监控和故障排除
StorageGRID software

NetApp
July 23, 2026

目录

监控 StorageGRID 系统并排除故障

监控 StorageGRID 系统

监控 StorageGRID 系统

定期监控您的 StorageGRID 系统，以确保其按预期运行。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "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菜单，然后选择*用户首选项*。

关于此任务

这些说明介绍了如何：

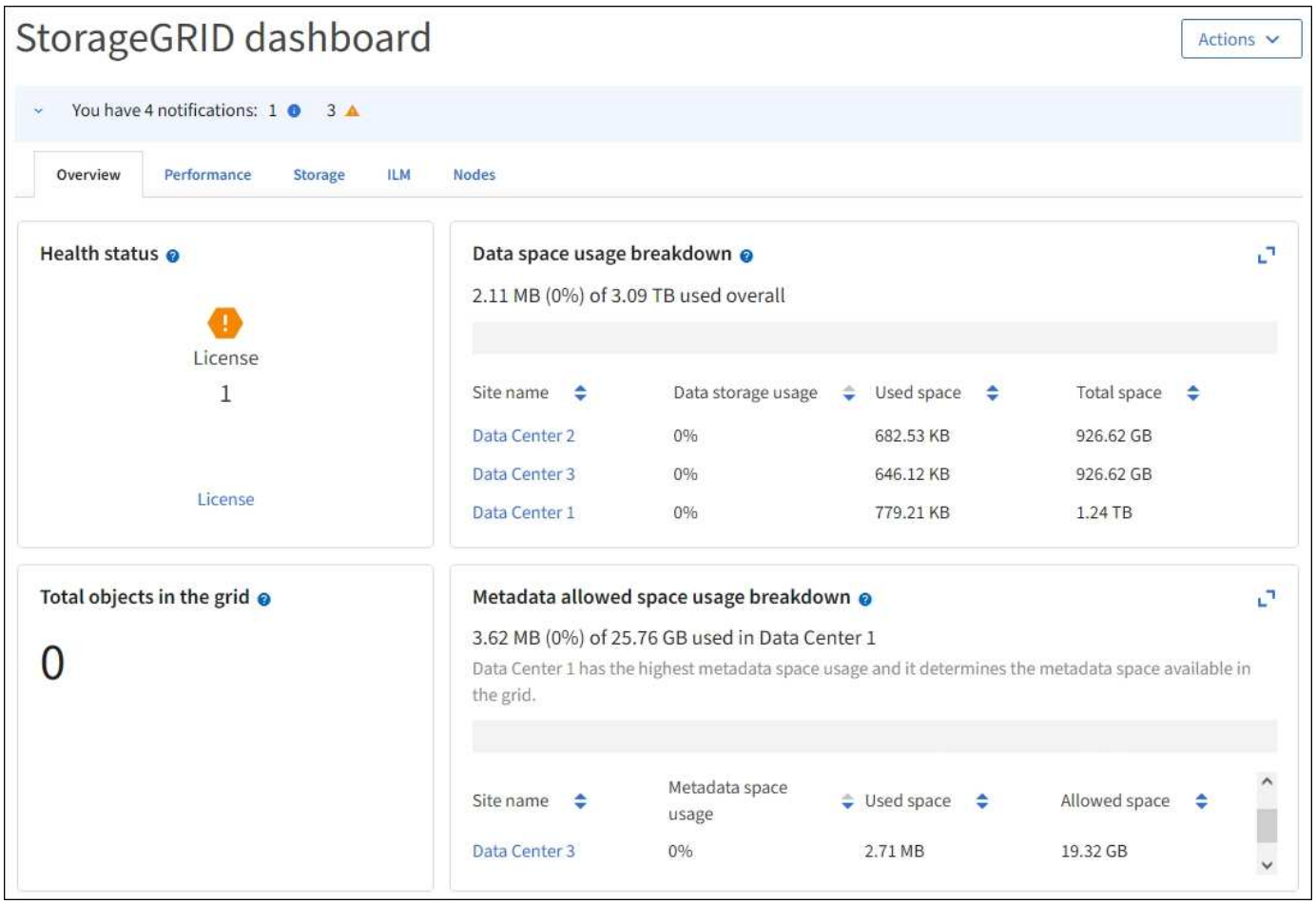
- "${post_edited_translations.segment}"
- "查看节点页面"
- "定期监控系统的以下方面："
  - "系统运行状况"
  - "存储容量"
  - "信息生命周期管理"
  - "网络和系统资源"
  - "租户活动"
  - "负载平衡操作"
  - "网格联盟连接"
- "${post_edited_translations.segment}"
- "查看日志文件"
- "配置日志管理和外部 syslog 服务器"
- "使用外部 syslog 服务器" 收集审计信息
- "使用 SNMP 进行监控"
- "更改I/O优先级" 更改 I/O 操作的相对优先级

在 StorageGRID 中查看和管理信息板

您可以使用仪表板一目了然地监控系统活动。您可以创建自定义仪表板来监控 StorageGRID。

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菜单，然后选择*用户首选项*。

您的控制面板可能因系统配置而异。



查看控制面板

仪表板由包含有关 StorageGRID 系统特定信息的选项卡组成。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仪表板。此外，您可以创建自定义仪表板，其中仅包含与监控 StorageGRID 实施相关的选项卡和卡片。

系统提供的仪表板选项卡包含具有以下类型信息的卡片：

系统提供的仪表板上的选项卡	包含
概述	有关网格的常规信息，例如活动警报、空间使用情况和网格中的对象总数。
性能	空间使用情况、长期使用的存储空间、S3 操作、请求持续时间、错误率。
存储	租户配额使用率和逻辑空间使用率。用户数据和元数据的空间使用预测。

系统提供的仪表板上的选项卡	包含
ILM	信息生命周期管理队列和评估率。
节点	按节点列出的 CPU、数据和内存使用情况。按节点列出的 S3 操作。节点到站点分布。

某些卡片可以最大化，以便更轻松地查看。选择卡片右上角的最大化图标 。要关闭最大化的卡片，请选择最小化图标 或选择 **Close**。

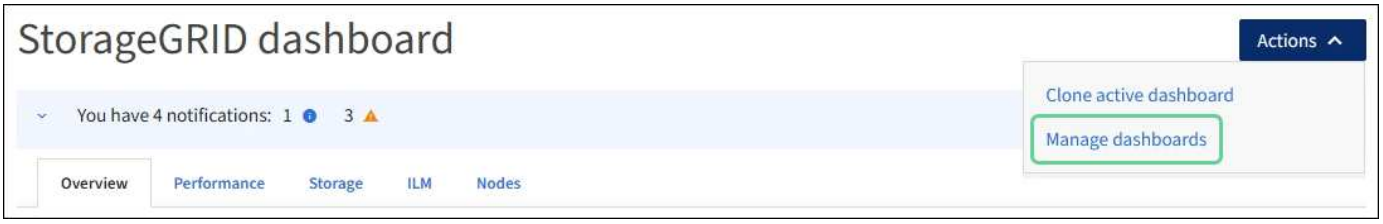
管理仪表板

如果您具有 Root 访问权限（请参阅"管理员组权限"），则可以对仪表板执行以下管理任务：

- 从头开始创建自定义仪表板。您可以使用自定义仪表板来控制显示哪些 StorageGRID 信息以及如何组织这些信息。
- 克隆仪表板以创建自定义仪表板。
- 为用户设置活动仪表板。活动仪表板可以是系统提供的仪表板或自定义仪表板。
- 设置默认仪表板，除非用户激活自己的仪表板，否则所有用户都会看到默认仪表板。
- 编辑仪表板名称。
- 编辑仪表板以添加或删除选项卡和卡片。您可以设置最少 1 个、最多 20 个标签页。
- 删除信息板。

如果您拥有 Root 访问权限以外的任何其他权限，则只能设置活动仪表板。

要管理仪表板，请选择*操作* > 管理仪表板。



配置信息板

要通过克隆活动仪表板来创建新仪表板，请选择*操作* > 克隆活动仪表板。

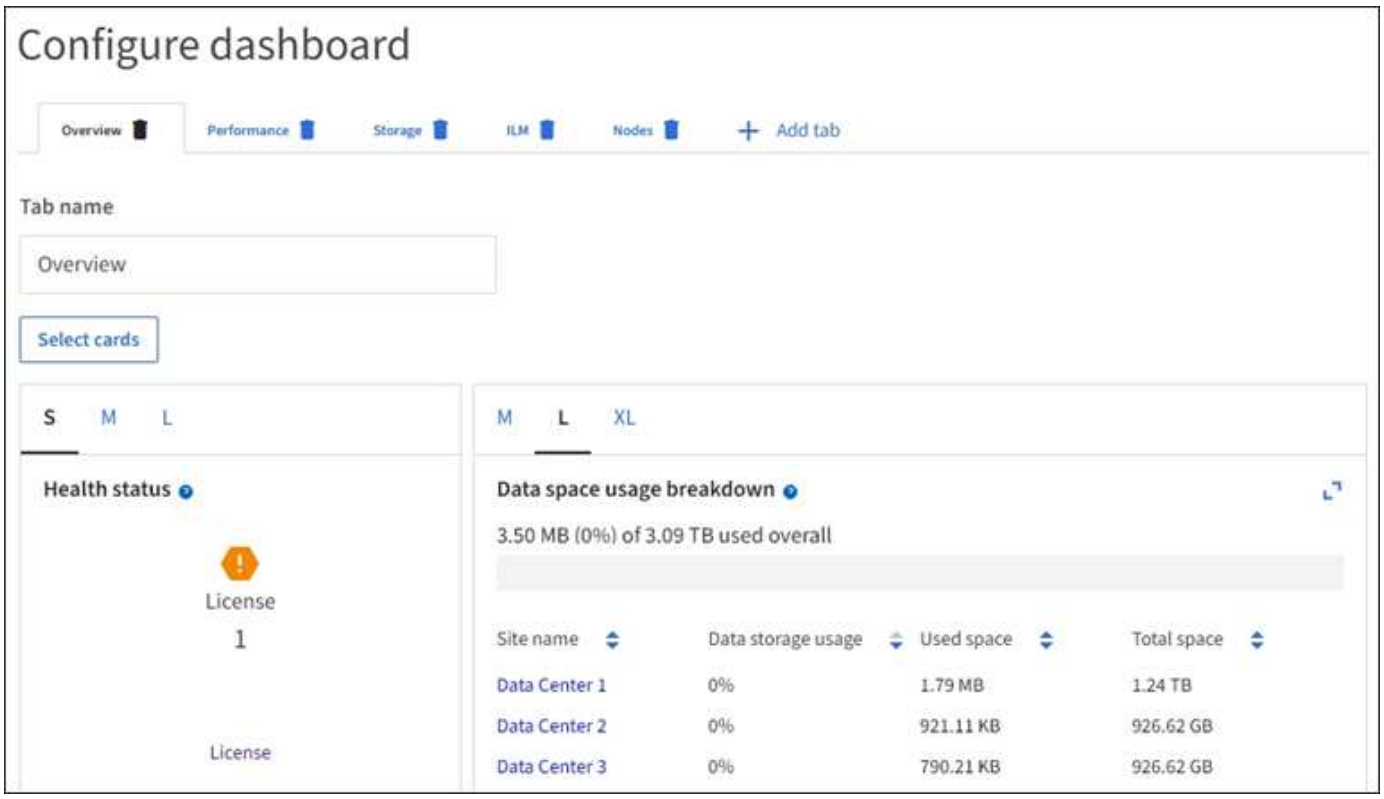
要编辑或克隆现有仪表板，请选择*操作* > 管理仪表板。

无法编辑或删除系统提供的控制面板。

配置仪表板时，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
- 通过选择卡片顶端的 **S**、**M**、**L** 或 **XL** 来选择单个卡片的尺寸



查看节点页面

查看 **StorageGRID** 节点页面

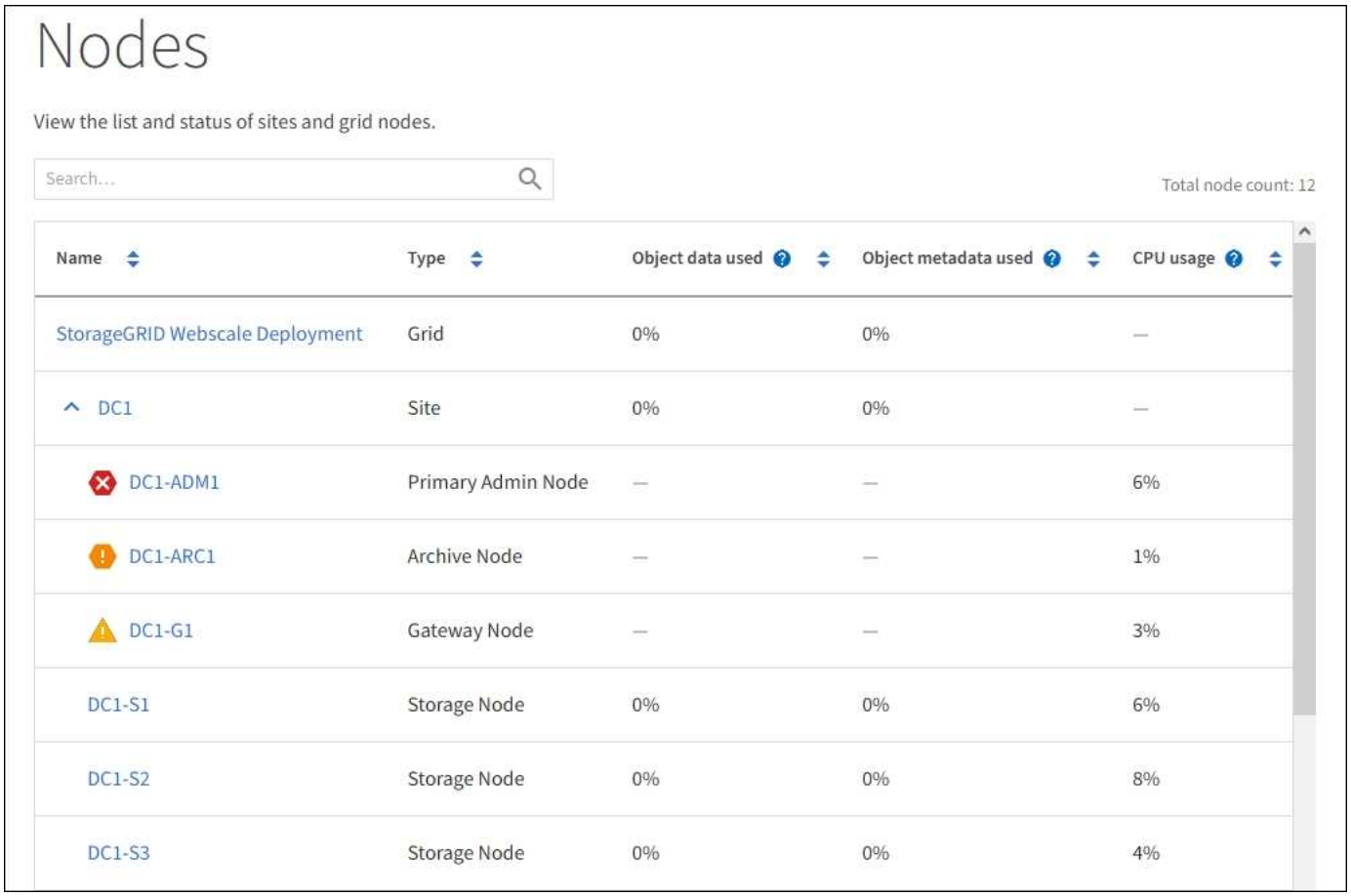
当您需要了解有关 StorageGRID 系统的更多详细信息（超出信息板所提供的内容）时，可以使用"节点"页面查看整个网格、网格中每个站点以及站点中每个节点的指标。

Nodes 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有活动的警报，则会在节点名称旁边显示一个图标。如果节点已连接且没有活动警报，则不会显示任何图标。

当节点未连接到网格时，例如在升级或断开连接状态下，某些指标可能不可用或被排除在站点和网格总计之外。节点重新连接到网格后，等待几分钟以使值稳定。

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菜单，然后选择*用户首选项*。

显示的屏幕截图只是示例。您的结果可能会因 StorageGRID 版本而异。



连接状态图标

如果某个节点与网格断开连接，则以下任一图标将显示在节点名称旁边。

图标	问题描述	需采取行动
	未连接 - 未知 由于未知原因，节点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，或者节点可能因电源故障或意外中断而失去网络连接。 *无法与节点通信*警报也可能被触发。其他警报也可能处于活动状态。	需要立即注意。"选择每个警报"并遵循建议的操作。 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：在托管关闭操作期间，节点可能显示为未知。在这些情况下，可以忽略未知状态。

图标	问题描述	需采取行动
	未连接 - 管理性关闭 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。一个或多个警报也可能处于活动状态。 根据潜在问题，这些节点通常无需干预即可重新上线。	确定是否有任何警报影响此节点。 如果一个或多个警报处于活动状态，"选择每个警报"请执行建议的操作。

如果节点与网格断开连接，则可能存在底层警报，但只会显示"未连接"图标。要查看节点的活动警报，请选择该节点。

警报图标

如果节点存在活动警报，则会在节点名称旁边显示以下图标之一：

严重：存在已停止 StorageGRID 节点或服务正常操作的异常情况。您必须立即解决根本问题。如果问题未得到解决，可能会导致服务中断和数据丢失。

重大：存在影响当前操作或接近严重警报阈值的异常情况。您应该调查重大警报并解决任何潜在问题，以确保异常情况不会阻止 StorageGRID 节点或服务的正常运行。

Minor：系统正常运行，但存在异常情况，如果继续运行，可能会影响系统的运行能力。您应该监控并解决未自行清除的轻微警报，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

要过滤节点表中显示的信息，请在*搜索*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：

- 选择网格名称以查看整个 StorageGRID 系统的统计汇总摘要。
- 选择特定数据中心站点以查看该站点上所有节点的统计信息的汇总摘要。
- 选择一个指定节点以查看该节点的详细信息。

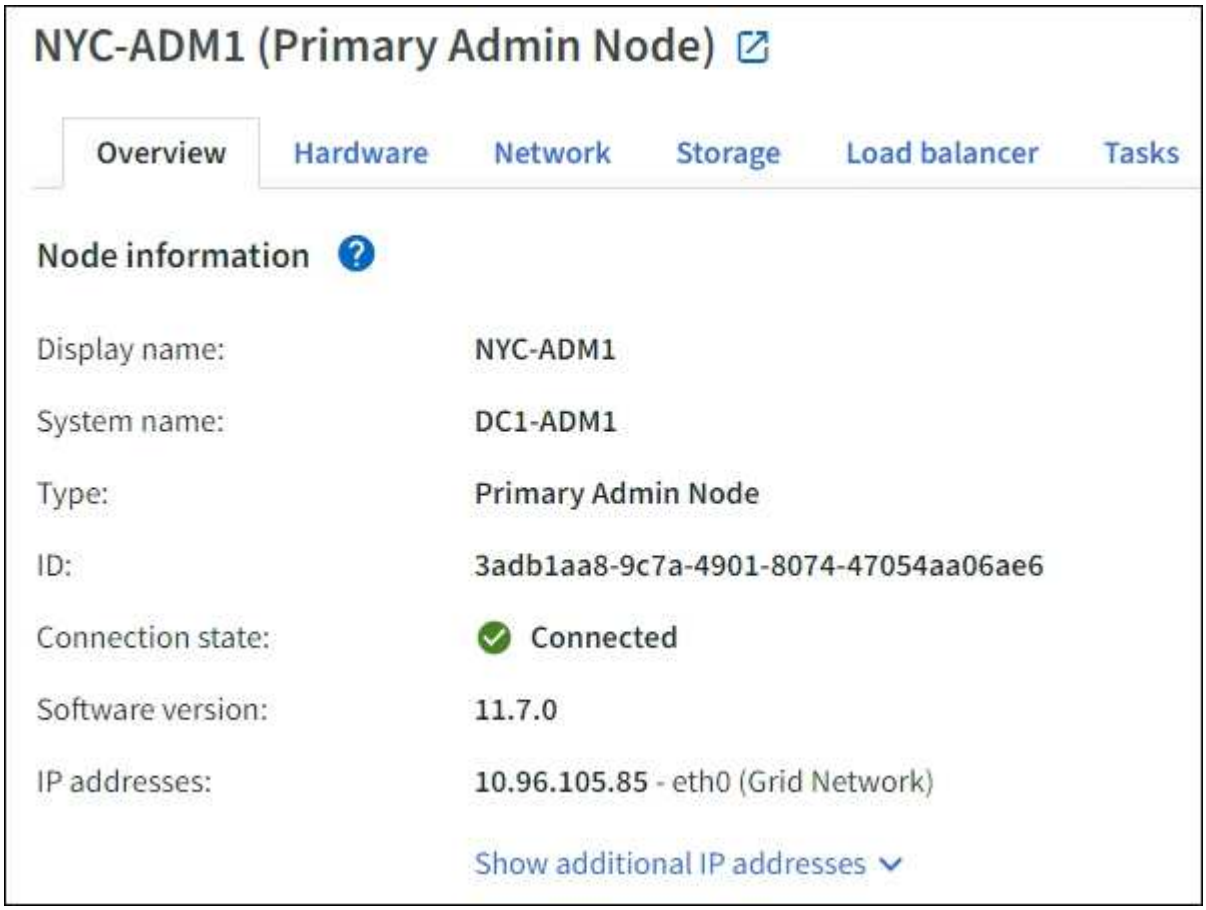
查看 **StorageGRID Overview** 选项卡

"概述"选项卡提供有关每个节点的基本信息。它还显示当前影响该节点的任何警报。

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"部分列出了有关该节点的基本信息。



节点的概述信息包括以下内容：

- 显示名称（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" 过程更新此值。
- 系统名称：您在安装过程中为节点输入的名称。系统名称用于内部 StorageGRID 操作，无法更改。
- 类型：节点类型——管理节点、主管理节点、存储节点或网关节点。
- **ID**：节点的唯一标识符，也称为 UUID。
- 连接状态：三种状态之一。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丢失、电源已关闭或服务已关闭。*无法与节点通信*警报也可能被触发。其他警报也可能处于活动状态。这种情况需要立即关注。

    在托管关闭操作期间，节点可能会显示为"未知"。在这些情况下，可以忽略未知状态。

  - 管理性关闭：由于预期的原因，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。一个或多个警报也可能处于活动状态。
  - 已连接：节点已连接到网格。
- **Storage used**：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占总可用空间的百分比。

- **Object metadata**：存储节点上已使用的对象元数据总允许空间的百分比。

- 软件版本：安装在节点上的 StorageGRID 版本。
- **HA groups**：仅适用于管理节点和网关节点。显示节点上的网络接口是否包含在高可用性组中，以及该接口是否为主接口。
- **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

"概览"选项卡的"提醒"部分列出了任何"当前影响此节点但尚未静默的警报"。选择警报名称以查看其他详细信息和建议操作。

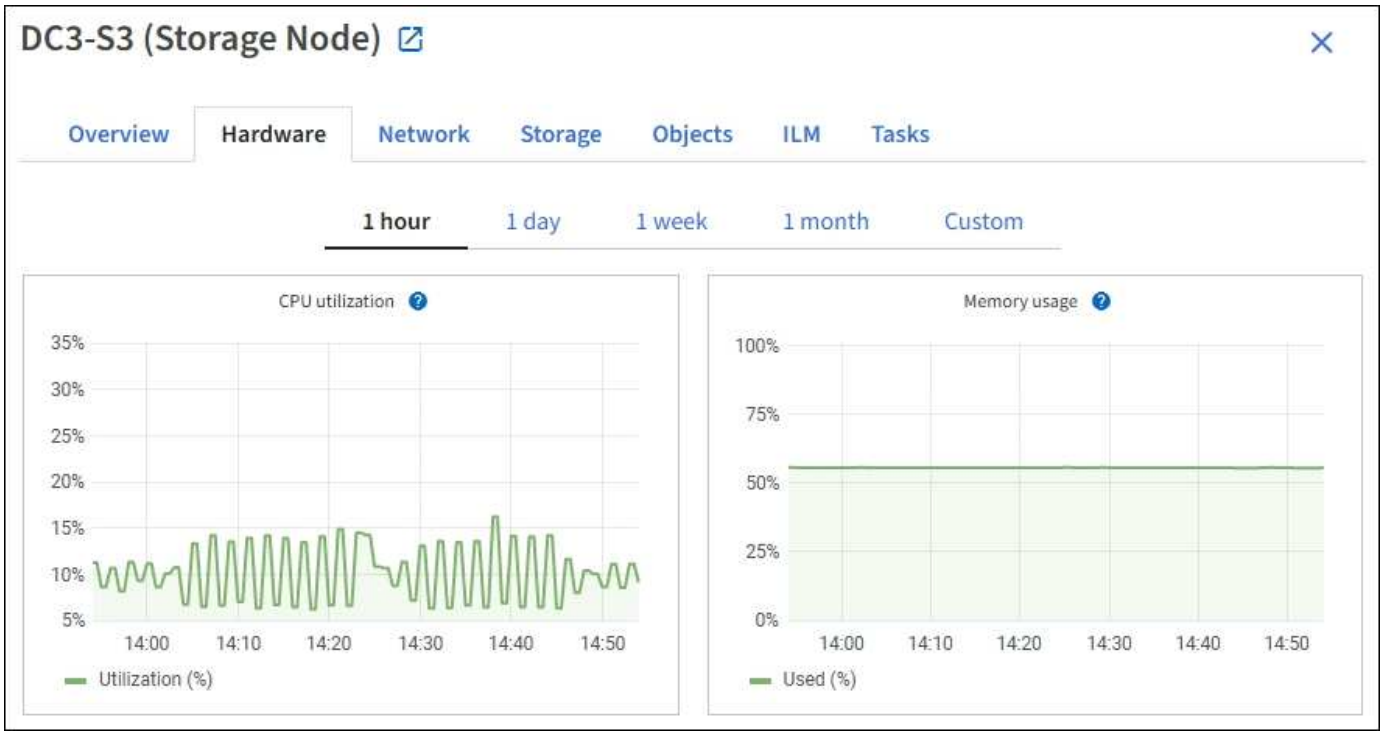
还包括适用于 "节点连接状态" 的警报。

查看 **StorageGRID** 硬件选项卡

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

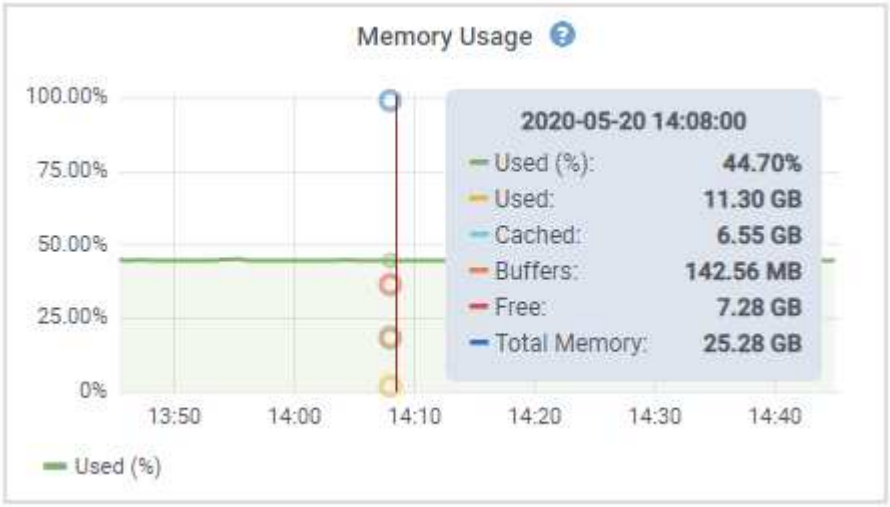
网格管理器随每个版本更新，可能与此页面上的示例屏幕截图不匹配。

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一个控件。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 利用率和内存使用率的详细信息，请将光标放置在每个图形上。



如果节点是设备节点，则此选项卡还包括有关设备硬件的详细信息的部分。

查看有关设备存储节点的信息

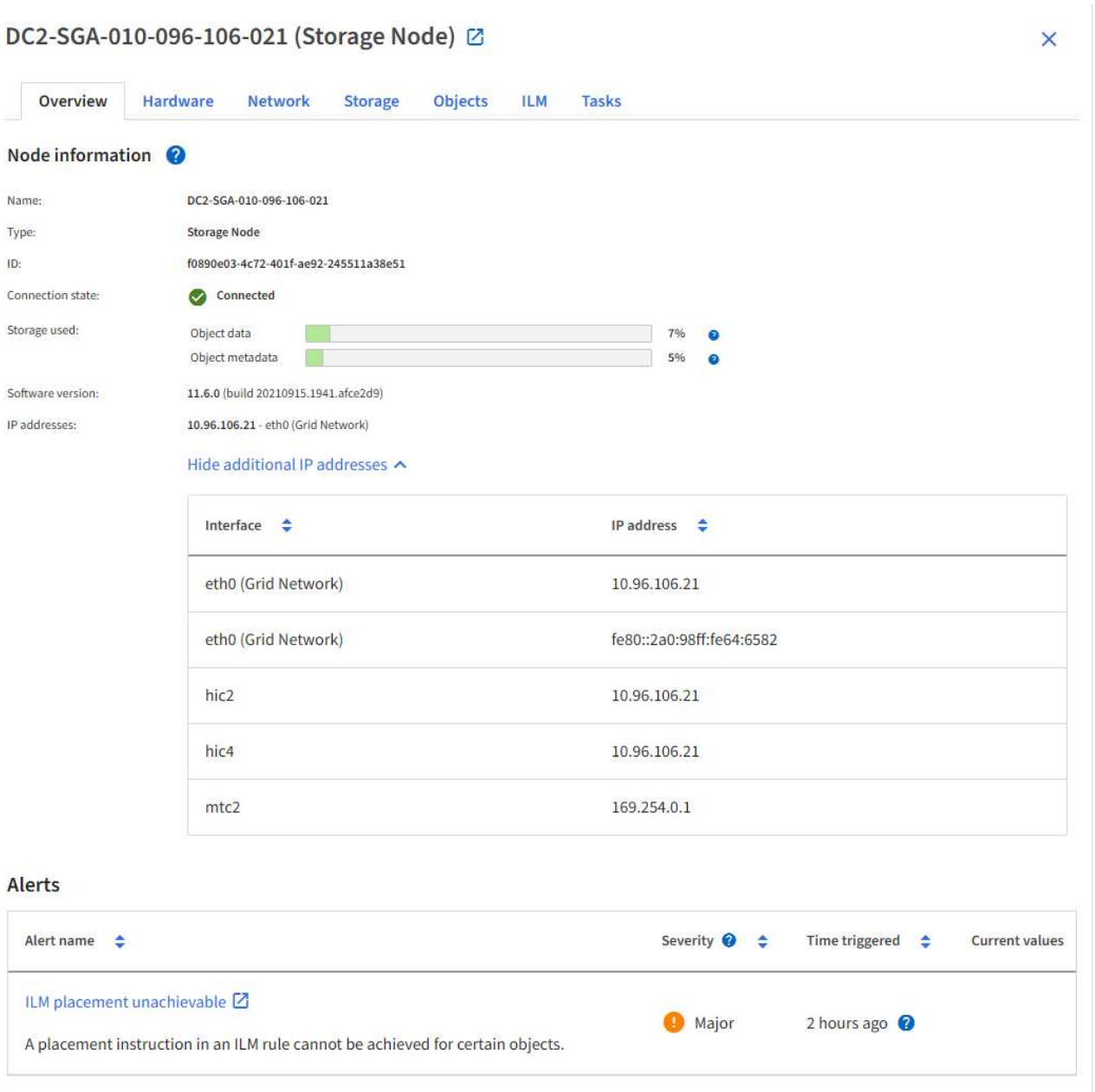
节点页面列出有关每个设备存储节点的服务健康状况以及所有计算、磁盘设备和网络资源的信息。您还可以查看内存、存储硬件、控制器固件版本、网络资源、网络接口、网络地址以及接收和传输数据。

步骤

1. 从节点页面中，选择一个设备存储节点。
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**：设备上的物理 10、25 或 100 GbE 端口之一。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**：设备上的物理 1 GbE 端口之一。一个或多个 mtc 接口绑定在一起，形成 StorageGRID 管理网络接口 (eth1)。您可以让其他 mtc 接口可供数据中心技术人员用于临时本地连接。

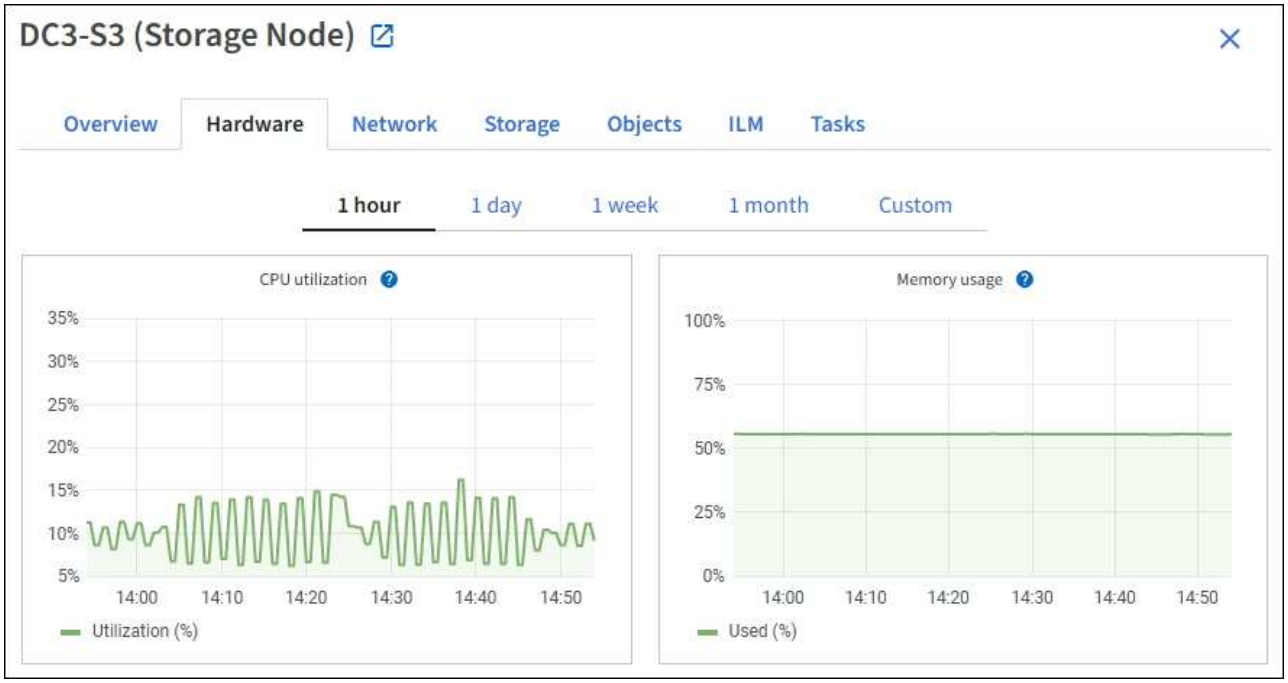


"概述"选项卡的"警报"部分显示该节点的所有活动警报。

3. 选择*硬件*以查看有关设备的详细信息。

   a. 查看 CPU 利用率和内存图表，以确定一段时间内 CPU 和内存利用率的百分比。要显示不同的时间间隔，请选择图表或图形上方的一个控件。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

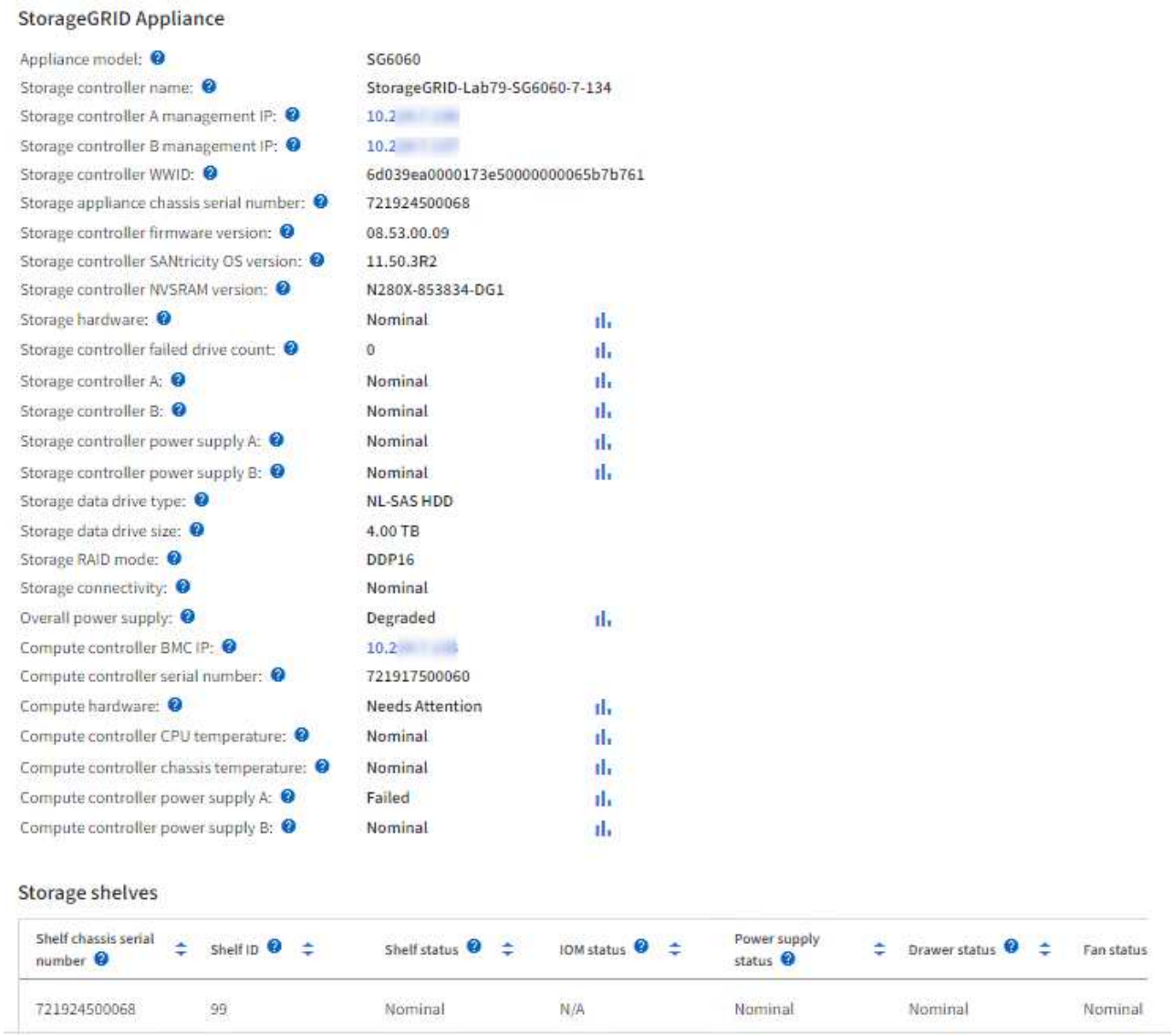
还可以设置自定义间隔，以指定日期和时间范围。



b. 向下滚动以查看设备的组件表。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）仅适用于具有该功能的设备。

存储架的组件以及扩展架（如果它们是安装的一部分）显示在设备表下方的单独表格中。



Appliance 表中的字段	问题描述
设备型号	SANtricity OS 中显示的此 StorageGRID 设备的型号。
存储控制器名称	此 StorageGRID 设备在 SANtricity 操作系统中显示的名称。
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 操作系统以解决存储问题。
存储控制器 B 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 操作系统以解决存储问题。 某些设备型号没有存储控制器 B。
存储控制器 WWID	SANtricity 操作系统中显示的存储控制器的全球标识符。
存储设备机箱序列号	设备的机箱序列号。

Appliance 表中的字段	问题描述
存储控制器固件版本	此设备的存储控制器上的固件版本。
存储控制器 SANtricity 操作系统版本	存储控制器 A 的 SANtricity 操作系统版本。
存储控制器 NVSRAM 版本	存储控制器的 NVSRAM 版本，由 SANtricity System Manager 报告。 对于 SG6060 和 SG6160，如果两个控制器之间存在 NVSRAM 版本不匹配，则显示控制器 A 的版本。如果控制器 A 未安装或未运行，则显示控制器 B 的版本。
存储硬件	存储控制器硬件的整体状态。如果 SANtricity System Manager 报告存储硬件的需要注意状态，StorageGRID 系统也会报告此值。 如果状态为"需要注意"，请先使用 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	非最优状态的驱动器数量。
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	存储控制器电源A的状态。
存储控制器电源B	存储控制器的电源 B 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。 对于 SG6160，还会显示缓存驱动器的大小。 注意：对于具有扩展架的节点，请改用 每个托架的数据驱动器大小。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	设备所有电源的状态。

Appliance 表中的字段	问题描述
计算控制器 BMC IP	计算控制器中基板管理控制器（BMC）端口的 IP 地址。您可以使用此 IP 连接到 BMC 接口，以监控和诊断设备硬件。 此字段不会为不包含 BMC 的设备型号显示。
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。

+

存储货架表中的列	问题描述
磁盘架机箱序列号	存储货架底盘的序列号。
磁盘架 ID	存储货架的数字标识符。 • 99：存储控制器磁盘架 • 0：第一个扩展架 • 1：第二个扩展架 注意： 扩展架仅适用于 SG6060 和 SG6160。
磁盘架状态	存储架的整体状态。
IOM 状态	任何扩展架中输入/输出模块 (IOM) 的状态。如果这不是扩展架，则不适用。
电源状态	存储架电源的整体状态。
抽屉状态	存储架中抽屉的状态。如果架子不包含抽屉，则不适用。
风扇状态	存储架中冷却风扇的整体状态。
驱动器插槽	存储盘架中的驱动器插槽总数。
数据驱动器	用于数据存储的存储盘架中的驱动器数。

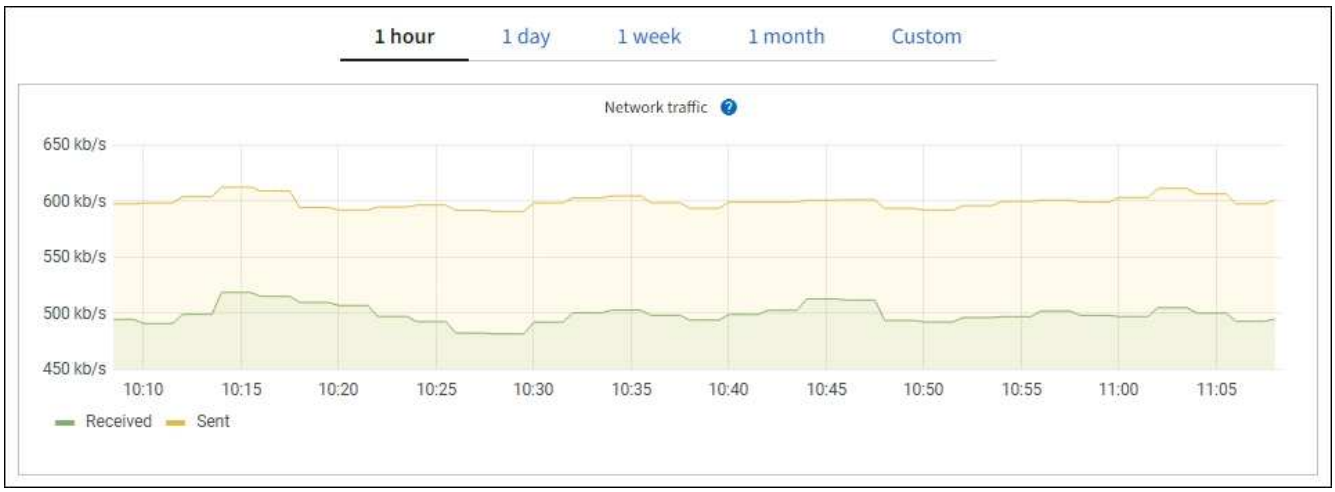
存储货架表中的列	问题描述
数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储盘架中用作缓存的驱动器数。
缓存驱动器大小	存储盘架中最小缓存驱动器的大小。通常，缓存驱动器的大小都相同。
配置状态	存储盘架的配置状态。

a. 确认所有状态均为"Nominal"。

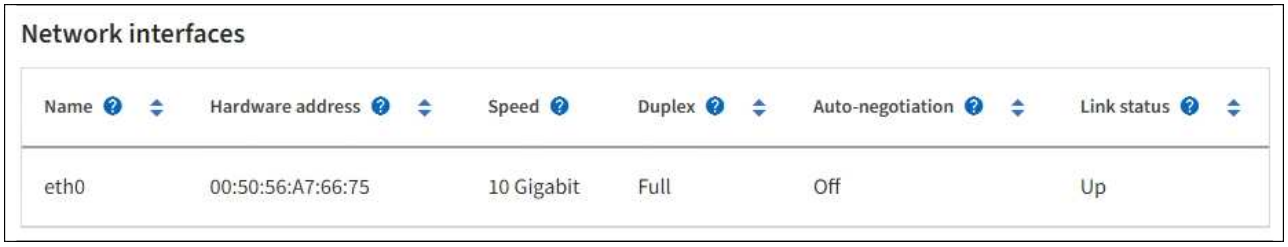
如果状态不是"Nominal"，请查看当前的任何警报。您还可以使用 SANtricity System Manager 了解有关这些硬件值的更多信息。请参阅安装和维护设备的说明。

4. 选择*网络*可查看每个网络的信息。

"网络流量"图表可提供整体网络流量的摘要。



a. 请查看"网络接口"部分。



使用下表以及网络接口表中*速度*列的值，确定设备上的 10/25-GbE 网络端口是否配置为使用主动/备份模式或 LACP 模式。

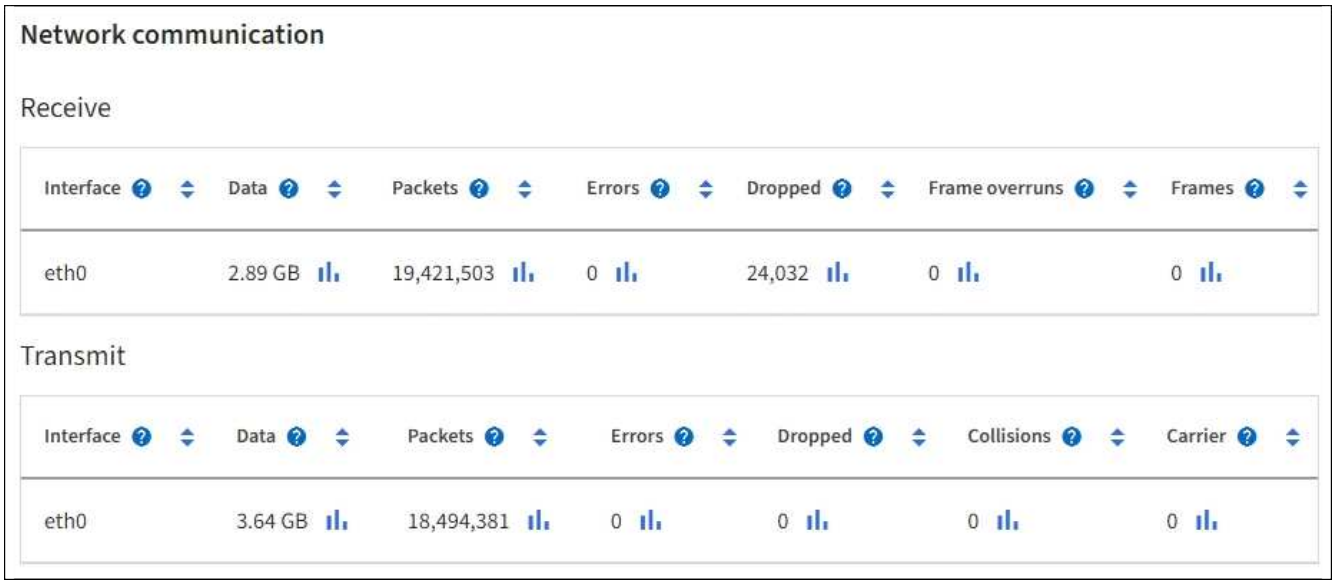
表中显示的值假设使用了全部四个链路。

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
固定	LACP	25	50
固定	主动/备份	25	25
聚合	LACP	10	40
固定	LACP	10	20
固定	主动/备份	10	10

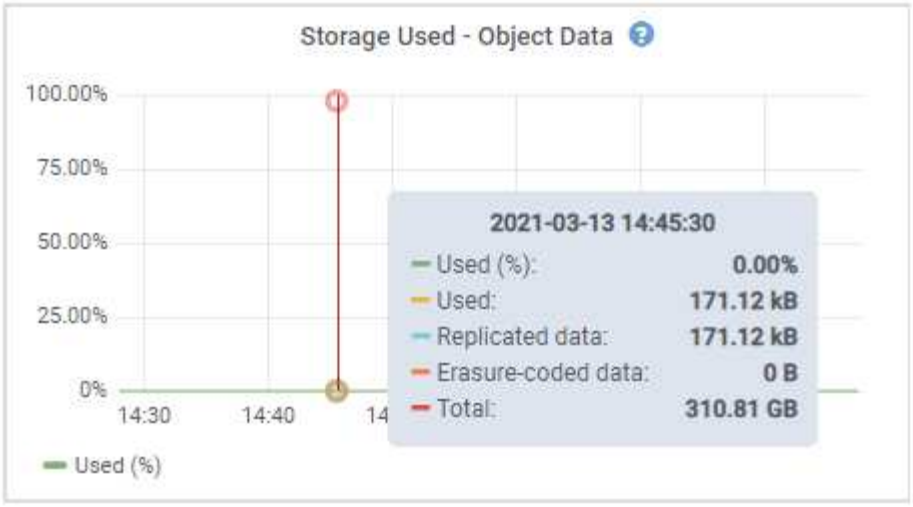
有关配置 10/25-GbE 端口的详细信息，请参见 "配置网络链接"。

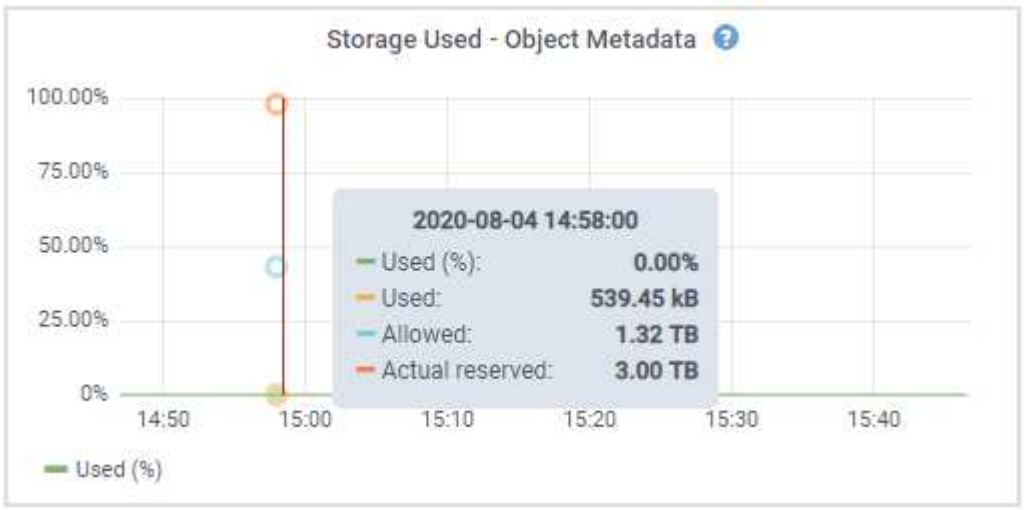
b. 请查看"网络通信"部分。

接收和传输表显示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随时间使用的存储百分比的图表，以及有关磁盘设备、卷和对象存储的信息。

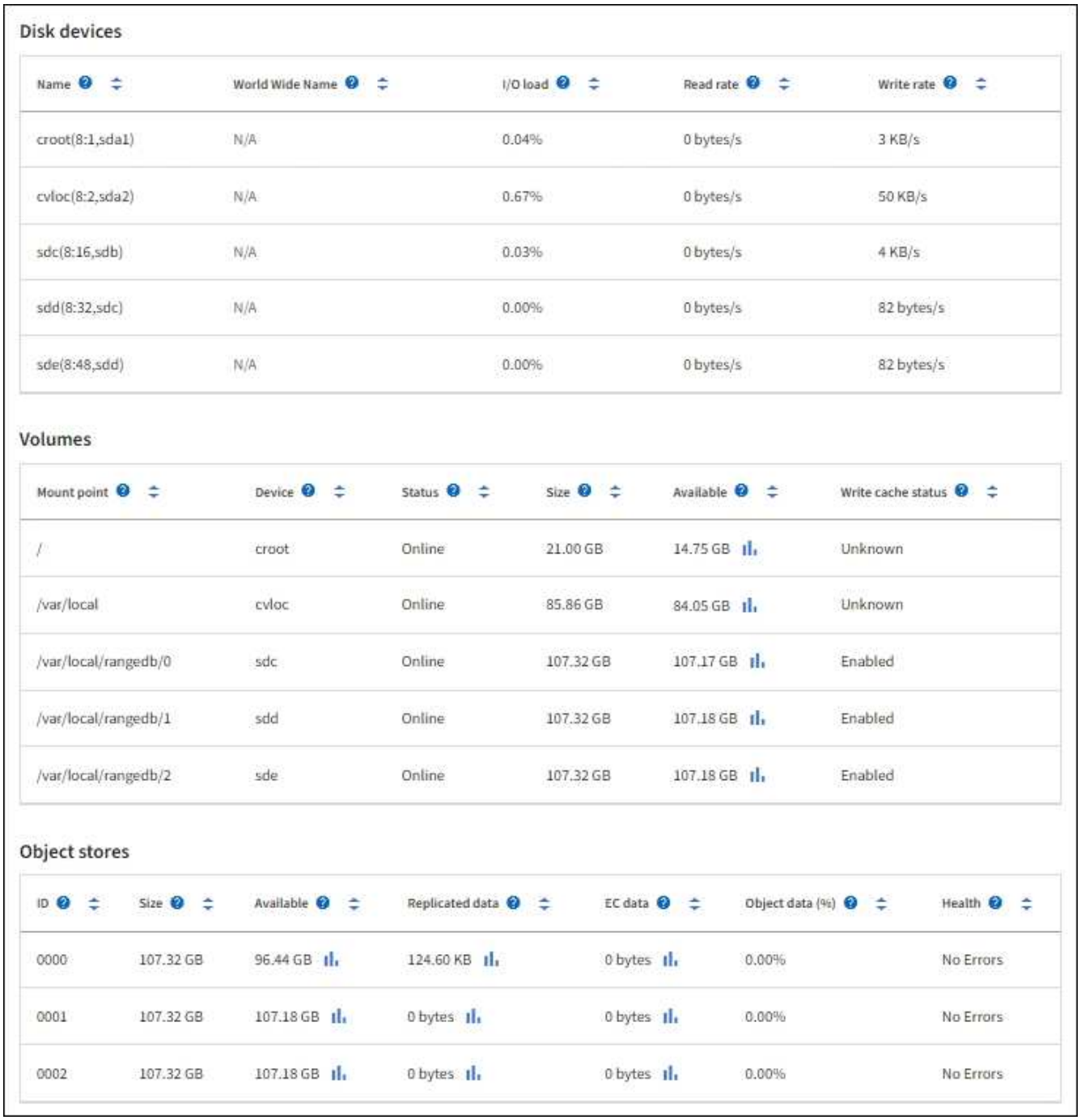




a. 向下滚动以查看每个卷和对象存储的可用存储量。

   每个磁盘的全球名称与在 SANtricity 操作系统（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标识符 (WWID) 相匹配。

   为了帮助您解释与卷挂载点相关的磁盘读写统计信息，磁盘设备表的 名称 列中显示的名称的第一部分（即 *sdc*、*sdd*、*sde* 等）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

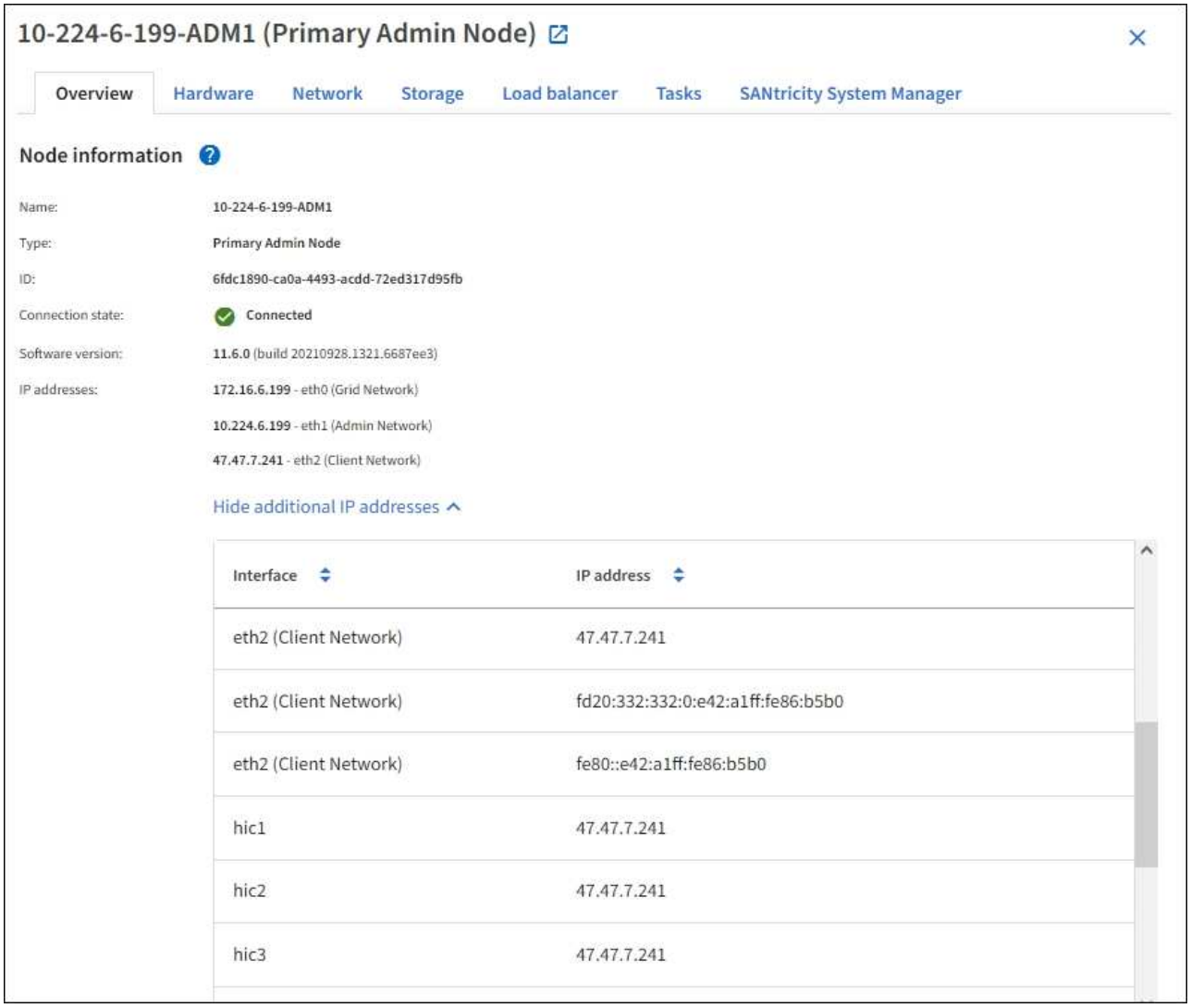
节点页面列出有关用作管理节点或网关节点的每个服务设备的服务运行状况以及所有计算、磁盘设备和网络资源的信息。您还可以查看内存、存储硬件、网络资源、网络接口、网络地址以及接收和传输数据。

步骤

1. 从节点页面中，选择一个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：

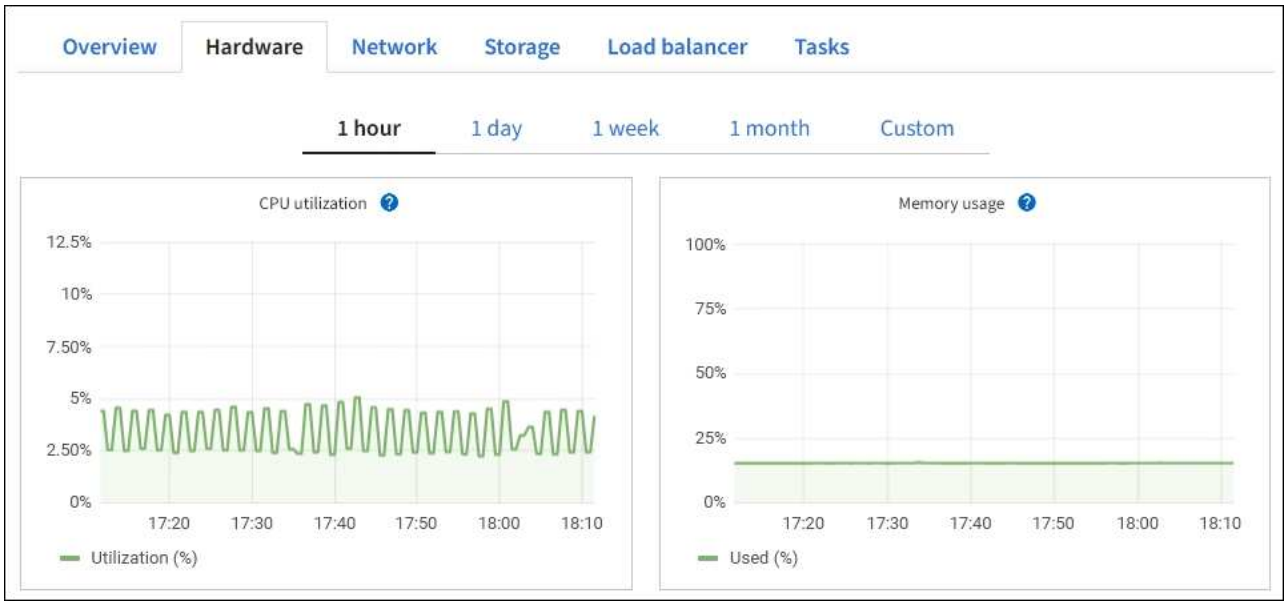
- **adllb** 和 **adlli**：显示管理网络接口是否使用活动/备份绑定
- **eth**：网格网络、管理网络或客户端网络。
- **hic**：设备上的物理 10、25 或 100 GbE 端口之一。这些端口可以绑定在一起并连接到 StorageGRID 网格网络（eth0）和客户端网络（eth2）。
- **mtc**：设备上的物理 1-GbE 端口之一。一个或多个 mtc 接口绑定在一起，形成管理网络接口 (eth1)。您可以让其他 mtc 接口可用于数据中心技术人员的临时本地连接。



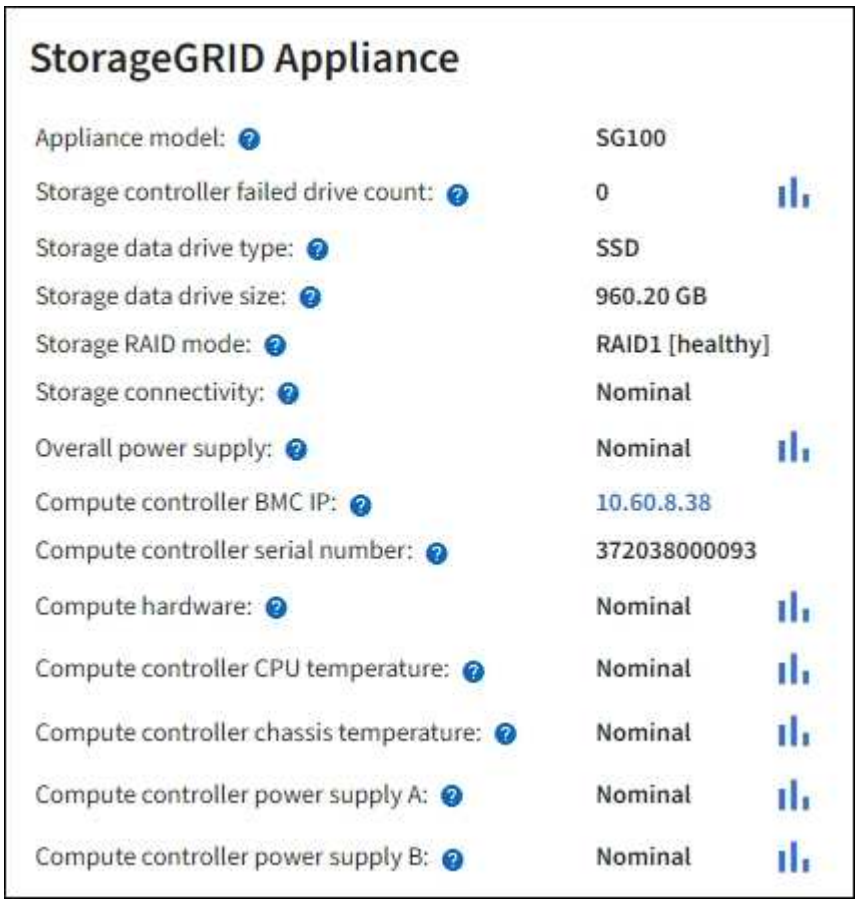
"概述"选项卡的"警报"部分显示该节点的所有活动警报。

3. 选择*硬件*以查看有关设备的详细信息。

   a. 查看 CPU 利用率和内存图表，以确定一段时间内 CPU 和内存利用率的百分比。要显示不同的时间间隔，请选择图表或图形上方的一个控件。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，以指定日期和时间范围。



b. 向下滚动以查看设备的组件表。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。



Appliance 表中的字段	问题描述
设备型号	此 StorageGRID 设备的型号。

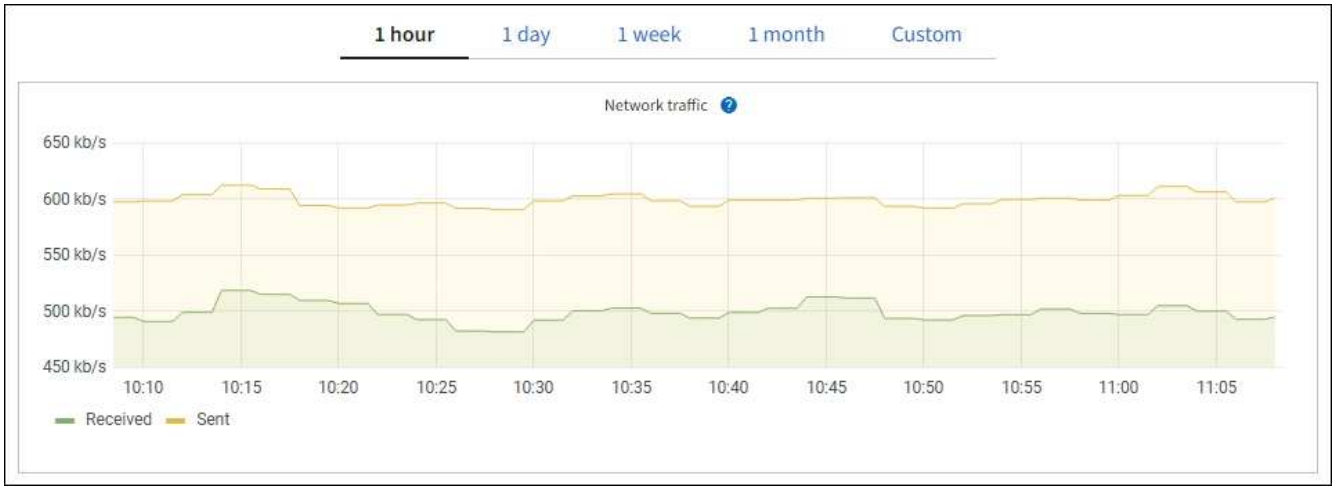
Appliance 表中的字段	问题描述
存储控制器故障驱动器计数	非最优状态的驱动器数量。
存储数据驱动器类型	设备中的驱动器类型，例如 HDD（硬盘驱动器）或 SSD（固态驱动器）。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中基板管理控制器（BMC）端口的 IP 地址。您可以使用此 IP 连接到 BMC 接口，以监控和诊断设备硬件。 此字段不会为不包含 BMC 的设备型号显示。
计算控制器序列号	计算控制器的序列号。
计算硬件	此计算控制器硬件的状态。
计算控制器 CPU 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"Nominal"。

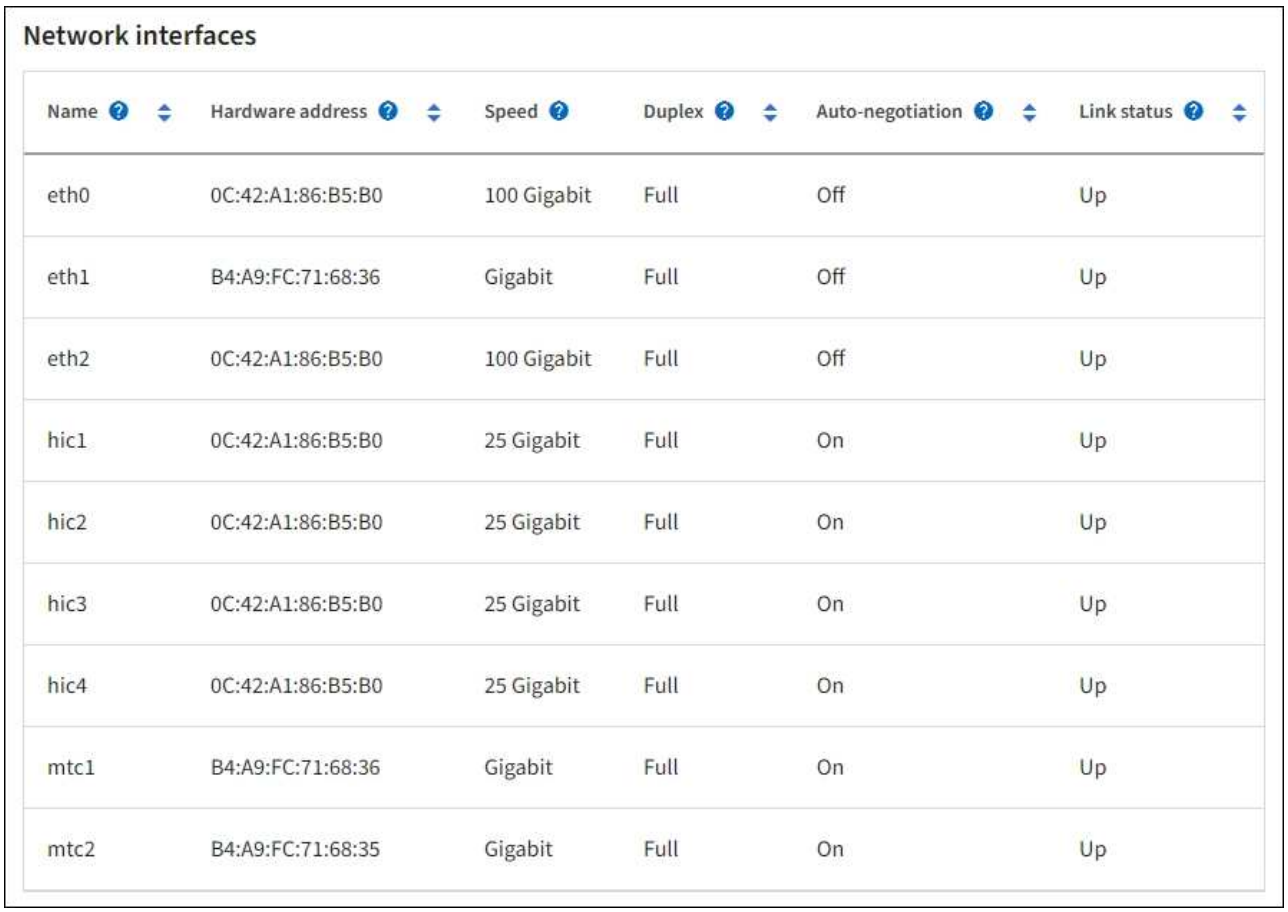
   如果状态不为"Nominal"，请查看当前的任何警报。

4. 选择*网络*可查看每个网络的信息。

"网络流量"图表可提供整体网络流量的摘要。



a. 请查看"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

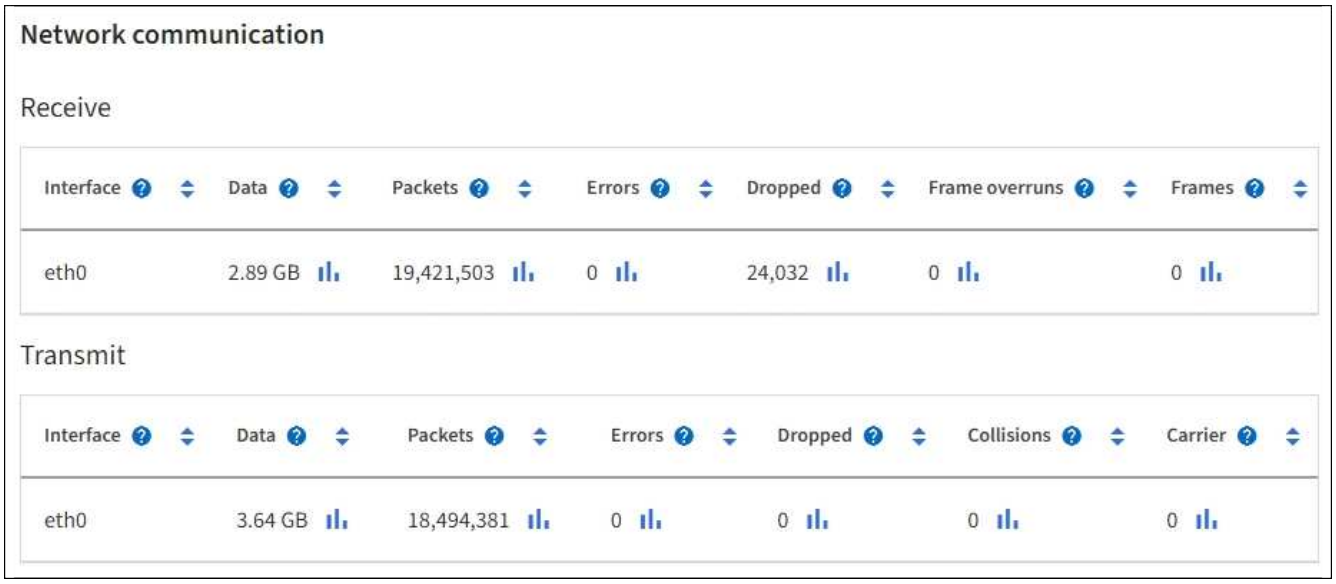
使用下表以及网络接口表中 **Speed** 列中的值，确定设备上的四个 40/100-GbE 网络端口是否配置为使用主动/备份模式或 LACP 模式。

表中显示的值假设使用了全部四个链路。

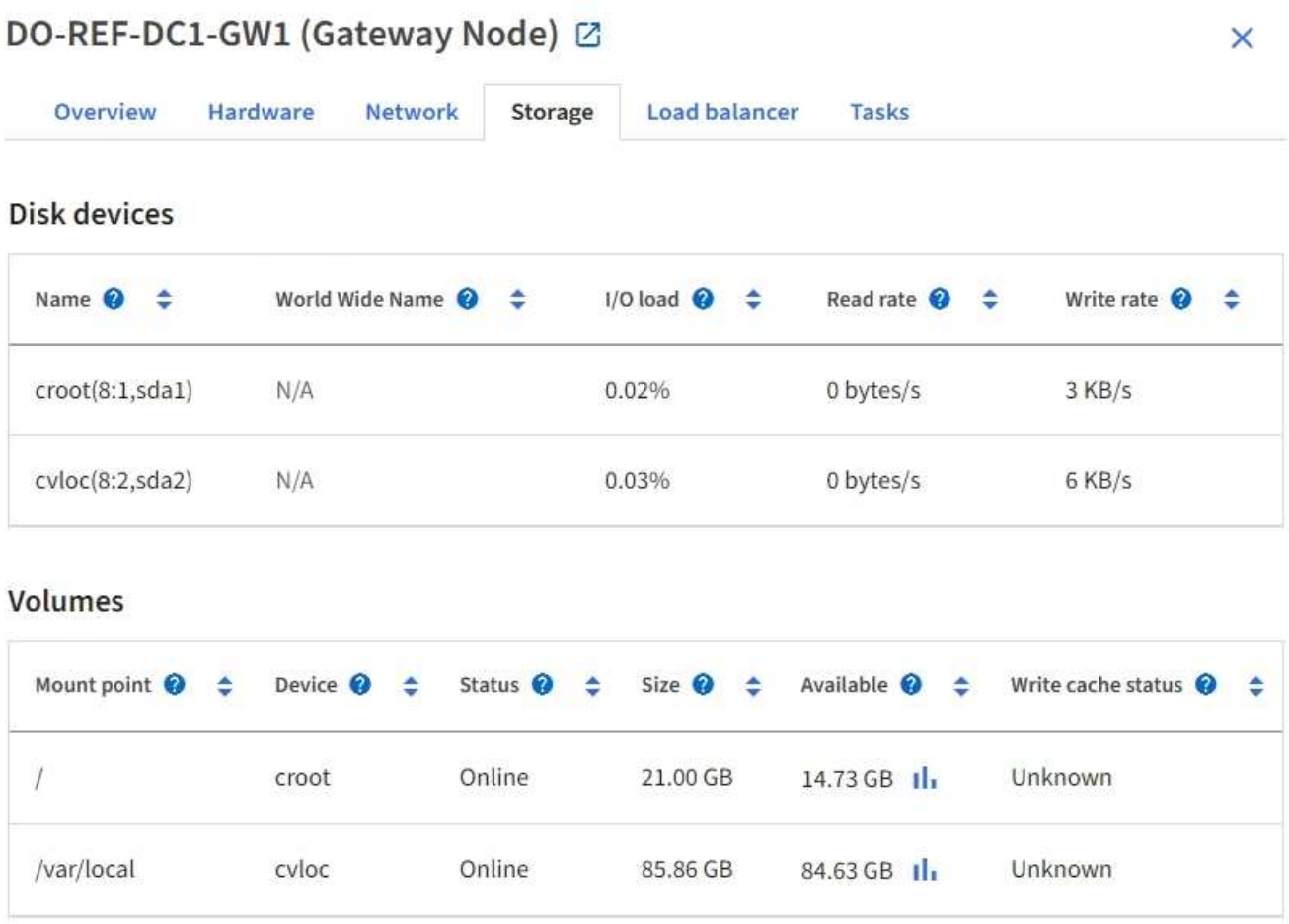
链路模式	绑定模式	单个 **HIC** 链路速度（**hic1**、**hic2**、**hic3**、**hic4**）	预期网格/客户端网络速度（**eth0, eth2**）
聚合	LACP	100	400
固定	LACP	100	200
固定	主动/备份	100	100
聚合	LACP	40	160
固定	LACP	40	80
固定	主动/备份	40	40

b. 请查看"网络通信"部分。

接收和传输表显示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*以查看有关服务设备上磁盘设备和卷的信息。



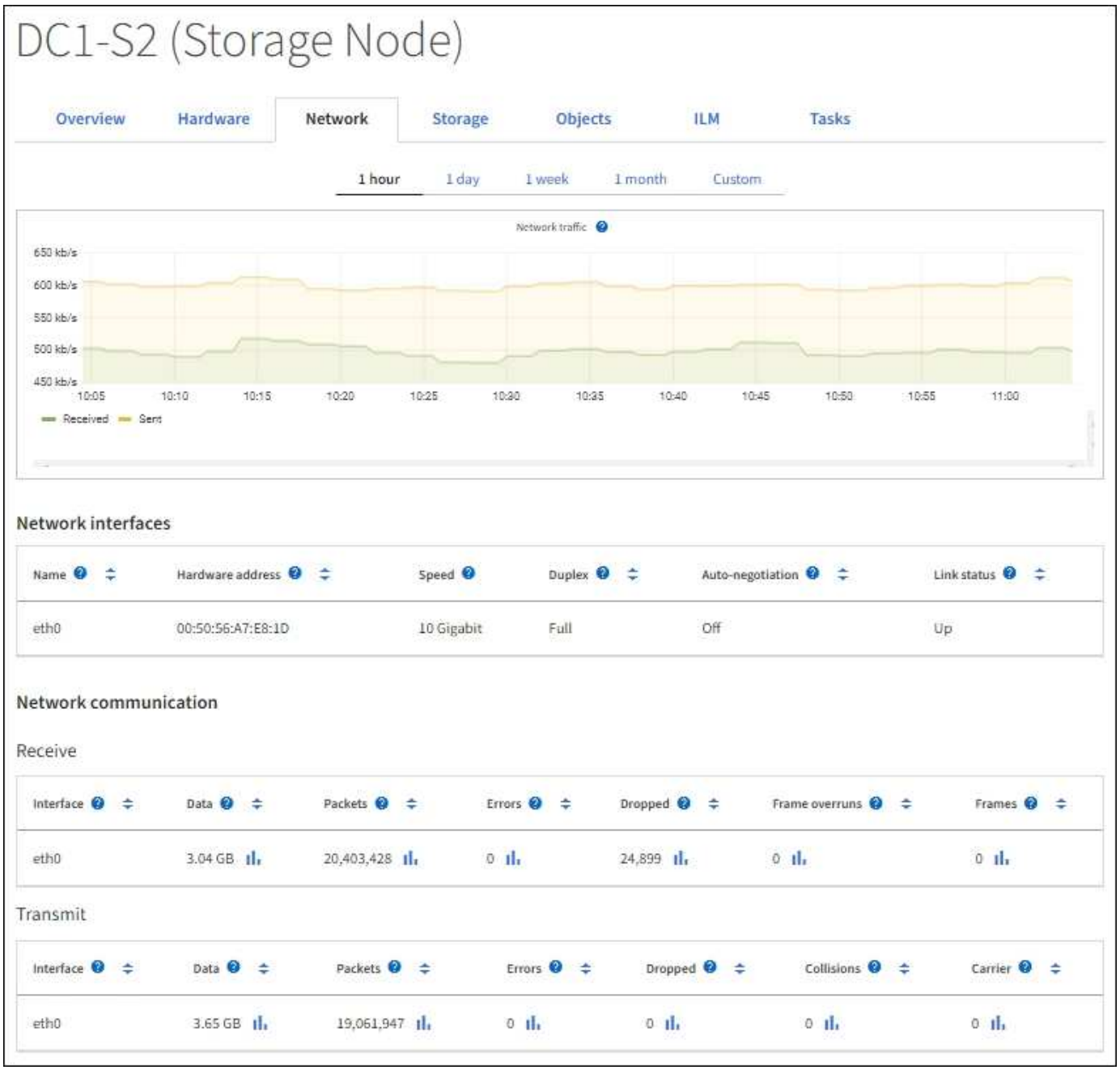
查看 **StorageGRID Network** 选项卡

"网络"选项卡显示一个图表，显示在节点、站点或网格上的所有网络接口上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一个控件。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，网络接口表提供有关每个节点的物理网络端口的信息。网络通信表提供了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 **StorageGRID Storage** 选项卡

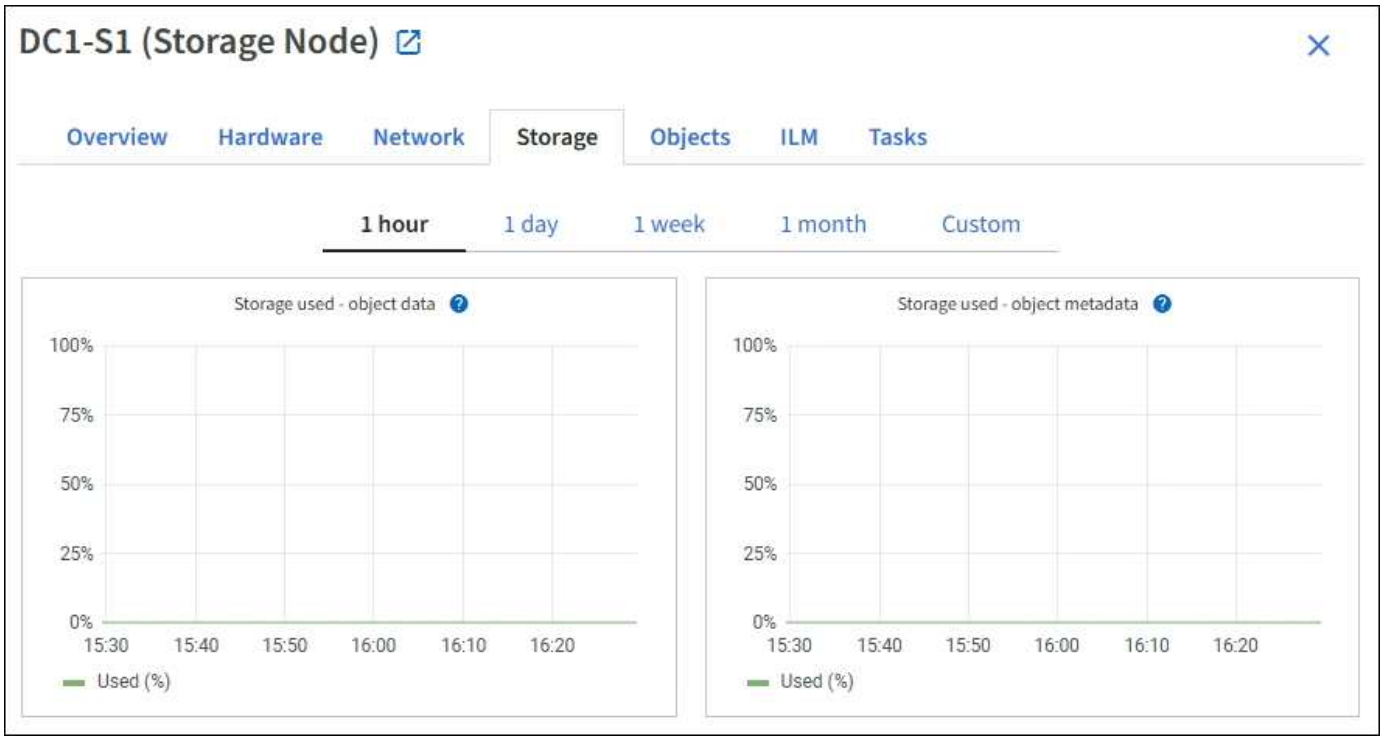
"存储"选项卡汇总了存储可用性和其他存储指标。

"存储"选项卡适用于所有节点、每个站点和整个网格。

存储使用图表

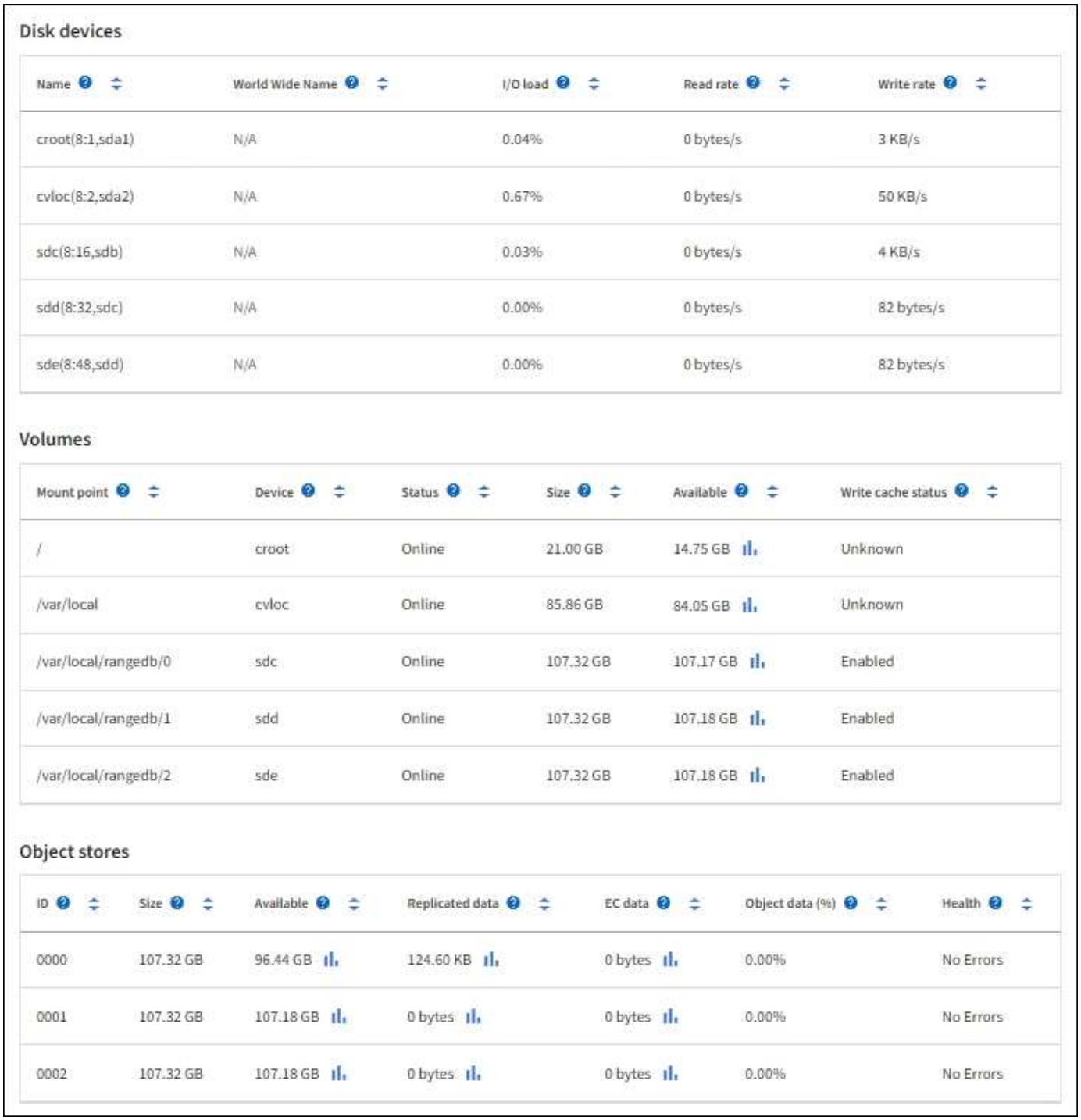
对于存储节点、每个站点和整个网格，"存储"选项卡包括显示对象数据和对象元数据随时间推移所用存储量的图形。

当节点未连接到网格时，例如在升级或断开连接状态下，某些指标可能不可用或被排除在站点和网格总计之外。节点重新连接到网格后，等待几分钟以使值稳定。



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

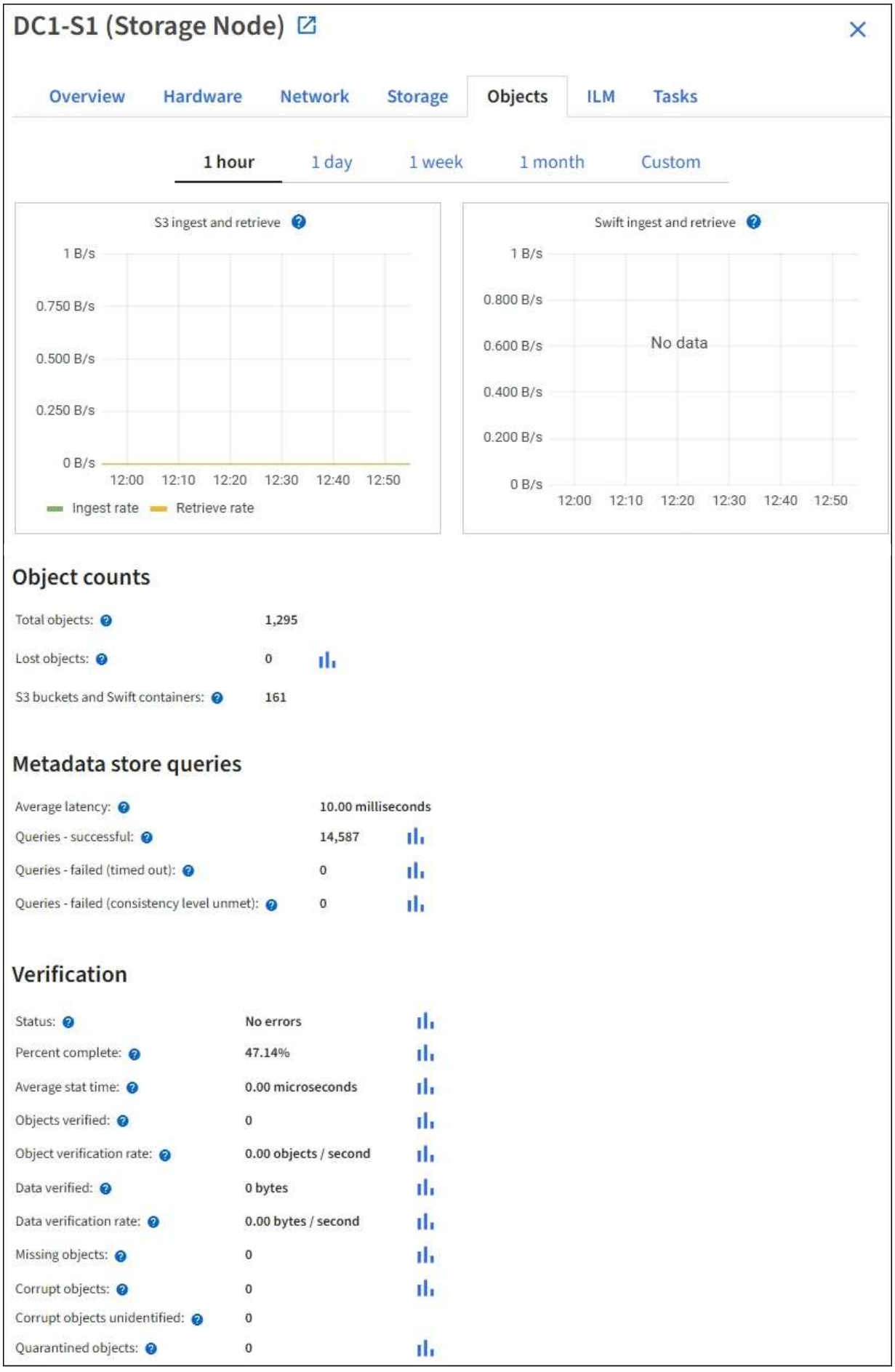
相关信息

"监控存储容量"

查看 **StorageGRID Objects** 选项卡

"对象"选项卡提供了有关 "S3 摄取和检索速率" 的信息。

每个存储节点、每个站点和整个网格都会显示"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。

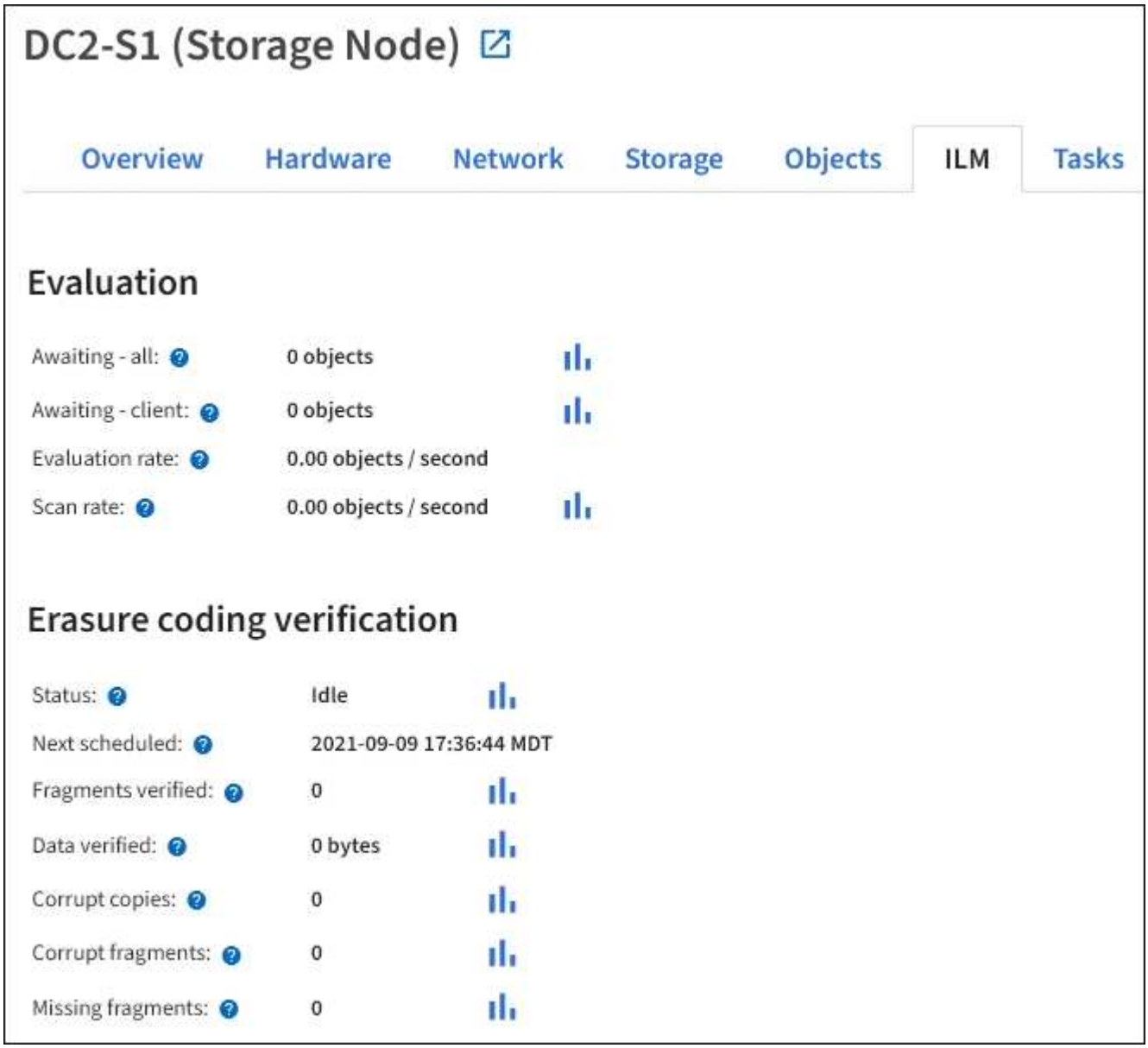

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

ILM 选项卡提供有关信息生命周期管理 (ILM) 操作的信息。

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 选项卡显示一段时间内 ILM 队列的图形。对于网格，此选项卡还提供完成所有对象的完整 ILM 扫描的估计时间。

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



相关信息

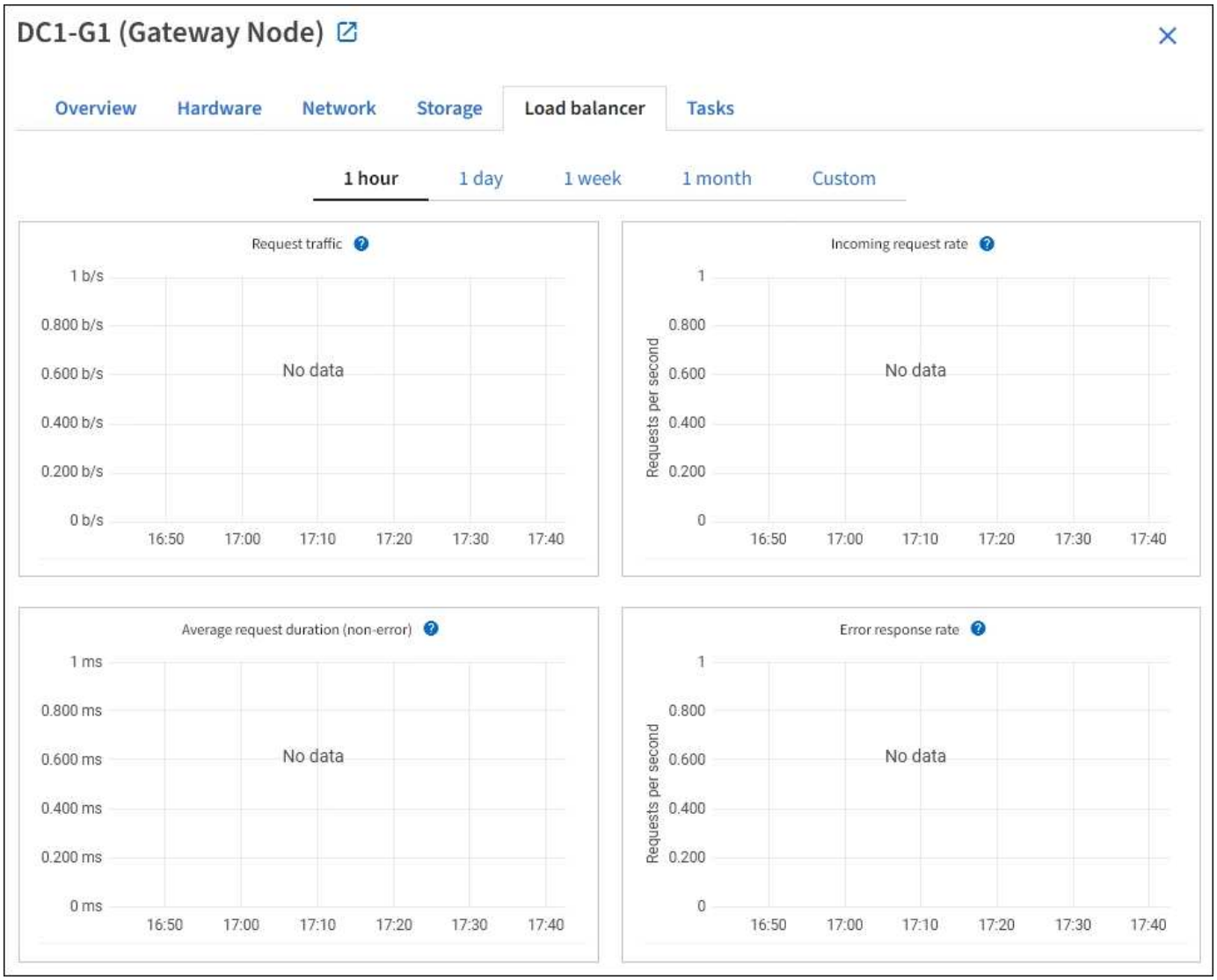
- "监控信息生命周期管理"
- "管理 StorageGRID"

查看 **StorageGRID** 负载平衡器选项卡

负载平衡器选项卡包括与负载平衡器服务操作相关的性能和诊断图形。

将显示管理节点和网关节点、每个站点和整个网格的负载平衡器选项卡。对于每个站点，负载平衡器选项卡提供该站点上所有节点的统计信息的汇总摘要。对于整个网格，负载平衡器选项卡提供所有站点统计数据的汇总摘要。

如果没有通过负载均衡器服务运行 I/O，或者没有配置负载均衡器，则图表显示"No data."



请求流量

此图表提供了负载均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，单位为位/秒。

> 此值会在每个请求完成时更新。因此，此值可能与低请求率或持续时间很长的请求的实时吞吐量不同。您可以查看"网络"选项卡，以更真实地了解当前的网络行为。

传入请求率

此图表按请求类型（GET、PUT、HEAD 和 DELETE）提供每秒新请求数的 3 分钟移动平均值。当新请求的标头通过验证后，此值将更新。

平均请求持续时间（非错误）

此图表按请求类型（GET、PUT、HEAD 和 DELETE）提供了请求持续时间的 3 分钟移动平均值。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，到完整的响应正文返回到客户端时结束。

错误响应率

此图表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了细分。

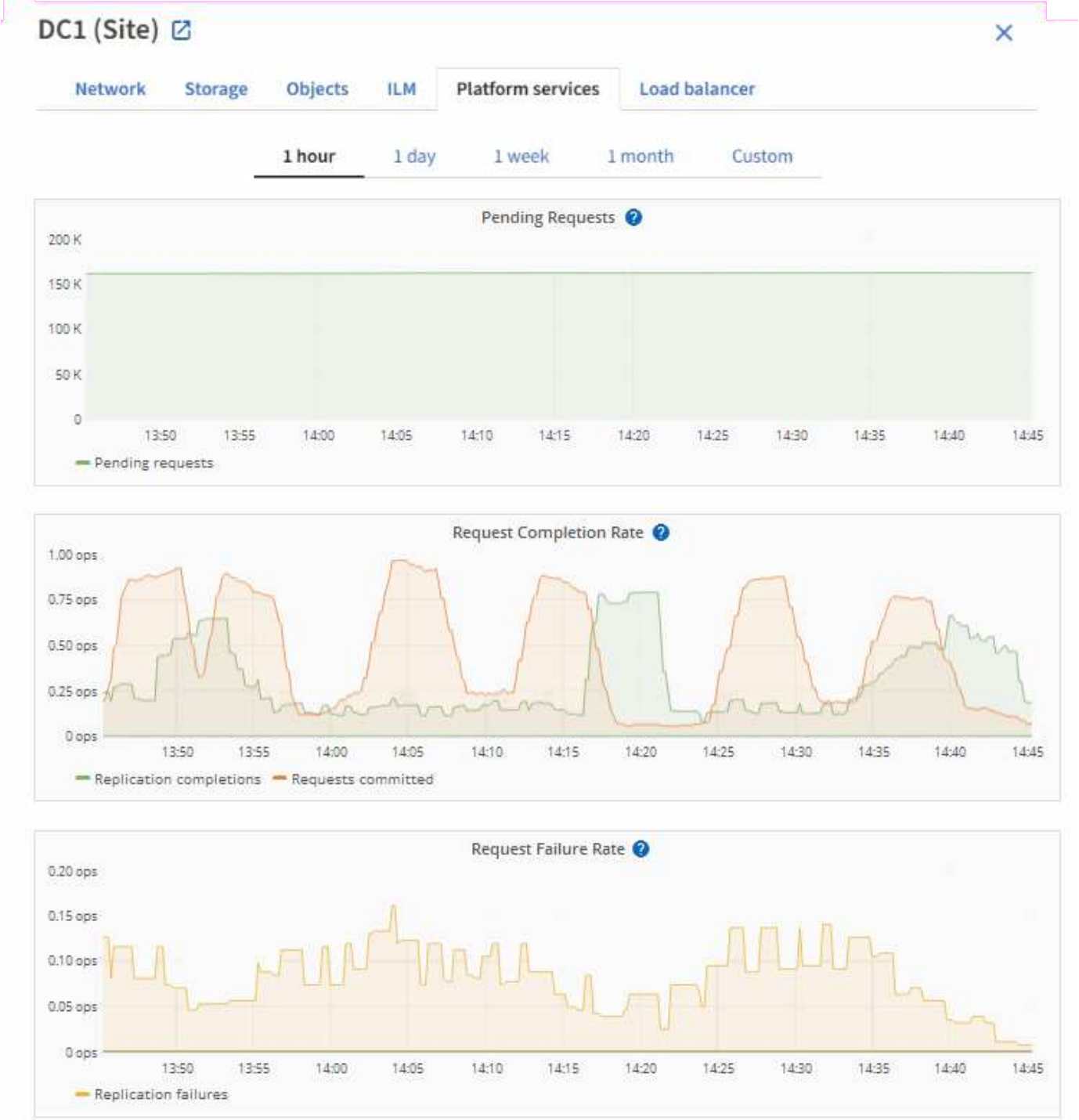
相关信息

- "监控负载平衡操作"
- "管理 StorageGRID"

查看 **StorageGRID** 平台服务选项卡

"平台服务"选项卡提供有关站点上任何 S3 平台服务操作的信息。

每个站点都会显示"平台服务"选项卡。此选项卡提供有关 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 "管理 StorageGRID 的说明"。

查看 **StorageGRID** 管理驱动器选项卡

通过管理驱动器选项卡，您可以访问支持此功能的设备中的驱动器的详细信息，并对其执行故障排除和维护任务。

使用"管理驱动器"选项卡，可以执行以下操作：

- 查看设备中数据存储驱动器的布局

- 查看列出每个驱动器位置、类型、状态、固件版本和序列号的表格
- 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，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，请参见 "使用"管理驱动器"选项卡"。

查看 **StorageGRID SANtricity System Manager** 选项卡

SANtricity System Manager 选项卡使您无需配置或连接存储设备的管理端口即可访问 SANtricity System Manager。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。

从 Grid Manager 访问 SANtricity System Manager 通常仅用于监控设备硬件和配置 E-Series AutoSupport。SANtricity System Manager 中的许多功能和操作（例如升级固件）不适用于监控您的 StorageGRID 设备。为避免出现问题，请始终遵循设备的硬件维护说明。要升级 SANtricity 固件，请参阅适用于您的存储设备的 "维护配置程序"。

SANtricity System Manager 选项卡仅对使用 E-Series 硬件的存储设备节点显示。

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

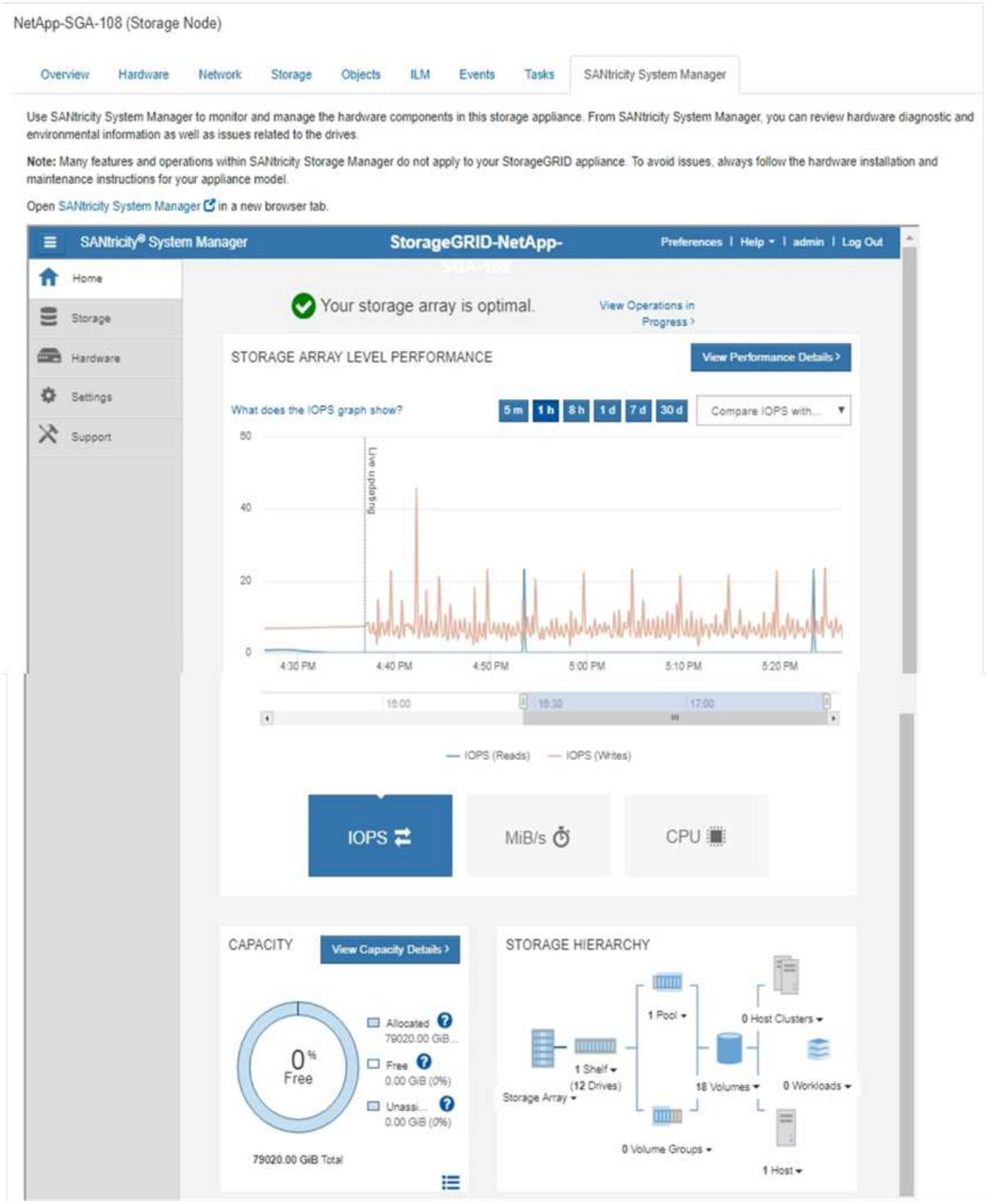
- 查看性能数据，例如存储阵列级别性能、I/O延迟、存储控制器CPU利用率和吞吐量。
- 检查硬件组件状态。
- 执行支持功能，包括查看诊断数据和配置 E 系列 AutoSupport。

要使用 SANtricity System Manager 为 E-Series AutoSupport 配置代理，请参阅 "通过 StorageGRID 发送 E-Series AutoSupport 包"。

要通过网格管理器访问 SANtricity System Manager，您必须具有 "存储设备管理员或 Root 访问权限"。

要使用 Grid Manager 访问 SANtricity System Manager，您必须拥有 SANtricity 固件 8.70 或更高版本。

该选项卡显示 SANtricity System Manager 的主页。



您可以使用 SANtricity System Manager 链接在新浏览器窗口中打开 SANtricity System Manager ，以便于查看。

要查看有关存储阵列级别性能和容量使用情况的详细信息，请将光标放置在每个图形上。

有关查看可从 SANtricity System Manager 选项卡访问的信息的更多详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

定期监控的信息

在 **StorageGRID** 中监控什么以及何时监控

即使 StorageGRID 系统可以在发生错误或网格部分节点不可用时继续运行，您也应该在潜在问题影响网格效率或可用性之前对其进行监控和处理。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "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持续监控的最重要信息的指导。

要监控的内容	频率
"系统运行状况"	每日
"存储节点对象和元数据容量" 的消耗速率	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 客户端操作"	每周
"负载平衡操作"	初始配置后和任何配置更改后
"网格联盟连接"	每周

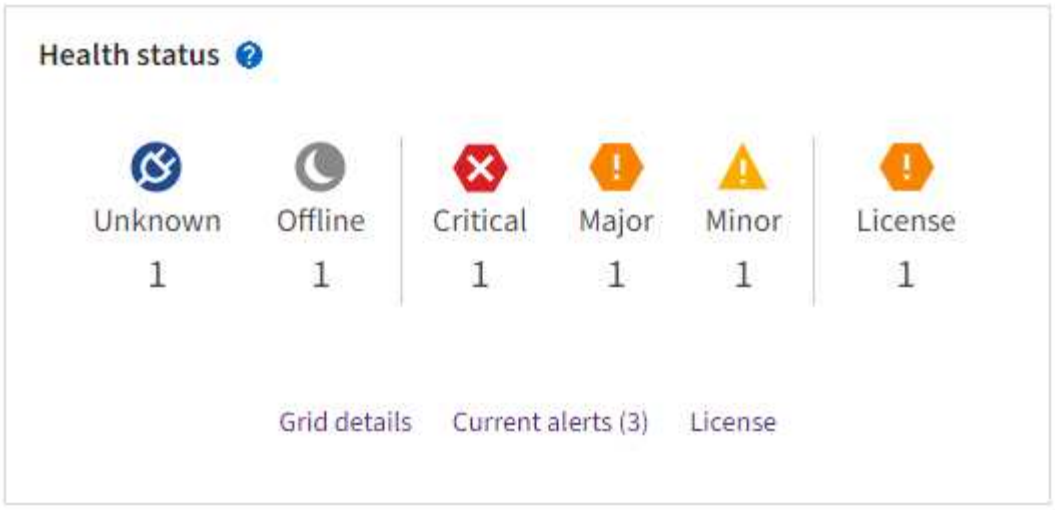
在 **StorageGRID** 中监控系统运行状况

每天监控 StorageGRID 系统的整体健康状况。

关于此任务

当网格的某些部分不可用时，StorageGRID 系统可以继续运行。警报指示的潜在问题不一定是系统操作问题。请调查 Grid Manager 信息板运行状况卡上汇总的问题。

若要在警报触发时立即收到通知，您可以 "为警报设置电子邮件通知"或"配置 SNMP 陷阱"。



存在问题时，将显示允许您查看其他详细信息的链接：

链路	出现在.....
网格详细信息	任何节点都已断开连接（连接状态未知或管理性关闭）。
当前警报（严重、重大、轻微）	警报是 <<${post_edited_translations.segment},当前活动>>。
最近已解决的提醒	过去一周内触发的警报 <<${post_edited_translations.segment},现已解决>>。
许可证	此 StorageGRID 系统的软件许可证存在问题。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，则可能会影响关键的 StorageGRID 操作。监控节点连接状态并及时解决任何问题。

图标	问题描述	需采取行动
	未连接 - 未知 由于未知原因，节点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，或者节点可能因电源故障或意外中断而失去网络连接。 *无法与节点通信*警报也可能被触发。其他警报也可能处于活动状态。	需要立即注意。<<${post_edited_translations.segment},选择每个警报>>并遵循建议的操作。 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：在托管关闭操作期间，节点可能显示为未知。在这些情况下，可以忽略未知状态。

图标	问题描述	需采取行动
	未连接 - 管理性关闭 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。一个或多个警报也可能处于活动状态。 根据潜在问题，这些节点通常无需干预即可重新上线。	确定是否有任何警报影响此节点。 如果一个或多个警报处于活动状态，<<${post_edited_translations.segment},选择每个警报>>请按照建议的操作执行。
	已连接 节点已连接到网格。	无需执行任何操作。

${post_edited_translations.segment}

当前警报：触发警报时，仪表板上会显示警报图标。节点页面上还会显示该节点的警报图标。如果"警报电子邮件通知已配置"，则还会发送电子邮件通知，除非警报已被静音。

已解决的警报：您可以搜索和查看已解决的警报历史记录。

或者，您已观看视频：

警报概述

下表描述了当前和已解决警报在 Grid Manager 中显示的信息。

列标头	问题描述
名称或标题	警报的名称及其描述。
严重性	警报的严重程度。对于当前警报，如果对多个警报进行分组，标题行会显示该警报在每个严重程度下发生的实例数。 严重：存在已停止 StorageGRID 节点或服务正常操作的异常情况。您必须立即解决根本问题。如果问题未得到解决，可能会导致服务中断和数据丢失。 重大：存在影响当前操作或接近严重警报阈值的异常情况。您应该调查重大警报并解决任何潜在问题，以确保异常情况不会阻止 StorageGRID 节点或服务的正常运行。 **Minor**：系统正常运行，但存在异常情况，如果继续运行，可能会影响系统的运行能力。您应该监控并解决未自行清除的轻微警报，以确保它们不会导致更严重的问题。

列标头	问题描述
时间触发	当前警报：在您的本地时间和 UTC 中触发警报的日期和时间。如果对多个警报进行了分组，标题行将显示警报最新实例（*newest*）和最旧实例（*oldest*）的时间。 已解决的警报：触发警报的时间。
站点/节点	正在发生或已发生警报的站点和节点的名称。
状态	警报是处于活动状态、静音状态还是已解决。如果对多个警报进行分组，并在下拉列表中选择了 **All alerts**，标题行将显示该警报处于活动状态的实例数以及已静默的实例数。
解决时间（仅限已解决的警报）	此警报已解决多久。
当前值或_数据值_	导致触发警报的指标值。对于某些警报，会显示其他值，以帮助您了解和调查警报。例如，为 **Low object data storage** 警报显示的值包括使用的磁盘空间百分比、磁盘空间总量以及使用的磁盘空间量。 注意： 如果对多个当前警报进行分组，则标题行中不会显示当前值。
触发值（仅已解决的警报）	导致触发警报的指标值。对于某些警报，会显示其他值，以帮助您了解和调查警报。例如，为 **Low object data storage** 警报显示的值包括使用的磁盘空间百分比、磁盘空间总量以及使用的磁盘空间量。

步骤

1. 选择*当前警报*或*已解决警报*链接可查看这些类别中的警报列表。您还可以通过选择*节点* > ***node*** > 概览，然后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：

   - 最近触发的警报将首先显示。
   - 相同类型的多个警报显示为一个组。
   - 已静音的警报不会显示。
   - 对于特定节点上的特定警报，如果超过一个严重程度达到阈值，则仅显示最严重的警报。也就是说，如果达到次要、主要和严重程度的警报阈值，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，请选择向下插入符号 ⌄。要折叠组中的单个警报，请选择向上插入符号 ⌃，或选择组的名称。
3. 要显示单个警报而不是警报组，请清除*Group alerts*复选框。
4. 要对当前警报或警报组进行排序，请选择每个列标题中的向上/向下箭头 ⇅。
   - 当选择*组警报*时，每个组内的警报组和单个警报都会被排序。例如，您可能希望按*触发时间*对组中的警报进行排序，以查找特定警报的最新实例。

- 清除*组警报*后，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（**All alerts**、**Active** 或 **Silenced**）过滤当前警报，请使用表格顶端的下拉菜单。

   请参阅 "静音警报通知"。

6. 要对已解决的警报进行排序：
   - 从*触发时*下拉菜单中选择时间段。
   - 从*严重程度*下拉菜单中选择一个或多个严重程度。
   - 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，以过滤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。对话框提供所选警报的详细信息和建议操作。
8. （可选）对于特定警报，选择"使此警报静音"可使导致触发此警报的警报规则静音。

   要使警报规则静音，您必须具有 "管理警报或 Root 访问权限"。

   > 决定将警报规则静音时要小心。如果警报规则被静音，则可能无法检测到潜在问题，直到该问题阻止关键操作完成。

9. 要查看警报规则的当前条件：
   a. 在警报详细信息中，选择*查看条件*。

      出现一个弹出窗口，列出每个定义的严重程度的 Prometheus 表达式。

   b. 要关闭弹出窗口，请单击弹出窗口之外的任何位置。
10. （可选）选择*编辑规则*以编辑触发此警报的警报规则。

    要编辑警报规则，您必须具有 "管理警报或 Root 访问权限"。

    > 在决定编辑警报规则时要小心。如果更改触发器值，则在阻止关键操作完成之前，可能无法检测到潜在问题。

11. 要关闭警报详细信息，请选择*Close*。

监控 **StorageGRID** 中的存储容量

监控可用的总可用空间，以确保 StorageGRID 系统不会耗尽对象或对象元数据的存储空间。

StorageGRID 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 数据库保留特定数量的空间。监控对象和对象元数据所消耗的总空间量，以及每项所消耗的空间量的趋势。这将使您能够提前规划节点的添加并避免任何服务中断。

您可以"查看存储容量信息"针对整个网格、每个站点以及 StorageGRID 系统中的每个存储节点。

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。了解存储容量随时间的变化情况有助于您计划在网格的可用存储容量消耗之前添加存储节点或存储卷。

网格管理器仪表板可让您快速评估整个网格和每个数据中心的可用存储量。节点页面提供了对象数据和对象元数据的更详细值。

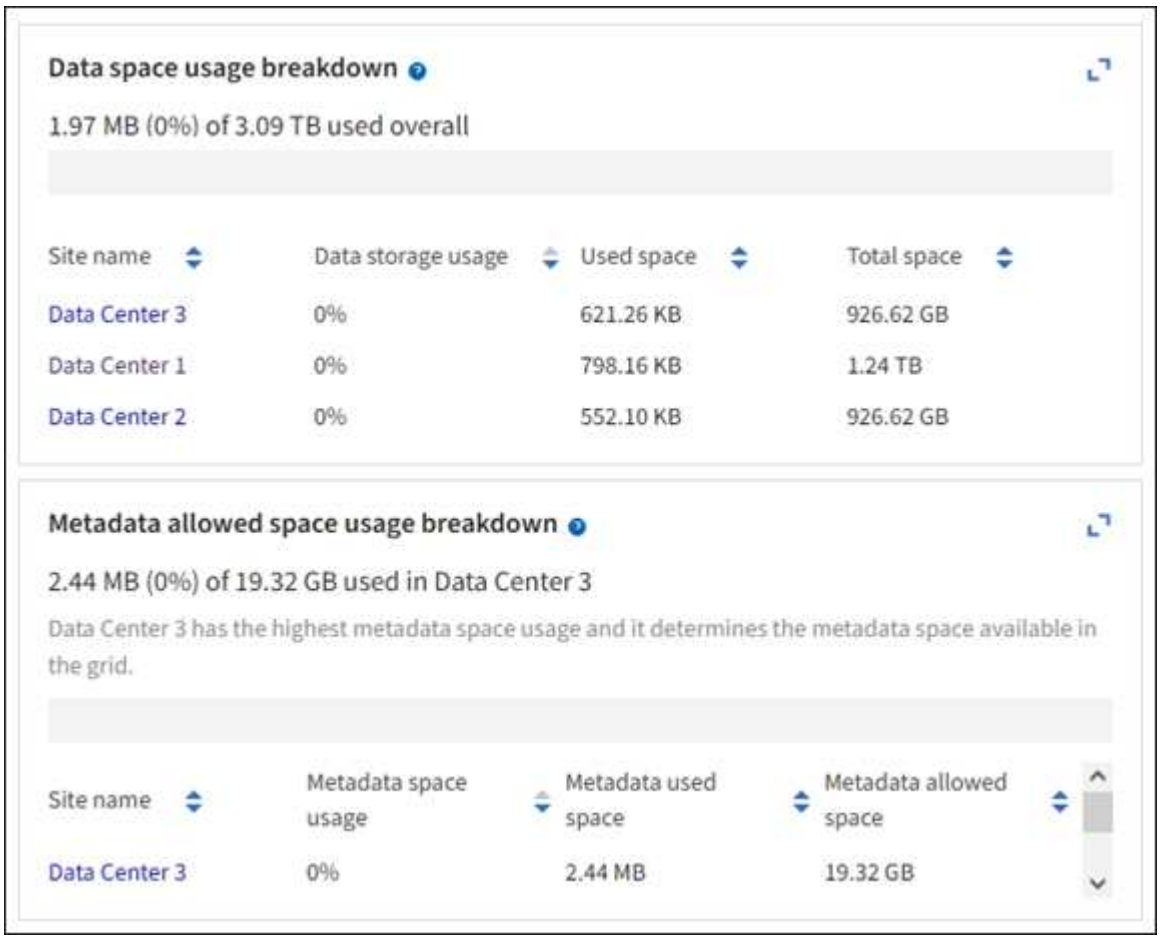
步骤

1. 评估整个网格和每个数据中心的可用存储容量。

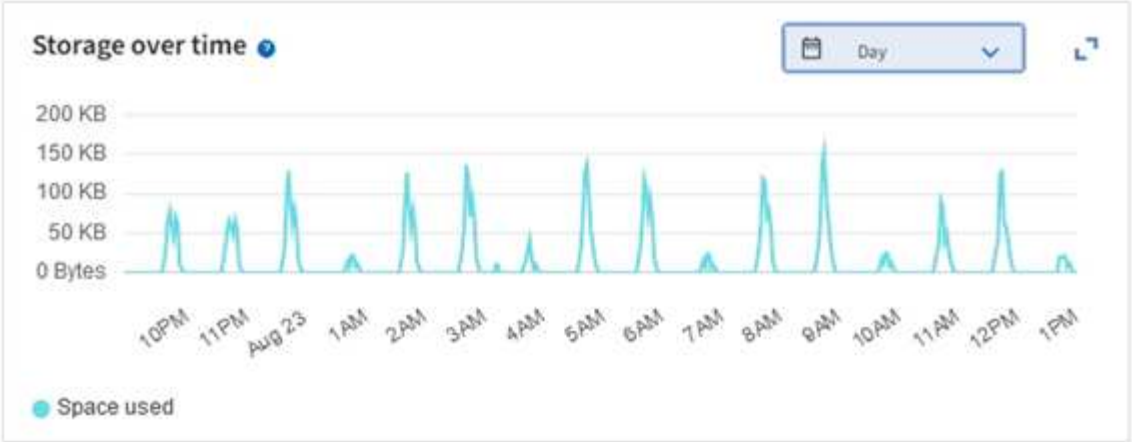
   a. 选择 **Dashboard > Overview**。

   b. 请注意数据空间使用情况细分和元数据允许的空间使用情况细分卡上的值。每张卡都列出了存储使用量的百分比、已用空间的容量以及站点可用或允许的总空间。

      此摘要不包括存档媒体。



   a. 请注意存储随时间推移卡上的图表。使用时间段下拉菜单可帮助您确定存储消耗的速度。



2. 使用"节点"页面可获取有关已使用多少存储空间以及网格中对象数据和对象元数据的可用存储空间的其他详细信息。

   a. 选择 **Nodes**。

   b. 选择 ***grid*** > **Storage**。

   c. 将光标放在*使用的存储 - 对象数据*和*使用的存储 - 对象元数据*图表上，以查看整个网格有多少对象存储和对象元数据存储可用，以及随时间推移使用了多少。

   站点或网格的总值不包括至少五分钟未报告指标的节点，例如离线节点。

3. 计划在网格的可用存储容量耗尽之前执行扩展，以添加存储节点或存储卷。

   在规划扩建时间时，请考虑采购和安装额外存储需要多长时间。

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

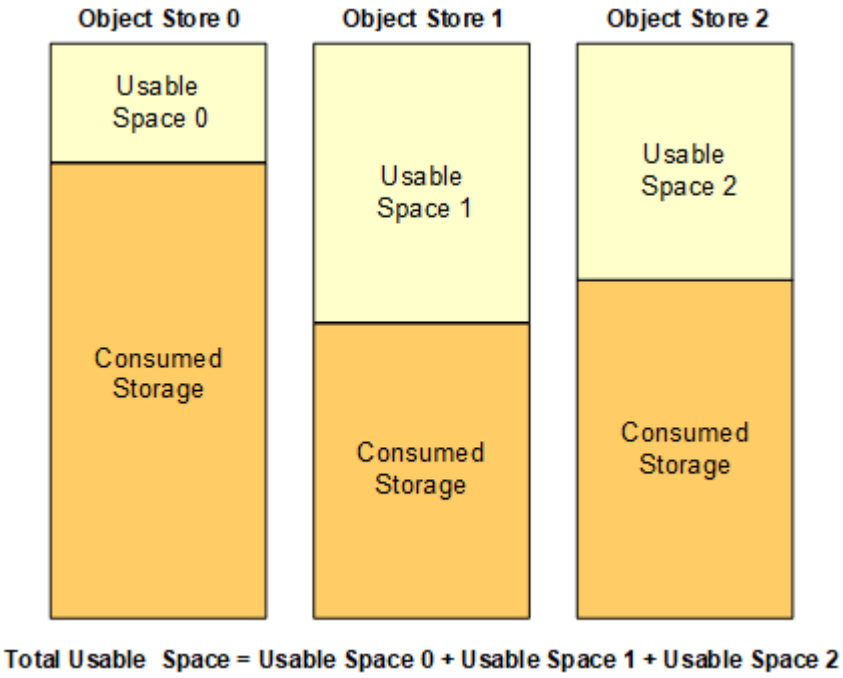
有关规划存储扩展的详细信息，请参见 "扩展 StorageGRID 的说明"。

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，以确保节点具有足够空间用于新对象数据。

关于此任务

可用空间是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内所有对象存储上的可用空间相加来计算的。



步骤

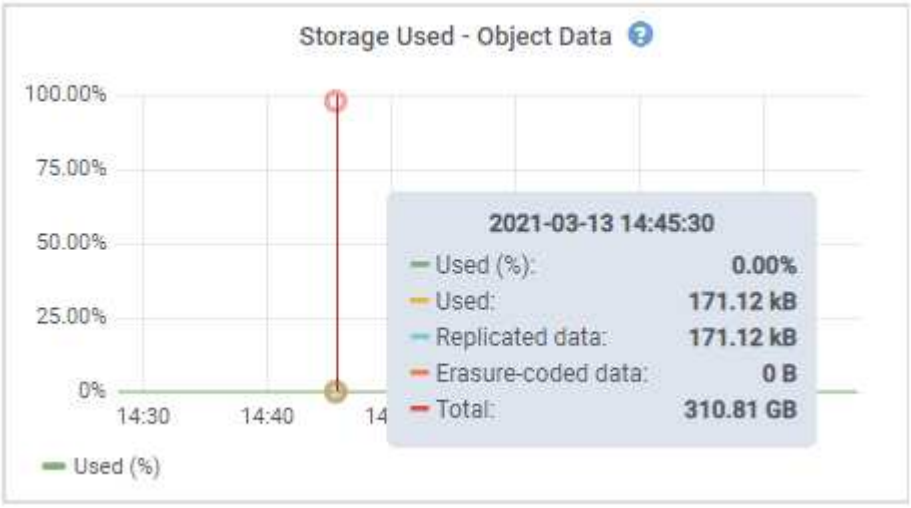
1. 选择*节点* > 存储节点 > 存储。

   此时将显示此节点的图形和表格。

2. 将光标置于已用存储 - 对象数据图形上。

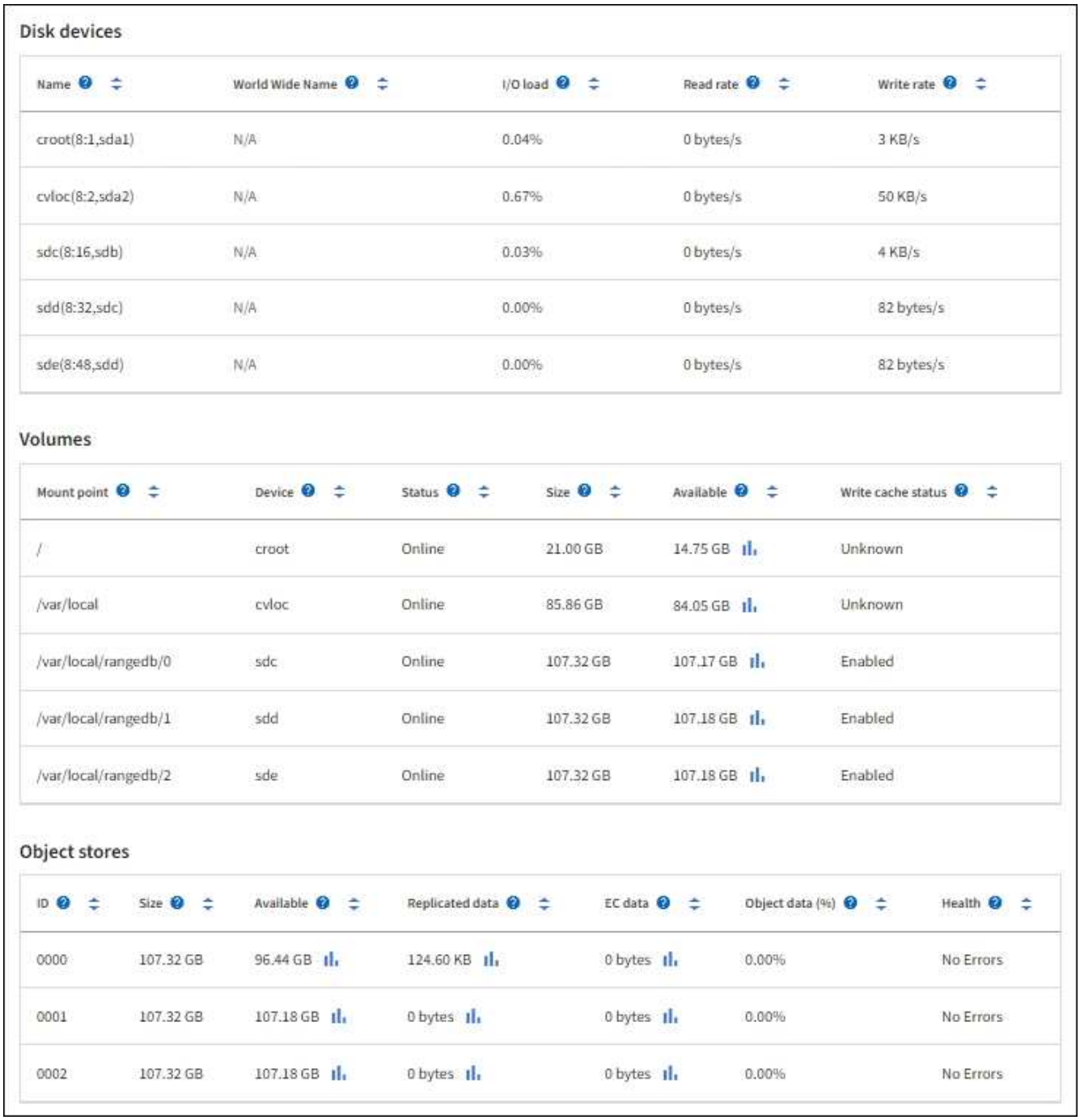
   此时将显示以下值：

   - 已用 **(%)**：已用于对象数据的总可用空间的百分比。
   - 已使用：已用于对象数据的总可用空间量。
   - 已复制数据：此节点、站点或网格上已复制对象数据量的估计值。
   - 纠删码数据：此节点、站点或网格上纠删码对象数据量的估计值。
   - **Total**：此节点、站点或网格上的可用空间总量。Used 值是 `storagegrid_storage_utilization_data_bytes`度量值。



3. 查看图表下方的 Volumes 和 Object stores 表中的 Available 值。

要查看这些值的图形，请单击"可用列"中的图表图标 。



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. 随时间推移监控这些值，以估计可用存储空间的消耗速率。
5. 若要维护正常系统操作，请在使用可用空间之前添加存储节点、添加存储卷或存档对象数据。

   在规划扩建时间时，请考虑采购和安装额外存储需要多长时间。

   > 如果您的 ILM 策略使用纠删码，您可能希望在现有存储节点已满约 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"。

   当存储节点上用于存储对象数据的空间不足时，将触发 "对象数据存储量低" 警报。

${post_edited_translations.segment}

监控每个存储节点的元数据使用情况，以确保有足够的空间可用于基本数据库操作。在对象元数据超过允许的元数据空间的 100% 之前，必须在每个站点添加新的存储节点。

关于此任务

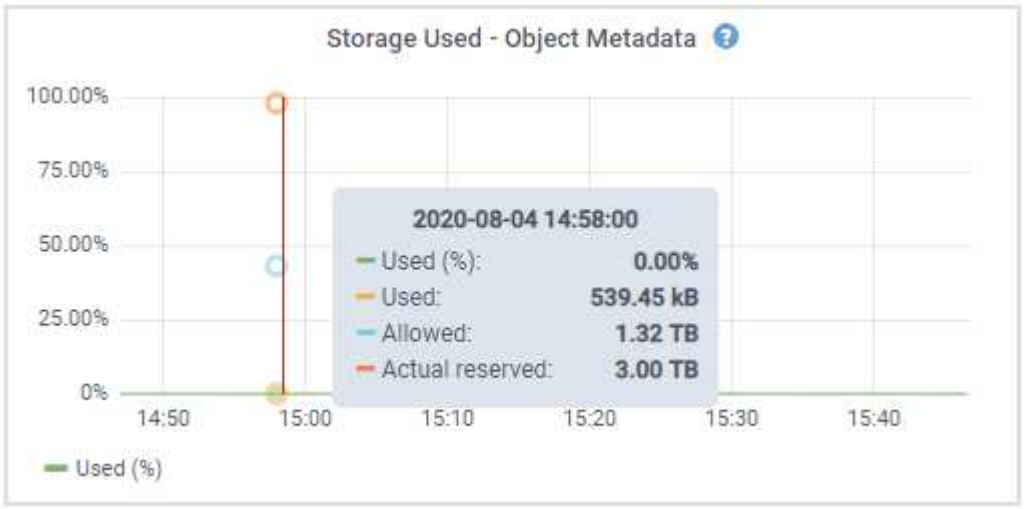
StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并保护对象元数据免于丢失。这三个副本均匀分布在每个站点的所有存储节点上，使用为每个存储节点的存储卷 0 上的元数据预留的空间。

在某些情况下，网格的对象元数据容量可能会比其对象存储容量消耗得更快。例如，如果您通常摄取大量小型对象，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。

可以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、多部分上传中的部分总数以及 ILM 存储位置的更改频率。

步骤

1. 选择*节点* > 存储节点 > 存储。
2. 将光标放在"已用存储 - 对象元数据"图形上，以查看特定时间的值。



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

在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

此存储节点上允许的对象元数据空间。要了解如何确定每个存储节点的此值，请参见 "允许元数据空间的完整说明"。

Prometheus 指标： `storagegrid_storage_utilization_metadata_allowed_bytes`

实际预留

在此存储节点上为元数据保留的实际空间。包括允许的空间和基本元数据操作所需的空间。要了解如何为每个存储节点计算此值，请参见 "元数据实际预留空间的完整说明"。

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，例如离线节点。

3. 如果 **Used (%)** 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，会触发 低元数据存储 警报。如果对象元数据占用超过 100% 的允许空间，则可能会出现不良结果。

添加新节点时，系统会自动重新平衡站点内所有存储节点的对象元数据。请参阅"扩展 StorageGRID 系统的说明"。

监控空间使用量预测

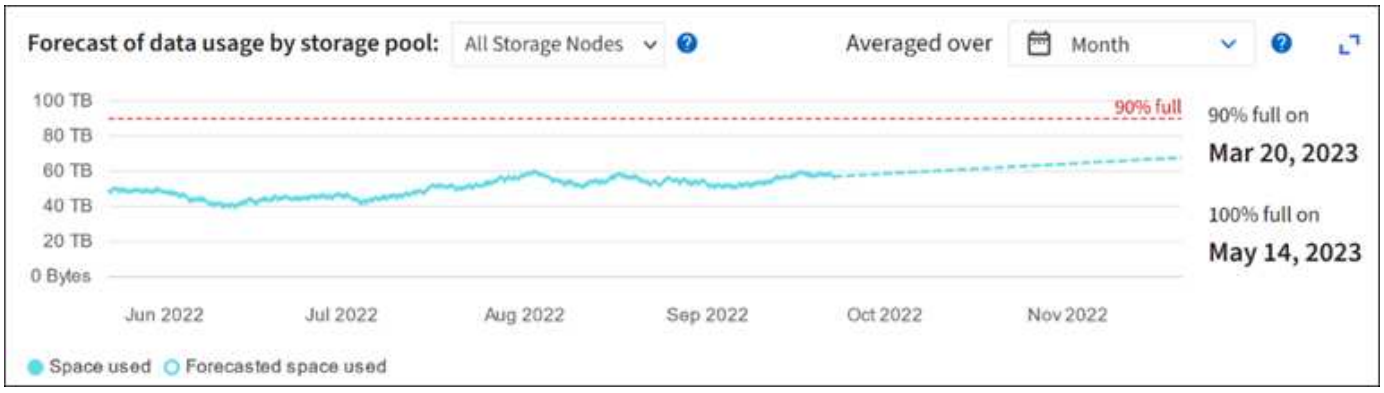
监控用户数据和元数据的空间使用预测，以估计何时需要 "展开网格"。

如果您注意到消耗率随时间变化，请从 **Averaged over** 下拉菜单中选择较短的范围，以仅反映最近的摄取模式。如果您注意到季节性模式，请选择较长的范围。

如果您有新的 StorageGRID 安装，请在评估空间使用预测之前允许数据和元数据累积。

步骤

1. 在控制面板上，选择*存储空间*。
2. 查看仪表板卡、按存储池预测数据使用情况以及按站点预测元数据使用情况。
3. 使用这些值来估计何时需要为数据和元数据存储添加新的存储节点。



监控 **StorageGRID** 中的信息生命周期管理

信息生命周期管理 (ILM) 系统为存储在网格中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 策略和相关的 ILM 规则确定制作的副本数、创建的

副本类型、放置副本的位置以及保留每个副本的时间长度。

对象摄取和其他与对象相关的活动可能超过 StorageGRID 评估 ILM 的速率，导致系统将无法近乎实时地完成 ILM 放置指令的对象排入队列。您应该监控 StorageGRID 是否能跟上客户端操作。

使用 **Grid Manager** 仪表板选项卡

步骤

使用网格管理器仪表板上的 ILM 选项卡来监控 ILM 操作：

1. ${post_edited_translations.segment}
2. 从仪表板中，选择 ILM 选项卡，并记录 ILM 队列（对象）卡和 ILM 评估率卡上的值。

   仪表板上 ILM 队列（对象）卡中出现临时峰值是正常现象。但是，如果队列持续增加且从不下降，则网格需要更多资源才能高效运行：要么增加更多 Storage Nodes，要么在 ILM 策略将对象放置在远程位置时增加更多网络带宽。

使用"节点"页面

步骤

此外，使用*节点*页面调查 ILM 队列：

> *节点*页面上的图表将在未来的 StorageGRID 版本中替换为相应的仪表板卡。

1. 选择 **Nodes**。
2. 选择 网格名称 > **ILM**。
3. 将光标放在 ILM 队列图上，以查看以下属性在给定时间点的值：
   - 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。
   - 排队对象（来自所有操作）：等待 ILM 评估的对象总数。
   - 扫描速率（对象/秒）：扫描网格中的对象并将其排入 ILM 队列的速率。
   - 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。

   > ILM 队列部分仅包含在网格中。此信息不会显示在站点或存储节点的 ILM 选项卡上。

4. 在 ILM 队列部分，查看以下属性。
   - 扫描周期 - 估计：完成所有对象的完整 ILM 扫描的预计时间。

     > 完全扫描并不能保证已将 ILM 应用于所有对象。

   - 尝试修复：已尝试的已复制数据的对象修复操作总数。每次存储节点尝试修复高风险对象时，此计数都会增加。如果网格变得繁忙，则优先处理高风险 ILM 修复。

     如果修复后复制失败，相同的对象修复可能会再次增加。+ 当您监控存储节点卷恢复的进度时，这些属性非常有用。如果尝试修复的次数已停止增加，并且已完成完全扫描，则修复可能已完成。

5. 或者，为 `storagegrid_ilm_scan_period_estimated_minutes`和 `storagegrid_ilm_repairs_attempted`提交

Prometheus 查询。

监控 StorageGRID 中的网络和系统资源

节点和站点之间的网络的完整性和带宽，以及单个网格节点的资源使用情况，对于高效运行至关重要。

监控网络连接和性能

如果您的信息生命周期管理 (ILM) 策略在站点之间复制复制对象或使用提供站点丢失保护的方案存储纠删编码的对象，则网络连接和带宽尤为重要。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的位置。这可能导致载入失败（当为 ILM 规则选择了严格载入选项时），或者导致载入性能低下和 ILM 积压。

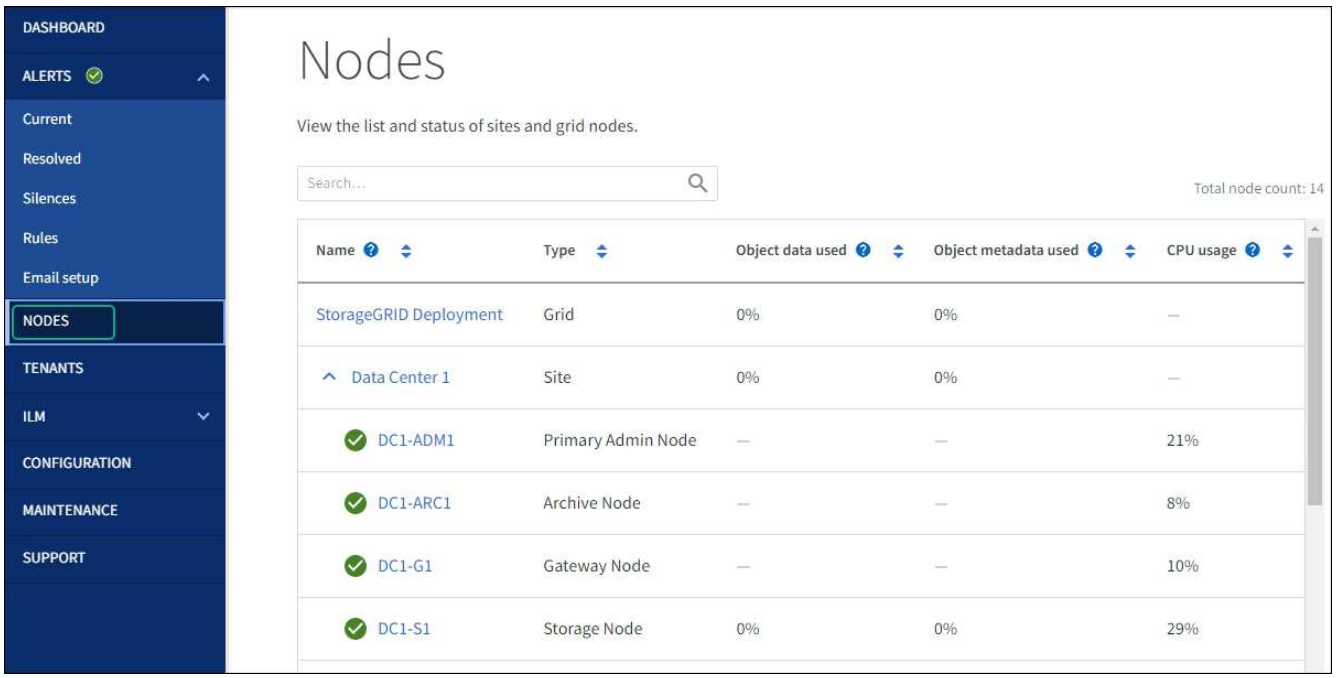
请使用 Grid Manager 监控连接和网络性能，以便及时解决任何问题。

此外，请考虑 "创建网络流量分类策略" 以便监控与特定租户、存储桶、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

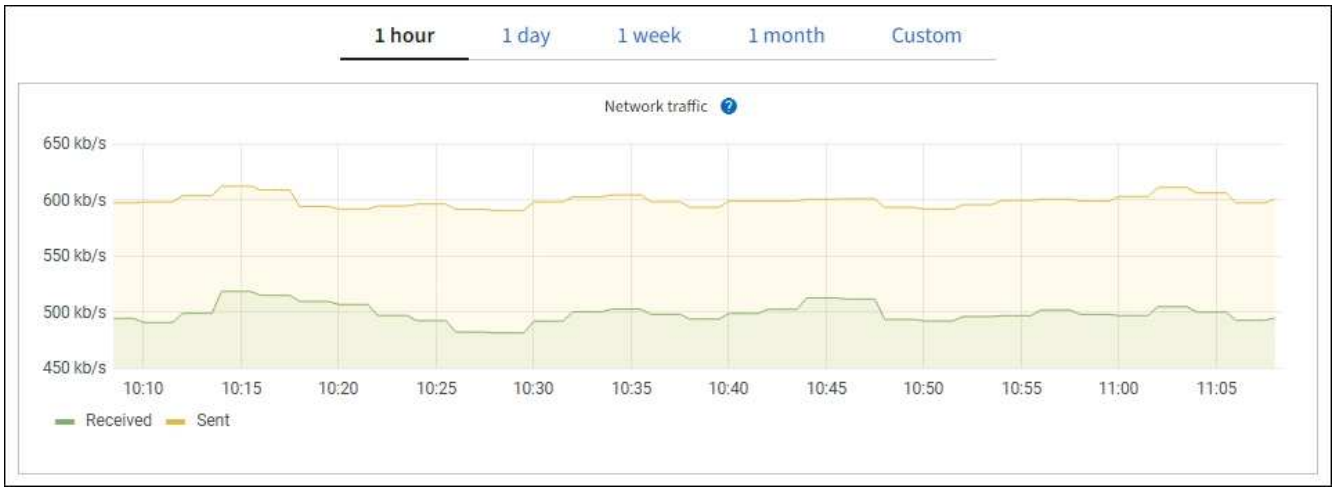
1. 选择 **Nodes**。

   此时将显示节点页面。网格中的每个节点都以表格格式列出。



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

   网络流量图表可提供整个网格、数据中心站点或节点的整体网络流量的摘要。



a. 如果您选择了网格节点，请向下滚动查看页面的*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，向下滚动查看页面的*网络通信*部分。

接收和传输表显示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

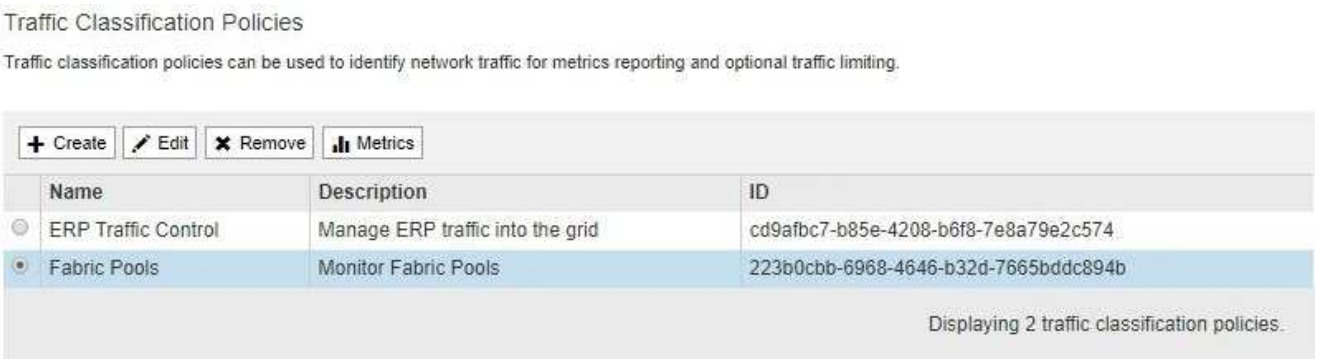
Transmit

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来监控网络流量。

a. 选择*配置* > 网络 > 流量分类。

此时将显示"Traffic Classification Policies"（流量分类策略）页面，表中列出了现有策略。



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

b. 请查看图表，了解与该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，请分析流量受限的频率，并确定该策略是否继续满足您的需求。不时地，"根据需要调整每项流量分类策略"。

相关信息

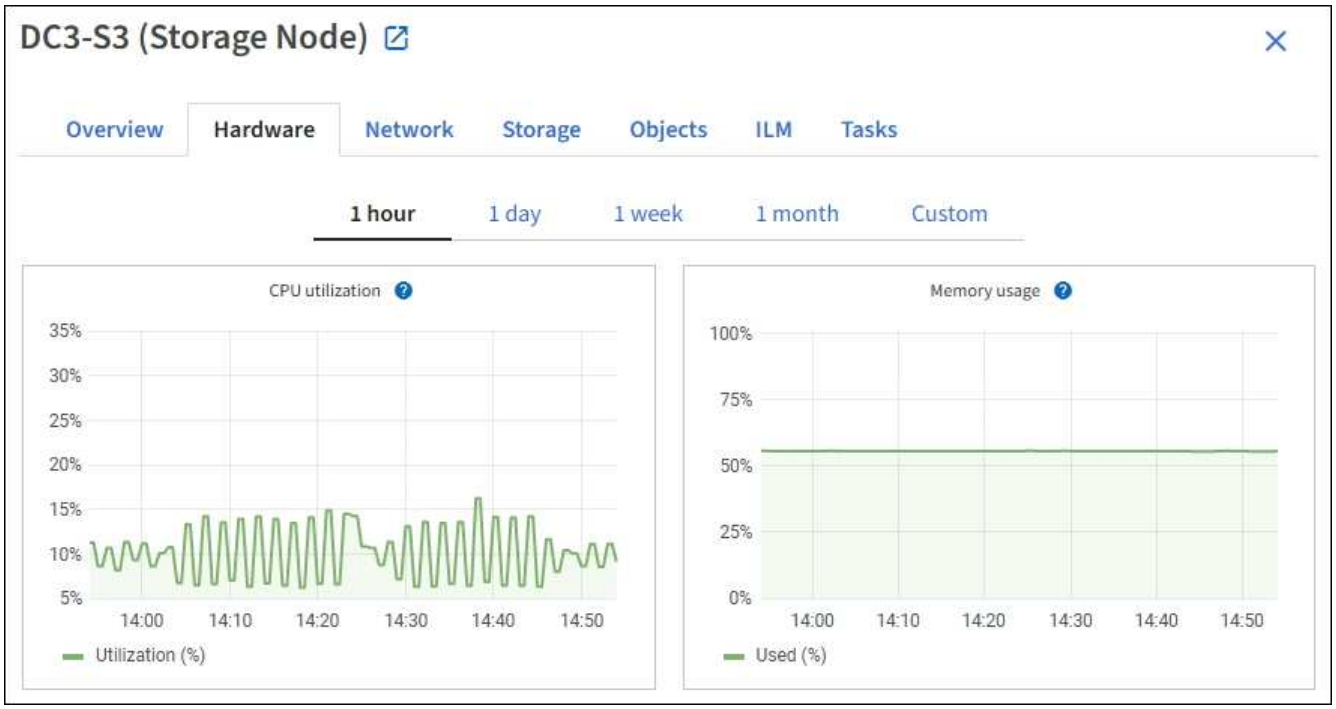
- "查看"网络"选项卡"
- "监控节点连接状态"

监控节点级资源

监控单个网格节点以检查其资源使用水平。如果节点持续过载，则可能需要更多节点来实现高效操作。

步骤

1. 从*节点*页面中，选择节点。
2. 选择 **Hardware** 选项卡以显示 CPU 利用率和内存使用率的图形。



3. 要显示不同的时间间隔，请选择图表或图形上方的一个控件。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。所有组件的状态应为"Nominal"。请检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 **StorageGRID** 中的租户活动

所有 S3 客户端活动都与 StorageGRID 租户帐户相关联。您可以使用 Grid Manager 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 仪表板收集有关租户如何使用 StorageGRID 的更多详细信息。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "Root 访问权限或租户帐户权限"。

查看所有租户

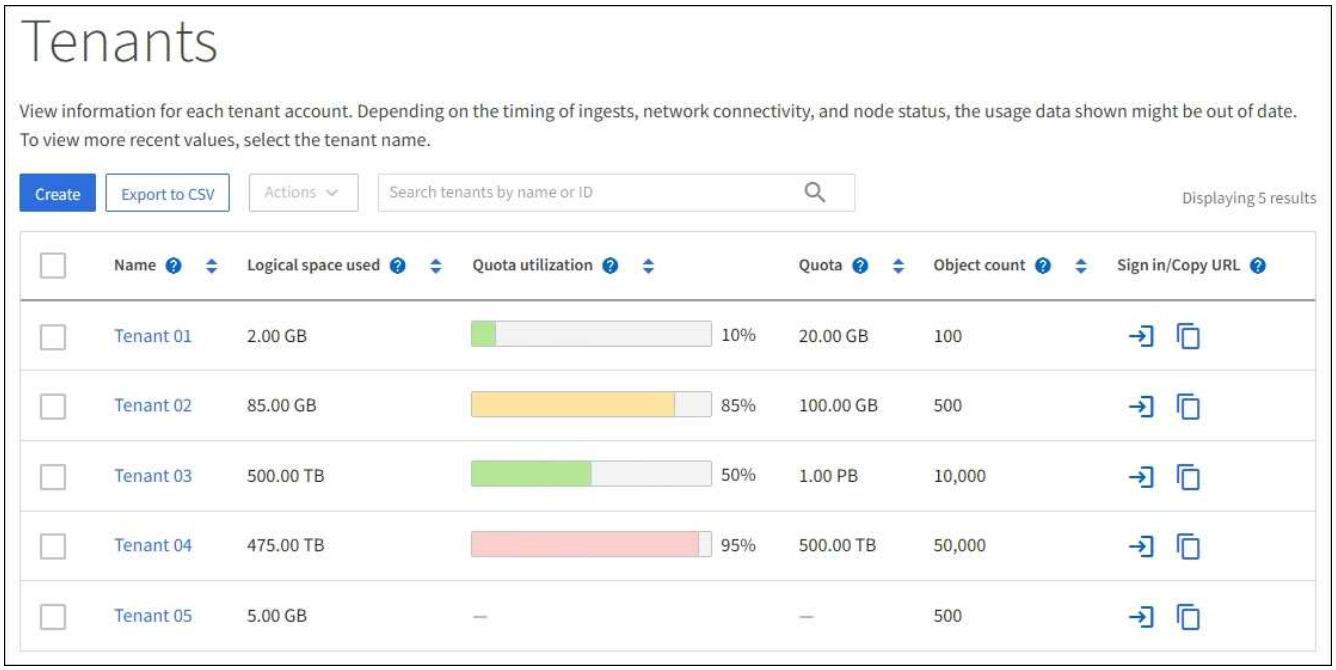
租户页面显示所有当前租户帐户的基本信息。

步骤

1. ${post_edited_translations.segment}
2. 查看租户页面上显示的信息。

   列出了每个租户的已用逻辑空间、配额使用情况、配额和对象计数。如果未为租户设置配额，则配额使用量和配额字段包含破折号（—）。

   > 属于此租户的所有对象的逻辑大小包括不完整和正在进行的多部分上传。此大小不包括用于 ILM 策略的额外物理空间。空间使用值为估算值。这些估算值受摄取时间、网络连接和节点状态的影响。



3. （可选）通过选择*登录/复制 URL* 列中的登录链接 登录到租户帐户。
4. 或者，通过选择*登录/复制 URL* 列中的复制 URL 链接，复制租户登录页面的 URL。
5. （可选）选择 **Export to CSV** 以查看和导出包含所有租户使用值的 `.csv`文件。

   系统会提示您打开或保存 `.csv`文件。

   `.csv` 文件的内容类似于以下示例：

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

   您可以在电子表格应用程序中打开 `.csv` 文件，也可以在自动化中使用它。

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

   如果帐户包含任何存储桶或容器，则无法删除租户帐户。

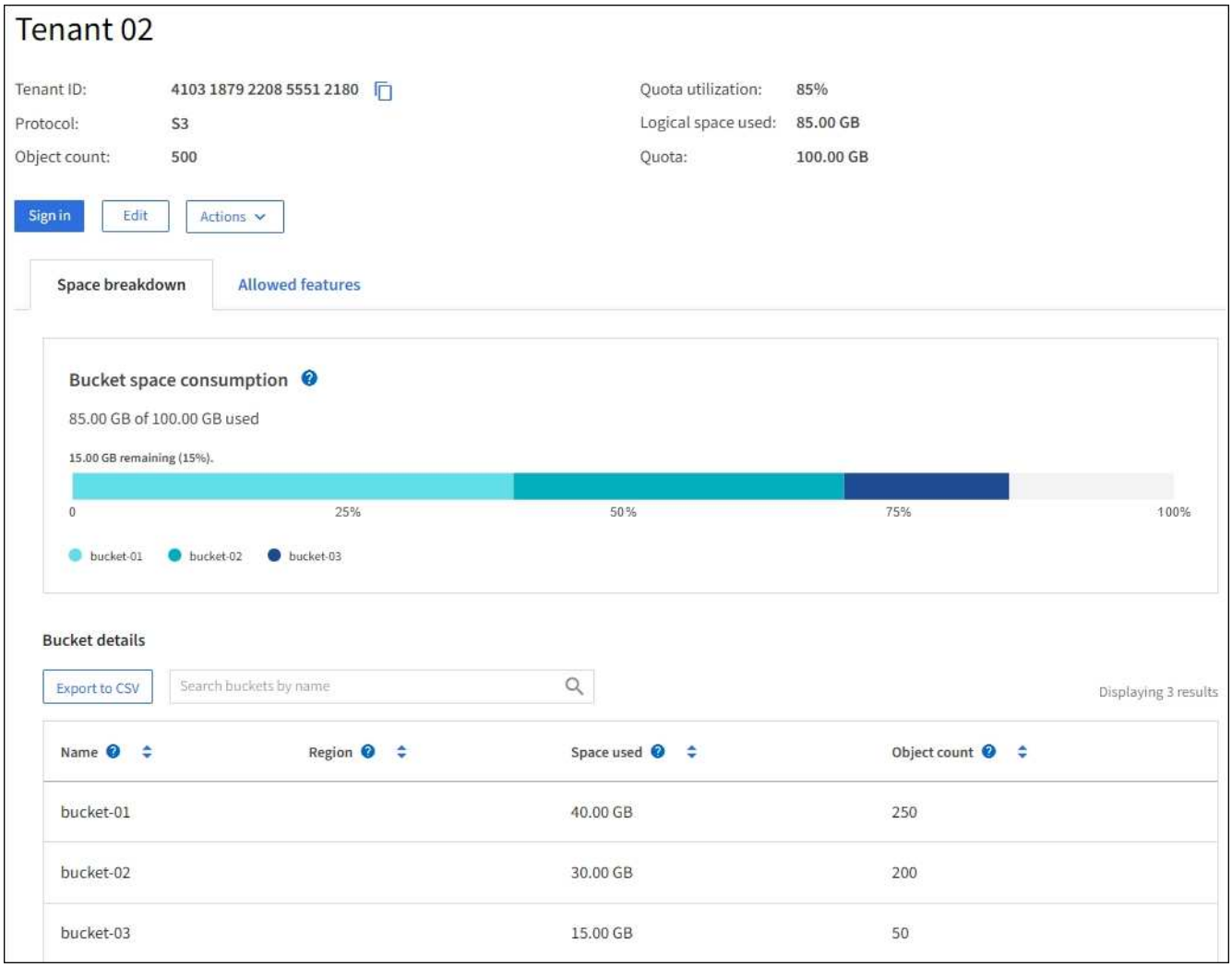
查看特定租户

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. 查看页面顶端的租户概述。

   详细信息页面的此部分提供租户的摘要信息，包括租户的对象计数、配额使用情况、使用的逻辑空间和配额设置。

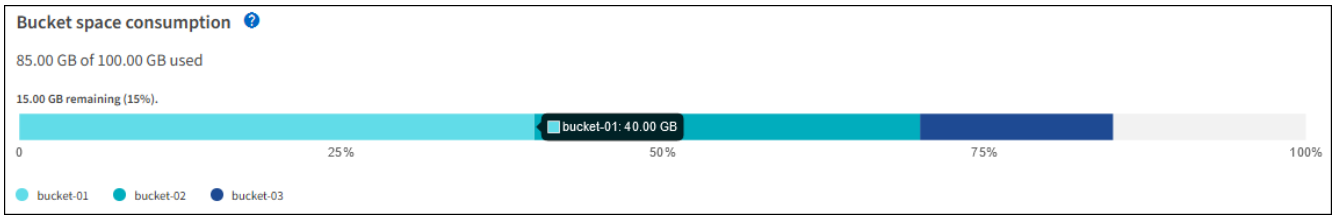
   > 属于此租户的所有对象的逻辑大小包括不完整和正在进行的多部分上传。此大小不包括用于 ILM 策略的额外物理空间。空间使用值为估算值。这些估算值受摄取时间、网络连接和节点状态的影响。

3. 在*空间明细*选项卡中，查看*空间消耗*图表。

   此图表显示了租户所有 S3 存储桶的总空间消耗情况。

   如果为此租户设置了配额，则使用和剩余的配额数量将以文本形式显示（例如， `85.00 GB of 100 GB used`）。如果未设置配额，则租户具有无限配额，并且文本仅包含已使用的空间量（例如， `85.00 GB used`）。条形图显示每个桶或容器中的配额百分比。如果租户超过存储配额超过 1% 且至少超过 1 GB，则图表将显示总配额和超额数量。

   您可以将光标放在条形图上，以查看每个存储桶或容器使用的存储空间。您可以将光标放在可用空间段上，以查看剩余的存储配额量。



配额使用率基于内部估计，在某些情况下可能会超出配额。例如，StorageGRID 会在租户开始上传对象时检查配额，如果租户已超出配额，则拒绝新的接收请求。但是，StorageGRID 在确定是否超过配额时不会考虑当前上传的大小。如果删除对象，则在重新计算配额使用量之前，可能会暂时阻止租户上传新对象。配额使用量计算可能需要 10 分钟或更长时间。

租户的配额使用情况表示租户已上传到 StorageGRID 的对象数据总量（逻辑大小）。配额使用情况不表示用于存储这些对象的副本及其元数据（物理大小）的空间。

您可以启用*租户配额使用率高*警报规则，以确定租户是否正在使用其配额。如果启用，则当租户已使用其配额的 90% 时会触发此警报。有关说明，请参见 "编辑警报规则"。

4. 在*空间明细*选项卡中，查看*存储桶详细信息*。

   此表列出了租户的 S3 存储桶。已用空间是存储桶或容器中对象数据的总量。此值不表示 ILM 副本和对象元数据所需的存储空间。

5. （可选）选择 **Export to CSV** 以查看和导出包含每个存储桶或容器使用值的 .csv 文件。

   单个 S3 租户 `.csv`文件的内容如下所示：

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

   您可以在电子表格应用程序中打开 `.csv` 文件，也可以在自动化中使用它。

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。如果需要更改这些设置，请参阅"编辑租户帐户"。
7. 如果租户具有*使用网格联合连接*权限，则可选择*网格联合*选项卡以了解有关连接的详细信息。

   请参见"什么是网格联盟？"和"管理网格联盟的允许租户"。

查看网络流量

如果为租户设置了流量分类策略，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"Traffic Classification Policies"（流量分类策略）页面，表中列出了现有策略。

2. 请查看策略列表，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。

有关详细信息，请参见 "${post_edited_translations.segment}"。

使用审核日志

您可以选择使用审核日志对租户的活动进行更精细的监控。

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

审核日志将写入文本文件，您可以使用所选的日志分析工具进行分析。这有助于您更好地了解客户端活动，或实施复杂的退款和计费模型。

有关详细信息，请参见 "查看审核日志"。

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 **Support** > **Tools** > **Metrics**。您可以使用现有仪表板（例如 S3 Overview）来查看客户端活动。

> "指标"页面上提供的工具主要用于技术支持。这些工具中的某些功能和菜单项故意设置为不可用。

- 在网格管理器顶部，选择帮助图标并选择 **API documentation**。您可以使用网格管理 API 的"指标"部分中的指标为租户活动创建自定义警报规则和仪表板。

有关详细信息，请参见 "查看支持指标"。

监控 **StorageGRID** 中的 **S3** 客户端操作

您可以监控对象的摄取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 系统中读取、写入和修改对象的成功和失败尝试次数。

开始之前

您已使用 "支持的 Web 浏览器" 登录到网格管理器。

步骤

1. 在控制面板中，选择 **Performance** 选项卡。
2. 请参阅 S3 图表，其中总结了存储节点在选定时间范围内执行的客户端操作数量和存储节点收到的 API 请求

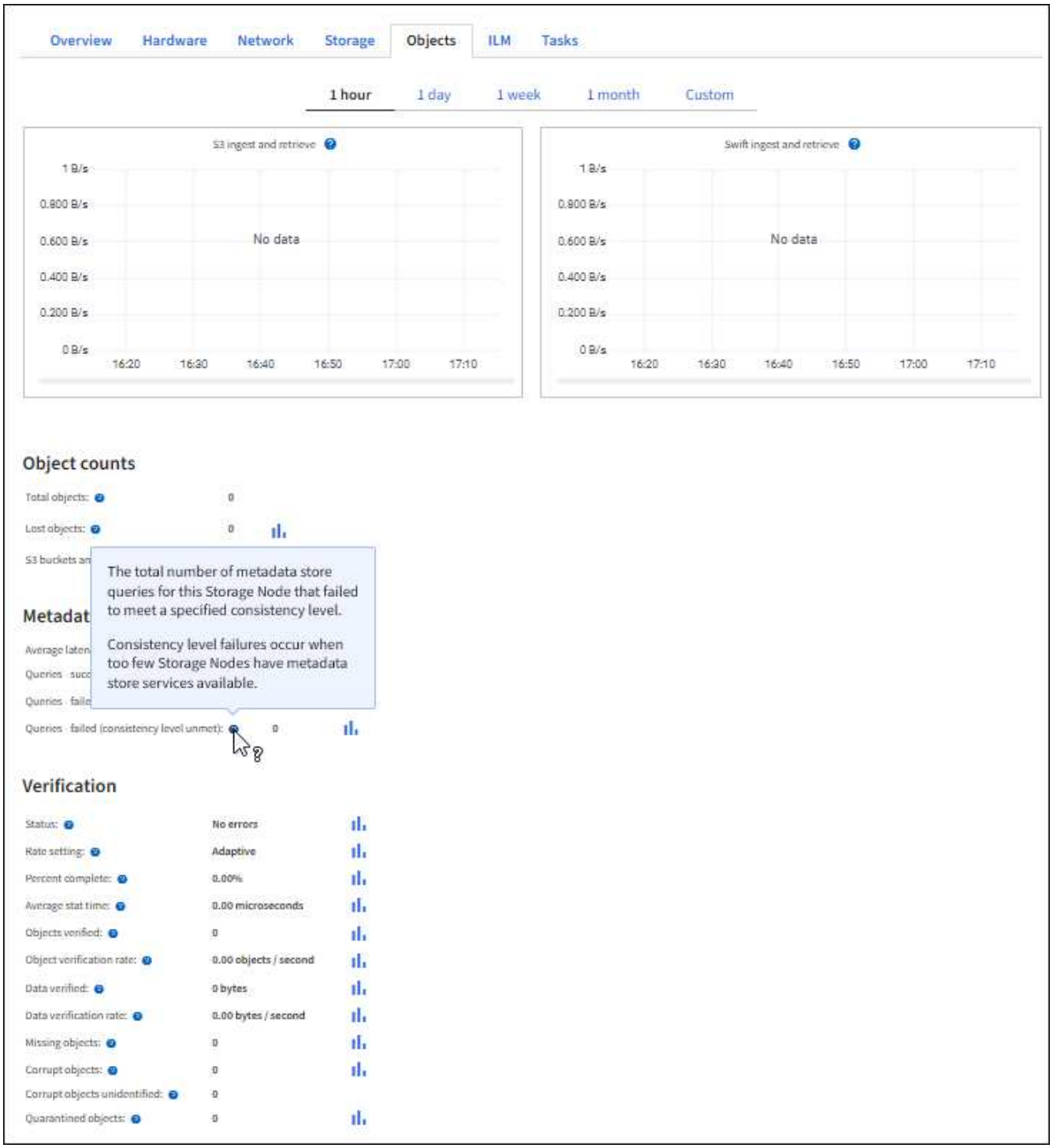
数量。

3. 选择*节点*以访问"节点"页面。
4. 从节点主页（网格级别）中，选择 **Objects** 选项卡。

   该图表显示了整个 StorageGRID 系统的 S3 摄取和检索速率（以字节/秒为单位）以及摄取或检索的数据量。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该节点，然后选择*对象*选项卡。

   该图表显示了节点的摄取和检索速率。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 StorageGRID 中的负载平衡操作

如果使用负载平衡器管理客户端与 StorageGRID 的连接，则应在初始配置系统后以及进行任何配置更改或执行扩展后监视负载平衡操作。

关于此任务

您可以使用管理节点或网关节点上的负载平衡器服务或外部第三方负载平衡器跨多个存储节点分发客户端请求。

配置负载平衡后，应确认对象摄取和检索操作均匀分布在存储节点上。均匀分布的请求可确保 StorageGRID 在负载下保持对客户端请求的响应，并有助于维持客户端性能。

如果在活动备份模式下配置了网关节点或管理节点的高可用性(HA)组，则该组中只有一个节点主动分发客户端请求。

有关详细信息，请参见 "配置 S3 客户端连接"。

步骤

1. 如果 S3 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正在按预期主动分布流量：
   a. 选择 **Nodes**。
   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。

      具有 Primary 角色的节点和不位于 HA 组中的节点应主动将请求分发到客户端。

   d. 对于应主动分发客户端请求的每个节点，选择 "负载平衡器选项卡"。
   e. 查看上周的负载均衡器请求流量图表，以确保节点已主动分发请求。

      活动备份 HA 组中的节点可能会不时担任备份角色。在此期间，节点不会分发客户端请求。

   f. 查看上周的负载均衡器传入请求率图表，以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这些步骤。
   h. （可选）使用流量分类策略查看负载均衡器服务所提供流量的更详细分析。
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这些步骤。

      所有存储节点的会话数应大致相等。

监控 StorageGRID 网格联合连接

您可以监控有关所有"网格联合连接"的基本信息、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

- 您使用 "支持的 Web 浏览器" 登录到任一网格上的 Grid Manager。
- 您拥有您登录的网格的"root 访问权限"。

查看所有连接

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

步骤

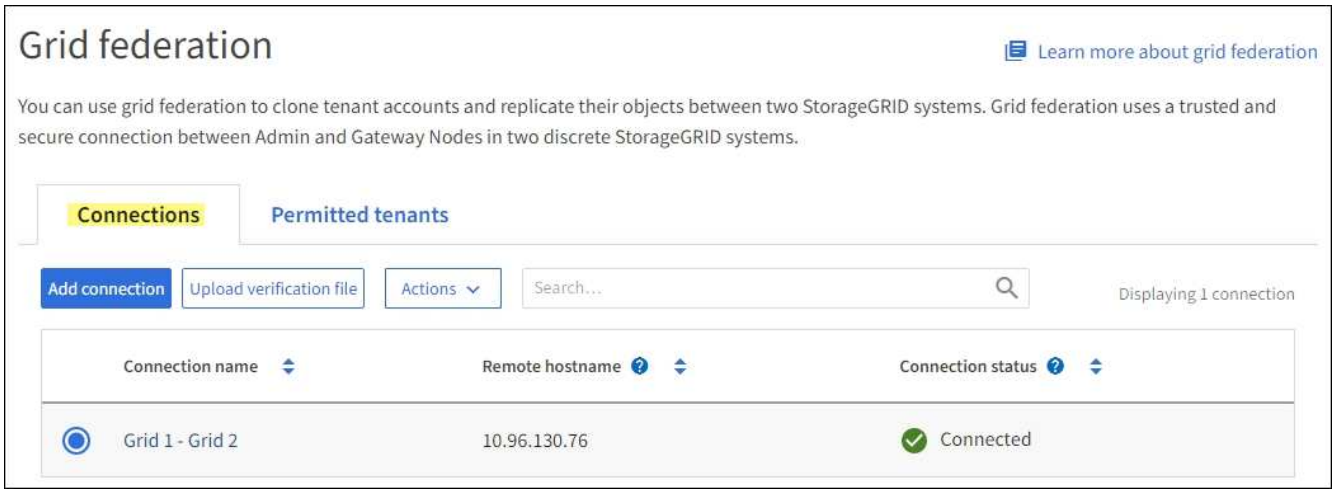
1. 选择*配置* > 系统 > 网格联合。

   此时将显示网格联合页面。

2. 要查看此网格上所有连接的基本信息，请选择*连接*选项卡。

   通过此选项卡，您可以：

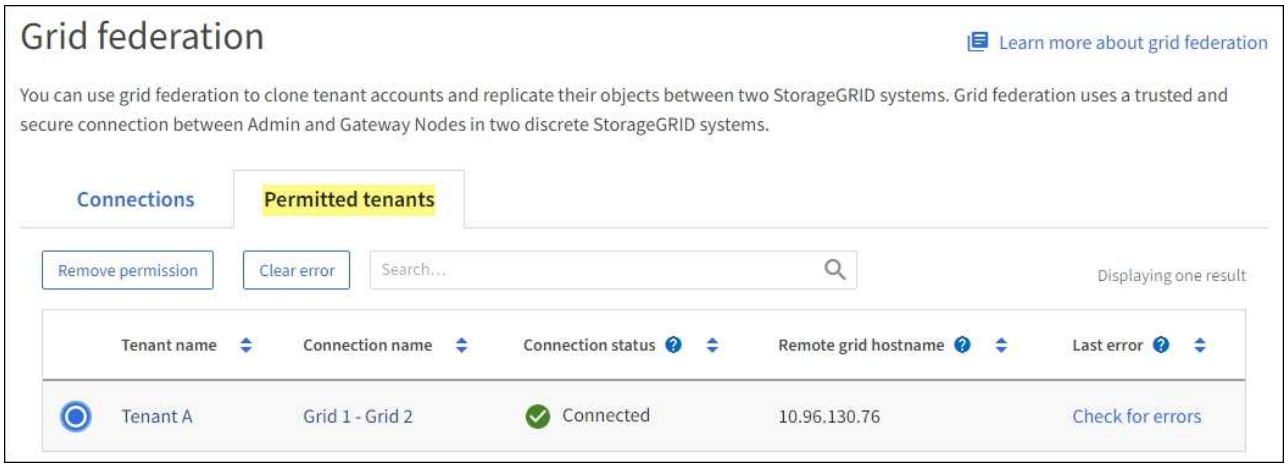
   - "创建新连接"。
   - 选择与 "编辑或测试" 的现有连接。



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。

   通过此选项卡，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。请参阅 查看特定连接。
   - 选择允许的租户和 "删除权限"。
   - 检查跨网格复制错误并清除最后一个错误（如果有）。请参阅 "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盟连接的详细信息。

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。

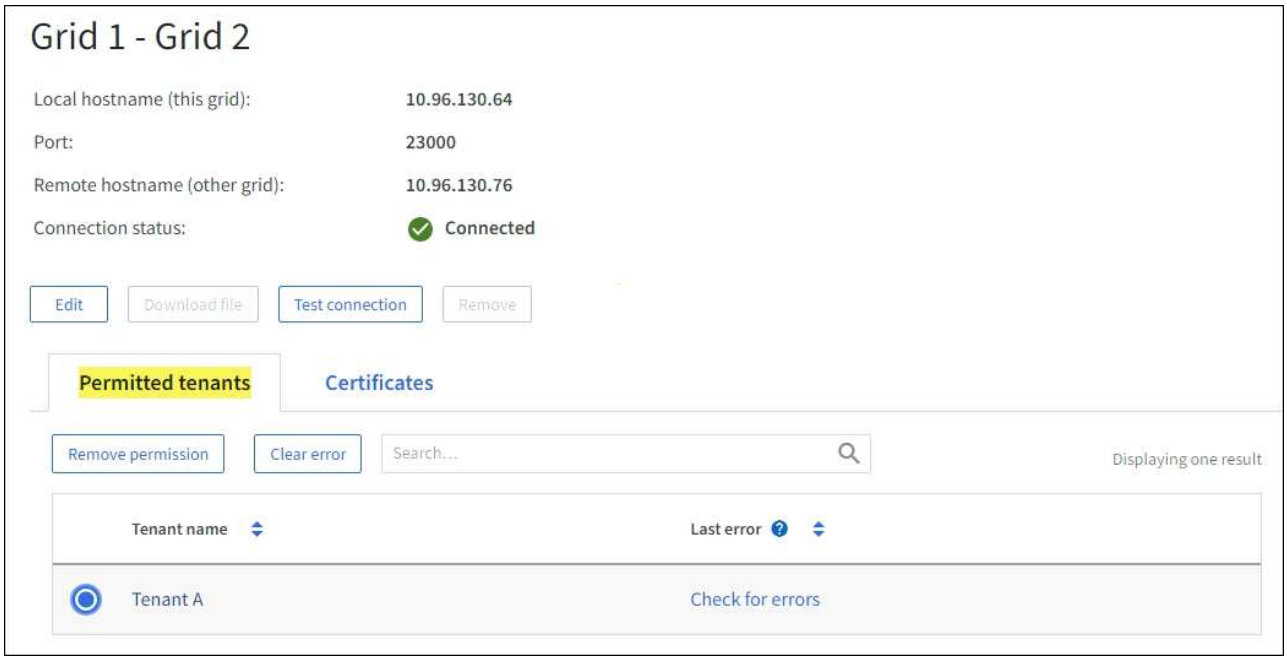
   在连接的详细信息页面中，您可以：

   - 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 "编辑、测试或删除" 的连接。

2. 查看特定连接时，选择*允许的租户*选项卡可查看有关该连接的允许租户的详细信息。

   通过此选项卡，您可以：

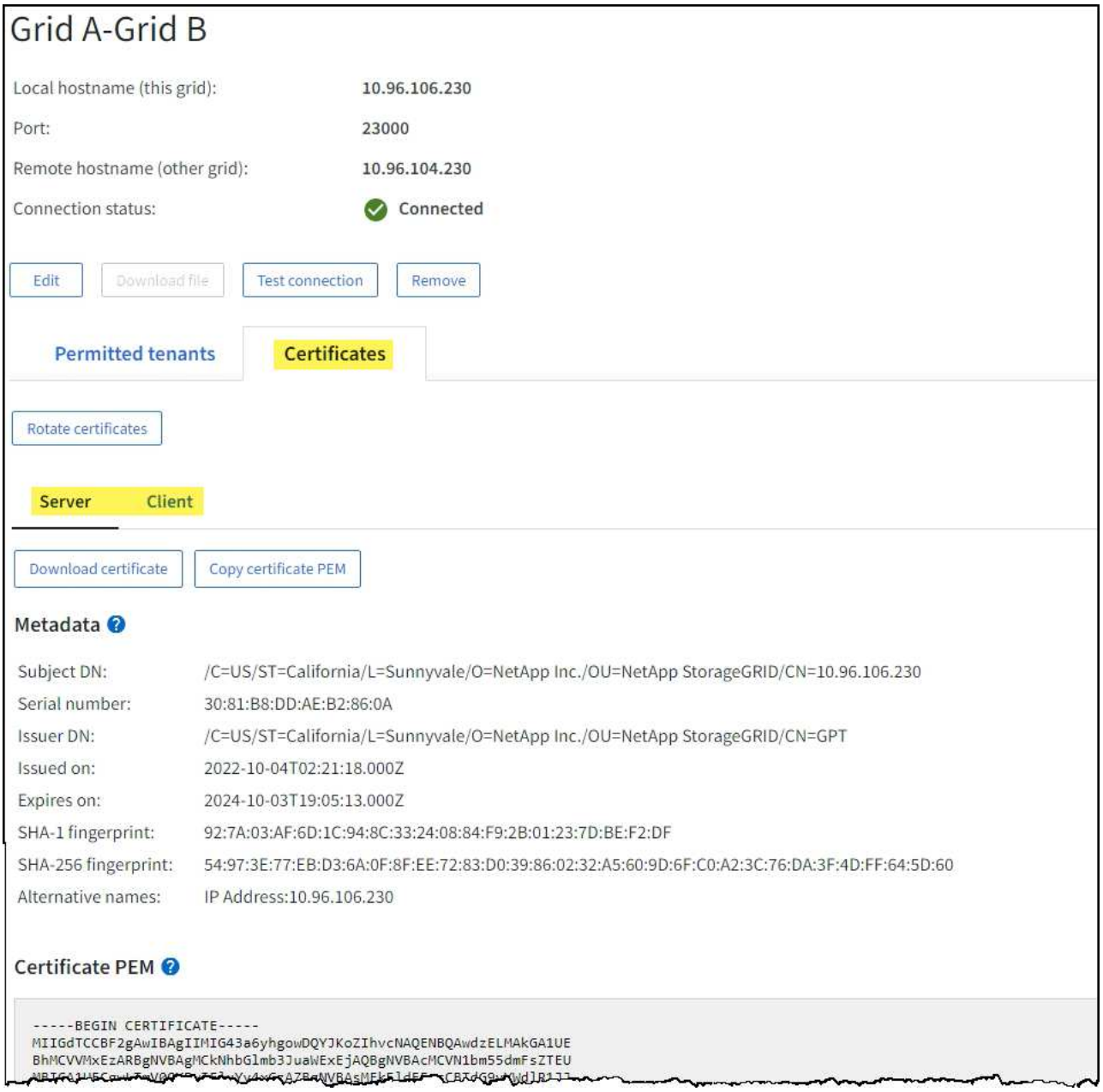
   - "查看每个允许租户的详细信息页面"。
   - "删除租户的权限" 以使用连接。
   - 检查跨网格复制错误并清除最后一个错误。请参阅 "对网格联合错误进行故障排除"。



3. 查看特定连接时，请选择*证书*选项卡以查看此连接的系统生成的服务器和客户端证书。

   通过此选项卡，您可以：

   - "轮换连接证书"。
   - 选择 **Server** 或 **Client** 以查看或下载相关证书或复制证书 PEM。



查看跨网格复制指标

您可以使用 Grafana 中的跨网格复制仪表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"页面上提供的工具仅供技术支持人员使用。这些工具中的某些功能和菜单项故意无法正常使用，可能会发生变化。查看 "常用的 Prometheus 指标" 的列表。

2. 在页面的 Grafana 部分，选择*跨网格复制*。

   有关详细说明，请参见"查看支持指标"。

3. 要重试无法复制的对象的复制，请参见 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

在 **StorageGRID** 中管理警报

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

当警报规则条件评估为真时，将在特定的严重程度级别触发警报。触发警报时，将执行以下操作：

- 警报严重性图标显示在 Grid Manager 的仪表板上，当前警报的数量会增加。
- 警报显示在*节点*摘要页面和*节点* > ***node*** > *概览*选项卡上。
- 系统将发送电子邮件通知，前提是您已配置 SMTP 服务器并为收件人提供了电子邮件地址。
- 假设您已配置 StorageGRID SNMP 代理，系统将发送简单网络管理协议 (SNMP) 通知。

您可以创建自定义提醒、编辑或禁用提醒，以及管理提醒通知。

要了解更多信息：

- 请查看视频：

  警报概述

  自定义提醒

- 请参见 "警报参考"。

查看 **StorageGRID** 警报规则

警报规则定义了触发 "特定警报" 的条件。StorageGRID 包括一组默认警报规则，您可以按原样使用或修改，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，以了解触发每个警报的条件，并查看是否禁用了任何警报。

开始之前

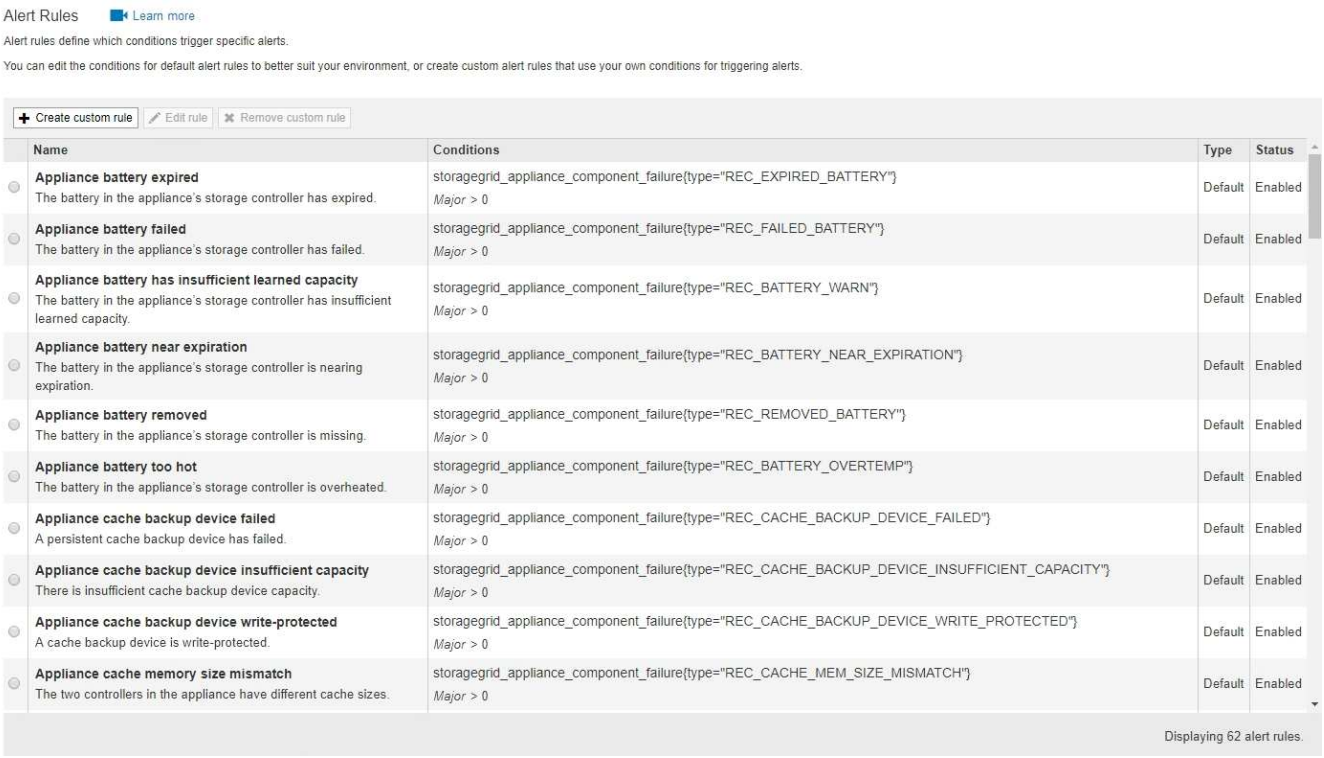
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "管理警报或 Root 访问权限"。
- 或者，您已观看视频：

  警报概述

步骤

1. 选择*Alerts* > **Rules**。

   此时将显示警报规则页面。



2. 查看警报规则表中的信息：

列标头	问题描述
名称	警报规则的唯一名称和说明。自定义警报规则排在前面，其次是默认警报规则。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程度级别触发警报，但不需要每个严重程度的条件。 • 严重：存在已停止 StorageGRID 节点或服务正常操作的异常情况。您必须立即解决根本问题。如果问题未得到解决，可能会导致服务中断和数据丢失。 • 重大：存在影响当前操作或接近严重警报阈值的异常情况。您应该调查重大警报并解决任何潜在问题，以确保异常情况不会阻止 StorageGRID 节点或服务的正常运行。 • 轻微：系统正常运行，但存在异常情况，如果继续运行，可能会影响系统的运行能力。您应该监控并解决未自行清除的轻微警报，以确保它们不会导致更严重的问题。

列标头	问题描述
类型	警报规则的类型： • 默认：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*：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为原始默认值。 • **Custom**：您创建的警报规则。您可以禁用、编辑和删除自定义警报规则。
状态	当前是启用还是禁用此警报规则。未评估禁用警报规则的条件，因此不会触发警报。

在 **StorageGRID** 中创建自定义警报规则

您可以创建自定义警报规则，以定义自己的触发警报的条件。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "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"。
- 或者，您已观看视频：

  自定义提醒

关于此任务

StorageGRID 不验证自定义警报。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有拼写错误和逻辑错误。
- 仅使用 Grid Management API 中列出的指标。
- 使用 Grid Management 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，您可以暂时将阈值设置为当前预期为 true 的值。

  例如，要测试表达式 `node_memory_MemTotal_bytes < 24000000000`，请先执行 `node_memory_MemTotal_bytes >= 0`并确保获得预期结果（所有节点都返回一个值）。然后，将运算符和阈值更改回预期值并再次执行。没有结果表明此表达式没有当前警报。

- 请勿假设自定义警报正在工作，除非您已验证该警报在预期时间触发。

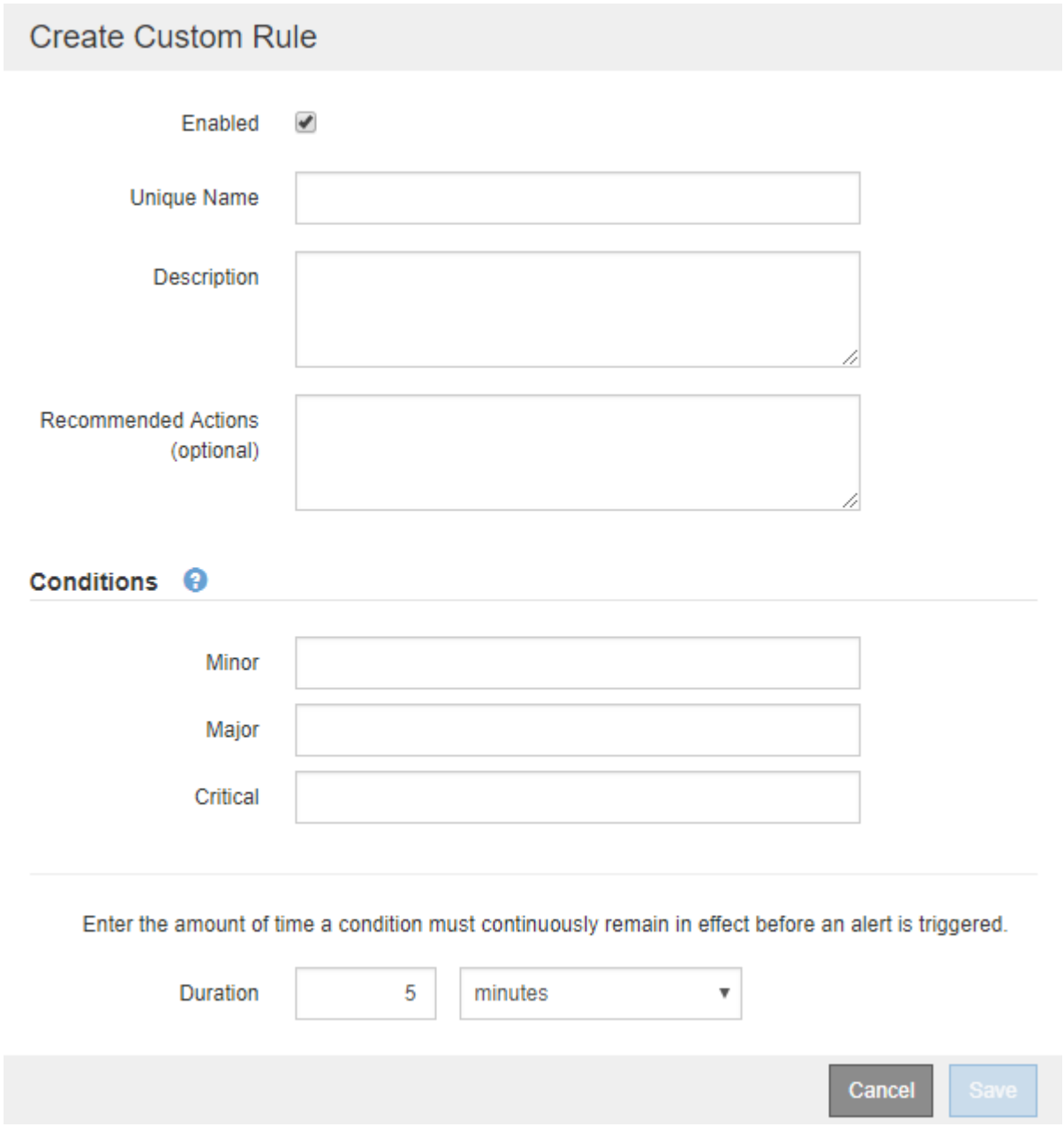
步骤

1. 选择*Alerts* > **Rules**。

此时将显示警报规则页面。

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。

   如果已禁用警报规则，则不会计算其表达式，也不会触发警报。

4. 输入以下信息：

字段	问题描述
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在 1 到 64 个字符之间。
问题描述	对正在发生的问题的描述。说明是警报页面和电子邮件通知中显示的警报消息。警报规则的描述可以介于 1 到 128 个字符之间。
建议操作	（可选）触发此警报时要采取的建议操作。以纯文本形式输入建议操作（无格式代码）。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，为一个或多个警报严重性级别输入 Prometheus 表达式。

   基本表达式的形式通常为：

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

   表达式可以是任意长度，但在用户界面中显示为一行。至少需要一个表达式。

   如果节点安装的 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
   ```

   要查看可用指标和测试 Prometheus 表达式，请选择帮助图标 并点击指向网格管理 API 的"指标"部分的链接。

6. 在*持续时间*字段中，输入条件在触发警报之前必须持续有效的时间量，并选择一个时间单位。

   要在条件变为真时立即触发警报，请输入 **0**。增加此值以防止临时条件触发警报。

   默认时间间隔为5分钟。

7. 选择 **Save**。

   对话框关闭，新的自定义警报规则显示在"警报规则"表中。

在 StorageGRID 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、描述和建议操作。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "管理警报或 Root 访问权限"。

关于此任务

编辑默认警报规则时，可以更改次要、主要和关键警报的条件以及持续时间。编辑自定义警报规则时，还可以编辑规则的名称、描述和建议操作。

在决定编辑警报规则时要小心。如果更改触发器值，则在阻止关键操作完成之前，可能无法检测到潜在问题。

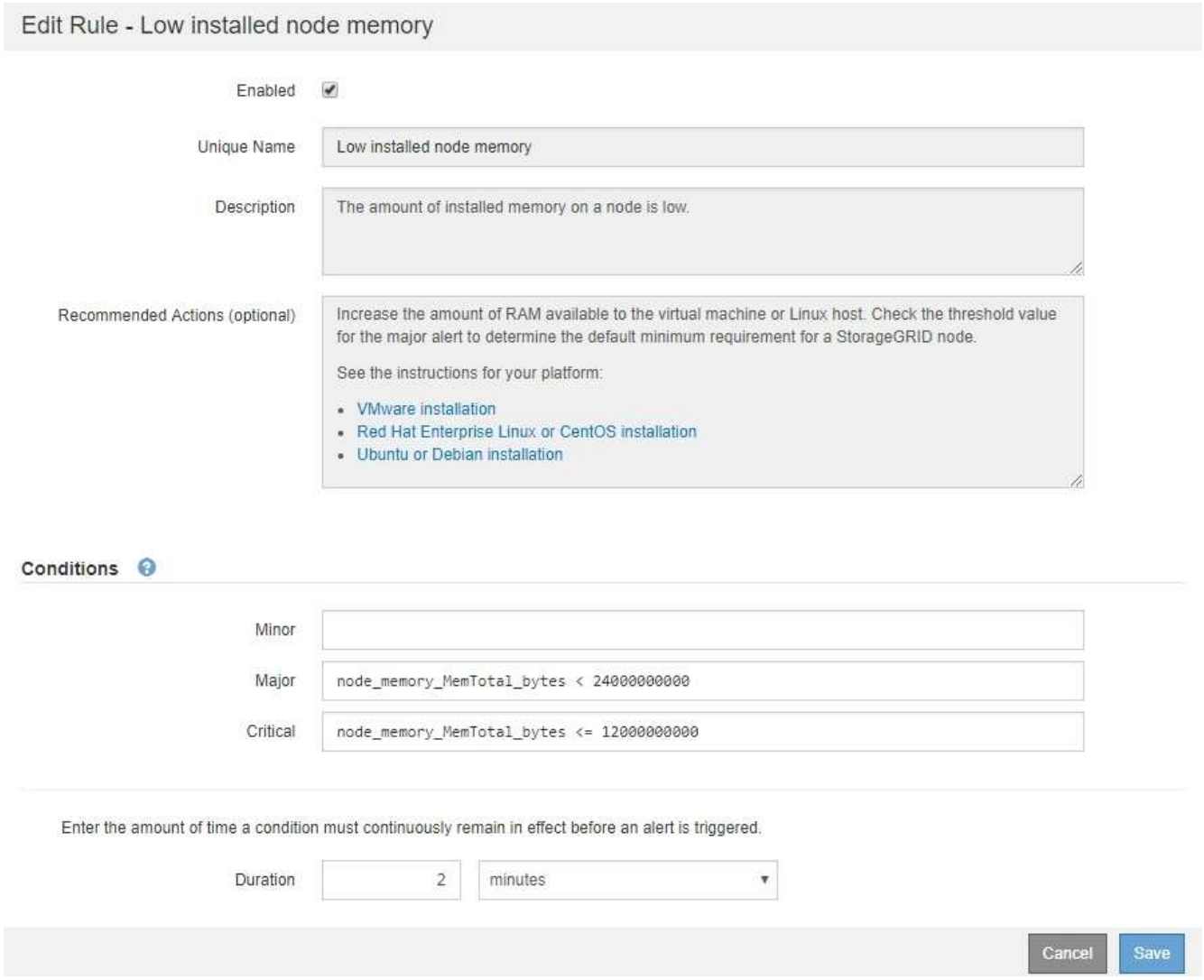
步骤

1. 选择*Alerts* > **Rules**。

   此时将显示警报规则页面。

2. 选择要编辑的警报规则的单选按钮。
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、描述和推荐操作字段已禁用，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。

   如果已禁用警报规则，则不会计算其表达式，也不会触发警报。

   如果禁用当前警报的警报规则，则必须等待几分钟，该警报才不再显示为活动警报。

一般来说，不建议禁用默认警报规则。如果警报规则被禁用，您可能无法检测到潜在问题，直到该问题阻止关键操作完成。

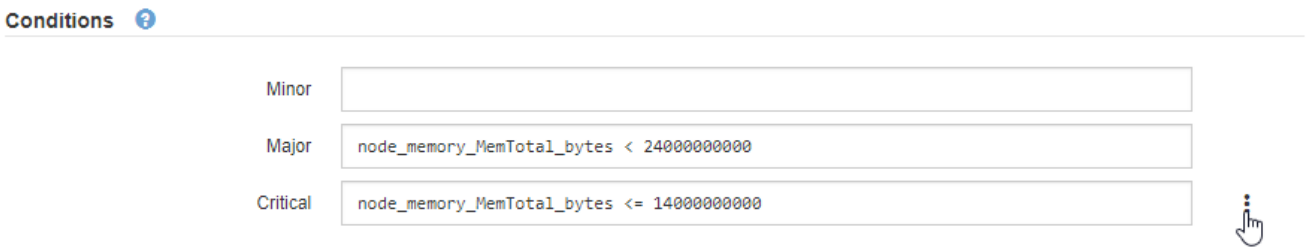
5. 对于自定义警报规则，请根据需要更新以下信息。

您无法编辑默认警报规则的此信息。

字段	问题描述
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在 1 到 64 个字符之间。
问题描述	对正在发生的问题的描述。说明是警报页面和电子邮件通知中显示的警报消息。警报规则的描述可以介于 1 到 128 个字符之间。
建议操作	（可选）触发此警报时要采取的建议操作。以纯文本形式输入建议操作（无格式代码）。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，输入或更新一个或多个警报严重性级别的 Prometheus 表达式。

如果要将已编辑的默认警报规则的条件恢复到其原始值，请选择已修改条件右侧的三个点。



如果更新当前警报的条件，则在解决先前条件之前，可能不会实施更改。下次满足规则的其中一个条件时，警报将反映更新的值。

基本表达式的形式通常为：

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

表达式可以是任意长度，但在用户界面中显示为一行。至少需要一个表达式。

如果节点安装的 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，输入条件在触发警报之前必须持续有效的时间量，并选择时间单位。

要在条件变为真时立即触发警报，请输入 **0**。增加此值以防止临时条件触发警报。

默认时间间隔为5分钟。

8. 选择 **Save**。

   如果您编辑了默认警报规则，**Default** 将显示在类型列中。如果您禁用了默认或自定义警报规则，**Disabled** 将显示在*状态*列中。

在 StorageGRID 中禁用警报规则

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

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "管理警报或 Root 访问权限"。

关于此任务

禁用警报规则时，不会计算其表达式，也不会触发警报。

> 一般来说，不建议禁用默认警报规则。如果警报规则被禁用，您可能无法检测到潜在问题，直到该问题阻止关键操作完成。

步骤

1. 选择*Alerts* > **Rules**。

   此时将显示警报规则页面。

2. 选择要禁用或启用的警报规则的单选按钮。
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。

   如果已禁用警报规则，则不会计算其表达式，也不会触发警报。

   > 如果禁用当前警报的警报规则，则必须等待几分钟，该警报才不再显示为活动警报。

5. 选择 **Save**。

   *已禁用*显示在*状态*列中。

删除 StorageGRID 中的自定义警报规则

如果不想再使用自定义提醒规则，则可以将其删除。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

- 您有 "管理警报或 Root 访问权限"。

步骤

1. 选择*Alerts* > **Rules**。

   此时将显示警报规则页面。

2. 选择要删除的自定义警报规则的单选按钮。

   您无法删除默认提醒规则。

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*删除警报规则。

   警报的所有活动实例将在 10 分钟内解决。

管理警报通知

为 **StorageGRID** 警报设置 **SNMP** 通知

如果希望 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 SNMP 协议的所有三个版本。

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通知：

- 陷阱是由 SNMP 代理发送的通知，不需要管理系统的确认。陷阱用于通知管理系统 StorageGRID 中发生了某些事件，例如触发了警报。所有三个版本的 SNMP 均支持陷阱。
- Inform 类似于陷阱，但需要管理系统确认。如果 SNMP 代理在一定时间内没有收到确认，它会重新发送 Inform，直到收到确认或达到最大重试值。SNMPv2c 和 SNMPv3 支持 Inform。

在任何严重级别触发默认或自定义警报时，都会发送陷阱和通知消息。要抑制警报的 SNMP 通知，必须为警报配置静默。请参阅"静音警报通知"。

如果您的 StorageGRID 部署包括多个管理节点，则主管理节点是警报通知、AutoSupport 包和 SNMP 陷阱和通知的首选发件人。如果主管理节点不可用，通知将由其他管理节点临时发送。请参阅 "什么是管理节点？ "。

为 **StorageGRID** 警报设置电子邮件通知

如果您希望在发生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

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "管理警报或 Root 访问权限"。

关于此任务

用于警报通知的电子邮件设置不适用于 AutoSupport 包。但是，您可以使用相同的电子邮件服务器发送所有通知。

如果您的 StorageGRID 部署包括多个管理节点，则主管理节点是警报通知、AutoSupport 包和 SNMP 陷阱和通知的首选发件人。如果主管理节点不可用，通知将由其他管理节点临时发送。请参阅 "什么是管理节点？"。

步骤

1. 选择*Alerts* > **Email setup**。

   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"过滤器"部分。

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

   如果您的 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	**Enter**
邮件服务器	SMTP 服务器的完全限定域名 (FQDN) 或 IP 地址。
端口	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）	如果您的 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）	如果您的 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，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，为每个电子邮件列表或在出现警报时应接收电子邮件的人输入电子邮件地址。

      选择加号图标 ➕ 以添加收件人。

5. 如果与 SMTP 服务器通信需要传输层安全性 (TLS)，请在传输层安全性 (TLS) 部分选择 **Require TLS**。
   a. 在 **CA Certificate** 字段中，提供用于验证 SMTP 服务器身份的 CA 证书。

      您可以将内容复制并粘贴到此字段，或选择*浏览*并选择文件。

必须提供包含每个中间颁发证书颁发机构 (CA) 的证书的单个文件。该文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。

b. 如果您的 SMTP 电子邮件服务器要求电子邮件发件人提供客户端证书进行身份验证，请选中 发送客户端证书 复选框。

c. 在 **Client Certificate** 字段中，提供要发送到 SMTP 服务器的 PEM 编码客户端证书。

您可以将内容复制并粘贴到此字段，或选择*浏览*并选择文件。

d. 在*专用密钥*字段中，输入未加密 PEM 编码的客户端证书专用密钥。

您可以将内容复制并粘贴到此字段，或选择*浏览*并选择文件。

如果需要编辑电子邮件设置，请选择铅笔图标以更新此字段。

6. 在"过滤器"部分，选择应触发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默。

严重性	问题描述
轻微、重大、危急	当满足警报规则的次要、主要或关键条件时，将发送电子邮件通知。
重大，严重	当满足警报规则的主要或关键条件时，将发送电子邮件通知。不会针对次要警报发送通知。
仅限严重	只有在满足警报规则的关键条件时，才会发送电子邮件通知。不会针对轻微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. 请检查所有电子邮件收件人的收件箱，并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，以验证来自所有站点的连接。

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 软件包不同，后者会由所有管理节点发送测试电子邮件。

8. 选择 **Save**。

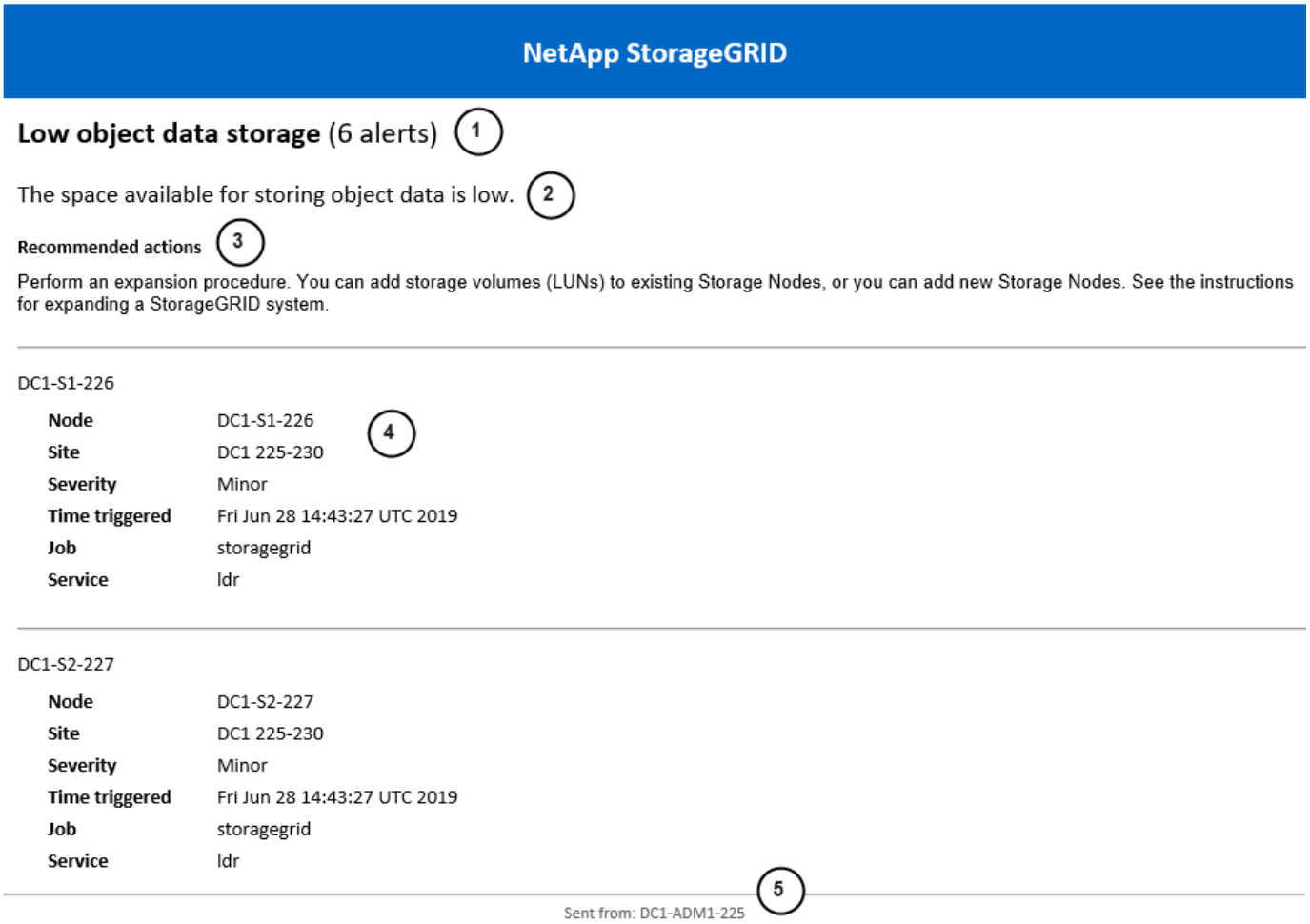
发送测试电子邮件不会保存您的设置。必须选择*Save*。

已保存电子邮件设置。

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，触发警报时会向指定收件人发送电子邮件通知，除非警报规则被静默抑制。请参阅"静音警报通知"。

电子邮件通知包含以下信息：



标注	问题描述
1	警报名称，后跟此警报的活动实例数。
2	对警报的描述。
3	此警报的任何建议操作。
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 时间以及受影响的作业和服务的名称。
5	发送通知的管理节点的主机名。

警报的分组方式

为了防止在触发警报时发送过多的电子邮件通知，StorageGRID 尝试对同一个通知中的多个警报进行分组。

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，请参阅下表。

行为	示例
每个警报通知仅适用于具有相同名称的警报。如果同时触发两个名称不同的警报，则会发送两个电子邮件通知。	• 警报A同时在两个节点上触发。只会发送一条通知。 • 节点 1 触发告警 A，节点 2 同时触发告警 B。系统会发送两条通知，每个告警对应一条。
对于特定节点上的特定警报，如果在多个严重程度上达到阈值，则仅针对最严重的警报发送通知。	• 警报 A 被触发，并且达到次要、主要和关键警报阈值。将为关键警报发送一条通知。
首次触发警报时，StorageGRID 等待 2 分钟后再发送通知。如果在此期间触发了同名的其他警报，StorageGRID 会将所有警报归入初始通知中。	1. 警报A于08:00在节点1上触发。不会发送任何通知。 2. 警报A在08:01在节点2上触发。不会发送任何通知。 3. 在 08:02，系统会发送通知，以报告这两个警报实例。
如果触发了另一个同名的警报，StorageGRID 会在发送新通知之前等待 10 分钟。新通知报告所有活动警报（未被静默的当前警报），即使它们之前已被报告。	1. 警报 A 于 08:00 在节点 1 上触发。通知将在 08:02 发送。 2. 警报A于08:05在节点2上触发。第二个通知将在08:15（10分钟后）发送。两个节点均已报告。
如果存在多个具有相同名称的当前警报，且其中一个警报已解决，则当该警报在已解决警报的节点上再次发生时，不会发送新通知。	1. 节点 1 触发了警报 A。系统将发送通知。 2. 节点 2 触发了警报 A。系统发送第二个通知。 3. 节点 2 的警报 A 已解决，但节点 1 的警报 A 仍处于活动状态。 4. 节点 2 再次触发警报 A。未发送新通知，因为节点 1 的警报仍处于活动状态。
StorageGRID 继续每 7 天发送一次电子邮件通知，直到警报的所有实例都得到解决或警报规则被静默。	1. 警报 A 于 3 月 8 日针对节点 1 触发。系统将发送通知。 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 日等日期发送。

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此问题。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

- 您有 "管理警报或 Root 访问权限"。

步骤

1. 验证您的设置。
   a. 选择*Alerts* > **Email setup**。
   b. 验证电子邮件 (SMTP) 服务器设置是否正确。
   c. 请验证是否已为收件人指定有效的电子邮件地址。
2. 请检查您的垃圾邮件过滤器，并确保电子邮件未发送到垃圾邮件文件夹。
3. 请让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，然后与技术支持联系。

   技术支持可以使用日志中的信息来帮助确定问题所在。例如，连接到指定的服务器时，prometheus.log 文件可能会显示错误。

   请参阅 "收集日志文件和系统数据"。

在 **StorageGRID** 中静音警报通知

或者，您可以配置静默来暂时抑制警报通知。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "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禁用警报规则。每个静默都会抑制单个警报规则或所有警报规则的所有通知。

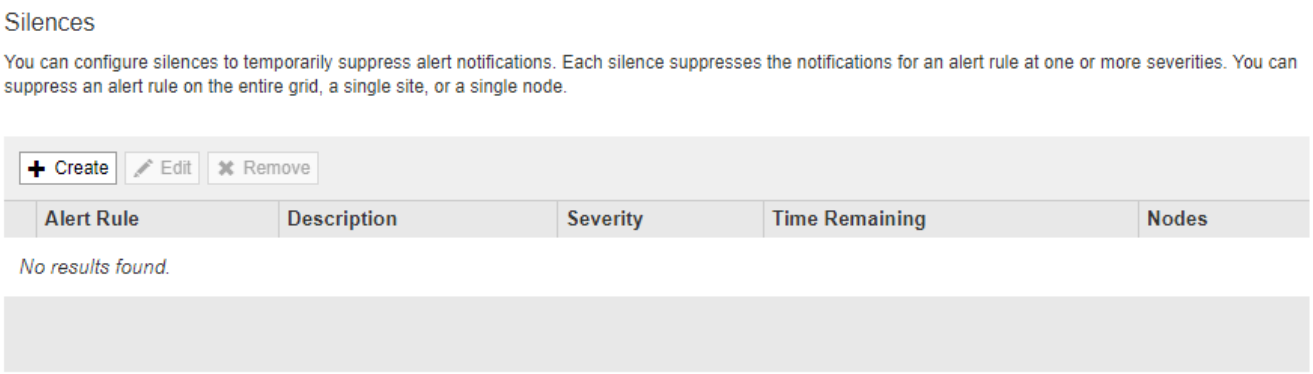
如果启用了 SNMP 代理，则静默也会抑制 SNMP 陷阱和通知。

> 决定将警报规则静音时要小心。如果使警报静音，则在阻止关键操作完成之前，您可能无法检测到潜在问题。

步骤

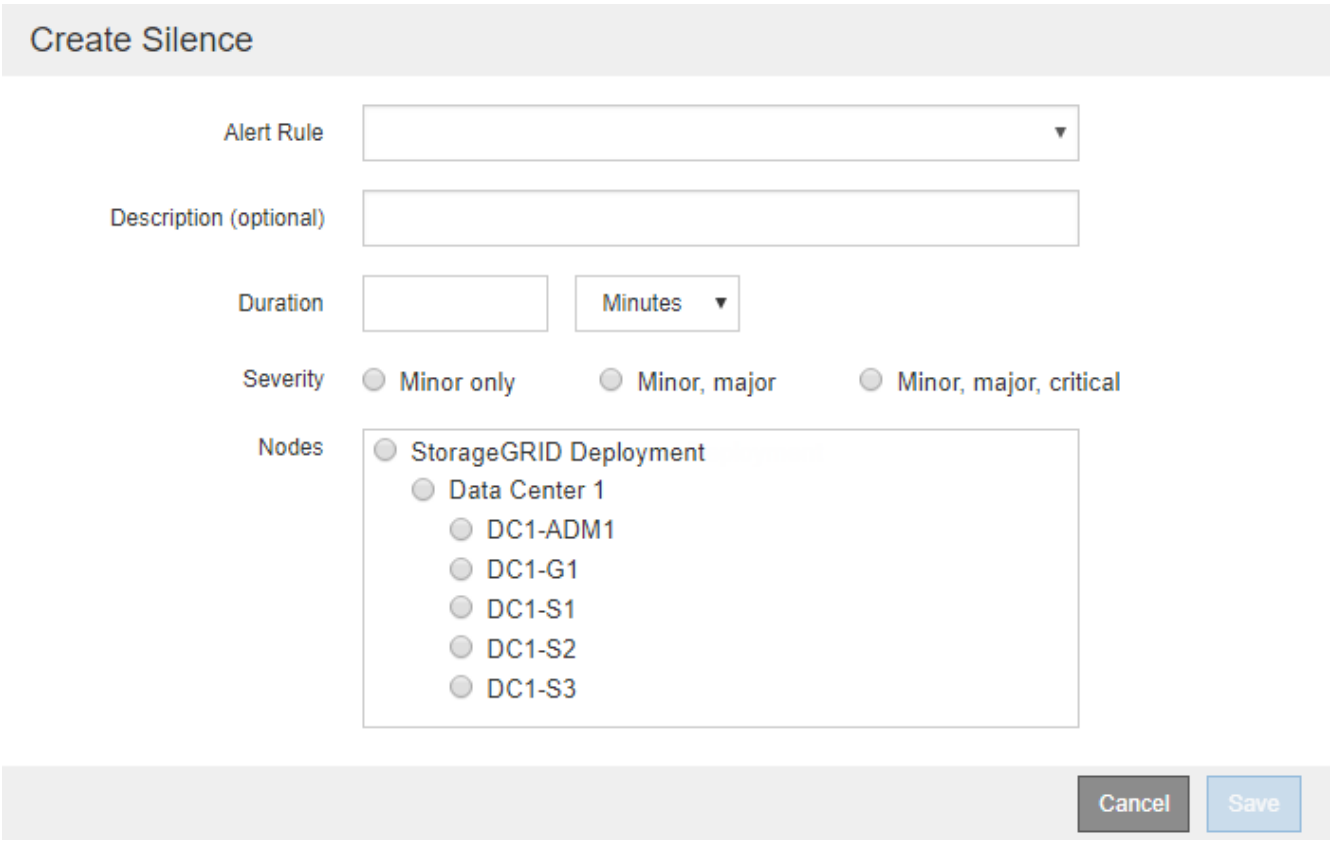
1. 选择*Alerts* > **Silences**。

   此时将显示"Silences"页面。



2. 选择 **Create**。

   此时将显示"创建静音"对话框。



3. 选择或输入以下信息：

字段	问题描述
警报规则	要静默的警报规则名称。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。 注意： 如果要使用此对话框中指定的条件使所有警报规则静默，请选择*所有规则*。
问题描述	可选地，对静默的描述。例如，描述此静默的目的。

字段	问题描述
持续时间	您希望此静默持续多长时间，以分钟、小时或天为单位。静默的有效期从 5 分钟到 1,825 天（5 年）不等。 注意： 您不应让警报规则长时间保持静默。如果警报规则被静默，则在阻止关键操作完成之前，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，例如 **Services appliance link down** 警报和 **Storage appliance link down** 警报，则可能需要使用扩展静默。
严重性	应静默哪些警报严重性级别。如果警报以所选严重性级别之一触发，则不会发送任何通知。
节点	您希望将此静默应用于哪个或哪些节点。您可以抑制整个网格、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，则静默适用于所有站点和所有节点。如果选择一个站点，则静默仅适用于该站点的节点。 注意： 您不能为每个静默选择多个节点或多个站点。如果要一次在多个节点或多个站点上禁止相同的警报规则，则必须创建其他静默。

4. 选择 **Save**。
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	问题描述
编辑静默	a. 选择*Alerts* > **Silences**。 b. 从表格中，选择要编辑的静音对应的单选按钮。 c. 选择*编辑*。 d. 更改描述、剩余时间、所选严重性或受影响的节点。 e. 选择 **Save**。
删除静默	a. 选择*Alerts* > **Silences**。 b. 从表中选择要删除的静音的单选按钮。 c. 选择 **Remove**。 d. 选择*确定*以确认要删除此静音。 注意：现在将在触发此警报时发送通知（除非被另一个静默所抑制）。如果当前触发了此警报，则可能需要几分钟才能发送电子邮件或 SNMP 通知，并更新"警报"页面。

相关信息

"配置 SNMP 代理"

StorageGRID 中的警报

此参考列出显示在 Grid Manager 中的默认警报。建议的操作在您收到的警报消息中。

根据需要，您可以创建自定义警报规则，以适应您的系统管理方法。

某些默认警报使用 "Prometheus 指标"。

设备警报

警报名称	问题描述
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。
设备电池学习容量不足	设备存储控制器中的电池学习容量不足。
设备电池即将到期	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) 的通信已中断。
检测到设备启动设备故障	在设备中检测到启动设备有问题。
设备缓存备份设备失败	永久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 CMOS 电池故障	检测到设备中的 CMOS 电池存在问题。
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标称阈值。
设备计算控制器 CPU 温度过高	StorageGRID 设备中计算控制器中 CPU 的温度已超过标称阈值。
设备计算控制器需要注意	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。

警报名称	问题描述
设备计算控制器电源 B 出现问题	计算控制器中的电源 B 出现问题。
设备计算硬件监视器服务已停止	监控存储硬件状态的服务已停止。
设备 DAS 驱动器超出每天写入数据的限制	每天向驱动器写入的数据量过大，这可能会导致其保修失效。
检测到设备 DAS 驱动器故障	检测到设备中的直接连接存储(DAS)驱动器存在问题。
设备 DAS 驱动器在错误的插槽或节点中	直接连接存储(DAS)驱动器位于错误的插槽或节点中
设备 DAS 驱动器定位器指示灯亮起	设备存储节点中一个或多个直接连接存储(DAS)驱动器的驱动器定位器指示灯亮起。
设备 DAS 驱动器重建	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，则这是正常现象。
检测到设备风扇故障	检测到设备中的风扇单元出现问题。
检测到设备光纤通道故障	检测到设备存储控制器和计算控制器之间存在光纤通道链接问题
设备光纤通道 HBA 端口故障	光纤通道 HBA 端口正在发生故障或已发生故障。
设备闪存缓存驱动器非最佳	用于 SSD 缓存的驱动器不是最佳驱动器。
设备互连/电池罐已拆除	缺少互连/电池罐。
设备 LACP 端口缺失	StorageGRID 设备上的端口未参与 LACP 绑定。
检测到设备网卡故障	检测到设备中的网络接口卡 (NIC) 存在问题。
设备整体电源降级	StorageGRID 设备的电源偏离了建议的工作电压。
需要更新设备 SANtricity 操作系统软件	SANtricity 软件版本低于此版本 StorageGRID 的建议最低版本。
设备 SSD 严重警告	设备 SSD 报告了严重警告。
设备存储控制器 A 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。

警报名称	问题描述
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状态。
设备存储控制器硬件问题	SANtricity 软件正在报告 StorageGRID 设备中某个组件的"需要注意"。
设备存储控制器电源A故障	StorageGRID 设备中的电源 A 偏离了建议的工作电压。
设备存储控制器电源 B 故障	StorageGRID 设备中的电源 B 偏离了建议的工作电压。
设备存储硬件监视器服务已停止	监控存储硬件状态的服务已停止。
设备存储架已降级	存储设备的存储架中的一个组件的状态已降级。
设备温度超出	已超出设备存储控制器的标称温度或最高温度。
已删除设备温度传感器	已删除温度传感器。
设备 UEFI 安全启动错误	设备尚未安全启动。
磁盘 I/O 非常慢	磁盘 I/O 速度非常慢，可能会影响网格性能。
检测到存储设备风扇故障	检测到设备的存储控制器中的风扇单元存在问题。
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存在问题。
存储设备无法访问	无法访问存储设备。

审核和 **syslog** 警报

警报名称	问题描述
正在将审核日志添加到内存中队列	节点无法将日志发送到本地 syslog 服务器，内存中队列正在填满。
外部syslog服务器转发错误	节点无法将日志转发到外部 syslog 服务器。
大型审核队列	审核消息的磁盘队列已满。如果不解决这种情况，S3 操作可能会失败。
正在将日志添加到磁盘上队列	节点无法将日志转发到外部 syslog 服务器，磁盘上的队列正在填满。

Bucket 警报

警报名称	问题描述
FabricPool 存储桶具有不受支持的存储桶一致性设置	FabricPool 存储区使用不支持的可用或强站点一致性级别。
FabricPool 存储桶具有不受支持的版本控制设置	FabricPool 存储桶已启用版本控制或 S3 对象锁定，不支持此功能。

Cassandra 警报

警报名称	问题描述
Cassandra 自动压缩器错误	Cassandra 自动压缩器出现错误。
Cassandra 自动压缩指标已过期	描述 Cassandra 自动压缩器的指标已过期。
Cassandra 通信错误	运行 Cassandra 服务的节点彼此通信时遇到问题。
Cassandra 压缩过载	Cassandra 压缩过程过载。
Cassandra超大写入错误	内部 StorageGRID 进程向 Cassandra 发送的写入请求太大。
Cassandra 修复指标已过期	描述 Cassandra 修复作业的指标已过期。
Cassandra 修复进度缓慢	Cassandra 数据库修复进度较慢。
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，它会自动重新启动。

云存储池警报

警报名称	问题描述
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。
IAM Roles Anywhere 端实体证书到期	IAM Roles Anywhere 最终实体证书即将过期。

跨网格复制警报

警报名称	问题描述
跨网格复制永久失败	出现跨网格复制错误，需要用户干预才能解决。

警报名称	问题描述
跨网格复制资源不可用	跨网格复制请求处于挂起状态，因为资源不可用。

DHCP警报

警报名称	问题描述
DHCP租用已过期	网络接口上的 DHCP 租约已过期。
DHCP租约即将到期	网络接口上的 DHCP 租约即将到期。
DHCP服务器不可用	DHCP 服务器不可用。

调试和跟踪警报

警报名称	问题描述
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	问题描述
AutoSupport 消息发送失败	最近一条 AutoSupport 消息发送失败。
域名解析失败	StorageGRID 节点无法解析域名。
电子邮件通知失败	无法发送警报的电子邮件通知。
未找到日志存档目标存储桶	日志存档目标存储桶缺失，这会阻止日志存档到目标存储桶。
SNMP inform 错误	向陷阱目标发送 SNMP inform 通知时出错。
SSH外部访问已启用	SSH 外部访问已启用超过 24 小时。
检测到 SSH 或控制台登录	在过去 24 小时内，用户已使用 Web Console 或 SSH 登录。

纠删码 **(EC)** 警报

警报名称	问题描述
EC再平衡失败	EC再平衡程序失败或已停止。
EC修复失败	EC数据的修复作业已失败或已停止。
EC修复停滞	EC数据的修复作业已停止。
擦除编码片段验证错误	无法再验证擦除编码片段。损坏的片段可能无法修复。

证书过期警报

警报名称	问题描述
管理员代理 CA 证书过期	管理代理服务器 CA 捆绑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 的全局服务器证书到期	S3 的全局服务器证书即将过期。
负载平衡器端点证书过期	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过期	用于管理接口的服务器证书即将过期。
外部 syslog CA 证书过期	用于对外部 syslog 服务器证书进行签名的证书颁发机构 (CA) 证书即将过期。
外部 syslog 客户端证书过期	外部 syslog 服务器的客户端证书即将过期。
外部系统日志服务器证书过期	外部 syslog 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	问题描述
网格网络MTU不匹配	网格网络接口 (eth0) 的 MTU 设置在网格中各节点之间存在显著差异。

网格联合警报

警报名称	问题描述
网格联盟证书过期	一个或多个网格联合证书即将过期。
网格联盟连接失败	本地和远程网格之间的网格联合连接不起作用。

高使用率或高延迟警报

警报名称	问题描述
高 Java 堆使用率	正在使用大量 Java 堆空间。
元数据查询的高延迟	Cassandra 元数据查询的平均时间太长。

身份联合警报

警报名称	问题描述
身份联合同步失败	无法从身份源同步联合组和用户。
租户的标识联合同步失败	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	问题描述
ILM放置无法实现	无法为某些对象实现 ILM 规则中的放置指令。
ILM 扫描率低	ILM 扫描速率设置为小于 100 个对象/秒。

密钥管理服务器**(KMS)**警报

警报名称	问题描述
KMS CA 证书过期	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 客户端证书过期	密钥管理服务器的客户端证书即将过期
${post_edited_translations.segment}	密钥管理服务器的配置已存在，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	已成功解密所有设备卷，但一个或多个卷无法轮换到最新密钥。
${post_edited_translations.segment}	此站点不存在密钥管理服务器。

警报名称	问题描述
${post_edited_translations.segment}	无法使用当前 KMS 密钥解密启用了节点加密的设备上的一个或多个卷。
KMS 服务器证书过期	密钥管理服务器(KMS)使用的服务器证书即将过期。
KMS 服务器连接失败	设备节点无法连接到其站点的密钥管理服务器群集中的一个或多个服务器。

负载均衡器警报

警报名称	问题描述
负载均衡器零请求连接数偏高	连接到负载均衡器端点但未执行请求即断开的连接百分比偏高。

本地时钟偏移警报

警报名称	问题描述
本地时钟大时间偏移	本地时钟和网络时间协议 (NTP) 时间之间的偏移太大。

内存不足或空间不足警报

警报名称	问题描述
审核日志磁盘容量不足	可用于审核日志的空间不足。如果此情况未得到解决，则 S3 操作可能会失败。
可用节点内存不足	节点上可用的 RAM 量较低。
存储池可用空间不足	可用于在存储节点中存储对象数据的空间不足。
已安装的节点内存不足	节点上已安装的内存量较低。
低元数据存储	可用于存储对象元数据的空间不足。
指标磁盘容量低	可用于指标数据库的空间不足。
对象数据存储量低	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值小于存储节点的最小优化水印。
根磁盘容量不足	根磁盘上的可用空间不足。

警报名称	问题描述
系统数据容量低	/var/local 的可用空间不足。如果此情况未得到解决，S3 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	问题描述
未达到 ADC 仲裁	具有 ADC 服务的存储节点已脱机。在 ADC 仲裁恢复之前，扩展和停用操作将被阻止。
管理员网络接收使用情况	管理网络上的接收使用率很高。
管理网络传输使用情况	管理网络上的传输使用率很高。
防火墙配置失败	无法应用防火墙配置。
备用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发生错误。
节点网络接收帧错误	节点接收的网络帧中有很大一部分存在错误。
节点与 NTP 服务器不同步	节点与网络时间协议(NTP)服务器不同步。
节点未与 NTP 服务器锁定	节点未锁定到网络时间协议（NTP）服务器。
非设备节点网络中断	一个或多个网络设备已关闭或断开连接。
管理网络上的服务设备链接断开	到管理网络 (eth1) 的设备接口已关闭或已断开连接。
管理网络端口 1 上的服务设备链路断开	设备上的管理网络端口 1 已关闭或已断开连接。
客户端网络上的服务设备链接断开	客户端网络(eth2)的设备接口已关闭或已断开连接。
网络端口 1 上的服务设备链路断开	设备上的网络端口 1 已关闭或已断开连接。
网络端口 2 上的服务设备链路断开	设备上的网络端口 2 已关闭或已断开连接。
网络端口 3 上的服务设备链路断开	设备上的网络端口 3 已关闭或已断开连接。

警报名称	问题描述
网络端口 4 上的服务设备链路断开	设备上的网络端口 4 已关闭或已断开连接。
管理网络上的存储设备链接断开	到管理网络 (eth1) 的设备接口已关闭或已断开连接。
管理网络端口 1 上的存储设备链路断开	设备上的管理网络端口 1 已关闭或已断开连接。
客户端网络上的存储设备链接断开	客户端网络(eth2)的设备接口已关闭或已断开连接。
网络端口 1 上的存储设备链路断开	设备上的网络端口 1 已关闭或已断开连接。
存储设备网络端口 2 链路断开	设备上的网络端口 2 已关闭或已断开连接。
网络端口 3 上的存储设备链路断开	设备上的网络端口 3 已关闭或已断开连接。
网络端口 4 上的存储设备链路断开	设备上的网络端口 4 已关闭或已断开连接。
存储节点未处于所需存储状态	由于内部错误或卷相关问题，存储节点上的 LDR 服务无法转换到所需状态
TCP 连接使用情况	此节点上的 TCP 连接数量接近可跟踪的最大数量。
无法与节点进行通信	一个或多个服务无响应，或者无法访问此节点。
意外节点重新启动	一个节点在过去 24 小时内意外重新启动。

对象警报

警报名称	问题描述
对象存在检查失败	对象存在性检查作业失败。
对象存在性检查已停顿	对象存在性检查作业已停止。
可能丢失的对象	一个或多个对象可能已从网格中丢失。
检测到孤立对象	检测到孤立对象。
S3 PUT 对象大小过大	客户端正在尝试执行超出 S3 大小限制的 PUT Object 操作。
检测到未识别的损坏对象	在已复制对象存储中找到无法识别为已复制对象的文件。

对象损坏警报

警报名称	问题描述
对象大小不匹配	在对象存在性检查过程中检测到意外的对象大小。

平台服务警报

警报名称	问题描述
平台服务待处理请求容量不足	Platform Services 待处理的请求数量正在接近容量上限。
平台服务不可用	站点上运行或可用的具有 RSM 服务的存储节点太少。

存储卷警报

警报名称	问题描述
存储卷需要注意	存储卷处于脱机状态，需要注意。
需要还原存储卷	已恢复存储卷，需要还原。
存储卷已脱机	存储卷已脱机超过 5 分钟。
已尝试重新挂载存储卷	存储卷已脱机并触发了自动重新装载。这可能表示驱动器问题或文件系统错误。
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	问题描述
nginx 服务使用备份配置	nginx 服务的配置无效。当前正在使用以前的配置。
使用备份配置的 nginx-gw 服务	nginx-gw 服务的配置无效。此时正在使用以前的配置。
需要重新启动才能禁用 FIPS	安全策略不需要 FIPS 模式，但正在使用 FIPS 模块。
启用 FIPS 需要重新启动	安全策略需要 FIPS 模式，但 FIPS 模块未使用。
使用备份配置的 SSH 服务	SSH 服务的配置无效。此时正在使用以前的配置。

警报名称	问题描述
租户配额使用率高	正在使用高百分比的配额空间。默认情况下，此规则处于禁用状态，因为它可能会导致过多通知。

StorageGRID 中常用的 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 "查询 Prometheus"。

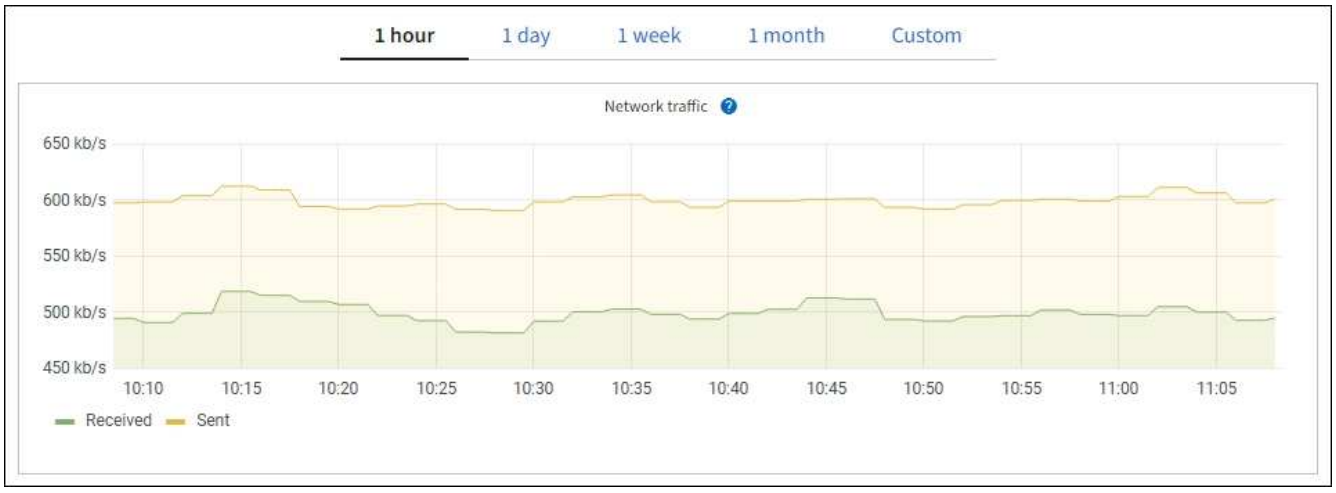
什么是 Prometheus 指标?

Prometheus 指标是时间序列测量。管理节点上的 Prometheus 服务从所有节点上的服务收集这些指标。指标存储在每个管理节点上，直到为 Prometheus 数据预留的空间已满。当 `/var/local/mysql_ibdata/` 卷达到容量时，将首先删除最旧的指标。

Prometheus 指标在哪里使用?

Prometheus 收集的指标在 Grid Manager 中的多个位置使用：

- 节点页面：节点页面中可用选项卡上的图形和图表使用 Grafana 可视化工具来显示 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 则作为后端数据源。



- 警报：当使用 Prometheus 指标的警报规则条件评估为 true 时，将在特定的严重程度级别触发警报。
- **Grid Management API**：您可以在自定义警报规则中使用 Prometheus 指标，也可以与外部自动化工具一起监控您的 StorageGRID 系统。网格管理 API 提供了 Prometheus 指标的完整列表。（在网格管理器顶部，选择帮助图标，然后选择 **API** 文档 > 指标。）虽然有超过一千个指标可用，但仅需要相对较少的数量来监控最关键的 StorageGRID 操作。

名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间如有更改，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人员使用，提供多种使用 Prometheus 指标值的工具和图表。

"指标"页面中的某些功能和菜单项故意无法正常使用，可能会发生变化。

最常见指标列表

以下列表包含最常用的 Prometheus 指标。

名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间如有更改，恕不另行通知。

alertmanager_notifications_failed_total

失败的警报通知的总数。

node_filesystem_avail_bytes

非根用户可用的文件系统空间量（以字节为单位）。

node_memory_MemAvailable_bytes

内存信息字段 MemAvailable_bytes。

node_network_carrier

承运人值 `/sys/class/net/iface`。

node_network_receive_errs_total

网络设备统计 `receive_errs`。

node_network_transmit_errs_total

网络设备统计 `transmit_errs`。

storagegrid_administratively_down

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_appliance_compute_controller_hardware_status

设备中计算控制器硬件的状态。

storagegrid_appliance_failed_disks

对于设备中的存储控制器，非最优驱动器的数量。

storagegrid_appliance_storage_controller_hardware_status

设备中存储控制器硬件的整体状态。

storagegrid_content_buckets_and_containers

此存储节点已知的 S3 存储桶总数。

storagegrid_content_objects

此存储节点已知的 S3 数据对象总数。计数仅对通过 S3 与系统交互的客户端应用程序创建的数据对象有效。

storagegrid_content_objects_lost

此服务检测到 StorageGRID 系统中缺少的对象总数。应采取措施确定损失原因以及是否可以恢复。

"对象数据丢失和缺失故障排除"

storagegrid_http_sessions_incoming_attempted

已尝试到存储节点的 HTTP 会话总数。

storagegrid_http_sessions_incoming_currently_established

存储节点上当前处于活动状态（打开）的HTTP会话数。

storagegrid_http_sessions_incoming_failed

由于 HTTP 请求格式错误或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。

storagegrid_ilm_awaiting_background_objects

此节点上等待 ILM 评估的对象总数（来自扫描）。

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

根据此节点上的 ILM 策略评估对象的当前速率。

storagegrid_ilm_awaiting_client_objects

此节点上等待通过客户端操作（例如，载入）进行 ILM 评估的对象总数。

storagegrid_ilm_awaiting_total_objects

等待 ILM 评估的对象总数。

storagegrid_ilm_scan_objects_per_second

扫描此节点拥有的对象并将其排入 ILM 队列的速率。

storagegrid_ilm_scan_period_estimated_minutes

在此节点上完成完整 ILM 扫描的预计时间。

注意： 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_cert_expiry_time

自 epoch 以来负载均衡器端点证书的到期时间（以秒为单位）。

storagegrid_metadata_queries_average_latency_milliseconds

通过此服务对元数据存储运行查询所需的平均时间。

storagegrid_network_received_bytes

自安装以来接收的总数据量。

storagegrid_network_transmitted_bytes

自安装以来发送的总数据量。

storagegrid_node_cpu_utilization_percentage

此服务当前使用的可用 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。

storagegrid_ntp_chosen_time_source_offset_milliseconds

所选时间源提供的系统时间偏移。当到达时间源的延迟不等于时间源到达 NTP 客户端所需的时间时，会引入偏移。

storagegrid_ntp_locked

节点未锁定到网络时间协议(NTP)服务器。

storagegrid_s3_data_transfers_bytes_ingested

自上次重置属性以来，从 S3 客户端摄取到此存储节点的数据总量。

storagegrid_s3_data_transfers_bytes_retrieved

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。

storagegrid_s3_operations_failed

S3 操作失败的总次数（HTTP 状态代码 4xx 和 5xx），不包括由 S3 授权失败引起的操作。

storagegrid_s3_operations_successful

S3 操作成功总数（HTTP 状态代码 2xx）。

storagegrid_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

管理接口证书过期前的天数。

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Object Storage API 证书过期前的天数。

storagegrid_service_cpu_seconds

自安装以来此服务已使用 CPU 的累计时间量。

storagegrid_service_memory_usage_bytes

此服务当前正在使用的内存量(RAM)。此值与 Linux top 实用程序显示为 RES 的值相同。

storagegrid_service_network_received_bytes

此服务自安装以来接收的总数据量。

storagegrid_service_network_transmitted_bytes

此服务发送的总数据量。

storagegrid_service_restarts

已重新启动服务的总次数。

storagegrid_service_runtime_seconds

自安装以来服务已运行的总时间量。

storagegrid_service_uptime_seconds

自上次重新启动以来，此服务已运行的总时间量。

storagegrid_storage_state_current

存储服务的当前状态。属性值为：

- 10 = 离线
- 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 = 过渡中
- 20 = 可用空间不足
- 30 = 卷不可用
- 40 = 错误

storagegrid_storage_utilization_data_bytes

存储节点上已复制和纠删码对象数据的总大小估计值。

storagegrid_storage_utilization_metadata_allowed_bytes

每个存储节点卷 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保留的实际空间，因为基本数据库操作（如压缩和修复）以及未来的硬件和软件升级需要保留空间的一部分。允许的对象元数据空间控制整体对象容量。

storagegrid_storage_utilization_metadata_bytes

存储卷0上的对象元数据量，以字节为单位。

storagegrid_storage_utilization_total_space_bytes

分配给所有对象存储的存储空间总量。

storagegrid_storage_utilization_usable_space_bytes

剩余对象存储空间的总量。通过将存储节点上所有对象存储的可用空间量相加计算得出。

storagegrid_tenant_usage_data_bytes

租户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，则可用空间无限。

获取所有指标的列表

要获取完整的指标列表，请使用 Grid Management API。

步骤

1. ${post_edited_translations.segment}
2. 找到*指标*操作。
3. 执行 `GET /grid/metric-names`操作。
4. 下载结果。

日志文件引用

StorageGRID 日志文件

StorageGRID 提供用于捕获事件、诊断消息和错误条件的日志。您可能需要收集日志文件并将其转发给技术支持部门，以协助进行故障排除。

日志分为以下几类：

- "StorageGRID 软件日志"
- "部署和维护日志"
- "关于 bycast.log"

> 为每种日志类型提供的详细信息仅供参考。这些日志用于技术支持人员的高级故障排除。涉及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这些说明的范围之内。

访问日志

要访问日志，可以"收集日志文件和系统数据"从一个或多个节点将日志作为单个日志文件存档下载。或者，您可以按如下方式访问每个网格节点的单独日志文件：

步骤

1. 输入以下命令： `ssh admin@grid_node_IP`
2. 输入 `Passwords.txt`文件中列出的密码。
3. 输入以下命令切换到 root： `su -`
4. 输入 `Passwords.txt`文件中列出的密码。

将日志导出到 **syslog** 服务器

将日志导出到 syslog 服务器可提供以下功能：

- 接收所有 Grid Manager 和 Tenant Manager 请求以及 S3 请求的列表。

- 更好地了解返回错误的 S3 请求，而不会受到审核日志记录方法造成的性能影响。
- 访问易于解析的 HTTP 层请求和错误代码。
- 更好地了解负载均衡器中流量分类器阻止的请求。

要导出日志，请参阅 "配置日志管理和外部 syslog 服务器"。

日志文件类别

StorageGRID 日志文件存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	问题描述
audit	正常系统运行期间生成的审核消息。
base-os-logs	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）。
cache-svc	缓存服务日志（仅适用于网关节点）。
cassandra	Cassandra 数据库信息和 Reaper 修复日志。
ec	按配置文件 ID 提供有关当前节点和 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.json	跨所有节点共享的网格配置文件。此外， `node.json`还特定于当前节点。
hagroups	高可用性组指标和日志。
安装	`Gdu-server` 和安装日志。
Lambda 仲裁器	与 S3 Select 代理请求相关的日志。
leakd	来自 leakd 服务的日志。
lumberjack.log	调试与日志收集相关的消息。
指标	Grafana、Jaeger、节点导出器和 Prometheus 的服务日志。
miscd	Miscd 访问和错误日志。
mysql	MariaDB 数据库配置和相关日志。

归档位置	问题描述
网络	由与网络相关的脚本和 Dynip 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 Tenant Manager 流量日志。
nginx-gw	• `access.log`：Grid Manager 和 Tenant Manager 请求日志消息。 ◦ 使用 syslog 导出时，这些消息的前缀为 `mgmt:`。 ◦ 这些日志消息的格式是 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`：入站跨网格复制请求。 ◦ 使用 syslog 导出时，这些消息的前缀为 `cgr:`。 ◦ 这些日志消息的格式是 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`：S3 请求到负载均衡器端点。 ◦ 使用 syslog 导出时，这些消息的前缀为 `endpoint:`。 ◦ 这些日志消息的格式是 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`：与新的 DNS 检查警报相关。
NTP	NTP 配置文件和日志。
孤立对象	与孤立对象相关的日志。
操作系统	节点和网格状态文件，包括服务 `pid`。
其他	`/var/local/log` 下方的日志文件未收集在其他文件夹中。
perf	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	与网格配置流程相关的日志。
raft	平台服务中使用的 Raft 集群日志。

归档位置	问题描述
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。
sockets-data	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，例如网络和磁盘使用情况。
synchronize-recovery-package	与维护托管 ADC 服务的所有管理节点和存储节点之间的最新恢复包的一致性相关。

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 syslog 服务器或更改审核信息的目标（如 `bycast.log`和 `nms.log`），请参阅"配置日志管理"。

常规 **StorageGRID** 日志

文件名	说明	发现于
/var/local/log/bycast.log	主要 StorageGRID 故障排除文件。	所有节点
/var/local/log/bycast-err.log	包含 `bycast.log`的子集（严重性为 ERROR 和 CRITICAL 的消息）。CRITICAL 消息也会显示在系统中。	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。 **Note**: 该文件 ``/var/local/core/kexec_cmd`通常存在于设备节点上，并不表示错误。	所有节点

密码相关日志

文件名	说明	发现于
/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

文件名	说明	发现于
/var/local/log/nginx/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/nginx-gw/config-generation.log	包含与生成nginx-gw配置（和重新加载nginx-gw服务）相关的日志。	管理和网关节点
/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

网格联盟日志

文件名	说明	发现于
/var/local/log/update_grid_federation_config.log	包含与为网格联合连接生成 nginx 和 nginx-gw 配置相关的日志。	所有节点

NMS 日志

文件名	说明	发现于
/var/local/log/nms.log	• 捕获来自 Grid Manager 和 Tenant Manager 的通知。 • 捕获与 NMS 服务操作相关的事件。例如，电子邮件通知和配置更改。 • 包含在系统中进行的配置更改导致的 XML 捆绑包更新。 • 包含与每天一次的属性降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。 • 包含与 AutoSupport 相关的日志。	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 Management API 到内部 StorageGRID 服务的传出连接的信息。	管理节点

服务器管理器日志

文件名	说明	发现于
/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 GUI 的日志文件。	所有节点

StorageGRID 服务日志

文件名	说明	发现于
/var/local/log/acct.errlog		运行 ADC 服务的存储节点
/var/local/log/adc.errlog	包含相应服务的标准错误 (stderr) 流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	运行 ADC 服务的存储节点
/var/local/log/ams.errlog		管理节点
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	缓存服务日志。	网关节点
/var/local/log/cassandra/system.log	元数据存储（Cassandra 数据库）的信息，可在添加新存储节点时出现问题或 nodetool repair 任务停止时使用。	存储节点
/var/local/log/cassandra-reaper.log	Cassandra Reaper 服务的信息，该服务对 Cassandra 数据库中的数据进行修复。	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本 StorageGRID 升级的系统上。它包含旧版信息。	存储节点
/var/local/log/dds.errlog		存储节点

文件名	说明	发现于
/var/local/log/dmv.errlog		存储节点
/var/local/log/dynip*	包含与 dynip 服务相关的日志，该服务监控网格中的动态 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 Grid Manager 中的指标可视化。	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 BACKUP 到 MASTER 或 FAULT 的转换。	管理节点和网关节点
/var/local/log/idnt.errlog		运行 ADC 服务的存储节点
/var/local/log/jaeger.log	与用于跟踪收集的 jaeger 服务关联的日志。	所有节点
/var/local/log/kstn.errlog		运行 ADC 服务的存储节点
/var/local/log/lambda*	包含 S3 Select 服务的日志。	管理和网关节点 只有某些管理节点和网关节点包含此日志。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/miscd/*.log	包含MISCd服务（信息服务控制守护程序）的日志，它提供了一个接口，用于查询和管理其他节点上的服务以及管理节点上的环境配置，例如查询其他节点上运行的服务的状态。	所有节点
/var/local/log/nginx/*.log	包含 nginx 服务的日志，该日志充当各种网格服务（例如 Prometheus 和 Dynip）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通信。	所有节点
/var/local/log/nginx-gw/*.log	包含与nginx-gw服务相关的一般日志，包括错误日志和管理节点上受限管理端口的日志。	管理节点和网关节点

文件名	说明	发现于
/var/local/log/nginx-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，基于网格联合配置。仅在跨网格复制的目标网格上找到。
/var/local/log/nginx-gw/endpoint-access.log.gz	包含负载平衡器服务的访问日志，该服务提供从客户端到存储节点的 S3 流量的负载平衡。	管理节点和网关节点
/var/local/log/persistence*	包含持久性服务的日志，该服务管理根磁盘上需要在重新启动后保持的文件。	所有节点
/var/local/log/prometheus.log	对于所有节点，包含节点导出服务日志和 ade-exporter 指标服务日志。 对于管理节点，还包含 Prometheus 和 Alert Manager 服务的日志。	所有节点
/var/local/log/raft.log	包含 RSM 服务用于 Raft 协议的库的输出。	具有 RSM 服务的存储节点
/var/local/log/rms.errlog	包含复制状态机服务 (RSM) 服务的日志，该服务用于 S3 平台服务。	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 S3 虚拟托管域名配置的处理更新相关的日志。请参阅实施 S3 客户端应用程序的说明。	管理和网关节点
/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 syslog 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。	管理和网关节点
/var/local/log/update-utcn.log	包含与此节点上的不受信任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"

StorageGRID 中的部署和维护日志

您可以使用部署和维护日志对问题进行故障排除。

文件名	说明	发现于
/var/local/log/install.log	在软件安装过程中创建。包含安装事件的记录。	所有节点
/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 `pa-move.sh`脚本时创建。	主管理节点
/var/local/log/pa-move-new_pa.log	在运行 `pa-move.sh`脚本时创建。	主管理节点
/var/local/log/pa-move-old_pa.log	在运行 `pa-move.sh`脚本时创建。	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。	管理节点
/var/local/log/send_admin_hw.log	在安装过程中创建。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

了解 StorageGRID bycast.log

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

此文件 `/var/local/log/bycast-err.log`是 `bycast.log`的子集。它包含严重性为 ERROR 和 CRITICAL 的消息。

也可以更改审核日志的目标，并将审核信息发送到外部 syslog 服务器。配置外部 syslog 服务器时，将继续生成和存储审核记录的本地日志。请参阅 "配置日志管理和外部 syslog 服务器"。

bycast.log 的文件轮换

当 `bycast.log`文件达到 1 GB 时，将保存现有文件，并启动新的日志文件。

保存的文件被重命名 `bycast.log.1`，新文件被命名为 `bycast.log`。当新的 `bycast.log`达到 1 GB 时，`bycast.log.1`将被重命名并压缩为 `bycast.log.2.gz`，`bycast.log`被重命名为 `bycast.log.1`。

的轮换限制 `bycast.log`为 21 个文件。创建 `bycast.log`文件的第 22 个版本时，将删除最旧的文件。

`bycast-err.log` 的轮换限制为七个文件。

如果日志文件已压缩，则不得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转脚本。

也可以更改审核日志的目标，并将审核信息发送到外部 syslog 服务器。配置外部 syslog 服务器时，将继续生成和存储审核记录的本地日志。请参阅 "配置日志管理和外部 syslog 服务器"。

相关信息

"收集日志文件和系统数据"

bycast.log 中的消息

`bycast.log` 中的消息由 ADE（异步分布式环境）写入。ADE 是每个网格节点的服务所使用的运行时环境。

ADE 消息示例：

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE消息中包含以下信息：

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.uuuuuu)
严重级别	错误
内部跟踪编号	0906
消息	SVMR：卷 3 的运行状况检查失败，原因为"TOUT"

bycast.log 中的消息严重性

`bycast.log`中的消息被分配了严重性级别。

例如：

- **NOTICE** — 应记录的事件已发生。大多数日志消息都在此级别。
- **WARNING** — 发生意外情况。
- **ERROR** — 发生严重错误，将影响操作。
- **CRITICAL** — 发生异常情况，已停止正常操作。您应立即解决潜在问题。

中的错误代码 bycast.log

中的大多数错误消息 `bycast.log`都包含错误代码。

下表列出了 bycast.log 中的常见非数字代码。非数字代码的确切含义取决于报告该代码时的上下文。

错误代码	含义
SUCS	无错误
GERR	未知
取消	已取消
ABRT	已中止
全部	超时
INVL	无效
NFND	未找到
VERS	版本
CONF	配置
失败	失败
ICPL	未完成
完成	完成

错误代码	含义
SUNV	服务不可用

下表列出了 `bycast.log` 中的数字错误代码。

错误编号	错误代码	含义
001	EPERM	不允许执行此操作
002	ENOENT	不存在此文件或目录
003	ESRCH	没有此类进程
004	EINTR	中断的系统调用
005	EIO	I/O错误
006	ENXIO	不存在此设备或地址
007	E2BIG	参数列表太长
008	ENOEXEC	Exec格式错误
009	EBADF	错误的文件编号
010	ECHILD	无子进程
011	EAGAIN	重试
012	ENOMEM	内存不足
013	EACCES	权限被拒绝
014	EFAULT	地址错误
015	ENOTBLK	需要块设备
016	EBUSY	设备或资源正忙
017	EEXIST	文件已存在
018	EXDEV	跨设备链接

错误编号	错误代码	含义
019	ENODEV	没有这样的设备
020	ENOTDIR	不是目录
021	EISDIR	是一个目录
022	EINVAL	参数无效
023	ENFILE	文件表溢出
024	EMFILE	打开的文件太多
025	ENOTTY	不是打字机
026	ETXTBSY	文本文件忙
027	EFBIG	文件过大
028	ENOSPC	No space left on device
029	ESPIPE	非法寻址
030	EROFS	只读文件系统
031	EMLINK	链接过多
032	EPIPE	管道断裂
033	EDOM	数学参数超出函数域
034	ERANGE	数学结果不可表示
035	EDEADLK	将发生资源死锁
036	ENAMETOOLONG	文件名太长
037	ENOLCK	无可用记录锁定
038	ENOSYS	功能未实现
039	ENOTEMPTY	目录不为空

错误编号	错误代码	含义
040	ELOOP	遇到太多符号链接
041		
042	ENOMSG	没有所需类型的消息
043	EIDRM	已删除标识符
044	ECHRNG	通道号超出范围
045	EL2NSYNC	2 级未同步
046	EL3HLT	Level 3 已停止
047	EL3RST	3 级重置
048	ELNRNG	链接数超出范围
049	EUNATCH	协议驱动程序未连接
050	ENOCSI	没有可用的CSI结构
051	EL2HLT	Level 2 已停止
052	EBADE	无效交换
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	EBADSLT	插槽无效
058		
059	EBFONT	字体文件格式错误
060	ENOSTR	设备不是流

错误编号	错误代码	含义
061	ENODATA	没有可用数据
062	ETIME	计时器已过期
063	ENOSR	流资源不足
064	ENONET	机器不在网络上
065	ENOPKG	未安装软件包
066	EREMOTE	对象是远程的
067	ENOLINK	链接已被切断
068	EADV	通告错误
069	ESRMNT	Srmount错误
070	ECOMM	发送时出现通信错误
071	EPROTO	协议错误
072	EMULTIHOP	已尝试多跳
073	EDOTDOT	RFS 特定错误
074	EBADMSG	不是数据消息
075	EOVERFLOW	值对于定义的数据类型太大
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	EREMCHG	远程地址已更改
079	ELIBACC	无法访问所需的共享库
080	ELIBBAD	访问已损坏的共享库
081	ELIBSCN	

错误编号	错误代码	含义
082	ELIBMAX	尝试链接过多共享库
083	ELIBEXEC	无法直接执行共享库
084	EILSEQ	非法的字节序列
085	ERESTART	中断的系统调用应重新启动
086	ESTRPIPE	Streams 管道错误
087	EUSERS	用户过多
088	ENOTSOCK	非套接字上的套接字操作
089	EDESTADDRREQ	目的地地址为必填项
090	EMSGSIZE	消息太长
091	EPROTOTYPE	套接字的协议类型错误
092	ENOPROTOOPT	协议不可用
093	EPROTONOSUPPORT	不支持此协议
094	ESOCKTNOSUPPORT	套接字类型不受支持
095	EOPNOTSUPP	传输端点不支持此操作
096	EPFNOSUPPORT	不支持的协议系列
097	EAFNOSUPPORT	协议不支持地址族
098	EADDRINUSE	地址已在使用
099	EADDRNOTAVAIL	无法分配请求的地址
100	ENETDOWN	网络已关闭
101	ENETUNREACH	网络不可达
102	ENETRESET	由于重置，网络连接中断

错误编号	错误代码	含义
103	ECONNABORTED	软件导致连接终止
104	ECONNRESET	对等体重置连接
105	ENOBUFS	没有可用的缓冲区空间
106	EISCONN	传输端点已连接
107	ENOTCONN	传输端点未连接
108	ESHUTDOWN	传输端点关闭后无法发送
109	ETOOMANYREFS	引用太多：无法拼接
110	ETIMEDOUT	连接超时
111	ECONNREFUSED	连接被拒绝
112	EHOSTDOWN	主机已关闭
113	EHOSTUNREACH	没有到主机的路由
114	EALREADY	操作已在进行中
115	EINPROGRESS	操作正在进行中
116		
117	EUCLEAN	结构需要清理
118	ENOTNAM	不是 XENIX 命名类型文件
119	ENAVAIL	没有可用的 XENIX 信号量
120	EISNAM	是命名类型文件
121	EREMOTEIO	远程 I/O 错误
122	EDQUOT	已超出配额
123	ENOMEDIUM	未找到介质

错误编号	错误代码	含义
124	EMEDIUMTYPE	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	EKEYREVOKED	密钥已被吊销
129	EKEYREJECTED	密钥被服务拒绝
130	EOWNERDEAD	对于健壮互斥锁：所有者已死亡
131	ENOTRECOVERABLE	对于稳健的互斥：状态不可恢复

配置日志管理和外部 **syslog** 服务器

StorageGRID 中的外部系统日志服务器

外部 syslog 服务器是 StorageGRID 外部的服务器，可用于在单个位置收集系统审核信息。使用外部 syslog 服务器可以减少管理节点上的网络流量并更有效地管理信息。对于 StorageGRID，出站 syslog 消息数据包格式符合 RFC 3164。

可以发送到外部syslog服务器的审核信息类型包括：

- 包含正常系统运行期间生成的审核消息的审核日志
- 与安全相关的事件，例如登录和升级到 root
- 如果需要开立支持案例以排查您所遇到的问题，可能会被要求提供的应用程序日志

何时使用外部 **syslog** 服务器

如果您有大型网格、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 syslog 服务器特别有用。向外部 syslog 服务器发送审核信息，您可以：

- 更有效地收集和管理审计消息、应用程序日志和安全事件等审计信息。
- 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 syslog 服务器，而无需通过管理节点。

> 当日志发送到外部 syslog 服务器时，大于 8,192 字节的单个日志将在消息末尾被截断，以符合外部 syslog 服务器实现中的常见限制。

为了在外部系统日志服务器发生故障时最大化完整数据恢复的选项，每个节点上最多维护 20 GB 的审核记录本地日志(`localaudit.log`）。

如何配置外部 **syslog** 服务器

要了解如何配置外部 syslog 服务器，请参见 "配置日志管理和外部 syslog 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：

- **Server CA certificates**：用于验证 PEM 编码的外部 syslog 服务器的一个或多个受信任的 CA 证书。如果省略，将使用默认网格 CA 证书。
- 客户端证书：用于以 PEM 编码向外部 syslog 服务器进行身份验证的客户端证书。
- 客户端私钥：PEM 编码的客户端证书私钥。

如果使用客户端证书，则还必须使用客户端私钥。如果提供加密的私钥，则还必须提供密码。使用加密私钥没有显著的安全性优势，因为必须存储密钥和密码；为简便起见，建议使用未加密的私钥（如果有）。

如何估计外部 **syslog** 服务器的大小

通常，您的网格大小应能达到所需的吞吐量，以每秒 S3 操作数或每秒字节数来定义。例如，您可能需要网格每秒处理 1,000 次 S3 操作，或每秒 2,000 MB 的对象提取和检索。您应根据网格的数据要求来调整外部 syslog 服务器的大小。

本节提供了一些启发式公式，可帮助您估计外部 syslog 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，以网格的已知或所需性能特征（每秒 S3 操作数）表示。

在估算公式中使用每秒 **S3** 操作数

如果您的网格大小是以每秒字节数表示的吞吐量，则必须将此大小转换为每秒 S3 操作才能使用估算公式。要转换网格吞吐量，您必须首先确定平均对象大小，可以使用现有审计日志和指标（如果有）中的信息，或利用您对将使用 StorageGRID 的应用程序的了解来确定。例如，如果网格的大小可达到 2,000 MB/秒的吞吐量，且平均对象大小为 2 MB，则网格的大小可处理每秒 1,000 次 S3 操作（2,000 MB / 2 MB）。

以下各节中的外部 syslog 服务器规模调整公式提供了常见情况估计（而不是最坏情况估计）。根据您的配置和工作负载，您可能会看到比公式预测的更高或更低的 syslog 消息速率或 syslog 数据量。这些公式仅用作指南。

审核日志的估算公式

如果除了网格每秒应支持的 S3 操作数之外，没有关于 S3 工作负载的信息，则可以使用以下公式估算外部 syslog 服务器需要处理的审核日志量，前提是将"审核级别"设置为默认值（所有类别都设置为"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，如果您的网格大小为每秒 1,000 个 S3 操作，则外部 syslog 服务器的大小应支持每秒 2,000 个 syslog 消息，并且应能够以每秒 1.6 MB 的速率接收（通常存储）审核日志数据。

如果您对工作负载有更多了解，则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 PUT（相对于 GET）操作占 S3 操作的百分比，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	问题描述
SACC	S3 租户帐户名称（请求发送方）	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（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
S3BK	S3 存储分段	S3 存储桶名称。
S3KY	S3密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。

让我们使用 P 来表示 S3 操作中 PUT 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、S3 存储桶和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account（13 个字节），存储桶具有固定长度的名称，如 /my/application/bucket-12345（28 个字节），并且对象具有固定长度的密钥，如 5733a5d7-f069-41ef-8fbd-13247494c69c（36 个字节）。则 K 的值为 90 (13+13+28+36)。

如果可以确定 P 和 K 的值，则可以使用以下公式估算外部 syslog 服务器需要处理的审核日志量，前提是将"审核级别"设置为默认值（所有类别都设置为"正常"，存储设置为"错误"除外）：

```
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 个 S3 操作，您的工作负载为 50% PUT，并且您的 S3 帐户名称、存储桶名称和对象名称平均为 90 个字节，则外部 syslog 服务器的大小应支持每秒 1,500 个 syslog 消息，并且应能够以约 1 MB/秒的速率接收（通常存储）审核日志数据。

非默认审核级别的估算公式

为审核日志提供的公式假设使用默认审核级别设置（所有类别均设置为"正常"，但"存储"除外，后者设置为"错误"）。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可用。但是，下表可用于粗略估计速率；您可以使用为审核日志提供的平均大小公式，但请注意，这可能会导致高估，因为"额外"审核消息平均小于默认审核消息。

条件	公式
复制：审核级别均设置为"调试"或"正常"	审核日志速率 = 8 x S3 操作速率

条件	公式
擦除编码：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，通常产生的日志和数据量可以忽略不计。出于这些原因，没有提供估算公式。

应用程序日志的估算公式

如果除了网格每秒预计支持的 S3 操作数量之外，您没有关于 S3 工作负载的信息，则可以使用以下公式估算外部 syslog 服务器需要处理的应用程序日志量：

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

因此，例如，如果您的网格大小为每秒 1,000 个 S3 操作，则外部 syslog 服务器的大小应支持每秒 3,300 个应用程序日志，并能够以每秒约 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，则可以进行更准确的估算。对于应用程序日志，最重要的附加变量是数据保护策略（复制与擦除编码）、属于 PUT 的 S3 操作的百分比（与 GET/其他相比）以及以下 S3 字段的平均大小（以字节为单位）（表中使用的 4 字符缩写是审计日志字段名称）：

代码	字段	问题描述
SACC	S3 租户帐户名称（请求发送方）	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（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
S3BK	S3 存储分段	S3 存储桶名称。
S3KY	S3密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。

示例规模估算

本节通过以下数据保护方法，说明如何使用网格估计公式的示例案例：

- 复制
- 纠删编码

如果使用复制进行数据保护

设 P 表示作为 PUT 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、S3 存储桶和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account（13 个字节），存储桶具有固定长度的名称，如 /my/application/bucket-12345（28 个字节），并且对象具有固定长度的密钥，如 5733a5d7-f069-41ef-8fbd-13247494c69c（36 个字节）。则 K 的值为 90（13+13+28+36）。

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

```
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，如果您的网格大小为每秒 1,000 次 S3 操作，您的工作负载为 50% 的 PUT，并且您的 S3 帐户名称、存储桶名称和对象名称平均为 90 个字节，则外部 syslog 服务器的大小应支持每秒 1800 个应用程序日志，并将以每秒 0.5 MB 的速率接收（通常存储）应用程序数据。

如果使用擦除编码进行数据保护

设 P 表示作为 PUT 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、S3 存储桶和 S3 密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account（13 个字节），存储桶具有固定长度的名称，如 /my/application/bucket-12345（28 个字节），并且对象具有固定长度的密钥，如 5733a5d7-f069-41ef-8fbd-13247494c69c（36 个字节）。则 K 的值为 90（13+13+28+36）。

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

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

因此，例如，如果您的网格大小为每秒 1,000 次 S3 操作，您的工作负载为 50% PUTs，并且您的 S3 帐户名、存储桶名和对象名平均为 90 个字节，则您的外部 syslog 服务器的大小应支持每秒 2,250 个应用程序日志，并且应能够以每秒 0.6 MB 的速率接收（通常为存储）应用程序数据。

在 **StorageGRID** 中配置日志管理

根据需要，配置审核级别、协议标头以及审核消息和日志的位置。

所有 StorageGRID 节点都会生成审计消息和日志，以跟踪系统活动和事件。审计消息和日志是监控和故障排除的重要工具。

或者，您可以"配置外部 syslog 服务器"远程保存审核信息。使用外部服务器可最大限度地减少审核消息日志记录的性能影响，而不会降低审核数据的完整性。如果您拥有大型网格、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 syslog 服务器特别有用。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。

- 如果您计划配置外部 syslog 服务器，则已查看并遵循 "使用外部 syslog 服务器的注意事项"。
- 如果您计划使用 TLS 或 RELP/TLS 协议配置外部 syslog 服务器，则拥有所需的服务器 CA 和客户端证书以及客户端私钥。

更改审核消息级别

可为审核日志中的以下每类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"
存储	错误	"对象存储审核消息"
管理	正常	"管理审计消息"
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审计消息"
跨网格复制	错误	"CGRR：跨网格复制请求"

在升级期间，审核级别配置不会立即生效。

步骤

1. 选择*配置* > 监控 > 日志管理。
2. 对于每个审计消息类别，从下拉列表中选择一个审计级别：

审核级别	问题描述
关闭	该类别中没有任何审核消息被记录。
错误	仅记录错误消息——结果代码未"成功"(SUCS)的审核消息。
正常	将记录标准事务性消息——这些说明中列出的该类别的消息。
调试	已弃用。此级别与正常审核级别相同。

任何特定级别所包含的消息，也包括将在更高级别记录的消息。例如，Normal 级别包含所有 Error 消息。

如果您不需要 S3 应用程序的客户端读取操作的详细记录，可以选择将*客户端读取*设置更改为*错误*，以减少审核日志中记录的审核消息数量。

3. 选择 **Save**。

定义 HTTP 请求标头

可以选择定义要包含在客户端读取和写入审核消息中的任何 HTTP 请求标头。

步骤

1. 在*审核协议标头*部分中，定义要包含在客户端读取和写入审核消息中的 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 **Add another header** 以创建其他标题。

   当在请求中找到 HTTP 标头时，它们将包含在 HTRH 字段下的审核消息中。

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

3. 选择 **Save**

配置日志位置

默认情况下，审核消息和日志保存在生成它们的节点上。它们会定期轮换并最终删除，以防止占用过多的磁盘空间。如果要在外部保存审核消息和日志子集，请 使用外部 syslog 服务器。

如果要在内部保存日志文件，请选择用于日志存储的租户和存储区并启用日志存档。

使用外部 syslog 服务器

您可以选择配置外部 syslog 服务器，以将审核日志、应用程序日志和安全事件日志保存到网格外部的位置。

如果不想使用外部 syslog 服务器，请跳过此步骤并转到 选择日志位置。

如果此过程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 `audit-destinations`端点应用其他配置选项，这些端点位于"网格管理 API"的私有 API 部分。例如，如果要为不同的节点组使用不同的 syslog 服务器，则可以使用 API。

输入 syslog 信息

访问配置外部 syslog 服务器向导，并提供 StorageGRID 访问外部 syslog 服务器所需的信息。

步骤

1. 从本地节点和外部服务器选项卡中，选择*配置外部 syslog 服务器*。或者，如果您之前已配置过外部 syslog 服务器，请选择*编辑外部 syslog 服务器*。

   此时将显示Configure external syslog server向导。

2. 对于向导的 **Enter syslog info** 步骤，请在 **Host** 字段中为外部 syslog 服务器输入有效的完全限定域名或 IPv4 或 IPv6 地址。
3. 输入外部 syslog 服务器上的目标端口（必须是 1 到 65535 之间的整数）。默认端口为 514。

4. 选择用于将审核信息发送到外部 syslog 服务器的协议。

   建议使用 **TLS** 或 **RELP/TLS**。您必须上传服务器证书才能使用这些选项之一。使用证书有助于保护网格与外部 syslog 服务器之间的连接。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 syslog 服务器的支持和配置。您必须选择一个与外部 syslog 服务器兼容的选项。

   > 可靠事件日志记录协议 (RELP) 扩展了 syslog 协议的功能，以提供事件消息的可靠传递。使用 RELP 有助于防止在外部 syslog 服务器重新启动时丢失审计信息。

5. 选择 **Continue**。
6. 如果您选择了 **TLS** 或 **RELP/TLS**，请上传服务器 CA 证书、客户端证书和客户端私钥。
   a. 选择要使用的证书或密钥的*浏览*。
   b. 选择证书或密钥文件。
   c. 选择*打开*以上传文件。

      证书或密钥文件名旁边将显示一个绿色复选标记，通知您已成功上传。

7. 选择 **Continue**。

管理系统日志内容

您可以选择要发送至外部 syslog 服务器的信息。

步骤

1. 对于向导的*管理 syslog 内容*步骤，选择要发送到外部 syslog 服务器的每种类型的审核信息。
   - 发送审核日志：发送 StorageGRID 事件和系统活动
   - **Send security events**：发送安全事件，例如当未经授权的用户尝试登录或用户以 root 身份登录时
   - 发送应用程序日志：发送"StorageGRID 软件日志文件"用于故障排除，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` （仅管理节点）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - 发送访问日志：将外部请求的 HTTP 访问日志发送到 Grid Manager、Tenant Manager、配置的负载均衡器端点以及来自远程系统的网格联合请求。
2. 使用下拉菜单为要发送的每个审核信息类别选择严重性和设施（消息类型）。

   设置严重程度和设施值可以帮助您以可自定义的方式聚合日志，以便更轻松地进行分析。

   a. 对于*严重程度*，选择*Passthrough*，或选择一个介于 0 到 7 之间的严重程度值。

如果选择一个值，则所选值将应用于所有此类型的消息。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。

严重性	问题描述
Passthrough	发送到外部 syslog 的每条消息都具有与本地记录到节点上时相同的严重性值： • 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 发行版生成。 • 对于应用程序日志，严重程度在"info"和"notice"之间有所不同，具体取决于问题是什么。例如，添加 NTP 服务器和配置 HA 组会给出"info"的值，而故意停止 SSM 或 RSM 服务会给出"notice"的值。 • 对于访问日志，严重性为"info"。
0	紧急情况：系统无法使用
1	警告：必须立即采取行动
2	严重：严重情况
3	错误:错误条件
4	警告：警告条件
5	注意：正常但重要的状况
6	Informational：信息性消息
7	调试：调试级消息

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

如果选择一个值，则它将应用于所有此类型的消息。如果使用固定值覆盖设施，则有关不同设施的信息将丢失。

工具	问题描述
Passthrough	发送到外部 syslog 的每条消息都具有与本地登录到节点时相同的设施值： • 对于审核日志，发送到外部 syslog 服务器的设施为"local7"。 • 对于安全事件，设施值由节点上的 linux 发行版生成。 • 对于应用程序日志，发送到外部 syslog 服务器的应用程序日志具有以下设施值： ◦ `bycast.log`：user 或 daemon ◦ `bycast-err.log`：user、daemon、local3 或 local4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`：local6 • 对于访问日志，发送到外部 syslog 服务器的设施为"local0"。
0	kern（内核消息）
1	用户（用户级消息）
2	邮件
3	守护程序（系统守护程序）
4	auth（安全/授权消息）
5	syslog（由 syslogd 内部生成的消息）
6	lpr（行打印机子系统）
7	news（网络新闻子系统）
8	UUCP
9	cron（时钟守护进程）
10	安全（安全/授权消息）
11	FTP

工具	问题描述
12	NTP
13	logaudit（日志审核）
14	logalert（日志警报）
15	clock（时钟守护进程）
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. 选择 **Continue**。

发送测试消息

在开始使用外部 syslog 服务器之前，应请求网格中的所有节点将测试消息发送到外部 syslog 服务器。在确认将数据发送到外部 syslog 服务器之前，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。

请勿使用外部 syslog 服务器配置，直到您确认外部 syslog 服务器收到来自网格中每个节点的测试消息，并且该消息已按预期处理。

步骤

1. 如果您不想发送测试消息，因为您确定外部 syslog 服务器已正确配置并且可以从网格中的所有节点接收审核信息，请选择*跳过并完成*。

   绿色横幅指示配置已保存。

2. 否则，请选择*发送测试消息*（推荐）。

   测试结果会不断显示在页面上，直至您停止测试为止。在测试进行期间，您的审核消息将继续发送到先前配置的目的地。

3. 如果在 syslog 服务器配置或运行时收到任何错误，请更正并再次选择*发送测试消息*。

   请参阅"对外部 syslog 服务器进行故障排除"以帮助解决任何错误。

4. 等待，直到您看到一个绿色横幅，指示所有节点已通过测试。
5. 检查您的 syslog 服务器，以确定是否按预期接收和处理测试消息。

   如果使用的是 UDP，请检查整个日志收集基础设施。UDP 协议不支持像其他协议那样严格的错误检测。

6. 选择*停止并完成*。

   您将返回到*审核和syslog服务器*页面。绿色横幅指示已保存syslog服务器配置。

   在选择包含外部 syslog 服务器的目标之前，StorageGRID 审核信息不会发送到外部 syslog 服务器。

选择日志位置

您可以指定审核日志、安全事件日志、"StorageGRID 应用程序日志"和访问日志的发送位置。

StorageGRID 默认为本地节点审核目标，并将审核信息存储在 `/var/local/log/localaudit.log`中。

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

仅当配置了外部 syslog 服务器时，某些目标才可用。

步骤

1. 选择*日志位置* > 本地节点和外部服务器。
2. 要更改日志类型的日志位置，请选择其他选项。

   *仅本地节点*和*外部 syslog 服务器*通常提供更好的性能。

选项	问题描述
仅本地节点（默认）	审核消息、安全事件日志和应用程序日志不会发送到管理节点。相反，它们仅保存在生成它们的节点（"本地节点"）上。在每个本地节点上生成的审核信息存储在 `/var/local/log/localaudit.log`中。 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，将保存现有文件，并启动一个新的日志文件。日志的轮换限制为 21 个文件。当创建日志文件的第 22 个版本时，将删除最旧的日志文件。每个节点上平均存储约 20 GB 的日志数据。要长时间存储日志，请 使用租户和存储桶进行日志存储。

选项	问题描述
管理节点/本地节点	审核消息发送到管理节点上的审核日志，安全事件日志和应用程序日志存储在生成它们的节点上。审核信息存储在以下文件中： • 管理节点（主节点和非主节点）：`/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log` 文件通常为空或缺失。它可能包含辅助信息，例如某些消息的其他副本。
外部 syslog 服务器	审核信息将发送到外部 syslog 服务器并保存在本地节点上（`/var/local/log/localaudit.log`）。发送的信息类型取决于您如何配置外部 syslog 服务器。只有在完成已配置外部 syslog 服务器之后，才会启用此选项。
管理节点和外部 syslog 服务器	审核消息发送到管理节点上的审核日志（`/var/local/audit/export/audit.log`），审核信息发送到外部 syslog 服务器并保存在本地节点上（`/var/local/log/localaudit.log`）。发送的信息类型取决于您如何配置外部 syslog 服务器。只有在完成已配置外部 syslog 服务器之后，才会启用此选项。

3. 选择 **Save**。

   此时将显示一条警告消息。

4. 选择*OK*以确认要更改审核信息的目标。

   新日志将发送到您选择的目的地。现有日志保留在其当前位置。

使用存储桶

日志会定期轮换。使用同一网格中的 S3 存储桶将日志存储较长时间。

1. 选择*日志位置* > 使用存储桶。
2. 选中*启用归档日志*复选框。
3. 如果列出的租户和存储桶不是您要使用的，请选择 **Change tenant and bucket**，然后选择 **Create tenant and bucket** 或 **Select tenant and bucket**。

创建租户和存储桶

a. 输入新的租户名称。
b. 输入并确认新租户的密码。
c. 输入新的存储桶名称。
d. 选择*创建并启用*。

选择租户和存储桶

a. 从下拉列表中选择租户名称。
b. 从下拉菜单中选择一个存储桶。
c. 选择*选择并启用*。

4. 选择 **Save**。

日志将存储在您指定的租户和存储桶中。日志的对象键名称采用以下格式：

```
system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
{last_modified_time}.gz
```

例如：

```
system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
```

使用 SNMP 监控

在 StorageGRID 中使用 SNMP 监控

如果要使用简单网络管理协议 (SNMP) 监控 StorageGRID，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 节点都运行提供 MIB 的 SNMP 代理或守护程序。StorageGRID MIB 包含警报的表和通知定义。MIB 还包含系统描述信息，例如每个节点的平台和型号。每个 StorageGRID 节点还支持 MIB-II 对象的子集。

如果您想在网格节点上下载 MIB 文件，请参阅 "访问 MIB 文件"。

最初，在所有节点上禁用 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通知：

陷阱

陷阱是由 SNMP 代理发送的通知，不需要管理系统的确认。陷阱用于通知管理系统 StorageGRID 中发生的事件，例如触发警报。

所有三个版本的 SNMP 均支持陷阱。

通知

Inform 类似于陷阱，但需要管理系统确认。如果 SNMP 代理在一定时间内没有收到确认，它会重新发送 inform，直到收到确认或达到最大重试值。

SNMPv2c 和 SNMPv3 支持 Inform。

在以下情况下会发送陷阱和通知消息：

- 在任何严重程度下都会触发默认或自定义警报。要抑制警报的 SNMP 通知，您必须"配置静默"为警报。警报通知由"首选发件人管理节点"发送。

  每个警报都会根据警报的严重性级别映射到三种陷阱类型之一：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"。

SNMP 版本支持

该表提供了每个 SNMP 版本支持内容的高级摘要。

	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 （TRAP 和 INFORM）	仅限陷阱	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	每个陷阱目的地的 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受相同的配置。

- SNMPv3：StorageGRID 不支持传输支持模式 (TSM)。
- SNMPv3：唯一支持的身份验证协议是 SHA (HMAC-SHA-96)。
- SNMPv3：唯一支持的隐私协议是 AES。

在 **StorageGRID** 中配置 **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

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

StorageGRID SNMP 代理支持 SNMPv1、SNMPv2c 和 SNMPv3。您可以为一个或多个版本配置此代理。对于 SNMPv3，仅支持用户安全模型 (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

第一步，启用 StorageGRID SNMP 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. 在基本配置部分输入以下信息。

字段	问题描述
系统联系人	可选。StorageGRID 系统的主要联系人，在 SNMP 消息中返回为 sysContact。 系统联系人通常是一个电子邮件地址。此值适用于 StorageGRID 系统中的所有节点。*系统联系人*最多可包含 255 个字符。
系统位置	可选。StorageGRID 系统的位置，在 SNMP 消息中返回为 sysLocation。 系统位置可以是用于识别 StorageGRID 系统位置的任何信息。例如，您可以使用设施的街道地址。此值适用于 StorageGRID 系统中的所有节点。*系统位置*最多可包含 255 个字符。

字段	问题描述
启用 SNMP 代理通知	• 如果选中，StorageGRID SNMP 代理将发送陷阱和通知消息。 • 如果未选中，则 SNMP 代理支持只读 MIB 访问，但不发送任何 SNMP 通知。
启用身份验证陷阱	如果选中此选项，则 StorageGRID SNMP 代理会在收到经过不正确身份验证的协议消息时发送身份验证陷阱。

输入团体字符串

如果使用 SNMPv1 或 SNMPv2c，请完成 Community strings 部分。

当管理系统查询 StorageGRID MIB 时，它会发送一个团体字符串。如果团体字符串与此处指定的值之一匹配，则 SNMP 代理将向管理系统发送响应。

步骤

1. 对于*只读社区*，可选择输入一个社区字符串，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"作为团体字符串。如果将此字段留空，SNMP 代理将使用 StorageGRID 系统的网格 ID 作为团体字符串。

   每个社区字符串最多可包含 32 个字符，并且不能包含空格字符。

2. 选择*Add another community string*以添加其他字符串。

   最多允许五个字符串。

创建陷阱目的地

使用"其他配置"部分中的"陷阱目标"选项卡可为 StorageGRID 陷阱或通知消息定义一个或多个目标。启用 SNMP 代理并选择*保存*后，StorageGRID 会在触发警报时向每个定义的目标发送通知。对于受支持的 MIB-II 实体（例如，ifDown 和 coldStart），也会发送标准通知。

步骤

1. 对于*默认陷阱社区*字段，可选择输入要用于 SNMPv1 或 SNMPv2 陷阱目的地的默认社区字符串。

   根据需要，您可以在定义特定陷阱目标时提供不同的（"自定义"）社区字符串。

   Default trap community 最多可包含 32 个字符，不能包含空格字符。

2. 要添加陷阱目的地，请选择 **Create**。
3. 选择此陷阱目标将使用的 SNMP 版本。
4. 为所选版本填写"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	问题描述
类型	必须是 SNMPv1 的陷阱。
主机	用于接收陷阱的 IPv4 或 IPv6 地址或完全限定域名 (FQDN)。
端口	使用 162，这是 SNMP 陷阱的标准端口，除非必须使用其他值。
协议	使用 UDP，这是标准的 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），或为此陷阱目标输入自定义团体字符串。 自定义社区字符串最多可包含 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	问题描述
类型	目的地是否将用于陷阱或通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。
端口	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，这是标准的 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），或为此陷阱目标输入自定义团体字符串。 自定义社区字符串最多可包含 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	问题描述
类型	目的地是否将用于陷阱或通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。

字段	问题描述
端口	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，这是标准的 SNMP 陷阱协议，除非您需要使用 TCP。
USM 用户	将用于身份验证的 USM 用户。 • 如果选择 **Trap**，则仅显示没有权威引擎 ID 的 USM 用户。 • 如果选择 **Inform**，则仅显示具有权威引擎 ID 的 USM 用户。 • 如果未显示用户： i. 创建并保存陷阱目标。 ii. 转到创建 USM 用户并创建用户。 iii. 返回"陷阱目的地"选项卡，从表中选择已保存的目的地，然后选择*编辑*。 iv. 选择用户。

5. 选择 **Create**。

   陷阱目标已创建并添加到表中。

创建代理地址

（可选）使用"其他配置"部分的"代理地址"选项卡指定一个或多个"侦听地址"。这些是 SNMP 代理可以接收查询的 StorageGRID 地址。

如果不配置代理地址，则默认侦听地址为所有 StorageGRID 网络上的 UDP 端口 161。

步骤

1. 选择 **Create**。
2. 输入以下信息。

字段	问题描述
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	问题描述
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：如果您将客户端网络用于不安全的数据，并为客户端网络创建代理地址，请注意 SNMP 流量也将是不安全的。
端口	（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都允许访问这些端口。

3. 选择 **Create**。

   已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。

> 对于 SNMPv3 *trap* 目标，建议为每个管理节点创建一个 USM 用户。如果每个管理节点都没有 USM 用户，则当主管理节点关闭时，您的管理系统可能会停止接收通知。

> SNMPv3 *inform* 目标必须具有带引擎 ID 的用户。SNMPv3 *trap* 目标不能有带引擎 ID 的用户。

如果仅使用 SNMPv1 或 SNMPv2c，则这些步骤不适用。

步骤

1. 选择 **Create**。
2. 输入以下信息。

字段	问题描述
用户名	此 USM 用户的唯一名称。 用户名最多可包含 32 个字符，并且不能包含空白字符。创建用户后无法更改用户名。

字段	问题描述
只读 MIB 访问	如果选中，此用户应具有对 MIB 的只读访问权限。
权威引擎 ID	如果此用户将在通知目标中使用，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 个字节），不带空格。对于将在陷阱目标中选择用于 informs 的 USM 用户，此值是必需的。对于将在陷阱目标中选择用于 traps 的 USM 用户，不允许使用此值。 注意：如果您选择了*只读 MIB 访问权限*，则不会显示此字段，因为具有只读 MIB 访问权限的 USM 用户无法拥有引擎 ID。
安全级别	USM 用户的安全级别： • **authPriv**：此用户使用身份验证和隐私（加密）进行通信。您必须指定身份验证协议和密码以及隐私协议和密码。 • **authNoPriv**：此用户通过身份验证进行通信，无需隐私（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，这是唯一受支持的协议（HMAC-SHA-96）。
密码	此用户将用于身份验证的密码。
隐私协议	仅当您选择 **authPriv** 时才会显示，并始终设置为 AES，这是唯一受支持的隐私协议。
密码	仅在您选择 **authPriv** 时显示。此用户将用于隐私的密码。

3. 选择 **Create**。

   已创建USM用户并将其添加到表中。

4. 完成 SNMP 代理配置后，选择*保存*。

   新的SNMP代理配置变为活动状态。

更新 **StorageGRID SNMP** 代理

您可以禁用 SNMP 通知、更新社区字符串或添加或删除代理地址、USM 用户和陷阱目标。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

有关 SNMP 代理页上每个字段的详细信息，请参阅 "配置 SNMP 代理"。您必须在页面底部选择 **Save**，以提交您对每个选项卡所做的任何更改。

步骤

1. 选择*配置* > 监控 > **SNMP**代理。

   此时将显示 SNMP 代理页面。

2. 要禁用所有网格节点上的 SNMP 代理，请清除*启用 SNMP*复选框，然后选择*保存*。

   如果重新启用 SNMP 代理，则保留所有以前的 SNMP 配置设置。

3. （可选）更新基本配置部分中的信息：

   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消息。

      清除此复选框后，SNMP 代理将支持只读 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 代理在接收到经过不正确身份验证的协议消息时是否发送身份验证陷阱。

4. 如果您使用 SNMPv1 或 SNMPv2c，则可以在社区字符串部分更新或添加*只读社区*。

5. 要更新陷阱目标，请在"其他配置"部分中选择"陷阱目标"选项卡。

   使用此选项卡可定义 StorageGRID 陷阱或通知消息的一个或多个目标。启用 SNMP 代理并选择*保存*后，StorageGRID 会在触发警报时向每个定义的目标发送通知。对于受支持的 MIB-II 实体（例如 ifDown 和 coldStart），也会发送标准通知。

   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，则必须首先确保任何现有的陷阱目标使用自定义团体字符串。

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

6. 要更新代理地址，请在"其他配置"部分中选择"代理地址"选项卡。

   使用此选项卡可指定一个或多个"监听地址"。这些是 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"。

   - 要添加代理地址，请选择*创建*。
   - 要编辑代理地址，请选择单选按钮，然后选择 **Edit**。
   - 要删除代理地址，请选择单选按钮，然后选择*删除*。

- 要提交更改，请选择页面底部的*保存*。

7. 要更新 USM 用户，请在其他配置部分中选择 USM 用户选项卡。

   使用此选项卡可定义有权查询 MIB 或接收陷阱和通知的 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*创建*。
   - 要编辑 USM 用户，请选择单选按钮，然后选择*编辑*。

     无法更改现有 USM 用户的用户名。如果需要更改用户名，则必须删除该用户并创建一个新用户。

     > 如果您添加或删除用户的权威引擎 ID，并且该用户当前被选为目标，则必须编辑或删除目标。否则，保存 SNMP 代理配置时会出现验证错误。

   - 要删除 USM 用户，请选择单选按钮，然后选择*删除*。

     > 如果您删除的用户当前被选为陷阱目标，则必须编辑或删除目标。否则，保存 SNMP 代理配置时会出现验证错误。

   - 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*保存*。

访问 **StorageGRID MIB** 文件

MIB 文件包含有关网格中节点的托管资源和服务属性的定义和信息。您可以访问定义 StorageGRID 对象和通知的 MIB 文件。这些文件对于监控网格非常有用。

有关 SNMP 和 MIB 文件的详细信息，请参见"使用 SNMP 监控"。

访问 **MIB** 文件

按照下面的步骤访问 MIB 文件。

步骤

1. 选择*配置* > 监控 > **SNMP**代理。
2. 在 SNMP 代理页上，选择要下载的文件：
   - **NETAPP-STORAGEGRID-MIB.txt**：定义在所有管理节点上可访问的警报表和通知（陷阱）。
   - **ES-NETAPP-06-MIB.mib**：定义基于 E-Series 设备的对象和通知。
   - **MIB_1_10.zip**：定义具有 BMC 接口的设备的对象和通知。

     > 您还可以访问任何 StorageGRID 节点上以下位置的 MIB 文件：`/usr/share/snmp/mibs`

3. 从 MIB 文件中提取 StorageGRID OID：

a. 获取 StorageGRID MIB 根的 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）

b. 在整个树中对 StorageGRID OID 执行 Grep 操作（使用 `paste`连接行）：

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

该 `snmptranslate`命令有许多选项，可用于探索 MIB。此命令可在任何 StorageGRID 节点上使用。

MIB 文件内容

所有对象都在 StorageGRID OID 下。

对象名称	对象**ID (OID)**	问题描述
		NetApp StorageGRID 实体的 MIB 模块。

MIB 对象

对象名称	对象**ID (OID)**	类型	访问	**MIB** 模块	问题描述
activeAlertCount		Integer32	只读	NETAPP-STORAGEGRID-MIB	activeAlertTable 中的活动警报数。
activeAlertTable		ActiveAlertEntry 的序列	不可访问	NETAPP-STORAGEGRID-MIB	StorageGRID 中活动警报的表格。
activeAlertEntry		序列	不可访问	NETAPP-STORAGEGRID-MIB	单个 StorageGRID 警报，按警报 ID 编制索引。
activeAlertId		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	警报的 ID。仅在当前活动警报集中唯一。
activeAlertName		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	警报的名称。
activeAlertInstance		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	生成警报的实体的名称，通常是节点名称。

对象名称	对象ID (OID)	类型	访问	MIB 模块	问题描述
activeAlertSeverity		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	警报的严重程度。
activeAlertStartTime		日期和时间	只读	NETAPP-STORAGEGRID-MIB	触发警报的时间。

收集其他 StorageGRID 数据

监控 StorageGRID 中的 PUT 和 GET 性能

您可以监控某些操作（如对象存储和检索）的性能，以帮助识别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 命令。使用这些方法，您可以独立于 StorageGRID 外部因素（例如客户端应用程序问题或外部网络问题）来评估性能。

执行 PUT 和 GET 操作测试时，请使用以下指南：

- 使用与通常载入网格的对象大小相当的对象大小。
- 对本地和远程站点执行操作。

"审核日志" 中的消息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 TIME 属性的值。您还可以在以下 S3 操作的审核消息中找到 TIME 属性：DELETE、GET、HEAD、Metadata Updated、POST、PUT

在分析结果时，请查看满足请求所需的平均时间，以及您可以实现的总体吞吐量。定期重复相同的测试并记录结果，以便识别可能需要调查的趋势。

- 您可以 "从 github 下载 S3tester"。

监控 StorageGRID 中的对象验证操作

StorageGRID 系统可以验证存储节点上对象数据的完整性，检查损坏和丢失的对象。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。

关于此任务

两个 "验证流程" 协同工作以确保数据完整性：

- *后台验证*自动运行，持续检查对象数据的正确性。

  后台验证会自动并持续检查所有存储节点，以确定是否存在已复制和擦除编码的对象数据的损坏副本。如果

发现问题，StorageGRID 系统会自动尝试从存储在系统其他位置的副本中替换损坏的对象数据。后台验证不对云存储池中的对象运行。

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。

- *对象存在性检查*可以由用户触发，以更快地验证对象数据的存在性（尽管不是正确性）。

  对象存在性检查验证对象和纠删码片段的所有预期复制副本是否存在于存储节点上。对象存在性检查提供了一种验证存储设备完整性的方法，特别是在最近的硬件问题可能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性检查的结果。立即调查任何损坏或丢失的对象数据实例，以确定根本原因。

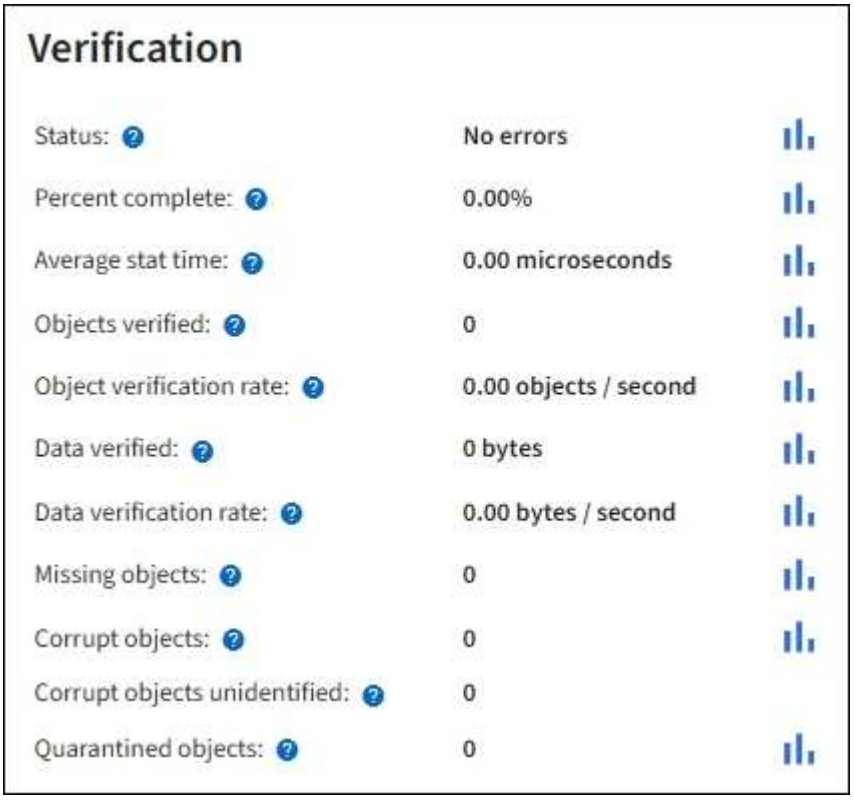
步骤

1. 请查看后台验证结果：

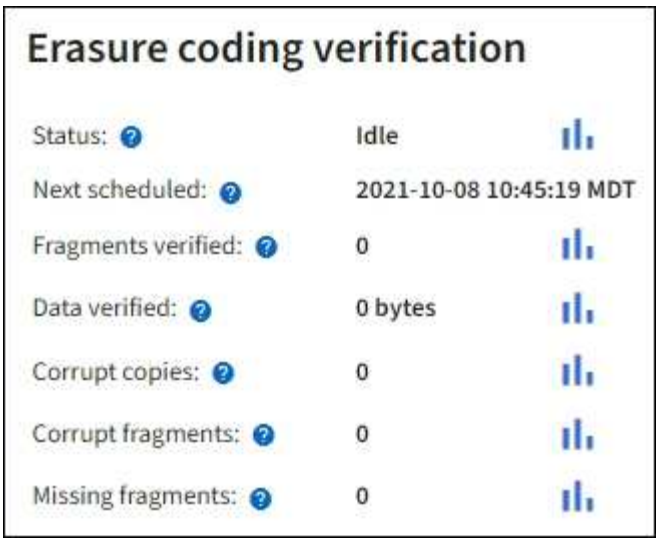
   a. 选择*节点* > 存储节点 > 对象。

   b. 检查验证结果：

      - 要检查复制对象数据验证，请查看验证部分中的属性。

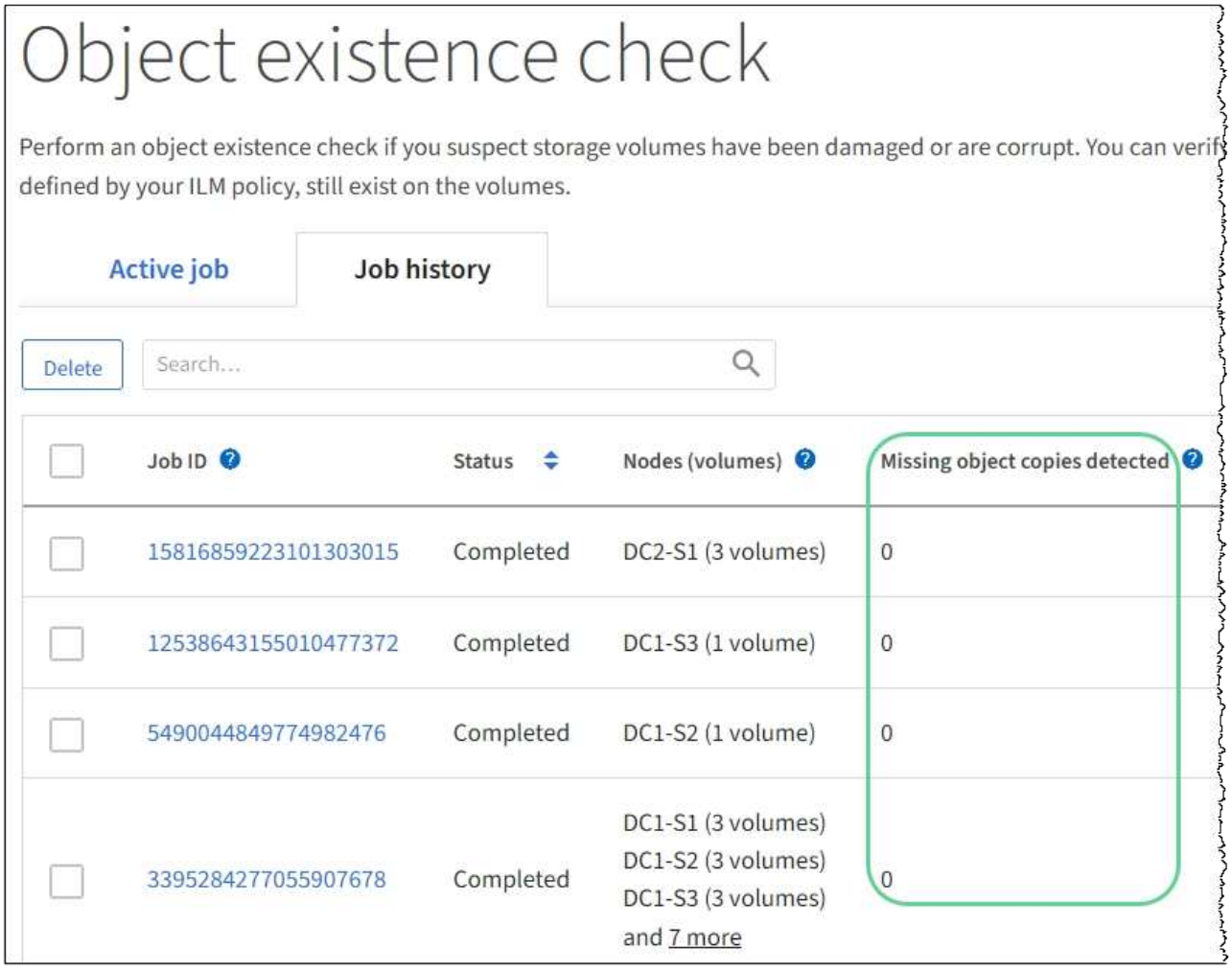


      - 要检查擦除编码片段验证，请选择*存储节点* > **ILM**，然后查看擦除编码验证部分中的属性。



选择属性名称旁边的问号 (?) 以显示帮助文本。

2. 查看对象存在性检查作业的结果：
   a. 选择*维护* > 对象存在性检查 > 作业历史记录。
   b. 扫描检测到的缺失对象副本列。如果任何作业导致 100 个或更多对象副本丢失，并且已触发*可能丢失的对象*警报，请联系技术支持。



查看 **StorageGRID** 审核消息

审核消息可以帮助您更好地了解 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。

在正常系统运行期间，所有 StorageGRID 服务都会生成以下审核消息：

- 系统审核消息涉及审核系统本身、网格节点状态、全系统任务活动和服务备份操作。
- 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 客户端应用程序请求创建、修改或检索对象时，将记录客户端读取和写入审核消息。
- 管理审核消息用于记录用户对 Management API 的请求。

每个管理节点都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）以及前几天的压缩审核日志。网格中的每个节点还存储在该节点上生成的审核信息的副本。

您可以直接从管理节点的命令行访问审核日志文件。

默认情况下，StorageGRID 可以发送审核信息，您也可以更改目标：

- StorageGRID 默认为本地节点审核目标。
- 网格管理器和租户管理器审核日志条目可能会发送到存储节点。
- 也可以更改审核日志的目标，并将审核信息发送到外部 syslog 服务器。配置外部 syslog 服务器时，将继续生成和存储审核记录的本地日志。
- "了解有关配置日志管理的信息"。

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，请参阅 "查看审核日志"。

收集 **StorageGRID** 日志文件和系统数据

您可以检索 StorageGRID 日志文件和系统数据，包括配置数据，并将其发送给技术支持。

开始之前

- 您使用 "支持的 Web 浏览器" 登录到任何管理节点上的网格管理器。
- 您有 "特定访问权限"。
- 您有配置密码短语。

关于此任务

使用 Grid Manager 收集"日志文件"您选择的时间段内任何网格节点的系统数据和配置数据。数据将被收集并存档到 `.tar.gz`文件中，您可以将其下载到本地计算机或发送给技术支持。

也可以更改审核日志的目标，并将审核信息发送到外部 syslog 服务器。配置外部 syslog 服务器时，将继续生成和存储审核记录的本地日志。请参阅 "配置日志管理和外部 syslog 服务器"。

步骤

1. 选择 **Support** > **Tools** > **Log collection**。将显示一个节点表。

2. 选择要为其收集日志文件的网格节点。

   您可以按节点名称、站点和节点类型排序。站点和节点类型列包含用于按单个站点和节点类型进行选择的筛选器。

3. 选择 **Continue**。
4. 选择要包含在日志文件中的数据的日期和时间范围。

   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，日志存档可能会变得太大而无法存储在节点上，或者太大而无法由管理节点收集以供下载。如果任何一种情况发生，请使用较小的数据集重新启动日志收集。

5. 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子集。
   - 审核日志：包含正常系统运行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** 数据库：来自所有节点上服务的时间序列指标。
6. （可选）使用*备注*文本框输入有关正在收集的日志文件的备注。

   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。您的注释将与有关日志文件收集的其他信息一起添加到名为 `info.txt`的文件中。该 `info.txt`文件保存在日志文件存档包中。

7. 在*配置密码*文本框中，输入 StorageGRID 系统的配置密码。
8. 选择*收集日志*。

   您可以使用日志收集页面监视每个网格节点的日志文件收集进度。

   如果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。

9. 如果日志收集失败：
   - 如果出现"日志收集失败"消息，您可以重试日志收集或在不重试的情况下完成会话。
   - 如果出现"日志收集部分失败"消息，您可以重试日志收集、完成会话、下载部分日志文件或将部分日志文件发送到 AutoSupport。
10. 日志文件收集完成后：
    - 选择*下载*以下载 `.tar.gz`文件。
    - 选择*发送到 AutoSupport*将 `.tar.gz`文件发送给技术支持。

      该 `.tar.gz`文件包含来自日志收集成功的所有网格节点的所有日志文件。组合的 `.tar.gz`文件包含每个网格节点的一个日志文件存档。

    AutoSupport 包的主题是 `USER_TRIGGERED_SUPPORT_BUNDLE`。

11. 选择 **Finish**。

    选择 **Finish** 时， `.tar.gz`文件将被删除。请务必先下载或发送文件。

手动触发 **StorageGRID AutoSupport** 包

为了帮助技术支持解决 StorageGRID 系统的问题，您可以手动触发发送 AutoSupport 软件包。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您具有根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 尝试将 AutoSupport 包发送到 NetApp 支持站点。如果尝试成功，**Results** （结果）选项卡上的 **Most Recent Result** （最近结果）和 **Last Successful Time** （上次成功时间）值将更新。如果出现问题，**Most Recent Result** 值将更新为"Failed"，StorageGRID 不会再次尝试发送 AutoSupport 包。

3. 1 分钟后，请在浏览器中刷新 AutoSupport 页面以访问最新结果。

此外，您可以"收集更广泛的日志文件和系统数据"并将它们发送到 NetApp 支持站点。

查看 **StorageGRID** 支持指标

解决问题时，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

- 必须使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

关于此任务

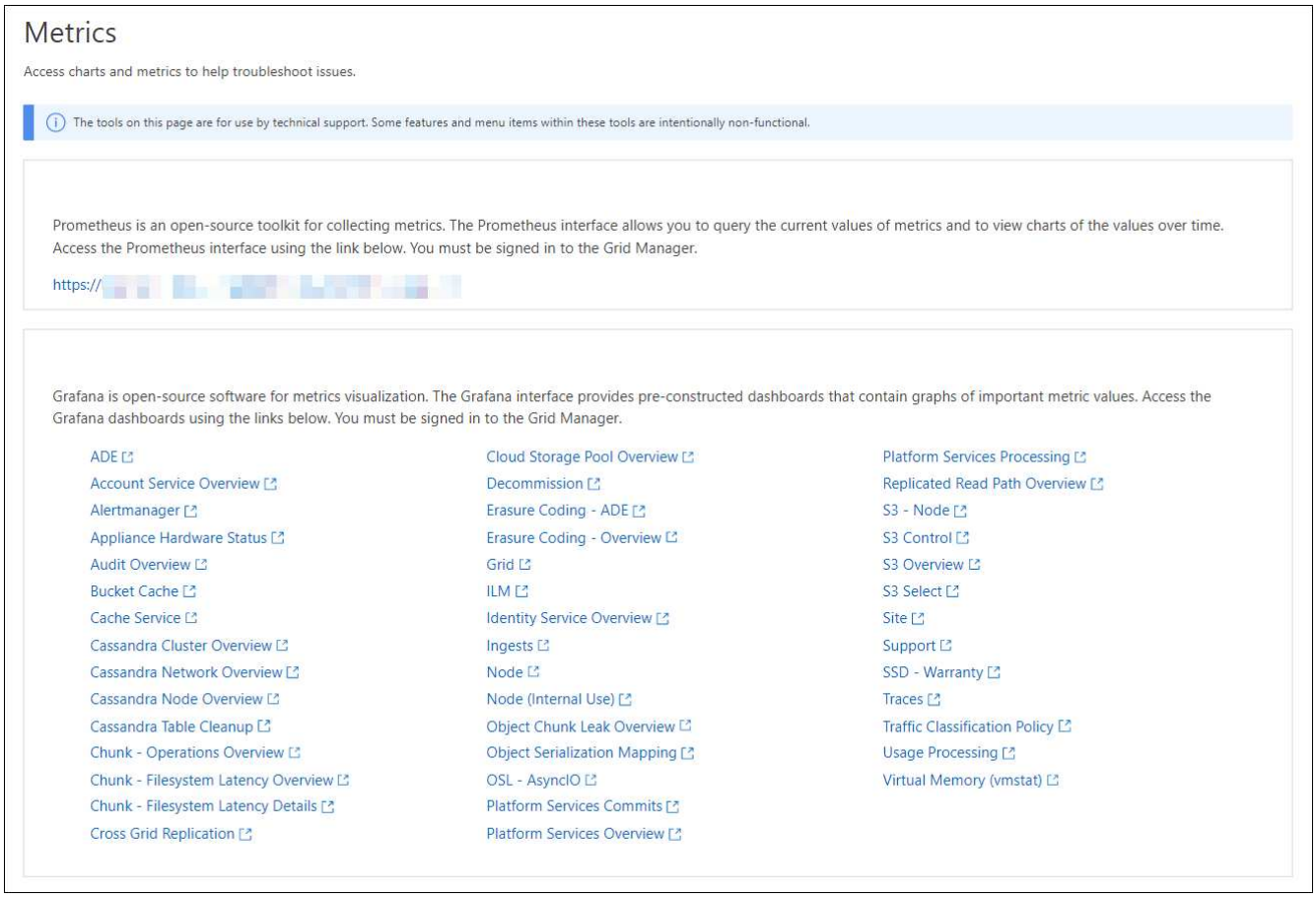
"指标"页面允许您访问 Prometheus 和 Grafana 用户界面。Prometheus 是用于收集指标的开源软件。Grafana 是用于指标可视化的开源软件。

"指标"页面上提供的工具仅供技术支持人员使用。这些工具中的某些功能和菜单项故意无法正常使用，可能会发生变化。查看 "常用的 Prometheus 指标" 的列表。

步骤

1. 根据技术支持的指示，选择*Support* > **Tools** > **Metrics**。

   此处显示了"指标"页面的示例：



2. 要查询 StorageGRID 指标的当前值并查看值随时间变化的图形，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，并随时间绘制 StorageGRID 指标的图形。

   > 名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间如有更改，恕不另行通知。

3. 要访问包含 StorageGRID 指标随时间变化图表的预构建仪表板，请单击 Grafana 部分中的链接。

   此时将显示您选择的链接的 Grafana 界面。

更改 **StorageGRID** 中的 **I/O** 优先级

输入/输出 (I/O) 优先级允许您更改网格上 I/O 操作的相对优先级。

默认情况下，客户端 PUT 和 GET I/O 流量比后台活动（如清除擦除编码（EC）数据和 EC 修复）具有最高优先级。通过提高清除擦除编码（EC）数据和 EC 修复活动的优先级，这些任务可能会更快地完成。I/O 优先级更改的有效性受客户端请求率、网络流量波动和其他正在进行的网络任务的影响。

开始之前

- 查看 I/O 优先级页面，以确定哪些选项可能会影响您的网格。
- 评估正在进行的客户端流量是否可以安全地处理更长的等待时间或客户端超时。
- 准备好监控优先级变更的效果，并在必要时进行调整。这些更改的实施速度很快，但其效果可能需要数小时才能显现。

步骤

1. 选择*支持* > **I/O** 优先级。

2. （可选）更改 EC 清除和修复优先级，以及用于清除 EC 数据的后台操作的默认值。

   对具有基于 RAID 的节点的网格，使用默认的低 EC 清除和修复优先级。

3. 选择 **Save**。
4. 监控"指标"以评估优先级更改的效果。

在 **StorageGRID** 中运行诊断

解决问题时，您可以与技术支持人员一起对 StorageGRID 系统运行诊断并查看结果。

- "查看支持指标"
- "常用 Prometheus 指标"

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

关于此任务

"诊断"页面对网格的当前状态执行一组诊断检查。每个诊断检查可以采用以下三种状态之一：

- **Normal**：所有值都在正常范围内。
- **Attention**：一个或多个值超出正常范围。
- **Caution**：一个或多个值明显超出正常范围。

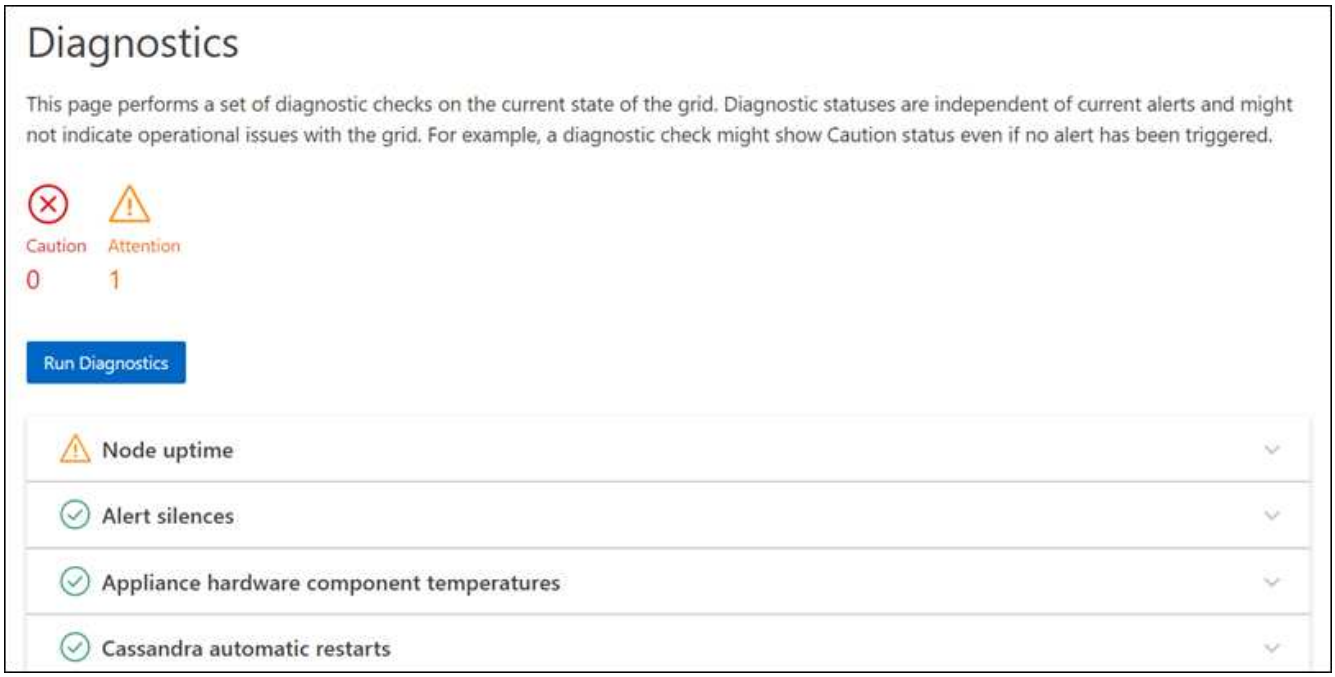
诊断状态独立于当前警报，可能不会指示网格的操作问题。例如，即使未触发任何警报，诊断检查也可能显示"警告"状态。

步骤

1. 选择*支持* > 工具 > 诊断。

   此时将显示"诊断"页面，并列出每次诊断检查的结果。结果按严重程度排序（警告、注意，然后是正常）。在每个严重程度内，结果按字母顺序排序。

   在此示例中，一个诊断具有"注意"状态，三个诊断具有"正常"状态。



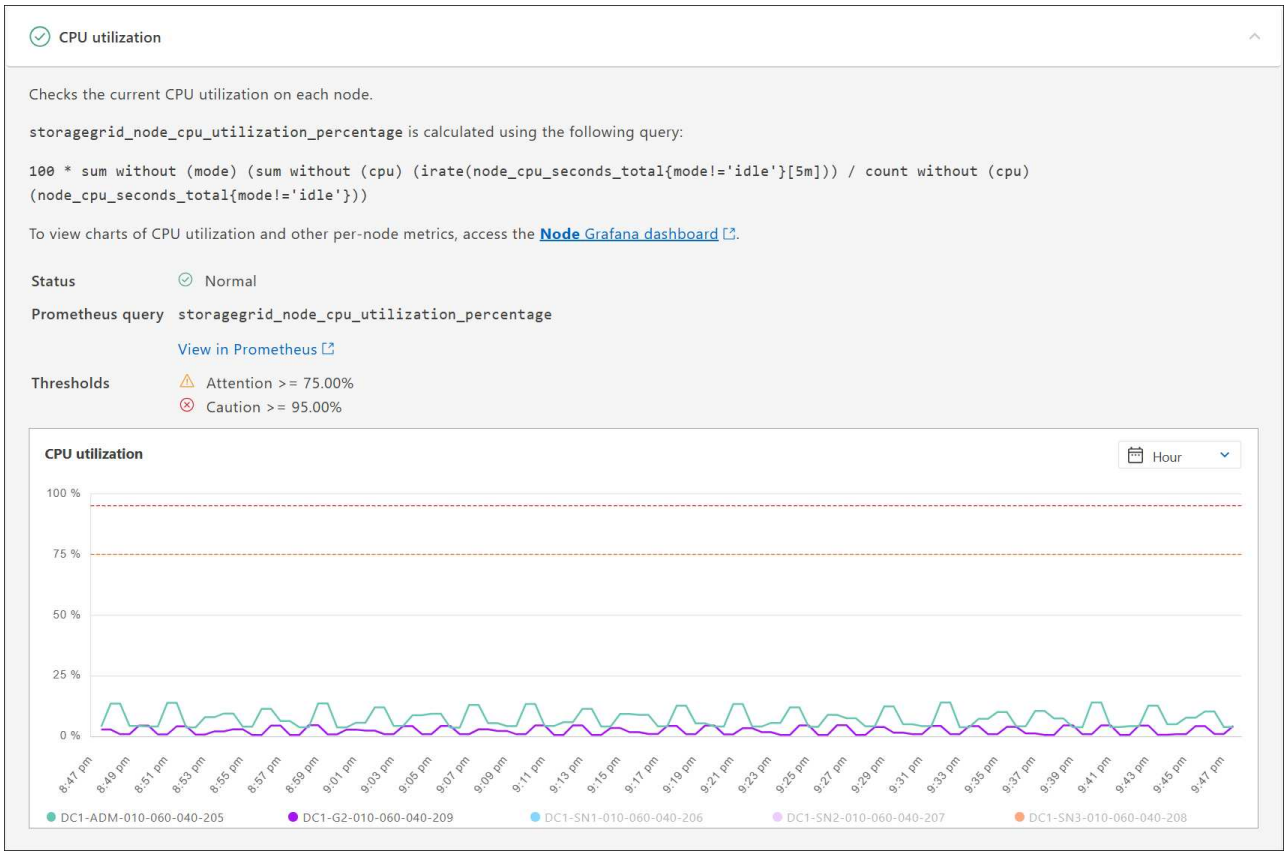
2. 要了解有关特定诊断的更多信息，请单击该行中的任意位置。

   此时将显示有关诊断及其当前结果的详细信息。此处列出了以下详细信息：

   - 状态：此诊断的当前状态：正常、注意或警告。
   - **Prometheus query**：如果用于诊断，则用于生成状态值的 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定义系统定义的阈值。（并非所有诊断都使用阈值。）

     您无法更改这些阈值。

   - 状态值：显示整个 StorageGRID 系统的状态和诊断值的图形和表格（屏幕截图中未显示表格）。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 Attention 和 Caution 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，请选择 **Grafana dashboard**。

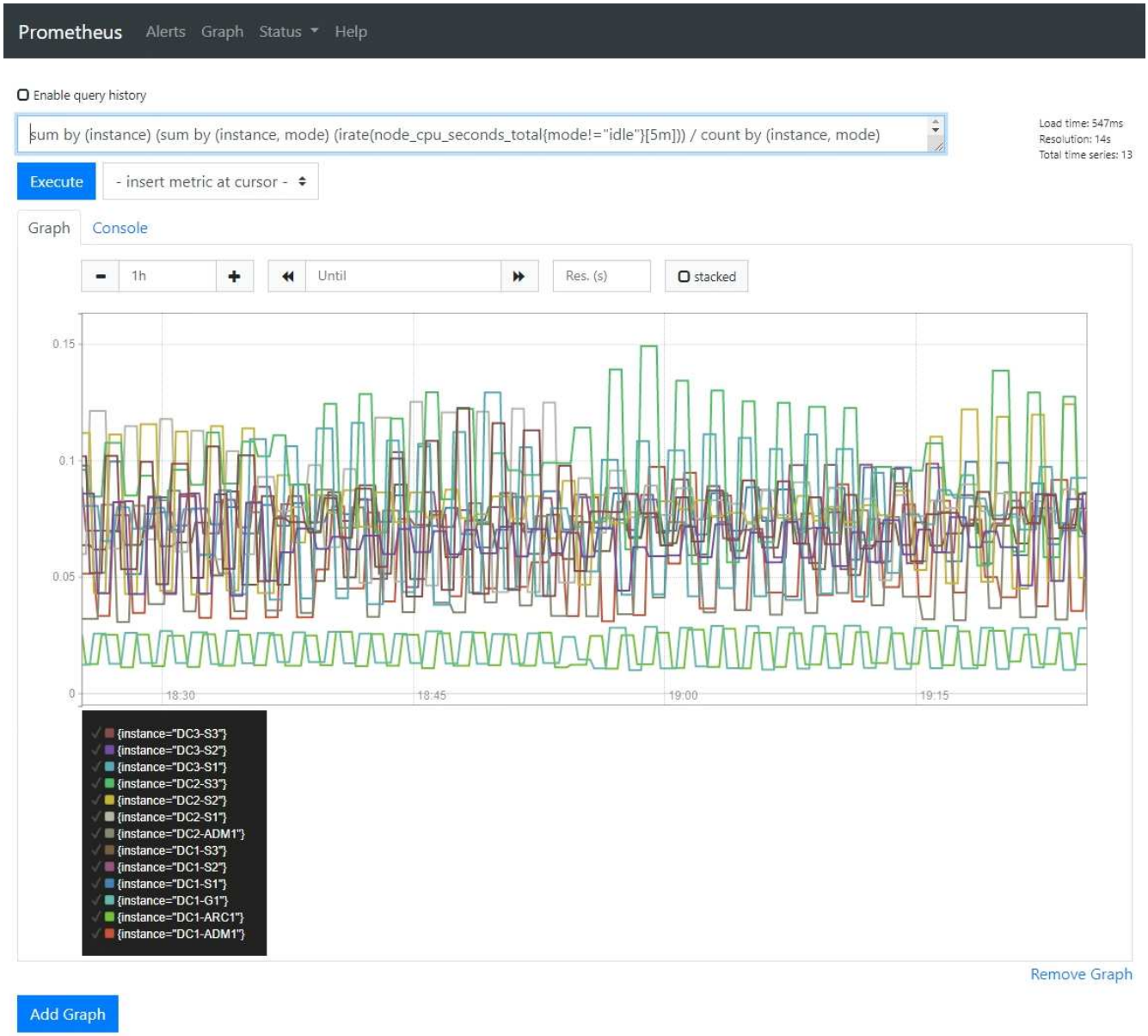
   并非所有诊断都显示此链接。

   此时将显示相关的 Grafana 控制面板。在此示例中，Node dashboard（节点仪表板）显示此节点随时间的 CPU 利用率以及该节点的其他 Grafana 图表。

   您还可以从*支持* > 工具 > *指标*页面的 Grafana 部分访问预构建的 Grafana 仪表板。

4. 可选：要查看 Prometheus 表达式随时间变化的图表，请单击 **View in Prometheus**。

   将显示诊断中使用的表达式的 Prometheus 图。



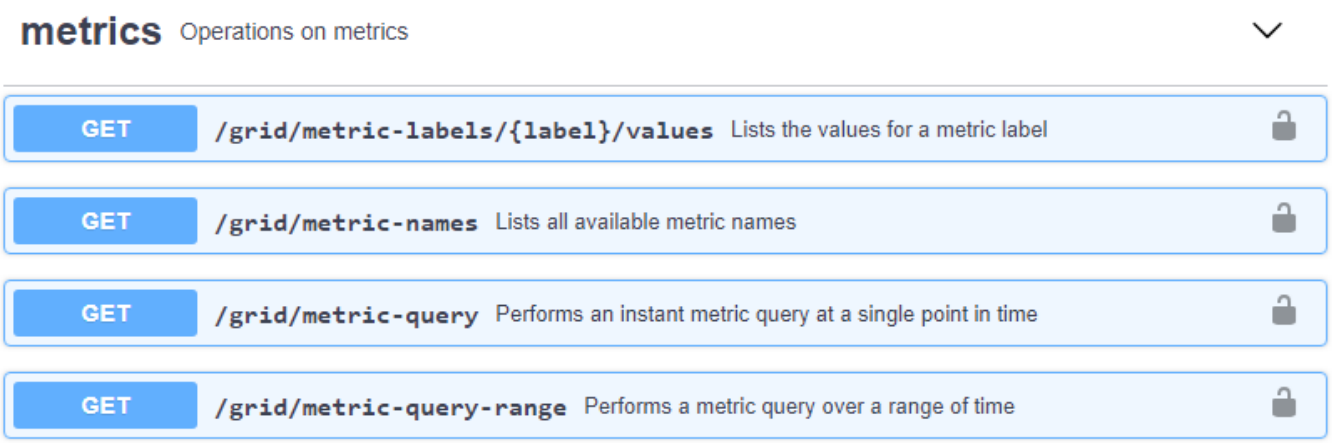
为 **StorageGRID** 创建自定义监控应用程序

您可以使用网格管理 API 中提供的 StorageGRID 指标构建自定义监控应用程序和仪表板。

如果要监视未显示在网格管理器现有页面上的指标，或者如果要为 StorageGRID 创建自定义信息板，则可以使用网格管理 API 查询 StorageGRID 指标。

您还可以使用外部监控工具（如 Grafana）直接访问 Prometheus 指标。使用外部工具需要上传或生成管理客户端证书，以允许 StorageGRID 对该工具进行身份验证以确保安全。请参阅 "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 Grid Manager。在页面顶端，选择帮助图标，然后选择 **API documentation** > **metrics**。



有关如何实现自定义监控应用程序的详细信息不在本文档的讨论范围之内。

StorageGRID 系统故障排除

对 StorageGRID 系统进行故障排除

如果在使用 StorageGRID 系统时遇到问题，请参阅本节中的提示和指南，以获取有关确定和解决此问题的帮助。

通常，您可以自行解决问题；但是，您可能需要将某些问题上报给技术支持。

定义问题

解决问题的第一步是清晰地定义问题。

下表提供了为定义问题而可能收集的信息类型的示例：

问题	响应示例
StorageGRID 系统在做什么或不做什么？其症状是什么？	客户端应用程序报告无法将对象接收到 StorageGRID。
问题是什么时候开始的？	对象摄取于2020年1月8日约14:50首次被拒绝。
您最初是如何注意到这个问题的？	由客户端应用程序通知。还收到了警报电子邮件通知。
问题是始终如一地发生，还是只是偶尔发生？	问题仍然存在。
如果此问题经常发生，导致其发生的步骤是什么	每次客户端尝试摄取对象时都会出现问题。
如果问题间歇性发生，何时发生？记录您所知的每次事件发生的时间。	问题不是间歇性的。

问题	响应示例
您以前见过这个问题吗？您过去有多少次遇到过这个问题？	这是我第一次看到此问题。

评估风险和对系统的影响

定义问题后，请评估其对 StorageGRID 系统的风险和影响。例如，存在关键警报并不一定意味着系统未能提供核心服务。

下表总结了示例问题对系统运行的影响：

问题	响应示例
StorageGRID 系统可以摄取内容吗？	目标卷
客户端应用程序可以检索内容吗？	某些对象可以检索，而其他对象则无法检索。
数据是否存在风险？	目标卷
开展业务的能力是否受到严重影响？	是的，因为客户端应用程序无法将对象存储到 StorageGRID 系统，并且无法一致地检索数据。

收集数据

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

要收集的数据类型	为何收集此数据	AutoSupport
创建最近更改的时间表	对 StorageGRID 系统、其配置或环境的更改可能会导致新的行为。	• 创建最近更改的时间表
查看警报	通过提供可能导致问题的底层问题的重要线索，警报可以帮助您快速确定问题的根本原因。 查看当前警报列表，以查看 StorageGRID 是否已为您确定了问题的根本原因。 查看过去触发的提醒，获取更多见解。	• "${post_edited_translations.segment}"
建立基线	收集有关各种操作值的正常水平的信息。这些基线值以及与这些基线的偏差可以提供有价值的线索。	• 建立基线
执行摄取和检索测试	要对接收和检索的性能问题进行故障排除，请使用工作站存储和检索对象。将结果与使用客户端应用程序时看到的结果进行比较。	• "监控 PUT 和 GET 性能"

要收集的数据类型	为何收集此数据	AutoSupport
查看审核消息	查看审核消息以详细跟踪 StorageGRID 操作。审核消息中的详细信息对于排除许多类型的问题（包括性能问题）非常有用。	• "查看审核消息"
检查对象位置和存储完整性	如果遇到存储问题，请验证对象是否放置在预期的位置。检查存储节点上对象数据的完整性。	• "监控对象验证操作" • "确认对象数据位置" • "验证对象完整性"
收集数据以获得技术支持	技术支持可能会要求您收集数据或查看特定信息以帮助解决问题。	• "收集日志文件和系统数据" • "手动触发 AutoSupport 包" • "查看支持指标"

创建最近更改的时间表

当出现问题时，您应该考虑最近发生了什么变化以及何时发生这些变化。

- 对 StorageGRID 系统、其配置或环境的更改可能会导致新的行为。
- 变更时间线可以帮助您确定哪些变更可能是导致问题的原因，以及每个变更可能对其发展产生的影响。

创建系统最近更改的表格，其中包括有关每次更改发生时间的信息以及有关更改的任何相关详细信息，例如有关更改进行期间发生的其他情况的信息：

变更时间	变更类型	详细信息
例如： • 您何时开始节点恢复？ • 软件升级何时完成？ • 您是否打断了这个过程？	发生了什么？您做了什么？	记录有关更改的任何相关详细信息。例如： • 网络更改的详细信息。 • 安装了哪个修补程序。 • 客户端工作负载如何发生变化。 请务必注意是否同时发生多个变更。例如，此更改是否在升级过程中进行？

近期重大变化示例

以下是一些潜在重大变化的示例：

- StorageGRID 系统最近是否安装、扩展或恢复？
- 系统最近是否已升级？是否已应用修补程序？
- 最近是否维修或更换过任何硬件？
- 是否已更新 ILM 策略？

- 客户工作负载是否发生了变化？
- 客户端应用程序或其行为是否已更改？
- 您是否更改了负载平衡器，或者添加或删除了管理节点或网关节点的高可用性组？
- 是否已开始执行任何可能需要很长时间才能完成的任务？示例包括：
  - 发生故障的存储节点的恢复
  - 存储节点退役
- 是否对用户身份验证进行了任何更改，例如添加租户或更改 LDAP 配置？
- 正在执行数据迁移吗？
- 最近是否启用或更改了平台服务？
- 最近是否启用了合规性？
- 是否已添加或删除云存储池？
- 是否对存储压缩或加密进行了任何更改？
- 网络基础设施是否有任何变化？例如，VLAN、路由器或 DNS。
- 是否对 NTP 源进行了任何更改？
- 是否对网格、管理或客户端网络接口进行了任何更改？
- 对 StorageGRID 系统或其环境是否进行了任何其他更改？

建立基线

您可以通过记录各种操作值的正常水平来为系统建立基线。未来，您可以将当前值与这些基线进行比较，以帮助检测和解决异常值。

属性	值	如何获取
平均存储消耗	每天消耗的 GB 每天消耗百分比	转到 Grid Manager。在"节点"页面上，选择整个网格或站点，然后转到"存储"选项卡。 在"使用的存储 - 对象数据"图表上，找到线条相当稳定的时间段。将光标放在图表上，以估计每天消耗的存储空间 您可以为整个系统或特定数据中心收集此信息。
平均元数据使用量	每天消耗的 GB 每天消耗百分比	转到 Grid Manager。在"节点"页面上，选择整个网格或站点，然后转到"存储"选项卡。 在"使用的存储 - 对象元数据"图表上，找到线条相当稳定的时间段。将光标放在图表上，以估计每天消耗的元数据存储量 您可以为整个系统或特定数据中心收集此信息。

属性	值	如何获取
S3 操作速率	操作/秒	在网格管理器仪表板上，选择 **Performance** > **S3 operations for Storage Nodes**。 要查看特定站点或节点的摄取和检索速率和计数，请选择 节点 > 站点或存储节点 > 对象。将光标放在 S3 摄取和检索图表上。
ILM评估率	对象/秒	在节点页面中，选择 ***grid*** > **ILM**。 在 ILM 队列图表中，找到线路相当稳定的时期。将光标放在图表上，以估计系统*评估率*的基线值。
ILM 扫描率	对象/秒	选择*节点* > 网格 > **ILM**。 在 ILM 队列图表中，找到线路相当稳定的时期。将光标放在图表上，以估计系统*扫描速率*的基线值。
从客户端操作排队的对象	对象/秒	选择*节点* > 网格 > **ILM**。 在 ILM 队列图表中，找到线路相当稳定的时期。将光标放在图表上，以估计系统的 **Objects queued (from client operations)** 的基线值。
平均查询延迟	毫秒	选择 **Nodes** > ***Storage Node*** > **Objects**。在"查询"表中，查看 Average Latency 的值。

分析数据

使用您收集的信息来确定问题的原因和潜在的解决方案。

分析取决于问题，但一般来说：

- 使用警报定位故障点和瓶颈。
- 使用警报历史记录和图表重建问题历史记录。
- 使用图表查找异常，并将问题情况与正常操作进行比较。

升级信息核对清单

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

✔	个项目	说明
	问题陈述	问题症状是什么？问题是什么时候开始的？这种情况是持续发生还是间歇性发生？如果是间歇性的，发生了几次？ 定义问题
	影响评估	问题的严重程度如何？对客户端应用程序有什么影响？ • 客户端之前是否已成功连接？ • 客户端是否可以摄取、检索和删除数据？
	StorageGRID 系统 ID	选择*维护* > 系统 > 许可证。StorageGRID 系统 ID 显示为当前许可证的一部分。
	软件版本	从网格管理器顶端，选择帮助图标并选择*About*以查看 StorageGRID 版本。
	自定义	总结 StorageGRID 系统的配置方式。例如，列出以下内容： • 网格是否使用存储压缩、存储加密或合规性？ • ILM 是否生成复制或纠删码对象？ILM 是否确保站点冗余？ILM 规则是否使用平衡、严格或双提交载入行为？
	日志文件和系统数据	收集系统的日志文件和系统数据。选择*支持* > 工具 > 日志收集。 您可以收集整个网格或选定节点的日志。 如果仅收集选定节点的日志，请确保至少包含一个具有 ADC 服务的存储节点。安装在站点的前三个存储节点包括 ADC 服务。
	基线信息	收集有关摄取操作、检索操作和存储消耗的基线信息。 建立基线
	最近更改的时间表	创建一个时间线，总结系统或其环境的任何最近更改。 创建最近更改的时间表
	诊断此问题的工作历史记录	如果您已自行采取措施诊断或排除问题，请务必记录您采取的步骤和结果。

对象和存储问题疑难解答

根据问题的不同，您可能需要"确认对象数据存储的位置"。例如，您可能需要验证 ILM 策略是否按预期执行，以及对象数据是否按预期存储。

开始之前

- 您必须有一个对象标识符，该标识符可以是以下之一：
  - **UUID**：对象的通用唯一标识符。请输入全大写的 UUID。
  - **CBID**：对象在 StorageGRID 中的唯一标识符。您可以从审核日志中获取对象的 CBID。输入全大写的 CBID。
  - **S3** 存储桶和对象密钥：当通过 "S3 接口" 接收对象时，客户端应用程序使用存储桶和对象密钥组合来存储和识别对象。

步骤

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

   您可以输入UUID、CBID或S3存储桶/对象密钥。

3. 如果要查找对象的特定版本，请输入版本 ID（可选）。

4. 选择*查找*。

   "对象元数据查找结果" 显示。此页面列出以下类型的信息：

   - 系统元数据，包括对象 ID (UUID)、版本 ID（可选）、对象名称、容器名称、租户帐户名称或 ID、对象的逻辑大小、对象首次创建的日期和时间以及对象上次修改的日期和时间。
   - 与对象关联的任何自定义用户元数据键值对。
   - 对于 S3 对象，与对象关联的任何对象标记键值对。
   - 对于复制的对象副本，每个副本的当前存储位置。
   - 对于擦除编码的对象副本，每个片段的当前存储位置。
   - 对于云存储池中的对象副本，对象的位置，包括外部存储桶的名称和对象的唯一标识符。
   - 对于分段对象和多部分对象，包括分段标识符和数据大小的对象分段列表。对于超过 100 个段的对象，仅显示前 100 个段。

- 未处理的内部存储格式中的所有对象元数据。此原始元数据包括不保证在各版本之间持续存在的内部系统元数据。

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


了解 **StorageGRID** 中存储卷的对象存储故障

存储节点上的底层存储划分为对象存储。对象存储也称为存储卷。

您可以查看每个存储节点的对象存储信息。选择 **Nodes** > ***Storage Node*** > **Storage**。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

根据故障的性质，存储卷的故障可能会反映在"存储卷警报"中。如果存储卷出现故障，则应修复出现故障的存储卷，以便尽快将存储节点恢复到完整功能。如有必要，您可以转到*配置*选项卡，"将存储节点置于只读状态"以便在准备完全恢复服务器时，StorageGRID 系统可以使用它进行数据检索。

验证 **StorageGRID** 中对象数据的完整性

StorageGRID 系统验证存储节点上对象数据的完整性，检查损坏和丢失的对象。

有两种验证过程：后台验证和对象存在性检查（以前称为前台验证）。它们协同工作以确保数据完整性。后台验证自动运行，并持续检查对象数据的正确性。用户可以触发对象存在性检查，以更快地验证对象的存在性（尽管不是正确性）。

什么是后台验证?

后台验证过程会自动并持续检查存储节点是否存在对象数据的损坏副本，并自动尝试修复发现的任何问题。

后台验证检查复制对象和擦除编码对象的完整性，如下所示：

- 复制对象：如果后台验证过程发现已损坏的复制对象，则损坏的副本将从其位置删除，并在存储节点的其他位置进行隔离。然后，生成并放置一个新的未损坏的副本以满足活动的 ILM 策略。新副本可能不会放置在用于原始副本的存储节点上。

  > 损坏的对象数据将被隔离而不是从系统中删除，因此仍然可以访问。有关访问隔离对象数据的详细信息，请联系技术支持。

- 擦除编码对象：如果后台验证过程检测到擦除编码对象的片段已损坏，StorageGRID 会使用剩余的数据和奇偶校验片段，自动尝试在同一存储节点上重建丢失的片段。如果无法重建损坏的片段，则会尝试检索对象的另一个副本。如果检索成功，则执行 ILM 评估以创建擦除编码对象的替换副本。

  后台验证过程仅检查存储节点上的对象。不会检查云存储池中的对象。对象必须超过四天才符合后台验证的条件。

后台验证以连续速率运行，旨在不干扰正常的系统活动。后台验证无法停止。但是，如果您怀疑存在问题，可以提高后台验证率以更快地验证存储节点的内容。

与后台验证相关的提醒

如果系统检测到无法自动更正的损坏对象（因为损坏会阻止对象被识别），则会触发 **Unidentified corrupt object detected** 警报。

如果后台验证因无法找到另一个副本而无法替换损坏的对象，则会触发 **Objects potentially lost** 警报。

什么是对象存在性检查?

对象存在性检查验证对象和擦除编码片段的所有预期复制副本是否存在于存储节点上。对象存在性检查不会验证对象数据本身（后台验证会执行此操作）；相反，它提供了一种验证存储设备完整性的方法，特别是在最近的硬件问题可能影响数据完整性的情况下。

与自动进行的后台验证不同，您必须手动启动对象存在性检查作业。

对象存在性检查读取存储在 StorageGRID 中的每个对象的元数据，并验证复制的对象副本和纠删码对象片段的存在性。任何缺失的数据将按以下方式处理：

- 复制副本：如果缺少复制对象数据的副本，StorageGRID 会自动尝试从存储在系统其他位置的副本中替换该副本。存储节点通过 ILM 评估运行现有副本，这将确定不再满足此对象的当前 ILM 策略，因为缺少另一个副本。系统将生成一个新副本并进行放置，以满足系统的活动 ILM 策略。此新副本可能不会放置在存储丢失副本的同一位置。
- 擦除编码片段：如果擦除编码对象的片段丢失，StorageGRID 会自动尝试使用剩余片段在同一存储节点上重建丢失的片段。如果无法重建丢失的片段（因为丢失了太多片段），ILM 将尝试查找对象的另一个副本，以生成新的擦除编码片段。

运行对象存在性检查

您每次创建并运行一个对象存在性检查作业。创建作业时，选择要验证的 Storage Nodes 和卷。您还可以选择作业的一致性。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 您已确保要检查的存储节点处于联机状态。选择 **Nodes** 以查看节点表。确保要检查的节点的节点名称旁边没有警报图标。
- 您已确保以下过程*不*在要检查的节点上运行：
  - 网格扩展以添加存储节点
  - 存储节点停用
  - 故障存储卷的恢复
  - 恢复具有故障系统驱动器的存储节点
  - EC 重新平衡
  - 设备节点克隆

这些过程正在进行中，对象存在性检查未提供有用信息。

关于此任务

对象存在检查作业可能需要几天或几周才能完成，具体取决于网格中的对象数量、选定的存储节点和卷以及选定的一致性。一次只能运行一个作业，但可以同时选择多个存储节点和卷。

步骤

1. 选择*维护* > 任务 > 对象存在性检查。
2. 选择*创建作业*。将显示创建对象存在性检查作业向导。
3. 选择包含要验证的卷的节点。要选择所有在线节点，请选中列标题中的 **Node name** 复选框。

   您可以按节点名称或站点进行搜索。

   您不能选择未连接到网格的节点。

4. 选择 **Continue**。
5. 为列表中的每个节点选择一个或多个卷。可以使用存储卷号或节点名称搜索卷。

   要为您选择的每个节点选择所有卷，请选中列标题中的*存储卷*复选框。

6. 选择 **Continue**。
7. 选择作业的一致性。

   一致性决定了用于对象存在性检查的对象元数据的副本数。

   - **Strong-site**：一个站点上的两个元数据副本。
   - **Strong-global**：每个站点两个元数据副本。
   - 所有（默认）：每个站点的所有三个元数据副本。

     有关一致性的详细信息，请参见向导中的说明。

8. 选择 **Continue**。
9. 查看并验证您的选择。您可以选择 **Previous** 转到向导中的上一步来更新您的选择。

   系统将生成并运行对象存在性检查作业，直到出现以下情况之一：

   - 作业已完成。
   - 您暂停或取消作业。您可以恢复已暂停的作业，但无法恢复已取消的作业。
   - 作业停止。*对象存在性检查已停止*警报被触发。遵循为警报指定的纠正措施。
   - 作业失败。*对象存在性检查失败*警报被触发。遵循为此警报指定的纠正措施。
   - 将显示"服务不可用"或"内部服务器错误"消息。一分钟后，刷新此页面以继续监控此作业。

     根据需要，您可以离开"对象存在性检查"页面，然后返回继续监视作业。

10. 作业运行时，查看*活动作业*选项卡并记下检测到的缺失对象副本的值。

    此值表示复制对象和具有一个或多个缺失片段的纠删编码对象的缺失副本总数。

    如果检测到的缺失对象副本数大于 100，则可能是存储节点的存储存在问题。

11. 作业完成后，采取任何其他必要措施：
    - 如果检测到的缺失对象副本为零，则未找到问题。无需执行操作。
    - 如果检测到的缺失对象副本大于零，并且尚未触发 **Objects potentially lost** 警报，则系统已修复所有缺失的副本。确认任何硬件问题都已得到纠正，以防止将来损坏对象副本。
    - 如果检测到的缺失对象副本大于零，并且已触发*可能丢失的对象*警报，则可能会影响数据完整性。请联系技术支持。
    - 您可以通过使用 grep 提取 LLST 审计消息来调查可能丢失的对象副本： `grep LLST audit_file_name`。

      此过程类似于 "调查可能丢失的对象" 的过程，尽管对于对象副本，您搜索的是 `LLST` 而不是 `OLST`。

12. 如果您为作业选择了强站点或强全局一致性，请等待大约三周以实现元数据一致性，然后在相同卷上重新运行作业。

    当 StorageGRID 为作业中包含的节点和卷实现元数据一致性后，重新运行作业可能会清除错误报告的缺失对象副本，或者在遗漏副本时触发对其他对象副本的检查。

a. 选择*维护* > 对象存在性检查 > 作业历史记录。

b. 确定哪些作业已准备好重新运行：

   i. 查看*结束时间*列，以确定哪些作业是在三周前运行的。

   ii. 对于这些作业，请扫描"一致性控制"列，查找 strong-site 或 strong-global。

c. 选中要重新运行的每个作业的复选框，然后选择*Rerun*。

d. 在"重新运行作业"向导中，查看选定节点和卷以及一致性。

e. 准备好重新运行作业时，选择 **Rerun**。

此时将显示活动作业选项卡。您选择的所有作业都作为一个作业在强站点的一致性下重新运行。"详细信息"部分的*相关作业*字段列出了原始作业的作业 ID。

解决 **StorageGRID** 中的 **S3 PUT** 对象大小过大警报

如果租户尝试执行超过 S3 大小限制（5 GiB）的非多部分 PutObject 操作，则会触发 S3 PUT Object size too large 警报。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

确定哪些租户使用大于 5 GiB 的对象，以便通知他们。

步骤

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

   a. 输入 `ssh admin@primary_Admin_Node_IP`

   b. 输入 `Passwords.txt`文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `Passwords.txt`文件中列出的密码。

   以 root 身份登录时，提示符将从 `$`更改为 `#`。

   e. 更改为审核日志所在的目录。

   ${post_edited_translations.segment}

选项	目标
${post_edited_translations.segment}	`/var/local/log/localaudit.log`

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

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

要了解更多信息，请参阅 "选择日志位置"。

f. 识别哪些租户正在使用大于 5 GiB 的对象。

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

ii. 对于结果中的每个审核消息，请查看 `S3AI`字段以确定租户帐户 ID。使用消息中的其他字段来确定客户端、存储桶和对象使用了哪个 IP 地址：

代码	问题描述
SAIP	源 IP
S3AI	租户 ID
S3BK	存储桶
S3KY	对象
CSIZ	大小（字节）

审核日志结果示例

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. 如果客户端写入不正常，请使用警报中的租户 ID 来标识租户：

   a. 转到 支持 > 工具 > 日志收集。收集警报中存储节点的应用程序日志。指定此警报前后的 15 分钟。请参阅 "收集日志文件和系统数据"。

   b. 提取文件并转到 `bycast.log`：

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

   c. 在日志中搜索 `method=PUT`，并在 `clientIP`字段中识别客户端。

      bycast.log 示例

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

4. 告知租户最大 PutObject 大小为 5 GiB，并对大于 5 GiB 的对象使用分段上传。
5. 如果应用程序已更改，则忽略此警报一周。

对象数据丢失和缺失故障排除

了解 **StorageGRID** 中丢失和缺失的对象数据

可以出于多种原因检索对象，包括来自客户端应用程序的读取请求、复制对象数据的后台验证、ILM 重新评估以及在存储节点恢复期间恢复对象数据。

StorageGRID 系统使用对象元数据中的位置信息来确定从哪个位置检索对象。如果在预期位置未找到该对象的副本，系统将尝试从系统中的其他位置检索该对象的另一个副本，前提是 ILM 策略包含为该对象创建两个或多个副本的规则。

如果此检索成功，StorageGRID 系统将替换对象的缺失副本。否则，将触发 **Objects potentially lost** 警报，如下所示：

- 对于复制的副本，如果无法检索另一个副本，则认为对象已丢失，并触发警报。
- 对于纠删码副本，如果无法从预期位置检索副本，则在尝试从另一位置检索副本之前，"检测到的损坏副本"(ECOR) 属性将递增 1。如果未找到其他副本，则会触发警报。

您应该立即调查所有*可能丢失的对象*警报，以确定丢失的根本原因，并确定对象是否仍然存在于离线或当前不可用的存储节点中。请参阅"调查可能丢失的对象"。可能会出于谨慎而错误地触发丢失对象警报。

在没有副本的对象数据丢失的情况下，没有恢复解决方案。但是，您必须"重置 Objects potentially lost 计数器"以防止已知丢失的对象掩盖任何新丢失的对象。

解决 **StorageGRID** 中可能丢失对象的警报

当触发 **Objects potentially lost** 警报时，您必须立即进行调查。收集有关受影响对象的信息并联系技术支持。

开始之前

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

关于此任务

*对象可能丢失*警报指示，根据 StorageGRID 中的可用信息，网格中没有对象的副本。数据可能已永久丢失。

立即调查丢失对象警报。您可能需要采取措施，以防止进一步的数据丢失。在某些情况下，如果及时采取措施，或许可以恢复丢失的对象。

如果报告丢失的对象超过 10 个，请联系技术支持。请勿自行执行此操作步骤。

步骤

1. 选择 **Nodes**。
2. 选择*存储节点* > 对象。
3. 查看"对象计数"表中显示的丢失对象数。

   此数字表示此网格节点检测到整个 StorageGRID 系统中缺少的对象总数。该值是 LDR 和 DDS 服务中数据存储组件的丢失对象计数器的总和。

4. 从管理节点，"访问审核日志"确定触发*可能丢失的对象*警报的对象的唯一标识符 (UUID)：
   a. ${post_edited_translations.segment}
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入 `Passwords.txt`文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `Passwords.txt` 文件中列出的密码。以 root 身份登录后，提示符将从 `$` 变为 `#`。
   b. 更改为审核日志所在的目录。

      ${post_edited_translations.segment}

选项	目标
${post_edited_translations.segment}	`/var/local/log/localaudit.log`
管理节点/本地节点	• 管理节点（主节点和非主节点）：`/var/local/audit/export/audit.log` • 所有节点：在此模式下，`/var/local/log/localaudit.log` 文件通常为空或缺失。
外部 syslog 服务器	`/var/local/log/localaudit.log`

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

要了解更多信息，请参阅 "选择日志位置"。

c. 使用 grep 提取对象丢失 (OLST) 审核消息。输入： `grep OLST audit_file_name`

d. 请注意消息中包含的UUID值。

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. 使用 UUID 查找丢失对象的元数据：

a. 选择 **ILM** > 对象元数据查找。

b. 输入 UUID，然后选择*查找*。

c. 查看元数据中的位置并采取适当的操作：

元数据	结束语
对象 <object_identifier> 未找到	如果未找到对象，则返回消息"ERROR": "。 如果未找到此对象，重置 Objects potentially lost 计数器以清除此警报。缺少对象表示此对象是故意删除的。
位置 > 0	如果输出中列出了位置，则 **Objects potentially lost** 警报可能是误报。 确认对象存在。使用输出中列出的节点 ID 和文件路径确认对象文件位于列出的位置。 如果对象存在，重置 Objects potentially lost 计数器 以清除此警报。
位置 = 0	如果输出中未列出位置，则可能缺少对象。请联系技术支持。 技术支持可能会要求您确定是否正在进行存储恢复过程。请参阅有关 "使用 Grid Manager 还原对象数据" 和 "将对象数据还原至存储卷" 的信息。

6. 解决丢失对象问题后，重置可能丢失的对象计数器，以确保警报不是误报：

a. 选择 **Nodes**。

b. 选择*存储节点* > 任务。

c. 在"重置可能丢失的对象"计数器部分，选择*Reset*。

解决 **StorageGRID** 中的低对象数据存储警报

*低对象数据存储*警报监控每个存储节点上可用于存储对象数据的空间。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

关于此任务

当存储节点上复制和纠删编码的对象数据总量满足警报规则中配置的条件之一时，会触发 **Low object data storage** 警报。

默认情况下，当此条件评估为 true 时将触发重大警报：

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

在此情况下：

- `storagegrid_storage_utilization_data_bytes` 是存储节点的已复制和纠删码对象数据总大小的估计值。
- `storagegrid_storage_utilization_usable_space_bytes` 是存储节点剩余的对象存储空间总量。

如果触发了主要或次要*低对象数据存储*警报，则应尽快执行扩展过程。

步骤

1. 选择*Alerts* > **Current**。

   此时将显示警报页面。

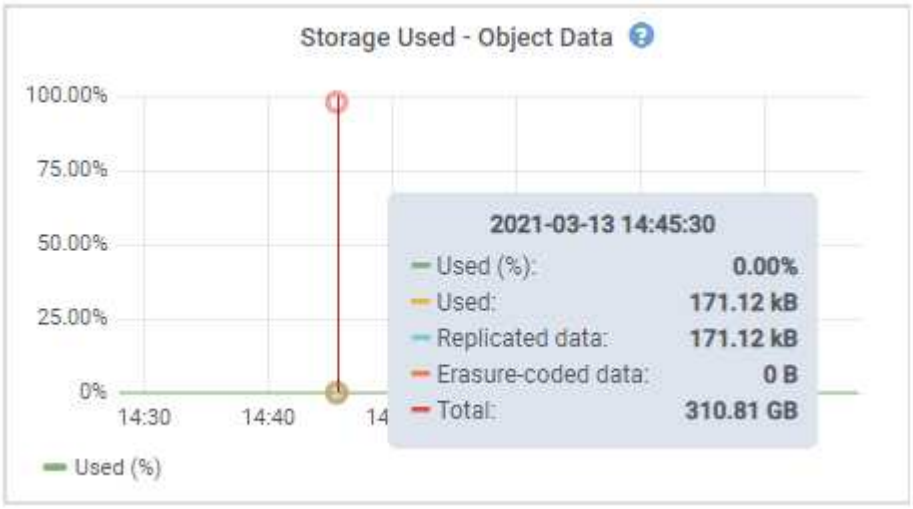
2. 如果需要，从警报表中展开*低对象数据存储*警报组，然后选择要查看的警报。

   选择警报，而不是一组警报的标题。

3. 查看对话框中的详细信息，并注意以下事项：
   - 时间触发
   - 站点和节点的名称
   - 此警报的指标的当前值
4. 选择*节点* > 存储节点或站点 > 存储。
5. 将光标放置在"已用存储 - 对象数据"图形上。

   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。
- 已使用：已用于对象数据的总可用空间量。
- 已复制数据：此节点、站点或网格上已复制对象数据量的估计值。
- 纠删码数据：此节点、站点或网格上纠删码对象数据量的估计值。
- **Total**：此节点、站点或网格上的可用空间总量。Used 值是 `storagegrid_storage_utilization_data_bytes`度量值。



6. 选择图表上方的时间控件，查看不同时间段的存储使用情况。

   查看一段时间内的存储使用情况可以帮助您了解在触发警报之前和之后使用了多少存储空间，并可以帮助您估计节点的剩余空间可能需要多长时间才能耗尽。

7. 尽快"添加存储容量"到您的网格。

   您可以将存储卷(LUN)添加到现有存储节点，也可以添加新的存储节点。

   有关详细信息，请参见 "管理完整存储节点"。

解决 **StorageGRID** 中的水印覆盖警报

如果对存储卷水印使用自定义值，则可能需要解决*低只读水印覆盖*警报。如果可能，您应该更新系统，开始使用优化后的值。

在以前的版本中，这三个"存储卷水印"是全局设置 — 应用于每个存储节点上每个存储卷的值相同。从 StorageGRID 11.6 开始，软件可以根据存储节点的大小和卷的相对容量为每个存储卷优化这些水印。

升级到 StorageGRID 11.6 或更高版本时，优化的只读和读写水印将自动应用于所有存储卷，除非满足以下条件之一：

- 您的系统已接近容量，如果应用了优化的水印，将无法接受新数据。在这种情况下，StorageGRID 不会更改水印设置。
- 您之前已将任何存储卷水印设置为自定义值。StorageGRID 不会使用优化值覆盖自定义水印设置。但是，如果存储卷软只读水印的自定义值太小，StorageGRID 可能会触发 低只读水印覆盖 警报。

了解此警报

如果对存储卷水印使用自定义值，则可能会为一个或多个存储节点触发*低只读水印覆盖*警报。

警报的每个实例都指示存储卷软只读水印的自定义值小于该存储节点的最小优化值。如果继续使用自定义设置，存储节点的空间可能会严重不足，从而无法安全地转换为只读状态。当节点达到容量时，某些存储卷可能无法访问（自动卸载）。

例如，假设您之前将存储卷软只读水印设置为 5 GB。现在假设 StorageGRID 已为存储节点 A 中的四个存储卷计算出以下优化值：

卷 0	12 GB
卷 1	12 GB
卷 2	11 GB
卷 3	15 GB

由于您的自定义水印（5 GB）小于该节点中所有卷的最小优化值（11 GB），因此会为存储节点 A 触发*低只读水印覆盖*警报。如果继续使用自定义设置，节点的空间可能会严重不足，从而无法安全地转换为只读状态。

解决警报

如果触发了一个或多个*低只读水印覆盖*警报，请按照以下步骤操作。如果您当前使用自定义水印设置，并且希望开始使用优化设置，即使没有触发任何警报，您也可以使用这些说明。

开始之前

- 您已完成升级到 StorageGRID 11.6 或更高版本。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

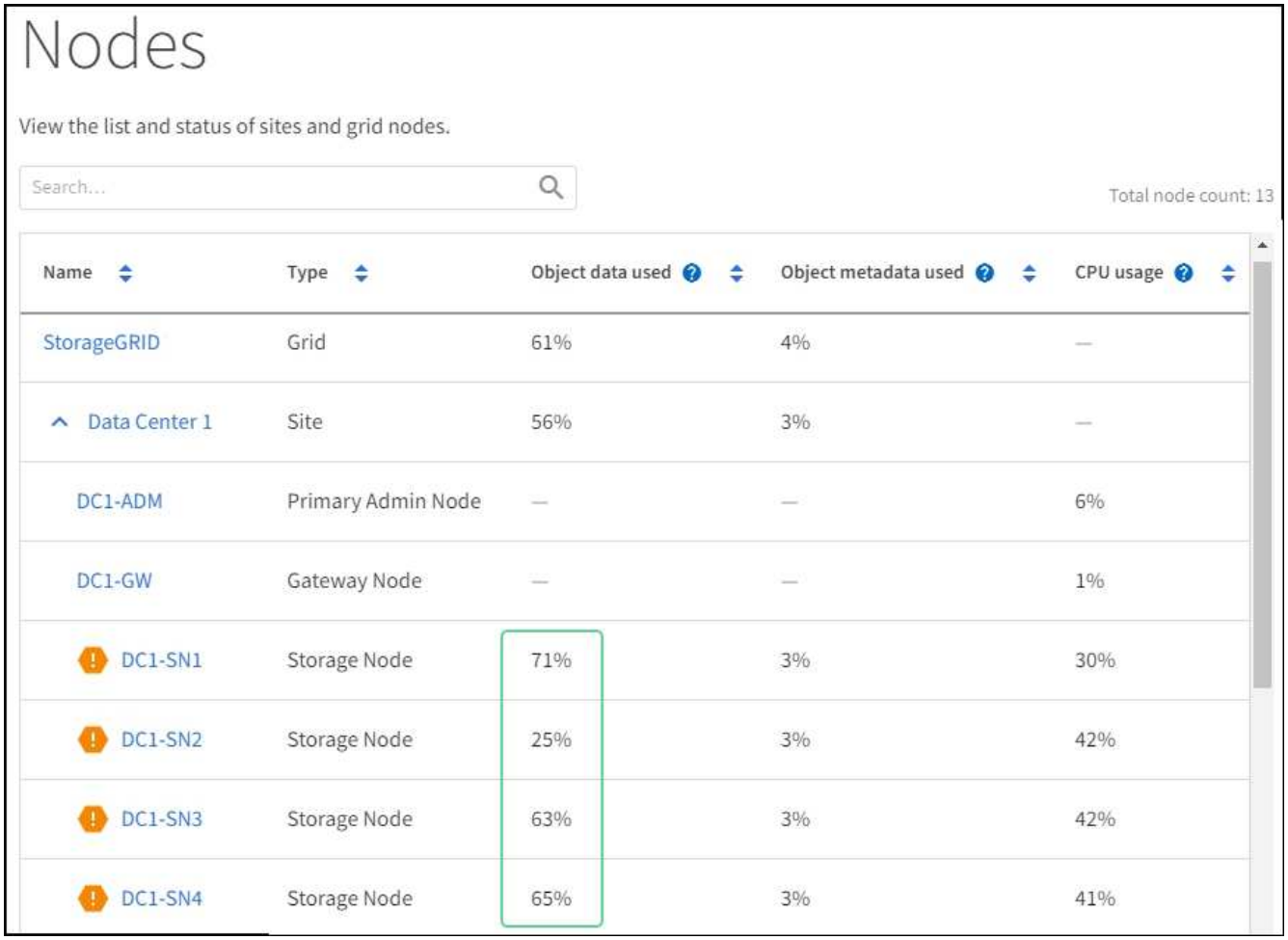
关于此任务

您可以通过将自定义水印设置更新为新的水印覆盖来解决*低只读水印覆盖*警报。但是，如果一个或多个存储节点接近满，或者您有特殊的 ILM 要求，则应首先查看优化的存储水印并确定使用它们是否安全。

评估整个网格的对象数据使用情况

步骤

1. 选择 **Nodes**。
2. 对于网格中的每个站点，展开节点列表。
3. 查看每个站点上每个存储节点的*使用的对象数据*列中显示的百分比值。



4. 按照相应的步骤进行操作：
   a. 如果没有存储节点接近满（例如，所有*使用的对象数据*值均小于 80%），则可以开始使用覆盖设置。转到 使用优化的水印。
   b. 如果 ILM 规则使用严格接收行为或特定存储池接近满，请执行 查看优化的存储水印 和 确定是否可以使用优化的水印 中的步骤。

查看优化的存储水印

StorageGRID 使用两个 Prometheus 指标来显示它为存储卷软只读水印计算的优化值。您可以查看网格中每个存储节点的最小和最大优化值。

步骤

1. ${post_edited_translations.segment}
2. 在 Prometheus 部分，选择链接以访问 Prometheus 用户界面。
3. 要查看推荐的最小软只读水印，请输入以下 Prometheus 指标，然后选择 **Execute**：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最小优化值。如果此值大于存储卷软只读水印的自定义设置，则会为存储节点触发 **Low read-only watermark override** 警报。

4. 要查看建议的最大软只读水印，请输入以下 Prometheus 指标，然后选择*执行*：

`storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark`

最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

5. 注意每个存储节点的最大优化值。

确定是否可以使用优化的水印

步骤

1. 选择 **Nodes**。
2. 对每个联机存储节点重复以下步骤：
   a. 选择 ***Storage Node*** > **Storage**。
   b. 向下滚动到 Object Stores 表。
   c. 将每个对象存储（卷）的*可用*值与您为该存储节点记录的最大优化水印进行比较。
3. 如果每个在线存储节点上至少有一个卷的可用空间大于该节点的最大优化水印，请转至使用优化的水印以开始使用优化水印。

   否则，请尽快扩展网格。可以 "添加存储卷" 到现有节点，也可以 "添加新的存储节点"。然后，转到 使用优化的水印 以更新水印设置。

4. 如果需要继续对存储卷水印使用自定义值，请"沉默"或"禁用" *低只读水印覆盖*警报。

> 相同的自定义水印值应用于每个存储节点上的每个存储卷。使用小于建议值的存储卷水印值可能会导致某些存储卷在节点达到容量时无法访问（自动卸载）。

使用优化的水印

步骤

1. 转到*支持* > 其他 > 存储水印。
2. 选中*使用优化值*复选框。
3. 选择 **Save**。

根据存储节点的大小和卷的相对容量，优化的存储卷水印设置现在对每个存储卷生效。

对 StorageGRID 中的元数据问题进行故障排除

如果出现元数据问题，警报将告知您问题的根源和建议采取的措施。特别是，如果触发了 Low metadata storage 警报，则必须添加新的存储节点。

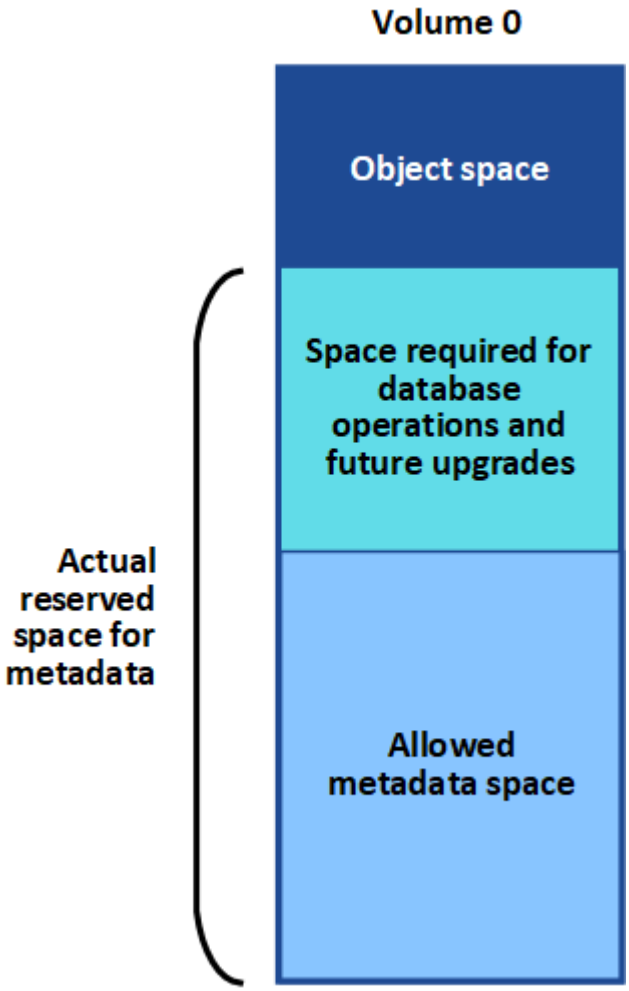
开始之前

您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

针对触发的每个与元数据相关的警报，遵循建议的操作。如果触发了*低元数据存储*警报，则必须添加新的存储节点。

StorageGRID 在每个存储节点的卷 0 上为对象元数据保留一定量的空间。该空间称为_实际保留空间_，细分为对象元数据所允许的空间（允许的元数据空间）和基本数据库操作（如压缩和修复）所需的空间。允许的元数据空间控制整体对象容量。



如果对象元数据占用的空间超过元数据允许空间的 100%，则数据库操作无法高效运行，并且将发生错误。

您可以 "监控每个存储节点的对象元数据容量" 帮助您预测错误并在错误发生前进行纠正。

StorageGRID 使用以下 Prometheus 指标来衡量允许的元数据空间的满度：

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

当此 Prometheus 表达式达到特定阈值时，将触发*低元数据存储*警报。

- **Minor**：对象元数据使用了 70% 或更多允许的元数据空间。您应尽快添加新的 Storage Nodes。
- **Major**：对象元数据使用了 90% 或更多允许的元数据空间。您必须立即添加新的存储节点。

> 当对象元数据使用 90% 或更多允许的元数据空间时，仪表板上将显示警告。如果出现此警告，则必须立即添加新的存储节点。切勿允许对象元数据使用超过允许空间的 100%。

- **Critical**：对象元数据正在使用 100% 或更多允许的元数据空间，并开始占用基本数据库操作所需的空间。您必须停止摄取新对象，并且必须立即添加新的存储节点。

> 如果卷 0 的大小小于元数据保留空间存储选项（例如，在非生产环境中），则*低元数据存储*警报的计算可能不准确。

步骤

1. 选择*Alerts* > **Current**。
2. 如果需要，从警报表中展开*低元数据存储*警报组，然后选择要查看的特定警报。
3. 查看警报对话框中的详细信息。
4. 如果已触发重大或关键的*低元数据存储*警报，请执行扩展以立即添加存储节点。

> 由于 StorageGRID 保留所有对象元数据的完整副本，因此整个网格的元数据容量受到最小站点的元数据容量的限制。如果需要向某个站点添加元数据容量，还应该"展开任何其他站点"添加相同数量的存储节点。

执行扩展后，StorageGRID 会将现有对象元数据重新分配到新节点，从而增加网格的整体元数据容量。无需用户操作。*低元数据存储*警报已清除。

对 **StorageGRID** 中的证书错误进行故障排除

如果您在尝试使用 Web 浏览器、S3 客户端或外部监控工具连接到 StorageGRID 时看到安全或证书问题，您应该检查证书。

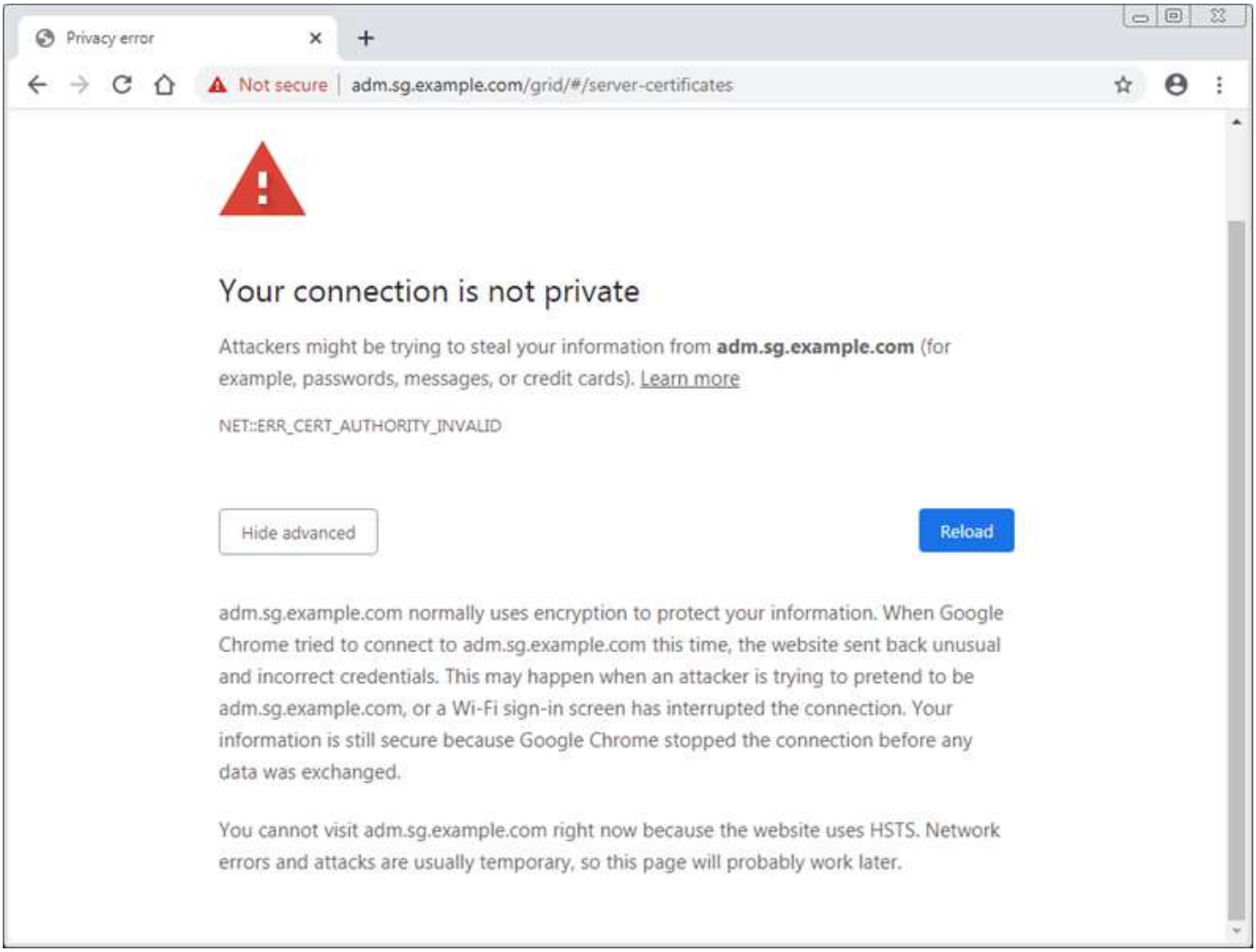
关于此任务

当您尝试使用 Grid Manager、Grid Management API、Tenant Manager 或 Tenant Management API 连接到 StorageGRID 时，证书错误可能会导致问题。当您尝试使用 S3 客户端或外部监控工具进行连接时，也可能会发生证书错误。

如果使用域名而不是 IP 地址访问 Grid Manager 或 Tenant Manager，则浏览器将显示证书错误，如果发生以下任一情况，则无法选择绕过：

- 您的自定义管理界面证书已过期。
- 将自定义管理接口证书还原为默认服务器证书。

自定义管理接口证书过期时出现证书错误的示例如下所示：



为了确保操作不会因服务器证书失效而中断，当服务器证书即将过期时，会触发 **Expiration of server certificate for Management Interface** 警报。

当您使用客户端证书进行外部 Prometheus 集成时，证书错误可能是由 StorageGRID 管理接口证书或客户端证书引起的。*证书页面上配置的客户端证书过期*警报在客户端证书即将过期时触发。

步骤

如果您收到有关过期证书的警报通知，请访问证书详细信息：。选择 **Configuration** > **Security** > **Certificates**，然后选择 "选择相应的证书选项卡"。

1. 检查证书的有效期。+ 某些 Web 浏览器和 S3 客户端不接受有效期超过 398 天的证书。
2. 如果证书已过期或即将过期，请上传或生成新证书。
   - 有关服务器证书，请参见 "为 Grid Manager 和 Tenant Manager 配置自定义服务器证书" 的步骤。
   - 有关客户端证书，请参见 "配置客户端证书" 的步骤。
3. 对于服务器证书错误，请尝试下列选项之一或两者：
   - 确保已填充证书的使用者备用名称 (SAN)，并且 SAN 与要连接到的节点的 IP 地址或主机名匹配。
   - 如果要使用域名连接到 StorageGRID：
     i. 输入管理节点的 IP 地址，而不是域名，以绕过连接错误并访问 Grid Manager。

ii. 从网格管理器中，选择*配置* > 安全 > 证书，然后 "选择相应的证书选项卡" 安装新的自定义证书或继续使用默认证书。

iii. 在管理 StorageGRID 的说明中，请参见 "为 Grid Manager 和 Tenant Manager 配置自定义服务器证书" 的步骤。

对 StorageGRID 中的管理节点和用户界面问题进行故障排除

您可以执行多个任务来帮助确定与管理节点和 StorageGRID 用户界面相关的问题的来源。

管理节点登录错误

如果您在登录 StorageGRID 管理节点时遇到错误，则您的系统可能存在 "网络连接" 或 "硬件" 问题、"管理节点服务" 问题，或连接的存储节点上的 "Cassandra 数据库的问题" 问题。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您拥有 `Passwords.txt` 文件。
- 您有 "特定访问权限"。

关于此任务

如果在尝试登录到管理节点时看到以下任一错误消息，请使用以下故障排除指南：

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

步骤

1. 请稍等 10 分钟，然后尝试重新登录。

   如果错误未自动解决，请转至下一步。

2. 如果您的 StorageGRID 系统有多个管理节点，请尝试从另一个管理节点登录到 Grid Manager，以检查不可用的管理节点的状态。
   - 如果您能够登录，可以使用*控制面板*、节点、*提醒*和*支持*选项来帮助确定错误的原因。
   - 如果您只有一个管理节点或仍无法登录，请转至下一步。
3. 确定节点的硬件是否已脱机。
4. 如果您的 StorageGRID 系统启用了单点登录 (SSO)，请参见 "配置单点登录" 的步骤。

   您可能需要暂时禁用并重新启用单个管理节点的 SSO 以解决相关问题。

   > 如果启用了 SSO，则无法使用受限端口登录。您必须使用端口 443。

5. 确定您使用的帐户是否属于联合用户。

   如果联合用户帐户不起作用，请尝试以本地用户（例如 root）身份登录到 Grid Manager。

   - 如果本地用户可以登录：
     i. 查看警报。
     ii. 选择*配置* > 访问控制 > 身份联合。
     iii. 单击*测试连接*以验证您的 LDAP 服务器连接设置。
     iv. 如果测试失败，请解决所有配置错误。
   - 如果本地用户无法登录，并且您确信凭据正确，请转到下一步。

6. 使用安全 Shell (SSH) 登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。

7. 查看网格节点上运行的所有服务的状态： `storagegrid-status`

   确保 nms、mi、nginx 和 mgmt api 服务均在运行。

   如果服务的状态发生变化，输出将立即更新。

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. 确认 nginx-gw 服务正在运行 `# service nginx-gw status`
9. 使用 Lumberjack 收集日志： `# /usr/local/sbin/lumberjack.rb`

   如果身份验证失败发生在过去，您可以使用 --start 和 --end Lumberjack 脚本选项指定适当的时间范围。有关这些选项的详细信息，请使用 lumberjack -h。

   终端的输出指示已复制日志存档的位置。

10. 查看以下日志：
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`

11. 如果您无法识别管理节点的任何问题，请发出以下命令之一，以确定在您的站点运行 ADC 服务的三个存储节点的 IP 地址。通常，这些是在该站点安装的前三个存储节点。

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

管理节点在身份验证过程中使用 ADC 服务。

12. 从管理节点，使用 ssh 登录到每个 ADC 存储节点，使用您确定的 IP 地址。
13. 查看网格节点上运行的所有服务的状态： `storagegrid-status`

确保 idnt、acct、nginx 和 cassandra 服务都在运行。

14. 重复步骤 使用 Lumberjack 收集日志 和 查看日志 以查看存储节点上的日志。
15. 如果您无法解决此问题，请与技术支持联系。

将您收集的日志提供给技术支持。另请参阅"日志文件引用"。

用户界面问题

升级 StorageGRID 软件后，Grid Manager 或 Tenant Manager 的用户界面可能无法按预期响应。

步骤

1. 请确保使用 "支持的 Web 浏览器"。
2. 清除 Web 浏览器缓存。

清除缓存可删除先前版本的 StorageGRID 软件使用的过时资源，并允许用户界面再次正常运行。有关说明，请参见 Web 浏览器的文档。

对 **StorageGRID** 中的网络、硬件和平台问题进行故障排除

可以执行多个任务来帮助确定与 StorageGRID 网络、硬件和平台问题相关的问题根源。

[[422-unprocessable-entity-errors]]
== "422: Unprocessable Entity"错误

错误 422：无法处理的实体可能出于不同原因而发生。请查看错误消息，以确定导致问题的原因。

如果您看到列出的错误消息之一，请执行建议的操作。

错误消息	根本原因和纠正措施

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	如果在使用 Windows Active Directory (AD) 配置身份联合时为传输层安全性 (TLS) 选择*不使用 TLS* 选项，则可能会出现此消息。
	
	对于强制 LDAP 签名的 AD 服务器，不支持使用 **Do not use TLS** 选项。您必须为 TLS 选择 **Use STARTTLS** 选项或 **Use LDAPS** 选项。

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	如果您尝试使用不受支持的密码从 StorageGRID 向用于身份联合或云存储池的外部系统建立传输层安全性 (TLS) 连接，则会显示此消息。
	
	检查外部系统提供的密码。系统必须使用其中一个 "StorageGRID 支持的密码" 用于传出 TLS 连接，如 StorageGRID 管理说明中所示。

网格网络 **MTU** 不匹配警报

当网格网络接口（eth0）的最大传输单元（MTU）设置在网格中的节点之间存在显著差异时，将触发*网格网络 MTU 不匹配*警报。

关于此任务

MTU 设置的差异可能表明部分（而非全部）eth0 网络已配置为巨型帧。MTU 大小不匹配超过 1000 可能会导致网络性能问题。

步骤

1. 默认情况下会阻止外部 SSH 访问。如有需要，"暂时允许访问"。
2. 列出所有节点上 eth0 的 MTU 设置。
   - 使用网格管理器中提供的查询。
   - 导航到 *primary Admin Node IP address*`/metrics/graph`并输入以下查询：`node_network_mtu_bytes{device="eth0"}`
3. "修改 MTU 设置" 根据需要进行调整，以确保所有节点上的网格网络接口 (eth0) 都相同。
   - 对于基于 Linux 和 VMware 的节点，请使用以下命令： `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     示例: `change-ip.py -n node 1500 grid admin`

     Note：在基于 Linux 的节点上，如果容器中网络所需的 MTU 值超过主机接口上已配置的值，则必须首先将主机接口配置为具有所需的 MTU 值，然后使用 `change-ip.py`脚本更改容器中网络的 MTU 值。

     使用以下参数修改基于 Linux 或 VMware 的节点上的 MTU。

位置参数	问题描述
`mtu`	要设置的 MTU。必须介于 1280 到 9216 之间。
`network`	要应用 MTU 的网络。包括以下一种或多种网络类型： • 网格 • admin • client

+

可选参数	问题描述
`-h, - help`	显示帮助消息并退出。
`-n node, --node node`	节点。默认值为本地节点。

4. 如果您已允许外部 SSH 访问，请在完成任务后"阻止访问"。

节点网络接收帧错误警报

*节点网络接收帧错误*警报可能是由 StorageGRID 和网络硬件之间的连接问题引起的。解决根本问题后，此警报会自行清除。

关于此任务

*节点网络接收帧错误*警报可能由连接到 StorageGRID 的以下网络硬件问题引起：

- 前向纠错（FEC）为必填项，当前未使用
- 交换机端口和 NIC MTU 不匹配
- 高链接错误率
- 网卡环缓冲区溢出

步骤

1. 根据网络配置，请按照故障排除步骤来解决此警报的所有潜在原因。
2. 请根据错误原因执行以下步骤：

FEC不匹配

这些步骤仅适用于由 StorageGRID 设备上的 FEC 不匹配引起的*节点网络接收帧错误*警报。

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

b. 检查从设备到交换机的电缆的物理完整性。

c. 如果要更改 FEC 设置以尝试解决警报，请首先确保在 StorageGRID Appliance Installer 的链路配置页面上将设备配置为 **Auto** 模式（请参阅设备的说明：

- "SG6160"
- "SGF6112"
- "SG6000"
- "SG5800"
- "SG5700"
- "SG110 和 SG1100"
- "SG100 和 SG1000"

d. 更改交换机端口上的 FEC 设置。如果可能，StorageGRID 设备端口将调整其 FEC 设置以进行匹配。

您无法在 StorageGRID 设备上配置 FEC 设置。相反，设备会尝试在其连接的交换机端口上发现并镜像 FEC 设置。如果链路被强制为 25-GbE 或 100-GbE 网络速度，交换机和 NIC 可能无法协商通用 FEC 设置。如果没有通用的 FEC 设置，网络将回退到"无 FEC"模式。未启用 FEC 时，连接更容易受到电气噪声引起的错误的影响。

StorageGRID 设备支持 Firecode (FC) 和 Reed Solomon (RS) FEC，以及无 FEC 模式。

交换机端口和 **NIC MTU** 不匹配

如果警报是由交换机端口和 NIC MTU 不匹配引起的，请检查节点上配置的 MTU 大小是否与交换机端口的 MTU 设置相同。

节点上配置的 MTU 大小可能小于节点连接的交换机端口上的设置。如果 StorageGRID 节点接收到大于其 MTU 的以太网帧（此配置下可能发生），则可能会报告*节点网络接收帧错误*警报。如果您认为这是正在发生的情况，请根据您的端到端 MTU 目标或要求，更改交换机端口的 MTU 以匹配 StorageGRID 网络接口 MTU，或更改 StorageGRID 网络接口的 MTU 以匹配交换机端口。

为了获得最佳网络性能，所有节点都应在其网格网络接口上配置类似的 MTU 值。如果单个节点上的网格网络的 MTU 设置存在显著差异，则会触发 网格网络 **MTU** 不匹配 警报。所有网络类型的 MTU 值不一定相同。有关详细信息，请参见 排查 Grid Network MTU 不匹配警报。

另请参见 "更改 MTU 设置"。

高链接错误率

a. 启用 FEC（如果尚未启用）。

b. 确认您的网络布线质量良好，没有损坏或连接不当。

c. 如果电缆似乎不是问题，请与技术支持联系。

> 在电气噪音较高的环境中，您可能会注意到较高的错误率。

网卡环缓冲区溢出

如果错误是 NIC 环缓冲区溢出，请与技术支持联系。

当 StorageGRID 系统过载且无法及时处理网络事件时，环形缓冲区可能会溢出。

3. 监控问题，如果警报未解决，请联系技术支持。

时间同步错误

您可能会在网格中看到时间同步问题。

如果遇到时间同步问题，请确认您已指定至少四个外部 NTP 源，每个 NTP 源都提供 Stratum 3 或更好的参考，并且所有外部 NTP 源均正常运行，且可由 StorageGRID 节点访问。

> 当 "指定外部 NTP 源" 对于生产级 StorageGRID 安装，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间 (W32Time) 服务。早期版本的 Windows 上的时间服务不够准确，Microsoft 不支持在高精度环境中使用，例如 StorageGRID。

Linux：网络连接问题

您可能会看到 Linux 主机上托管的 StorageGRID 节点的网络连接问题。

MAC地址克隆

在某些情况下，可以通过使用 MAC 地址克隆来解决网络问题。如果使用虚拟主机，请在节点配置文件中将每个网络的 MAC 地址克隆密钥的值设置为"true"。此设置会导致 StorageGRID 容器的 MAC 地址使用主机的 MAC 地址。请参阅 "创建节点配置文件" 的说明。

> 创建单独的虚拟网络接口供 Linux 主机操作系统使用。如果未在虚拟机监控程序上启用混杂模式，则对 Linux 主机操作系统和 StorageGRID 容器使用相同的网络接口可能会导致主机操作系统无法访问。

有关详细信息，请参见 "启用MAC克隆" 的说明。

混杂模式

如果您不想使用 MAC 地址克隆，而是希望允许所有接口接收和传输虚拟机管理程序所分配地址以外的 MAC 地址数据，请确保虚拟交换机和端口组级别的安全属性针对混杂模式、MAC 地址更改和伪造传输均设置为 **Accept**。虚拟交换机上设置的值可被端口组级别的值覆盖，因此请确保两处的设置相同。

有关使用混杂模式的详细信息，请参见 "如何配置主机网络" 的说明。

Linux：节点状态为"orphaned"

处于孤立状态的 Linux 节点通常表示控制节点容器的 storagegrid 服务或 StorageGRID 节点守护进程意外终止。

关于此任务

如果 Linux 节点报告它处于孤立状态，则应：

- 检查日志中的错误和消息。
- 请尝试重新启动此节点。
- 如有必要，使用容器引擎命令停止现有节点容器。
- 重新启动节点。

步骤

1. 检查服务后台程序和孤立节点的日志，查看是否有明显的错误或有关意外退出的消息。
2. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
3. 通过运行以下命令再次尝试启动节点： `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   如果节点已孤立，则响应为

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. 在 Linux 中，停止容器引擎和任何控制 storagegrid-node 的进程。例如：`sudo docker stop --time secondscontainer-name`

   对于 `seconds`，请输入要等待容器停止的秒数（通常为 15 分钟或更短）。例如：

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. 重新启动节点： `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

Linux：IPv6 支持故障排除

如果您在 Linux 主机上安装了 StorageGRID 节点，并且注意到 IPv6 地址未按预期分配给节点容器，则可能需要在内核中启用 IPv6 支持。

关于此任务

要查看已分配给网格节点的 IPv6 地址：

1. 选择*节点*并选择节点。
2. 在"概述"选项卡上，选择 **IP** 地址*旁边的*显示其他 **IP** 地址。

如果未显示 IPv6 地址，并且节点安装在 Linux 主机上，请按照以下步骤在内核中启用 IPv6 支持。

步骤

1. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
2. 运行以下命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

结果应为0。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> 如果结果不是 0，请参阅操作系统的文档以更改 `sysctl`设置。然后，在继续之前将此值更改为 0。

3. 进入 StorageGRID 节点容器： `storagegrid node enter node-name`
4. 运行以下命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

结果应为 1。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> 如果结果不是 1，则此程序不适用。请联系技术支持。

5. 退出此容器： `exit`

```
root@DC1-S1:~ # exit
```

6. 以超级用户身份编辑以下文件： `/var/lib/storagegrid/settings/sysctl.d/net.conf`。

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 找到以下两行并删除注释标记。然后，保存并关闭此文件。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 运行以下命令以重新启动 StorageGRID 容器：

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

对 StorageGRID 外部系统日志服务器错误消息进行故障排除

下表介绍了可能与使用外部 syslog 服务器相关的错误消息，并列出了纠正措施。

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

运行时出现的问题可能会由 "外部syslog服务器转发错误" 警报报告。如果收到此警报，请按照此警报中的说明重新发送测试消息，以便获取详细的错误消息。

有关向外部 syslog 服务器发送审核信息的详细信息，请参见：

- "使用外部 syslog 服务器的注意事项"
- "配置日志管理和外部 syslog 服务器"

错误消息	说明和建议操作
无法解析主机名称	无法将您为 syslog 服务器输入的 FQDN 解析为 IP 地址。 1. 检查您输入的主机名。如果您输入了 IP 地址，请确保它是 W.X.Y.Z（"点分十进制"）表示法的有效 IP 地址。 2. 请检查DNS服务器配置是否正确。 3. 确认每个节点都可以访问 DNS 服务器的 IP 地址。
连接被拒绝	与 syslog 服务器的 TCP 或 TLS 连接被拒绝。主机的 TCP 或 TLS 端口上可能没有侦听服务，或者防火墙可能正在阻止访问。 1. 请检查您输入的系统日志服务器的 FQDN 或 IP 地址、端口和协议是否正确。 2. 确认 syslog 服务的主机正在运行侦听指定端口的 syslog 守护程序。 3. 确认防火墙没有阻止从节点到 syslog 服务器的 IP 和端口的 TCP/TLS 连接访问。

错误消息	说明和建议操作
网络不可达	syslog 服务器不在直接连接的子网上。路由器返回了 ICMP 故障消息，表示无法将测试消息从列出的节点转发到 syslog 服务器。 1. 检查是否为 syslog 服务器输入了正确的 FQDN 或 IP 地址。 2. 对于列出的每个节点，请检查网格网络子网列表、管理网络子网列表和客户端网络网关。确认这些配置为通过预期的网络接口和网关（网格、管理或客户端）将流量路由到 syslog 服务器。
主机不可达	syslog 服务器位于直接连接的子网（列出的节点用于其网格、管理或客户端 IP 地址的子网）上。节点尝试发送测试消息，但未收到针对 syslog 服务器 MAC 地址的 ARP 请求的响应。 1. 检查是否为 syslog 服务器输入了正确的 FQDN 或 IP 地址。 2. 检查运行 syslog 服务的主机是否已启动。
连接超时	已尝试 TCP/TLS 连接，但长时间未收到来自 syslog 服务器的响应。可能存在路由配置错误，或者防火墙可能在未发送任何响应的情况下丢弃流量（常见配置）。 1. 检查是否为 syslog 服务器输入了正确的 FQDN 或 IP 地址。 2. 对于列出的每个节点，请检查网格网络子网列表、管理网络子网列表和客户端网络网关。确认这些配置为使用您希望访问 syslog 服务器的网络接口和网关（网格、管理员或客户端）将流量路由到 syslog 服务器。 3. 确认防火墙没有阻止从列出的节点到 syslog 服务器的 IP 和端口的 TCP/TLS 连接访问。
连接被合作伙伴关闭	与 syslog 服务器的 TCP 连接已成功建立，但后来被关闭。原因可能包括： • Syslog 服务器可能已重新启动或重启。 • 节点和 syslog 服务器可能具有不同的 TCP/TLS 设置。 • 中间防火墙可能正在关闭空闲的 TCP 连接。 • 侦听 syslog 服务器端口的非 syslog 服务器可能已关闭连接。 要解决此问题： 1. 请检查您输入的系统日志服务器的 FQDN 或 IP 地址、端口和协议是否正确。 2. 如果使用的是 TLS，请确认 syslog 服务器也在使用 TLS。如果使用的是 TCP，请确认 syslog 服务器也在使用 TCP。 3. 检查中间防火墙是否配置为关闭空闲的 TCP 连接。

错误消息	说明和建议操作
TLS证书错误	从 syslog 服务器收到的服务器证书与您提供的 CA 证书捆绑包和客户端证书不兼容。 1. 确认 CA 证书捆绑包和客户端证书（如果有）与 syslog 服务器上的服务器证书兼容。 2. 确认来自 syslog 服务器的服务器证书中的标识包含预期的 IP 或 FQDN 值。
转发已暂停	Syslog 记录不再转发到 syslog 服务器，StorageGRID 无法检测到原因。 查看此错误提供的调试日志，以尝试确定根本原因。
TLS会话已终止	syslog 服务器终止了 TLS 会话，StorageGRID 无法检测到原因。 1. 查看此错误提供的调试日志，以尝试确定根本原因。 2. 请检查您输入的系统日志服务器的 FQDN 或 IP 地址、端口和协议是否正确。 3. 如果使用的是 TLS，请确认 syslog 服务器也在使用 TLS。如果使用的是 TCP，请确认 syslog 服务器也在使用 TCP。 4. 确认 CA 证书捆绑包和客户端证书（如果有）与来自 syslog 服务器的服务器证书兼容。 5. 确认来自 syslog 服务器的服务器证书中的标识包含预期的 IP 或 FQDN 值。
结果查询失败	用于 syslog 服务器配置和测试的管理节点无法从列出的节点请求测试结果。一个或多个节点可能已关闭。 1. 遵循标准故障排除步骤，确保节点处于联机状态，并且所有预期的服务都在运行。 2. 在列出的节点上重新启动 miscd 服务。

了解 StorageGRID 中的负载均衡器缓存问题

了解负载平衡器缓存可能存在的问题以及如何对其进行故障排除。

确定请求是否为缓存命中

- X-Cache 标头在对缓存服务处理的请求的响应中设置。可能的代码：
  - `HIT`：对象从缓存提供
  - `PARTIAL-HIT`：存储桶/密钥在缓存中有记录，但并非所有请求的范围都能够从缓存提供
  - `STALE`：存储桶/密钥在缓存中有记录，但该对象自上次从缓存中提供以来已更新。
  - `MISS`：对象未在缓存中
- 请求的 `nginx-gw/endpoint-access.log.gz`记录包含由缓存处理的请求的"unix:/run/cache-svc/cache-svc.sock"。

- `cache-svc/cache-svc.log` 报告诸如"Request 320390：已成功完成（缓存命中）"或"Request 320375：已成功完成（缓存未命中）"之类的消息。通过搜索具有相同"Request *<number>*"字符串的其他记录来查找请求的路径。

缓存命中率低

- 当添加新的工作负载或工作负载访问的工作集发生变化时，缓存命中率可能会较低。在这些情况下，命中率预计会随着时间的推移而增加。
- 如果多个工作负载正在使用缓存，请考虑添加流量分类策略，以隔离由缓存提供服务的部分工作负载。缓存命中率指标可按流量分类策略查看。如果某些工作负载的缓存命中率不高，请考虑将这些工作负载移动到未启用缓存的其他端点。
- 评估缓存逐出率。如果缓存太小，无法容纳工作集，则会出现较高的逐出率，并可能导致较低的命中率。
- FPVR 下可能提供提高某些工作负载命中率的选项。

性能低下

- 评估缓存命中率。缓存命中率低可能导致整体性能低下。
- 评估缓存逐出率。在逐出期间，一些存储资源用于从磁盘中删除现有对象。如果逐出过程跟不上新对象的访问，系统可能会达到硬水印阈值并开始绕过缓存。
- 使用"Network interfaces receive usage"和"Network interfaces transmit usage"诊断检查网络限制。

查看审核日志

审核消息和日志

这些说明包含有关 StorageGRID 审计消息和审计日志的结构和内容的信息。您可以使用此信息阅读和分析系统活动的审计跟踪。

这些说明适用于负责生成系统活动和使用情况报告的管理员，这些报告需要分析 StorageGRID 系统的审计消息。

要使用文本日志文件，必须能够访问管理节点上配置的审计共享。

有关配置审核消息级别和使用外部 syslog 服务器的信息，请参见 "配置日志管理和外部 syslog 服务器"。

审核消息如何通过 **StorageGRID** 系统移动到 **audit.log** 文件以进行保留

所有 StorageGRID 服务在正常系统操作期间生成审核消息。您应该了解这些审核消息如何通过 StorageGRID 系统移动到 `audit.log`文件。

以下审核消息和审核消息保留的工作流程仅适用于为 **Admin Nodes/local nodes** 或 **Admin Node and external syslog server** 配置的 StorageGRID。如果 StorageGRID 配置为"Local nodes only"（默认）或"External syslog server"，则审核消息将本地保存在每个节点的 `/var/local/log/localaudit.log`文件中，且无法由 Admin Nodes 或 Storage Nodes 处理。

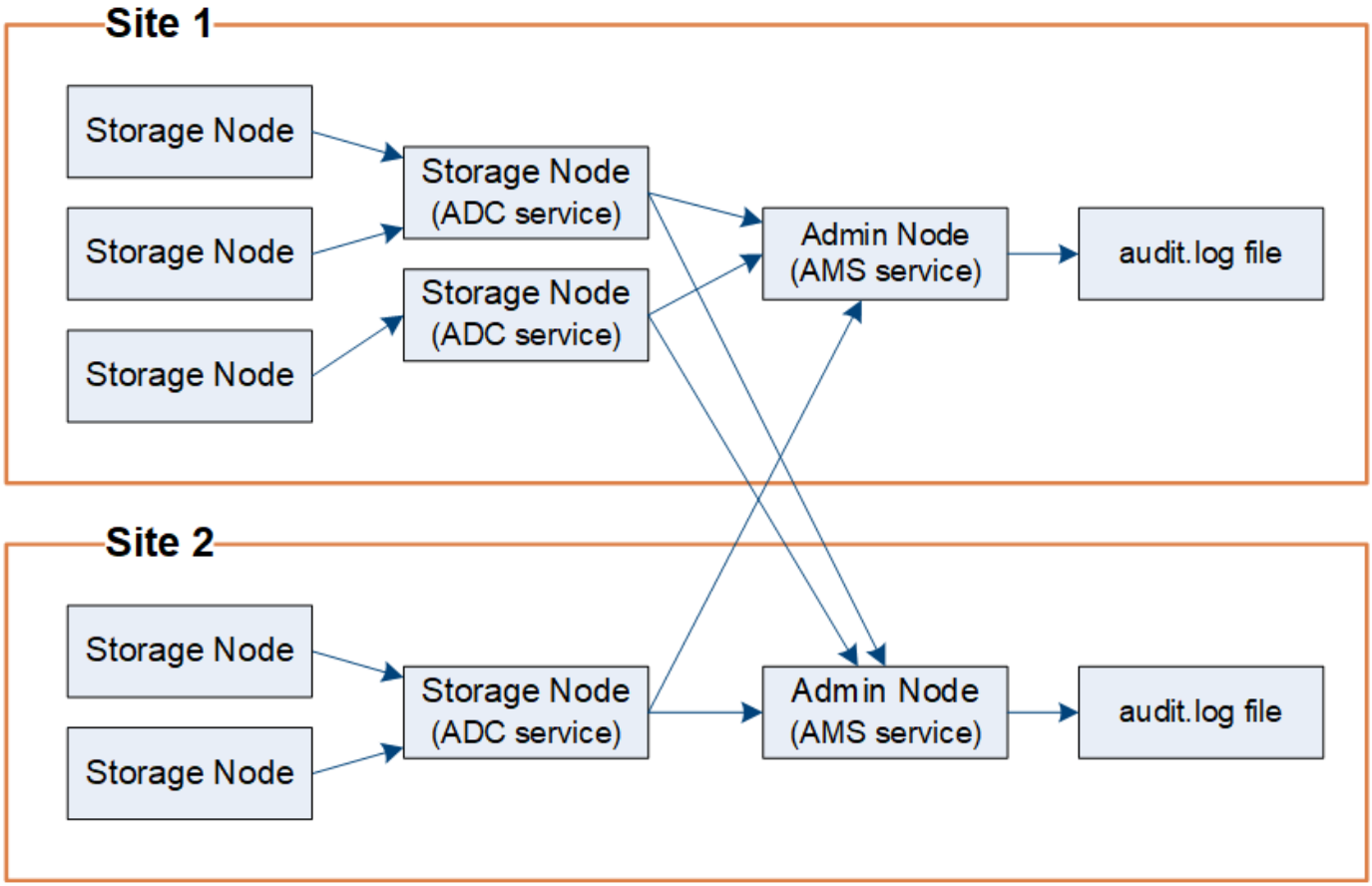
审核消息流

当 StorageGRID 配置为*管理节点/本地节点*或*管理节点和外部 syslog 服务器*时，审核消息由管理节点以及具有管理域控制器 (ADC) 服务的存储节点处理。

如审核消息流程图所示，每个 StorageGRID 节点都会将其审核消息发送到数据中心站点的 ADC 服务之一。ADC 服务将自动为每个站点上安装的前三个存储节点启用。

反过来，每个ADC服务都充当中继，并将其审计消息集合发送到StorageGRID系统中的每个管理节点，从而为每个管理节点提供系统活动的完整记录。

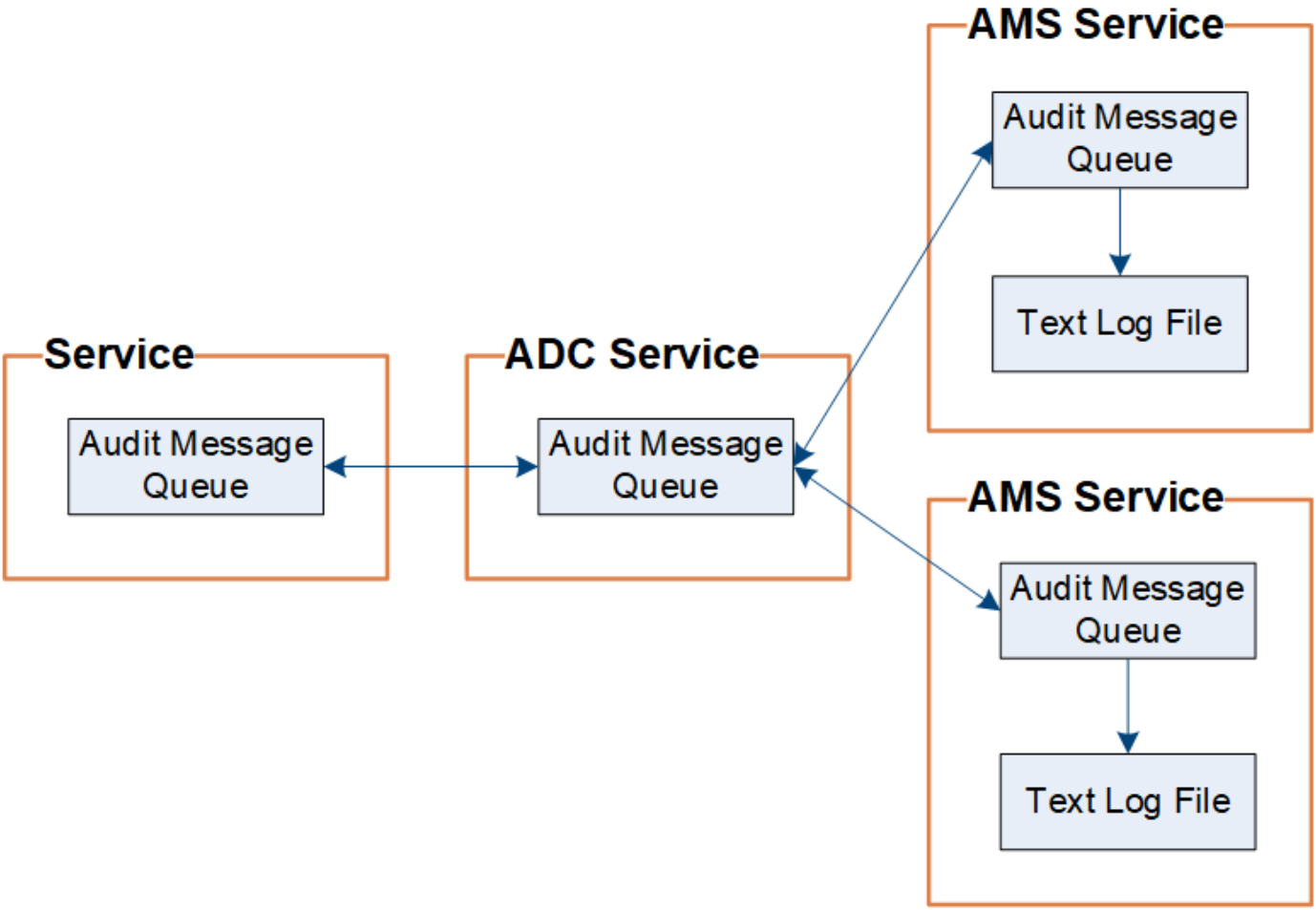
每个管理节点将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log`。



审核消息保留

StorageGRID 使用复制和删除流程，以确保审核消息在写入审核日志之前不会丢失。

当节点生成或中继审核消息时，该消息存储在网格节点系统磁盘上的审核消息队列中。消息的副本始终保存在审核消息队列中，直到消息被写入管理节点 `/var/local/audit/export`目录中的审核日志文件。这有助于防止在传输过程中丢失审核消息。



由于网络连接问题或审核容量不足，审核消息队列可能会暂时增加。随着队列的增加，它们会占用每个节点的`/var/local/`目录中更多的可用空间。如果问题仍然存在，且节点的审核消息目录已过满，则各个节点将优先处理其积压工作，并暂时无法接收新消息。

具体而言，您可能会看到以下行为：

- 如果管理节点使用 `/var/local/audit/export`的目录已满，则管理节点将被标记为不可用于新审核消息，直到目录不再满为止。S3 客户端请求不受影响。当审核存储库无法访问时，会触发 XAMS（无法访问的审核存储库）警报。
- 如果具有 ADC 服务的存储节点使用的 `/var/local/`目录已满 92%，则该节点将被标记为不可用于审核消息，直到目录仅满 87%。S3 客户端对其他节点的请求不受影响。当无法访问审核中继时，会触发 NRLY（可用审核中继）警报。

> 如果没有带有 ADC 服务的可用存储节点，则存储节点将审计消息本地存储在`/var/local/log/localaudit.log`文件中。

- 如果 Storage Node 使用的 `/var/local/`目录已满 `85%`，则该节点将开始拒绝 `S3` 客户端请求，并返回 `503 Service Unavailable`。

以下类型的问题可能导致审核消息队列增长非常大：

- 使用 ADC 服务的管理节点或存储节点的中断。如果系统的某个节点出现故障，则其余节点可能会出现积压。

- ${post_edited_translations.segment}
- ADC 存储节点上的 `/var/local/` 空间因与审计消息无关的原因而变满。发生这种情况时，该节点将停止接受新的审计消息，并优先处理其当前的积压工作，这可能会导致其他节点上出现积压。

${post_edited_translations.segment}

为了帮助您随时间监控审核消息队列的大小，当存储节点队列或管理节点队列中的消息数量达到特定阈值时，会触发 **Large audit queue** 警报和旧版 AMQS 警报。

${post_edited_translations.segment}

如果警报或警示持续存在且严重程度增加，请查看队列大小图表。如果该数值在数小时或数天内持续增加，则审计负载可能已超过系统的审计容量。通过将“Client Writes”（客户端写入）和“Client Reads”（客户端读取）的审计级别更改为“Error”（错误）或“Off”（关闭），可以降低客户端操作速率或减少记录的审计消息数量。请参见 "配置日志管理和外部 syslog 服务器"。

重复消息

如果发生网络或节点故障，StorageGRID 系统会采取保守的方法。因此，审核日志中可能会存在重复的消息。

从 StorageGRID 管理节点命令行访问审核日志文件

审核共享包含活动 `audit.log`文件和任何压缩的审核日志文件。您可以直接从管理节点的命令行访问审核日志文件。

除非您为 管理节点/本地节点 或 管理节点和外部 **syslog** 服务器 配置 StorageGRID，否则 `audit.log`文件将保持为空。有关详细信息，请参阅 "选择日志位置"。

开始之前

- 您有 "特定访问权限"。
- 您必须具有该 `Passwords.txt`文件。
- 您必须知道管理节点的 IP 地址。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。
2. ${post_edited_translations.segment}

   ```
   cd /var/local/audit/export/
   ```
3. ${post_edited_translations.segment}

了解 StorageGRID 中的审核日志文件轮换

如果 StorageGRID 配置为 **Admin Nodes/local nodes** 或 **Admin Node and external syslog server**，则审核日志文件将保存到 Admin Node 的 `/var/local/audit/export/`目录中。活动审核日志文件命名为 `audit.log`。

> 也可以更改审核日志的目标，并将审核信息发送到外部 syslog 服务器。配置外部 syslog 服务器时，将继续生成和存储审核记录的本地日志。请参阅 "配置审核消息和外部 syslog 服务器"。

每天一次，活动 `audit.log`文件将被保存，并启动一个新的 `audit.log`文件。已保存文件的名称以格式 `*yyyy-mm-dd.txt*`表示其保存时间。如果在一天内创建了多个审核日志，文件名将使用文件保存的日期，并附加一个数字，格式为 `*yyyy-mm-dd.txt.n*`。例如，`2018-04-15.txt`和 `2018-04-15.txt.1`是2018年4月15日创建和保存的第一个和第二个日志文件。

一天后，保存的文件将被压缩并重命名，格式为 *yyyy-mm-dd.txt.gz*，该格式保留原始日期。随着时间的推移，分配给审核日志的管理节点存储将被消耗。脚本监控审核日志空间消耗，并根据需要删除日志文件，以释放 `/var/local/audit/export/`目录中的空间。审核日志将根据其创建日期进行删除。最旧的日志将首先删除。您可以在以下文件中监视脚本的操作： `/var/local/log/manage-audit.log`。

此示例显示活动 `audit.log`文件、前一天的文件（`2018-04-15.txt`）和前一天的压缩文件(`2018-04-14.txt.gz`）。

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

审核日志文件格式

了解 **StorageGRID** 中审计日志文件的格式

审核日志文件位于每个管理节点上，包含各个审核消息的集合。

每条审核消息都包含以下内容：

- 触发审核消息 (ATIM) 的事件的协调世界时 (UTC)，采用 ISO 8601 格式，后跟空格：

  YYYY-MM-DDTHH:MM:SS.UUUUUU，其中 `*UUUUUU*`为微秒。

- 审核消息本身，括在方括号内并以 `AUDT`开头。

以下示例显示了审计日志文件中的三条审计消息（为可读性添加了换行符）。当租户创建 S3 存储桶并将两个对象添加到该存储桶时，会生成这些消息。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

在默认格式中，审核日志文件中的审核消息不容易阅读或解释。您可以使用 "audit-explain 工具" 获取审核日志中审核消息的简化摘要。您可以使用 "audit-sum 工具" 汇总记录了多少次写入、读取和删除操作以及这些操作花费了多长时间。

使用 **audit-explain** 工具翻译 **StorageGRID** 审核消息

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

开始之前

- 您有 "特定访问权限"。
- 您必须具有该 `Passwords.txt`文件。
- ${post_edited_translations.segment}

关于此任务

该 `audit-explain`工具位于主管理节点上，可在审计日志中提供审计消息的简化摘要。

> 该 `audit-explain` 工具主要供技术支持人员在故障排除操作期间使用。处理 `audit-explain` 查询可能会消耗大量的 CPU 资源，从而可能影响 StorageGRID 的运行。

此示例显示了 `audit-explain`工具的典型输出。当帐户 ID 为 92484777680322627870 的 S3 租户使用 S3 PUT 请求创建名为"bucket1"的存储桶并向该存储桶添加三个对象时，会生成这四个"SPUT"审核消息。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

该 `audit-explain`工具可以执行以下操作：

- 处理纯文本或压缩的审计日志。例如：

  ```
  audit-explain audit.log

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

- 同时处理多个文件。例如：

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- 接受来自管道的输入，这允许您使用 `grep` 命令或其他方式对输入进行过滤和预处理。例如：

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

由于审计日志可能非常大且解析速度较慢，您可以通过过滤要查看的部分并在这些部分（而不是整个文件）上运行 `audit-explain` 来节省时间。

该 `audit-explain`工具不接受压缩文件作为管道输入。要处理压缩文件，请提供其文件名作为命令行参数，或先使用 `zcat`工具解压缩文件。例如：

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

使用 `help (-h)`选项可查看可用选项。例如：

```
$ audit-explain -h
```

步骤

1. ${post_edited_translations.segment}
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。

2. 输入以下命令，其中 `/var/local/audit/export/audit.log` 表示您要分析的一个或多个文件的名称和位置：

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   该 `audit-explain`工具打印指定一个或多个文件中所有消息的人类可读解释。

   为了减少行长并提高可读性，默认情况下不显示时间戳。如果要查看时间戳，请使用 timestamp (`-t`) 选项。

使用 **audit-sum** 工具汇总 **StorageGRID** 审核消息

您可以使用该 `audit-sum`工具对写入、读取、标头和删除审核消息进行计数，并查看每种操作类型的最短、最大和平均时间（或大小）。

开始之前

- 您有 "特定访问权限"。
- 您拥有 `Passwords.txt` 文件。
- 您知道主管理节点的 IP 地址。

关于此任务

该 `audit-sum`工具可在主管理节点上使用，它汇总了记录的写入、读取和删除操作的数量以及这些操作所用的时间。

该 `audit-sum`工具主要供技术支持人员在故障排除操作期间使用。处理 `audit-sum`查询可能会消耗大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 `audit-sum`工具的典型输出。此示例显示了协议操作花费的时间。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

该 `audit-sum`工具在审核日志中提供以下 S3 和 ILM 审核消息的计数和时间。

> 审核代码将随功能弃用而从产品和文档中删除。如果遇到此处未列出的审核代码，请查看本主题的早期版本以了解较旧的 StorageGRID 版本。例如， "${post_edited_translations.segment}"。

代码	问题描述	请参阅
IDEL	ILM Initiated Delete：在 ILM 开始删除对象的过程时记录日志。	"IDEL：ILM Initiated Delete"
SDEL	S3 DELETE：记录成功删除对象或存储桶的事务。	"SDEL：S3 DELETE"
SGET	S3 GET：记录成功的事务以检索对象或列出存储桶中的对象。	"SGET：S3 GET"
SHEA	S3 HEAD：记录成功的事务以检查对象或存储桶是否存在。	"SHEA: S3 HEAD"
SPUT	S3 PUT：记录成功的事务以创建新对象或存储桶。	"SPUT：S3 PUT"

该 `audit-sum`工具可以执行以下操作：

- 处理纯文本或压缩的审计日志。例如：

```
audit-sum audit.log

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

- 同时处理多个文件。例如：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- 接受来自管道的输入，这允许您使用 `grep` 命令或其他方式对输入进行过滤和预处理。例如：

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> 此工具不接受压缩文件作为管道输入。要处理压缩文件，请提供其文件名作为命令行参数，或者先使用 `zcat` 工具解压缩文件。例如：
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

您可以使用命令行选项将存储区上的操作与对象上的操作分开汇总，或按存储区名称、时间段或目标类型对消息摘要进行分组。默认情况下，摘要显示最小、最大和平均操作时间，但您可以使用 `size (-s)`选项查看对象大小。

使用 `help (-h)`选项可查看可用选项。例如：

```
$ audit-sum -h
```

步骤

1. ${post_edited_translations.segment}
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。

2. 如果要分析与写入、读取、HEAD和DELETE操作相关的所有消息，请执行以下步骤：
   a. 输入以下命令，其中 `/var/local/audit/export/audit.log` 表示您要分析的一个或多个文件的名称和位置：

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      此示例显示了 `audit-sum`工具的典型输出。此示例显示了协议操作花费的时间。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

在此示例中，SGET（S3 GET）操作平均最慢，为 1.13 秒，但 SGET 和 SPUT（S3 PUT）操作都显示了约 1,770 秒的最坏情况时间。

b. 要显示最慢的 10 个检索操作，请使用 grep 命令仅选择 SGET 消息并添加 long 输出选项(`-l`）以包含对象路径：

```
grep SGET audit.log | audit-sum -l
```

${post_edited_translations.segment}

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
从此示例输出中，您可以看到三个最慢的 S3 GET 请求是针对大小约为 5 GB 的对象，比其他对象大得多。较大的大小导致最坏情况下的检索时间较慢。

3. 如果要确定从网格中摄取和检索的对象的大小，请使用大小选项(`-s`)：

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

在此示例中，SPUT 的平均对象大小低于 2.5 MB，但 SGET 的平均大小要大得多。SPUT 消息的数量远高于 SGET 消息的数量，这表明大多数对象从未被检索过。

4. 如果要确定昨天的检索速度是否很慢：

   a. 在相应的审核日志上运行该命令，并使用按时间分组选项 (`-gt`），后跟时间段（例如 15M、1H、10S ）：

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

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

这些结果表明，S3 GET 流量在 06:00 到 07:00 之间出现激增。在此时间段内，最大时间和平均时间均明显更高，并且它们并没有随着次数的增加而逐渐递增。这些指标表明容量已超出，可能是网络容量超限，也可能是网格处理请求的能力超限。

b. 要确定昨天每小时检索了哪些大小的对象，请向命令中添加大小选项 (`-s`)：

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

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

这些结果表明，当总体检索流量达到最大值时，会发生一些非常大的检索。

c. 要查看更多详细信息，请使用 "audit-explain 工具" 查看该小时内的所有 SGET 操作：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

如果 grep 命令的输出预计为多行，请添加 `less`命令，以每次一页（一个屏幕）的方式显示审核日志文件的内容。

5. 如果要确定存储桶上的 SPUT 操作是否比对象的 SPUT 操作慢：

a. 首先使用 `-go` 选项，该选项将对象和存储桶操作的消息分别进行分组：

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

${post_edited_translations.segment}

b. 要确定哪些存储桶的 SPUT 操作最慢，请使用 `-gb`选项，该选项按存储桶对消息进行分组：

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. 要确定哪些存储桶的 SPUT 对象大小最大，请同时使用 `-gb` 和 `-s` 选项：

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

审核消息格式

了解 **StorageGRID** 审核消息的结构

在 StorageGRID 系统内交换的审核消息包括所有消息通用的标准信息以及描述所报告事件或活动的特定内容。

如果"audit-explain"和"audit-sum"工具提供的摘要信息不足，请参阅本节以了解所有审计消息的一般格式。

下面是审核日志文件中可能出现的审核消息示例：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

每个审核消息都包含一个属性元素字符串。整个字符串用括号括起来(`[ ]`），字符串中的每个属性元素具有以下特点：

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

每个元素都包含以下格式报告的属性代码、数据类型和值：

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

消息中的属性元素数量取决于消息的事件类型。属性元素不按任何特定顺序列出。

以下列表描述了属性元素：

- `ATTR` 是所报告属性的四个字符的代码。有些属性是所有审计消息共有的，有些属性则是特定于事件的。
- `type` 是值编程数据类型的四个字符的标识符，例如 UI64、FC32 等。该类型用括号括起来 `( )`。
- `value` 是属性的内容，通常是数值或文本值。值始终跟在冒号 (`:` 后面）。数据类型为 CSTR 的值用双引号 " " 括起来。

StorageGRID 审核消息中的数据类型

不同的数据类型用于在审核消息中存储信息。

类型	问题描述
UI32	无符号长整数（32位）；它可以存储数字 0 到 4,294,967,295。
UI64	无符号双长整数（64 位）；它可以存储 0 到 18,446,744,073,709,551,615 的数字。
FC32	四字符常量；32 位无符号整数值，表示为四个 ASCII 字符，例如"ABCD"。
IPAD	用于 IP 地址。
CSTR	可变长度的 UTF-8 字符数组。字符可以使用以下约定进行转义： • 反斜杠为\\。 • 回车符为 \r。 • 双引号为\"。 • 换行符（新行）为 \n。 • 字符可以替换为其十六进制等效字符（格式为 \xHH，其中 HH 是表示该字符的十六进制值）。

StorageGRID 审核消息中的事件特定数据

审核日志中的每个审核消息都记录特定于系统事件的数据。

在用于标识消息本身的起始 `[AUDT:`容器之后，下一组属性将提供有关审计消息所描述的事件或操作的信息。以下示例中突出显示了这些属性：

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

The `ATYP` 元素（在示例中带下划线）标识生成消息的事件。此示例消息包括"SHEA"消息代码（[ATYP(FC32):SHEA]），表示它是由成功的 S3 HEAD 请求生成的。

StorageGRID 审核消息中的常见元素

所有审核消息都包含通用元素。

代码	类型	问题描述
AMID	FC32	模块 ID：生成消息的模块 ID 的四字符标识符。这表示生成审核消息的代码段。
ANID	UI32	节点 ID：分配给生成消息的服务的网格节点 ID。在配置和安装 StorageGRID 系统时，每个服务都会分配一个唯一标识符。此 ID 无法更改。
ASES	UI64	审核会话标识符：在以前的版本中，此元素指示服务启动后审核系统初始化的时间。此时间值以微秒为单位，自操作系统纪元（1970 年 1 月 1 日 00:00:00 UTC）起计算。 注： 此元素已过时，不再显示在审核消息中。
ASQN	UI64	序列计数：在以前的版本中，对于网格节点 (ANID) 上生成的每个审核消息，此计数器都会递增，并在服务重新启动时重置为零。 注： 此元素已过时，不再显示在审核消息中。
ATID	UI64	跟踪 ID：由单个事件触发的一组消息共享的标识符。

代码	类型	问题描述
ATIM	UI64	时间戳：触发审核消息的事件生成时间，以操作系统时期（1970 年 1 月 1 日 00:00:00 UTC）以来的微秒为单位。请注意，将时间戳转换为本地日期和时间的大多数可用工具基于毫秒。 可能需要对记录的时间戳进行四舍五入或截断。 `audit.log`文件中审核消息开头显示的人工可读时间是 `ISO 8601` 格式的 `ATIM` 属性。日期和时间表示为 `*YYYY-MMDDTHH:MM:SS.UUUUUU*`，其中 `T`是表示日期时间段开头的文字字符串字符。`*UUUUUU*`为微秒。
ATYP	FC32	事件类型：正在记录的事件的四字符标识符。这决定了消息的"有效负载"内容：包含的属性。
平均	UI32	版本：审核消息的版本。随着 StorageGRID 软件的发展，新版本的服务可能会在审计报告中加入新功能。此字段可在 AMS 服务中实现向后兼容性，以处理来自旧版本服务的消息。
RSLT	FC32	结果：事件、流程或事务的结果。如果与消息无关，则使用 NONE 而非 SUCS，以免意外过滤消息。

StorageGRID 审核消息格式和示例

您可以在每条审核消息中找到详细信息。所有审核消息都使用相同的格式。

以下是审计消息示例，该消息可能出现在 `audit.log`文件中：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

审核消息包含有关正在记录的事件的信息，以及有关审核消息本身的信息。

要识别审核消息记录的是哪个事件，请查找 ATYP 属性（下面突出显示）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性的值为 SPUT。"SPUT" 表示 S3 PUT 事务，该事务将对象的摄取记录到存储桶。

以下审核消息还显示了与对象关联的存储区：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

要发现 PUT 事件何时发生，请注意审核消息开头的通用协调时间 (UTC) 时间戳。此值是审核消息本身的 ATIM 属性的人类可读版本：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM记录自UNIX纪元开始以来的时间，以微秒为单位。在该示例中，该值 `1405631878959669`转换为2014年7月17日星期四 21:17:59 UTC。

审核消息和对象生命周期

在 **StorageGRID** 中生成审核消息时

每次摄入、检索或删除对象时，都会生成审计消息。您可以通过定位特定于 S3 API 的审计消息，在审计日志中识别这些交易。

${post_edited_translations.segment}

协议	代码
链接 S3 操作	S3BK（存储桶）、S3KY（密钥）或两者
链接内部操作	CBID（对象的内部标识符）

审核消息的时间安排

由于网格节点之间的时间差异、对象大小和网络延迟等因素，不同服务生成的审核消息的顺序可能与本节示例中所示的顺序不同。

StorageGRID 中对象摄取事务的审核消息

您可以通过查找 S3 API 特定的审核消息，在审核日志中识别客户端摄取事务。

并非在接收事务期间生成的所有审核消息都列在下表中。仅包括跟踪接收事务所需的消息。

S3 提取审核消息

代码	名称	问题描述	跟踪	请参见
SPUT	S3 PUT 事务	S3 PUT 摄取事务已成功完成。	CBID、S3BK、S3KY	"SPUT：S3 PUT"
ORLM	满足对象规则	已满足此对象的 ILM 策略。	CBID	"ORLM：Object Rules Met"

示例：**S3** 对象提取

以下一系列审核消息是当 S3 客户端将对象摄入到存储节点（LDR 服务）时生成并保存到审核日志中的审核消息的示例。

在此示例中，活动 ILM 策略包括 Make 2 Copies ILM 规则。

> 并非事务期间生成的所有审计消息都列在下面的示例中。仅列出与 S3 摄取事务 (SPUT) 相关的内容。

此示例假定先前已创建 S3 存储桶。

SPUT：S3 PUT

生成 SPUT 消息以指示已发出 S3 PUT 事务以在特定存储桶中创建对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM：Object Rules Met

ORLM 消息指示此对象已满足 ILM 策略。消息包括对象的 CBID 和应用的 ILM 规则的名称。

对于复制的对象，LOCS 字段包括对象位置的 LDR 节点 ID 和卷 ID。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

对于纠删码对象，LOCS 字段包括纠删码配置文件 ID 和纠删码组 ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

路径字段包括 S3 存储桶和密钥信息。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

StorageGRID 中对象删除事务的审核消息

您可以通过查找 S3 API 特定的审核消息，在审核日志中识别对象删除事务。

下表中未列出删除事务期间生成的所有审核消息。仅包括跟踪删除事务所需的消息。

S3 删除审核消息

代码	名称	问题描述	跟踪	请参见
SDEL	S3 删除	请求从存储桶中删除对象。	CBID, S3KY	"SDEL：S3 DELETE"

示例：**S3** 对象删除

当 S3 客户端从存储节点（LDR 服务）中删除对象时，会生成审核消息并保存到审核日志中。

> 并非删除事务期间生成的所有审核消息都列在下面的示例中。仅列出与 S3 删除事务 (SDEL) 相关的内容。

SDEL：S3 Delete

当客户端向 LDR 服务发送 DeleteObject 请求时，对象删除开始。消息包含要从中删除对象的存储桶和对象的 S3 Key，用于标识对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

您可以通过查找 S3 API 特定的审核消息，在审核日志中识别对象检索事务。

并非在检索事务期间生成的所有审核消息都会在下表中列出。仅包括跟踪检索事务所需的消息。

S3检索审核消息

代码	名称	问题描述	跟踪	请参见
SGET	S3 GET	从存储桶检索对象的请求。	CBID、S3BK、S3KY	"SGET：S3 GET"

示例：**S3** 对象检索

当 S3 客户端从存储节点（LDR 服务）检索对象时，会生成审核消息并保存到审核日志中。

请注意，并非所有在事务期间生成的审核消息都列在下面的示例中。仅列出与 S3 检索事务 (SGET) 相关的内容。

SGET：S3 GET

当客户端向 LDR 服务发送 GetObject 请求时，对象检索开始。消息包含从中检索对象的存储桶和对象的 S3 Key，用于标识对象。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

如果存储桶策略允许，客户端可以匿名检索对象，或者可以从不同租户帐户拥有的存储桶中检索对象。审核消息包含有关存储桶所有者租户帐户的信息，以便可以跟踪这些匿名和跨帐户请求。

在以下示例消息中，客户端发送 GetObject 请求，以获取存储在其不拥有的存储桶中的对象。SBAI 和 SBAC 的值记录存储桶所有者的租户帐户 ID 和名称，这与 S3AI 和 SACC 中记录的客户端租户帐户 ID 和名称不同。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

示例：**S3 Select** 对象

当 S3 客户端在对象上发出 S3 Select 查询时，将生成审核消息并保存到审核日志中。

请注意，并非所有在事务期间生成的审核消息都列在下面的示例中。仅列出与 S3 Select 事务（SelectObjectContent）相关的内容。

每个查询会生成两条审核消息：一条用于执行 S3 Select 请求的授权（S3SR 字段设置为 "select"），另一条是在处理过程中从存储中检索数据的后续标准 GET 操作。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

StorageGRID 中 **S3** 对象元数据更新的审核消息

当 S3 客户端更新对象的元数据时，系统会生成审核消息。

S3元数据更新审核消息

代码	名称	问题描述	跟踪	请参见
SUPD	S3 元数据已更新	当 S3 客户端更新已摄取对象的元数据时生成。	CBID、S3KY、HTRH	"SUPD：S3 元数据已更新"

示例：**S3** 元数据更新

此示例显示用于更新现有 S3 对象的元数据的成功事务。

SUPD: S3元数据更新

S3 客户端发出请求 (SUPD)，以更新 S3 对象 (S3KY) 的指定元数据(`x-amz-meta-*`。在此示例中，请求标头包含在 HTRH 字段中，因为它已配置为审核协议标头（*Configuration* > **Monitoring** > **Audit and syslog server**）。请参阅"配置日志管理和外部 syslog 服务器"。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

审核消息

了解 **StorageGRID** 中的审计消息类型和代码

以下各节列出了系统返回的审计消息的详细说明。每个审计消息首先在表格中列出，该表格按消息表示的活动类别对相关消息进行分组。这些分组对于了解被审计的活动类型以及选择所需的审计消息过滤类型都很有用。

审核消息还按其四个字符代码的字母顺序列出。通过此字母列表，您可以查找有关特定消息的信息。

本章中使用的四个字符代码是审计消息中找到的 ATYP 值，如下面的示例消息所示：

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

有关设置审核消息级别、更改日志目标以及使用外部 syslog 服务器获取审核信息的信息，请参见 "配置日志管理和外部 syslog 服务器"

审核消息类别

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

代码	消息标题和描述	请参见
ECMC	缺少擦除编码数据片段：表示检测到缺少擦除编码数据片段。	"ECMC：缺少擦除编码数据片段"
ECOC	损坏的擦除编码数据片段：表示检测到损坏的擦除编码数据片段。	"ECOC：损坏的擦除编码数据片段"
ETAF	安全身份验证失败：使用传输层安全 (TLS) 的连接尝试失败。	"ETAF：安全身份验证失败"
GNRG	${post_edited_translations.segment}	"GNRG: GNDS注册"
GNUR	GNDS注销：服务已从StorageGRID系统中注销。	"GNUR：GNDS 注销"
GTED	网格任务已结束：CMN 服务已完成处理网格任务。	"GTED：网格任务已结束"
GTST	网格任务已启动：CMN 服务已开始处理网格任务。	"${post_edited_translations.segment}"
GTSU	已提交网格任务：已将网格任务提交到 CMN 服务。	"GTSU：网格任务已提交"
LLST	${post_edited_translations.segment}	"LLST：位置丢失"
OLST	对象丢失：无法在 StorageGRID 系统中找到请求的对象。	"OLST：系统检测到丢失对象"
SADD	安全审核禁用：已关闭审核消息日志记录。	"SADD：安全审核禁用"
${post_edited_translations.segment}	安全审核启用：已还原审核消息日志记录。	"SADE：启用安全审计"
SVRF	对象存储验证失败：内容块验证检查失败。	"SVRF：对象存储验证失败"
SVRU	对象存储验证未知：在对象存储中检测到意外的对象数据。	"SVRU：对象存储验证未知"
SYSD	${post_edited_translations.segment}	"SYSD：节点停止"
SYST	节点停止：服务已启动正常停止。	"SYST：节点停止"

代码	消息标题和描述	请参见
SYSU	节点启动：服务已启动；消息中显示了上一次关闭的性质。	"SYSU：节点启动"

StorageGRID 中对象存储事件的审核消息

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

审核代码将随功能弃用而从产品和文档中删除。如果您遇到此处未列出的审核代码，请查看本主题的早期版本以获取较旧的 SG 版本信息。例如， "StorageGRID 11.8 对象存储审核消息"。

代码	问题描述	请参见
BROR	存储区只读请求：存储区进入或退出只读模式。	"BROR：Bucket 只读请求"
CBSE	对象发送结束：源实体完成了从网格节点到网格节点的数据传输操作。	"CBSE：对象发送结束"
CBRE	对象接收结束：目标实体完成了网格节点到网格节点的数据传输操作。	"CBRE：对象接收端"
CGRR	跨网格复制请求：StorageGRID 尝试进行跨网格复制操作，以在网格联合连接中的存储桶之间复制对象。	"CGRR：跨网格复制请求"
EBDL	空存储桶删除：ILM 扫描程序删除了一个存储桶中的对象，该存储桶正在删除所有对象（执行清空存储桶操作）。	"EBDL：空桶删除"
${post_edited_translations.segment}	空桶请求：用户发送了打开或关闭清空存储桶的请求（即删除存储桶对象或停止删除对象）。	"EBKR：空存储桶请求"
${post_edited_translations.segment}	${post_edited_translations.segment}	"${post_edited_translations.segment}"
${post_edited_translations.segment}	对象存储删除：内容块已从网格节点中删除，无法再直接请求。	"SREM：对象存储删除"

StorageGRID 中客户端读取操作的审核消息

当 S3 客户端应用程序请求检索对象时，将记录客户端读取审核消息。

代码	问题描述	使用者	请参见
S3SL	S3 Select 请求：记录 S3 Select 请求返回到客户端后的完成情况。S3SL 消息可以包括错误消息和错误代码详细信息。请求可能未成功。	S3客户端	"S3SL: S3 Select 请求"
SGET	S3 GET：记录成功的事务以检索对象或列出存储桶中的对象。 注意： 如果事务在子资源上操作，则审核消息将包括字段 S3SR。	S3客户端	"SGET：S3 GET"
SHEA	S3 HEAD：记录成功的事务以检查对象或存储桶是否存在。	S3客户端	"SHEA: S3 HEAD"

StorageGRID 中客户端写入操作的审核消息

当 S3 客户端应用程序请求创建或修改对象时，将记录客户端写入审核消息。

代码	问题描述	使用者	请参见
OVWR	对象覆盖：记录事务以用另一个对象覆盖一个对象。	S3客户端	"OVWR：对象覆盖"
SDEL	S3 DELETE：记录成功删除对象或存储桶的事务。 注意： 如果事务在子资源上操作，则审核消息将包括字段 S3SR。	S3客户端	"SDEL：S3 DELETE"
SPOS	S3 POST：记录成功的事务以将对象从 AWS Glacier 存储还原到 Cloud Storage Pool。	S3客户端	"SPOS：S3 POST"
SPUT	S3 PUT：记录成功的事务以创建新对象或存储桶。 注意： 如果事务在子资源上操作，则审核消息将包括字段 S3SR。	S3客户端	"SPUT：S3 PUT"
SUPD	S3 Metadata Updated：记录成功更新现有对象或存储桶元数据的事务。	S3客户端	"SUPD：S3 元数据已更新"

StorageGRID 管理审核消息

"管理"类别将用户请求记录到管理 API。

代码	消息标题和描述	请参见
${post_edited_translations.segment}	Management API 审核消息：用户请求的日志。	"${post_edited_translations.segment}"

StorageGRID ILM 审核消息

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

代码	消息标题和描述	请参见
IDEL	ILM Initiated Delete：此审核消息在 ILM 开始删除对象的过程时生成。	"IDEL：ILM Initiated Delete"
LKCU	覆盖的对象清理。自动删除覆盖的对象以释放存储空间时会生成此审核消息。	"LKCU：覆盖对象清理"
ORLM	符合对象规则：此审核消息在按照 ILM 规则指定存储对象数据时生成。	"ORLM：Object Rules Met"

审核消息参考

StorageGRID 中存储桶只读请求的 BROR 审核消息

当存储区进入或退出只读模式时，LDR 服务会生成此审核消息。例如，在删除所有对象时，存储区进入只读模式。

代码	字段	问题描述
BKHD	存储桶 UUID	存储桶 ID。
BROV	存储区只读请求值	存储桶是否处于只读状态或正在退出只读状态（1 = 只读，0 = 非只读）。
BROS	存储桶只读原因	存储区被设为只读或离开只读状态的原因。例如，emptyBucket。
S3AI	S3租户帐户ID	发送请求的租户帐户的 ID。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储桶名称。

StorageGRID 中对象接收开始的 CBRB 审核消息

在正常系统运行期间，随着数据的访问、复制和保留，内容块在不同节点之间不断传输。当从一个节点向另一个节点传输内容块时，此消息由目标实体发出。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。
CTES	预期结束序列计数	指示请求的最后一个序列计数。如果成功，则在接收到此序列计数时认为传输已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS：已成功开始传输。

此审核消息表示在单个内容上启动了节点到节点的数据传输操作，由其内容块标识符标识。操作请求从"Start Sequence Count"到"Expected End Sequence Count"的数据。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流，并与存储审计消息相结合，以验证副本计数。

StorageGRID 中对象接收结束的 **CBRE** 审核消息

当从一个节点到另一个节点的内容块传输完成时，此消息由目标实体发出。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。

代码	字段	问题描述
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示开始传输的序列计数。
CTAS	实际结束序列计数	指示上次成功传输的序列计数。如果实际结束序列计数与开始序列计数相同，且传输结果不成功，则未交换任何数据。
RSLT	传输结果	传输操作的结果（从发送实体的角度）： SUCS：已成功完成传输；已发送所有请求的序列计数。 CONL：传输过程中连接丢失 CTMO：建立或传输期间连接超时 UNRE：目标节点 ID 无法访问 CRPT：由于接收到损坏或无效的数据而终止传输

此审核消息表示节点到节点的数据传输操作已完成。如果传输结果成功，则操作将数据从"开始序列计数"传输到"实际结束序列计数"。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流并定位、制表和分析错误。与存储审核消息结合使用时，还可用于验证副本计数。

StorageGRID 中对象发送开始的 **CBSB** 审核消息

在正常系统运行期间，随着数据的访问、复制和保留，内容块在不同节点之间不断传输。当从一个节点向另一个节点传输内容块时，此消息由源实体发出。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。

代码	字段	问题描述
CTES	预期结束序列计数	指示请求的最后一个序列计数。如果成功，则在接收到此序列计数时认为传输已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS：已成功开始传输。

此审核消息表示在单个内容上启动了节点到节点的数据传输操作，由其内容块标识符标识。操作请求从"Start Sequence Count"到"Expected End Sequence Count"的数据。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流，并与存储审计消息相结合，以验证副本计数。

StorageGRID 中对象发送结束的 **CBSE** 审核消息

当内容块从一个节点转移到另一个节点的操作完成时，源实体将发出此消息。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示开始传输的序列计数。
CTAS	实际结束序列计数	指示上次成功传输的序列计数。如果实际结束序列计数与开始序列计数相同，且传输结果不成功，则未交换任何数据。

代码	字段	问题描述
RSLT	传输结果	传输操作的结果（从发送实体的角度）： SUCS：已成功完成传输；已发送所有请求的序列计数。 CONL：传输过程中连接丢失 CTMO：建立或传输期间连接超时 UNRE：目标节点 ID 无法访问 CRPT：由于接收到损坏或无效的数据而终止传输

此审核消息表示节点到节点的数据传输操作已完成。如果传输结果成功，则操作将数据从"开始序列计数"传输到"实际结束序列计数"。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流并定位、制表和分析错误。与存储审核消息结合使用时，还可用于验证副本计数。

StorageGRID 中跨网格复制请求的 **CGRR** 审核消息

当 StorageGRID 尝试跨网格复制操作以在网格联合连接中的存储桶之间复制对象时，将生成此消息。

代码	字段	问题描述
CSIZ	对象大小	对象的大小（以字节为单位）。 CSIZ 属性已在 StorageGRID 11.8 中引入。因此，跨 StorageGRID 11.7 到 11.8 升级的跨网格复制请求的总对象大小可能不准确。
S3AI	S3租户帐户ID	拥有从中复制对象的存储桶的租户帐户的 ID。
GFID	网格联合连接 ID	用于跨网格复制的网格联合连接的 ID。
OPER	CGR操作	尝试的跨网格复制操作类型： • 0 = 复制对象 • 1 = 复制多部分对象 • 2 = 复制删除标记
S3BK	S3 存储分段	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。
VSID	版本 ID	正在复制的对象的特定版本的版本 ID。

代码	字段	问题描述
RSLT	结果代码	返回成功(SUCS)或一般错误(GERR)。

StorageGRID 中空存储桶对象删除的 **EBDL** 审核消息

ILM 扫描程序删除了一个存储桶中的对象，该存储桶正在删除所有对象（执行清空存储桶操作）。

代码	字段	问题描述
CSIZ	对象大小	对象的大小（以字节为单位）。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
SEGC	容器UUID	分段对象的容器的 UUID。此值仅在对象已分段时可用。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
RSLT	删除操作的结果	事件、流程或事务的结果。如果与消息无关，则使用 NONE 而不是 SUCS，以免意外过滤消息。

StorageGRID 中空存储桶请求的 **EBKR** 审核消息

此消息表示用户发送了打开或关闭空存储桶的请求（即删除存储桶对象或停止删除对象）。

代码	字段	问题描述
BUID	存储桶 UUID	存储桶 ID。
EBJS	空的 Bucket JSON 配置	包含表示当前 Empty Bucket 配置的 JSON。
S3AI	S3租户帐户ID	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。

StorageGRID 中缺失纠删码数据的 **ECMC** 审计消息

此审核消息指示系统检测到缺失的擦除编码数据片段。

代码	字段	问题描述
VCMC	VCS ID	包含丢失区块的VCS的名称。

代码	字段	问题描述
MCID	区块ID	缺少的擦除编码片段的标识符。
RSLT	结果	此字段的值为"NONE"。RSLT 是必填消息字段，但与此特定消息无关。使用"NONE"而不是"SUCS"，因此不会过滤此消息。

StorageGRID 中损坏的纠删编码数据的 **ECOC** 审核消息

此审核消息指示系统已检测到损坏的擦除编码数据片段。

代码	字段	问题描述
VCCO	VCS ID	包含损坏区块的 VCS 的名称。
VLID	Volume ID	包含损坏的纠删编码片段的 RangeDB 卷。
CCID	区块ID	损坏的擦除编码片段的标识符。
RSLT	结果	此字段的值为"NONE"。RSLT 是必填消息字段，但与此特定消息无关。使用"NONE"而不是"SUCS"，因此不会过滤此消息。

StorageGRID 中安全身份验证失败的 **ETAF** 审核消息

当使用传输层安全性 (TLS) 的连接尝试失败时，将生成此消息。

代码	字段	问题描述
CNID	连接标识符	身份验证失败的 TCP/IP 连接的唯一系统标识符。
RUID	用户身份	表示远程用户标识的服务相关标识符。

代码	字段	问题描述
RSLT	原因代码	故障原因： SCNI：安全连接建立失败。 CERM：证书缺失。 CERT：证书无效。 CERE：证书已过期。 CERR：证书已被吊销。 CSGN：证书签名无效。 CSGU：证书签名者未知。 UCRM：用户凭据缺失。 UCRI：用户凭据无效。 UCRU：不允许使用用户凭据。 TOUT：身份验证超时。

建立与使用 TLS 的安全服务的连接后，将使用 TLS 配置文件和内置于服务中的其他逻辑来验证远程实体的凭据。如果此身份验证由于无效、意外或不允许的证书或凭据而失败，则会记录审核消息。这样可以查询未经授权的访问尝试和其他与安全相关的连接问题。

该消息可能源于远程实体配置不正确，或者源于尝试向系统呈现无效或不允许的凭据。应监控此审核消息，以检测尝试获取对系统的未经授权访问的行为。

StorageGRID 中 GNDS 注册的 GNRG 审核消息

当服务在 StorageGRID 系统中更新或注册了有关自身的信息时，CMN 服务会生成此审核消息。

代码	字段	问题描述
RSLT	结果	更新请求的结果： • SUCS：成功 • SUNV：服务不可用 • GERR：其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID。
GNTP	设备类型	网格节点的设备类型（例如，LDR 服务的 BLDR）。

代码	字段	问题描述
GNDV	设备型号版本	标识 DMDL 捆绑包中网格节点的设备模型版本的字符串。
GNGP	组	网格节点所属的组（在链接成本和服务查询排名的上下文中）。
GNIA	IP 地址	网格节点的 IP 地址。

每当网格节点更新其在网格节点捆绑包中的条目时，都会生成此消息。

StorageGRID 中 **GNDS** 注销的 **GNUR** 审核消息

当服务从 StorageGRID 系统注销其自身相关信息时，CMN 服务将生成此审核消息。

代码	字段	问题描述
RSLT	结果	更新请求的结果： • SUCS：成功 • SUNV：服务不可用 • GERR：其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID。

StorageGRID 中已结束网格任务的 **GTED** 审核消息

此审核消息指示 CMN 服务已完成处理指定的网格任务并将任务移至历史表。如果结果为 SUCS、ABRT 或 ROLF，则会出现相应的 Grid Task Started 审核消息。其他结果表明，此网格任务的处理从未开始。

代码	字段	问题描述
TSID	任务 ID	此字段唯一标识生成的网格任务，并允许在其生命周期内管理网格任务。 注意： 任务 ID 在生成网格任务时分配，而不是在提交网格任务时分配。给定的网格任务可以多次提交，在这种情况下，"任务 ID"字段不足以唯一链接"已提交"、"已开始"和"已结束"审核消息。

代码	字段	问题描述
RSLT	结果	网格任务的最终状态结果： • SUCS：已成功完成网格任务。 • ABRT：网格任务已终止，没有回滚错误。 • ROLF：网格任务已终止，无法完成回滚过程。 • CANC：网格任务在启动前已被用户取消。 • EXPR:网格任务在启动前已过期。 • IVLD：网格任务无效。 • AUTH：网格任务未授权。 • DUPL：网格任务因重复而被拒绝。

StorageGRID 中已启动网格任务的 **GTST** 审核消息

此审计消息指示 CMN 服务已开始处理指定的网格任务。对于由内部网格任务提交服务启动并选择自动激活的网格任务，审计消息紧跟在网格任务提交消息之后。对于提交到"挂起"表的网格任务，此消息在用户启动网格任务时生成。

代码	字段	问题描述
TSID	任务 ID	此字段唯一标识生成的网格任务，并允许在其生命周期内管理任务。 注意： 任务 ID 在生成网格任务时分配，而不是在提交网格任务时分配。给定的网格任务可以多次提交，在这种情况下，"任务 ID"字段不足以唯一链接"已提交"、"已开始"和"已结束"审核消息。
RSLT	结果	结果。此字段只有一个值： • SUCS：已成功启动网格任务。

StorageGRID 中已提交网格任务的 **GTSU** 审核消息

此审核消息表示已将网格任务提交到 CMN 服务。

代码	字段	问题描述
TSID	任务 ID	唯一标识生成的网格任务，并允许在其生命周期内管理任务。 注意： 任务 ID 在生成网格任务时分配，而不是在提交网格任务时分配。给定的网格任务可以多次提交，在这种情况下，"任务 ID"字段不足以唯一链接"已提交"、"已开始"和"已结束"审核消息。
TTYP	任务类型	网格任务的类型。

代码	字段	问题描述
TVER	任务版本	表示网格任务版本的数字。
TDSC	任务说明	网格任务的人工可读说明。
VATS	在时间戳之后有效	网格任务有效的最早时间（从 1970 年 1 月 1 日起的 UINT64 微秒 - UNIX 时间）。
VBTS	有效期截止时间戳	网格任务有效的最新时间（从 1970 年 1 月 1 日起的 UINT64 微秒 - UNIX 时间）。
TSRC	源	任务的源： • TXTB：网格任务通过 StorageGRID 系统作为签名文本块提交。 • 网格：网格任务已通过内部网格任务提交服务提交。
ACTV	激活类型	激活类型： • AUTO: 网格任务已提交以进行自动激活。 • PEND：网格任务已提交到挂起表中。这是 TXTB 源唯一的可能性。
RSLT	结果	提交结果： • SUCS：网格任务已成功提交。 • 失败：此任务已直接移至历史记录表。

StorageGRID 中 **ILM** 启动删除的 **IDEL** 审核消息

此消息在 ILM 开始删除对象的过程时生成。

在以下任何一种情况下都会生成IDEL消息：

- 对于合规 **S3** 存储桶中的对象：当 ILM 开始自动删除对象的过程时，会生成此消息，因为其保留期已过期（假设已启用自动删除设置且法律保留已关闭）。
- 对于不合规 **S3** 存储桶中的对象。此消息在 ILM 开始删除对象的过程时生成，因为当前活动 ILM 策略中没有放置指令适用于该对象。

代码	字段	问题描述
CBID	内容块标识符	对象的CBID。
${post_edited_translations.segment}	${post_edited_translations.segment}	仅适用于合规 S3 存储桶中的对象。0（false）或 1（true），表示合规对象的保留期结束时是否应自动删除，除非存储桶处于合法冻结状态。

代码	字段	问题描述
CMPL	合规性：法律保留	仅适用于合规 S3 存储桶中的对象。0 (false) 或 1 (true)，指示存储桶当前是否处于合法冻结状态。
CMPR	合规性：保留期限	仅适用于合规 S3 存储桶中的对象。对象保留期的长度（以分钟为单位）。
CTME	合规性：采集时间	仅适用于合规 S3 存储桶中的对象。对象的摄取时间。您可以将保留期（以分钟为单位）添加到此值，以确定何时可以从存储桶中删除对象。
DMRK	删除标记版本 ID	从版本化存储桶中删除对象时创建的删除标记的版本 ID。存储桶上的操作不包括此字段。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOCS	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，它已被删除），则 LOCS 的值为""。 CLEC：对于纠删码对象，应用于对象数据的纠删码配置文件 ID 和纠删码组 ID。 CLDI：对于复制对象，LDR 节点 ID 和对象位置的卷 ID。 CLNL：如果对象数据已存档，则为对象位置的 ARC 节点 ID。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
RSLT	结果	ILM 操作的结果。 SUCS：ILM 操作成功。
规则	规则标签	• 如果合规 S3 存储桶中的对象由于其保留期已过期而被自动删除，则此字段为空。 • 如果由于当前没有适用于该对象的放置指令而正在删除该对象，则此字段显示最后一个适用于该对象的 ILM 规则的可读标签。
SGRP	站点（组）	如果存在，则对象已在指定站点被删除，该站点不是接收对象的站点。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中覆盖对象清理的 **LKCU** 审核消息

此消息是在 StorageGRID 删除先前需要清理以释放存储空间的已覆盖对象时生成的。当

S3 客户端将对象写入已包含对象的路径时，对象将被覆盖。删除过程会自动在后台执行。

代码	字段	问题描述
CSIZ	内容大小	对象的大小（以字节为单位）。
LTYP	清理类型	仅供内部使用。
LUID	已删除对象 UUID	已删除的对象的标识符。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
SEGC	容器UUID	分段对象的容器的 UUID。此值仅在对象已分段时可用。
UUID	通用唯一标识符	仍然存在的对象的标识符。此值仅在对象未被删除时可用。

StorageGRID 中泄漏对象清理的 LKDM 审计消息

当已清理或删除泄漏的区块时，将生成此消息。区块可以是复制对象或擦除编码对象的一部分。

代码	字段	问题描述
CLOC	区块位置	已删除的已泄露区块的文件路径。

CTYP	区块类型	区块类型：
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

代码	字段	问题描述

LTYP	泄漏类型	可检测到的五种泄漏类型：
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	区块创建时间	创建泄漏块的时间。
UUID	通用唯一标识符	${post_edited_translations.segment}
CBID	内容块标识符	泄漏区块所属对象的 CBID。
CSIZ	内容大小	区块的大小（以字节为单位）。

StorageGRID 中丢失对象副本位置的 **LLST** 审核消息

每当找不到对象副本（复制或擦除编码）的位置时，都会生成此消息。

代码	字段	问题描述
CBIL	CBID	受影响的CBID。
ECPR	纠删码配置文件	用于擦除编码对象数据。使用的擦除编码配置文件的 ID。
LTYP	位置类型	CLDI（在线）：用于复制对象数据 CLEC（在线）：用于擦除编码对象数据 CLNL（近线）：用于已存档的复制对象数据
NOID	源节点 ID	丢失位置的节点 ID。

代码	字段	问题描述
PCLD	复制对象的路径	丢失对象数据的磁盘位置的完整路径。仅当 LTYP 的值为 CLDI 时（即对于复制对象）才返回。 格式为 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	结果	始终为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，因此不会过滤此消息。
TSRC	触发源	USER: 用户已触发 SYST：系统触发
UUID	通用唯一ID	${post_edited_translations.segment}

StorageGRID 中管理 **API** 请求的 **MGAU** 审核消息

管理类别将用户请求记录到 Management API。每个向有效 API URI 发出的非 GET 或 HEAD 的 HTTP 请求都会记录包含用户名、IP 和 API 请求类型的响应。无效的 API URI（如 /api/v3-authorize）以及向有效 API URI 发出的无效请求不会被记录。

代码	字段	问题描述
MDIP	目标 IP 地址	服务器（目标）IP 地址。
MDNA	域名	主机域名。
${post_edited_translations.segment}	请求路径	请求路径。
MPQP	请求查询参数	请求的查询参数。
MRBD	请求正文	请求正文的内容。默认情况下会记录响应正文，但在某些情况下，当响应正文为空时，会记录请求正文。由于响应正文中没有以下信息，因此它是从以下 POST 方法的请求正文中获取的： • **POST authorize** 中的用户名和帐户 ID • **POST /grid/grid-networks/update** 中的新子网配置 • **POST /grid/ntp-servers/update** 中的新 NTP 服务器 • **POST /grid/servers/decommission** 中已停用的服务器 ID 注意： 敏感信息将被删除（例如 S3 访问密钥）或用星号掩盖（例如密码）。

代码	字段	问题描述
${post_edited_translations.segment}	请求方法	${post_edited_translations.segment} • POST • PUT • DELETE • PATCH
MRSC	响应代码	${post_edited_translations.segment}
MRSP	响应正文	默认情况下会记录响应的内容（响应正文）。 注意： 敏感信息将被删除（例如 S3 访问密钥）或用星号掩盖（例如密码）。
MSIP	${post_edited_translations.segment}	客户端（源） IP 地址。
MUUN	用户 URN	发送请求的用户的 URN（统一资源名称）。
RSLT	结果	返回成功(SUCS)或后端报告的错误。

StorageGRID 中系统检测到丢失对象的 **OLST** 审核消息

当 DDS 服务无法在 StorageGRID 系统中找到任何对象副本时，将生成此消息。

代码	字段	问题描述
CBID	内容块标识符	丢失对象的 CBID。
NOID	节点 ID	如果可用，则为丢失对象的最后已知直接或近线位置。如果卷信息不可用，则可以仅具有无卷 ID 的节点 ID。
路径	S3 存储桶/键	如果有，请提供 S3 存储桶名称和 S3 密钥名称。
RSLT	结果	此字段的值为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，以确保此消息不会被过滤。
UUID	通用唯一ID	StorageGRID 系统中丢失对象的标识符。
VOLI	Volume ID	如果可用，则为丢失对象的最后已知位置的存储节点的卷 ID。

${post_edited_translations.segment}

如果策略中的其他规则使用"对象大小"高级筛选器，则根据默认的"生成 2 个副本"规则成功存储对象时，不会生成 ORLM 消息。

代码	字段	问题描述
BUID	${post_edited_translations.segment}	Bucket ID 字段。用于内部操作。仅在 STAT 为 PRGD 时出现。
CBID	内容块标识符	对象的CBID。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOCS	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，它已被删除），则 LOCS 的值为"。 CLEC：对于纠删码对象，应用于对象数据的纠删码配置文件 ID 和纠删码组 ID。 CLDI：对于复制对象，LDR 节点 ID 和对象位置的卷 ID。 CLNL：如果对象数据已存档，则为对象位置的 ARC 节点 ID。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
RSLT	结果	ILM 操作的结果。 SUCS：ILM 操作成功。
规则	规则标签	${post_edited_translations.segment}
SEGC	容器UUID	分段对象的容器的 UUID。此值仅在对象已分段时可用。
${post_edited_translations.segment}	容器 CBID	分段对象的容器的 CBID。此值仅适用于分段和多部分对象。

代码	字段	问题描述
STAT	状态	ILM 操作的状态。 完成：针对对象的 ILM 操作已完成。 DFER：此对象已标记为将来的 ILM 重新评估。 PRGD：已从 StorageGRID 系统中删除此对象。 NLOC：无法再在 StorageGRID 系统中找到对象数据。此状态可能表示对象数据的所有副本都丢失或损坏。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在版本化存储桶中创建的新对象的版本 ID。对未版本化存储桶中的存储桶和对象的操作不包括此字段。

可以为单个对象多次发出 ORLM 审核消息。例如，每当发生以下事件之一时，就会发出此通知：

- 永远满足对象的 ILM 规则。
- 此纪元满足对象的 ILM 规则。
- ILM规则已删除该对象。
- 后台验证过程检测到已复制对象数据的副本已损坏。StorageGRID 系统执行 ILM 评估以替换损坏的对象。

相关信息

- "对象摄取事务"
- "对象删除事务"

StorageGRID 中对象覆写的 **OVWR** 审核消息

当外部（客户端请求）操作导致一个对象被另一个对象覆盖时，会生成此消息。

代码	字段	问题描述
CBID	内容块标识符（新增）	新对象的CBID。
CSIZ	上一个对象大小	要覆盖的对象的大小（以字节为单位）。
OCBD	内容块标识符（上一个）	上一个对象的CBID。
UUID	通用唯一ID (新增)	StorageGRID 系统中新对象的标识符。

代码	字段	问题描述
OUID	通用唯一 ID（以前）	StorageGRID 系统中上一个对象的标识符。
路径	S3 对象路径	用于上一个对象和新对象的S3对象路径
RSLT	结果代码	对象覆盖事务的结果。结果始终为： SUCS：成功
SGRP	站点（组）	如果存在，则在指定站点上删除被覆盖的对象，该站点不是接收被覆盖对象的站点。

StorageGRID 中 **S3 Select** 请求的 **S3SL** 审核消息

此消息记录 S3 Select 请求返回到客户端后的完成情况。S3SL 消息可以包括错误消息和错误代码详细信息。请求可能未成功。

代码	字段	问题描述
BYSC	扫描的字节数	从存储节点扫描（接收）的字节数。 如果对象被压缩，BYSC 和 BYPR 可能不同。如果对象被压缩，BYSC 将包含压缩字节数，BYPR 将是解压缩后的字节数。
BYPR	已处理字节数	已处理的字节数。指示 S3 Select 作业实际处理或操作的"Bytes Scanned"字节数。
BYRT	返回的字节数	S3 Select 作业返回到客户端的字节数。
REPR	已处理的记录	S3 Select 作业从存储节点接收的记录或行数。
RERT	返回的记录	S3 Select 作业返回到客户端的记录或行数。
JOFI	作业已完成	指示 S3 Select 作业是否已完成处理。如果为 false，则作业无法完成，错误字段可能包含数据。客户端可能收到了部分结果，或者根本没有结果。
REID	请求 ID	S3 Select 请求的标识符。
EXTM	执行时间	S3 Select 作业完成所需的时间（以秒为单位）。
ERMG	错误消息	S3 Select 作业生成的错误消息。
ERTY	错误类型	S3 Select 作业生成的错误类型。

代码	字段	问题描述
ERST	错误堆栈跟踪	S3 Select 作业生成的错误堆栈跟踪。
S3BK	S3 存储分段	S3 存储桶名称。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的 S3 访问密钥 ID。
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。

StorageGRID 中安全审核禁用的 SADD 审核消息

此消息指示原始服务（节点 ID）已关闭审核消息日志记录。StorageGRID 不再收集或传递审核消息。

代码	字段	问题描述
AETM	启用方法	用于禁用审核的方法。
AEUN	用户名	执行命令以禁用审核日志记录的用户名。
RSLT	结果	此字段的值为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，以确保此消息不会被过滤。

该消息暗示日志记录以前已启用，但现在已被禁用。这通常仅在批量摄取时使用，以提高系统性能。在批量活动之后，将恢复审核（SADE），然后永久阻止禁用审核的功能。

StorageGRID 中启用安全审核的 SADE 审核消息

此消息指示发起服务（节点 ID）已恢复审核消息日志记录。StorageGRID 再次收集和传递审核消息。

代码	字段	问题描述
AETM	启用方法	用于启用审核的方法。
AEUN	用户名	执行命令以启用审核日志记录的用户名。
RSLT	结果	此字段的值为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，以确保此消息不会被过滤。

该消息暗示日志记录以前被禁用（SADD），但现在已恢复。这通常仅用于批量载入以提高系统性能。在批量活

动之后，将恢复审核，然后永久阻止禁用审核的功能。

StorageGRID 中对象存储提交的 SCMT 审核消息

在提交之前（即持久存储之前），网格内容不会被提供或识别为已存储。持久存储的内容已完全写入磁盘，并通过了相关的完整性检查。当内容块提交到存储时，将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	提交给永久存储的内容块的唯一标识符。
RSLT	结果代码	对象存储到磁盘时的状态： SUCS: 对象已成功存储。

此消息表示给定的内容块已完全存储和验证，现在可以请求。它可用于跟踪系统内的数据流。

StorageGRID 中 S3 DELETE 事务的 SDEL 审核消息

当 S3 客户端发出删除事务时，将发出删除指定对象或存储桶或删除存储桶/对象子资源的请求。如果事务成功，此消息将由服务器发出。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
DMRK	删除标记版本 ID	从版本化存储桶中删除对象时创建的删除标记的版本 ID。存储桶上的操作不包括此字段。
GFID	网格联盟连接 ID	与跨网格复制删除请求关联的网格联合连接的连接 ID。仅包含在目标网格的审核日志中。
GFSA	网格联盟源帐户 ID	跨网格复制删除请求的源网格上租户的帐户 ID。仅包含在目标网格的审核日志中。

代码	字段	问题描述
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。 x-amz-bypass-governance-retention 如果请求中存在该内容，则会自动包含在内。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，指示上次修改对象的时间。
RSLT	结果代码	DELETE 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SGRP	站点（组）	如果存在，则对象已在指定站点被删除，该站点不是接收对象的站点。

代码	字段	问题描述
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUDM	删除标记的通用唯一标识符	删除标记的标识符。审核日志消息指定 UUDM 或 UUID，其中 UUDM 表示由于对象删除请求而创建的删除标记，UUID 表示对象。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 GET** 事务的 **SGET** 审核消息

当 S3 客户端发出 GET 事务时，将发出请求以检索对象或在存储桶中列出对象，或删除存储桶/对象子资源。如果事务成功，服务器将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。

代码	字段	问题描述
LITY	ListObjectsV2	已请求 *v2 format* 响应。有关详细信息，请参见 "AWS ListObjectsV2"。仅适用于 GET bucket 操作。
NCHD	子项数量	包括密钥和常用前缀。仅适用于 GET bucket 操作。
RANG	范围读取	仅适用于范围读取操作。指示此请求读取的字节范围。斜杠（/）之后的值显示整个对象的大小。
RSLT	结果代码	GET 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。

代码	字段	问题描述
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
TRNC	截断或未截断	如果返回所有结果，则设置为 false。如果有更多结果可返回，则设置为 true。仅适用于 GET bucket 操作。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	请求的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 HEAD** 操作的 **SHEA** 审核消息

当 S3 客户端发出 HEAD 操作时，会请求检查对象或存储桶是否存在并检索有关对象的元数据。如果操作成功，服务器将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	选中对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。
RSLT	结果代码	GET 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。

代码	字段	问题描述
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	请求的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 POST** 事务的 **SPOS** 审核消息

当 S3 客户端发出 POST 对象请求时，如果事务成功，服务器将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。

代码	字段	问题描述
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。 （不适用于SPOS）。
RSLT	结果代码	RestoreObject 请求的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。 对于 S3 Select 操作，设置为"select"。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。

代码	字段	问题描述
SRCF	子资源配置	还原信息。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	请求的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 PUT** 事务的 **SPUT** 审核消息

当 S3 客户端发出 PUT 事务时，会请求创建新对象或存储桶，或删除存储桶/对象子资源。如果事务成功，此消息将由服务器发出。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CMPS	合规性设置	创建存储桶时使用的合规性设置（如果存在于请求中）（截断为前 1024 个字符）。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
GFID	网格联盟连接 ID	与跨网格复制 PUT 请求关联的网格联合连接的连接 ID。仅包含在目标网格的审核日志中。
GFSA	网格联盟源帐户 ID	跨网格复制 PUT 请求的源网格上租户的帐户 ID。仅包含在目标网格的审核日志中。

代码	字段	问题描述
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。 x-amz-bypass-governance-retention 如果请求中存在该内容，则会自动包含在内。
LKEN	对象锁定已启用	请求标头的值 x-amz-bucket-object-lock-enabled（如果存在于请求中）。
LKLH	对象锁定法律保留	请求标头 `x-amz-object-lock-legal-hold`的值（如果存在于 PutObject 请求中）。
LKMD	对象锁定保留模式	请求标头 `x-amz-object-lock-mode`的值（如果存在于 PutObject 请求中）。
LKRU	对象锁定保留至日期	请求标头 `x-amz-object-lock-retain-until-date`的值（如果存在于 PutObject 请求中）。值限制在对象载入日期起 100 年以内。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。

代码	字段	问题描述
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SRCF	子资源配置	新的子资源配置（截断为前 1024 个字符）。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
ULID	上传 ID	仅包含在 CompleteMultipartUpload 操作的 SPUT 消息中。表示所有分段已上传并组装完成。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在版本化存储桶中创建的新对象的版本 ID。对未版本化存储桶中的存储桶和对象的操作不包括此字段。
VSST	版本控制状态	存储区的新版本控制状态。使用两种状态："已启用"或"已暂停"。对象上的操作不包括此字段。

StorageGRID 中对象存储删除的 **SREM** 审核消息

当内容从永久存储中删除且无法再通过常规 API 访问时，将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	从永久存储中删除的内容块的唯一标识符。

代码	字段	问题描述
RSLT	结果代码	指示内容删除操作的结果。唯一定义的值是： SUCS：已从永久存储中删除内容

此审核消息表示给定的内容块已从节点中删除，无法再直接请求。该消息可用于跟踪系统内已删除内容的流动。

StorageGRID 中 **S3** 元数据更新的 **SUPD** 审核消息

当 S3 客户端更新已载入对象的元数据时，此消息由 S3 API 生成。如果元数据更新成功，则该消息由服务器发出。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNCH	一致性控制标头	更新存储桶的合规性设置时，Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。
RSLT	结果代码	GET 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。

代码	字段	问题描述
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已更新元数据的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中对象存储验证失败的 **SVRF** 审核消息

每当内容块未通过验证过程时，都会显示此消息。每次从磁盘读取或写入复制对象数据时，都会执行多次验证和完整性检查，以确保发送给请求用户的数据与最初摄入系统的数据相同。如果任何这些检查失败，系统会自动隔离损坏的复制对象数据，以防止再次检索。

代码	字段	问题描述
CBID	内容块标识符	验证失败的内容块的唯一标识符。

代码	字段	问题描述
RSLT	结果代码	验证失败类型： CRCF：Cyclic redundancy check (CRC) 失败。 HMAC：基于哈希的消息验证码 (HMAC) 检查失败。 EHSH：意外的加密内容哈希。 PHSH：意外的原始内容哈希。 SEQC：磁盘上的数据序列不正确。 PERR：磁盘文件的结构无效。 DERR：磁盘错误。 FNAM：文件名错误。

应密切监控此消息。内容验证失败可能表明即将发生硬件故障。

要确定触发消息的操作，请参阅 AMID（模块 ID）字段的值。例如，SVFY 值表示消息是由存储验证器模块生成的，即后台验证，而 STOR 表示消息是由内容检索触发的。

StorageGRID 中未知对象存储内容的 SVRU 审核消息

LDR 服务的存储组件持续扫描对象存储中已复制对象数据的所有副本。当在对象存储中检测到已复制对象数据的未知或意外副本并将其移动到隔离目录时，将发出此消息。

代码	字段	问题描述
FPTH	文件路径	意外对象副本的文件路径。
RSLT	结果	此字段的值为"NONE"。RSLT 是必填消息字段，但与此消息无关。使用"NONE"而不是"SUCS"，因此不会过滤此消息。

应密切监控 SVRU：Object Store Verify Unknown 审核消息。这意味着在对象存储中检测到对象数据的意外副本。应立即调查这种情况，以确定这些副本是如何创建的，因为这可能表明硬件即将发生故障。

StorageGRID 中正常节点停止的 SYSD 审核消息

正常停止服务时，将生成此消息以指示请求关闭。通常，此消息仅在后续重新启动后发送，因为在关闭之前不会清除审核消息队列。如果服务尚未重新启动，请查找在关闭序列开始时发送的 SYST 消息。

代码	字段	问题描述
RSLT	正常关机	关闭的性质： SUCS：系统已正常关闭。

该消息不指示主机服务器是否正在停止，仅指示报告服务。SYSD 的 RSLT 不能指示"脏"关闭，因为消息仅由"干净"关闭生成。

StorageGRID 中节点停止的 SYST 审核消息

当服务正常停止时，将生成此消息以指示已请求关闭，并且该服务已启动其关闭序列。SYST 可用于在服务重新启动之前确定是否已请求关闭（与 SYSD 不同，SYSD 通常在服务重新启动后发送）。

代码	字段	问题描述
RSLT	正常关机	关闭的性质： SUCS：系统已正常关闭。

该消息不指示主机服务器是否正在停止，仅指示报告服务。SYST 消息的 RSLT 代码不能指示"脏"关闭，因为该消息仅由"干净"关闭生成。

节点的 SYSU 审核消息在 StorageGRID 中开始

当服务重新启动时，将生成此消息，以指示上一次关闭是正常的（受控）还是异常的（意外）。

代码	字段	问题描述
RSLT	正常关机	关闭的性质： SUCS：系统已正常关闭。 DSDN：系统未完全关闭。 VRGN：系统在服务器安装（或重新安装）后首次启动。

该消息不指示主机服务器是否已启动，仅指示报告服务。此消息可用于：

- 检测审计跟踪中的不连续性。
- 确定服务在运行期间是否发生故障（因为 StorageGRID 系统的分布式特性可能会掩盖这些故障）。Server Manager 会自动重启发生故障的服务。