监控和故障排除
StorageGRID

NetApp
December 03, 2025

目录

监控StorageGRID系统并对其进行故障排除

监控StorageGRID 系统

监控StorageGRID 系统：概述

定期监控StorageGRID系统以确保其按预期运行。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

> 要更改网格管理器中显示的存储值的单位，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。

关于此任务

这些说明介绍了如何：

- "查看和管理信息板"
- "查看节点页面"
- "定期监控系统的以下方面："
  - "系统运行状况"
  - "存储容量"
  - "信息生命周期管理"
  - "网络和系统资源"
  - "租户活动"
  - "负载平衡操作"
  - "网格联合连接"
  - "归档容量"
- "管理警报和旧警报"
- "查看日志文件"
- "配置审核消息和日志目标"
- "使用外部系统日志服务器" 收集审核信息
- "使用SNMP进行监控"
- "获取其他StorageGRID数据"，包括度量和诊断

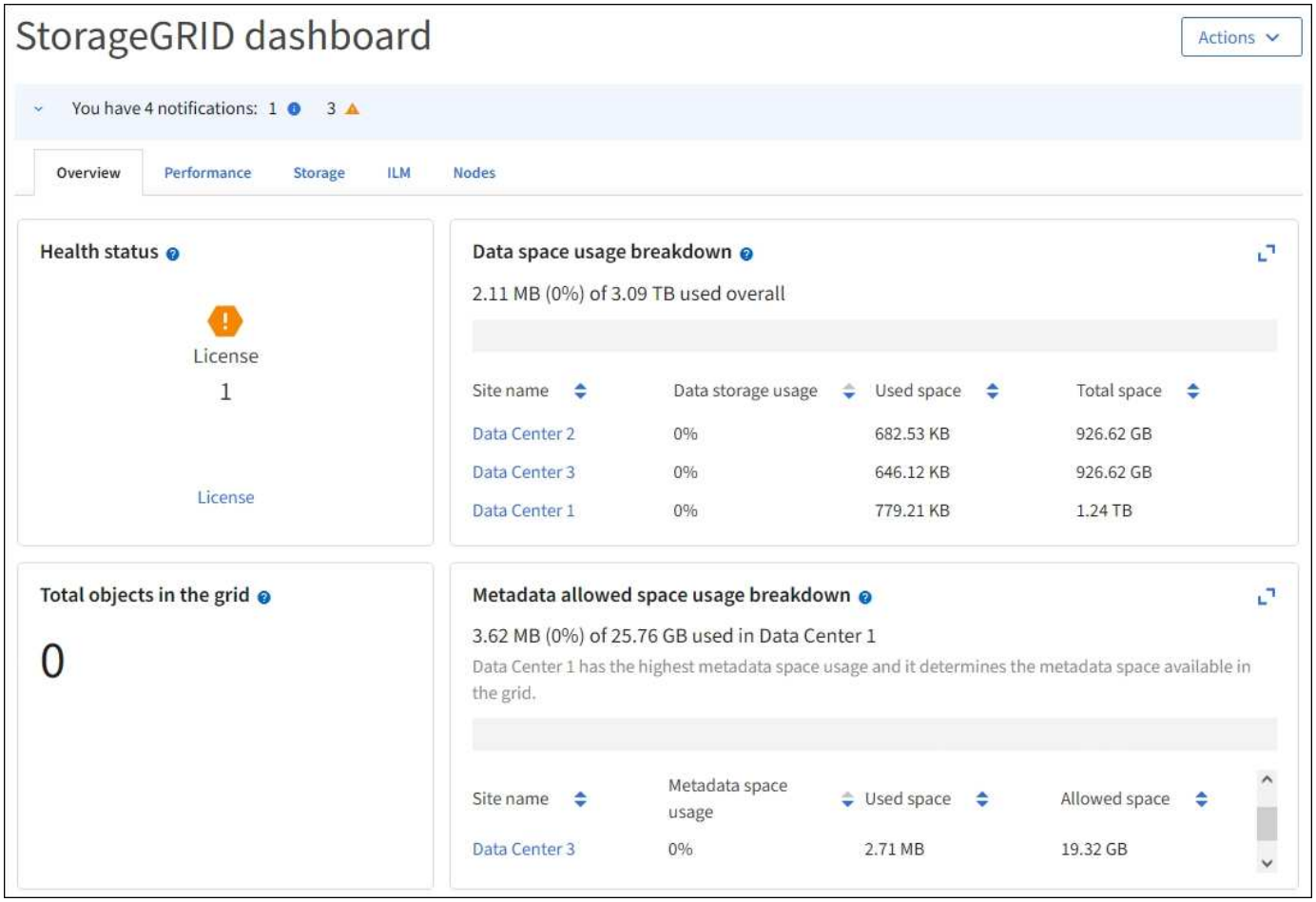
查看和管理信息板

您可以使用信息板一目了然地监控系统活动。您可以创建自定义信息板来监

控StorageGRID 的实施。

要更改网格管理器中显示的存储值的单位，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。

您的信息板可能会因系统配置而有所不同。



查看信息板

信息板包含多个选项卡、其中包含有关StorageGRID 系统的特定信息。每个选项卡都包含卡片上显示的信息类别。

您可以按原样使用系统提供的信息板。此外、您还可以创建仅包含与监控StorageGRID 实施相关的选项卡和卡片的自定义信息板。

系统提供的信息板选项卡包含具有以下类型信息的卡：

选项卡	包含
概述	有关网格的常规信息、例如活动警报、空间使用量和网格中的总对象数。
性能	空间使用量、一段时间内使用的存储、S3或Swift操作、请求持续时间、错误率。

选项卡	包含
存储	租户配额使用量和逻辑空间使用量。预测用户数据和元数据的空间使用量。
ILM	信息生命周期管理队列和评估率。
节点	按节点显示的CPU、数据和内存使用情况。按节点执行S3或Swift操作。节点到站点分布。

某些卡可以最大化、以便于查看。选择最大化图标 在卡的右上角。要关闭已最大化的卡，请选择最小化图标 或选择*关闭*。

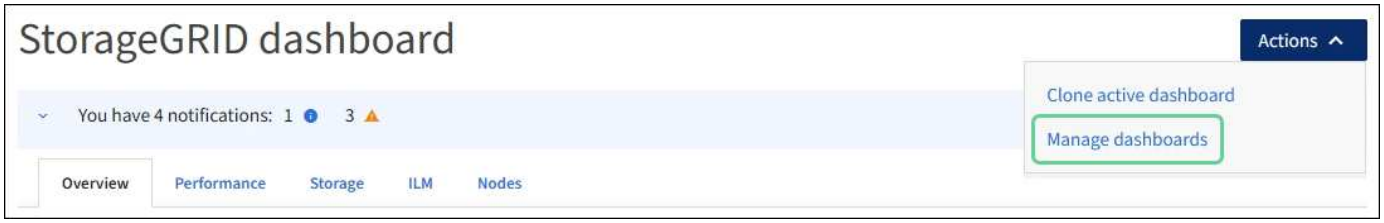
管理信息板

如果您具有root访问权限(请参见 "管理组权限")、则可以对信息板执行以下管理任务：

- 从头开始创建自定义信息板。您可以使用自定义信息板控制显示的StorageGRID 信息以及该信息的组织方式。
- 克隆信息板以创建自定义信息板。
- 为用户设置活动信息板。活动信息板可以是系统提供的信息板、也可以是自定义信息板。
- 设置默认信息板、除非用户激活自己的信息板、否则所有用户都会看到该信息板。
- 编辑信息板名称。
- 编辑信息板以添加或删除选项卡和卡。您至少可以有1个选项卡、最多可以有20个选项卡。
- 删除信息板。

如果您拥有除root访问权限之外的任何其他权限、则只能设置活动信息板。

要管理信息板，请选择*Actions*>*Manage Dards*。



配置信息板

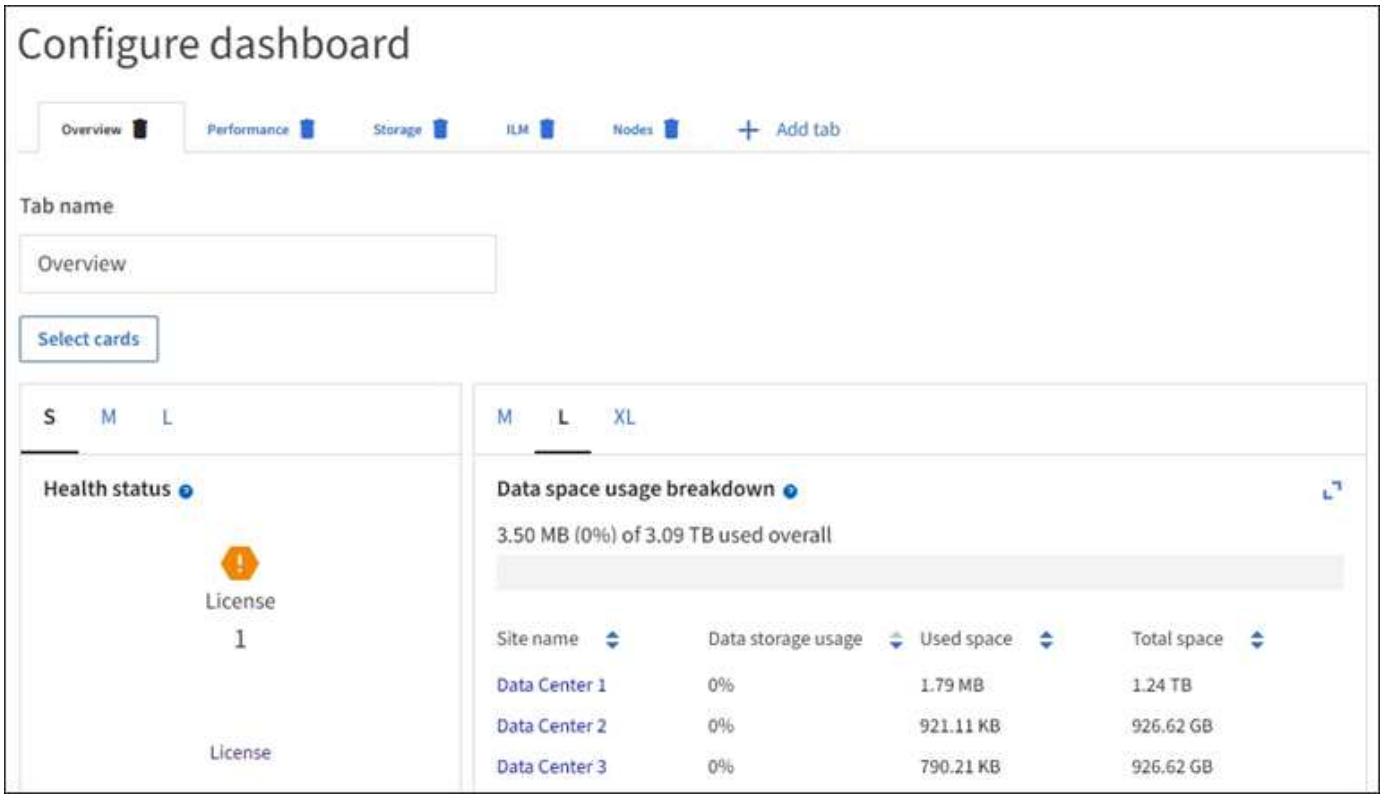
要通过克隆活动信息板来创建新信息板，请选择*Actions*>*Clone active DDashboard *。

要编辑或克隆现有信息板，请选择*Actions*>*Manage Dards*。

无法编辑或删除系统提供的信息板。

配置信息板时、您可以：

- 添加或删除选项卡
- 重命名选项卡并为新选项卡指定唯一名称
- 为每个选项卡添加、删除或重新排列(拖动)卡片
- 选择卡片顶部的*S*、**M**、**L***或***XL**，选择单张卡片的大小



查看节点页面

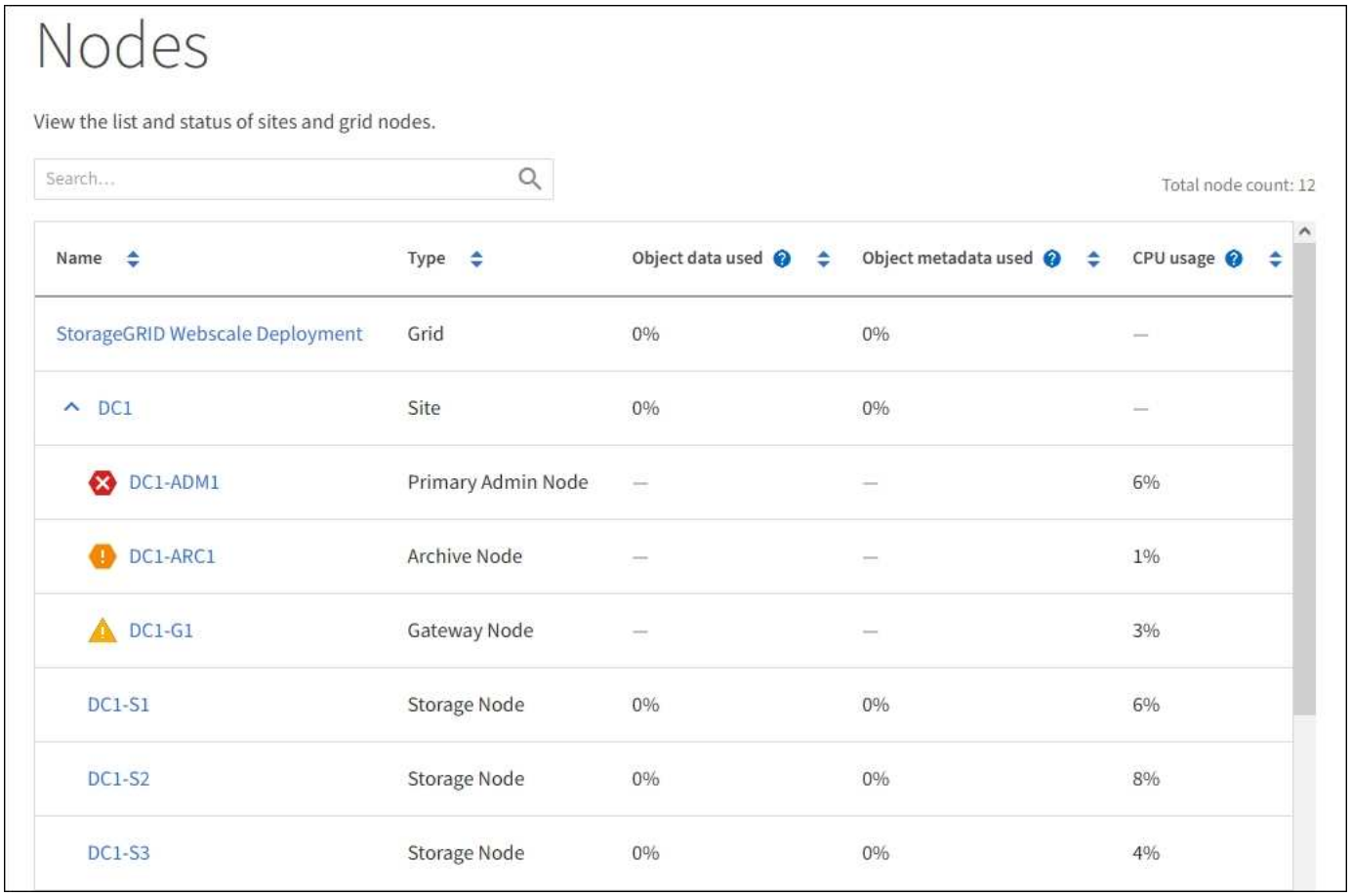
查看节点页面：**Overview**

如果您需要的StorageGRID 系统信息比信息板提供的信息更详细、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中的每个节点的指标。

节点表列出了整个网格、每个站点和每个节点的摘要信息。如果节点已断开连接或存在活动警报、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。

如果节点未连接到网格、例如在升级期间或处于断开状态时、某些指标可能不可用或不在站点和网格总数中。节点重新连接到网格后、请等待几分钟、使值稳定下来。

要更改网格管理器中显示的存储值的单位，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。



连接状态图标

如果节点与网格断开连接、则节点名称旁边会显示以下任一图标。

图标。	Description	需要执行操作
	• 未连接 - 未知 * 由于未知原因、节点已断开连接或节点上的服务意外关闭。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。 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。	需要立即关注。 "选择每个警报" 并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。 注意：在受管关闭操作期间，节点可能显示为未知。在这些情况下，您可以忽略未知状态。

图标。	Description	需要执行操作
	• 未连接 - 已管理员关闭 * 出于预期原因、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。 根据底层问题描述 、这些节点通常无需任何干预即可恢复联机。	确定是否有任何警报正在影响此节点。 如果一个或多个警报处于活动状态、 "选择每个警报" 并按照建议的操作进行操作。

如果节点与网格断开连接、则可能会出现底层警报、但仅会显示"未连接"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：存在异常情况、已停止StorageGRID 节点或服务的正常运行。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、可能会影响其运行能力。您应监控和解决无法自行清除的次要警报、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

要筛选节点表中显示的信息，请在*Search*字段中输入搜索字符串。您可以按系统名称、显示名称或类型进行搜索(例如，输入*gat*以快速查找所有网关节点)。

要查看网格、站点或节点的信息、请执行以下操作：

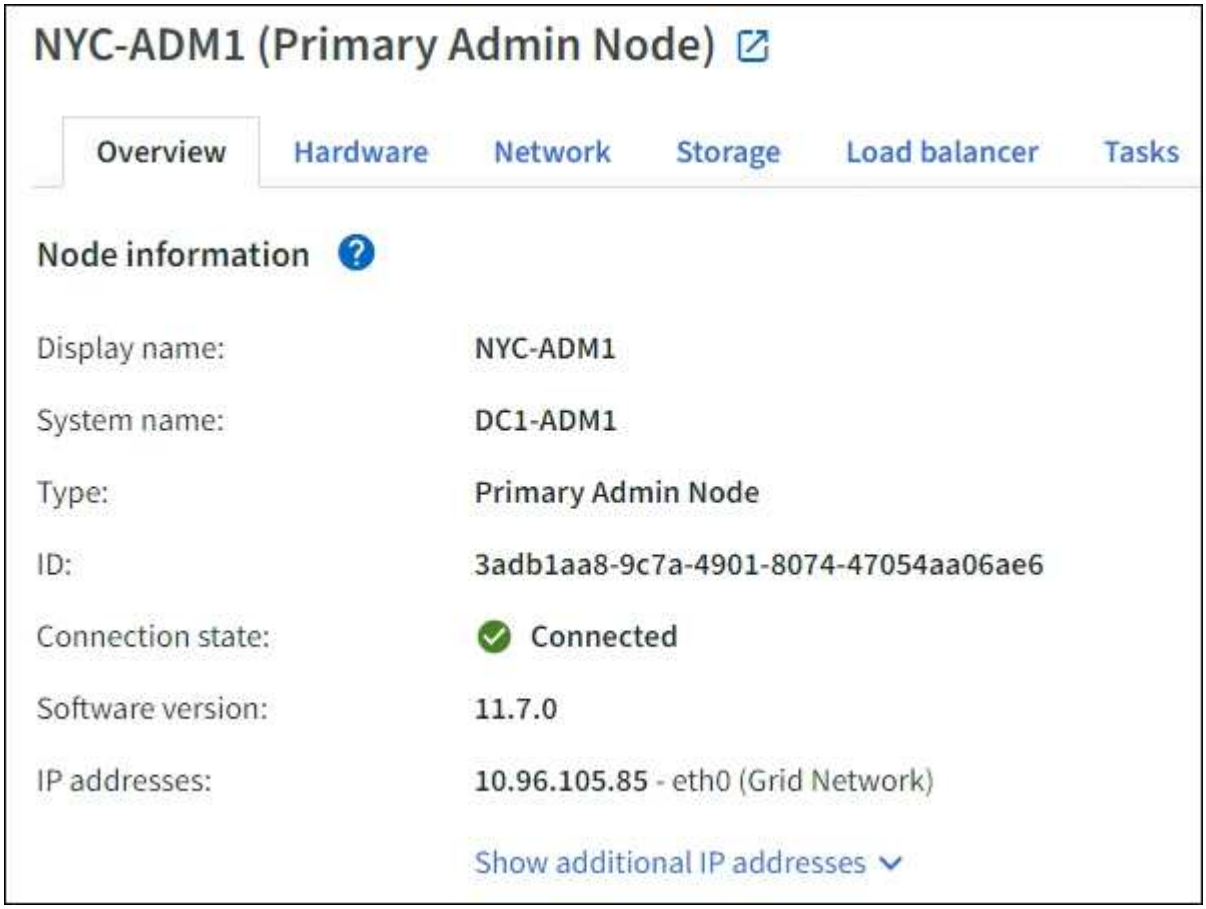
- 选择网格名称可查看整个 StorageGRID 系统统计信息的聚合摘要。
- 选择一个特定的数据中心站点，以查看该站点上所有节点的统计信息的聚合摘要。
- 选择一个特定节点以查看该节点的详细信息。

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。

概述选项卡的节点信息部分列出了有关节点的基本信息。



节点的概述信息包括：

- **Display name**(仅在节点已重命名时显示)：节点的当前显示名称。使用 "重命名网格、站点和节点" 操作步骤以更新此值。
- 系统名称：您在安装期间为节点输入的名称。系统名称用于内部StorageGRID 操作、无法更改。
- * 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。

  对归档节点的支持已弃用、将在未来版本中删除。通过 S3 API 将对象从归档节点移动到外部归档存储系统已被 ILM 云存储池所取代，它可提供更多功能。

- * 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 * ：由于未知原因，节点未连接到网格，或者一个或多个服务意外关闭。例如、节点之间的网络连接已断开、电源已关闭或服务已关闭。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"部分列出了任何 "当前影响此节点且尚未被禁止的警报"。选择警报名称可查看其他详细信息和建议的操作。

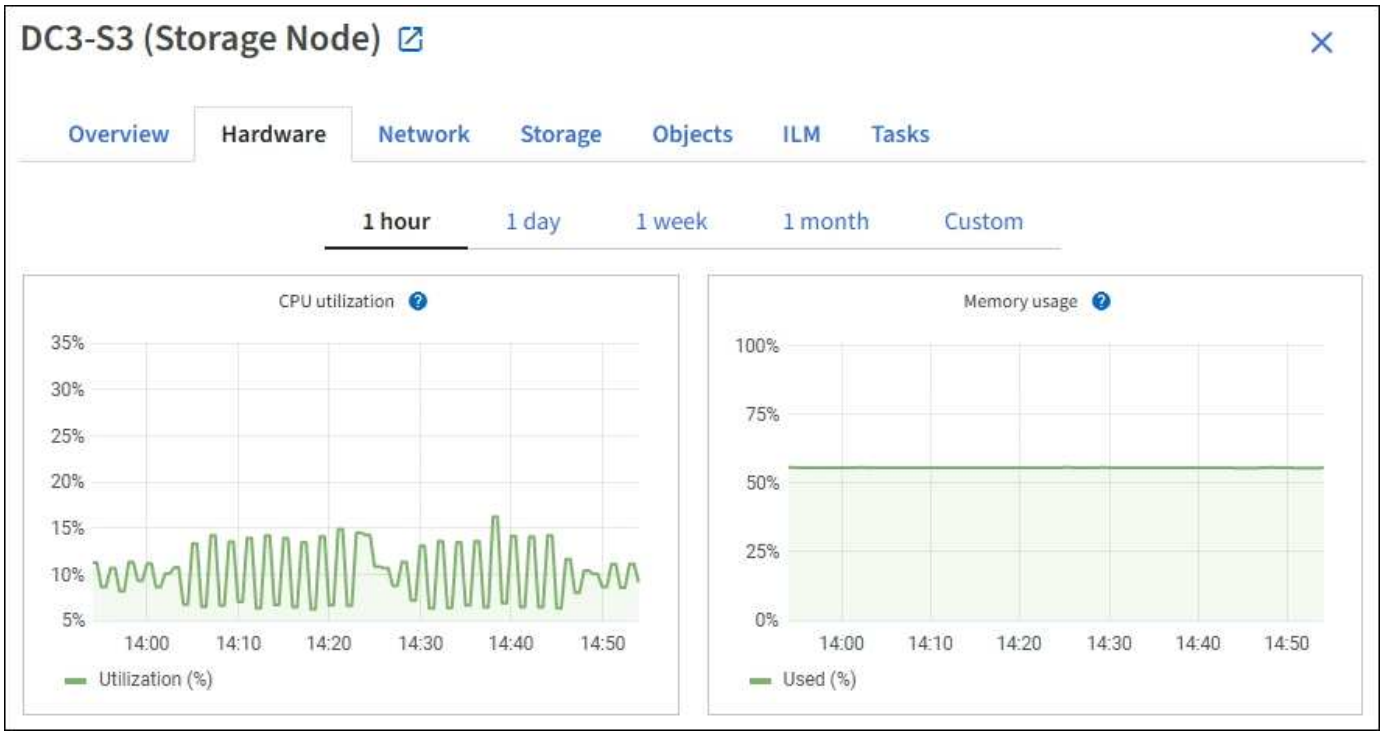
警报也包括在中 "节点连接状态"。

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。

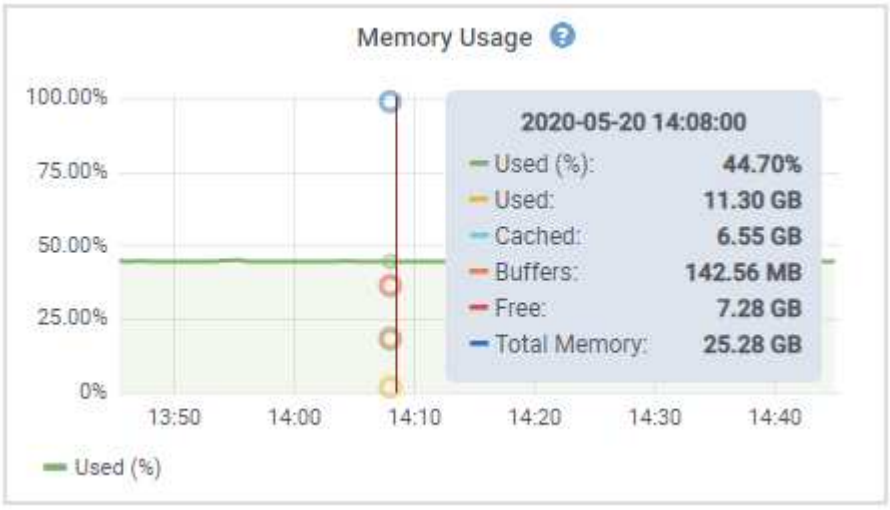
Grid Manager随每个版本更新、可能与此页面上的示例屏幕截图不匹配。

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CPU利用率和内存使用情况的详细信息、请将光标置于每个图形上方。



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

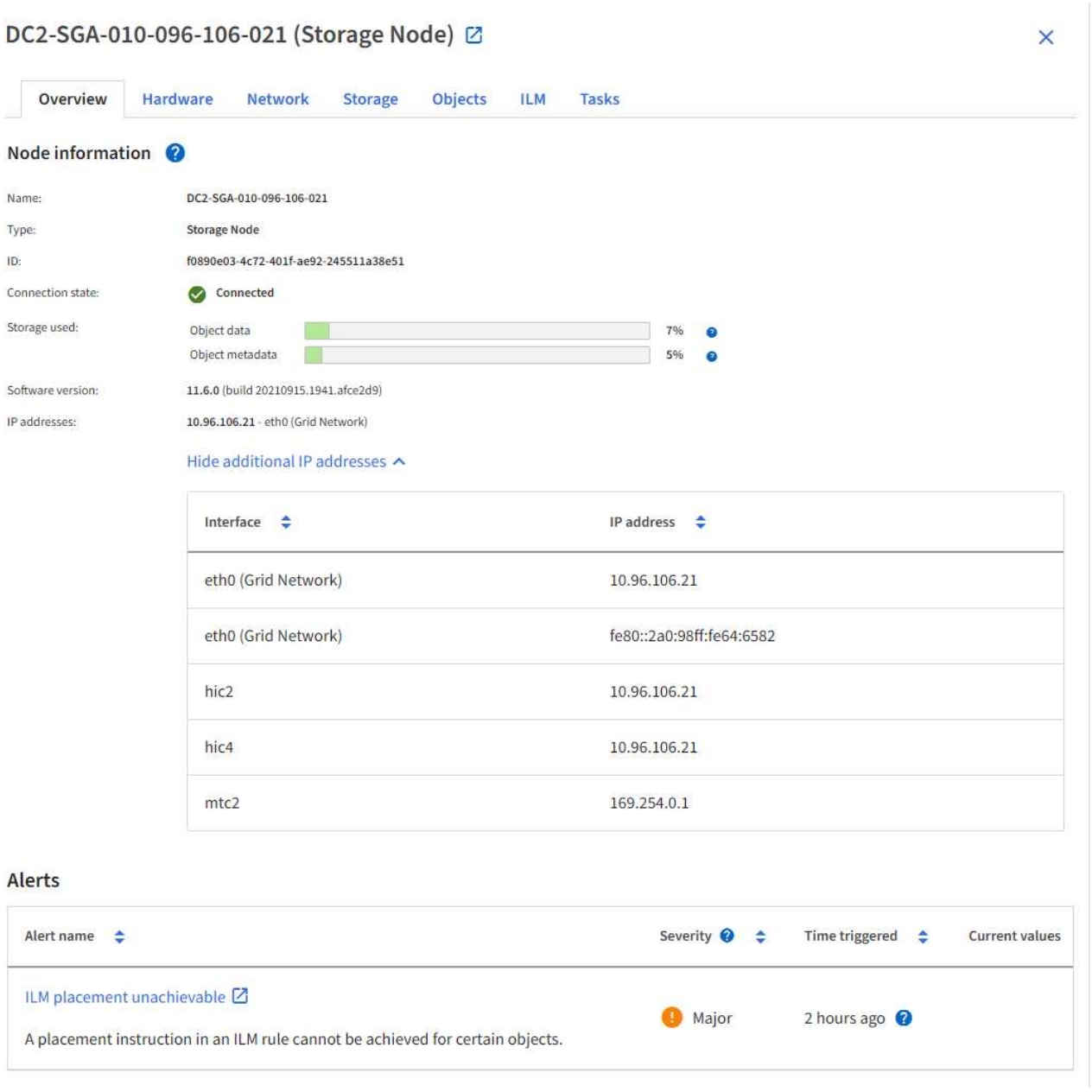
节点页面列出了有关每个设备存储节点的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，控制器固件版本，网络资源，网络接口， 网络地址以及接收和传输数据。

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。

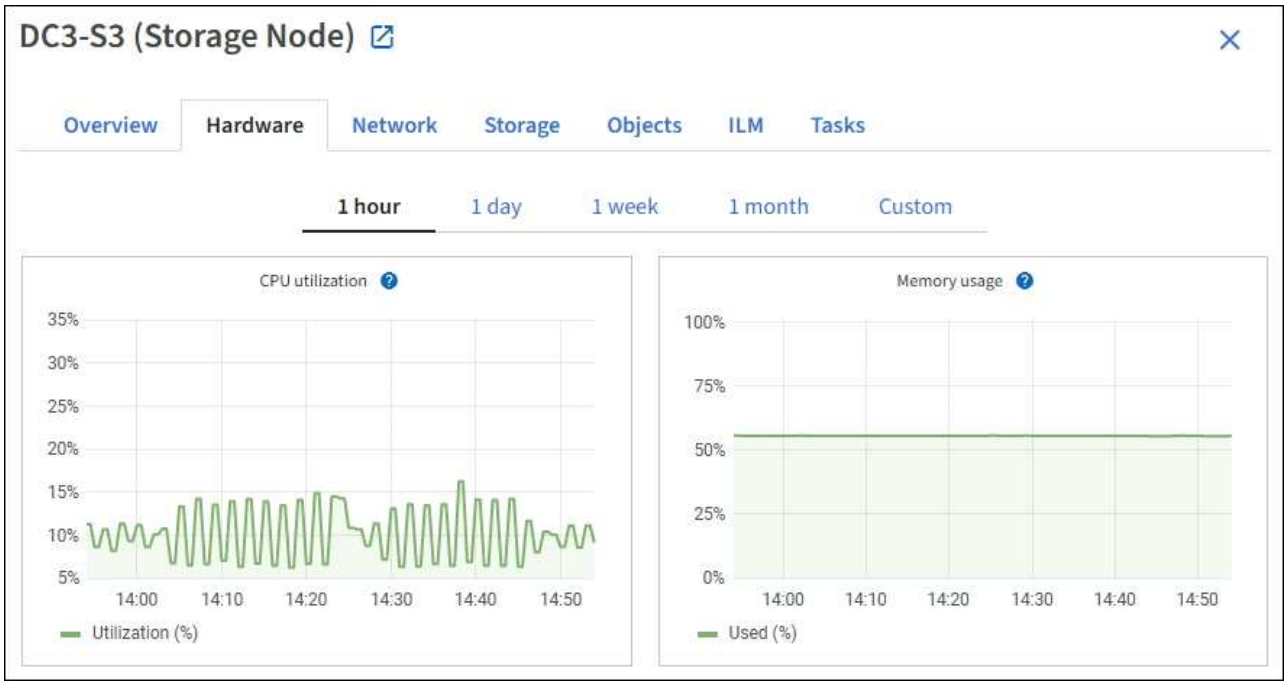


" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

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。

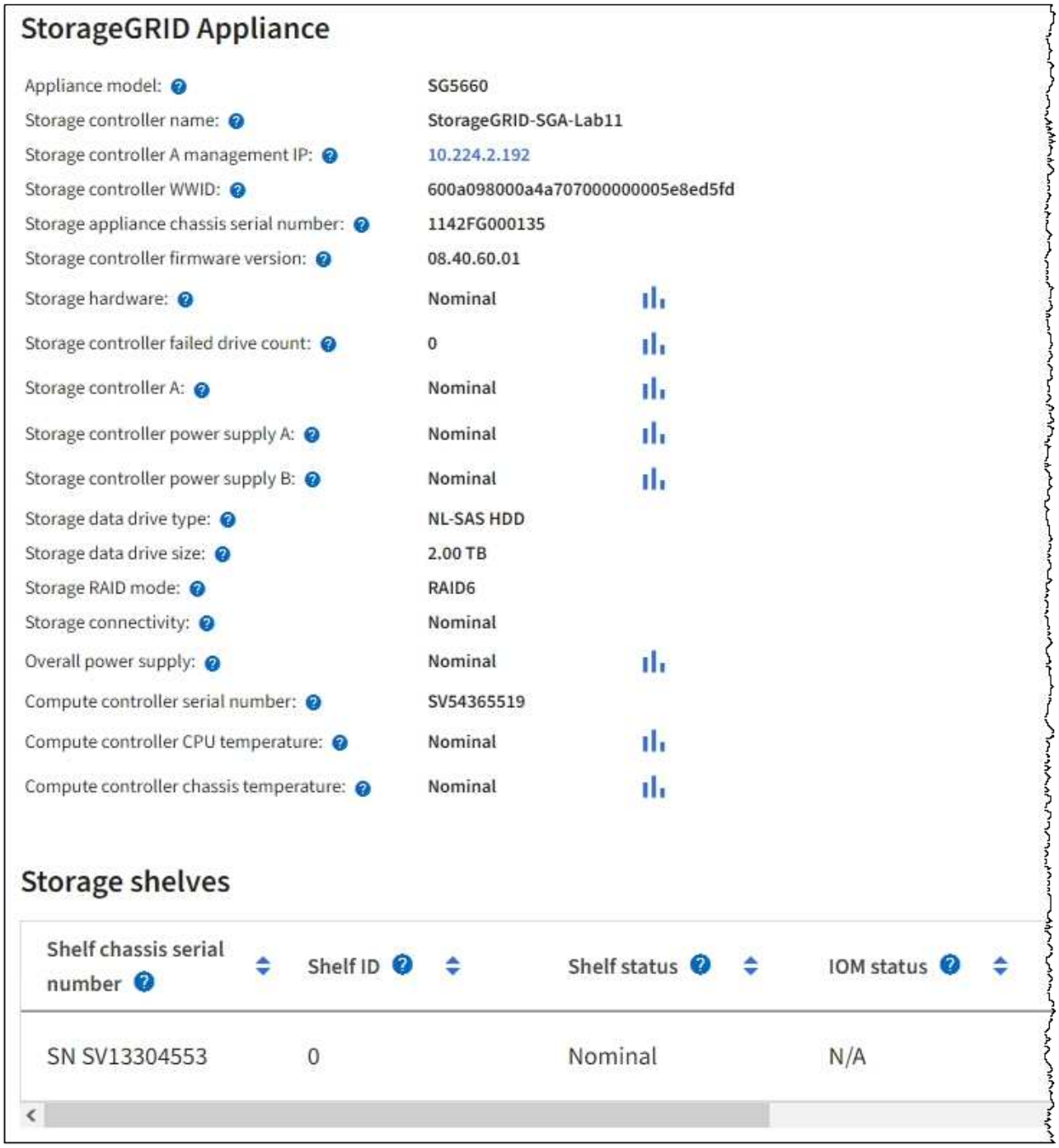
您还可以设置自定义间隔，以便指定日期和时间范围。



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 OS中显示的此StorageGRID 设备的型号。
存储控制器名称	SANtricity OS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操作系统来对存储问题进行故障排除。

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操作系统来对存储问题进行故障排除。 某些设备型号没有存储控制器B
存储控制器 WWID	SANtricity 操作系统中显示的存储控制器的全球通用标识符。
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"需要引起注意"、请首先使用SANtricity操作系统检查存储控制器。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	不是最佳驱动器的数量。
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SG6160。
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。

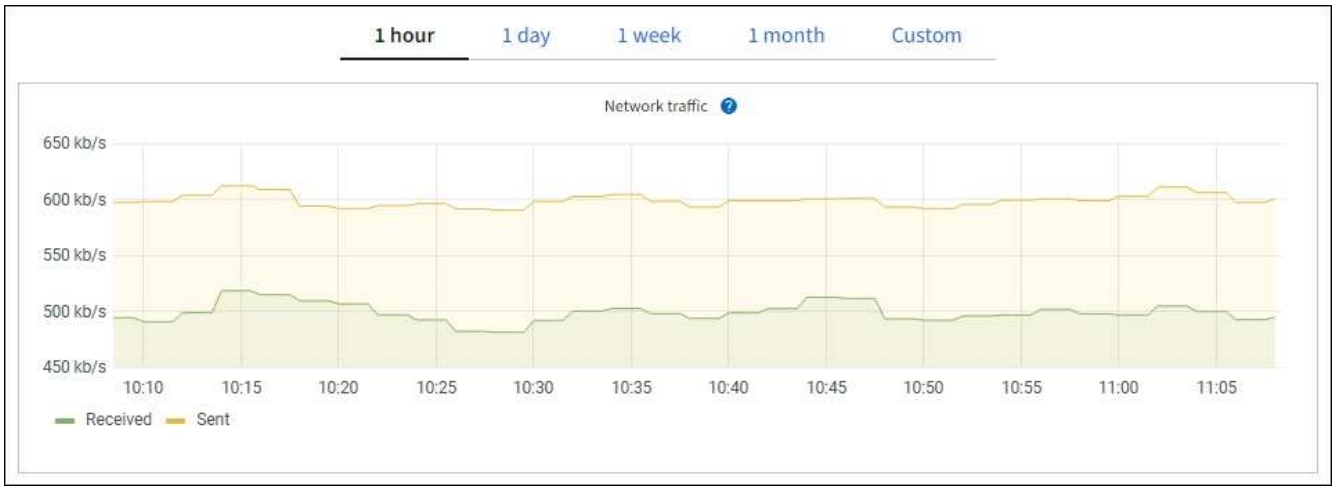
存储架表中的列	Description
【磁盘架数据驱动器大小】数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储架中用作缓存的驱动器数量。
缓存驱动器大小	存储架中最小缓存驱动器的大小。通常，缓存驱动器的大小相同。
配置状态	存储架的配置状态。

a. 确认所有状态均为"标称"。

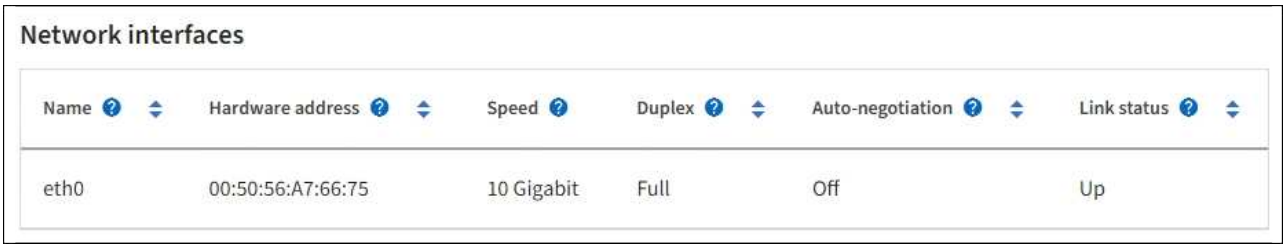
如果状态不是"标称"、请查看任何当前警报。您还可以使用 SANtricity 系统管理器详细了解其中一些硬件值。请参见有关安装和维护设备的说明。

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。



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。

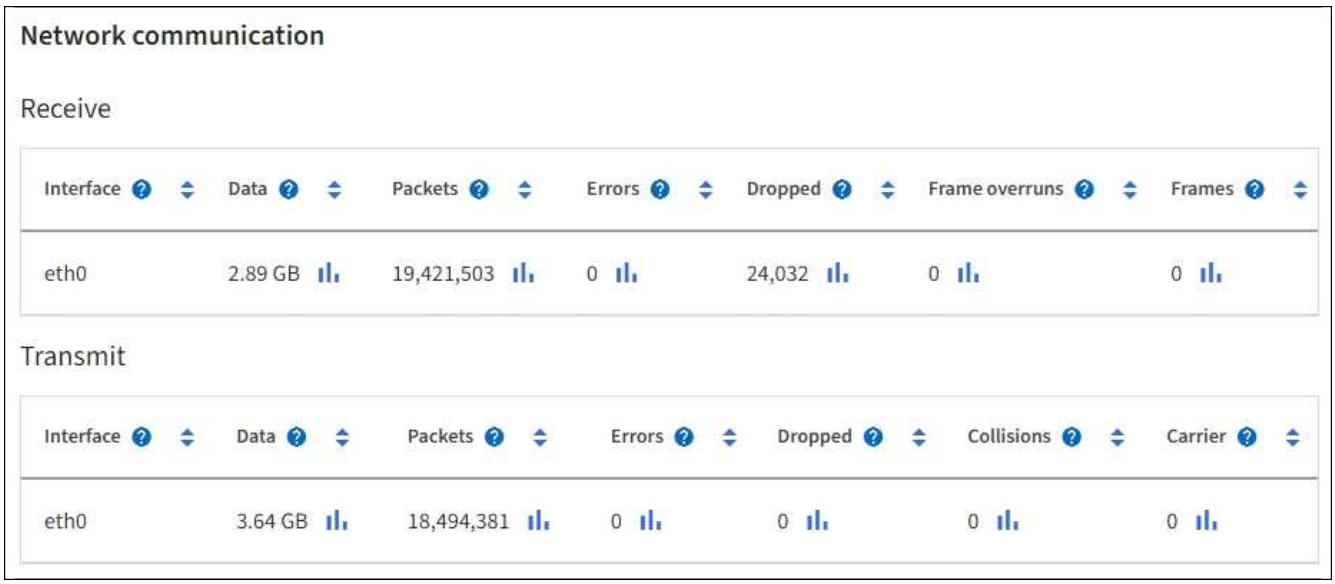
表中显示的值假定使用了所有四个链路。

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

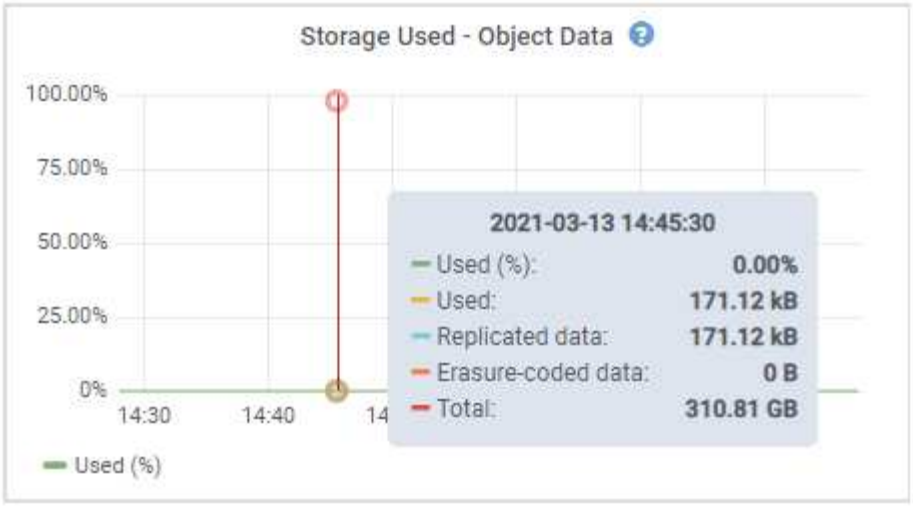
请参见 "配置网络链路" 有关配置10/C5-GbE端口的详细信息、请参见。

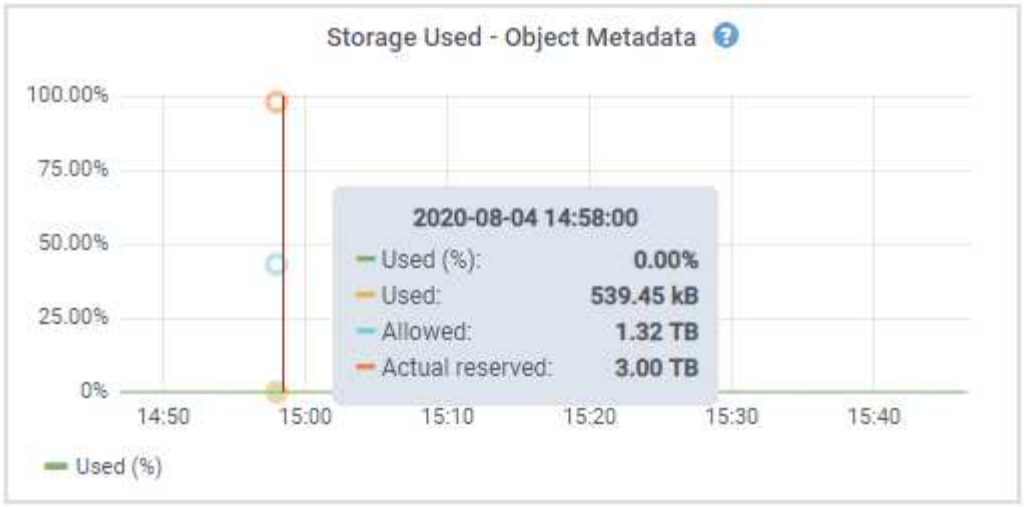
b. 查看网络通信部分。

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。

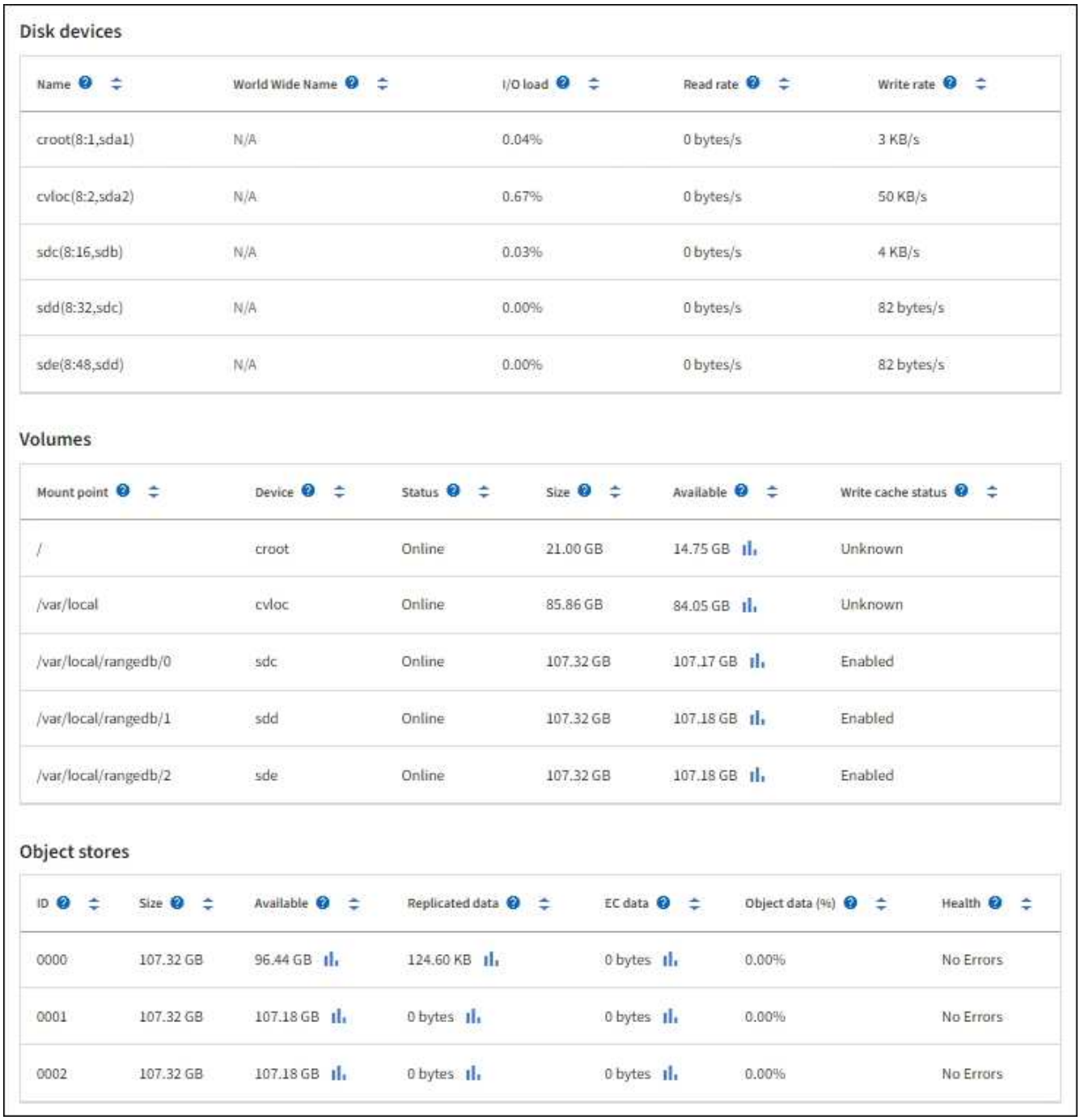




a. 向下滚动以查看每个卷和对象存储的可用存储容量。

   每个磁盘的全球通用名称与在SANtricity OS (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

查看有关设备管理节点和网关节点的信息

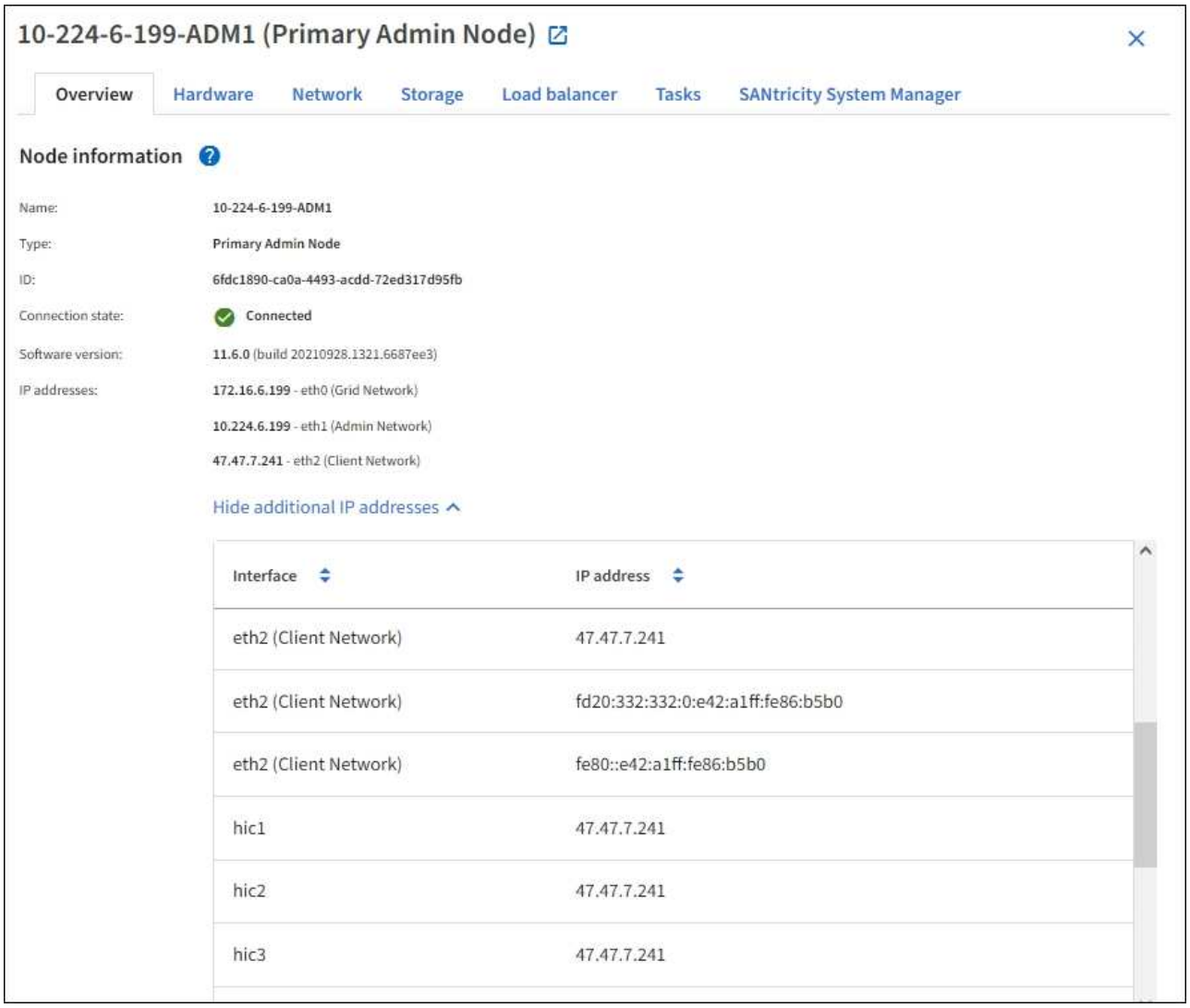
节点页面列出了有关用作管理节点或网关节点的每个服务设备的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，网络资源，网络接口，网络地址， 以及接收和传输数据。

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：

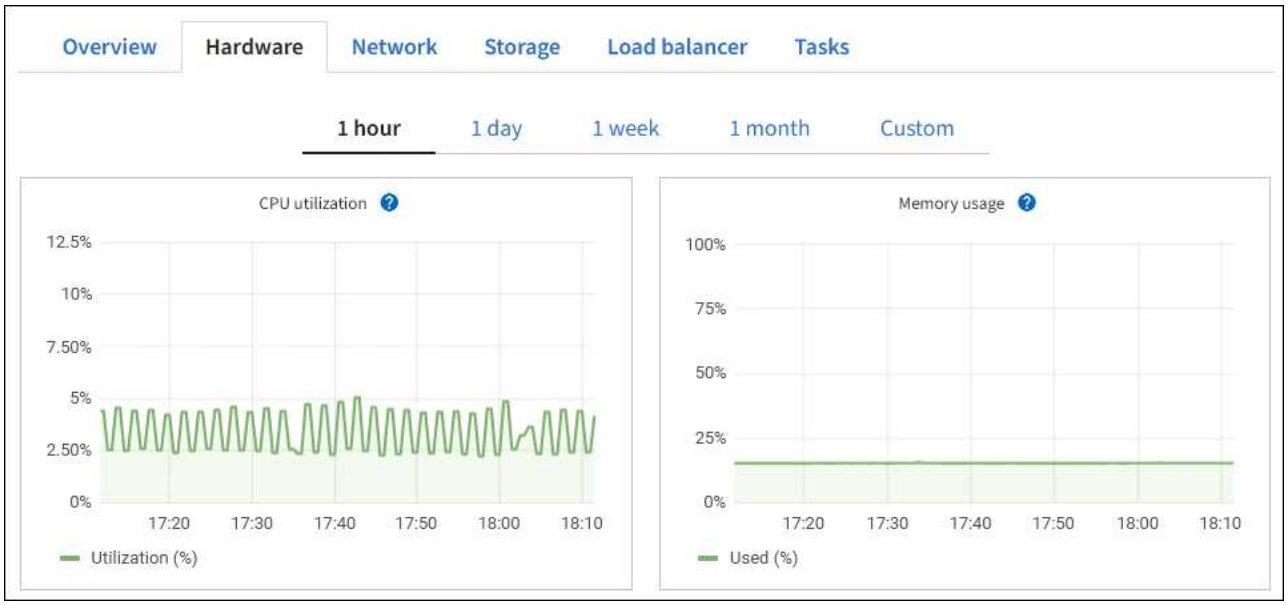
- * adllb* 和 * adlli* ： 如果对管理网络接口使用主动 / 备份绑定，则显示此信息
- * eth * ： 网格网络，管理网络或客户端网络。
- * hic* ： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
- * MTC* ： 设备上的一个物理 1-GbE 端口。 一个或多个 MTC 接口已绑定，以构成管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。



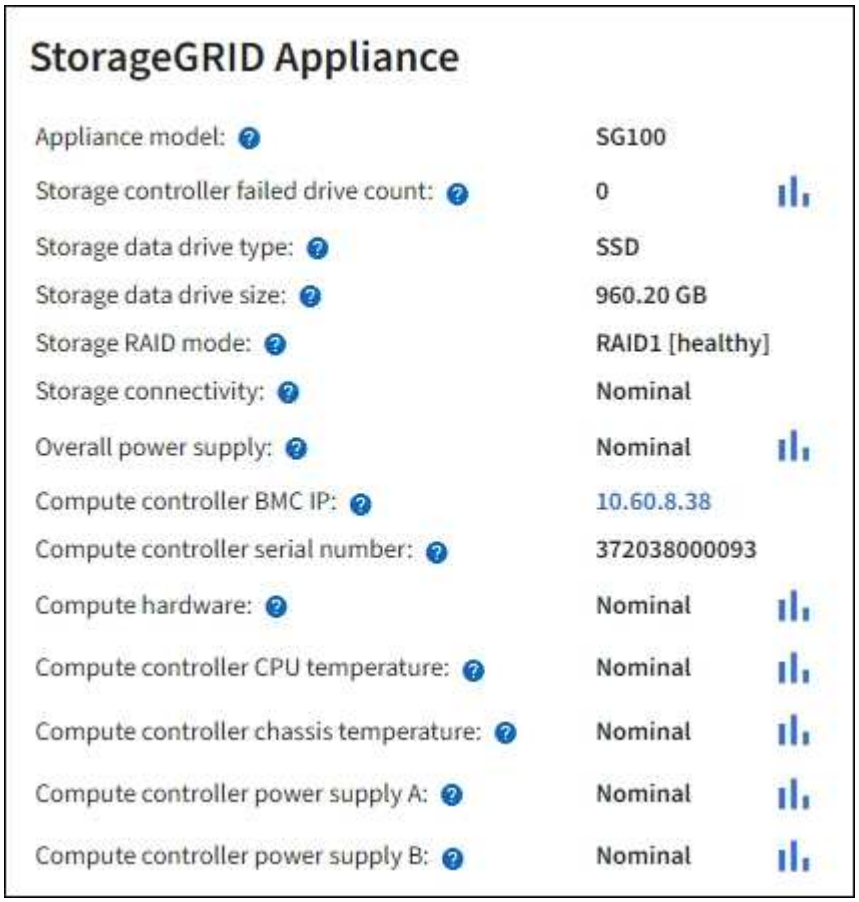
" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

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	不是最佳驱动器的数量。

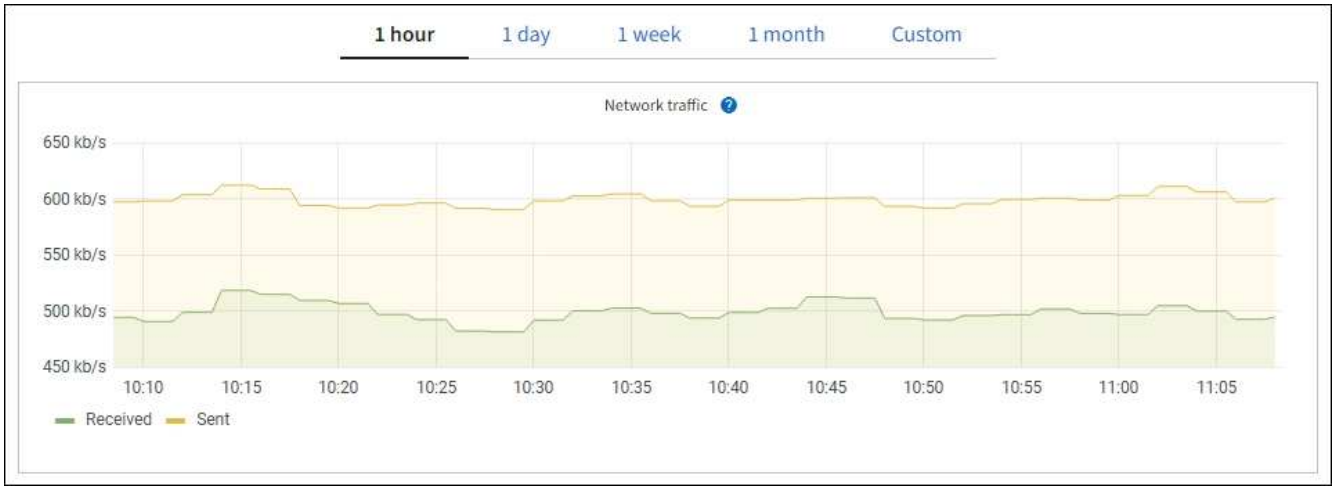
字段	Description
存储数据驱动器类型	设备中的驱动器类型、例如HDD (硬盘驱动器)或SSD (固态驱动器)。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller ， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含BMC的设备型号、不会显示此字段。
计算控制器序列号	计算控制器的序列号。
计算硬件	计算控制器硬件的状态。
计算控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

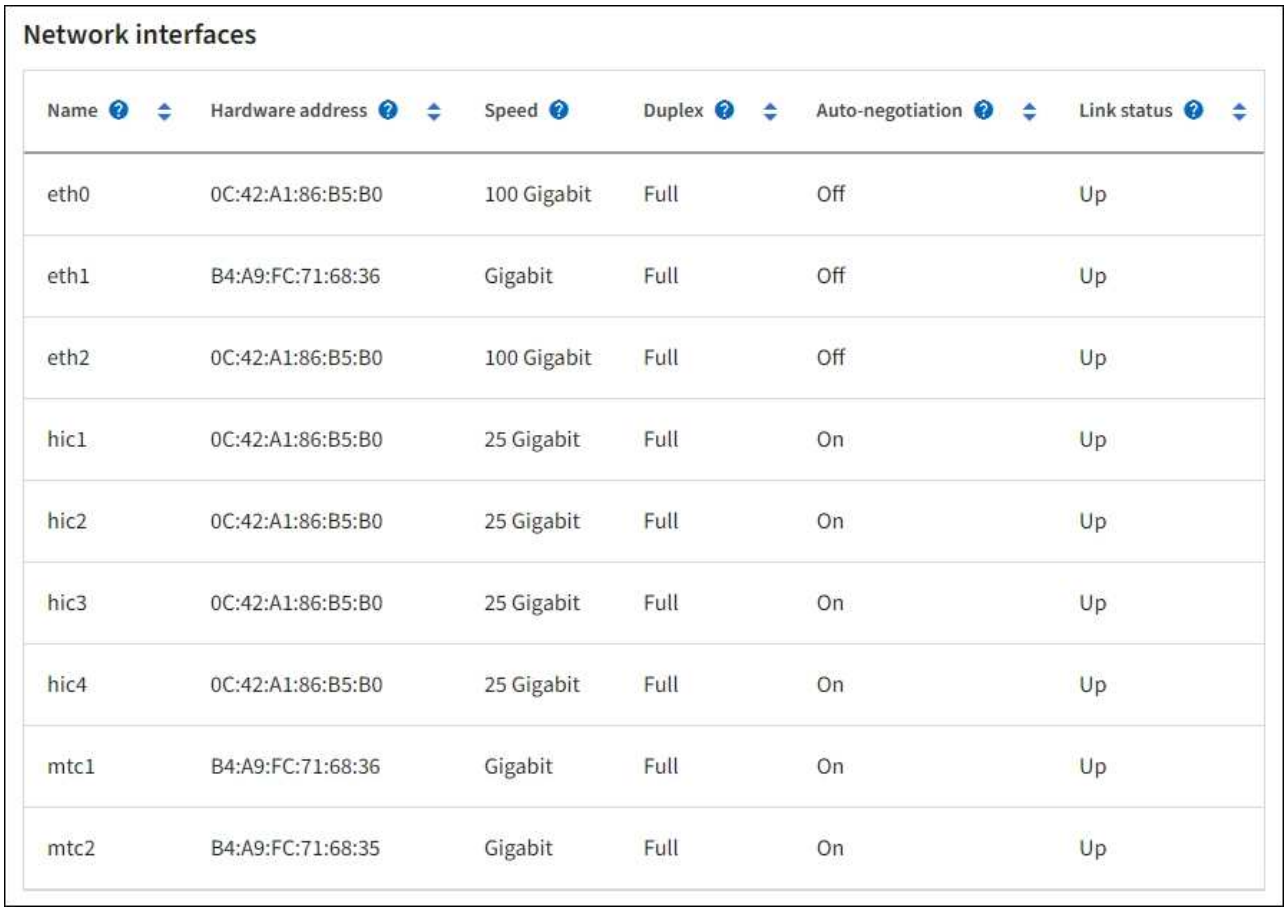
如果状态不是"标称"、请查看任何当前警报。

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

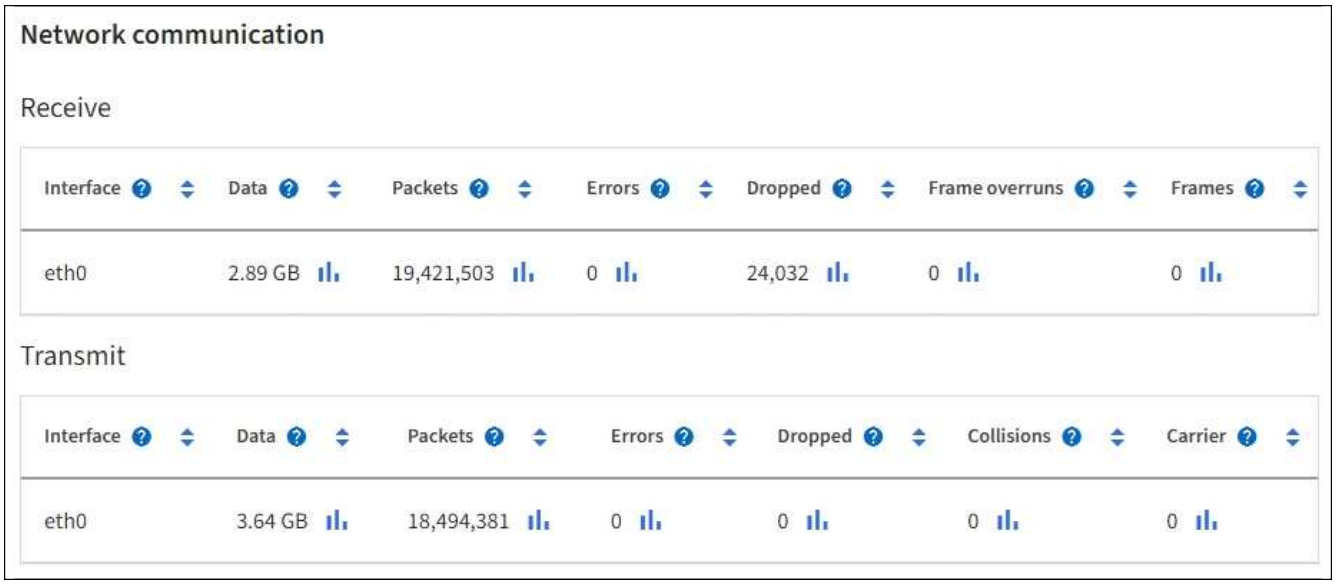
使用下表以及网络接口表中 * 速度 * 列中的值确定设备上的四个 40/100-GbE 网络端口是否配置为使用主动 / 备份模式或 LACP 模式。

表中显示的值假定使用了所有四个链路。

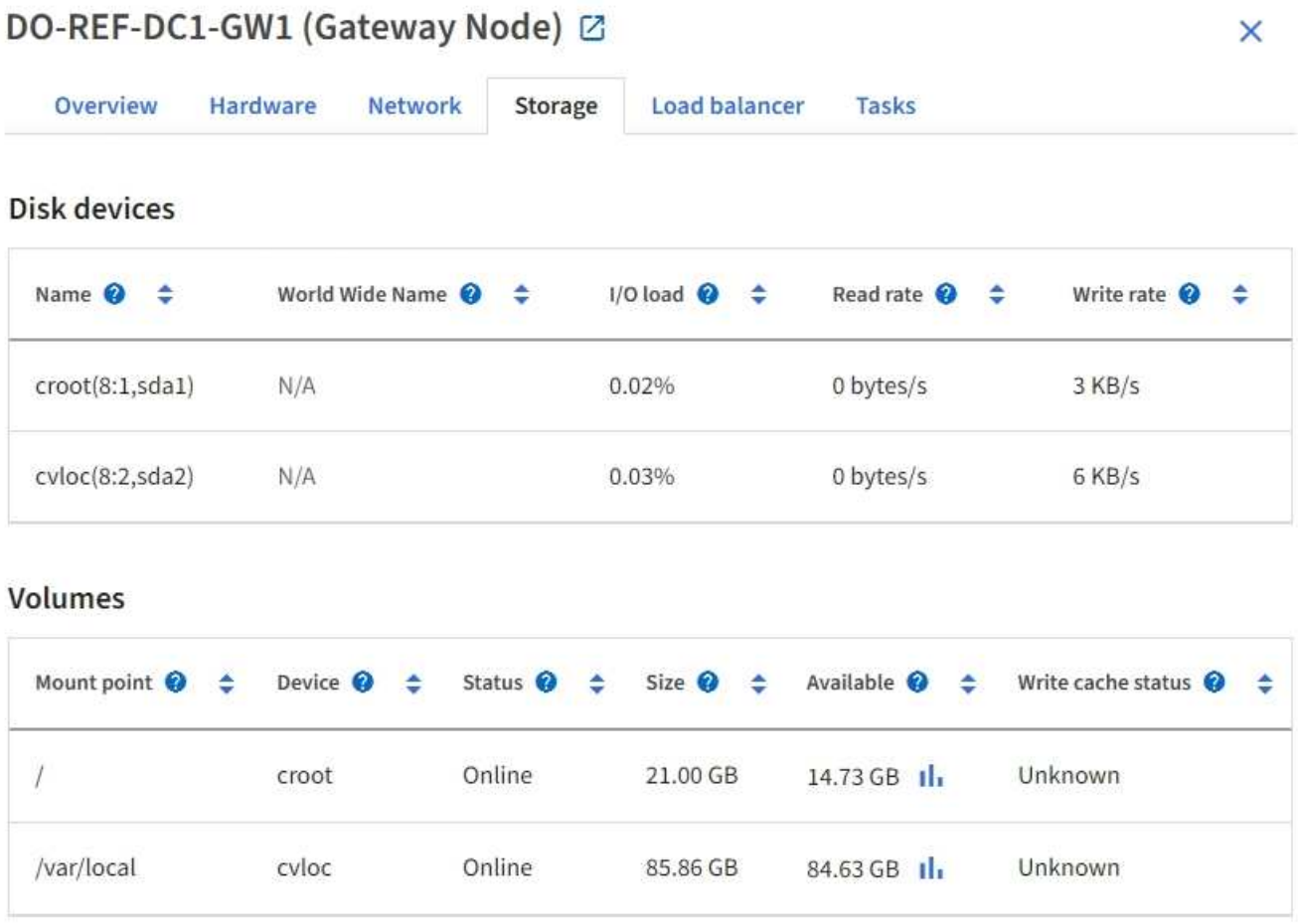
链路模式	绑定模式	单个 **HIC** 链路速度（ **hic1** ， **hic2** ， **hic3** ， **hic4** ）	预期网格 / 客户端网络速度（ **eth0** ， **eth2** ）
聚合	LACP	100	400
已修复	LACP	100	200
已修复	主动 / 备份	100	100
聚合	LACP	40	160
已修复	LACP	40	80
已修复	主动 / 备份	40	40

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。



查看网络选项卡

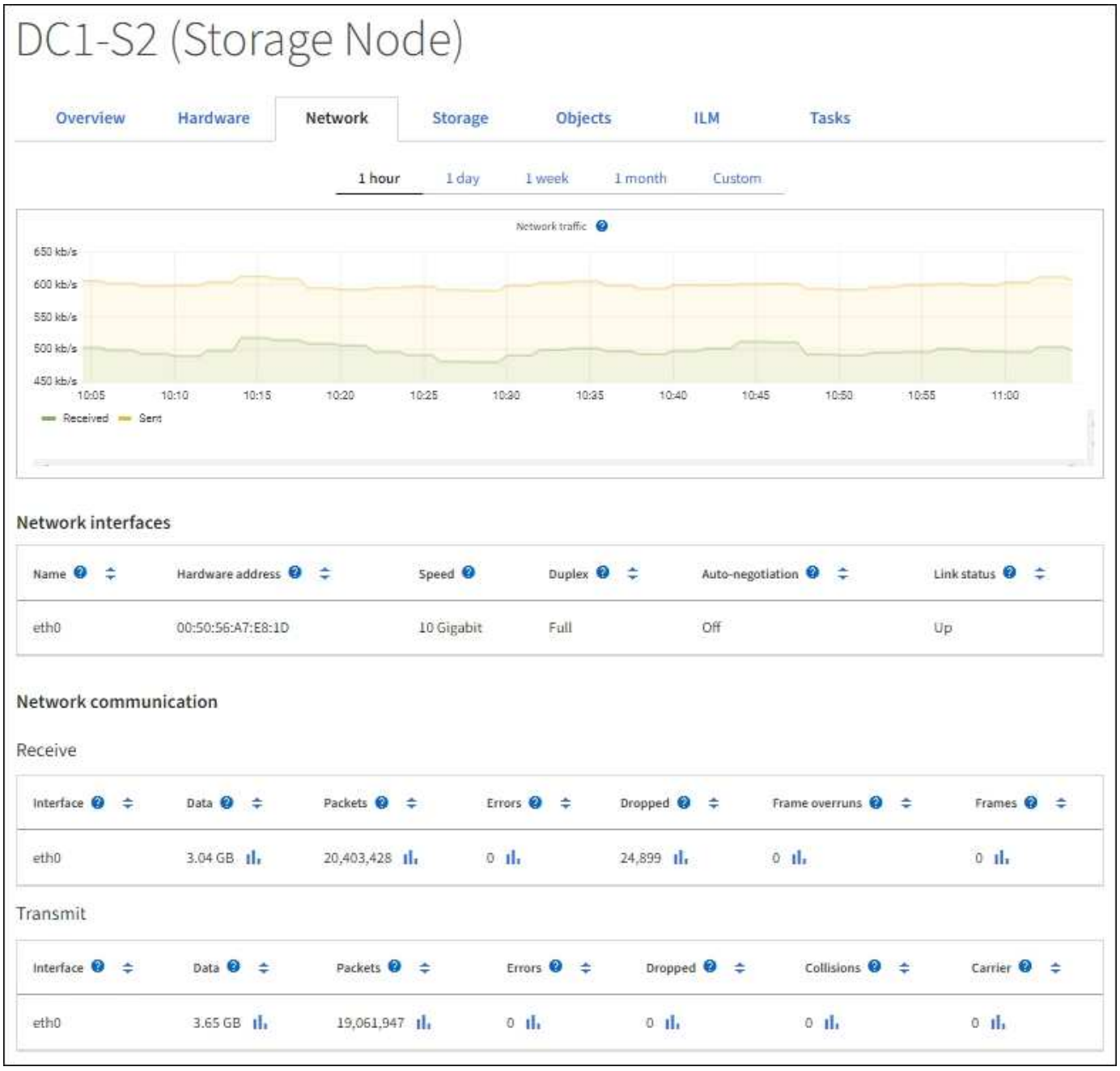
网络选项卡显示一个图形，其中显示了通过节点，站点或网格上的所有网络接口接收和发

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

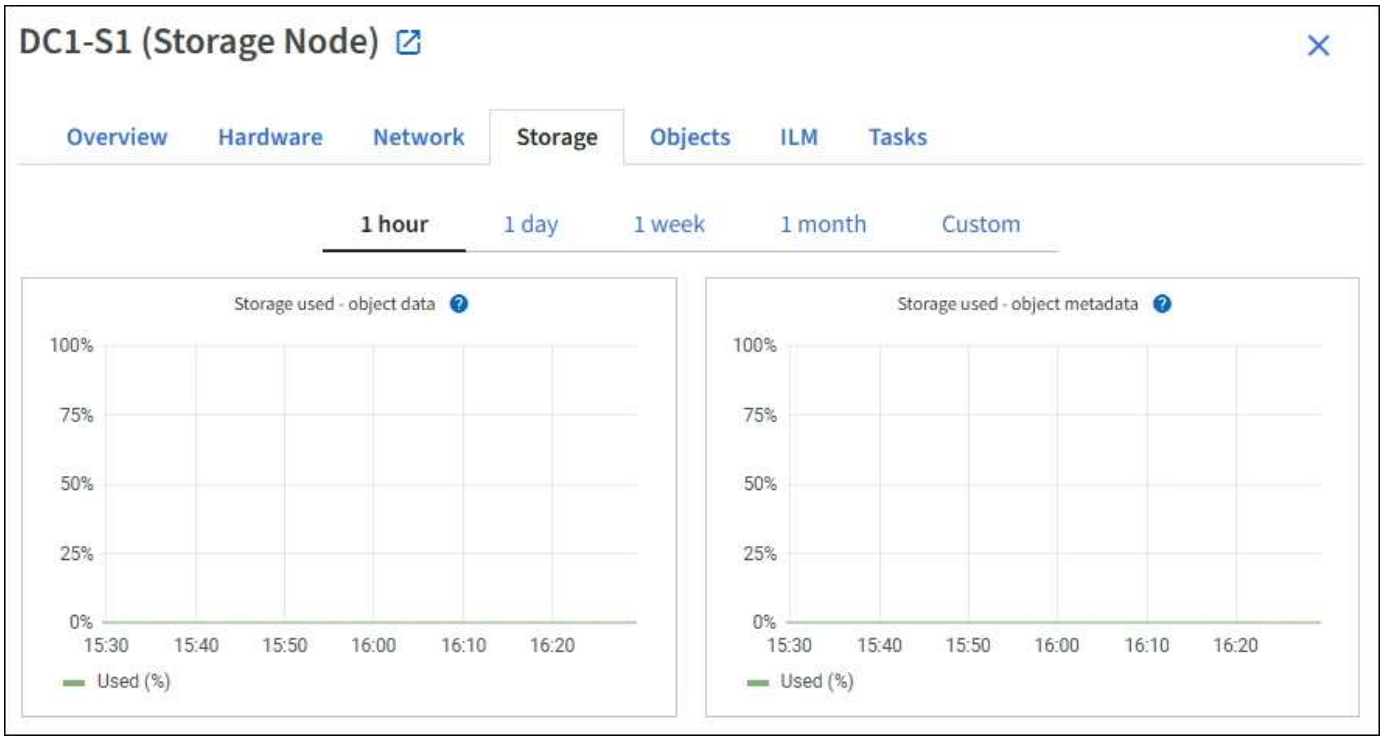
存储选项卡汇总了存储可用性和其他存储指标。

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

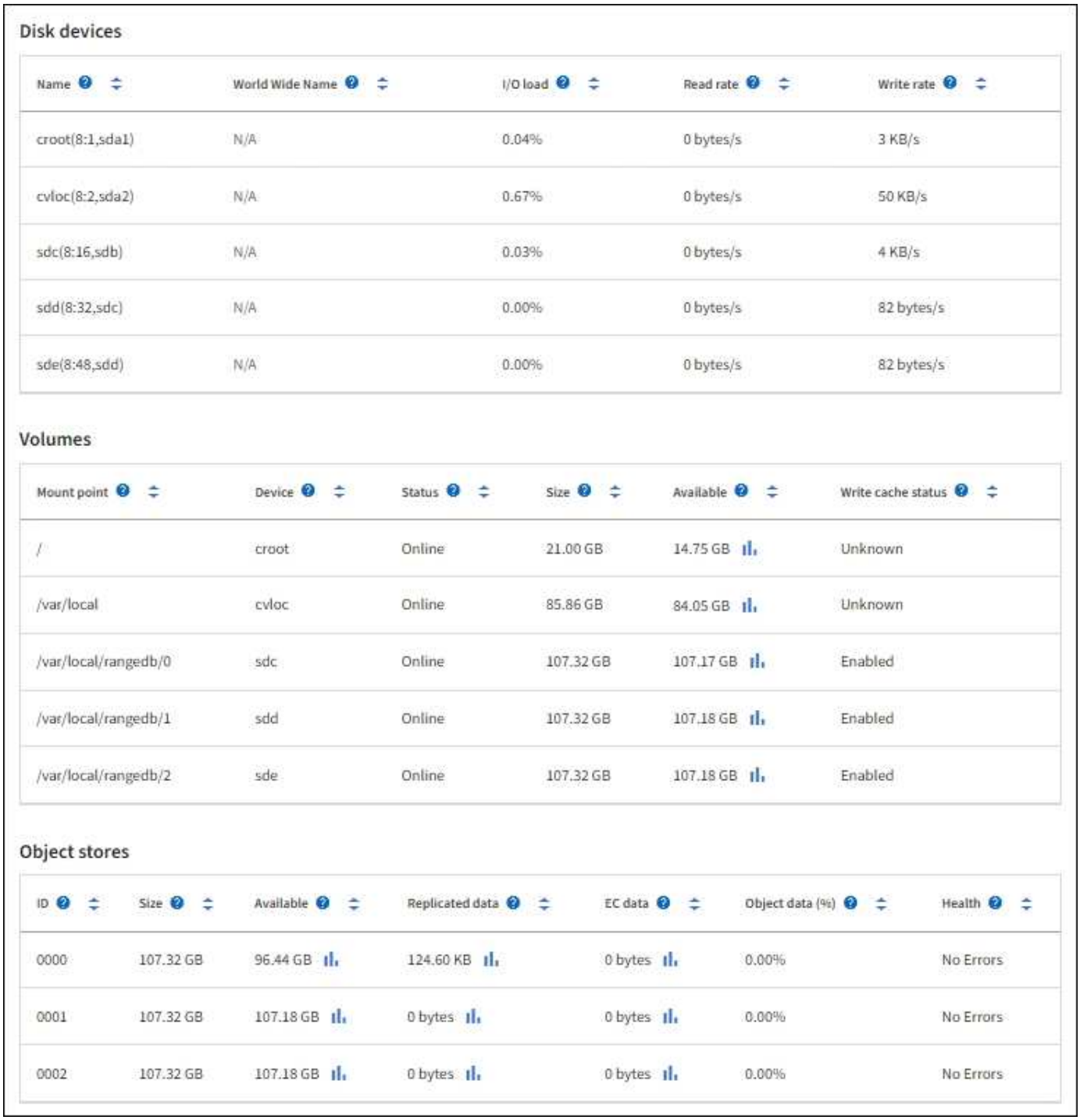
对于存储节点，每个站点和整个网格， " 存储 " 选项卡包含一些图形，用于显示对象数据和对象元数据在一段时间内使用了多少存储。

如果节点未连接到网格、例如在升级期间或处于断开状态时、某些指标可能不可用或不在站点和网格总数中。节点重新连接到网格后、请等待几分钟、使值稳定下来。



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

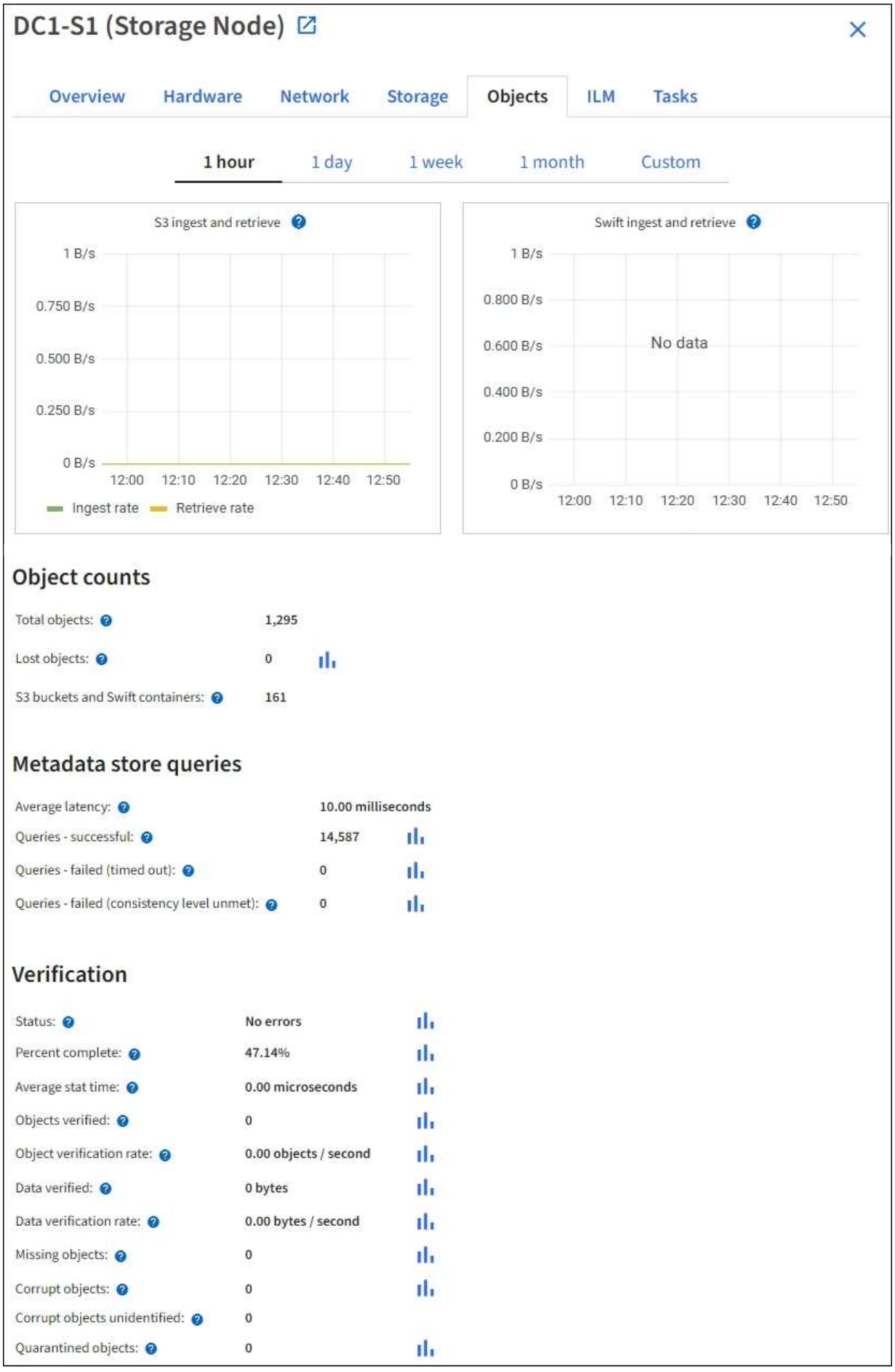
相关信息

"监控存储容量"

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。

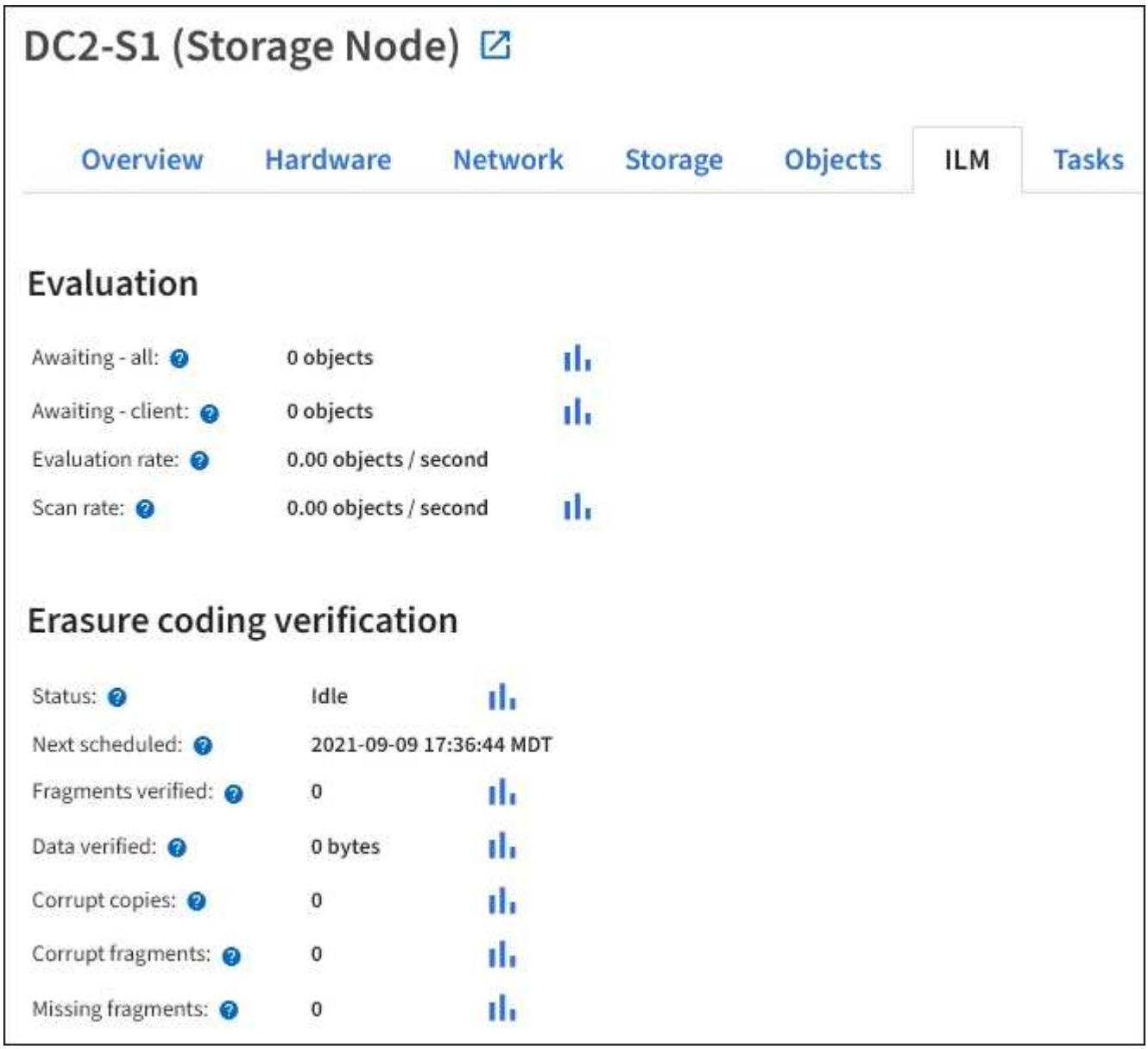

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 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选项卡提供了有关对已进行过身份验证的对象进行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"

使用任务选项卡

此时将显示所有节点的任务选项卡。您可以使用此选项卡重命名或重新启动节点、或者将

设备节点置于维护模式。

有关此选项卡上每个选项的完整要求和说明、请参见以下内容：

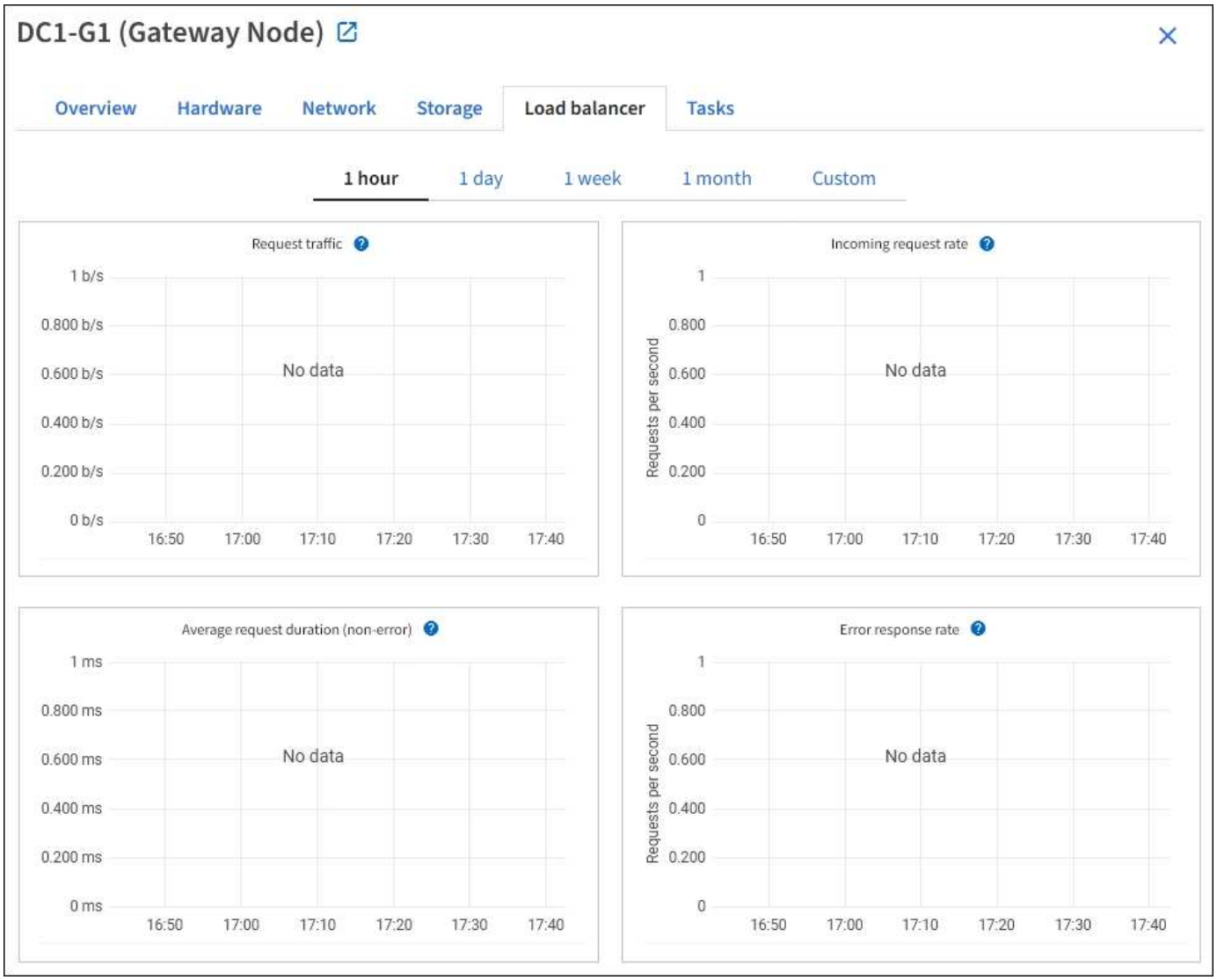
- "重命名网格、站点和节点"
- "重新启动网格节点"
- "将设备置于维护模式"

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"无数据"。



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

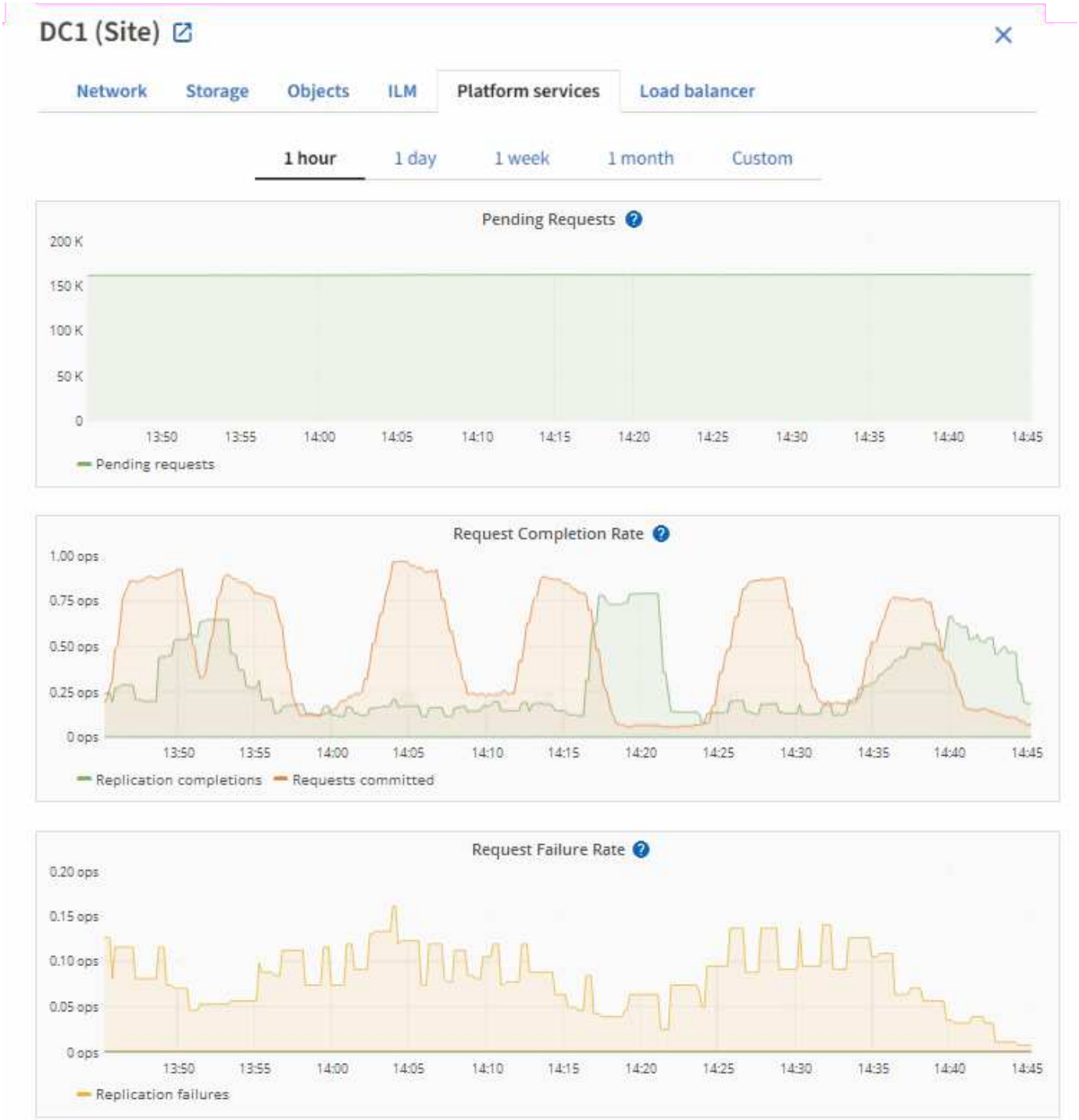
"监控负载平衡操作"

"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"。

查看管理驱动器选项卡(仅限**GF6112**)

通过管理驱动器选项卡、您可以访问有关SGF6112设备中驱动器的详细信息并对其执行故障排除和维护任务。

只有SGF6112存储设备节点才会显示管理驱动器选项卡。

使用管理驱动器选项卡、您可以执行以下操作：

- 查看设备中的数据存储驱动器布局
- 查看一个表、其中列出了每个驱动器位置、类型、状态、固件版本和序列号
- 对每个驱动器执行故障排除和维护功能

要访问管理驱动器选项卡、您必须具有 "存储设备管理员或root访问权限"。

有关使用管理驱动器选项卡的信息、请参阅 "使用管理驱动器选项卡"。

查看**SANtricity**系统管理器选项卡(仅限**E**系列)

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。

只有使用E系列硬件的存储设备节点才会显示SANtricity 系统管理器选项卡。

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

- 查看性能数据、例如存储阵列级别的性能、I/O延迟、存储控制器CPU利用率和吞吐量。
- 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。

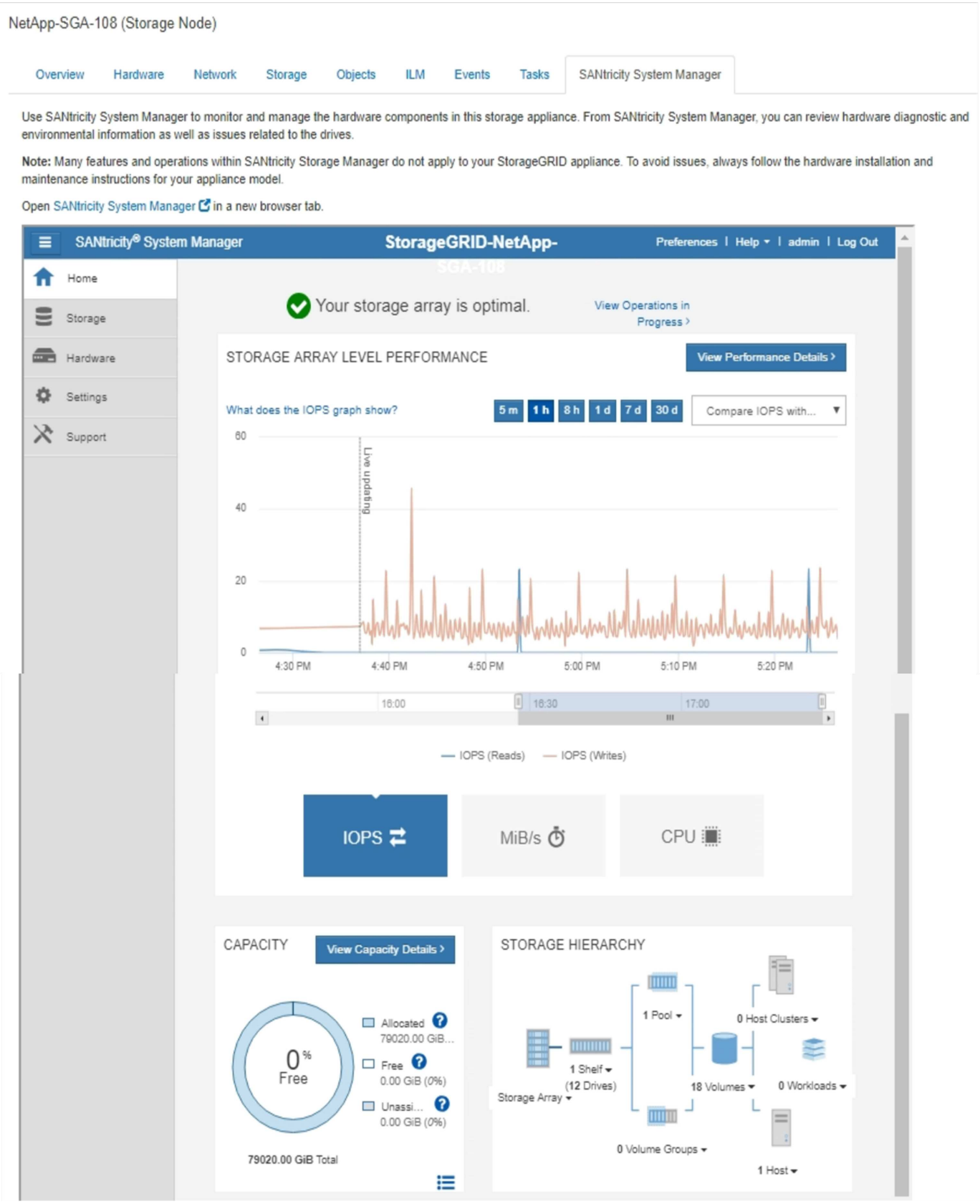
要使用SANtricity 系统管理器为E系列AutoSupport 配置代理、请参见 "通过StorageGRID发送E系列AutoSupport软件包"。

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 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 系统管理器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、请始终按照设备的硬件维护说明进行操作。

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、请将光标置于每个图形上方。

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"。

要定期监控的信息

监控的内容和时间

即使发生错误或部分网格不可用时StorageGRID 系统仍可继续运行、您也应监控并解决潜在问题、以免影响网格的效率或可用性。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

关于监控任务

繁忙的系统会生成大量信息。以下列表提供了有关需要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"	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
"网络和系统资源"	每周
"租户活动"	每周
"S3和Swift客户端操作"	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
"网格联合连接"	每周
"外部归档存储系统的容量"	每周

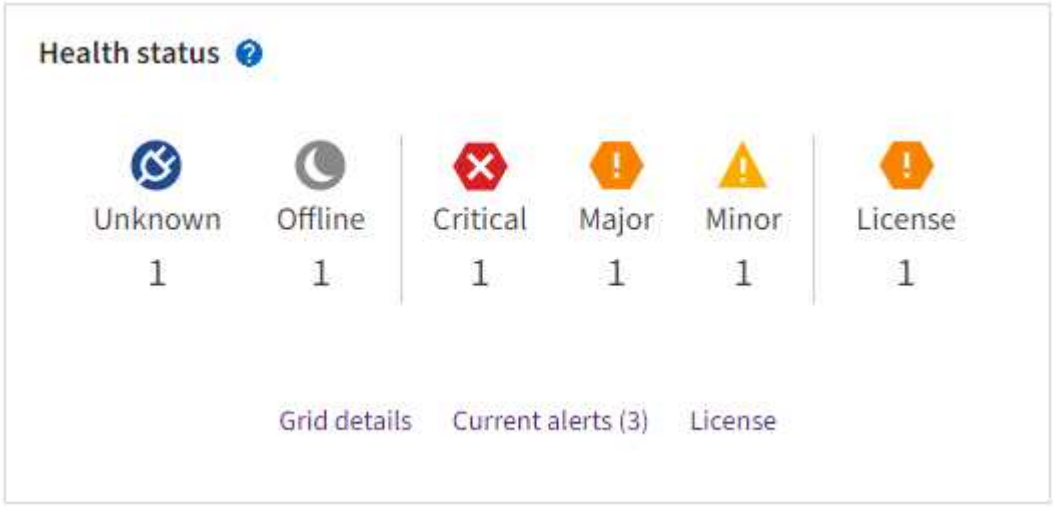
监控系统运行状况

每天监控StorageGRID 系统的整体运行状况。

关于此任务

StorageGRID 系统可在部分网格不可用时继续运行。警报或警报指示的潜在问题(传统系统)不一定是系统操作的问题。调查Grid Manager信息板的运行状况卡上汇总的问题。

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"。



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。	出现以下情况时显示...
网格详细信息	所有节点均已断开连接(连接状态未知或已被管理员关闭)。
当前警报(严重、主要、次要)	警报为 当前处于活动状态。
最近解决的警报	过去一周触发的警报 现已解决。
许可证	此StorageGRID 系统具有一个具有软件许可证的问题描述。您可以 "根据需要更新许可证信息"。

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。监控节点连接状态并及时解决任何问题。

图标。	**Description**	需要执行操作
	• 未连接 - 未知 * 由于未知原因、节点已断开连接或节点上的服务意外关闭。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。 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。	需要立即关注。 选择每个警报 并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。 注意：在受管关闭操作期间，节点可能显示为未知。在这些情况下，您可以忽略未知状态。

图标。	Description	需要执行操作
	• 未连接 - 已管理员关闭 * 出于预期原因、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。 根据底层问题描述 、这些节点通常无需任何干预即可恢复联机。	确定是否有任何警报正在影响此节点。 如果一个或多个警报处于活动状态、 选择每个警报 并按照建议的操作进行操作。
	• 已连接 * 节点已连接到网格。	无需执行任何操作。

查看当前警报和已解决警报

当前警报：触发警报时、信息板上会显示警报图标。节点页面上还会显示节点的警报图标。条件 "已配置警报电子邮件通知"，也会发送电子邮件通知，除非警报已被禁用。

已解决警报：您可以搜索和查看已解决警报的历史记录。

您也可以观看以下视频： "视频：StorageGRID 11.8."

下表介绍了网格管理器中显示的当前警报和已解决警报的信息。

列标题	Description
姓名或职务	警报及其问题描述 的名称。

列标题	Description
severity	警报的严重性。对于当前警报、如果对多个警报进行了分组、则标题行会显示每个严重性发生的警报实例数。 严重：存在异常情况、已停止StorageGRID 节点或服务的正常运行。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、可能会影响其运行能力。您应监控和解决无法自行清除的次要警报、以确保它们不会导致更严重的问题。
时间已触发	当前警报：在您的本地时间和UTC时间内触发警报的日期和时间。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。 已解决警报：警报在多长时间前触发。
站点 / 节点	正在或已发生警报的站点和节点的名称。
Status	警报处于活动状态、已被关闭还是已解决。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。
解决时间(仅限已解决警报)	警报解决多长时间前。
Current Values或_data values"	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。 *注意：*如果对多个当前警报进行了分组，则当前值不会显示在标题行中。
触发值(仅限已解决警报)	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。

步骤

1. 选择*当前警报*或*已解决警报*链接可查看这些类别的警报列表。您也可以通过选择*N节点*>* *NODE*>*Overview*并从“警报”表中选择警报来查看警报的详细信息。

   默认情况下、当前警报显示如下：

   - 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。
- 未显示已被设置为"已被设置为"状态的警报。
- 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. 要展开警报组、请选择down脱机脱字符 。要折叠组中的单个警报、请选择向上脱字符 或选择组的名称。
3. 要显示单个警报而不是一组警报，请清除*组警报*复选框。
4. 要对当前警报或警报组进行排序、请选择向上/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。
   - 清除*组警报*后，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。
5. 要按状态(所有警报、活动*或*已关闭)过滤当前警报，请使用表顶部的下拉菜单。

   请参见 "静默警报通知"。

6. 对已解决的警报进行排序：
   - 从*触发时*下拉菜单中选择一个时间段。
   - 从*严重性*下拉菜单中选择一个或多个严重性。
   - 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。
   - 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。
7. 要查看特定警报的详细信息、请选择该警报。此时将显示一个对话框、其中提供了选定警报的详细信息和建议操作。
8. (可选)对于特定警报、选择SILENCE this alAlert,以使导致触发此警报的警报规则静音。

   您必须具有 "管理警报或root访问权限" 使警报规则静音。

   > 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。

9. 要查看警报规则的当前条件，请执行以下操作：
   a. 从警报详细信息中选择*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。

   b. 要关闭此弹出窗口，请单击此弹出窗口以外的任意位置。
10. (可选)选择*编辑规则*以编辑导致触发此警报的警报规则。

    您必须具有 "管理警报或root访问权限" 编辑警报规则。

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。

11. 要关闭警报详细信息，请选择*关闭*。

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

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。

通过Grid Manager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。

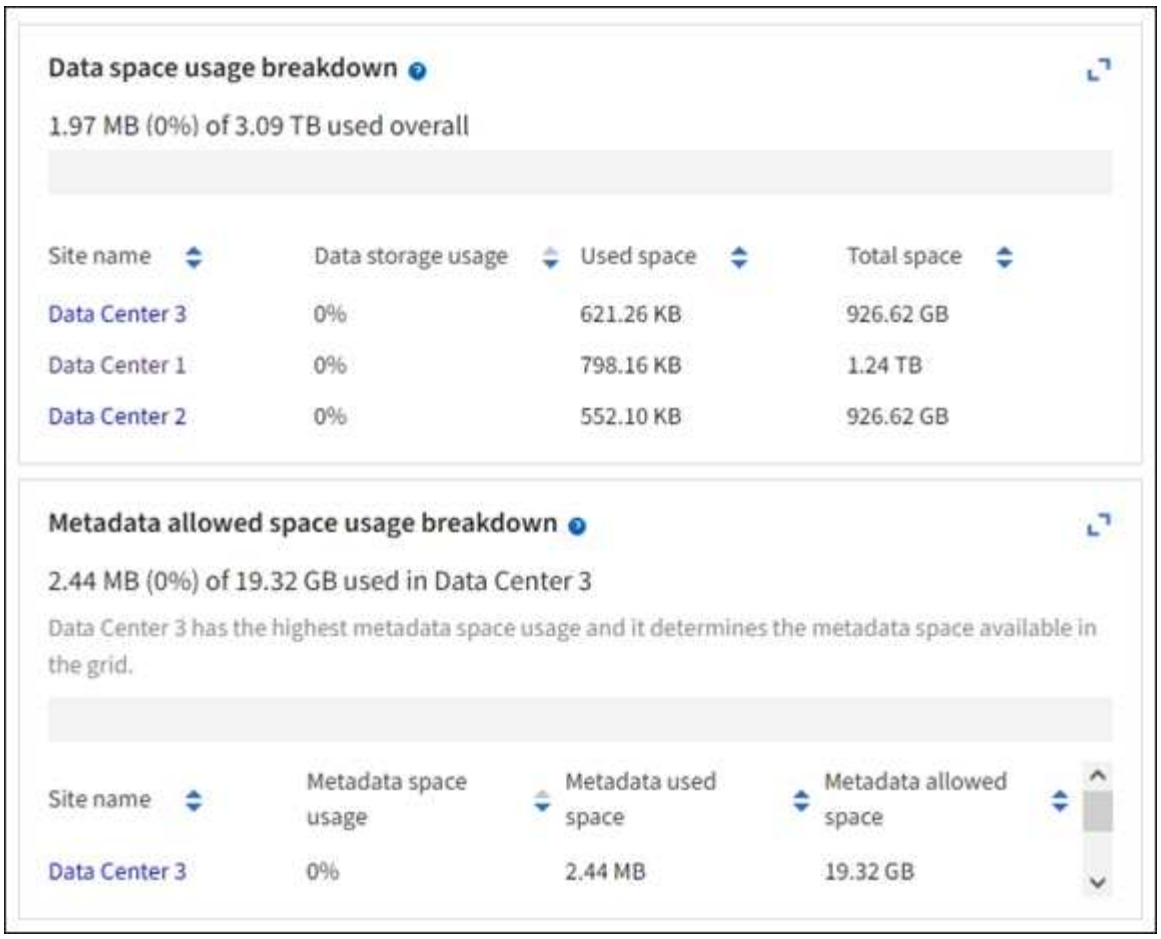
步骤

1. 评估可用于整个网格和每个数据中心的存储量。

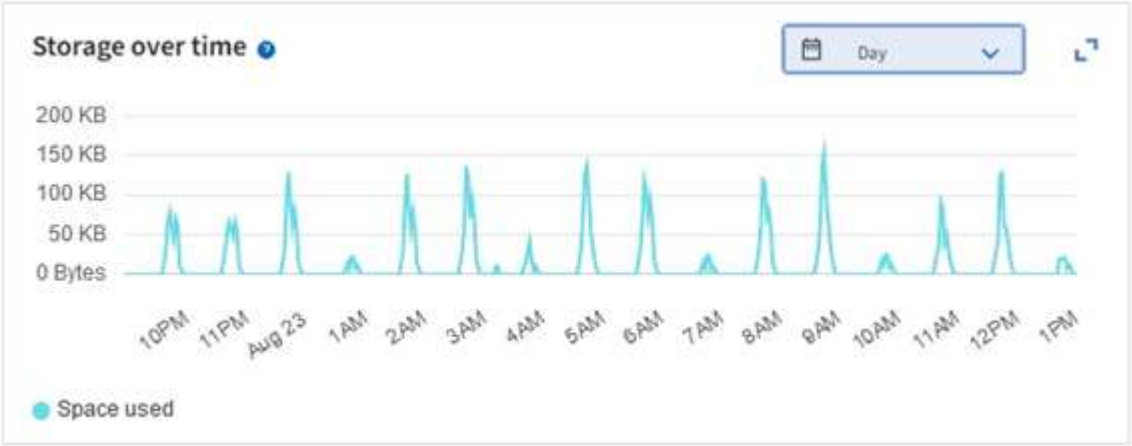
   a. 选择*信息板>概述*。

   b. 记下数据空间使用量细分卡和元数据允许的空间使用量细分卡上的值。每个卡都会列出存储使用量的百分比、已用空间容量以及站点可用或允许的总空间。

      此摘要不包括归档介质。



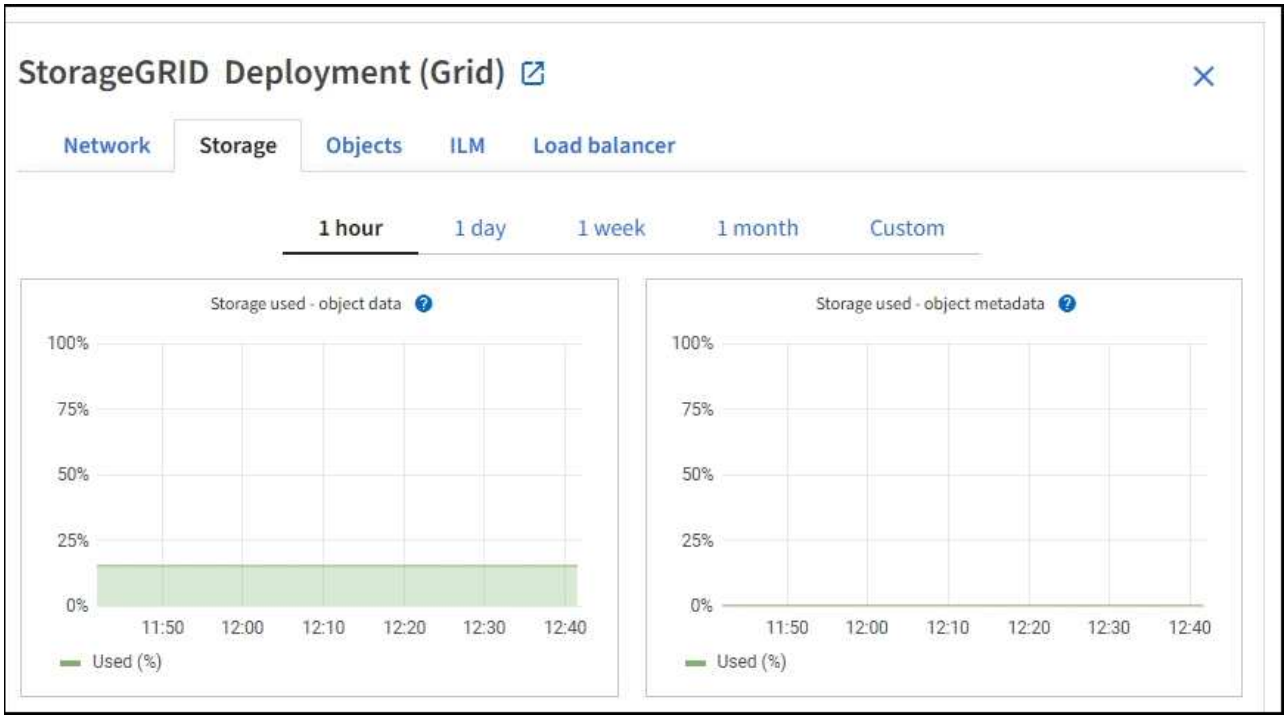
a. 记下随时间变化的存储卡上的图表。使用时间段下拉列表帮助您确定存储的使用速度。



2. 有关已使用的存储容量以及网格中可用于存储对象数据和对象元数据的存储容量的其他详细信息、请使用节点页面。

a. 选择 * 节点 * 。

b. 选择 * ； grid_* > * 存储 * 。



c. 将光标置于*已用存储-对象数据*和*已用存储-对象元数据*图表上方、可查看整个网格可用的对象存储和对象元数据存储量以及一段时间内已使用的容量。

> 站点或网格的总值不包括至少五分钟未报告指标的节点、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。

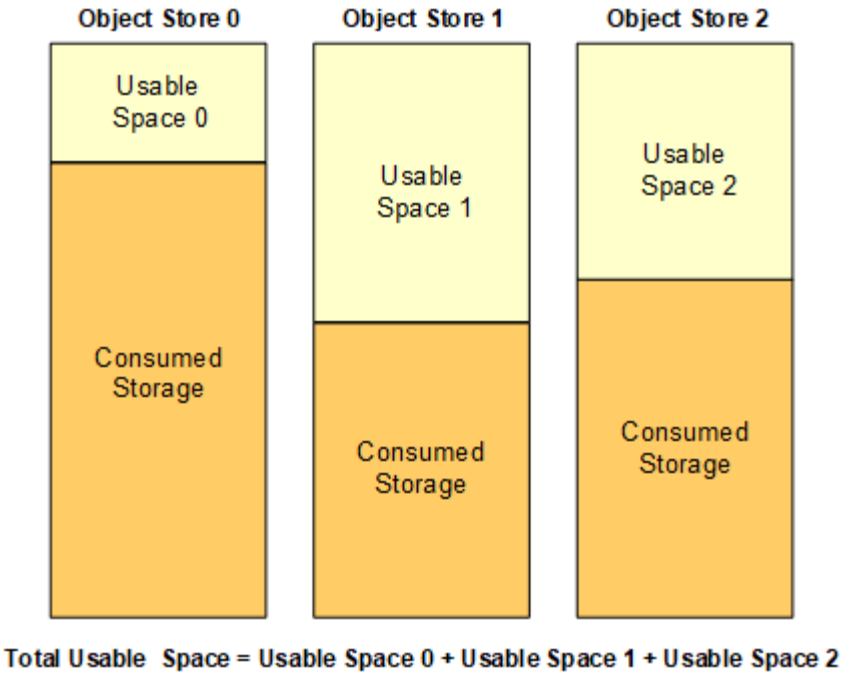
有关规划存储扩展的详细信息、请参见 "扩展 StorageGRID 的说明"。

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。

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

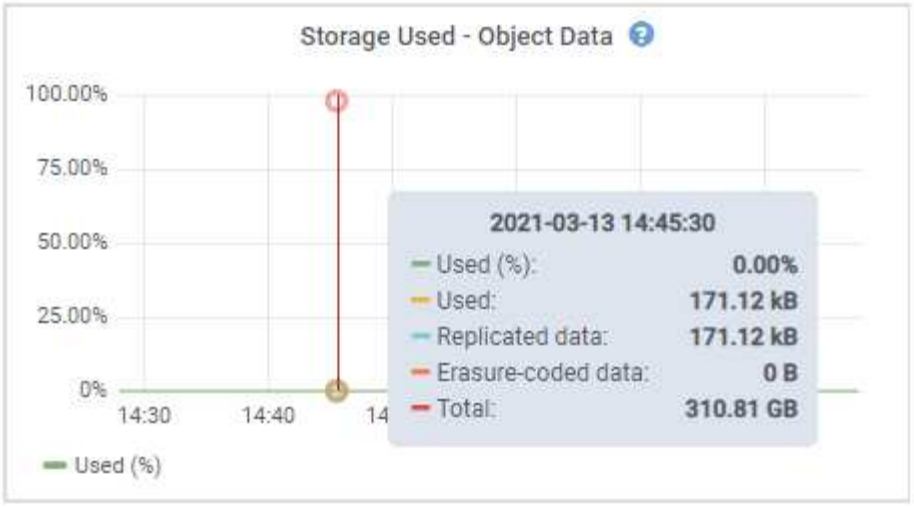
1. 选择 * 节点 * > * 存储节点 _* > * 存储 * 。

   此时将显示节点的图形和表。

2. 将光标置于已用存储-对象数据图上。

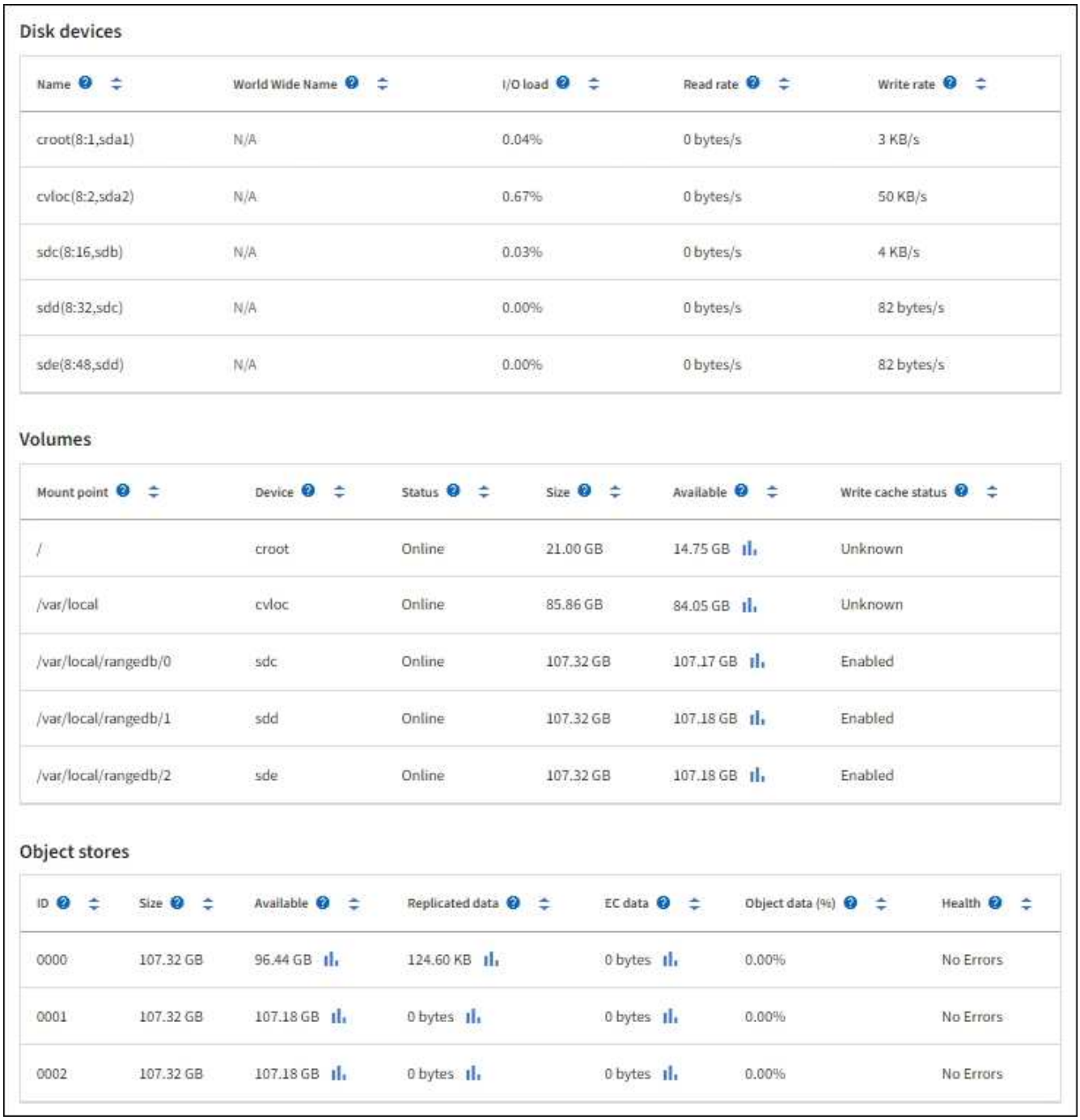
   此时将显示以下值：

   - * 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。
     已用值为 `storagegrid_storage_utilization_data_bytes` 衡量指标。



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。

关于此任务

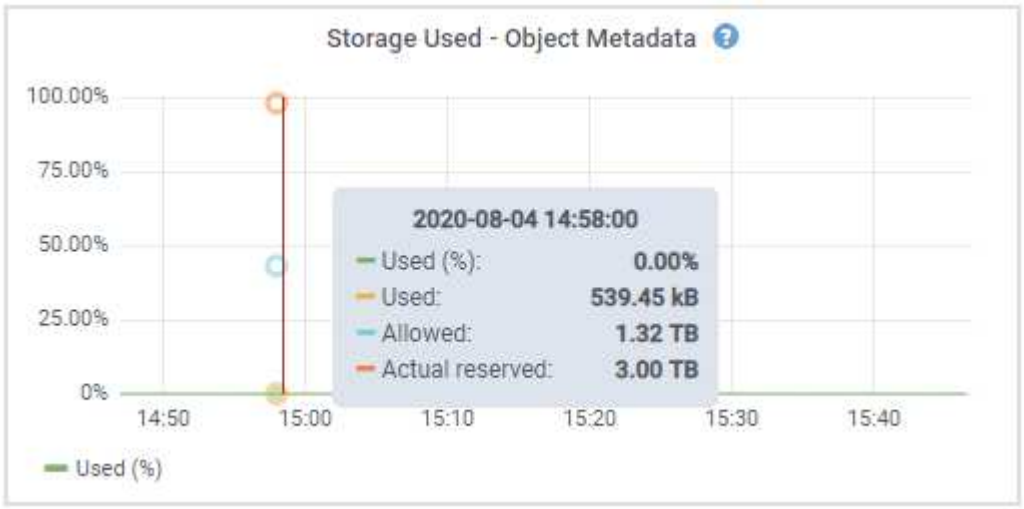
StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并防止对象元数据丢失。这三个副本会使用每个存储节点的存储卷 0 上为元数据预留的空间均匀分布在每个站点的所有存储节点上。

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. 将光标置于已用存储-对象元数据图上方、可查看特定时间的值。



已用（ **%** ）

此存储节点上已使用的允许元数据空间的百分比。

Prometheus指标： `storagegrid_storage_utilization_metadata_bytes` 和 `storagegrid_storage_utilization_metadata_allowed_bytes`

已用

此存储节点上已使用的允许元数据空间的字节数。

Prometheus指标： `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 "允许的元数据空间的完整问题描述"。

Prometheus指标： `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 "元数据的实际预留空间的完整问题描述"。

*Prometheus*指标将在未来版本中添加。

站点或网格的总值不包括至少五分钟未报告指标的节点、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"。

监控空间使用量预测

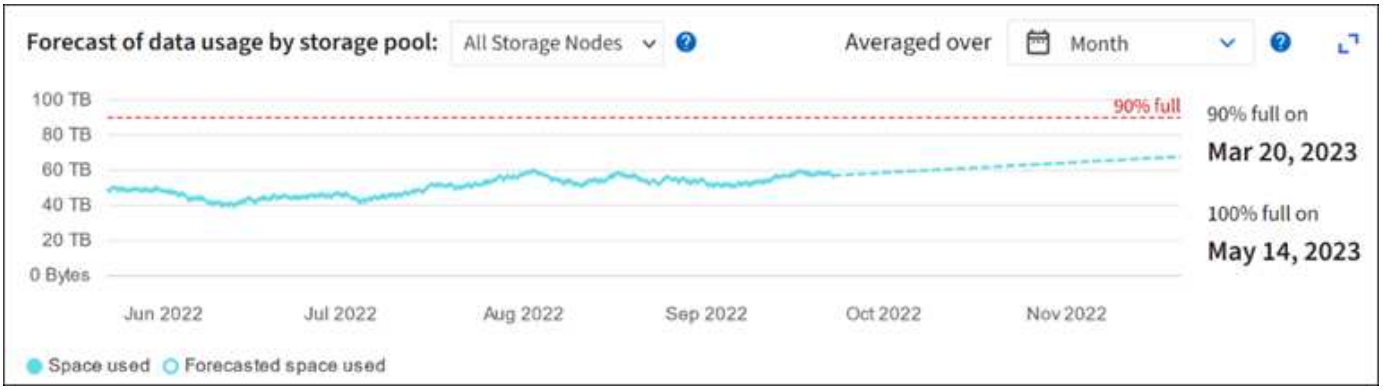
监控用户数据和元数据的空间使用情况预测、以估算何时需要 "扩展网格"。

如果您注意到消耗率随时间的变化、请从*平均值超过*下拉列表中选择一个较短的范围、以仅反映最新的接收模式。如果您注意到季节性模式、请选择更长的范围。

如果您安装了新的StorageGRID 、请在评估空间使用量预测之前、先累积数据和元数据。

步骤

1. 在信息板上，选择*Storage*。
2. 查看信息板卡、按存储池显示的数据使用情况预测以及按站点显示的元数据使用情况预测。
3. 使用这些值可估算何时需要为数据和元数据存储添加新存储节点。



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。

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。

对象加载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。您应监控StorageGRID是否与客户端操作保持一致。

使用**Grid Manager**信息板选项卡

步骤

使用网格管理器信息板上的ILM选项卡监控ILM操作：

1. 登录到网格管理器。
2. 从信息板中、选择ILM选项卡、并记下ILM队列(对象)卡和ILM评估速率卡上的值。

   信息板上的ILM队列(对象)卡可能会出现临时峰值。但是、如果队列持续增加而从未减少、网格需要更多资源才能高效运行：要么增加存储节点、要么增加ILM策略将对象放置在远程位置的网络带宽。

使用节点页面

步骤

此外，请使用*N节点*页调查ILM队列：

> 在未来的StorageGRID版本中，*节点*页面上的图表将替换为相应的信息板卡。

1. 选择 * 节点 * 。
2. 选择 * 网格名称 _* > * ILM * 。
3. 将光标置于ILM队列图上方、可查看在给定时间点的以下属性值：
   - * 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队列部分仅适用于网格。此信息不会显示在站点或存储节点的 "ILM " 选项卡上。

   - 扫描期限-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的总数。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。如果尝试的维修次数停止增加、并且已完成完全扫描、则修复可能已完成。

节点和站点之间网络的完整性和带宽以及各个网格节点的资源使用情况对于高效运营至关重要。

监控网络连接和性能

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。如果为ILM规则选择了严格的写入选项、则可能会导致写入失败、或者导致写入性能不佳和ILM积压。

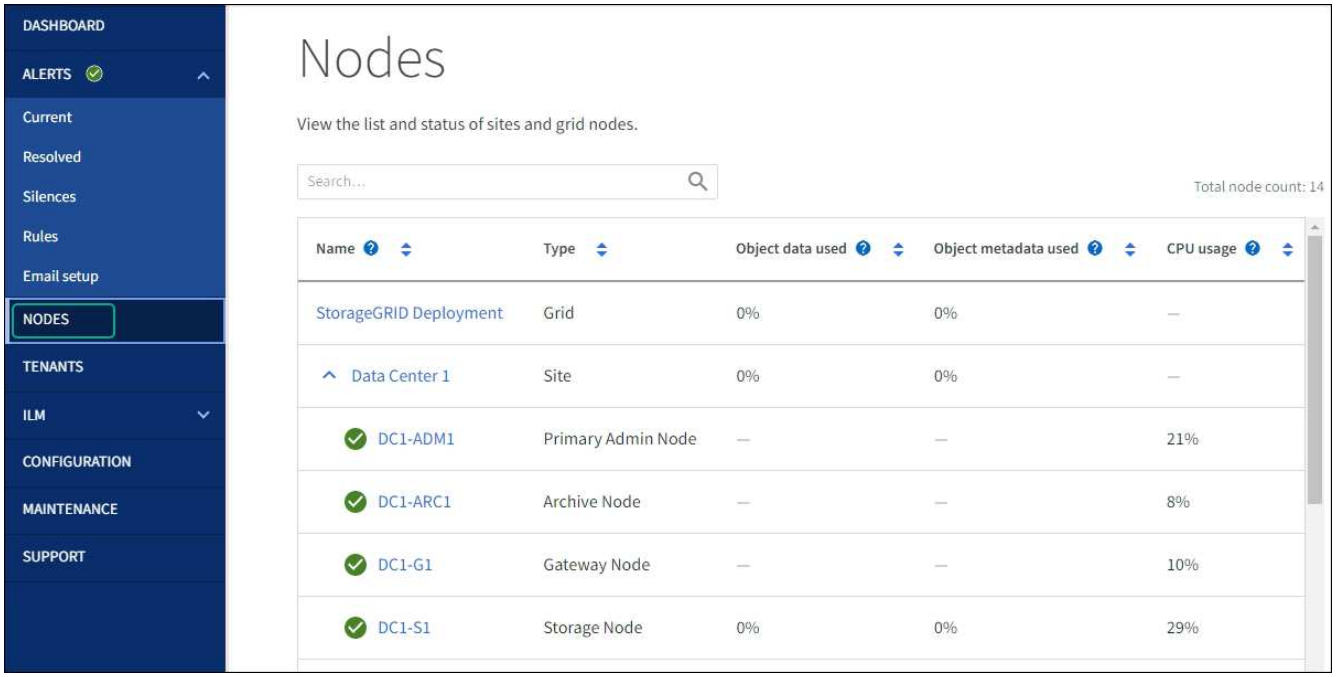
使用网格管理器监控连接和网络性能、以便及时解决任何问题。

此外、请考虑 "创建网络流量分类策略" 以便监控与特定租户、分段、子网或负载平衡器端点相关的流量。您可以根据需要设置流量限制策略。

步骤

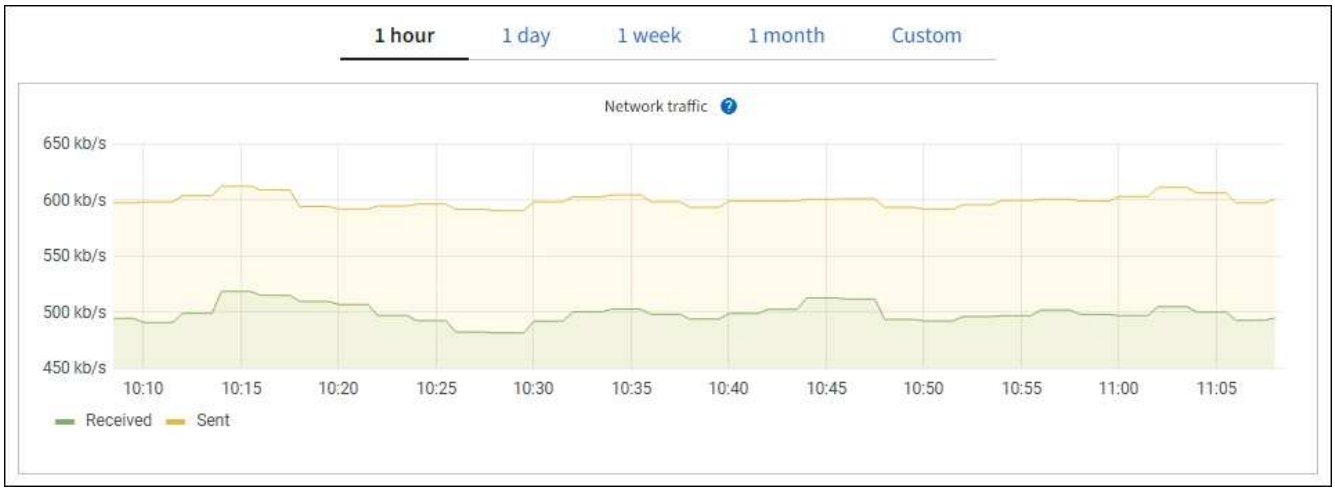
1. 选择 * 节点 * 。

   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

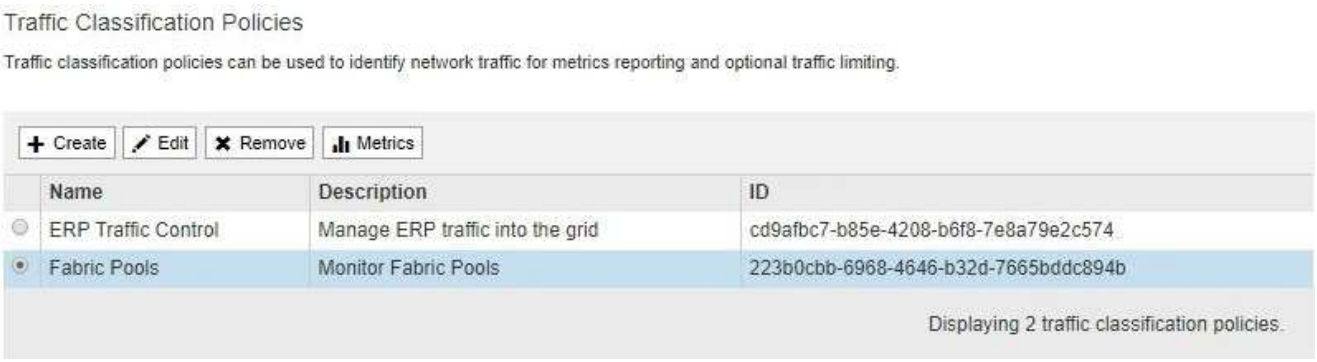
Transmit

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。



a. 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 * 。

b. 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。不时、 "根据需要调整每个流量分类策略"。

相关信息

"查看网络选项卡"

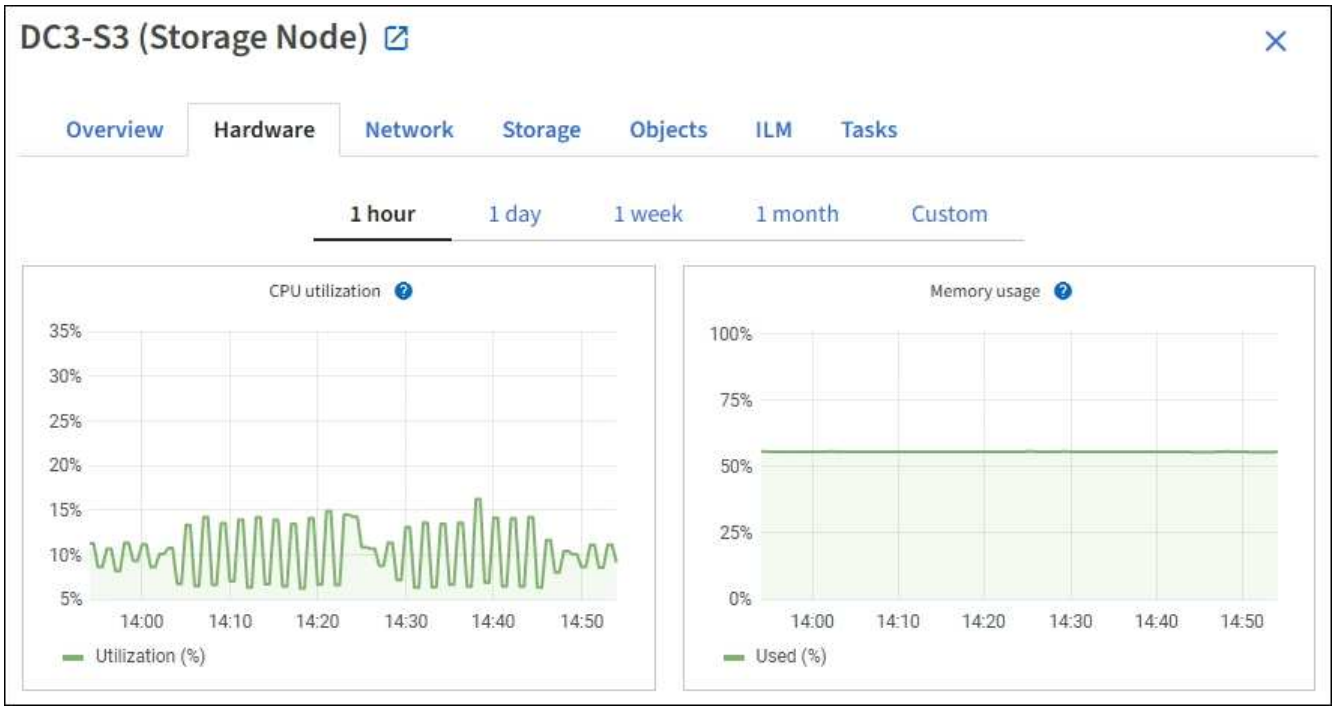
"监控节点连接状态"

监控节点级资源

监控各个网格节点以检查其资源使用情况。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. 从 * 节点 * 页面中，选择节点。
2. 选择 * 硬件 * 选项卡以显示 CPU 利用率和内存使用情况的图形。



3. 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。
4. 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"。 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S3和Swift客户端活动都与StorageGRID 租户帐户相关联。您可以使用网格管理器监控所有租户或特定租户的存储使用情况或网络流量。您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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限或租户帐户权限"。

查看所有租户

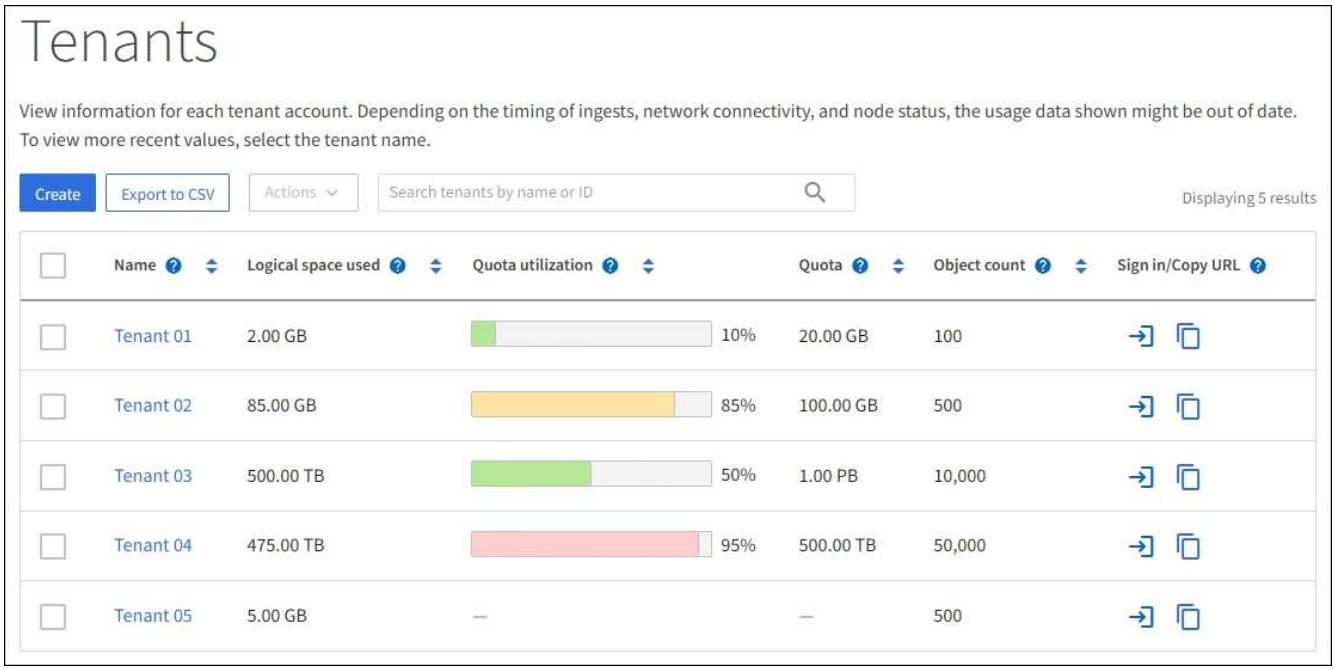
租户页面显示所有当前租户帐户的基本信息。

步骤

1. 选择 * 租户 * 。
2. 查看租户页面上显示的信息。

   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 ；）。

   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。



3. (可选)通过选择登录链接登录到租户帐户 在*登录/复制URL*列中。
4. (可选)通过选择复制URL链接复制租户登录页面的URL 在*登录/复制URL*列中。
5. (可选)选择*导出至CSV-*以查看和导出 `.csv` 包含所有租户的使用量值的文件。

   系统将提示您打开或保存 `.csv` 文件

   的内容 `.csv` 文件类似于以下示例：

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

   您可以打开 `.csv` 文件或在自动化中使用。

6. 如果未列出任何对象，也可以选择*Actions*>*Delete*以删除一个或多个租户。请参见 "删除租户帐户"。

   如果租户帐户包含任何分段或容器、则不能删除该帐户。

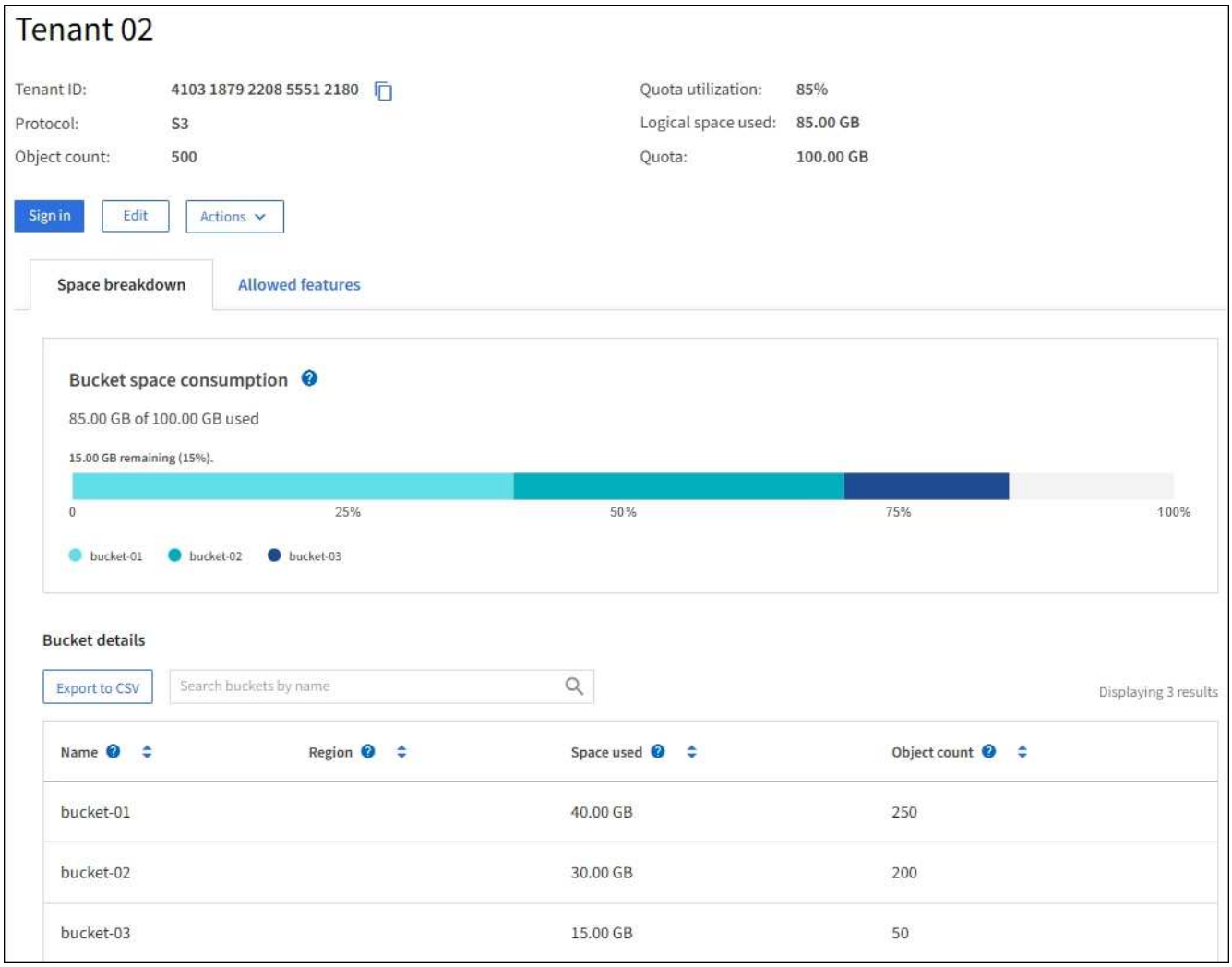
查看特定租户

您可以查看特定租户的详细信息。

步骤

1. 从租户页面中选择租户名称。

   此时将显示租户详细信息页面。



2. 查看页面顶部的租户概述。

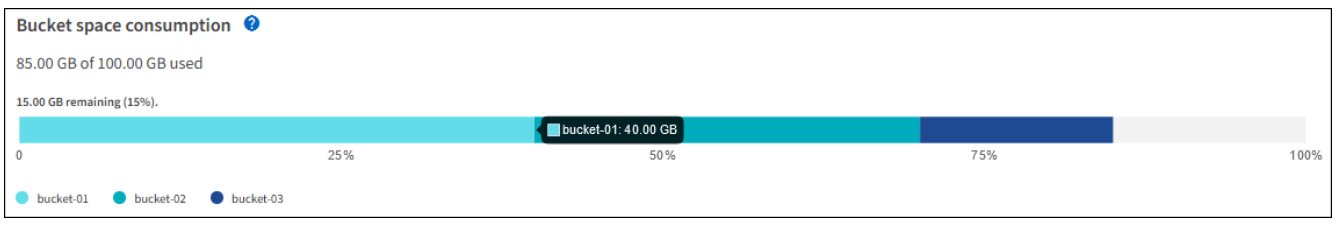
   此部分详细信息页面提供了租户的摘要信息、包括租户的对象计数、配额利用率、已用逻辑空间和配额设置。

3. 在*空间细分*选项卡中，查看*空间消耗*图表。

   此图表显示租户的所有S3存储分段(或Swift容器)的总空间消耗。

   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`）。如果未设置任何配额、则租户具有无限配额、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*警报规则来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。有关说明，请参见 "编辑警报规则"。

4. 在*空间细分*选项卡中、查看*存储分段详细信息*。

   此表列出了租户的S3存储分段(或Swift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。

5. 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租户的内容 `.csv` 文件类似于以下示例：

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

   您可以打开 `.csv` 文件或在自动化中使用。

6. (可选)选择*允许的功能*选项卡以查看为租户启用的权限和功能列表。请参见 "编辑租户帐户" 如果需要更改其中任何设置。
7. 如果租户具有*使用网格联合连接*权限，则可以选择*网格联合*选项卡以了解有关连接的更多信息。

   请参见 "什么是网格联合？ " 和 "管理网格联盟允许的租户"。

查看网络流量

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。

步骤

1. 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。

2. 查看策略列表以确定适用于特定租户的策略。
3. 要查看与策略关联的指标，请选择策略左侧的单选按钮，然后选择*Metrics*。
4. 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。

请参见 "管理流量分类策略" 有关详细信息 …

使用审核日志

您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。

请参见 "查看审核日志" 有关详细信息 …

使用**Prometheus**指标

(可选)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。

- 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。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。

请参见 "查看支持指标" 有关详细信息 …

监控**S3**和**Swift**客户端操作

您可以监控对象载入和检索速率，以及对象计数，查询和验证的指标。您可以查看客户端应用程序在 StorageGRID 系统中成功尝试读取，写入和修改对象的次数和失败的尝试次数。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

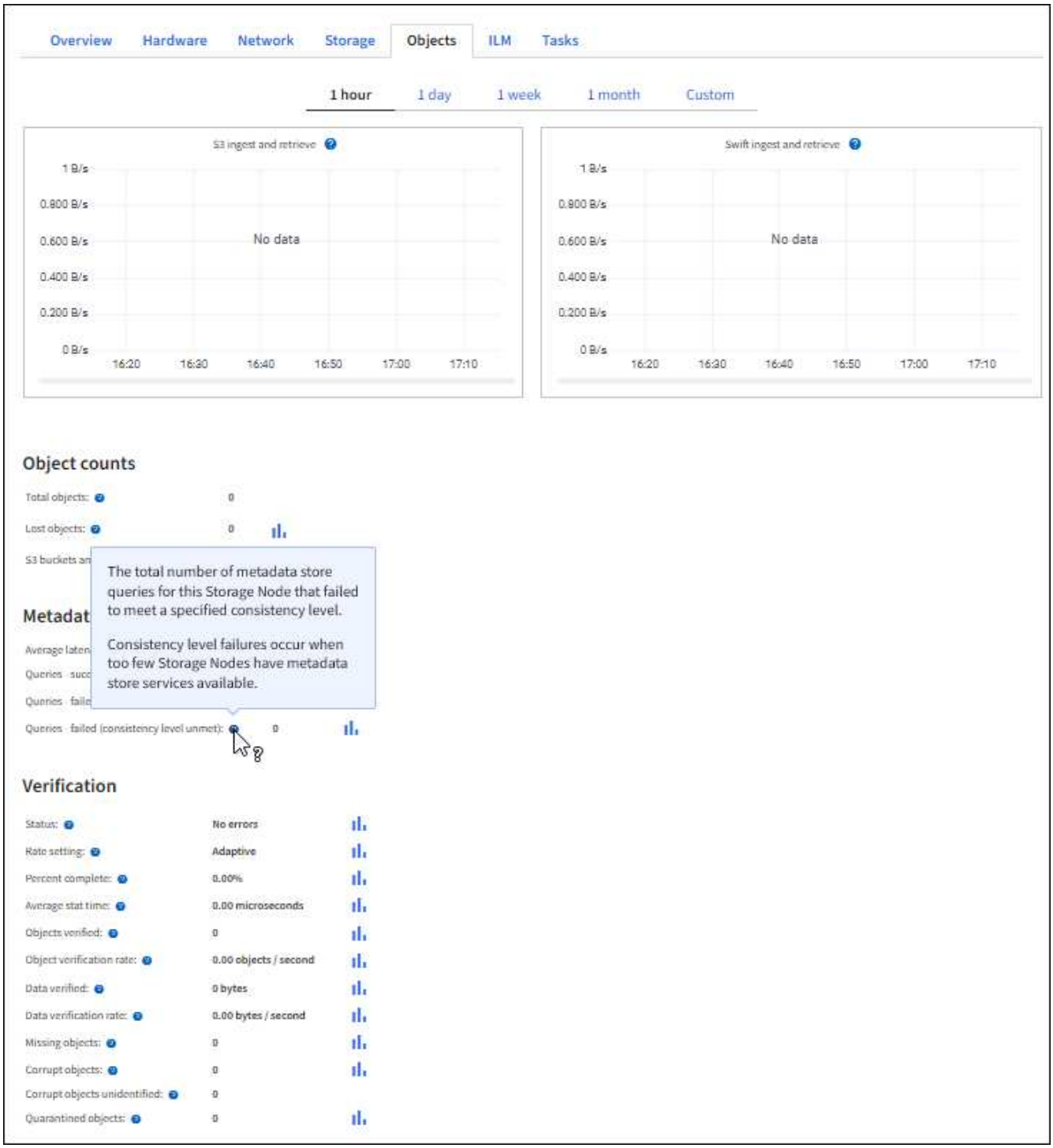
步骤

1. 从信息板中，选择*Performance*选项卡。
2. 请参见S3和Swift图表、其中汇总了在选定时间范围内存储节点执行的客户端操作数以及存储节点收到的API请求数。
3. 选择*N节点*以访问节点页面。
4. 从节点主页(网格级)中，选择*Objects*选项卡。

   该图表显示整个StorageGRID系统的S3和Swift加载和检索速率(以字节/秒为单位)以及加载或检索的数据量。您可以选择时间间隔或应用自定义间隔。

5. 要查看特定存储节点的信息，请从左侧列表中选择节点，然后选择*Objects*选项卡。

   此图表将显示节点的加热和检索速率。该选项卡还包括对象计数、元数据查询和验证操作的指标。



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。

关于此任务

您可以在管理节点、网关节点或外部第三方负载平衡器上使用负载平衡器服务在多个存储节点之间分布客户端请求。

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。

有关详细信息，请参见 "配置 S3 和 Swift 客户端连接"。

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*Overview*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Primary角色。

      角色为Primary的节点以及不属于HA组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、请选择 "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. (可选)使用流量分类策略查看负载平衡器服务提供的流量的更详细分析。
2. 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。

监控网格联合连接

您可以监控所有的基本信息 "网格联合连接"、有关特定连接的详细信息或有关跨网格复制操作的Prometheus指标。您可以从任一网格监控连接。

开始之前

- 您已使用登录到任一网格上的网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限" 已登录到的网格。

查看所有连接

"网格联盟"页面显示有关所有网格联盟连接以及允许使用网格联盟连接的所有租户帐户的基本信息。

步骤

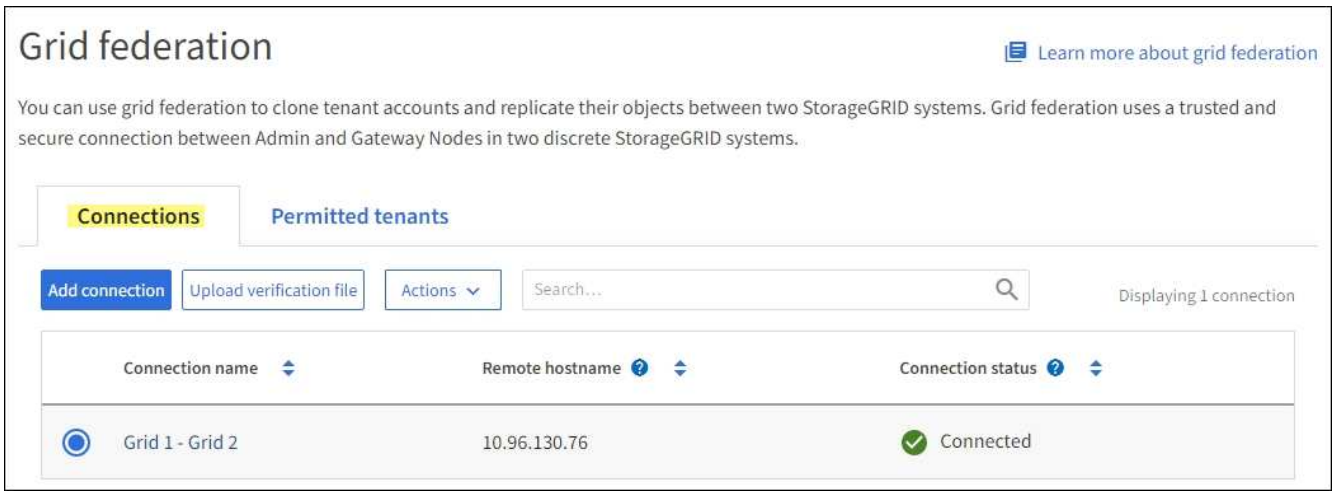
1. 选择*configuration*>*System*>*Grid Federation。

   此时将显示Grid Federation页面。

2. 要查看此网格上所有连接的基本信息，请选择*Connections*选项卡。

   在此选项卡中、您可以：

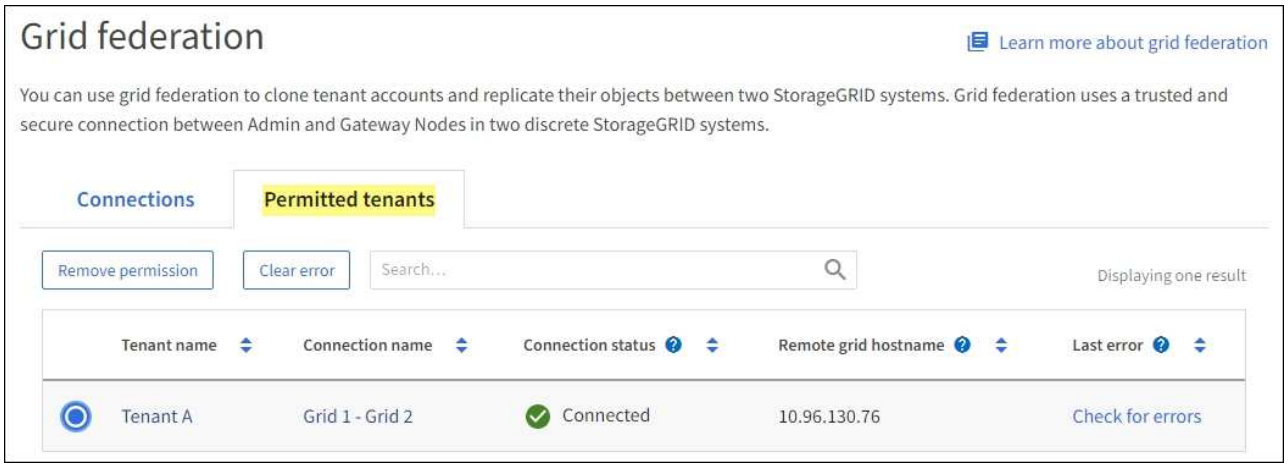
   - "创建新连接"。
   - 选择与的现有连接 "编辑或测试"。



3. 要查看此网格上具有*使用网格联合连接*权限的所有租户帐户的基本信息、请选择*允许的租户*选项卡。

   在此选项卡中、您可以：

   - "查看每个允许租户的详细信息页面"。
   - 查看每个连接的详细信息页面。请参见 查看特定连接。
   - 选择允许的租户、然后 "删除权限"。
   - 检查是否存在跨网格复制错误、如果有、请清除最后一个错误。请参见 "对网格联合错误进行故障排除"。



查看特定连接

您可以查看特定网格联合连接的详细信息。

步骤

1. 从"网格联合"页面中选择任一选项卡、然后从表中选择连接名称。

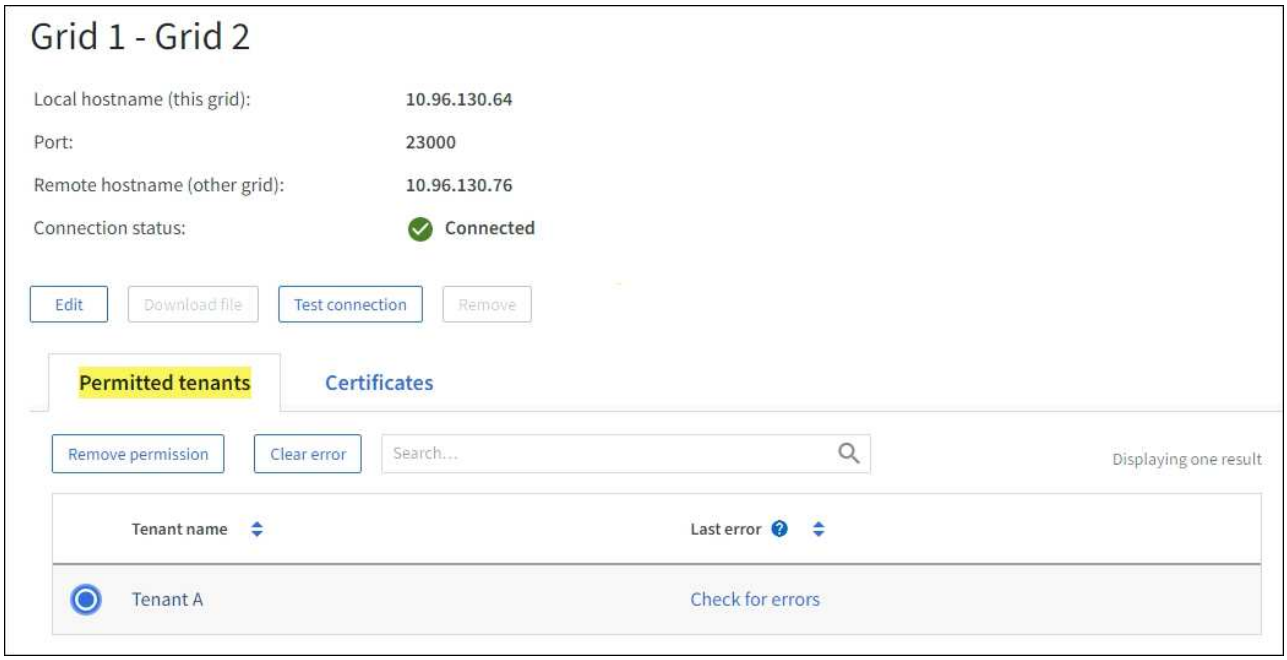
   在连接的详细信息页面中、您可以：

   - 查看有关连接的基本状态信息、包括本地和远程主机名、端口和连接状态。
   - 选择与的连接 "编辑、测试或删除"。

2. 查看特定连接时，请选择*允许的租户*选项卡以查看有关该连接允许的租户的详细信息。

   在此选项卡中、您可以：

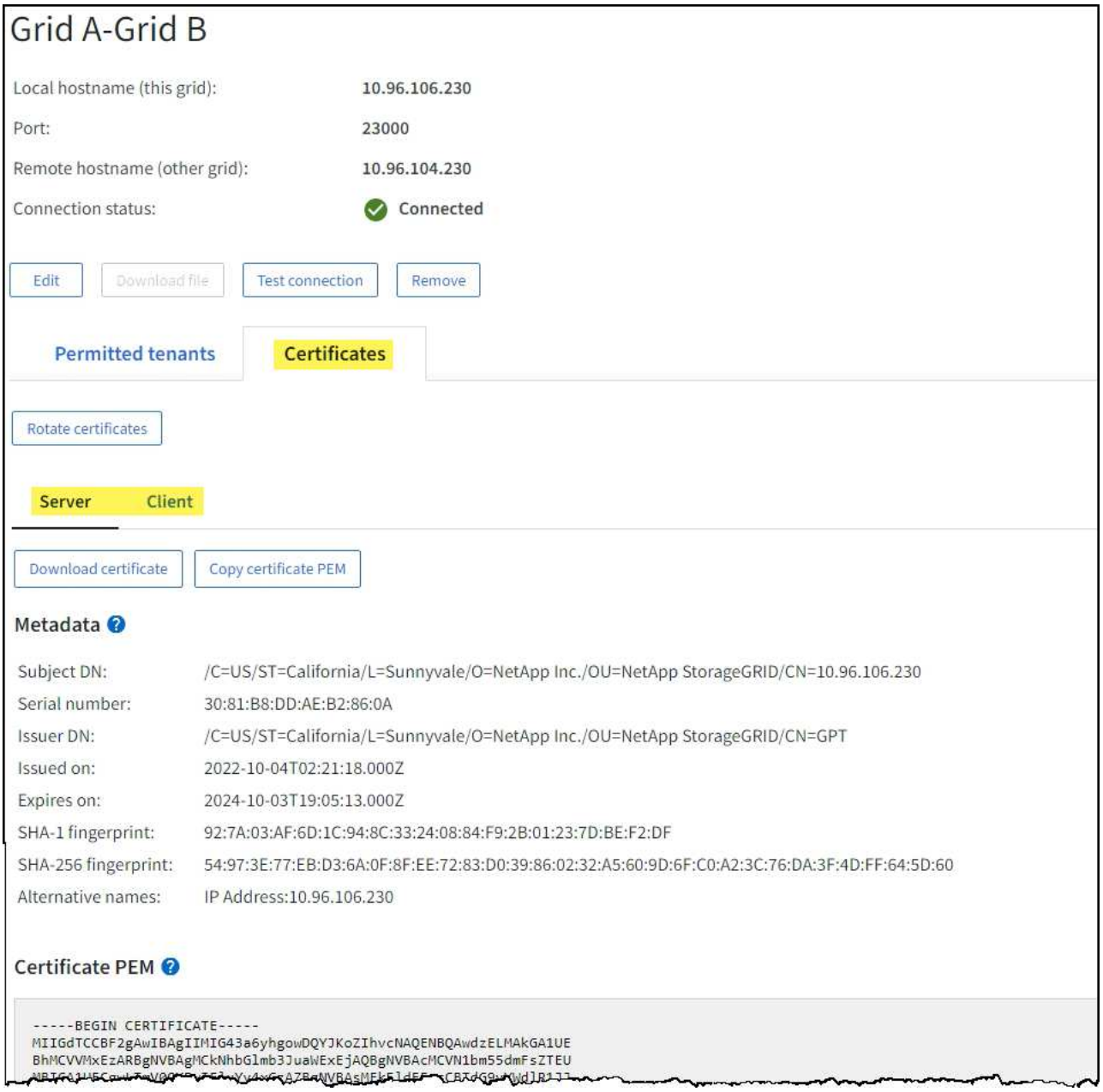
   - "查看每个允许租户的详细信息页面"。
   - "删除租户的权限" 可使用连接。
   - 检查是否存在跨网格复制错误、并清除最后一个错误。请参见 "对网格联合错误进行故障排除"。



3. 查看特定连接时，选择*Certificates*选项卡以查看系统为此连接生成的服务器和客户机证书。

   在此选项卡中、您可以：

   - "轮换连接证书"。
   - 选择*服务器*或*客户端*以查看或下载关联的证书或复制证书PEM。



查看跨网格复制指标

您可以使用Grafana中的跨网格复制信息板查看有关网格上跨网格复制操作的Prometheus指标。

步骤

1. 在网格管理器中，选择*support*>*Tools*>*Metrics *。

   > 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"。

2. 在页面的Grafana部分中，选择*跨网格复制*。

   有关详细说明、请参见 "查看支持指标"。

3. 要重试复制无法复制的对象、请参见 "确定并重试失败的复制操作"。

监控归档容量

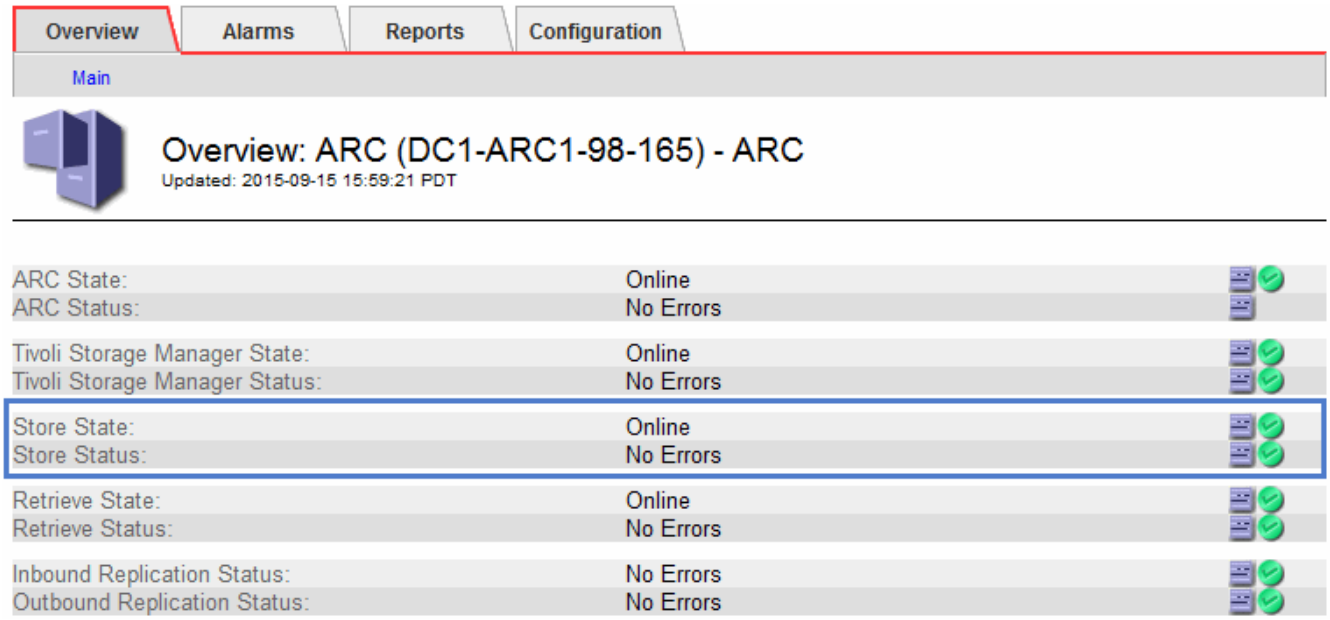
您不能通过StorageGRID 系统直接监控外部归档存储系统的容量。但是，您可以监控归档节点是否仍可将对象数据发送到归档目标，这可能表示需要扩展归档介质。

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。

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：

- 在网格管理器的信息板上会显示警报严重性图标、当前警报的计数将递增。
- 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。(不会针对所有警报或警报严重程度发送SNMP通知。)

比较警报和警报

警报系统和传统警报系统之间有几个相似之处、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）"

	警报	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）"
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 * 。 "查看当前警报和已解决警报"	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。 • 您必须同时具有网格拓扑页面配置和其他网格配置权限、才能管理全局警报和电子邮件通知。 "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"	不支持

	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(首选发送方)。 "什么是管理节点？"	一个管理节点(首选发送方)。 "什么是管理节点？"
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"	不支持
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. 清除*Enabled"(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. 清除*Enabled"(已启用)复选框。 "管理警报（旧系统）"

管理警报

管理警报：概述

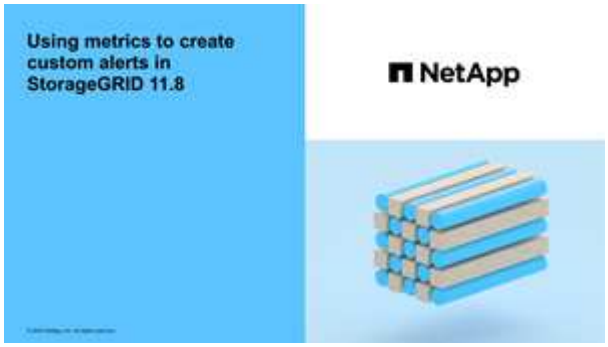
警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

您可以创建自定义警报、编辑或禁用警报以及管理警报通知。

了解更多信息：

- 观看视频： "视频：StorageGRID 11.8."

- 观看视频： "视频：在StorageGRID 11.8.中使用指标创建自定义警报"



- 请参见 "警报参考"。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root访问权限"。
- 您也可以观看以下视频： "视频：StorageGRID 11.8."

步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

Alert Rules Learn more

Alert rules define which conditions trigger specific alerts.

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

+ Create custom rule | Edit rule | Remove custom rule

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

Displaying 62 alert rules.

2. 查看警报规则表中的信息：

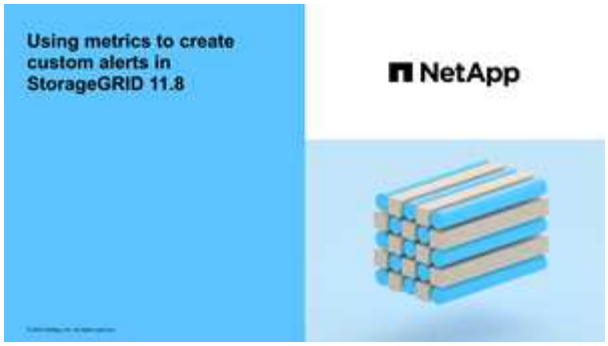
列标题	Description
Name	警报规则的唯一名称和问题描述 。首先列出自定义警报规则，然后列出默认警报规则。警报规则名称是电子邮件通知的主题。
条件	用于确定何时触发此警报的 Prometheus 表达式。可以在以下一个或多个严重性级别触发警报，但不需要为每个严重性设置一个条件。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 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。您应监控和解决无法自行清除的次要警报、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。您无法删除默认警报规则。 • * 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。系统不会评估已禁用警报规则的条件、因此不会触发警报。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root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：在StorageGRID 11.8.中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。
- 使用网格管理API测试表达式时、请注意、"成功"响应可能是空响应正文(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、用于测试表达式 `node_memory_MemTotal_bytes < 24000000000`、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。

- 除非您已验证自定义警报是按预期触发的、否则不要假定该警报正常工作。

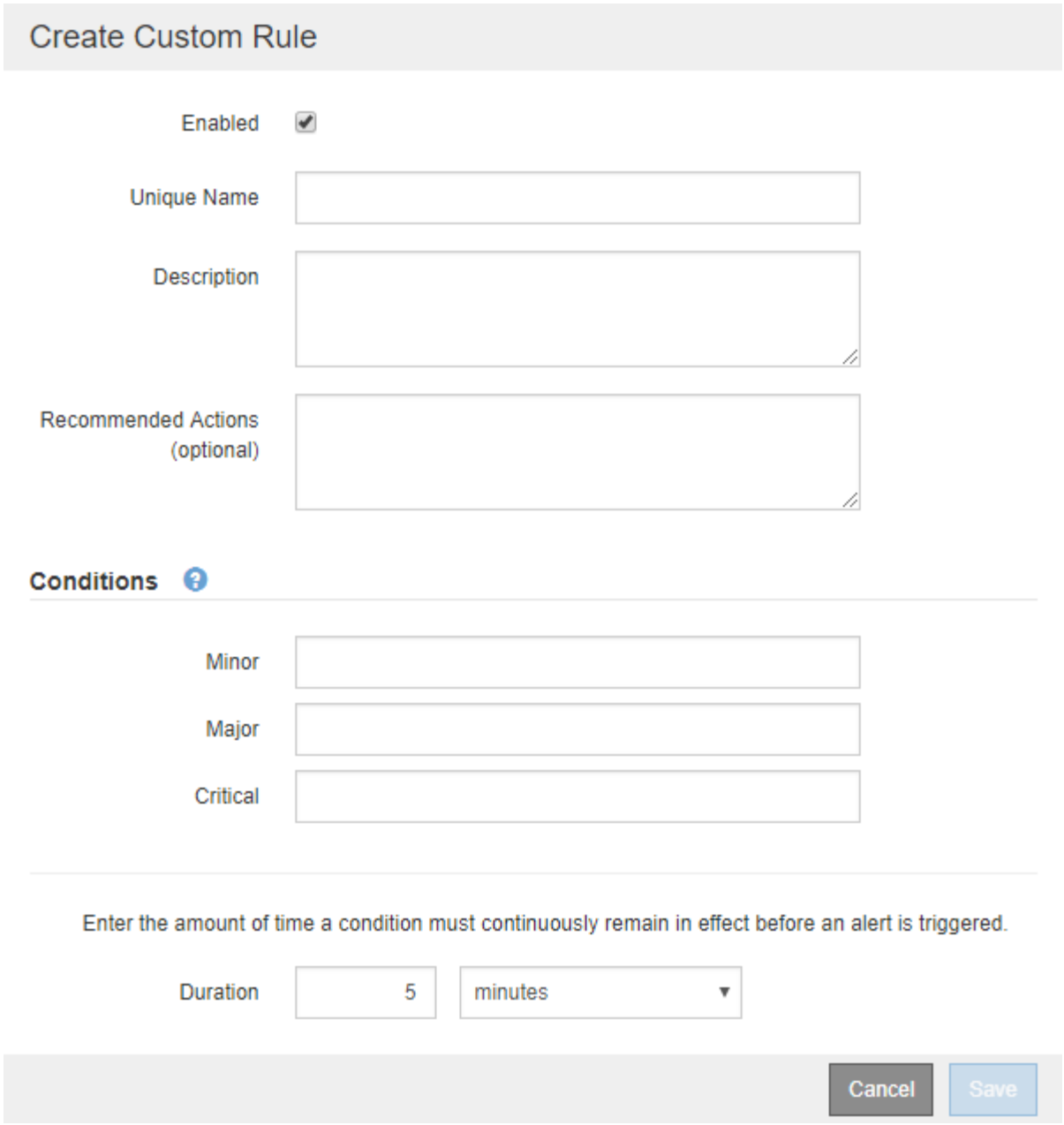
步骤

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. 选中或清除*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、则不会对其表达式进行评估、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：

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

   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 < 24000000000
   ```

   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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root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。

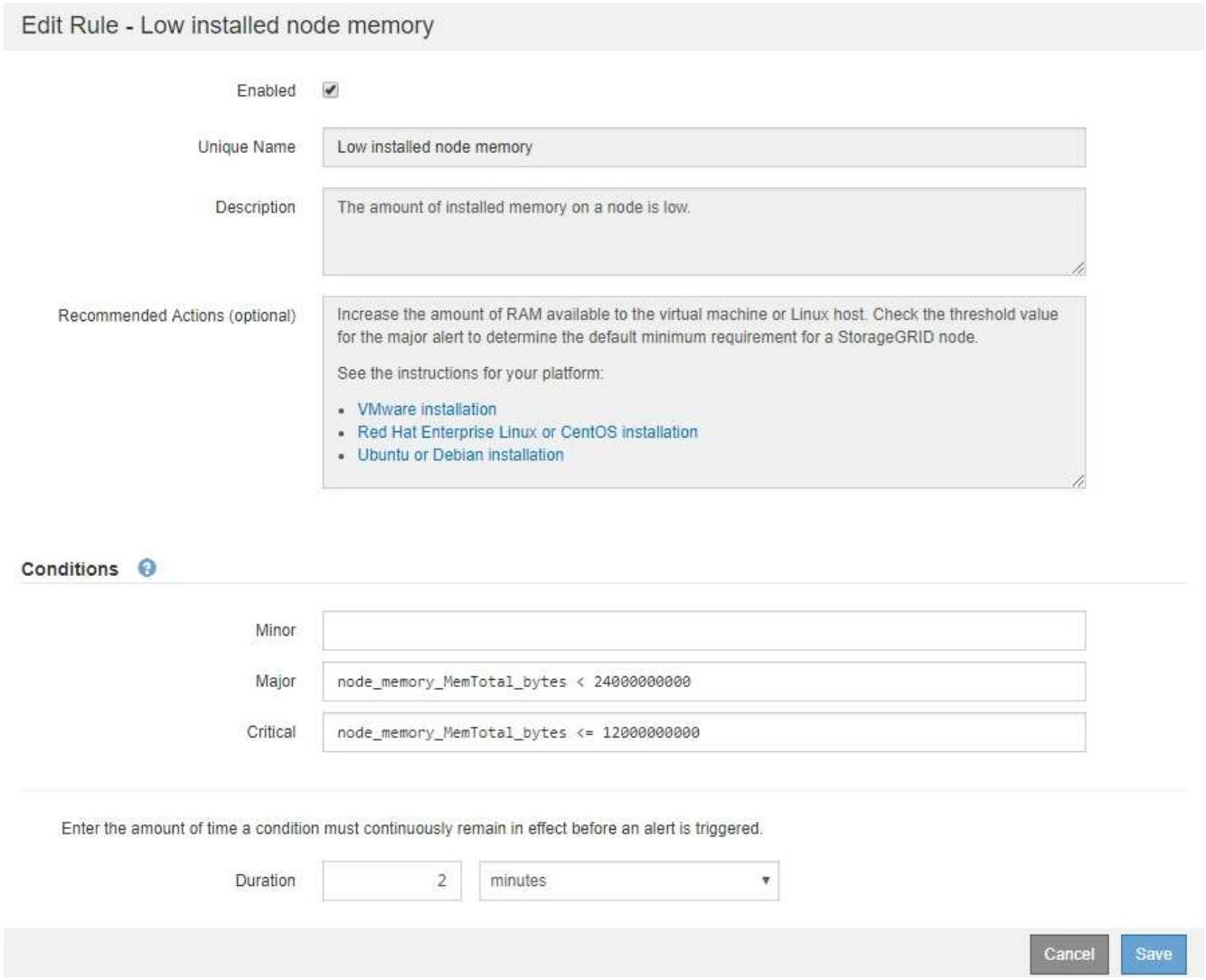
步骤

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：“唯一名称”、“问题描述 ”和“建议操作”字段已禁用，无法编辑。



4. 选中或清除*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、则不会对其表达式进行评估、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。

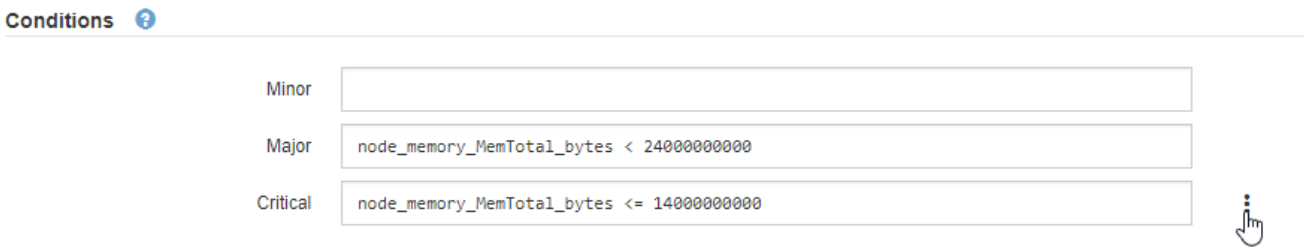
5. 对于自定义警报规则，请根据需要更新以下信息。

您无法编辑默认警报规则的此信息。

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：

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

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 < 24000000000
```

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root访问权限"。

关于此任务

禁用警报规则后、不会对其表达式进行评估、也不会触发警报。

> 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. 选中或清除*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、则不会对其表达式进行评估、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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root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。

您无法删除默认警报规则。

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：

- 陷阱是由SNMP代理发送的通知、不需要管理系统进行确认。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"。

如果您的StorageGRID部署包含多个管理节点、则主管理节点是警报通知、AutoSupport软件包、SNMP陷阱和通知以及原有警报通知的首选发送方。如果主管理节点不可用、则其他管理节点会临时发送通知。请参见 "什么是管理节点？"。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root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用于警报通知和AutoSupport软件包。但是，您可以对所有通知使用同一个电子邮件服务器。

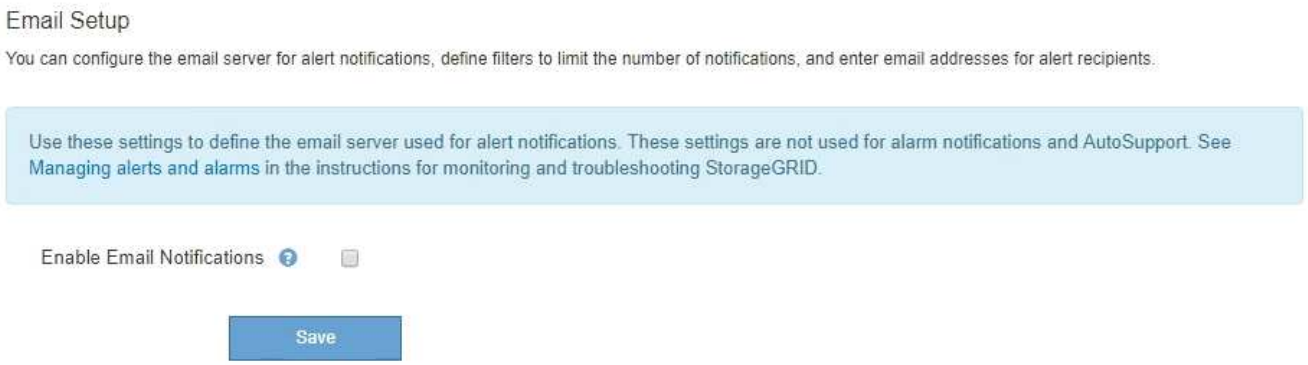
如果您的StorageGRID部署包含多个管理节点、则主管理节点是警报通知、AutoSupport软件包、SNMP陷阱和

通知以及原有警报通知的首选发送方。如果主管理节点不可用、则其他管理节点会临时发送通知。请参见 "什么是管理节点？"。

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客户端证书以进行身份验证，请选中*发送客户端证书*复选框。

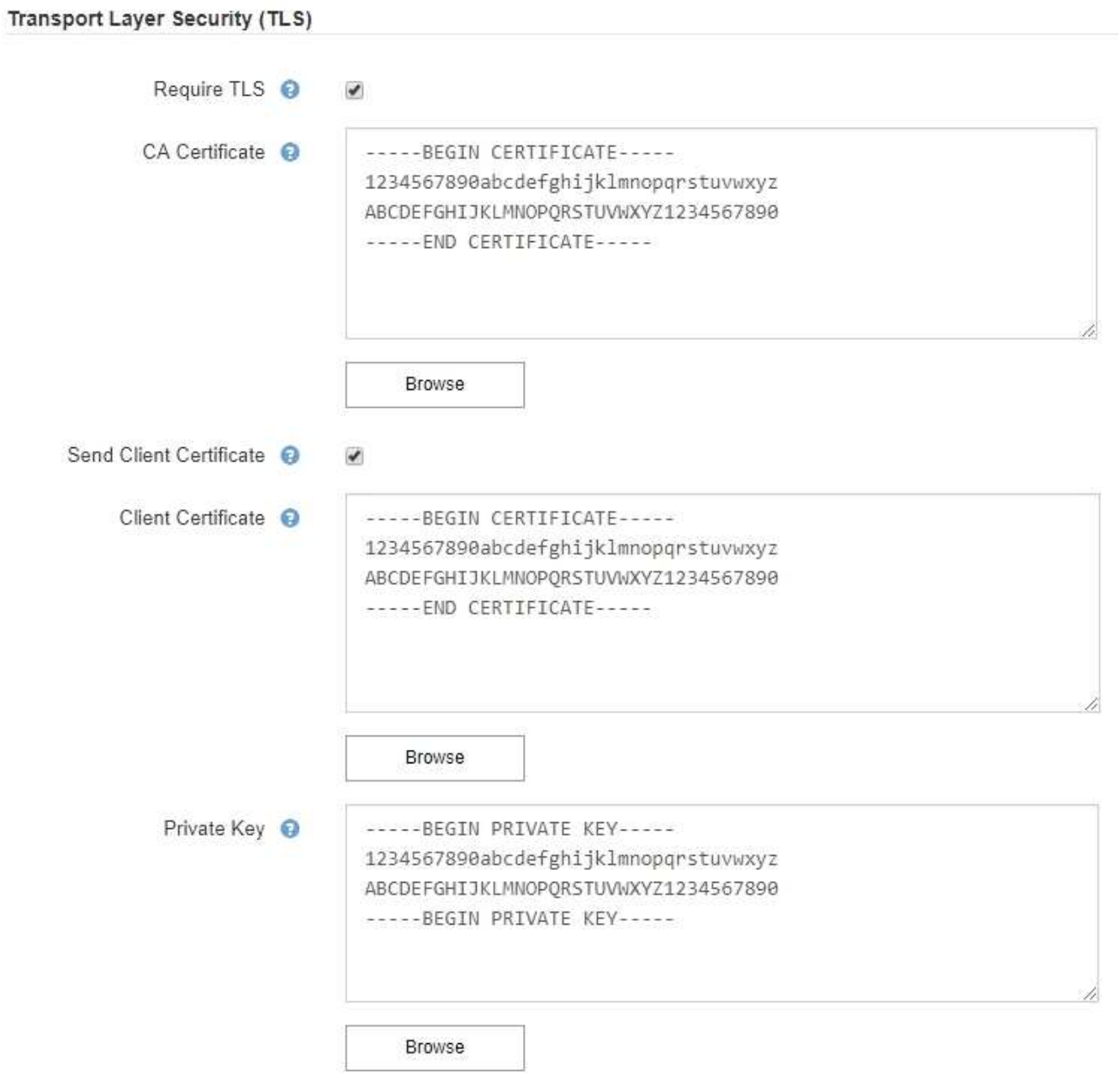
c. 在 * 客户端证书 * 字段中，提供 PEM 编码的客户端证书以发送到 SMTP 服务器。

   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。不会针对次要或重大警报发送通知。

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AutoSupport软件包和传统警报通知不同、所有管理节点都会发送测试电子邮件。

8. 选择 * 保存 * 。

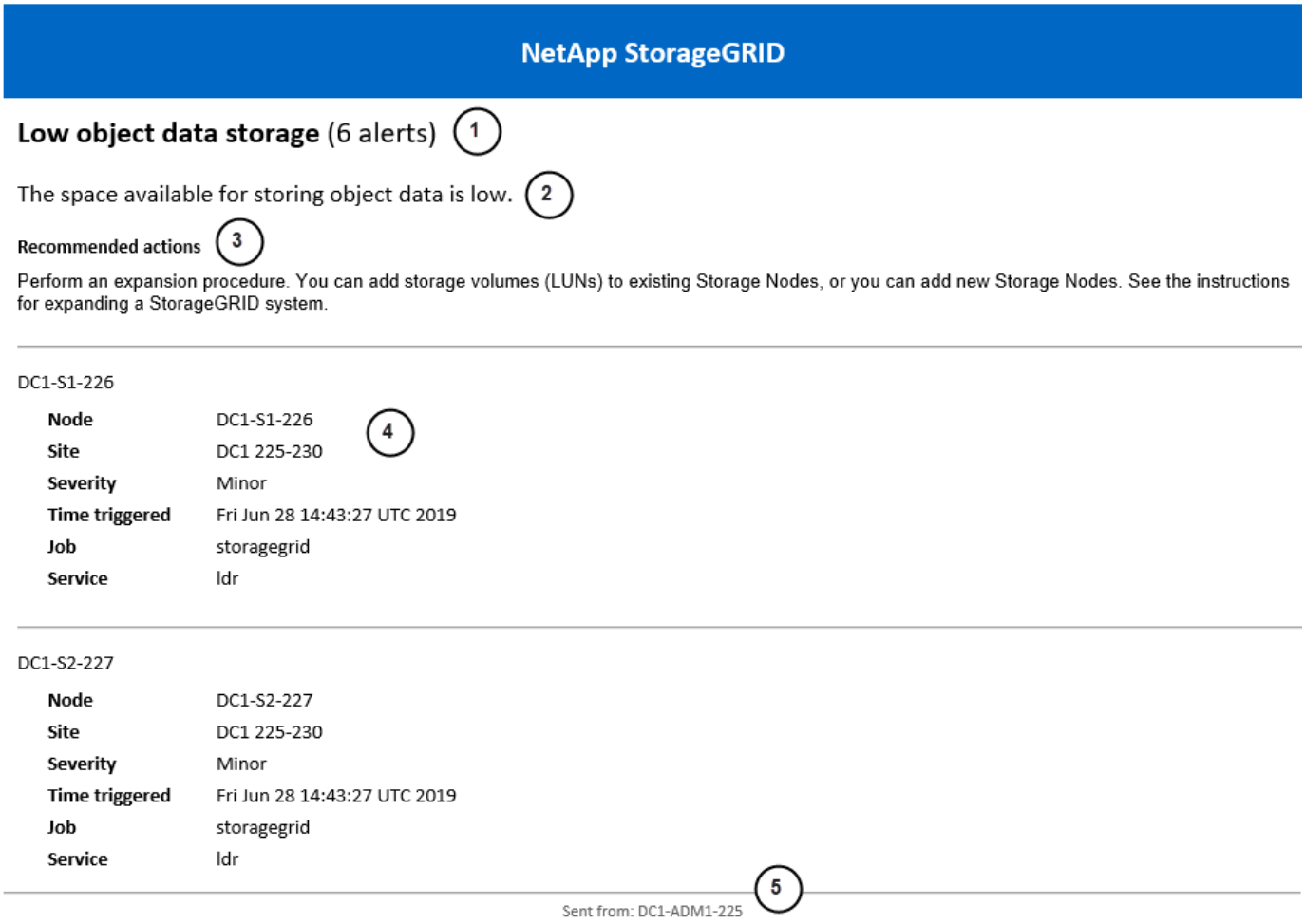
   发送测试电子邮件不会保存您的设置。您必须选择 * 保存 * 。

   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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root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来自发件人地址的电子邮件未被阻止。
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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "管理警报或root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。

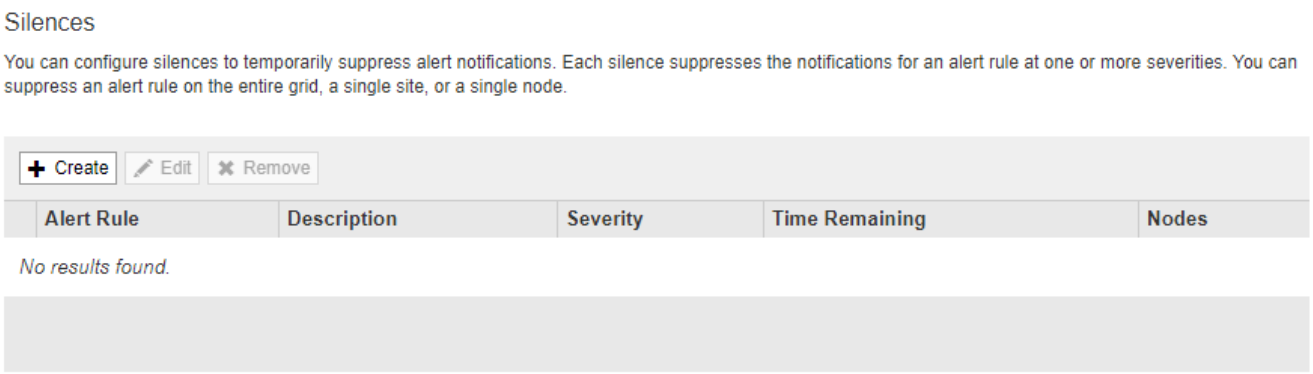
在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

由于警报和警报是独立的系统、因此不能使用此功能来禁止警报通知。

步骤

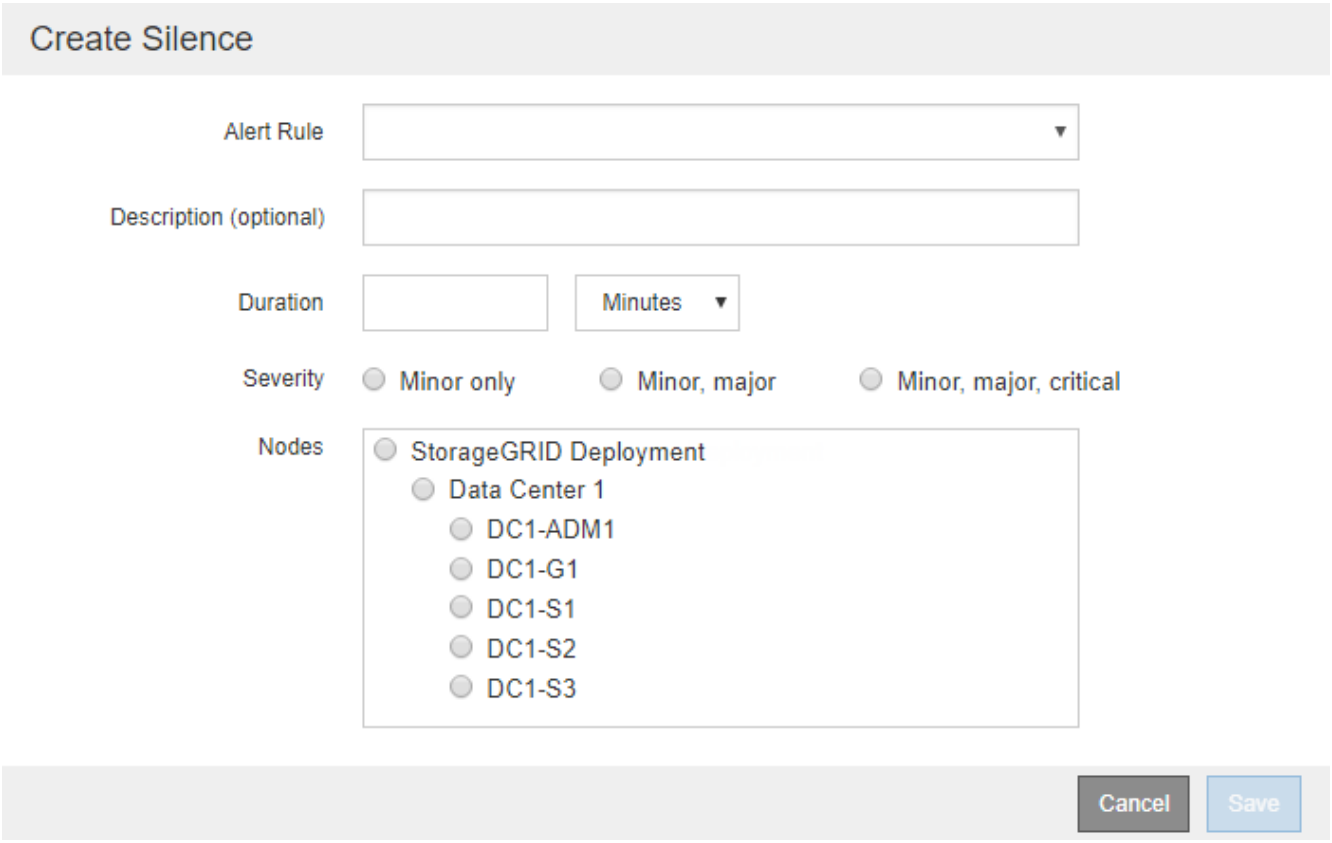
1. 选择 * 警报 * > * 静音 * 。

   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"

警报参考

此参考列出了网格管理器中显示的默认警报。建议的操作会显示在您收到的警报消息中。

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。

某些默认警报使用 "Prometheus 指标"。

设备警报

警报名称	Description
设备电池已过期	设备存储控制器中的电池已过期。
设备电池出现故障	设备存储控制器中的电池出现故障。
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。
设备电池即将过期	设备存储控制器中的电池即将过期。
已取出设备电池	设备存储控制器中的电池缺失。
设备电池过热	设备存储控制器中的电池过热。
设备 BMC 通信错误	与基板管理控制器（ BMC ）的通信已丢失。
设备缓存备份设备失败	永久性缓存备份设备出现故障。
设备缓存备份设备容量不足	缓存备份设备容量不足。
设备缓存备份设备已写保护	缓存备份设备受写保护。
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。
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。
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。
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。
设备计算控制器电源 A 出现问题	计算控制器中的电源A出现问题。
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。
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。

警报名称	Description
设备DAS驱动器超过每天写入数据的限制	每天向驱动器写入的数据量过多、这可能会使其保修失效。
检测到设备DAS驱动器故障	检测到设备中的直连存储(DAS)驱动器存在问题。
设备DAS驱动器定位灯亮起	设备存储节点中的一个或多个直连存储(DAS)驱动器的驱动器定位灯亮起。
设备DAS驱动器正在重建	正在重建直连存储(DAS)驱动器。如果最近更换或移除/重新插入、则这是预期的。
检测到设备风扇故障	检测到产品中的风扇装置有问题。
检测到设备光纤通道故障	检测到设备存储控制器与计算控制器之间存在光纤通道链路问题
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。
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。
已卸下设备互连 / 电池箱	互连 / 电池箱缺失。
缺少设备 LACP 端口	StorageGRID 设备上的端口不参与 LACP 绑定。
检测到设备NIC故障	检测到设备中的网络接口卡(NIC)有问题。
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。
设备SSD严重警告	设备SSD报告严重警告。
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。
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。
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。
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 " 。
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。
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。
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。

警报名称	Description
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。
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。
已卸下设备温度传感器	已卸下温度传感器。
设备UEFI安全启动错误	设备未安全启动。
磁盘 I/O 速度非常慢	磁盘I/O非常慢可能会影响网格性能。
检测到存储设备风扇故障	检测到设备存储控制器中的风扇单元出现问题。
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。
无法访问存储设备	无法访问存储设备。

审核和系统日志警报

警报名称	Description
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。
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。
审核队列较大	审核消息的磁盘队列已满。如果不解决此问题、S3或Swift操作可能会失败。
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。

存储分段警报

警报名称	Description
FabricPool 存储分段具有不受支持的存储分段一致性设置	FabricPool分段使用可用或强站点一致性级别、这种级别不受支持。

Cassandia警报

警报名称	Description
Cassandra auto-compactor 错误	Cassandra 自动 compactor 出现错误。

警报名称	Description
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 通信错误	运行 Cassandra 服务的节点无法彼此通信。
Cassandra compActions 已过载	Cassandra 数据缩减过程过载。
Cassand拉 特写错误	内部StorageGRID 进程向Cassanda发送了一个过大的写入请求。
Cassandra 修复指标已过期	描述 Cassandra 修复作业的指标已过时。
Cassandra 修复进度缓慢	Cassandra 数据库修复进度缓慢。
Cassandra 修复服务不可用	Cassandra 修复服务不可用。
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。

云存储池警报

警报名称	Description
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。

跨网格复制警报

警报名称	Description
跨网格复制永久失败	发生跨网格复制错误、需要用户干预才能解决。
跨网格复制资源不可用	由于资源不可用、跨网格复制请求处于待处理状态。

DHCP警报

警报名称	Description
DHCP 租约已过期	网络接口上的 DHCP 租约已过期。
DHCP 租约即将到期	网络接口上的 DHCP 租约即将到期。
DHCP 服务器不可用	DHCP 服务器不可用。

调试和跟踪警报

警报名称	Description
调试性能影响	启用调试模式后、系统性能可能会受到负面影响。
已启用跟踪配置	启用跟踪配置后、系统性能可能会受到负面影响。

电子邮件和**AutoSupport** 警报

警报名称	Description
无法发送AutoSupport 消息	无法发送最新的AutoSupport 消息。
电子邮件通知失败	无法发送警报电子邮件通知。

纠删编码**(EC)**警报

警报名称	Description
EC 重新平衡失败	EC重新平衡操作步骤 失败或已停止。
EC 修复失败	EC数据的修复作业失败或已停止。
EC 修复已停止	EC数据的修复作业已停止。

证书到期警报

警报名称	Description
管理代理CA证书到期	管理代理服务器CA包中的一个或多个证书即将过期。
客户端证书到期	一个或多个客户端证书即将过期。
S3和Swift的全局服务器证书到期	S3和Swift的全局服务器证书即将过期。
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。
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。
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。
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。

警报名称	Description
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。

网格网络警报

警报名称	Description
网格网络 MTU 不匹配	网格网络接口(eth0)的MTU设置在网格中的各个节点之间差别很大。

网格联盟警报

警报名称	Description
网格联合证书到期	一个或多个网格联合证书即将过期。
网格联合连接失败	本地网格与远程网格之间的网格联合连接不起作用。

高使用量或高延迟警报

警报名称	Description
Java 堆使用率较高	正在使用的 Java 堆空间百分比很高。
元数据查询延迟较长	Cassandra 元数据查询的平均时间过长。

身份联合警报

警报名称	Description
身份联合同步失败	无法从身份源同步联合组和用户。
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。

信息生命周期管理**(ILM)**警报

警报名称	Description
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。
ILM 扫描周期过长	扫描、评估ILM并将其应用于对象所需的时间过长。
ILM 扫描速率低	ILM 扫描速率设置为每秒不到 100 个对象。

密钥管理服务器(KMS)警报

警报名称	Description
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。
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
无法加载 Kms 配置	密钥管理服务器的配置存在，但无法加载。
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。
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。
Kms 加密密钥轮换失败	所有设备卷均已成功解密、但一个或多个卷无法转换为最新密钥。
未配置公里	此站点不存在密钥管理服务器。
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。
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。

本地时钟偏移警报

警报名称	Description
本地时钟大时间偏移	本地时钟和网络时间协议(NTP)时间之间的偏移过大。

内存不足或空间不足警报

警报名称	Description
审核日志磁盘容量低	可用于审核日志的空间不足。如果不解决此问题、S3或Swift操作可能会失败。
可用节点内存不足	节点上的可用 RAM 量较低。
存储池可用空间不足	存储节点中可用于存储对象数据的空间不足。
节点内存不足	节点上安装的内存量不足。
元数据存储不足	可用于存储对象元数据的空间不足。

警报名称	Description
低指标磁盘容量	可用于指标数据库的空间不足。
对象数据存储不足	可用于存储对象数据的空间不足。
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。
根磁盘容量低	根磁盘上的可用空间不足。
系统数据容量低	/var/local的可用空间不足。如果不解决此问题、S3或Swift操作可能会失败。
tmp 目录可用空间不足	/tmp 目录中的可用空间不足。

节点或节点网络警报

警报名称	Description
管理网络接收使用量	管理网络上的接收使用率较高。
管理网络传输使用量	管理网络上的传输使用率较高。
防火墙配置失败	无法应用防火墙配置。
回退模式下的管理接口端点	所有管理接口端点回退到默认端口的时间过长。
节点网络连接错误	在节点之间传输数据时出错。
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。
节点与 NTP 服务器不同步	此节点与网络时间协议(NTP)服务器不同步。
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。
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。
管理网络上的服务设备链接已关闭	管理网络(eth1)的设备接口已关闭或断开连接。
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。
客户端网络上的服务设备链路关闭	客户端网络(eth2)的设备接口已关闭或断开连接。

警报名称	Description
网络端口1上的服务设备链路关闭	设备上的网络端口1已关闭或断开连接。
网络端口2上的服务设备链路已关闭	设备上的网络端口2已关闭或断开连接。
网络端口3上的服务设备链路关闭	设备上的网络端口3已关闭或断开连接。
网络端口4上的服务设备链路关闭	设备上的网络端口4已关闭或断开连接。
管理网络上的存储设备链路关闭	管理网络(eth1)的设备接口已关闭或断开连接。
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。
客户端网络上的存储设备链路关闭	客户端网络(eth2)的设备接口已关闭或断开连接。
网络端口1上的存储设备链路关闭	设备上的网络端口1已关闭或断开连接。
网络端口2上的存储设备链路关闭	设备上的网络端口2已关闭或断开连接。
网络端口3上的存储设备链路关闭	设备上的网络端口3已关闭或断开连接。
网络端口4上的存储设备链路关闭	设备上的网络端口4已关闭或断开连接。
存储节点未处于所需的存储状态	由于内部错误或与卷相关的问题描述、存储节点上的LDR服务无法过渡到所需状态
TCP连接使用情况	此节点上的TCP连接数即将达到可跟踪的最大数量。
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。
节点意外重新启动	节点在过去 24 小时内意外重新启动。

对象警报

警报名称	Description
对象存在检查失败	对象存在检查作业失败。
对象存在检查已停止	对象存在检查作业已停止。
对象丢失	一个或多个对象已从网格中丢失。

警报名称	Description
S3放置对象大小太大	客户端尝试的Put Object操作超出S3大小限制。
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。

平台服务警报

警报名称	Description
平台服务待处理请求容量低	平台服务待处理请求的数量即将达到容量。
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。

存储卷警报

警报名称	Description
存储卷需要引起注意	存储卷已脱机、需要引起注意。
需要还原存储卷	存储卷已恢复、需要还原。
存储卷脱机	某个存储卷已脱机5分钟以上、可能是因为此节点在卷格式化步骤期间重新启动。
卷还原无法启动复制的数据修复	无法自动启动已修复卷的复制数据修复。

StorageGRID 服务警报

警报名称	Description
使用备份配置的NGinx服务	Nginx服务的配置无效。现在正在使用先前的配置。
使用备份配置的Ngins-GW服务	Ngins-GW服务的配置无效。现在正在使用先前的配置。
要禁用FIPS、需要重新启动	此安全策略不需要FIPS模式、但已启用NetApp加密安全模块。
要启用FIPS、需要重新启动	此安全策略需要FIPS模式、但NetApp加密安全模块已禁用。
使用备份配置的SSH服务	SSH服务的配置无效。现在正在使用先前的配置。

租户警报

警报名称	Description
租户配额使用量高	正在使用的配额空间百分比较高。默认情况下、此规则处于禁用状态、因为它可能发生原因 会发送过多通知。

常用的 **Prometheus** 指标

请参阅此常用Prometheus指标列表、以更好地了解默认警报规则中的条件或构建自定义警报规则的条件。

您也可以 获取所有指标的完整列表。

有关Prometheus查询语法的详细信息、请参见 "正在查询Prometheus"。

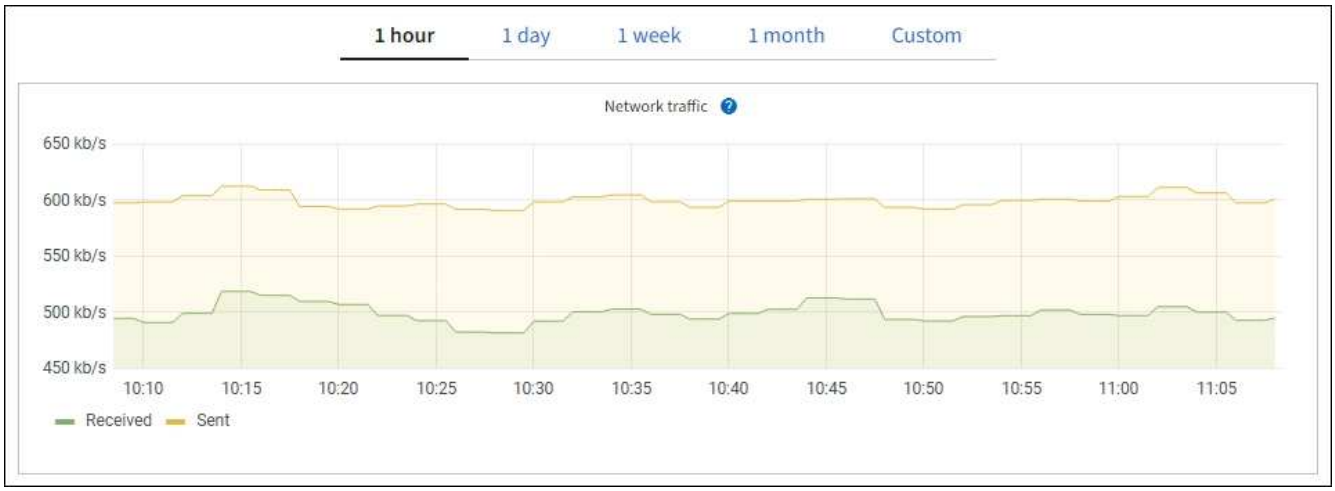
什么是**Prometheus**指标?

Prometheus指标是时间序列测量值。管理节点上的Prometheus服务会从所有节点上的服务收集这些指标。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、系统会先删除最早的指标。

Prometheus指标在哪里使用?

Prometheus收集的指标在网格管理器的多个位置使用：

- * 节点页面 * ： 节点页面上提供的选项卡上的图形和图表使用 Grafana 可视化工具显示 Prometheus 收集的时间序列指标。Grafana 以图形和图表格式显示时间序列数据，而 Prometheus 用作后端数据源。



- * 警报 * ： 如果使用 Prometheus 指标的警报规则条件评估为 true ，则会在特定严重性级别触发警报。
- * 网格管理 APi* ： 您可以在自定义警报规则中使用 Prometheus 指标，也可以使用外部自动化工具来监控 StorageGRID 系统。有关完整的 Prometheus 指标列表，请访问网格管理 API 。(从网格管理器的顶部，选择帮助图标，然后选择*API documents*>*metrics*。) 尽管有超过1000个指标可用、但监控最关键的StorageGRID 操作所需的指标数量相对较少。

> 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。

- 支持*>*工具*>*诊断*页面和*支持*>*工具*>*指标*页面：这些页面主要供技术支持使用，提供了多个使用Prometheus指标值的工具和图表。

> 指标页面中的某些功能和菜单项有意不起作用，可能会发生更改。

列出最常见的指标

以下列表包含最常用的Prometheus指标。

> 名称中包含_privly_的指标仅供内部使用、可能会在不同StorageGRID 版本之间进行更改、恕不另行通知。

alertmanager_notifications _failed_total

失败警报通知的总数。

node_filesystem_avail_bytes

可供非root用户使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

托架值为 `/sys/class/net/iface`。

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、不是最佳驱动器的数量。

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。

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。

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

此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。

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

storagegrid存储利用率数据字节

存储节点上已复制和已进行过彻底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 ）。

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。

获取所有指标的列表

[[obtain all-metrics]]要获取完整的指标列表、请使用网格管理API。

1. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
2. 找到 * 指标 * 操作。
3. 执行 `GET /grid/metric-names` 操作。
4. 下载结果。

管理警报（旧系统）

管理警报（旧系统）

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 系统都提供了默认警报、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、则这些警报将按"自上而下"优先级进行评估。

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 ）。

Global Alarms

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

Global Custom Alarms (0 Result(s))

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

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 ）。

Global Alarms

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

Global Custom Alarms (0 Result(s))

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

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions

Apply Changes

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。不能为表中的单个行禁用警报。

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VMFI警报(表中当前的两个严重警报均显示为绿色)； 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。

开始之前

- 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。通常、您可以忽略警报(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。

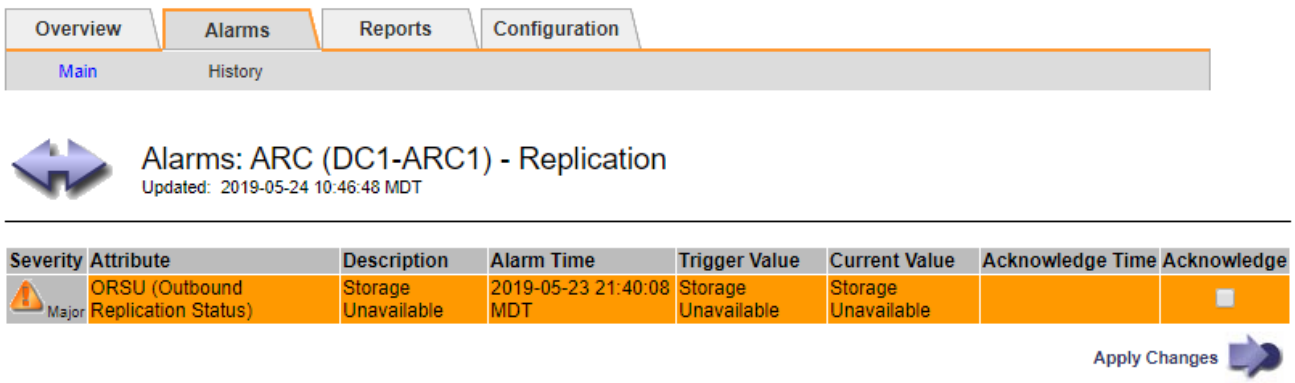
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

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. 选中报警的*Accheckbox*(确认*)复选框，然后单击*Apply changes*(应用更改*)。

   报警不再显示在信息板或当前报警页面上。

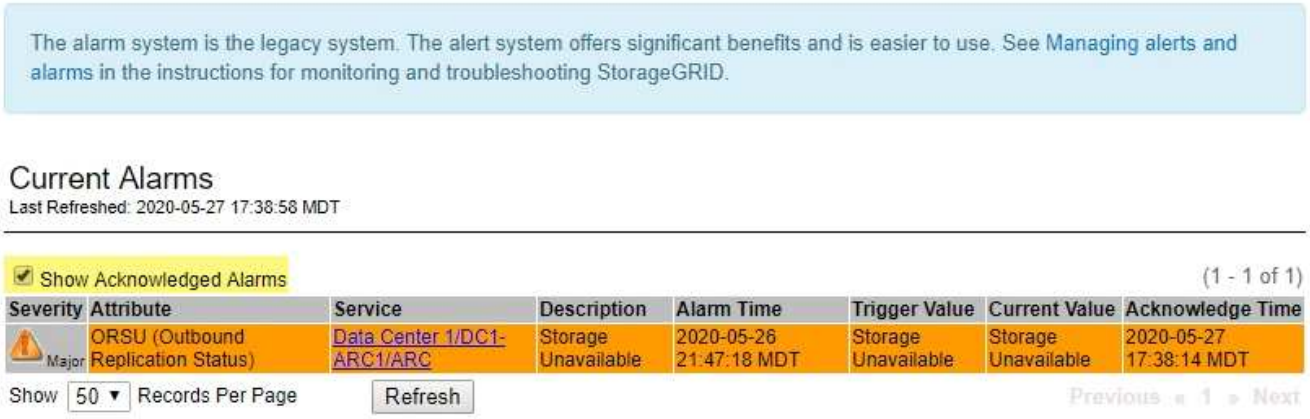
   确认警报后，确认不会复制到其他管理节点。因此、如果您从其他管理节点查看信息板、则可能仍会看到活动警报。

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。

开始之前

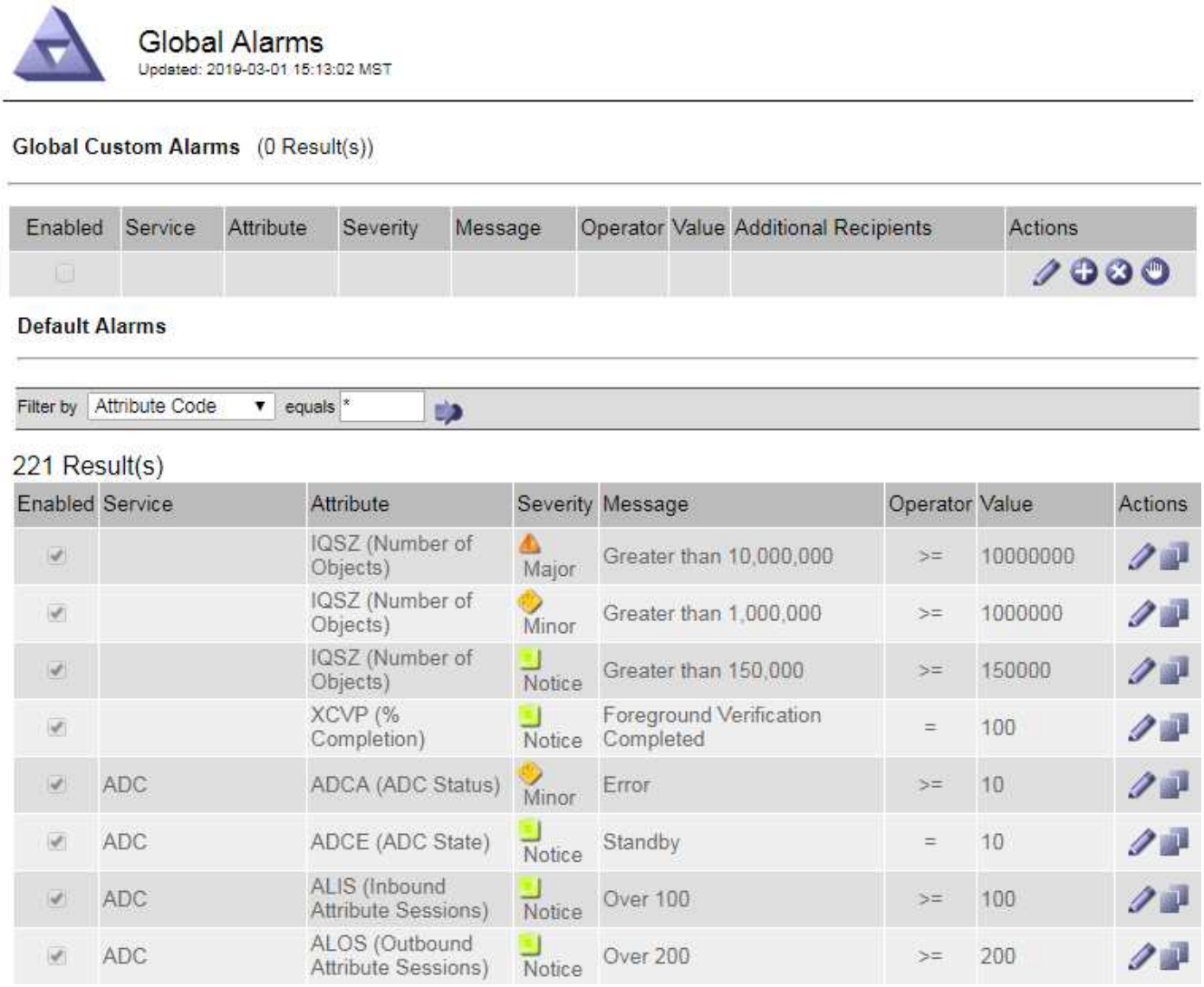
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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、输入一个星号： *
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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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。全局自定义警报的警报级别可能会覆盖默认警报、也可能会监控没有默认警报的属性。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

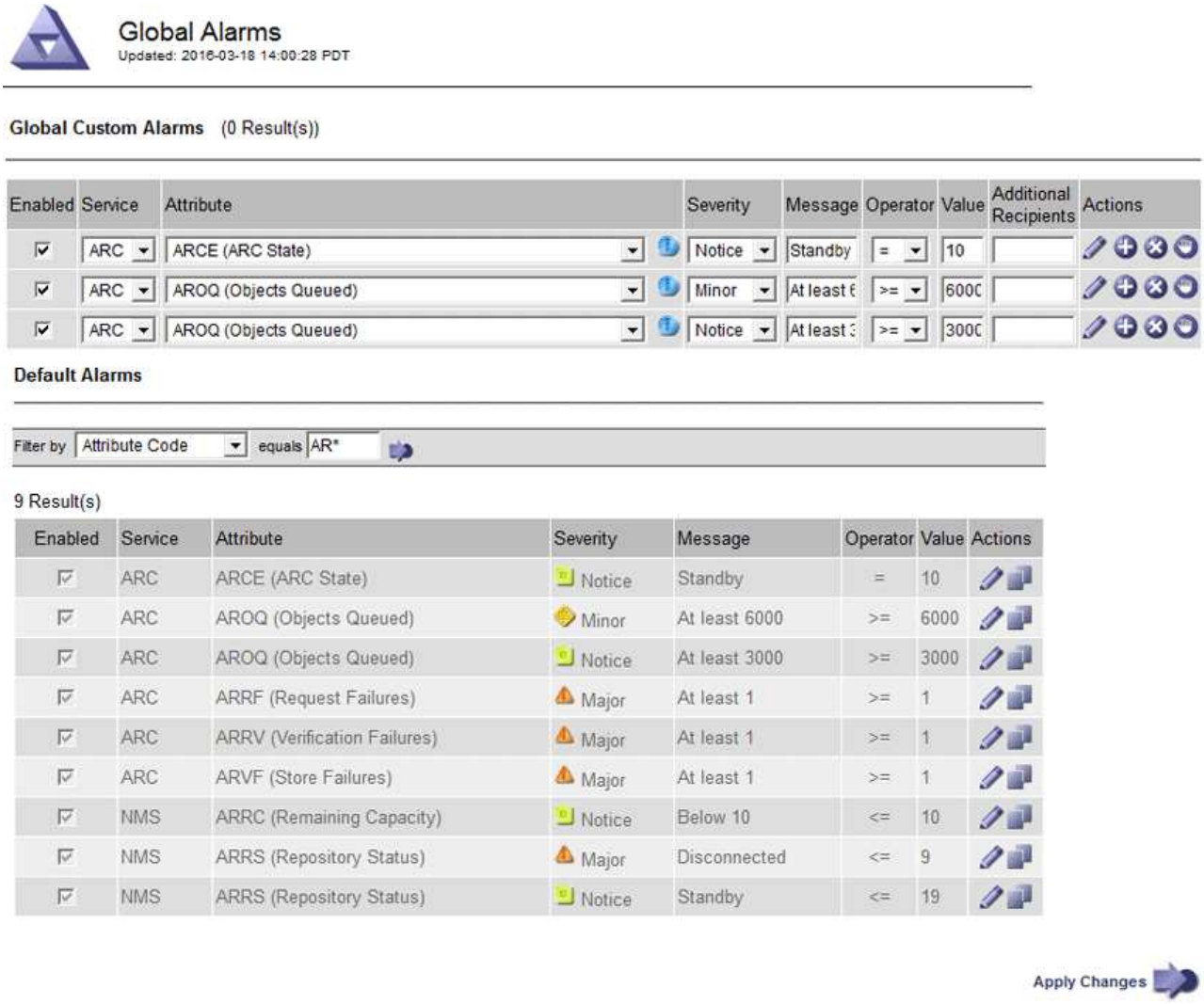
> 虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

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。

> 更改报警设置时要小心。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	选中或清除该复选框以启用或禁用警报。

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。 *注意：*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 + 向上或向下拖动行 + 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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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。

在完全转换到新警报系统之前、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

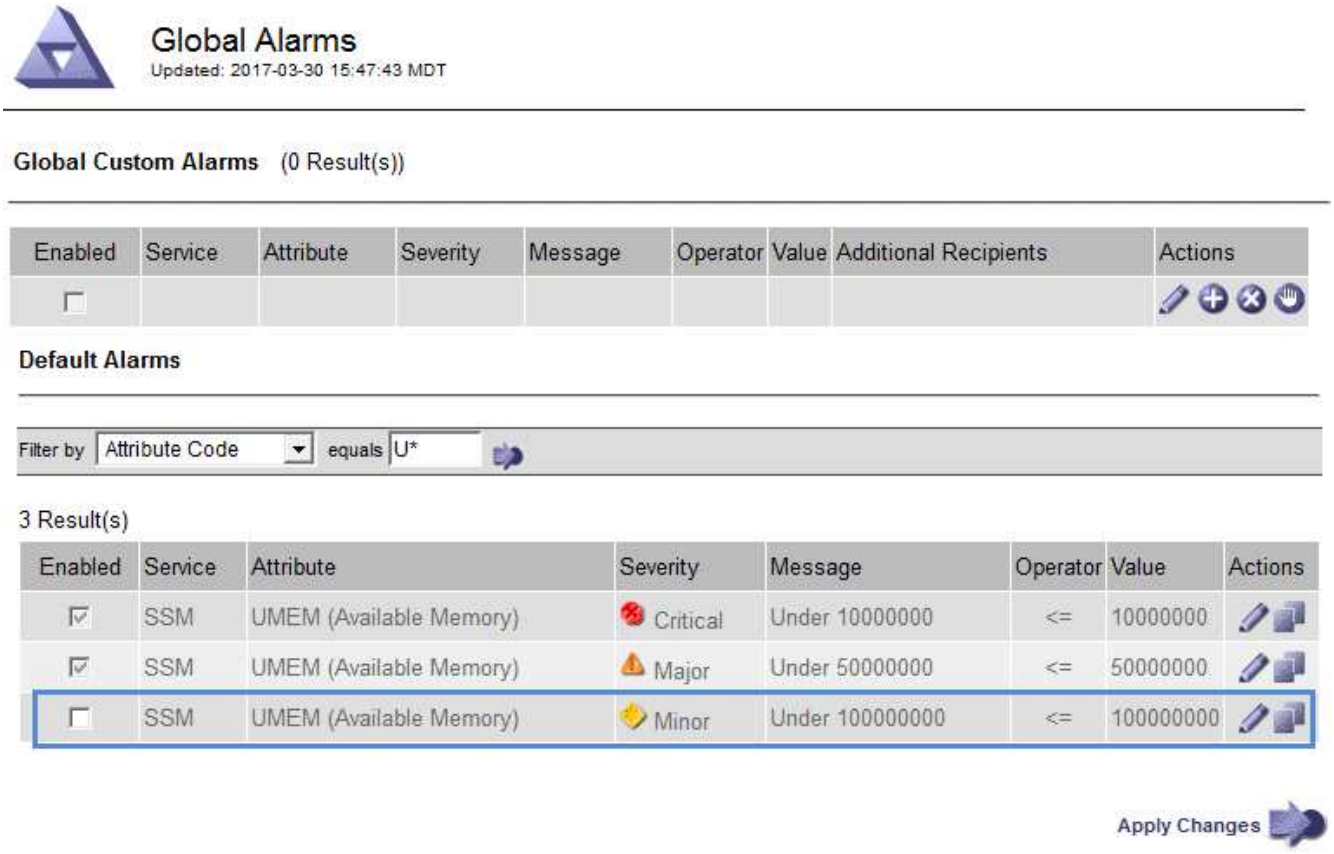
1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 搜索要禁用的默认警报。
   a. 在默认警报部分中，选择 * 筛选依据 * > * 属性代码 * 或 * 属性名称 * 。
   b. 键入搜索字符串。

      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。



选定报警的*Enabled"(已启用)复选框将被激活。

4. 清除*Enabled"(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。

开始之前

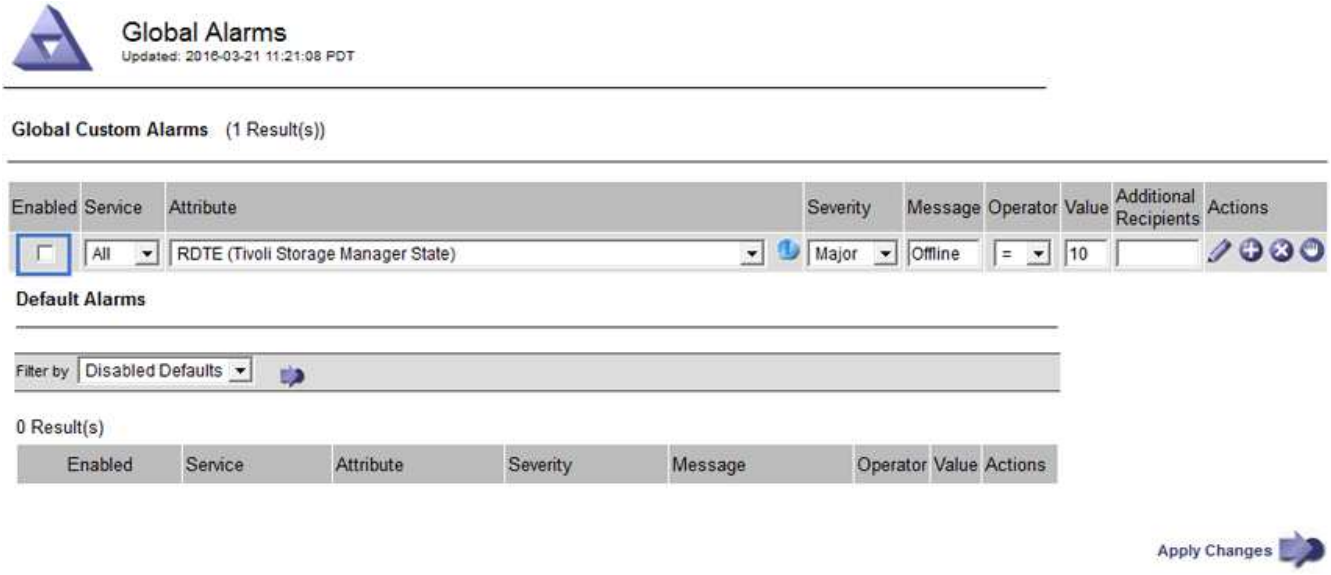
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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. 清除*Enabled"(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。

开始之前

- 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. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。
3. 重新启动NMS服务： `service nms restart`
4. 从管理节点中注销： `exit`

   警报已清除。

配置警报通知（旧系统）

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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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。

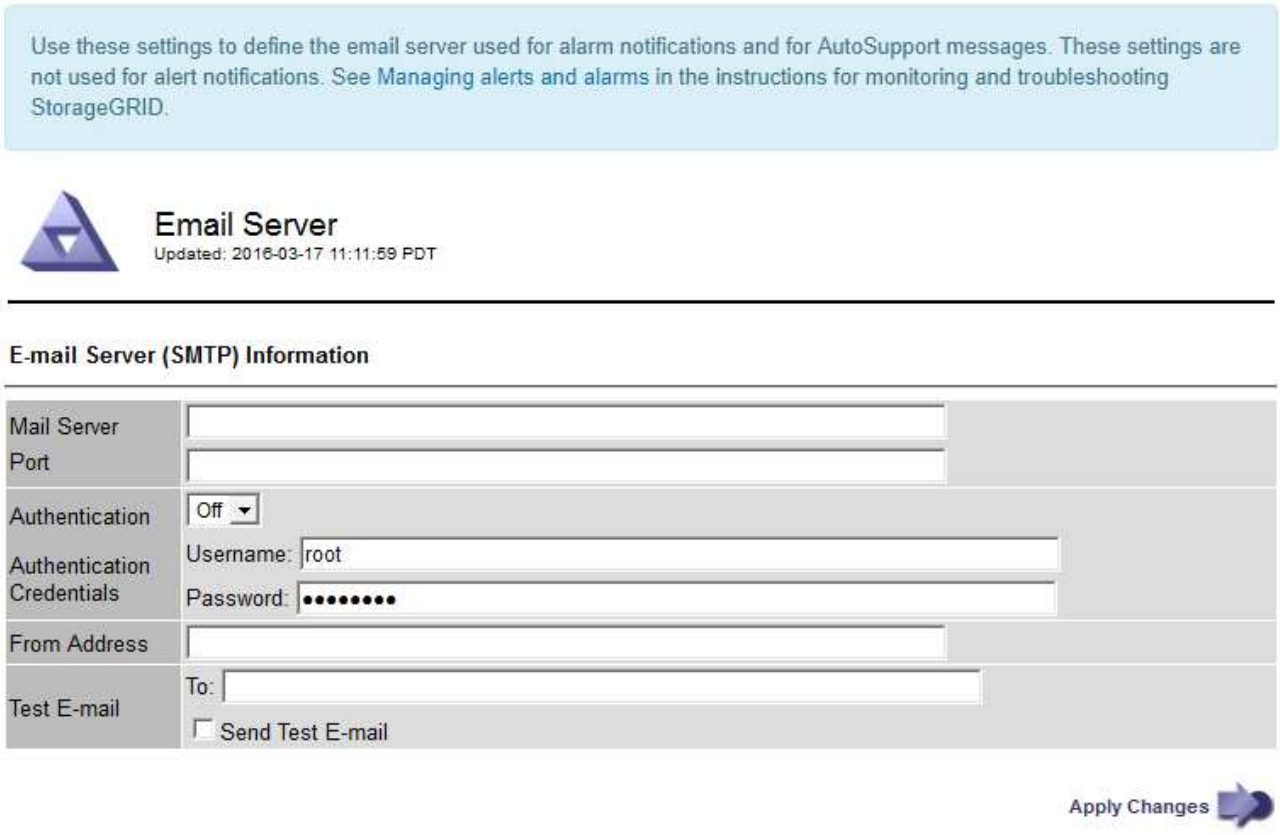
> 如果使用SMTP作为AutoSupport包的协议、则可能已配置SMTP邮件服务器。同一个 SMTP 服务器用于警报电子邮件通知，因此您可以跳过此操作步骤 。请参见 "有关管理 StorageGRID 的说明"。

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软件包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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

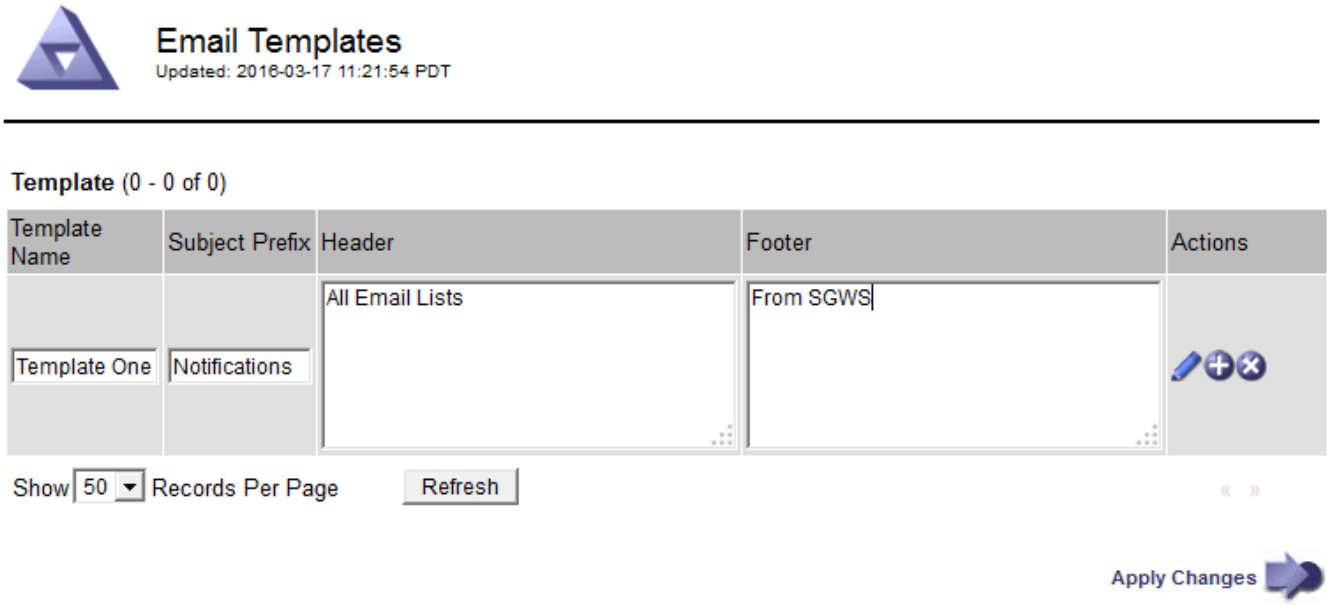
关于此任务

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。模板不包括电子邮件的正文。

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。

开始之前

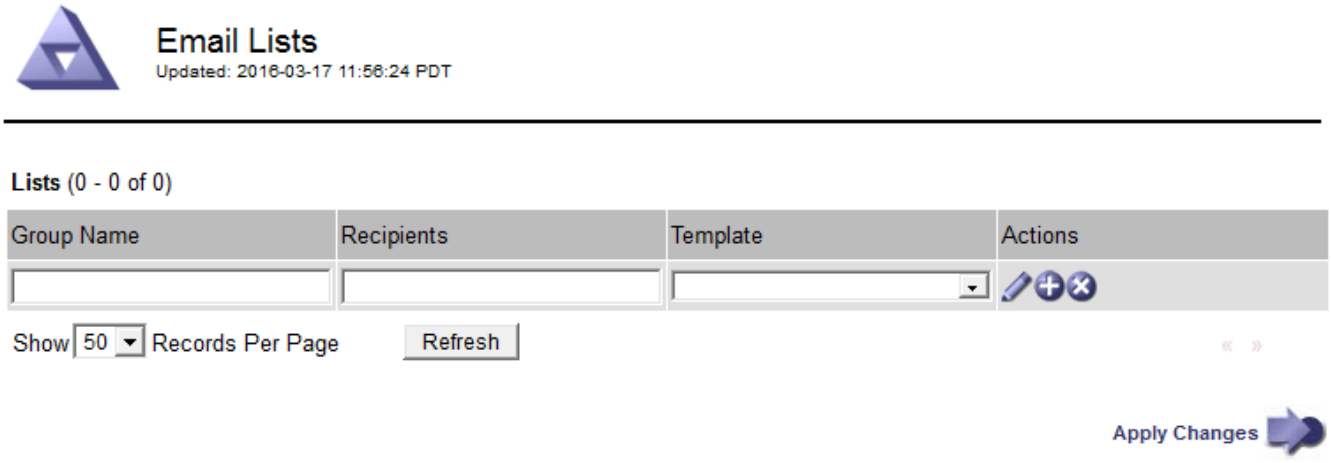
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 如果要为邮件列表指定电子邮件模板（自定义页眉，页脚和主题行），则必须已创建此模板。

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。不能复制邮件列表名称。 • 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）

要接收传统报警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中。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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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。

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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。

步骤

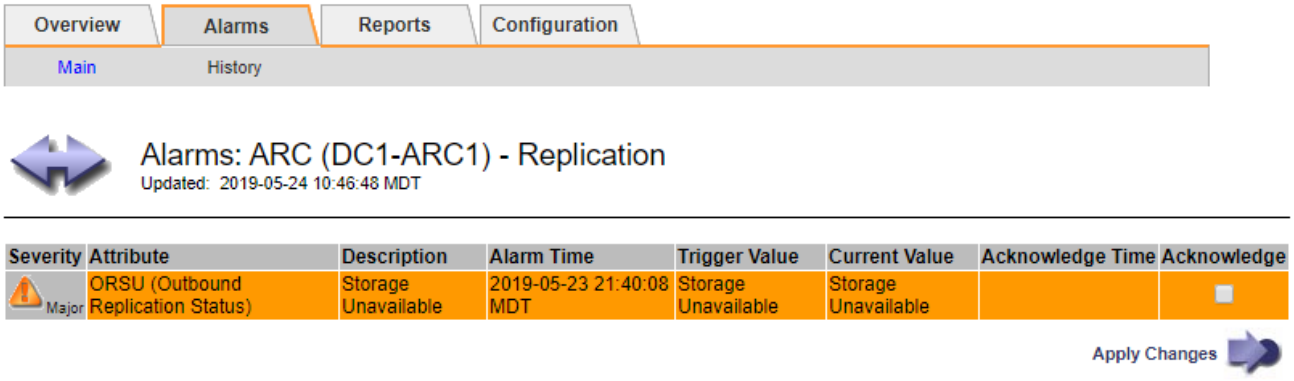
1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。

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）"

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、则无法处理入数据或检索事务。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。

代码	**Name**	服务	建议的操作
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。
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。

代码	**Name**	服务	建议的操作
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。
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	如果无法立即将审核消息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"。

代码	**Name**	服务	建议的操作
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。
APM	存储多路径连接	SSM	如果多路径状态警报显示为“已降级”(选择*support*>*工具*>*网格拓扑*，然后选择**ssite**>**grid NODE**>*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。 插入另一根电缆至少五分钟后再拔下另一根电缆。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“已降级”多路径状态是否已更改为“额定”。
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。

代码	**Name**	服务	建议的操作
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。
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。 解决触发此警报的问题后、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。

代码	**Name**	服务	建议的操作
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。
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、如果由于无法达到ADC仲裁而无法分配对象标识符、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、则在重新建立ADC仲裁之前、CMN服务无法分配新的标识符块。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。

代码	**Name**	服务	建议的操作
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。
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，或选择*support*>*Tools*>*网格拓扑*，然后选择**ssite*>**grid NODE*>*DDS*>*资源*>*概述*>*主*。 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、以admin和身份登录 `su` 使用Passwords.txt文件中列出的密码以root用户身份访问。 2. 输入 ... `service cassandra status` 3. 如果Cassandra未运行、请重新启动它：`service 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。
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、网格管理器中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"。 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。
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。

代码	**Name**	服务	建议的操作
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	如果后台验证过程检测到已删除编码的片段已损坏、则会触发警报。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。如果计数确实增加、则存储节点的底层存储可能存在问题。除非丢失或损坏的片段数量违反了删除代码的容错能力、否则不会将经过删除编码的对象数据副本视为缺失；因此、可能会出现损坏的片段、并且仍然能够检索对象。 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已进行过身份验证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。
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。

代码	**Name**	服务	建议的操作
HSTU	HTTP 状态	BLDR	HSTE和HSTU与所有LDR流量的HTTP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已脱机、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保持脱机状态、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 * 。
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。

代码	**Name**	服务	建议的操作
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）"
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。

代码	**Name**	服务	建议的操作
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"。
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。

代码	**Name**	服务	建议的操作
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。
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。

代码	**Name**	服务	建议的操作
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。
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

代码	**Name**	服务	建议的操作
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 * 。
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、正在重新连接、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 * 。

代码	**Name**	服务	建议的操作
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。
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 1213/11 ")。 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 * 。 如果要停止的网格任务的状态值为错误、请重试结束网格任务。 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。

代码	**Name**	服务	建议的操作
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
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。

代码	**Name**	服务	建议的操作
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。
SOSS	存储操作系统状态	SSM	如果SANtricity操作系统指示问题描述StorageGRID设备中的组件存在"需要引起注意"、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 操作系统中、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： • 此服务已手动停止 (`/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。

代码	Name	服务	建议的操作
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。
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。

日志文件参考

日志文件参考：概述

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。

访问日志

要访问日志、您可以 "收集日志文件和系统数据" 从一个或多个节点作为单个日志文件归档。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. 输入中列出的密码 `Passwords.txt` 文件
3. 输入以下命令切换到root： `su -`
4. 输入中列出的密码 `Passwords.txt` 文件

日志文件类别

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列出的有关当前节点和EC组信息的vCS信息。
网格	常规网格日志、包括调试 (`bycast.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` 并安装日志。
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。

归档位置	Description
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	负载平衡器和网格联合配置文件和日志。还包括 Grid Manager 和租户管理器流量日志。
nginx 网关	负载平衡器和网格联合配置文件和日志。
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	下的日志文件 `/var/local/log` 未收集到其他文件夹中的。
性能	CPU ，网络和磁盘 I/O 的性能信息
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。
SSH	与SSH配置和服务相关的日志。
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。

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审核信息的目标、例如 `bycast.log` 和 `nms.log`，请参阅 "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/bycast.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/bycast-err.log	包含的子集 `bycast.log` (严重性为错误且严重的消息)。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。 注：文件 `` `/var/local/core/kexec_cmd `` 通常存在于设备节点上、并不表示存在错误。	所有节点

与密码相关的日志

文件名	注释：	在上找到
/var/local/log/ssh-config-generation.log	包含与生成SSH配置和重新加载SSH服务相关的日志。	所有节点
/var/local/log/ginx/config-generation.log	包含与生成Nginx配置和重新加载Nginx服务相关的日志。	所有节点
/var/local/log/Ngins-gw/ config-generation.log	包含与生成Ngins-GW配置(以及重新加载Ngins-GW服务)相关的日志。	管理节点和网关节点
/var/local/log/update-cipher-configurations.log	包含与配置TLS和SSH策略相关的日志。	所有节点

网格联合日志

文件名	注释：	在上找到
/var/local/log/update_grid_federation_config.log	包含与为网格联盟连接生成Nginx和Ngins-GW配置相关的日志。	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

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

文件名	注释：	在上找到
/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/Cassanda/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/chunk．errlog		存储节点
/var/local/log/CMN.errlog		管理节点
/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/Csts.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/ds.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/hagroups_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

文件名	注释：	在上找到
/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/兰 百德*	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/ldr.errlog		存储节点
/var/local/log/m3cd /*。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/ginx/*.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/Ngins-gw/*.log	包含与Ngins-GW服务相关的常规日志、包括错误日志以及管理节点上受限管理端口的日志。	管理节点和网关节点
/var/local/log/Ngins-gw/ cgr-access.log.gz	包含与跨网格复制流量相关的访问日志。	管理节点、网关节点或两者、具体取决于网格联合配置。 仅在用于跨网格复制的目标网格上找到。
/var/local/log/Ngins-gw/ endpoint-access.log.gz	包含负载平衡器服务的访问日志、该服务可为从客户端到存储节点的S3和Swift流量提供负载平衡。	管理节点和网关节点
/var/local/log/perency*	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

文件名	注释：	在上找到
/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/raft.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
/var/local/log/update-traffic-classes.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

相关信息

"关于 bycast.log"

"使用S3 REST API"

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/expansion-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/pa-move.log	在运行时创建 `pa-move.sh` 脚本。	主管理节点
/var/local/log/pa-move-new_pa.log	在运行时创建 `pa-move.sh` 脚本。	主管理节点
/var/local/log/pa-move-old_pa.log	在运行时创建 `pa-move.sh` 脚本。	主管理节点
/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/myql.err /var/local/log/mysql-slow.log	MySQL 生成的日志文件。 `mysql.err` 捕获数据库错误和事件、例如、开始和关闭。 `mysql-slow.log` (慢速查询日志)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

类别	文件名	注释：	在上找到
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	`/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

关于 bycast.log

文件 `/var/local/log/bycast.log` 是StorageGRID 软件的主要故障排除文件。有一个 `bycast.log` 每个网格节点的文件。该文件包含特定于该网格节点的消息。

文件 `/var/local/log/bycast-err.log` 是的一部分 `bycast.log`。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 `bycast.log` 文件达到1 GB、现有文件将被保存、新日志文件将启动。

已保存的文件将重命名 `bycast.log.1`、新文件名为 `bycast.log`。当出现新的时 `bycast.log` 达到1 GB、`bycast.log.1` 已重命名并压缩为 `bycast.log.2.gz`，和 `bycast.log` 已重命名 `bycast.log.1`。

的轮换限制 `bycast.log` 为21个文件。当的第22版 `bycast.log` 文件已创建、最早的文件将被删除。

的轮换限制 `bycast-err.log` 是七个文件。

> 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

消息 `bycast.log` 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

中的消息 `bycast.log` 已分配严重性级别。

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`

中的大多数错误消息 `bycast.log` 包含错误代码。

下表列出了中常见的非数字代码 `bycast.log`。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
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

下表列出了中的数字错误代码 `bycast.log`。

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

错误编号	错误代码	含义
007	E2BIG	参数列表太长
008	ENOExec	Exec 格式错误
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

错误编号	错误代码	含义
028	ENOSPC	设备上没有剩余空间
029	ESPIPE	非法寻道
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

错误编号	错误代码	含义
049	EUNATCH	未连接协议驱动程序
050	ENOCSI	没有可用的 CSI 结构
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

错误编号	错误代码	含义
070	eComm	发送时出现通信错误
071	EPROTO	协议错误
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

错误编号	错误代码	含义
091	EPROTOTYPE	套接字的协议类型错误
092	ENOPROTOOPT	协议不可用
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	软件导致连接终止
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	参考太多：无法拼接
110	ETIMEDOUT	连接超时
111.	ECONNREFUSED	连接被拒绝

错误编号	错误代码	含义
112	EHOSTDOWN	主机已关闭
113	EHOSTUNREACH	没有到主机的路由
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

配置审核消息和日志目标

使用外部系统日志服务器的注意事项

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、您可以减少管理节点上的网络流量、并更高效地管理信息。对于StorageGRID、出站系统日志消息数据包格式符合RFC 3164。

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

何时使用外部系统日志服务器

如果您的网格较大、使用多种类型的S3应用程序或希望保留所有审核数据、则外部系统日志服务器尤其有用。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8、192字节的单个日志会在消息末尾被截断、以符合外部系统日志服务器实施中的常见限制。

> 要在外部系统日志服务器发生故障时最大限度地恢复数据、可使用多达20 GB的本地审核记录日志 (`localaudit.log`)。

如何配置外部系统日志服务器

要了解如何配置外部系统日志服务器、请参见 "配置审核消息和外部系统日志服务器"。

如果您计划配置使用TLS或RELP/TLS协议、则必须具有以下证书：

- 服务器**CA**证书：一个或多个可信CA证书，用于验证采用PEM编码的外部系统日志服务器。如果省略此参数，则会使用默认网格 CA 证书。
- 客户端证书：以PEM编码向外部系统日志服务器进行身份验证的客户端证书。
- 客户端专用密钥：PEM编码的客户端证书专用密钥。

> 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）。

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。

代码	字段	Description
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 ）。

让我们使用K来表示S3帐户名称、S3存储分段和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）。未提供用于估计非默认审核级别设置的审核消息速率和平均大小的详细公式。不过，下表可用于粗略估计费率； 您可以使用为审核日志提供的平均大小公式、但请注意、它可能会导致高估、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、通常会生成极少的日志和数据。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存储分段和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存储分段和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
```

例如、如果您的网格的规模为每秒1、000次S3操作、则您的工作负载为50%的"放置"、而您的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为每秒支持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(并通常存储)应用程序数据。

配置审核消息和外部系统日志服务器

您可以配置与审核消息相关的许多设置。您可以调整记录的审核消息数；定义要包含在客户端读写审核消息中的任何HTTP请求标头；配置外部系统日志服务器；以及指定审核日志、安全事件日志和StorageGRID软件日志的发送位置。

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。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。

您也可以配置外部系统日志服务器以远程保存审核信息。使用外部服务器可以最大限度地降低审核消息日志记录对性能的影响、而不会降低审核数据的完整性。如果您的网格较大、使用多种类型的S3应用程序或希望保留所有审核数据、则外部系统日志服务器尤其有用。请参见 "外部系统日志服务器的注意事项" 了解详细信息。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "维护或root访问权限"。
- 如果您计划配置外部系统日志服务器、则已查看 "使用外部系统日志服务器的注意事项" 并确保服务器有足够的容量来接收和存储日志文件。
- 如果您计划使用TLS或RELP/TLS协议配置外部系统日志服务器、则您具有所需的服务器CA和客户端证书以及客户端专用密钥。

更改审核消息级别

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	默认设置	更多信息
系统	正常	"系统审核消息"

审核类别	默认设置	更多信息
存储	error	"对象存储审核消息"
管理	正常	"管理审核消息"
客户端读取	正常	"客户端读取审核消息"
客户端写入	正常	"客户端写入审核消息"
ILM	正常	"ILM审核消息"
跨网格复制	error	"CGRR：跨网格复制请求"

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。如果您最初使用的是早期版本的StorageGRID、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。
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。

如果不需要S3应用程序的客户端读取操作详细记录，可以选择将*Client Reads*设置更改为*Error*，以减少审核日志中记录的审核消息数。

3. 选择 * 保存 * 。

绿色横幅表示您的配置已保存。

定义HTTP请求标头

您可以选择定义要包含在客户端读写审核消息中的任何HTTP请求标头。这些协议标头仅适用于S3和Swift请求。

步骤

1. 在*Audit protocol headers*部分中，定义要包含在客户端读写审核消息中的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。

2. 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。

3. 选择 * 保存 *

   绿色横幅表示您的配置已保存。

使用外部系统日志服务器

您可以选择配置外部系统日志服务器、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某个位置。

> 如果不想使用外部系统日志服务器，请跳过此步骤并转到选择审核信息目标。

> 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、则可以使用应用其他配置选项 `audit-destinations` 端点、位于的专用API部分中 "网格管理 API"。例如、如果要对不同的节点组使用不同的系统日志服务器、则可以使用API。

输入系统日志信息

访问配置外部系统日志服务器向导、并提供StorageGRID访问外部系统日志服务器所需的信息。

步骤

1. 从 Audit and syslog server 页面中，选择 * 配置外部系统日志服务器 * 。或者，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*。

   此时将显示配置外部系统日志服务器向导。

2. 对于向导的*Enter syslog info*步骤，在*Host*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。
3. 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 。
4. 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 "管理安全证书"。

   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。

5. 选择 * 继续 * 。
6. [[attache-certificate]如果选择了*tls*或*RELP/tls*，请上传服务器CA证书、客户端证书和客户端专用密钥。
   a. 为要使用的证书或密钥选择 * 浏览 * 。
   b. 选择证书或密钥文件。
   c. 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。
7. 选择 * 继续 * 。

管理系统日志内容

您可以选择要发送到外部系统日志服务器的信息。

步骤

1. 对于向导的*管理系统日志内容*步骤，选择要发送到外部系统日志服务器的每种审核信息类型。
   - 发送审核日志：发送StorageGRID 事件和系统活动
   - 发送安全事件：发送安全事件，例如未授权用户尝试登录或用户以root身份登录时
   - 发送应用程序日志：发送对故障排除有用的日志文件，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (仅限管理节点)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   有关StorageGRID软件日志的信息、请参见 "StorageGRID 软件日志"。
2. 使用下拉菜单为您要发送的每类审核信息选择严重性和设施(消息类型)。

   设置严重性和设施值可帮助您以可自定义的方式聚合日志、以便于分析。
   a. 对于*严重性*，请选择*直通*，或选择介于0到7之间的严重性值。

      如果您选择一个值、则所选值将应用于此类型的所有消息。如果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
直通	发送到外部系统日志的每条消息的严重性值与在本地记录到节点时的严重性值相同： • 对于审核日志、严重性为"info"。 • 对于安全事件、严重性值由节点上的Linux分发版生成。 • 对于应用程序日志、"info"和"noty"之间的严重级别因问题描述的定义而异。例如、添加NTP服务器并配置HA组时、值为"info"、而故意停止SSM或RSM服务时、值为"note"。
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
6.	Informational ： 信息性消息
7.	debug ： 调试级别的消息

b. 对于*facilty*，选择*PassThrough *，或选择一个介于0到23之间的设施值。

如果您选择一个值，它将应用于此类型的所有消息。如果您使用固定值覆盖医院、则有关不同医院的信息将丢失。

设施	Description
直通	发送到外部系统日志的每条消息都具有与在本地记录到节点上时相同的工具值： • 对于审核日志、发送到外部系统日志服务器的工具为"local7"。 • 对于安全事件、工具值由节点上的Linux分发版生成。 • 对于应用程序日志、发送到外部系统日志服务器的应用程序日志具有以下工具值： ◦ `bycast.log`：用户或守护进程 ◦ `bycast-err.log`：用户、守护进程、local3或local4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3. ◦ `prometheus.log`：本地4 ◦ `raft.log`：local5. ◦ `hagroups.log`：local6
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）
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

设施	Description
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收到来自网格中每个节点的测试消息且该消息已按预期处理之前、请勿使用外部系统日志服务器配置。

步骤

1. 如果由于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而不想发送测试消息，请选择*跳过并完成*。

   绿色横幅表示配置已保存。

2. 否则，请选择*发送测试消息*(建议)。

   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. 如果您在 syslog 服务器配置期间或运行时收到任何错误，请更正它们并再次选择*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协议不支持像其他协议那样严格的错误检测
   协议。

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。绿色横幅表示系统日志服务器配置已保存。

   只有在选择包含外部系统日志服务器的目标后、才会将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

您可以指定审核日志、安全事件日志和的位置 "StorageGRID 软件日志" 已发送。

StorageGRID默认使用本地节点审核目标，并将审核信息存储在中 `/var/local/log/localaudit.log`。

使用时 `/var/local/log/localaudit.log`，Grid Manager和租户管理器审核日志条目可能会发送到存储节点。您可以使用命令查找哪个节点具有最新的条目 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`。

只有在配置了外部系统日志服务器后、某些目标才可用。

步骤

1. 在审核和系统日志服务器页面上、选择审核信息的目标。

   *仅限本地节点*和*外部系统日志服务器*通常可提供更好的性能。

选项	Description
仅本地节点(默认)	审核消息、安全事件日志和应用程序日志不会发送到管理节点。而是仅保存在生成这些卷的节点("本地节点")上。在每个本地节点上生成的审核信息存储在中 `/var/local/log/localaudit.log`。 注意：StorageGRID会定期轮换删除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。

选项	Description
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、安全事件日志和应用程序日志会存储在生成这些消息的节点上。审核信息存储在以下文件中： • 管理节点(主节点和非主节点)：`/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log`文件通常为空或缺失。它可能包含辅助信息、例如某些消息的附加副本。
外部系统日志服务器	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(`/var/local/log/localaudit.log`)。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(`/var/local/audit/export/audit.log`管理节点上的审核日志()，而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(/var/local/log/localaudit.log`)。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。

2. 选择 * 保存 * 。

   此时将显示一条警告消息。

3. 选择*OK*确认要更改审核信息的目标。

   绿色横幅表示已保存审核配置。

   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。

使用 SNMP 监控

使用SNMP监控：概述

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、用于提供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。

请参见 "访问MIB文件" 要在网格节点上下载MIB文件的选项。

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

陷阱是由SNMP代理发送的通知、不需要管理系统进行确认。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

通知与陷阱类似，但需要管理系统确认。如果SNMP代理未在一定时间内收到确认、则会重新发送通知、直到收到确认或已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、您必须执行此操作 "配置静音" 警报。警报通知由发送 "首选发件人管理节点"。

  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 。有关可触发这些陷阱的警报列表、请参见 "警报参考"。

- 肯定的 "警报(传统系统)" 在指定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 (GET 和GETNEXT)	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 (陷阱和通知)	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 。

配置 **SNMP** 代理

您可以将StorageGRID SNMP代理配置为使用第三方SNMP管理系统进行只读MIB访问和通知。

开始之前

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

关于此任务

StorageGRID SNMP代理支持SNMPv1、SNMPv2c和SNMPv3。您可以为代理配置一个或多个版本。对于SNMPv3、仅支持用户安全模型(User Security Model、USM)身份验证。

网格中的所有节点都使用相同的SNMP配置。

指定基本配置

首先、启用StorageGRID SMNP代理并提供基本信息。

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*Enable SNMP*复选框。
3. 在Basic configuration部分中输入以下信息。

字段	**Description**
系统联系人	可选。StorageGRID系统的主要联系人、在SNMP消息中以sysContact的形式返回。 系统联系人通常是一个电子邮件地址。此值用于适用场景StorageGRID系统中的所有节点。*系统联系人*最多可以包含255个字符。

字段	Description
系统位置	可选。StorageGRID系统的位置、在SNMP消息中以sysLocation的形式返回。 系统位置可以是任何有助于确定StorageGRID系统所在位置的信息。例如，您可以使用设施的街道地址。此值用于适用场景StorageGRID系统中的所有节点。*系统位置*最多可以是255个字符。
启用SNMP代理通知	• 如果选中此选项、StorageGRID SNMP代理将发送陷阱和通知通知。 • 如果未选中、则SNMP代理支持只读MIB访问、但不会发送任何SNMP通知。
启用身份验证陷阱	如果选中此选项、则StorageGRID SNMP代理会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。

输入社区字符串

如果使用SNMPv1或SNMPv2c、请完成社区字符串部分。

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。

步骤

1. 对于*只读社区*，可选择输入社区字符串，以允许对IPv4和IPv6代理地址进行只读MIB访问。

   为确保StorageGRID系统的安全性、请勿使用"public"作为社区字符串。如果将此字段留空、SNMP代理将使用StorageGRID系统的网格ID作为社区字符串。

   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。

2. 选择*添加其他社区字符串*以添加其他字符串。

   最多允许五个字符串。

创建陷阱目标

使用其他配置部分中的陷阱目标选项卡为StorageGRID陷阱或通知定义一个或多个目标。如果启用SNMP代理并选择*保存*，则在触发警报时，StorageGRID会向每个定义的目标发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

步骤

1. 对于*默认陷阱社区*字段、可选择输入要用于SNMPv1或SNMPv2陷阱目标的默认社区字符串。

   定义特定陷阱目标时、您可以根据需要提供不同的("自定义")社区字符串。

   *默认陷阱社区*最多可包含32个字符、不能包含空格字符。

2. 要添加陷阱目标，请选择*Cree*。
3. 选择要用于此陷阱目标的SNMP版本。
4. 完成所选版本的创建陷阱目标表单。

SNMPv1

如果选择SNMPv1作为版本、请填写这些字段。

字段	Description
Type	必须为SNMPv1陷阱。
主机	用于接收陷阱的IPv4或IPv6地址或完全限定域名(FQDN)。
Port	使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
社区字符串	使用默认陷阱团体(如果已指定)、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。

SNMPv2c

如果选择SNMPv2c作为版本、请填写这些字段。

字段	Description
Type	目标将用于陷阱还是通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。
Port	请使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
社区字符串	使用默认陷阱团体(如果已指定)、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

如果选择SNMPv3作为版本、请填写这些字段。

字段	Description
Type	目标将用于陷阱还是通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。

字段	Description
Port	请使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
USM用户	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。 • 如果未显示任何用户： i. 创建并保存陷阱目标。 ii. 转至 创建USM用户 并创建用户。 iii. 返回到陷阱目标选项卡，从表中选择保存的目标，然后选择*Edit*。 iv. 选择用户。

5. 选择 * 创建 * 。

   此时将创建陷阱目标并将其添加到表中。

创建代理地址

(可选)使用“其他配置”部分中的“业务代表地址”选项卡指定一个或多个“侦听地址”。 这些地址是SNMP代理可以接收查询的StorageGRID地址。

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。

步骤

1. 选择 * 创建 * 。
2. 输入以下信息。

字段	Description
互联网协议	此地址将使用IPv4还是IPv6。 默认情况下， SNMP 使用 IPv4 。
传输协议	此地址将使用UDP还是TCP。 默认情况下， SNMP 使用 UDP 。

字段	Description
StorageGRID网络	代理将侦听哪个StorageGRID网络。 • 网格、管理和客户端网络：SNMP代理将侦听所有三个网络上的查询。 • 网格网络 • 管理网络 • 客户端网络 注意：如果使用客户端网络处理不安全的数据，并为客户端网络创建代理地址，请注意SNMP流量也不安全。
Port	(可选) 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。 注意：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。

3. 选择 * 创建 * 。

   此时将创建代理地址并将其添加到表中。

创建USM用户

如果使用SNMPv3、请使用其他配置部分中的USM用户选项卡定义有权查询MIB或接收陷阱和通知的USM用户。

> 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。

如果您仅使用SNMPv1或SNMPv2c、则这些步骤不适用。

步骤

1. 选择 * 创建 * 。
2. 输入以下信息。

字段	Description
Username	此USM用户的唯一名称。 用户名最多可以包含32个字符、且不能包含空格字符。创建用户后、无法更改此用户名。

字段	Description
只读MIB访问	如果选中、则此用户应对MIB具有只读访问权限。
权威引擎ID	如果要在通知目标中使用此用户、则为该用户的权威引擎ID。 输入10到64个十六进制字符(5到32字节)、不含空格。要在陷阱目标中选择用于通知的USM用户需要此值。要在陷阱目标中为陷阱选择的USM用户不允许使用此值。 注意：如果您选择了*只读MIB访问*，则不会显示此字段，因为具有只读MIB访问权限的USM用户不能具有引擎ID。
安全级别	USM用户的安全级别： • * 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。
身份验证协议	始终设置为SHA、这是唯一支持的协议(HMAC-SHA-96)。
Password	此用户将用于身份验证的密码。
隐私协议	仅当您选择了*authPriv*并始终设置为AES时显示，AES是唯一支持的隐私协议。
Password	仅在选择了*authSv*时显示。此用户用于保护隐私的密码。

3. 选择 * 创建 * 。

   此时将创建 USM 用户并将其添加到表中。

4. 完成SNMP代理配置后，选择*Save*。

   新的 SNMP 代理配置将变为活动状态。

更新 **SNMP** 代理

您可以禁用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。

开始之前

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

关于此任务

请参见 "配置 SNMP 代理" 有关SNMP代理页面上每个字段的详细信息。您必须选择页面底部的*保存*以提交您在每个选项卡上所做的任何更改。

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

   此时将显示SNMP代理页面。

2. 要在所有网格节点上禁用SNMP代理，请清除*Enable SNMP*复选框，然后选择*Save*。

   如果重新启用SNMP代理、则会保留先前的任何SNMP配置设置。

3. (可选)更新Basic configuration部分中的信息：

   a. 根据需要更新*系统联系人*和*系统位置*。

   b. (可选)选中或清除*启用SNMP代理通知*复选框以控制StorageGRID SNMP代理是否发送陷阱和通知通知。

      清除此复选框后、SNMP代理支持只读MIB访问、但不会发送SNMP通知。

   c. (可选)选中或清除*启用身份验证陷阱*复选框，以控制StorageGRID SNMP代理在收到未经正确身份验证的协议消息时是否发送身份验证陷阱。

4. 如果使用SNMPv1或SNMPv2c，则可以选择在“团体字符串”部分中更新或添加*只读社区*。

5. 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。

   使用此选项卡可以定义StorageGRID陷阱或通知通知的一个或多个目标。如果启用SNMP代理并选择*保存*，则在触发警报时，StorageGRID会向每个定义的目标发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

   有关输入内容的详细信息、请参见 "创建陷阱目标"。

   - (可选)更新或删除默认陷阱社区。

     如果删除默认陷阱团体、则必须先确保任何现有陷阱目标使用自定义社区字符串。

   - 要添加陷阱目标，请选择*Cree*。
   - 要编辑陷阱目标，请选择单选按钮，然后选择*Edit*。
   - 要删除陷阱目标，请选择单选按钮，然后选择*Remove*。
   - 要提交更改，请选择页面底部的*保存*。

6. 要更新业务代表地址，请选择其他配置部分中的业务代表地址选项卡。

   使用此选项卡指定一个或多个"侦听地址"。 这些地址是SNMP代理可以接收查询的StorageGRID地址。

   有关输入内容的详细信息、请参见 "创建代理地址"。

   - 要增加业务代表地址，请选择*Cree*。
   - 要编辑业务代表地址，请选择单选按钮，然后选择*Edit*。
   - 要删除业务代表地址，请选择单选按钮，然后选择*Remove*。

- 要提交更改，请选择页面底部的*保存*。

7. 要更新USM用户、请选择其他配置部分中的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。

   有关输入内容的详细信息、请参见 "创建USM用户"。

   - 要添加USM用户，请选择*Cree*。
   - 要编辑USM用户，请选择单选按钮，然后选择*Edit*。

     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。

     > 如果添加或删除用户的权威引擎ID、并且当前已为目标选择该用户、则必须编辑或删除目标。否则，在保存 SNMP 代理配置时会发生验证错误。

   - 要删除USM用户，请选择单选按钮，然后选择*Remove*。

     > 如果您删除的用户当前已被选定为陷阱目标、则必须编辑或删除该目标。否则，在保存 SNMP 代理配置时会发生验证错误。

   - 要提交更改，请选择页面底部的*保存*。

8. 更新SNMP代理配置后，选择*Save*。

访问**MIB**文件

MIB文件包含有关网格中节点的受管资源和服务属性的定义和信息。您可以访问用于定义StorageGRID 对象和通知的MIB文件。这些文件可用于监控网格。

请参见 "使用 SNMP 监控" 有关SNMP和MIB文件的详细信息。

访问**MIB**文件

按照以下步骤访问MIB文件。

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。
2. 在SNMP代理页面上、选择要下载的文件：
   - **NetApp-STORAGEGRID-MIB.TXT**：定义可在所有管理节点上访问的警报表和通知(陷阱)。
   - **ES-NetApp-06-MIB.MIB**：为基于E系列的设备定义对象和通知。
   - **mib_1_10.zip**：使用BMC接口为设备定义对象和通知。

     > 您还可以在任何StorageGRID节点上访问以下位置的MIB文件：
     > `/usr/share/snmp/mibs`

3. 要从MIB文件中提取StorageGRID OID、请执行以下操作：

   a. 获取StorageGRID MIB根目录的OID：

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

结果 `.1.3.6.1.4.1.789.28669` (`28669` 始终是StorageGRID 的OID)

   a. 整个树中StorageGRID OID的gep (使用 `paste` 连接线)：

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

。 `snmptranslate` 命令提供了许多可用于浏览MIB的选项。此命令可在任何StorageGRID 节点上使用。

MIB文件内容

所有对象都位于StorageGRID OID下。

对象名称	对象**ID (OID)**	**Description**
iso.org.dod.internet。+ 私有企业。+ NetApp.storagegrid		NetApp StorageGRID实体的MIB模块。

MIB对象

对象名称	对象**ID (OID)**	**Description**
活动的计数	1.3.6.1.4.1。+ 789.28669.1.3	activeAlert表中活动警报的数量。
活动的活动的表	1.3.6.1.4.1。+ 789.28669.1.4	StorageGRID 中活动警报的表。
活动的标识号	1.3.6.1.4.1。+ 789.28669.1.4.1.1	警报的ID。仅在当前一组活动警报中是唯一的。
活动报告名称	1.3.6.1.4.1。+ 789.28669.1.4.1.2	警报的名称。
已执行的活动的活动的实例	1.3.6.1.4.1。+ 789.28669.6.4.1.3	生成警报的实体的名称、通常为节点名称。
活动告警严重性	1.3.6.1.4.1。+ 789.28669.1.4.1.4	警报的严重性。

对象名称	对象ID (OID)	Description
活动的起始时间	1.3.6.1.4.1。+ 789.28669.1.4.1.5	触发警报的日期和时间。

通知类型(陷阱)

所有通知都包含以下变量作为变量绑定：

- 活动的标识号
- 活动报告名称
- 已执行的活动的活动的实例
- 活动告警严重性
- 活动的起始时间

通知类型	对象ID (OID)	Description
活动MinorAlert	1.3.6.1.4.1。+ 789.28669.0.6	严重性较低的警报
活动主要警报	1.3.6.1.4.1。+ 789.28669.0.7	严重性为"重大"的警报
活动状态警报	1.3.6.1.4.1。+ 789.28669.0.8	严重性为严重的警报

收集其他 StorageGRID 数据

使用图表和图形

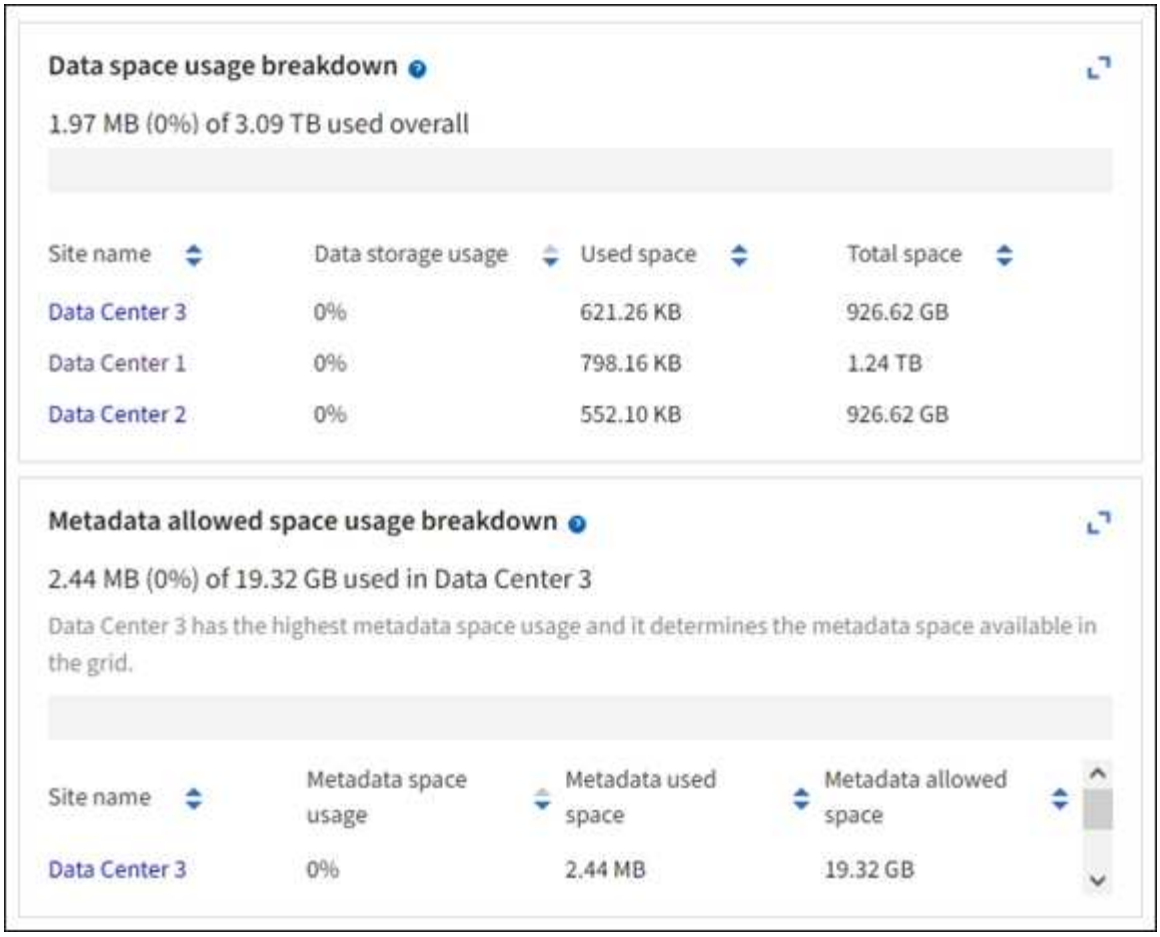
您可以使用图表和报告监控 StorageGRID 系统的状态并对问题进行故障排除。

Grid Manager随每个版本更新、可能与此页面上的示例屏幕截图不匹配。

图表类型

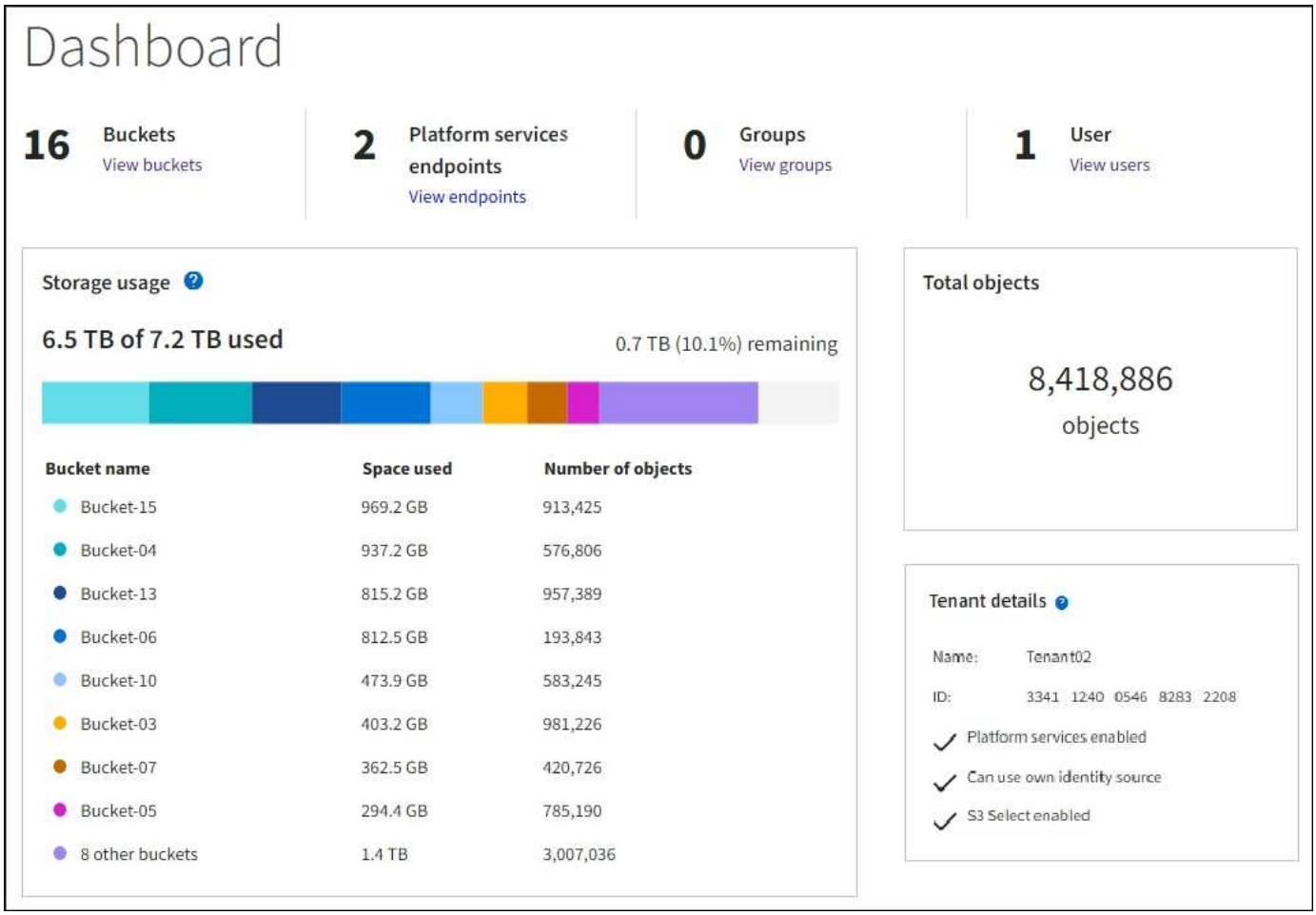
图表和图形汇总了特定 StorageGRID 指标和属性的值。

网格管理器信息板包含一些卡片、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量面板显示以下内容：

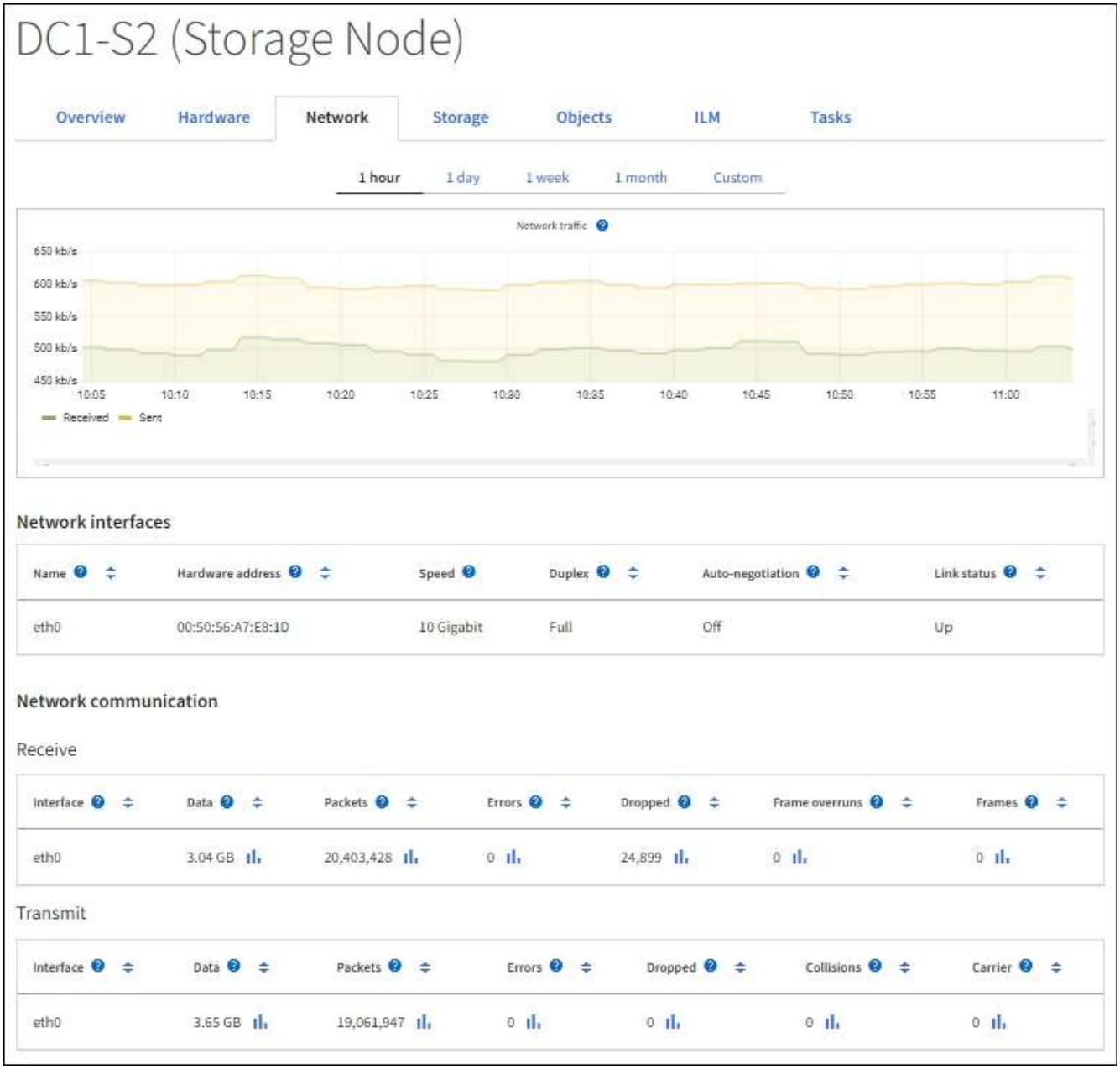
- 租户最大的分段（ S3 ）或容器（ Swift ）列表
- 一个条形图，表示最大分段或容器的相对大小
- 已用总空间量，如果设置了配额，则还会显示剩余空间量和百分比



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。

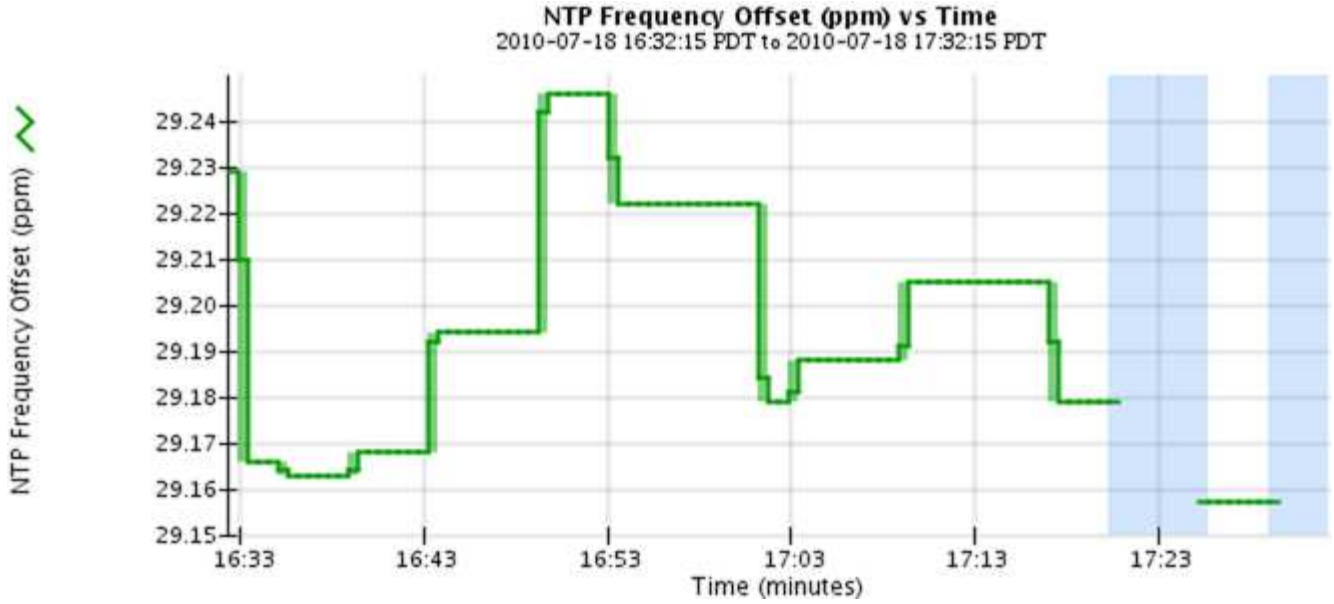
图形有四种类型：

- * 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。

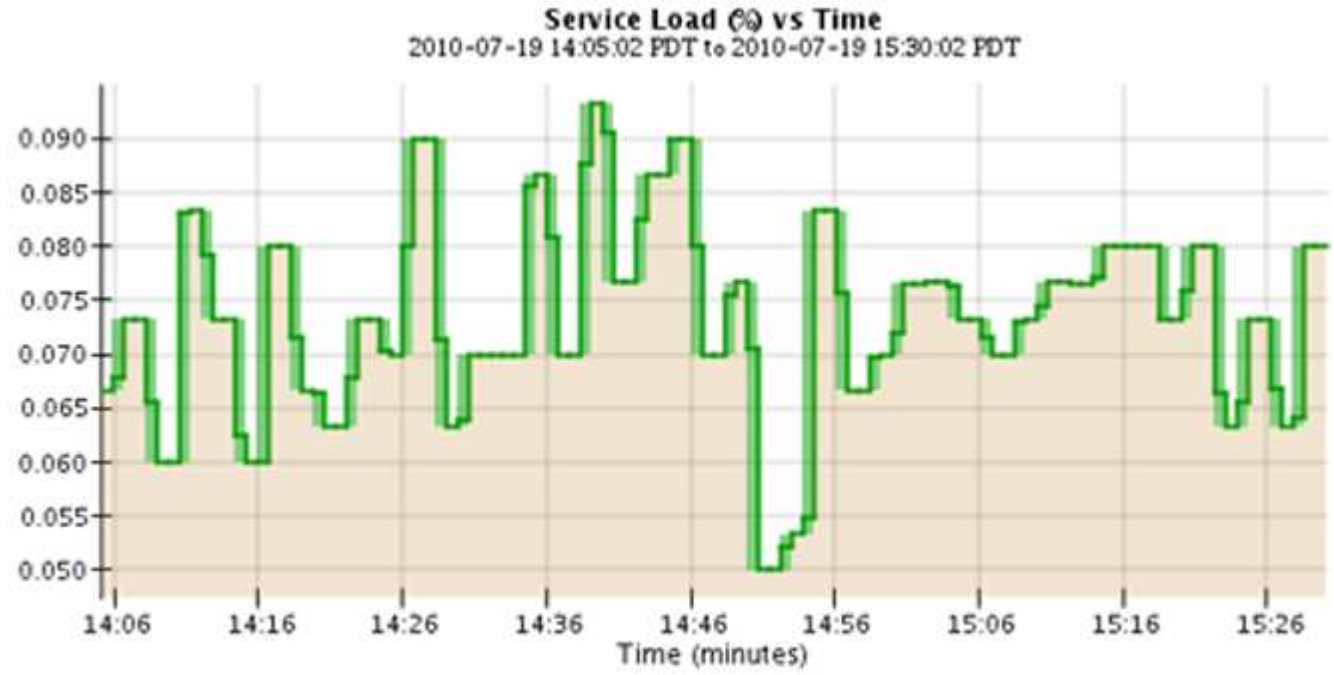


Grafana 图表也包含在预构建的信息板中，这些信息板可从 * 支持 * > * 工具 * > * 指标 * 页面获得。

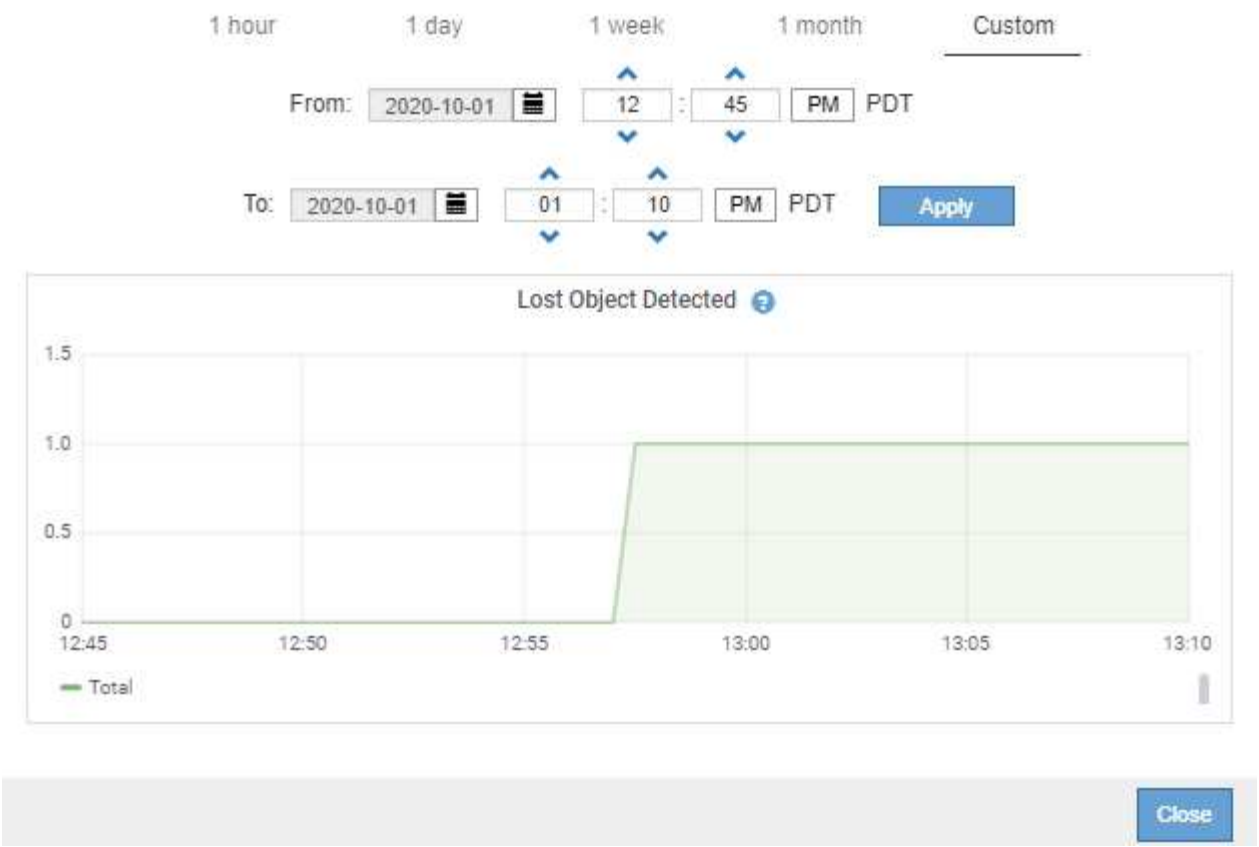
- * 折线图 * ： 可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用折线图绘制具有单位值（例如 NTP 频率偏移，以 PPM 为单位）的 StorageGRID 属性值。值的更改会按定期数据间隔（箱）绘制。



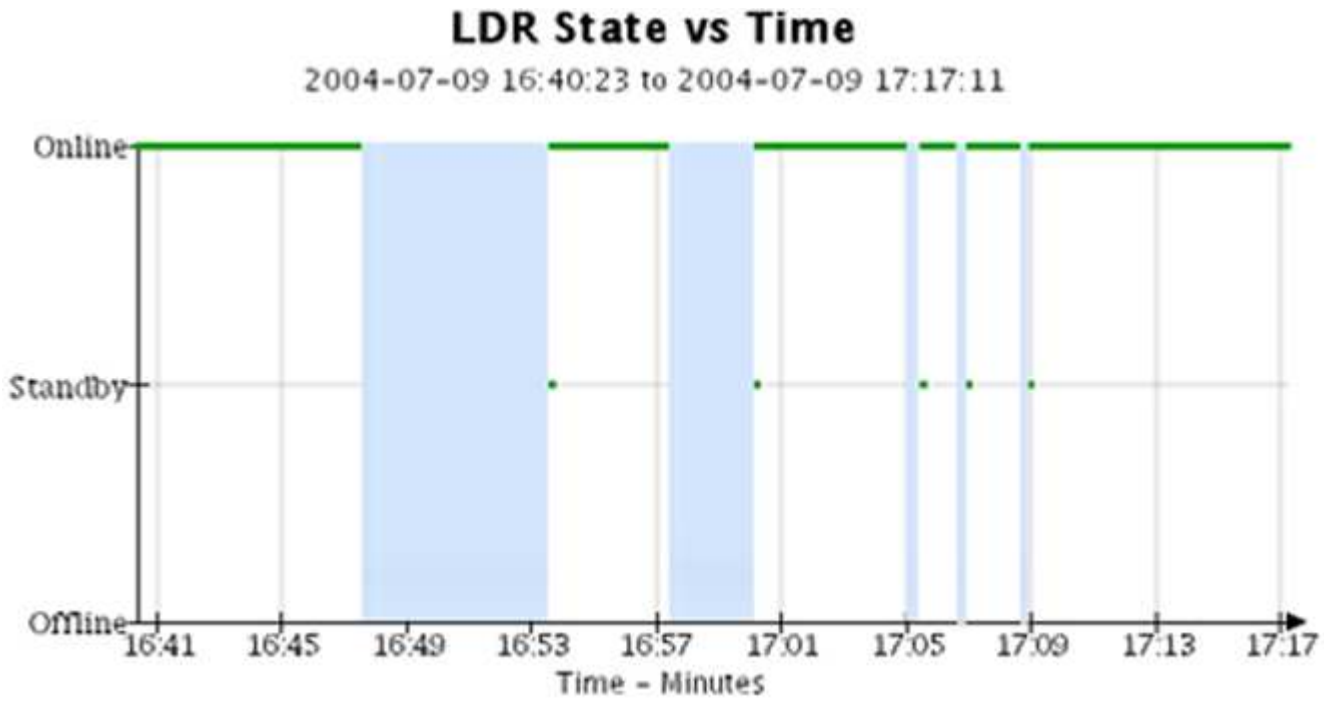
- * 区域图形 * ： 可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用分区图绘制容量属性数量，例如对象计数或服务负载值。区域图形与折线图类似，但在折线下方会显示浅棕色阴影。值的更改会按定期数据间隔（箱）绘制。



- 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

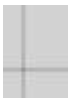
"查看节点页面"

"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。
	深绿色线条周围的浅绿色阴影表示该时间范围内的实际值会有所不同、并已进行"分箱"以加快绘图速度。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。

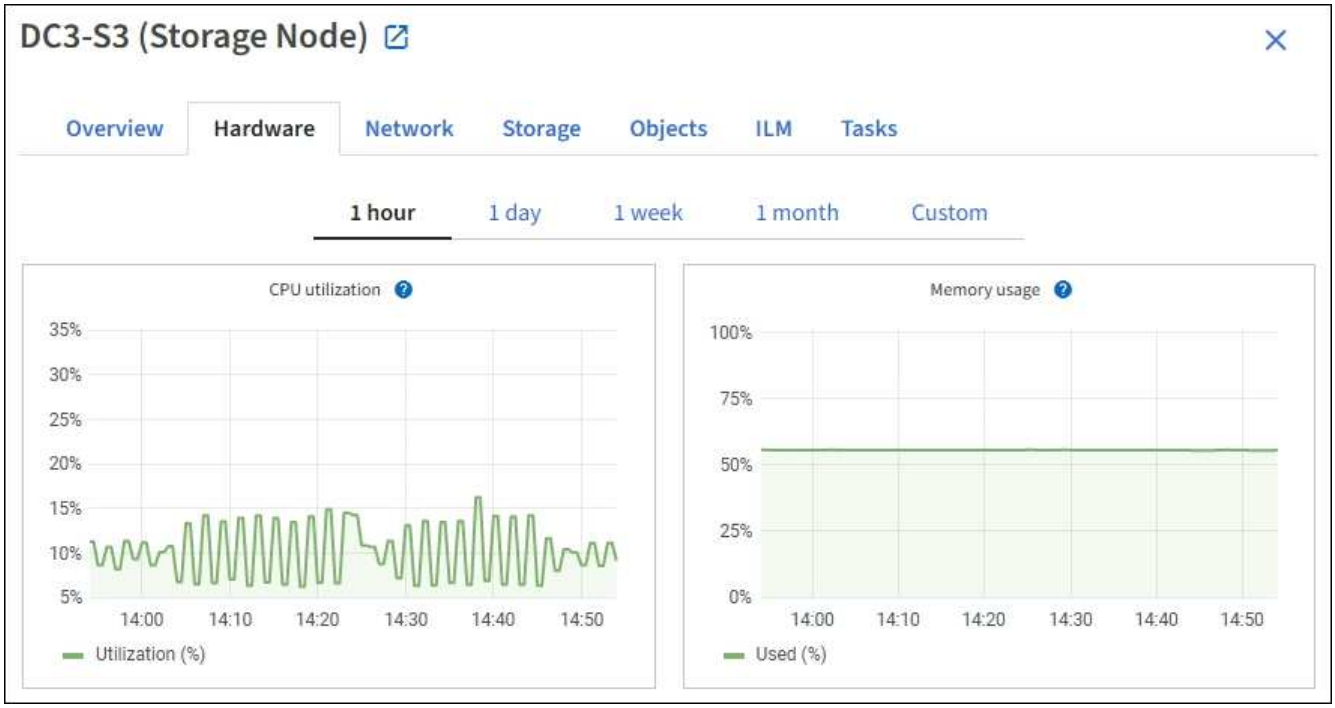
开始之前

您必须使用登录到网格管理器 "支持的 Web 浏览器"。

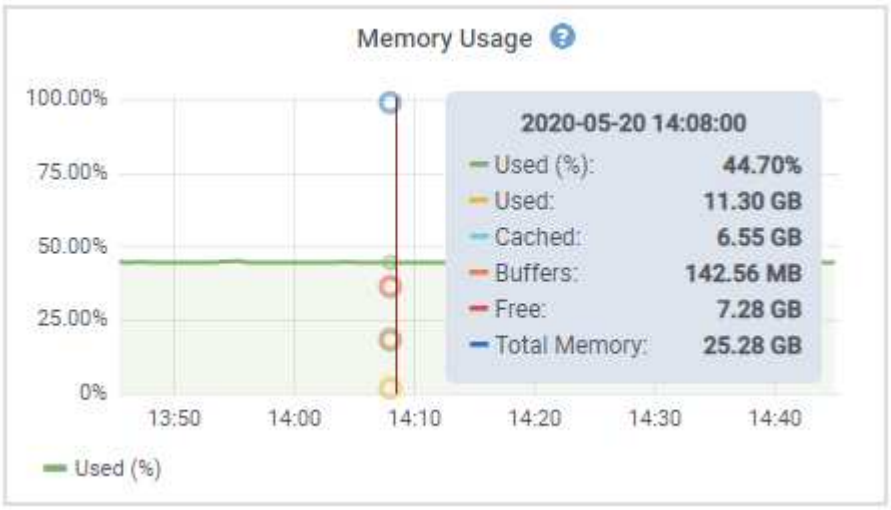
步骤

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。



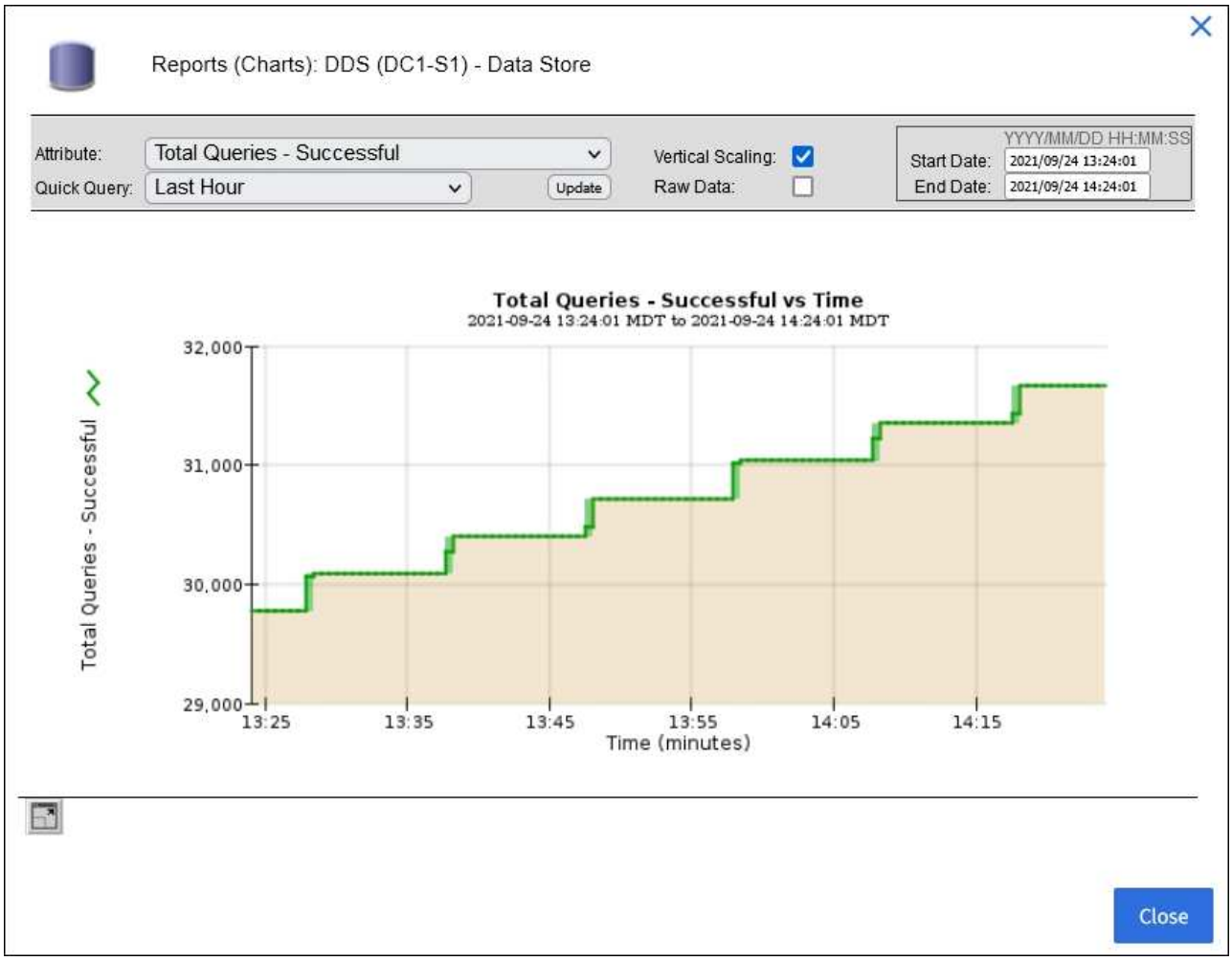
3. (可选)将光标置于图表上方、以查看特定时间点的更多详细值。

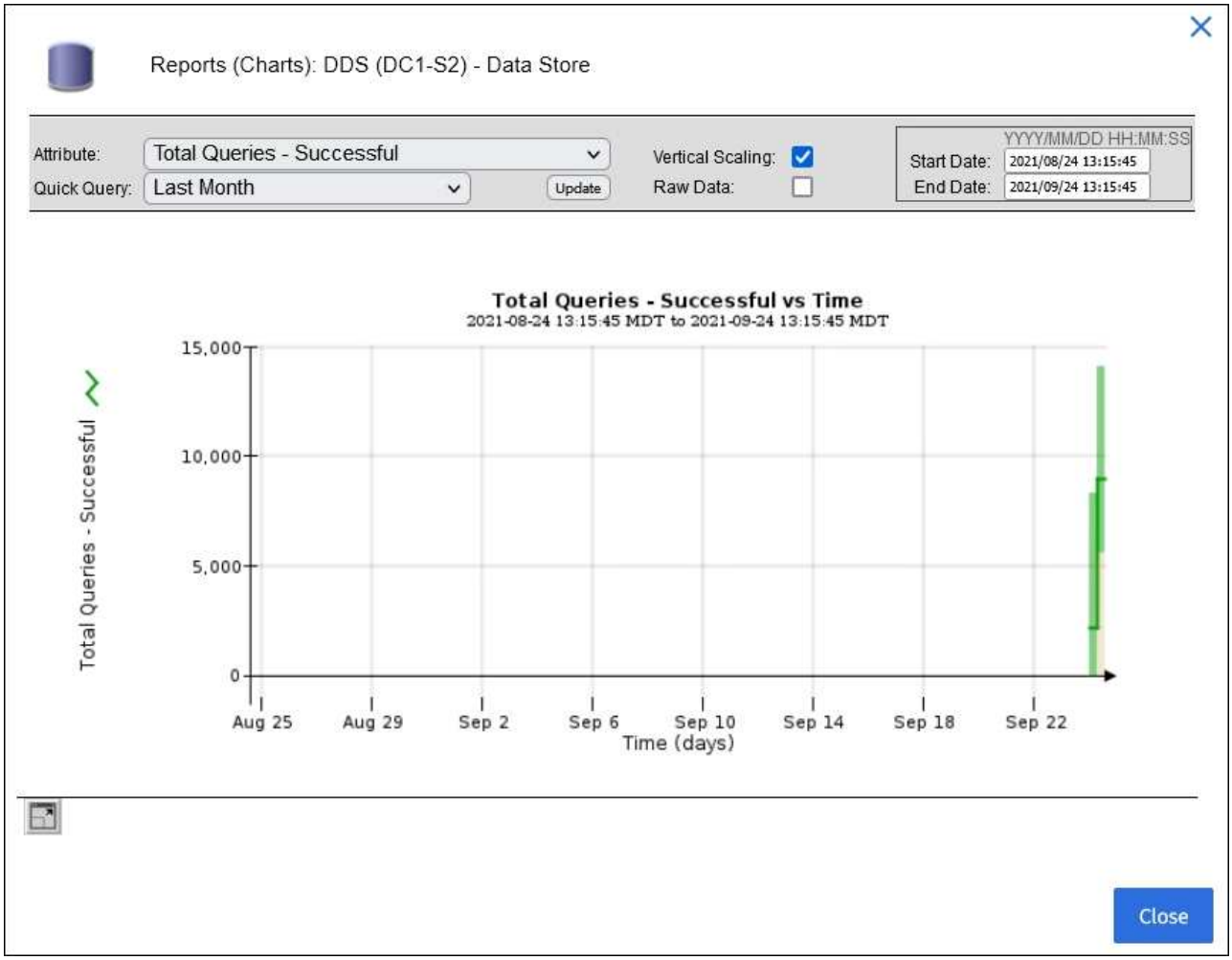


4. 您通常可以根据需要显示特定属性或指标的图表。从节点页面上的表中，选择图表图标 属性名称右侧。

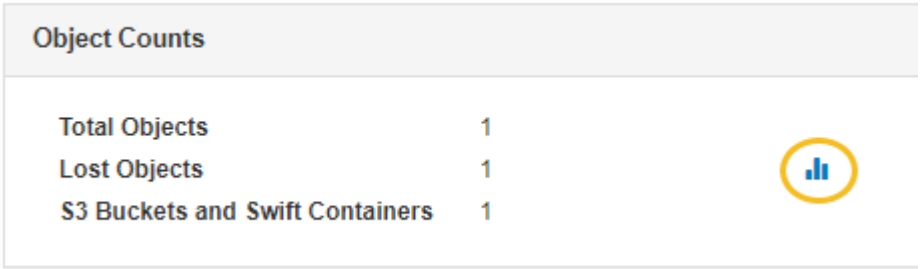
   图表并非适用于所有指标和属性。

   - 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。

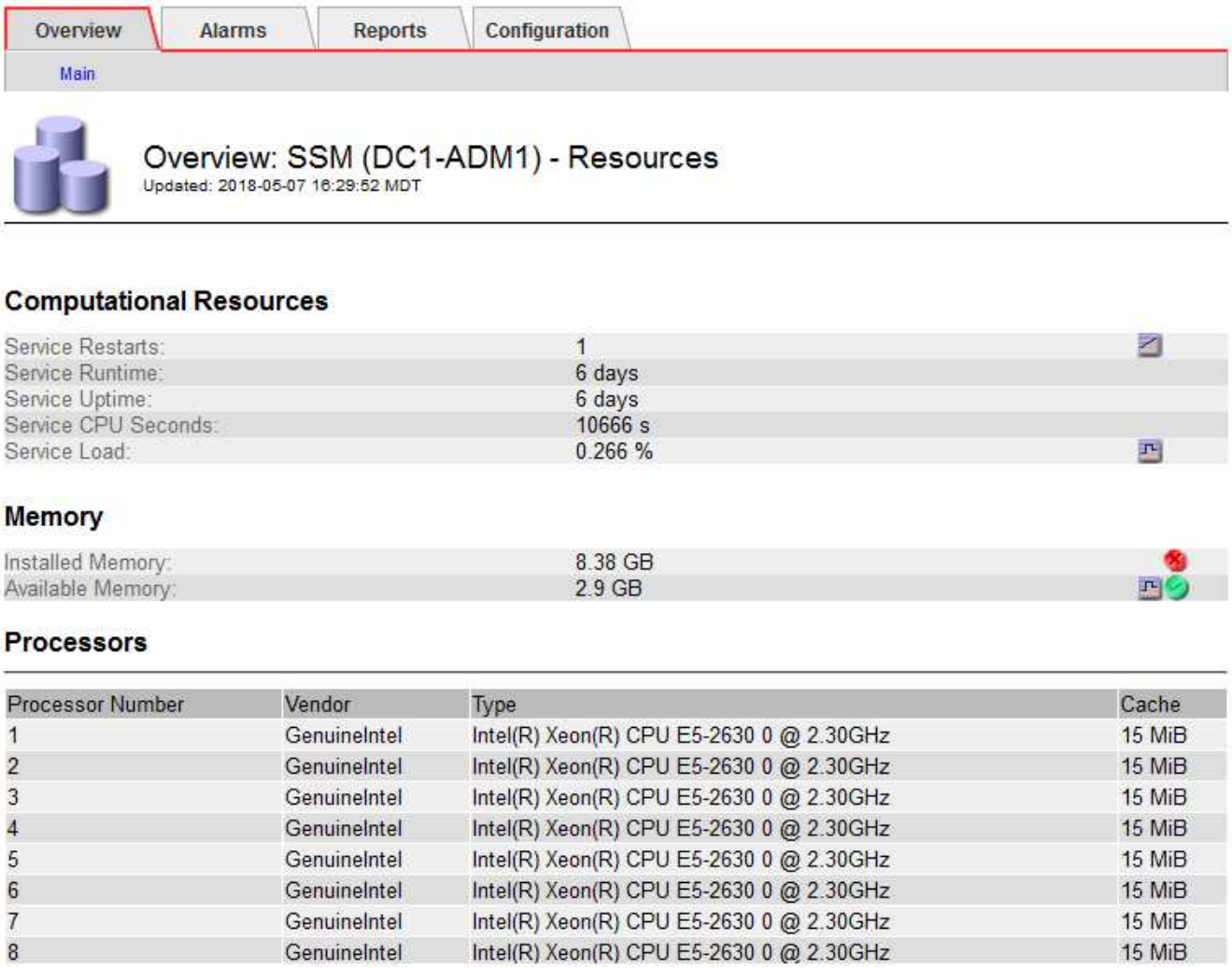

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 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"页上未显示的属性的图表，请选择*support*>*Tools*>*Grid Topology。
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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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，请清除*垂直缩放*复选框。
5. 要以全精度显示值，请选中*Raw Data*复选框，或者要将值舍入到小数点后三位(例如，对于以百分比形式报告的属性)，请清除*Raw Data*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。

   使用格式 *YYYY/MM/DDHH:MM:SS* 在本地时间。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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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. 要将值舍入到小数点后三位(例如，对于以百分比形式报告的属性)，请清除*Raw Data*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。

   使用格式 `YYYY/MM/DDHH:MM:SS` 在本地时间。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

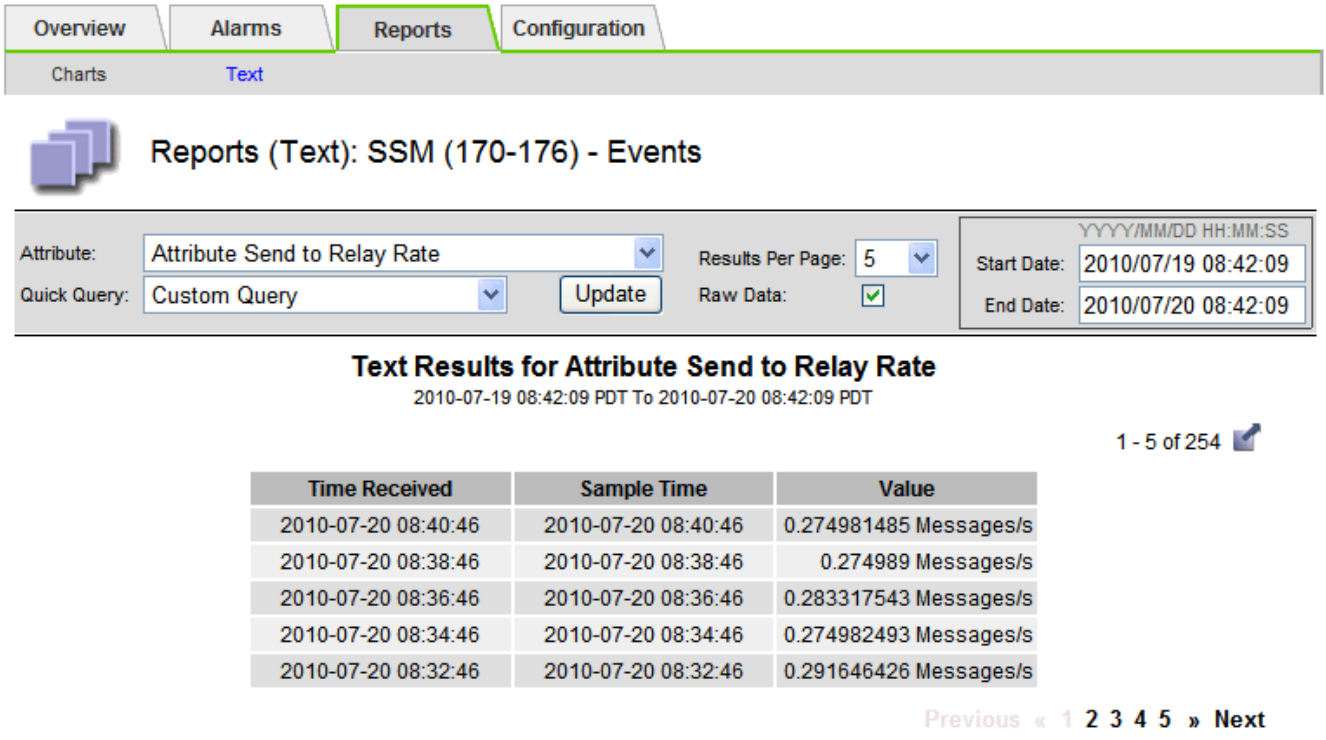
导出的文本报告将打开一个新的浏览器选项卡，在此可以选择和复制数据。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "维护或root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*检测到未识别的损坏对象*警报。

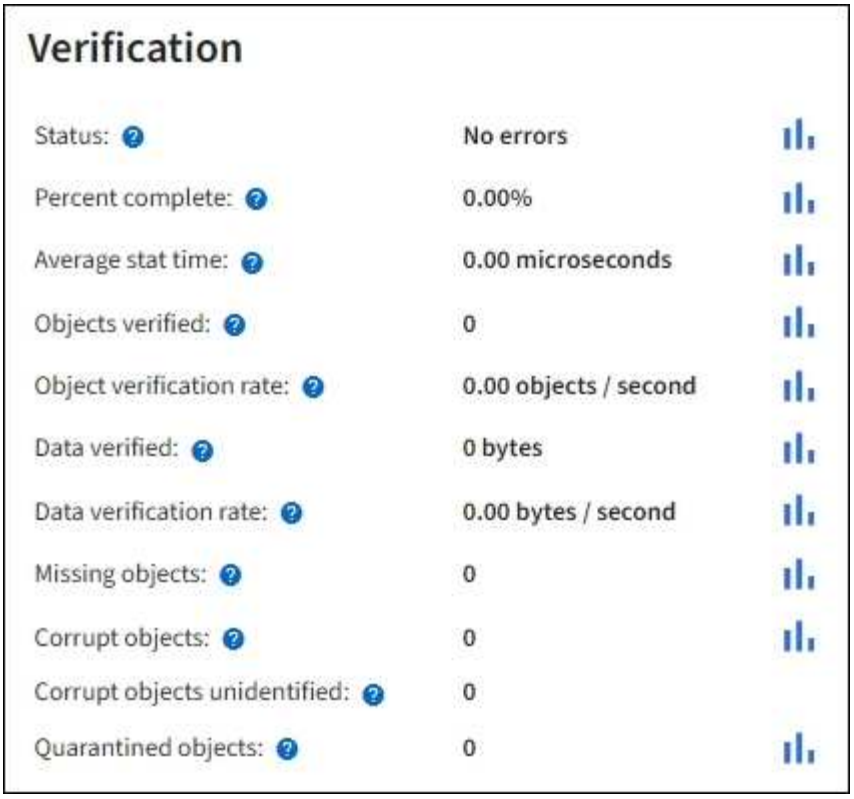
- 用户可以触发 * 对象存在检查 * ，以便更快速地验证对象数据是否存在（尽管不是正确）。

  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。

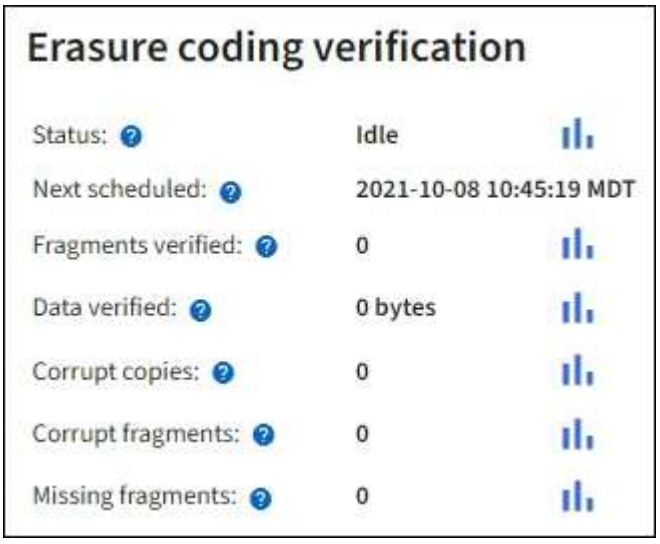
您应定期查看后台验证和对象存在检查的结果。立即调查任何对象数据损坏或丢失的实例，以确定根发生原因。

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。

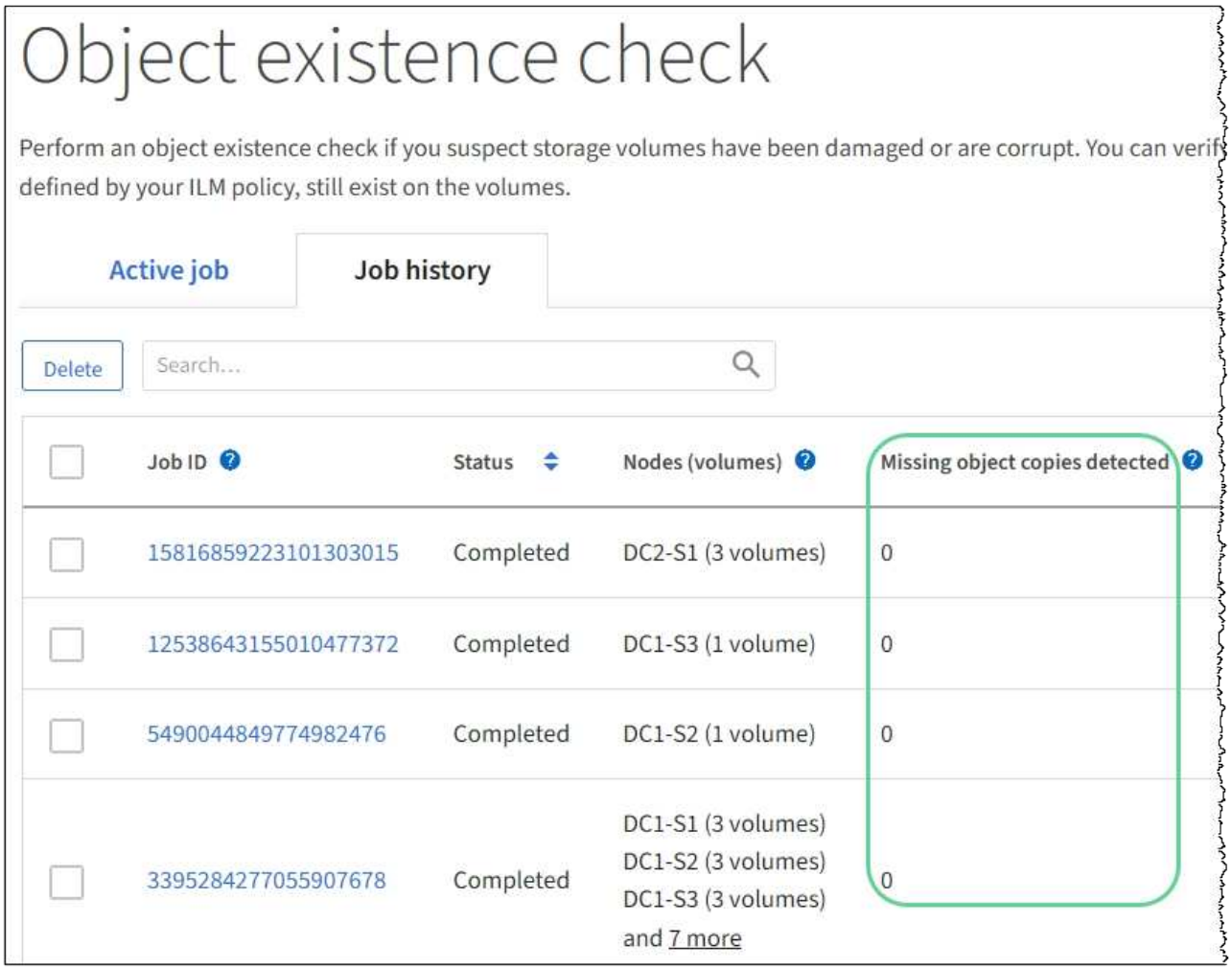


- 要检查擦除编码的片段验证，请选择 * 存储节点 _* > * ILM * ，然后查看擦除编码验证部分中的属性。



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、并且触发了*对象丢失*警报、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。

事件消息也会在中列出 `/var/local/log/bycast-err.log` 日志文件。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。本节提供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

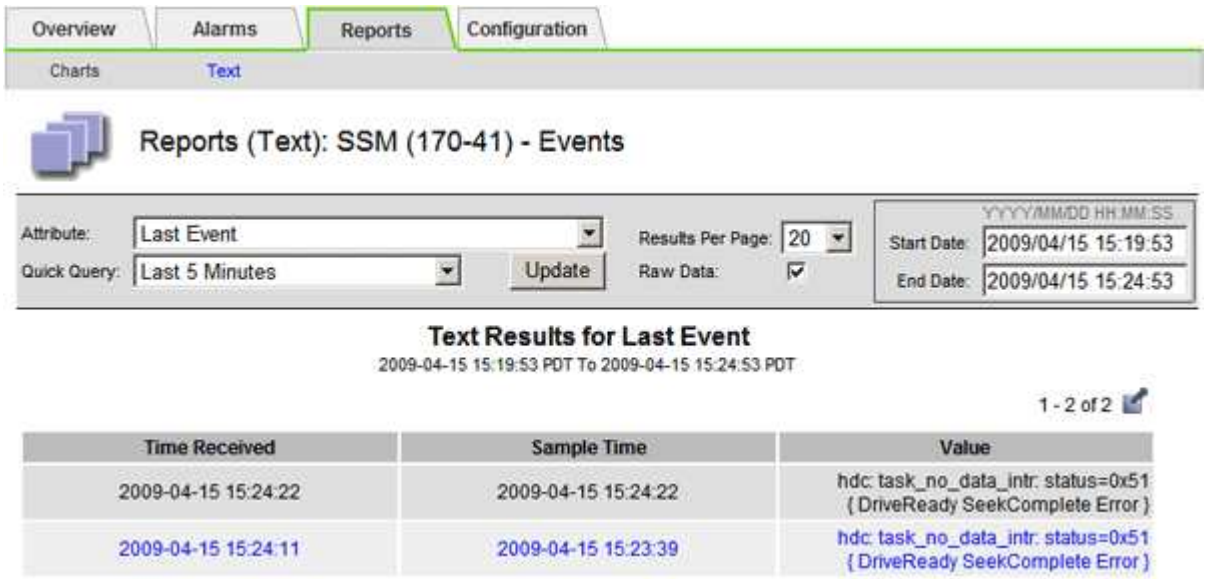
1. 查看每个网格节点的系统事件：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 概述 * > * 主 * 。
2. 生成先前事件消息的列表，以帮助隔离过去发生的问题：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 报告 * 。
   c. 选择 * 文本 * 。

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

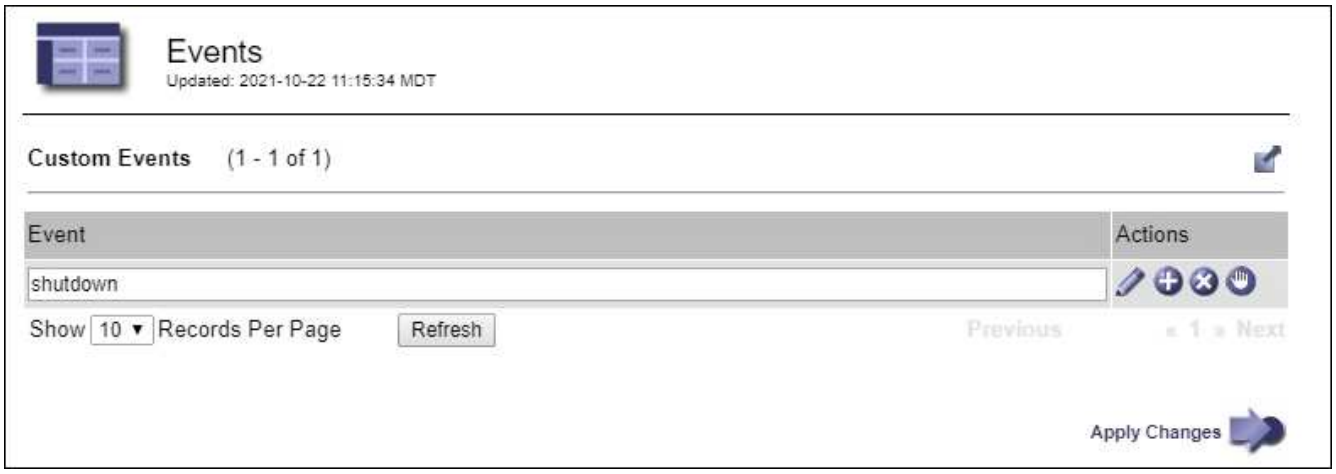
请考虑创建自定义事件以监控重复出现的问题。以下注意事项适用于自定义事件。

- 创建自定义事件后，系统会监控其每次发生情况。
- 基于中的关键字创建自定义事件 `/var/local/log/messages` 文件、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：*中并非所有条目 `/var/local/log/messages` 除非文件满足上述要求、否则将匹配这些文件。

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。

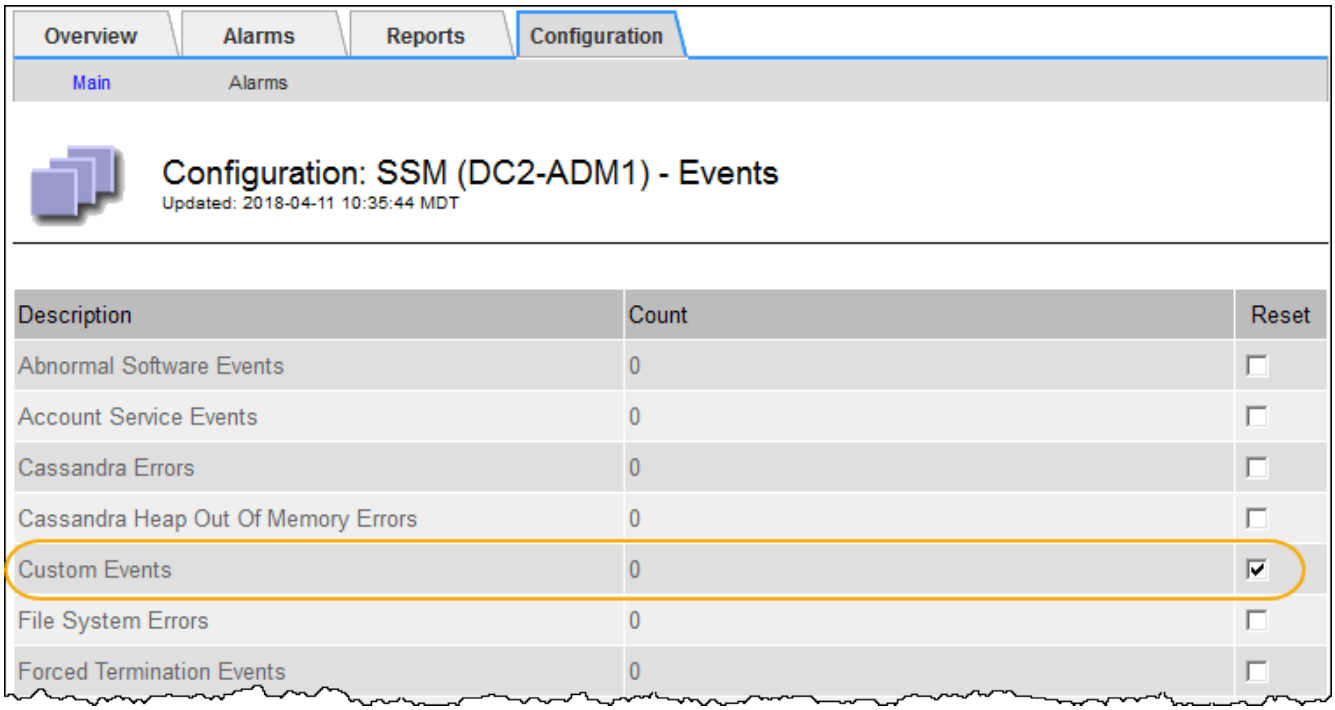
将自定义事件计数重置为零

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。

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。

步骤

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*Reset *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。

为了轻松访问审核日志、您可以 "配置NFS的审核客户端访问"。您也可以直接从管理节点的命令行访问审核日志文件。

默认情况下、StorageGRID可以发送审核信息、也可以更改目标：

- StorageGRID默认为本地节点审核目标。
- 可能会将网格管理器和租户管理器审核日志条目发送到存储节点。
- 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。
- "了解如何配置审核消息和日志目标"(英文)

有关审核日志文件、审核消息格式、审核消息类型以及可用于分析审核消息的工具的详细信息、请参见 "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）。

开始之前

- 您必须使用登录到主管理节点上的网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您必须具有配置密码短语。

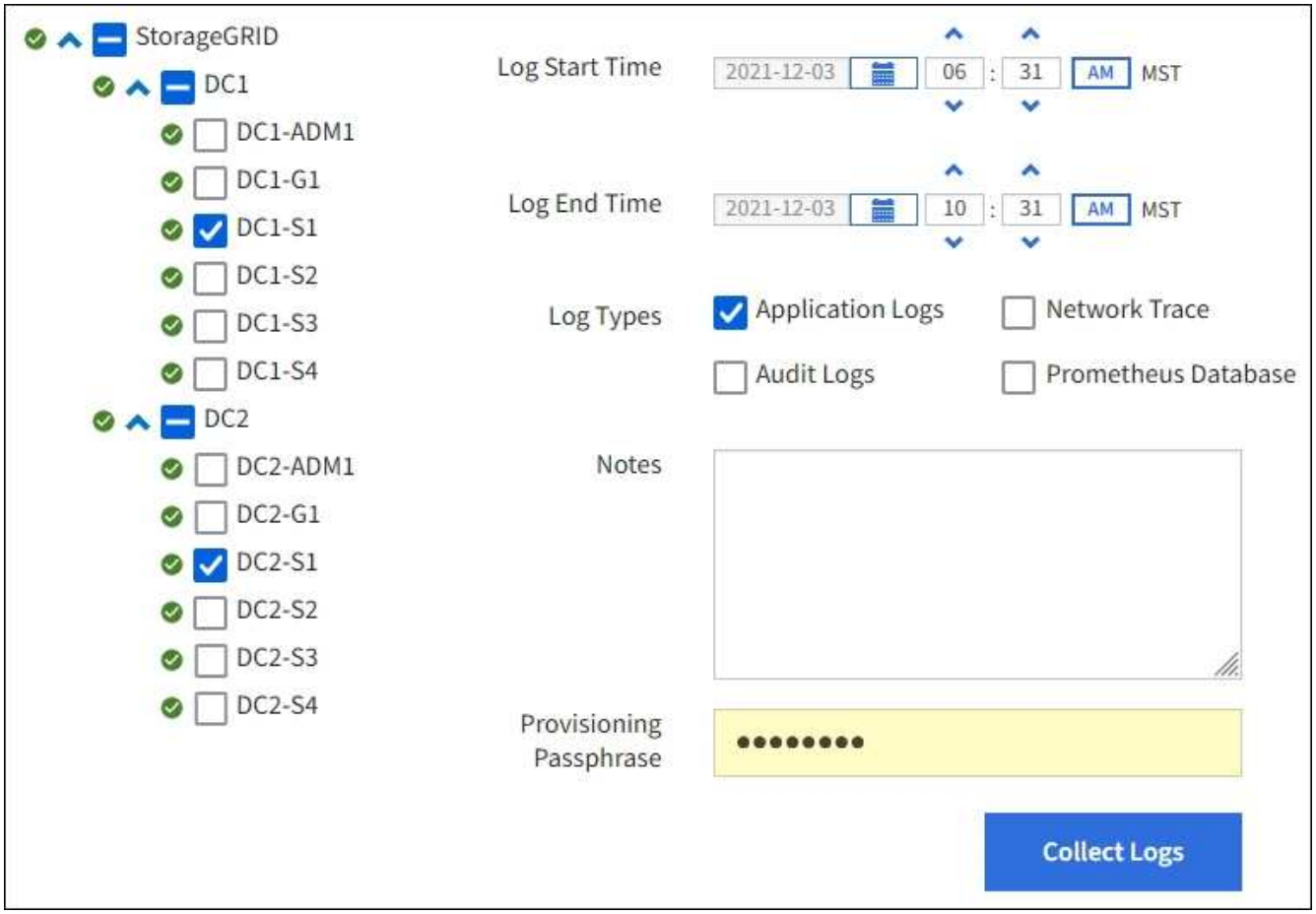
关于此任务

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。您的注释将添加到名为的文件中 `info.txt`以及有关日志文件收集的其他信息。。 `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**软件包

要帮助技术支持解决StorageGRID系统的问题、您可以手动触发要发送的AutoSupport软件包。

开始之前

- 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访问权限或其他网格配置权限。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 在*操作*选项卡上，选择*发送用户触发的AutoSupport *。

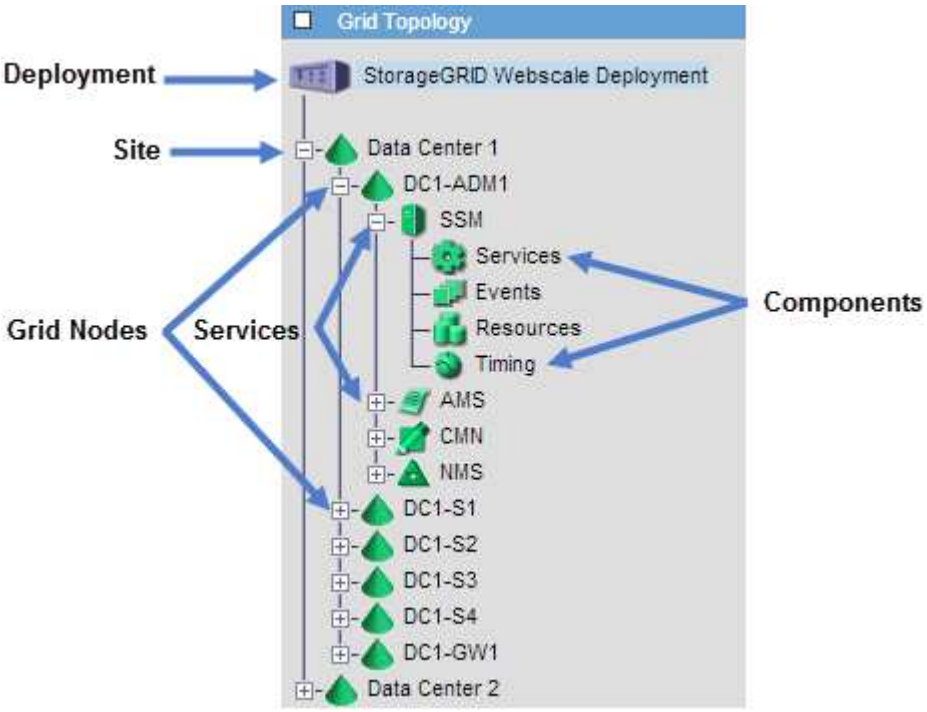
   StorageGRID尝试向NetApp 支持站点 发送AutoSupport软件包。如果尝试成功，则会更新 * 结果 * 选项卡上的 * 最新结果 * 和 * 最后成功时间 * 值。如果出现问题，“最新结果”值将更新为“失败”，并且StorageGRID不会尝试再次发送AutoSupport软件包。

   发送用户触发的AutoSupport软件包后、请在1分钟后刷新浏览器中的AutoSupport页面以访问最新结果。

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。

StorageGRID 属性

属性可报告 StorageGRID 系统许多功能的值和状态。每个网格节点，每个站点和整个网格均可使用属性值。

StorageGRID 属性在网格管理器的多个位置使用：

- * 节点页面 * ： 节点页面上显示的许多值都是 StorageGRID 属性。 （ Prometheus 指标也显示在节点页面上。）

- * 警报 * ： 当属性达到定义的阈值时， StorageGRID 警报（原有系统）将在特定严重性级别触发。
- * 网格拓扑树 * ： 属性值显示在网格拓扑树中（ * 支持 * > * 工具 * > * 网格拓扑 * ）。
- * 事件 * ： 当某些属性记录节点的错误或故障情况时，发生系统事件，包括网络错误等错误。

属性值

属性会尽力报告，并且大致正确。在某些情况下，属性更新可能会丢失，例如服务崩溃或网格节点故障和重建。

此外，传播延迟可能会减慢属性报告的速度。大多数属性的更新值会按固定间隔发送到 StorageGRID 系统。更新可能需要几分钟才能在系统中显示出来，并且可以在稍不同的时间报告同时更改的两个属性。

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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

关于此任务

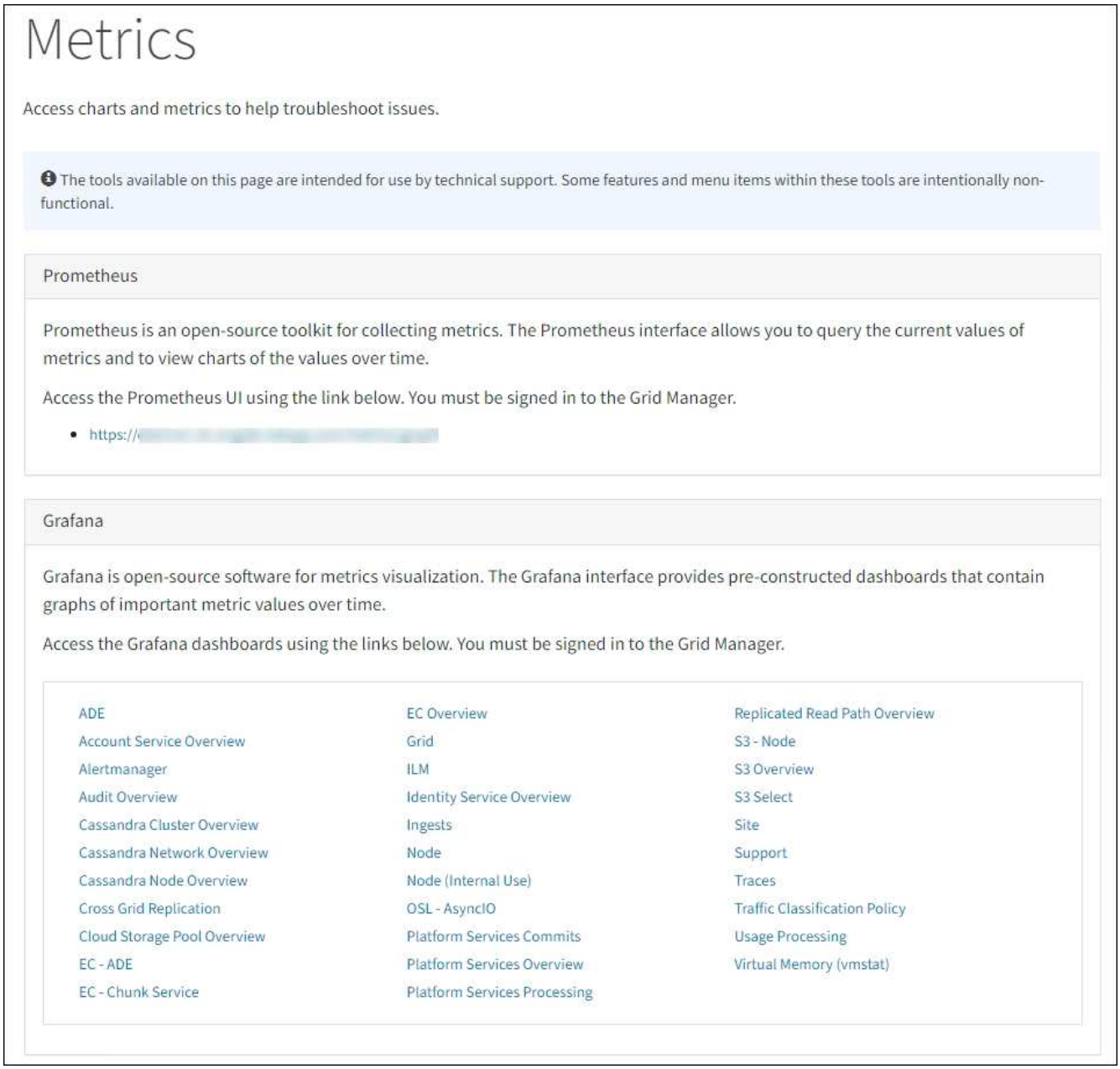
您可以通过指标页面访问 Prometheus 和 Grafana 用户界面。Prometheus 是用于收集指标的开源软件。Grafana 是用于可视化指标的开源软件。

> 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"

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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。

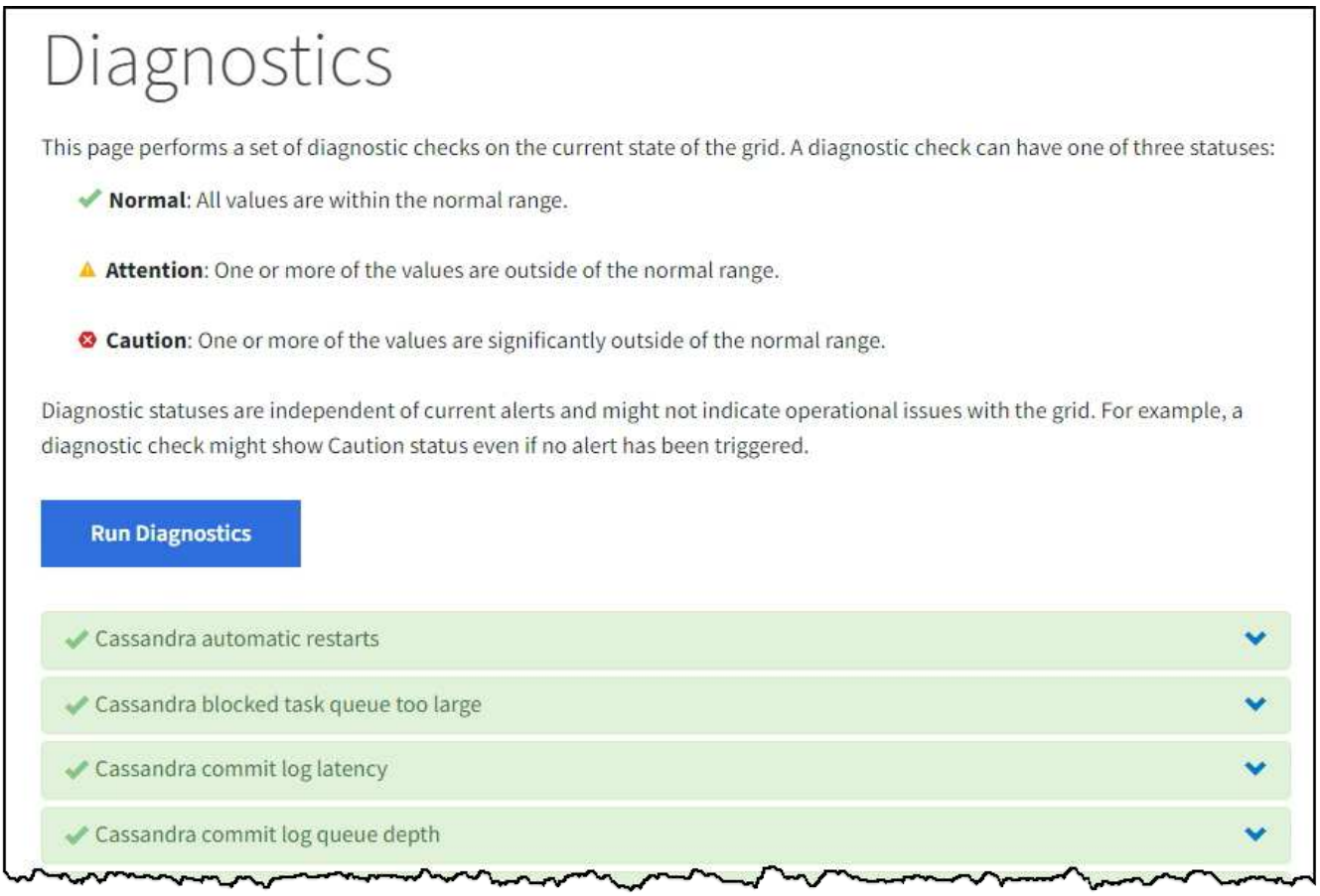
诊断状态与当前警报无关，可能并不表示网格存在操作问题。例如，即使未触发任何警报，诊断检查也可能会显示 " 小心 " 状态。

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。



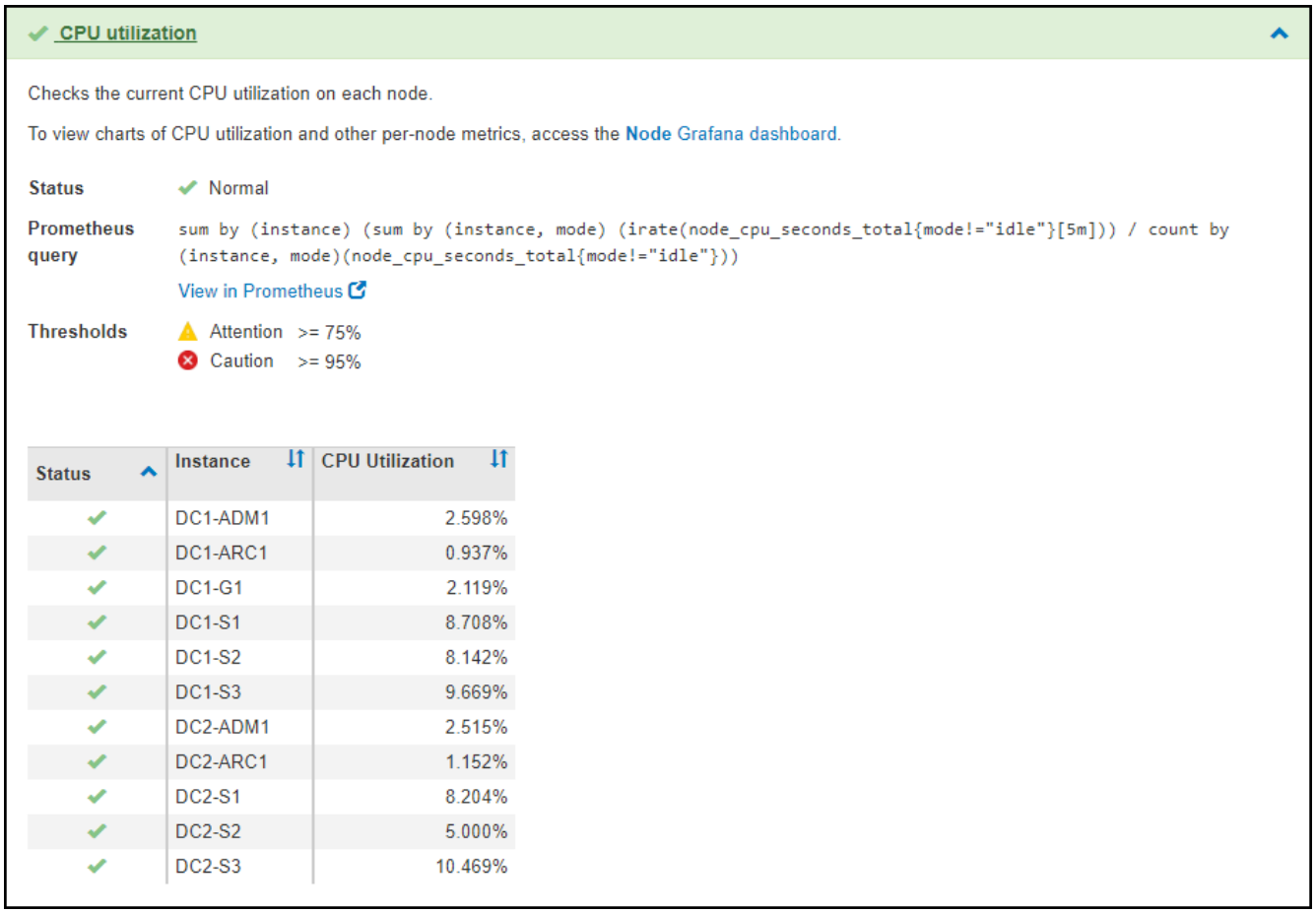
2. 要了解有关特定诊断的详细信息，请单击行中的任意位置。

   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。(阈值并不用于所有诊断。)

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。

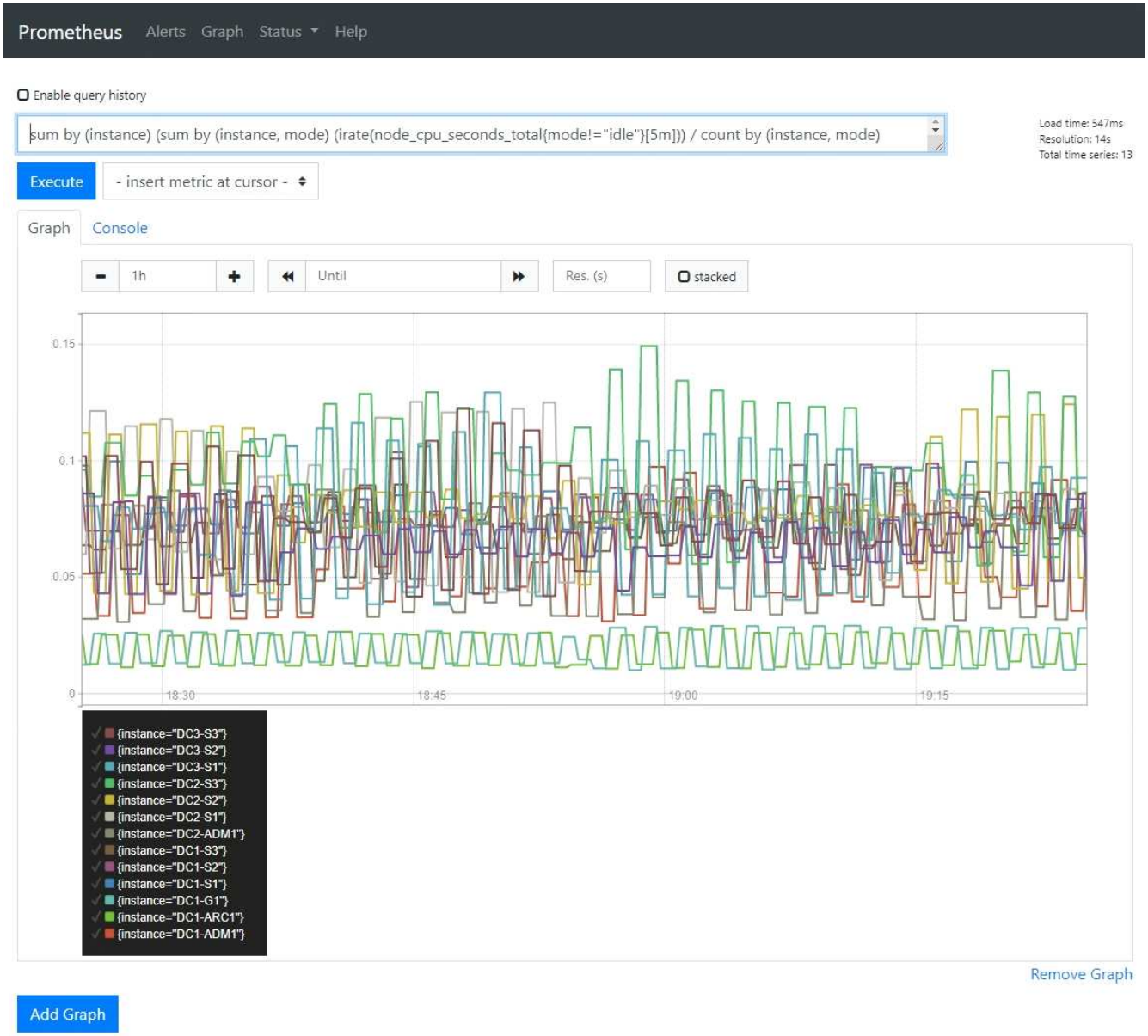
   并非所有诊断都显示此链接。

   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。



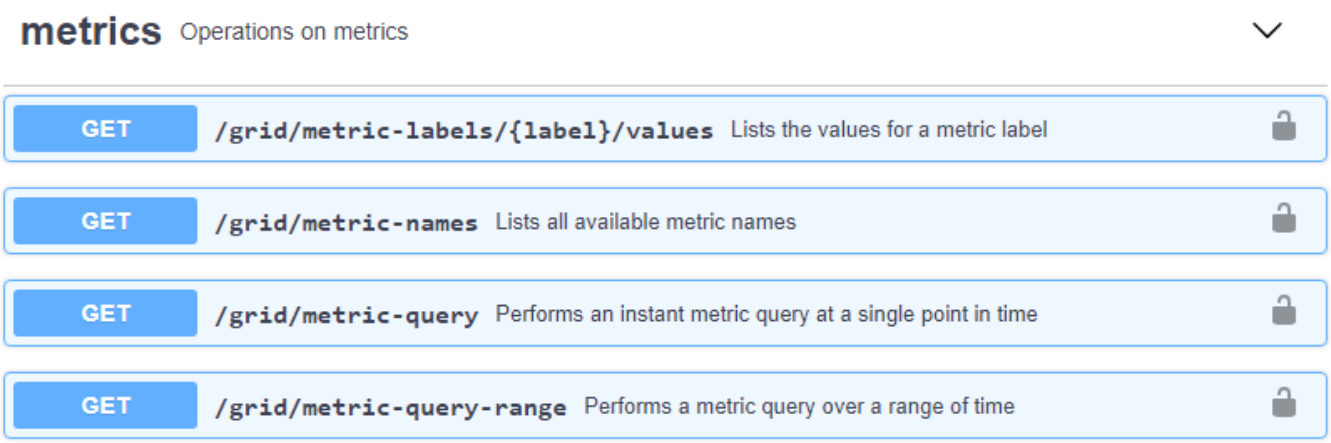
创建自定义监控应用程序

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，然后选择*API documents*>*metrics*。



本文档不会详细介绍如何实施自定义监控应用程序。

排除StorageGRID 系统故障

StorageGRID 系统故障排除：概述

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 。

通常、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插入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。

问题	响应示例
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？	某些对象可以检索、而其他对象则无法检索。
数据是否存在风险？	否
开展业务的能力是否受到严重影响？	是、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	为什么要收集此数据	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。	• "查看当前警报和已解决警报" • "管理警报（旧系统）"
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"

要收集的数据类型	为什么要收集此数据	说明
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软件包" • "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

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。将光标置于图表上方、以估计每天占用的存储容量 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。将光标置于图表上方、以估计每天占用的元数据存储容量 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	在Grid Manager信息板上，选择*Performance*>*S3 operations*或*Performance*>*Swift operations*。 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 * 。将光标置于"lng设置"上、然后检索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。
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。将光标置于图表上方以估算系统的*评估率*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。将光标置于图表上方，估算系统的*Scan Rate (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。将光标置于图表上方可估算系统*已排队(来自客户端操作)的对象*的基线值。

属性	价值	如何获取
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是否创建复制的或经过重复编码的对象？ILM 是否可确保站点冗余？ILM规则是否使用平衡、严格或双重提交加网行为？

✔	项目	注释：
	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
	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

根据问题的不同、您可能希望这样做 "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。

开始之前

- 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**存储分段和对象关键字：通过插入对象时 "S3接口"，则客户端应用程序使用存储分段和对象键组合来存储和标识对象。
  - **Swift**容器和对象名称:通过装载对象时 "Swift接口"，则客户端应用程序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 * 。

。 "对象元数据查找结果" 显示。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",
```


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

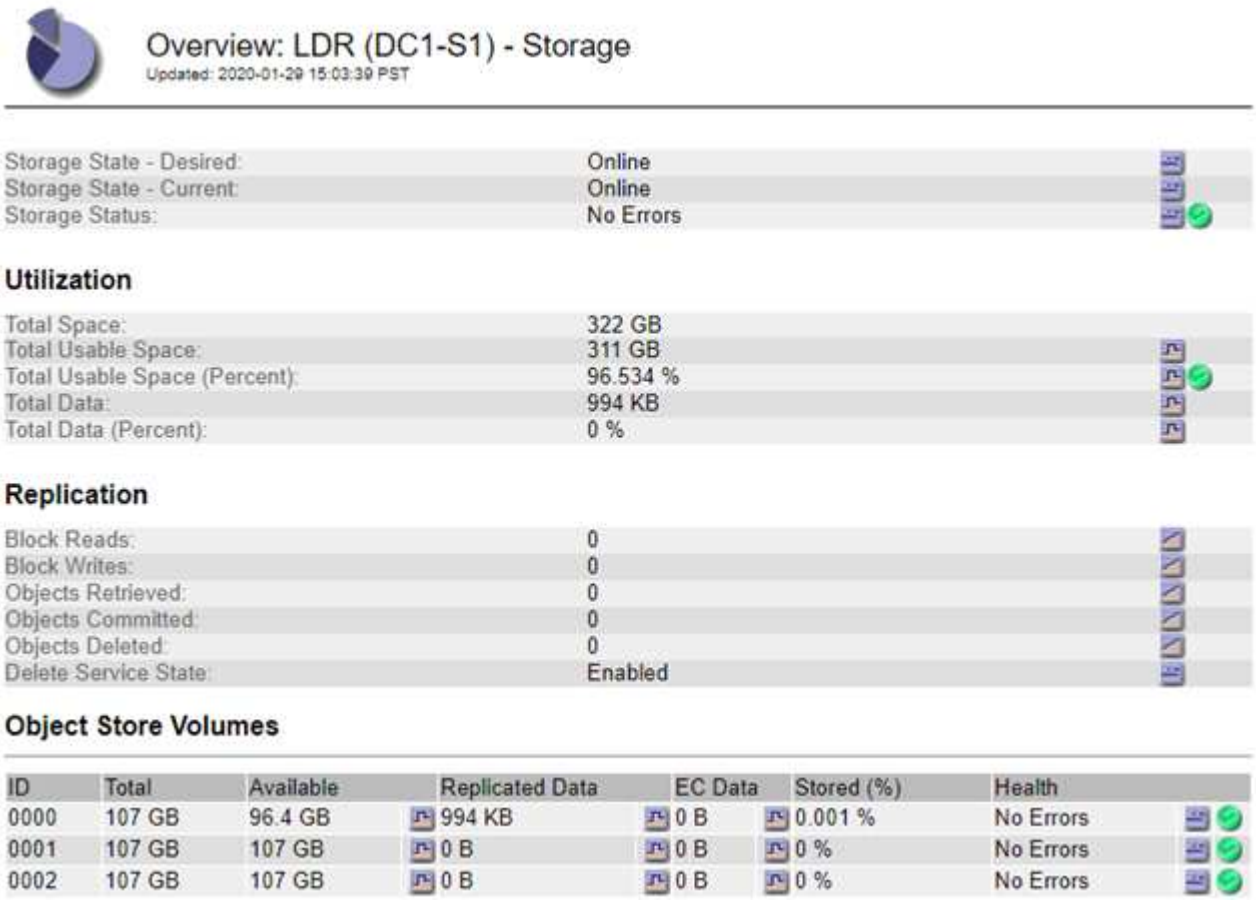
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

以查看更多信息 "有关每个存储节点的详细信息"、请按照以下步骤操作：

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，可以转到*Configuration*选项卡和 "将存储节点置于只读 - 状态" 以便StorageGRID 系统可以在您准备完全恢复服务器时使用它进行数据检索。

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、系统将生成并放置一个未损坏的新副本、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。有关访问已拒绝的对象数据的详细信息、请与技术支持联系。

- * 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。如果无法重建损坏的片段、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）

如果系统检测到无法自动更正的损坏对象(因为损坏导致无法识别该对象)，将触发*检测到未识别的损坏对象*警报。

如果后台验证由于找不到另一个副本而无法替换损坏的对象，则会触发*Objects Lost*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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

关于此任务

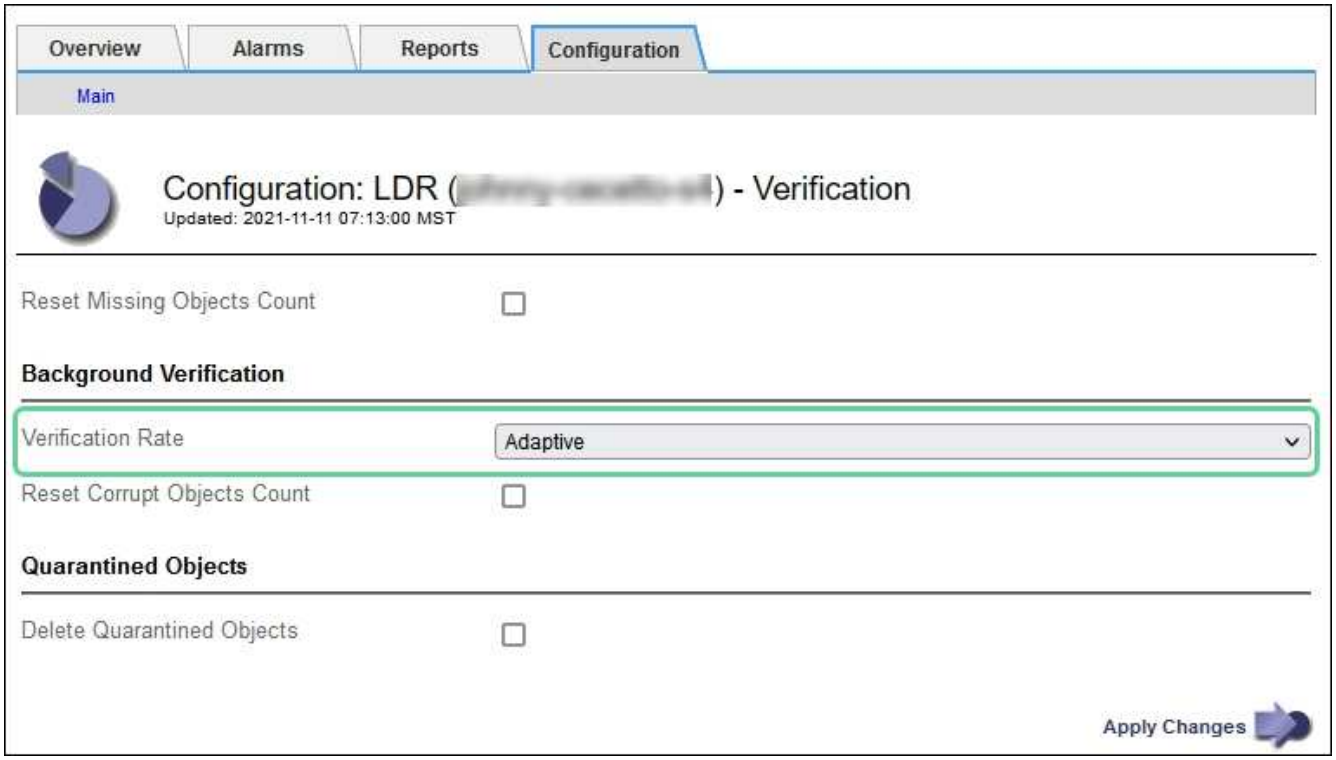
您可以更改存储节点上用于后台验证的验证速率：

- 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。新副本可以在StorageGRID系统中满足活动ILM策略的任何位置创建。
      - 如果无法提取对象标识符(因为它已损坏)，则*已损坏对象未识别*度量将递增，并触发*已检测到未识别损坏对象*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. 如果您确信不需要被检查的对象、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。此时将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(因为丢失的片段太多)、ILM将尝试查找对象的另一个副本、它可以使用该副本生成新的经过删除编码的片段。

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。您还可以选择作业的一致性。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "维护或root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

对象存在性检查作业可能需要数天或数周才能完成、具体取决于网格中的对象数量、选定存储节点和卷以及选定一致性。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*Node name*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。

   一致性决定了用于对象存在性检查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、但不能恢复已取消的作业。
   - 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。

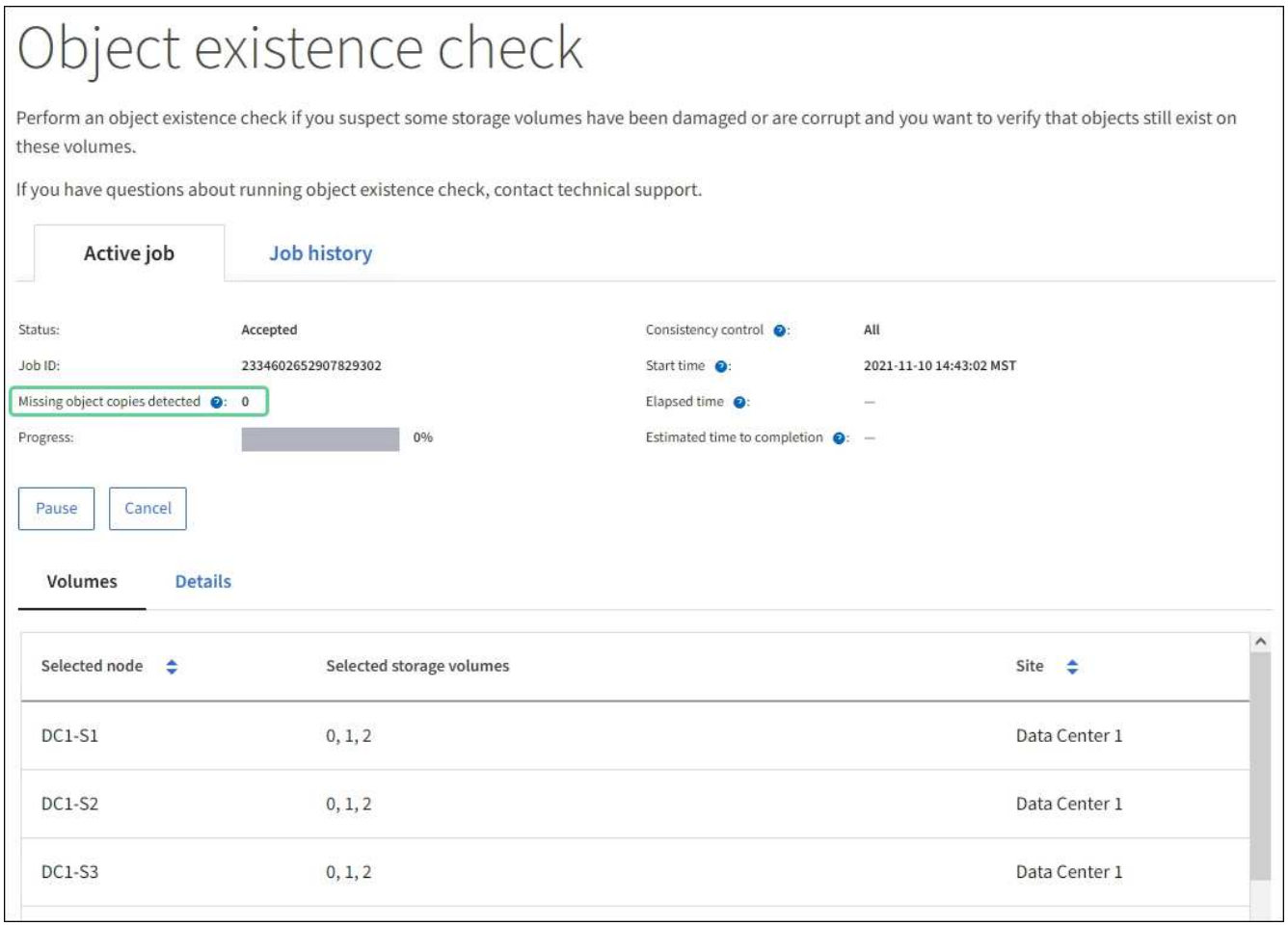
- 出现“Service不可用”或“内部服务器错误”消息。一分钟后，刷新页面以继续监控作业。

  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"，但对于您搜索的对象副本 `LLST` 而不是 `OLST`。

12. 如果为此作业选择了强站点或强全局一致性、请等待大约三周、以确保元数据一致性、然后在相同的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。

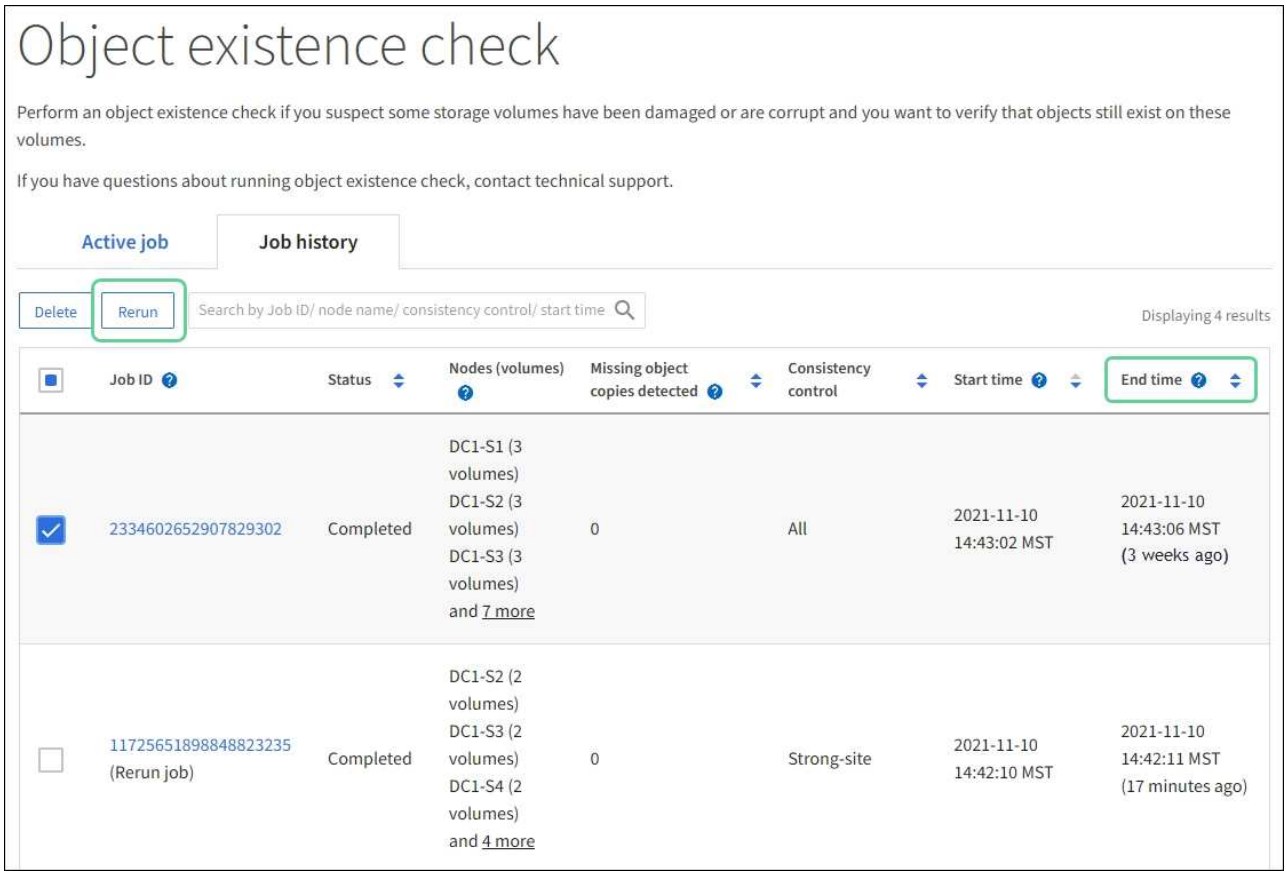
a. 选择 * 维护 * > * 对象存在检查 * > * 作业历史记录 * 。

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*Rerun*。



d. 在重新运行作业向导中、查看选定节点和卷以及一致性。

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。您选择的所有作业将以一个作业的形式重新运行、并保持Strong站点一致性。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。

对**S3**放置对象大小太大警报进行故障排除

如果租户尝试执行的非多部分PutObject操作超过S3大小限制5 GiB、则会触发"S3 Put Object Size Too Lize"警报。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

确定哪些租户使用大于5 GiB的对象、以便您可以向其发出通知。

步骤

1. 转到*configuration*>*Monitoring*>*Audit and syslog server*。
2. 如果客户端写入正常、请访问审核日志：

   a. 输入 … `ssh admin@primary_Admin_Node_IP`

   b. 输入中列出的密码 `Passwords.txt` 文件

   c. 输入以下命令切换到root： `su -`

   d. 输入中列出的密码 `Passwords.txt` 文件

   以root用户身份登录后、提示符将从变为 `$` to `#`。

   e. 更改为审核日志所在的目录。

   审核日志目录和适用节点取决于您的审核目标设置。

选项	目标
本地节点(默认)	`/var/local/log/localaudit.log`
管理节点/本地节点	• 管理节点(主节点和非主节点)：`/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log`在此模式下、文件通常为空或缺失。
外部系统日志服务器	`/var/local/log/localaudit.log`

   根据您的审核目标设置、输入： `cd /var/local/log`或 `/var/local/audit/export/`

   要了解更多信息，请参阅 "选择审核信息目标"。

   f. 确定哪些租户正在使用大于5 GiB的对象。

      i. 输入 `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. 对于结果中的每个审核消息、请查看 `S3AI` 字段以确定租户帐户ID。使用消息中的其他字段确定客户端、存储分段和对象使用的IP地址：

代码	**Description**
SAIP	源IP

代码	Description
S3AI	租户ID
S3BK	存储分段
S3KY	对象
CSIZ	大小(字节)

审核日志结果示例

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CSTR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:identity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][SBAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. 如果客户端写入不正常、请使用警报中的租户ID来标识租户：
   a. 转到*support*>*Tools*>*Logs*。收集警报中存储节点的应用程序日志。指定警报前后15分钟。
   b. 提取文件并转到 `bycast.log`：

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. 在日志中搜索 `method=PUT` 并在中确定客户端 `clientIP` 字段。

      示例**bycast**。**log**

      ```
      Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA 2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ: EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
      ```

4. 通知租户PutObject的最大大小为5 GiB、并对大于5 GiB的对象使用多部分上传。
5. 如果应用程序已更改、请忽略警报一周。

对丢失和丢失的对象数据进行故障排除

对丢失和缺失的对象数据进行故障排除：概述

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。
- 对于经过删除编码的副本、如果无法从预期位置检索副本、则在尝试从其他位置检索副本之前、已检测到损坏的副本(ECO)属性会增加一个。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。请参见 "调查丢失的对象"。

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。请参见 "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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您必须具有 `Passwords.txt` 文件

关于此任务

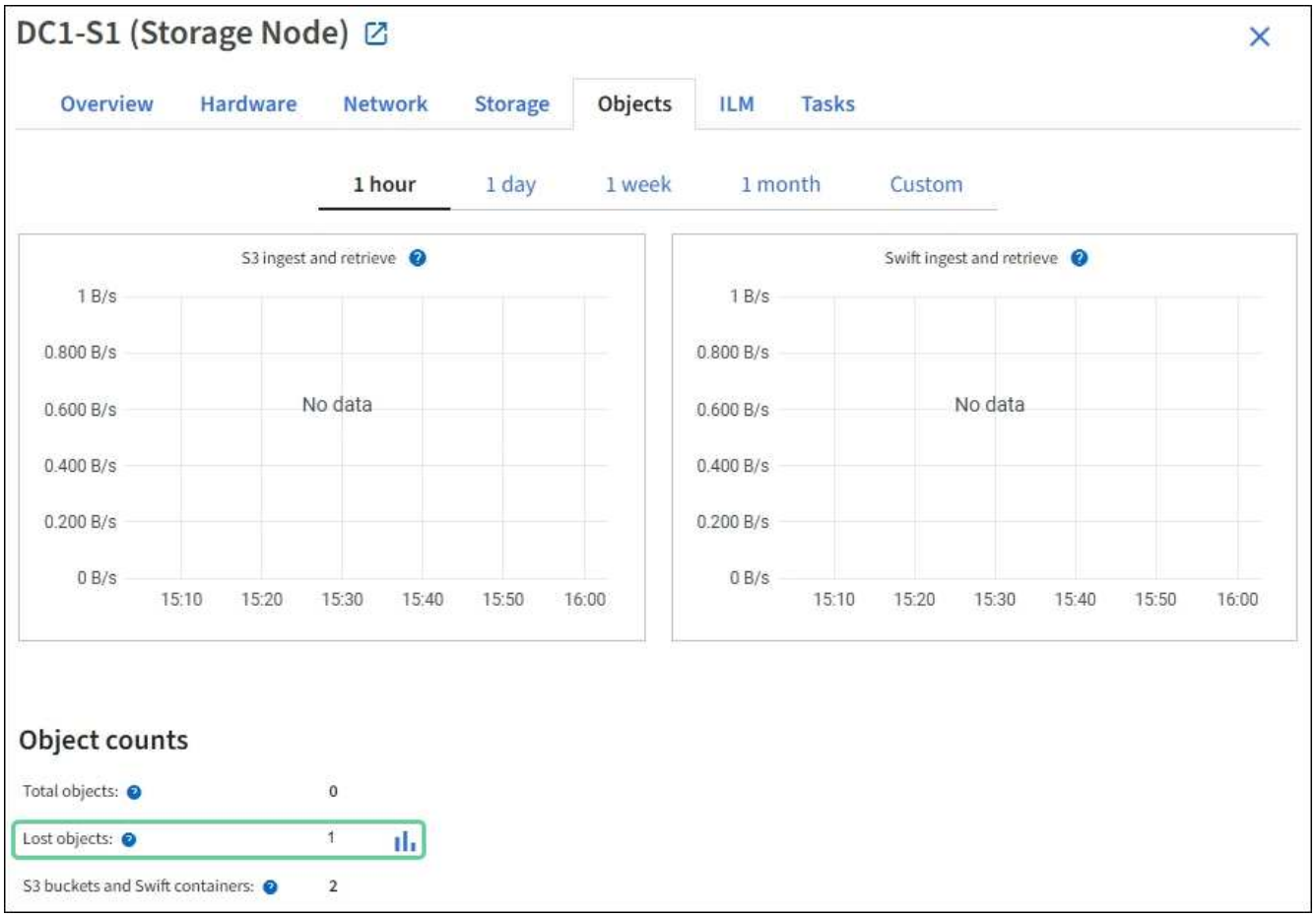
"* 对象丢失 * " 警报表示 StorageGRID 认为网格中没有对象副本。数据可能已永久丢失。

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" 要确定触发*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. 输入中列出的密码 `Passwords.txt` 文件

      iii. 输入以下命令切换到root： `su -`

      iv. 输入中列出的密码 `Passwords.txt` 文件
      以root用户身份登录后、提示符将从变为 `$` to `#`。

   b. 更改为审核日志所在的目录。

      审核日志目录和适用节点取决于您的审核目标设置。

选项	目标
本地节点(默认)	`/var/local/log/localaudit.log`
管理节点/本地节点	• 管理节点(主节点和非主节点)：`/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log`在此模式下、文件通常为空或缺失。

选项	目标
外部系统日志服务器	`/var/local/log/localaudit.log`

根据您的审核目标设置、输入： `cd /var/local/log`或 `/var/local/audit/export/`

要了解更多信息，请参阅 "选择审核信息目标"。

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` 命令以按标识符(UUID)查找对象、然后确定数据是否存在风险。

a. 使用SSH登录到任何存储节点。然后输入"telnet 0 1402"访问LDR控制台。

b. 输入 ... `/proc/OBRP/ObjectByUUID UUID_value`

在第一个示例中、是对象 `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` 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、是对象 `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` 未列出任何位置。

```
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 。请参见有关的信息 "使用网格管理器还原对象数据" 和 "将对象数据还原到存储卷"。

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。

开始之前

- 您具有中标识的任何丢失对象的UUID "调查丢失的对象"。
- 您拥有 `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. 输入中列出的密码 `Passwords.txt` 文件
        iii. 输入以下命令切换到root： `su -`

iv. 输入中列出的密码 `Passwords.txt` 文件
以root用户身份登录后、提示符将从变为 `$` to `#`。

b. 更改为审核日志所在的目录。

审核日志目录和适用节点取决于您的审核目标设置。

选项	目标
本地节点(默认)	`/var/local/log/localaudit.log`
管理节点/本地节点	• 管理节点(主节点和非主节点): `/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log`在此模式下、文件通常为空或缺失。
外部系统日志服务器	`/var/local/log/localaudit.log`

根据您的审核目标设置、输入： `cd /var/local/log`或 `/var/local/audit/export/`

要了解更多信息，请参阅 "选择审核信息目标"。

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 >
/var/local/tmp/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 /var/local/tmp/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):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

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。

a. 找到与此LDR节点ID关联的存储节点。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服务的节点ID位于节点信息表中。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。

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. 输入中列出的密码 `Passwords.txt` 文件

iii. 输入以下命令切换到root： `su -`

iv. 输入中列出的密码 `Passwords.txt` 文件

以root用户身份登录后、提示符将从变为 `$` to `#`。

b. 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'
```

在命令中、始终将对象文件路径用单引号引起来以转义任何特殊字符。

- 如果未找到对象路径、则对象将丢失、无法使用此操作步骤 还原。请联系技术支持。
- 如果找到对象路径、请继续执行下一步。您可以尝试将找到的对象还原回 StorageGRID 。

3. 如果找到对象路径、请尝试将此对象还原到StorageGRID ：

a. 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-user:bycast 'file_path_of_object'`

b. 使用SSH登录到任何存储节点。然后输入"telnet 0 1402"访问LDR控制台。

c. 输入 … `cd /proc/STOR`

d. 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 `Object\_Found` 命令将向网格通知对象的位置。它还会触发活动ILM策略、这些策略会根据每个策略中的指定创建额外的副本。

> 如果找到对象的存储节点处于脱机状态、您可以将对象复制到任何处于联机状态的存储节点。将对象放置在联机存储节点的任何 /var/local/rangedb 目录中。然后、问题描述 `Object\_Found` 命令。

- 如果无法还原对象、则 `Object\_Found` 命令失败。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'
```

继续下一步。

4. 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 UUID_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"
```

```
            }
        ]
}
```

a. 从 LDR 控制台注销。输入 ... `exit`

5. 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。

a. 登录到网格节点：

i. 输入以下命令： `ssh admin@grid_node_IP`

ii. 输入中列出的密码 `Passwords.txt` 文件

iii. 输入以下命令切换到root： `su -`

iv. 输入中列出的密码 `Passwords.txt` 文件
以root用户身份登录后、提示符将从变为 `$` to `#`。

b. 更改为审核日志所在的目录。请参阅 子步骤1. b.。

c. 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 >
/var/local/tmp/messages_about_restored_object.txt
```

d. 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 /var/local/tmp/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]]
```

a. 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。

6. "重置丢失和丢失的对象计数" 在网格管理器中。

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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

关于此任务

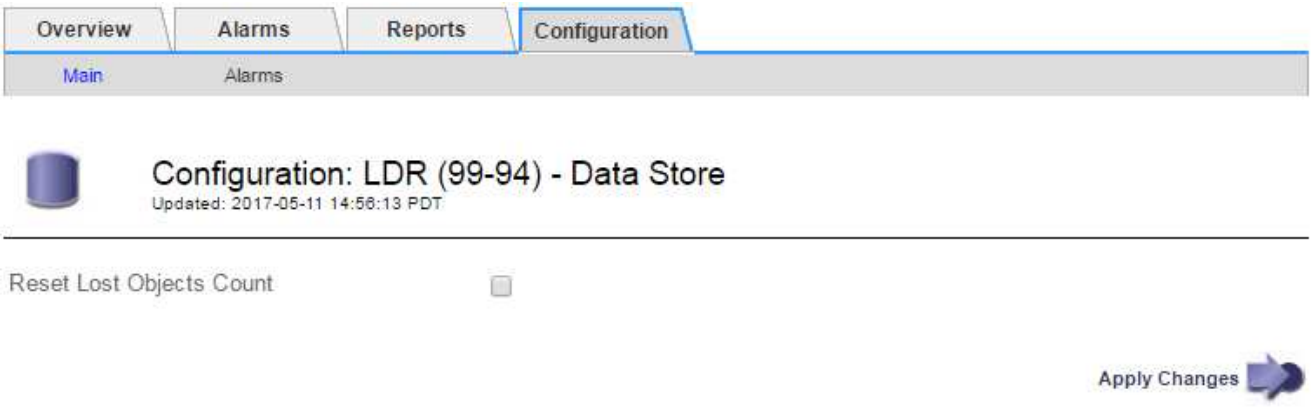
您可以从以下任一页面重置丢失的对象计数器：

- * 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. 如果您确信不需要被检查的对象，可以选择*删除被检查的对象*。

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。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

关于此任务

当存储节点上复制和经过数据线程的对象数据总量满足警报规则中配置的条件之一时，将触发“对象数据存储不足”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` 是对存储节点中已复制和已进行过彻底编码的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。

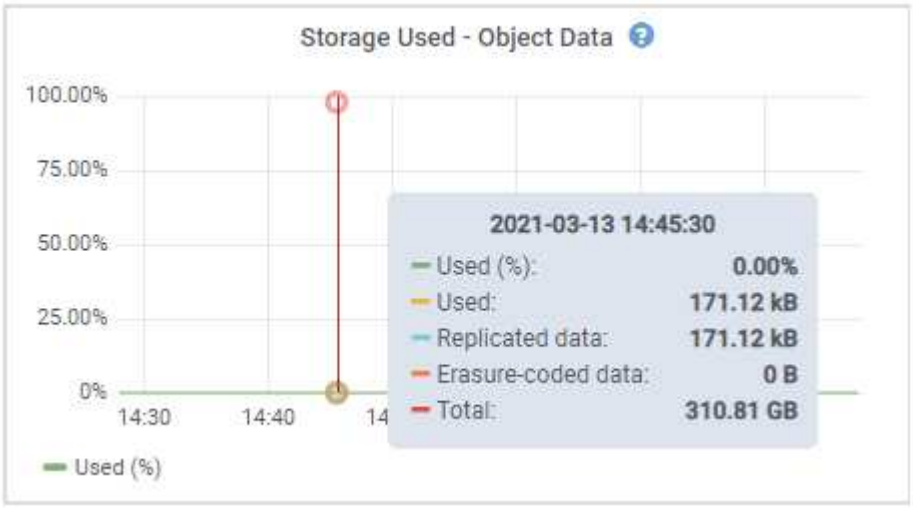
2. 如果需要，从警报表中展开 * 对象数据存储空间不足 * 警报组，然后选择要查看的警报。

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. 将光标置于"Storage Used - Object Data"(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。
     已用值为 `storagegrid_storage_utilization_data_bytes` 衡量指标。



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 "添加存储容量" 连接到网格。

   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。

有关详细信息，请参见 "管理完整存储节点"。

相关信息

"对存储状态(SSTS)警报进行故障排除(原有)"

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或更高版本时、优化的只读和读写水印会自动应用于所有存储卷、除非满足以下任一条件：

- 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。

开始之前

- 您已完成StorageGRID 11.6或更高版本的升级。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限"。

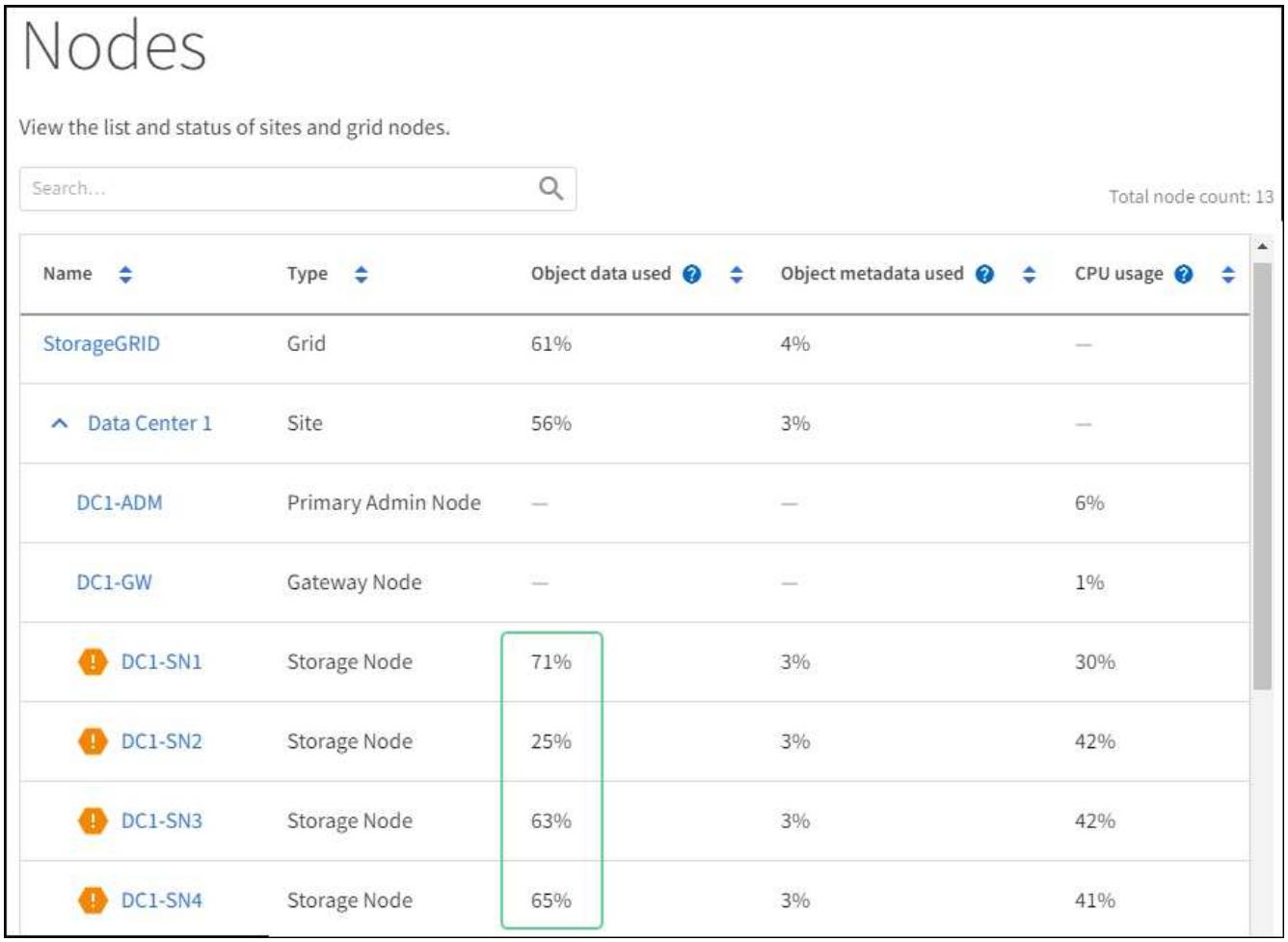
关于此任务

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

步骤

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. 按照相应步骤操作：
   a. 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。
   b. 如果ILM规则使用严格的加载行为、或者特定存储池接近全满、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。

[[view-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。

步骤

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_watermark
   ```

   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_maximum_optimized_soft_readonly_watermark
   ```

   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

步骤

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、请尽快扩展网格。两者之一 "添加存储卷" 到现有节点或 "添加新存储节点"。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）。

[[use-优化 水印**]]**使用优化水印

步骤

1. 转到*support*>*other **>***存储水印。
2. 选中*使用优化值*复选框。
3. 选择 * 保存 * 。

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。

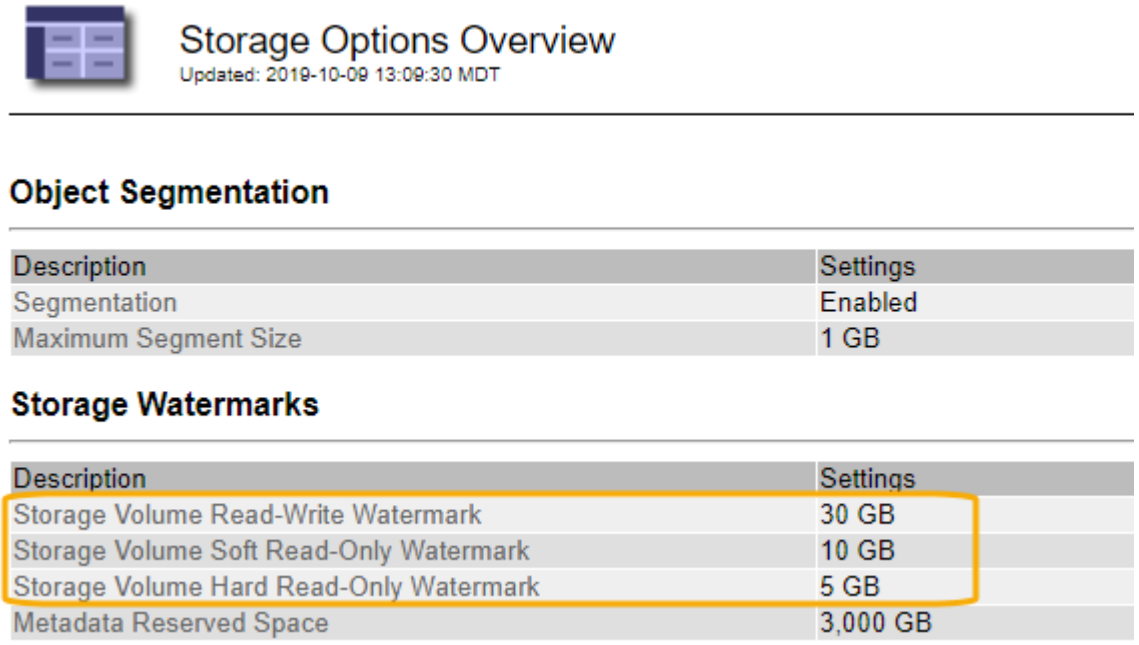
如果存储节点的对象存储剩余可用空间不足，则会触发存储状态（ SSTS ）警报。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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

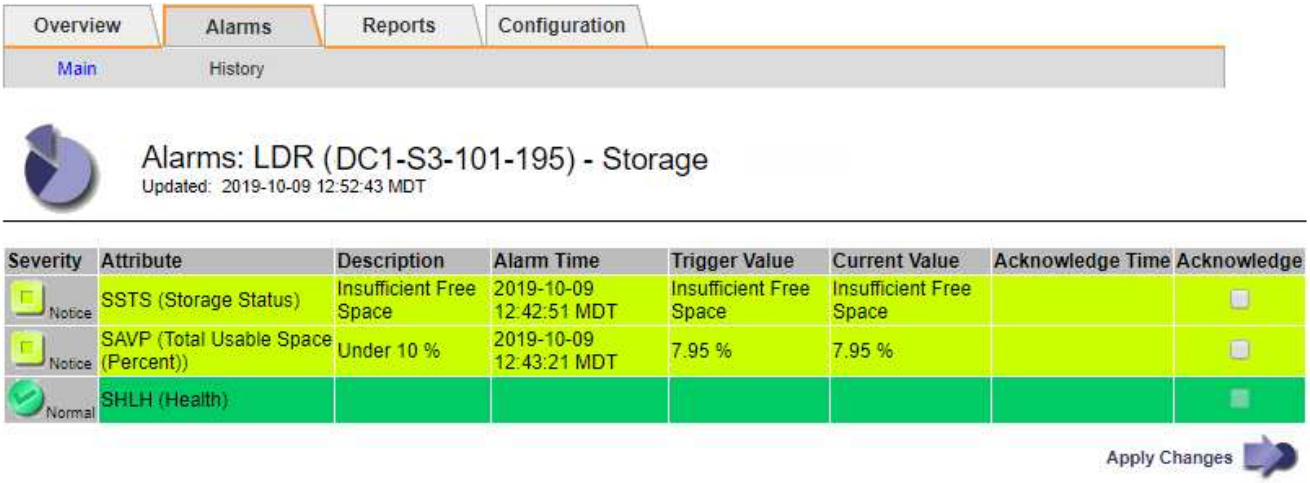
例如，假设存储卷软只读水印设置为 10 GB ，这是其默认值。如果存储节点中的每个存储卷上的可用空间不足 10 GB ，则会触发 SSTS 警报。如果任何卷具有 10 GB 或更大的可用空间，则不会触发警报。

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。

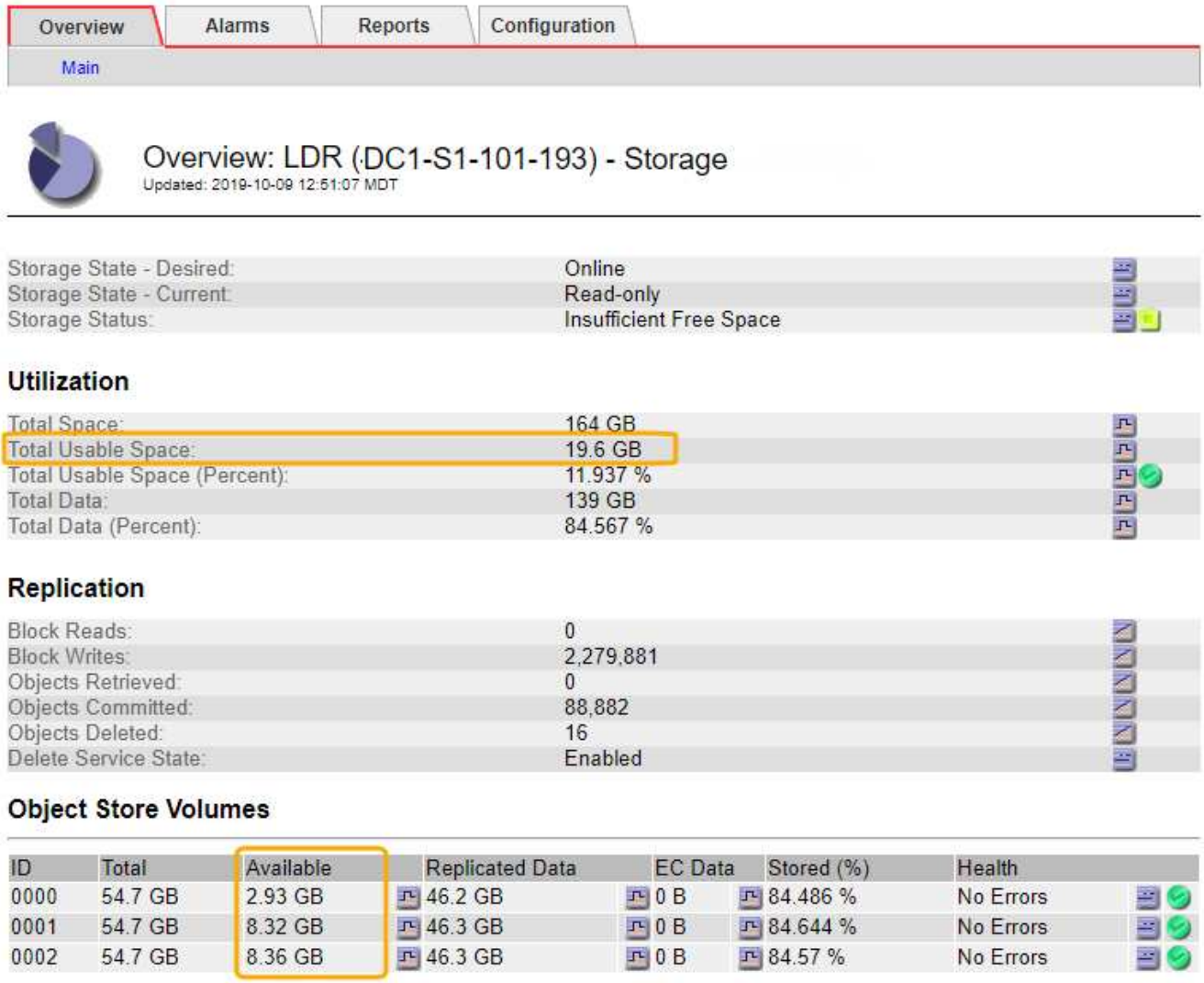
   此时将显示网格拓扑页面。警报选项卡显示选定节点和服务的活动警报。



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。

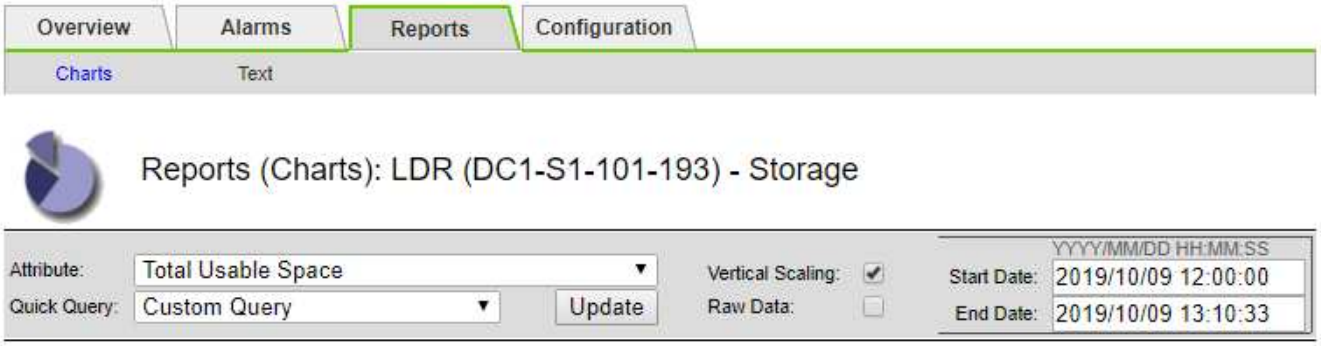
3. 要确定实际可用空间量，请选择 * LDR* > * 存储 * > * 概述 * ，然后找到总可用空间（ STAMP ）属性。

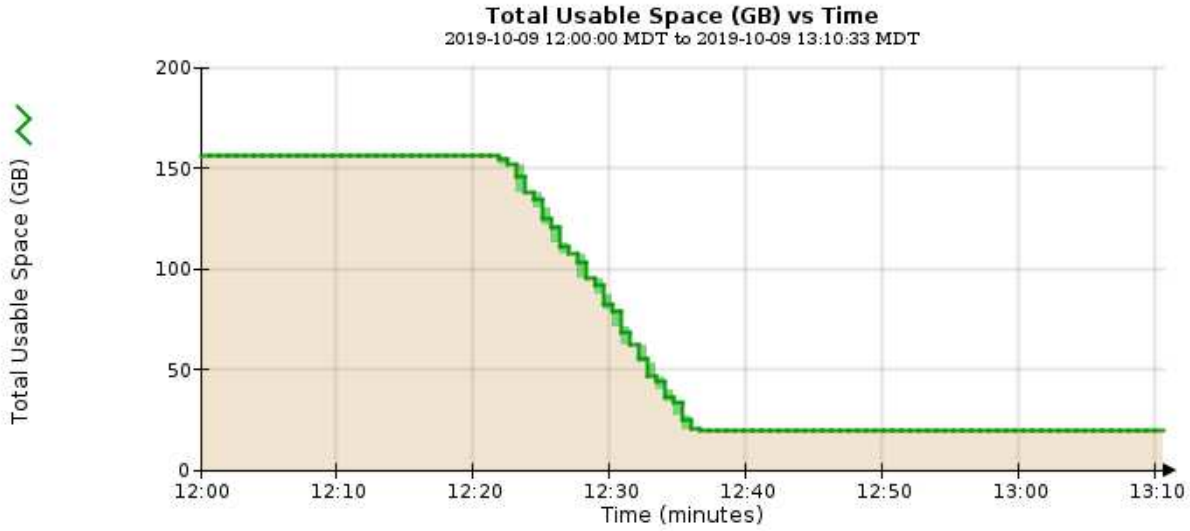


在此示例中，此存储节点上 164 GB 空间中只有 19.6 GB 可用。请注意，总计值是三个对象存储卷的 * 可用 * 值之和。之所以触发 SSTS 警报，是因为这三个存储卷中的每个卷的可用空间均小于 10 GB 。

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。

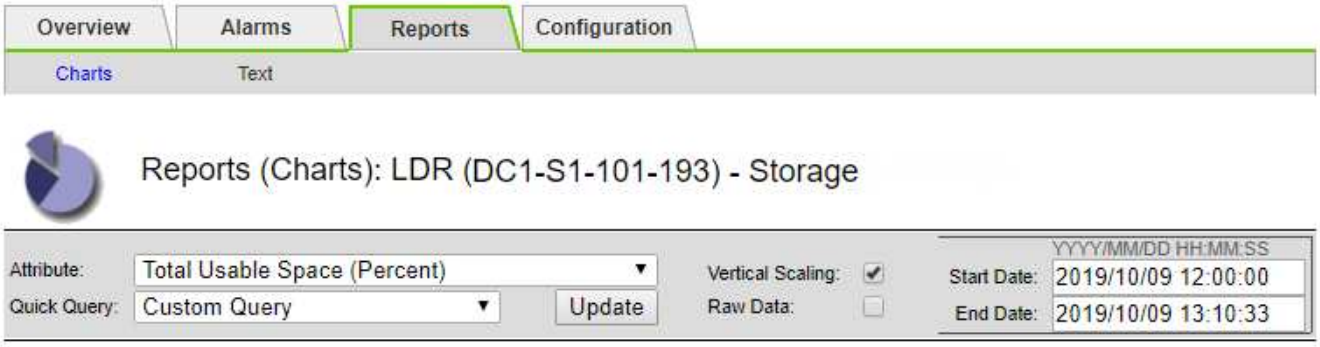
   在此示例中，总可用空间从 12： 00 处的大约 155 GB 降至 12： 35 处的 20 GB ，这与触发 SSTS 警报的时间相对应。

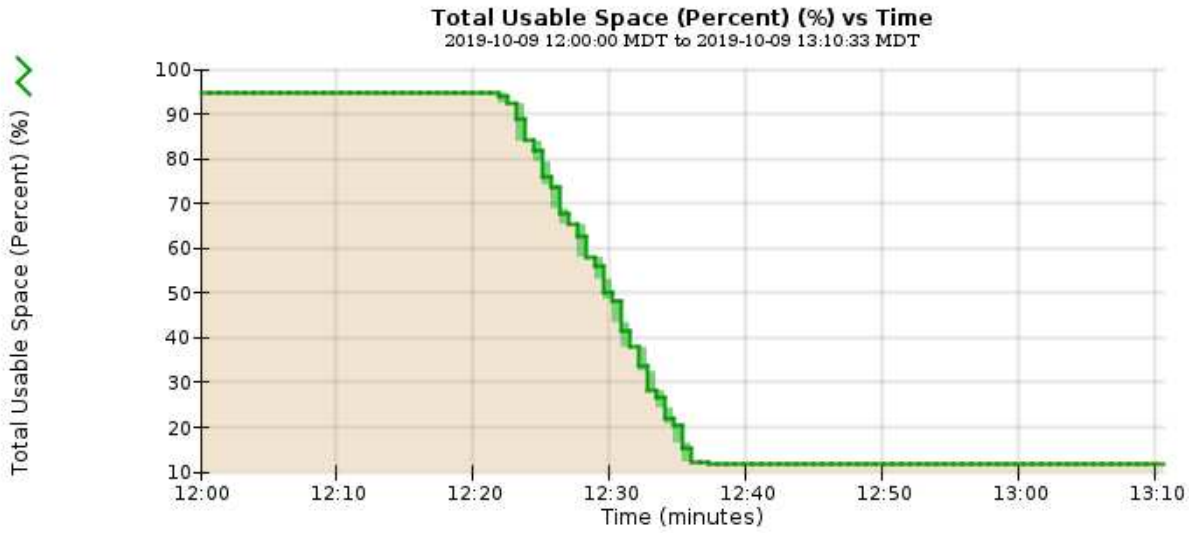




5. 要了解存储的使用情况占总空间的百分比，请绘制过去几小时的总可用空间（百分比）。

   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"。

   另请参见 "管理完整存储节点"。

对平台服务消息的传送进行故障排除（ **SMTTT** 警报）

如果平台服务消息发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(SMTT)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。

SMTTT警报包含最后一个事件消息、该消息指出： `Failed to publish notifications for bucket-name object key` 通知失败的最后一个对象。

事件消息也会在中列出 `/var/local/log/bycast-err.log` 日志文件。请参见 "日志文件参考"。

对于追加信息，请参见 "对平台服务进行故障排除"。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。

   事件消息也会在中列出 `/var/local/log/bycast-err.log`。

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。

元数据存储不足警报

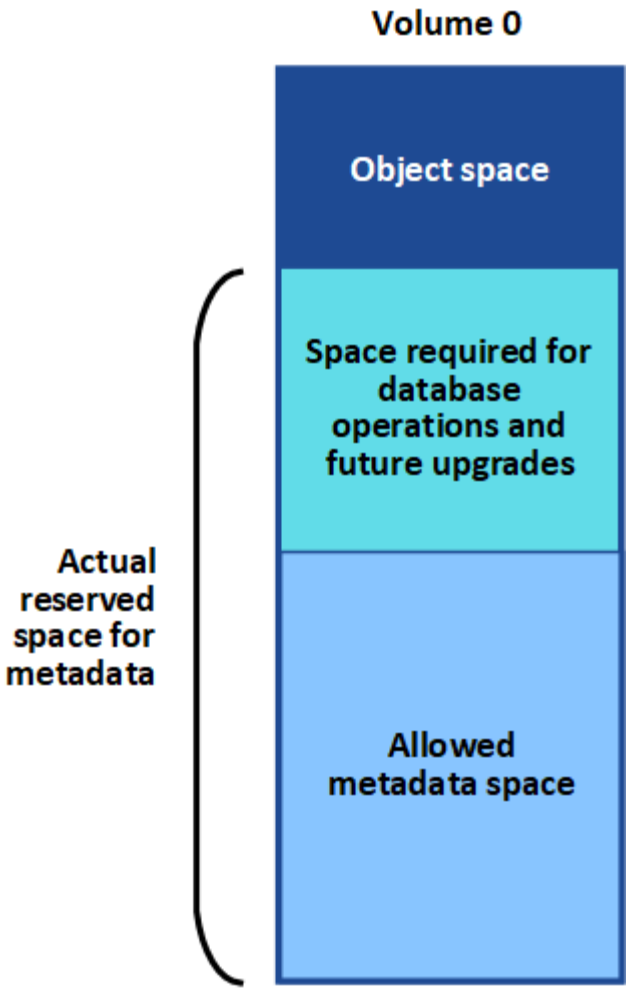
如果触发 * 低元数据存储 * 警报，则必须添加新的存储节点。

开始之前

- 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 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所允许的全部空间、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。

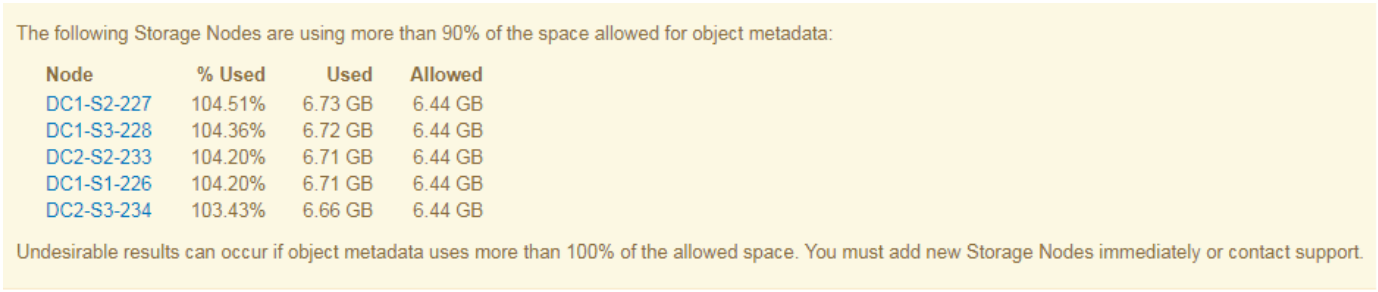
- * 次要 * ： 对象元数据正在使用允许的元数据空间的 70% 或更多。您应尽快添加新的存储节点。
- * 主要 * ： 对象元数据正在使用允许的元数据空间的 90% 或更多。您必须立即添加新的存储节点。

> 当对象元数据使用90%或更多允许的元数据空间时、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。

Services (服务**)**：状态**- Cassanda (SVST)**警报

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。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 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。

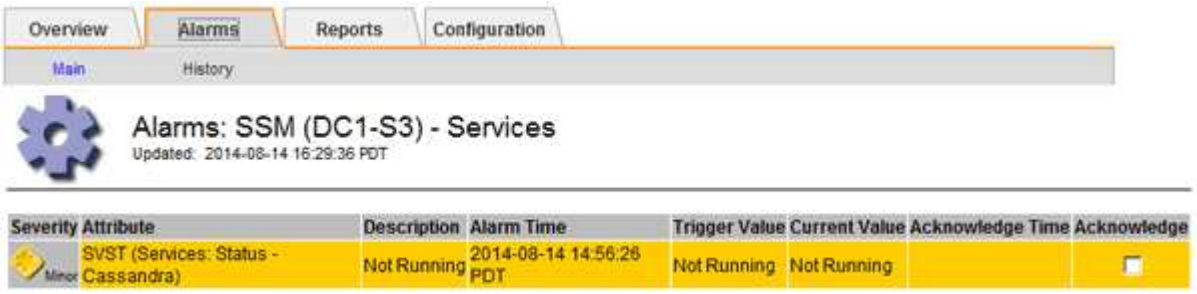
您可以 "运行诊断" 获取有关网格当前状态的追加信息。

如果两个或更多Cassandr数据库服务已关闭超过15天、请联系技术支持、并且不要继续执行以下步骤。

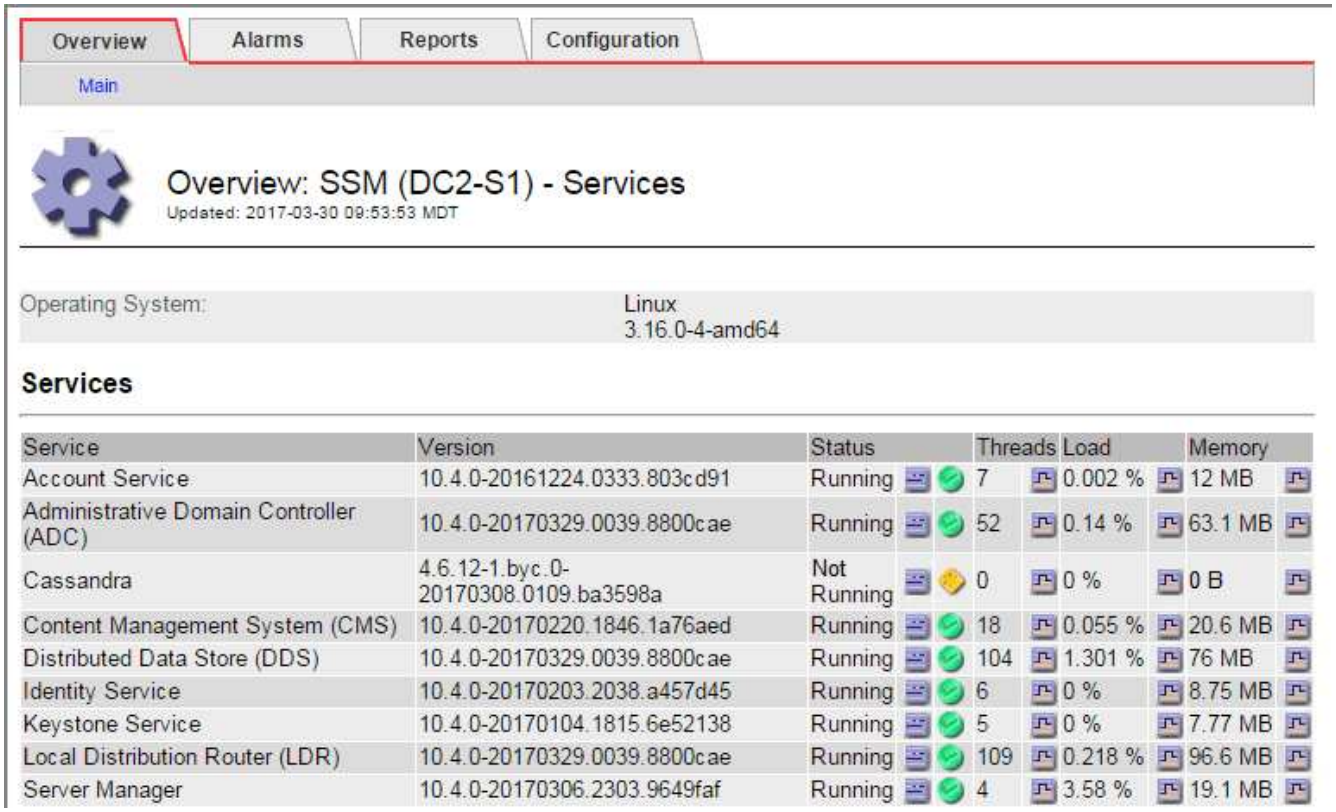
步骤

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. [[restart cassanda_from’the _Storage_Node]]尝试从存储节点重新启动Cassand拉：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入中列出的密码 `Passwords.txt` 文件
      iii. 输入以下命令切换到root： `su -`
      iv. 输入中列出的密码 `Passwords.txt` 文件
      以root用户身份登录后、提示符将从变为 `$` to `#`。
   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。

> 如果两个或多个Cassandr数据库服务已关闭、请联系技术支持、并且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 * 。

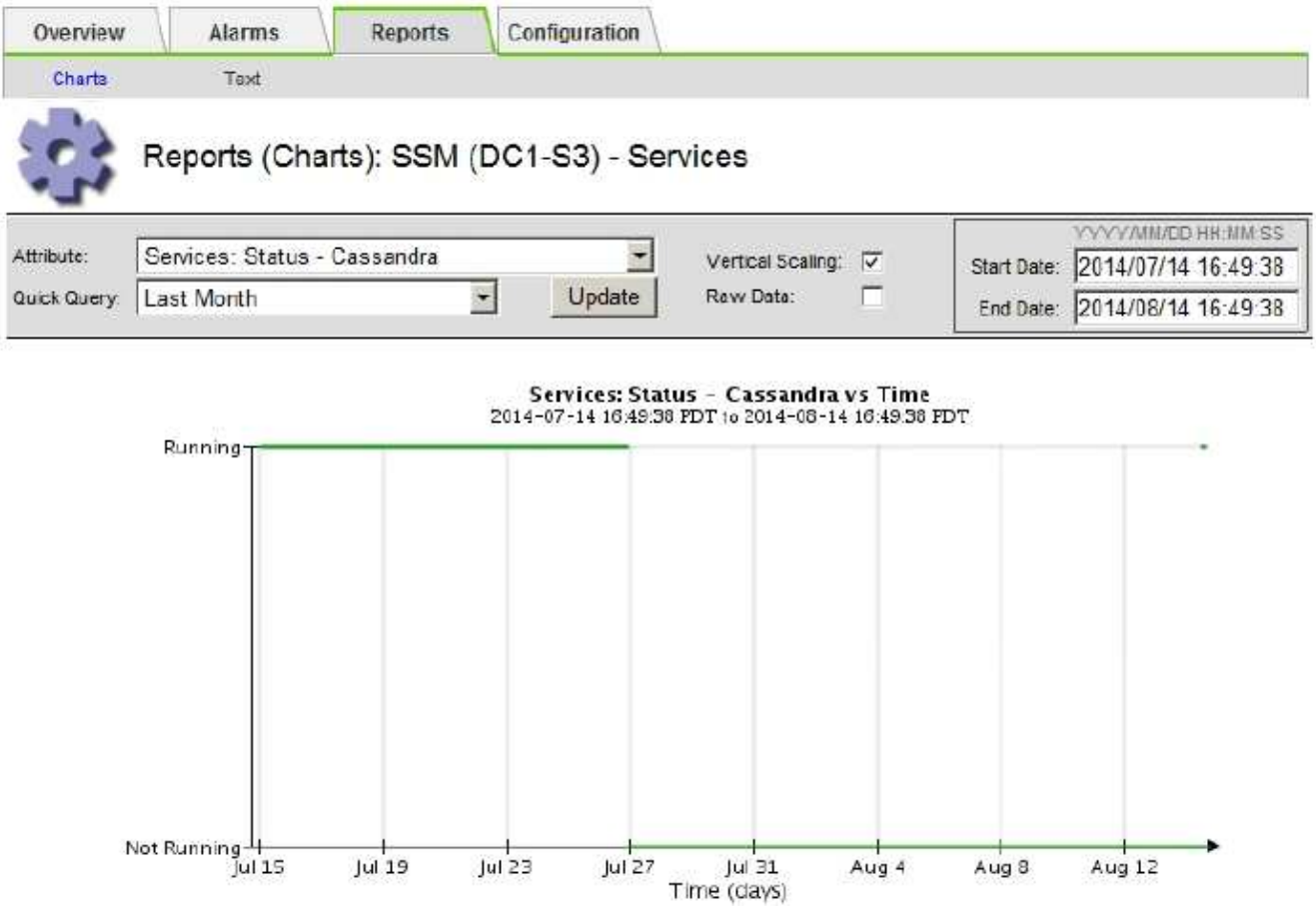
b. 选择 * 属性 * > * 服务：状态 - Cassandra* 。

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。



6. 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. 输入中列出的密码 `Passwords.txt` 文件

iii. 输入以下命令切换到root： `su -`

iv. 输入中列出的密码 `Passwords.txt` 文件
以root用户身份登录后、提示符将从变为 `$` to `#`。

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Cassandre构建 后警报未清除、请联系技术支持。

Cassanda内存不足错误(SMTT警报)

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. 查看活动：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 展开站点，然后选择**grid_node**。
   c. 选择 **SSM**，然后选择 事件 > 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" 获取有关网格当前状态的追加信息。
3. 使用 SSH 以“admin”身份登录选定节点，并切换到本地 root 用户。

4. 转至 `/var/local/core/`、压缩 `Cassandra.hprof` 并将其发送给技术支持。
5. 创建的备份 `Cassandra.hprof` 文件、然后将其从中删除 `/var/local/core/ directory`。

   此文件最大可达 24 GB ，因此您应将其删除以释放空间。

6. 解决问题描述 后，选中“Cassand拉 堆内存不足错误”计数的*Reset*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。

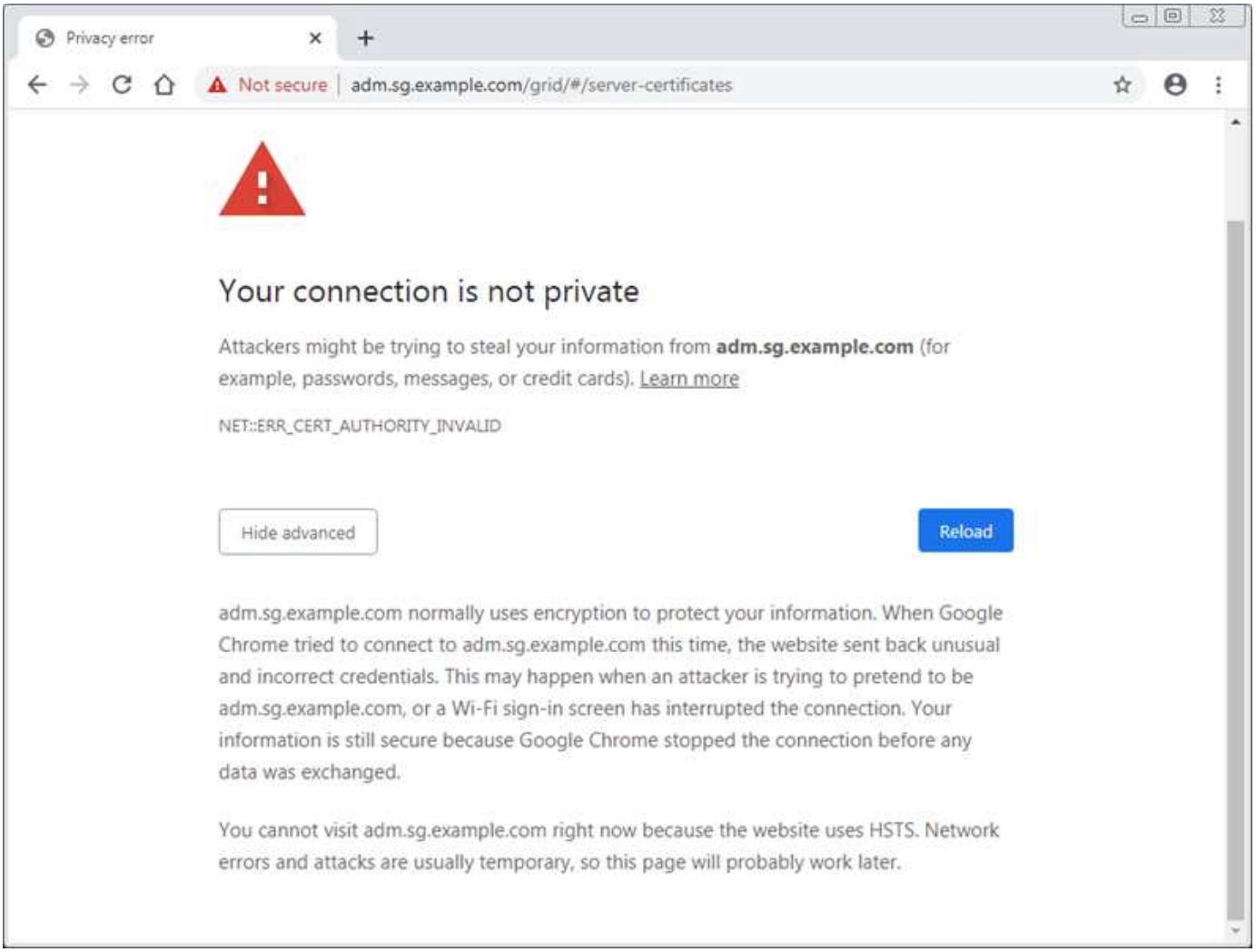
关于此任务

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，当服务器证书即将到期时，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浏览器和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。

登录错误

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具有的问题描述 "身份联合配置"、A "网络连接" 或 "硬件" 问题、使用的问题描述 "管理节点服务"或 "使用Cassand拉 数据库的问题描述" 已连接存储节点上。

开始之前

- 您拥有 `Passwords.txt` 文件
- 您已拥有 "特定访问权限"。

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：

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

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 。
   - 如果您只有一个管理节点或仍无法登录、请转到下一步。
3. 确定节点的硬件是否脱机。
4. 如果您的StorageGRID 系统启用了单点登录(SSO)、请参阅的步骤 "配置单点登录"。

   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. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。

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Ngins-GW服务正在运行 `# service nginx-gw status`
9. [[use_Lumberjack_to _col收集_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/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

- `**/*commands.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. 输入中列出的密码 `Passwords.txt` 文件
    c. 输入以下命令切换到root： `su -`
    d. 输入中列出的密码 `Passwords.txt` 文件

    以root用户身份登录后、提示符将从变为 `$` to `#`。

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"。

用户界面问题

升级StorageGRID 软件后、网格管理器或租户管理器的用户界面可能无法按预期响应。

步骤

1. 确保您使用的是 "支持的 Web 浏览器"。

   浏览器支持可能会随每个StorageGRID 版本的不同而有所不同。确认您使用的浏览器受您的StorageGRID 版本支持。

2. 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。

管理节点不可用

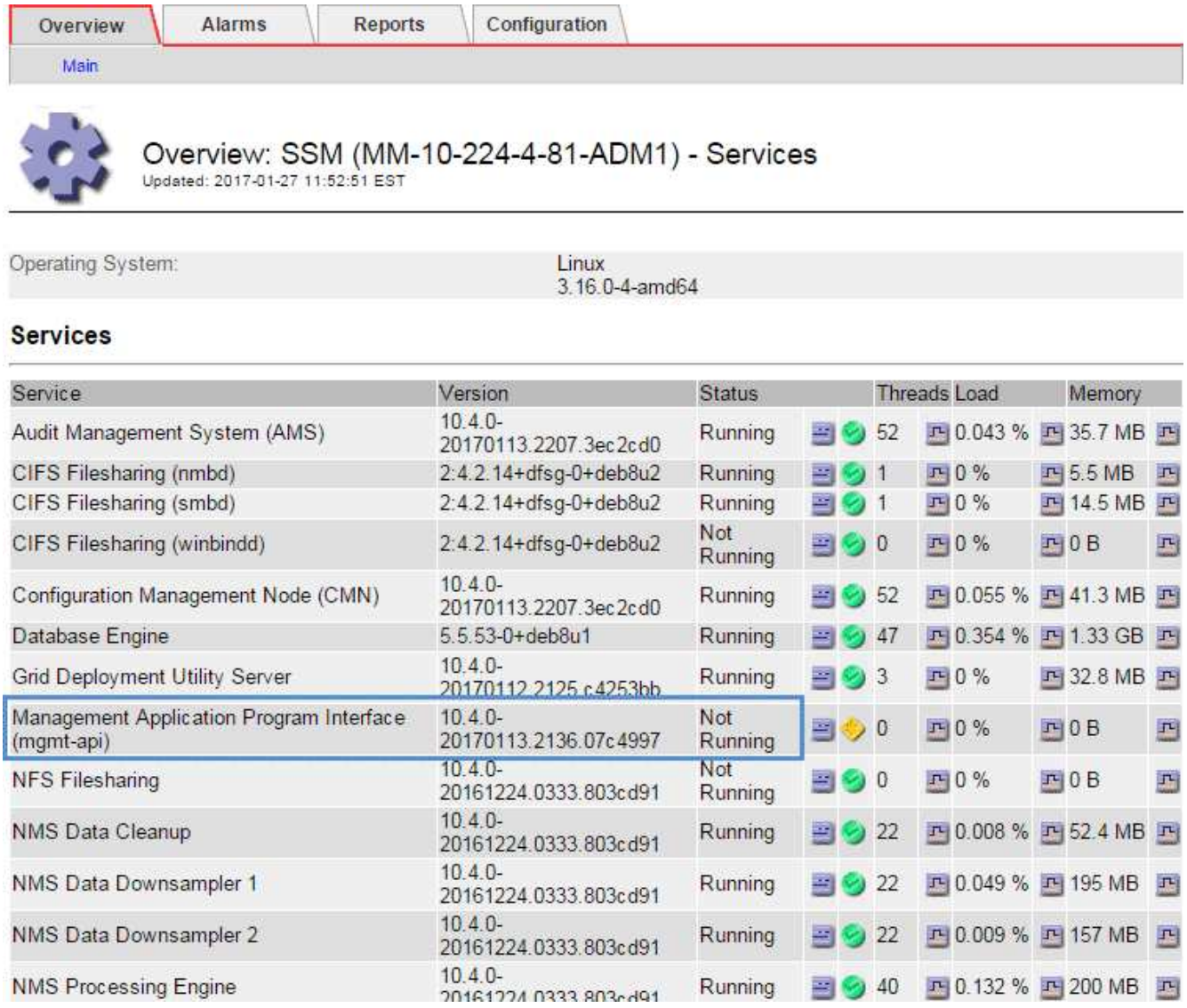
如果 StorageGRID 系统包含多个管理节点，则可以使用另一个管理节点检查不可用管理节点的状态。

开始之前

您已拥有 "特定访问权限"。

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 。

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。

"422：Unprocessable Entry"(422：无法处理的实体)错误

错误422：Unprocessable实体可能会因不同原因而出现。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。系统必须使用其中一个 "StorageGRID 支持的加密方法" 对于传出TLS连接、如管理StorageGRID 的说明中所示。

[[INROTY_MTU/警报]]网格网络MTU不匹配警报

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 *primary Admin Node IP address*`/metrics/graph` 并输入以下查询：
     `node_network_mtu_bytes{device="eth0"}`
2. "修改MTU设置" 根据需要确保所有节点上的网格网络接口(eth0)的设置相同。
   - 对于基于Linux和VMware的节点、请使用以下命令： `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`
     - 示例 * ： `change-ip.py -n node 1500 grid admin`

       注意：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` 用于更改容器中网络的MTU值的脚本。

   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。
`network`	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, - help`	显示帮助消息并退出。
`-n node, --node node`	节点。默认值为本地节点。

网络接收错误**(NRegR)**警报

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。如果错误未清除、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。
2. 根据错误的发生原因 执行以下步骤：

FEC不匹配

这些步骤仅适用于因StorageGRID 设备上的FEC不匹配而导致的NERR错误。

a. 检查连接到 StorageGRID 设备的交换机中端口的 FEC 状态。

b. 检查从设备到交换机的缆线的物理完整性。

c. 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“链接配置”页面上将设备配置为*Auto*模式(请参阅设备说明：

- "SG6160"
- "GF6112"
- "SG6000"
- "SGs了"
- "SG5700"
- "SG110和SG1100"
- "SG100和SG1000"

d. 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。

您无法在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FEC设置、网络将回退到"无FEC"模式。如果未启用FEC、则连接更容易受到电噪声引起的错误的影响。

StorageGRID 设备支持光纤编码(FC)和Reed Solomon (RS) FEC、但不支持FEC。

交换机端口和 **NIC MTU** 不匹配

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值都必须相同。请参见 对网格网络 MTU 不匹配警报进行故障排除 有关详细信息 …

另请参见 "更改 MTU 设置"。

链路错误率较高

a. 启用 FEC （如果尚未启用）。

b. 确认网络布线质量良好，并且未损坏或连接不正确。

c. 如果缆线没有问题、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。

NIC 环缓冲区溢出

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。

3. 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

"警报参考（旧系统）"

时间同步错误

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。

时间 "指定外部NTP源" 对于生产级StorageGRID 安装、请勿在早于Windows Server 2016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。

Linux： 网络连接问题

您可能会发现Linux主机上托管的StorageGRID节点的网络连接出现问题。

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、请参见的说明 "Red Hat Enterprise Linux" 或 "Ubuntu 或 Debian"。

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、请参见的说明 "Red Hat Enterprise Linux" 或 "Ubuntu 或 Debian"。

混杂模式

如果您不想使用MAC地址克隆、而是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、

确保将虚拟交换机和端口组级别的安全属性设置为*接受*(用于Pro味 式、MAC地址更改和伪传输)。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。

有关使用Pro味 噌模式的详细信息、请参见的说明 "Red Hat Enterprise Linux" 或 "Ubuntu 或 Debian"。

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. 尝试运行以下命令重新启动节点： `$ 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`

   适用于 `seconds`下、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进行更改 `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/storagegrid/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

下表介绍了可能与外部系统日志服务器相关的错误消息、并列出了更正操作。

如果您在发送测试消息以验证外部系统日志服务器是否正确配置时遇到问题，则配置外部系统日志服务器向导会显示这些错误。

运行时问题可能会由"外部系统日志服务器转发错误"警报。如果您收到此警报，请按照警报中的说明重新发送测试消息，以便您可以获得详细的错误消息。

有关将审核信息发送到外部系统日志服务器的详细信息、请参见：

- "使用外部系统日志服务器的注意事项"
- "配置审核消息和外部系统日志服务器"

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、请确保该地址是有效的IP地址、采用w.x.y.z ("点分十进制")表示法。 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。
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。确认已将这些端口配置为使用网络接口和网关(网格、管理或客户端)将流量路由到系统日志服务器、系统日志服务器将通过这些接口和网关访问。 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。

错误消息	问题描述 和建议的操作
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。 要解决此问题描述，请执行以下操作： 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. 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 。 3. 检查中间防火墙是否未配置为关闭空闲 TCP 连接。
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。

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"。

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

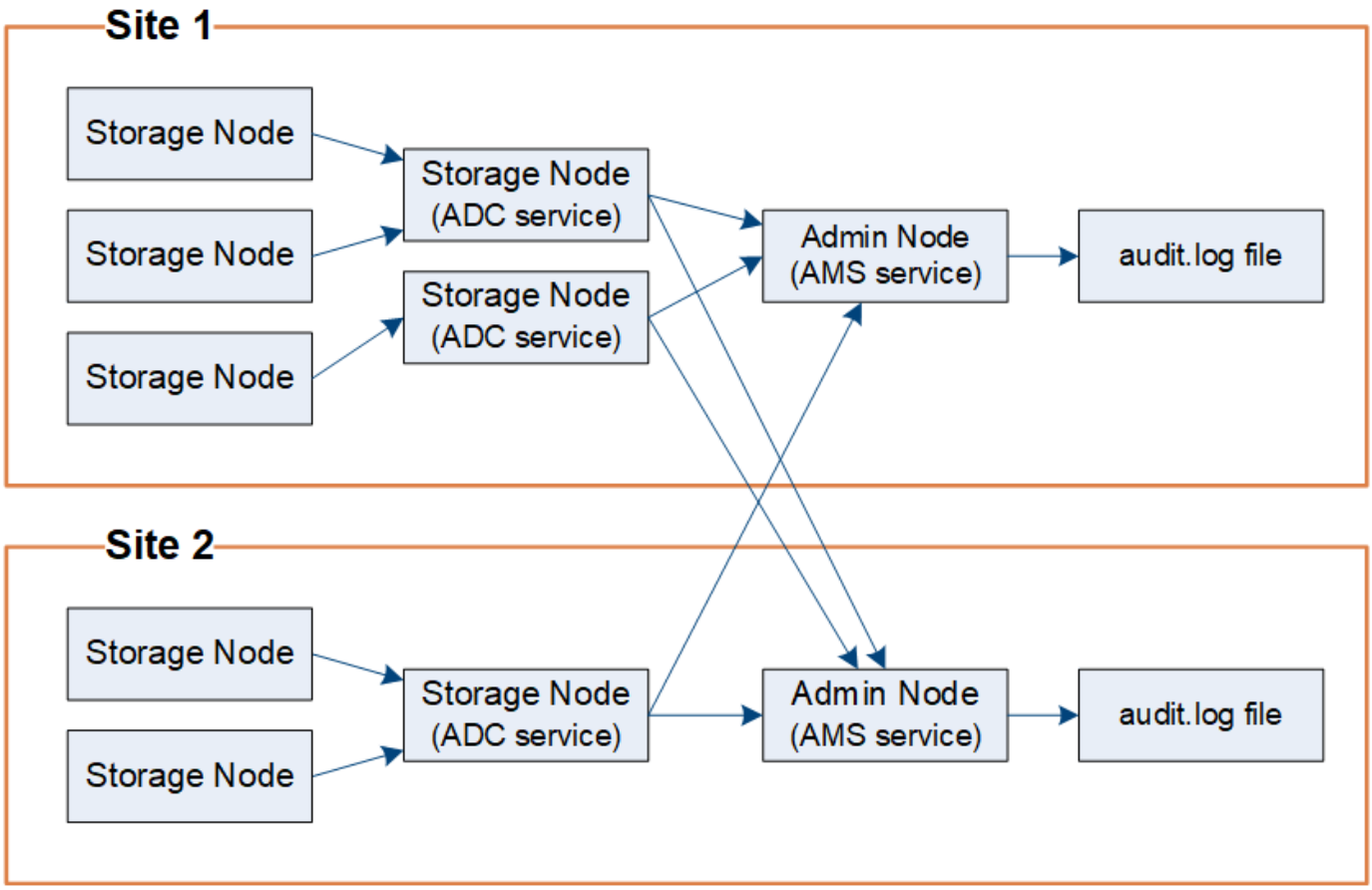
审核消息流

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。

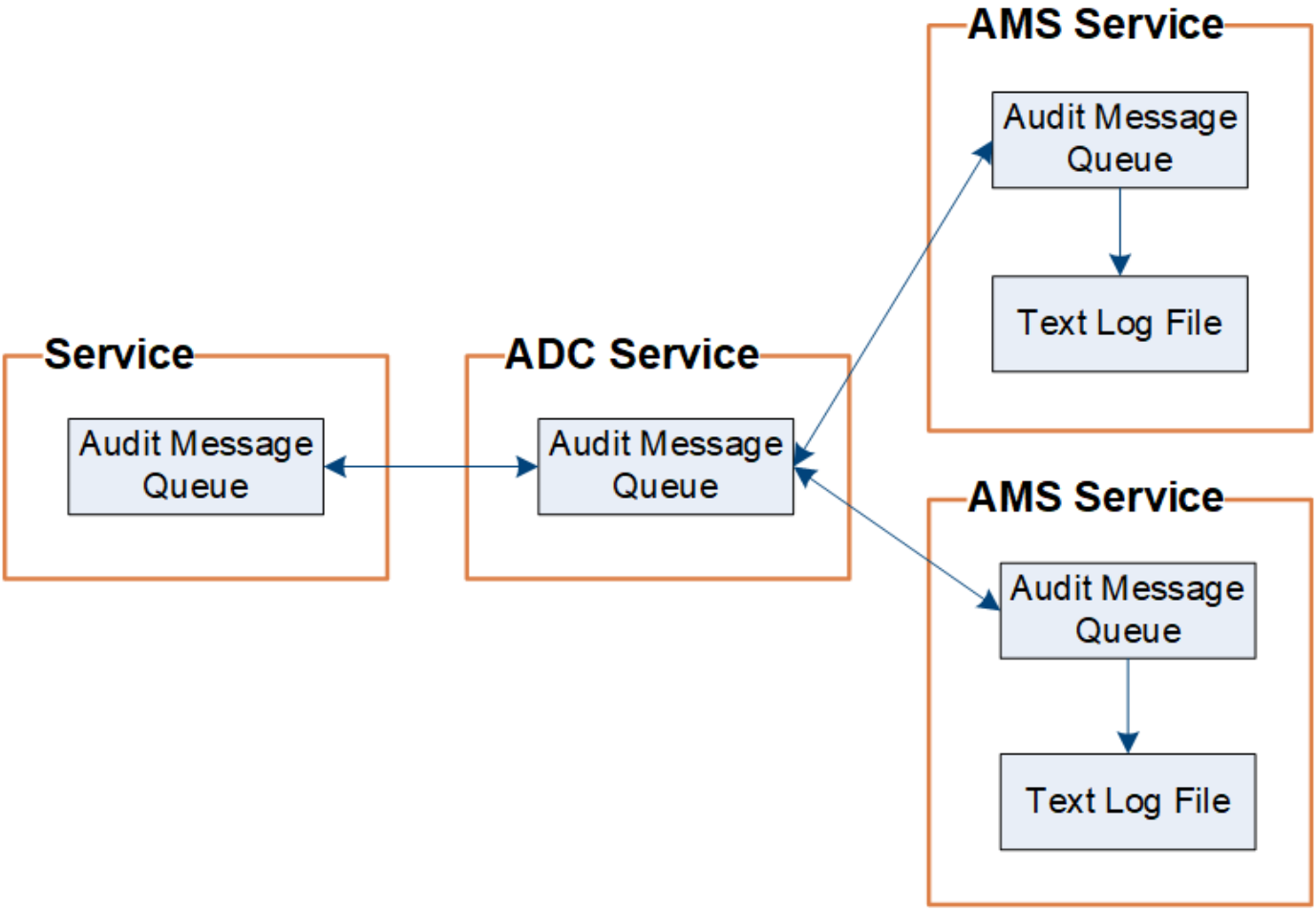
每个管理节点都会将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log`。



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。消息的副本始终保留在审核消息队列中、直到消息写入管理节点的审核日志文件为止 `/var/local/log` 目录。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中更多的可用空间 `/var/local/` 目录。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 `/var/local/log` 管理节点使用的目录已满、管理节点将标记为不可用于新审核消息、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 `/var/local/` 具有此ADA服务的存储节点使用的目录已满92%、此节点将被标记为不可用于审核消息、直到目录已满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。

> 如果没有具有ADC服务的可用存储节点、则存储节点会将审核消息存储在本地中 `/var/local/log/localaudit.log` 文件

- 如果 `/var/local/` 存储节点使用的目录已满85%、此节点将开始拒绝S3和Swift客户端请求 `503 Service Unavailable`。

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。
- 。 `/var/local/` 由于与审核消息无关的原因、一个模块存储节点上的空间已满。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 `audit.log` 文件和任何压缩的审核日志文件。您可以直接从管理节点的命令行访问审核日志文件。

开始之前

- 您已拥有 "特定访问权限"。
- 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. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。
2. 转到包含审核日志文件的目录：

   ```
   cd /var/local/log
   ```
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。

审核日志文件轮换

审核日志文件会保存到管理节点的中 `/var/local/log` 目录。活动审核日志文件名为 `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"。

每天执行一次活动 `audit.log` 此时将保存文件、并显示一个新的 `audit.log` 文件已启动。已保存文件的名称以格式指示其保存的时间 *`yyyy-mm-dd.txt`*。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。

一天之后、保存的文件将按格式进行压缩和重命名 *`yyyy-mm-dd.txt.gz`*、用于保留原始日期。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中的空间 `/var/local/log` 目录。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` file、前一天的文件 (`2018-04-15.txt`)、以及前一天的压缩文件 (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

审核日志文件格式

审核日志文件格式：概述

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.UUUUUU`、其中 *`UUUUUU`* 为微秒。

- 审核消息本身、括在方括号内、以开头 `AUDT`。

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::17530064241597054
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::17530064241597054
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):84396067221084560 22]]

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::17530064241597054
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]]
```

在默认格式下、审核日志文件中的审核消息不易阅读或解释。您可以使用 "Audy-讲解 工具" 以获取审核日志中审核消息的简化摘要。您可以使用 "audy-sum工具" 总结记录了多少写入、读取和删除操作以及这些操作所用的时间。

使用审核解释工具

您可以使用 `audit-explain` 用于将审核日志中的审核消息转换为易于阅读的格式的工具。

开始之前

- 您已拥有 "特定访问权限"。
- 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

。 `audit-explain` 主管理节点上提供的工具可在审核日志中提供审核消息的简化摘要。

> 。 `audit-explain` 此工具主要供技术支持在故障排除操作期间使用。正在处理 `audit-explain` 查询可能会占用大量CPU资源、这可能会影响StorageGRID 操作。

此示例显示了中的典型输出 `audit-explain` 工具。这四个 "SPUT" 如果帐户ID为92484777680322627870的S3租户使用S3 Put请求创建名为bucket1的分段并向该分段添加三个对象、则会生成审核消息。

```
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` 工具可执行以下操作：

- 处理普通或压缩的审核日志。例如：

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- 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/log/*
  ```

- 接受来自管道的输入、这样您可以使用筛选和预处理输入 `grep` 命令或其他方式。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、因此您可以筛选要查看和运行的部分来节省时间 `audit-explain` 而不是整个文件。

。 `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、请以命令行参数形式提供其文件名、或者使用 `zcat` 用于先解压缩文件的工具。例如：

```
zcat audit.log.gz | audit-explain
```

使用 `help (-h)` 选项以查看可用选项。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. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

   以root用户身份登录后、提示符将从变为 `$` to `#`。
2. 输入以下命令、其中 `/var/local/log/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/log/audit.log
   ```

   。 `audit-explain` 该工具可打印指定文件中所有消息的可读解释。

   为了缩短线长并提高可读性、默认情况下不会显示时间戳。如果要查看时间戳、请使用时间戳 (`-t`)选项。

使用 **audit-sum** 工具

您可以使用 `audit-sum` 用于计算写入、读取、磁头和删除审核消息的计数以及查看每种操作类型的最小、最大和平均时间(或大小)的工具。

开始之前

- 您已拥有 "特定访问权限"。
- 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

。 `audit-sum` 主管理节点上提供的工具总结了记录的写入、读取和删除操作的数量以及这些操作所需的时间。

。 `audit-sum` 此工具主要供技术支持在故障排除操作期间使用。正在处理 `audit-sum` 查询可能会占用大量CPU资源、这可能会影响StorageGRID 操作。

此示例显示了中的典型输出 `audit-sum` 工具。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"
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"

代码	Description	请参见
WWPUT	Swift PUT ： 记录成功的事务以创建新对象或容器。	"WWPUT ： Swift PUT"

。 `audit-sum` 工具可执行以下操作：

- 处理普通或压缩的审核日志。例如：

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- 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/log/*
```

- 接受来自管道的输入、这样您可以使用筛选和预处理输入 `grep` 命令或其他方式。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、请以命令行参数形式提供其文件名、或者使用 `zcat` 用于先解压缩文件的工具。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、摘要显示最小、最大和平均操作时间、但您可以使用 `size (-s)` 可选择查看对象大小。

使用 `help (-h)` 选项以查看可用选项。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. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`

d. 输入中列出的密码 `Passwords.txt` 文件

   以root用户身份登录后、提示符将从变为 `$` to `#`。

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/log/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/log/audit.log
   ```

   此示例显示了中的典型输出 `audit-sum` 工具。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消息并添加长输出选项 (`-l`)以包括对象路径：

   ```
   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. 如果要确定要在网格中输入和检索的对象大小、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使用问题描述 命令并使用group-by-time选项 (`-gt`)、后跟时间段(例如15M、1H、10S)：

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

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、请添加size选项 (`-s`)到命令：

```
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 "Audy-讲解 工具" 要查看该时段内的所有SGET操作、请执行以下操作：

```
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、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、用于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、用于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、请使用这两个 `-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
```

审核消息格式

审核消息格式：概述

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。

如果提供的摘要信息 "审核说明" 和 "审计和" 工具不足、请参见本节以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（`[ ]`）、并且字符串中的每个属性元素都具有以下特征：

- 括在方括号中 `[ ]`
- 由字符串引入 `AUDT`、表示审核消息
- 前后不带分隔符（无逗号或空格）
- 由换行符终止 `\n`

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。属性元素不会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。值始终后跟一个冒号 (`:`) 。数据类型CStr的值由双引号""括起来。

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；32位无符号整数值、表示为四个ASCII字符、例如"ABCD"。
iPad	用于 IP 地址。
CStr	长度可变的UTF-8字符数组。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。

在会议开始后 `[AUDT:` 用于标识消息本身的容器、下一组属性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 [AUDT：**\\[RSLT\(FC32\)：SUCs\]**
\\[时间\(UI64\)：11454\]\[SAIP\(iPad\)："10.224.0.100"\]\[S3AI\(CStr\)："6002562159561124649 9"\]
\[SACC\(CStr\)："account"\]\[S3AK\(CStr\)
："SGKH4_Nc8SO1H6w3w0nCOFCGk__E6dYzKlumRsKGA="\]
\\[SUSR\(CStr\)："urn：sgws：Identity：：：6002562159561124649：root"\]
\\[SBAI\(CStr\)："6002562159561124649"\\]\[SBAC\(CStr\)："account"\\]\[S3BK\(CStr\)："bket"\\]
\[S3KY\(CStr\)："object"\]\[CBID\(UI64\)：0xCC128B9B9E2283274\]
\\[UUID\(CStr\)："B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"\\[CSEZ\(UI64\)：30720\][aver (UI32)：10]
\[ATIM (UI64)：1543998285921845]\[ATYP\(FC32\)：Shea\]\[ANID (UI32)：12281045][AMID (FC32)：S3RQ]
\[Atid (UI64)：15552417629170647261]]

。 `ATYP` Element (在示例中带下划线)用于标识生成消息的事件。此示例消息包括 "Shea" 消息代码([ATYP (FC32)：Shea])、表示它是由成功的S3机头请求生成的。

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。
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。

代码	Type	Description
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。显示在中审核消息开头的可供用户读取的时间 `audit.log` file是ISO 8601格式的ATIM属性。日期和时间表示为 *`YYYY-MMDDTHH:MM:SS.UUUUUU`*、其中 `T` 是一个文字字符串、用于指示日期时间段的开始。 *`UUUUUU`* 为微秒。
ATYP	FC32	Event Type：要记录的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。

以下是可能显示在中的审核消息示例 `audit.log` 文件：

```
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、该事务会将对象的写入记录到存储分段中。

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。此值是审核消息本身的ATIM属性的可读版本：

```
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。在示例中、为值 `1405631878959669` 转换为2014年7月17日星期四21：17：59 UTC。

审核消息和对象生命周期

何时生成审核消息?

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 (铲斗)、S3KY (钥匙)或两者
链接 Swift 操作	WCON (容器)、WOBJ(对象)或两者
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。

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。

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"创建2个副本"ILM规则。

> 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]]
```

对于纠删编码对象、LOCS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DeleteObject请求时、对象删除开始。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GetObject请求时、对象检索开始。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、客户端针对存储在非其所有存储分段中的对象发送GetObject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：一条用于授权S3 Select请求(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)更新指定的元数据 (`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 "* ）。请参见 "配置审核消息和日志目标"。

```
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]]
```

审核消息

审核消息：概述

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。通过此字母列表、您可以查找有关特定消息的信息。

本章中使用的四字符代码是在审核消息中找到的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

系统审核消息

属于系统审核类别的审核消息用于与审核系统本身、网格节点状态、系统范围任务活动(网格任务)和服务备份操作相关的事件。

代码	消息标题和问题描述	请参见
ECMC	缺失经过删除编码的数据片段：表示检测到缺失经过删除编码的数据片段。	"ECMC：缺少经过Erasure编码的数据片段"
ECOC	经删除编码的数据片段已损坏：表示检测到经删除编码的数据片段已损坏。	"EECO：经过Erasure编码的数据片段已损坏"
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"
LLST	Location Lost ： 当某个位置丢失时，会生成此审核消息。	"LLST ： 位置丢失"

代码	消息标题和问题描述	请参见
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"
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"

对象存储审核消息

属于对象存储审核类别的审核消息用于与StorageGRID 系统中的对象存储和管理相关的事件。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"

代码	Description	请参见
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"
运动内衣	存储分段只读请求：存储分段已进入或退出只读模式。	"BROR：存储分段只读请求"
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"
CRR	跨网格复制请求：StorageGRID 尝试执行跨网格复制操作、以便在网格联合连接中的分段之间复制对象。	"CGRR：跨网格复制请求"
EBDL	清空存储分段删除：ILM扫描程序删除存储分段中正在删除所有对象的对象(执行空存储分段操作)。	"EBDL：清空存储分段删除"
EBKR	空分段请求：用户发送了打开或关闭空分段的请求(即删除分段对象或停止删除对象)。	"EBKR：空分段请求"
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：对象存储提交请求"
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
S3SL	S3 Select请求：在S3 Select请求返回到客户端后记录完成。S3SL消息可以包括错误消息和错误代码详细信息。此请求可能未成功。	S3 客户端	"S3SL：S3选择请求"
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和Swift客户端	"OVWR ： 对象覆盖"
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"

代码	Description	使用人	请参见
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"

ILM审核消息

属于ILM审核类别的审核消息用于与信息生命周期管理(ILM)操作相关的事件。

代码	消息标题和问题描述	请参见
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"
ORLM	满足对象规则：在按照ILM规则指定的方式存储对象数据时、将生成此审核消息。	"ORLM ： 符合对象规则"

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。

代码	字段	Description
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	数据已归档到的卷的标识符。如果未找到内容的归档位置、则返回卷ID 0。
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。
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。

代码	字段	Description
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。

代码	字段	Description
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 。

BROR：存储分段只读请求

当存储分段进入或退出只读模式时、LDR服务会生成此审核消息。例如、删除所有对象时、存储分段将进入只读模式。

代码	字段	Description
BKHD	存储分段UUID	分段标识。
BROV	存储分段只读请求值	存储分段是设置为只读状态还是保持只读状态(1 =只读、0 =非只读)。
Bros.	存储分段只读原因	将存储分段设为只读或保持只读状态的原因。例如、emptyBucket.
S3AI	S3租户帐户ID	发送请求的租户帐户的ID。空值表示匿名访问。
S3BK	S3存储分段	S3 存储分段名称。

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。
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。

代码	字段	Description
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。
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数据、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。

代码	字段	Description
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。
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。

代码	字段	Description
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。
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数据、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。

CGRR：跨网格复制请求

当StorageGRID 尝试跨网格复制操作在网格联盟连接中的分段之间复制对象时、将生成此消息。

代码	字段	Description
CSIZ	对象大小	对象的大小（以字节为单位）。 StorageGRID 11.8.因此、跨网格复制请求(从StorageGRID 11.7升级到11.8)可能具有不准确的总对象大小。
S3AI	S3租户帐户ID	拥有从中复制对象的存储分段的租户帐户的ID。
GFID	网格联合连接ID	用于跨网格复制的网格联合连接的ID。
工序	CGR操作	尝试的跨网格复制操作的类型： • 0 = Replicate对象 • 1 =重复多部分对象 • 2= Replicate delete标记
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。

代码	字段	Description
VSID	版本 ID	正在复制的对象的特定版本的版本ID。
RSLT	结果代码	返回成功(SUC)或一般错误(ERR)。

EBDL：清空存储分段删除

ILM扫描程序删除了存储分段中正在删除所有对象的对象(执行空存储分段操作)。

代码	字段	Description
CSIZ	对象大小	对象的大小（以字节为单位）。
路径	S3存储分段/密钥	S3存储分段名称和S3密钥名称。
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	StorageGRID 系统中对象的标识符。
RSLT	删除操作的结果	事件、流程或事务的结果。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。

EBKR：空分段请求

此消息指示用户发送了打开或关闭空存储分段的请求(即删除存储分段对象或停止删除对象)。

代码	字段	Description
BUID	存储分段UUID	分段标识。
EBJS	空存储分段JSON配置	包含表示当前空分段配置的JSON。
S3AI	S3租户帐户ID	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。

ECMC：缺少经过**Erasure**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。

EECO：经过**Erasure**编码的数据片段已损坏

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。
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。

代码	字段	Description
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 ）。

代码	字段	Description
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。

代码	字段	Description
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：网格任务已终止、但未发生回滚错误。 • Rolf：网格任务已终止、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。

代码	字段	Description
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）。
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 * 。当ILM开始删除对象时、会生成此消息、因为活动ILM策略中当前没有应用于对象的放置指令。

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。

代码	字段	Description
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。
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 "" 。 CEC：对于纠删编码对象、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 。对未受版本管理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

每当找不到对象副本(已复制或经过删除编码)的位置时、都会生成此消息。

代码	字段	**Description**
CBIL	CBID	受影响的 CBID 。
ECPR	纠删编码配置文件	用于经过擦除编码的对象数据。所用纠删编码配置文件的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
NOID	源节点 ID	丢失位置的节点 ID 。
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。 采用的形式 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`

代码	字段	Description
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
UUID	通用唯一 ID	StorageGRID 系统中受影响对象的标识符。

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。
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

代码	字段	Description
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	丢失对象的最后一个已知直接或近线位置(如果可用)。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）。
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 "" 。 CEC：对于纠删编码对象、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。
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 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

对于单个对象、可以多次发出ORLM审核消息。例如、每当发生以下事件之一时、都会发出此命令：

- 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。

S3SL：**S3**选择请求

此消息会在S3 Select请求返回给客户端后记录完成。S3SL消息可以包括错误消息和错误代码详细信息。此请求可能未成功。

代码	字段	Description
BYSC	已扫描字节数	从存储节点扫描(接收)的字节数。 如果对对象进行压缩、BYSC和BYPR可能会有所不同。如果对象已压缩、则BYSC将具有经过压缩的字节计数、而BYPR将是解压缩后的字节。
BYPR	已处理的字节数	已处理的字节数。指示S3 Select作业实际处理或处理了多少字节的"已扫描字节数"。
BYRT	返回的字节数	S3 Select作业返回到客户端的字节数。
重新	记录已处理	S3 Select作业从存储节点收到的记录或行数。
RERT	返回的记录	S3 Select作业返回到客户端的记录或行数。
JOFI	作业已完成	指示S3 Select作业是否已完成处理。如果此值为false、则作业无法完成、并且错误字段中可能包含数据。客户端可能已收到部分结果、或者根本没有结果。
Reid	请求 ID	S3 Select请求的标识符。
EXTM	执行时间	S3选择作业完成所需的时间(以秒为单位)。
ERMG	错误消息	S3 Select作业生成的错误消息。
很差	错误类型	S3 Select作业生成的错误类型。
错误	Stacktrace错误	S3 Select作业生成的Stacktrace出错。
S3BK	S3存储分段	S3 存储分段名称。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的S3访问密钥ID。
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 。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。

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。
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、或者删除存储分段/对象子资源。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。
GFID	网格联合连接ID	与跨网格复制删除请求关联的网格联合连接的连接ID。仅包含在目标网格的审核日志中。
GFSA	网格联合源帐户ID	源网格上用于跨网格复制删除请求的租户帐户ID。仅包含在目标网格的审核日志中。
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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。 x-amz-bypass-governance-retention 如果请求中存在、则会自动包含。
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。

代码	字段	Description
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。
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。
UUDM	删除标记的通用唯一标识符	删除标记的标识符。审核日志消息指定UUDM或UUID、其中UDM表示因对象删除请求而创建的删除标记、UUID表示对象。
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 。对未受版本管理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、或者删除存储分段/对象子资源。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	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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
。	ListObjectsV2	请求了_v2 format_响应。有关详细信息，请参见 "AWS List对象V2"。仅适用于GET分段操作。
NCHD	儿童人数	包括密钥和通用前缀。仅适用于GET分段操作。
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。

代码	字段	Description
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。
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。
常闭	已截断或未截断	如果返回所有结果、请设置为false。如果可返回更多结果、请设置为true。仅适用于GET分段操作。
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 。对未受版本管理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。

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。
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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
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 。对未受版本管理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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。 (SPOS不需要)。
RSLT	结果代码	RestorEObject请求的结果。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。

代码	字段	Description
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。
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 。对未受版本管理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、或者删除存储分段/对象子资源。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。
GFID	网格联合连接ID	与跨网格复制放置请求关联的网格联合连接的连接ID。仅包含在目标网格的审核日志中。
GFSA	网格联合源帐户ID	源网格上用于跨网格复制放置请求的租户帐户ID。仅包含在目标网格的审核日志中。
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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。 x-amz-bypass-governance-retention 如果请求中存在、则会自动包含。
LKEN	对象锁定已启用	请求标头的值 x-amz-bucket-object-lock-enabled，如果在请求中存在。
LKLH	对象锁定合法保留	请求标头的值 x-amz-object-lock-legal-hold，如果在PutObject请求中存在。
LKMD	对象锁定保留模式	请求标头的值 x-amz-object-lock-mode，如果在PutObject请求中存在。
LKRU	对象锁定保留至日期	请求标头的值 x-amz-object-lock-retain-until-date，如果在PutObject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。

代码	字段	Description
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	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。
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。

代码	字段	Description
ULID	上传 ID	仅包含在CompleteMultipartUpload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 。对未受版本管理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："已启用"或"已暂停"。 对象操作不包括此字段。

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。

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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
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。
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	已更新其元数据的对象的特定版本的版本 ID 。对未受版本管理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。

应密切监视此消息。内容验证失败可能表示即将发生硬件故障。

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。

应密切监控SVRU：对象存储验证未知审核消息。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、因为它可能表示即将发生硬件故障。

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、因为在关闭前不会清除审核消息队列。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无法指示"异常"关机、因为该消息仅由"干净"关机生成。

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"关机、因为该消息仅由"干净"关机生成。

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。

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 。容器上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）。容器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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
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。

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。容器上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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
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。

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。
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。帐户操作不包括此字段。
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。

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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
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。

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。
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。帐户操作不包括此字段。
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 。容器上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）。容器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。 `X-Forwarded-For` 如果请求中存在此参数、则会自动包含此参数 `X-Forwarded-For` 值与请求发件人IP地址(SAIP审核字段)不同。
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。
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。
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。容器上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。