



监控 **StorageGRID** 系统

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/storagegrid-120/monitor/index.html> on July 23, 2026. Always check docs.netapp.com for the latest.

目录

监控 StorageGRID 系统	1
监控 StorageGRID 系统	1
在 StorageGRID 中查看和管理信息板	1
查看控制面板	2
管理仪表盘	3
配置信息板	3
查看节点页面	4
查看 StorageGRID 节点页面	4
查看 StorageGRID Overview 选项卡	6
查看 StorageGRID 硬件选项卡	8
查看 StorageGRID Network 选项卡	24
查看 StorageGRID Storage 选项卡	25
查看 StorageGRID Objects 选项卡	26
查看 StorageGRID ILM 选项卡	28
查看 StorageGRID 负载均衡器选项卡	28
查看 StorageGRID 平台服务选项卡	30
查看 StorageGRID 管理驱动器选项卡	31
查看 StorageGRID SANtricity System Manager 选项卡	32
定期监控的信息	34
在 StorageGRID 中监控什么以及何时监控	34
在 StorageGRID 中监控系统运行状况	34
监控 StorageGRID 中的存储容量	38
监控 StorageGRID 中的信息生命周期管理	45
监控 StorageGRID 中的网络 and 系统资源	47
监控 StorageGRID 中的租户活动	50
监控 StorageGRID 中的 S3 客户端操作	54
监控 StorageGRID 中的负载均衡操作	56
监控 StorageGRID 网络联合连接	57
\${post_edited_translations.segment}	61
在 StorageGRID 中管理警报	61
查看 StorageGRID 警报规则	61
在 StorageGRID 中创建自定义警报规则	63
在 StorageGRID 中编辑警报规则	65
在 StorageGRID 中禁用警报规则	68
删除 StorageGRID 中的自定义警报规则	68
管理警报通知	69
StorageGRID 中的警报	77
StorageGRID 中常用的 Prometheus 指标	88
日志文件引用	93

StorageGRID 日志文件	93
StorageGRID 软件日志	96
StorageGRID 中的部署和维护日志	101
了解 StorageGRID bycast.log	101
配置日志管理和外部 syslog 服务器	110
StorageGRID 中的外部系统日志服务器	110
在 StorageGRID 中配置日志管理	114
使用 SNMP 监控	123
在 StorageGRID 中使用 SNMP 监控	123
在 StorageGRID 中配置 SNMP 代理	125
更新 StorageGRID SNMP 代理	130
访问 StorageGRID MIB 文件	132
收集其他 StorageGRID 数据	134
监控 StorageGRID 中的 PUT 和 GET 性能	134
监控 StorageGRID 中的对象验证操作	134
查看 StorageGRID 审核消息	137
收集 StorageGRID 日志文件和系统数据	138
手动触发 StorageGRID AutoSupport 包	139
查看 StorageGRID 支持指标	140
更改 StorageGRID 中的 I/O 优先级	141
在 StorageGRID 中运行诊断	142
为 StorageGRID 创建自定义监控应用程序	146

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

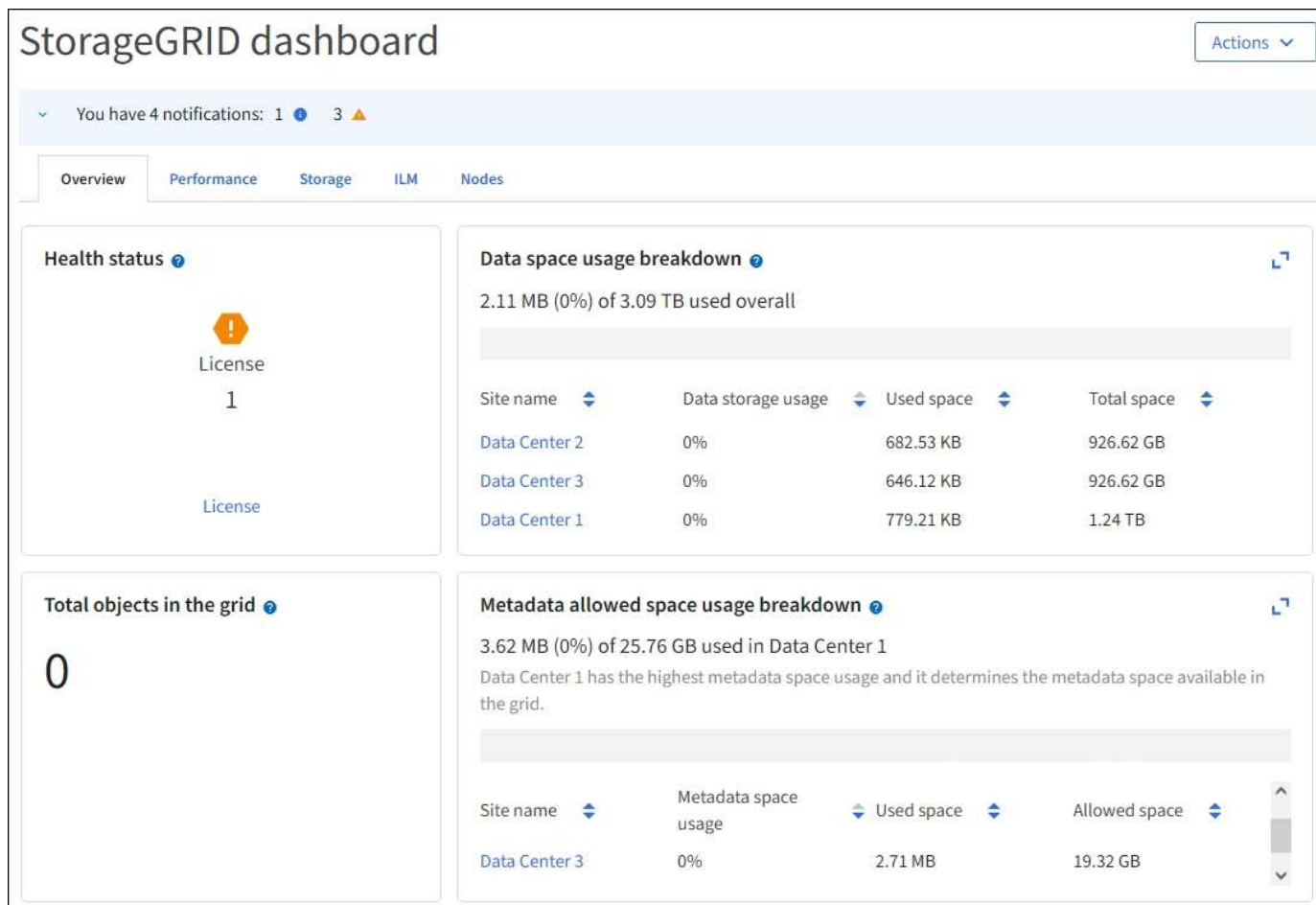
在 StorageGRID 中查看和管理信息板

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。

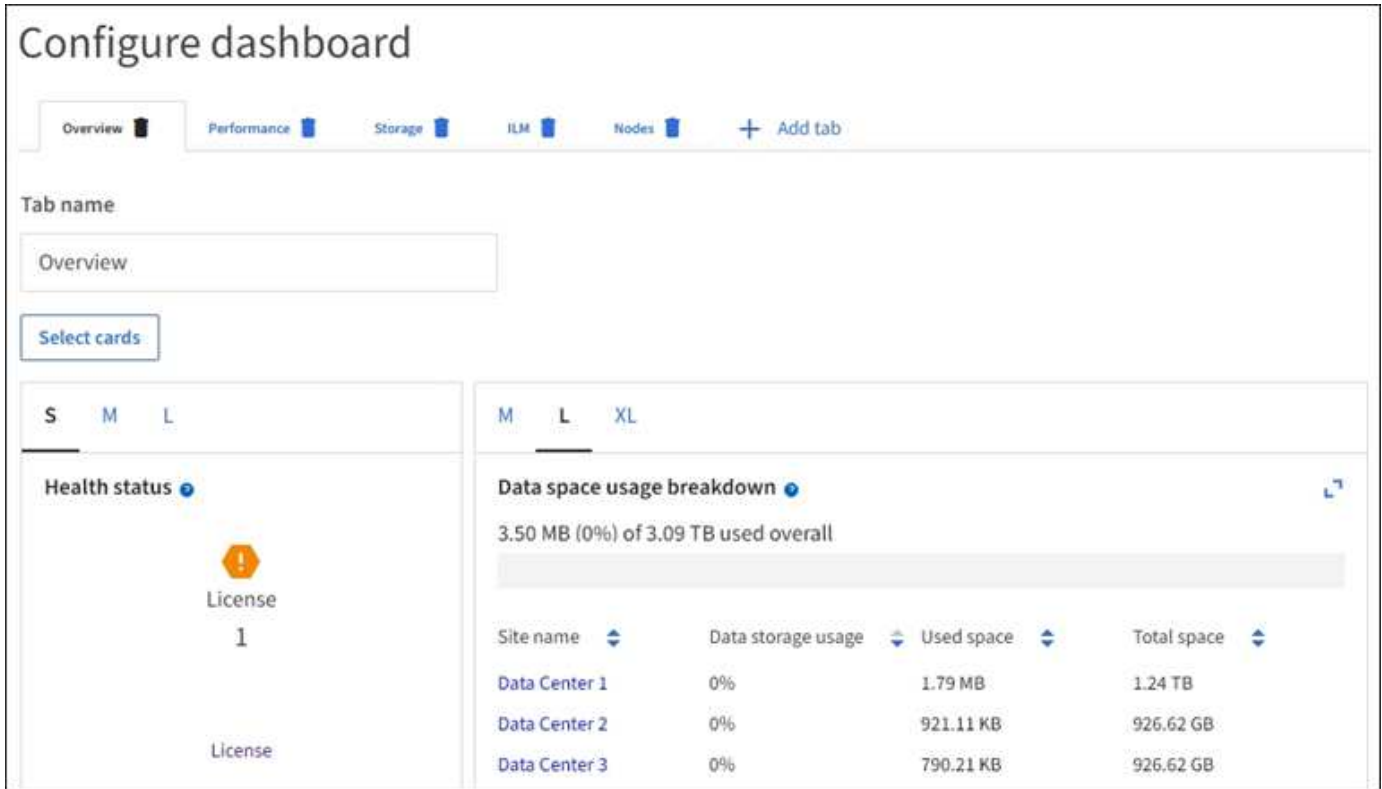


无法编辑或删除系统提供的控制面板。

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。

Nodes

View the list and status of sites and grid nodes.

Search...

Total node count: 12

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
^ DC1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	6%
 DC1-ARC1	Archive Node	—	—	1%
 DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%

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。

NYC-ADM1 (Primary Admin Node) [🔗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Load balancer](#) [Tasks](#)

Node information [?](#)

Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	✔ Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#) [▼](#)

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。

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

还包括适用于 "[节点连接状态](#)" 的警报。

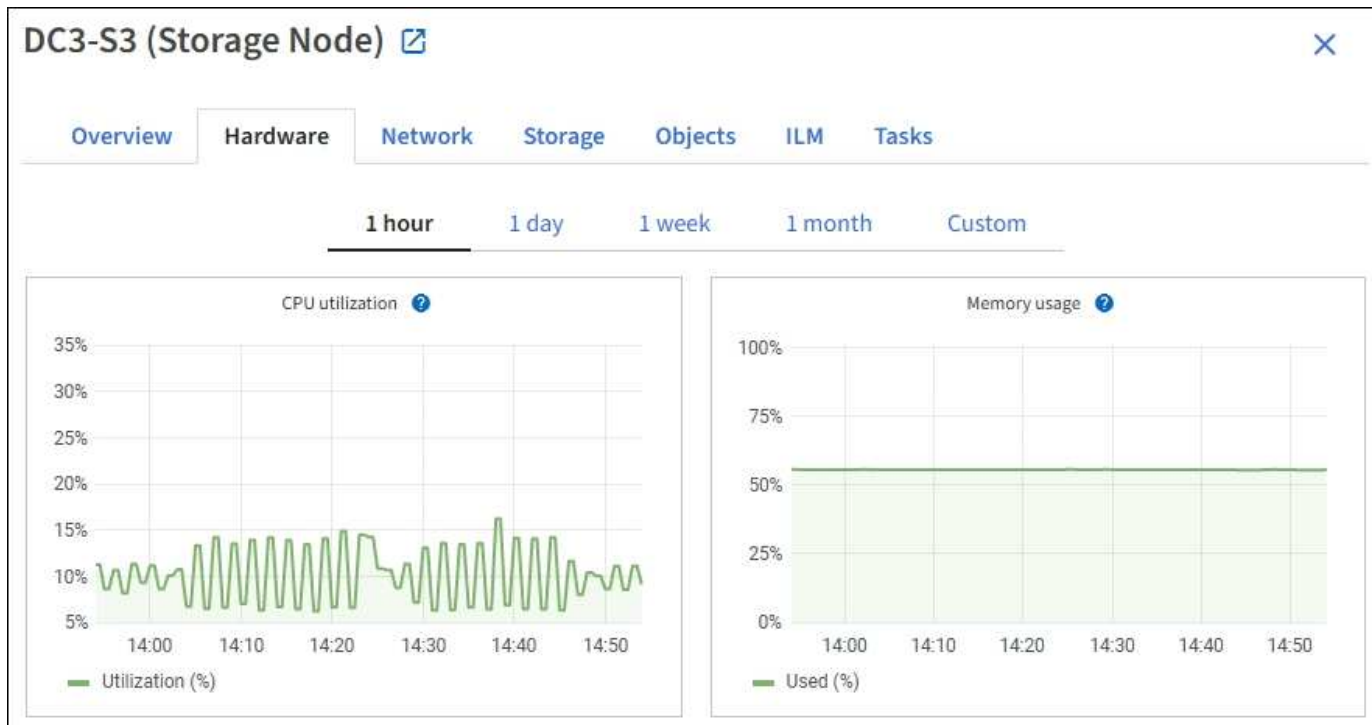
查看 StorageGRID 硬件选项卡

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。



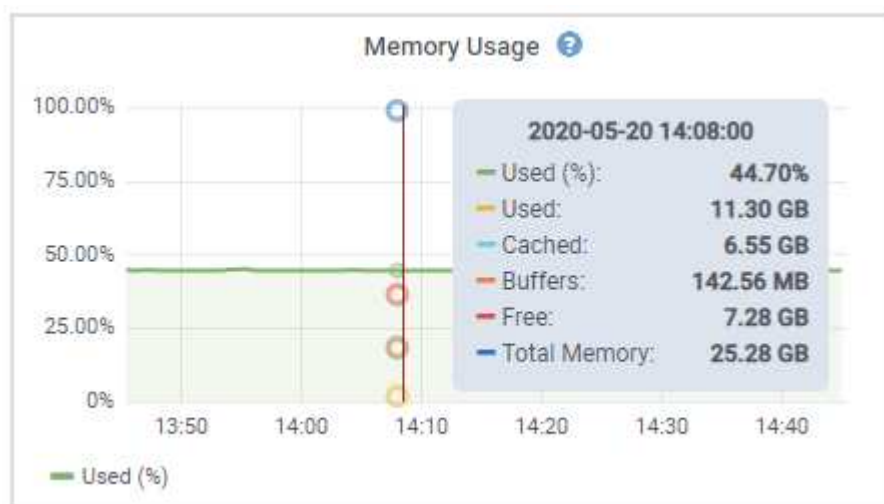
网络管理器随每个版本更新, 可能与此页面上的示例屏幕截图不匹配。

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。

DC2-SGA-010-096-106-021 (Storage Node) ✕

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

Node information ?

Name:

DC2-SGA-010-096-106-021

Type:

Storage Node

ID:

f0890e03-4c72-401f-ae92-245511a38e51

Connection state:

✔ Connected

Storage used:

Object data

7%

?

Object metadata

5%

?

Software version:

11.6.0 (build 20210915.1941.afce2d9)

IP addresses:

10.96.106.21 - eth0 (Grid Network)

Hide additional IP addresses ^

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

Alerts

Alert name ⌵

Severity ? ⌵

Time triggered ⌵

Current values

ILM placement unachievable 🔗

A placement instruction in an ILM rule cannot be achieved for certain objects.

🚨 Major

2 hours ago ?

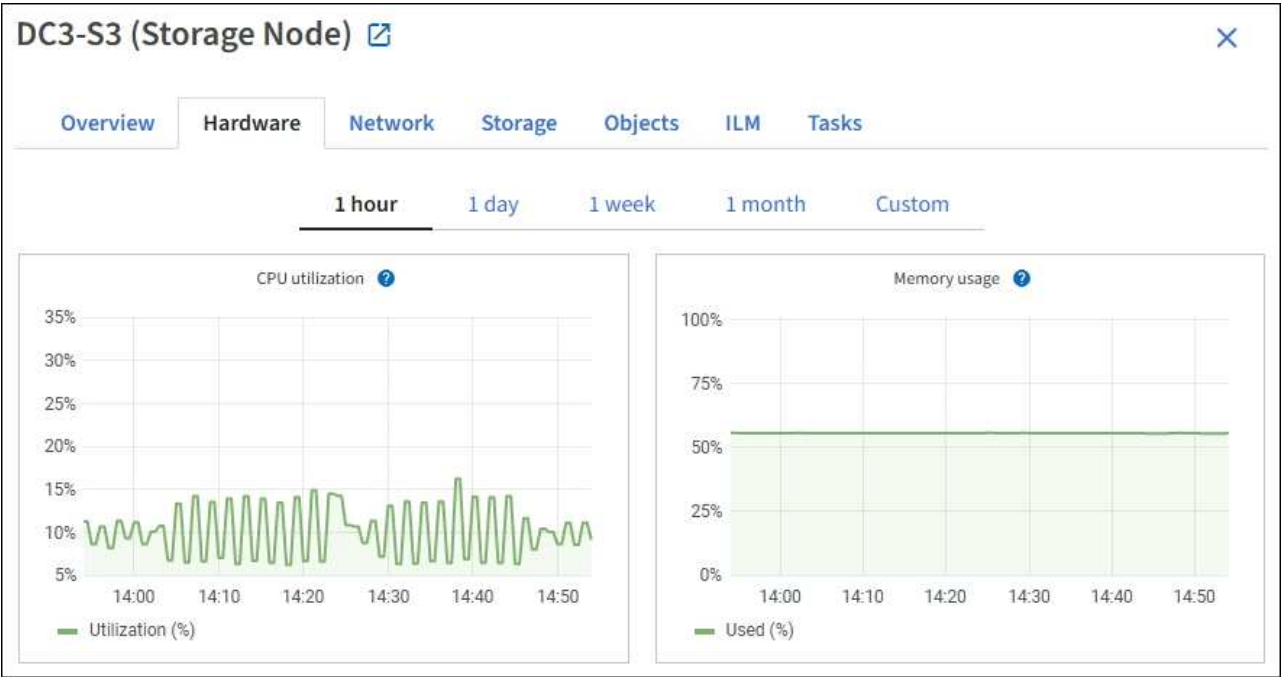
"概述"选项卡的"警报"部分显示该节点的所有活动警报。

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

10

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。

StorageGRID Appliance

Appliance model: ?	SG6060	
Storage controller name: ?	StorageGRID-Lab79-SG6060-7-134	
Storage controller A management IP: ?	10.2	
Storage controller B management IP: ?	10.2	
Storage controller WWID: ?	6d039ea0000173e50000000065b7b761	
Storage appliance chassis serial number: ?	721924500068	
Storage controller firmware version: ?	08.53.00.09	
Storage controller SANtricity OS version: ?	11.50.3R2	
Storage controller NVSRAM version: ?	N280X-853834-DG1	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller B: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	4.00 TB	
Storage RAID mode: ?	DDP16	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Degraded	
Compute controller BMC IP: ?	10.2	
Compute controller serial number: ?	721917500060	
Compute hardware: ?	Needs Attention	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Failed	
Compute controller power supply B: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?	Power supply status ?	Drawer status ?	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

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。

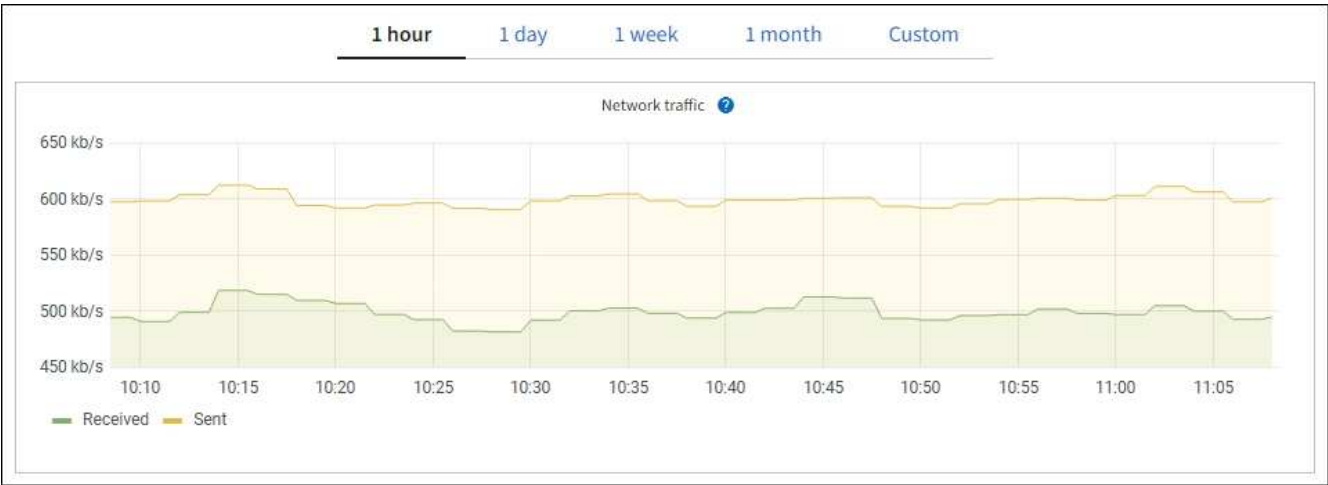
存储货架表中的列	问题描述
数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储盘架中用作缓存的驱动器数。
缓存驱动器大小	存储盘架中最小缓存驱动器的大小。通常，缓存驱动器的大小都相同。
配置状态	存储盘架的配置状态。

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。

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

使用下表以及网络接口表中*速度*列的值，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)	预期网络/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

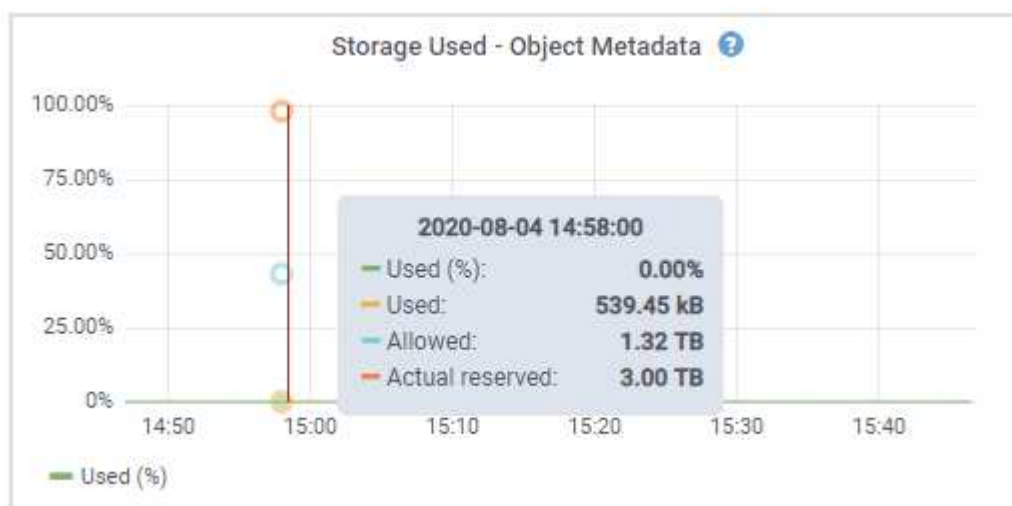
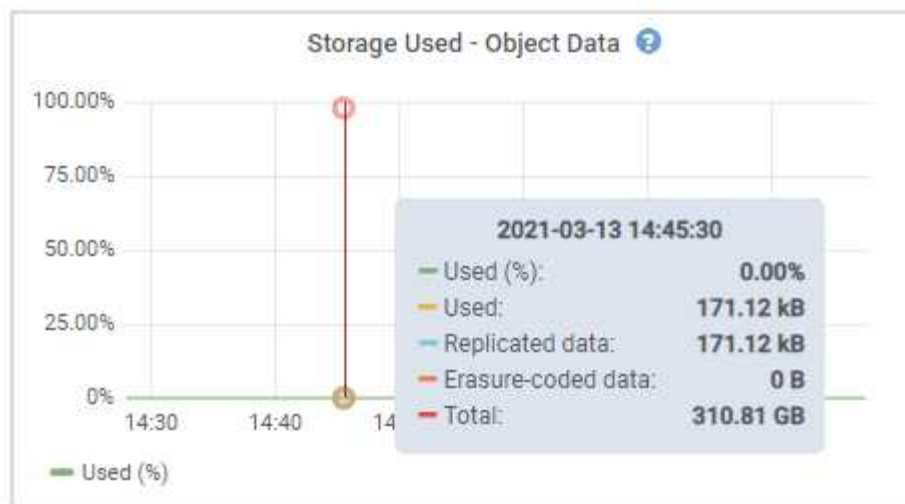
有关配置 10/25-GbE 端口的详细信息，请参见 ["配置网络链接"](#)。

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。

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

- 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。

10-224-6-199-ADM1 (Primary Admin Node) 🔗

Overview

Hardware

Network

Storage

Load balancer

Tasks

SANtricity System Manager

Node information ?

Name:

10-224-6-199-ADM1

Type:

Primary Admin Node

ID:

6fdc1890-ca0a-4493-acdd-72ed317d95fb

Connection state:

🟢

Connected

Software version:

11.6.0 (build 20210928.1321.6687ee3)

IP addresses:

172.16.6.199 - eth0 (Grid Network)

10.224.6.199 - eth1 (Admin Network)

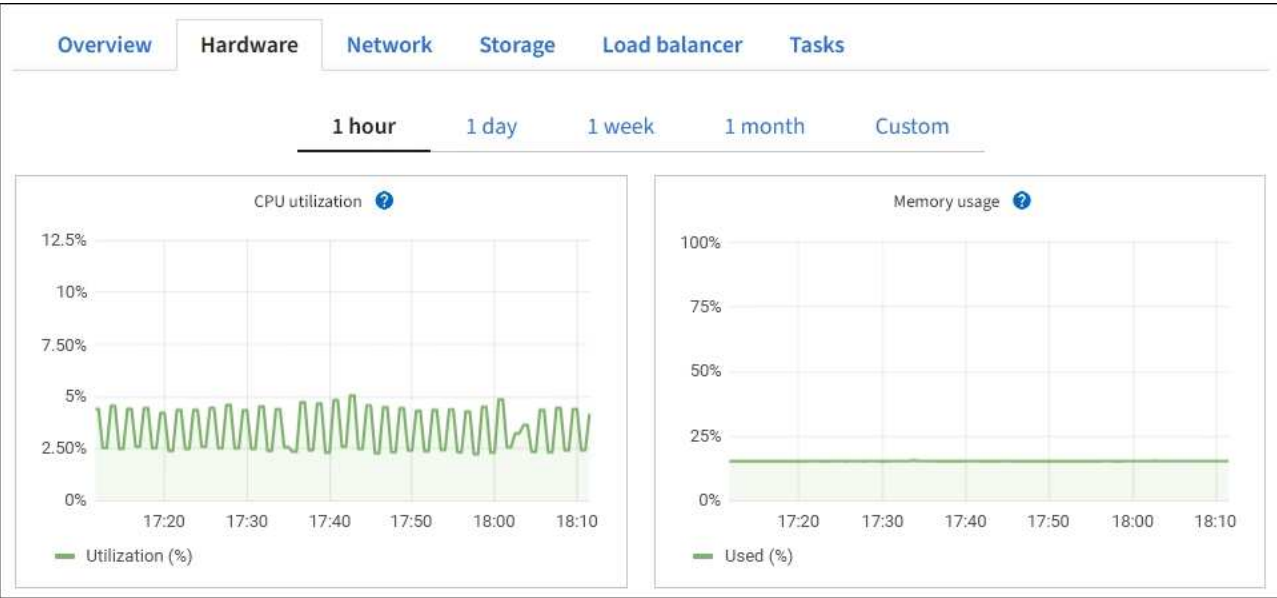
47.47.7.241 - eth2 (Client Network)

Hide additional IP addresses ^

Interface ⌵	IP address ⌵
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

"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。

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

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

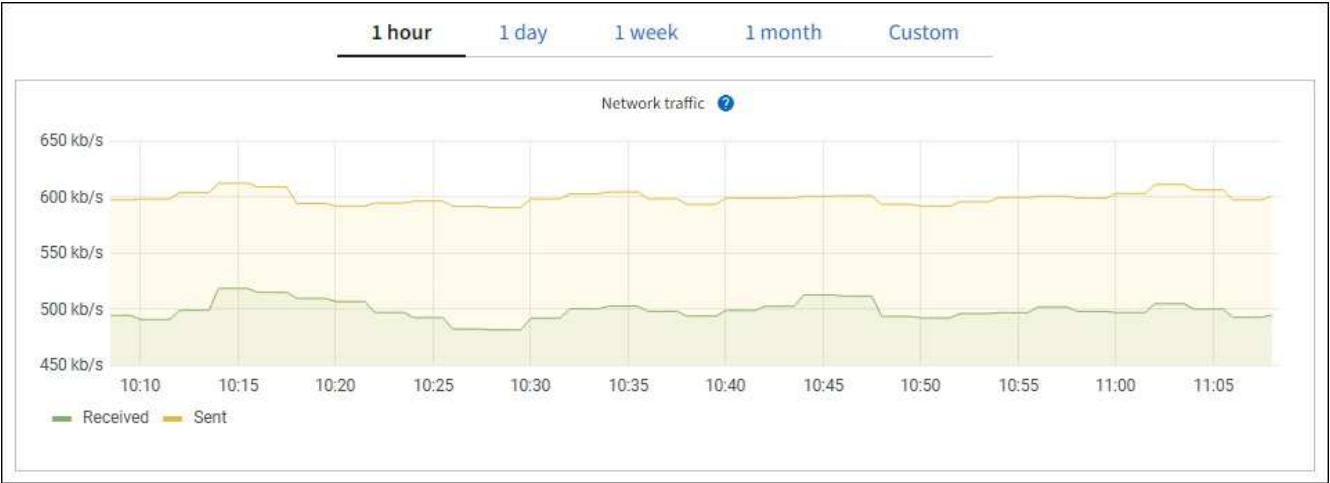
Appliance 表中的字段	问题描述
存储控制器故障驱动器计数	非最优状态的驱动器数量。
存储数据驱动器类型	设备中的驱动器类型，例如 HDD（硬盘驱动器）或 SSD（固态硬盘）。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中基板管理控制器（BMC）端口的 IP 地址。您可以使用此 IP 连接到 BMC 接口，以监控和诊断设备硬件。 此字段不会为不包含 BMC 的设备型号显示。
计算控制器序列号	计算控制器的序列号。
计算硬件	此计算控制器硬件的状态。
计算控制器 CPU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

Network communication						
Receive						
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

5. 选择*存储*以查看有关服务设备上磁盘设备和卷的信息。

DO-REF-DC1-GW1 (Gateway Node)



Overview

Hardware

Network

Storage

Load balancer

Tasks

Disk devices

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

Volumes

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

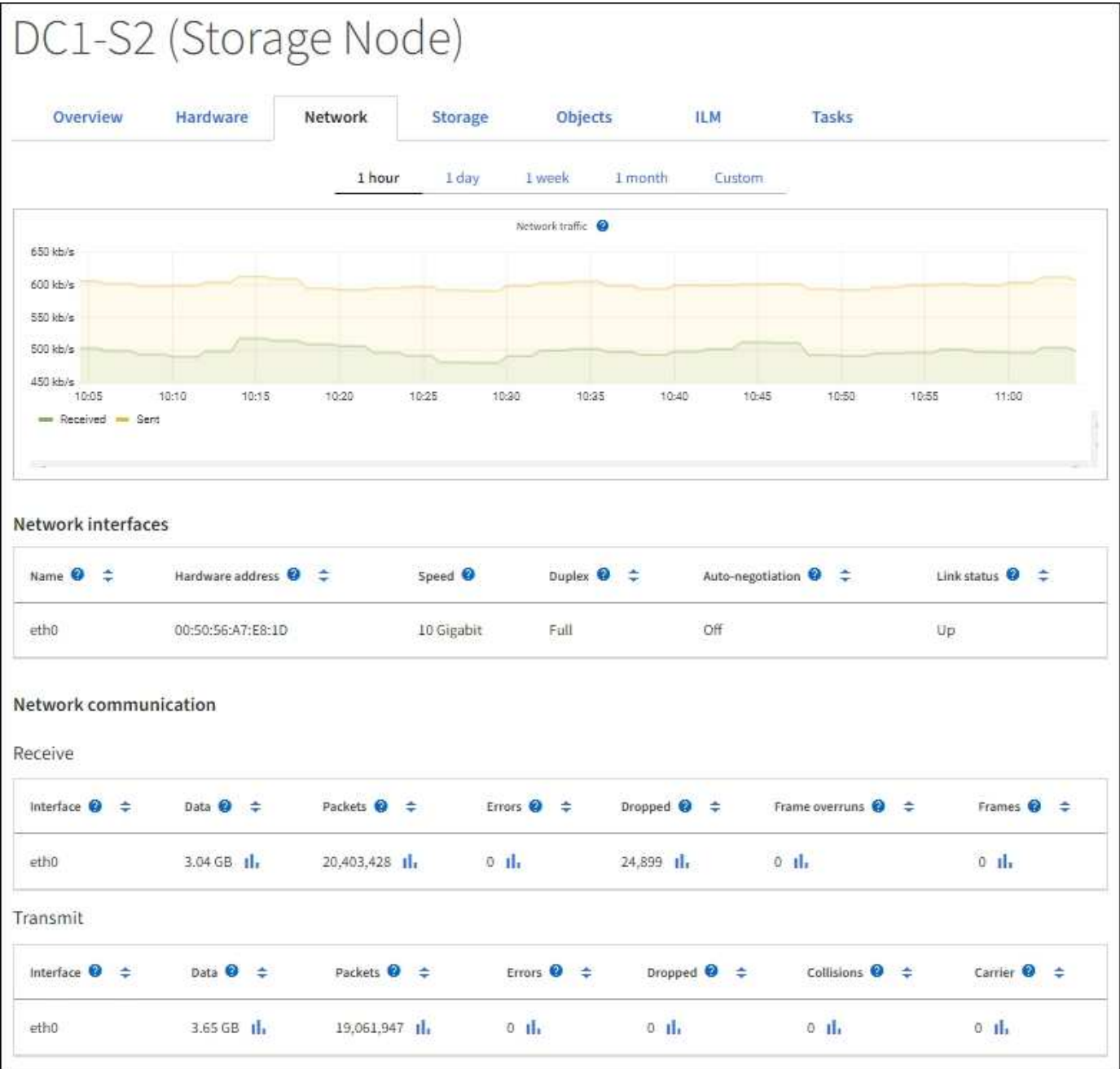
查看 StorageGRID Network 选项卡

"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

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。

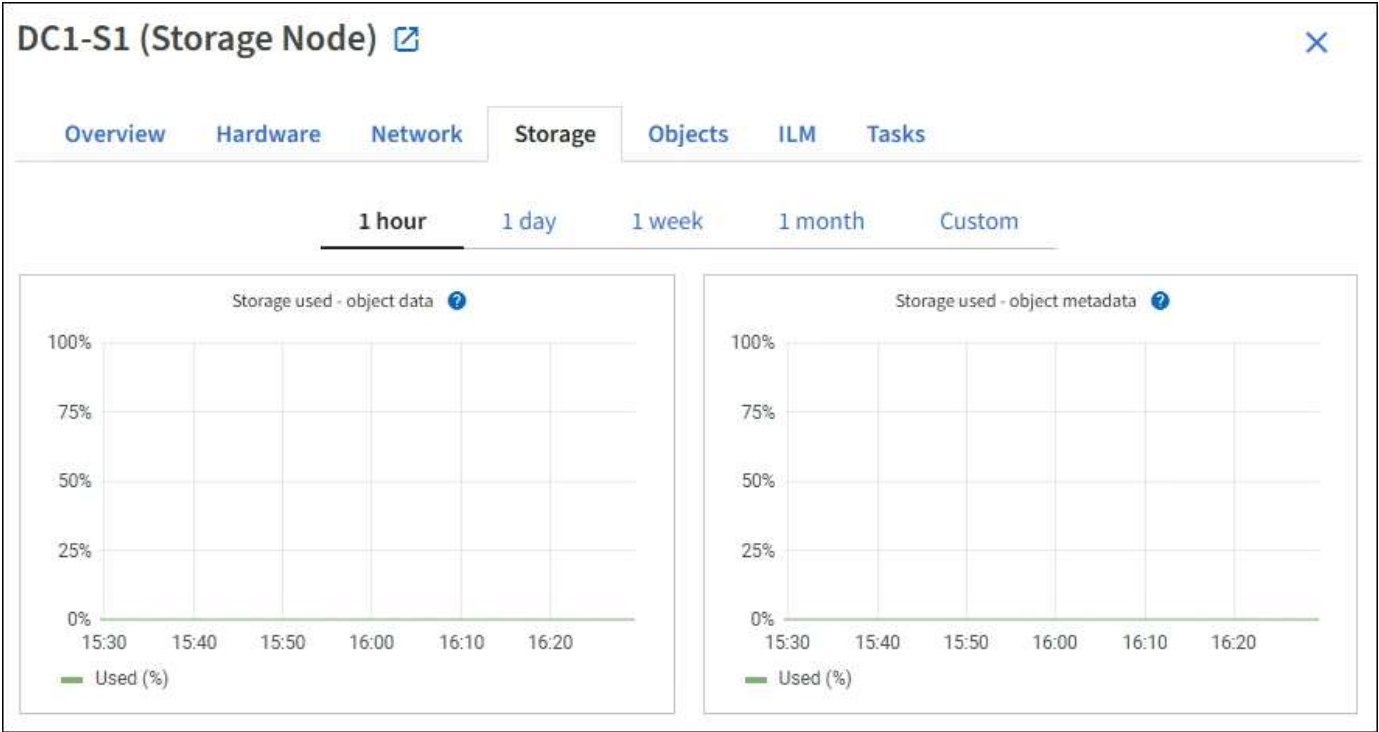
"存储"选项卡适用于所有节点、每个站点和整个网格。

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

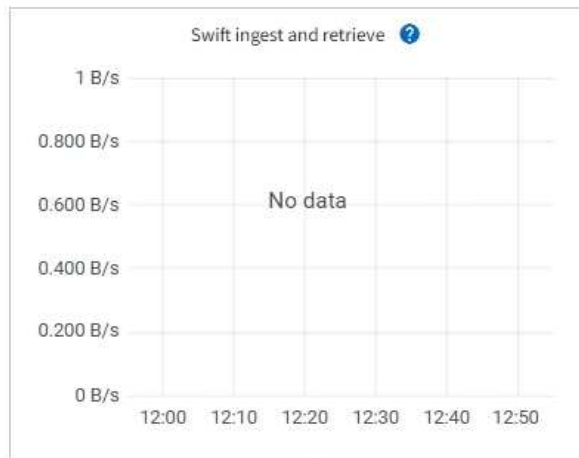
"[监控存储容量](#)"

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](#)

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

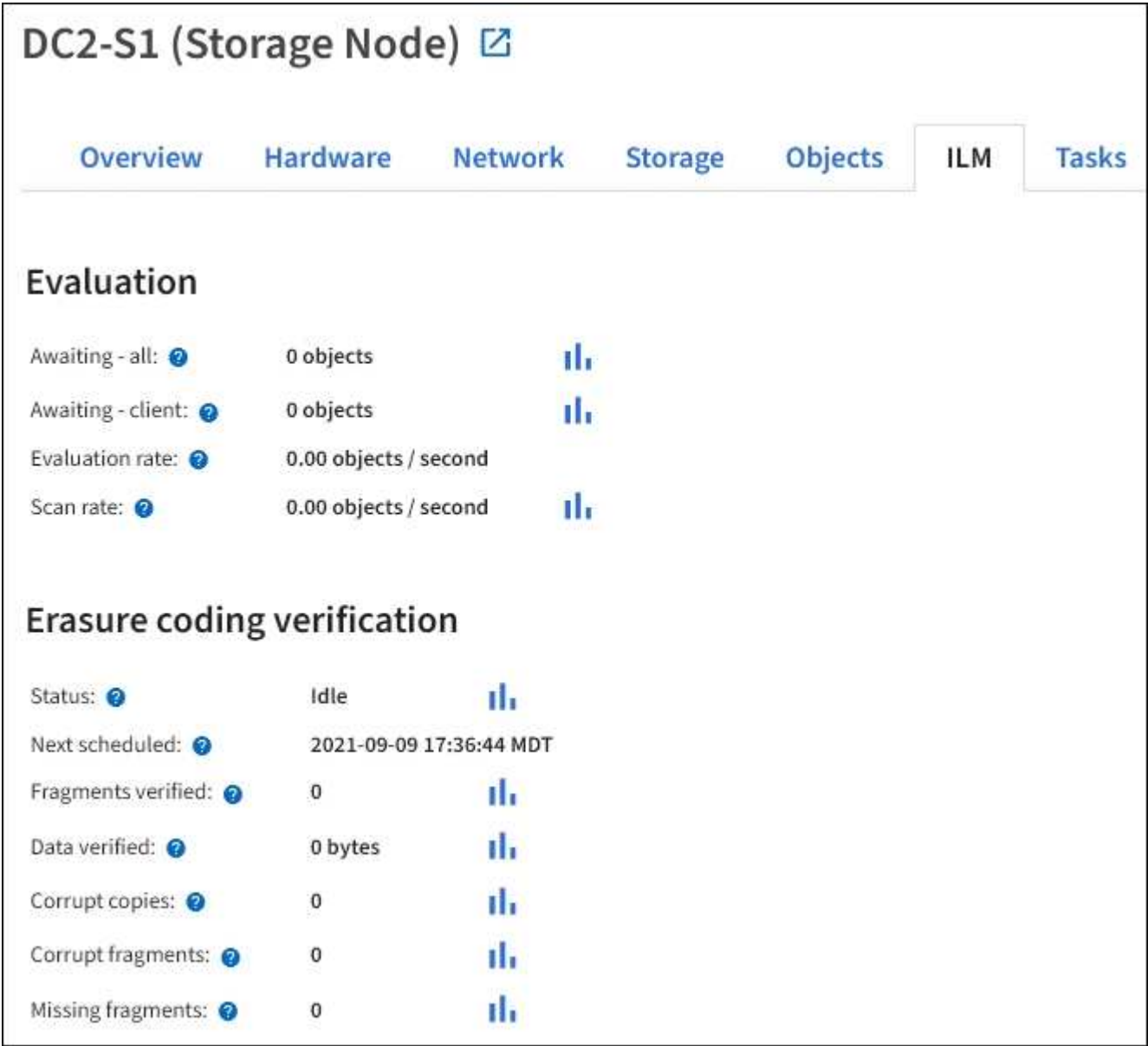
Quarantined objects: [?](#) 0

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

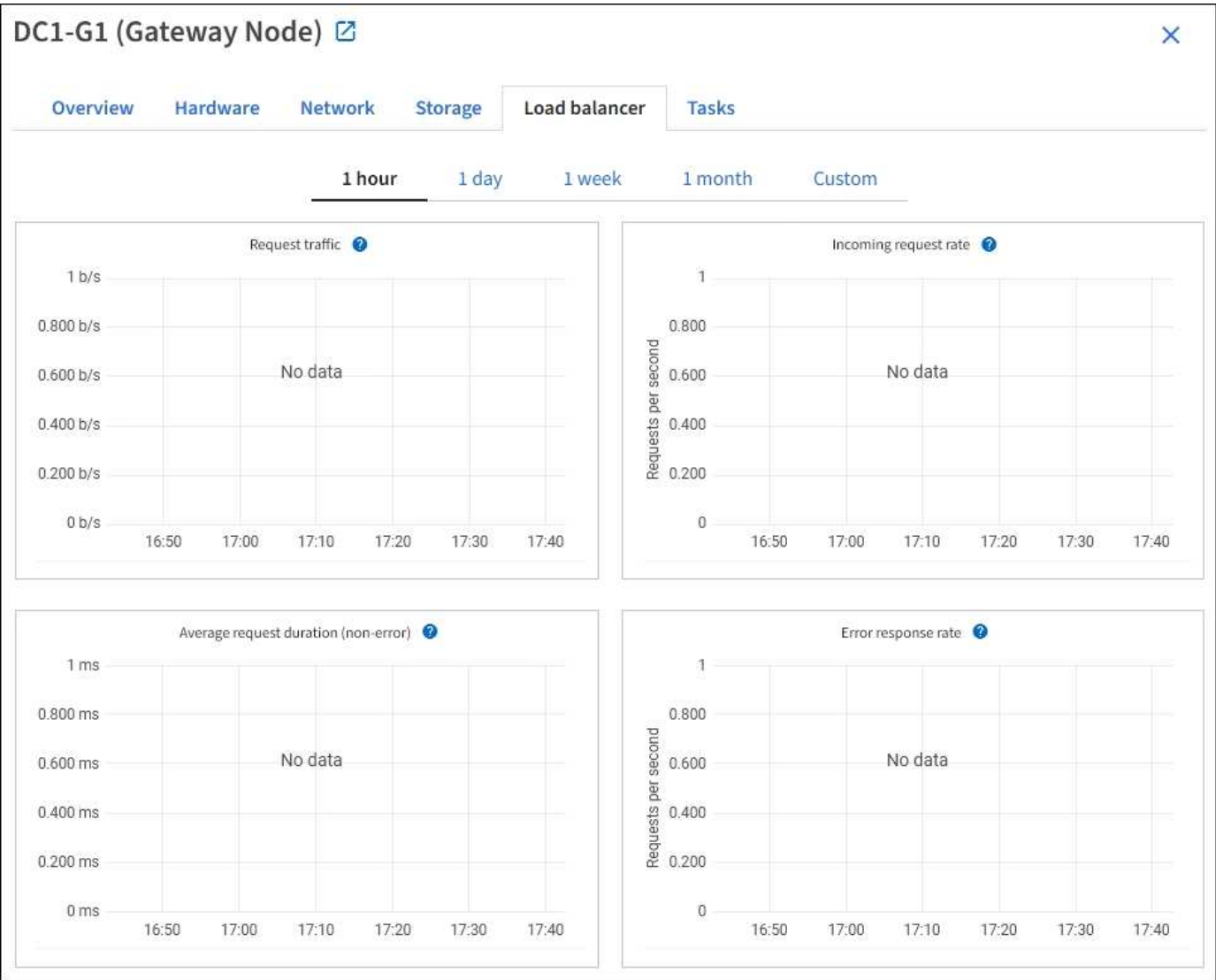
- ["监控信息生命周期管理"](#)
- ["管理 StorageGRID"](#)

查看 **StorageGRID** 负载均衡器选项卡

负载均衡器选项卡包括与负载均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均衡器选项卡。对于每个站点，负载均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，负载均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均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

- ["监控负载均衡操作"](#)
- ["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。

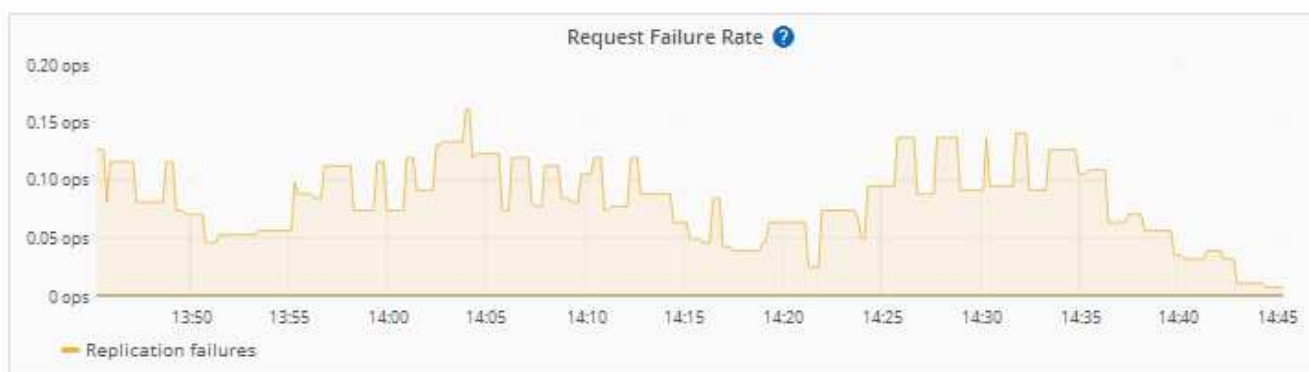
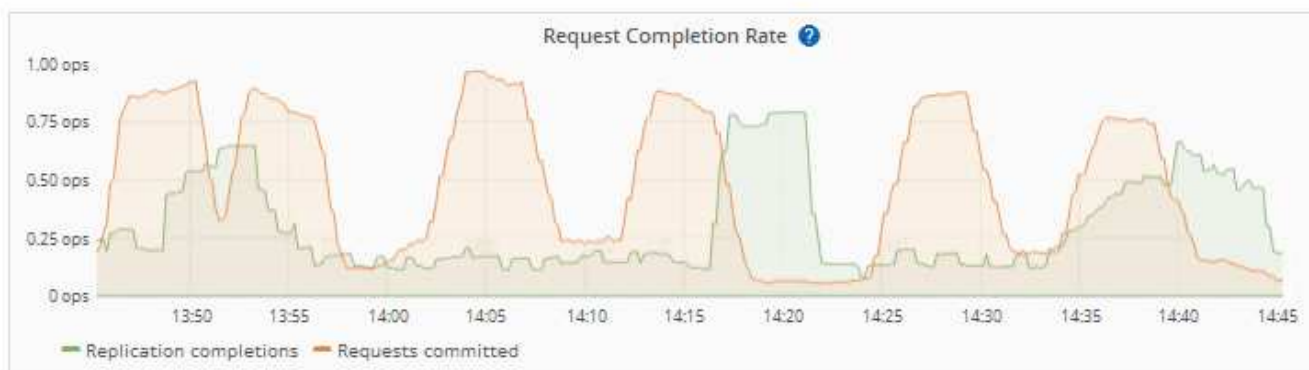
1 hour

1 day

1 week

1 month

Custom



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。

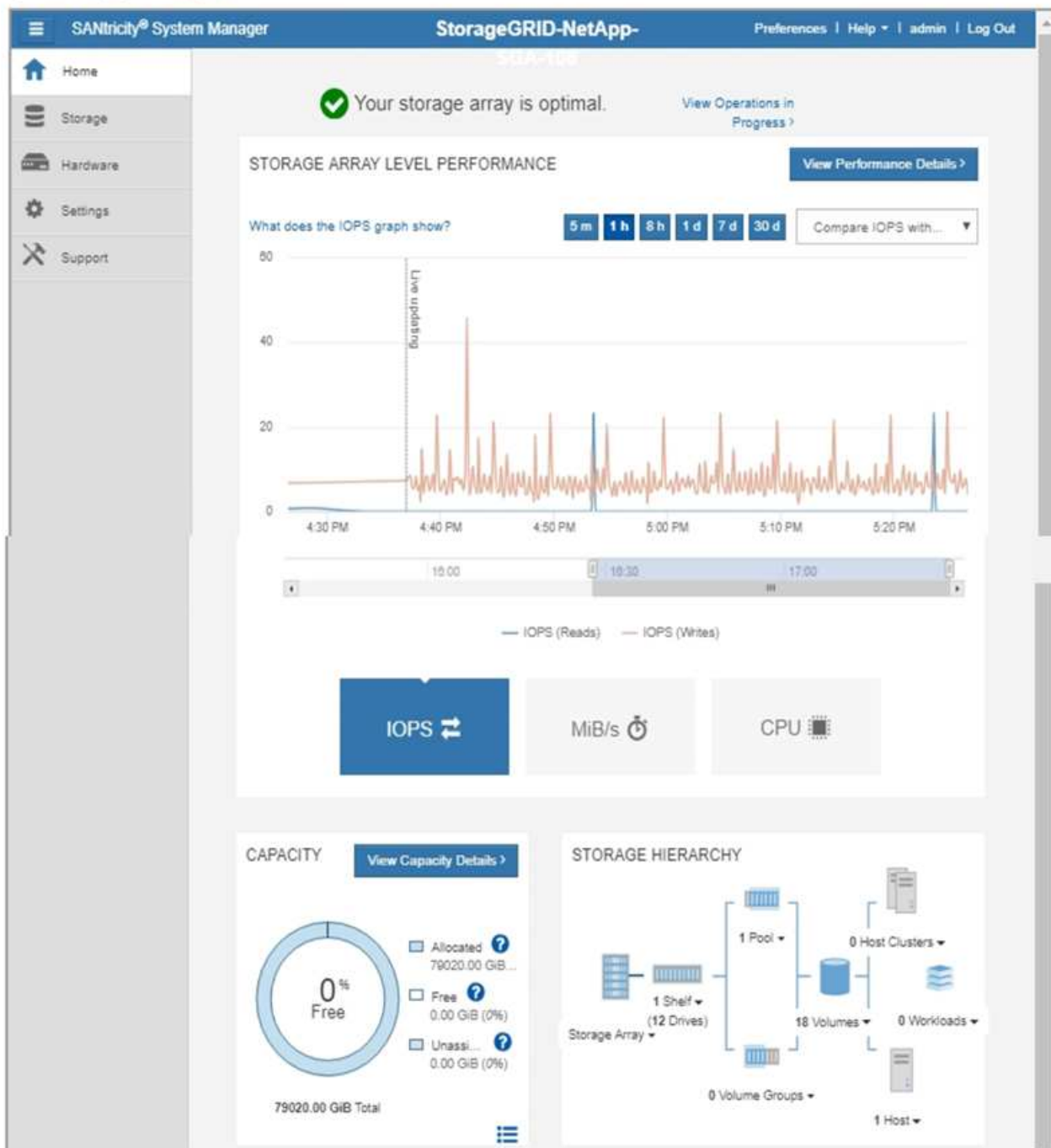
该选项卡显示 SANtricity System Manager 的主页。

Overview Hardware Network Storage Objects ILM Events Tasks SANtricity System Manager

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.



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 and 系统资源"	每周
"租户活动"	每周
"S3 客户端操作"	每周
"负载均衡操作"	初始配置后和任何配置更改后
"网格联盟连接"	每周

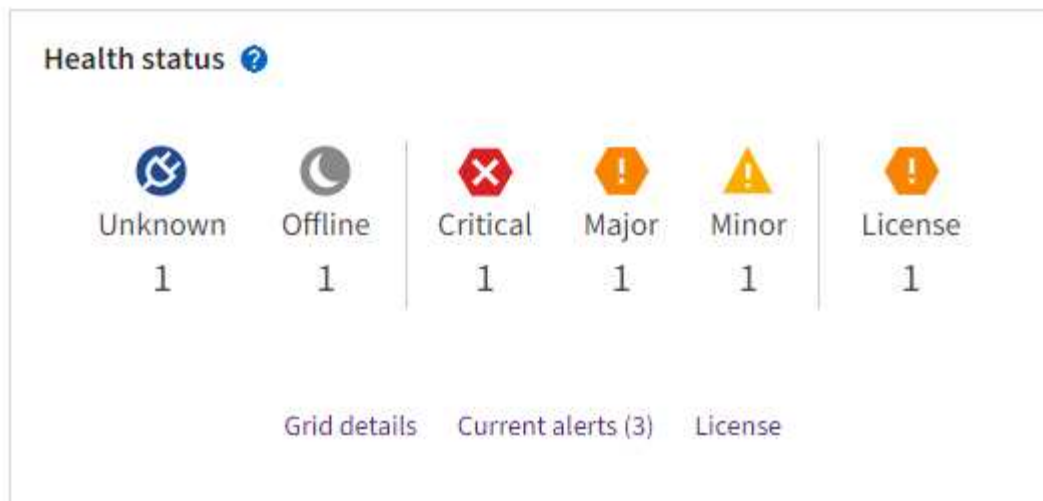
在 StorageGRID 中监控系统运行状况

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.....
网络详细信息	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（<i>newest</i>）和最旧实例（<i>oldest</i>）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音的实例数。
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。

监控整个网格的存储容量

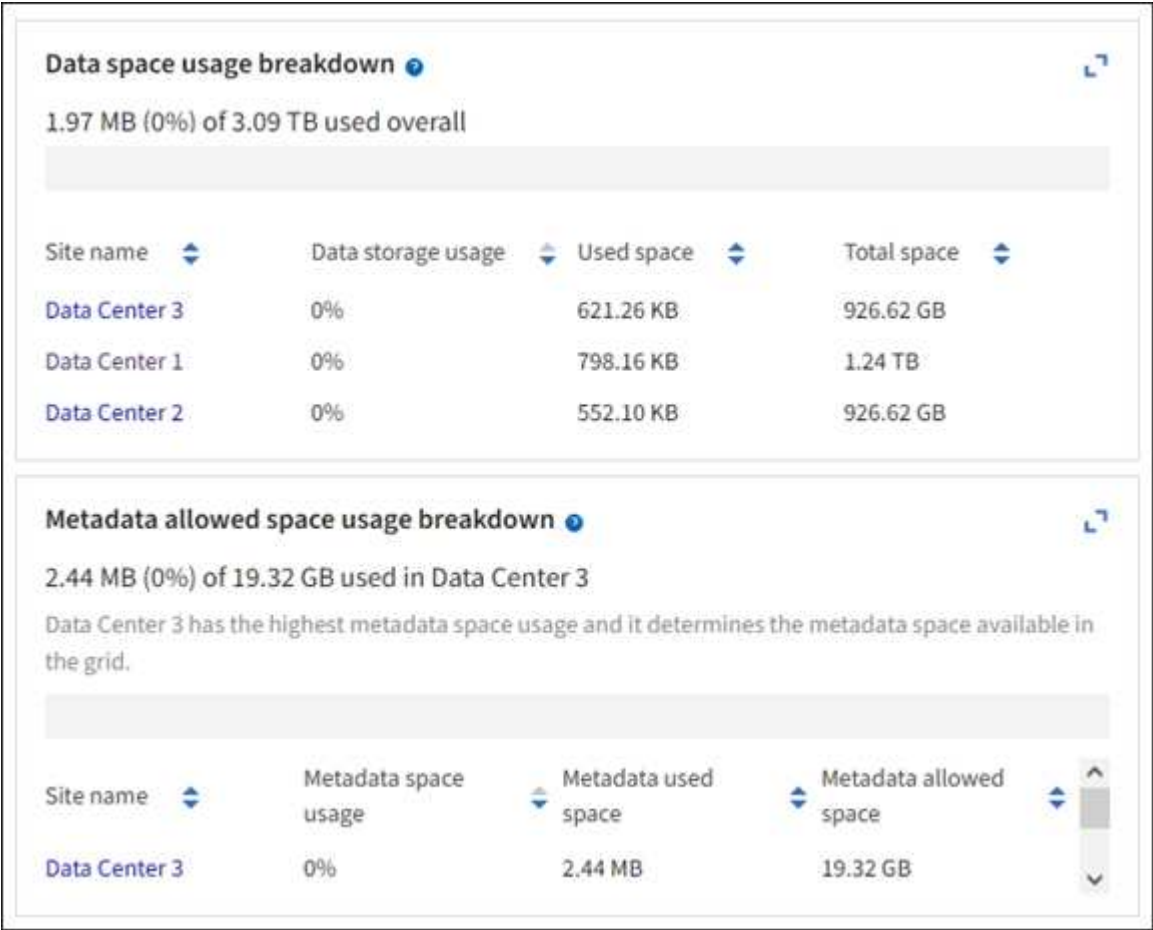
监控网格的整体存储容量，以确保为对象数据和对象元数据保留足够的可用空间。了解存储容量随时间的变化情况有助于您计划在网格的可用存储容量消耗之前添加存储节点或存储卷。

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。

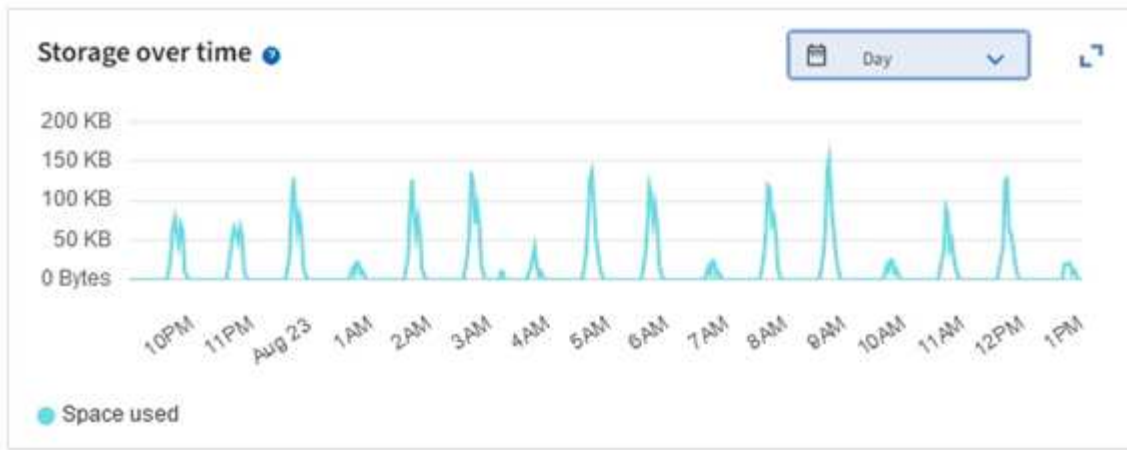
步骤

- 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。

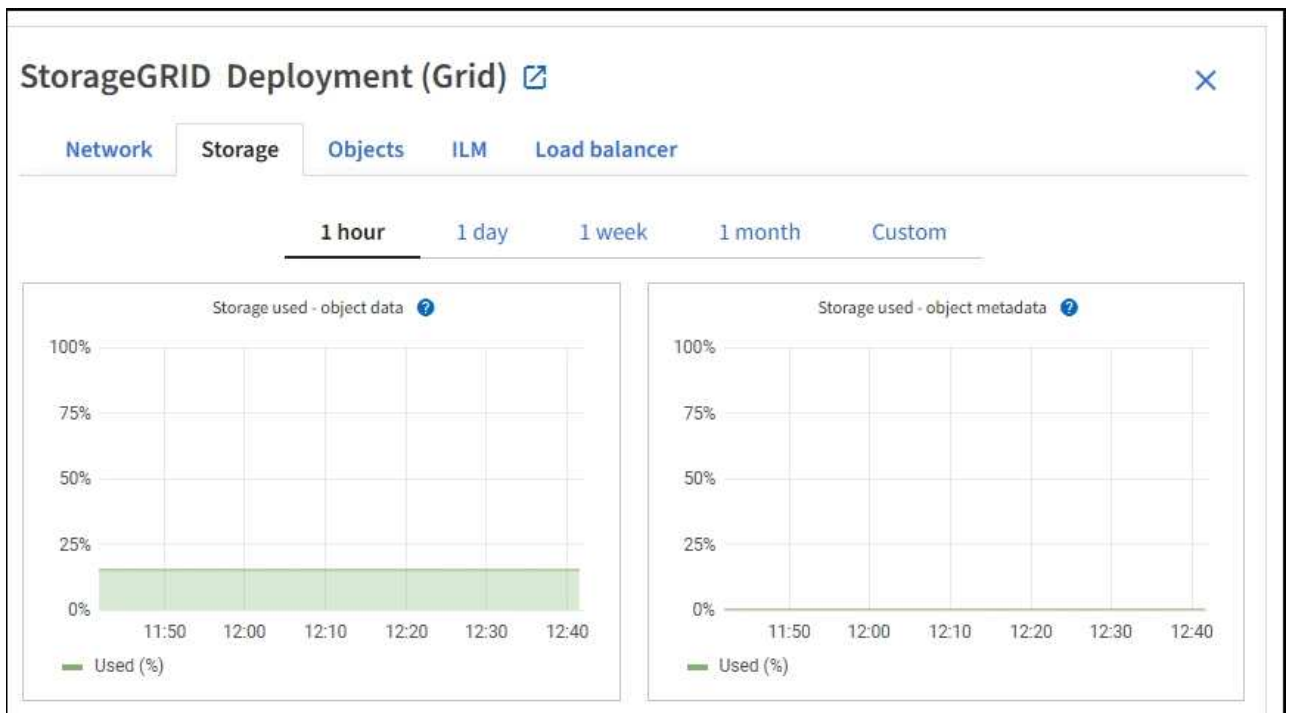


- a. 请注意存储随时间推移卡上的图表。使用时间段下拉菜单可帮助您确定存储消耗的速度。



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。

- 选择 **Nodes**。
- 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。

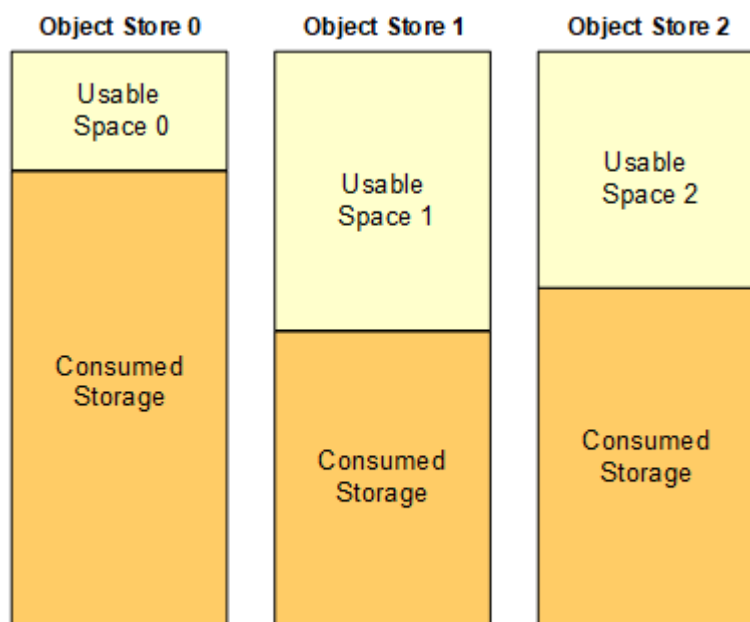
有关规划存储扩展的详细信息，请参见 ["扩展 StorageGRID 的说明"](#)。

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。



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

步骤

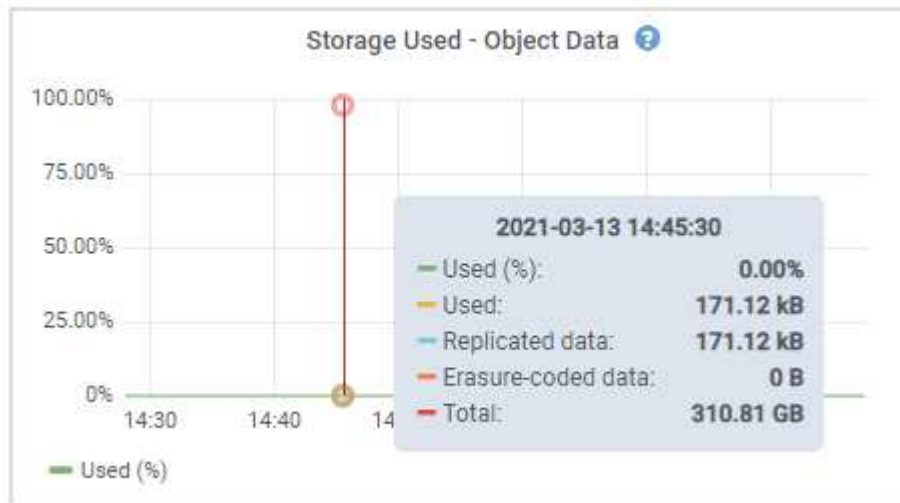
1. 选择*节点* > 存储节点 > 存储。

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

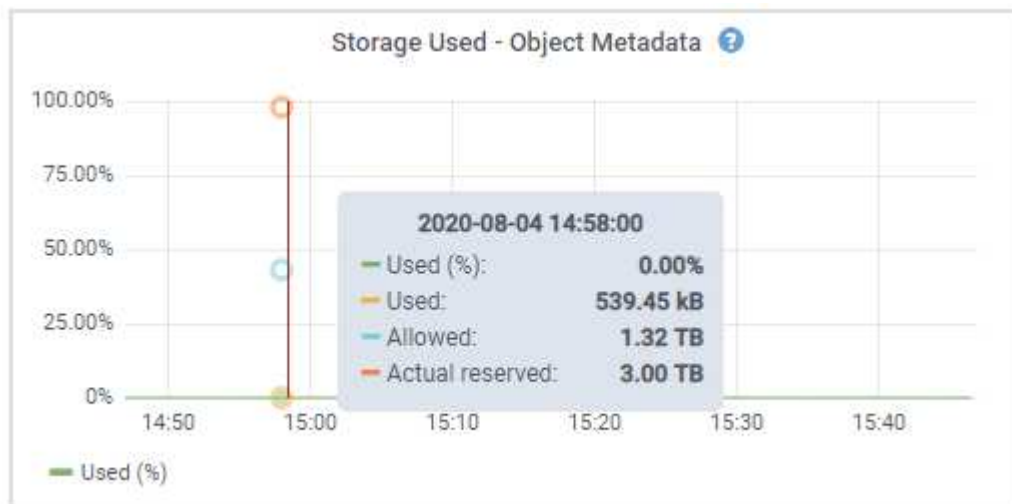
StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并保护对象元数据免于丢失。这三个副本均匀分布在每个站点的所有存储节点上，使用为每个存储节点的存储卷 0 上的元数据预留的空间。

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間。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。



站点或网络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

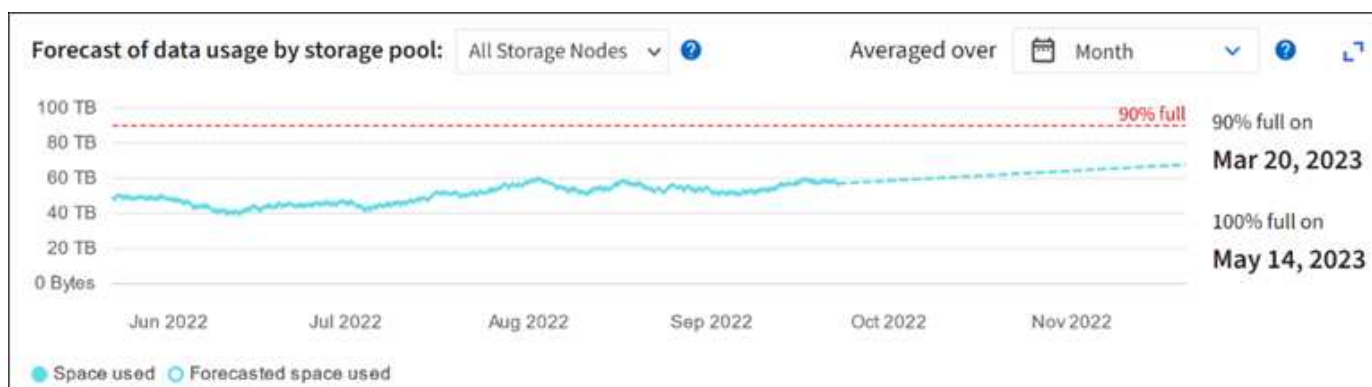
监控用户数据和元数据的空间使用预测，以估计何时需要 ["展开网络"](#)。

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

使用网络管理器仪表板上的 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 网络名称 > **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 and 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。

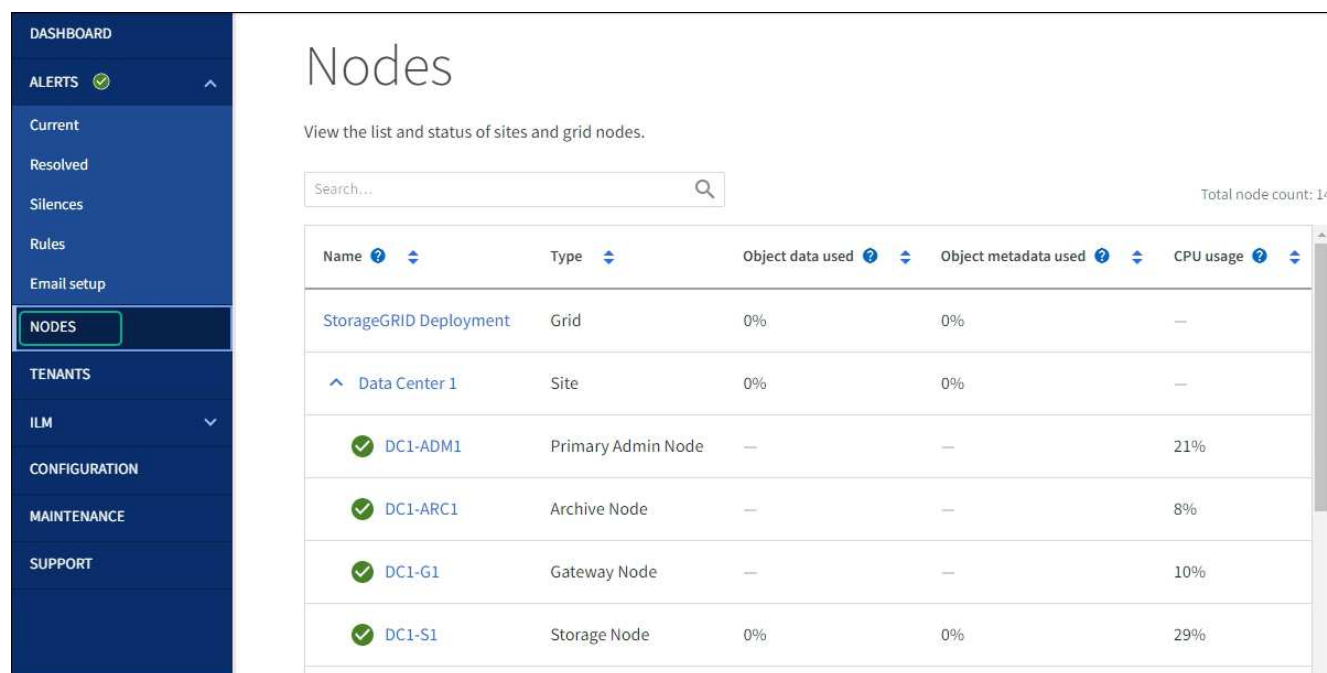
请使用 Grid Manager 监控连接和网络性能，以便及时解决任何问题。

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、子网或负载均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**。

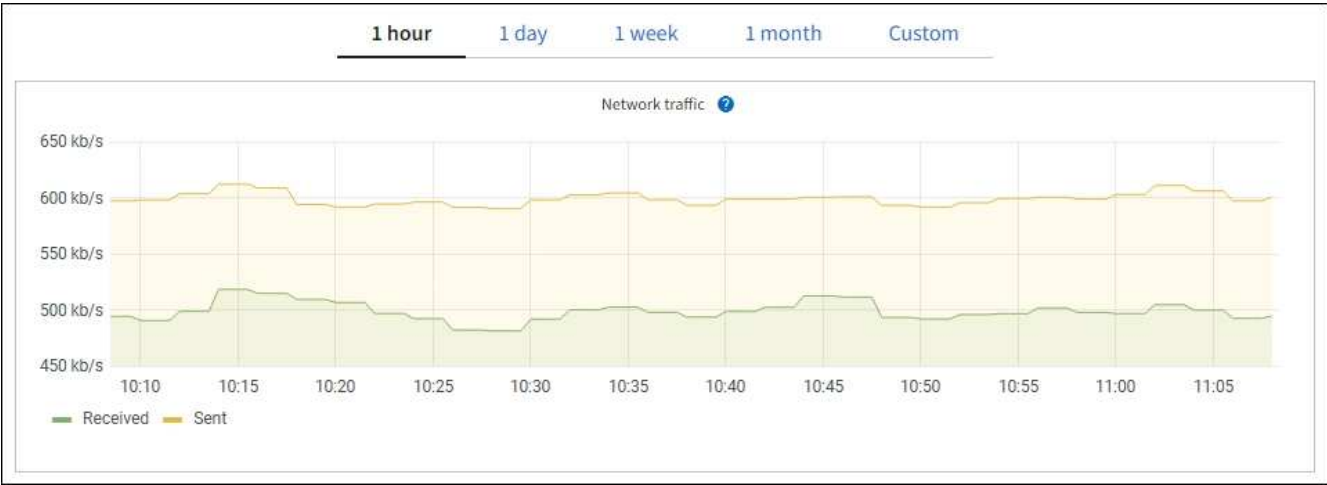
此时将显示节点页面。网格中的每个节点都以表格格式列出。



Nodes				
View the list and status of sites and grid nodes.				
Search...				
Total node count: 14				
Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

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. 如果您选择了网络节点，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. 对于网络节点，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。

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit ✕ Remove Metrics		
Name	Description	ID
☐ ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒ Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b

Displaying 2 traffic classification policies.

- 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*。
- 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

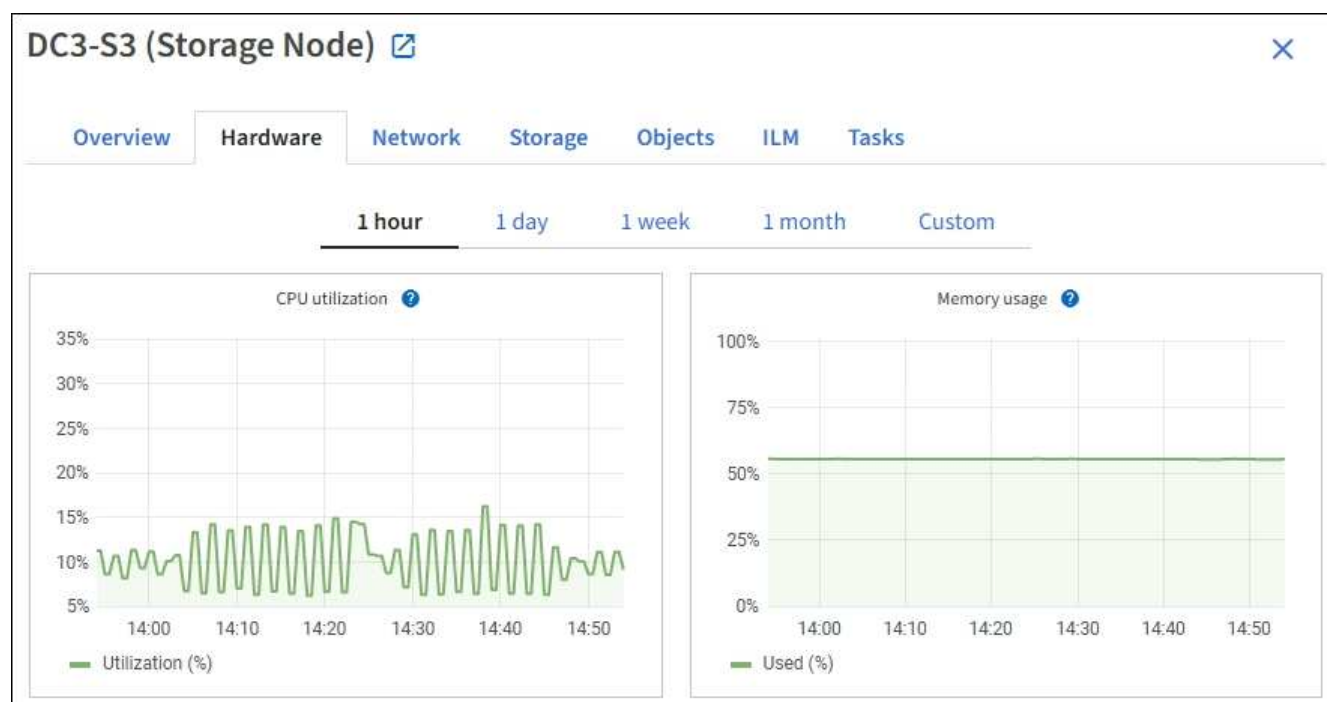
- ["查看"网络"选项卡"](#)
- ["监控节点连接状态"](#)

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

- 从*节点*页面中，选择节点。
- 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。

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

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

- (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。
- 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。
- (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	1100000000	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。

- 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。

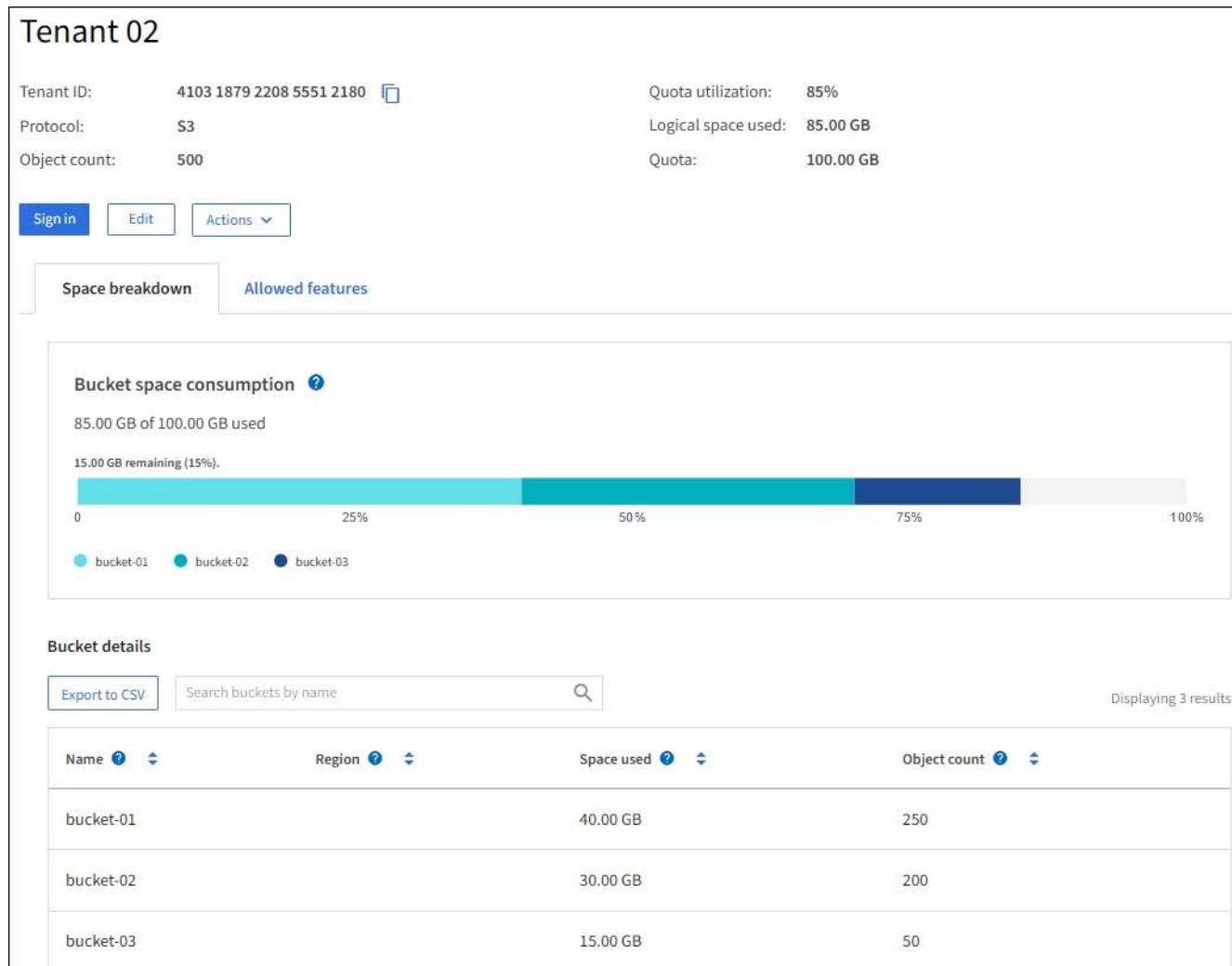
查看特定租户

您可以查看特定租户的详细信息。

步骤

- 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。



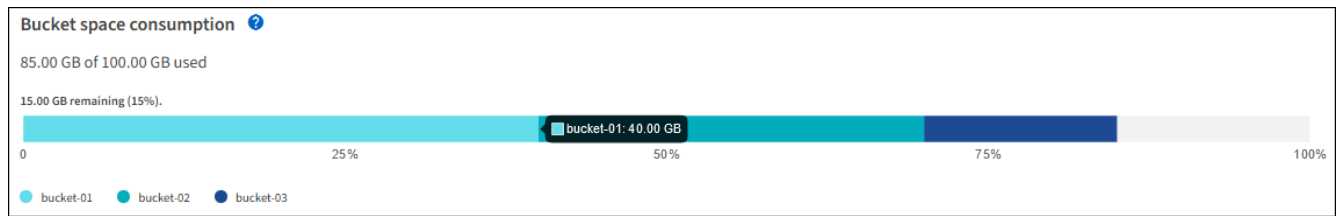
属于此租户的所有对象的逻辑大小包括不完整和正在进行的多部分上传。此大小不包括用于 ILM 策略的额外物理空间。空间使用值为估算值。这些估算值受摄取时间、网络连接和节点状态的影响。

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 客户端使用负载均衡器服务进行连接，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 ["负载均衡器选项卡"](#)。
- 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 网络联合连接

您可以监控有关所有["网络联合连接"](#)的基本信息、有关特定连接的详细信息，或有关跨网络复制操作的 Prometheus 指标。您可以从任一网络监控连接。

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络联合连接以及允许使用网络联合连接的所有租户帐户的基本信息。

步骤

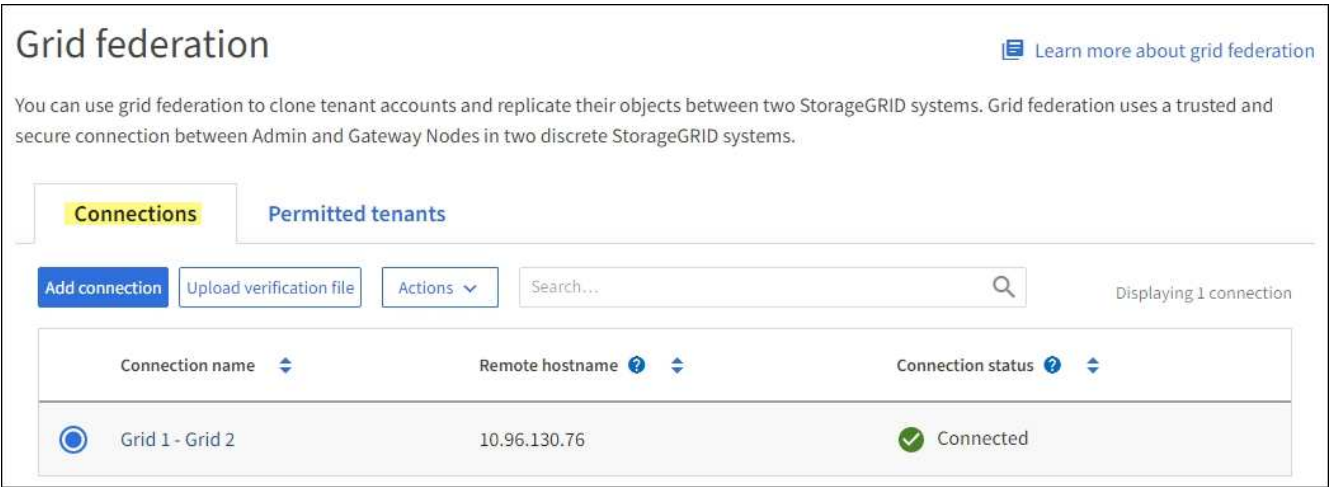
1. 选择*配置* > 系统 > 网络联合。

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：

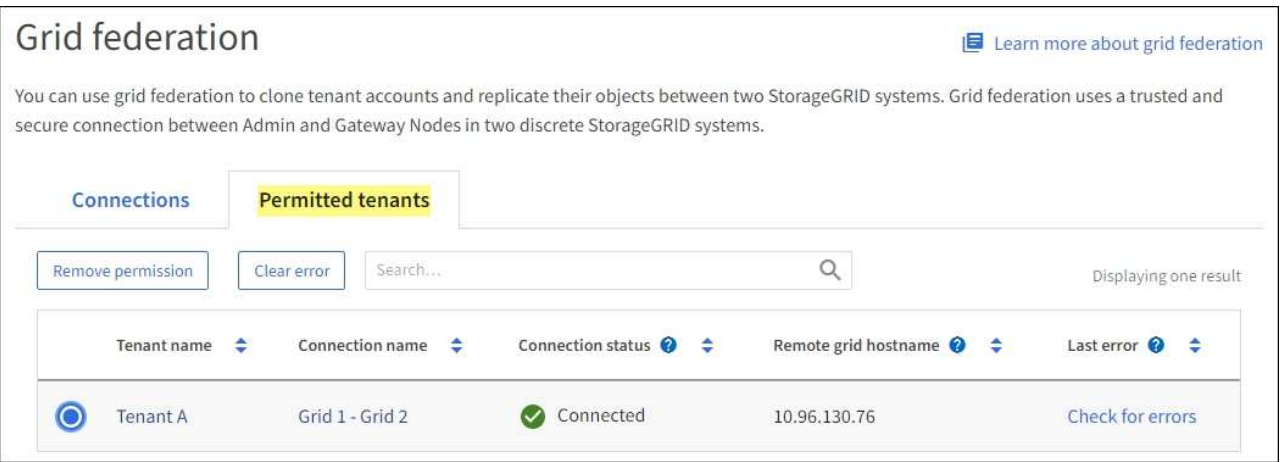
- "创建新连接"。
- 选择与 "编辑或测试" 的现有连接。



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。

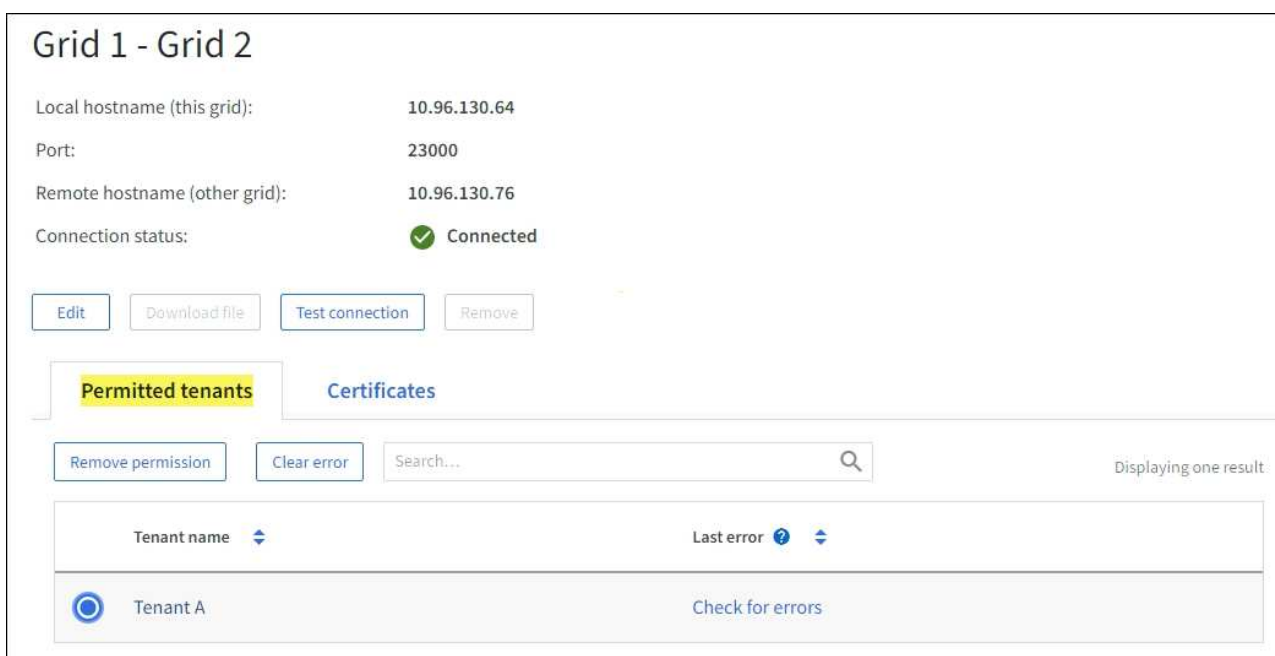
在连接的详细信息页面中，您可以：

- 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。

Grid A-Grid B

Local hostname (this grid): 10.96.106.230

Port: 23000

Remote hostname (other grid): 10.96.104.230

Connection status: ✔ Connected

[Edit](#)
[Download file](#)
[Test connection](#)
[Remove](#)

[Permitted tenants](#)
[Certificates](#)

[Rotate certificates](#)

[Server](#)
[Client](#)

[Download certificate](#)
[Copy certificate PEM](#)

Metadata ?

Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230

Serial number: 30:81:B8:DD:AE:B2:86:0A

Issuer DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT

Issued on: 2022-10-04T02:21:18.000Z

Expires on: 2024-10-03T19:05:13.000Z

SHA-1 fingerprint: 92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF

SHA-256 fingerprint: 54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60

Alternative names: IP Address:10.96.106.230

Certificate PEM ?

```
-----BEGIN CERTIFICATE-----
MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE
BhMCVVMxEzARBgNVBAGMCkNhbg1mb3JuaWExEjAQBgNVBACMCVN1bm55dmFsZTEU
NDAwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQwMDQw
-----
```

查看跨网络复制指标

您可以使用 Grafana 中的跨网络复制仪表板查看有关网络上跨网络复制操作的 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*跨网络复制*。

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 操作期间可能發生的问题。

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。

Alert rules define which conditions trigger specific alerts.

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

+ Create custom rule ✎ Edit rule ✕ Remove custom rule			
Name	Conditions	Type	Status
Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled
Displaying 62 alert rules.			

2. 查看警报规则表中的信息：

列标头	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级别的条件。 - 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。

Create Custom Rule

Enabled

☒

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

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

Duration

5

minutes

Cancel

Save

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：

64

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。

- 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。

- 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。

- 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。

Edit Rule - Low installed node memory

Enabled

☒

Unique Name

Low installed node memory

Description

The amount of installed memory on a node is low.

Recommended Actions (optional)

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Conditions ?

Minor

Major

node_memory_MemTotal_bytes < 24000000000

Critical

node_memory_MemTotal_bytes <= 12000000000

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

Duration

2

minutes

Cancel

Save

4. 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。



如果要已将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。

Conditions ?

Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 14000000000



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。

您可以使用网络管理器中的 ***配置* > 监控 > *SNMP 代理*** 选项或网络管理 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"](#) 登录到网络管理器。
- 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：

NetApp StorageGRID

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node

Site

Severity

Time triggered

Job

Service

DC1-S1-226

DC1 225-230

Minor

Fri Jun 28 14:43:27 UTC 2019

storagegrid

ldr

4

DC1-S2-227

Node

Site

Severity

Time triggered

Job

Service

DC1-S2-227

DC1 225-230

Minor

Fri Jun 28 14:43:27 UTC 2019

storagegrid

ldr

5

Sent from: DC1-ADM1-225

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"](#) 登录到网络管理器。

- 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。

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create

✎ Edit

✕ Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. 选择 **Create**。

此时将显示"创建静音"对话框。

Create Silence

Alert Rule

Description (optional)

Duration

Minutes

Severity

☐ Minor only

☐ Minor, major

☐ Minor, major, critical

Nodes

☐ StorageGRID Deployment

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

Cancel

Save

3. 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	- 选择*Alerts* > Silences。 - 从表格中，选择要编辑的静音对应的单选按钮。 - 选择*编辑*。 - 更改描述、剩余时间、所选严重性或受影响的节点。 - 选择 Save。
删除静默	- 选择*Alerts* > Silences。 - 从表中选择要删除的静音的单选按钮。 - 选择 Remove。 - 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。

警报名称	问题描述
设备计算控制器电源 A 出现问题	计算控制器中的电源 A 出现问题。
设备计算控制器电源 B 出现问题	计算控制器中的电源 B 出现问题。
设备计算硬件监视器服务已停止	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。

警报名称	问题描述
设备存储控制器 B 故障	StorageGRID 设备中的存储控制器 B 出现故障。
设备存储控制器驱动器故障	StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳状态。
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。
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。
负载均衡器端点证书过期	一个或多个负载均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。

警报名称	问题描述
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。

警报名称	问题描述
<code>\${post_edited_translations.segment}</code>	此站点不存在密钥管理服务器。
<code>\${post_edited_translations.segment}</code>	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。

警报名称	问题描述
根磁盘容量不足	根磁盘上的可用空间不足。
系统数据容量低	/var/local 的可用空间不足。如果此情况未得到解决，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。

警报名称	问题描述
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。
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。

警报名称	问题描述
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。

警报名称	问题描述
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。

租户警报

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(<code>bycast.log</code>) 和 <code>`servermanager`</code> 日志。
grid.json	跨所有节点共享的网格配置文件。此外， <code>`node.json`</code> 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。

归档位置	问题描述
miscd	Miscd 访问和错误日志。
mysql	MariaDB 数据库配置和相关日志。
网络	由与网络相关的脚本和 Dynip 服务生成的日志。
nginx	负载均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）。

归档位置	问题描述
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。
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。



如果要將日志发送到外部 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
<code>/var/local/log/bycast.log</code>	主要 StorageGRID 故障排除文件。	所有节点
<code>/var/local/log/bycast-err.log</code>	包含 <code>`bycast.log`</code> 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
<code>/var/local/core/</code>	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 <code>`/var/local/core/kexec_cmd`</code> 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
/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白。	管理节点

文件名	说明	发现于
/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白。	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

文件名	说明	发现于
/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
/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

文件名	说明	发现于
/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
/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	包含负载均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 流量的负载均衡。	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

文件名	说明	发现于
/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

消息段	示例中的值
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.uuuuuuu)
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

错误代码	含义
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
SUNV	服务不可用

下表列出了 `broadcast.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

错误编号	错误代码	含义
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
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

错误编号	错误代码	含义
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	无可用的记录锁定
038	ENOSYS	功能未实现
039	ENOTEMPTY	目录不为空
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

错误编号	错误代码	含义
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
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

错误编号	错误代码	含义
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	
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

错误编号	错误代码	含义
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
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		

错误编号	错误代码	含义
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
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 $0 \leq P \leq 1$ （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
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 $0 \leq P \leq 1$ （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 $0 \leq P \leq 1$ （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。

审核级别	问题描述
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。



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"网络管理 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 **Facility**，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）

工具	问题描述
11	FTP
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，网络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 <code>/var/local/log/localaudit.log</code> 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 文件通常为空白或缺失。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

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

选择租户和存储桶

- 从下拉列表中选择租户名称。
- 从下拉菜单中选择一个存储桶。
- 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。



如果您想在网络节点上下载 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。
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"](#) 登录到网络管理器。
- 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-adml:~ # 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-adml:~ # 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。

对象名称	对象ID (OID)	类型	访问	MIB 模块	问题描述
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。
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。

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- 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。

Erasure coding verification		
Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

选择属性名称旁边的问号 ? 以显示帮助文本。

- 查看对象存在性检查作业的结果：
 - 选择*维护* > 对象存在性检查 > 作业历史记录。
 - 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。

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job
Job history

Delete

☐	Job ID ?	Status ?	Nodes (volumes) ?	Missing object copies detected ?
☐	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
☐	12538643155010477372	Completed	DC1-S3 (1 volume)	0
☐	5490044849774982476	Completed	DC1-S2 (1 volume)	0
☐	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0

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。
- 网络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络管理器。
- 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时间和日期范围。

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：

Metrics

Access charts and metrics to help troubleshoot issues.

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

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time. Access the Prometheus interface using the link below. You must be signed in to the Grid Manager.

[https://](#)

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values. Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	Cloud Storage Pool Overview	Platform Services Processing
Account Service Overview	Decommission	Replicated Read Path Overview
Alertmanager	Erasure Coding - ADE	S3 - Node
Appliance Hardware Status	Erasure Coding - Overview	S3 Control
Audit Overview	Grid	S3 Overview
Bucket Cache	ILM	S3 Select
Cache Service	Identity Service Overview	Site
Cassandra Cluster Overview	Ingests	Support
Cassandra Network Overview	Node	SSD - Warranty
Cassandra Node Overview	Node (Internal Use)	Traces
Cassandra Table Cleanup	Object Chunk Leak Overview	Traffic Classification Policy
Chunk - Operations Overview	Object Serialization Mapping	Usage Processing
Chunk - Filesystem Latency Overview	OSL - AsyncIO	Virtual Memory (vmstat)
Chunk - Filesystem Latency Details	Platform Services Commits	
Cross Grid Replication	Platform Services Overview	

- 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。

- 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。

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.


Caution
0


Attention
1

Run Diagnostics

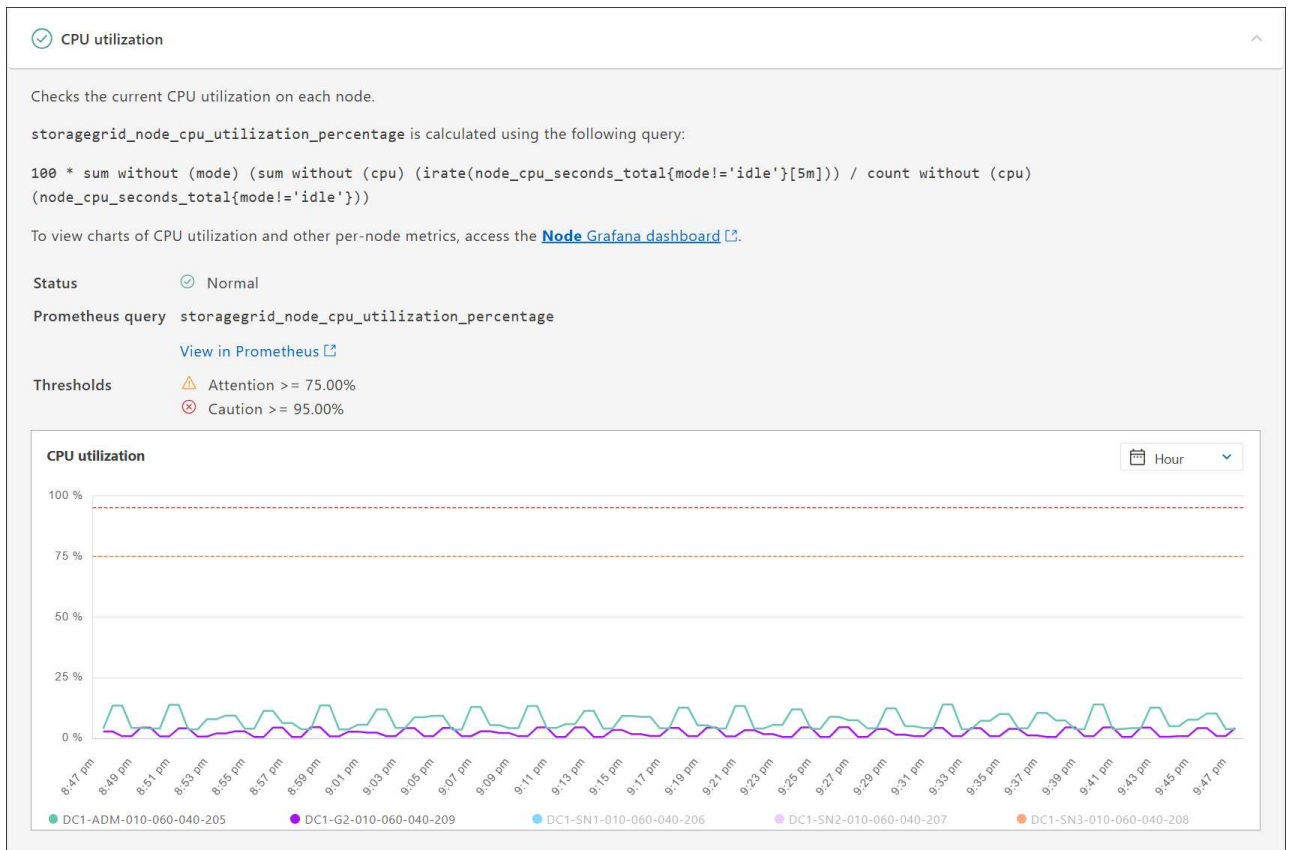
 Node uptime	▼
 Alert silences	▼
 Appliance hardware component temperatures	▼
 Cassandra automatic restarts	▼

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。

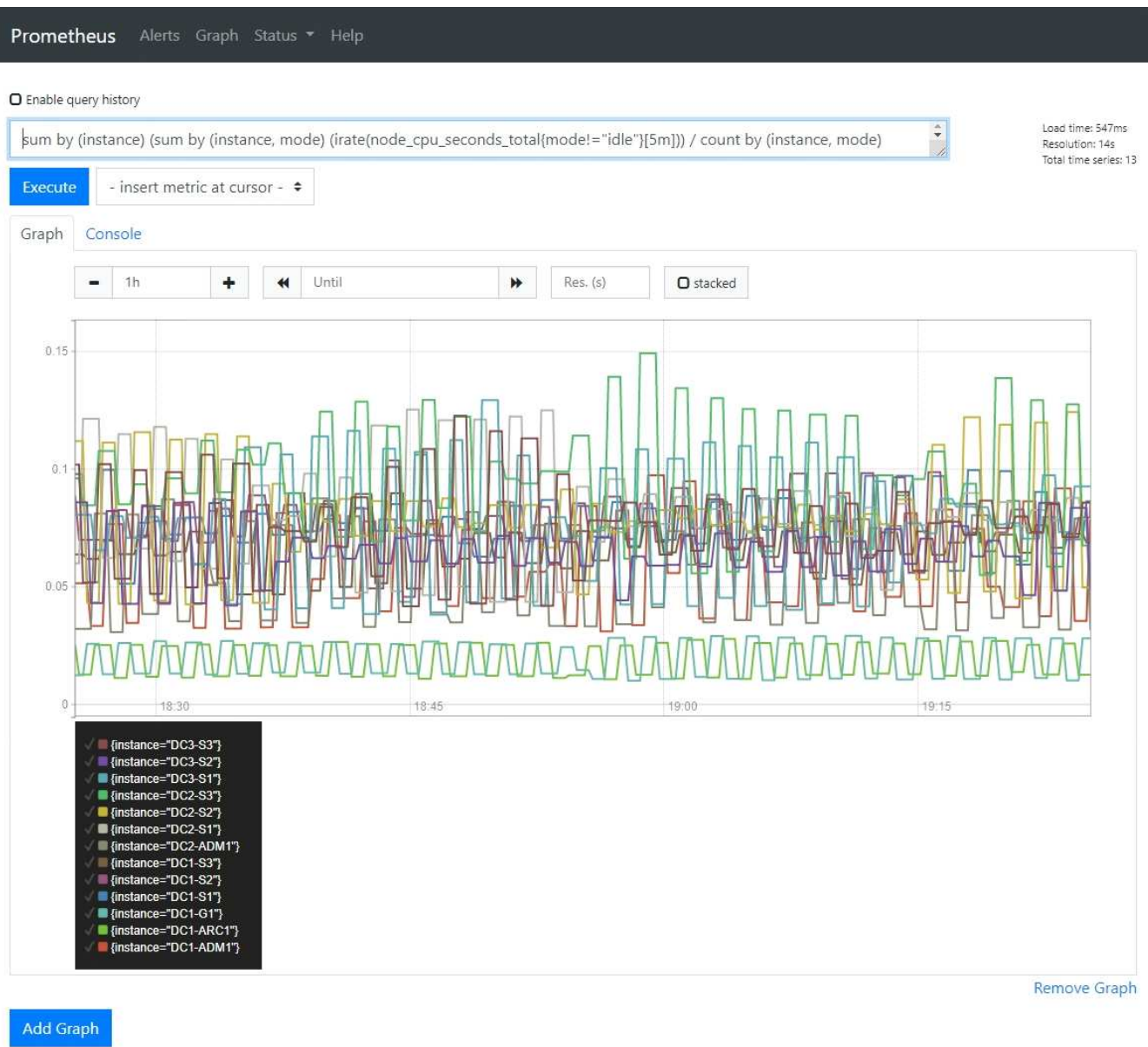


您还可以从*支持* > 工具 > *指标*页面的 Grafana 部分访问预构建的 Grafana 仪表板。



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

您可以使用网络管理 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络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，则可以使用网络管理 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**。

GET

/grid/metric-labels/{label}/values Lists the values for a metric label



GET

/grid/metric-names Lists all available metric names



GET

/grid/metric-query Performs an instant metric query at a single point in time



GET

/grid/metric-query-range Performs a metric query over a range of time



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。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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