用擦除编码配置文件。 • * 未在任何 ILM 规则中使用 * ：停用擦除编码配置文件。 ◦ 注： * 如果您尝试停用擦除编码配置文件，但对象数据仍与该配置文件关联，则会显示一条错误消息。您可能需要等待几周才能再次尝试停用过程。 有关通过信息生命周期管理管理对象的说明，请了解如何停用擦除编码配置文件。

4. 【解压缩程序选择】如果节点可以停用，请确定需要执行的操作步骤：

网格是否包括 ...	转至 ...
任何已断开连接的网格节点	停用已断开连接的网格节点
仅连接网格节点	停用已连接的网格节点

相关信息

检查数据修复作业

了解模数转换器仲裁

使用 ILM 管理对象

扩展网格

管理 StorageGRID

停用已断开连接的网格节点

您可能需要停用当前未连接到网格的节点（运行状况为未知或管理员关闭的节点）。

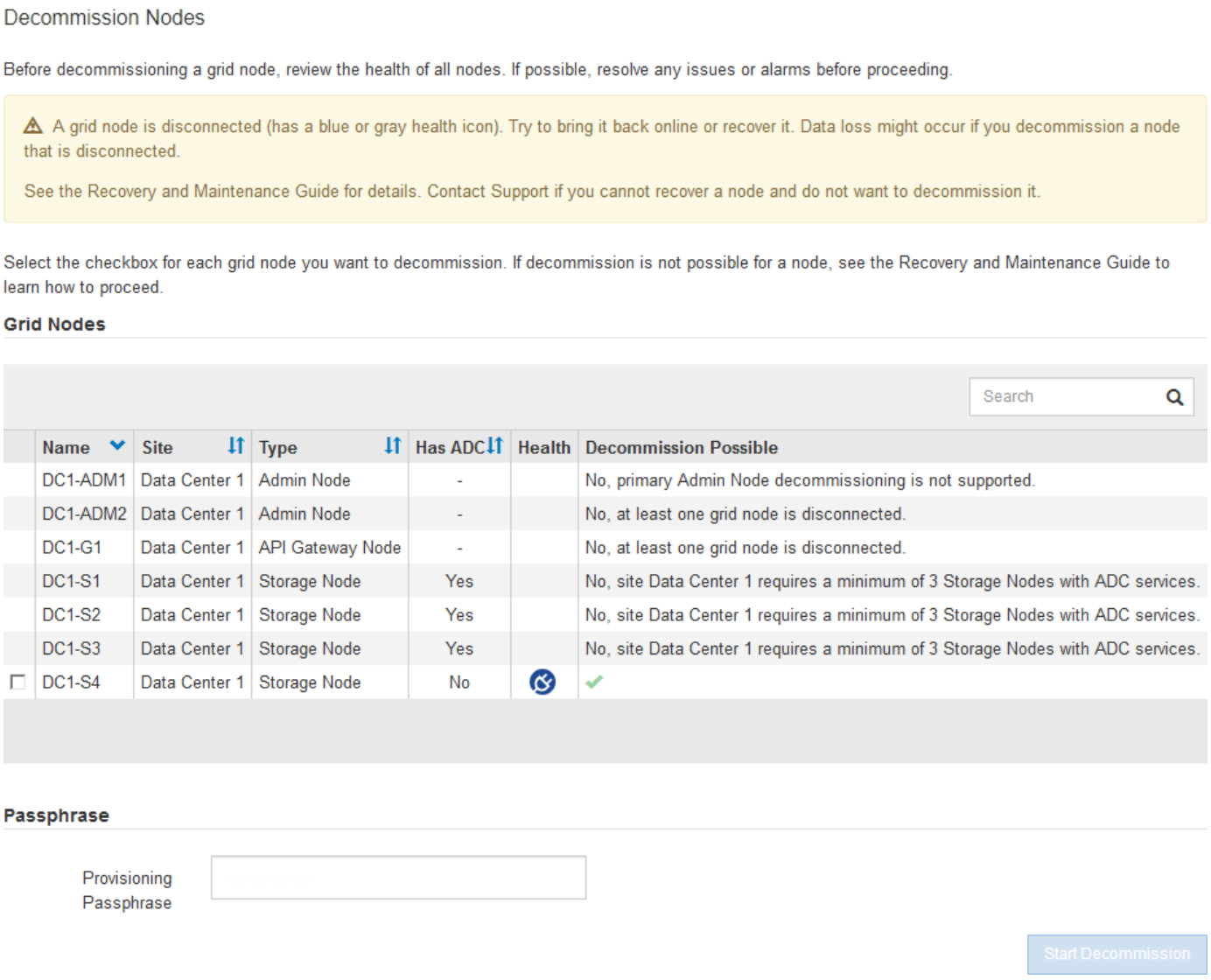
您需要的内容

- 您了解要求和 停用网格节点的注意事项。
- 您已获取所有前提条件项。
- 您已确保没有处于活动状态的数据修复作业。请参见 检查数据修复作业。

- 您已确认网格中的任何位置均未进行存储节点恢复。如果是，则必须等待在恢复过程中执行的任何 Cassandra 重建完成。然后，您可以继续停用。
- 您已确保在节点停用操作步骤 运行期间不会运行其他维护过程，除非节点停用操作步骤 已暂停。
- 要停用的已断开连接节点的 * 可停用 * 列包含一个绿色复选标记。
- 您必须具有配置密码短语。

关于此任务

您可以通过在 * 运行状况 * 列中查找未知（蓝色）或管理员关闭（灰色）图标来识别已断开连接的节点。在此示例中，名为 DC1-S4 的存储节点已断开连接；所有其他节点均已连接。



停用任何已断开连接的节点之前，请注意以下事项：

- 此操作步骤 主要用于删除一个断开连接的节点。如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。

> 一次停用多个断开连接的网格节点时，请务必小心，尤其是在选择多个断开连接的存储节点时。

- 如果无法删除已断开连接的节点（例如，为实现模数转换器仲裁所需的存储节点），则不能删除任何其他已断开连接的节点。

停用已断开连接的 * 存储节点 * 之前，请注意以下事项

- 您不应停用已断开连接的存储节点，除非您确定它无法联机或恢复。

> 如果您认为仍可从节点恢复对象数据，请勿执行此操作步骤 。请联系技术支持以确定是否可以进行节点恢复。

- 如果停用多个已断开连接的存储节点，则可能会发生数据丢失。如果没有足够的对象副本，纠删编码片段或对象元数据保持可用，则系统可能无法重建数据。

> 如果有多个已断开连接的存储节点无法恢复，请联系技术支持以确定最佳操作方案。

- 停用已断开连接的存储节点时， StorageGRID 会在停用过程结束时启动数据修复作业。这些作业会尝试重建已断开连接的节点上存储的对象数据和元数据。
- 停用已断开连接的存储节点时，停用操作步骤 的完成速度相对较快。但是，数据修复作业可能需要数天或数周才能运行，并且不受停用操作步骤 的监控。您必须手动监控这些作业并根据需要重新启动它们。请参见检查数据修复作业。
- 如果停用的存储节点已断开连接，而该存储节点包含某个对象的唯一副本，则该对象将丢失。只有当当前连接的存储节点上至少存在一个复制副本或足够多的纠删编码片段时，数据修复作业才能重建和恢复对象。

停用已断开连接的 * 管理节点 * 或 * 网关节点 * 之前，请注意以下事项：

- 停用已断开连接的管理节点时，该节点上的审核日志将丢失；但是，这些日志也应存在于主管理节点上。
- 您可以在网关节点断开连接时安全地停用它。

步骤

1. 尝试将任何已断开连接的网格节点恢复联机或进行恢复。

   有关说明，请参见恢复过程。

2. 如果无法恢复已断开连接的网格节点，并且您希望在该节点断开连接后将其停用，请选中该节点的复选框。

> 如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。

> 如果选择一次停用多个断开连接的网格节点，请务必格外小心，尤其是在选择多个断开连接的存储节点时。如果有多个已断开连接的存储节点无法恢复，请联系技术支持以确定最佳操作方案。

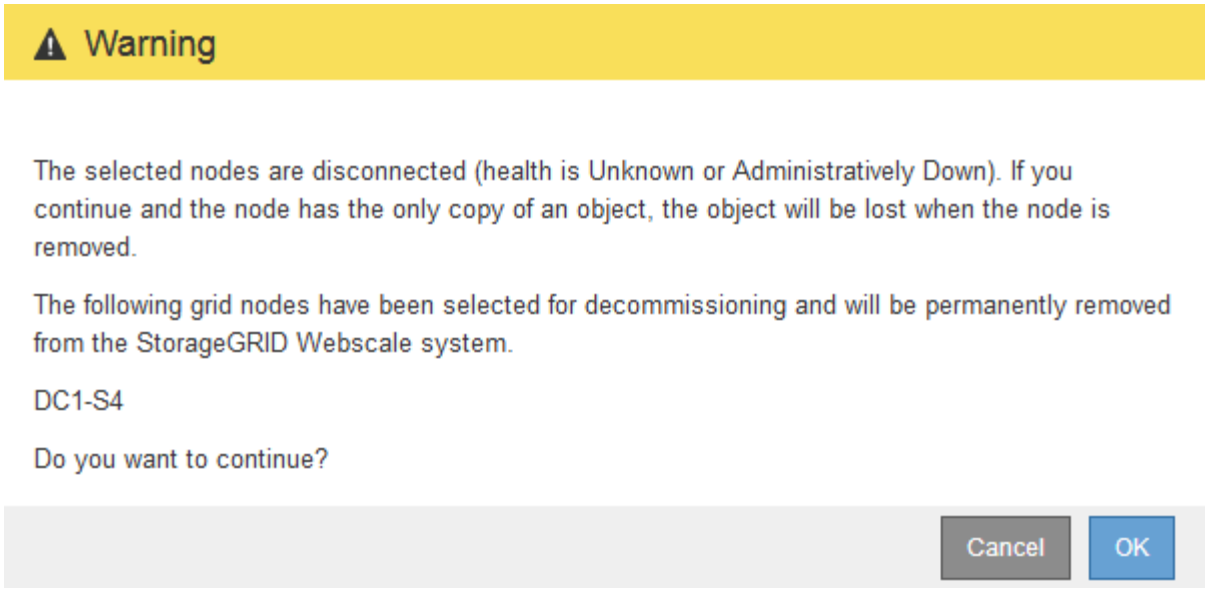
3. 输入配置密码短语。

   已启用 * 开始取消配置 * 按钮。

4. 单击 * 开始取消配置 * 。

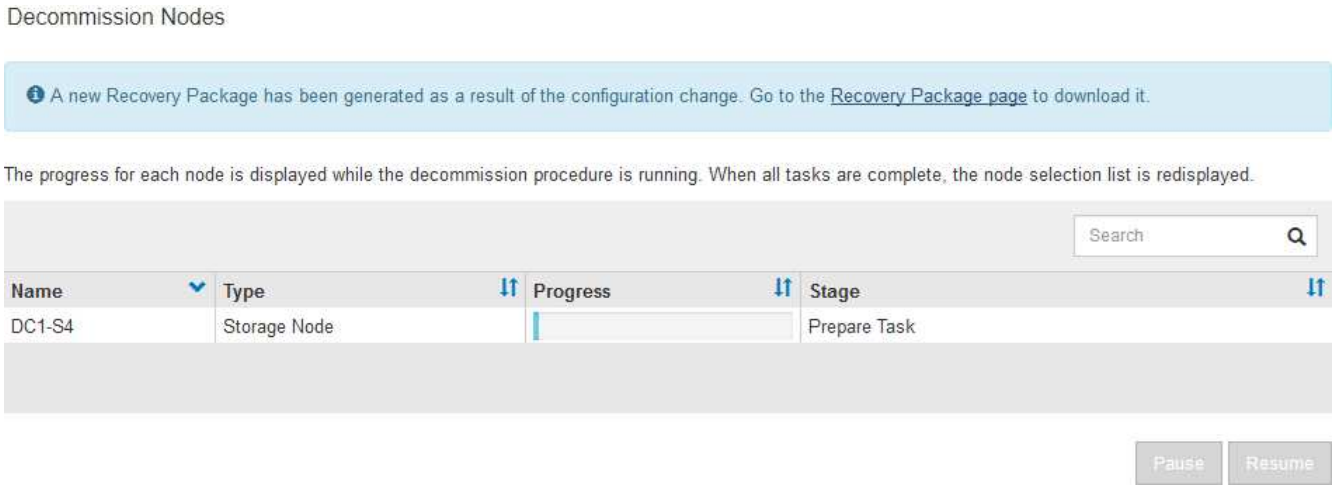
   此时将显示一条警告，指示您已选择断开连接的节点，如果此节点具有唯一的对象副本，则此对象数据将丢

失。



5. 查看节点列表，然后单击 * 确定 * 。

   停用操作步骤 将启动，并显示每个节点的进度。在操作步骤 期间，将生成一个新的恢复软件包，其中包含网格配置更改。



6. 新的恢复软件包一旦可用，请单击链接或选择 * 维护 * > * 系统 * > * 恢复软件包 * 以访问 " 恢复软件包 " 页面。然后，下载 ` .zip` 文件。

   请参见的说明 正在下载恢复包。

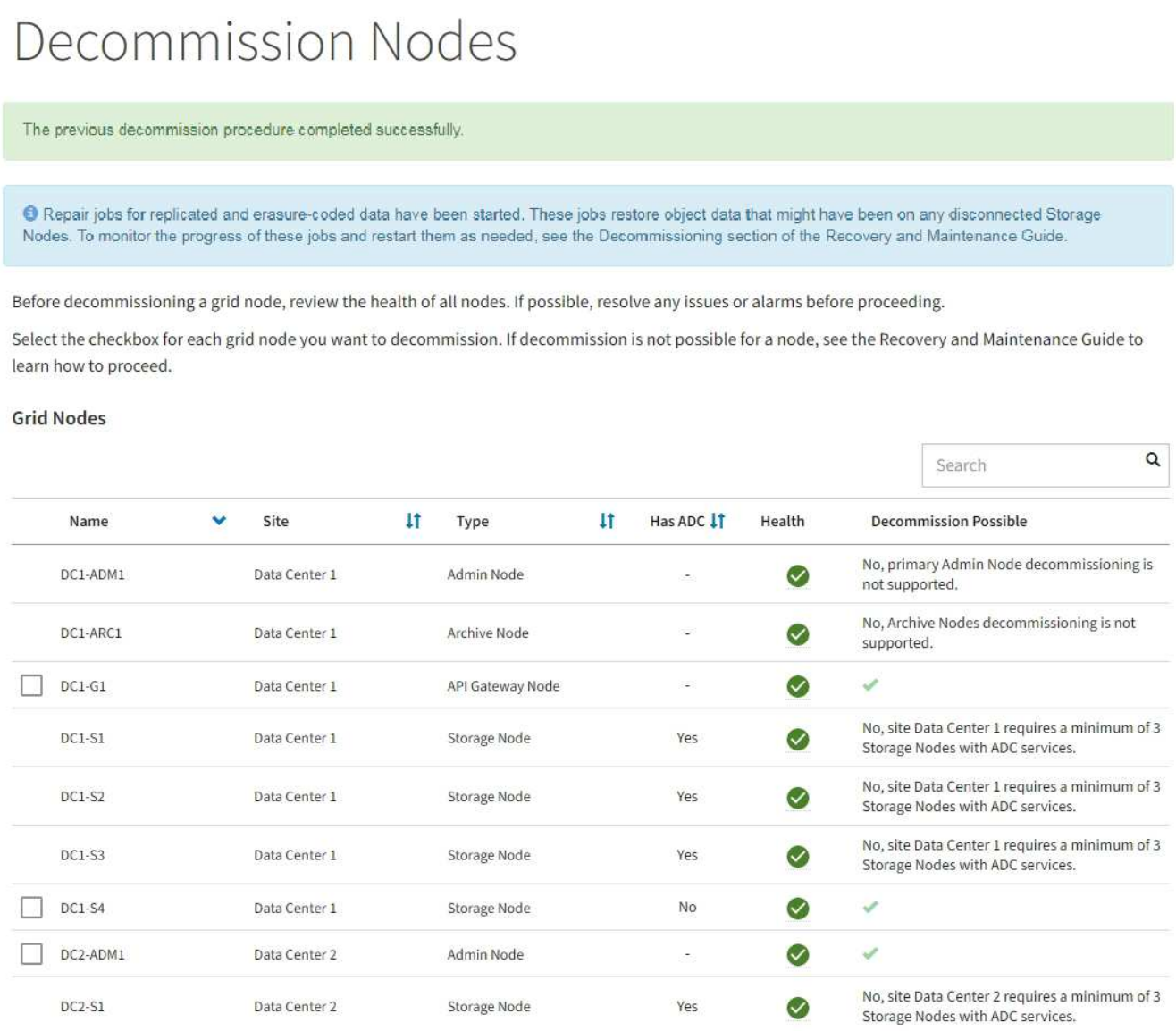
   请尽快下载恢复包，以确保在停用操作步骤 期间出现问题时可以恢复网格。

   恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

7. 定期监控 " 停用 " 页面，以确保所有选定节点均已成功停用。

   存储节点停用可能需要数天或数周时间。完成所有任务后，系统将重新显示节点选择列表，并显示成功消

息。如果停用了已断开连接的存储节点，则会显示一条信息消息，指出修复作业已启动。



8. 在停用操作步骤 期间自动关闭节点后，请删除与已停用节点关联的任何剩余虚拟机或其他资源。

   在节点自动关闭之前，请勿执行此步骤。

9. 如果要停用存储节点，请监控在停用过程中自动启动的 * 复制数据 * 和 * 纠删编码（ EC ）数据 * 修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

完成后

一旦断开连接的节点停用并完成所有数据修复作业，您就可以根据需要停用任何已连接的网格节点。

然后，在完成停用操作步骤 后完成以下步骤：

- 确保已停用网格节点的驱动器已擦除干净。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果您停用了某个设备节点，并且该设备上的数据已使用节点加密进行保护，请使用 StorageGRID 设备安装程序清除密钥管理服务器配置（清除 KMS ）。如果要将设备添加到另一个网格，则必须清除 KMS 配置。
  - SG100 和 SG1000 服务设备
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备

相关信息

网格节点恢复过程

停用已连接的网格节点

您可以停用并永久删除连接到网格的节点。

- 您必须了解要求和 停用网格节点的注意事项。
- 您必须已收集所有必需的材料。
- 您必须确保没有处于活动状态的数据修复作业。
- 您必须已确认网格中任何位置均未进行存储节点恢复。如果是，则必须等待在恢复过程中执行的任何 Cassandra 重建完成。然后，您可以继续停用。
- 您必须确保在节点停用操作步骤 运行期间不会运行其他维护过程，除非节点停用操作步骤 已暂停。
- 您必须具有配置密码短语。
- 已连接网格节点。
- 要停用的一个或多个节点的 * 可能停用 * 列必须包含一个绿色复选标记。

- 所有网格节点都必须运行状况正常（绿色） 。如果您在 * 运行状况 * 列中看到以下图标之一，则必须尝试解析问题描述：

图标。	颜色	severity
	黄色	通知
	浅橙色	次要
	深橙色	major
	红色	严重

- 如果您先前停用了已断开连接的存储节点，则数据修复作业均已成功完成。请参见 检查数据修复作业。

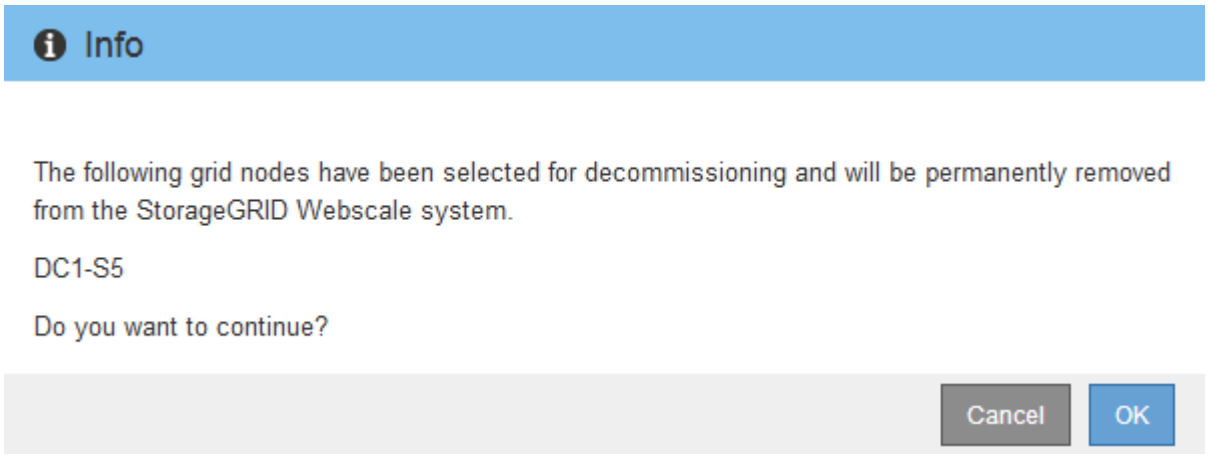
> 除非在此操作步骤 中指示删除网格节点的虚拟机或其他资源，否则请勿删除此虚拟机或其他资源。

1. 从 " 停用节点 " 页面中，选中要停用的每个网格节点对应的复选框。
2. 输入配置密码短语。

   已启用 * 开始取消配置 * 按钮。

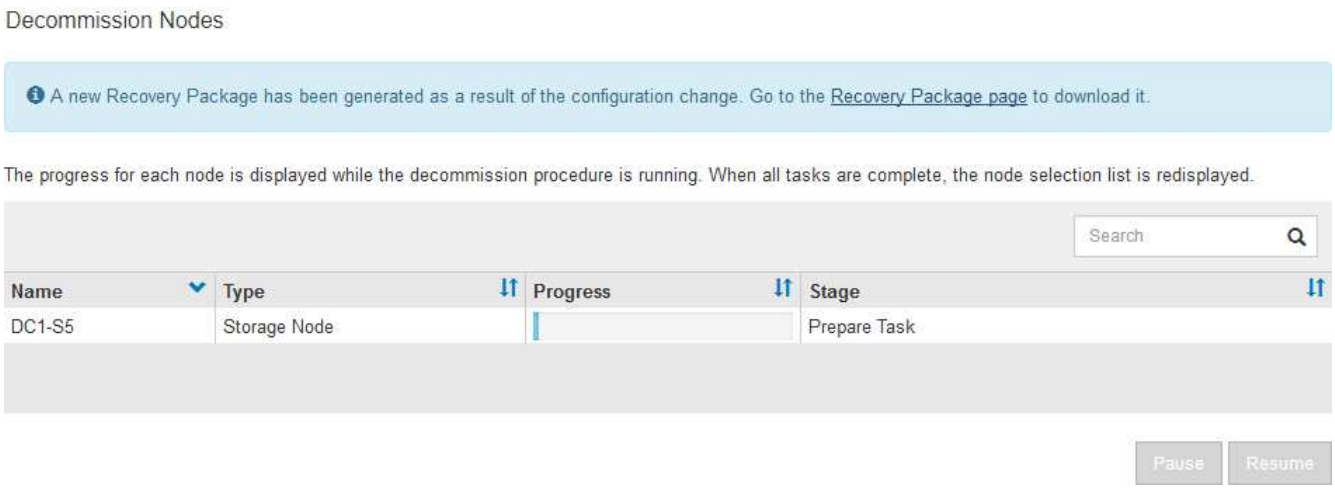
3. 单击 * 开始取消配置 * 。

   此时将显示确认对话框。



4. 查看选定节点的列表，然后单击 * 确定 * 。

   此时将启动节点停用操作步骤 ，并显示每个节点的进度。在操作步骤 期间，系统会生成一个新的恢复软件包以显示网格配置更改。



停用操作步骤 启动后，请勿使存储节点脱机。更改状态可能会导致某些内容未复制到其他位置。

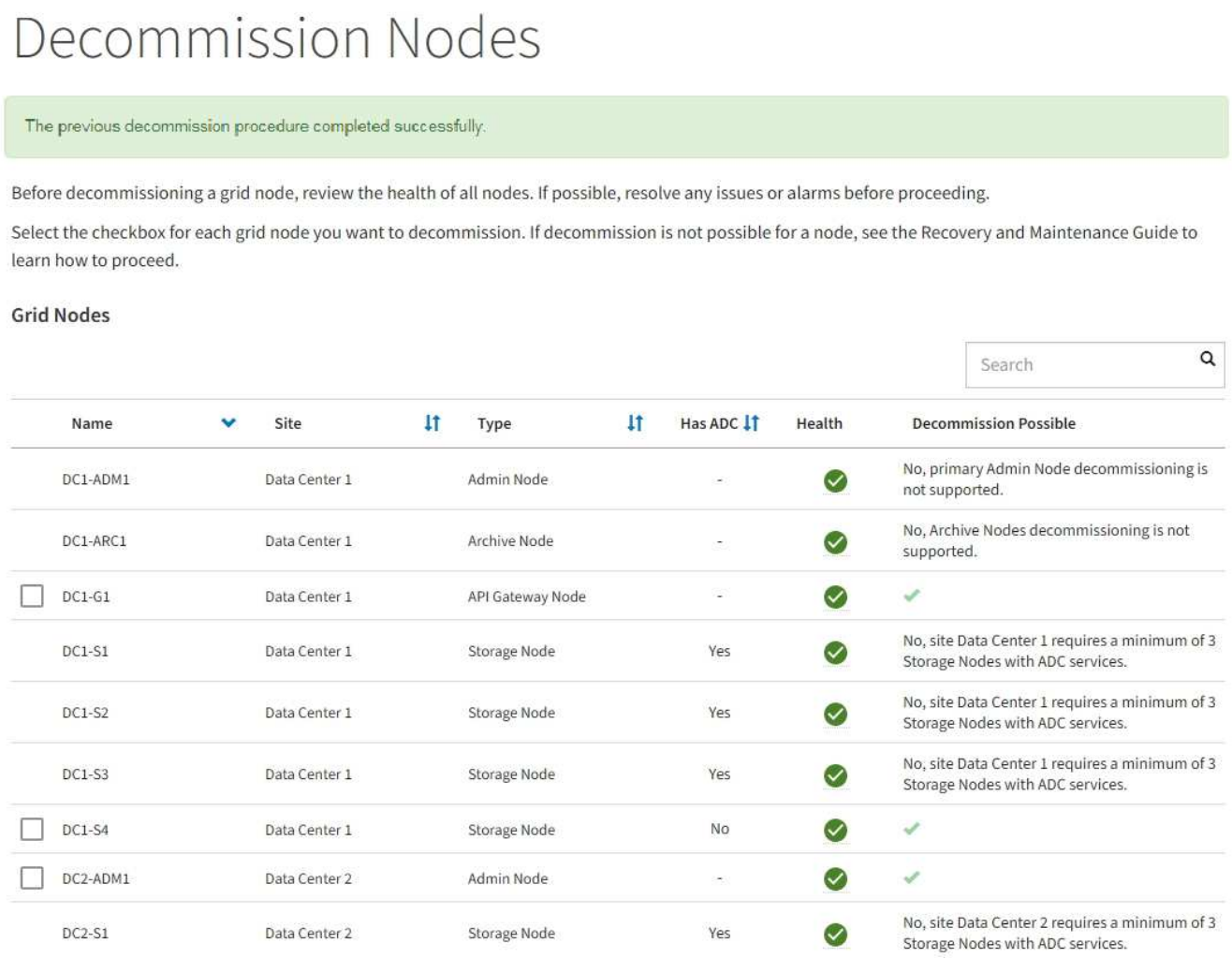
5. 新的恢复软件包一旦可用，请单击链接或选择 * 维护 * > * 系统 * > * 恢复软件包 * 以访问 " 恢复软件包 " 页面。然后，下载 ` .zip` 文件。

   请参见的说明 正在下载恢复包。

   请尽快下载恢复包，以确保在停用操作步骤 期间出现问题时可以恢复网格。

6. 定期监控 " 停用节点 " 页面，以确保所有选定节点均已成功停用。

   存储节点停用可能需要数天或数周时间。完成所有任务后，系统将重新显示节点选择列表，并显示成功消息。



7. 按照适用于您的平台的步骤进行操作。例如：
   - * Linux * ： 您可能需要断开卷的连接并删除在安装期间创建的节点配置文件。
   - * D * ： 您可能需要使用 vCenter 的 " 从磁盘删除 " 选项来删除虚拟机。您可能还需要删除独立于虚拟机的任何数据磁盘。
   - * StorageGRID 设备 * ： 设备节点会自动恢复为未部署状态，您可以在此状态下访问 StorageGRID 设备安装程序。您可以关闭设备电源或将其添加到另一个 StorageGRID 系统。

完成节点停用操作步骤 后，请完成以下步骤：

- 确保已停用网格节点的驱动器已擦除干净。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果您停用了某个设备节点，并且该设备上的数据已使用节点加密进行保护，请使用 StorageGRID 设备安装程序清除密钥管理服务器配置（清除 KMS ）。如果要在另一网格中使用此设备，则必须清除 KMS 配置。

SG100 和 SG1000 服务设备

SG5600 存储设备

SG5700 存储设备

SG6000 存储设备

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

暂停和恢复存储节点的停用过程

如果需要执行第二个维护操作步骤 ，可以在某些阶段暂停存储节点的停用操作步骤 。另一个操作步骤 完成后，您可以恢复停用。

只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。

步骤

1. 选择 * 维护 * > * 任务 * > * 取消配置 * 。

   此时将显示 Decommission 页面。

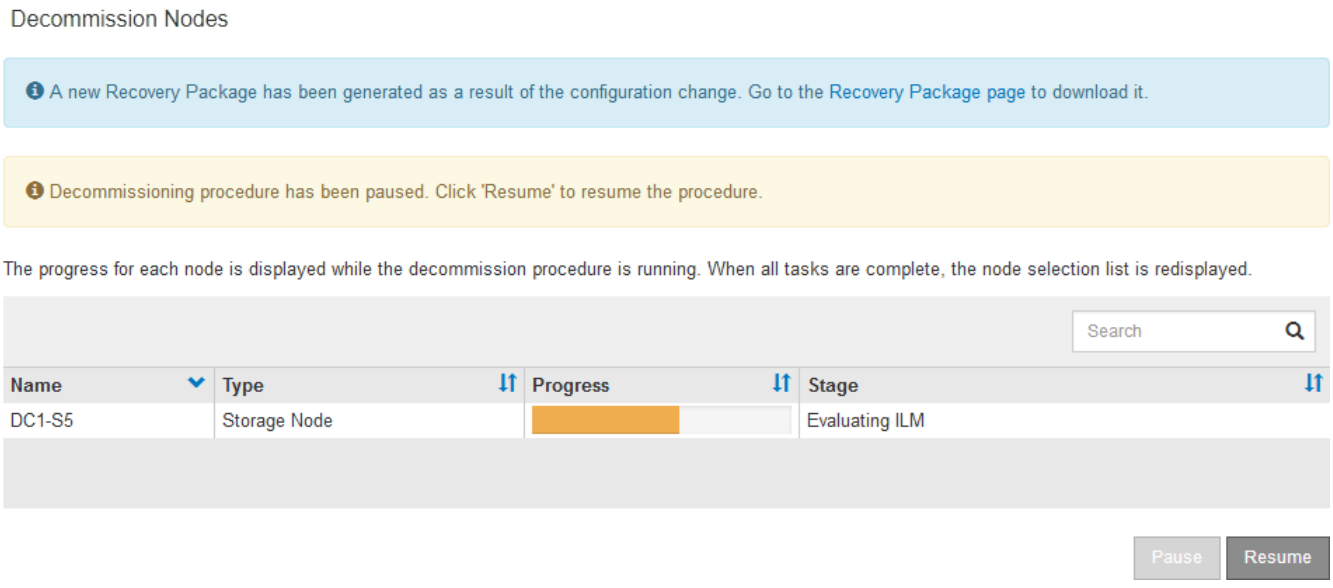
2. 选择 * 取消配置节点 * 。

   此时将显示 Decommission Nodes 页面。当停用操作步骤 达到以下任一阶段时， * 暂停 * 按钮将处于启用状态。

   - 评估 ILM
   - 停用纠删编码数据

3. 选择 * 暂停 * 以暂停操作步骤 。

   当前阶段已暂停，并且 * 恢复 * 按钮已启用。



4. 另一个维护操作步骤 完成后，选择 * 恢复 * 继续执行停用。

如果节点停用操作步骤 因错误而停止，您可以采取特定步骤对问题进行故障排除。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

如果关闭要停用的网格节点，则此任务将停止，直到网格节点重新启动为止。网格节点必须处于联机状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 在网格拓扑树中，展开每个存储节点条目，并验证 DDS 和 LDR 服务是否均联机。

   要执行存储节点停用，在联机节点 / 站点停用开始时，所有节点和所有服务都必须运行正常。

3. 要查看活动的网格任务，请选择 * 主管理节点 * > * 。 CMN* > * 网格任务 * > * 概述 * 。
4. 检查停用网格任务的状态。

   a. 如果停用网格任务的状态指示保存网格任务包时出现问题，请选择 * 主管理节点 * > * 。 CMN* > * 事件 * > * 。概述 *

   b. 检查可用审核中继的数量。

      如果可用审核中继属性为一个或多个，则 CMN 服务至少会连接到一个 ADE 服务。ADC" 服务 " 充当审核中继。

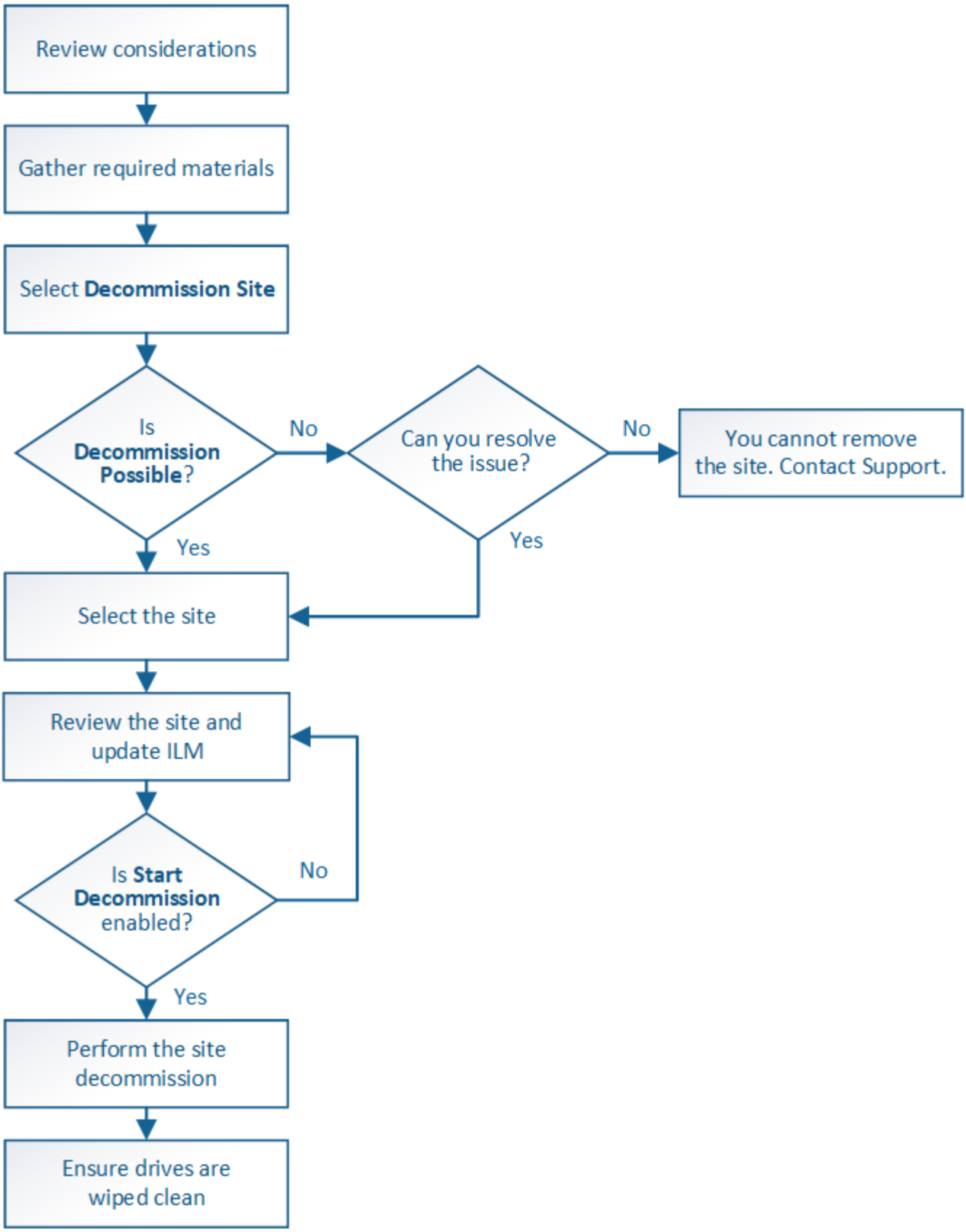
   CMN 服务必须至少连接到一个 StorageGRID 服务，并且必须有大部分（ 50% 加上一个）的系统的 ADC 服务可用，才能使网格任务从停用的一个阶段转移到另一个阶段并完成。

   a. 如果 CMN 服务未连接到足够的模块转换服务，请确保存储节点处于联机状态，并检查主管理节点与存储节点之间的网络连接。

站点停用

您可能需要从 StorageGRID 系统中删除数据中心站点。要删除站点，必须停用它。

流程图显示了停用站点的高级步骤。



删除站点的注意事项

在使用站点停用操作步骤 删除站点之前，您必须查看注意事项。

停用站点时会发生什么情况

停用站点时， StorageGRID 会从 StorageGRID 系统中永久删除站点上的所有节点以及站点本身。

站点停用操作步骤 完成后：

- 您不能再使用 StorageGRID 查看或访问站点或站点上的任何节点。
- 您不能再使用引用此站点的任何存储池或擦除编码配置文件。当 StorageGRID 停用站点时，它会自动删除这些存储池并停用这些擦除编码配置文件。

已连接站点与已断开站点停用过程之间的差异

您可以使用站点停用操作步骤 删除所有节点均已连接到 StorageGRID 的站点（称为已连接站点停用），或者删除所有节点均已与 StorageGRID 断开连接的站点（称为已断开连接的站点停用）。开始之前，您必须了解这些过程之间的差异。

> 如果站点包含混合的 Connected （）和已断开连接的节点（ 或 ），您必须使所有脱机节点重新联机。

- 通过已连接站点停用，您可以从 StorageGRID 系统中删除操作站点。例如，您可以执行已连接站点停用以删除正常运行但不再需要的站点。
- 当 StorageGRID 删除已连接站点时，它会使用 ILM 管理该站点上的对象数据。在开始停用已连接站点之前，必须先从所有 ILM 规则中删除此站点并激活新的 ILM 策略。迁移对象数据的 ILM 过程和删除站点的内部过程可以同时进行，但最佳实践是，在开始实际停用操作步骤 之前，允许完成 ILM 步骤。
- 断开连接的站点停用允许您从 StorageGRID 系统中删除故障站点。例如，您可以执行已断开连接的站点停用，以删除已被火灾或洪水破坏的站点。

  当 StorageGRID 删除已断开连接的站点时，它会将所有节点视为不可恢复的，并且不会尝试保留数据。但是，在开始执行已断开连接的站点停用之前，必须先从所有 ILM 规则中删除此站点并激活新的 ILM 策略。

> 在执行已断开连接的站点停用操作步骤 之前，您必须联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。如果您认为可以恢复站点或从站点恢复对象数据，则不应尝试执行已断开连接的站点停用。

删除已连接或已断开连接的站点的一般要求

在删除已连接或已断开连接的站点之前，您必须了解以下要求：

- 您不能停用包含主管理节点的站点。
- 您不能停用包含归档节点的站点。
- 如果任何节点的接口属于高可用性（ HA ）组，则无法停用站点。您必须编辑 HA 组以删除节点的接口或删除整个 HA 组。
- 如果站点包含已连接（）并断开连接（ 或 ）节点。
- 如果任何其他站点上的任何节点已断开连接（ 或 ）。
- 如果正在执行 EC-node-repair 操作，则无法启动站点停用操作步骤 。请参见 检查数据修复作业 跟踪纠删编码数据的修复情况。

- 站点停用操作步骤 运行时：
  - 您不能创建引用要停用的站点的 ILM 规则。您也不能编辑现有 ILM 规则来引用站点。
  - 您不能执行其他维护过程，例如扩展或升级。

> 如果您需要在已连接站点停用期间执行另一个维护操作步骤 ，则可以 在删除存储节点时暂停操作步骤。只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。第二个维护操作步骤 完成后，您可以恢复停用。

  - 如果您需要在启动站点停用操作步骤 后恢复任何节点，必须联系支持部门。
- 您不能一次停用多个站点。
- 如果站点包含一个或多个管理节点，并且为 StorageGRID 系统启用了单点登录（ Single Sign-On ， SSO ），则必须从 Active Directory 联合身份验证服务（ Active Directory Federation Services ， AD FS ）中删除此站点的所有依赖方信任。

信息生命周期管理（ **ILM** ）的要求

在删除站点时，您必须更新 ILM 配置。" 取消配置站点 " 向导将指导您完成许多前提条件步骤，以确保满足以下要求：

- 此站点不是由活动 ILM 策略引用的。如果是，则必须使用新的 ILM 规则创建并激活新的 ILM 策略。
- 不存在建议的 ILM 策略。如果您有建议的策略，则必须将其删除。
- 任何 ILM 规则都不引用站点，即使活动策略或建议策略中未使用这些规则也是如此。您必须删除或编辑引用此站点的所有规则。

当 StorageGRID 停用站点时，它将自动停用引用该站点的任何未使用的擦除编码配置文件，并自动删除引用该站点的任何未使用的存储池。系统默认的所有存储节点存储池将被删除，因为它会使用所有站点。

> 在删除站点之前，您可能需要创建新的 ILM 规则并激活新的 ILM 策略。这些说明假定您已充分了解 ILM 的工作原理，并且熟悉创建存储池，擦除编码配置文件， ILM 规则以及模拟和激活 ILM 策略。请参见有关通过信息生命周期管理来管理对象的说明。

使用 ILM 管理对象

已连接站点上的对象数据注意事项

如果要执行已连接站点停用，则必须在创建新的 ILM 规则和新的 ILM 策略时确定如何处理站点上的现有对象数据。您可以执行以下任一操作，也可以同时执行这两项操作：

- 将对象数据从选定站点移动到网格中的一个或多个其他站点。
- 移动数据的示例 * ：假设您要停用罗利的某个站点，因为您在森尼韦尔添加了一个新站点。在此示例中，您希望将所有对象数据从旧站点移动到新站点。在更新 ILM 规则和 ILM 策略之前，您必须查看两个站点的容量。您必须确保森尼韦尔站点具有足够的容量来容纳来自罗利站点的对象数据，并且森尼韦尔将保留足够的容量以满足未来增长的需要。

> 要确保有足够的可用容量，您可能需要先向现有站点添加存储卷或存储节点，或者添加新站点，然后再执行此操作步骤 。请参见有关扩展 StorageGRID 系统的说明。

- 从选定站点删除对象副本。
- 删除数据的示例 * ：假设您当前使用 3 个副本 ILM 规则在三个站点之间复制对象数据。在停用站点之前，您可以创建等效的双副本 ILM 规则，以便仅将数据存储在两个站点上。激活使用双副本规则的新 ILM 策略时， StorageGRID 会从第三个站点删除这些副本，因为它们不再满足 ILM 要求。但是，对象数据仍会受到保护，其余两个站点的容量将保持不变。

> 切勿创建单个副本 ILM 规则来容纳站点的删除。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

已连接站点停用的其他要求

在 StorageGRID 删除已连接站点之前，您必须确保满足以下条件：

- StorageGRID 系统中的所有节点的连接状态都必须为 * 已连接 * （）；但是，节点可以具有活动警报。

> 如果一个或多个节点断开连接，您可以完成 " 取消配置站点 " 向导的步骤 1-4 。但是，除非所有节点均已连接，否则无法完成向导的第 5 步，该步骤将启动停用过程。

- 如果要删除的站点包含用于负载平衡的网关节点或管理节点，则可能需要执行扩展操作步骤 ，以便在另一个站点添加等效的新节点。在启动站点停用操作步骤 之前，请确保客户端可以连接到替代节点。
- 如果要删除的站点包含高可用性（ HA ）组中的任何网关节点或管理节点，则可以完成 " 取消配置站点 " 向导的步骤 1-4 。但是，在从所有 HA 组中删除这些节点之前，您无法完成向导的第 5 步，该步骤将启动停用过程。如果现有客户端连接到包含站点中节点的 HA 组，则必须确保它们可以在删除站点后继续连接到 StorageGRID 。
- 如果客户端直接连接到您要删除的站点上的存储节点，则必须确保它们可以连接到其他站点上的存储节点，然后再启动站点停用操作步骤 。
- 您必须在其余站点上提供足够的空间，以容纳因活动 ILM 策略更改而要移动的任何对象数据。在某些情况下，您可能需要先通过添加存储节点，存储卷或新站点来扩展 StorageGRID 系统，然后才能完成已连接站点的停用。
- 您必须留出足够的时间来完成停用操作步骤 。StorageGRID ILM 过程可能需要数天，数周甚至数月才能从站点中移动或删除对象数据，然后才能停用此站点。

> 从站点移动或删除对象数据可能需要数天，数周甚至数月的时间，具体取决于站点上的数据量，系统上的负载，网络延迟以及所需 ILM 更改的性质。

- 您应尽可能早地完成 " 弃用站点 " 向导的步骤 1-4 。如果您允许在启动实际停用操作步骤 之前从站点移动数据，则停用操作步骤 将更快地完成，并且中断和性能影响更少（方法是在向导的步骤 5 中选择 * 启动停用 * ）。

断开连接的站点停用的其他要求

在 StorageGRID 删除已断开连接的站点之前，您必须确保满足以下条件：

- 您已联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。

如果您认为可以恢复站点或从站点恢复任何对象数据，则不应尝试执行已断开连接的站点停用。

- 站点上的所有节点的连接状态必须为以下之一：
  - * 未知 * （）：节点未连接到网格，原因未知。例如，节点之间的网络连接已断开或电源已关闭。
  - * 管理员关闭 * （）：由于预期原因，节点未连接到网格。例如，节点上的一个或多个节点已正常关闭。
- 所有其他站点上的所有节点的连接状态都必须为 * 已连接 * （）；但是，这些其他节点可能具有活动警报。
- 您必须了解，您将无法再使用 StorageGRID 查看或检索站点上存储的任何对象数据。当 StorageGRID 执行此操作步骤 时，它不会尝试保留已断开连接的站点中的任何数据。

如果您的 ILM 规则和策略旨在防止单个站点丢失，则其余站点上仍存在对象的副本。

- 您必须了解，如果站点包含对象的唯一副本，则该对象将丢失，无法检索。

删除站点时的一致性控制注意事项

S3 存储分段或 Swift 容器的一致性级别可确定 StorageGRID 是否在通知客户端对象载入成功之前将对象元数据完全复制到所有节点和站点。一致性控制可以在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。

StorageGRID 删除站点时，需要确保不会向要删除的站点写入任何数据。因此，它会临时覆盖每个分段或容器的一致性级别。启动站点停用过程后， StorageGRID 会暂时使用强站点一致性来防止将对象元数据写入要删除的站点。

由于这种临时覆盖，请注意，如果其他站点上的多个节点不可用，则站点停用期间发生的任何客户端写入，更新和删除操作都可能失败。

相关信息

技术支持如何执行站点恢复

使用 ILM 管理对象

扩展网格

收集所需材料

停用站点之前，您必须获取以下材料。

项目	注释：
恢复软件包 ` .zip` 文件	您必须下载最新的恢复软件包 ` .zip` 文件（ `sGWS-recovery-package-id-revision.zip` ）。如果发生故障，您可以使用恢复包文件还原系统。

`passwords.txt` file	此文件包含在命令行上访问网格节点所需的密码，并包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
停用前 StorageGRID 系统拓扑的问题描述	如果有，请获取描述系统当前拓扑的任何文档。

相关信息

Web 浏览器要求

下载恢复包

第 **1** 步：选择站点

要确定是否可以停用某个站点，请首先访问 " 停用站点 " 向导。

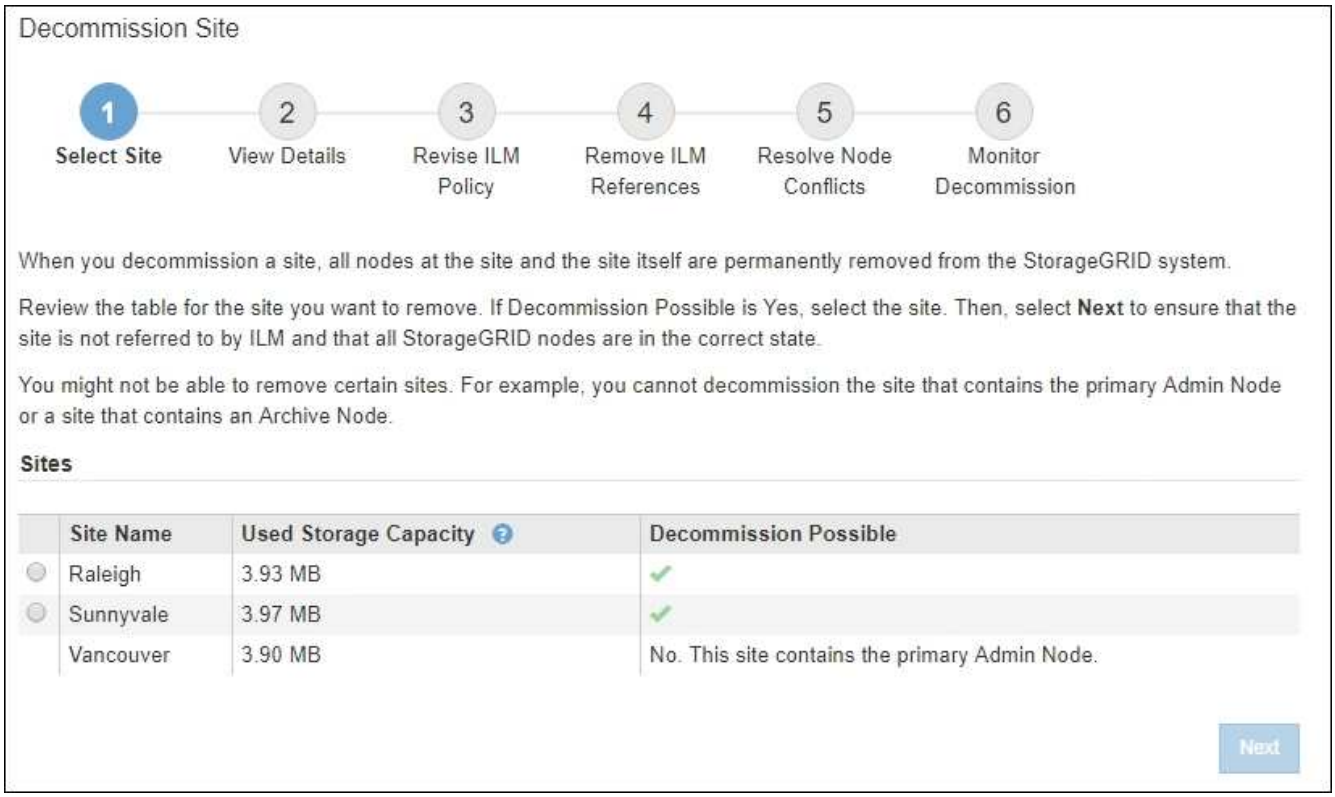
您需要的内容

- 您必须已获取所有必需的材料。
- 您必须已查看删除站点的注意事项。
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有 " 根访问 " 权限或 " 维护 " 和 "ILM " 权限。

步骤

1. 选择 * 维护 * > * 任务 * > * 取消配置 * 。
2. 选择 * 取消配置站点 * 。

   此时将显示取消配置站点向导的第 1 步（选择站点）。此步骤包含 StorageGRID 系统中站点的字母列表。



3. 查看 * 已用存储容量 * 列中的值，确定每个站点上的对象数据当前使用的存储容量。

   已用存储容量是一个估计值。如果节点处于脱机状态，则已用存储容量是站点的最后一个已知值。

   - 对于已连接站点停用，此值表示在安全停用此站点之前需要将多少对象数据移动到其他站点或由 ILM 删除。
   - 对于已断开连接的站点停用，此值表示停用此站点后系统的数据存储容量将变得不可访问。

   如果您的 ILM 策略旨在防止单个站点丢失，则其余站点上仍应存在对象数据的副本。

4. 查看 * 可能停用 * 列中的原因，确定哪些站点当前可以停用。

   如果无法停用某个站点的原因不止一个，则会显示最关键的原因。

停用可能的原因	Description	下一步
绿色复选标记（✔）	您可以停用此站点。	转至 下一步。
否此站点包含主管理节点。	您不能停用包含主管理节点的站点。	无您无法执行此操作步骤 。
否此站点包含一个或多个归档节点。	您不能停用包含归档节点的站点。	无您无法执行此操作步骤 。

停用可能的原因	Description	下一步
否此站点上的所有节点均已断开连接。请联系您的 NetApp 客户代表。	除非站点中的每个节点都已连接（）。	如果您要执行已断开连接的站点停用，必须联系您的 NetApp 客户代表，客户代表将查看您的要求并启用停用站点向导的其余部分。 • 重要信息 *：切勿使联机节点脱机，以便可以删除站点。您将丢失数据。

此示例显示了一个包含三个站点的 StorageGRID 系统。绿色复选标记（）对于罗利和森尼韦尔站点，表示您可以停用这些站点。但是，您无法停用温哥华站点，因为它包含主管理节点。

1. 如果可以停用，请选择站点的单选按钮。

   此时将启用 * 下一步 * 按钮。

2. 选择 * 下一步 * 。

   此时将显示第 2 步（查看详细信息）。

第 **2** 步：查看详细信息

从 " 弃用站点 " 向导的第 2 步（查看详细信息）中，您可以查看站点中包含的节点，查看每个存储节点上已使用的空间量，并评估网格中其他站点上的可用空间量。

您需要的内容

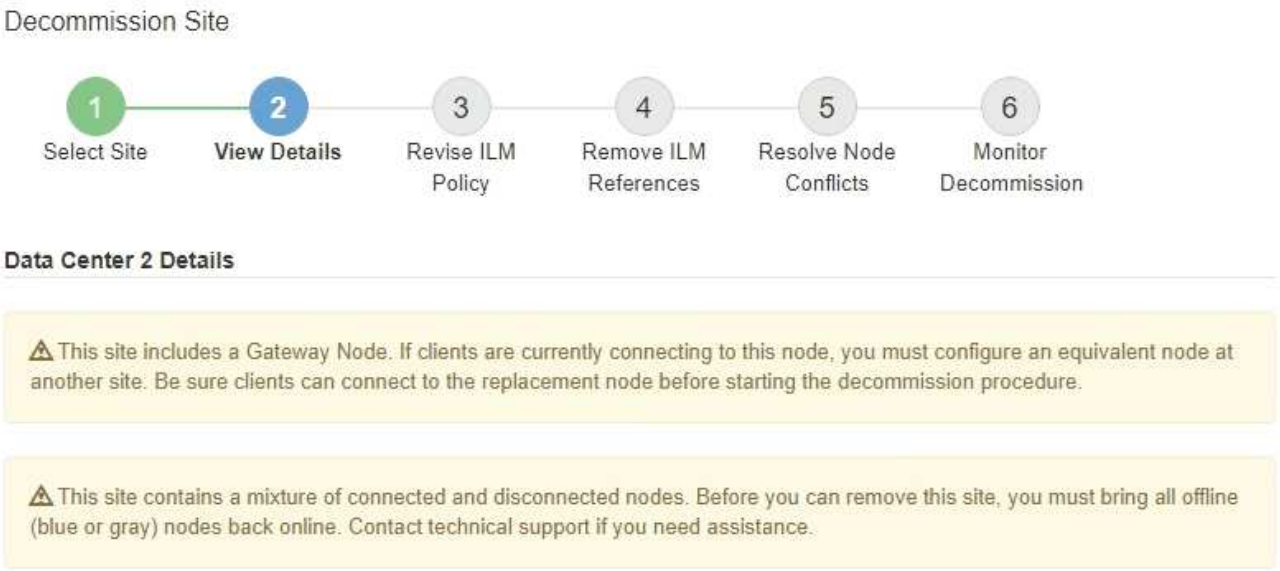
停用站点之前，您必须查看站点上存在的对象数据量。

- 如果您要执行已连接站点停用，则必须先了解站点上当前存在的对象数据量，然后再更新 ILM 。根据站点容量和数据保护需求，您可以创建新的 ILM 规则，将数据移动到其他站点或从站点中删除对象数据。
- 如果可能，请在启动停用操作步骤 之前执行任何所需的存储节点扩展。
- 如果您要执行断开连接的站点停用，则必须了解删除此站点后将永久无法访问多少对象数据。

> 如果您正在执行断开连接的站点停用， ILM 将无法移动或删除对象数据。站点上保留的所有数据都将丢失。但是，如果您的 ILM 策略旨在防止单个站点丢失，则其余站点上仍存在对象数据的副本。

步骤

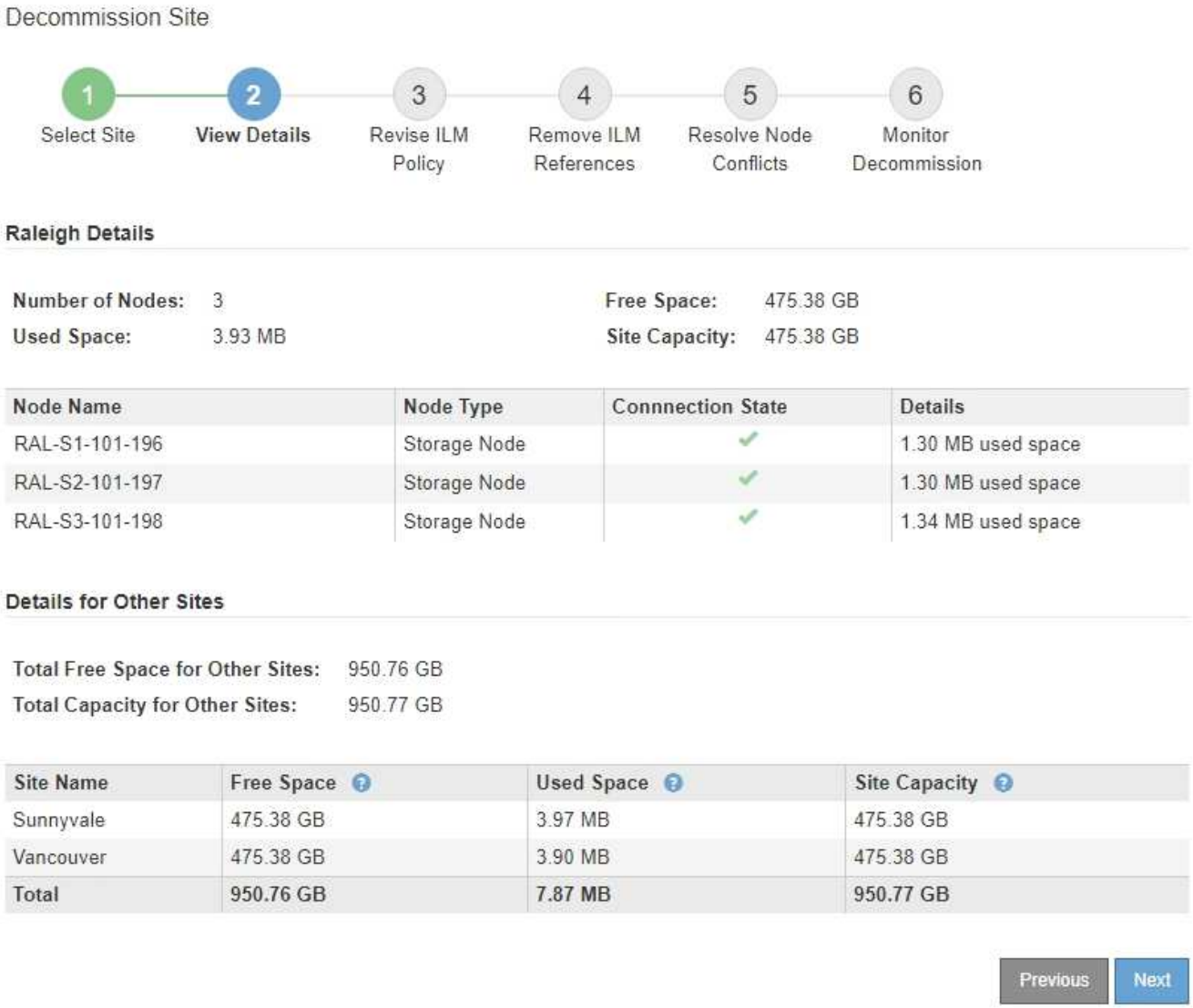
1. 从第 2 步（查看详细信息）中，查看与您选择删除的站点相关的任何警告。



在以下情况下会显示警告：

- 此站点包含一个网关节点。如果 S3 和 Swift 客户端当前正在连接到此节点，则必须在另一站点配置等效节点。在继续执行停用操作步骤 之前，请确保客户端可以连接到替代节点。
- 此站点包含一个混合的 Connected （）和已断开连接的节点（ 或 ）。在删除此站点之前，您必须使所有脱机节点重新联机。

2. 查看有关选定要删除的站点的详细信息。



选定站点包含以下信息：

- 节点数
- 站点中所有存储节点的已用总空间，可用空间和容量。
  - 对于已连接站点停用， * 已用空间 * 值表示必须将多少对象数据移动到其他站点或使用 ILM 删除。
  - 对于已断开连接的站点停用， * 已用空间 * 值表示删除此站点后将无法访问多少对象数据。
- 节点名称，类型和连接状态：
  - （已连接）
  - （管理员关闭）
  - （未知）
- 有关每个节点的详细信息：
  - 对于每个存储节点，为对象数据使用的空间量。
  - 对于管理节点和网关节点，表示此节点当前是否在高可用性（ HA ）组中使用。您不能停用HA组中

使用的管理节点或网关节点。开始停用之前，必须编辑 HA 组以删除站点上的所有节点。或者，如果 HA 组仅包含此站点中的节点，则可以将其删除。

管理 StorageGRID

3. 在页面的其他站点的详细信息部分中，评估网格中其他站点的可用空间量。

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

如果您正在执行已连接站点停用，并且计划使用 ILM 从选定站点移动对象数据（而不是仅删除该数据），则必须确保其他站点具有足够的容量来容纳移动的数据，并且为未来的增长保留足够的容量。

如果要删除的站点的 * 已用空间 * 大于 * 其他站点的总可用空间 * ，则会显示警告。要确保删除站点后有足够的存储容量可用，您可能需要在执行此操作步骤 之前执行扩展。

4. 选择 * 下一步 * 。

此时将显示第 3 步（修订 ILM 策略）。

相关信息

使用 ILM 管理对象

第 3 步：修订 ILM 策略

从 " 弃用站点 " 向导的第 3 步（修订 ILM 策略）中，您可以确定活动的 ILM 策略是否引用此站点。

您需要的内容

您很好地了解 ILM 的工作原理，并且熟悉创建存储池，擦除编码配置文件， ILM 规则以及模拟和激活 ILM 策略。

使用 ILM 管理对象

关于此任务

如果某个站点是由活动 ILM 策略中的任何 ILM 规则引用的，则 StorageGRID 无法停用该站点。

如果您当前的 ILM 策略是指要删除的站点，则必须激活满足特定要求的新 ILM 策略。具体而言，新的 ILM 策略：

- 无法使用引用站点的存储池。

- 无法使用引用站点的擦除编码配置文件。
- 无法使用默认的 * 所有存储节点 * 存储池或默认的 * 所有站点 * 站点。
- 无法使用常用 * 创建 2 个副本 * 规则。
- 必须设计为完全保护所有对象数据。

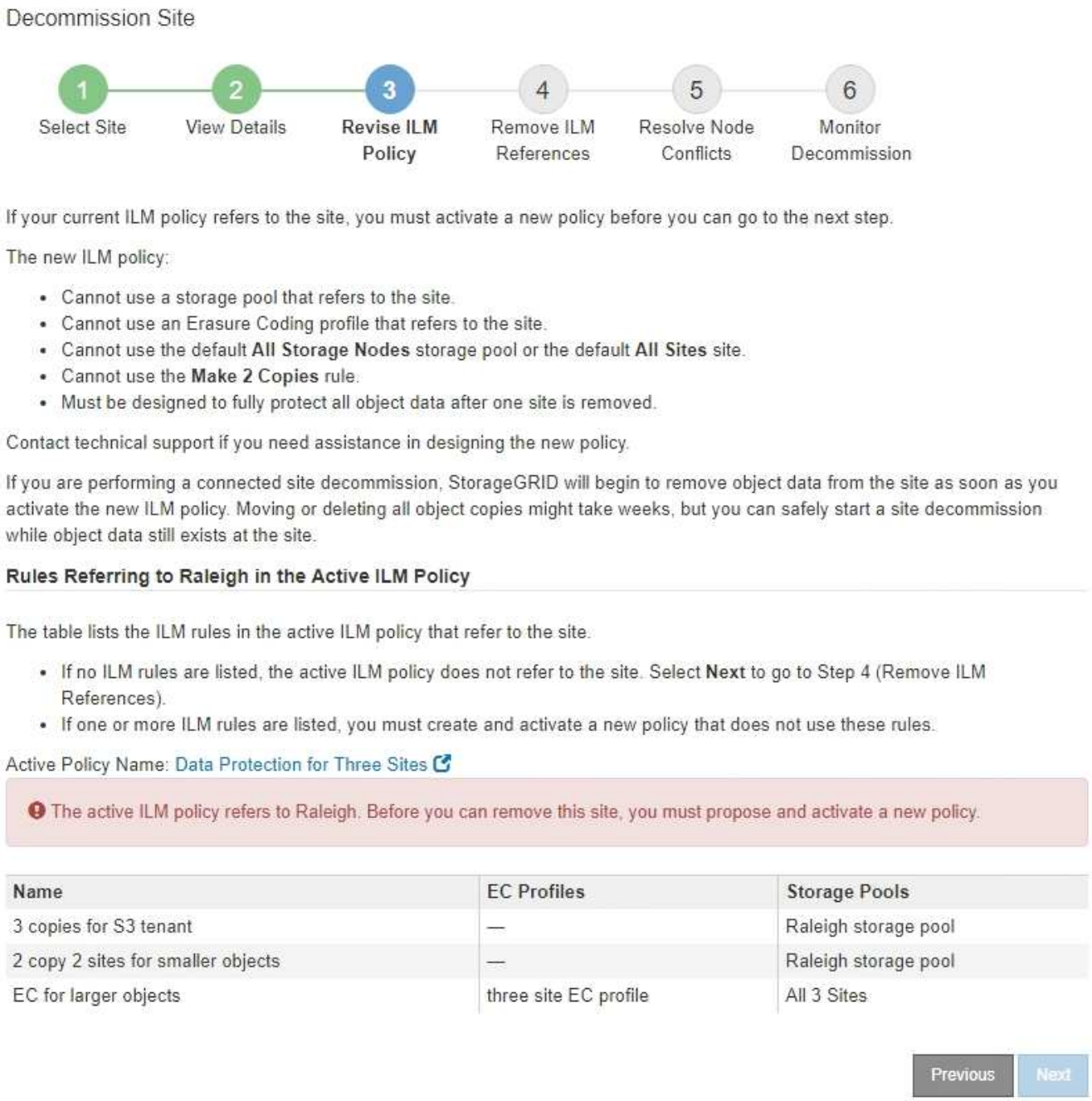
> 切勿创建单个副本 ILM 规则来容纳站点的删除。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

如果您要执行 *connected site decommission* ，则必须考虑 StorageGRID 应如何管理您要删除的站点上当前的对象数据。根据您的数据保护要求，新规则可以将现有对象数据移动到不同的站点，也可以删除不再需要的任何额外对象副本。

如果您在设计新策略时需要帮助，请联系技术支持。

步骤

1. 从第 3 步（修订 ILM 策略）中，确定活动 ILM 策略中的任何 ILM 规则是否引用您选择删除的站点。



2. 如果未列出任何规则，请选择 * 下一步 * 以转到步骤 4 （删除 ILM 引用）

   第 4 步：删除 ILM 引用

3. 如果表中列出了一个或多个 ILM 规则，请选择 * 活动策略名称 * 旁边的链接。

   此时， ILM 策略页面将显示在新的浏览器选项卡中。使用此选项卡更新 ILM 。" 取消配置站点 " 页面将在 " 其他 " 选项卡上保持打开状态。

   a. 如有必要，请选择 * ILM * > * 存储池 * 以创建一个或多个不引用站点的存储池。

      有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

b. 如果您计划使用纠删编码，请选择 * 。 IL* > * 纠删编码 * 以创建一个或多个纠删编码配置文件。

您必须选择不引用站点的存储池。

请勿在擦除编码配置文件中使用 * 所有存储节点 * 存储池。

4. 选择 * ILM * > * 规则 * ，然后克隆步骤 3 （修订 ILM 策略）表中列出的每个规则。

有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

a. 使用名称可以轻松地在新策略中选择这些规则。

b. 更新放置说明。

删除引用站点的任何存储池或擦除编码配置文件，并将其替换为新的存储池或擦除编码配置文件。

请勿在新规则中使用 * 所有存储节点 * 存储池。

5. 选择 * ILM * > * 策略 * ，然后创建一个使用新规则的新策略。

有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

a. 选择活动策略，然后选择 * 克隆 * 。

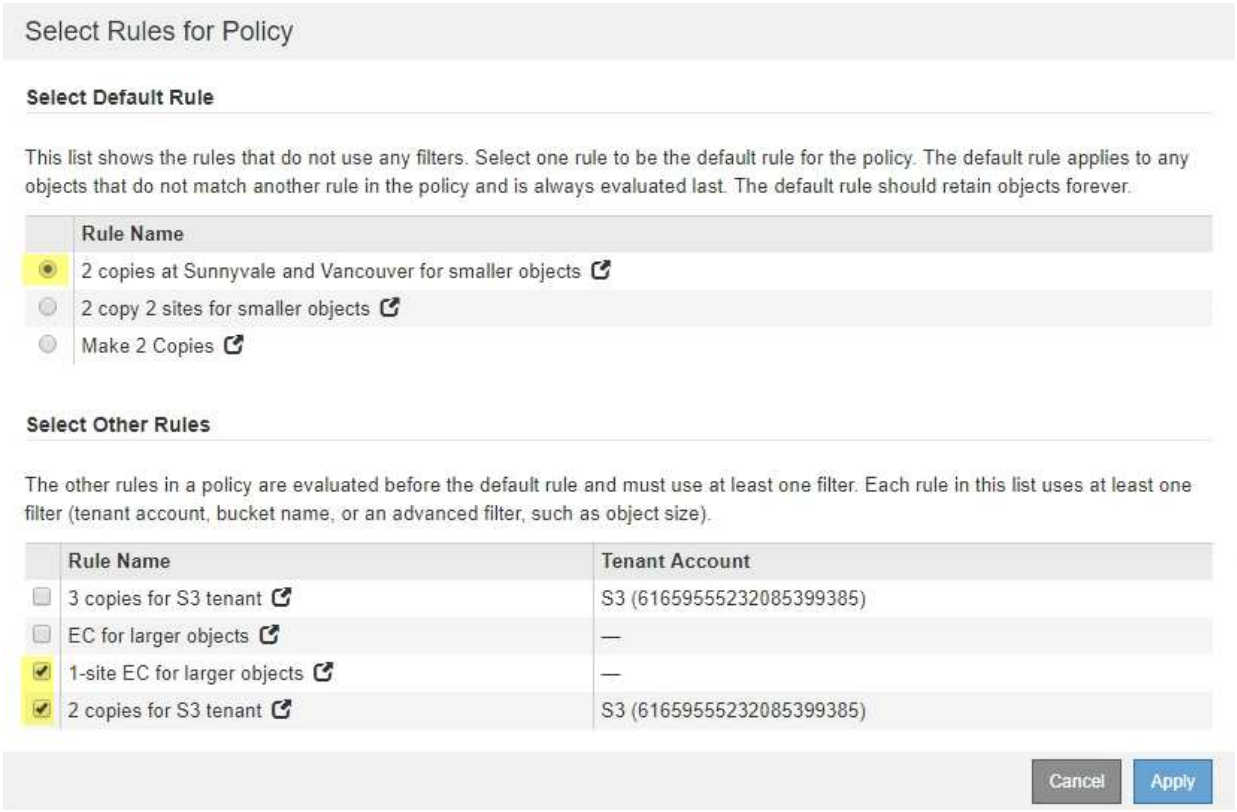
b. 指定策略名称和更改原因。

c. 为克隆的策略选择规则。

- 取消选择 " 弃用站点 " 页面的第 3 步（修订 ILM 策略）中列出的所有规则。
- 选择不引用站点的默认规则。

请勿选择 * 创建 2 个副本 * 规则，因为该规则使用 * 所有存储节点 * 存储池，这是不允许的。

- 选择您创建的其他替换规则。这些规则不应引用站点。



d. 选择 * 应用 * 。

e. 拖放这些行以重新排列策略中的规则。

您不能移动默认规则。

> 您必须确认 ILM 规则的顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。

a. 保存建议的策略。

6. 载入测试对象并模拟建议的策略，以确保应用正确的规则。

> ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。在激活策略之前，请仔细查看并模拟策略，以确认策略将按预期运行。

> 激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

7. 激活新策略。

如果您要执行已连接站点停用，则一旦激活新的 ILM 策略， StorageGRID 就会开始从选定站点删除对象数据。移动或删除所有对象副本可能需要数周时间。尽管在站点上仍存在对象数据的情况下，您可以安全地开始站点停用，但如果您允许在实际停用操作步骤 之前从站点移动数据，则停用操作步骤 将更快地完成，并减少中断和性能影响 （通过在向导的步骤 5 中选择 * 启动取消配置 * ）。

8. 返回到 * 步骤 3 （修订 ILM 策略） * ，以确保新活动策略中没有引用站点的 ILM 规则，并且已启用 * 下一步

* 按钮。



如果列出了任何规则，则必须先创建并激活新的 ILM 策略，然后才能继续。

9. 如果未列出任何规则，请选择 * 下一步 * 。

   此时将显示第 4 步（删除 ILM 参考）。

第 **4** 步：删除 **ILM** 引用

从 " 弃用站点 " 向导的第 4 步（删除 ILM 引用）中，您可以删除建议的策略（如果存在），并删除或编辑仍引用此站点的任何未使用的 ILM 规则。

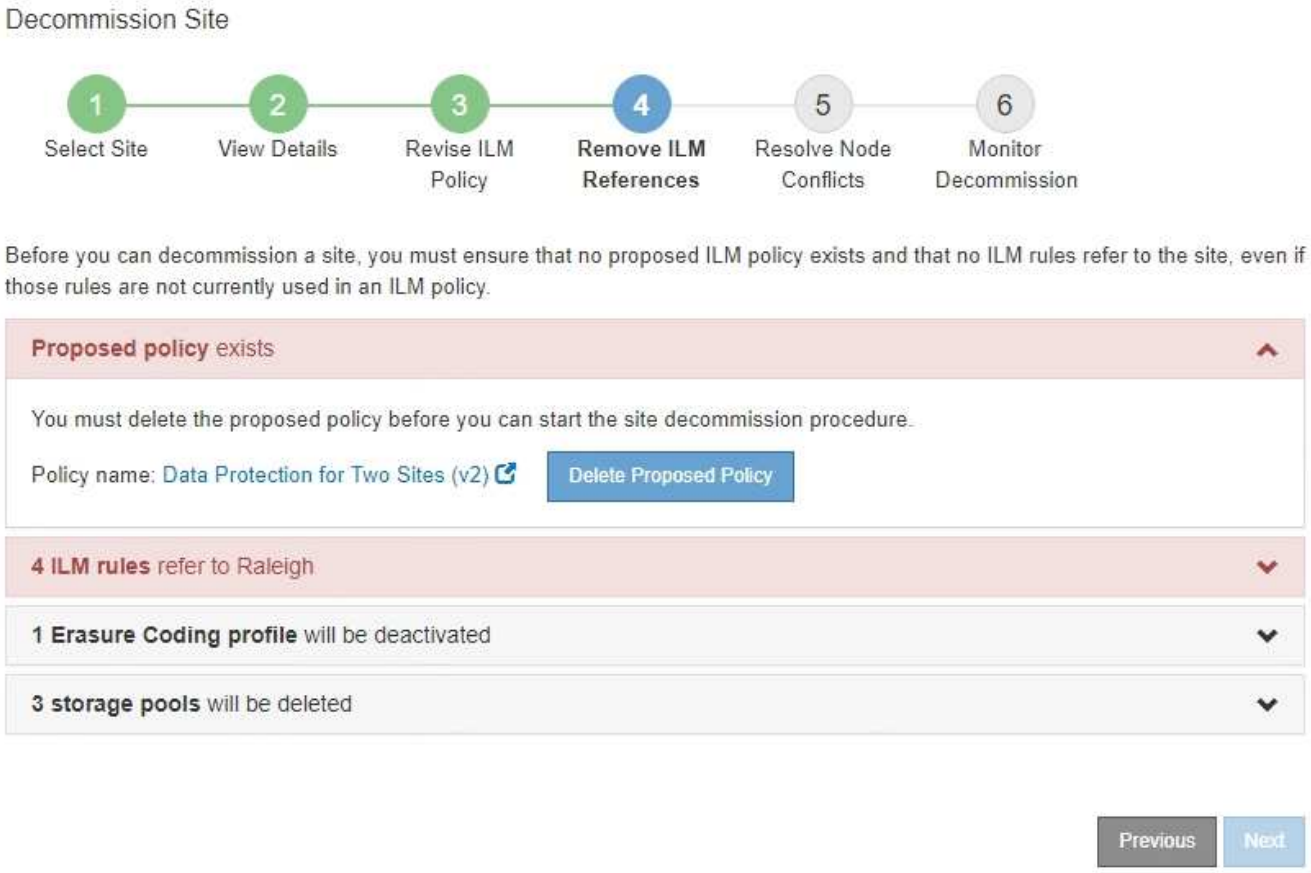
关于此任务

在以下情况下，您将无法启动站点停用操作步骤：

- 已存在建议的 ILM 策略。如果您有建议的策略，则必须将其删除。
- 任何 ILM 规则均指站点，即使此规则未在任何 ILM 策略中使用也是如此。您必须删除或编辑引用此站点的所有规则。

步骤

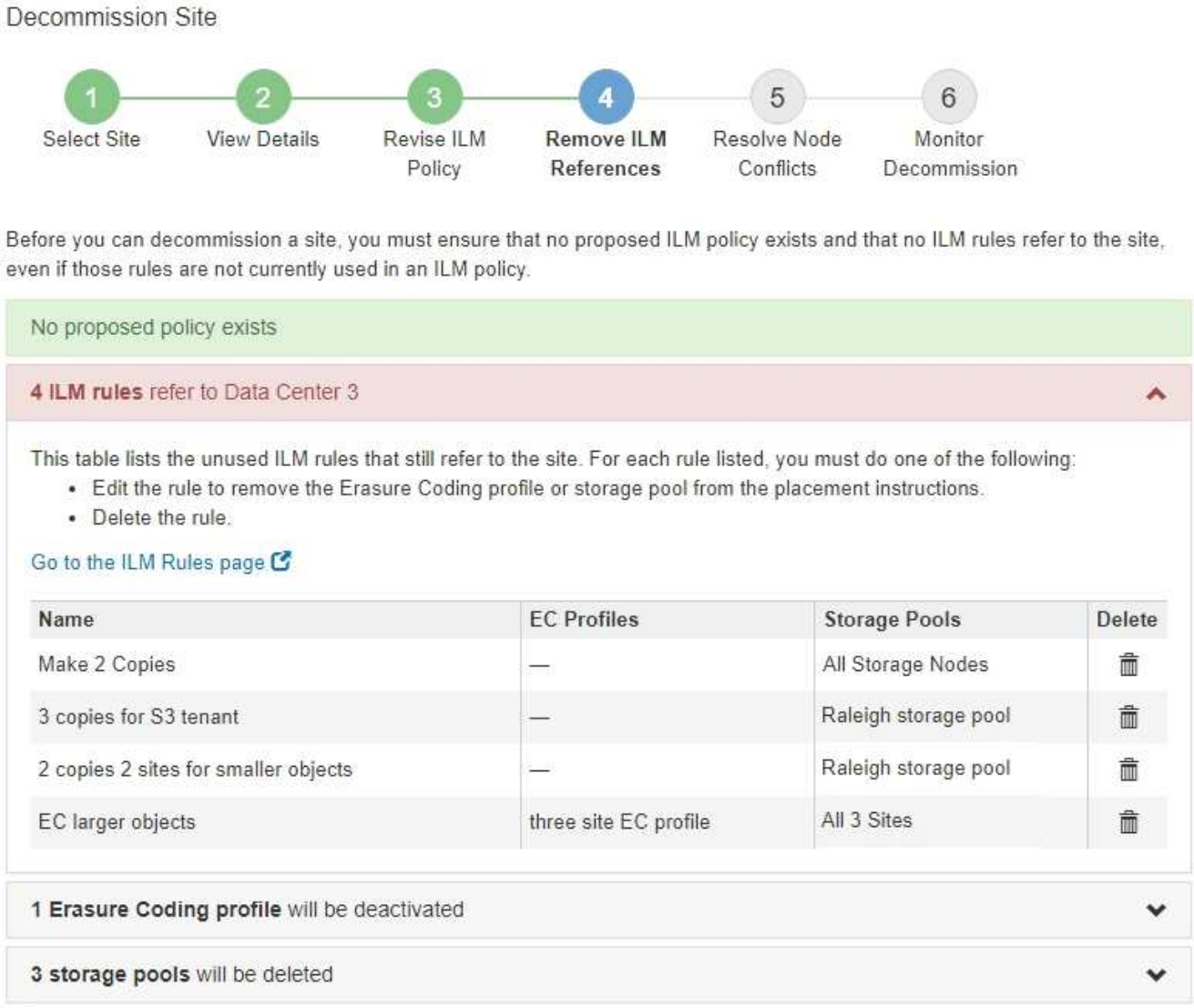
1. 如果列出了建议的策略，请将其删除。



a. 选择 * 删除建议的策略 * 。

b. 在确认对话框中选择 * 确定 * 。

2. 确定任何未使用的 ILM 规则是否引用站点。



列出的任何 ILM 规则仍引用站点，但不会在任何策略中使用。在示例中：

- 常用 * 创建 2 个副本 * 规则使用系统默认的 * 所有存储节点 * 存储池，该存储池使用所有站点站点站点。
- S3 租户 * 未使用的 * 3 个副本规则是指 * 罗利 * 存储池。
- 对于较小对象 * ，未使用的 * 2 个副本 2 个站点是指 * 罗利 * 存储池。
- 未使用的 * 较大对象 * 规则使用 * 所有 3 个站点 * 纠删编码配置文件中的罗利站点。
- 如果未列出 ILM 规则，请选择 * 下一步 * 以转到 * 步骤 5 （解决节点冲突） * 。

  第 5 步：解决节点冲突（并开始停用）

  > 当 StorageGRID 停用站点时，它将自动停用引用该站点的任何未使用的擦除编码配置文件，并自动删除引用该站点的任何未使用的存储池。系统默认的所有存储节点存储池将被删除，因为它使用的是所有站点站点站点。

- 如果列出了一个或多个 ILM 规则，请转至下一步。

3. 编辑或删除每个未使用的规则：

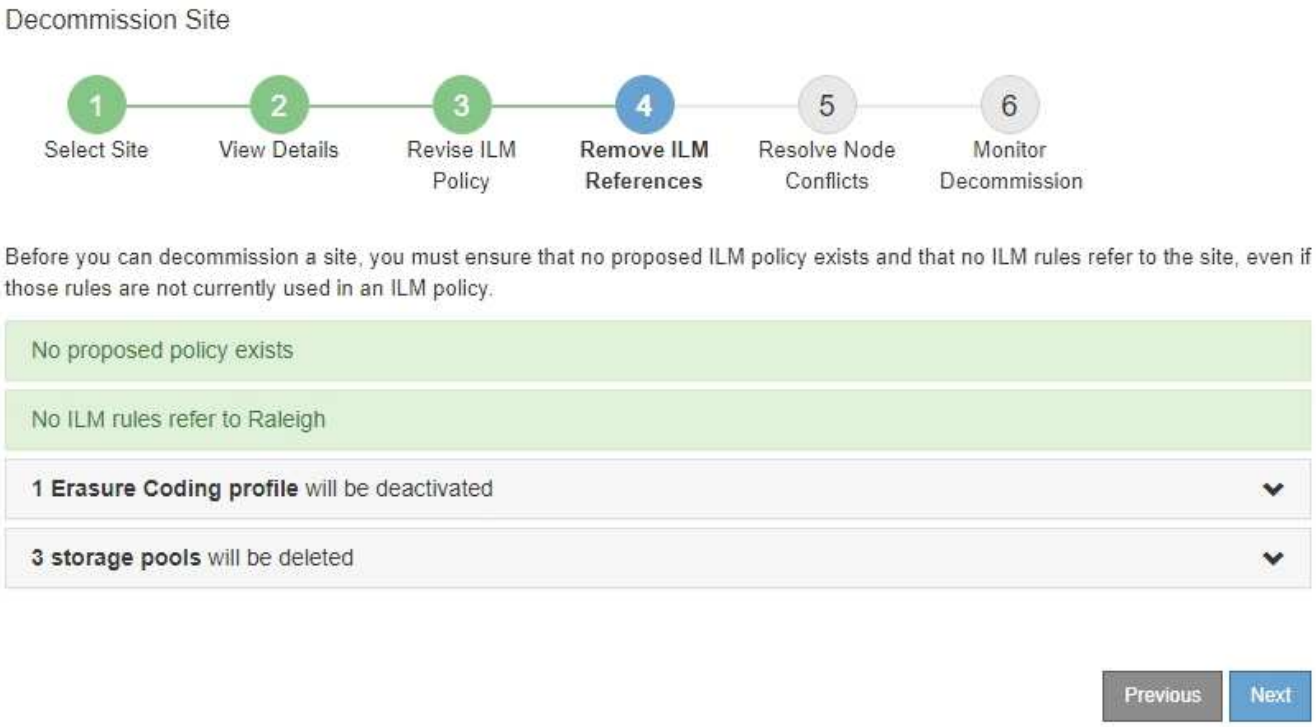
- 要编辑规则，请转到 "ILM 规则 " 页面，并更新使用擦除编码配置文件或引用站点的存储池的所有放置位置。然后，返回到 * 步骤 4 （删除 ILM 参考） * 。

  有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

- 要删除规则，请选择垃圾桶图标 并选择 * 确定 * 。

  您必须先删除常用的 * 创建 2 个副本 * 规则，然后才能停用站点。

4. 确认不存在建议的 ILM 策略，未使用的 ILM 规则均未引用此站点，并且已启用 * 下一步 * 按钮。



5. 选择 * 下一步 * 。

   删除此站点后，引用此站点的任何剩余存储池和擦除编码配置文件将无效。当 StorageGRID 停用站点时，它将自动停用引用该站点的任何未使用的擦除编码配置文件，并自动删除引用该站点的任何未使用的存储池。系统默认的所有存储节点存储池将被删除，因为它使用的是所有站点站点站点。

此时将显示第 5 步（解决节点冲突）。

第 **5** 步：解决节点冲突（并开始停用）

从 " 弃用站点 " 向导的第 5 步（解决节点冲突）中，您可以确定 StorageGRID 系统中的任何节点是否已断开连接，或者选定站点中的任何节点是否属于高可用性（ HA ）组。解决任何节点冲突后，您可以从此页面启动停用操作步骤 。

您必须确保 StorageGRID 系统中的所有节点均处于正确状态，如下所示：

- StorageGRID 系统中的所有节点都必须已连接（）。

> 如果要执行已断开连接的站点停用，则必须断开要删除站点上的所有节点，并且必须连接所有其他站点上的所有节点。

- 要删除的站点上的任何节点都不能具有属于高可用性（ HA ）组的接口。

如果步骤 5 （解决节点冲突）中列出了任何节点，则必须更正问题描述 ，然后才能开始停用。

在此页面中启动站点停用操作步骤 之前，请查看以下注意事项：

- 您必须留出足够的时间来完成停用操作步骤 。

> 从站点移动或删除对象数据可能需要数天，数周甚至数月的时间，具体取决于站点上的数据量，系统上的负载，网络延迟以及所需 ILM 更改的性质。

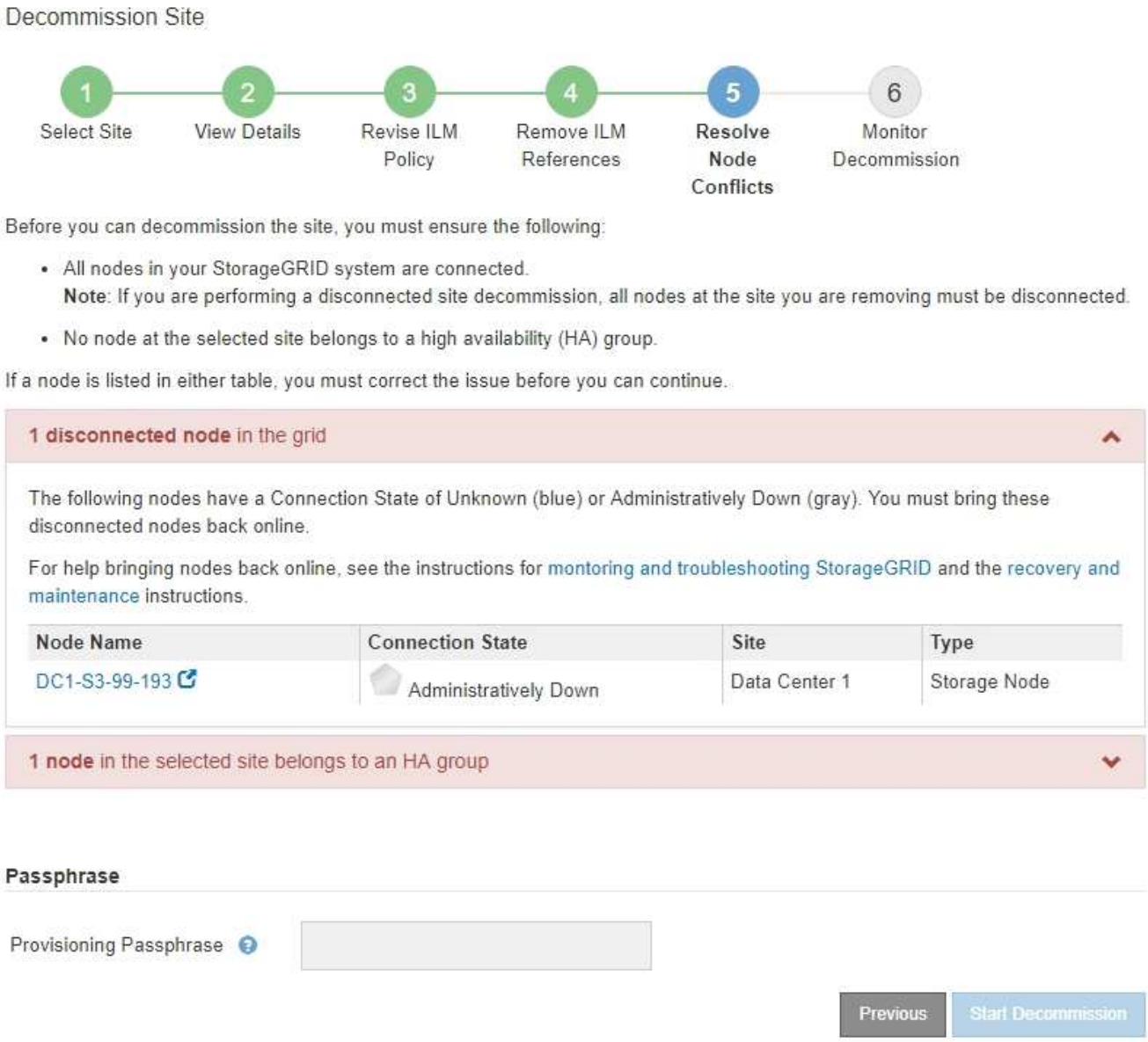
- 站点停用操作步骤 运行时：
  - 您不能创建引用要停用的站点的 ILM 规则。您也不能编辑现有 ILM 规则来引用站点。
  - 您不能执行其他维护过程，例如扩展或升级。

> 如果在已连接站点停用期间需要执行另一个维护操作步骤 ，则可以在删除存储节点时暂停操作步骤 。在 " D复制和擦除编码数据 " 阶段， * 暂停 * 按钮将启用。

  - 如果您需要在启动站点停用操作步骤 后恢复任何节点，必须联系支持部门。

步骤

1. 查看步骤 5 （解决节点冲突）中的已断开节点部分，确定 StorageGRID 系统中的任何节点的连接状态是否为未知（）或管理员关闭（）。

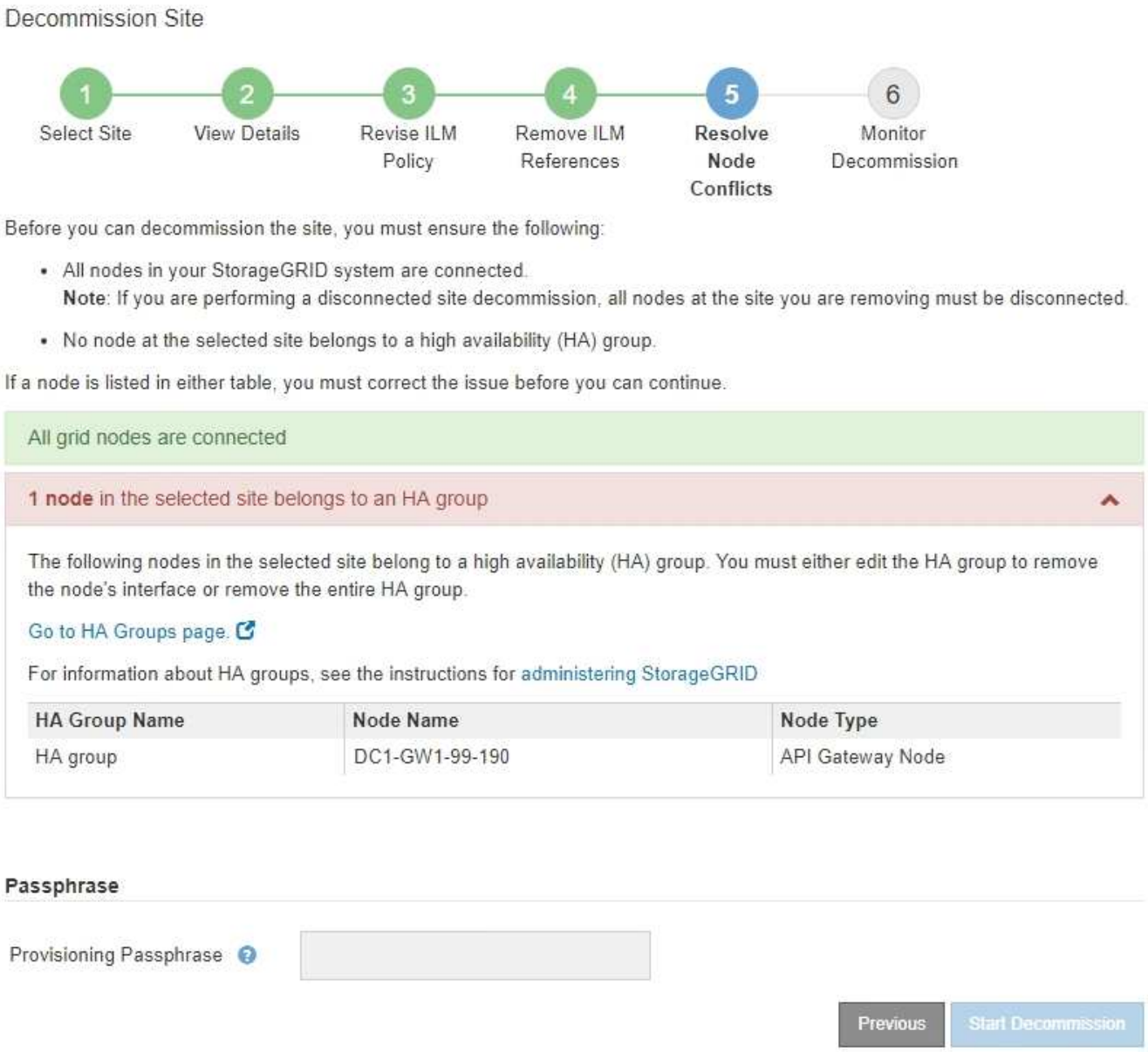


2. 如果任何节点已断开连接，请将其恢复联机。

   请参见有关监控 StorageGRID 和网格节点过程并对其进行故障排除的说明。如需帮助，请联系技术支持。

3. 当所有已断开连接的节点恢复联机后，请查看步骤 5 （解决节点冲突）中的 HA 组部分。

   此表列出了选定站点中属于高可用性（ HA ）组的任何节点。



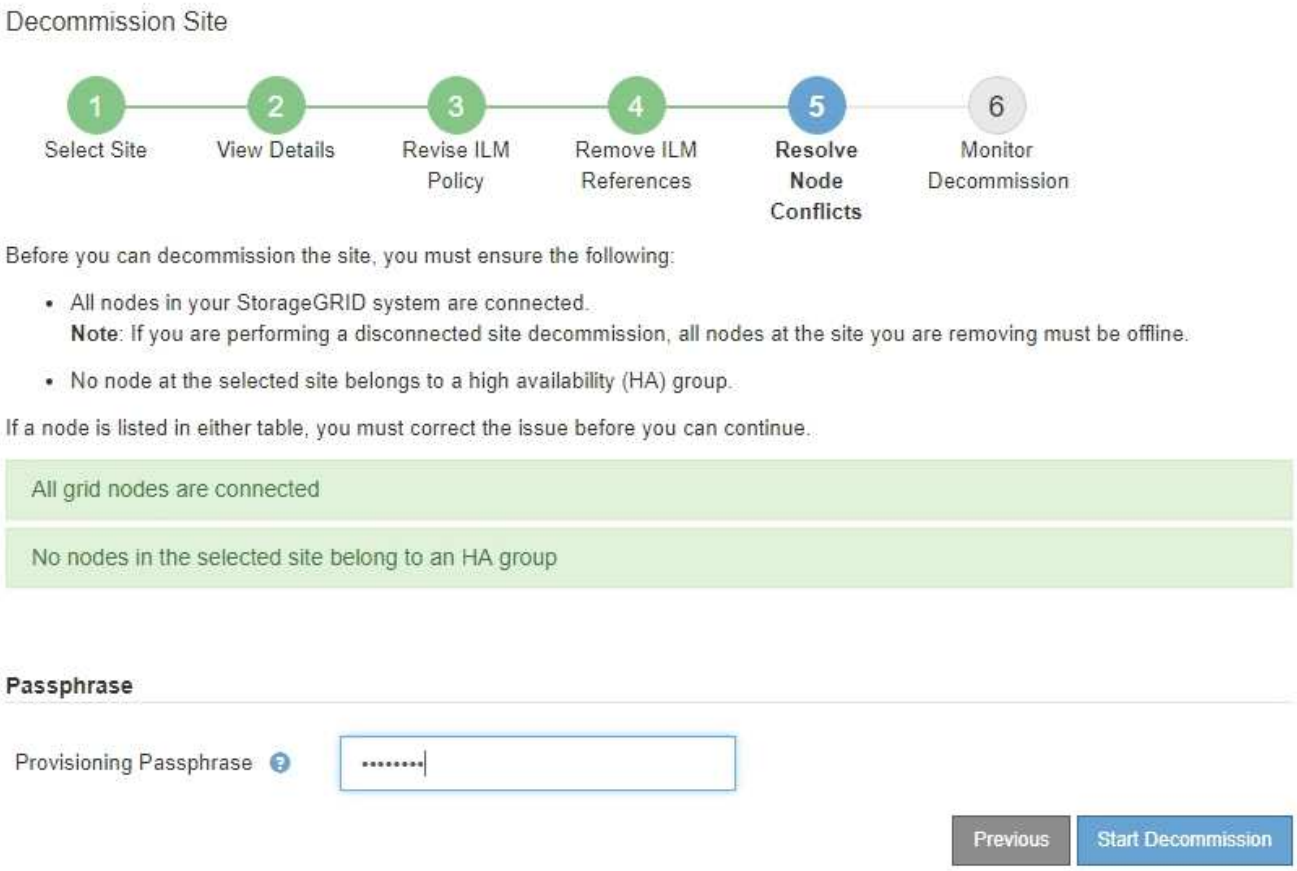
4. 如果列出了任何节点，请执行以下操作之一：

   - 编辑每个受影响的 HA 组以删除节点接口。
   - 从此站点中删除仅包含节点的 HA 组。请参见有关管理 StorageGRID 的说明。

   如果连接了所有节点，并且在 HA 组中未使用选定站点中的任何节点，则会启用 * 配置密码短语 * 字段。

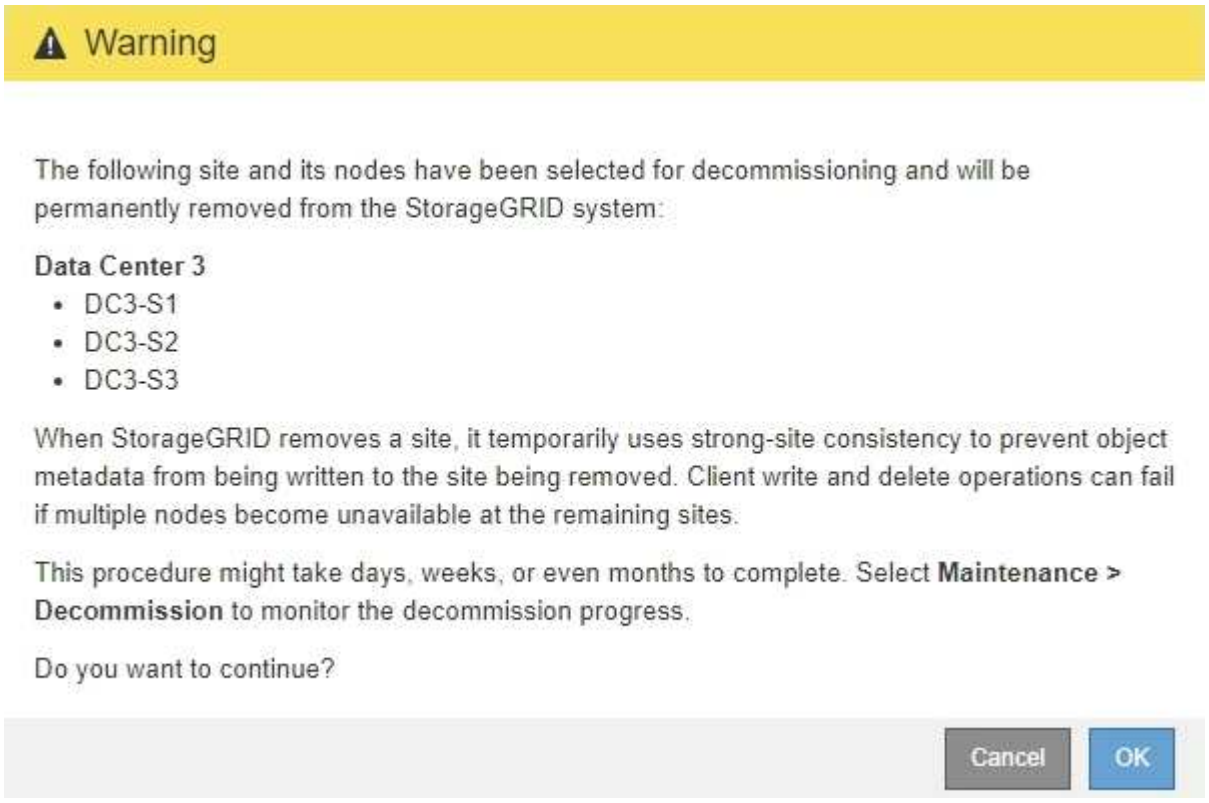
5. 输入配置密码短语。

   此时， * 开始取消配置 * 按钮将变为启用状态。



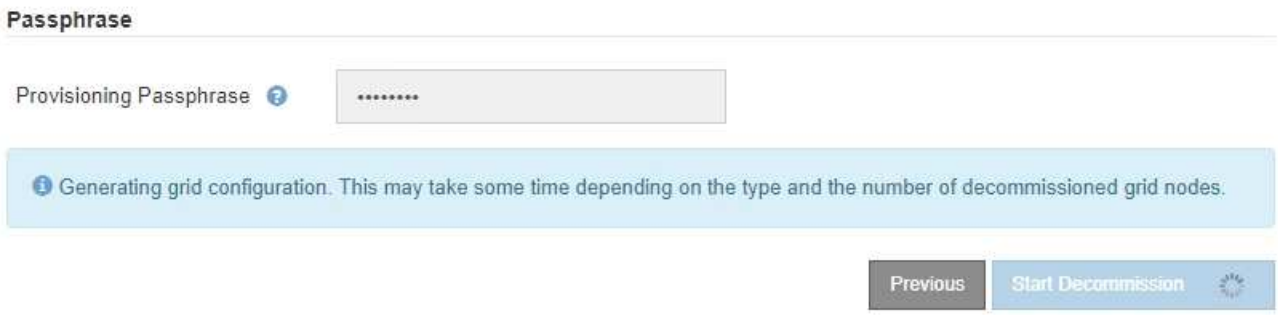
6. 如果您已准备好启动站点停用操作步骤，请选择 * 启动停用 * 。

警告将列出要删除的站点和节点。系统会提醒您，完全删除此站点可能需要数天，数周甚至数月的时间。



7. 查看警告。如果您已准备好开始，请选择 * 确定 * 。

   生成新网格配置时，将显示一条消息。此过程可能需要一些时间，具体取决于停用的网格节点的类型和数量。



   生成新网格配置后，将显示步骤 6 （监控取消配置）。

   在停用完成之前， * 上一步 * 按钮将保持禁用状态。

相关信息

监控和故障排除

网格节点过程

管理 StorageGRID

第 6 步：监控取消配置

从 " 取消配置站点 " 页面向导的第 6 步（监控取消配置）中，您可以在删除站点时监控进度。

关于此任务

当 StorageGRID 删除已连接站点时，它将按以下顺序删除节点：

1. 网关节点
2. 管理节点
3. 存储节点

当 StorageGRID 删除已断开连接的站点时，它会按以下顺序删除节点：

1. 网关节点
2. 存储节点
3. 管理节点

每个网关节点或管理节点可能只需要几分钟或一小时即可删除；但是，存储节点可能需要数天或数周的时间。

步骤

1. 生成新的恢复软件包后，立即下载该文件。



请尽快下载恢复包，以确保在停用操作步骤 期间出现问题时可以恢复网格。

a. 选择消息中的链接，或选择 * 维护 * > * 系统 * > * 恢复软件包 * 。

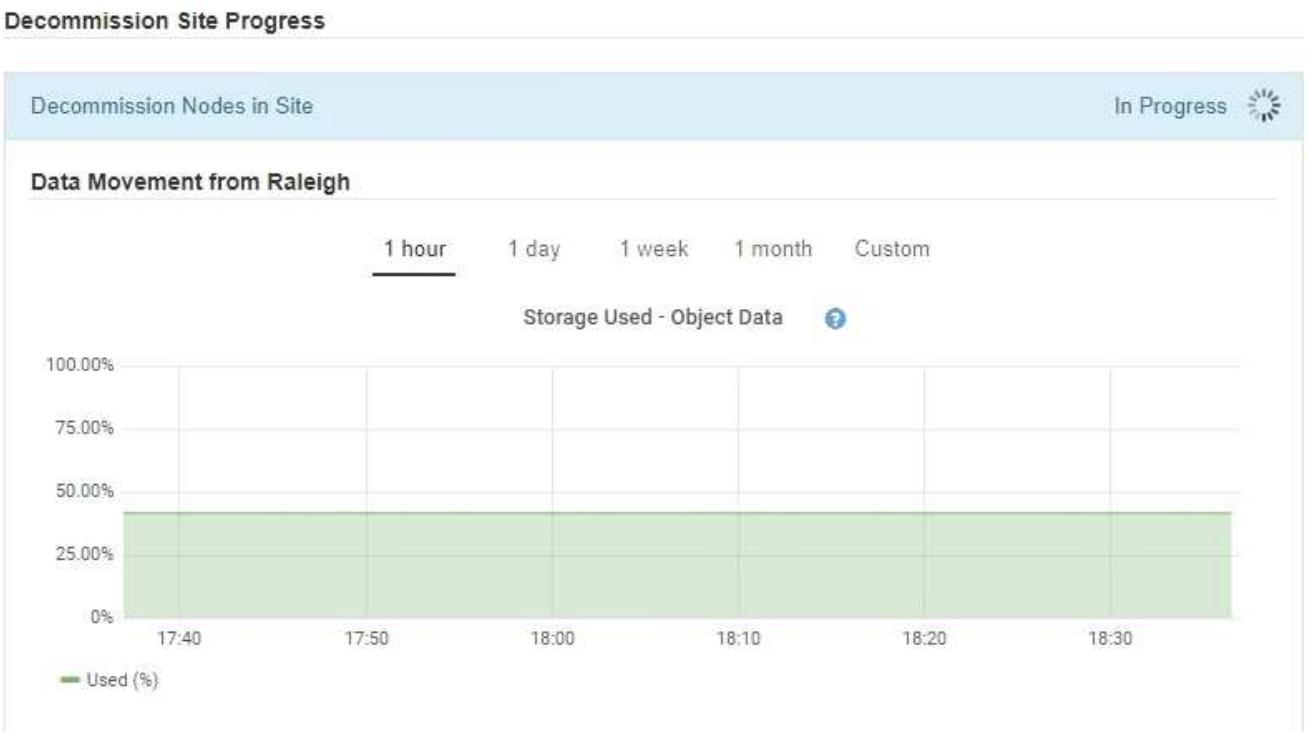
b. 下载 ` .zip` 文件。

请参见的说明 正在下载恢复包。

恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

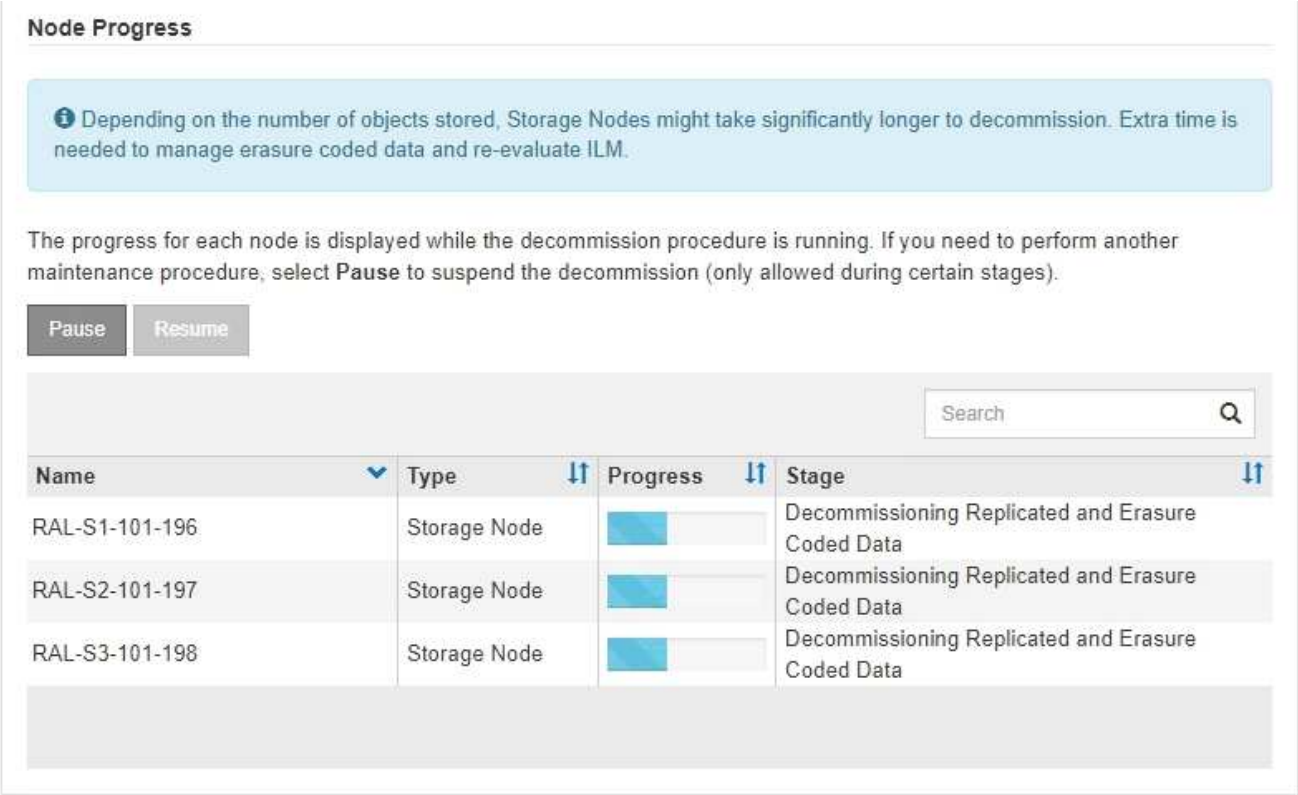
2. 使用 " 数据移动 " 图表监控对象数据从该站点到其他站点的移动情况。

在步骤 3 （修订 ILM 策略）中激活新的 ILM 策略后，数据移动开始。数据移动将在整个停用操作步骤 中进行。



3. 在页面的节点进度部分中，在删除节点时监控停用操作步骤 的进度。

删除存储节点后，每个节点将经历一系列阶段。尽管其中大多数阶段发生得很快甚至不可能发生，但根据需要移动的数据量，您可能需要等待几天甚至几周才能完成其他阶段。需要更多时间来管理经过纠删编码的数据并重新评估 ILM 。



如果您正在监控已连接站点停用的进度，请参阅此表以了解存储节点的停用阶段：

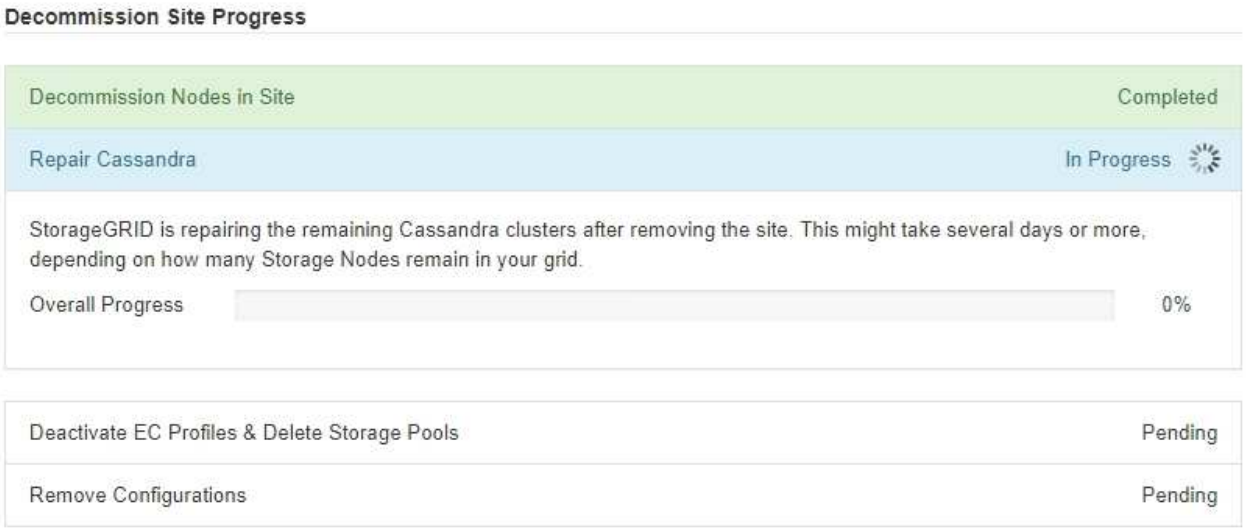
阶段	估计持续时间
待定	分钟或更短
等待锁定	minutes
准备任务	分钟或更短
将 LDR 标记为已停用	minutes
停用复制的数据和擦除编码的数据	小时，天或周，具体取决于数据量 • 注意 *： 如果您需要执行其他维护活动，可以在此阶段暂停站点停用。
LDR 设置状态	minutes
刷新审核队列	分钟到小时，具体取决于消息数量和网络延迟。

阶段	估计持续时间
完成	minutes

如果您要监控已断开连接的站点停用的进度，请参见下表以了解存储节点的停用阶段：

阶段	估计持续时间
待定	分钟或更短
等待锁定	minutes
准备任务	分钟或更短
禁用外部服务	minutes
证书撤消	minutes
节点取消注册	minutes
存储级别取消注册	minutes
删除存储组	minutes
实体删除	minutes
完成	minutes

4. 在所有节点均已达到完成阶段后，请等待其余站点停用操作完成。
   - 在 * 修复 Cassandra* 步骤中， StorageGRID 会对网格中保留的 Cassandra 集群进行任何必要的修复。这些修复可能需要几天或更长时间，具体取决于网格中剩余的存储节点数。



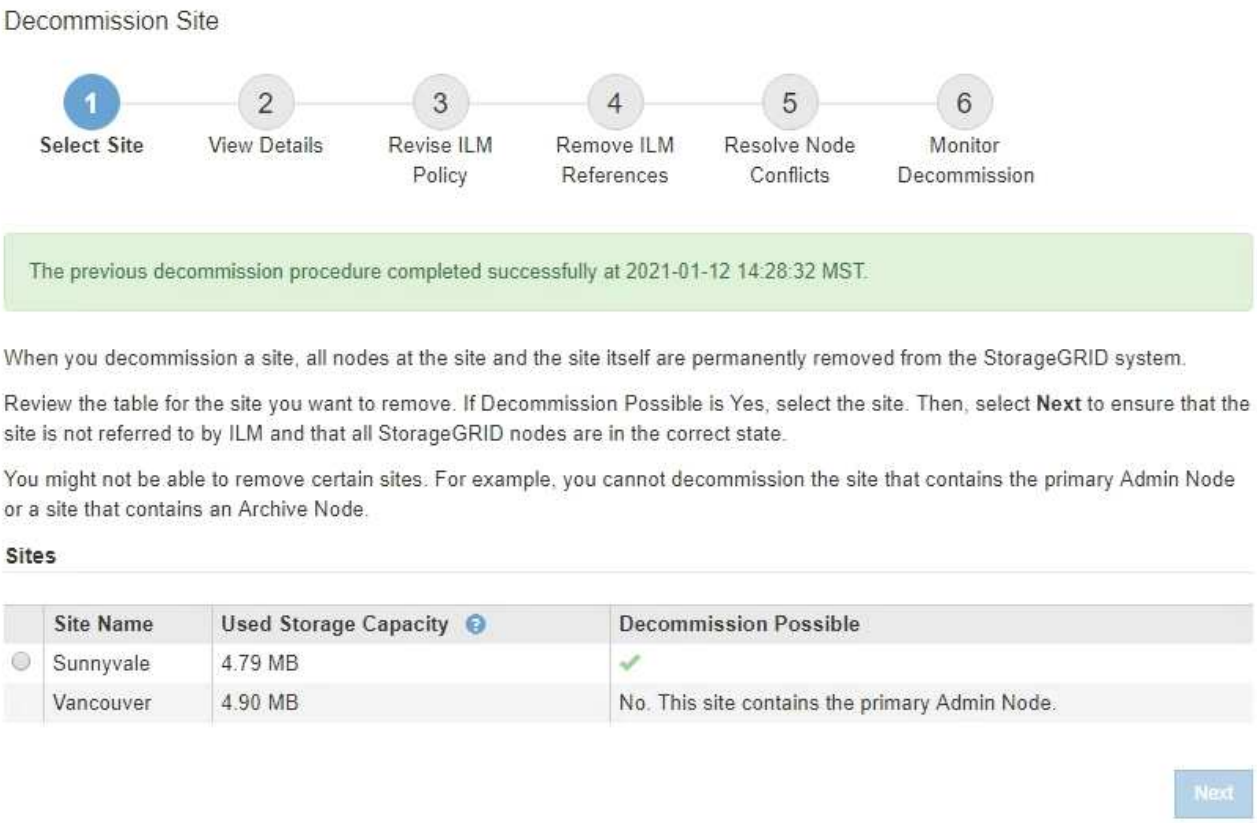
- 在 * 停用 EC 配置文件并删除存储池 * 步骤中，将进行以下 ILM 更改：
  - 引用此站点的任何擦除编码配置文件均会被停用。
  - 系统将删除引用此站点的任何存储池。

  系统默认的所有存储节点存储池也会被删除，因为它使用的是所有站点站点站点。

- 最后，在 * 删除配置 * 步骤中，对站点及其节点的任何剩余引用都将从网格的其余部分中删除。



5. 停用操作步骤 完成后， " 停用站点 " 页面将显示一条成功消息，并且不再显示已删除的站点。



完成后

完成站点停用操作步骤 后，完成以下任务：

- 确保已擦除已停用站点中所有存储节点的驱动器。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果此站点包含一个或多个管理节点，并且已为您的 StorageGRID 系统启用单点登录（ SSO ），请从 Active Directory 联合身份验证服务（ AD FS ）中删除此站点的所有依赖方信任。
- 在已连接站点停用操作步骤 期间正常关闭节点后，请删除关联的虚拟机。

网络维护过程

更新网格网络的子网

StorageGRID 会维护一个网络子网列表，用于在网格网络（ eth0 ）上的网格节点之间进行通信。这些条目包括 StorageGRID 系统中每个站点用于网格网络的子网，以及通过网格网络网关访问的 NTP ， DNS ， LDAP 或其他外部服务器所使用的任何子网。在扩展中添加网格节点或新站点时，您可能需要更新子网或向网格网络添加子网。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。

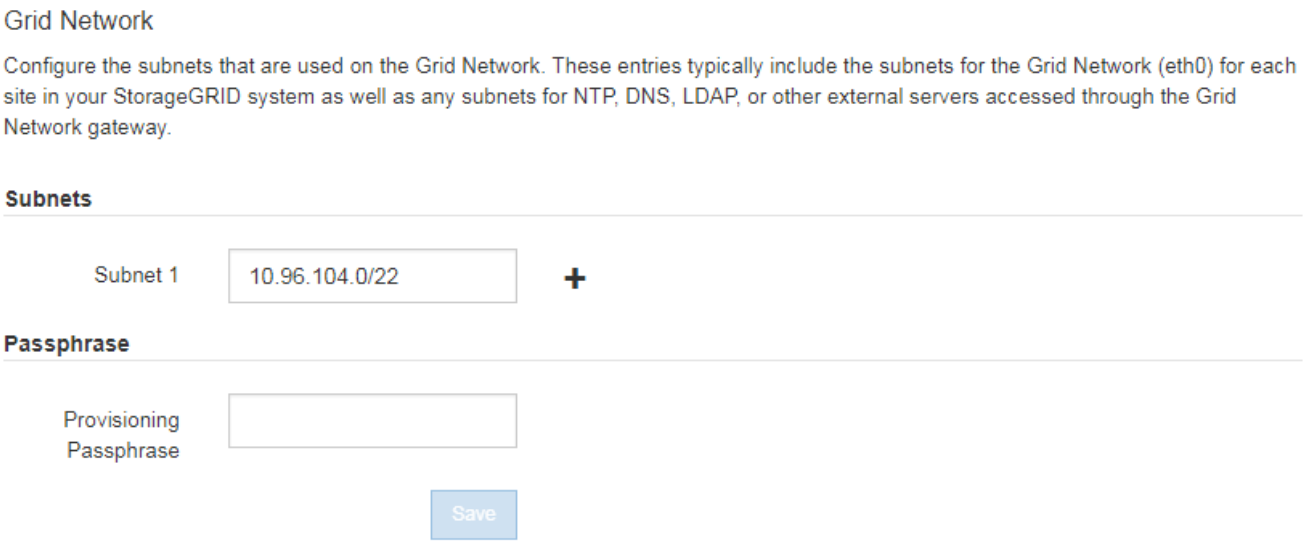
- 您必须具有要配置的子网的网络地址，以 CIDR 表示法表示。

关于此任务

如果要执行的扩展活动包括添加新子网，则必须先添加新的网格子网，然后再启动扩展操作步骤 。

步骤

1. 选择 * 维护 * > * 网络 * > * 网格网络 * 。



2. 在子网列表中，单击加号以 CIDR 表示法添加新子网。

   例如，输入 `10.96.104.0/22` 。

3. 输入配置密码短语，然后单击 * 保存 * 。

   您指定的子网将自动为 StorageGRID 系统配置。

4. 从网格管理器下载新的恢复软件包。
   a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
   b. 输入配置密码短语。

配置 **IP** 地址

您可以使用更改 IP 工具为网格节点配置 IP 地址来执行网络配置。

您必须使用更改 IP 工具对网格部署期间最初设置的网络配置进行大部分更改。使用标准 Linux 网络命令和文件进行的手动更改可能不会传播到所有 StorageGRID 服务，并且可能不会在升级，重新启动或节点恢复过程中持续存在。

如果要更改网格中所有节点的网格网络 IP 地址，请使用 适用于网格范围更改的特殊操作步骤。

如果仅更改网格网络子网列表，请使用网格管理器添加或更改网络配置。否则，如果网格管理器因网络配置问题描述 而无法访问，或者您同时执行网格网络路由更改和其他网络更改，请使用更改 IP 工具。

IP 更改操作步骤 可以是中断操作步骤 。在应用新配置之前，网格的某些部分可能不可用。

- 以太网接口 *

分配给 eth0 的 IP 地址始终是网格节点的网格网络 IP 地址。分配给 eth1 的 IP 地址始终是网格节点的管理网络 IP 地址。分配给 eth2 的 IP 地址始终是网格节点的客户端网络 IP 地址。

请注意，在某些平台上，例如 StorageGRID 设备， eth0 ， eth1 和 eth2 可能是由物理或 VLAN 接口的从属网桥或绑定组成的聚合接口。在这些平台上， * SSM* > * 资源 * 选项卡可能会显示除 eth0 ， eth1 或 eth2 之外分配给其他接口的网格，管理员和客户端网络 IP 地址。

- DHCP *

您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。如果要更改网格节点的 IP 地址，子网掩码和默认网关，则必须使用 IP 地址更改过程。使用更改 IP 工具将使发生原因 DHCP 地址变为静态地址。

- 高可用性（ HA ）组 *
- 如果客户端网络接口包含在 HA 组中，则不能将该接口的客户端网络 IP 地址更改为为 HA 组配置的子网之外的地址。
- 您不能将客户端网络 IP 地址更改为分配给客户端网络接口上配置的 HA 组的现有虚拟 IP 地址的值。
- 如果网格网络接口包含在 HA 组中，则不能将该接口的网格网络 IP 地址更改为为 HA 组配置的子网之外的地址。
- 您不能将网格网络 IP 地址更改为分配给在网格网络接口上配置的 HA 组的现有虚拟 IP 地址的值。

更改节点网络配置

您可以使用更改 IP 工具更改一个或多个节点的网络配置。您可以更改网格网络的配置，或者添加，更改或删除管理员网络或客户端网络。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

- Linux： * 如果您是首次将网格节点添加到管理网络或客户端网络，并且先前未在节点配置文件中配置 admin_network_target 或 client_network_target ，则必须立即执行此操作。

请参见适用于您的 Linux 操作系统的 StorageGRID 安装说明。

- 设备： * 在 StorageGRID 设备上，如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络，则无法仅使用更改 IP 工具添加网络。首先，您必须 将设备置于维护模式，配置链路，将设备恢复为正常运行模式，然后使用更改 IP 工具修改网络配置。有关如何配置网络链路的信息，请参见适用于您的设备的安装和维护说明中的操作步骤 。

您可以更改任何网络上一个或多个节点的 IP 地址，子网掩码，网关或 MTU 值。

您还可以从客户端网络或管理网络添加或删除节点：

- 您可以通过向客户端网络或管理网络添加节点上的 IP 地址 / 子网掩码来将该节点添加到该节点。
- 您可以通过删除客户端网络或管理网络中某个节点的 IP 地址 / 子网掩码来从该网络中删除该节点。

  无法从网格网络中删除节点。

> 不允许使用 IP 地址交换。如果必须在网格节点之间交换 IP 地址，则必须使用临时中间 IP 地址。

> 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且您要更改管理节点的 IP 地址，请注意，使用管理节点的 IP 地址（而不是建议的完全限定域名）配置的任何依赖方信任都将无效。您将无法再登录到此节点。更改 IP 地址后，您必须立即使用新的 IP 地址更新或重新配置 Active Directory 联合身份验证服务（ AD FS ）中节点的依赖方信任。请参见有关管理 StorageGRID 的说明。

> 使用更改 IP 工具对网络所做的任何更改都会传播到 StorageGRID 设备的安装程序固件。这样，如果在设备上重新安装 StorageGRID 软件，或者将设备置于维护模式，则网络配置将正确无误。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 输入以下命令以启动更改 IP 工具： `change-ip`
3. 在提示符处输入配置密码短语。

   此时将显示主菜单。

```
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. 也可以选择 * 1 * 来选择要更新的节点。然后选择以下选项之一：

- * 1 *： 单节点—按名称选择
- * 2 *： 单节点—按站点选择，然后按名称选择
- **3**： 单节点—按当前 IP 选择
- **4**： 站点上的所有节点
- **5**： 网格中的所有节点
  - 注： * 如果要更新所有节点，请允许 " 全部 " 保持选中状态。

选择后，将显示主菜单，并更新 * 选定节点 * 字段以反映您的选择。所有后续操作仅在显示的节点上执行。

5. 在主菜单上，选择选项 * 2 * 以编辑选定节点的 IP/ 掩码，网关和 MTU 信息。
   a. 选择要更改的网络：
      - * 1 *： 网格网络
      - * 2 *： 管理网络
      - * 3 *： 客户端网络
      - **4**： 选择所有网络后，提示符将显示节点名称，网络名称（网格，管理员或客户端），数据类型（ IP/ 掩码， 网关或 MTU ）和当前值。

        编辑 DHCP 配置接口的 IP 地址，前缀长度，网关或 MTU 将使接口更改为静态。如果选择更改由 DHCP 配置的接口，则会显示一条警告，通知您该接口将更改为静态。

      无法编辑配置为 `FIXED` 的接口。

   b. 要设置新值，请按当前值所示格式输入该值。
   c. 要保持当前值不变，请按 * 输入 * 。
   d. 如果数据类型为 `IP/ 掩码` ，则可以输入 * d* 或 * 。 0.0.0.0/0* 从节点中删除管理员网络或客户端网络。
   e. 编辑要更改的所有节点后，输入 * 。 q* 返回主菜单。

      您所做的更改将一直保留，直到清除或应用为止。

6. 选择以下选项之一，查看您所做的更改：
   - * 5* ： 显示输出中的编辑内容，这些编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如示例输出所示：

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

- * 6 *： 显示输出中显示的编辑内容，其中显示了完整配置。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。正确显示取决于您的终端客户端是否支持必要的 VT100 转义序列。

7. 选择选项 * 7* 以验证所有更改。

   此验证可确保不会违反网格，管理和客户端网络的规则，例如不使用重叠的子网。

   在此示例中，验证返回错误。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   在此示例中，验证已通过。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. 验证通过后，请选择以下选项之一：

- **8**：保存未应用的更改。

  使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

- * 。 10*：应用新网络配置。

9. 如果选择了选项 * 。 10* ，请选择以下选项之一：

   - * 应用 *：立即应用更改，并在必要时自动重新启动每个节点。

     如果新网络配置不需要更改任何物理网络连接，您可以选择 * 应用 * 以立即应用更改。如果需要，节点将自动重新启动。此时将显示需要重新启动的节点。

   - * 阶段 *：下次手动重新启动节点时应用更改。

     如果要使新网络配置正常运行，需要更改物理或虚拟网络配置，则必须使用 * 阶段 * 选项，关闭受影响的节点，进行必要的物理网络更改并重新启动受影响的节点。如果选择 * 应用 * 而未先进行这些网络更改，则更改通常会失败。

     如果使用 * 阶段 * 选项，则必须在暂存后尽快重新启动节点，以最大程度地减少中断。

   - * 取消 *：此时不要更改任何网络。

     如果您不知道建议的更改需要重新启动节点，则可以推迟更改以最大限度地减少对用户的影响。选择 * 取消 * 将返回到主菜单并保留所做的更改，以便稍后应用。

     如果选择 * 应用 * 或 * 阶段 * ，则会生成一个新的网络配置文件，并执行配置，同时会使用新的工作信息更新节点。

     在配置期间，输出将在应用更新时显示状态。

     ```
     Generating new grid networking description file...

     Running provisioning...

     Updating grid network configuration on Name
     ```

   应用或暂存更改后，由于网格配置更改，系统将生成新的恢复软件包。

10. 如果选择了 * 阶段 * ，请在配置完成后按照以下步骤进行操作：

    a. 根据需要进行物理或虚拟网络更改。

       - 物理网络更改 *：进行必要的物理网络更改，必要时安全关闭节点。
       - Linux *：如果您是首次将节点添加到管理网络或客户端网络，请确保已按照 "`将接口添加到现有节点 " 中所述添加接口。`

    b. 重新启动受影响的节点。

11. 完成更改后，选择 * 。 0* 退出更改 IP 工具。

12. 从网格管理器下载新的恢复软件包。

a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
b. 输入配置密码短语。

相关信息

Linux ：向现有节点添加接口

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

管理 StorageGRID

配置 IP 地址

在管理网络上添加或更改子网列表

您可以在管理网络子网列表中添加，删除或更改一个或多个节点的子网。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

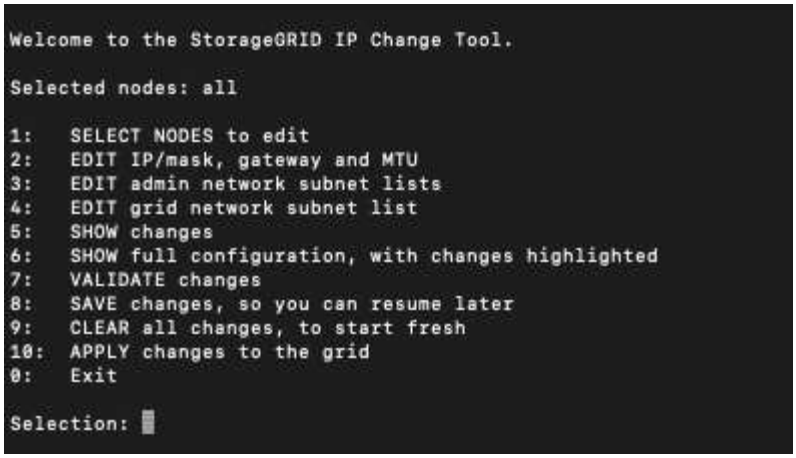
您可以为管理网络子网列表中的所有节点添加，删除或更改子网。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root ： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 输入以下命令以启动更改 IP 工具： `change-ip`
3. 在提示符处输入配置密码短语。

   此时将显示主菜单。



4. 或者，也可以限制执行操作的网络 / 节点。选择以下选项之一：
   - 如果要筛选要执行操作的特定节点，请选择 * 1 * 以选择要编辑的节点。选择以下选项之一：
     - * 1 * ：单个节点（按名称选择）
     - * 2 * ：单个节点（按站点选择，然后按名称选择）
     - * 3 * ：单个节点（由当前 IP 选择）
     - **4** ：站点上的所有节点
     - **5** ：网格中的所有节点
     - **0** ：返回
   - 允许 "`所有` " 保持选中状态。进行选择后，将显示主菜单屏幕。选定节点字段反映了您的新选择，现在，选定的所有操作将仅对此项执行。
5. 在主菜单上，选择用于编辑管理网络子网的选项（选项 * 3 * ）。
6. 选择以下选项之一：
   - 输入以下命令添加子网： `add CIDR`
   - 输入以下命令删除子网： `del CIDR`
   - 输入以下命令设置子网列表： `set CIDR`

   对于所有命令，您可以使用以下格式输入多个地址： `add CIDR , CIDR`

   示例： `add 172.14.0.0/16 , 172.15.0.0/16 , 172.16.0.0/16`

   您可以使用 "`向上箭头` " 将先前键入的值调用到当前输入提示符，然后根据需要对其进行编辑，从而减少所需的键入量。

   以下示例输入显示了如何向管理网络子网列表添加子网：

```
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. 准备好后，输入 * 。 q* 可返回主菜单屏幕。您所做的更改将一直保留，直到清除或应用为止。

> 如果您在步骤 2 中选择了任何 " 全部 " 节点选择模式，则必须按 * 输入 * （不带 * q* ）才能访问列表中的下一个节点。

8. 选择以下选项之一：

   - 选择选项 * 5* 可显示输出中的编辑内容，而输出中的编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如以下示例输出所示：

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - 选择选项 **6** 可在显示完整配置的输出中显示编辑内容。更改将以绿色（添加项）或红色（删除项）突出显示。* 注： * 某些终端模拟器可能会使用删除线格式显示添加和删除内容。

     尝试更改子网列表时，将显示以下消息：

```
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.
```

如果您未明确将 NTP 和 DNS 服务器子网分配给网络，则 StorageGRID 会自动为此连接创建一个主机路由（ /32 ）。例如，如果您希望使用 /16 或 /24 路由与 DNS 或 NTP 服务器建立出站连接，则应删除自动创建的 /32 路由并添加所需的路由。如果不删除自动创建的主机路由，则在对子网列表进行任何更改后，此路由将保留。

> 虽然您可以使用这些自动发现的主机路由，但通常应手动配置 DNS 和 NTP 路由以确保连接。

9. 选择选项 * 7* 以验证所有暂存更改。

   此验证可确保遵循网格网络，管理网络和客户端网络的规则，例如使用重叠的子网。

10. （可选）选择选项 * 8* 保存所有分阶段更改，稍后返回以继续进行更改。

    使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

11. 执行以下操作之一：
    - 如果要在不保存或应用新网络配置的情况下清除所有更改，请选择选项 * 。
    - 如果您已准备好应用更改并配置新的网络配置，请选择选项 * 。在配置期间，输出将在应用更新时显示状态，如以下示例输出所示：

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. 从网格管理器下载新的恢复软件包。
    a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
    b. 输入配置密码短语。

相关信息

配置 IP 地址

您可以使用更改 IP 工具在网格网络上添加或更改子网。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

您可以在网格网络子网列表中添加，删除或更改子网。更改将影响网格中所有节点上的路由。

> 如果仅更改网格网络子网列表，请使用网格管理器添加或更改网络配置。否则，如果网格管理器因网络配置问题描述 而无法访问，或者您同时执行网格网络路由更改和其他网络更改，请使用更改 IP 工具。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 输入以下命令以启动更改 IP 工具： `change-ip`
3. 在提示符处输入配置密码短语。

   此时将显示主菜单。

```
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. 在主菜单上，选择用于编辑网格网络子网的选项（选项 * 4* ）。

   > 对网格网络子网列表所做的更改在网格范围内进行。

5. 选择以下选项之一：
   - 输入以下命令添加子网： `add CIDR`

- 输入以下命令删除子网： `del CIDR`
- 输入以下命令设置子网列表： `set CIDR`

> 对于所有命令，您可以使用以下格式输入多个地址： `add CIDR ， CIDR`

示例： `add 172.14.0.0/16 ， 172.15.0.0/16 ， 172.16.0.0/16`

> 您可以使用 "`向上箭头` " 将先前键入的值调用到当前输入提示符，然后根据需要对其进行编辑，从而减少所需的键入量。

以下示例输入显示了为网格网络子网列表设置子网：

```
Editing: Grid Network Subnet List

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

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. 准备好后，输入 * 。 q* 可返回主菜单屏幕。您所做的更改将一直保留，直到清除或应用为止。
7. 选择以下选项之一：
   - 选择选项 * 5* 可显示输出中的编辑内容，而输出中的编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如以下示例输出所示：

```
================================================================================
Grid Network Subnet List (GNSL)
================================================================================
                                                    add 172.30.0.0/21
                                                    add 172.31.0.0/21
                                                    del 172.16.0.0/21
                                                    del 172.17.0.0/21
                                                    del 172.18.0.0/21
                              [      172.30.0.0/21 ]
                              [      172.31.0.0/21 ]
                              [    192.168.0.0/21 ]
Press Enter to continue
```

   - 选择选项 **6** 可在显示完整配置的输出中显示编辑内容。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。

8. 选择选项 * 7* 以验证所有暂存更改。

   此验证可确保遵循网格网络，管理网络和客户端网络的规则，例如使用重叠的子网。

9. （可选）选择选项 * 8* 保存所有分阶段更改，稍后返回以继续进行更改。

   使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

10. 执行以下操作之一：

    - 如果要在不保存或应用新网络配置的情况下清除所有更改，请选择选项 * 。
    - 如果您已准备好应用更改并配置新的网络配置，请选择选项 * 。在配置期间，输出将在应用更新时显示状态，如以下示例输出所示：

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

11. 如果在更改网格网络时选择了选项 * 。 10 ，请选择以下选项之一：

    - * 应用 * ： 立即应用更改，并在必要时自动重新启动每个节点。

      如果新网络配置将与旧网络配置同时运行而不进行任何外部更改，则可以使用 * 应用 * 选项进行完全自动化的配置更改。

    - * 阶段 * ： 下次重新启动节点时应用更改。

      如果要使新网络配置正常运行，需要更改物理或虚拟网络配置，则必须使用 * 阶段 * 选项，关闭受影响的节点，进行必要的物理网络更改并重新启动受影响的节点。

      > 如果使用 * 阶段 * 选项，则必须在暂存后尽快重新启动节点，以最大程度地减少中断。

    - * 取消 * ： 此时不要更改任何网络。

      如果您不知道建议的更改需要重新启动节点，则可以推迟更改以最大限度地减少对用户的影响。选择 * 取消 * 将返回到主菜单并保留所做的更改，以便稍后应用。

    应用或暂存更改后，由于网格配置更改，系统将生成新的恢复软件包。

12. 如果配置因错误而停止，则可以使用以下选项：

    - 要中止 IP 更改操作步骤 并返回主菜单，请输入 * A* 。
    - 要重试失败的操作，请输入 * 。
    - 要继续执行下一个操作，请输入 * c* 。

      稍后可以从主菜单中选择选项 * 10 * （应用更改）重试失败的操作。只有成功完成所有操作后， IP 更改操作步骤 才会完成。

◦ 如果您必须手动干预（例如重新启动节点），并确信工具认为失败的操作已实际成功完成，请输入 * f* 将其标记为成功并移至下一操作。

13. 从网格管理器下载新的恢复软件包。

a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。

b. 输入配置密码短语。

恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

相关信息

配置 IP 地址

更改网格中所有节点的 **IP** 地址

如果需要更改网格中所有节点的网格网络 IP 地址，则必须遵循此专用操作步骤 。您不能使用操作步骤 更改单个节点来更改网格范围的网格网络 IP 。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

要确保网格成功启动，您必须一次性完成所有更改。

此 操作步骤 适用场景 仅适用于网格网络。您不能使用此操作步骤 更改管理员网络或客户端网络上的 IP 地址。

如果要仅更改一个站点上节点的 IP 地址和 MTU ，请按照执行操作 更改节点网络配置 说明。

步骤

1. 提前规划需要在更改 IP 工具之外进行的更改，例如更改 DNS 或 NTP 以及更改单点登录（ Single Sign-On ， SSO ）配置（如果使用）。

如果现有 NTP 服务器无法通过新 IP 地址访问网格，请在执行 change-IP 操作步骤 之前添加新的 NTP 服务器。

如果现有 DNS 服务器无法通过新 IP 地址访问网格，请在执行 change-IP 操作步骤 之前添加新的 DNS 服务器。

如果为 StorageGRID 系统启用了 SSO ，并且任何依赖方信任均使用管理节点 IP 地址（而不是建议的完全限定域名）进行配置，请准备在 Active Directory 联合身份验证服务（ AD FS ）中更新或重新配置这些依赖方信任 更改 IP 地址后立即执行。请参见有关管理 StorageGRID 的说明。

如有必要，请为新 IP 地址添加新子网。

2. 登录到主管理节点：

a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

3. 输入以下命令以启动更改 IP 工具： `change-ip`

4. 在提示符处输入配置密码短语。

此时将显示主菜单。默认情况下， `SElected nodes` 字段设置为 `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. 在主菜单上，选择 * 。 2* 以编辑所有节点的 IP/ 子网掩码，网关和 MTU 信息。

a. 选择 * 1 * 以更改网格网络。

选择后，提示符将显示节点名称，网格网络名称，数据类型（ IP/ 掩码，网关或 MTU ）， 和当前值。

编辑 DHCP 配置接口的 IP 地址，前缀长度，网关或 MTU 将使接口更改为静态。在 DHCP 配置每个接口之前，系统会显示一条警告。

无法编辑配置为 `FIXED` 的接口。

a. 要设置新值，请按当前值所示格式输入该值。

b. 编辑要更改的所有节点后，输入 * 。 q* 返回主菜单。

您所做的更改将一直保留，直到清除或应用为止。

6. 选择以下选项之一，查看您所做的更改：

◦ * 5* ：显示输出中的编辑内容，这些编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如示例输出所示：

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

- * 6 *： 显示输出中显示的编辑内容，其中显示了完整配置。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。正确显示取决于您的终端客户端是否支持必要的 VT100 转义序列。

7. 选择选项 * 7* 以验证所有更改。

   此验证可确保不会违反网格网络的规则，例如不使用重叠的子网。

   在此示例中，验证返回错误。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   在此示例中，验证已通过。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. 验证通过后，选择 * 。 10* 以应用新的网络配置。

9. 选择 * 阶段 * ，以便在下次重新启动节点时应用更改。

> 必须选择 * 阶段 * 。请勿手动或通过选择 * 应用 * 而不是 * 阶段 * 来执行滚动重新启动；网格将无法成功启动。

10. 完成更改后，选择 * 。 0* 退出更改 IP 工具。
11. 同时关闭所有节点。

> 必须一次性关闭整个网格，以便所有节点同时关闭。

12. 根据需要进行物理或虚拟网络更改。
13. 验证所有网格节点是否均已关闭。
14. 打开所有节点的电源。
15. 成功启动网格后：
    a. 如果添加了新的 NTP 服务器，请删除旧的 NTP 服务器值。
    b. 如果添加了新的 DNS 服务器，请删除旧的 DNS 服务器值。
16. 从网格管理器下载新的恢复软件包。
    a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
    b. 输入配置密码短语。

相关信息

管理 StorageGRID

在网格网络上添加或更改子网列表

关闭网格节点

向现有节点添加接口

Linux： 将管理员或客户端接口添加到现有节点

按照以下步骤将管理网络或客户端网络上的接口添加到安装后的 Linux 节点中。

如果在安装期间未在 Linux 主机上的节点配置文件中配置 admin_network_target 或 client_network_target ，请使用此操作步骤 添加接口。有关节点配置文件的详细信息，请参见适用于 Linux 操作系统的说明：

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian

您可以在托管需要新网络分配的节点的 Linux 服务器上执行此操作步骤 ，而不是在节点内部执行。此操作步骤仅会将接口添加到节点；如果您尝试指定任何其他网络参数，则会发生验证错误。

要提供地址信息，必须使用更改 IP 工具。请参见 更改节点网络配置。

步骤

1. 登录到托管此节点的 Linux 服务器。
2. 编辑节点配置文件： ` /etc/storagegRid/nodes/*node-name*.conf` 。

   请勿指定任何其他网络参数，否则将导致验证错误。

   a. 为新网络目标添加一个条目。例如：

      ```
      client_network_target = bond0.3206
      ```

   b. 可选：为 MAC 地址添加一个条目。例如：

      ```
      client_network_MAC = aa ： 57 ： 61 ： 07 ： ea ： 5c
      ```

3. 运行 node validate 命令：

   ```
   sUdo StorageGRID node validate node-name
   ```

4. 解决所有验证错误。
5. 运行 node reload 命令：

   ```
   sUdo StorageGRID node reload node-name
   ```

Linux： 向节点添加中继或访问接口

安装 Linux 节点后，您可以向该节点添加额外的中继或访问接口。添加的接口将显示在 VLAN 接口页面和 HA 组页面上。

您需要的内容

- 您可以访问有关在 Linux 平台上安装 StorageGRID 的说明。
  - 安装 Red Hat Enterprise Linux 或 CentOS
  - 安装 Ubuntu 或 Debian
- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

在软件升级，恢复操作步骤 或扩展操作步骤 处于活动状态时，请勿尝试向节点添加接口。

关于此任务

安装完 Linux 节点后，请按照以下步骤向该节点添加一个或多个额外的接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。

添加接口时，节点暂时不可用。您应一次在一个节点上执行此操作步骤 。

步骤

1. 登录到托管此节点的 Linux 服务器。
2. 使用 vim 或 pico 等文本编辑器编辑节点配置文件：

   ` /etc/storaggrid/nodes/*node-name*.conf`

3. 向文件中添加一个条目，以指定要添加到节点的每个额外接口的名称以及问题描述 （可选）。请使用此格式。

   ```
   interfaces_target_nnn=value
   ```

   对于 *nnnn* ，请为要添加的每个 `interfaces_target` 条目指定一个唯一编号。

   对于 *value* ，指定裸机主机上物理接口的名称。然后，也可以添加一个逗号并提供接口的问题描述 ，该接口将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。

   例如：

   ```
   interfaces_target_01=ens256 ，中继
   ```

   请勿指定任何其他网络参数，否则将导致验证错误。

4. 运行以下命令以验证对节点配置文件所做的更改：

   ```
   sUdo StorageGRID node validate node-name
   ```

   解决所有错误或警告，然后再继续下一步。

5. 运行以下命令以更新节点的配置：

   ```
   sUdo StorageGRID node reload node-name
   ```

完成后

- 如果添加了一个或多个中继接口，请转到 配置 VLAN 接口 为每个新的父接口配置一个或多个 VLAN 接口。
- 如果添加了一个或多个访问接口，请转到 配置高可用性组 将新接口直接添加到 HA 组。

VMware： 向节点添加中继或访问接口

您可以在安装 VM 节点后向该节点添加中继或访问接口。添加的接口将显示在 VLAN 接口页面和 HA 组页面上。

您需要的内容

- 您可以访问有关在 VMware 平台上安装 StorageGRID 的说明。

安装 VMware

- 您已配置 StorageGRID 11.6.
- 您拥有管理节点和网关节点 VMware 虚拟机。
- 您的网络子网未用作网格，管理员或客户端网络。

- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

> 在软件升级，恢复操作步骤 或扩展操作步骤 处于活动状态时，请勿尝试向节点添加接口。

关于此任务

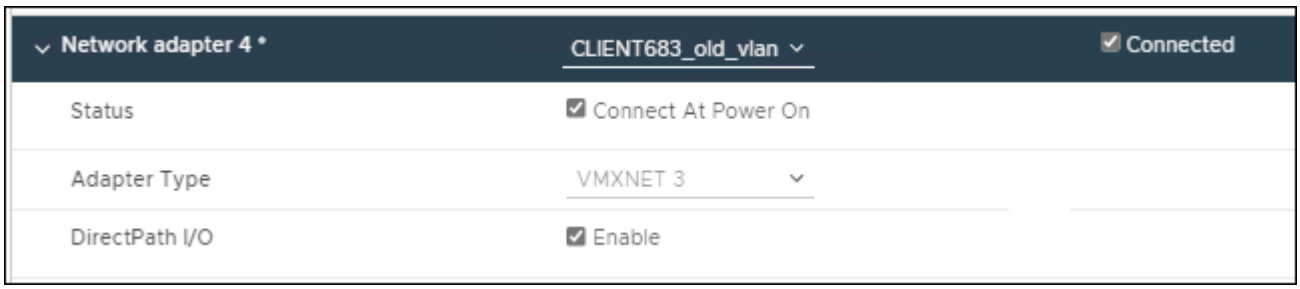
安装 VMware 节点后，请按照以下步骤向该节点添加一个或多个额外接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。

添加接口时，节点可能会暂时不可用。

步骤

1. 在 vCenter 中，向管理节点和网关节点虚拟机添加新的网络适配器（类型为 VMXNET3 ）。选中 * 已连接 * 和 * 在启动时连接 * 复选框。



2. 使用 SSH 登录到管理节点或网关节点。
3. 使用 `ip link show` 确认检测到新的网络接口 ens256 。

```
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
```

完成后

- 如果添加了一个或多个中继接口，请转到 配置 VLAN 接口 为每个新的父接口配置一个或多个 VLAN 接口。
- 如果添加了一个或多个访问接口，请转到 配置高可用性组 将新接口直接添加到 HA 组。

配置 **DNS** 服务器

您可以添加，删除和更新域名系统（ DNS ）服务器，以便使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有要配置的 DNS 服务器的 IP 地址。

通过指定 DNS 服务器信息，您可以对电子邮件或 SNMP 通知和 AutoSupport 使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。建议至少指定两个 DNS 服务器。

> 为 DNS 服务器提供 2 到 6 个 IP 地址。通常，选择每个站点在发生网络隔离时可在本地访问的 DNS 服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以 进一步自定义每个节点的 DNS 服务器列表。

如果省略 DNS 服务器信息或 DNS 服务器信息配置不正确，则会在每个网格节点的 SSM 服务上触发 DNST 警报。如果 DNS 配置正确且新服务器信息已到达所有网格节点，则警报将清除。

步骤

1. 选择 * 维护 * > * 网络 * > * DNS 服务器 * 。
2. 在服务器部分中，根据需要添加更新或删除 DNS 服务器条目。

   最佳做法是，每个站点至少指定两个 DNS 服务器。最多可以指定六个 DNS 服务器。

3. 单击 * 保存 * 。

修改单网格节点的 **DNS** 配置

您可以运行一个脚本，为每个网格节点配置不同的 DNS ，而不是在整个部署中全局配置域名系统（ Domain Name System ， DNS ）。

通常，您应使用网格管理器上的 * 维护 * > * 网络 * > * DNS 服务器 * 选项来配置 DNS 服务器。只有在需要为不同网格节点使用不同 DNS 服务器时，才可使用以下脚本。

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root ： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 `$` 更改为 `#` 。

e. 将 SSH 专用密钥添加到 SSH 代理。输入： `ssh-add`

f. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

2. 【登录到要使用自定义 DNS 配置更新的节点： `ssh node_ip_address`

3. 运行 DNS 设置脚本： `setup_resolv.rb` 。

此脚本将以支持的命令列表进行响应。

```
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. 添加为网络提供域名服务的服务器的 IPv4 地址： `add <nameserver IP_address>`

5. 重复 `add nameserver` 命令以添加名称服务器。
6. 按照提示输入其他命令时的说明进行操作。
7. 保存所做的更改并退出应用程序： `save`
8. 关闭服务器上的命令 Shell： `exit`
9. 对于每个网格节点，重复中的步骤 登录到节点 到 关闭命令 Shell。
10. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入： `ssh-add -D`

配置 NTP 服务器

您可以添加，更新或删除网络时间协议（ Network Time Protocol ， NTP ）服务器，以确保 StorageGRID 系统中的网格节点之间准确同步数据。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须具有要配置的 NTP 服务器的 IPv4 地址。

关于此任务

StorageGRID 系统使用网络时间协议（ NTP ）来同步网格中所有网格节点之间的时间。

在每个站点上，至少会为 StorageGRID 系统中的两个节点分配主 NTP 角色。它们会同步到建议的至少四个外部时间源，最多六个外部时间源以及彼此之间。StorageGRID 系统中不是主 NTP 节点的每个节点都充当 NTP 客户端，并与这些主 NTP 节点同步。

外部 NTP 服务器连接到先前已为其分配主 NTP 角色的节点。因此，建议至少指定两个具有主 NTP 角色的节点。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

指定的外部 NTP 服务器必须使用 NTP 协议。您必须指定 Stratum 3 或更高的 NTP 服务器引用，以防止出现时间偏差问题。

> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。

"支持边界，用于为高精度环境配置 Windows 时间服务"

如果您遇到安装期间最初指定的 NTP 服务器的稳定性或可用性问题，可以通过添加其他服务器或更新或删除现有服务器来更新 StorageGRID 系统使用的外部 NTP 源列表。

步骤

1. 选择 * 维护 * > * 网络 * > * NTP 服务器 * 。

2. 在服务器部分中，根据需要添加更新或删除 NTP 服务器条目。

   您应至少包含 4 个 NTP 服务器，并且最多可以指定 6 个服务器。

3. 在 * 配置密码短语 * 文本框中，输入 StorageGRID 系统的配置密码短语，然后单击 * 保存 * 。

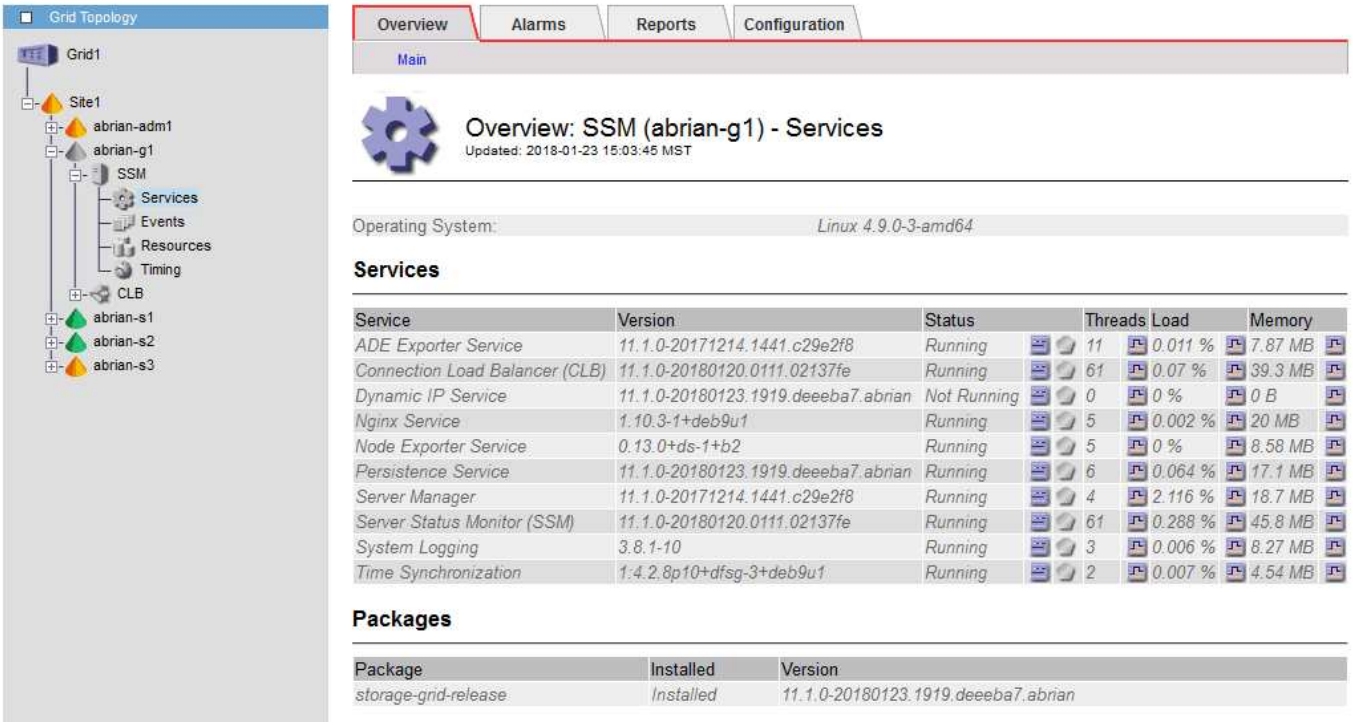
   操作步骤 的状态显示在页面顶部。在配置更新完成之前，此页面将处于禁用状态。

   如果在保存新 NTP 服务器后所有 NTP 服务器均未通过连接测试，请勿继续。请联系技术支持。

恢复隔离节点的网络连接

在某些情况下，例如站点范围或网格范围的 IP 地址更改，一组或多组节点可能无法与网格的其余部分联系。

在网格管理器（ * 支持 * > * 工具 * > * 网格拓扑 * ）中，如果某个节点为灰色，或者某个节点为蓝色，其许多服务显示的状态不是 " 正在运行 " ，则应检查节点隔离情况。



隔离节点会产生以下后果：

- 如果隔离了多个节点，您可能无法登录或访问网格管理器。
- 如果隔离了多个节点，则租户管理器的信息板上显示的存储使用量和配额值可能已过时。恢复网络连接后，总数将更新。

要解决隔离问题描述 ，您可以在与网格隔离的每个隔离节点或组中的一个节点（子网中不包含主管理节点的所有节点）上运行命令行实用程序。该实用程序可为节点提供网格中非隔离节点的 IP 地址，从而使隔离的节点或节点组能够再次访问整个网格。

如果在网络中禁用了多播域名系统（ mDNS ），则可能需要在每个隔离节点上运行命令行实用程序。

1. 访问此节点并检查 ` /var/local/log/dynip.log` 中是否存在隔离消息。

   例如：

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action may be required.
   ```

   如果您使用的是 VMware 控制台，则它将包含一条消息，指出此节点可能已隔离。

   在 Linux 部署中，隔离消息将显示在 ` /var/log/storagegrid/node/<nodename>.log` 文件中。

2. 如果隔离消息重复出现且持久，请运行以下命令：

   `add_node_ip.py < 地址 >`

   其中 ` < 地址 >` 是连接到网格的远程节点的 IP 地址。

   ```
   # /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. 验证先前隔离的每个节点的以下情况：
   - 节点的服务已启动。
   - 运行 `storagegRid-status` 命令后，动态 IP 服务的状态为 "`running` " 。
   - 在网格拓扑树中，节点不再显示为与网格其余部分断开连接。

如果运行 `add_node_ip.py` 命令无法解决此问题，则可能还有其他网络问题需要解决。

主机级别和中间件过程

某些维护过程专用于 StorageGRID 的 Linux 或 VMware 部署，或者专用于 StorageGRID 解决方案 的其他组件。

Linux： 将网格节点迁移到新主机

您可以将 StorageGRID 节点从一台 Linux 主机迁移到另一台 Linux 主机以执行主机维护（例如操作系统修补和重新启动），而不会影响网格的功能或可用性。

您将一个或多个节点从一个 Linux 主机（" s源主机 "）迁移到另一个 Linux 主机（"`目标主机` "）。目标主机必须事先已准备好供 StorageGRID 使用。

只有在您计划的 StorageGRID 部署包含迁移支持时，才能使用此操作步骤 。

要将网格节点迁移到新主机，必须满足以下两个条件：

- 共享存储用于所有每个节点的存储卷
- 网络接口在主机之间的名称一致

在生产部署中，请勿在一台主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

可以在同一主机上部署其他类型的节点，例如管理节点或网关节点。但是，如果您有多个相同类型的节点（例如两个网关节点），请勿将所有实例安装在同一主机上。

有关详细信息，请参见适用于 Linux 操作系统的 StorageGRID 安装说明中的 "`节点迁移要求` " 。

相关信息

部署新的 Linux 主机

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

Linux： 从源主机导出节点

关闭网格节点并将其从源 Linux 主机导出。

在源 Linux 主机上运行以下命令。

1. 获取源主机上当前正在运行的所有节点的状态。

```
sudo storagegrid node status all
```

名称 `Config-State Run-State`

`dC1-ADM1` 配置为运行

`dC1-ARC1` 已配置为运行

`dC1-GW1` 已配置为运行

`dC1-S1` 已配置为运行

`dC1-S2` 配置为运行

`dC1-S3` 已配置为运行

2. 确定要迁移的节点的名称，如果其运行状态为 `running` ，则将其停止。

```
sudo storagegrid node stop DC1-S3
```

s顶部节点 `DC1-S3`

等待长达 `630` 秒以关闭节点

3. 从源主机导出节点。

```
sudo storagegrid node export DC1-S3
```

已将节点 `DC1-S3` 导出到 `/dev/mapper/sgws-DC1-s3-var-local` 。

如果您，请使用 StorageGRID 节点导入 /dev/mapper/sgws-DC1-s3-var-local

希望重新导入。

4. 记下 `export` 命令输出中建议的 `import 命令。

您将在下一步的目标主机上运行此命令。

Linux：目标主机上的导入节点

从源主机导出节点后，您可以在目标 Linux 主机上导入并验证此节点。验证可确认节点可以访问与源主机上相同的块存储和网络接口设备。

在目标 Linux 主机上运行以下命令。

1. 在目标主机上导入节点。

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

已从 `/dev/mapper/sgws-DC1-s3-var-local` 导入节点 `DC1-S3` 。

您应运行 `StorageGRID node validate DC1-s3"`

2. 验证新主机上的节点配置。

```
sudo storagegrid node validate DC1-S3
```

` + 确认节点 DC1-S3 存在 … 已通过 +`

` + 检查节点 DC1-S3 的配置文件 /etc/storaggrid/nodes/DC1-s3.conf … 已通过 +`

` + 检查唯一值是否重复 … 已通过 +`

3. 如果发生任何验证错误，请在启动迁移的节点之前解决这些错误。

   有关故障排除信息，请参见适用于 Linux 操作系统的 StorageGRID 安装说明。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

Linux：启动已迁移的节点

验证迁移的节点后，您可以在目标 Linux 主机上运行命令来启动该节点。

步骤

1. 在新主机上启动节点。

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. 在网格管理器中，验证节点的状态是否为绿色，并且未针对该节点发出任何警报。

   验证节点的状态是否为绿色可确保已迁移的节点已完全重新启动并重新加入网格。如果状态不是绿色，请勿迁移任何其他节点，以免多个节点停止服务。

   如果无法访问网格管理器，请等待 10 分钟，然后运行以下命令：

   `sUdo StorageGRID 节点状态 * ； node-name_*`

   确认迁移的节点的运行状态为 `running` 。

TSM 中间件的归档节点维护

可以将归档节点配置为通过 TSM 中间件服务器锁定磁带或通过 S3 API 将云锁定。配置后，无法更改归档节点的目标。

如果托管归档节点的服务器发生故障，请更换该服务器并按照相应的恢复操作步骤 进行操作。

归档存储设备出现故障

如果您确定归档节点通过 Tivoli Storage Manager （ TSM ）访问的归档存储设备存在故障，请使归档节点脱机，以限制 StorageGRID 系统中显示的警报数量。然后，您可以使用 TSM 服务器或存储设备的管理工具或这两者来进一步诊断和解决问题。

使目标组件脱机

在对 TSM 中间件服务器进行任何可能导致其不可供归档节点使用的维护之前，请使目标组件脱机，以限制在

TSM 中间件服务器不可用时触发的警报数量。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARC* > * 目标 * > * 配置 * > * 主 * 。
3. 将 Tivoli Storage Manager State 的值更改为 * 脱机 * ，然后单击 * 应用更改 * 。
4. 维护完成后，将 Tivoli Storage Manager State 的值更改为 * 联机 * ，然后单击 * 应用更改 * 。

Tivoli Storage Manager 管理工具

dsmadc 工具是安装在归档节点上的 TSM 中间件服务器的管理控制台。您可以通过在服务器的命令行中键入 `dsmadc` 来访问此工具。使用与为 ARC-Service 配置的管理用户名和密码相同的管理用户名和密码登录到管理控制台。

创建 `tsmquery.rb` 脚本是为了以更易读的形式从 dsmadc 生成状态信息。您可以在归档节点的命令行中输入以下命令来运行此脚本： ` /usr/local/arc/tsmquery.rb status`

有关 TSM 管理控制台 dsmadc 的详细信息，请参见 *Tivoli Storage Manager for Linux： Administrator's Referation*.

对象永久不可用

当归档节点从 Tivoli Storage Manager （ TSM ）服务器请求对象而检索失败时，归档节点会在 10 秒间隔后重试此请求。如果对象永久不可用（例如，由于对象在磁带上损坏）， TSM API 无法向归档节点指示此情况，因此归档节点会继续重试此请求。

发生这种情况时，系统会触发警报，并且此值会继续增加。要查看警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 归档节点 * > * ARC/ * 检索 * > * 请求故障 * 。

如果对象永久不可用，则必须确定该对象，然后按照操作步骤 中所述手动取消归档节点的请求。 确定对象是否永久不可用。

如果对象暂时不可用，检索也可能失败。在这种情况下，后续检索请求最终应成功。

如果将 StorageGRID 系统配置为使用创建单个对象副本的 ILM 规则，并且无法检索该副本，则该对象将丢失，无法恢复。但是，您仍然必须按照操作步骤 来确定对象是否永久不可用于 "`清理` " StorageGRID 系统，取消归档节点的请求以及清除丢失对象的元数据。

确定对象是否永久不可用

您可以通过使用 TSM 管理控制台发出请求来确定对象是否永久不可用。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。
- 您必须知道管理节点的 IP 地址。

关于此任务

此示例仅供您参考；此操作步骤 无法帮助您确定可能导致对象或磁带卷不可用的所有故障情况。有关 TSM 管理的信息，请参见 TSM 服务器文档。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 确定归档节点无法检索到的一个或多个对象：
   a. 转到包含审核日志文件的目录： `cd /var/local/audit/export`

      活动的审核日志文件名为 audit.log 。每天保存一次活动的 `audit.log` 文件，并启动一个新的 `audit.log` 文件。已保存文件的名称以 `yyyy-mm-dd.txt` 格式指示其保存时间。一天之后，保存的文件将被压缩并重命名，格式为 `yyyy-mm-dd.txt.gz` ，从而保留原始日期。

   b. 在相关审核日志文件中搜索指示无法检索归档对象的消息。例如，输入： `grep Arce audit.log ； less -n`

      如果无法从归档节点检索对象，则 Arce 审核消息（归档对象检索结束）会在结果字段中显示 Arun （归档中间件不可用）或 GERR （一般错误）。审核日志中的以下示例行显示，对于 CBID 498D8A1F681F05B3 ， Arce 消息已终止，结果为 Arun 。

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      有关详细信息，请参见了解审核消息的说明。

   c. 记录请求失败的每个对象的 CBID 。

      您可能还需要记录 TSM 用于标识归档节点保存的对象的以下追加信息：

      - * 文件空间名称 * ： 等效于归档节点 ID 。要查找归档节点 ID ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 归档节点 * > * ARC/ * 目标 * > * 概述 * 。
      - * 高级名称 * ： 相当于归档节点分配给对象的卷 ID 。卷 ID 采用日期的形式（例如， `2009 1127` ），并在归档审核消息中记录为对象的 VLID 。
      - * 低级别名称 * ： 相当于 StorageGRID 系统分配给对象的 CBID 。

   d. 注销命令 Shell： `exit`
3. 检查 TSM 服务器，查看步骤 2 中标识的对象是否永久不可用：
   a. 登录到 TSM 服务器的管理控制台： `dsmadc`

      请使用为该应用程序中心服务配置的管理用户名和密码。在网格管理器中输入用户名和密码。（要查看

用户名，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 归档节点 * > * ARC* > * 目标 * > * 配置 * 。）

b. 确定对象是否永久不可用。

例如，您可以在 TSM 活动日志中搜索该对象的数据完整性错误。以下示例显示了在过去一天的活动日志中搜索 CBID `498D8A1F681F05B3` 的对象。

```
> 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)
>
```

根据错误的性质， CBID 可能不会记录在 TSM 活动日志中。您可能需要在日志中搜索请求失败前后的其他 TSM 错误。

c. 如果整个磁带永久不可用，请确定存储在该卷上的所有对象的 CBID： `query content Tsm_Volume_Name`

其中 `TSM_Volume_Name` 是不可用磁带的 TSM 名称。以下是此命令的输出示例：

```
 > 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
```

文件名` 的 客户端名称与归档节点卷 `ID` （或 `TSM "`high level name`"`）相同，后跟对象的 CBID （或 TSM "`low level name`"）。也就是说， `Client` 的 `Name for File Name` 采用 ` /Archive Node 卷 ID /CBID` 的形式。在示例输出的第一行中，文件名` 的 客户端名称是 ` `/20081201/C1D172940E6C7E12` 。

另请记住， 文件空间 是归档节点的节点 ID 。

要取消检索请求，您需要卷上存储的每个对象的 CBID 以及归档节点的节点 ID 。

4. 对于永久不可用的每个对象，请取消检索请求并执行问题描述 a 命令，以通知 StorageGRID 系统对象副本已丢失：

> 请谨慎使用 ADE 控制台。如果控制台使用不当，则可能会中断系统操作并损坏数据。请认真输入命令，并且只能使用此操作步骤 中记录的命令。

a. 如果尚未登录到归档节点，请按以下方式登录：

i. 输入以下命令： `ssh admin@ grid_node_ip_`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。

b. 访问该 ARC 服务的 ADE 控制台： `telnet localhost 1409`

c. 取消对象的请求： ` /proc/BRTR/cancel -c CBID`

其中 `CBID` 是无法从 TSM 检索到的对象的标识符。

如果此对象的唯一副本位于磁带上，则 "`bulk retrretr检 索` " 请求将被取消，并显示消息 "`1 Requests cancelled` " 。如果对象的副本位于系统中的其他位置，则对象检索将由其他模块处理，因此对消息的响应为 "`0 Requests cancelled` " 。

d. 问题描述 一个命令，用于通知 StorageGRID 系统某个对象副本已丢失且必须创建另一个副本： ` /proc/CMSI/Object_Lost CBID node_ID`

其中， `CBID` 是无法从 TSM 服务器检索的对象的标识符， `node_ID` 是检索失败的归档节点的节点 ID 。

您必须为每个丢失的对象副本输入一个单独的命令：不支持输入 CBID 范围。

在大多数情况下， StorageGRID 系统会立即开始为对象数据创建更多副本，以确保系统的 ILM 策略得到遵守。

但是，如果对象的 ILM 规则指定只创建一个副本，而该副本现已丢失，则无法恢复该对象。在这种情况下，运行 `Object_Lost` 命令可从 StorageGRID 系统清除丢失对象的元数据。

当 `Object_Lost` 命令成功完成后，将返回以下消息：

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

ℹ ` /proc/CMSI/Object_Lost` 命令仅适用于归档节点上存储的丢失对象。

a. 退出 ADE 控制台： `exit`

b. 从归档节点中注销： `exit`

5. 重置 StorageGRID 系统中的请求失败值：

a. 转到 * 归档节点 * > * ARC* > * 检索 * > * 配置 * ，然后选择 * 重置请求失败计数 * 。

b. 单击 * 应用更改 * 。

相关信息

管理 StorageGRID

查看审核日志

VMware：配置虚拟机以进行自动重新启动

如果在重新启动 VMware vSphere 虚拟机管理程序后虚拟机未重新启动，则可能需要对虚拟机进行配置，使其自动重新启动。

如果在恢复网格节点或执行其他维护操作步骤 期间发现虚拟机未重新启动，则应执行此操作步骤 。

步骤

1. 在 VMware vSphere Client 树中，选择未启动的虚拟机。
2. 右键单击虚拟机，然后选择 * 启动 * 。
3. 配置 VMware vSphere 虚拟机管理程序，以便将来自动重新启动虚拟机。

网格节点过程

您可能需要在特定网格节点上执行相关过程。虽然您可以从网格管理器执行其中几个过程，但大多数过程都要求您从节点的命令行访问 Server Manager 。

服务器管理器在每个网格节点上运行，用于监控服务的启动和停止，并确保服务正常加入和退出 StorageGRID 系统。Server Manager 还会监控每个网格节点上的服务，并自动尝试重新启动报告故障的任何服务。

只有在技术支持指示您访问 Server Manager 时，才应访问此服务器管理器。

使用完 Server Manager 后，您必须关闭当前命令 Shell 会话并注销。输入： `exit`

查看 **Server Manager** 状态和版本

对于每个网格节点，您可以查看该网格节点上运行的 Server Manager 的当前状态和版本。您还可以获取该网格节点上运行的所有服务的当前状态。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 查看网格节点上运行的 Server Manager 的当前状态： ` * service servermanager status*`

   报告网格节点上运行的 Server Manager 的当前状态（无论是否正在运行）。如果 Server Manager 的状态为 `running` ，则会列出自上次启动以来其一直运行的时间。例如：

```
servermanager running for 1d, 13h, 0m, 30s
```

3. 查看在网格节点上运行的 Server Manager 的当前版本： ` * 服务服务器管理器版本 *`

   此时将列出当前版本。例如：

```
11.1.0-20180425.1905.39c9493
```

4. 从命令 Shell ` * exit *` 中注销

查看所有服务的当前状态

您可以随时查看网格节点上运行的所有服务的当前状态。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

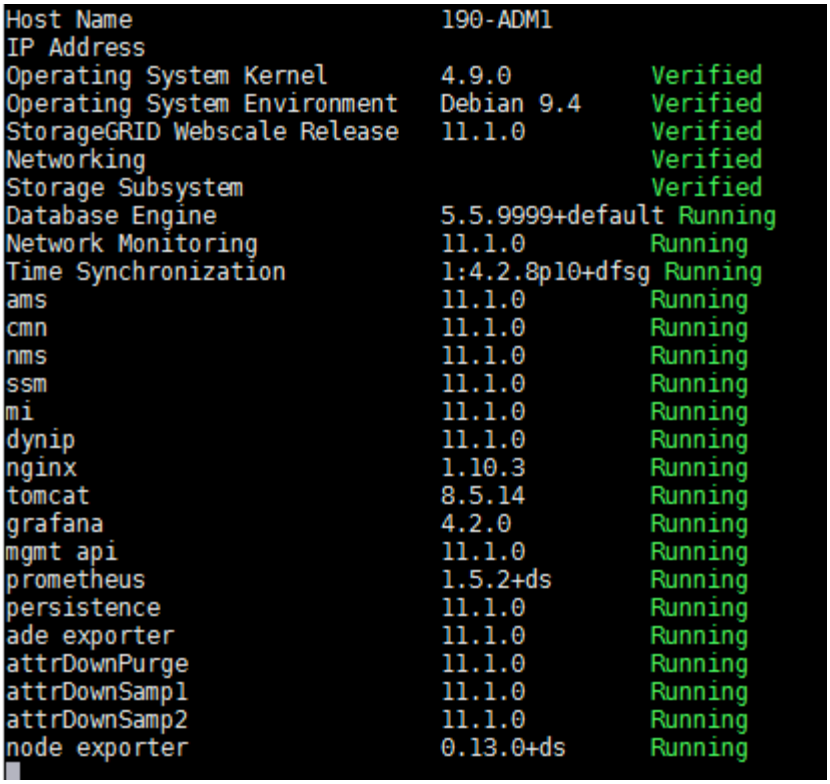
   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 查看网格节点上运行的所有服务的状态： `storagegRid-status`

   例如，主管理节点的输出将 AMS ， CMN 和 NMS 服务的当前状态显示为正在运行。如果服务状态发生变化，此输出将立即更新。



3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 也可以查看网格节点上运行的所有服务的静态报告： ` /usr/local/servermanager/reader.rb`

   此报告包含与持续更新报告相同的信息，但如果服务状态发生变化，则不会更新此报告。

5. 注销命令 Shell： `exit`

启动服务器管理器和所有服务

您可能需要启动 Server Manager ，该操作也会启动网格节点上的所有服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

如果在已运行 Server Manager 的网格节点上启动 Server Manager ，则会重新启动 Server Manager 以及网格节点上的所有服务。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 启动服务器管理器： `service servermanager start`
3. 注销命令 Shell： `exit`

重新启动 **Server Manager** 和所有服务

您可能需要重新启动服务器管理器以及网格节点上运行的所有服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 重新启动服务器管理器以及网格节点上的所有服务： `service servermanager restart`

   Server Manager 以及网格节点上的所有服务将停止并重新启动。

   使用 `restart` 命令与依次使用 `stop` 命令和 `sstart` 命令相同。
3. 注销命令 Shell： `exit`

停止 **Server Manager** 和所有服务

Server Manager 可始终运行，但您可能需要停止 Server Manager 以及网格节点上运行的所有服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止服务器管理器以及网格节点上运行的所有服务： `sservice servermanager stop`

   服务器管理器以及网格节点上运行的所有服务均正常终止。服务可能需要长达 15 分钟才能关闭。

3. 注销命令 Shell： `exit`

查看服务的当前状态

您可以随时查看网格节点上运行的服务的当前状态。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 查看在网格节点上运行的服务的当前状态： ` * service *servicename* status* 报告在网格节点上运行的请求服务的当前状态（无论是否正在运行）。例如：

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. 从命令 Shell ` * exit *` 中注销

停止服务

某些维护过程要求您停止一项服务，同时保持网格节点上的其他服务正常运行。只有在维护操作步骤 指示停止单个服务时，才停止这些服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

使用以下步骤 "`以管理员方式停止` " 服务时， Server Manager 不会自动重新启动该服务。您必须手动启动单个服务或重新启动 Server Manager 。

如果需要停止存储节点上的 LDR 服务，请注意，如果存在活动连接，则停止此服务可能需要一段时间。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止单个服务： `sservice_servicename_ stop`

   例如：

   ```
   service ldr stop
   ```

   > 服务可能需要长达 11 分钟才能停止。

3. 注销命令 Shell： `exit`

相关信息

强制终止服务

将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

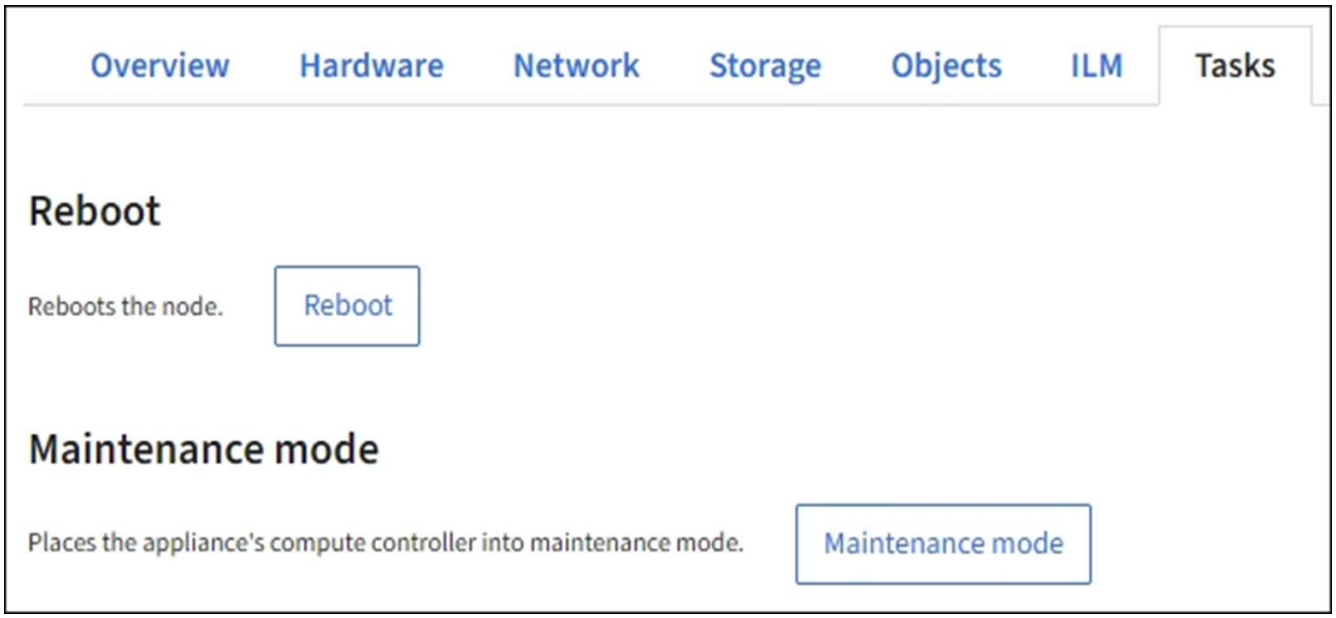
关于此任务

在极少数情况下，将 StorageGRID 设备置于维护模式可能会使该设备无法进行远程访问。

> 处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

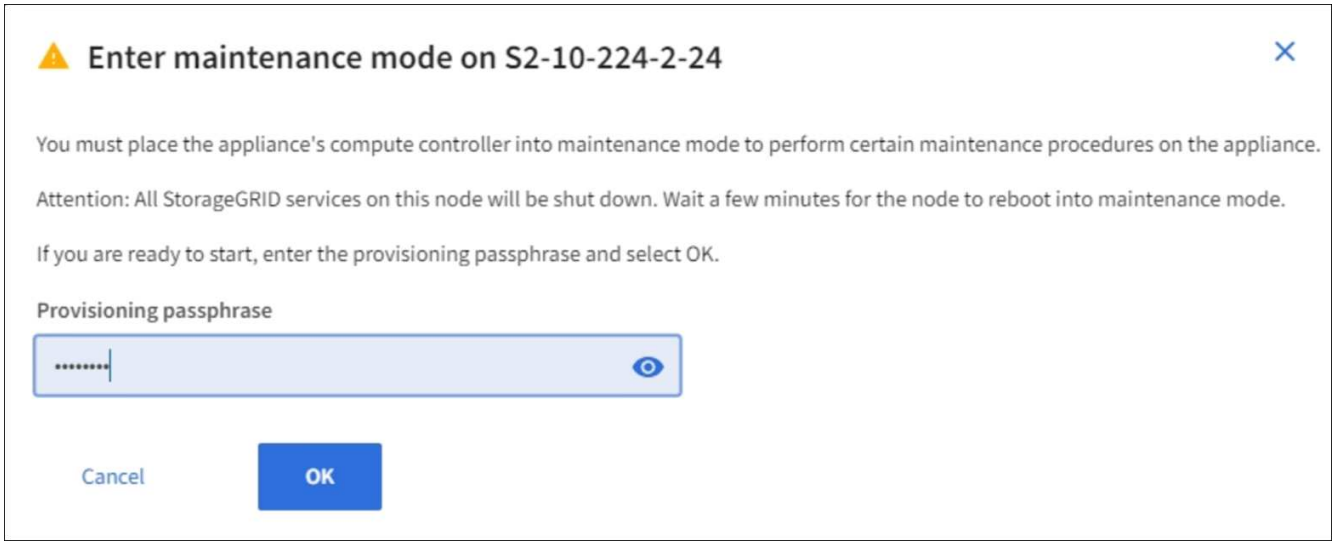
步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面的树视图中，选择设备存储节点。
3. 选择 * 任务 * 。



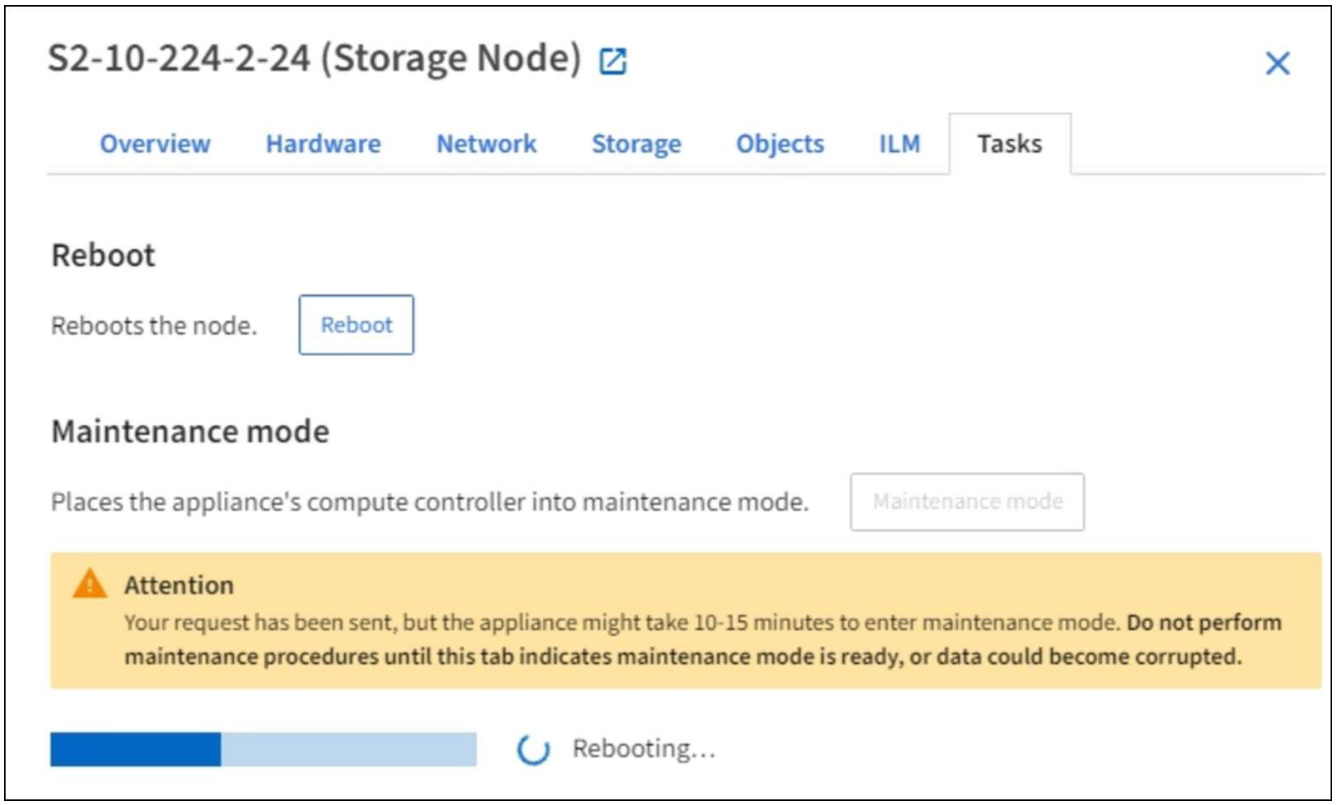
4. 选择 * 维护模式 * 。

   此时将显示确认对话框。

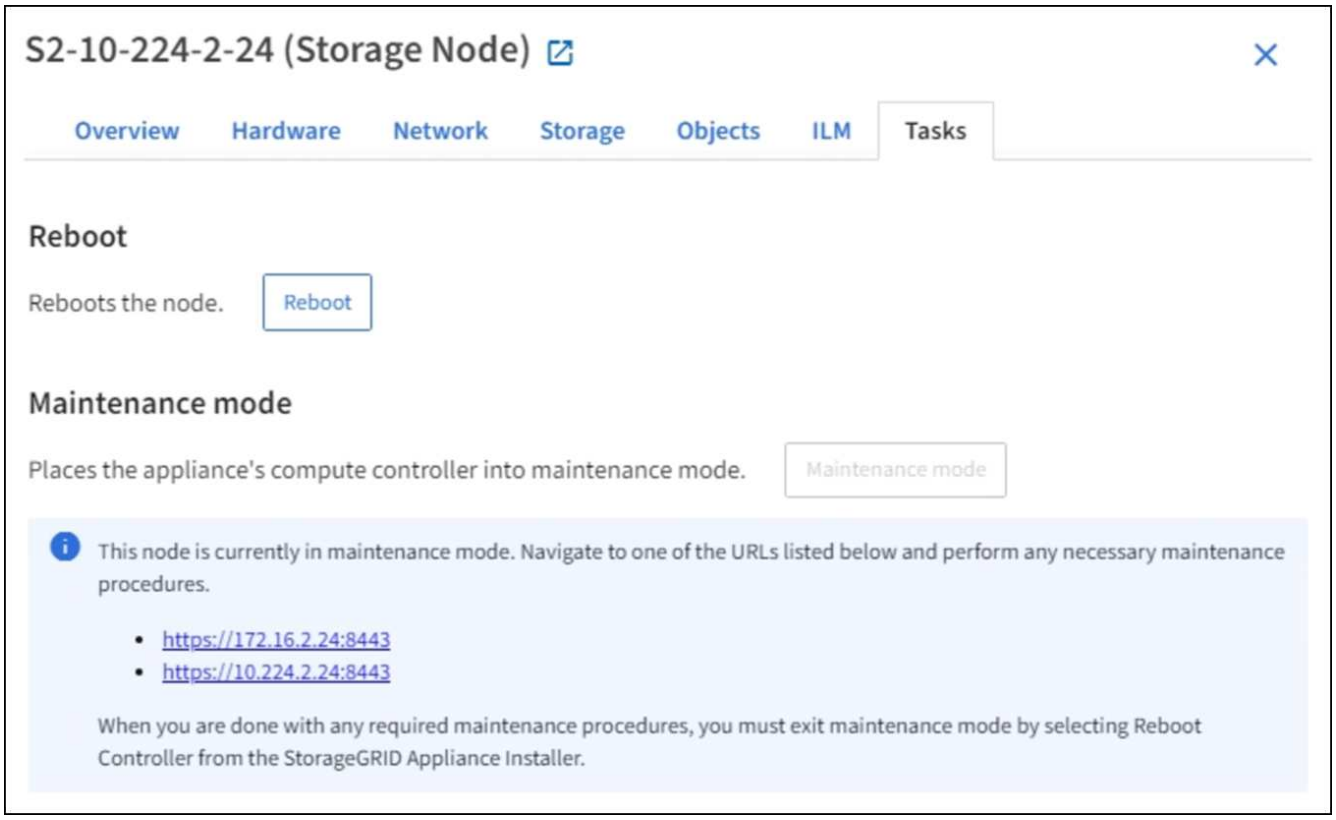


5. 输入配置密码短语，然后选择 * 确定 * 。

   进度条和一系列消息（包括 " 已发送请求 " ， " 正在停止 StorageGRID " 和 " 正在重新启动 " ）表示设备正在完成进入维护模式的步骤。



设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL 。



6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL 。

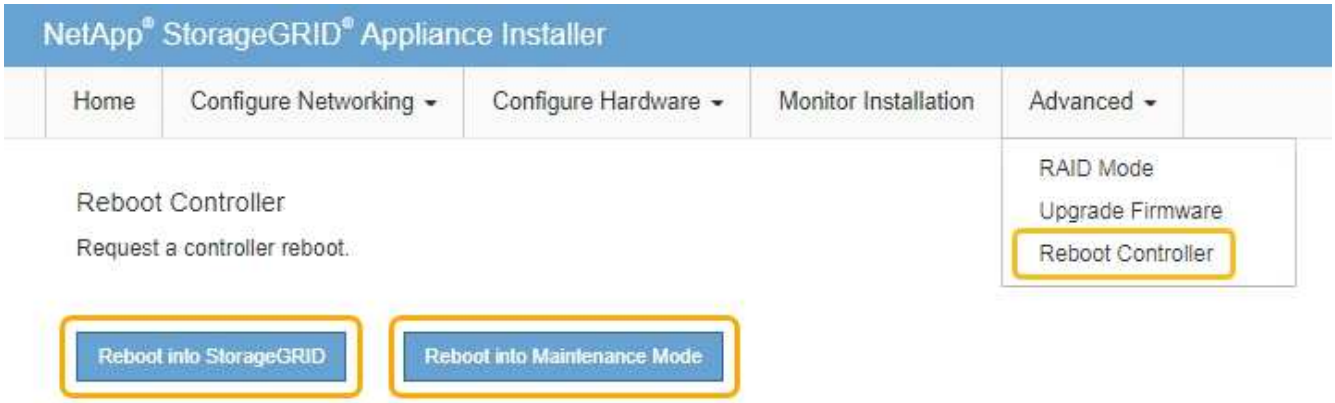
   如果可能，请使用包含设备管理网络端口 IP 地址的 URL 。

访问 ` + https://169.254.0.1:8443+` 需要直接连接到本地管理端口。

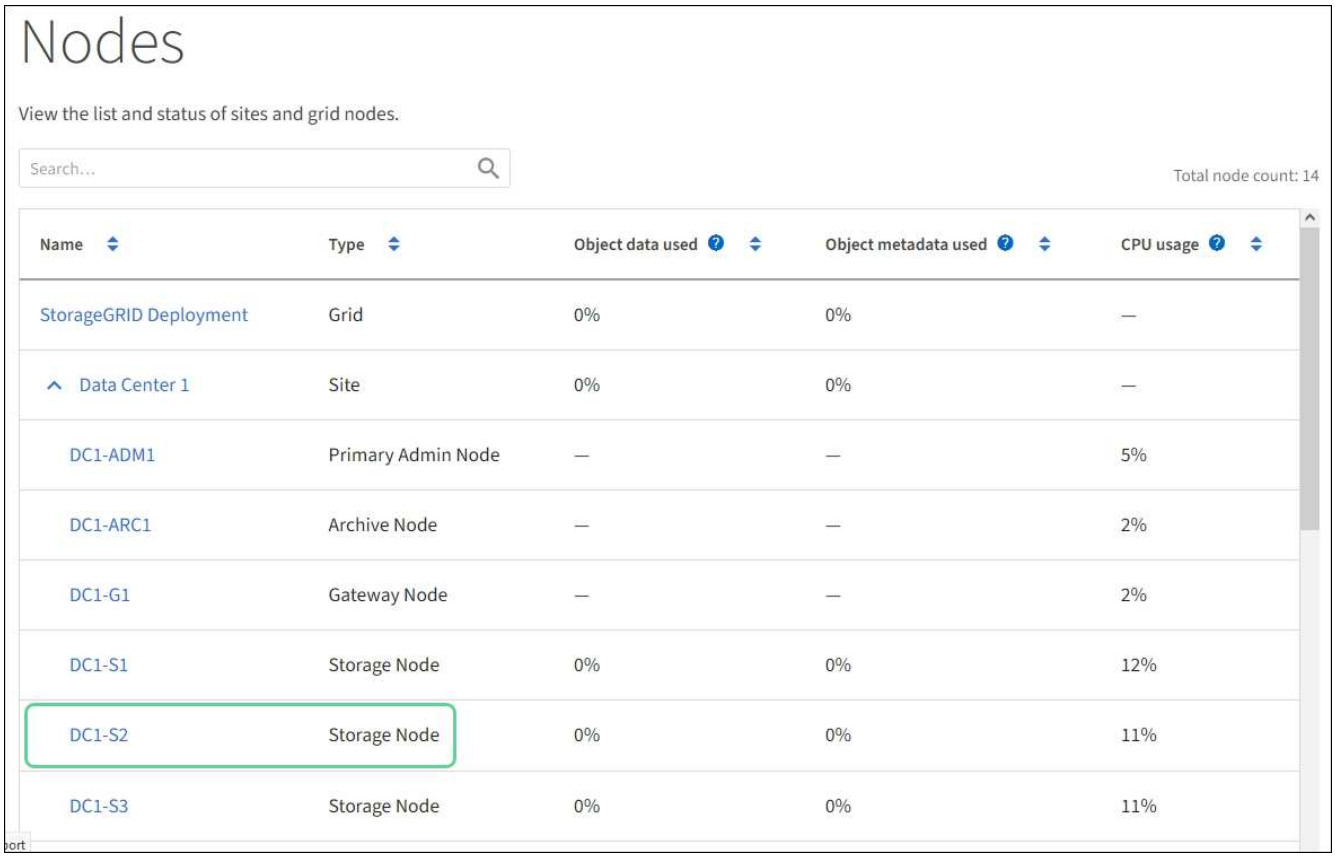
7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。



8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"* 节点 * " 页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



强制终止服务

如果需要立即停止服务，可以使用 `force-stop` 命令。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 手动强制终止服务： `service servicename force-stop`

   例如：

```
service ldr force-stop
```

系统将等待 30 秒，然后再终止此服务。

3. 注销命令 Shell： `exit`

启动或重新启动服务

您可能需要启动已停止的服务，或者可能需要停止并重新启动服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 根据服务当前是正在运行还是已停止，确定向问题描述 发出的命令。
   - 如果此服务当前已停止，请使用 `sstart` 命令手动启动此服务： `service servicename start`

     例如：

     ```
     service ldr start
     ```

   - 如果此服务当前正在运行，请使用 `restart` 命令停止此服务，然后重新启动它： `service servicename restart`

     例如：

```
service ldr restart
```

+

> 使用 `restart` 命令与依次使用 `stop` 命令和 `sstart` 命令相同。即使服务当前已停止，您也可以使用问题描述 `restart` 。

3. 注销命令 Shell： `exit`

删除端口重新映射

如果要为负载平衡器服务配置端点，并且要使用已配置为端口重新映射的映射到端口的端

口，则必须先删除现有端口重新映射，否则此端点将无效。您必须在每个管理节点和网关节点上运行一个脚本，该节点具有冲突的重新映射端口，以删除该节点的所有端口重新映射。

关于此任务

此操作步骤 将删除所有端口重新映射。如果需要保留部分重新映射，请联系技术支持。

有关配置负载平衡器端点的信息，请参见有关管理 StorageGRID 的说明。

如果端口重新映射提供了客户端访问，则应重新配置客户端，以便尽可能使用配置为负载平衡器端点的其他端口，以避免服务丢失，否则，删除端口映射将导致客户端访问丢失，并应相应地进行计划。

对于在裸机主机上部署为容器的 StorageGRID 系统，此操作步骤 不起作用。请参见的说明 删除裸机主机上的端口重新映射。

步骤

1. 登录到此节点。
   a. 输入以下命令： `ssh -p 8022 admin@node_ip`

      端口 8022 是基础操作系统的 SSH 端口，而端口 22 是运行 StorageGRID 的容器引擎的 SSH 端口。

   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 运行以下脚本： `remove-port-remap.sh`
3. 重新启动节点。

   按照的说明进行操作 重新启动网格节点。

4. 对具有冲突重新映射端口的每个管理节点和网关节点重复上述步骤。

相关信息

管理 StorageGRID

删除裸机主机上的端口重新映射

如果要为负载平衡器服务配置端点，并且要使用已配置为端口重新映射的映射到端口的端口，则必须先删除现有端口重新映射，否则此端点将无效。如果您在裸机主机上运行 StorageGRID ，请按照此操作步骤 而不是常规操作步骤 删除端口重新映射。您必须为每个管理节点和网关节点编辑节点配置文件，该节点的重新映射端口相互冲突，以删除该节点的所有端口重新映射并重新启动该节点。

关于此任务

此操作步骤 将删除所有端口重新映射。如果需要保留部分重新映射，请联系技术支持。

有关配置负载平衡器端点的信息，请参见有关管理 StorageGRID 的说明。

此操作步骤 可能会在节点重新启动时暂时丢失服务。

步骤

1. 登录到支持此节点的主机。以 root 用户身份或使用具有 sudo 权限的帐户登录。
2. 运行以下命令以临时禁用节点： `sUdo StorageGRID node stop node-name`
3. 使用 vim 或 pico 等文本编辑器编辑节点的节点配置文件。

   节点配置文件位于 ` /etc/storaggrid/nodes/*node-name*.conf` 中。

4. 找到节点配置文件中包含端口重新映射的部分。

   请参见以下示例中的最后两行。

```
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. 编辑 port_remap 和 port_remap_inbound 条目以删除端口重新映射。

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 运行以下命令以验证对节点的节点配置文件所做的更改： `sUdo StorageGRID node validate node-name`

   解决所有错误或警告，然后再继续下一步。

7. 运行以下命令以在不重新映射端口的情况下重新启动节点： `sUdo StorageGRID node start node-name`
8. 使用 `passwords.txt` 文件中列出的密码以管理员身份登录到此节点。
9. 验证服务是否正确启动。
   a. 查看服务器上所有服务的状态列表：`sudo storagegRid-status`

      状态将自动更新。

   b. 请等待，直到所有服务的状态均为 " 正在运行 " 或 " 已验证 " 。
   c. 退出状态屏幕：`Ctrl+C`
10. 对具有冲突重新映射端口的每个管理节点和网关节点重复上述步骤。

重新启动网格节点

您可以从网格管理器或节点的命令 Shell 重新启动网格节点。

关于此任务

重新启动网格节点时，该节点将关闭并重新启动。所有服务都会自动重新启动。

如果您计划重新启动存储节点，请注意以下事项：

- 如果 ILM 规则指定了 " 双提交 " 的载入行为或规则指定了 " 已平衡 " ，并且无法立即创建所有必需的副本，则 StorageGRID 会立即将任何新载入的对象提交到同一站点上的两个存储节点，并在稍后评估 ILM 。如果要重新启动给定站点上的两个或多个存储节点，则在重新启动期间可能无法访问这些对象。
- 为了确保您可以在存储节点重新启动时访问所有对象，请在重新启动节点之前，停止在站点上载入对象大约一小时。

相关信息

管理 StorageGRID

从网格管理器重新启动网格节点

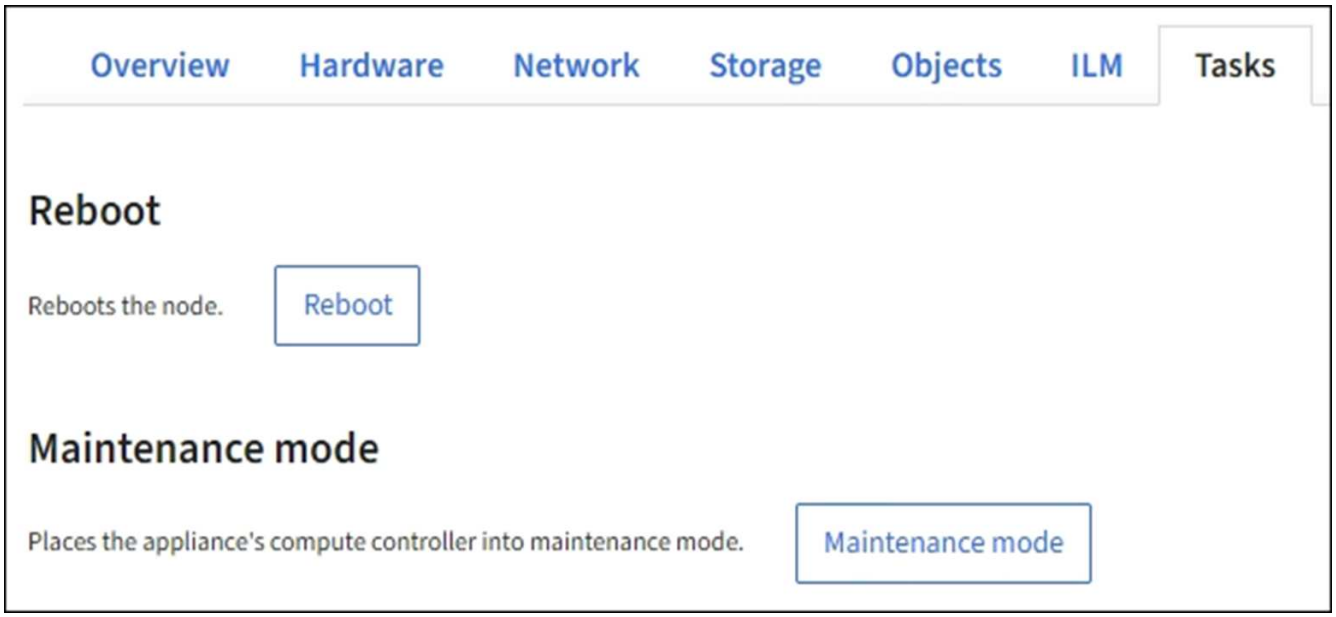
从网格管理器重新启动网格节点会在目标节点上发出 `reboot` 命令。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有配置密码短语。

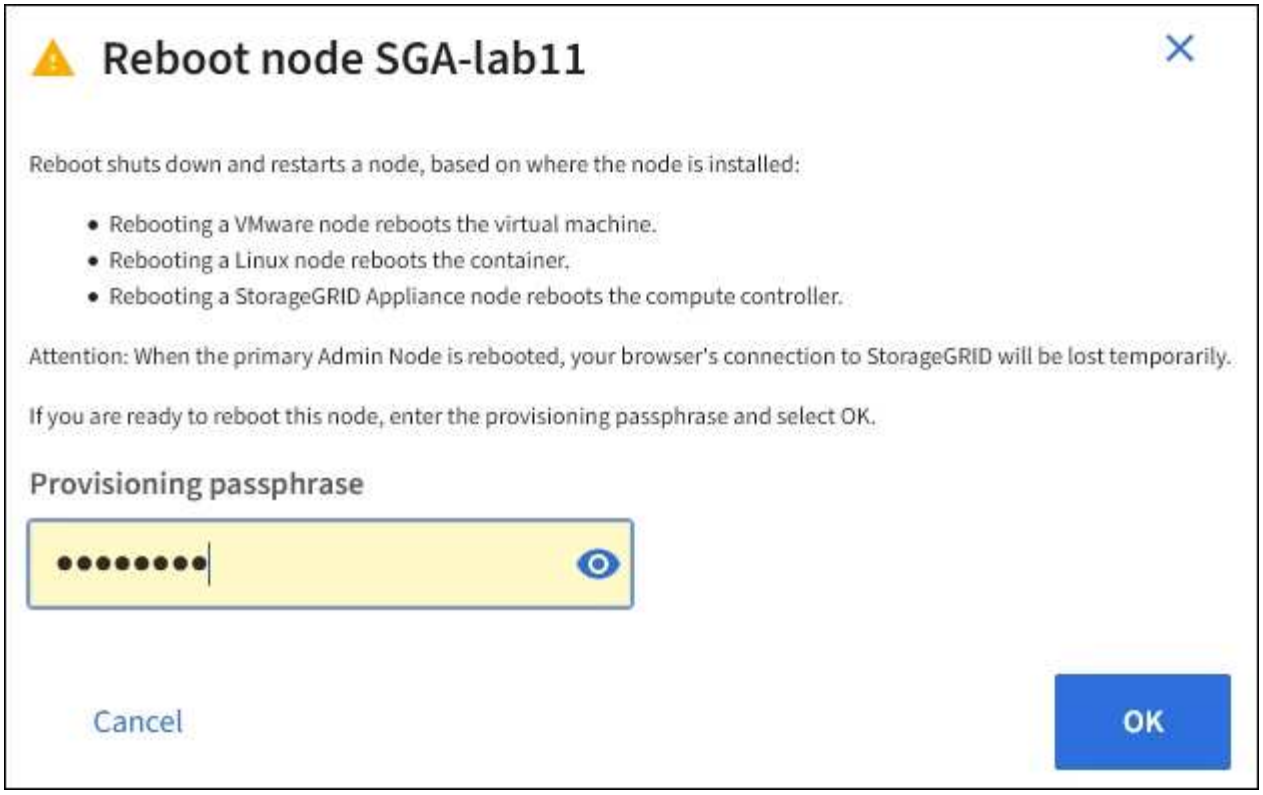
步骤

1. 选择 * 节点 * 。
2. 选择要重新启动的网格节点。
3. 选择 * 任务 * 选项卡。



4. 选择 * 重新启动 * 。

   此时将显示确认对话框。



如果要重新启动主管理节点，则确认对话框会提醒您，服务停止后，浏览器与网格管理器的连接将暂时断开。

5. 输入配置密码短语，然后单击 * 确定 * 。
6. 等待节点重新启动。

   关闭服务可能需要一些时间。

   节点重新启动时， * 节点 * 页面左侧会显示灰色图标（管理员关闭）。当所有服务重新启动且节点已成功连接到网格时， * 节点 * 页面应显示正常状态（节点名称左侧没有图标），表示没有活动警报且节点已连接到网格。

从命令 **Shell** 重新启动网格节点

如果您需要更密切地监控重新启动操作，或者无法访问网格管理器，则可以登录到网格节点并从命令 Shell 运行 Server Manager reboot 命令。

您必须具有 `passwords.txt` 文件。

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 或者，停止服务： `service servermanager stop`

   停止服务是一个可选步骤，但建议执行此步骤。服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程，然后再在下一步中重新启动节点。

3. 重新启动网格节点： `reboot`
4. 注销命令 Shell： `exit`

关闭网格节点

您可以使用节点的命令 Shell 关闭网格节点。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

关于此任务

在执行此操作步骤 之前，请查看以下注意事项：

- 通常，一次关闭的节点不应超过一个，以避免中断。
- 除非文档或技术支持明确指示，否则请勿在维护操作步骤 期间关闭节点。
- 关闭过程取决于节点的安装位置，如下所示：
  - 关闭 VMware 节点将关闭虚拟机。
  - 关闭 Linux 节点将关闭容器。
  - 关闭 StorageGRID 设备节点将关闭计算控制器。
- 如果您计划关闭一个站点上的多个存储节点、请在关闭这些节点之前停止在该站点上载入对象大约一小时。

  如果任何ILM规则使用*双提交*载入选项(或者某个规则使用*平衡*选项、并且无法立即创建所有必需的副本)、则StorageGRID 会立即将任何新载入的对象提交到同一站点上的两个存储节点、并在稍后对ILM进行评估。如果某个站点上的多个存储节点关闭、则在关闭期间、您可能无法访问新载入的对象。如果站点上的可用存储节点太少、写入操作也可能失败。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。

3. 如果此节点正在 VMware 虚拟机上运行或它是设备节点，请使用问题描述 关闭命令： `shutdown -h now`

   执行此步骤，无论 `sservice servermanager stop` 命令的结果如何。

   > 在设备节点上执行问题描述 `shutdown -h now` 命令后，必须重新启动设备以重新启动节点。

   对于设备，此命令将关闭控制器，但设备仍处于打开状态。您必须完成下一步。

4. 如果要关闭设备节点：
   - 对于 SG100 或 SG1000 服务设备
     i. 关闭设备电源。
     ii. 等待蓝色电源 LED 熄灭。
   - 对于 SG6000 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

     当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，然后等待蓝色电源 LED 熄灭。
   - 对于 SG5700 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

     当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，等待所有 LED 和七段显示活动停止。

相关信息

管理 StorageGRID

关闭主机

在关闭主机电源之前，必须停止该主机上所有网格节点上的服务。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止节点上运行的所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。

3. 对主机上的每个节点重复步骤 1 和 2 。
4. 如果您使用的是 Linux 主机：
   a. 登录到主机操作系统。
   b. 停止节点： `StorageGRID node stop`
   c. 关闭主机操作系统。
5. 如果此节点正在 VMware 虚拟机上运行或它是设备节点，请使用问题描述 关闭命令： `shutdown -h now`

   执行此步骤，无论 `sservice servermanager stop` 命令的结果如何。

   > 在设备节点上执行问题描述 `shutdown -h now` 命令后，必须重新启动设备以重新启动节点。

   对于设备，此命令将关闭控制器，但设备仍处于打开状态。您必须完成下一步。
6. 如果要关闭设备节点：
   - 对于 SG100 或 SG1000 服务设备
     i. 关闭设备电源。
     ii. 等待蓝色电源 LED 熄灭。
   - 对于 SG6000 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，然后等待蓝色电源 LED 熄灭。
   - 对于 SG5700 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，等待所有 LED 和七段显示活动停止。
7. 注销命令 Shell： `exit`

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

关闭并打开网格中的所有节点

例如，如果要移动数据中心，您可能需要关闭整个 StorageGRID 系统。以下步骤简要概述了执行受控关闭和启动的建议顺序。

关闭站点或网格中的所有节点后，在存储节点脱机时，您将无法访问已载入的对象。

停止服务并关闭网格节点

在关闭 StorageGRID 系统之前，必须先停止每个网格节点上运行的所有服务，然后关闭所有 VMware 虚拟机，容器引擎和 StorageGRID 设备。

关于此任务

首先停止管理节点和 API 网关节点上的服务，然后停止存储节点上的服务。

通过此方法，您可以使用主管理节点尽可能长时间地监控其他网格节点的状态。

> 如果一个主机包含多个网格节点，请勿关闭该主机，直到停止该主机上的所有节点为止。如果主机包含主管理节点，请最后关闭该主机。

> 如果需要，您可以 将节点从一台 Linux 主机迁移到另一台 Linux 主机 在不影响网格功能或可用性的情况下执行主机维护。

步骤

1. 停止所有客户端应用程序访问网格。
2. 【登录到每个网关节点】登录到每个网关节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
3. 【 stop_all_services]] 停止节点上运行的所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。
4. 重复上述两个步骤，停止所有存储节点，归档节点和非主管理节点上的服务。

   您可以按任何顺序停止这些节点上的服务。

   > 如果问题描述 您使用 `sservice servermanager stop` 命令停止设备存储节点上的服务，则必须重新启动设备以重新启动节点。
5. 对于主管理节点，重复执行的步骤 登录到节点 和 停止节点上的所有服务。
6. 对于在 Linux 主机上运行的节点：
   a. 登录到主机操作系统。
   b. 停止节点： `StorageGRID node stop`
   c. 关闭主机操作系统。

7. 对于在 VMware 虚拟机上运行的节点以及设备存储节点，请使用问题描述 关闭命令： `shutdown -h now`

   执行此步骤，无论 `sservice servermanager stop` 命令的结果如何。

   对于设备，此命令将关闭计算控制器，但设备仍处于打开状态。您必须完成下一步。

8. 如果您有设备节点：
   - 对于 SG100 或 SG1000 服务设备
     i. 关闭设备电源。
     ii. 等待蓝色电源 LED 熄灭。
   - 对于 SG6000 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，然后等待蓝色电源 LED 熄灭。
   - 对于 SG5700 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，等待所有 LED 和七段显示活动停止。
9. 如果需要，请注销命令 Shell： `exit`

   此时， StorageGRID 网格已关闭。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

启动网格节点

按照以下顺序在完全关闭后启动网格节点。

> 您需要什么？ **#8217**；将需要什么
>
> 如果整个网格已关闭超过 15 天，则在启动任何网格节点之前，您必须联系技术支持。请勿尝试执行重建 Cassandra 数据的恢复过程。这样做可能会导致数据丢失。

关于此任务

如果可能，应按以下顺序启动网格节点：

- 首先为管理节点接通电源。

- 请最后为网关节点通电。

如果主机包含多个网格节点，则在启动主机时，这些节点将自动恢复联机。

步骤

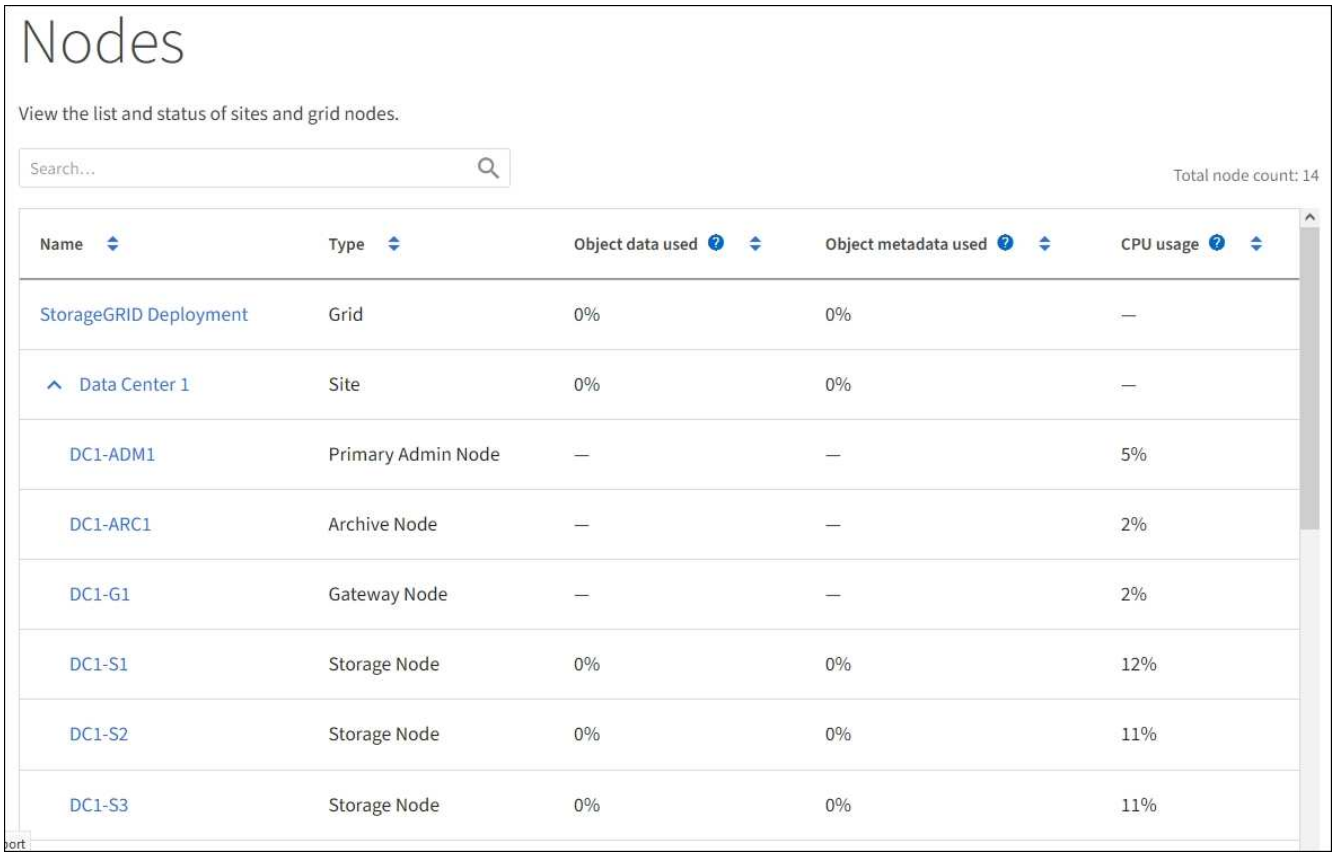
1. 打开主管理节点和任何非主管理节点的主机的电源。

   在重新启动存储节点之前，您将无法登录到管理节点。

2. 启动所有归档节点和存储节点的主机。

   您可以按任意顺序打开这些节点的电源。

3. 启动所有网关节点的主机。
4. 登录到网格管理器。
5. 选择 * 节点 * 并监控网格节点的状态。验证节点名称旁边是否没有警报图标。



使用 **DoNotStart** 文件

如果您在技术支持的指导下执行各种维护或配置过程，则可能会要求您使用 DoNotStart 文件来防止在启动或重新启动 Server Manager 时启动服务。

只有在技术支持要求您添加或删除 DoNotStart 文件时，才应添加或删除此文件。

要阻止服务启动，请将 DoNotStart 文件置于要阻止启动的服务的目录中。启动时， Server Manager 将查找 DoNotStart 文件。如果文件存在，则会阻止服务（以及与之相关的任何服务）启动。删除 DoNotStart 文件后，先前停止的服务将在下次启动或重新启动 Server Manager 时启动。删除 DoNotStart 文件后，服务不会自动启动。

阻止所有服务重新启动的最有效方法是阻止 NTP 服务启动。所有服务都依赖于 NTP 服务，如果 NTP 服务未运行，则无法运行。

为服务添加 **DoNotStart** 文件

通过将 DoNotStart 文件添加到网格节点上某个服务的目录中，您可以阻止单个服务启动。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 添加 DoNotStart 文件： `touch /etc/sv/service/DoNotStart`

   其中 `sservice` 是要阻止启动的服务的名称。例如：

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   此时将创建 DoNotStart 文件。不需要文件内容。

   重新启动 Server Manager 或网格节点后， Server Manager 将重新启动，但服务不会重新启动。
3. 注销命令 Shell： `exit`

删除 **DoNotStart** 文件以进行维护

删除阻止服务启动的 DoNotStart 文件时，必须启动该服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 从服务目录中删除 DoNotStart 文件： `rm /etc/sv/service/DoNotStart`

   其中 `sservice` 是服务的名称。例如：

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. 启动服务： `sservice_servicename_ start`

4. 注销命令 Shell： `exit`

对 Server Manager 进行故障排除

访问 Server Manager 日志文件

如果使用 Server Manager 时出现问题，请检查其日志文件。

与 Server Manager 相关的错误消息会记录在 Server Manager 日志文件中，该文件位于 ` /var/local/log/servermanager.log`

检查此文件中有关故障的错误消息。如果需要，请将问题描述 升级到技术支持。系统可能会要求您将日志文件转发给技术支持。

存在错误状态的服务

如果您检测到某个服务已进入错误状态，请尝试重新启动此服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

Server Manager 可监控服务并重新启动任何意外停止的服务。如果服务失败， Server Manager 将尝试重新启动它。如果在五分钟内启动服务的尝试失败三次，则该服务将进入错误状态。Server Manager 不会尝试再次重新启动。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 确认服务的错误状态： `sservice_servicename_ status`

   例如：

   ```
   service ldr status
   ```

   如果服务处于错误状态，则会返回以下消息： ` *servicename* in error state` 。例如：

   ```
   ldr in error state
   ```

   如果服务状态为 d**已禁用** ，请参见的说明 删除服务的 DoNotStart 文件。

3. 尝试通过重新启动服务来删除错误状态： `sservice_servicename_ restart`

   如果服务无法重新启动，请联系技术支持。

4. 注销命令 Shell： `exit`

设备节点克隆

您可以在 StorageGRID 中克隆设备节点，以使用设计较新或功能增强的设备。克隆会将现有节点上的所有信息传输到新设备，提供易于执行的硬件升级过程，并提供停用和扩展的替代方案来更换设备。

设备节点克隆的工作原理

通过设备节点克隆，您可以轻松地将网格中的现有设备节点（源）替换为同一逻辑 StorageGRID 站点中的兼容设备（目标）。此过程会将所有数据传输到新设备，从而使其投入使用以更换旧设备节点，并使旧设备处于预安装状态。

为何克隆设备节点?

如果需要，您可以克隆设备节点：

- 更换即将达到使用寿命的设备。
- 升级现有节点以利用经过改进的设备技术。
- 增加网格存储容量，而不更改 StorageGRID 系统中的存储节点数。
- 提高存储效率，例如将 RAID 模式从 DDP-8 更改为 DDP-16 或 RAID-6 。
- 高效地实施节点加密，以允许使用外部密钥管理服务器（ KMS ）。

使用的是哪个 **StorageGRID** 网络?

克隆可通过三个 StorageGRID 网络中的任何一个将数据从源节点直接传输到目标设备。通常使用网格网络，但如果源设备连接到这些网络，您也可以使用管理网络或客户端网络。选择用于克隆流量的网络，该网络可在不降低 StorageGRID 网络性能或数据可用性的情况下提供最佳数据传输性能。

安装替代设备时，必须为 StorageGRID 连接和数据传输指定临时 IP 地址。由于替代设备将与它所替代的设备节点属于同一网络，因此您必须为替代设备上的每个网络指定临时 IP 地址。

目标设备兼容性

替代设备的类型必须与要替换的源节点相同，并且这两个设备都必须属于同一逻辑 StorageGRID 站点。

- 替代服务设备可以不同于要替换的管理节点或网关节点。
  - 您可以将 SG100 源节点设备克隆到 SG1000 服务目标设备，以增强管理节点或网关节点的功能。
  - 您可以将 SG1000 源节点设备克隆到 SG100 服务目标设备，以便为要求更苛刻的应用程序重新部署 SG1000 。

    例如，如果将 SG1000 源节点设备用作管理节点，而您希望将其用作专用负载平衡节点。

  - 将 SG1000 源节点设备更换为 SG100 服务目标设备会将网络端口的最大速度从 100-GbE 降低到 25-GbE 。
  - SG100 和 SG1000 设备具有不同的网络连接器。更改设备类型可能需要更换缆线或 SFP 模块。
- 更换用的存储设备的容量必须等于或大于要更换的存储节点的容量。
  - 如果目标存储设备与源节点具有相同数量的驱动器，则目标设备中的驱动器必须具有相同或更大的容量（以 TB 为单位）。
  - 如果您计划在目标节点上使用与源节点上相同的 RAID 模式， 或者，如果 RAID 模式的存储效率较低（例如，从 RAID6 切换到 DDP ），则目标设备中的驱动器必须大于源设备中的驱动器（以 TB 为单位）。
  - 如果由于安装了固态驱动器（ SSD ），目标存储设备中安装的标准驱动器数量小于源节点中的驱动器数量，则目标设备中标准驱动器的整体存储容量（以 TB 为单位） 必须满足或超过源存储节点中所有驱动器的总功能驱动器容量。

    例如、在将包含60个驱动器的SG5660源存储节点设备克隆到包含58个标准驱动器的SG6060或SG60X目标设备时、应在克隆之前在SG6060或SG60X目标设备中安装更大的驱动器、以保持存储容量。（目标设备中包含 SSD 的两个驱动器插槽不包括在设备存储总容量中。）

    但是、如果为60个驱动器的SG5660源节点设备配置了SANtricity 动态磁盘池DDP-8、则使用DDP-16配置58个驱动器大小相同的SG6060或SG6060X目标设备可能会使SG6060或SG6060X设备成为有效的克隆目标、因为它提高了存储效率。

  您可以在网格管理器的 * 节点 * 页面上查看有关源设备节点当前 RAID 模式的信息。选择设备的 * 存储 * 选项卡。

哪些信息不会克隆?

在克隆期间，以下设备配置不会传输到替代设备。您必须在更换设备的初始设置期间对其进行配置。

- BMC 接口

- 网络链路
- 节点加密状态
- SANtricity 系统管理器（适用于存储节点）
- RAID 模式（适用于存储节点）

哪些问题会阻止克隆?

如果在克隆时遇到以下任何问题，则克隆过程将暂停并生成错误消息：

- 网络配置错误
- 源设备与目标设备之间缺乏连接
- 源设备和目标设备不兼容
- 对于存储节点，是指容量不足的替代设备

要继续克隆，必须解析每个问题描述 。

设备节点克隆的注意事项和要求

在克隆设备节点之前，您必须了解注意事项和要求。

更换设备的硬件要求

确保替代设备符合以下标准：

- 源节点（要更换的设备）和目标（新）设备必须为相同类型的设备：
  - 您只能将管理节点设备或网关节点设备克隆到新的服务设备。
  - 您只能将存储节点设备克隆到新的存储设备。
- 对于管理节点或网关节点设备，源节点设备和目标设备不必是相同类型的设备；但是，更改设备类型可能需要更换缆线或 SFP 模块。

  例如，您可以将 SG1000 节点设备更换为 SG100 ，也可以将 SG100 设备更换为 SG1000 设备。

- 对于存储节点设备，源节点设备和目标设备不必是相同类型的设备；但是，目标设备的存储容量必须大于源设备。

  例如，您可以将 SG5600 节点设备更换为 SG5700 或 SG6000 设备。

请联系您的 StorageGRID 销售代表，以帮助您选择兼容的替代设备来克隆 StorageGRID 安装中的特定设备节点。

准备克隆设备节点

克隆设备节点之前，您必须具有以下信息：

- 从网络管理员处获取网格网络的临时 IP 地址，以便在初始安装期间与目标设备配合使用。如果源节点属于管理网络或客户端网络，请获取这些网络的临时 IP 地址。

临时 IP 地址通常与要克隆的源节点设备位于同一子网中，克隆完成后不需要这些地址。源设备和目标设备都必须连接到 StorageGRID 的主管理节点，才能建立克隆连接。

- 确定要使用哪个网络克隆数据传输流量，从而在不降低 StorageGRID 网络性能或数据可用性的情况下提供最佳数据传输性能。

  使用 1-GbE 管理网络进行克隆数据传输会导致克隆速度变慢。

- 确定目标设备是否将使用密钥管理服务器（ KMS ）进行节点加密，以便在克隆之前在初始目标设备安装期间启用节点加密。您可以按照设备安装中所述检查源设备节点上是否启用了节点加密。

  源节点和目标设备可以具有不同的节点加密设置。在数据传输期间以及目标节点重新启动并加入网格时，系统会自动执行数据解密和加密。

  - SG100 和 SG1000 服务设备
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备

- 确定是否应更改目标设备上的 RAID 模式及其默认设置，以便您可以在克隆之前的初始目标设备安装期间指定此信息。您可以在网格管理器的 * 节点 * 页面上查看有关源设备节点当前 RAID 模式的信息。选择设备的 * 存储 * 选项卡。

  源节点和目标设备可以具有不同的 RAID 设置。

- 规划足够的时间以完成节点克隆过程。将数据从运行中的存储节点传输到目标设备可能需要几天时间。计划一次克隆，尽可能地减少对业务的影响。
- 一次只能克隆一个设备节点。克隆可能会阻止您同时执行其他 StorageGRID 维护功能。
- 克隆设备节点后，您可以使用已恢复预安装状态的源设备作为克隆另一个兼容节点设备的目标。

克隆设备节点

克隆过程可能需要几天时间才能在源节点（正在更换的设备）和目标（新）设备之间传输数据。

您需要的内容

- 您已将兼容的目标设备安装到机柜或机架中，并已连接所有缆线并已接通电源。
- 您已验证更换设备上的 StorageGRID 设备安装程序版本是否与 StorageGRID 系统的软件版本匹配，如有必要，可升级 StorageGRID 设备安装程序固件。
- 您已配置目标设备，包括配置 StorageGRID 连接， SANtricity 系统管理器（仅限存储设备）和 BMC 接口。
  - 配置 StorageGRID 连接时，请使用临时 IP 地址。
  - 配置网络链路时，请使用最终的链路配置。

完成初始目标设备配置后，保持 StorageGRID 设备安装程序处于打开状态。启动节点克隆过程后，您将返回到目标设备的安装程序页面。

- 您也可以选择为目标设备启用节点加密。
- 您也可以为目标设备（仅限存储设备）设置 RAID 模式。
- 设备节点克隆的注意事项和要求

  SG100 和 SG1000 服务设备

  SG5600 存储设备

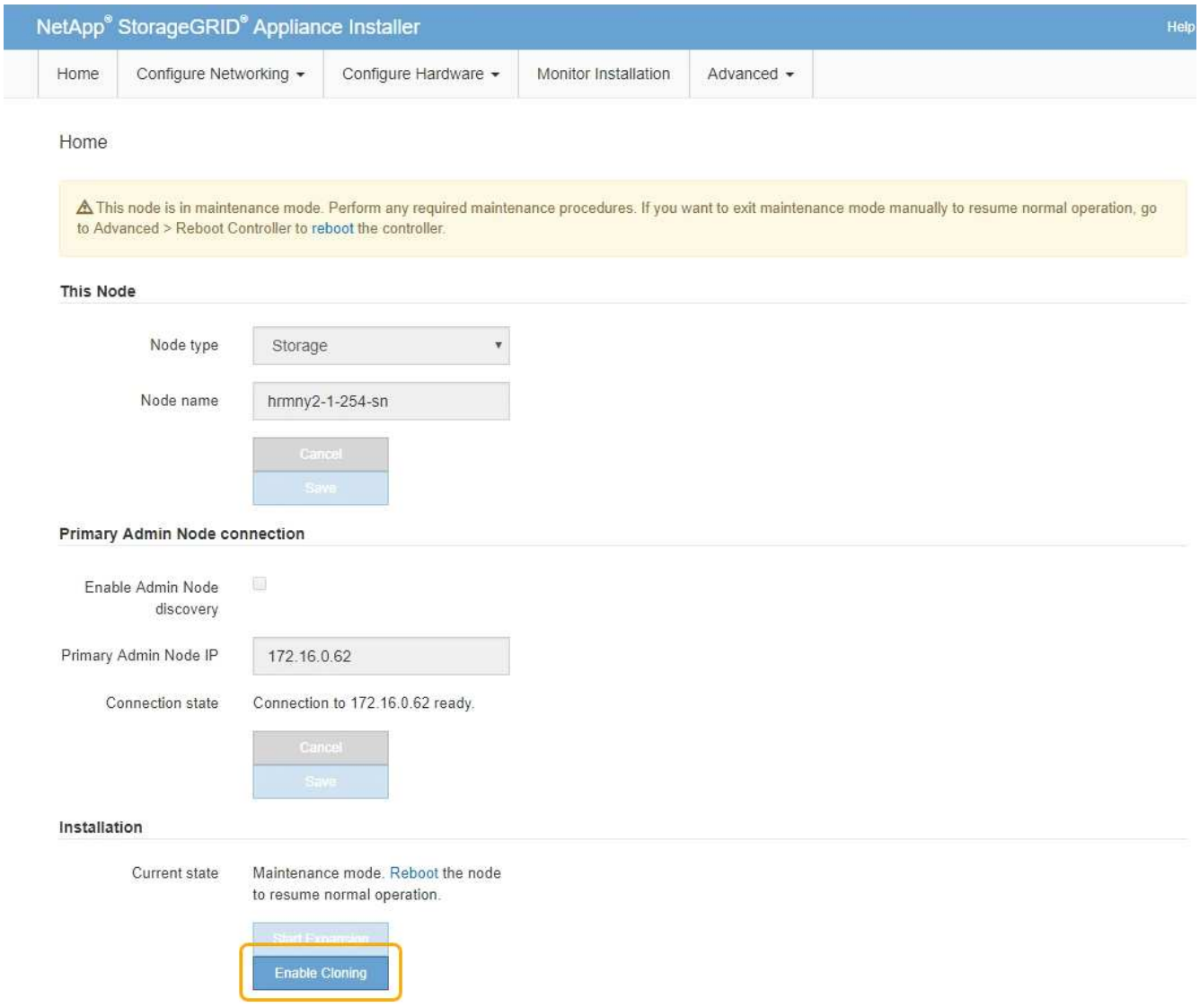
  SG5700 存储设备

  SG6000 存储设备

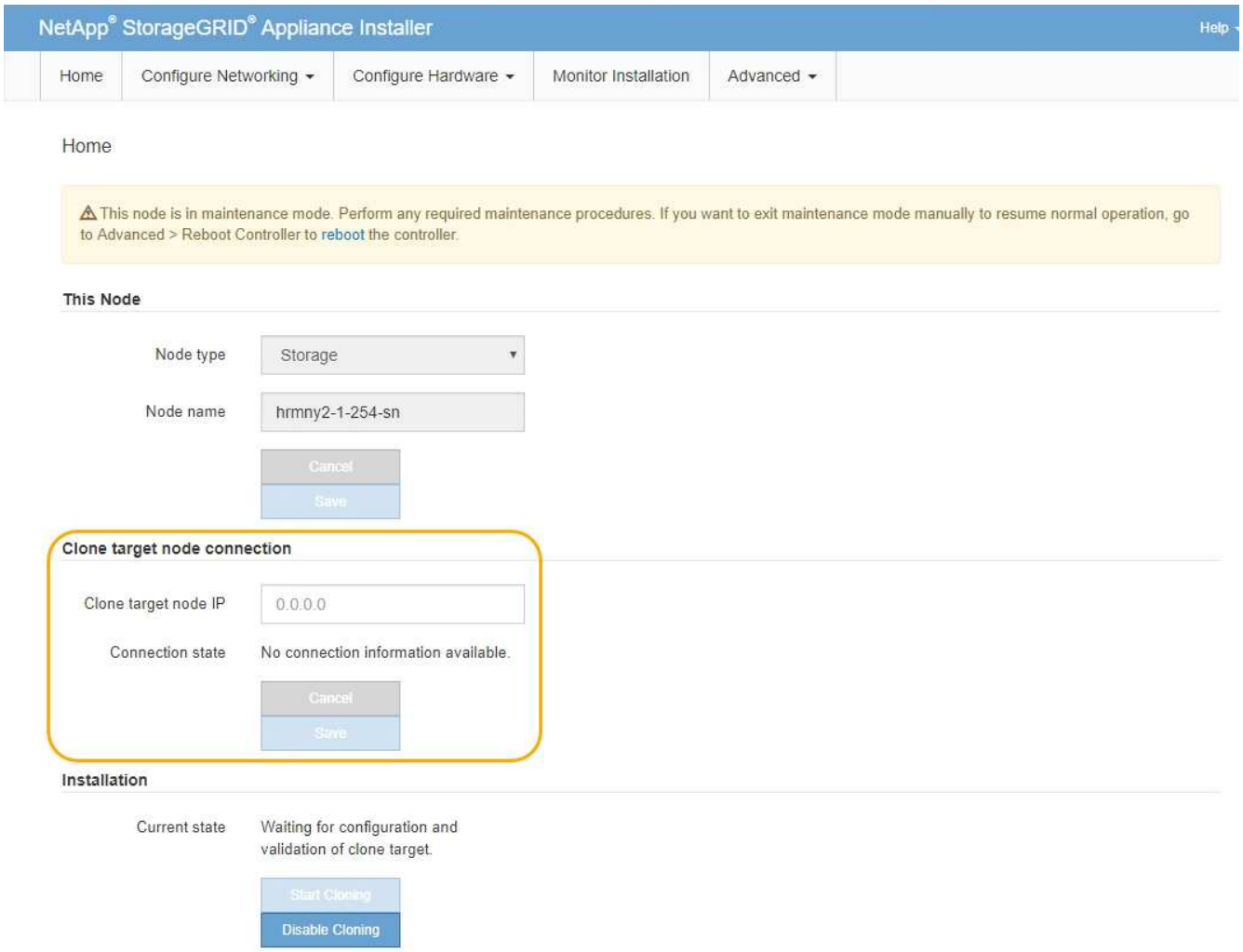
一次只应克隆一个设备节点，以保持 StorageGRID 网络性能和数据可用性。

步骤

1. 将要克隆的源节点置于维护模式。
2. 从源节点上的 StorageGRID 设备安装程序中，在主页的安装部分中，选择 * 启用克隆 * 。



主管理节点连接部分将替换为克隆目标节点连接部分。

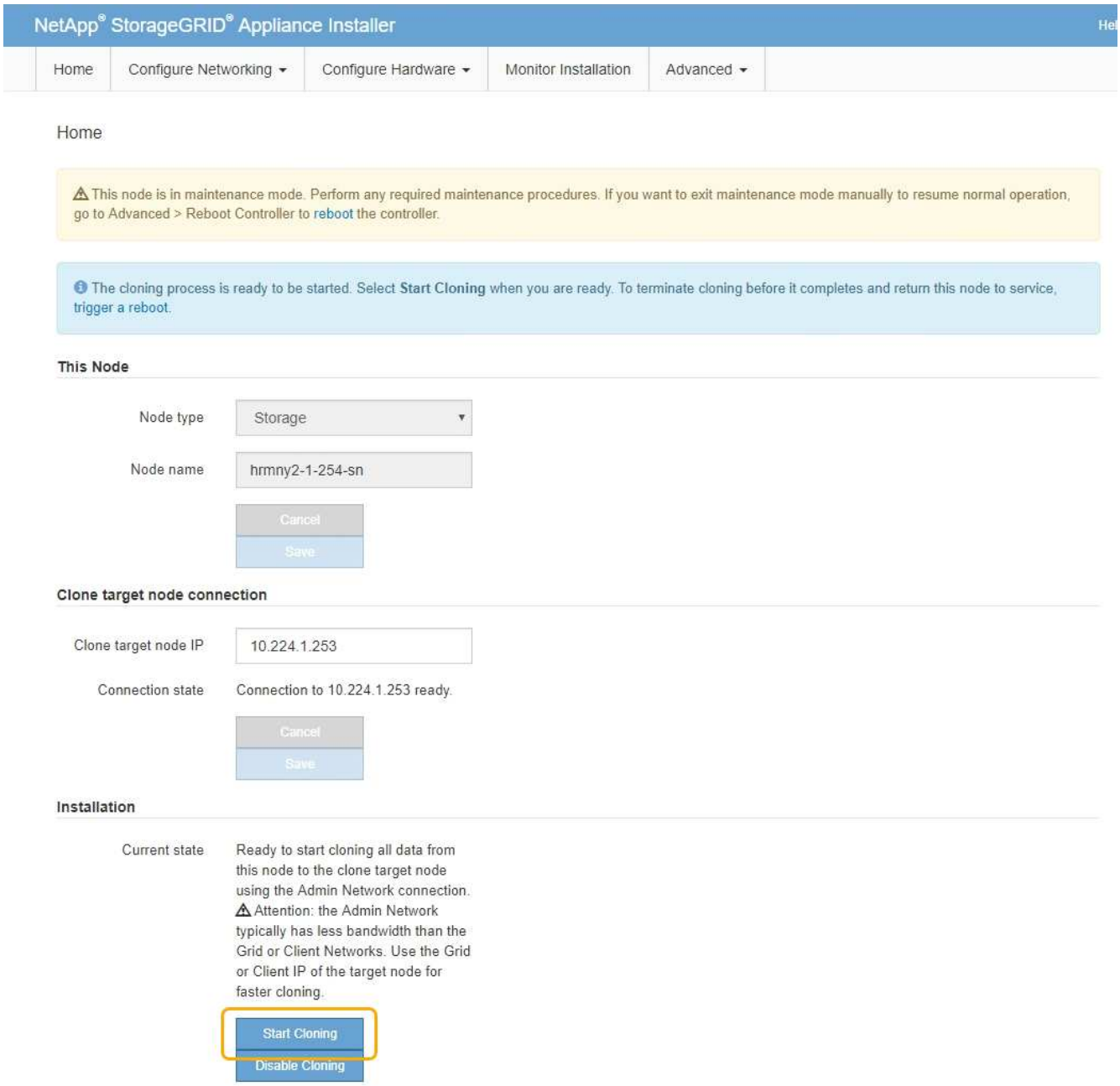


3. 对于 * 克隆目标节点 IP* ，输入分配给目标节点的临时 IP 地址，以便网络用于克隆数据传输流量，然后选择 * 保存 * 。

   通常，您可以输入网格网络的 IP 地址，但如果需要使用其他网络来传输克隆数据传输流量，请输入该网络上目标节点的 IP 地址。

   使用 1-GbE 管理网络进行克隆数据传输会导致克隆速度变慢。

   配置并验证目标设备后，在 "Installation" 部分中，源节点上会启用 * 开始克隆 * 。



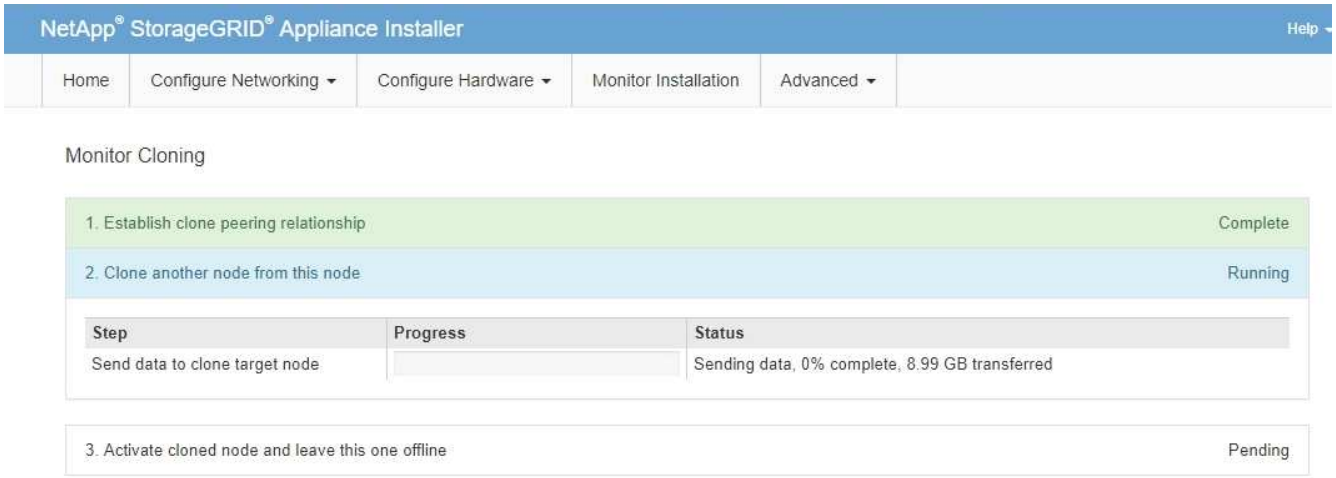
如果存在阻止克隆的问题，则不会启用 * 启动克隆 * ，必须解决的问题将列为 * 连接状态 * 。源节点和目标设备的 StorageGRID 设备安装程序主页均列出了这些问题。一次仅显示一个问题描述，状态会随着条件的变化自动更新。解决所有克隆问题以启用 * 开始克隆 * 。

启用 * 开始克隆 * 后， * 当前状态 * 将指示为克隆流量选择的 StorageGRID 网络以及有关使用该网络连接的信息。

设备节点克隆的注意事项和要求

4. 在源节点上选择 * 开始克隆 * 。
5. 在源节点或目标节点上使用 StorageGRID 设备安装程序监控克隆进度。

   源节点和目标节点上的 StorageGRID 设备安装程序指示相同的状态。



"Monitor Cloning" 页面提供了克隆过程每个阶段的详细进度：

- * 建立克隆对等关系 * 显示克隆设置和配置的进度。
- * 从此节点克隆另一个节点 * 将显示数据传输的进度。（克隆过程的这一部分可能需要几天时间才能完成。）
- * 激活克隆的节点并使其脱机 * 将显示在数据传输完成后将控制权移交给目标节点并将源节点置于预安装状态的进度。

6. 如果需要在克隆完成之前终止克隆过程并将源节点恢复服务，请在源节点上转到 StorageGRID 设备安装程序主页页面，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动到 StorageGRID * 。

   如果克隆过程终止：

   - 源节点将退出维护模式并重新加入 StorageGRID 。
   - 目标节点将保持预安装状态。要重新启动源节点的克隆，请从步骤 1 中重新启动克隆过程。

成功完成克隆后：

- 源节点和目标节点交换 IP 地址：
  - 现在，目标节点将使用最初分配给源节点的网格网络，管理网络和客户端网络 IP 地址。
  - 现在，源节点将使用最初分配给目标节点的临时 IP 地址。
- 目标节点将退出维护模式并加入 StorageGRID ，从而替换源节点。
- 源设备处于预安装状态，就像您已安装一样 已准备好重新安装。

> 如果设备未重新加入网格，请转到源节点的 StorageGRID 设备安装程序主页页面，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动到维护模式 * 。在源节点以维护模式重新启动后，重复节点克隆操作步骤 。

如果目标节点发生意外的问题描述 ，则用户数据将作为恢复选项保留在源设备上。目标节点成功重新加入 StorageGRID 后，源设备上的用户数据已过时，不再需要。如果需要，请 StorageGRID 支持部门清除源设备以销毁此数据。

您可以

- 将源设备用作其他克隆操作的目标：不需要其他配置。此设备已分配最初为第一个克隆目标指定的临时 IP 地址。
- 将源设备安装为新设备节点并进行设置。
- 如果源设备不再用于 StorageGRID ，请丢弃该源设备。

查看审核日志

查看审核日志：概述

这些说明包含有关 StorageGRID 审核消息和审核日志的结构和内容的信息。您可以使用此信息读取和分析系统活动的审核跟踪。

这些说明适用于负责生成系统活动和使用情况报告的管理员，这些报告需要分析 StorageGRID 系统的审核消息。

要使用文本日志文件，您必须有权访问管理节点上配置的审核共享。

有关配置审核消息级别和使用外部系统日志服务器的信息，请参见 配置审核消息和日志目标。

相关信息

- 管理 StorageGRID

审核消息流和保留

所有 StorageGRID 服务都会在系统正常运行期间生成审核消息。您应了解这些审核消息如何在 StorageGRID 系统中移动到 `audit.log` 文件。

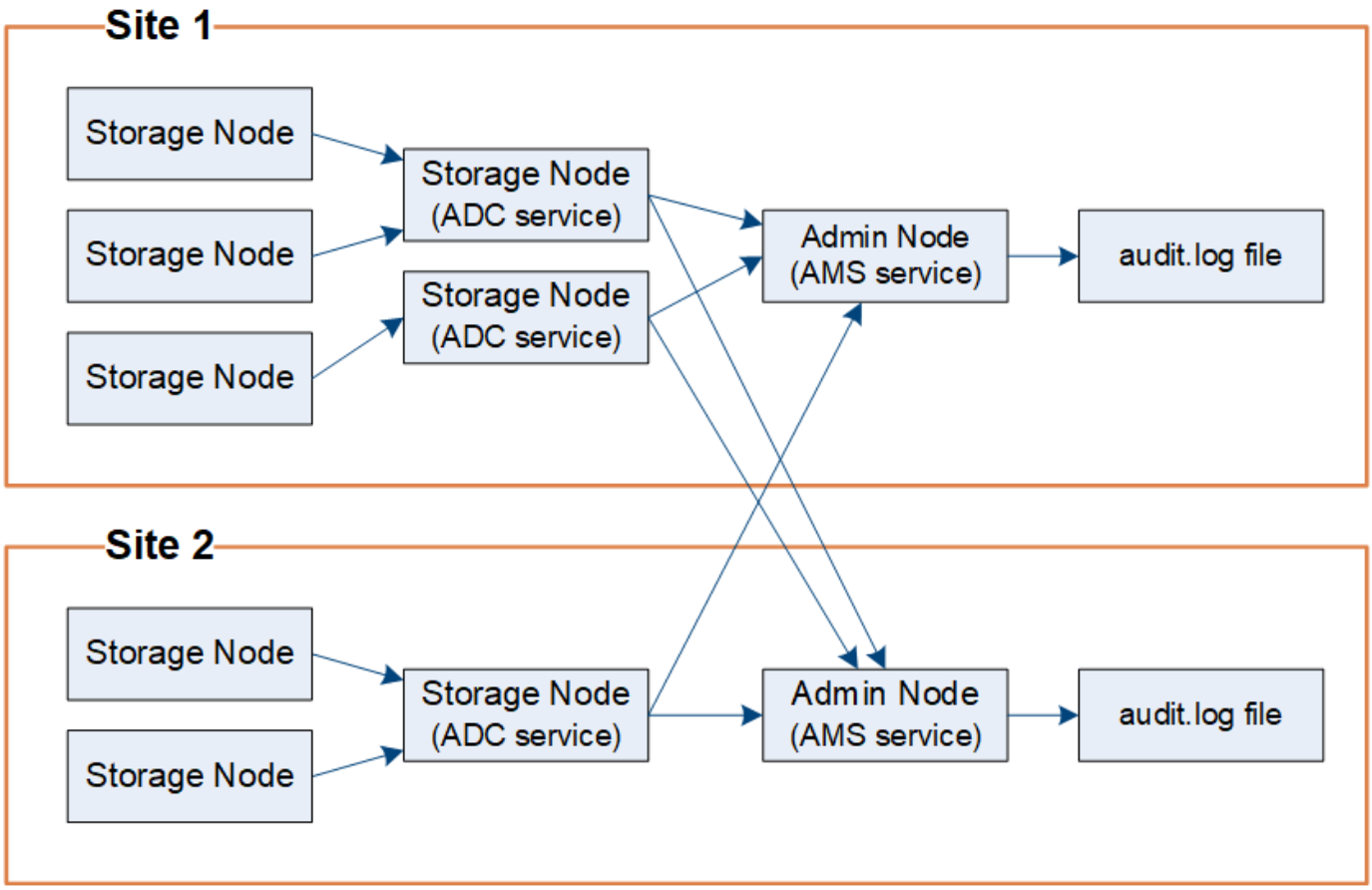
审核消息流

审核消息由管理节点以及具有管理域控制器（ ADO ）服务的存储节点处理。

如审核消息流程图所示，每个 StorageGRID 节点都会将其审核消息发送到数据中心站点的一个模板服务。每个站点上安装的前三个存储节点会自动启用此 ADC-Service 。

反过来，每个 ADC 服务都充当中继，并将其审核消息集合发送到 StorageGRID 系统中的每个管理节点，从而为每个管理节点提供完整的系统活动记录。

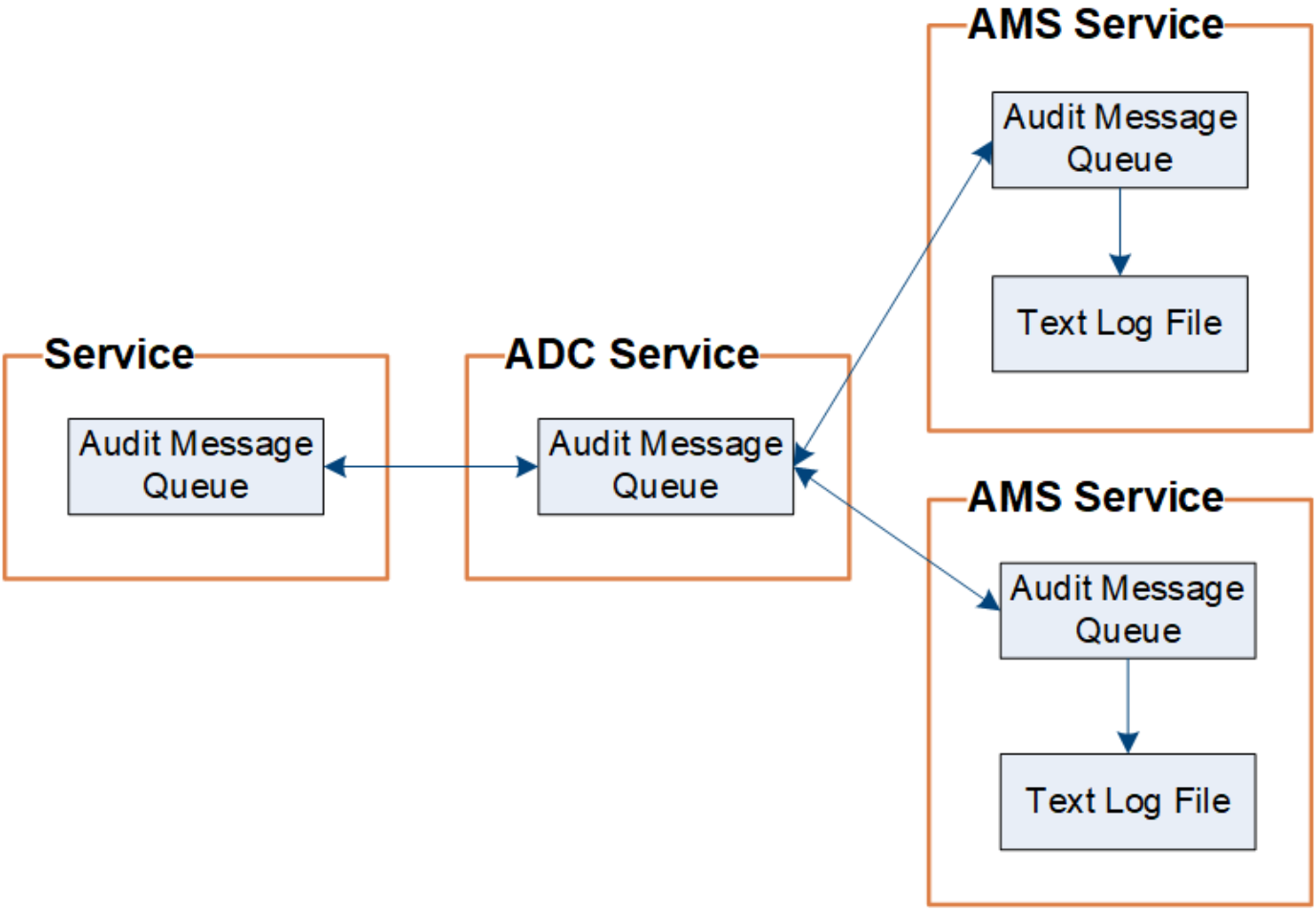
每个管理节点都会将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log` 。



审核消息保留

StorageGRID 使用复制和删除过程来确保在将审核消息写入审核日志之前不会丢失任何审核消息。

当节点生成或转发审核消息时，此消息会存储在网格节点的系统磁盘上的审核消息队列中。此消息的副本始终保留在审核消息队列中，直到将此消息写入管理节点的 ` /var/local/audit/export` 目录中的审核日志文件为止。这有助于防止传输期间丢失审核消息。



由于网络连接问题或审核容量不足，审核消息队列可能会暂时增加。随着队列的增加，它们会占用每个节点的 ` /var/local/` 目录中更多的可用空间。如果问题描述 仍然存在，并且节点的审核消息目录过满，则各个节点将优先处理其积压工作，并暂时不可用于处理新消息。

具体来说，您可能会看到以下行为：

- 如果管理节点使用的 ` /var/local/audit/export` 目录已满，则管理节点将标记为不可用于新的审核消息，直到目录不再全满为止。S3 和 Swift 客户端请求不受影响。如果无法访问审核存储库，则会触发 XAMS （无法访问审核存储库）警报。
- 如果具有` 服务的存储节点使用的 ` /var/local/ 目录已满 92% ，则该节点将标记为不可用于审核消息，直到该目录仅已满 87% 为止。对其他节点的 S3 和 Swift 客户端请求不受影响。如果无法访问审核中继，则会触发 NRLY （可用审核中继）警报。

> 如果没有可用于此` 服务的存储节点，则存储节点会将审核消息本地存储在 ` /var/local/log/localaudit.log 文件中。

- 如果存储节点使用的 ` /var/local/` 目录已满 85% ，则该节点将开始拒绝服务不可用` 为 `503 的 S3 和 Swift 客户端请求。

以下类型的问题可能会使发生原因 审核消息队列变得非常庞大：

- 管理节点或存储节点使用 ADC-Service 中断的情况。如果系统的一个节点已关闭，则其余节点可能会回记录。

- 超过系统审核容量的持续活动率。
- 由于与审核消息无关的原因，` 存储节点上的 ` /var/local/ 空间已满。发生这种情况时，节点将停止接受新的审核消息，并优先处理当前的积压工作，而这可能会使发生原因 回退到其他节点上。

大型审核队列警报和审核消息已排队（ **Audit Messages Queued** ， **AMQS** ）警报

为了帮助您监控一段时间内审核消息队列的大小，当存储节点队列或管理节点队列中的消息数量达到特定阈值时，将触发 * 大型审核队列 * 警报和原有 AMQS 警报。

如果触发了 * 大型审核队列 * 警报或原有 AMQS 警报，请首先检查系统上的负载—如果最近发生了大量事务，则警报和警报应随着时间的推移而解决，并且可以忽略。

如果警报或警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将客户端写入和客户端读取的审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 "配置审核消息和日志目标。 "

重复的消息

如果发生网络或节点故障， StorageGRID 系统会采取保守的方法。因此，审核日志中可能存在重复的消息。

访问审核日志文件

审核共享包含活动的 `audit.log` 文件和任何压缩的审核日志文件。为了便于访问审核日志，您可以配置客户端对 NFS 和 CIFS 的审核共享的访问权限（ CIFS 已弃用）。您也可以直接从管理节点的命令行访问审核日志文件。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。
- 您必须知道管理节点的 IP 地址。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 转到包含审核日志文件的目录：

```
cd /var/local/audit/export
```

3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

相关信息

管理 StorageGRID

审核日志文件轮换

审核日志文件会保存到管理节点的 ` /var/local/audit/export` 目录中。活动的审核日志文件

名为 `audit.log` 。

> 您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

每天保存一次活动的 `audit.log` 文件，并启动一个新的 `audit.log` 文件。已保存文件的名称以 ` yyyy-mm-dd.txt_` 的格式指示其保存时间。如果在一天内创建了多个审核日志，则文件名将使用保存文件的日期，并附加一个数字，格式为 ` yyyy-mm-dd.txt.n_` 。例如， `2018-04-15.txt` 和 `2018-04-15.txt.1` 是在 2018 年 4 月 15 日创建并保存的第一个和第二个日志文件。

一天后，保存的文件将按 ` yyyy-mm-dd.txt.gz_` 格式进行压缩和重命名，从而保留原始日期。随着时间的推移，这会导致为管理节点上的审核日志分配的存储被占用。脚本可监控审核日志空间占用情况，并根据需要删除日志文件，以释放 ` /var/local/audit/export` 目录中的空间。审核日志会根据创建日期进行删除，最早的日志会先删除。您可以在以下文件中监控脚本的操作： ` /var/local/log/manage-audit.log` 。

此示例显示了活动的 `audit.log` 文件，前一天的文件（ `2018-04-15.txt` ）和前一天的压缩文件（ `2018-04-14.txt.gz` ）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

审核日志文件和消息格式

您可以使用审核日志收集有关系统的信息并对问题进行故障排除。您应了解审核日志文件的格式以及审核消息使用的常规格式。

审核日志文件格式

审核日志文件位于每个管理节点上，其中包含一组单独的审核消息。

每个审核消息都包含以下内容：

- 触发审核消息（ ATIM ）的事件的协调世界时（ UTC ），格式为 ISO 8601 ，后跟一个空格：

  ` YYYY-MM-DDTHH： MM： SS.UUUUUUU_` ，其中 ` *UUUU*` 为微秒。

- 审核消息本身，括在方括号内，以 `AUDT` 开头。

以下示例显示了一个审核日志文件中的三条审核消息（为便于阅读，添加了换行符）。这些消息是在租户创建 S3 存储分段并向该存储分段添加两个对象时生成的。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

以默认格式，审核日志文件中的审核消息不易阅读或解释。您可以使用 `audit-explain` 工具获取审核日志中审核消息的简化摘要。您可以使用 `audit-sum` 工具总结已记录的写入，读取和删除操作的数量以及这些操作所需的时间。

相关信息

使用审核解释工具

使用 audit-sum 工具

您可以使用 audit-explain 工具将审核日志中的审核消息转换为易于阅读的格式。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 passwords.txt 文件。
- 您必须知道主管理节点的 IP 地址。

关于此任务

主管理节点上提供的 audit-explain 工具可在审核日志中简化审核消息的摘要。

audit-explain 工具主要供技术支持在故障排除操作期间使用。处理 审核 - 解释 查询可能会占用大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 audit-explain 工具的典型输出。当帐户 ID 为 92484777680322627870 的 S3 租户使用 S3 PUT 请求创建名为 "Bucket1" 的存储分段并向该存储分段添加三个对象时，会生成这四条 SPUT 审核消息。

```
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
```

audit-explain 工具可以处理简单或压缩的审核日志。例如：

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

audit-explain 工具还可以同时处理多个文件。例如：

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

最后， audit-explain 工具可以接受来自管道的输入，这样，您可以使用 grep 命令或其他方法筛选和预处理输入。例如：

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

由于审核日志可能非常大且解析速度较慢，因此您可以通过筛选要查看的部分并在这些部分（而不是整个文件）上运行 `audit-explain` 来节省时间。

> `audit-explain` 工具不接受将压缩文件作为管道输入。要处理压缩的文件，请将其文件名作为命令行参数提供，或者使用 `zcat` 工具先解压缩这些文件。例如：

```
zcat audit.log.gz | audit-explain
```

使用 `help` （ `-h` ） 选项查看可用选项。例如：

```
$ audit-explain -h
```

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 输入以下命令，其中 ` /var/local/audit/export/audit.log` 表示要分析的一个或多个文件的名称和位置：

   ` $ audit-explain /var/local/audit/export/audit.log`

   `audit-explain` 工具可为指定文件中的所有消息输出可供用户读取的解释。

   > 为了缩短行长度并提高可读性，默认情况下不会显示时间戳。如果要查看时间戳，请使用 timestamp （` -t` ）选项。

相关信息

SPUT： S3 PUT

使用 **audit-sum** 工具

您可以使用 `audit-sum` 工具对写入，读取，标头和删除审核消息进行计数，并查看每种操作类型的最小，最大和平均时间（或大小）。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。

- 您必须知道主管理节点的 IP 地址。

关于此任务

主管理节点上提供的 `audit-sum` 工具总结了记录的写入，读取和删除操作数量以及这些操作所需的时间。

> `audit-sum` 工具主要供技术支持在故障排除操作期间使用。处理 `audit-sum` 查询可能会占用大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 `audit-sum` 工具的典型输出。此示例显示了协议操作所需的时间。

```
  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
```

`audit-sum` 工具可在审核日志中提供以下 S3 ， Swift 和 ILM 审核消息的计数和时间：

代码	**Description**	请参见
ARCT	从云层检索归档	ARCT ： 从云层检索归档
上一个月	归档存储云层	SCT ： 归档存储云层
标识	ILM Initiated Delete ： 记录 ILM 开始删除对象的过程。	idel ： ILM 已启动删除
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。	SDEL ： S3 delete
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。	SGET ： S3 GET
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	Shea ： S3 机头

代码	Description	请参见
SPUT	S3 PUT： 记录成功的事务以创建新对象或存储分段。	SPUT： S3 PUT
WDEL	Swift delete： 记录成功的事务以删除对象或容器。	WDEL： Swift delete
wget	Swift get： 记录成功的事务以检索对象或列出容器中的对象。	WGET： Swift GET
WHEA	Swift head： 记录成功的事务以检查是否存在对象或容器。	WHEA： Swift head
WWPUT	Swift PUT： 记录成功的事务以创建新对象或容器。	WWPUT： Swift PUT

`audit-sum` 工具可以处理纯审核日志或压缩的审核日志。例如：

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

`audit-sum` 工具还可以同时处理多个文件。例如：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

最后， `audit-sum` 工具还可以接受来自管道的输入，这样，您可以使用 `grep` 命令或其他方法筛选和预处理输入。例如：

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

此工具不接受将压缩文件作为管道输入。要处理压缩的文件，请将其文件名作为命令行参数提供，或者使用 `zcat` 工具先解压缩这些文件。例如：

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

您可以使用命令行选项将存储分段上的操作与对象上的操作分开进行汇总，或者按存储分段名称，时间段或目标类型对消息摘要进行分组。默认情况下，摘要会显示最小，最大和平均操作时间，但您可以使用 `size` （ `-s` ） 选项查看对象大小。

使用 `help` （ `-h` ） 选项查看可用选项。例如：

```
 $ audit-sum -h
```

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 如果要分析与写入，读取，磁头和删除操作相关的所有消息，请执行以下步骤：
   a. 输入以下命令，其中 ` /var/local/audit/export/audit.log` 表示要分析的一个或多个文件的名称和位置：

   ```
   $ audit-sum /var/local/audit/export/audit.log
   ```

   此示例显示了 `audit-sum` 工具的典型输出。此示例显示了协议操作所需的时间。

   ```
     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
   ```

在此示例中， SGET （ S3 GET ）操作的平均速度最慢，为 1.13 秒，但 SGET 和 SPUT （ S3 PUT ）操作的最坏情况时间都较长，约为 1 ， 770 秒。

b. 要显示速度最慢的 10 个检索操作，请使用 grep 命令仅选择 SGET 消息，并添加较长的输出选项（` -l` ）以包含对象路径： `grep SGET audit.log ； audit-sum -l`

结果包括类型（对象或分段）和路径，您可以通过此类结果在审核日志中添加与这些特定对象相关的其他消息。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+ 在此示例输出中，您可以看到，三个最慢的 S3 GET 请求针对的是大小约为 5 GB 的对象，该大小远远大于其他对象。大容量导致最差情况检索时间较慢。

3. 如果要确定要将哪些大小的对象输入网格并从网格中检索到，请使用 size 选项（` -s` ）：

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

在此示例中， SPUT 的平均对象大小小于 2.5 MB ，但 SGET 的平均大小要大得多。SPUT 消息的数量远远高于 SGET 消息的数量，这表明大多数对象永远不会被检索到。

4. 如果要确定昨天的检索速度是否较慢：

   a. 在相应的审核日志上输入命令并使用 group-by-time 选项（` -gt` ），后跟时间段（例如 15M ， 1H ， 10S ）问题描述：

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

这些结果显示 S3 GET 流量在 06： 00 到 07： 00 之间达到高峰。这些时间的最大和平均时间也明显较高，并且不会随着数量的增加而逐渐增加。这表明容量已超出某个位置，可能是在网络中，也可能是在网格处理请求的能力中。

b. 要确定昨天每小时检索的对象大小，请在命令中添加 size 选项（` -s` ）：

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

这些结果表明，当整体检索流量达到最大值时，会发生一些非常大的检索。

c. 要查看更多详细信息，请使用 `audit-explain` 工具查看该时段的所有 SGET 操作：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

如果 grep 命令的输出应为多行，请添加 `less` 命令，以便一次显示一页（一个屏幕）的审核日志文件内容。

5. 如果要确定存储分段上的 SPUT 操作是否比对象的 SPUT 操作慢：

a. 首先使用 ` -go` 选项，该选项可分别对对象和存储分段操作的消息进行分组：

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

结果显示，存储分段的 SPUT 操作与对象的 SPUT 操作具有不同的性能特征。

b. 要确定哪些存储分段的 SPUT 操作最慢，请使用 ` -GB` 选项，该选项可按存储分段对消息进行分组：

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. 要确定哪些分段的 SPUT 对象大小最大，请使用 ` -GB` 和 ` -s` 选项：

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

相关信息

使用审核解释工具

审核消息格式

在 StorageGRID 系统中交换的审核消息包括所有消息通用的标准信息以及描述所报告事件或活动的特定内容。

如果 `audit-explain` 和 `audit-sum` 工具提供的摘要信息不足，请参阅本节了解所有审核消息的常规格式。

下面是可能显示在审核日志文件中的审核消息示例：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

每个审核消息都包含一个属性元素字符串。整个字符串用方括号（`[]` ）括起来，字符串中的每个属性元素都具有以下特征：

- 括在方括号中 `` .....
- 由字符串 `AUDT` 引入，表示审核消息
- 前后不带分隔符（无逗号或空格）
- 由换行符 ` n` 终止

每个元素都包含一个属性代码，一个数据类型以及一个以以下格式报告的值：

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

消息中的属性元素数量取决于消息的事件类型。属性元素不按任何特定顺序列出。

以下列表介绍了这些属性元素：

- `attr` 是所报告属性的四字符代码。某些属性对于所有审核消息都是通用的，而其他属性则针对事件。
- `type` 是值的编程数据类型的四字符标识符，例如 UI64 ， FC32 等。此类型用圆括号括起来 ` （） ` 。
- `value` 是属性的内容，通常为数字或文本值。值始终后跟冒号（ ` ： ` ）。数据类型 CStr 的值由双引号 ` " "` 括起来。

相关信息

使用审核解释工具

使用 audit-sum 工具

审核消息

审核消息中的常见元素

数据类型

审核消息示例

数据类型

使用不同的数据类型将信息存储在审核消息中。

Type	Description
UI32	无符号长整数（ 32 位）；它可以存储 0 到 4 ， 294 ， 967 ， 295 之间的数字。
UI64	无符号双长整数（ 64 位）；它可以存储 0 到 18 ， 446 ， 744 ， 073 ， 709 ， 551 ， 615 之间的数字。
FC32	四字符常量；一个 32 - 位无符号整数值，表示为四个 ASCII 字符，如 "ABCD" 。
iPad	用于 IP 地址。

Type	Description
CStr	一个长度可变的数组，由 UTF-8 - 字符组成。可以按照以下约定对字符进行转义： • 反斜杠为 \\ 。 • 回车符为 • 双引号为 " 。 • 换行符（新行）为 • 字符可以替换为其十六进制等效项（格式为 \xHH ，其中 HH 是表示该字符的十六进制值）。

事件专用数据

审核日志中的每个审核消息都会记录特定于系统事件的数据。

在用于标识消息本身的打开 ` [AUDT ： ` 容器之后，下一组属性将提供有关审核消息所述事件或操作的信息。以下示例突出显示了这些属性：

```
2018-12-05T08： 24： 45.921845 [AUTT： \[RSLT\ （ FC32\ ）： SUC\] \[ 时间 \ （ UI64\ ）：
11454\]\[SAIP\ （ IPAD\ ）： "10.224.0.100"\]\"S3AI\ （ C3CSST\" ）： "： "KST" （ S36599" ）：
```

`ATYP` 元素（在示例中加下划线）用于标识生成消息的事件。此示例消息包含 Shea 消息代码（ [ATYP （ FC32 ）： Shea] ），表示此消息是由成功的 S3 head 请求生成的。

相关信息

审核消息中的常见元素

审核消息

审核消息中的常见元素

所有审核消息都包含通用要素。

代码	Type	Description
在中	FC32	模块 ID ： 生成消息的模块 ID 的四个 - 字符标识符。这表示生成审核消息的代码段。
ANID	UI32	Node ID ： 分配给生成消息的服务的网格节点 ID 。在配置和安装 StorageGRID 系统时，系统会为每个服务分配一个唯一的标识符。无法更改此 ID 。

代码	Type	Description
ASE	UI64	审核会话标识符：在先前版本中，此元素表示在服务启动后初始化审核系统的时间。此时间值是自操作系统 Epoch （ 1970 年 1 月 1 日 00： 00： 00 UTC ）以来以微秒为单位测量的。 • 注： * 此元素已废弃，不再显示在审核消息中。
ASQN	UI64	序列计数：在先前版本中，对于网格节点（ ANID ）上生成的每个审核消息，此计数器会递增，并在服务重新启动时重置为零。 • 注： * 此元素已废弃，不再显示在审核消息中。
Atid	UI64	跟踪 ID ： 由单个事件触发的一组消息共享的标识符。
Atim	UI64	timestamp ： 生成触发审核消息的事件的时间，以操作系统 Epoch （ 1970 年 1 月 1 日 00： 00： 00 UTC ）之后的微秒为单位。请注意，用于将时间戳转换为本地日期和时间的大多数可用工具均以毫秒为基础。 可能需要对记录的时间戳进行舍入或截断。`audit.log` 文件中审核消息开头显示的人工 - 可读时间是 ISO 8601 格式的 ATIM 属性。日期和时间以 ` YYYY-MMDDDTHH： MM： SS.UUUUUUU_` 表示，其中 `T` 是一个文字字符串，用于指示日期时间段的开始。` UUUUUUU_` 为微秒。
ATYP	FC32	Event Type ： 所记录事件的四 - 字符标识符。这将控制消息的 " 有效负载 " 内容：包含的属性。
保护程序	UI32	version ： 审核消息的版本。随着 StorageGRID 软件的发展，新版本的服务可能会在审核报告中加入新功能。通过此字段，可以在 AMS 服务中实现向后兼容性，以处理来自旧版本服务的消息。
RSLT	FC32	result ： 事件，进程或事务的结果。如果与消息无关，则不会使用 none 而不是 SUC ，这样就不会意外筛选该消息。

审核消息示例

您可以在每个审核消息中找到详细信息。所有审核消息都使用相同的格式。

以下是可能出现在 `audit.log` 文件中的审核消息示例：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

审核消息包含有关所记录事件的信息以及有关审核消息本身的信息。

要确定审核消息记录的事件，请查找 ATYP 属性（突出显示在下方）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP\(FC32\):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性的值为 SPUT 。SPUT 表示 S3 PUT 事务，用于记录对象载入到存储分段的情况。

以下审核消息还会显示与对象关联的存储分段：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

要发现 PUT 事件发生的时间，请注意审核消息开头的通用协调时间（ UTC ）时间戳。此值为审核消息本身的 ATIM 属性的用户 - 可读版本：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

Atim 会以微秒为单位记录自 UNIX Epoch 开始以来的时间。在此示例中，值 `1405631878959669` 转换为 2014 年 7 月 17 日星期四 21： 17： 59 UTC 。

相关信息

SPUT： S3 PUT

审核消息中的常见元素

审核消息和对象生命周期

每次载入，检索或删除对象时都会生成审核消息。您可以通过查找特定于 API （ S3 或 Swift ）的审核消息在审核日志中标识这些事务。

审核消息通过每个协议专用的标识符进行链接。

协议	代码
链接 S3 操作	S3BK （ S3 分段）和 / 或 S3KY （ S3 密钥）
链接 Swift 操作	WCON （ Swift 容器）和 / 或 WOBJ （ Swift 对象）
链接内部操作	CBID （对象的内部标识符）

审核消息的时间

由于网格节点之间的时间差异，对象大小和网络延迟等因素，不同服务生成的审核消息的顺序可能与本节示例中所示的顺序不同。

信息生命周期管理策略配置

使用默认 ILM 策略（基线 2 副本），对象数据复制一次，总共复制两个副本。如果 ILM 策略需要两个以上的副本，则每个额外的副本还会另外显示一组 CBRE ， CBSE 和 SCMT 消息。有关 ILM 策略的详细信息，请参见有关通过信息生命周期管理管理对象的信息。

归档节点

归档节点向外部归档存储系统发送对象数据时生成的一系列审核消息与存储节点的类似，只是没有 SCMT （存储对象提交）消息。 对于对象数据的每个归档副本，系统会生成 ATCE （ Archive Object Store Begin ）和

ASCE （ Archive Object Store End ）消息。

归档节点从外部归档存储系统检索对象数据时生成的一系列审核消息与存储节点的类似，只是为每个检索到的对象数据副本生成了 ARCB （归档对象检索开始）和 Arce （归档对象检索结束）消息。

归档节点从外部归档存储系统删除对象数据时生成的一系列审核消息与存储节点的类似，只是没有 Srem （对象存储删除）消息，并且每个删除请求都有一条 AREM （归档对象删除）消息。

相关信息

使用 ILM 管理对象

对象载入事务

您可以通过查找特定于 API （ S3 或 Swift ）的审核消息，在审核日志中确定客户端载入事务。

下表列出了在载入事务期间生成的并非所有审核消息。仅包含跟踪载入事务所需的消息。

S3 载入审核消息

代码	**Name**	**Description**	跟踪	请参见
SPUT	S3 PUT 事务	S3 PUT 载入事务已成功完成。	CBID ， S3BK ， S3KY	SPUT ： S3 PUT
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	ORLM ： 符合对象规则

Swift 载入审核消息

代码	**Name**	**Description**	跟踪	请参见
WWPUT	Swift PUT 事务	Swift PUT 载入事务已成功完成。	CBID ， WCON ， WOBJ	WWPUT ： Swift PUT
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	ORLM ： 符合对象规则

示例： **S3** 对象载入

下面的一系列审核消息是在 S3 客户端将对象载入存储节点（ LDR 服务）时生成并保存到审核日志中的审核消息的示例。

在此示例中，活动 ILM 策略包括常用 ILM 规则，创建 2 个副本。

> 在以下示例中并未列出事务期间生成的所有审核消息。仅列出与 S3 载入事务（ SPUT ）相关的那些。

此示例假设先前已创建 S3 存储分段。

SPUT： S3 PUT

此时将生成 SPUT 消息，以指示已发出 S3 PUT 事务，以便在特定存储分段中创建对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][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： 符合对象规则

ORLM 消息指示已对此对象满足 ILM 策略要求。此消息包含对象的 CBID 以及应用的 ILM 规则的名称。

对于复制的对象， " LOC" 字段包含对象位置的 LDR 节点 ID 和卷 ID 。

```
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]]
```

对于经过纠删编码的对象， LOC 字段包括纠删编码配置文件 ID 和纠删编码组 ID

```
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]]
```

路径字段包括 S3 存储分段和密钥信息或 Swift 容器和对象信息，具体取决于所使用的 API 。

```
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]]
```

对象删除事务

您可以通过查找特定于 API （ S3 和 Swift ）的审核消息来确定审核日志中的对象删除事务。

下表列出了在删除事务期间生成的并非所有审核消息。仅包含跟踪删除事务所需的消息。

S3 删除审核消息

代码	Name	Description	跟踪	请参见
SDEL	S3 删除	请求从存储分段中删除对象。	CBID ， S3KY	SDEL： S3 delete

Swift 删除审核消息

代码	Name	Description	跟踪	请参见
WDEL	Swift 删除	请求从容器或容器中删除对象。	CBID ， WOBJ	WDEL： Swift delete

示例： **S3** 对象删除

当 S3 客户端从存储节点（ LDR 服务）中删除对象时，系统会生成一条审核消息并将其保存到审核日志中。

在删除事务期间生成的审核消息并非都在以下示例中列出。仅列出与 S3 删除事务（ SDEL ）相关的那些。

SDEL： S3 删除

当客户端向 LDR 服务发送删除对象请求时，对象删除即开始。此消息包含用于删除对象的存储分段以及用于标识对象的 S3 密钥。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[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]]
```

对象检索事务

您可以通过查找特定于 API （ S3 和 Swift ）的审核消息来确定审核日志中的对象检索事务。

下表列出了在检索事务期间生成的并非所有审核消息。仅包含跟踪检索事务所需的消息。

S3 检索审核消息

代码	Name	Description	跟踪	请参见
SGET	S3 GET	请求从存储分段中检索对象。	CBID ， S3BK ， S3KY	SGET： S3 GET

Swift 检索审核消息

代码	Name	Description	跟踪	请参见
wget	Swift GET	请求从容器中检索对象。	CBID ， WCON ， WOBJ	WGET： Swift GET

示例： **S3** 对象检索

当 S3 客户端从存储节点（ LDR 服务）检索对象时，系统会生成一条审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 检索事务（ SGET ）相关的那些。

SGET： S3 GET

当客户端向 LDR 服务发送获取对象请求时，对象检索即开始。此消息包含用于检索对象的存储分段以及用于标识对象的 S3 密钥。

```
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]
]
```

如果存储分段策略允许，客户端可以匿名检索对象，或者从其他租户帐户拥有的存储分段中检索对象。审核消息包含有关存储分段所有者的租户帐户的信息，以便您可以跟踪这些匿名请求和跨帐户请求。

在以下示例消息中，客户端会为存储在非自有存储分段中的对象发送 GET 对象请求。SBAI 和 SBAC 的值会记录存储分段所有者的租户帐户 ID 和名称，这与 S3AI 和 SACC 中记录的租户帐户 ID 和客户端名称不同。

```
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]]
```

示例：对象上的 **S3 Select**

当 S3 客户端对某个对象发出 S3 Select 查询时，系统会生成审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 Select 事务（ SelectObjectContent ）相关的那些内容。

每个查询都会生成两条审核消息：一条用于执行 S3 Select 请求的授权（ S3SR 字段设置为 "Select" ），另一条用于在处理期间从存储中检索数据的后续标准 GET 操作。

```
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]]
```

元数据更新消息

当 S3 客户端更新对象的元数据时，系统会生成审核消息。

S3 元数据更新审核消息

代码	Name	Description	跟踪	请参见
SUPD	已更新 S3 元数据	当 S3 客户端更新已载入对象的元数据时生成。	CBID ， S3KY ， HTRH	SUPD ： 已更新 S3 元数据

示例： **S3** 元数据更新

此示例显示了更新现有 S3 对象的元数据的成功事务。

SUPD： S3 元数据更新

S3 客户端请求（ SUPD ）更新 S3 对象（ S3KY ）的指定元数据（`x-AMZ-meta-*` ）。在此示例中，请求标头包含在字段 HTRH 中，因为它已配置为审核协议标头（ "* 配置 ">"* 监控 ""><"* 审核和系统日志服务器 "* ）。

```
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]]
```

相关信息

配置审核消息和日志目标

审核消息

以下各节列出了系统返回的审核消息的详细说明。每个审核消息首先列在一个表中，该表按相关消息所代表的活动类别对相关消息进行分组。这些分组对于了解要审核的活动类型以及选择所需的审核消息筛选类型都很有用。

审核消息也会按其四个字符的代码的字母顺序列出。此字母列表可用于查找有关特定消息的信息。

本章中使用的四字符代码是审核消息中的 ATYP 值，如以下示例消息所示：

```
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]]
```

有关设置审核消息级别，更改日志目标以及使用外部系统日志服务器获取审核信息的信息，请参见 配置审核消

息和日志目标

审核消息类别

您应熟悉对审核消息进行分组的各个类别。这些组将根据消息表示的活动类别进行组织。

系统审核消息

您应熟悉属于系统审核类别的审核消息。这些事件与审核系统本身，网格节点状态，系统范围的任务活动（网格任务）和服务备份操作相关，可帮助您解决潜在问题。

代码	消息标题和问题描述	请参见
ECMC	缺少纠删编码数据片段：表示检测到缺少纠删编码数据片段。	ECMC ： 缺少擦除编码的数据片段
ECOC	Erasure 编码数据片段损坏：表示检测到擦除编码数据片段损坏。	EcC ： 擦除编码数据片段损坏
ETAF	安全身份验证失败：尝试使用传输层安全（ Transport Layer Security ， TLS ）进行连接失败。	ETAF ： 安全身份验证失败
GNRG	GNDS 注册：服务在 StorageGRID 系统中更新或注册了有关自身的信息。	GNRG ： GNDS 注册
GNUR	GNDS 注销：服务已从 StorageGRID 系统中注销自身。	GN-R ： GNDS 注销
GTED	网格任务已结束： CMN 服务已完成网格任务的处理。	GTed ： 网格任务已结束
GTSt	网格任务已启动： CMN 服务已开始处理网格任务。	GTST ： 已启动网格任务
GTSU	已提交网格任务：已将网格任务提交到 CMN 服务。	GTSU ： 已提交网格任务
标识	ILM Initiated Delete ： 当 ILM 开始删除对象的过程时，会生成此审核消息。	idel ： ILM 已启动删除
LKCU	已覆盖对象清理。自动删除已覆盖的对象以释放存储空间时会生成此审核消息。	LKCU ： 覆盖对象清理

代码	消息标题和问题描述	请参见
LLST	Location Lost ： 当某个位置丢失时，会生成此审核消息。	LLST ： 位置丢失
OLST	对象丢失：无法在 StorageGRID 系统中找到请求的对象。	OLST ： 系统检测到丢失对象
ORLM	满足对象规则：对象数据按照 ILM 规则的指定进行存储。	ORLM ： 符合对象规则
Sadd	禁用安全审核：已关闭审核消息日志记录。	Sadd ： 禁用安全审核
Sade	启用安全审核：审核消息日志记录已还原。	Sade ： 启用安全审核
SVRF	对象存储验证失败：内容块验证检查失败。	SVRF ： 对象存储验证失败
SVRU	对象存储验证未知：在对象存储中检测到意外的对象数据。	SVRU ： 对象存储验证未知
系统	节点停止：已请求关闭。	SYSD ： 节点停止
系统	节点停止：服务已正常停止。	Syst ： 节点正在停止
系统	节点启动：服务已启动；消息中显示了上次关闭的性质。	SYSU ： 节点启动
VLST	User Initiated Volume Lost ： 已运行 ` /proc/CMSI/Volume_Lost` 命令。	VLST ： 用户启动的卷丢失

相关信息

LKCU ： 覆盖对象清理

对象存储审核消息

您应熟悉属于对象存储审核类别的审核消息。这些事件与 StorageGRID 系统中对象的存储和管理相关。其中包括对象存储和检索，网格节点到网格节点的传输以及验证。

代码	Description	请参见
APCT	从云层清除归档：已归档的对象数据将从外部归档存储系统中删除，该系统通过 S3 API 连接到 StorageGRID 。	APCT ： 从云层清除归档
ARCB	归档对象检索开始： ARC-Service 开始从外部归档存储系统检索对象数据。	ARCB ： 开始归档对象检索
Arce	归档对象检索结束：对象数据已从外部归档存储系统中检索，并且 ARC-Service 会报告检索操作的状态。	Arce ： 归档对象检索结束
ARCT	从云层检索归档：归档对象数据从外部归档存储系统中检索，该系统通过 S3 API 连接到 StorageGRID 。	ARCT ： 从云层检索归档
AREM	归档对象删除：已从外部归档存储系统成功或未成功删除内容块。	AREM ： 归档对象删除
ASCE	归档对象存储结束：已将内容块写入外部归档存储系统，并且 ARC-Service 会报告写入操作的状态。	ASCE ： 归档对象存储结束
上一个月	归档存储云层：对象数据存储到外部归档存储系统，该系统通过 S3 API 连接到 StorageGRID 。	SCT ： 归档存储云层
ATCE	归档对象存储开始：已开始向外部归档存储写入内容块。	ATCE ： 开始归档对象存储
AVCC	归档验证云层配置：提供的帐户和存储分段设置已成功验证或未成功验证。	AVCC ： 归档验证云层配置
CBSE	对象发送结束：源实体完成了网格节点到网格节点的数据传输操作。	CBSE ： 对象发送结束
CBRE	对象接收结束：目标实体完成了网格节点到网格节点的数据传输操作。	CBRE ： 对象接收结束
SCMT	对象存储提交：内容块已完全存储和验证，现在可以请求。	SCMT ： 对象存储提交

代码	Description	请参见
Srem	对象存储删除：已从网格节点中删除内容块，无法再直接请求。	Srem ： 对象存储删除

客户端读取审核消息

当 S3 或 Swift 客户端应用程序请求检索对象时，系统会记录客户端读取审核消息。

代码	Description	使用人	请参见
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	SGET ： S3 GET
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	S3 客户端	Shea ： S3 机头
wget	Swift get ： 记录成功的事务以检索对象或列出容器中的对象。	Swift 客户端	WGET ： Swift GET
WHEA	Swift head ： 记录成功的事务以检查是否存在对象或容器。	Swift 客户端	WHEA ： Swift head

客户端写入审核消息

当 S3 或 Swift 客户端应用程序请求创建或修改对象时，系统会记录客户端写入审核消息。

代码	Description	使用人	请参见
OVWR	对象覆盖：记录一个事务，以便使用另一个对象覆盖一个对象。	S3 客户端 Swift 客户端	OVWR ： 对象覆盖

代码	Description	使用人	请参见
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	SDEL ： S3 delete
SPOS	S3 POST ： 记录将对象从 AWS Glacier 存储还原到云存储池的成功事务。	S3 客户端	SPOS ： S3 POST
SPUT	S3 PUT ： 记录成功的事务以创建新对象或存储分段。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	SPUT ： S3 PUT
SUPD	S3 元数据已更新：记录成功的事务以更新现有对象或存储分段的元数据。	S3 客户端	SUPD ： 已更新 S3 元数据
WDEL	Swift delete ： 记录成功的事务以删除对象或容器。	Swift 客户端	WDEL ： Swift delete
WWPUT	Swift PUT ： 记录成功的事务以创建新对象或容器。	Swift 客户端	WWPUT ： Swift PUT

管理审核消息

" 管理 " 类别可将用户请求记录到管理 API 。

代码	消息标题和问题描述	请参见
MGAU	Management API 审核消息：用户请求日志。	MGAU ： 管理审核消息

审核消息参考

APCT ： 从云层清除归档

从通过 S3 API 连接到 StorageGRID 的外部归档存储系统中删除归档对象数据时会生成此

消息。

代码	字段	Description
CBID	内容块 ID	已删除的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。始终返回 0 。
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	从中删除对象的云层的唯一标识符（ UUID ）。

ARCB ： 开始归档对象检索

在请求检索归档的对象数据且检索过程开始时会生成此消息。检索请求会立即处理，但可以重新排序，以提高从磁带等线性介质检索的效率。

代码	字段	Description
CBID	内容块 ID	要从外部归档存储系统检索的内容块的唯一标识符。
RSLT	结果	指示启动归档检索过程的结果。当前定义的值为： suC ： 已收到内容请求并排队等待检索。

此审核消息用于标记归档检索的时间。通过该选项，您可以将该消息与相应的 Arce End 消息进行匹配，以确定归档检索的持续时间以及操作是否成功。

Arce ： 归档对象检索结束

当归档节点尝试从外部归档存储系统检索对象数据时，将生成此消息。如果成功，则此消息指示已从归档位置完全读取请求的对象数据，并已成功验证。检索并验证对象数据后，这些数据将传送到请求服务。

代码	字段	Description
CBID	内容块 ID	要从外部归档存储系统检索的内容块的唯一标识符。
VLID	卷标识符	归档数据的卷的标识符。如果未找到内容的归档位置，则返回卷 ID 0 。

代码	字段	Description
RSLT	检索结果	归档检索过程的完成状态： • SUC ： 成功 • VRFL ： 失败（对象验证失败） • Arun ： 失败（外部归档存储系统不可用） • 取消：失败（已取消检索操作） • GERR ： 失败（一般错误）

将此消息与相应的 ARCB 消息进行匹配可以指示执行归档检索所需的时间。此消息指示检索是否成功，如果失败，则指示检索内容块失败的发生原因 。

ARCT ： 从云层检索归档

从通过 S3 API 连接到 StorageGRID 的外部归档存储系统检索归档对象数据时会生成此消息。

代码	字段	Description
CBID	内容块 ID	已检索到的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。此值仅适用于成功检索。
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	外部归档存储系统的唯一标识符（ UUID ）。
时间	时间	请求的总处理时间，以微秒为单位。

AREM ： 归档对象删除

" 归档对象删除 " 审核消息指示已从归档节点成功删除内容块或未成功删除内容块。如果结果成功，则归档节点已成功通知外部归档存储系统 StorageGRID 已释放对象位置。对象是否从外部归档存储系统中删除取决于系统类型及其配置。

代码	字段	Description
CBID	内容块 ID	要从外部归档介质系统检索的内容块的唯一标识符。

代码	字段	Description
VLID	卷标识符	用于归档对象数据的卷的标识符。
RSLT	结果	归档删除过程的完成状态： • SUC ： 成功 • Arun ： 失败（外部归档存储系统不可用） • GERR ： 失败（一般错误）

ASCE ： 归档对象存储结束

此消息表示向外部归档存储系统写入内容块的操作已结束。

代码	字段	Description
CBID	内容块标识符	存储在外部归档存储系统上的内容块的标识符。
VLID	卷标识符	将对象数据写入到的归档卷的唯一标识符。
VRN	已启用验证	指示是否对内容块执行验证。当前定义的值为： • vena ： 已启用验证 • VDSA ： 已禁用验证
MCLS	管理类	一个字符串，用于标识内容块分配到的 TSM 管理类（如果适用）。
RSLT	结果	指示归档过程的结果。当前定义的值为： • SUC ： 成功（归档过程成功） • OFFL ： 失败（归档已脱机） • VRFL ： 失败（对象验证失败） • Arun ： 失败（外部归档存储系统不可用） • GERR ： 失败（一般错误）

此审核消息表示指定的内容块已写入外部归档存储系统。如果写入失败，则结果将提供有关故障发生位置的基本故障排除信息。有关归档故障的更多详细信息，请参见 StorageGRID 系统中的归档节点属性。

SCT： 归档存储云层

将归档对象数据存储到外部归档存储系统时会生成此消息，该系统通过 S3 API 连接到 StorageGRID 。

代码	字段	Description
CBID	内容块 ID	已检索到的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	存储内容的云层的唯一标识符（ UUID ）。
时间	时间	请求的总处理时间，以微秒为单位。

ATCE： 开始归档对象存储

此消息表示已开始向外部归档存储写入内容块。

代码	字段	Description
CBID	内容块 ID	要归档的内容块的唯一标识符。
VLID	卷标识符	将内容块写入到的卷的唯一标识符。如果操作失败，则返回卷 ID 0 。
RSLT	结果	指示内容块传输的结果。当前定义的值为： • SUC ： 成功（已成功存储内容块） • exis ： 忽略（内容块已存储） • ISFD ： 发生故障（磁盘空间不足） • ster ： 失败（存储 CBID 时出错） • OFFL ： 失败（归档已脱机） • GERR ： 失败（一般错误）

AVCC： 归档验证云层配置

验证 Cloud Tiering - Simple Storage Service （ S3 ）目标类型的配置设置时，会生成此消息。

代码	字段	Description
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	与要验证的外部归档存储系统关联的 UUID 。

CBRB： 对象接收开始

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，目标实体会发出此消息。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push： 发送实体请求传输操作。 Pull： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。
CTES	预期结束序列计数	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。

代码	字段	Description
RSLT	传输开始状态	传输开始时的状态： SUCS ： 已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从 " 开始序列计数 " 到 " 预期结束序列计数 " 请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

CBRE ： 对象接收结束

内容块从一个节点传输到另一个节点完成后，此消息将由目标实体发出。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。

代码	字段	Description
RSLT	传输结果	传输操作的结果（从发送实体的角度来看）： SUC ： 传输成功完成；已发送请求的所有序列计数。 CONL ： 传输期间连接丢失 CTMO： 建立或传输期间连接超时 UNDE ： 无法访问目标节点 ID CRPT ： 由于接收到损坏或无效的数据（可能表示发生篡改），传输已结束

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 " 。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

CBSB ： 对象发送开始

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，源实体会发出此消息。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。

代码	字段	Description
CTES	预期结束序列计数	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS ： 已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从 " 开始序列计数 " 到 " 预期结束序列计数 " 请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

CBSE ： 对象发送结束

在将内容块从一个节点传输到另一个节点后，源实体会发出此消息。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。

代码	字段	Description
RSLT	传输结果	传输操作的结果（从发送实体的角度来看）： SUC ： 传输成功完成；已发送请求的所有序列计数。 CONL ： 传输期间连接丢失 CTMO： 建立或传输期间连接超时 UNDE ： 无法访问目标节点 ID CRPT ： 由于接收到损坏或无效的数据（可能表示发生篡改），传输已结束

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 " 。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

ECMC ： 缺少擦除编码的数据片段

此审核消息指示系统检测到缺少经过纠删编码的数据片段。

代码	字段	Description
VCMC	VCS ID	包含缺少的块的 VCS 的名称。
MCID	区块 ID	缺少纠删编码片段的标识符。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

EcC ： 擦除编码数据片段损坏

此审核消息指示系统检测到经过纠删编码的数据片段已损坏。

代码	字段	Description
VCCO	VCS ID	包含损坏区块的 VCS 的名称。
VLID	卷 ID	包含损坏的纠删编码片段的 RangeDB 卷。

代码	字段	Description
CCID	区块 ID	已损坏的纠删编码片段的标识符。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

ETAF ： 安全身份验证失败

如果尝试使用传输层安全（ Transport Layer Security ， TLS ）进行连接失败，则会生成此消息。

代码	字段	Description
CNID	连接标识符	身份验证失败的 TCP/IP 连接的唯一系统标识符。
RID	用户身份	表示远程用户身份的服务相关标识符。
RSLT	原因代码	失败的原因： SCNI ： 安全连接建立失败。 CERM ： 证书缺失。 证书：证书无效。 cere ： 证书已过期。 CERR ： 证书已撤销。 CSGN ： 证书签名无效。 CSGU ： 证书签名者未知。 UCRM ： 缺少用户凭据。 UCRI ： 用户凭据无效。 UCRU ： 不允许使用用户凭据。 tout ： 身份验证超时。

在与使用 TLS 的安全服务建立连接后，系统会使用 TLS 配置文件和服务中内置的其他逻辑来验证远程实体的凭据。如果此身份验证因证书或凭据无效，意外或不允许而失败，则会记录审核消息。这样可以查询未经授权的访问尝试以及其他与安全相关的连接问题。

此消息可能是由于远程实体的配置不正确或尝试向系统提供无效或不允许的凭据而导致的。应监控此审核消息，以检测未经授权访问系统的尝试。

GNRG： GNDS 注册

如果某个服务在 StorageGRID 系统中更新或注册了有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	**Description**
RSLT	结果	更新请求的结果： • SUC： 成功 • SUNV： 服务不可用 • GERR： 其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID 。
GNTP	设备类型	网格节点的设备类型（例如 LDR 服务的 BLDR ）。
GNDV	设备型号版本	标识 DMDL 捆绑包中网格节点设备型号版本的字符串。
GNGP	组	网格节点所属的组（在链路成本和服务查询排名环境中）。
GNIA	IP 地址	网格节点的 IP 地址。

每当网格节点更新其在网格节点包中的条目时，都会生成此消息。

GN-R： GNDS 注销

如果某个服务已从 StorageGRID 系统中取消注册有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	**Description**
RSLT	结果	更新请求的结果： • SUC： 成功 • SUNV： 服务不可用 • GERR： 其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID 。

GTed： 网格任务已结束

此审核消息表示 CMN 服务已完成指定网格任务的处理，并已将此任务移至历史表。如果结果为 SUC ， ABRT 或 Rolf ，则会显示相应的 Grid Task Started 审核消息。其他结果表明，此网格任务的处理从未开始。

代码	字段	Description
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在整个生命周期内对网格任务进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	网格任务的最终状态结果： • SUC ： 已成功完成网格任务。 • ABRT ： 已中止网格任务，但未出现回滚错误。 • Rolf ： 网格任务已中止，无法完成回滚过程。 • 取消：用户在启动网格任务之前已取消此任务。 • expr ： 网格任务在启动之前已过期。 • IVLD ： 网格任务无效。 • auth ： 未授权网格任务。 • DUPL ： 网格任务被拒绝为重复项。

GTST： 已启动网格任务

此审核消息指示 CMN 服务已开始处理指定的网格任务。对于由内部网格任务提交服务启动并选择自动激活的网格任务，审核消息会紧跟在网格任务提交消息之后。对于提交到 "Pending" 表中的网格任务，用户启动网格任务时会生成此消息。

代码	字段	Description
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在任务的整个生命周期内对其进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	结果。此字段只有一个值： • SUC ： 已成功启动网格任务。

GTSU ： 已提交网格任务

此审核消息表示已将网格任务提交到 CMN 服务。

代码	字段	Description
SID	任务 ID	唯一标识生成的网格任务，并允许在整个生命周期内对该任务进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
TTYP	任务类型	网格任务的类型。
版本	任务版本	指示网格任务版本的数字。
TDSC	任务问题描述	网格任务的用户可读问题描述 。
VAT	在时间戳之后有效	网格任务最早有效的时间（从 1970 年 1 月 1 日开始的 UINT64 微秒 - UNIX 时间）。
Vbts	在时间戳之前有效	网格任务有效的最新时间（从 1970 年 1 月 1 日开始的 UINT64 微秒 - UNIX 时间）。

代码	字段	Description
TRC	源	任务源： • TXTB ： 网格任务是以签名文本块的形式通过 StorageGRID 系统提交的。 • 网格：网格任务是通过内部网格任务提交服务提交的。
ACTV	激活类型	激活类型： • Auto ： 已提交网格任务以自动激活。 • PEND ： 网格任务已提交到待定表中。这是 TXTB 源的唯一可能性。
RSLT	结果	提交结果： • SUC ： 已成功提交网格任务。 • fail ： 任务已直接移至历史表。

idel ： ILM 已启动删除

ILM 开始删除对象时会生成此消息。

在以下任一情况下都会生成 idel 消息：

- * 对于合规 S3 存储分段中的对象 * ： 当 ILM 开始自动删除对象的过程时，系统会生成此消息，因为该对象的保留期限已过期（假设已启用自动删除设置且已关闭合法保留）。
- * 用于不合规 S3 存储分段或 Swift 容器中的对象 * 。ILM 开始删除对象的过程时会生成此消息，因为活动 ILM 策略中的放置说明当前不适用于此对象。

代码	字段	Description
CBID	内容块标识符	对象的 CBID 。
CMPA	合规性：自动删除	仅适用于合规 S3 存储分段中的对象。0 （ false ）或 1 （ true ），指示合规对象在保留期限结束时是否应自动删除，除非分段处于合法保留状态。
Cmpl	合规性：法律保留	仅适用于合规 S3 存储分段中的对象。0 （ false ）或 1 （ true ），指示存储分段当前是否处于合法保留状态。
CMPR	合规性：保留期限	仅适用于合规 S3 存储分段中的对象。对象保留期限的长度，以分钟为单位。

代码	字段	Description
CTME	合规性：载入时间	仅适用于合规 S3 存储分段中的对象。对象的载入时间。您可以将保留期限（以分钟为单位）添加到此值，以确定何时可以从存储分段中删除对象。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID 。存储分段上的操作不包括此字段。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOC	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 "" 。 CLEC ： 对于经过纠删编码的对象，应用于对象数据的纠删编码配置文件 ID 和纠删编码组 ID 。 CLDI ： 对于复制的对象， LDR 节点 ID 和对象位置的卷 ID 。 CLNL ： 归档对象数据时对象位置的弧节点 ID 。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	ILM 操作的结果。 SUC ： ILM 操作成功。
规则	规则标签	• 如果合规 S3 存储分段中的某个对象因其保留期限已过期而被自动删除，则此字段为空。 • 如果由于当前没有其他应用于对象的放置指令而删除对象，则此字段将显示应用于对象的最后一个 ILM 规则的可读标签。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

LKCU ： 覆盖对象清理

如果 StorageGRID 删除了先前需要清理以释放存储空间的已覆盖对象，则会生成此消息。当 S3 或 Swift 客户端将对象写入已包含对象的路径时，对象将被覆盖。删除过程会自动在后台进行。

代码	字段	Description
CSIZ	内容大小	对象的大小（以字节为单位）。
LTYP	清理类型	_ 仅供内部使用。 _
LUID	已删除对象 UUID	已删除的对象的标识符。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
SEGC	容器 UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
UUID	通用唯一标识符	仍存在的对象的标识符。只有在尚未删除对象时，此值才可用。

LLST： 位置丢失

如果找不到对象副本的位置（复制或擦除编码），则会生成此消息。

代码	字段	Description
CBIL	CBID	受影响的 CBID 。
NOID	源节点 ID	丢失位置的节点 ID 。
UUID	通用唯一 ID	StorageGRID 系统中受影响对象的标识符。
ECPR	纠删编码配置文件	用于经过擦除编码的对象数据。使用的擦除编码配置文件的 ID 。
LTYP	位置类型	CLDI （联机）：用于复制的对象数据 CLEC （联机）：用于经过纠删编码的对象数据 CLNL （近线）：用于归档复制的对象数据

代码	字段	Description
PCLD	复制对象的路径	丢失对象数据的磁盘位置的完整路径。仅当 LTYP 的值为 CLDI （即，对于复制的对象）时才返回。 采用 ` /var/local/rangedb/2/p/13/13/00oJs6X% ｛h ｛U） SeUFxE@` 的形式
RSLT	结果	始终为无。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。
TRC	触发源	User ： 用户触发 Syst ： 系统已触发

MGAU ： 管理审核消息

" 管理 " 类别可将用户请求记录到管理 API 。对于 API ，并非 GET 或 HEAD 请求的每个请求都会记录一个响应，其中包含 API 的用户名， IP 和请求类型。

代码	字段	Description
MDIP	目标 IP 地址	服务器（目标） IP 地址。
MDNA	域名	主机域名。
MPAT	请求路径	请求路径。
MPQP	请求查询参数	请求的查询参数。

代码	字段	Description
MRBD	请求正文	请求正文的内容。虽然默认情况下会记录响应正文，但在某些情况下，如果响应正文为空，则会记录请求正文。由于响应正文中不提供以下信息，因此会从以下 POST 方法的请求正文中获取这些信息： • * POST Authorize * 中的用户名和帐户 ID • * POST /grid/grid-networks/update* 中的新子网配置 • * POST /grid/ntp-servers/update* 中的新 NTP 服务器 • 已停用的服务器 ID 位于 * POST /grid/servers/decommission* 中 • 注： * 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。
MRmd	请求方法	HTTP 请求方法： • 发布 • PUT • 删除 • patch
MRSC	响应代码	响应代码。
MRSP	响应正文	默认情况下，系统会记录响应的内容（响应正文）。 • 注： * 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。
MSIP	源 IP 地址	客户端（源） IP 地址。
MUN	用户 URN	发送请求的用户的 URN （统一资源名称）。
RSLT	结果	返回成功（ SUC ）或后端报告的错误。

OLST： 系统检测到丢失对象

如果 DDS 服务在 StorageGRID 系统中找不到对象的任何副本，则会生成此消息。

代码	字段	Description
CBID	内容块标识符	丢失对象的 CBID 。
NOID	节点 ID	如果可用，则为丢失对象的最后一个已知直接位置或近线位置。如果卷信息不可用，则只能使用节点 ID 而不使用卷 ID 。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	如果可用，则为 S3 存储分段名称和 S3 密钥名称，或者 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。
UUID	通用唯一 ID	StorageGRID 系统中丢失对象的标识符。
卷	卷 ID	如果可用，则为丢失对象的最后一个已知位置的存储节点或归档节点的卷 ID 。

ORLM： 符合对象规则

如果对象已按照 ILM 规则的指定成功存储和复制，则会生成此消息。

如果策略中的另一条规则使用对象大小高级筛选器，则使用默认的 Make 2 Copies 规则成功存储对象时不会生成 ORLM 消息。

代码	字段	Description
BUID	存储分段标题	存储分段 ID 字段。用于内部操作。仅当统计数据为 PRGD 时才显示。
CBID	内容块标识符	对象的 CBID 。
CSIZ	内容大小	对象的大小（以字节为单位）。

代码	字段	Description
LOC	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 "" 。 CLEC ： 对于经过纠删编码的对象，应用于对象数据的纠删编码配置文件 ID 和纠删编码组 ID 。 CLDI ： 对于复制的对象， LDR 节点 ID 和对象位置的卷 ID 。 CLNL ： 归档对象数据时对象位置的弧节点 ID 。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	ILM 操作的结果。 SUC ： ILM 操作成功。
规则	规则标签	为应用于此对象的 ILM 规则提供的可读标签。
SEGC	容器 UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
SGCB	容器 CBID	已分段对象的容器的 CBID 。此值仅适用于已分段和多部分对象。
统计	Status	ILM 操作的状态。 Done ： 已完成对对象的 ILM 操作。 DDER ： 对象已标记为待未来 ILM 重新评估。 PRGD ： 此对象已从 StorageGRID 系统中删除。 NLOC ： 在 StorageGRID 系统中找不到对象数据。此状态可能表示对象数据的所有副本均缺失或已损坏。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

可以对单个对象多次发出 ORLM 审核消息。例如，每当发生以下事件之一时都会发出此消息：

- 对象的 ILM 规则将永久满足。
- 此 Epoch 已满足对象的 ILM 规则。
- ILM 规则已删除此对象。
- 后台验证过程检测到复制的对象数据的副本已损坏。StorageGRID 系统会执行 ILM 评估以替换损坏的对

象。

相关信息

- 对象载入事务
- 对象删除事务

OVWR：对象覆盖

如果外部（客户端请求的）操作导致一个对象被另一个对象覆盖，则会生成此消息。

代码	字段	Description
CBID	内容块标识符（新增）	新对象的 CBID 。
CSIZ	先前对象大小	要覆盖的对象的大小（以字节为单位）。
OCBD	内容块标识符（上一个）	上一个对象的 CBID 。
UUID	通用唯一 ID （新）	StorageGRID 系统中新对象的标识符。
OUID	通用唯一 ID （以前的）	StorageGRID 系统中上一个对象的标识符。
路径	S3 或 Swift 对象路径	用于上一个对象和新对象的 S3 或 Swift 对象路径
RSLT	结果代码	对象覆盖事务的结果。结果始终为： SUC ：成功
SGRP	站点（组）	如果存在此参数，则会在指定的站点上删除此覆盖对象，而不是在其中载入此覆盖对象的站点。

Sadd：禁用安全审核

此消息指示发起服务（节点 ID ）已关闭审核消息日志记录；不再收集或传送审核消息。

代码	字段	Description
AETM	启用方法	用于禁用审核的方法。
AEUN	用户名	执行命令以禁用审核日志记录的用户名。

代码	字段	Description
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。

此消息表示先前已启用日志记录，但现在已禁用。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，将还原审核（ SAade ），并永久阻止禁用审核的功能。

Sade ： 启用安全审核

此消息表示发起服务（节点 ID ）已还原审核消息日志记录；正在再次收集和传送审核消息。

代码	字段	Description
AETM	启用方法	用于启用审核的方法。
AEUN	用户名	执行命令以启用审核日志记录的用户名。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。

此消息表示先前已禁用日志记录（ Sadd ），但现在已还原。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，审核将恢复，而禁用审核的功能将被永久阻止。

SCMT ： 对象存储提交

网格内容在提交之前不可用或无法识别为已存储（这意味着它已持久存储）。持久存储的内容已完全写入磁盘，并已通过相关的完整性检查。将内容块提交到存储时会发出此消息。

代码	字段	Description
CBID	内容块标识符	提交到永久存储的内容块的唯一标识符。
RSLT	结果代码	将对象存储到磁盘时的状态： SUCS ： 对象已成功存储。

此消息表示给定内容块已完全存储和验证，现在可以请求。它可用于跟踪系统内的数据流。

SDEL： S3 delete

当 S3 客户端发出删除事务时，系统会请求删除指定的对象或存储分段。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID 。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	删除事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。

代码	字段	Description
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SGET： S3 GET

当 S3 客户端发出 GET 事务时，系统会请求检索对象或列出存储分段中的对象。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。

代码	字段	Description
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
已振铃	范围读取	仅适用于范围读取操作。指示此请求读取的字节数范围。斜杠（ / ）后面的值显示整个对象的大小。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

Shea： S3 机头

当 S3 客户端发出 HEAD 事务时，系统会请求检查是否存在对象或存储分段，并检索有关对象的元数据。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检查对象的大小（以字节为单位）。存储分段上的操作不包括此字段。

代码	字段	Description
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。

代码	字段	Description
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SPOS： S3 POST

当 S3 客户端发出 POST 对象请求时，如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	POST 对象还原请求的结果。结果始终为： SUC ： 成功

代码	字段	Description
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。 对于 S3 Select 操作，设置为 `select` 。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SRCF	子资源配置	还原信息。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。

代码	字段	Description
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SPUT： S3 PUT

当 S3 客户端发出 PUT 事务时，系统会请求创建新对象或存储分段。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CMPS	合规性设置	创建存储分段时使用的合规性设置（如果 PUT 存储分段请求中存在）（截断为前 1024 个字符）
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。

代码	字段	Description
LKEN	对象锁定已启用	请求标题 `x-AMZ-bucket-object-lock-enabled` 的值（如果 PUT Bucket 请求中存在）。
LKLH	对象锁定合法保留	请求标题 `x-AMZ-object-lock-legal-hold` 的值（如果 PUT 对象请求中存在）。
LKMD	对象锁定保留模式	请求标题 `x-AMZ-object-lock-mode` 的值（如果 PUT 对象请求中存在）。
LKRU	对象锁定保留至日期	请求标题 `x-AMZ-object-lock-retain-until date` 的值（如果 PUT 对象请求中存在）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3KY	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SRCF	子资源配置	新的子资源配置（截断为前 1024 个字符）。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
ULID	上传 ID	仅包含在用于完成多部件上传操作的 SPUT 消息中。表示所有部件均已上传和组装。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在受版本控制的存储分段中创建的新对象的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。
VSST	版本控制状态	存储分段的新版本控制状态。使用两种状态： "enabled" 或 "suspended" 。 对对象执行的操作不包括此字段。

Srem ： 对象存储删除

从永久性存储中删除内容后会发出此消息，并且无法再通过常规 API 进行访问。

代码	字段	Description
CBID	内容块标识符	从永久存储中删除的内容块的唯一标识符。
RSLT	结果代码	指示内容删除操作的结果。唯一定义的值为： SUC ： 从永久性存储中删除的内容

此审核消息表示已从节点中删除给定内容块，无法再直接请求。此消息可用于跟踪系统中已删除内容的流。

SUPD ： 已更新 **S3** 元数据

当 S3 客户端更新所载入对象的元数据时， S3 API 会生成此消息。如果元数据更新成功，则服务器会发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	更新存储分段的合规性设置时，如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功

代码	字段	Description
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

代码	字段	Description
VSID	版本 ID	已更新其元数据的对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SVRF ： 对象存储验证失败

每当内容块验证过程失败时，都会发出此消息。每次从磁盘读取或写入复制的对象数据时，都会执行多项验证和完整性检查，以确保发送给请求用户的数据与最初载入系统的数据完全相同。如果其中任何一项检查失败，系统会自动隔离损坏的复制对象数据，以防止再次检索该数据。

代码	字段	Description
CBID	内容块标识符	验证失败的内容块的唯一标识符。
RSLT	结果代码	验证失败类型： CRCF ： 循环冗余检查（ CRC ）失败。 HMAC ： 基于哈希的消息身份验证代码（ HMAC ）检查失败。 EHSH ： 意外的加密内容哈希。 PHSH ： 意外的原始内容哈希。 SEQC ： 磁盘上的数据顺序不正确。 PERR ： 磁盘文件的结构无效。 DERR ： 磁盘错误。 fnam ： 文件名错误。

- 注： * 应密切监控此消息。内容验证失败可能表示尝试篡改内容或即将发生的硬件故障。

要确定哪个操作触发了消息，请参见 amid （模块 ID ）字段的值。例如， SV财年 值表示消息是由存储验证程序模块生成的，即后台验证， STor 表示消息是通过内容检索触发的。

SVRU ： 对象存储验证未知

LDR 服务的存储组件会持续扫描对象存储中复制的对象数据的所有副本。如果在对象存储中检测到复制的对象数据的未知或意外副本并将其移动到隔离目录，则会发出此消息。

代码	字段	Description
FPTH	文件路径	意外对象副本的文件路径。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

- 注： * 应密切监控 SVRU： Object Store Verify Unknown 审核消息。这意味着在对象存储中检测到意外的对象数据副本。应立即调查这种情况，以确定这些副本是如何创建的，因为这可能表示尝试篡改内容或即将发生硬件故障。

SYSD： 节点停止

如果服务正常停止，则会生成此消息以指示已请求关闭。通常，只有在后续重新启动后才会发送此消息，因为在关闭之前未清除审核消息队列。如果服务未重新启动，请查找在关闭序列开始时发送的 SYST 消息。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC： 系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYSD 的 RSLT 不能指示 " 异常 " 关闭，因为只有 " 清理 " 关闭才会生成此消息。

Syst： 节点正在停止

如果服务正常停止，则会生成此消息，以指示已请求关闭，并且此服务已启动其关闭序列。Syst 可用于确定是否在重新启动服务之前请求关闭（与通常在服务重新启动后发送的 SYSD 不同）。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC： 系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYST 消息的 RSLT 代码不能指示 " 异常 " 关闭，因为只有 " 清理 " 关闭才会生成此消息。

SYSU： 节点启动

重新启动服务时，系统会生成此消息，以指示上次关闭是正常关闭（已发出命令）还是无序关闭（意外关闭）。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC ： 系统已完全关闭。 DSDN ： 系统未完全关闭。 VRGN ： 在安装（或重新安装）服务器后首次启动系统。

此消息不会指示是否已启动主机服务器，仅会指示报告服务。此消息可用于：

- 检测审核跟踪中的不连续性。
- 确定服务在运行期间是否出现故障（因为 StorageGRID 系统的分布式特征可能会掩盖这些故障）。Server Manager 会自动重新启动失败的服务。

VLST ： 用户启动的卷丢失

每当运行 ` /proc/CMSI/Volume_Lost` 命令时，都会发出此消息。

代码	字段	Description
VOLL	卷标识符下限	受影响卷范围的下端或单个卷。
VOLU	卷标识符上限	受影响卷范围的上限。如果只有一个卷，则等于 VOLL 。
NOID	源节点 ID	丢失位置的节点 ID 。
LTYP	位置类型	"CLDI" （联机）或 "CLNL" （近线）。如果未指定，则默认为 "CLDI" 。
RSLT	结果	始终为 " 无 " 。RSLT- 是一个必填消息字段，但与此消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

WDEL ： Swift delete

当 Swift 客户端发出删除事务时，系统会请求删除指定的对象或容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对容器执行的操作不包括此字段。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。对容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	删除事务的结果。结果始终为： SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。
WOBJ	Swift 对象	Swift 对象标识符。对容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WGET： Swift GET

当 Swift 客户端发出 GET 事务时，系统会请求检索对象，列出容器中的对象或列出帐户中的容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对帐户和容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对帐户和容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	GET 事务的结果。结果始终为 SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。对帐户执行的操作不包括此字段。
WOBJ	Swift 对象	Swift 对象标识符。对帐户和容器执行的操作不包括此字段。

代码	字段	Description
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WHEA： Swift head

当 Swift 客户端发出 HEAD 事务时，系统会请求检查是否存在帐户，容器或对象，并检索任何相关元数据。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对帐户和容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对帐户和容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	HEAD 事务的结果。结果始终为： SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

代码	字段	Description
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。对帐户执行的操作不包括此字段。
WOBJ	Swift 对象	Swift 对象标识符。对帐户和容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WWPUT： Swift PUT

当 Swift 客户端发出 PUT 事务时，系统会请求创建新的对象或容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。
WOBJ	Swift 对象	Swift 对象标识符。对容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

版权信息

版权所有 © 2023 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。