监控StorageGRID 系统

StorageGRID 11.8

NetApp
May 17, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-118/monitor/index.html on May 17, 2024. Always check docs.netapp.com for the latest.

目录

监控StorageGRID 系统 1
监控StorageGRID 系统：概述 1
查看和管理信息板 1
查看节点页面 4
要定期监控的信息 34
警报和警报 62
日志文件参考 140
配置审核消息和日志目标 158
使用 SNMP 监控 170
收集其他 StorageGRID 数据 181

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：

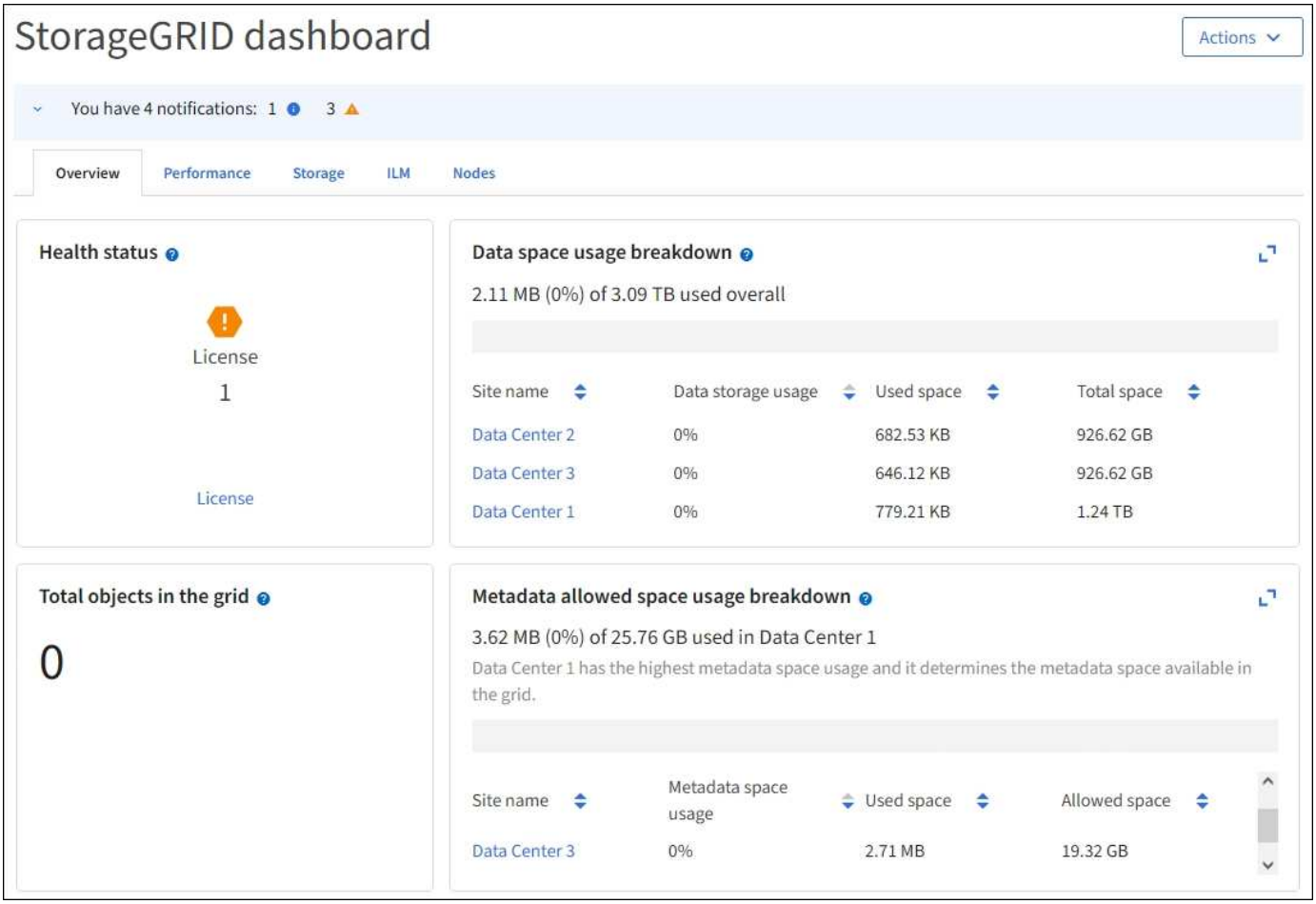
- "查看和管理信息板"
- "查看节点页面"
- "定期监控系统的以下方面："
  - "系统运行状况"
  - "存储容量"
  - "信息生命周期管理"
  - "网络和系统资源"
  - "租户活动"
  - "负载平衡操作"
  - "网格联合连接"
  - "归档容量"
- "管理警报和旧警报"
- "查看日志文件"
- "配置审核消息和日志目标"
- "使用外部系统日志服务器" 收集审核信息
- "使用SNMP进行监控"
- "获取其他StorageGRID数据"，包括度量和诊断

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。
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。

选项卡	包含
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*。

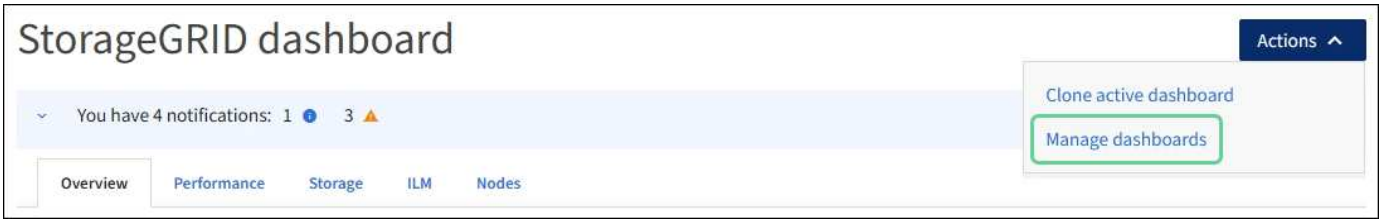
管理信息板

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 *。

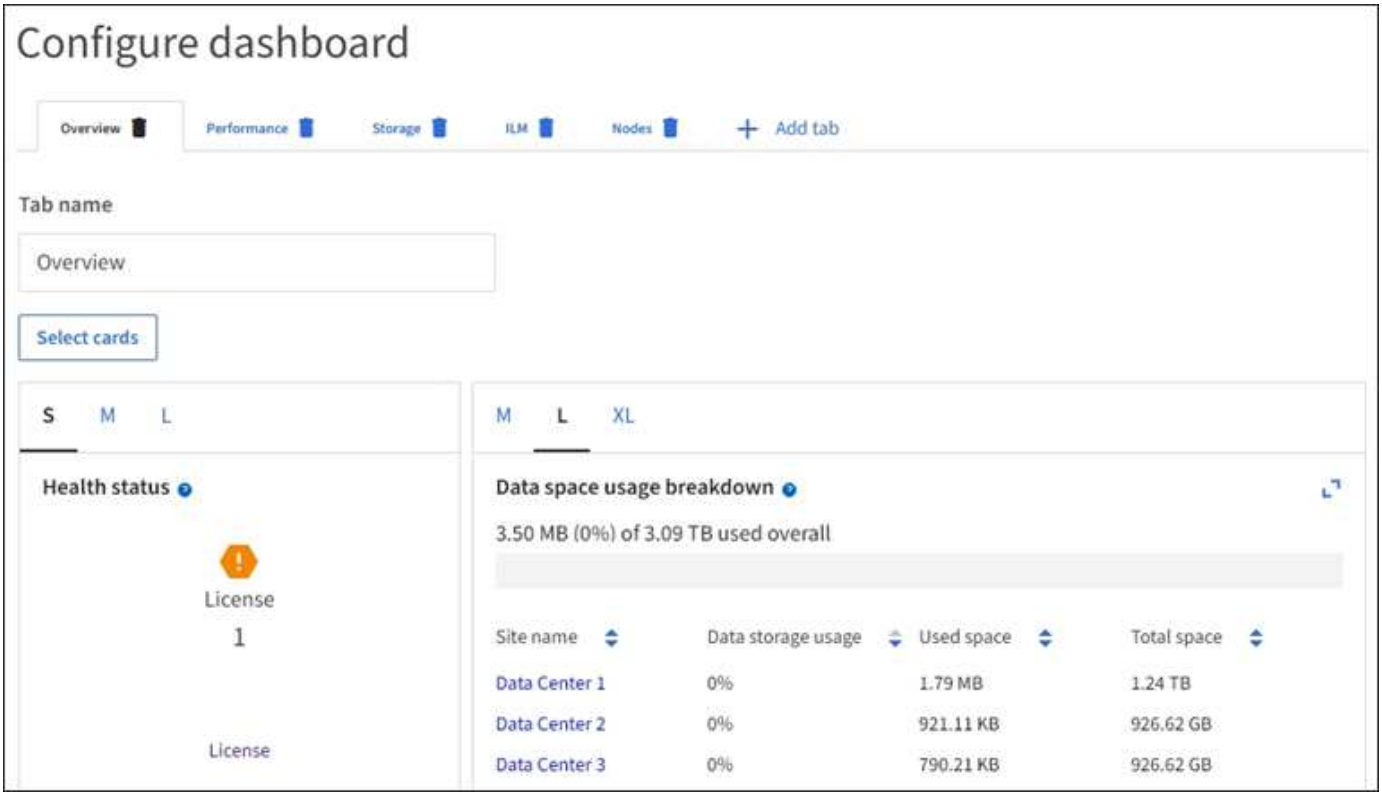
要编辑或克隆现有信息板，请选择*Actions*>*Manage Dards*。

> 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

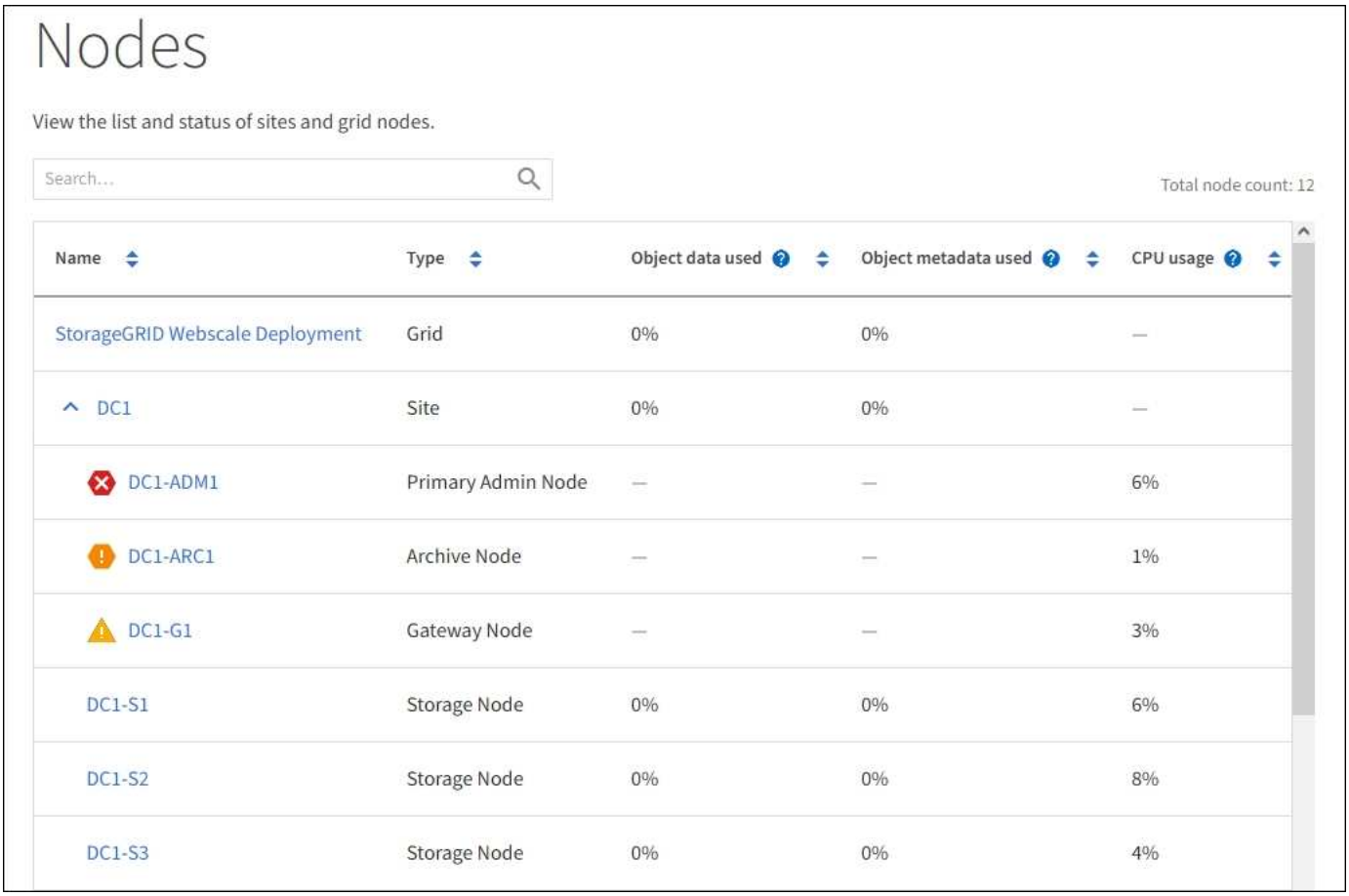
查看节点页面：**Overview**

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。

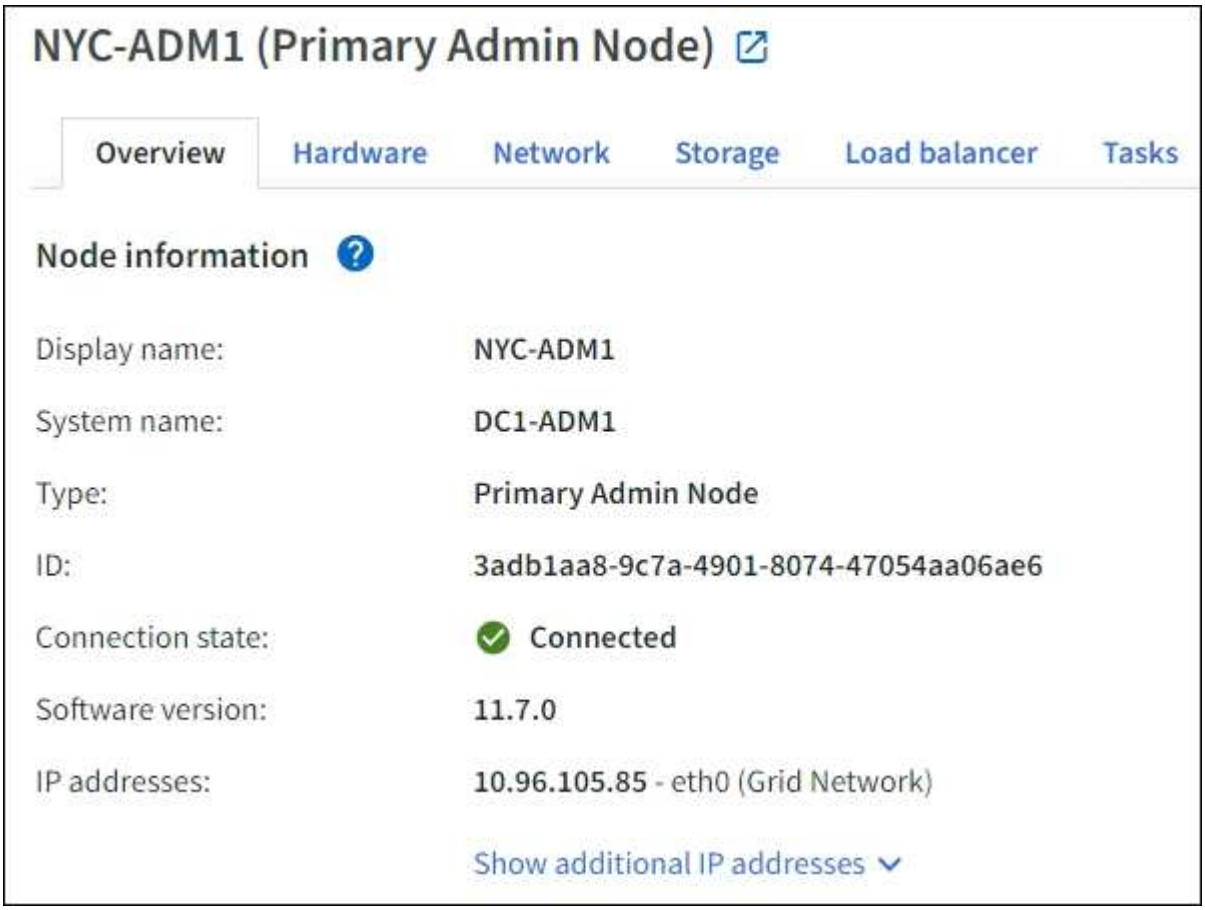
查看概述选项卡

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。

节点信息

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。

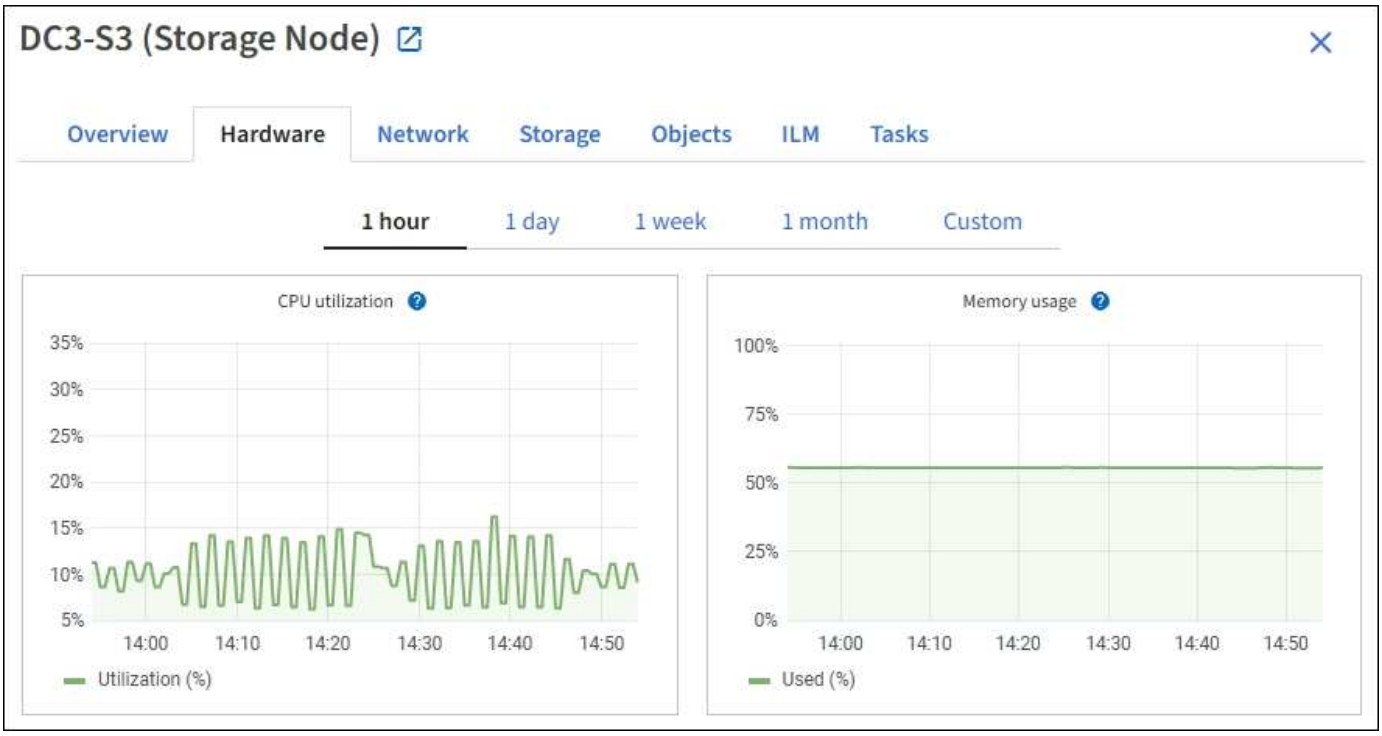
警报也包括在中 "节点连接状态"。

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。

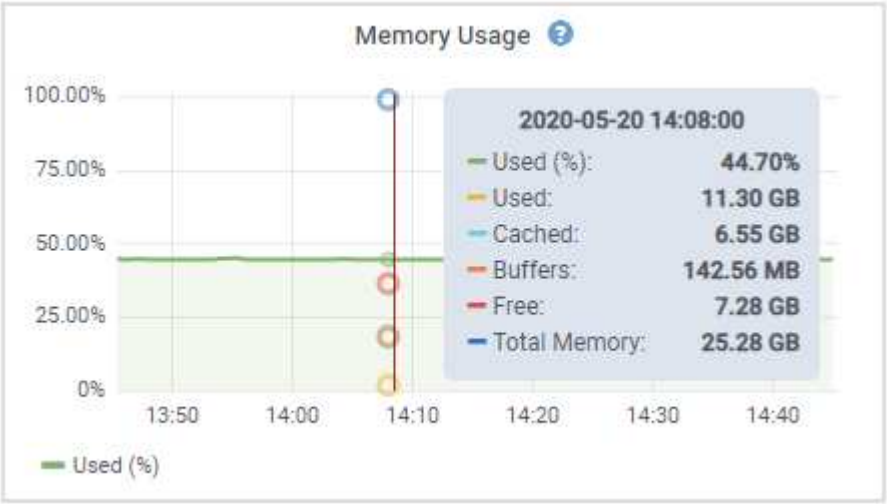
Grid Manager随每个版本更新、可能与此页面上的示例屏幕截图不匹配。

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

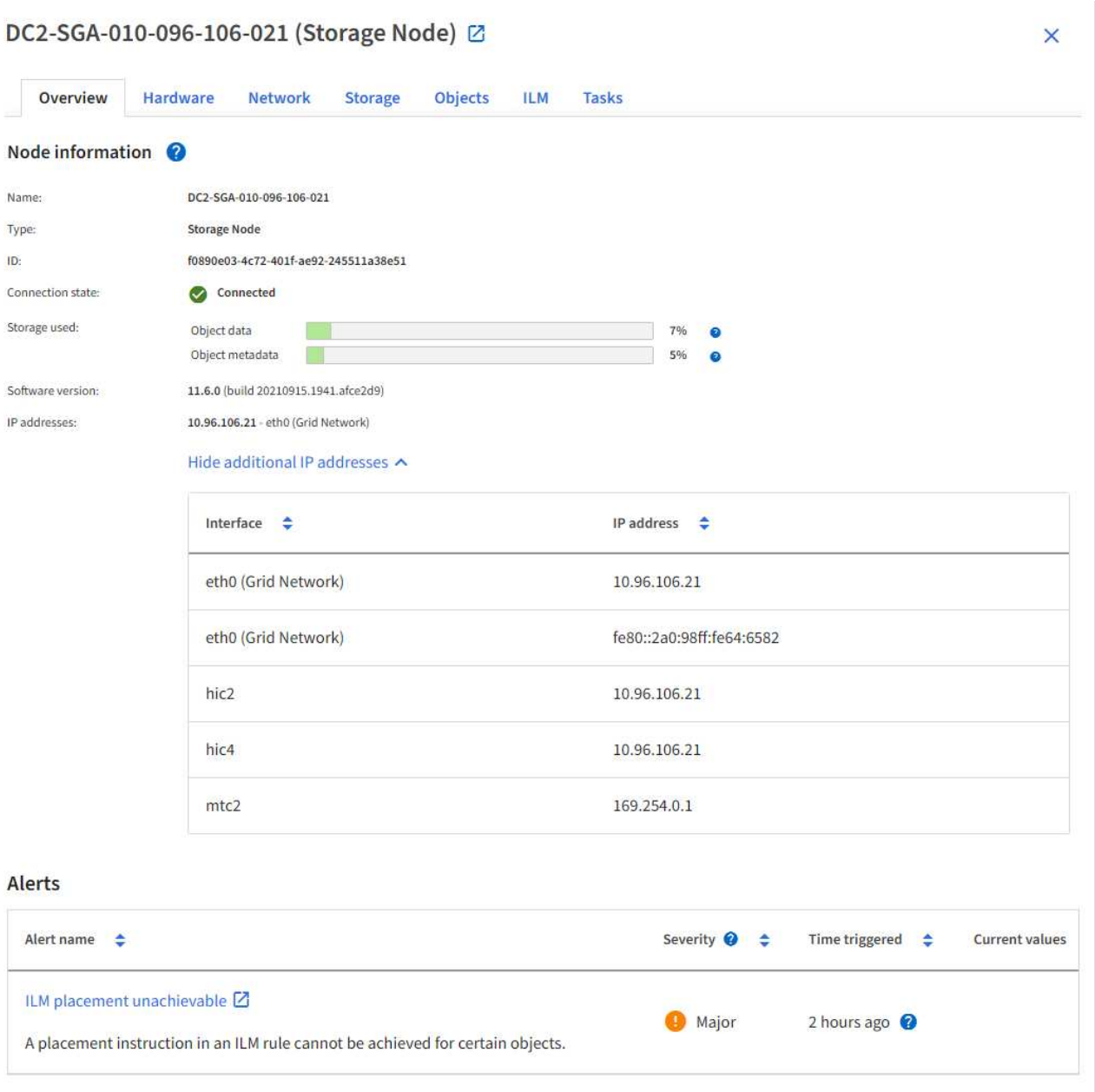
节点页面列出了有关每个设备存储节点的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，控制器固件版本，网络资源，网络接口， 网络地址以及接收和传输数据。

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。

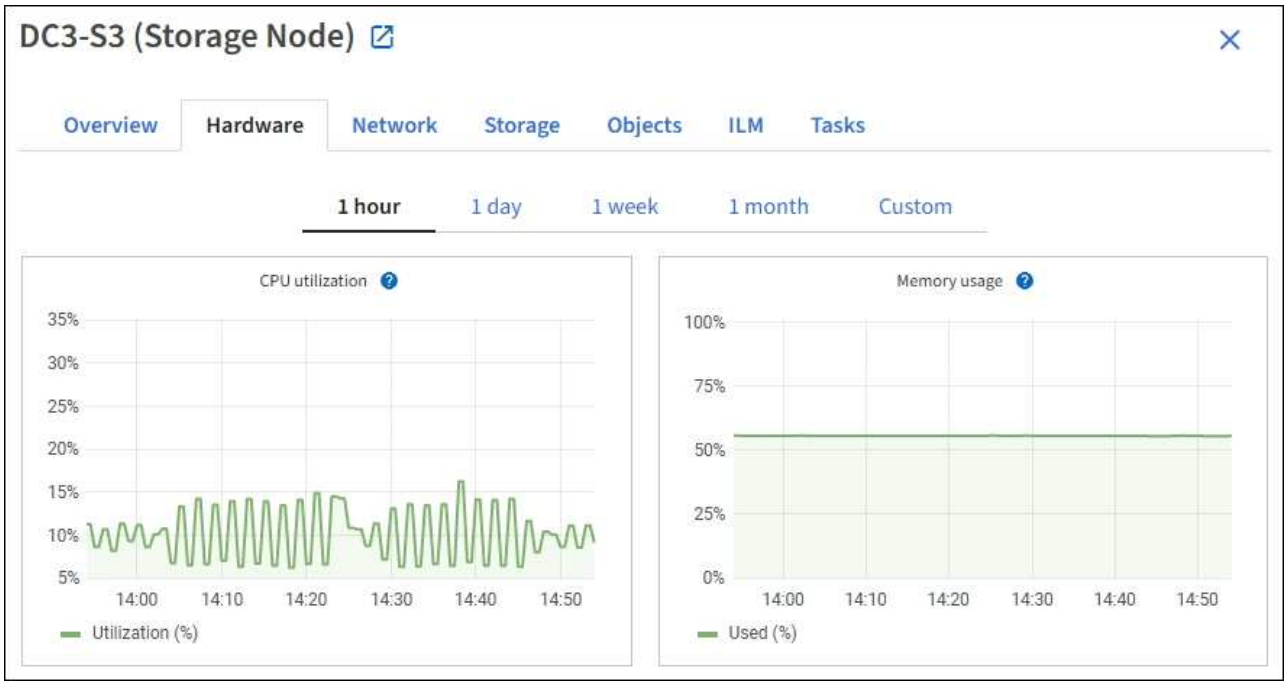


" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

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。

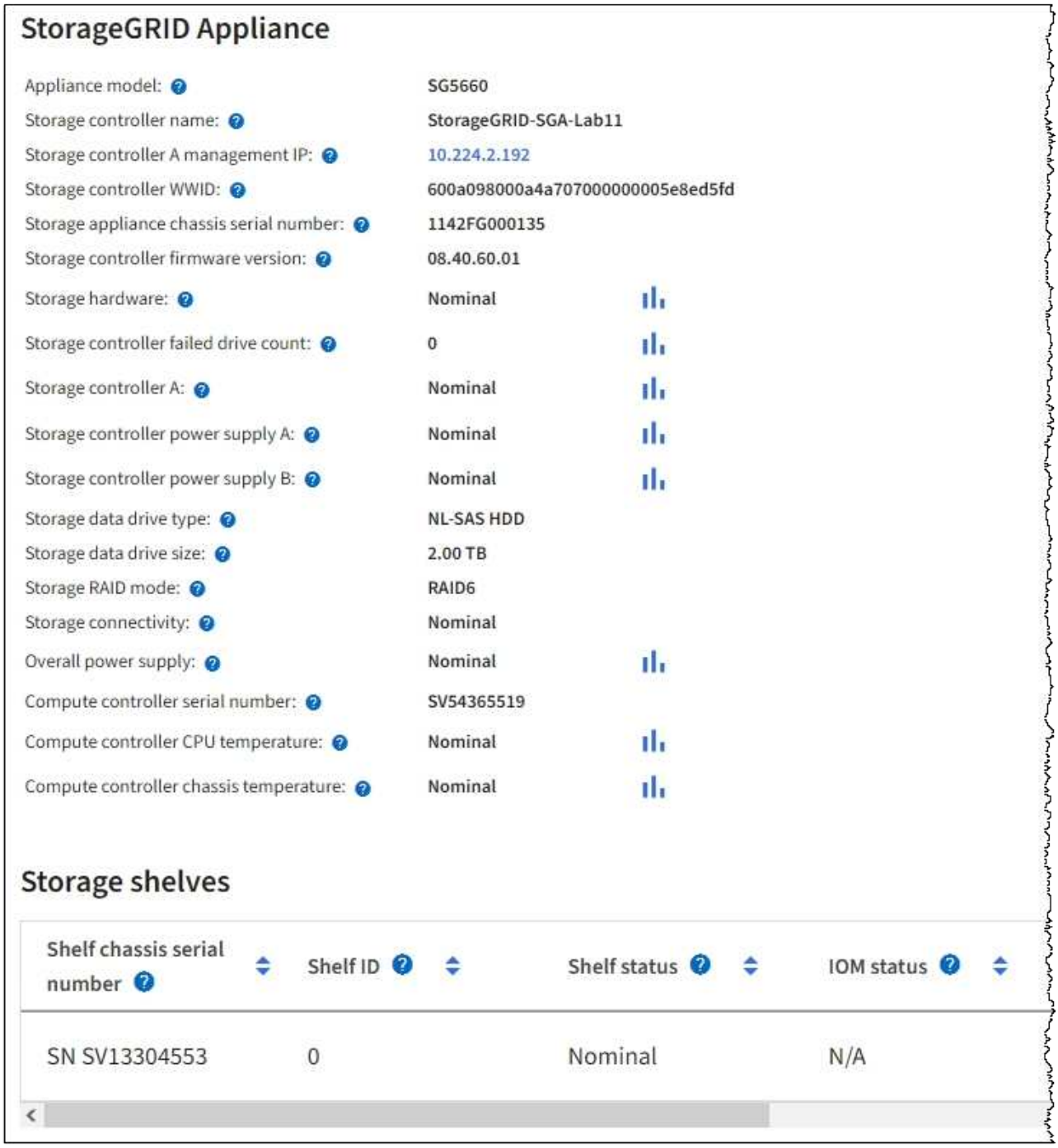
您还可以设置自定义间隔，以便指定日期和时间范围。



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 。
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。

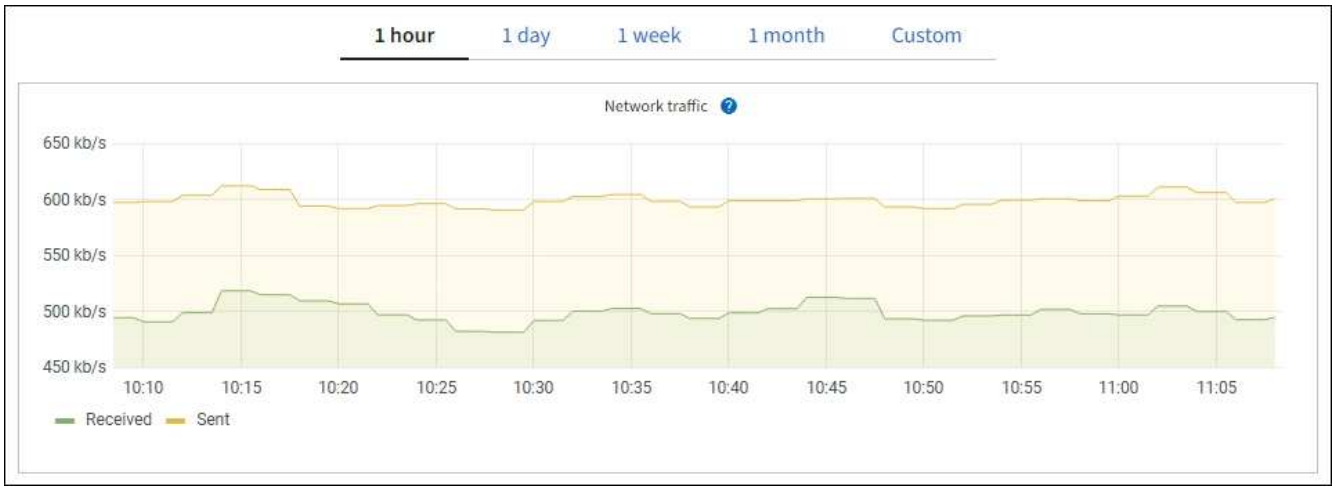
存储架表中的列	Description
【磁盘架数据驱动器大小】数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储架中用作缓存的驱动器数量。
缓存驱动器大小	存储架中最小缓存驱动器的大小。通常，缓存驱动器的大小相同。
配置状态	存储架的配置状态。

a. 确认所有状态均为"标称"。

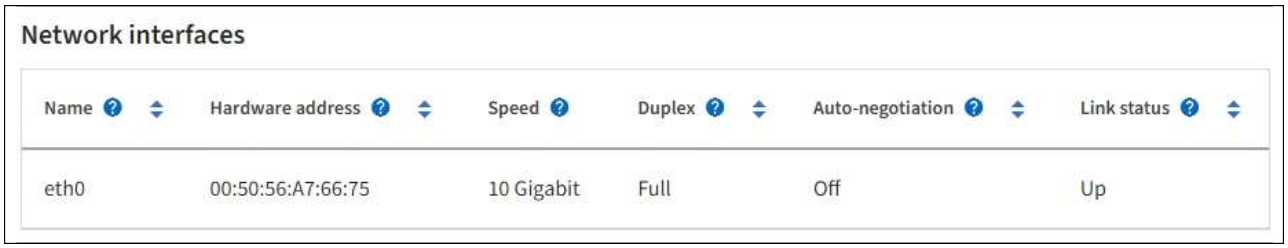
   如果状态不是"标称"、请查看任何当前警报。您还可以使用 SANtricity 系统管理器详细了解其中一些硬件值。请参见有关安装和维护设备的说明。

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。



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	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 10/225-GbE 网络端口是配置为使用主动 / 备份模式还是 LACP 模式。

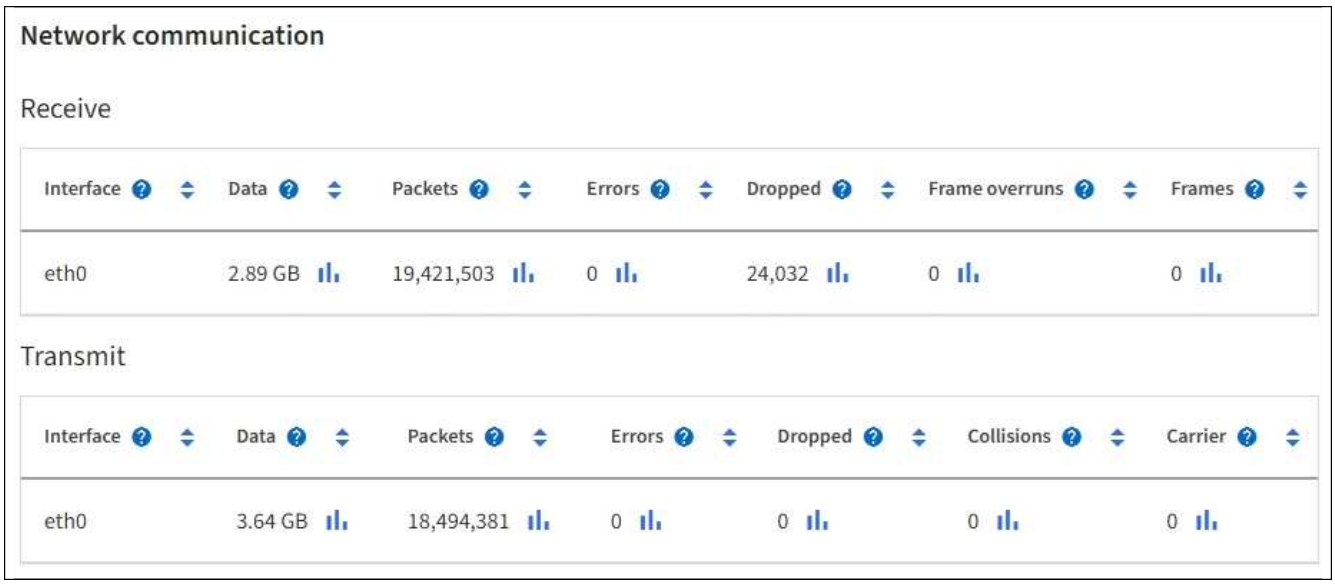
> 表中显示的值假定使用了所有四个链路。

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

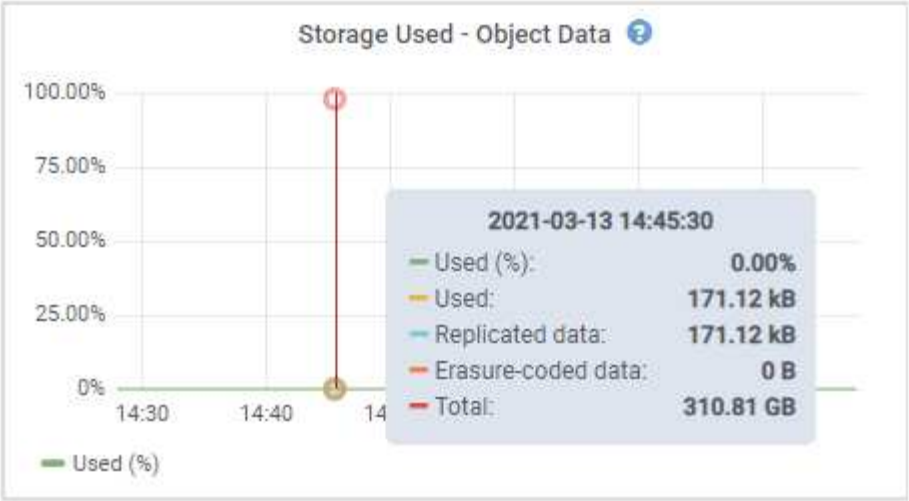
请参见 "配置网络链路" 有关配置10/C5-GbE端口的详细信息、请参见。

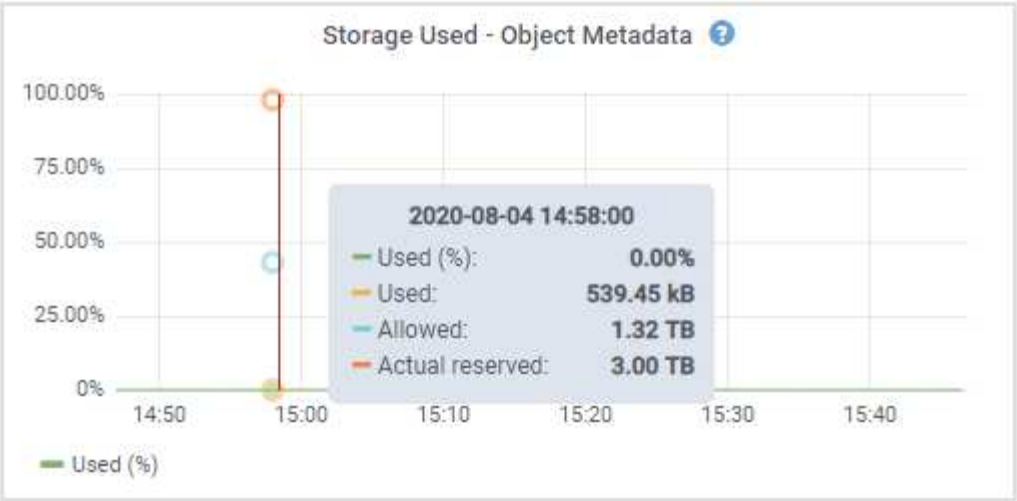
b. 查看网络通信部分。

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

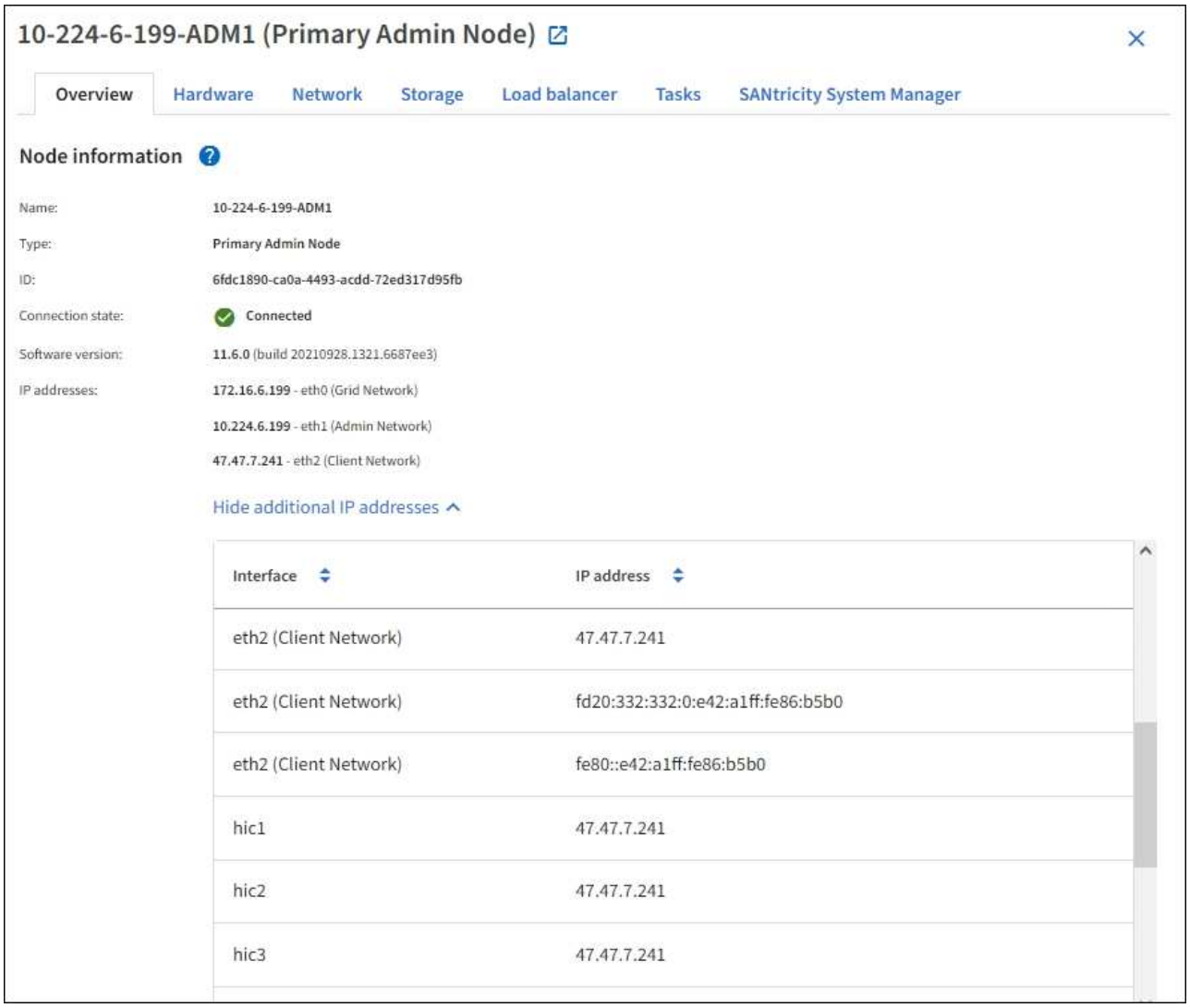
节点页面列出了有关用作管理节点或网关节点的每个服务设备的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，网络资源，网络接口，网络地址， 以及接收和传输数据。

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：

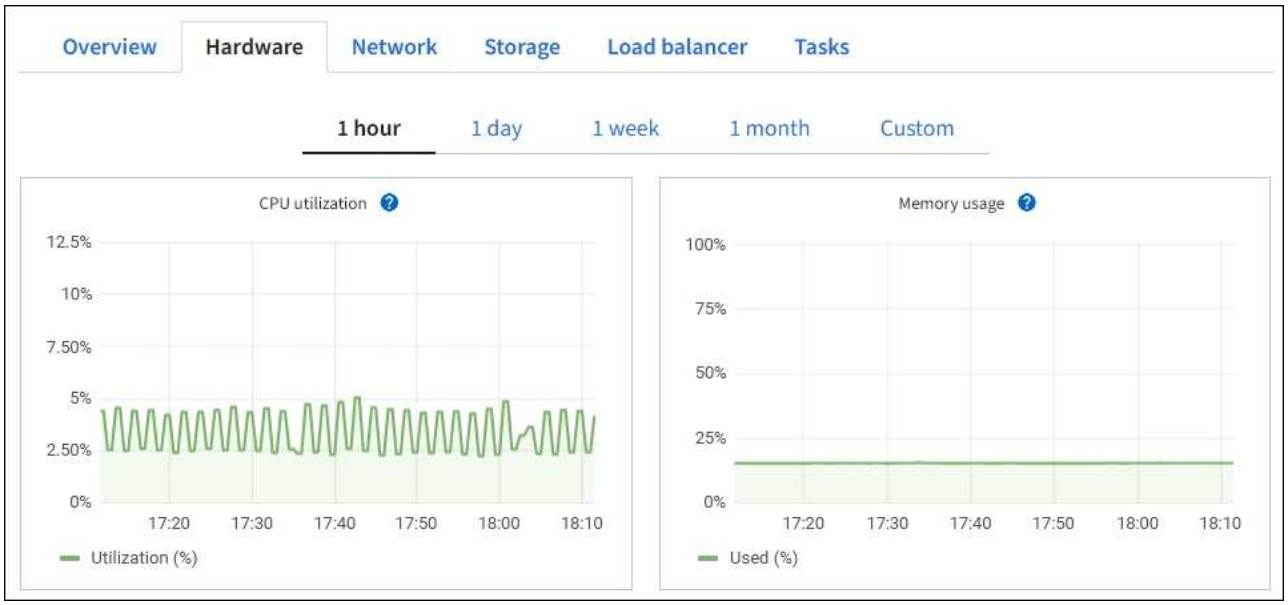
- * adllb* 和 * adlli*： 如果对管理网络接口使用主动 / 备份绑定，则显示此信息
- * eth *： 网格网络，管理网络或客户端网络。
- * hic*： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
- * MTC*： 设备上的一个物理 1-GbE 端口。 一个或多个 MTC 接口已绑定，以构成管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。



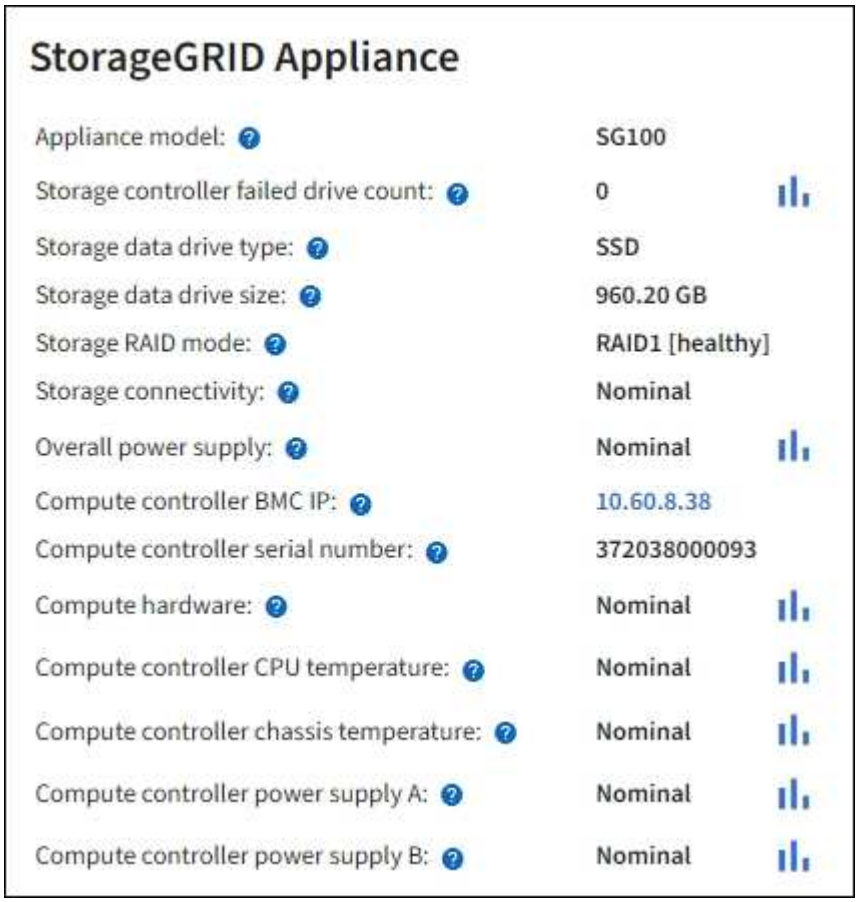
" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

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。

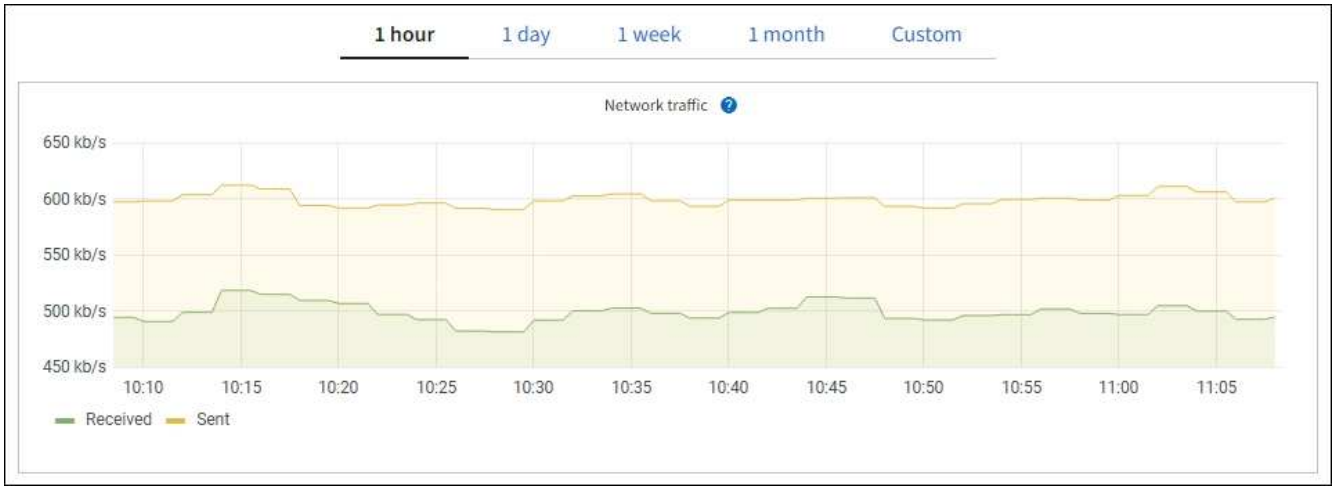
字段	Description
存储数据驱动器类型	设备中的驱动器类型、例如HDD (硬盘驱动器)或SSD (固态驱动器)。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller ， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含BMC的设备型号、不会显示此字段。
计算控制器序列号	计算控制器的序列号。
计算硬件	计算控制器硬件的状态。
计算控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

Network communication

Receive

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

Transmit

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

5. 选择 * 存储 * 可查看有关服务设备上的磁盘设备和卷的信息。

DO-REF-DC1-GW1 (Gateway Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks

Disk devices

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

Volumes

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

查看网络选项卡

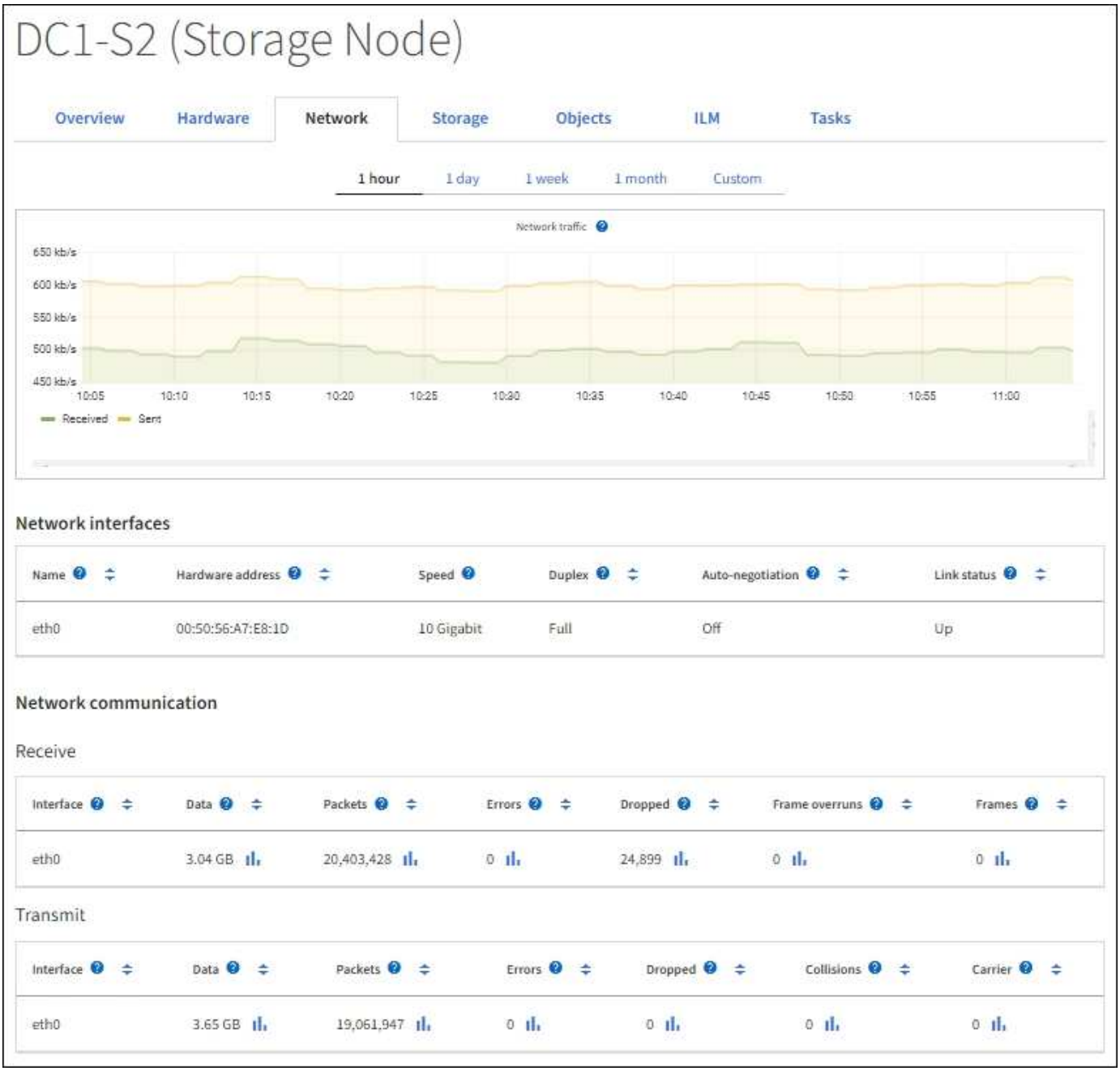
网络选项卡显示一个图形，其中显示了通过节点，站点或网格上的所有网络接口接收和发

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

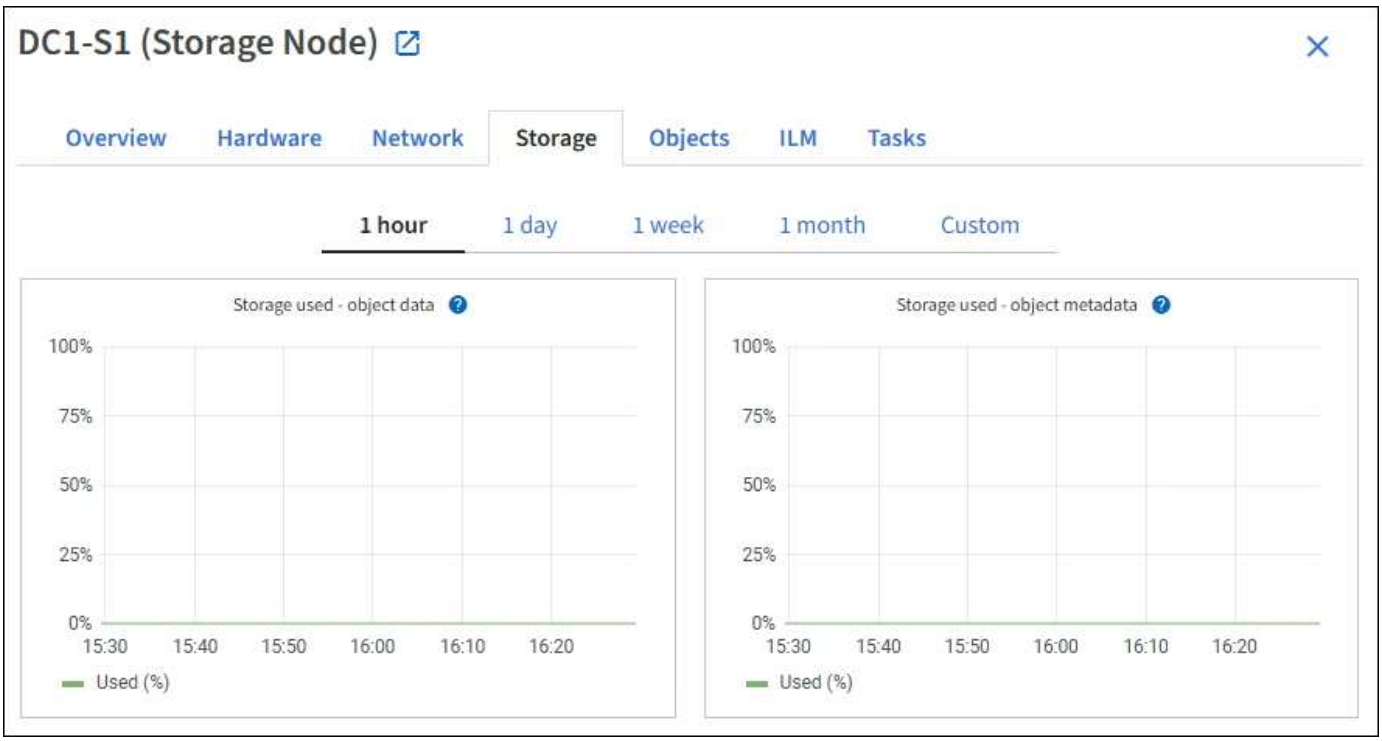
存储选项卡汇总了存储可用性和其他存储指标。

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

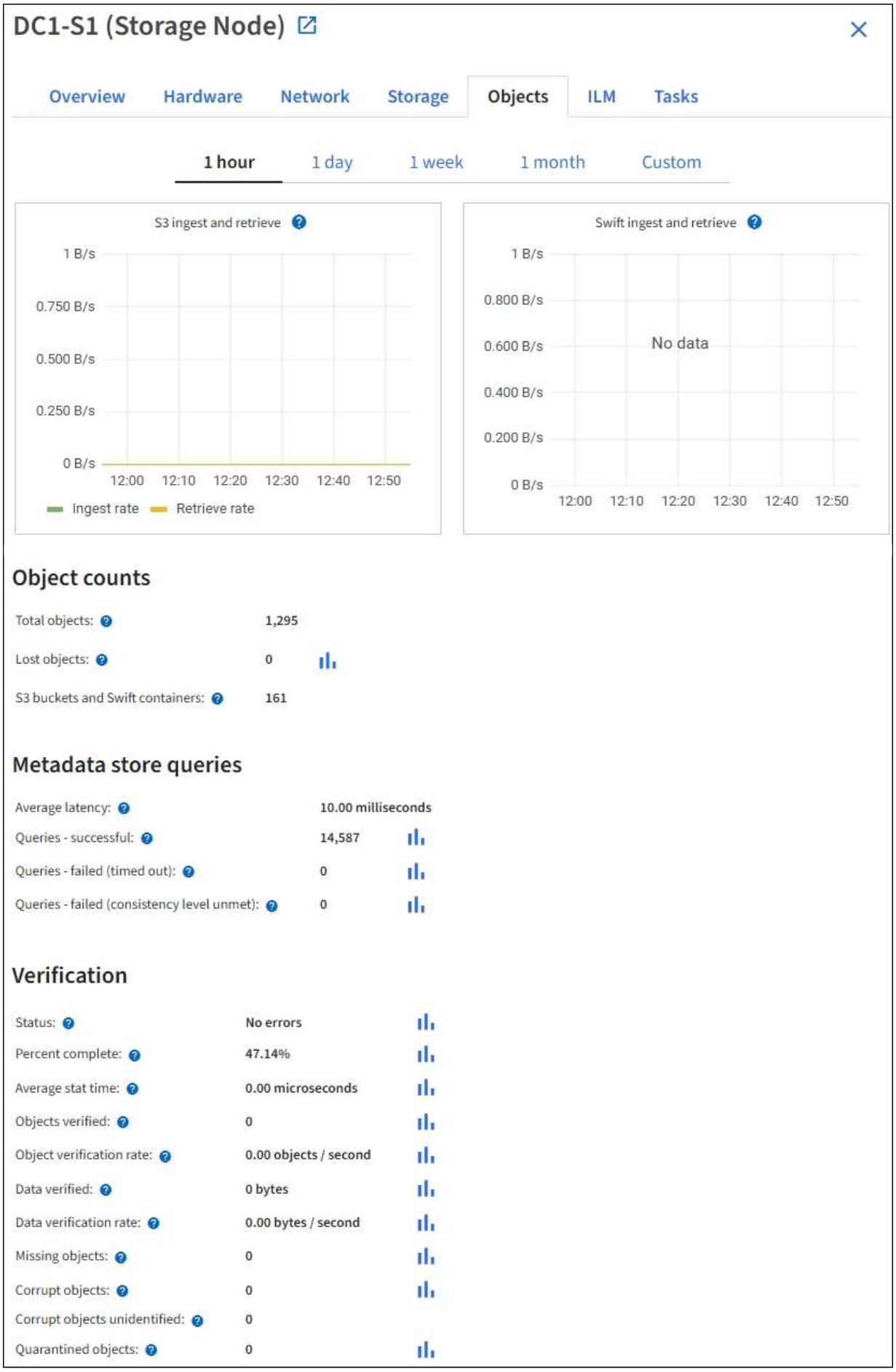
相关信息

"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。

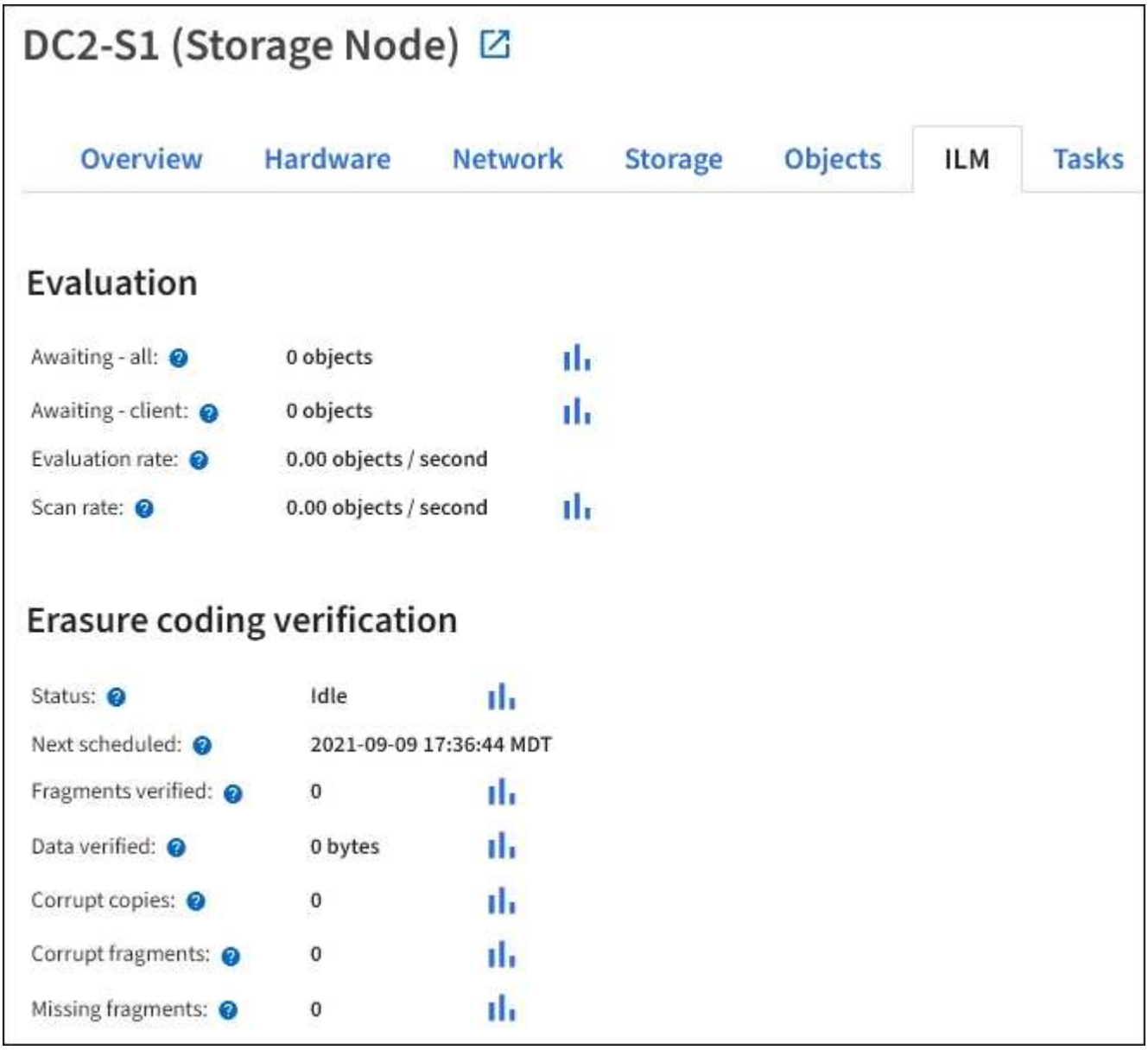

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 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

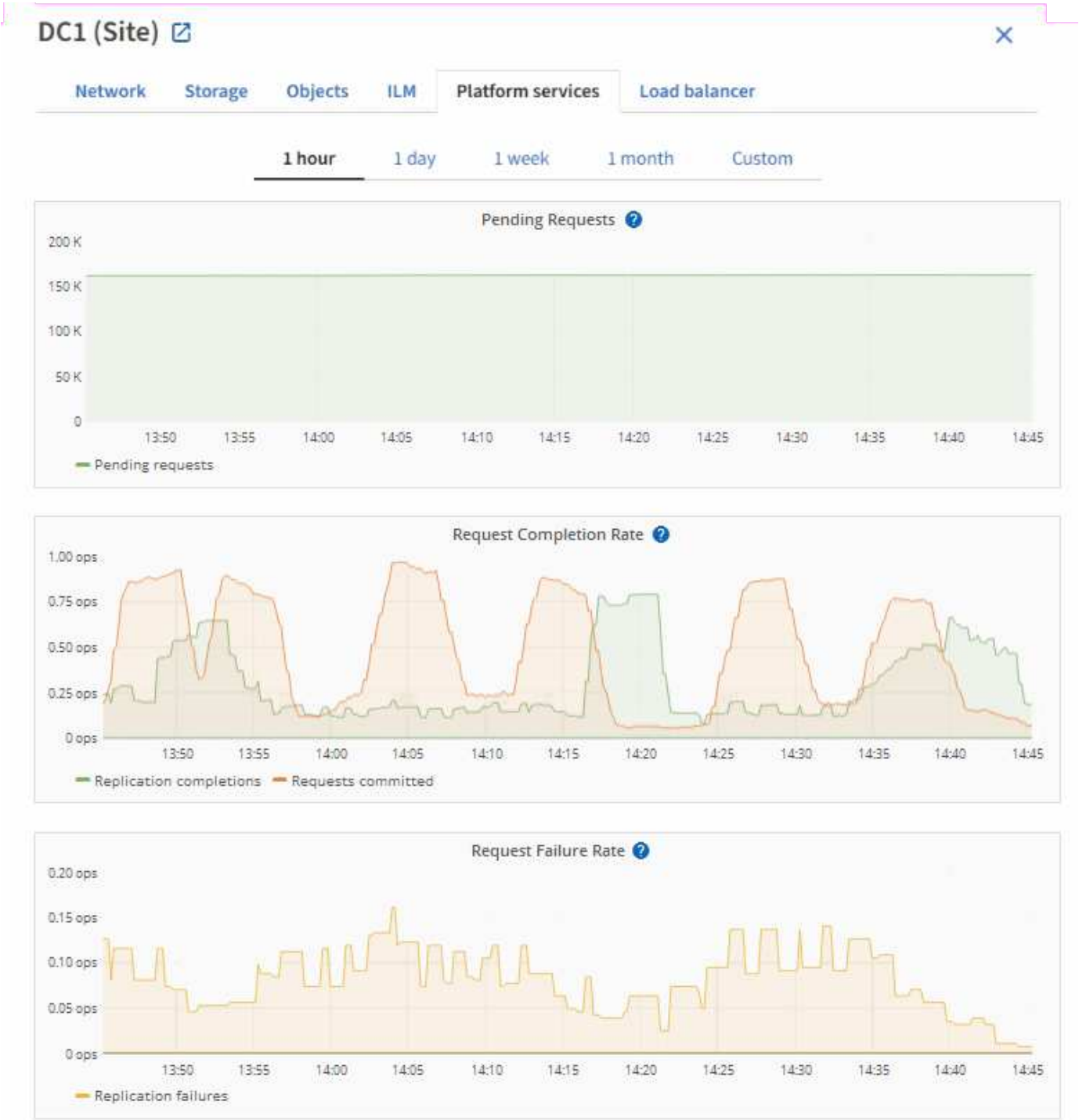
"监控负载平衡操作"

"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。

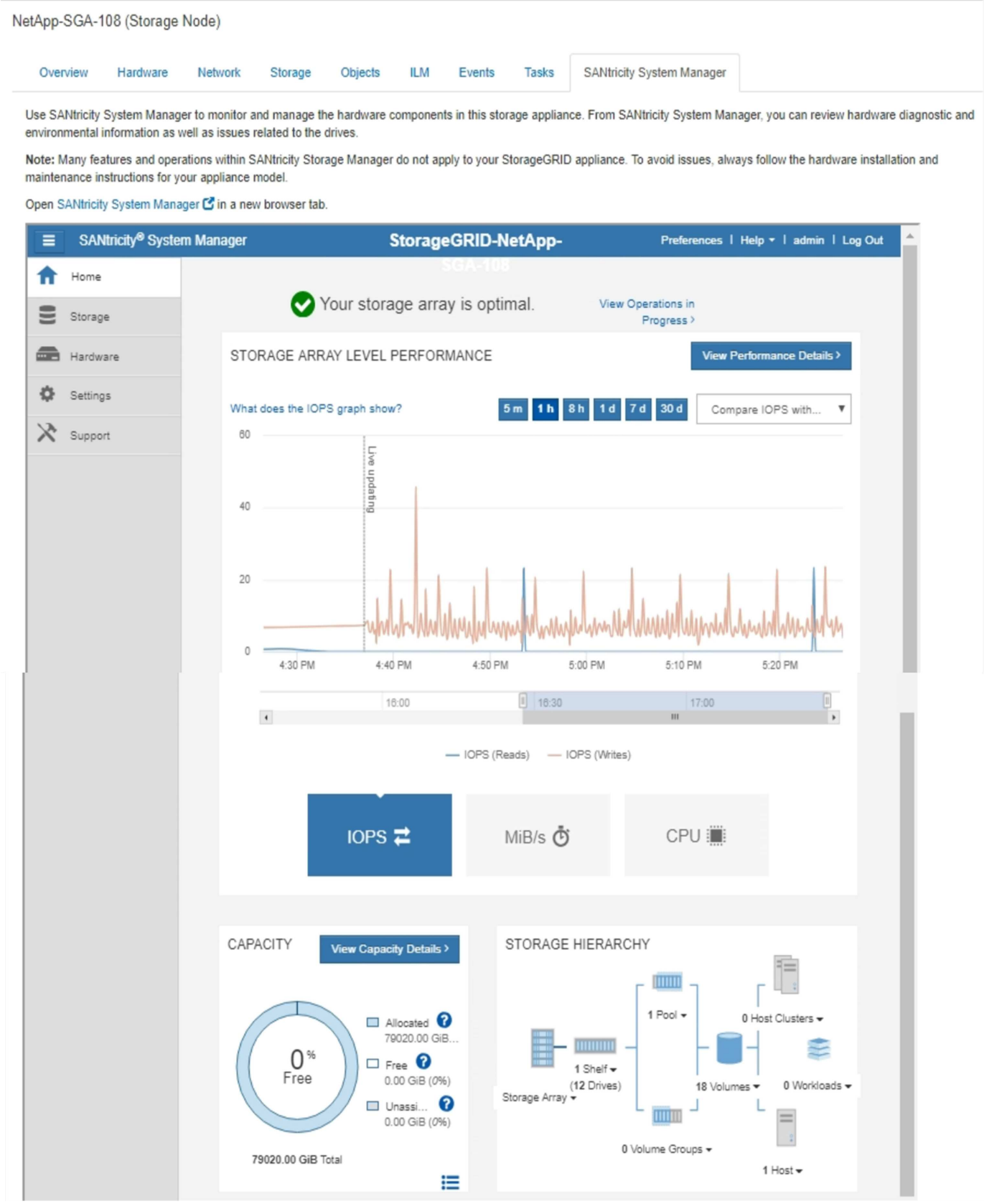
> 要使用SANtricity 系统管理器为E系列AutoSupport 配置代理、请参见 "通过StorageGRID发送E系列AutoSupport软件包"。

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

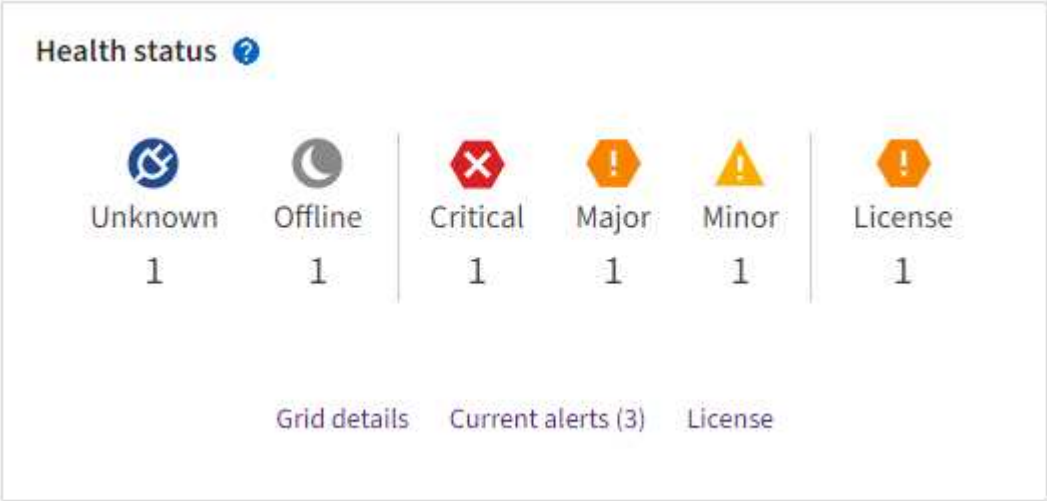
监控系统运行状况

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。

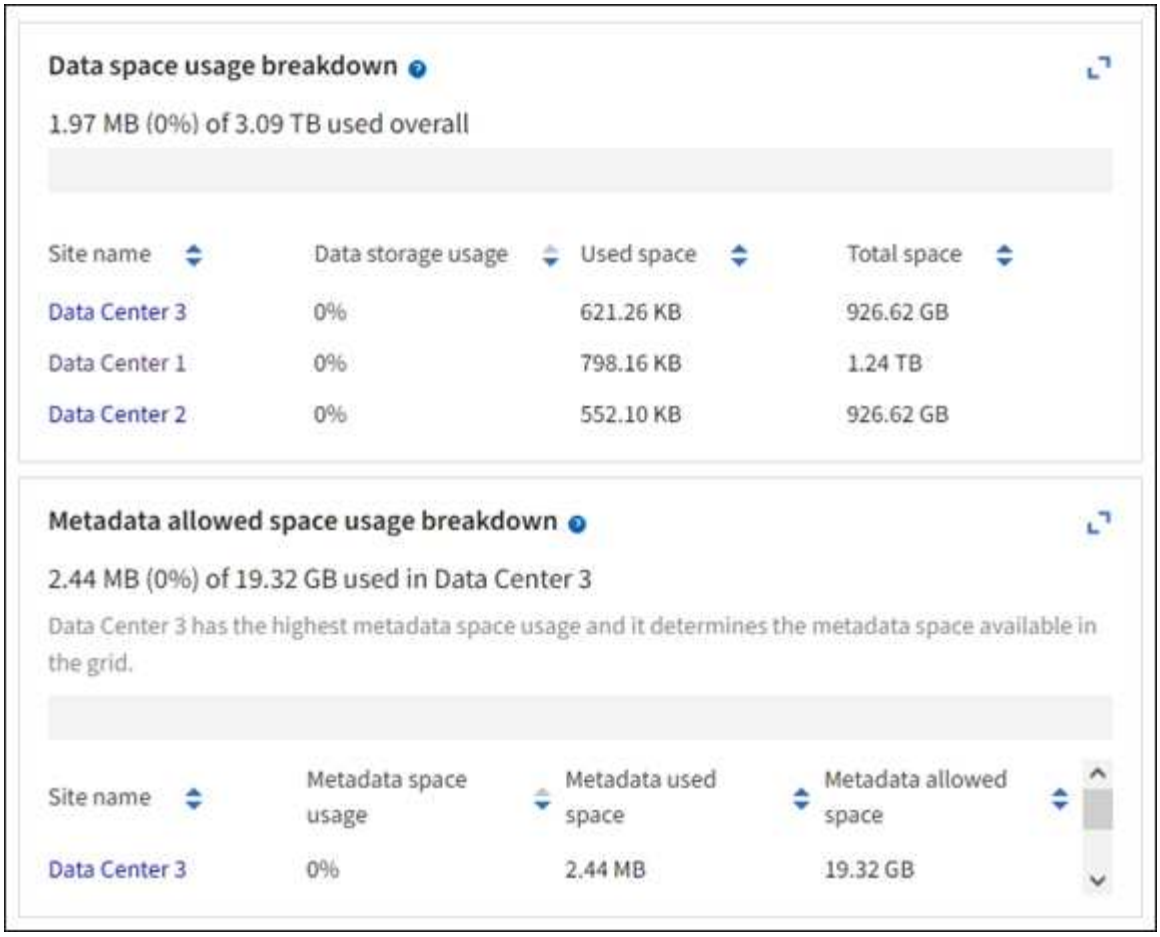
步骤

1. 评估可用于整个网格和每个数据中心的存储量。

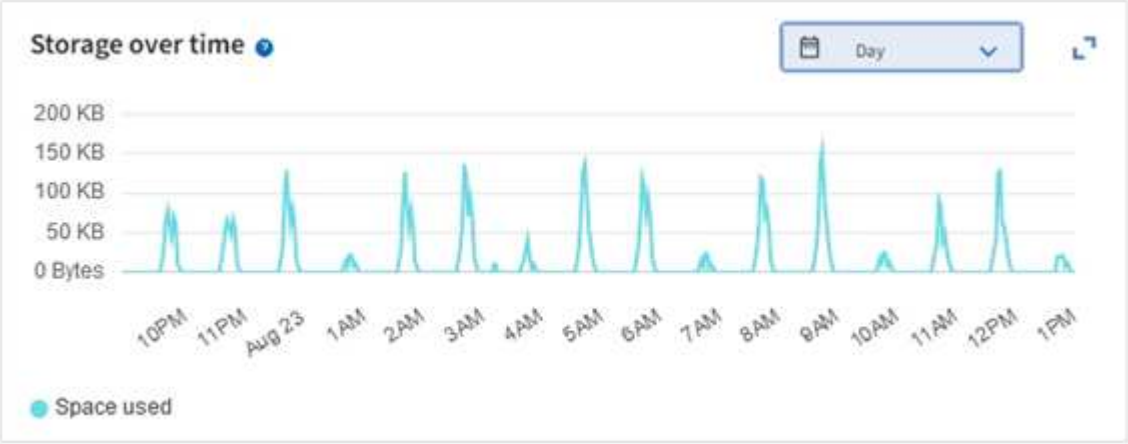
   a. 选择*信息板>概述*。

   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。



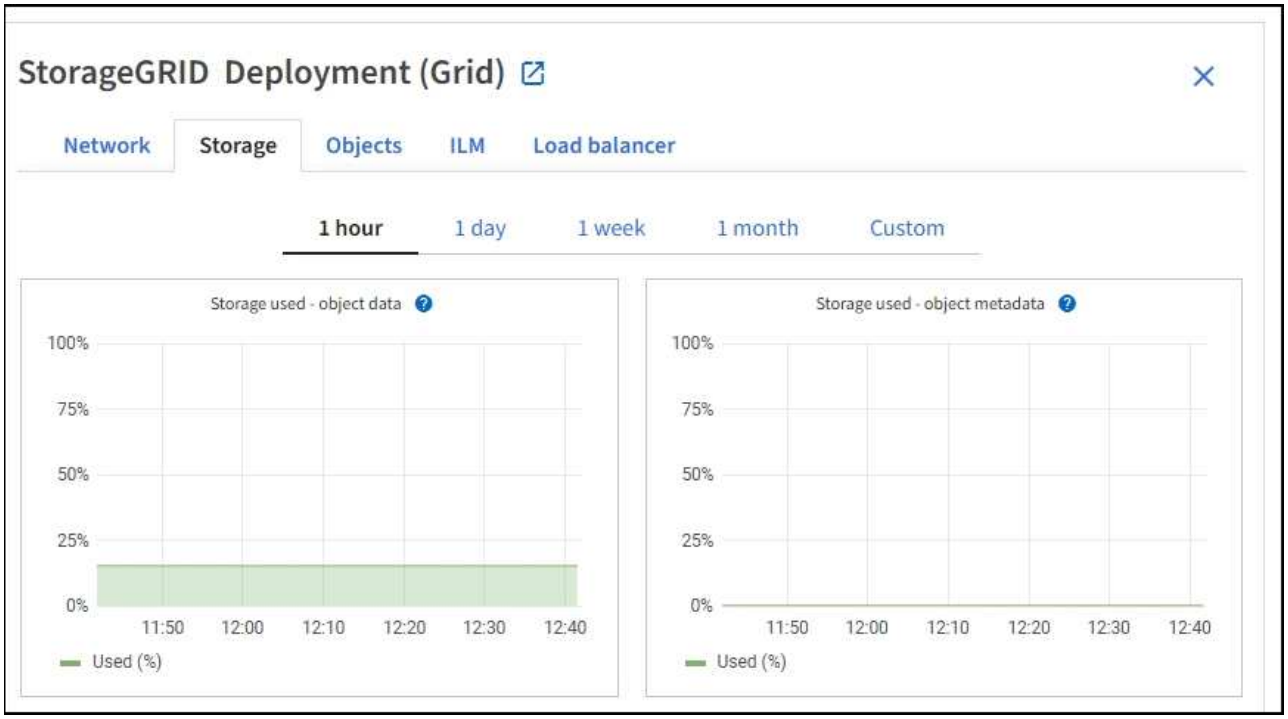
a. 记下随时间变化的存储卡上的图表。使用时间段下拉列表帮助您确定存储的使用速度。



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。

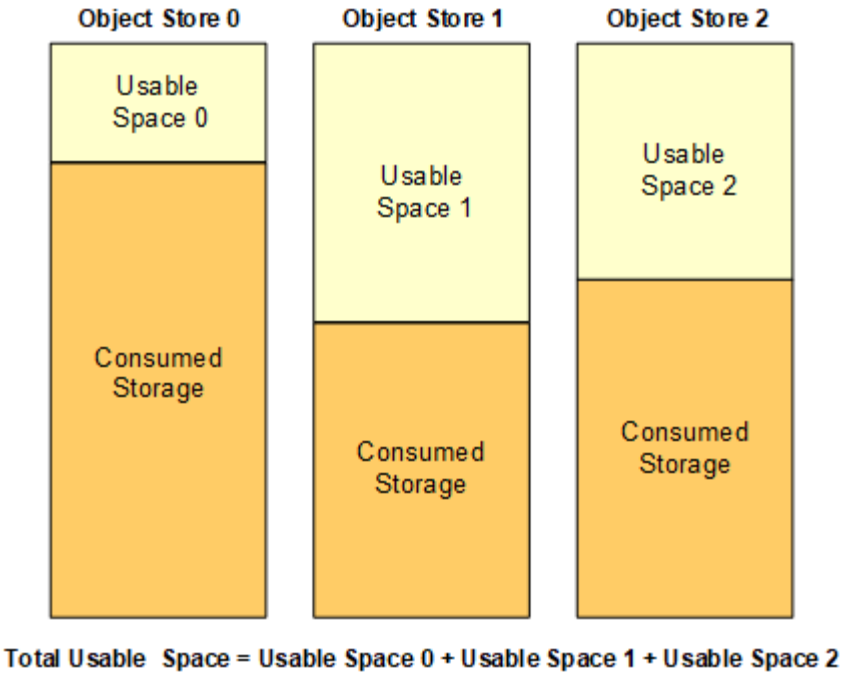
   有关规划存储扩展的详细信息、请参见 "扩展 StorageGRID 的说明"。

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

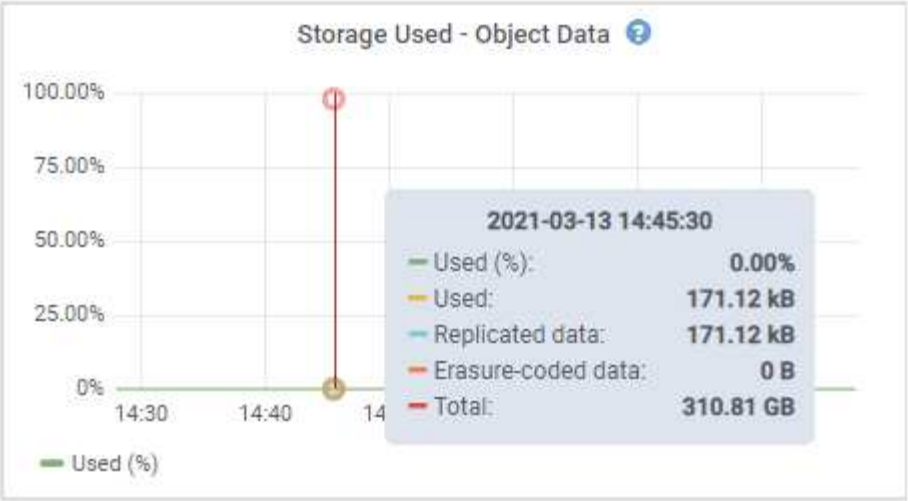
1. 选择 * 节点 * > * 存储节点 _* > * 存储 * 。

   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对象元数据容量

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

关于此任务

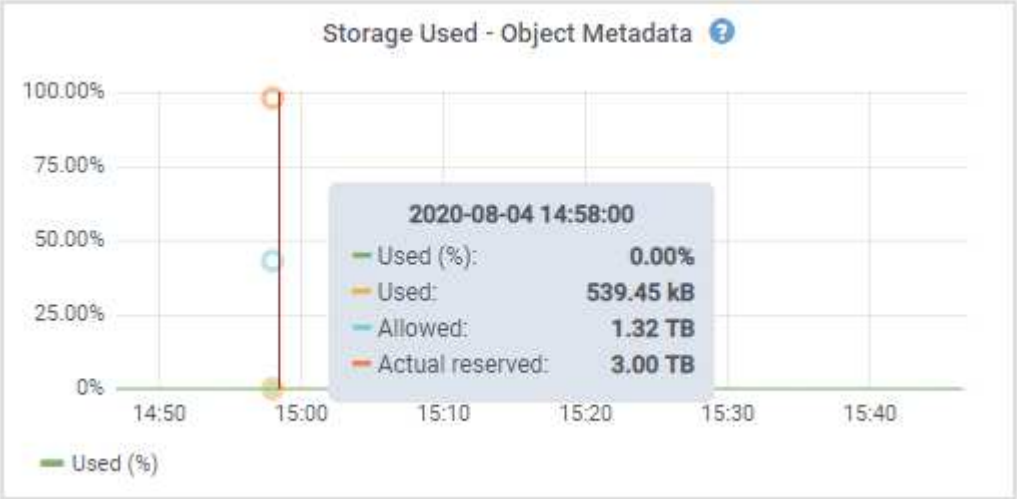
StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并防止对象元数据丢失。这三个副本会使用每个存储节点的存储卷 0 上为元数据预留的空间均匀分布在每个站点的所有存储节点上。

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

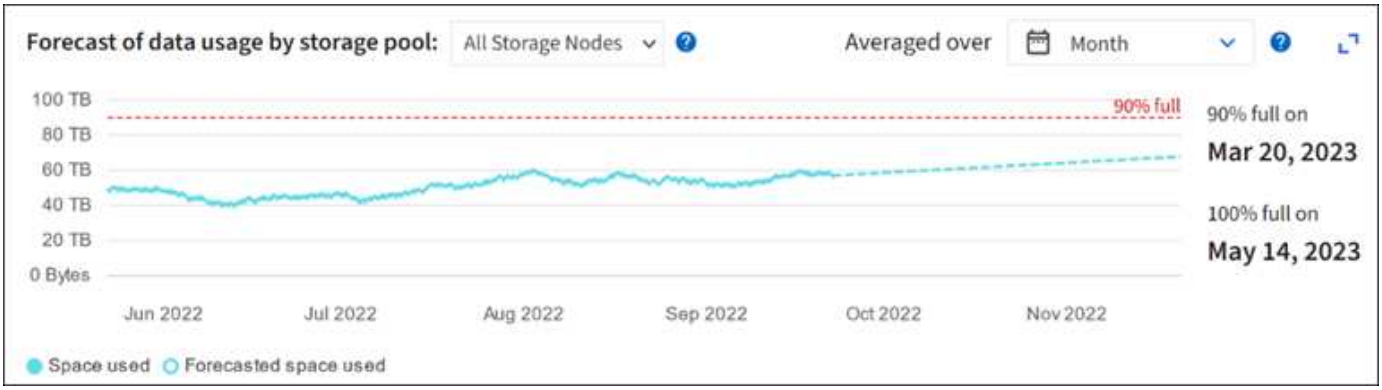
监控用户数据和元数据的空间使用情况预测、以估算何时需要 "扩展网格"。

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。

监控网络和系统资源

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。

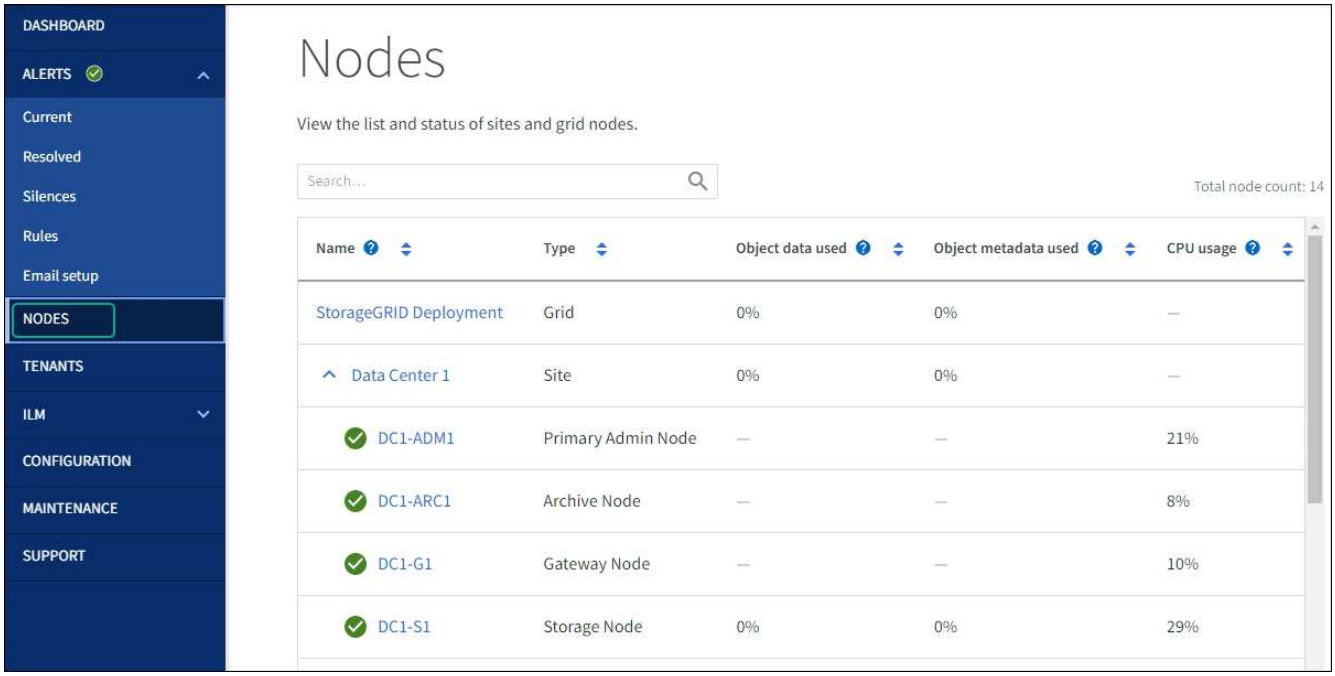
使用网格管理器监控连接和网络性能、以便及时解决任何问题。

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

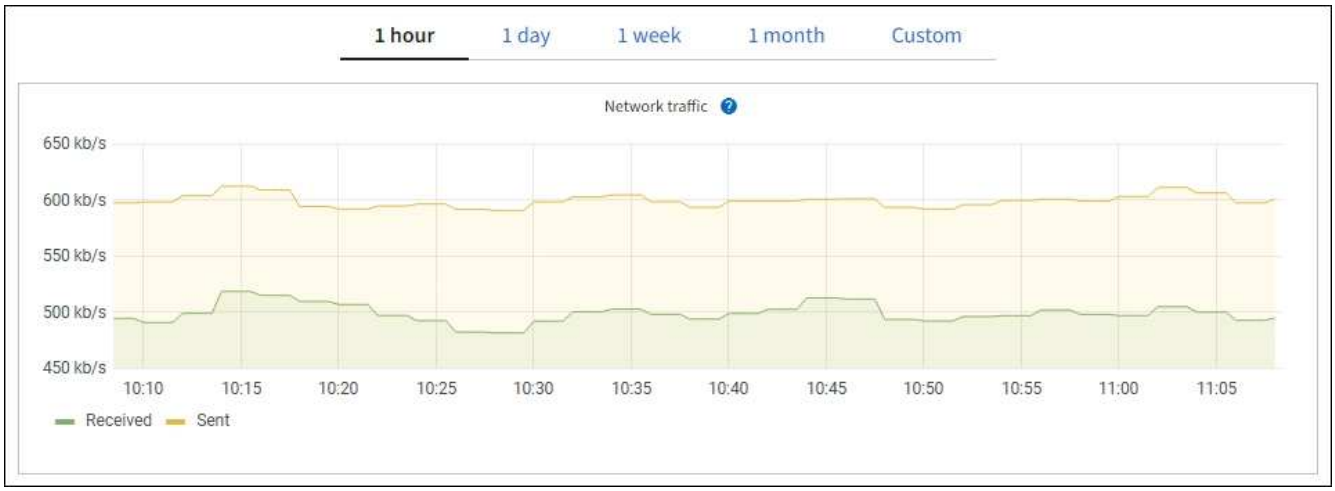
1. 选择 * 节点 * 。

   此时将显示节点页面。网格中的每个节点均以表格式列出。

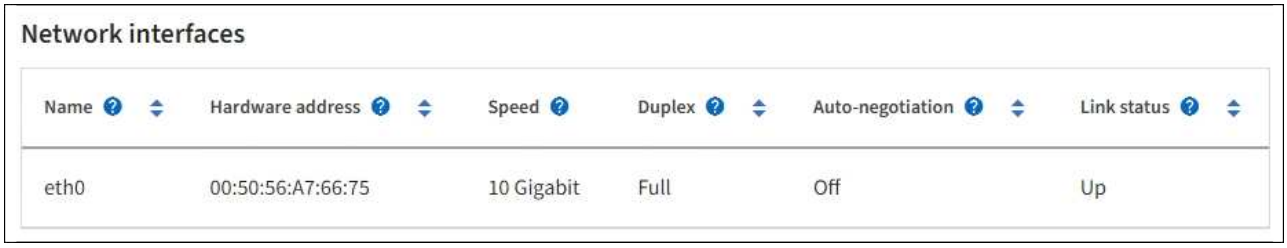


2. 选择网格名称，特定数据中心站点或网格节点，然后选择 * 网络 * 选项卡。

   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。

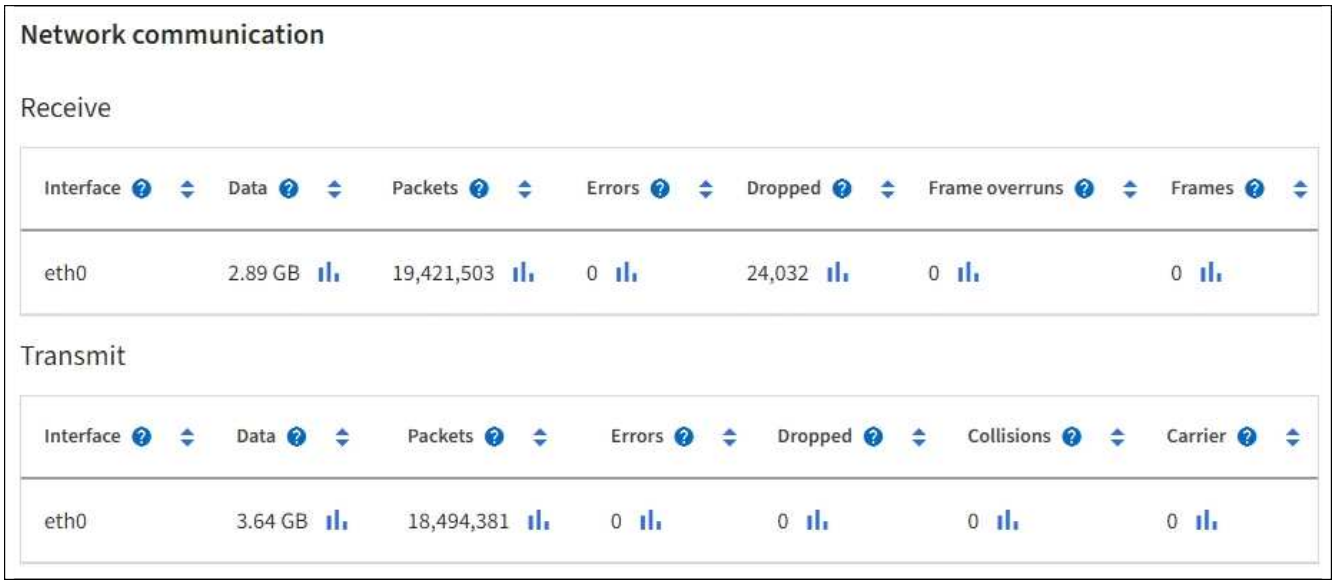


Network interfaces

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

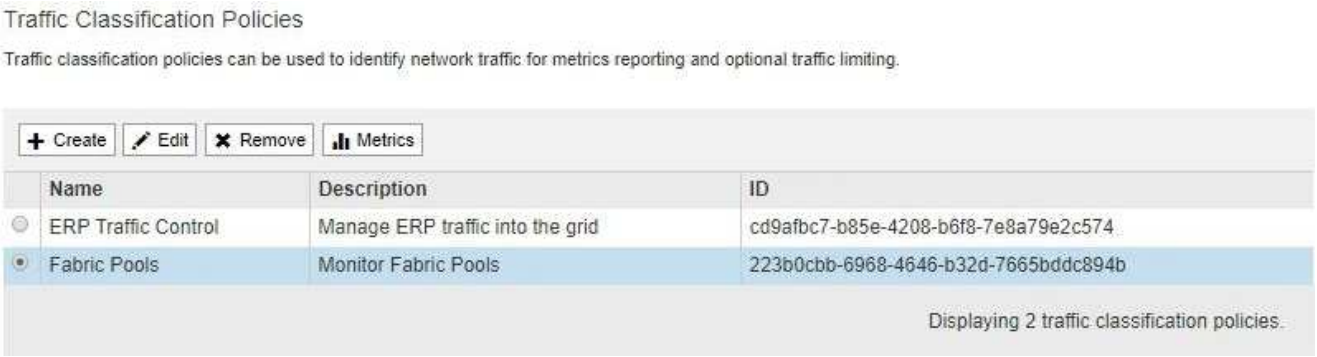
Transmit

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"

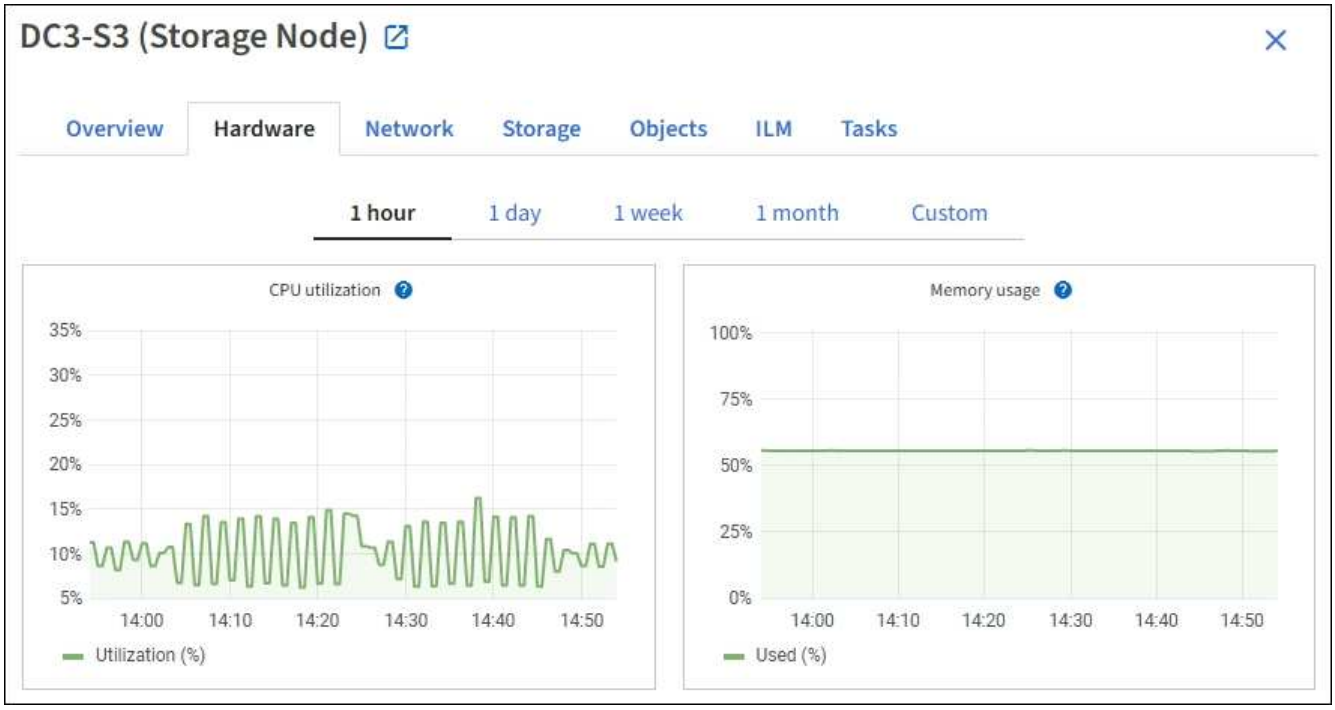
"监控节点连接状态"

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

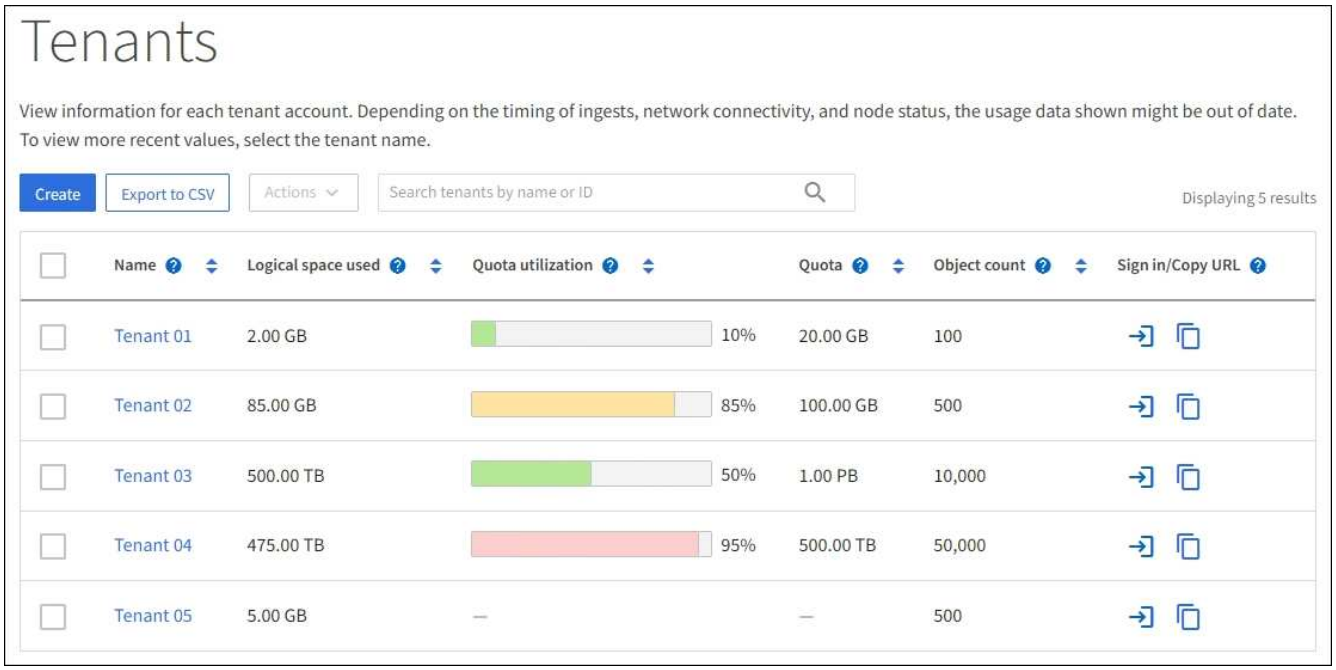
租户页面显示所有当前租户帐户的基本信息。

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。

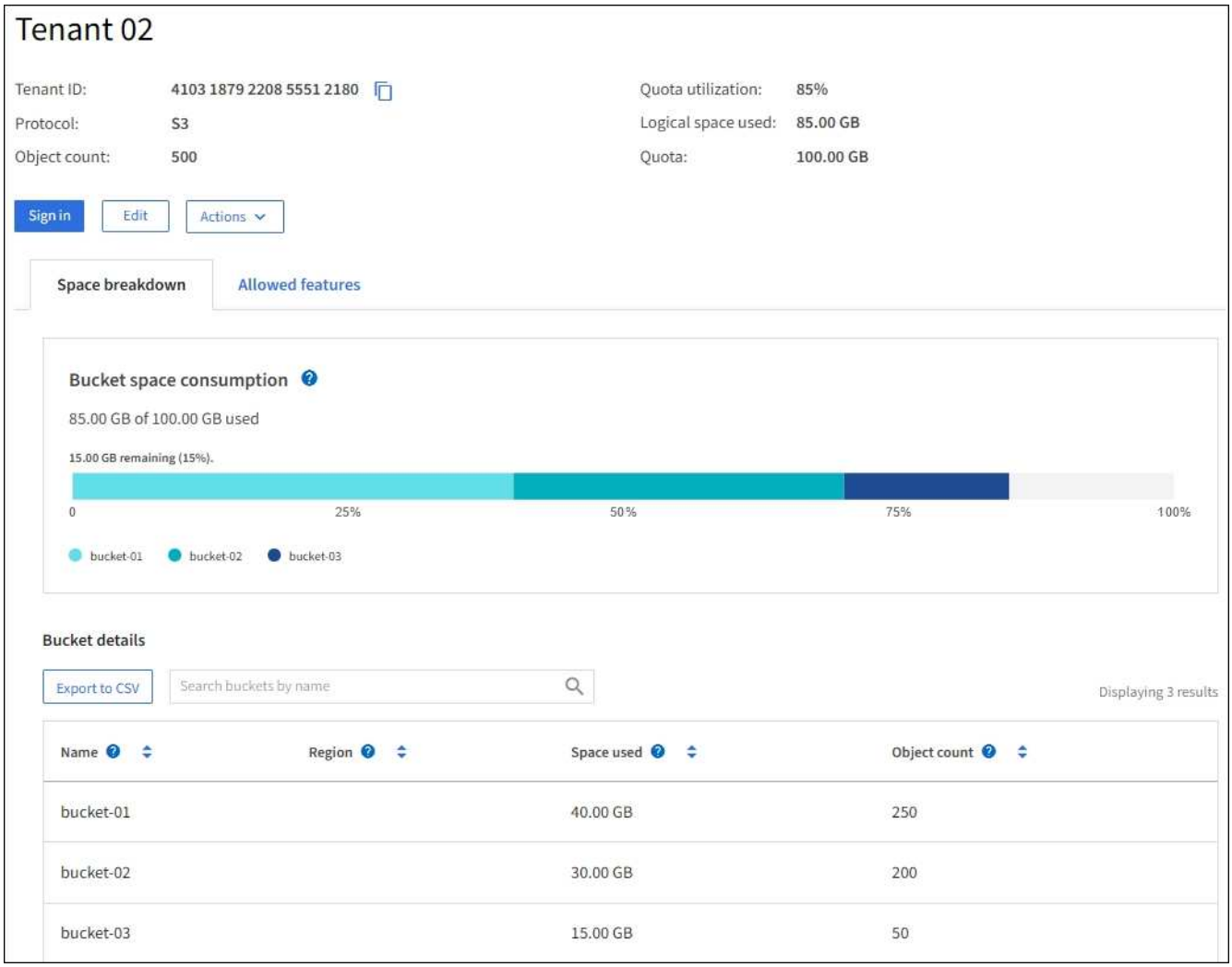
查看特定租户

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。

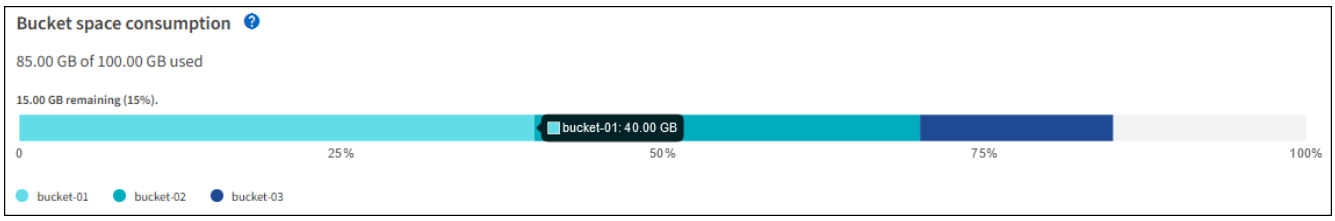
   此部分详细信息页面提供了租户的摘要信息、包括租户的对象计数、配额利用率、已用逻辑空间和配额设置。

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"。

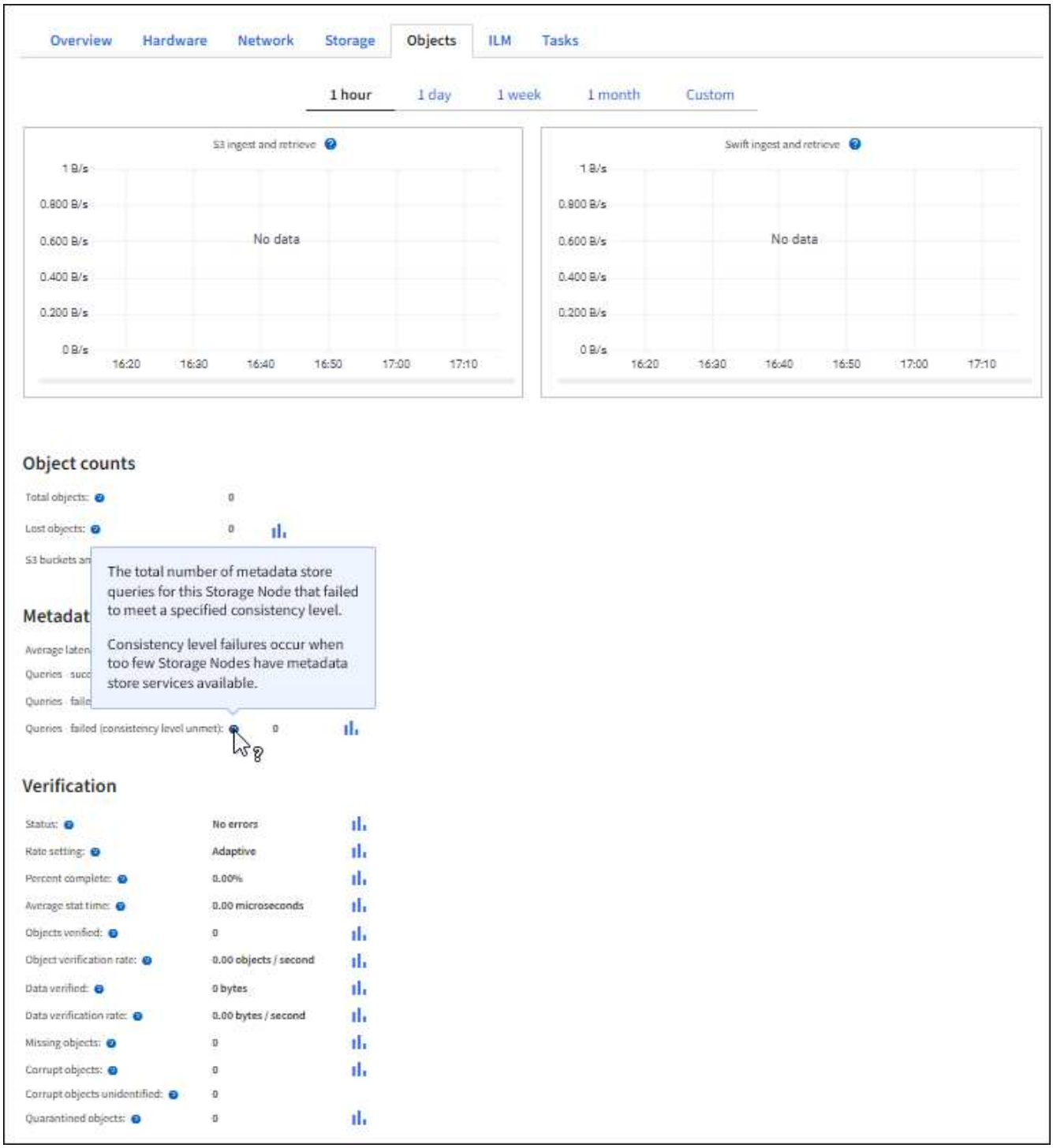
步骤

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

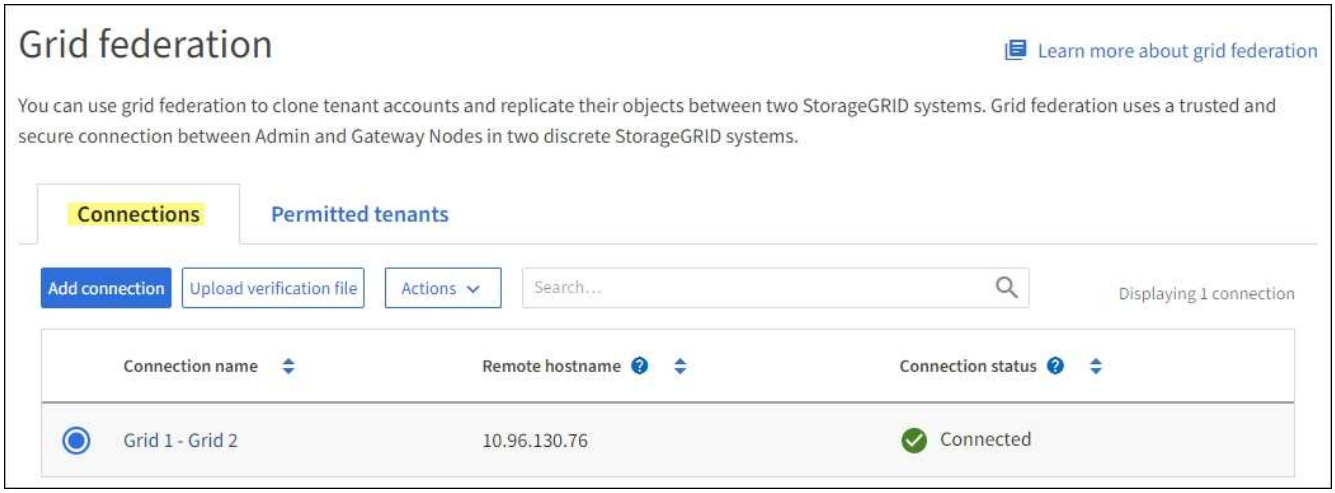
1. 选择*configuration*>*System*>*Grid Federation。

   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：

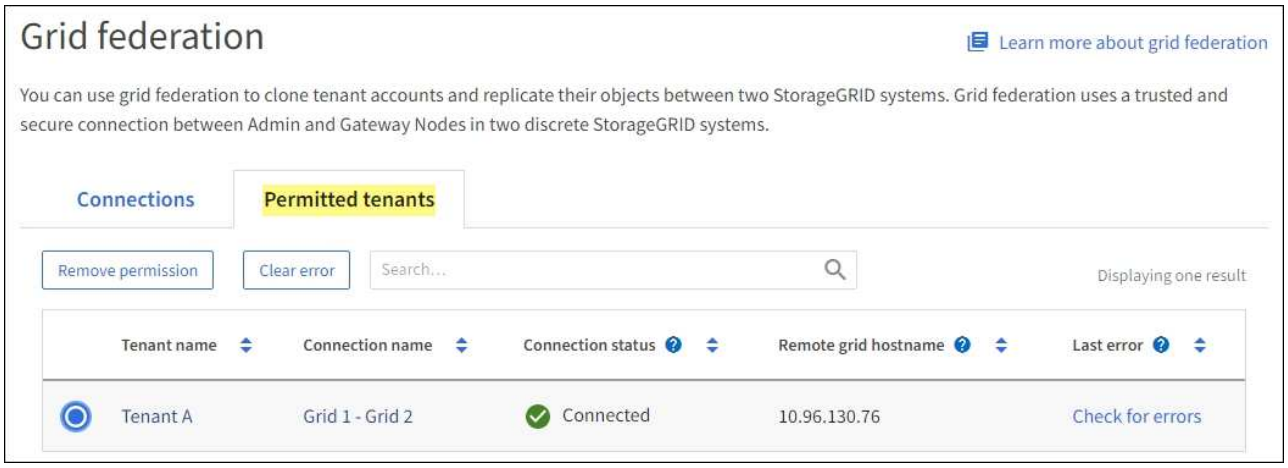
   - "创建新连接"。
   - 选择与的现有连接 "编辑或测试"。



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。

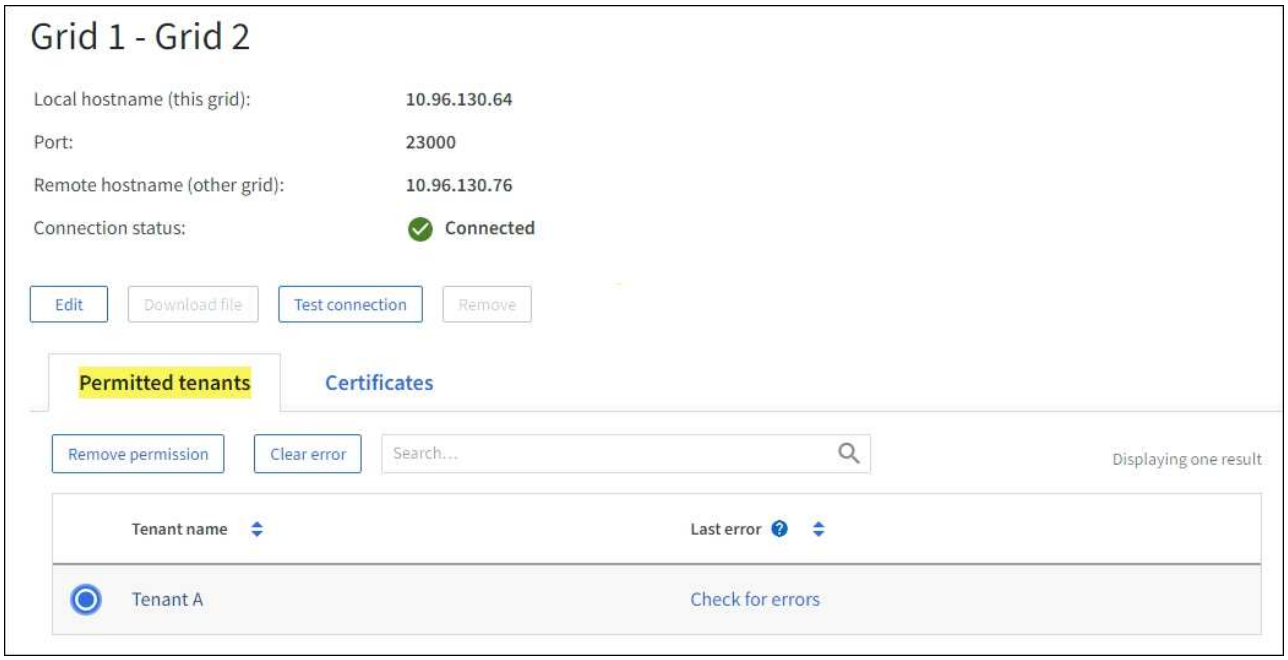
   在连接的详细信息页面中、您可以：

   - 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：

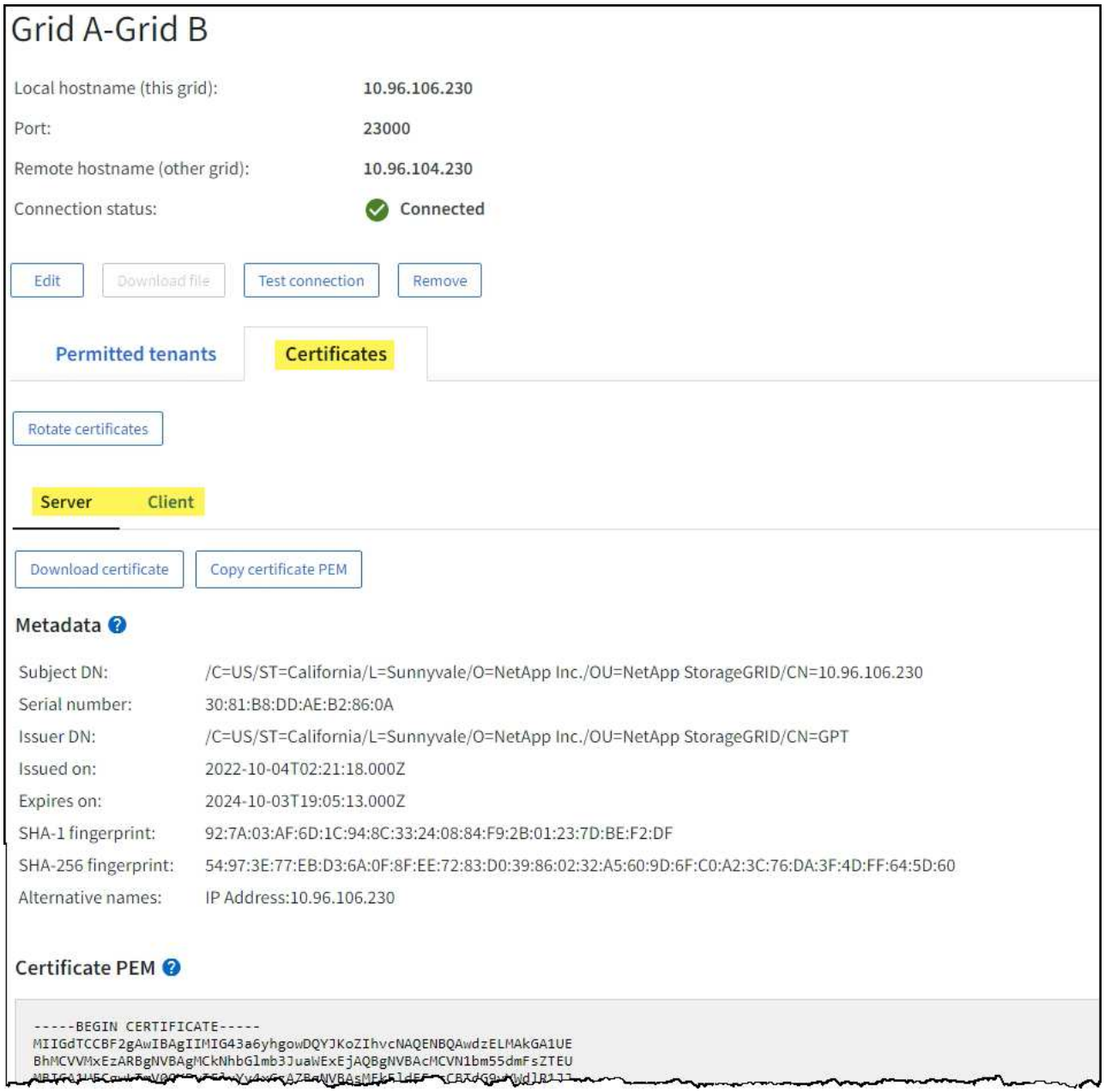
   - "查看每个允许租户的详细信息页面"。
   - "删除租户的权限" 可使用连接。
   - 检查是否存在跨网格复制错误、并清除最后一个错误。请参见 "对网格联合错误进行故障排除"。



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

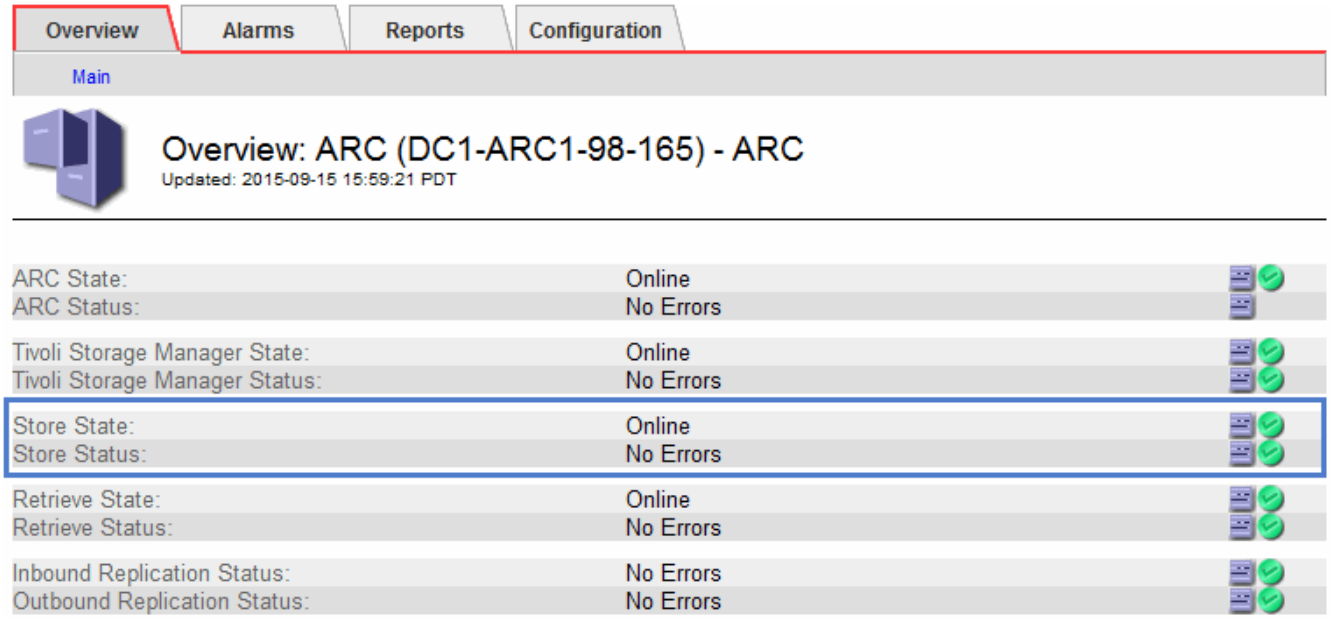
您不能通过StorageGRID 系统直接监控外部归档存储系统的容量。但是，您可以监控归档节点是否仍可将对象数据发送到归档目标，这可能表示需要扩展归档介质。

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

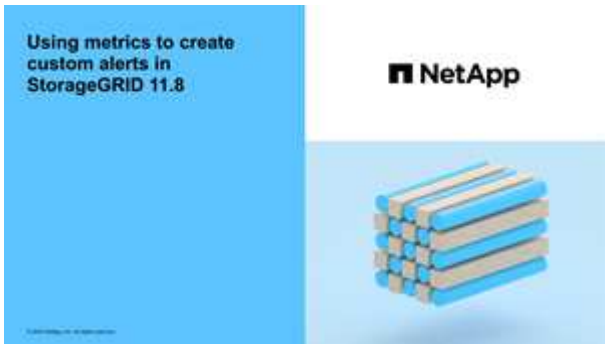
警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

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。

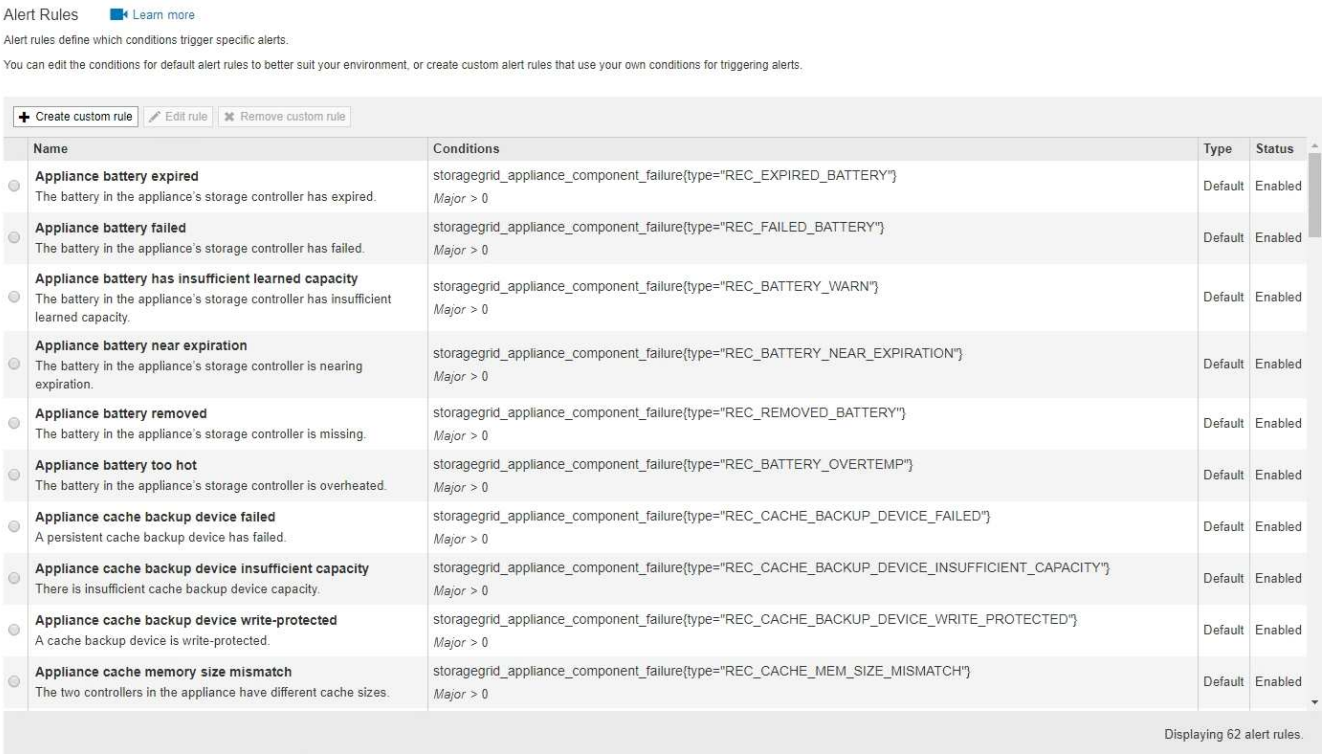
开始之前

- 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：

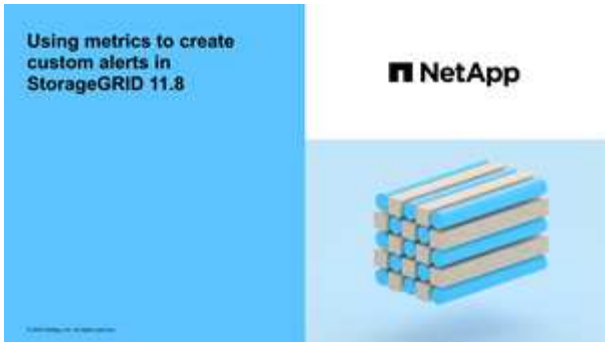
列标题	Description
Name	警报规则的唯一名称和问题描述 。首先列出自定义警报规则，然后列出默认警报规则。警报规则名称是电子邮件通知的主题。
条件	用于确定何时触发此警报的 Prometheus 表达式。可以在以下一个或多个严重性级别触发警报，但不需要为每个严重性设置一个条件。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID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

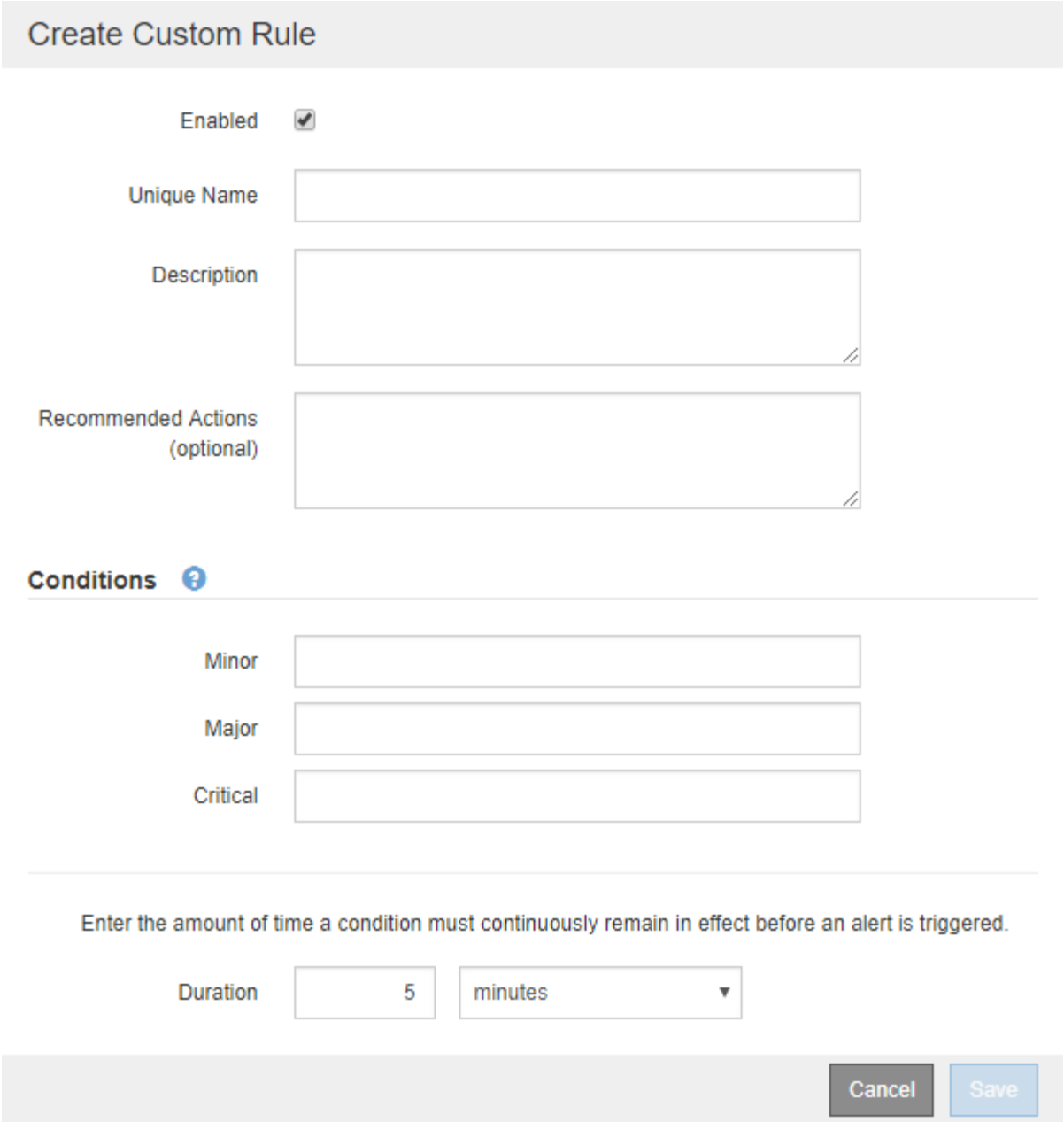
步骤

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。

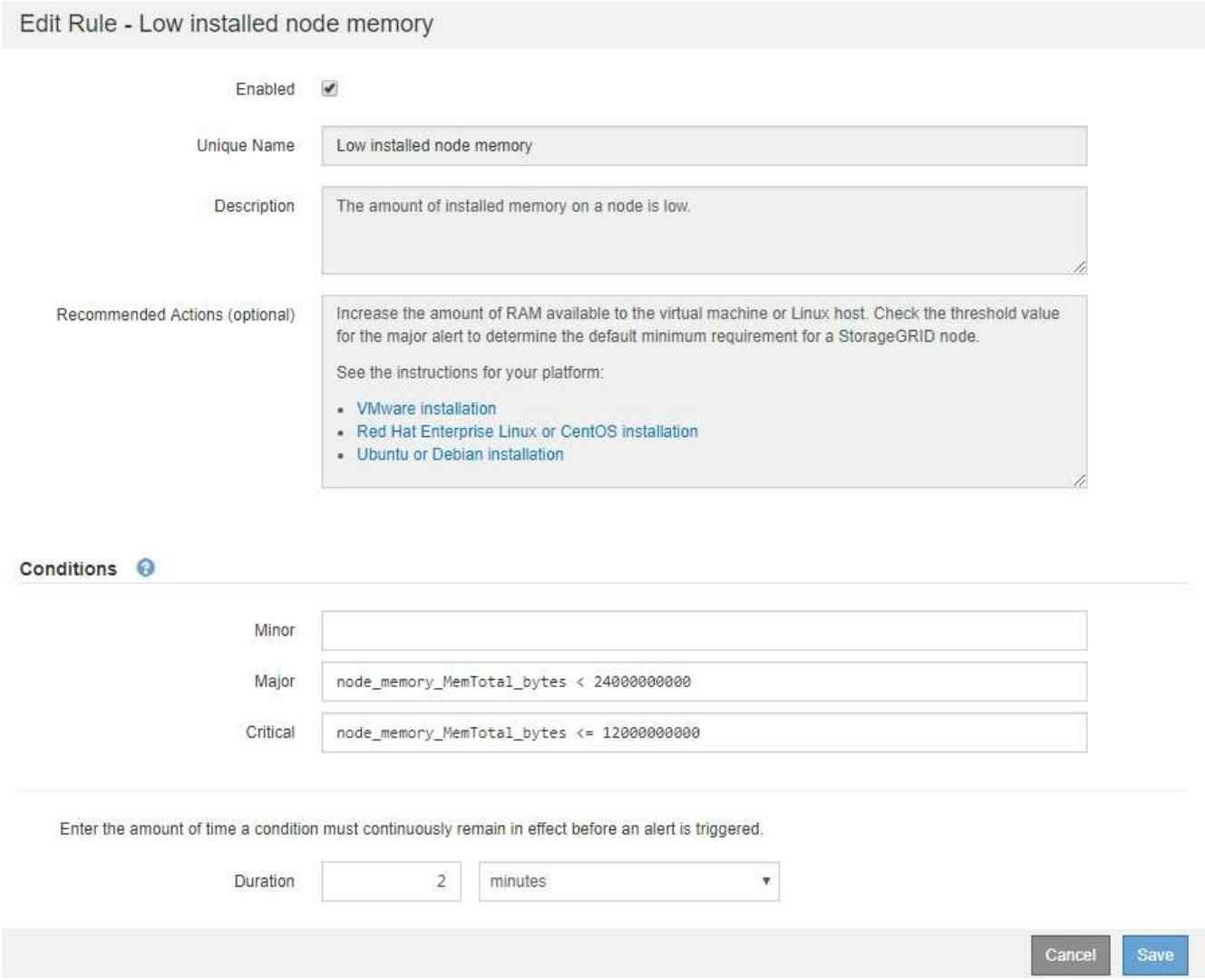
步骤

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。

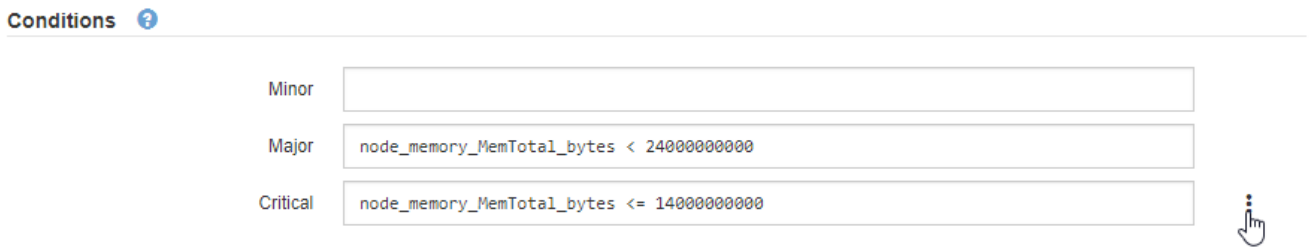
5. 对于自定义警报规则，请根据需要更新以下信息。

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。

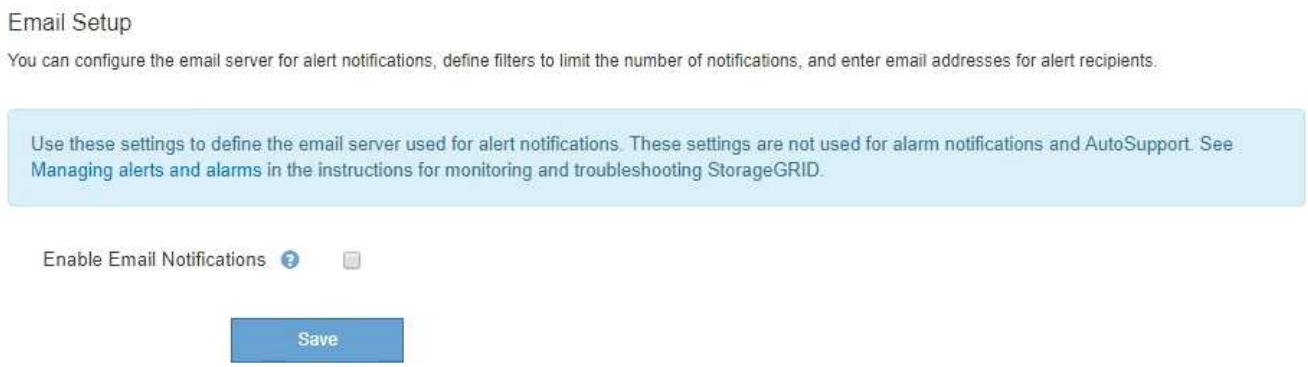
如果您的StorageGRID部署包含多个管理节点、则主管理节点是警报通知、AutoSupport软件包、SNMP陷阱和

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。

Transport Layer Security (TLS)

Require TLS ☑

CA Certificate

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

Browse

Send Client Certificate ☑

Client Certificate

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

Browse

Private Key

```
-----BEGIN PRIVATE KEY-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----BEGIN PRIVATE KEY-----
```

Browse

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 * 。

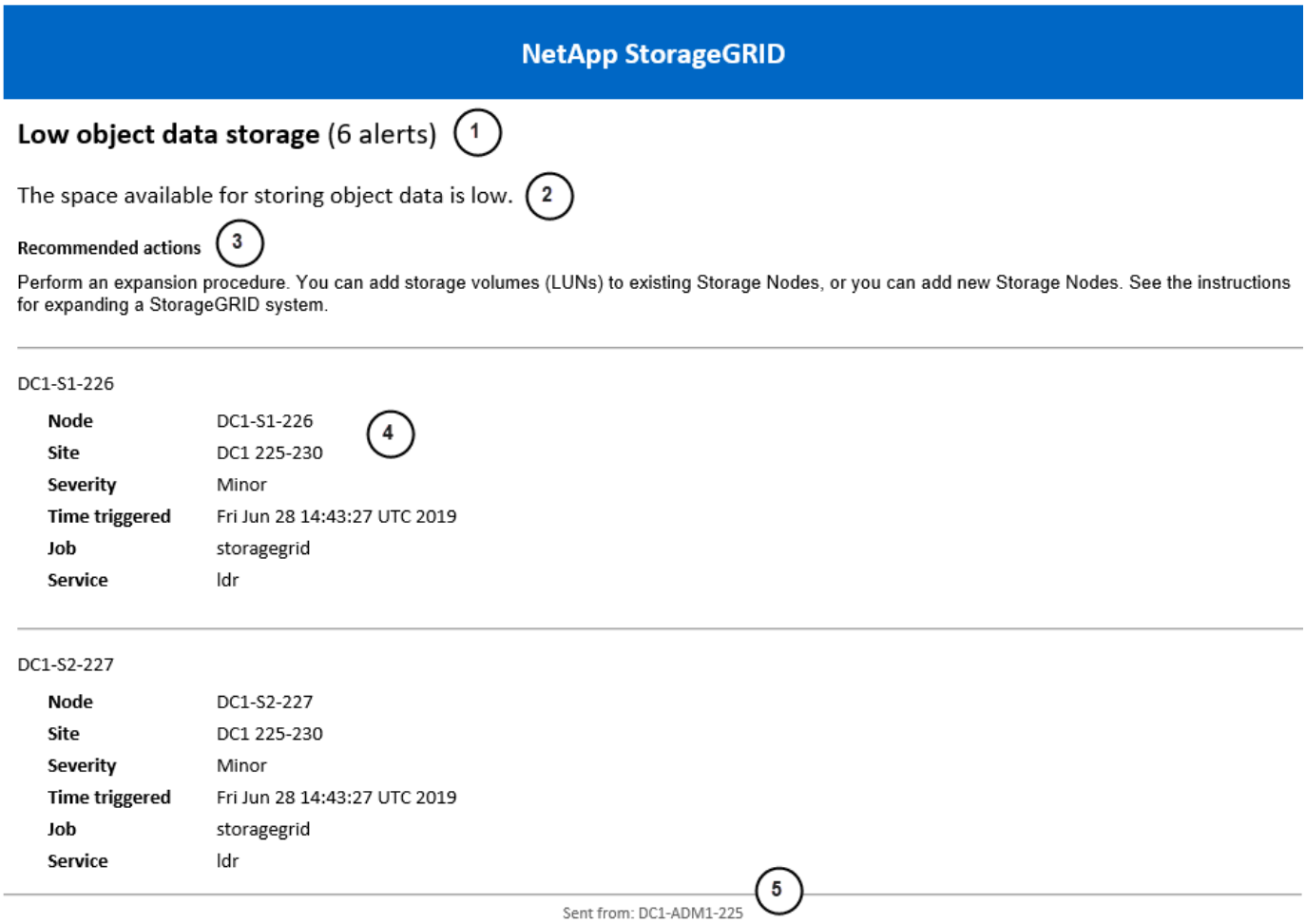
   发送测试电子邮件不会保存您的设置。您必须选择 * 保存 * 。

   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。

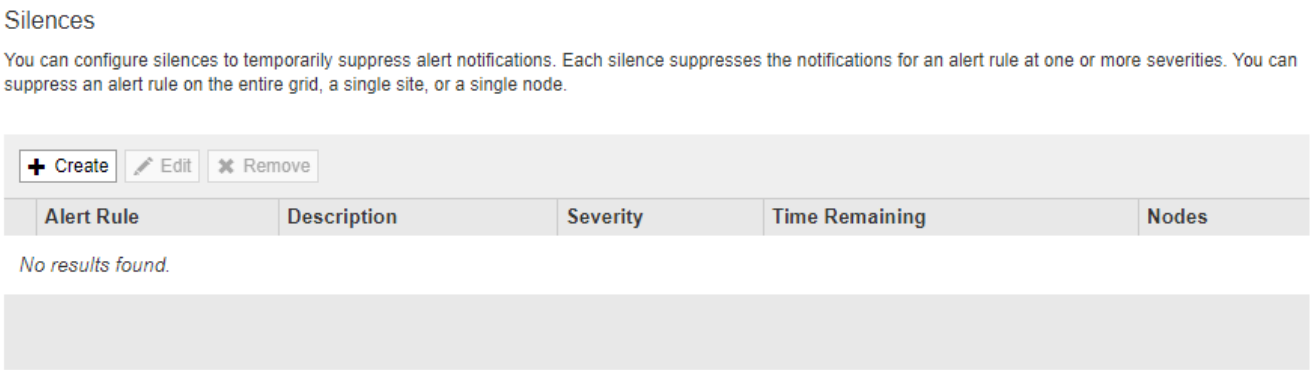
> 在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

> 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

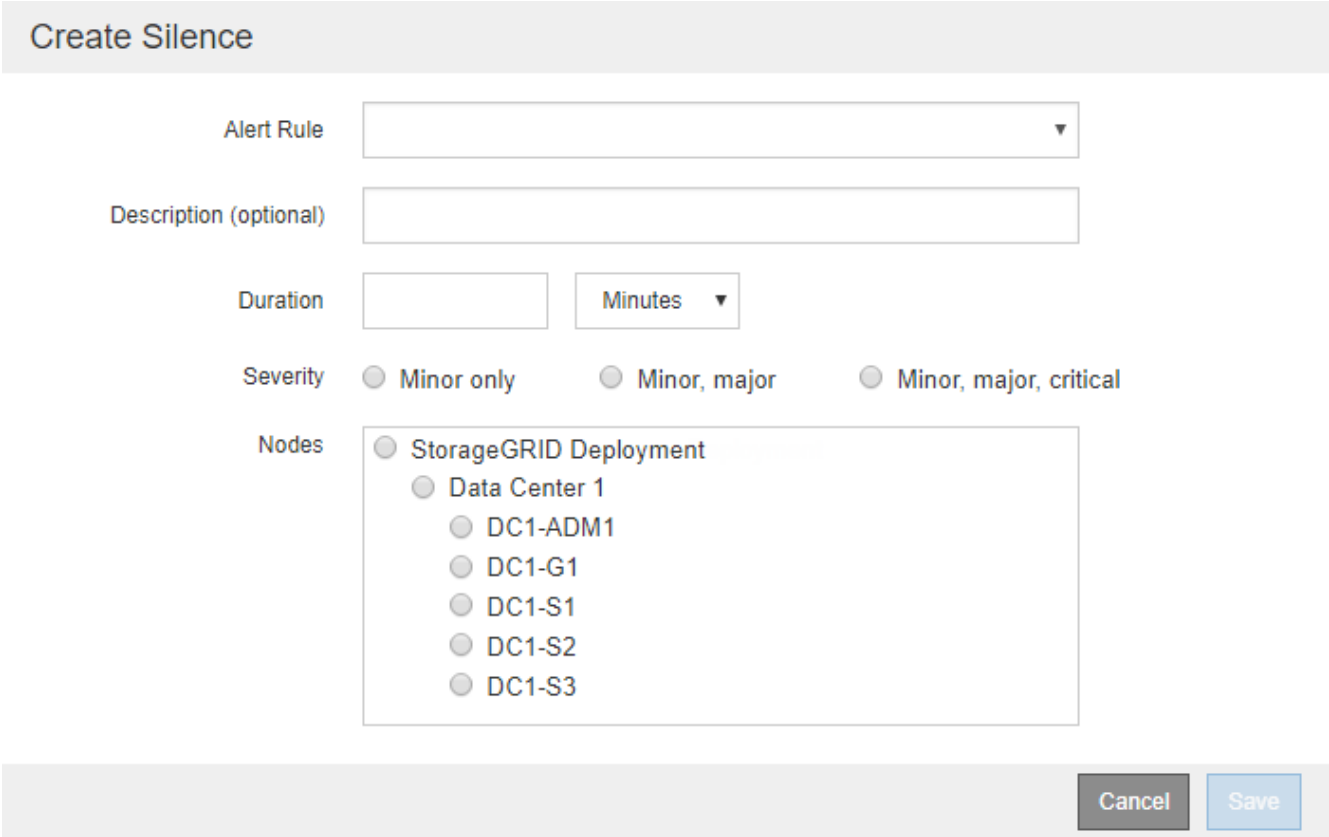
1. 选择 * 警报 * > * 静音 * 。

   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。

警报名称	Description
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。
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。

警报名称	Description
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。
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。
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。

警报名称	**Description**
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。

警报名称	**Description**
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。
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。

警报名称	Description
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。

警报名称	Description
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。
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。

警报名称	Description
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。
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。
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。

警报名称	Description
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"。

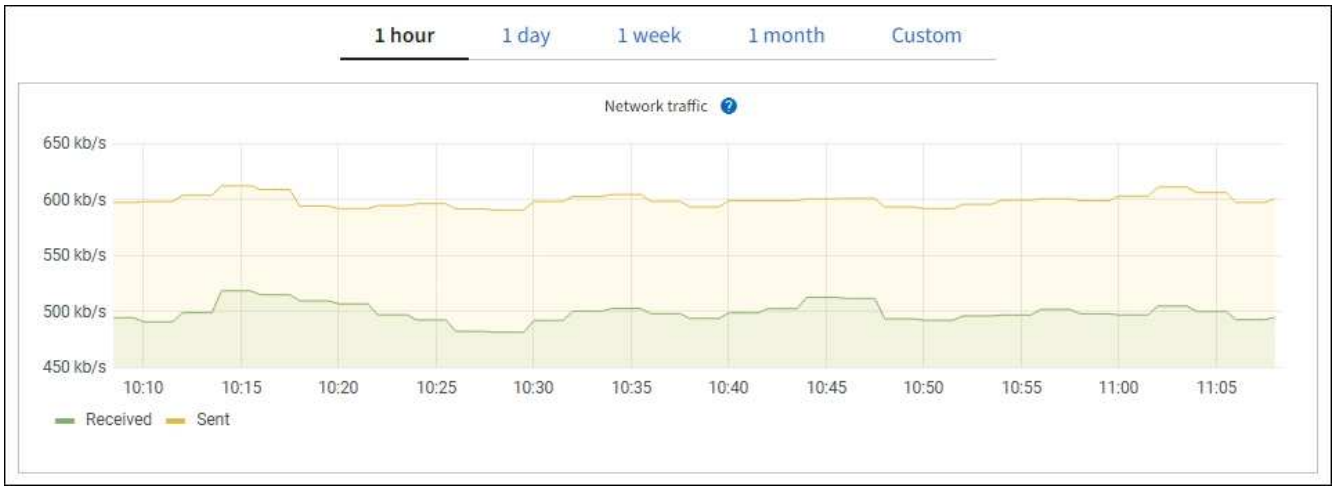
什么是Prometheus指标?

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。

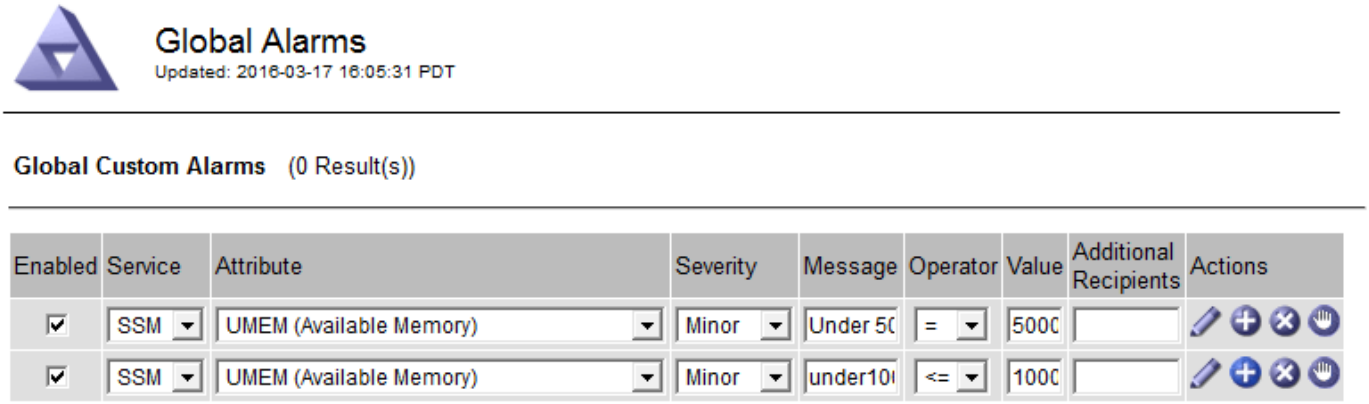
在上述情形之后，如果禁用了全局自定义警报，则不会发生任何更改。在触发新的警报级别之前，必须重新评估属性值。

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。

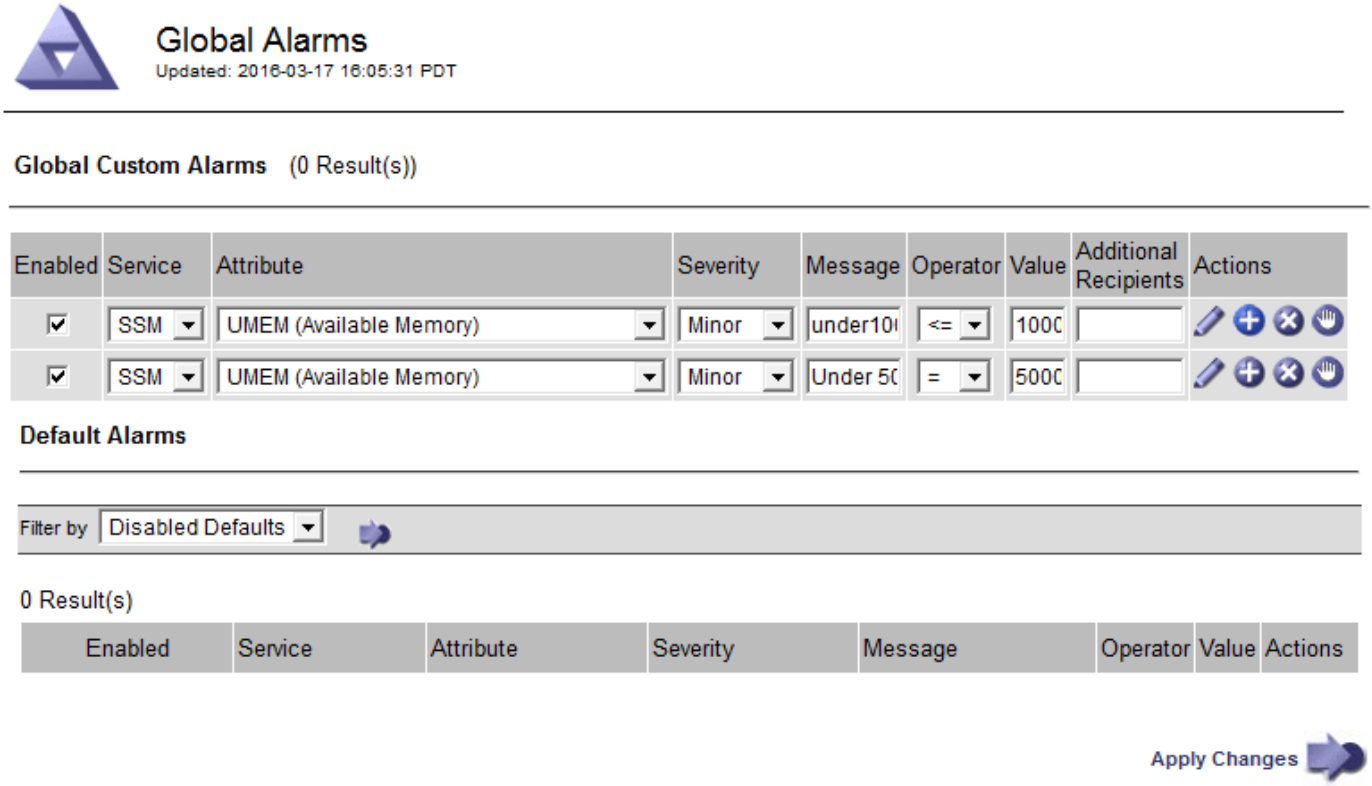
严重性相同的警报

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 ）。



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



通知

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

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

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

新服务

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

警报和表

表中显示的警报属性可以在系统级别禁用。不能为表中的单个行禁用警报。

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 * 。

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

Current Alarms

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

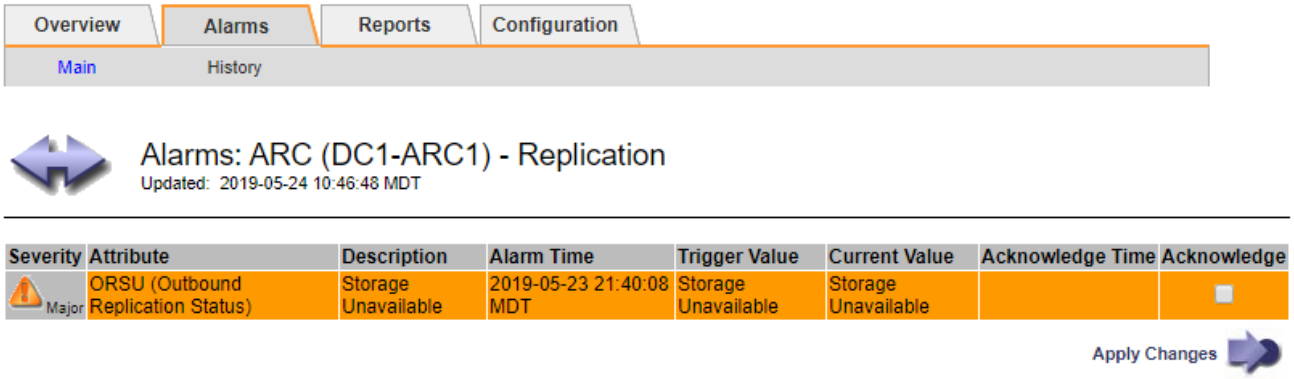
Show Acknowledged Alarms (1 - 1 of 1)

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

Show 50 Records Per Page Refresh Previous « 1 » Next

2. 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。

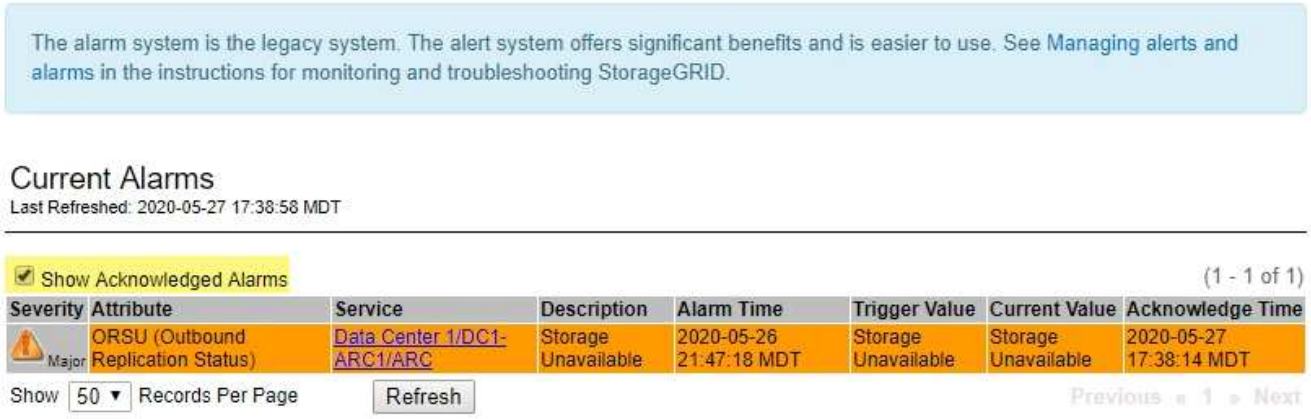
   > 确认警报后，确认不会复制到其他管理节点。因此、如果您从其他管理节点查看信息板、则可能仍会看到活动警报。

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

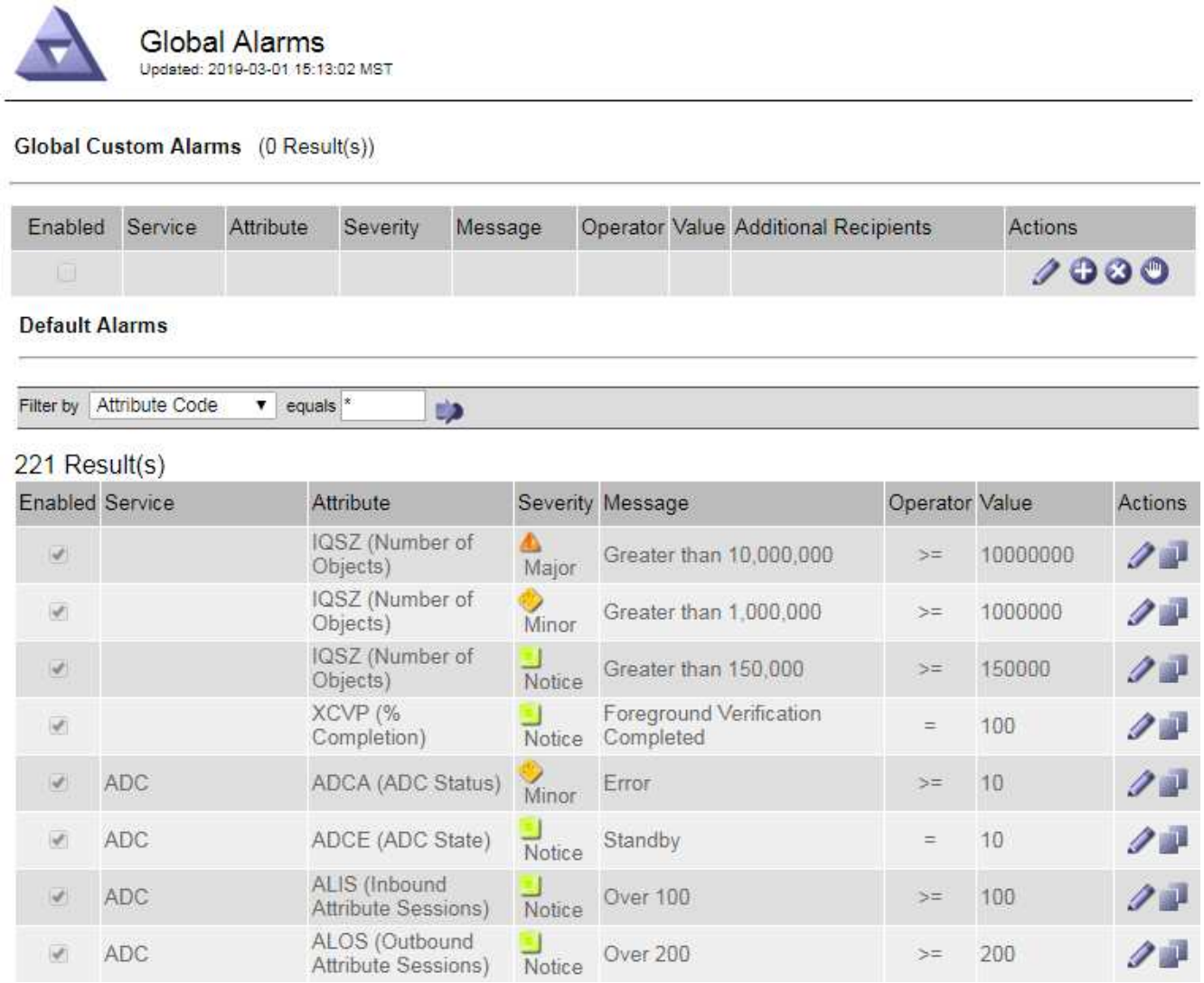
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

> 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"。

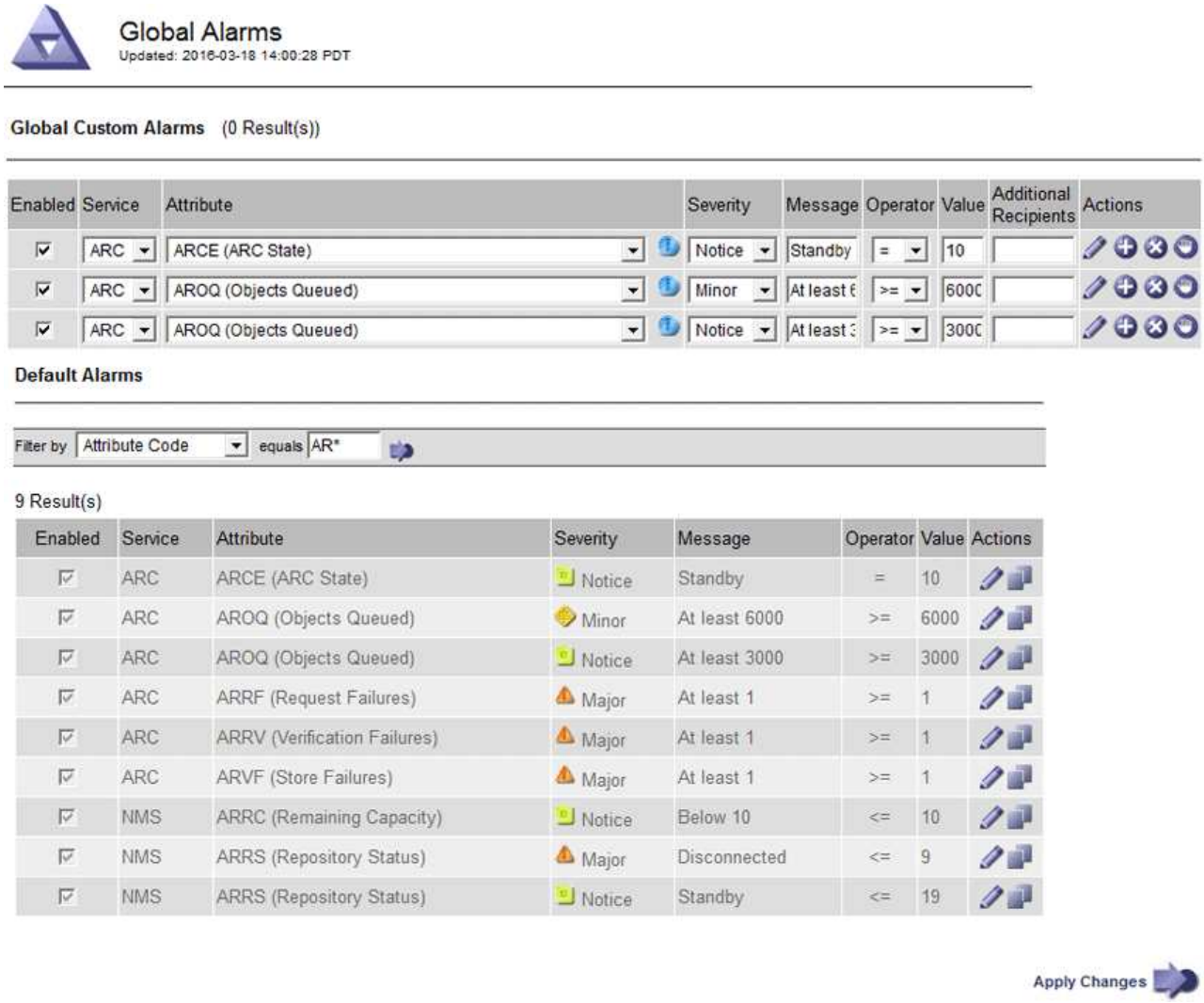
> 虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

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

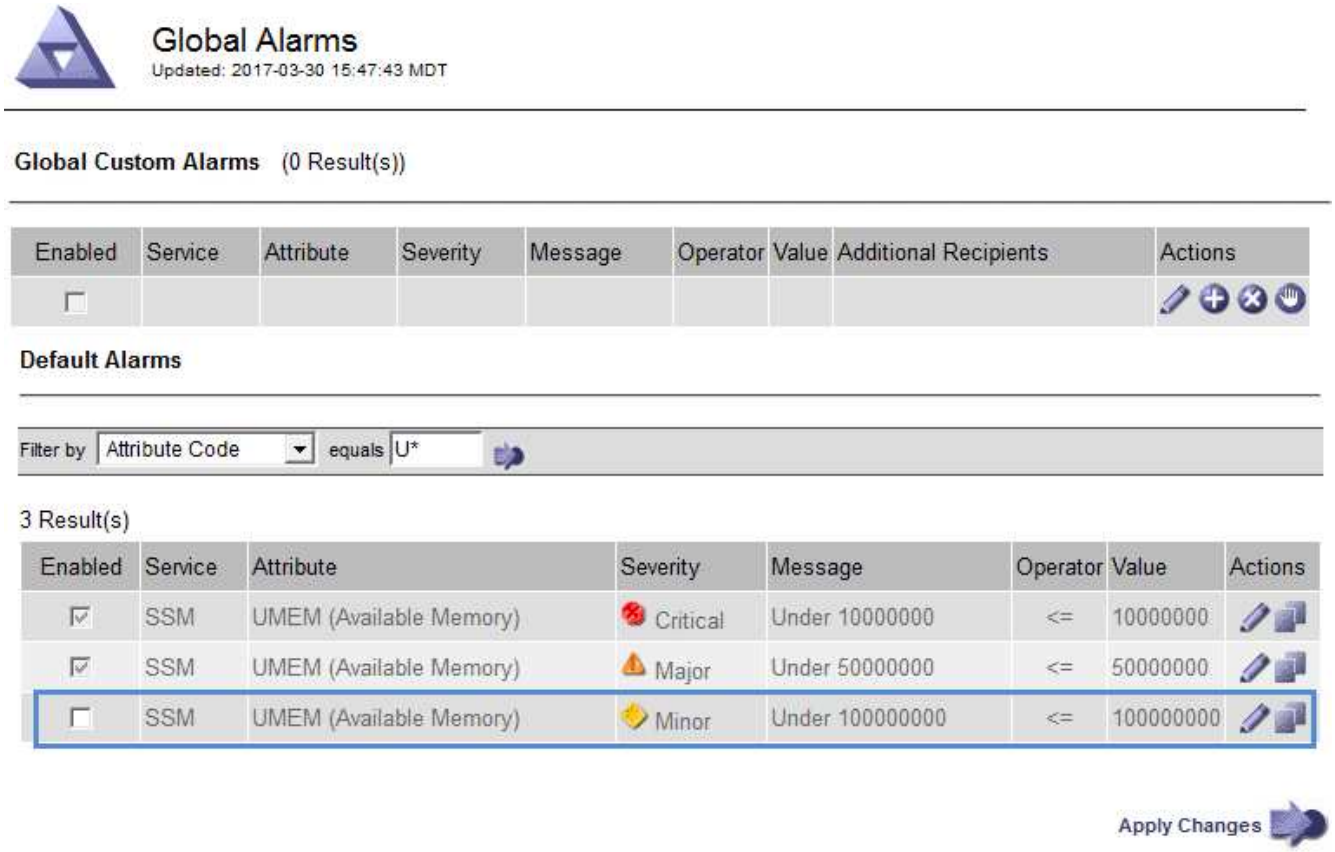
1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 搜索要禁用的默认警报。
   a. 在默认警报部分中，选择 * 筛选依据 * > * 属性代码 * 或 * 属性名称 * 。
   b. 键入搜索字符串。

      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

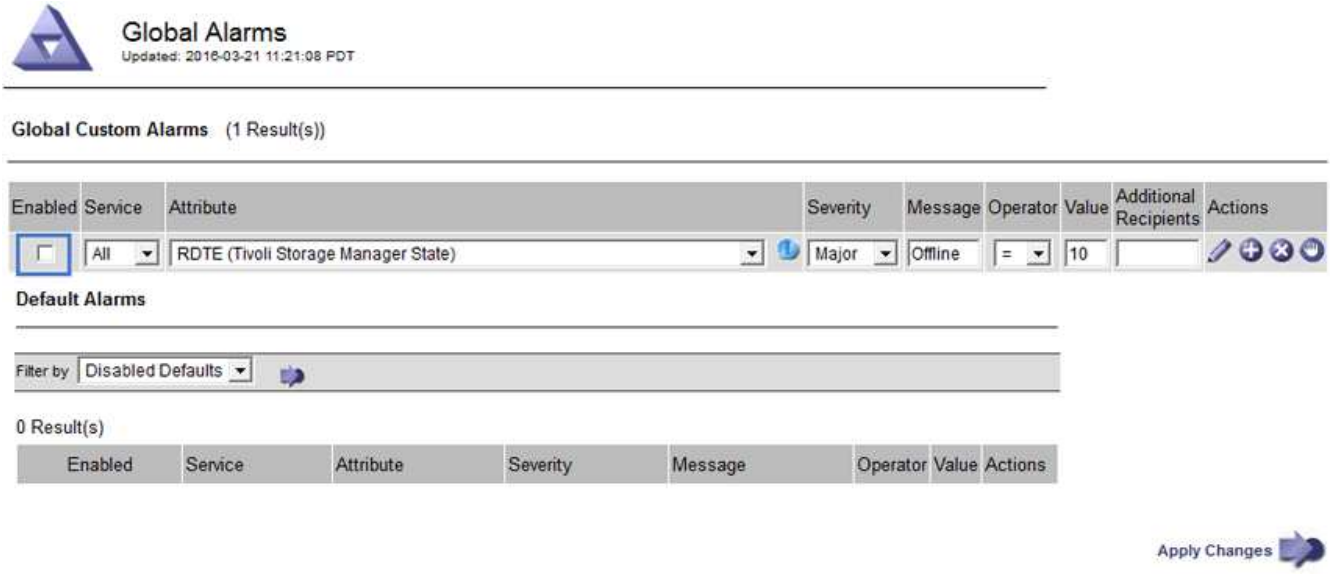
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。

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。

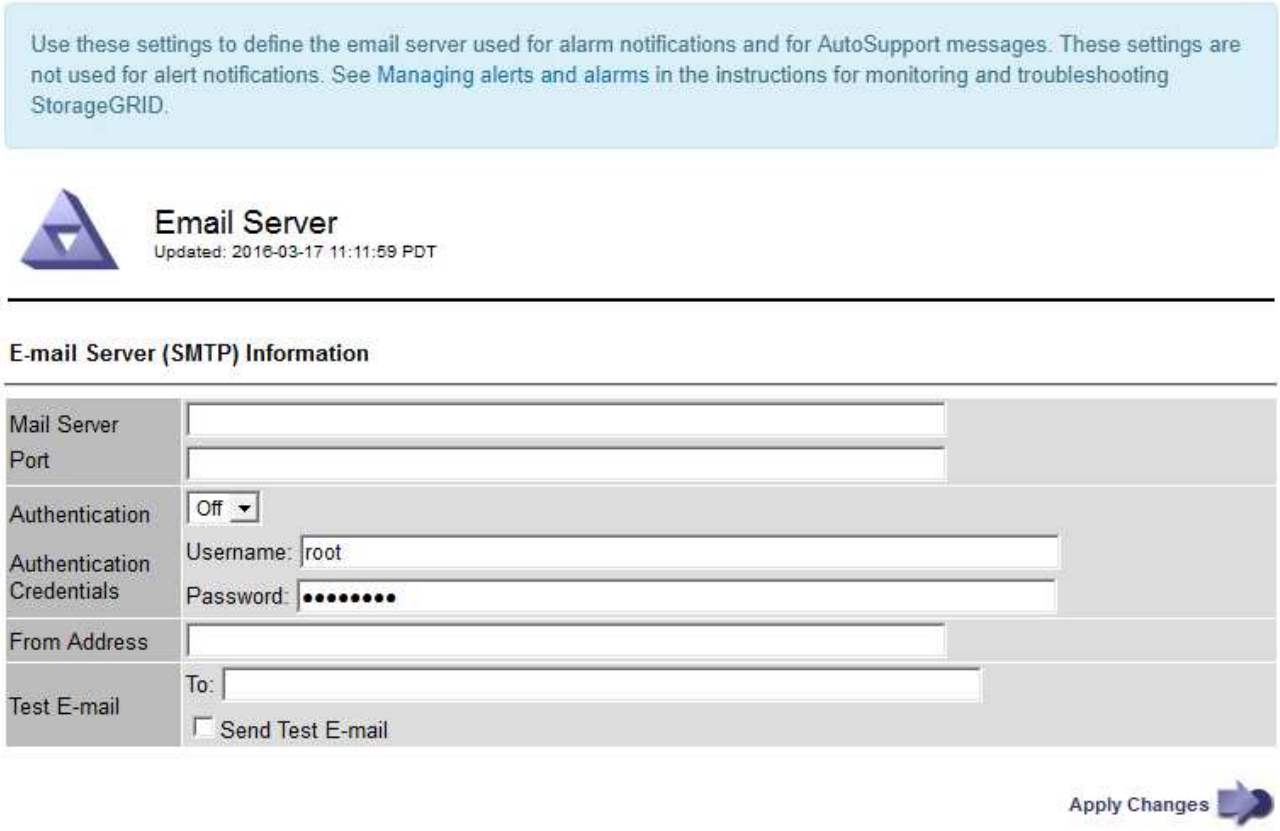
> 如果使用SMTP作为AutoSupport包的协议、则可能已配置SMTP邮件服务器。同一个 SMTP 服务器用于警报电子邮件通知，因此您可以跳过此操作步骤 。请参见 "有关管理 StorageGRID 的说明"。

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"。

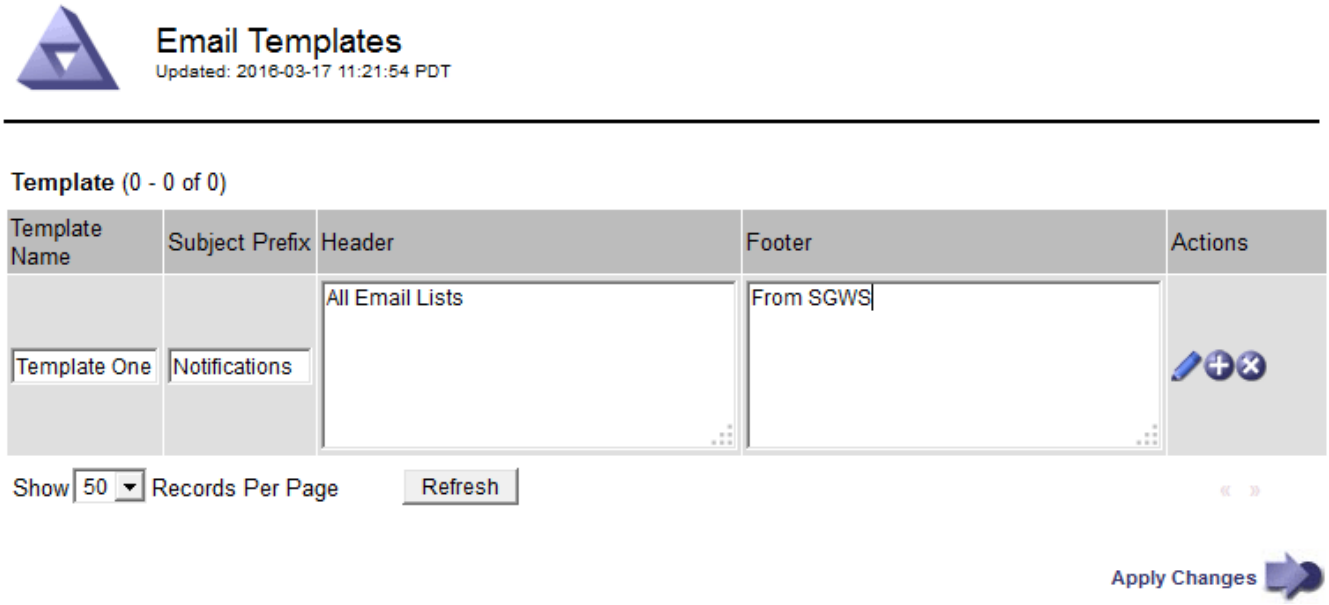
关于此任务

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

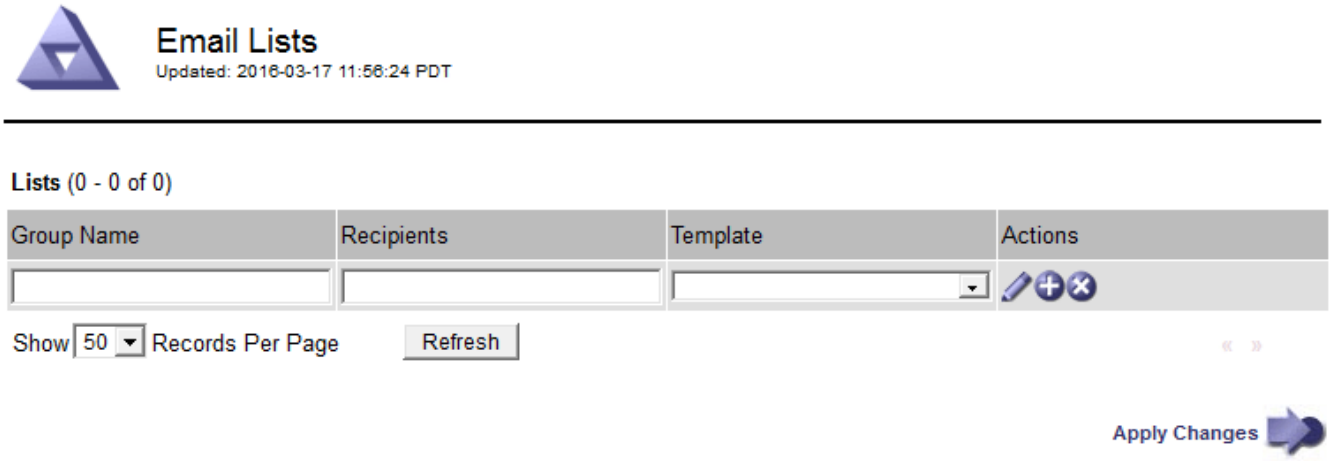
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 如果要为邮件列表指定电子邮件模板（自定义页眉，页脚和主题行），则必须已创建此模板。

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。

查看旧警报

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

> 虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

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

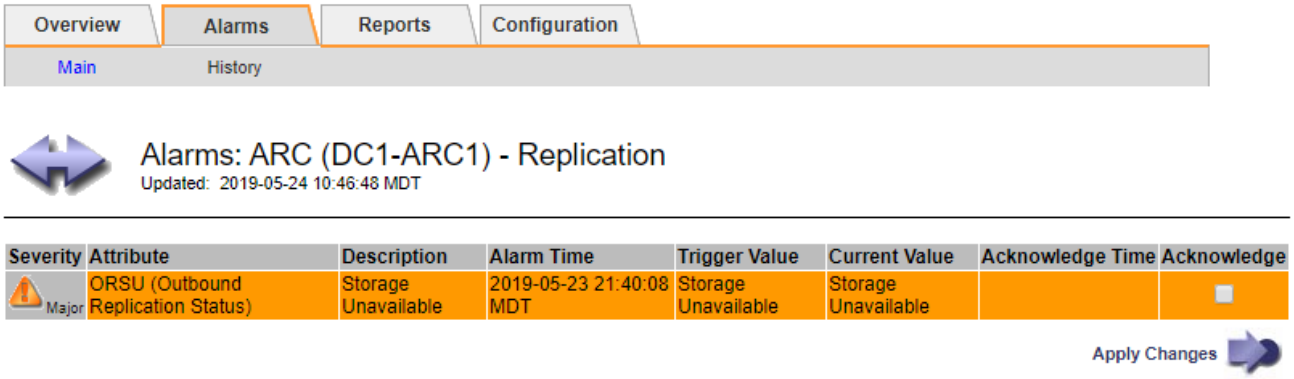
1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。

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）。

如何估算外部系统日志服务器的大小

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

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

在估计公式中使用每秒 S3 操作数

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

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

审核日志的估计公式

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

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

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

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

代码	字段	**Description**
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3存储分段	S3 存储分段名称。

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. 如果收到任何错误，请更正这些错误，然后再次选择 * 发送测试消息 * 。

   请参见 "对外部系统日志服务器进行故障排除" 以帮助您解决任何错误。

4. 请等待，直到看到一个绿色横幅，指示所有节点均已通过测试。
5. 检查系统日志服务器以确定是否按预期接收和处理了测试消息。

   > 如果使用的是 UDP ，请检查整个日志收集基础架构。UDP协议不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。

> 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
仅限本地节点	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。
管理节点/本地节点	审核消息会发送到审核日志 (`/var/local/log/audit.log`)、安全事件日志和应用程序日志存储在生成这些日志的节点上。
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。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。

选项	Description
管理节点和外部系统日志服务器	审核消息会发送到审核日志 (`/var/local/log/audit.log`)、审核信息将发送到外部系统日志服务器并保存在本地节点上。发送的信息类型取决于您配置外部系统日志服务器的方式。只有在配置了外部系统日志服务器之后，才会启用此选项。

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。
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。

字段	Description
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

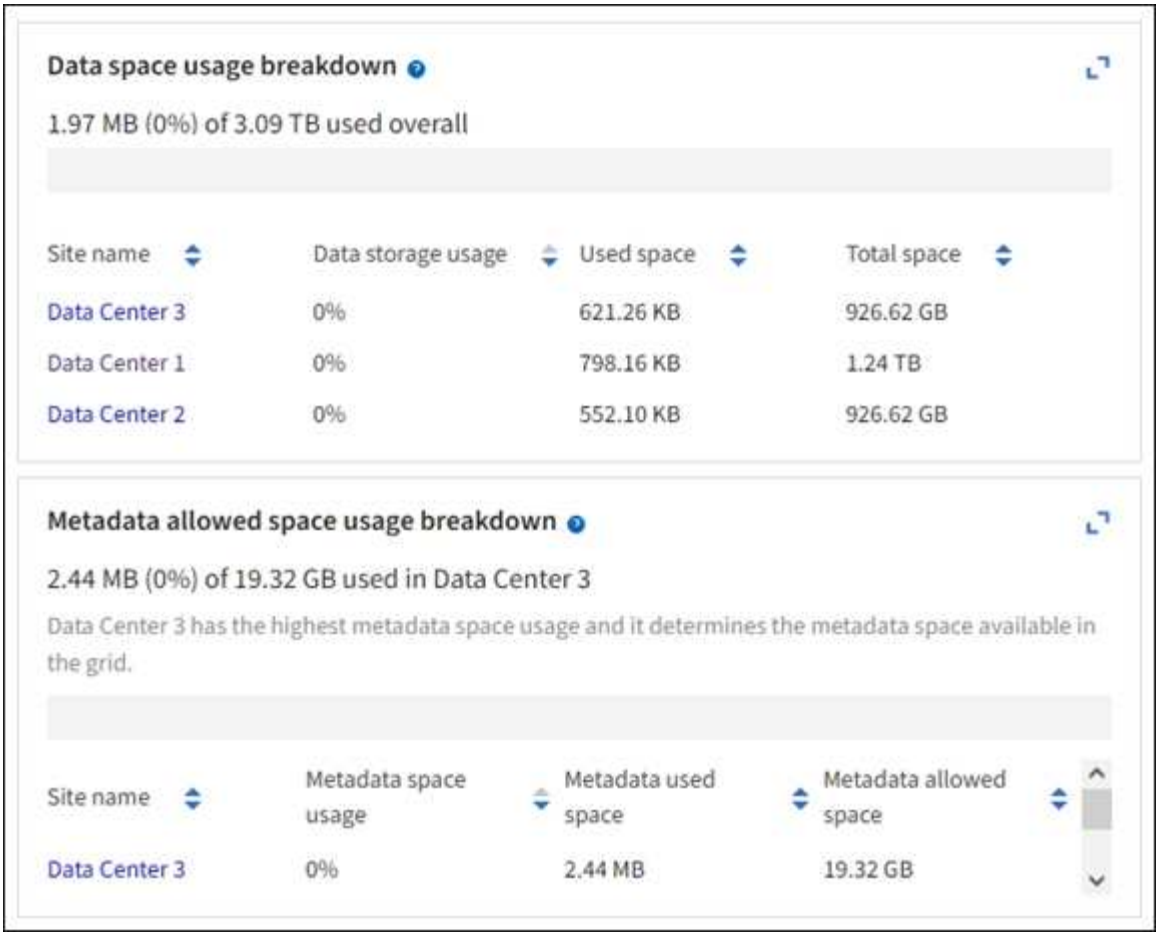
您可以使用图表和报告监控 StorageGRID 系统的状态并对问题进行故障排除。

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

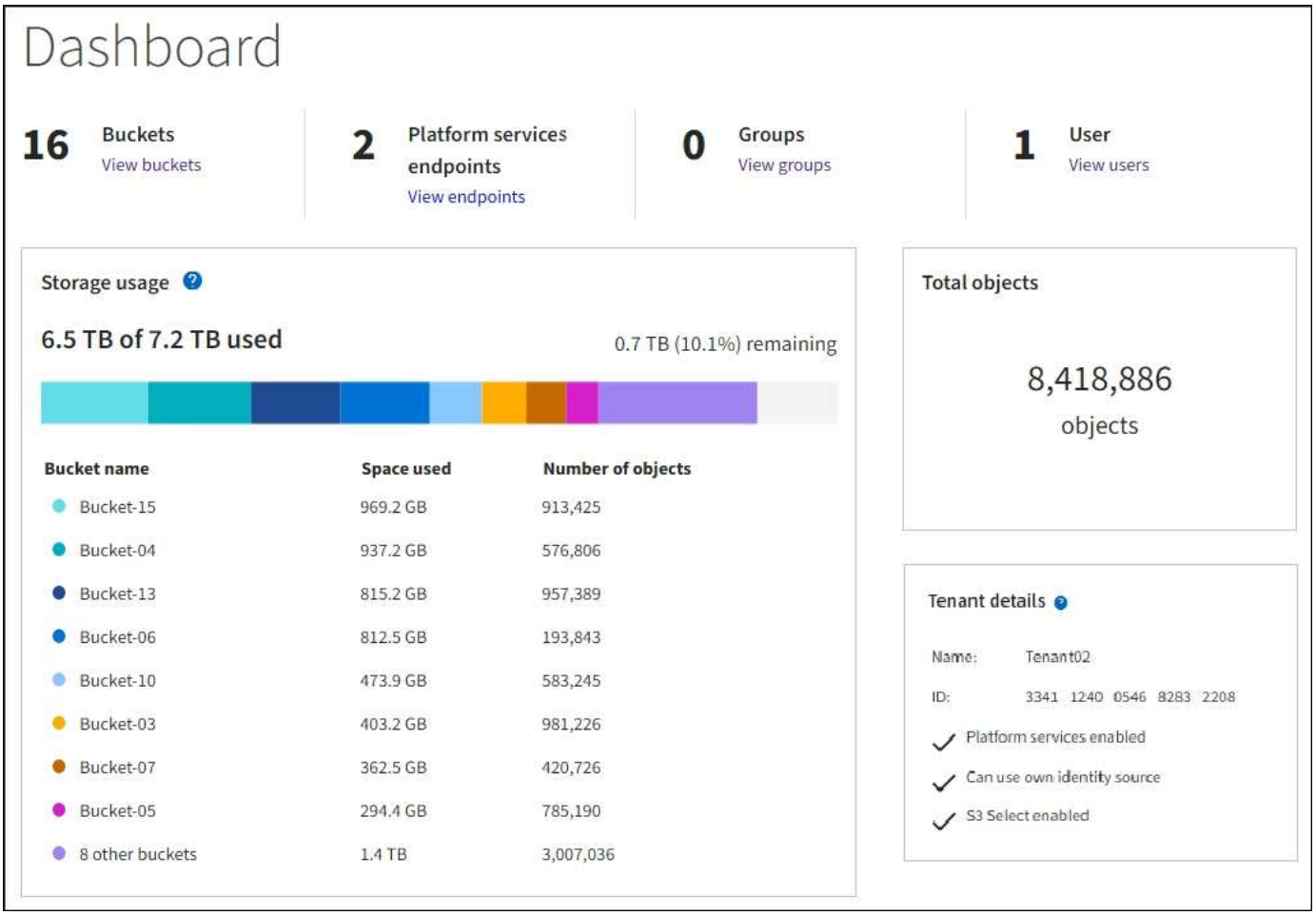
图表和图形汇总了特定 StorageGRID 指标和属性的值。

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：

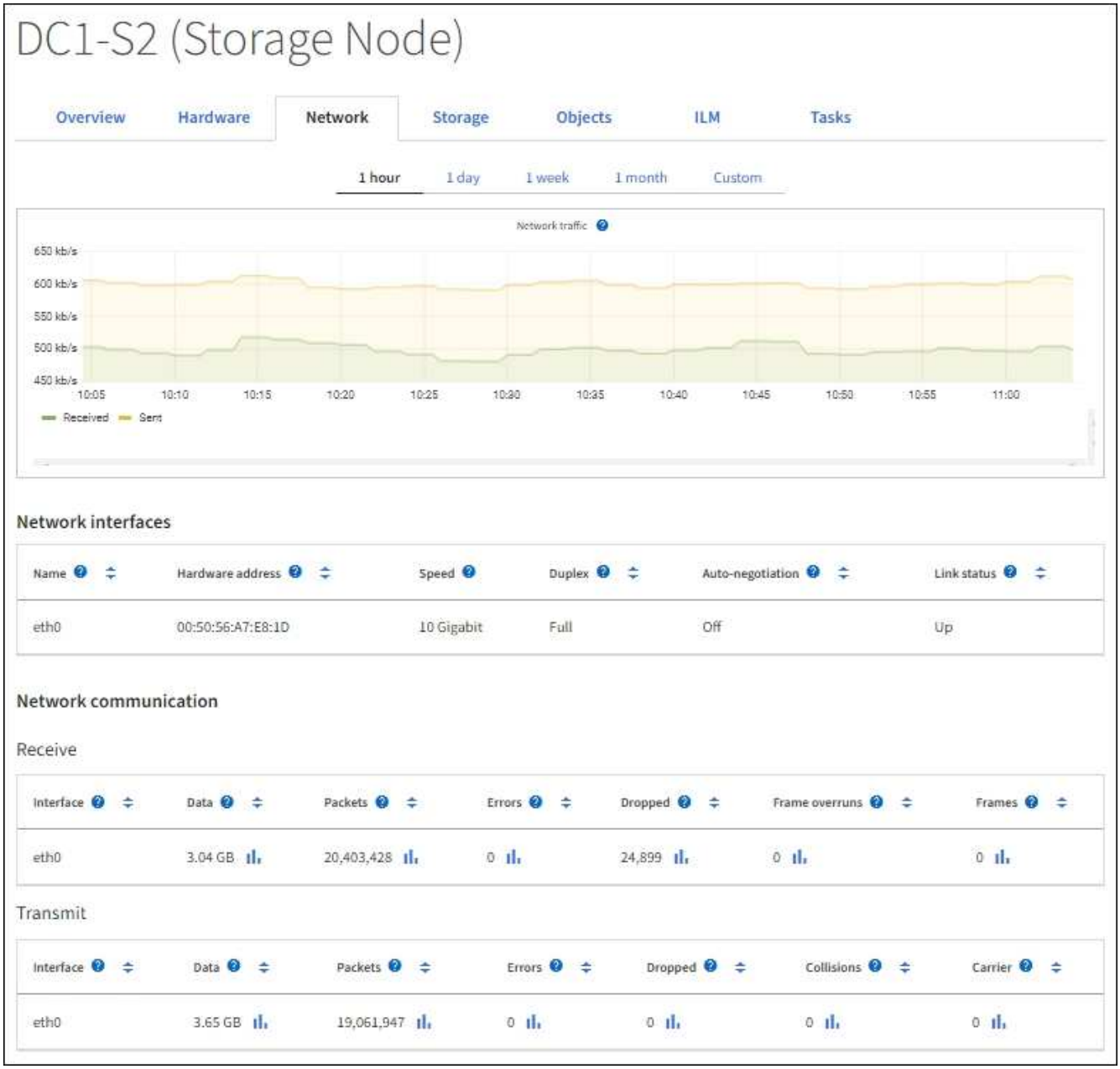
- 租户最大的分段（ S3 ）或容器（ Swift ）列表
- 一个条形图，表示最大分段或容器的相对大小
- 已用总空间量，如果设置了配额，则还会显示剩余空间量和百分比



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。

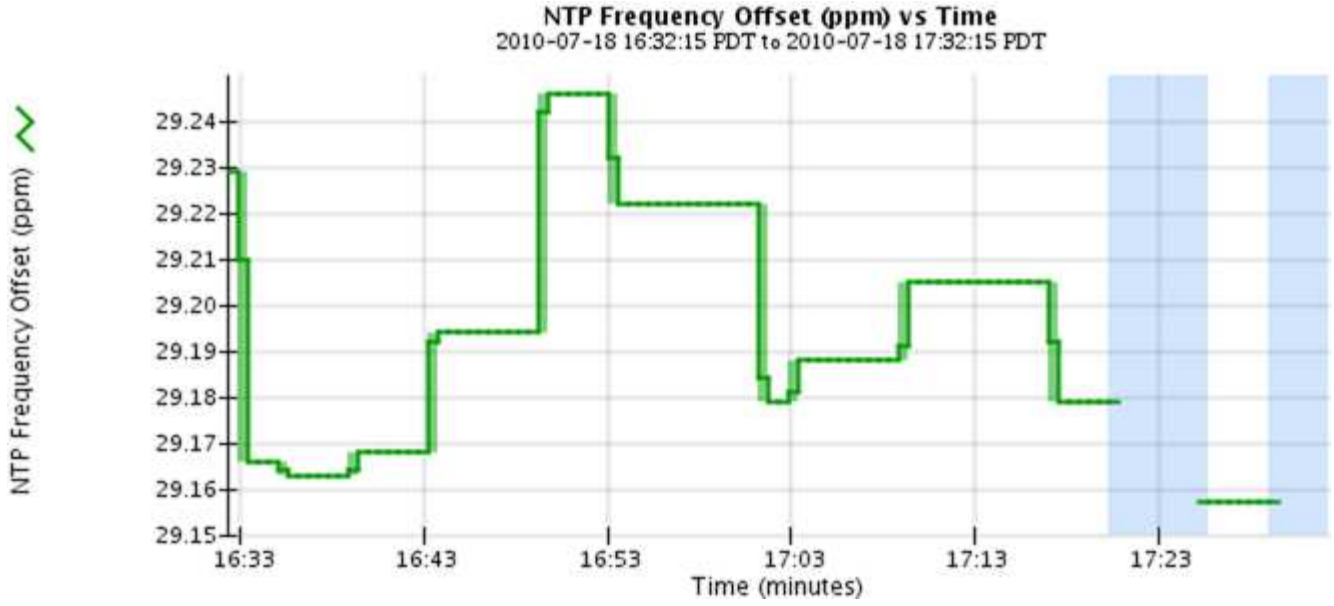
图形有四种类型：

- * 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。

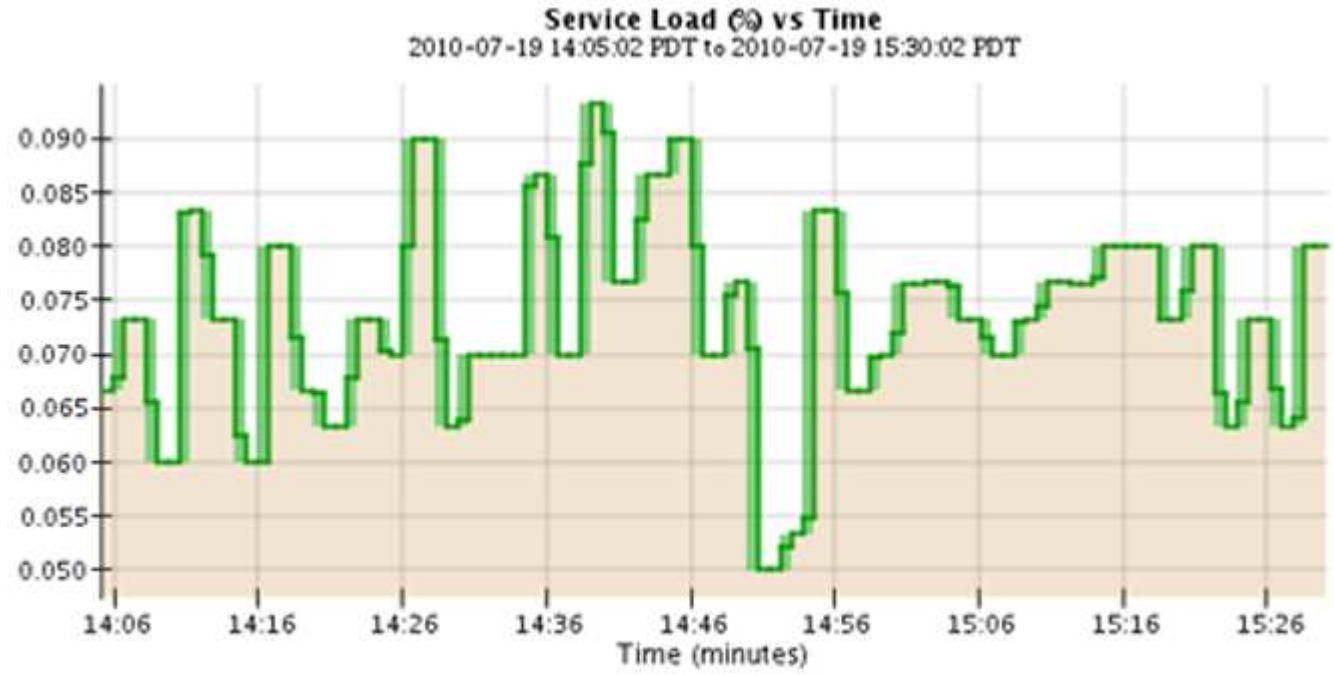


Grafana 图表也包含在预构建的信息板中，这些信息板可从 * 支持 * > * 工具 * > * 指标 * 页面获得。

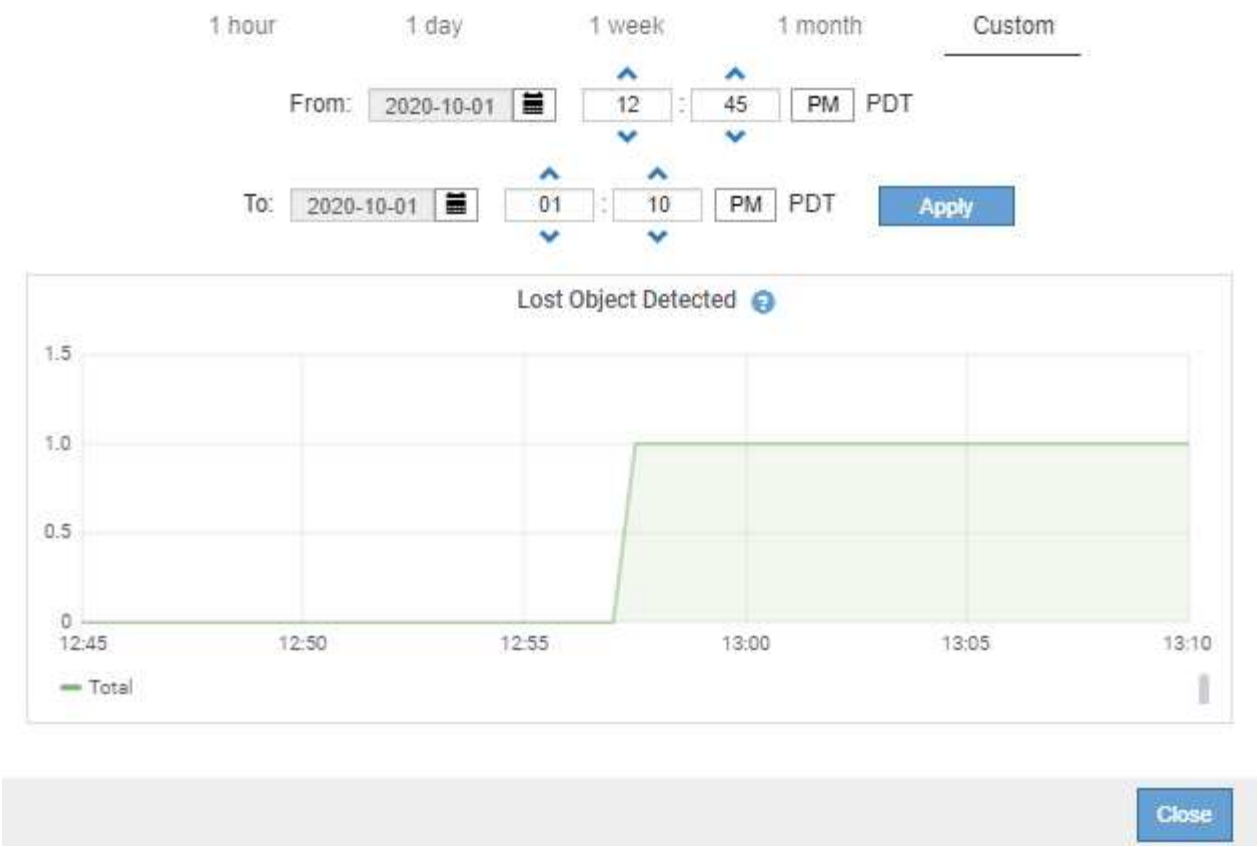
- * 折线图 *： 可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用折线图绘制具有单位值（例如 NTP 频率偏移，以 PPM 为单位）的 StorageGRID 属性值。值的更改会按定期数据间隔（箱）绘制。



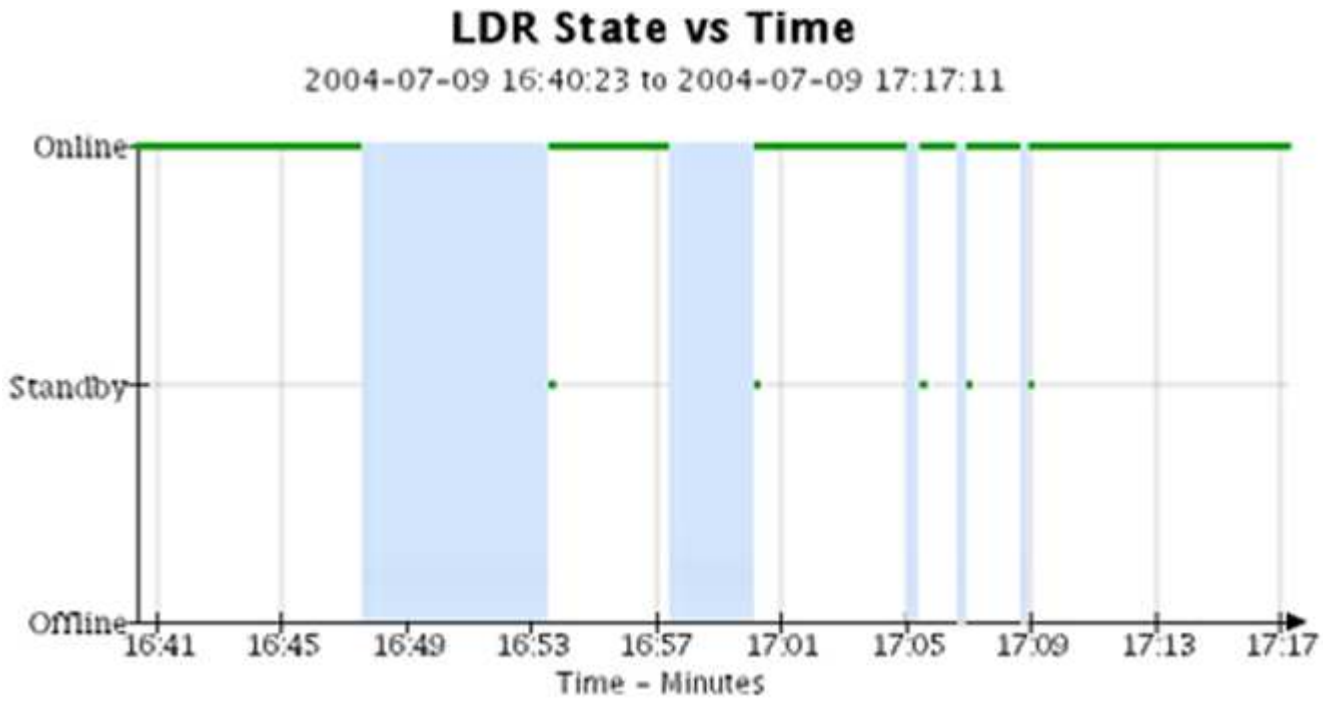
- * 区域图形 *：可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用分区图绘制容量属性数量，例如对象计数或服务负载值。区域图形与折线图类似，但在折线下方会显示浅棕色阴影。值的更改会按定期数据间隔（箱）绘制。



- 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

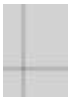
"查看节点页面"

"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。

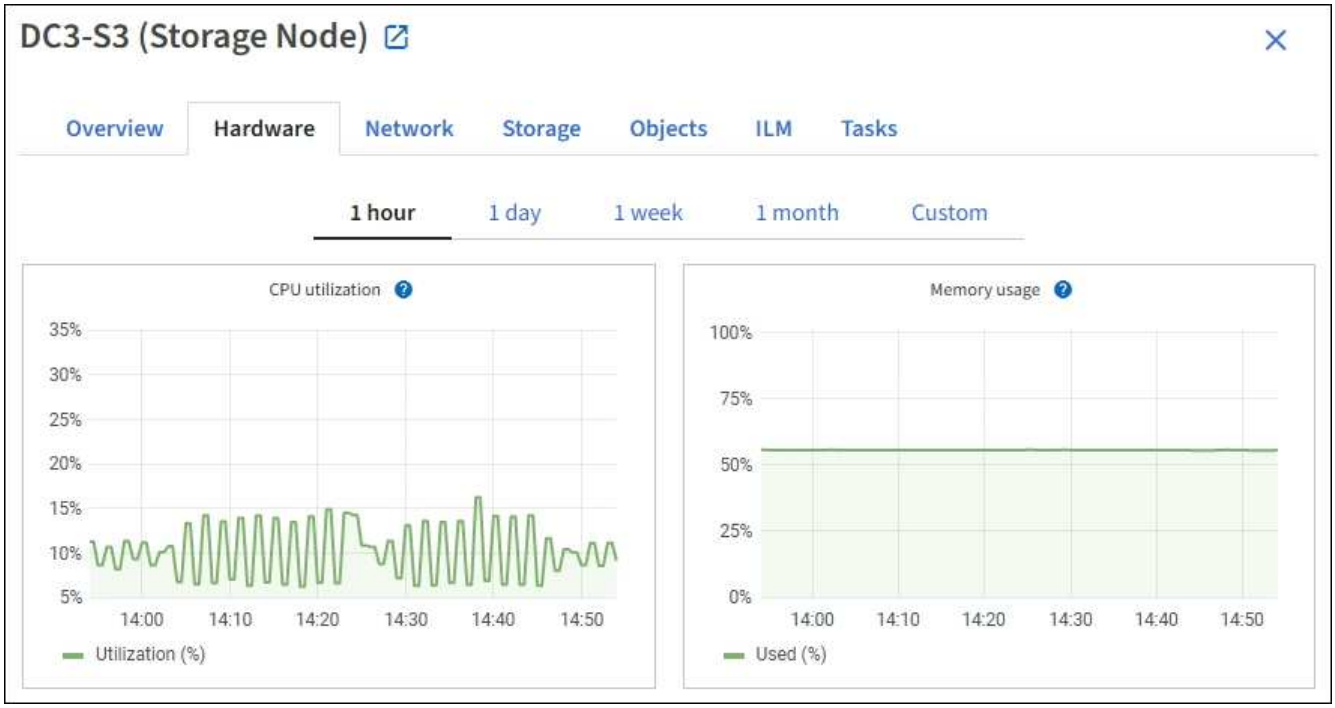
开始之前

您必须使用登录到网格管理器 "支持的 Web 浏览器"。

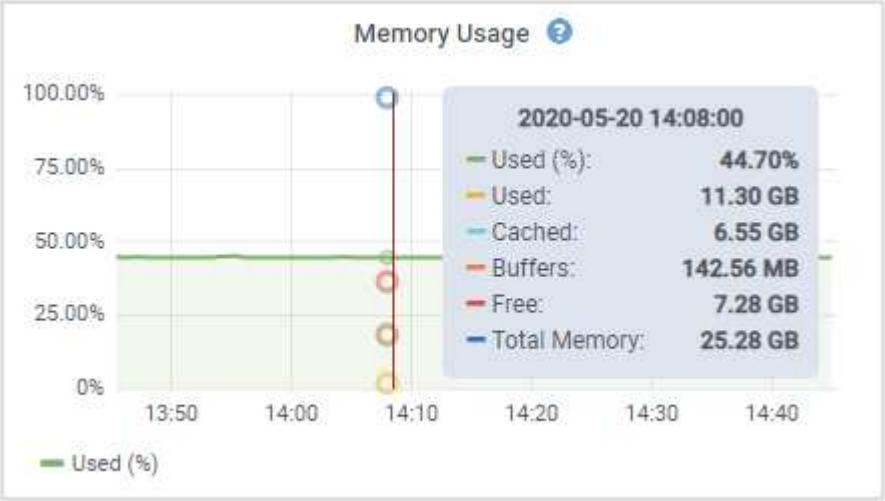
步骤

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。



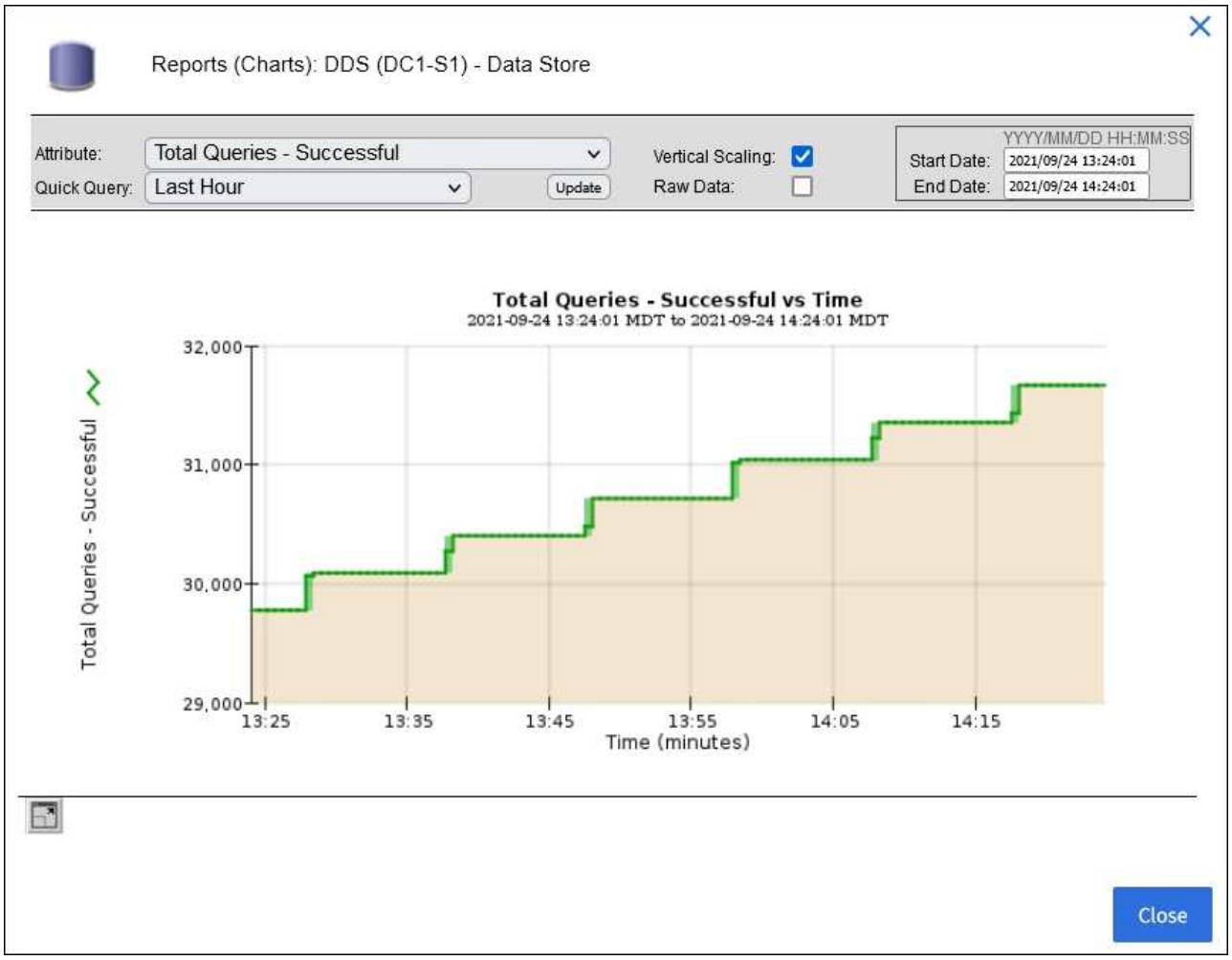
3. (可选)将光标置于图表上方、以查看特定时间点的更多详细值。

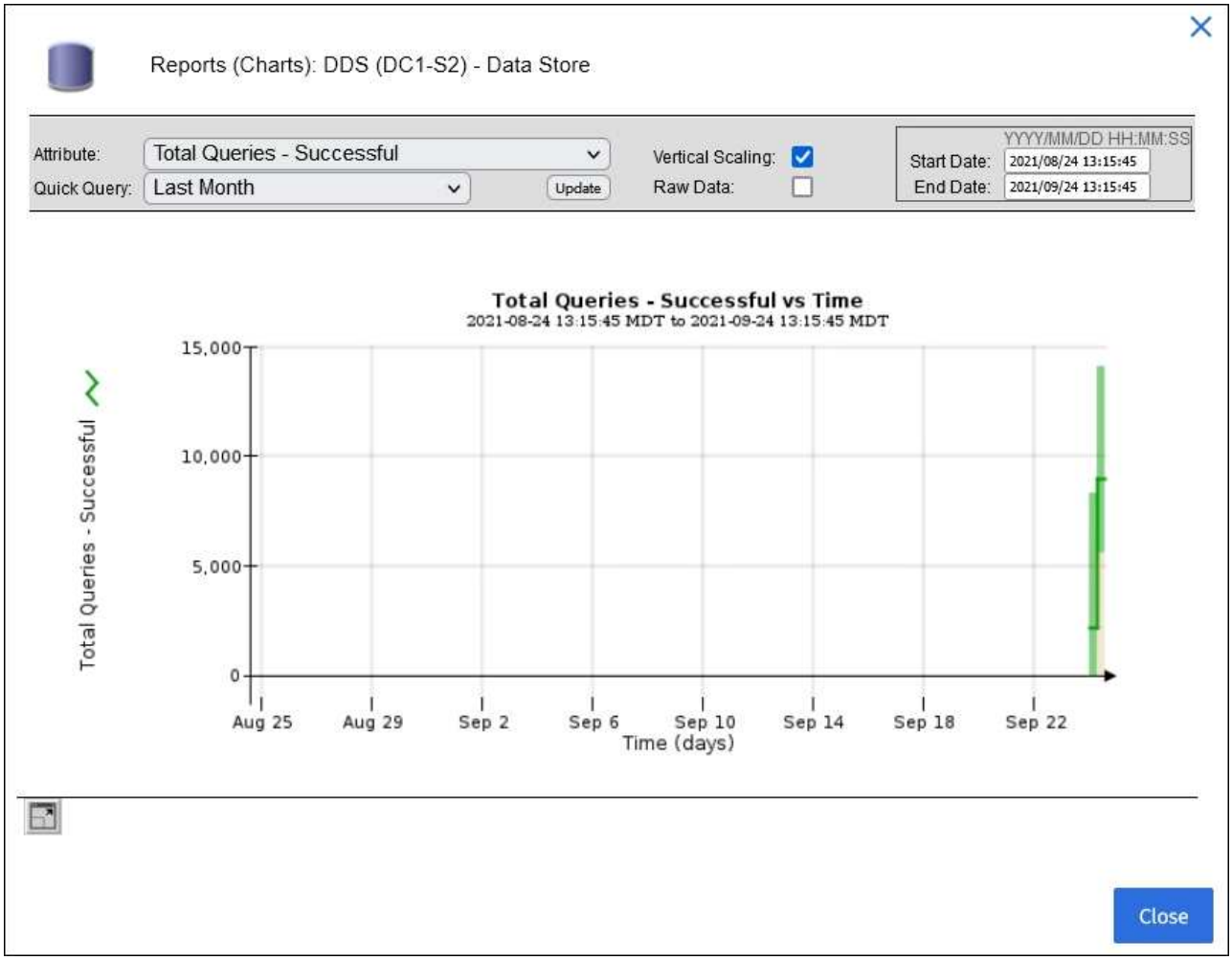


4. 您通常可以根据需要显示特定属性或指标的图表。从节点页面上的表中，选择图表图标 属性名称右侧。

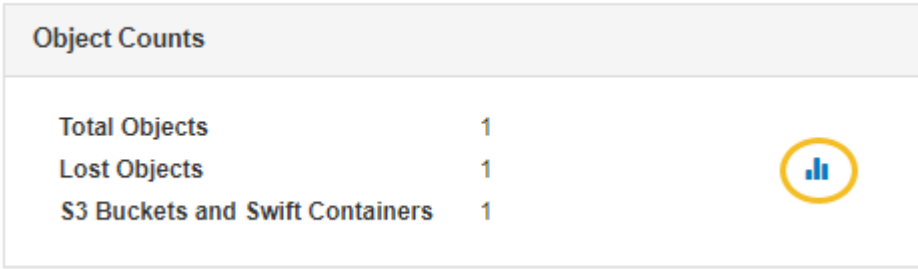
> 图表并非适用于所有指标和属性。

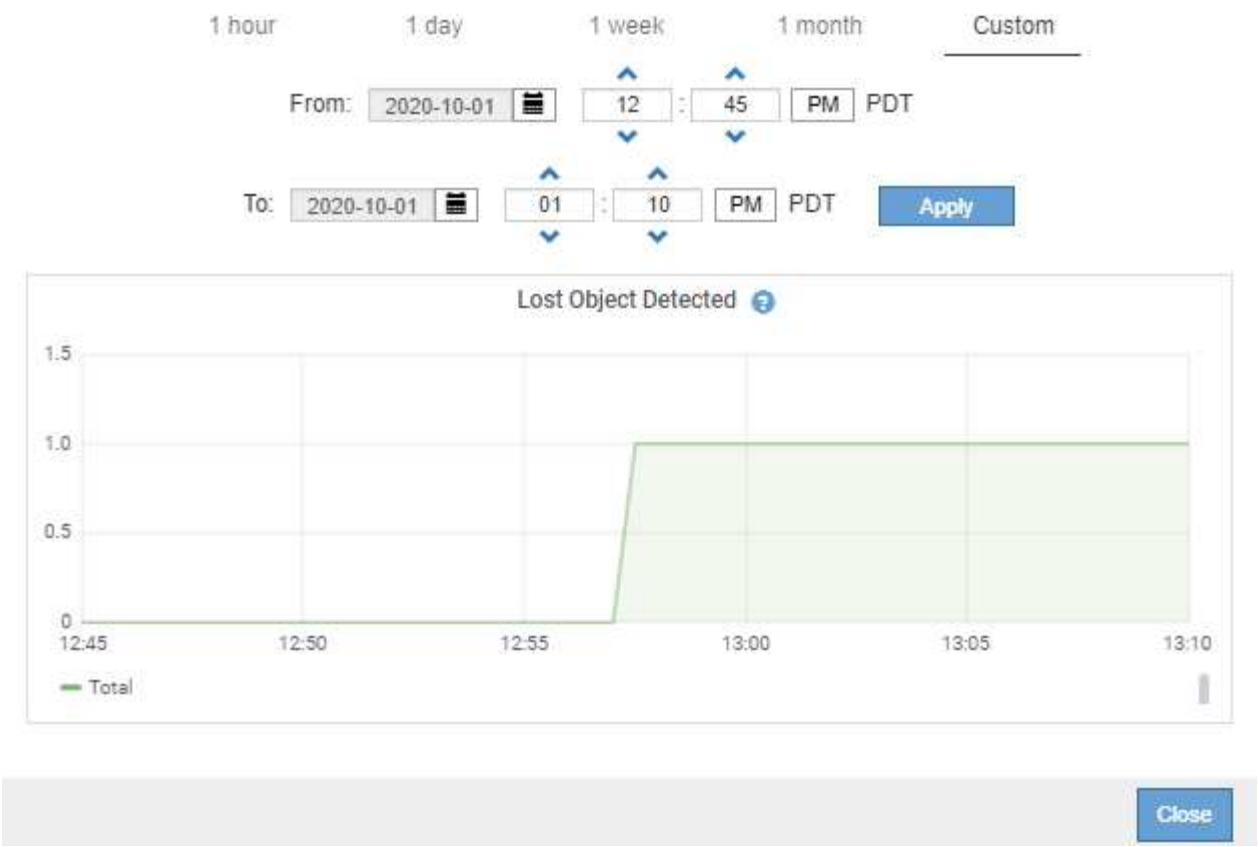
- 示例 1*：从存储节点的对象选项卡中，您可以选择图表图标 可查看存储节点的成功元数据存储查询总数。


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

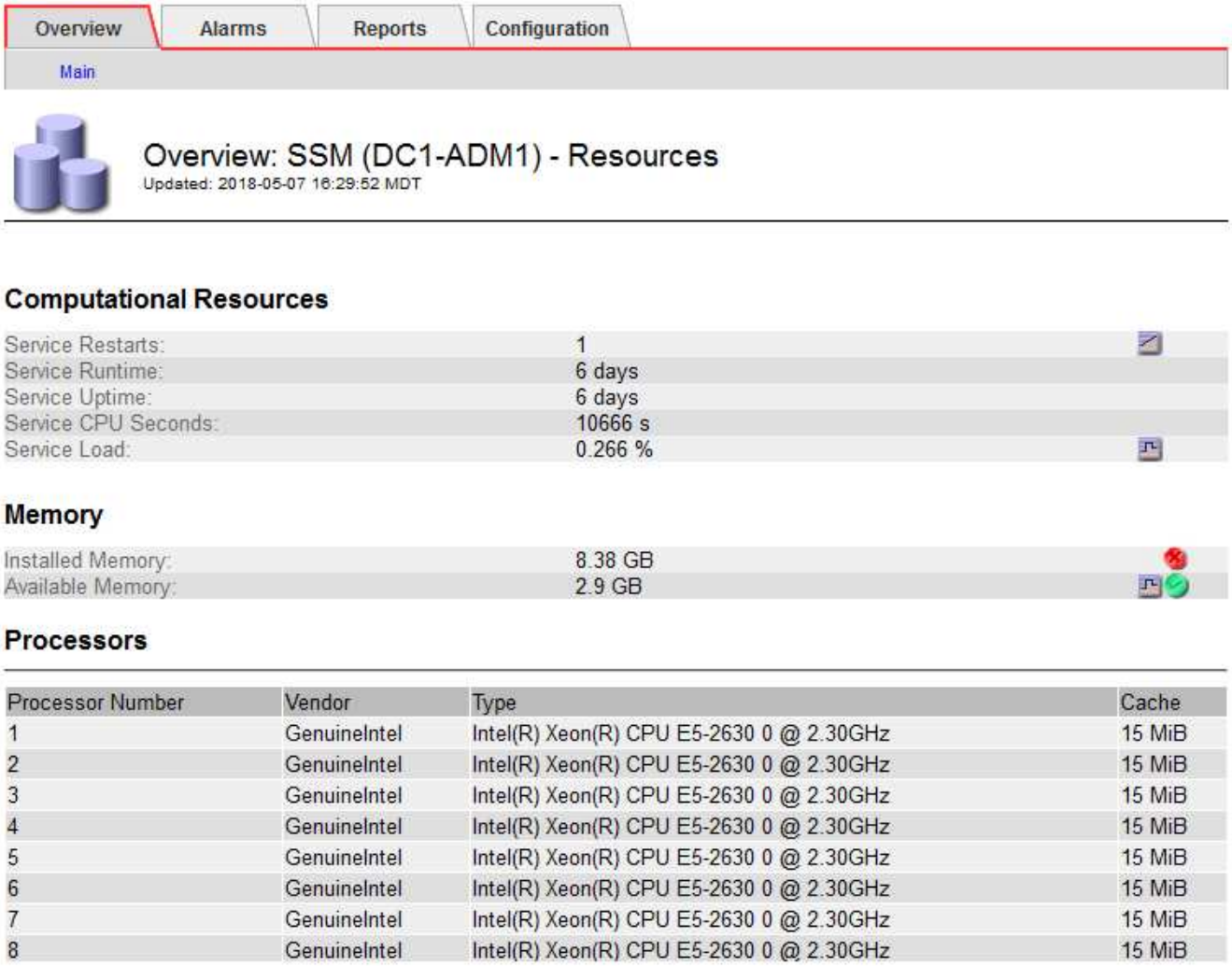


- 示例 2*： 从存储节点的对象选项卡中，您可以选择图表图标 可查看随时间检测到的丢失对象计数的 Grafana 图形。





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

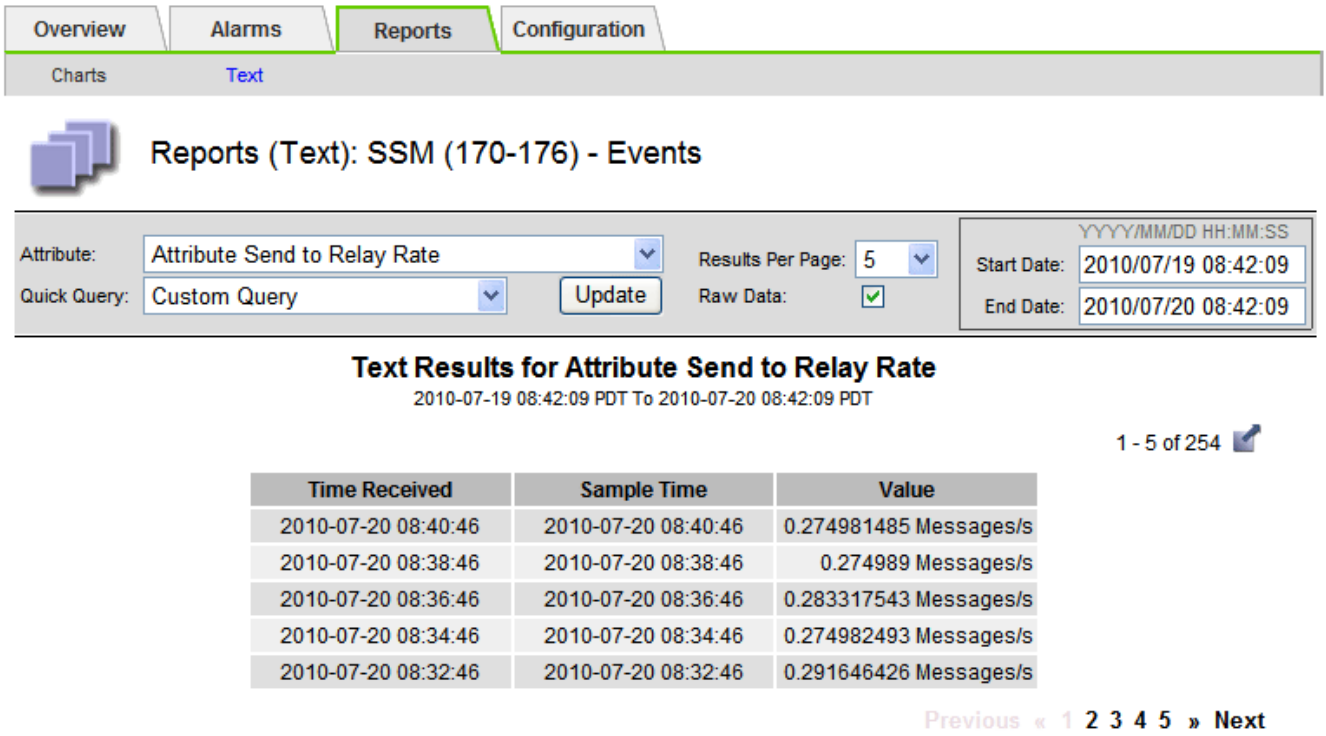
导出的文本报告将打开一个新的浏览器选项卡，在此可以选择和复制数据。

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: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
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"。

监控对象验证操作

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。

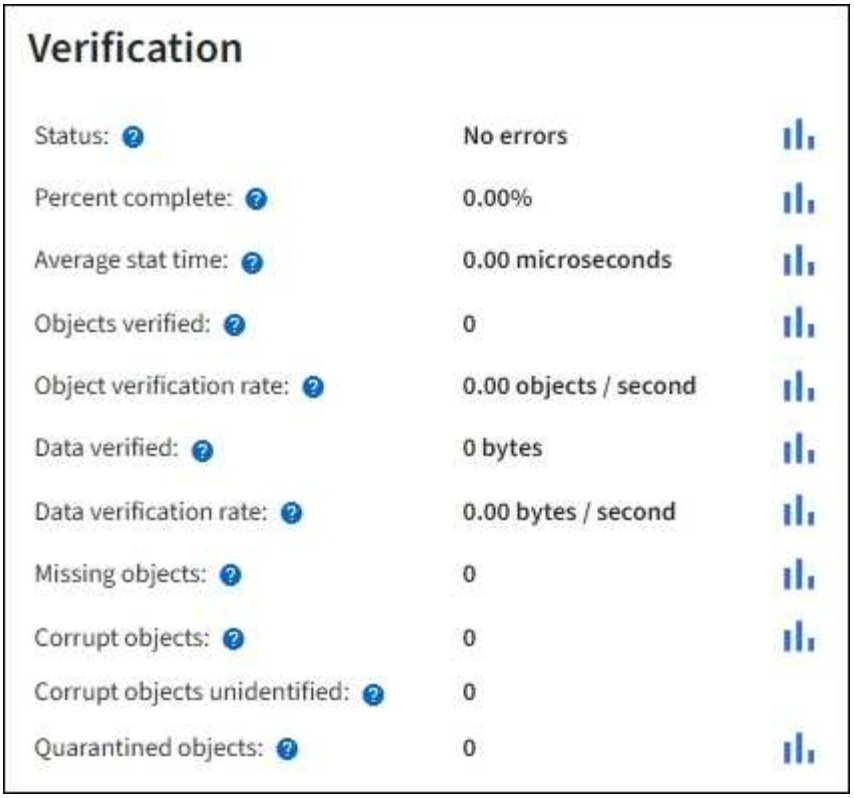
步骤

1. 查看后台验证的结果：

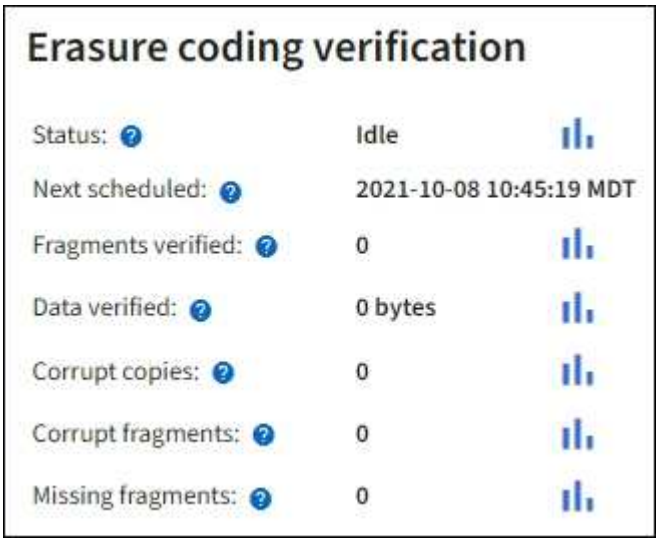
   a. 选择 * 节点 * > * 存储节点 _* > * 对象 * 。

   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。

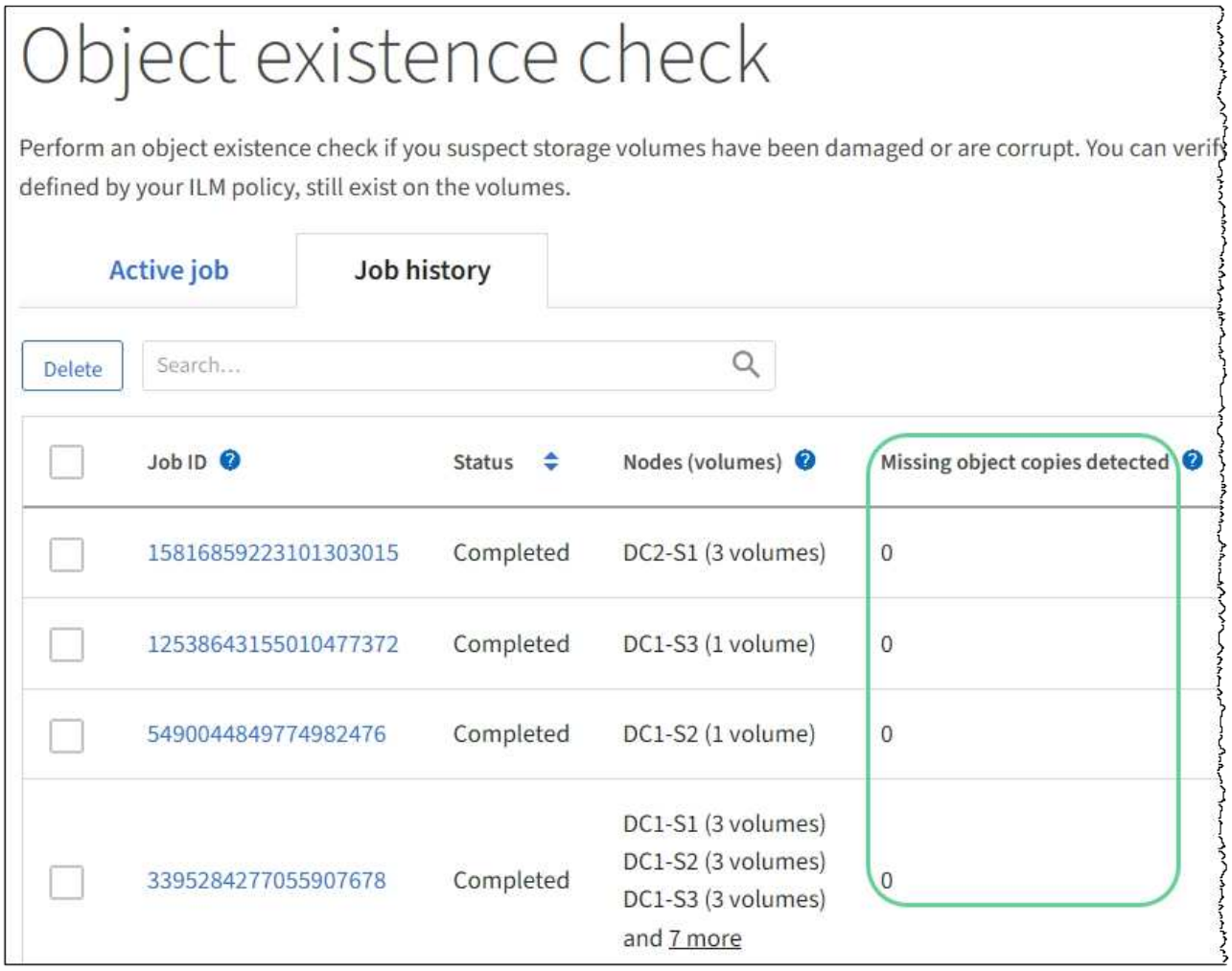


- 要检查擦除编码的片段验证，请选择 * 存储节点 _* > * ILM * ，然后查看擦除编码验证部分中的属性。



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

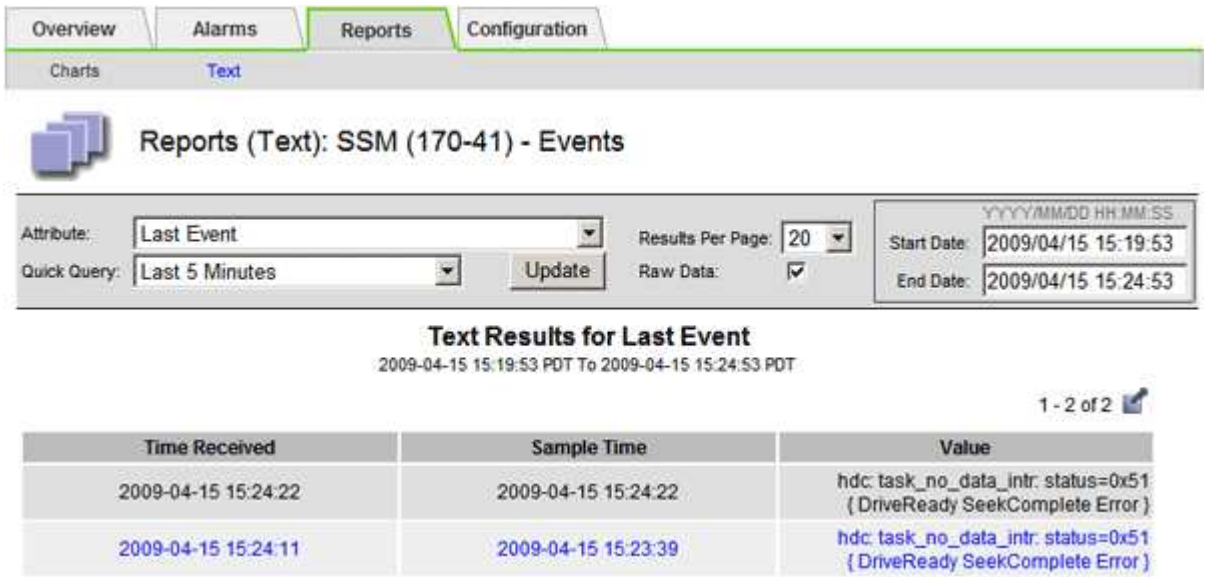
1. 查看每个网格节点的系统事件：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 概述 * > * 主 * 。
2. 生成先前事件消息的列表，以帮助隔离过去发生的问题：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 报告 * 。
   c. 选择 * 文本 * 。

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

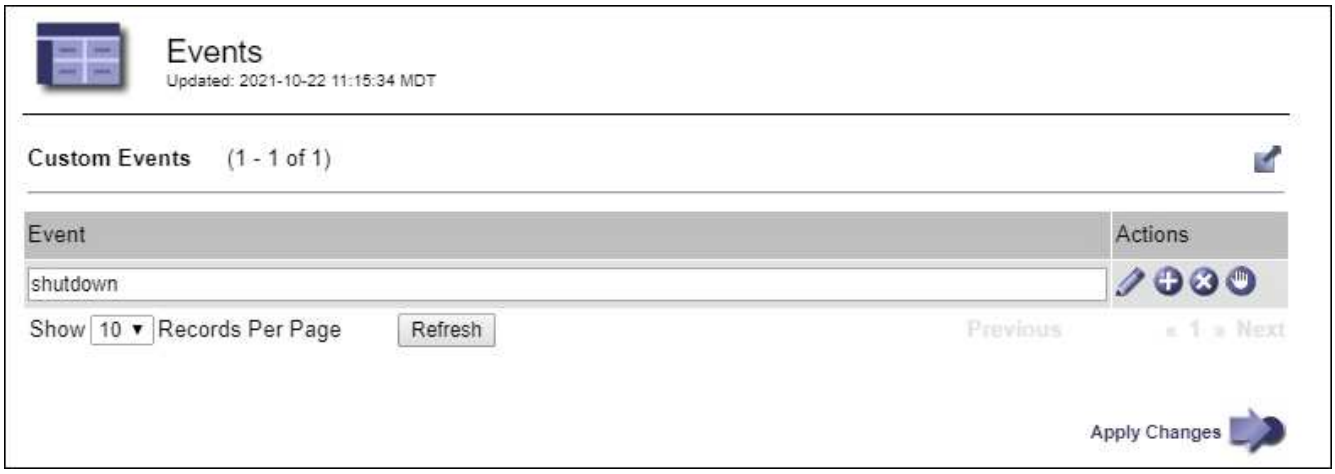
请考虑创建自定义事件以监控重复出现的问题。以下注意事项适用于自定义事件。

- 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。

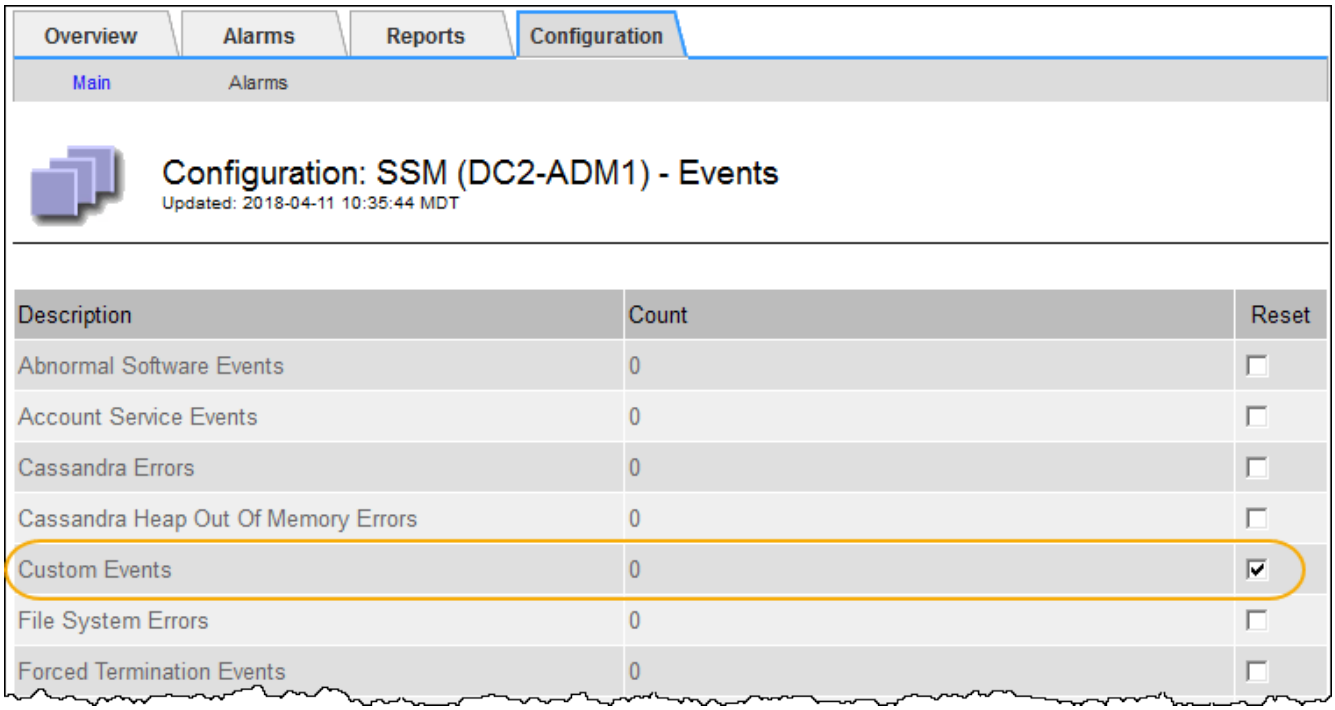
将自定义事件计数重置为零

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。

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

有关审核日志文件、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。

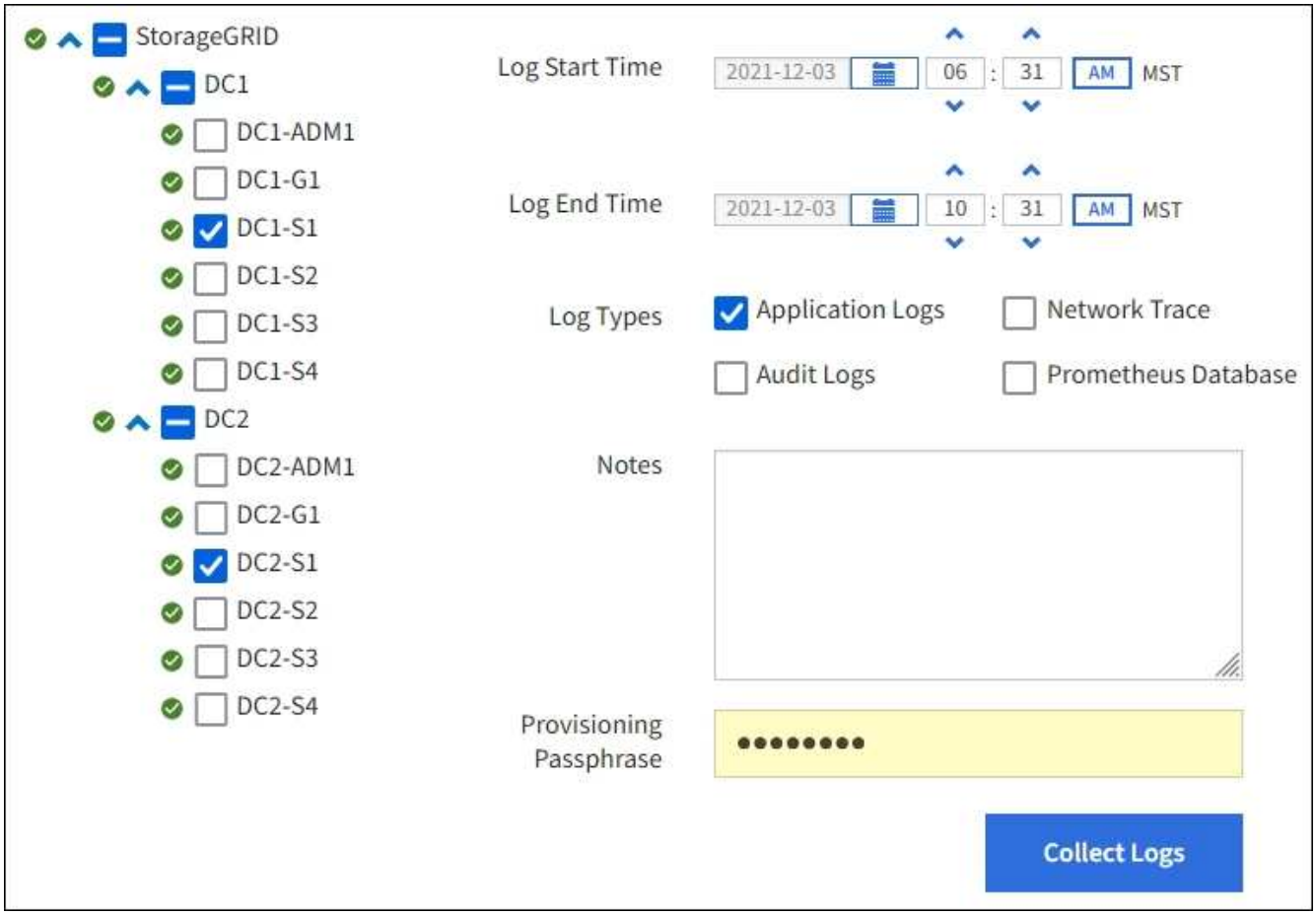
关于此任务

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 *。

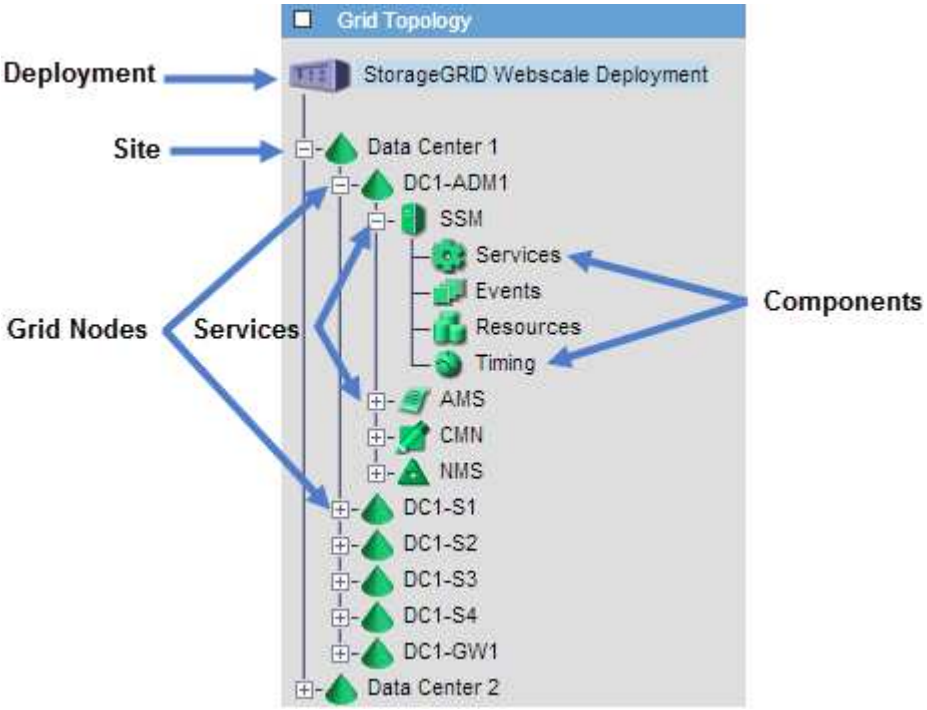
   StorageGRID尝试向NetApp 支持站点 发送AutoSupport软件包。如果尝试成功，则会更新 * 结果 * 选项卡上的 * 最新结果 * 和 * 最后成功时间 * 值。如果出现问题，“最新结果”值将更新为“失败”，并且StorageGRID不会尝试再次发送AutoSupport软件包。

   > 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

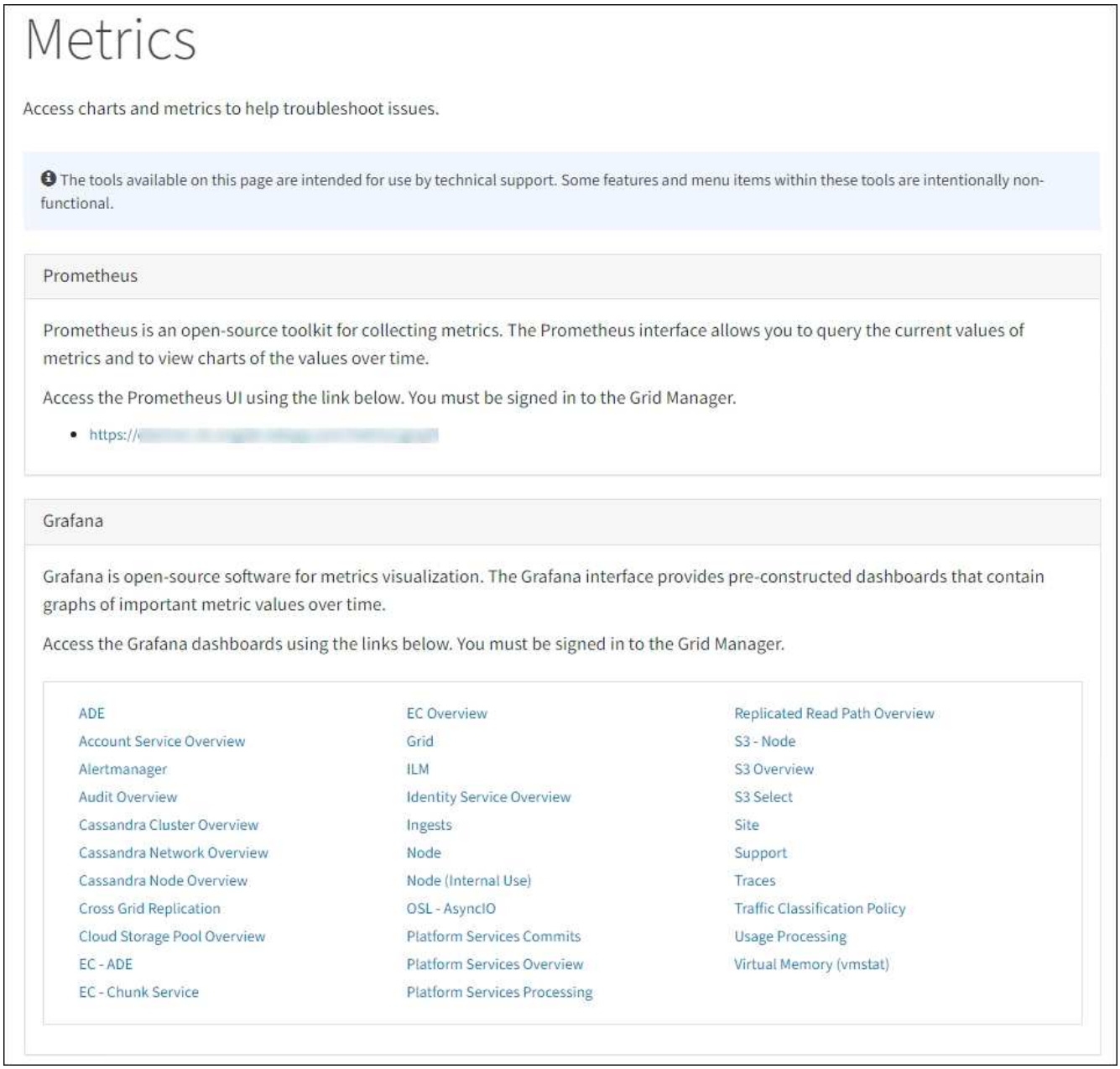
您可以通过指标页面访问 Prometheus 和 Grafana 用户界面。Prometheus 是用于收集指标的开源软件。Grafana 是用于可视化指标的开源软件。

> 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。

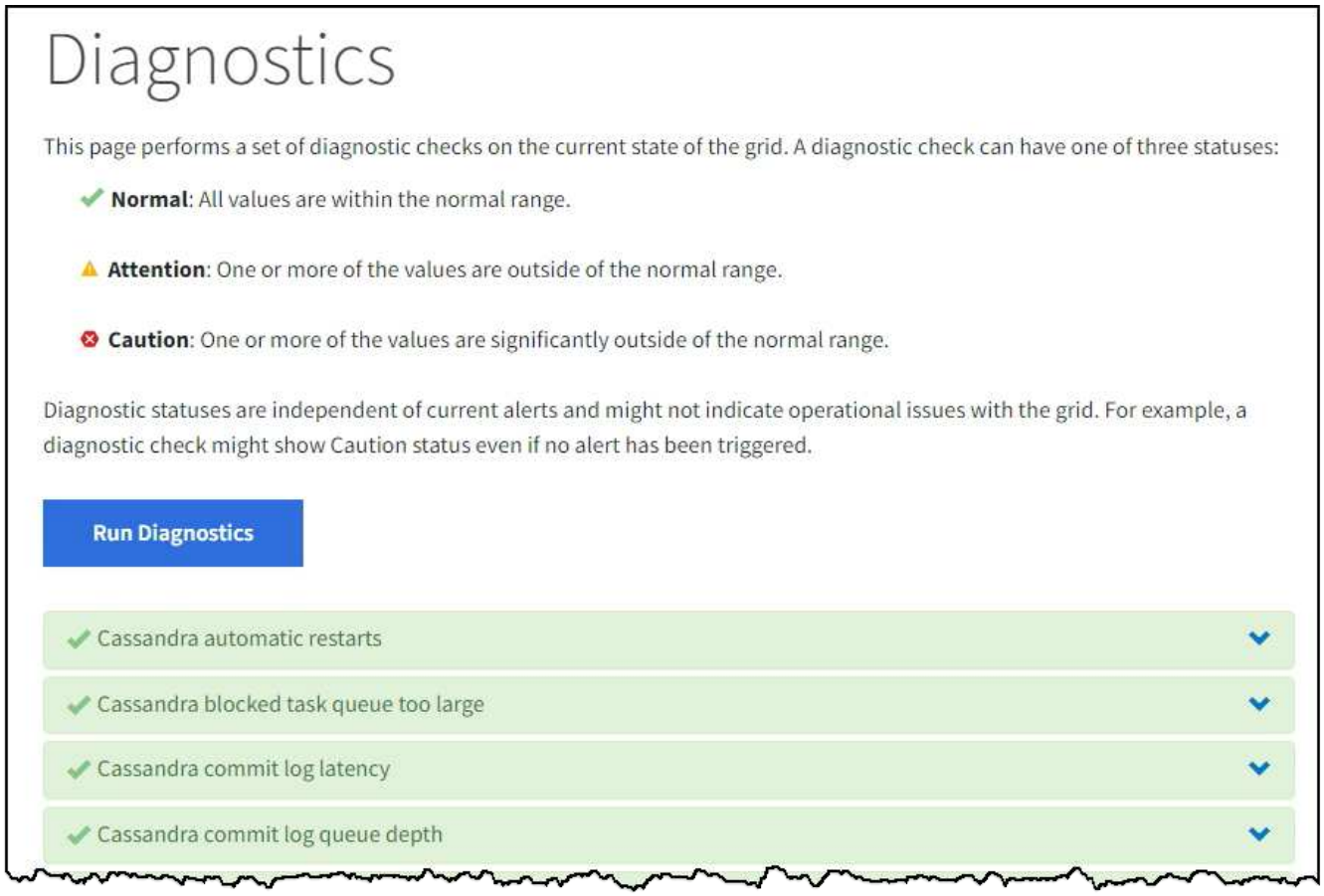
诊断状态与当前警报无关，可能并不表示网格存在操作问题。例如，即使未触发任何警报，诊断检查也可能会显示 " 小心 " 状态。

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。

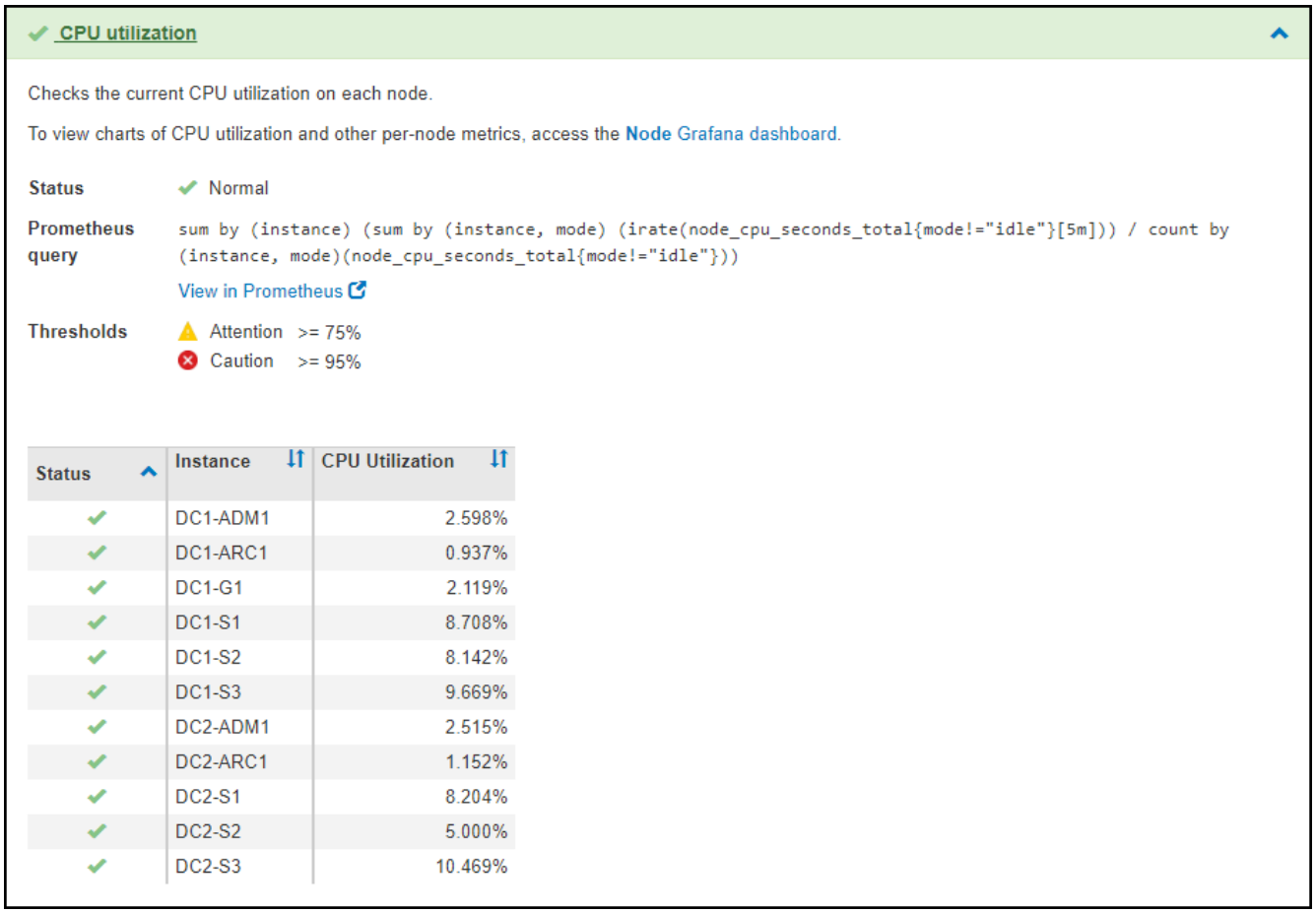
   此时将显示有关此诊断及其当前结果的详细信息。此时将列出以下详细信息：

   - * 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。

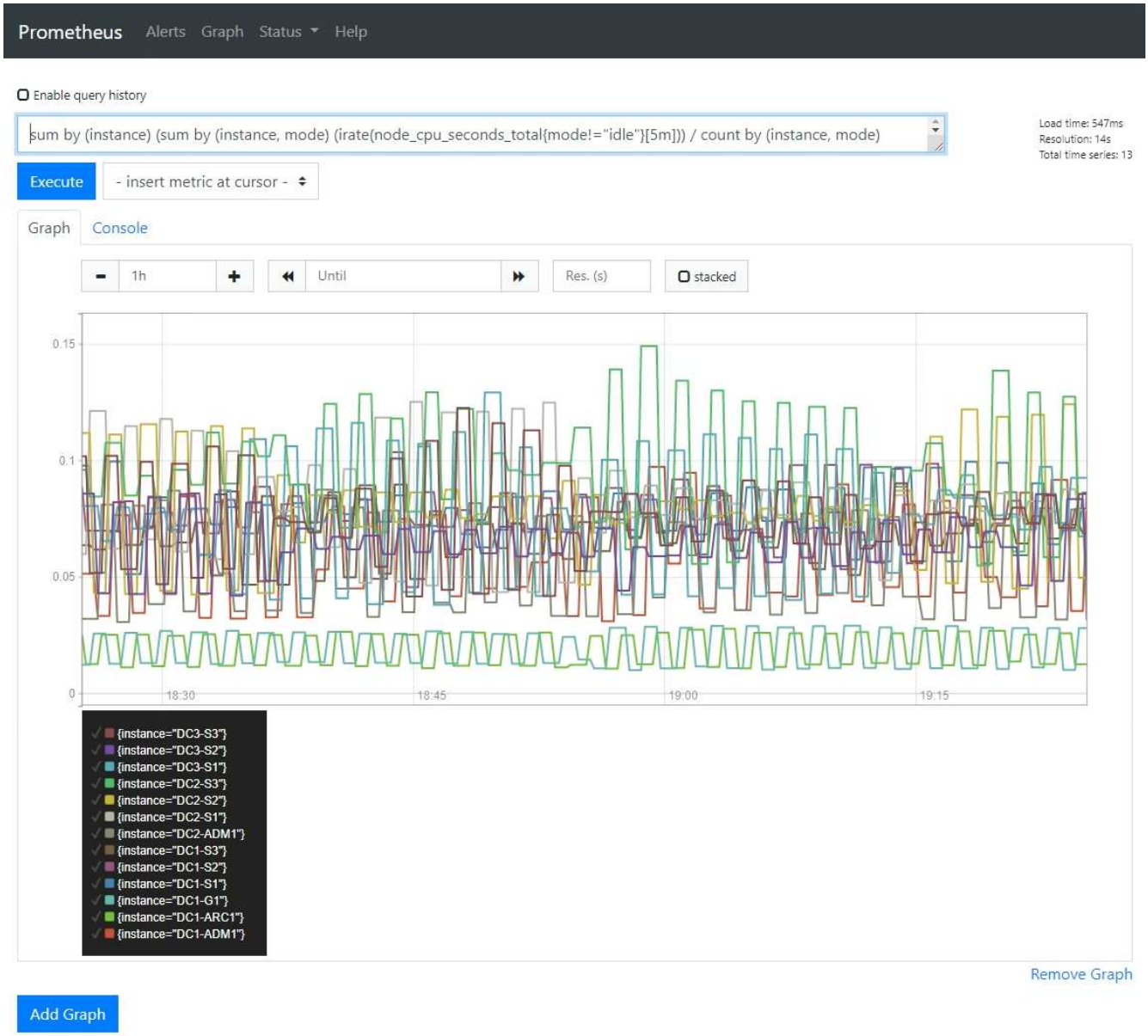
   并非所有诊断都显示此链接。

   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*。

metrics Operations on metrics

GET	`/grid/metric-labels/{label}/values`	Lists the values for a metric label
GET	`/grid/metric-names`	Lists all available metric names
GET	`/grid/metric-query`	Performs an instant metric query at a single point in time
GET	`/grid/metric-query-range`	Performs a metric query over a range of time

本文档不会详细介绍如何实施自定义监控应用程序。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。